aws

Guide de l’utilisateur

Amazon Elastic Compute Cloud

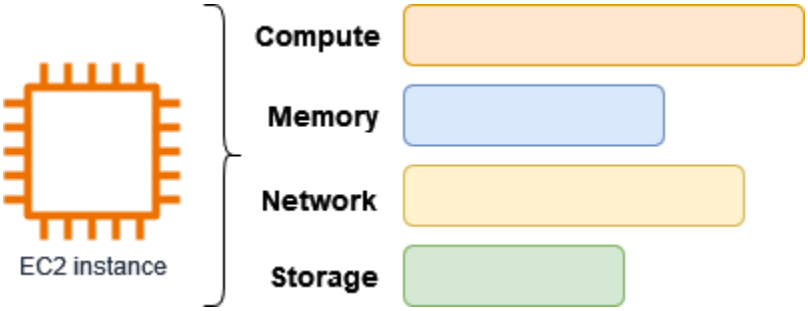
Amazon Elastic Compute Cloud: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'Amazon EC2 ?

Amazon Elastic Compute Cloud (AmazonEC2) fournit une capacité de calcul évolutive à la demande dans le cloud Amazon Web Services (AWS). L'utilisation d'Amazon EC2 réduit les coûts matériels afin que vous puissiez développer et déployer des applications plus rapidement. Vous pouvez utiliser Amazon EC2 pour lancer autant ou aussi peu de serveurs virtuels que nécessaire, configurer la sécurité et le réseau, et gérer le stockage. Vous pouvez ajouter de la capacité (augmenter) pour gérer les tâches lourdes en termes de calcul, telles que les processus mensuels ou annuels, ou les pics de trafic sur les sites web. Lorsque l'utilisation diminue, vous pouvez de nouveau restreindre la capacité (réduire).

Une EC2 instance est un serveur virtuel dans le AWS Cloud. Lorsque vous lancez une EC2 instance, le type d'instance que vous spécifiez détermine le matériel disponible pour votre instance. Chaque type d'instance offre un équilibre différent entre les ressources de calcul, de mémoire, de réseau et de stockage. Pour plus d'informations, consultez le guide des types d'EC2instances Amazon.



Caractéristiques d'Amazon EC2

Amazon EC2 propose les fonctionnalités de haut niveau suivantes :

instances

Serveurs virtuels.

Images de machines Amazon (AMIs)

Modèles préconfigurés pour vos instances qui regroupent les packages des composants dont vous avez besoin pour votre serveur (y compris le système d'exploitation et les logiciels supplémentaires).

Types d'instances

Différentes configurations de mémoireCPU, de stockage, de capacité réseau et de matériel graphique pour vos instances.

EBSVolumes Amazon

Volumes de stockage persistants pour vos données à l'aide d'Amazon Elastic Block Store (AmazonEBS).

Volumes de stockage d'instances

Volumes de stockage pour les données temporaires qui sont supprimées lorsque vous arrêtez, mettez en veille prolongée ou résiliez votre instance.

Paires de clés

Informations de connexion sécurisées pour vos instances. AWS stocke la clé publique et vous stockez la clé privée dans un endroit sécurisé.

Groupes de sécurité

Un pare-feu virtuel qui vous permet de spécifier les protocoles, les ports et les plages d'adresses IP source qui peuvent atteindre vos instances, ainsi que les plages d'adresses IP de destination auxquelles vos instances peuvent se connecter.

Amazon EC2 prend en charge le traitement, le stockage et la transmission des données de carte de crédit par un commerçant ou un fournisseur de services, et sa conformité à la norme de sécurité des données du secteur des cartes de paiement (PCI) a été validée (DSS). Pour plus d'informations PCIDSS, notamment sur la manière de demander une copie du Package de AWS PCI conformité, consultez le PCIDSSniveau 1.

Services connexes

Services à utiliser avec Amazon EC2

Vous pouvez en utiliser d'autres services AWS avec les instances que vous déployez à l'aide d'AmazonEC2.

Amazon EC2 Auto Scaling

Permet de garantir que vous disposez du nombre correct d'EC2instances Amazon disponibles pour gérer la charge de votre application.

AWS Backup

Automatisez la sauvegarde de vos EC2 instances Amazon et des EBS volumes Amazon qui y sont associés.

Amazon CloudWatch

Surveillez vos instances et vos EBS volumes Amazon.

Elastic Load Balancing

Répartissez automatiquement le trafic applicatif entrant sur plusieurs instances.

Amazon GuardDuty

Détectez les utilisations potentiellement non autorisées ou malveillantes de vos EC2 instances.

EC2 Image Builder

Automatisez la création, la gestion et le déploiement d'images personnalisées, sécurisées et de up-to-date serveur.

AWS Launch Wizard

Dimensionnez, configurez et déployez des AWS ressources pour des applications tierces sans avoir à identifier et à provisionner manuellement AWS des ressources individuelles.

AWS Systems Manager

Effectuez des opérations à grande échelle sur EC2 les instances grâce à cette solution end-to-end de gestion sécurisée.

Services informatiques supplémentaires

Vous pouvez lancer des instances à l'aide d'un autre service de AWS calcul au lieu d'AmazonEC2.

Amazon Lightsail

Créez des sites Web ou des applications Web à l'aide d'Amazon Lightsail, une plateforme cloud qui fournit les ressources dont vous avez besoin pour déployer rapidement votre projet, à un prix mensuel bas et prévisible. Pour comparer Amazon EC2 et Lightsail, consultez Amazon Lightsail ou Amazon. EC2

Amazon Elastic Container Service (AmazonECS)

Déployez, gérez et dimensionnez des applications conteneurisées sur un cluster d'EC2instances. Pour plus d'informations, consultez la section Choix d'un service de AWS conteneur.

Amazon Elastic Kubernetes Service (Amazon) EKS

Exécutez vos applications Kubernetes sur AWS. Pour plus d'informations, consultez la section Choix d'un service de AWS conteneur.

Accédez à Amazon EC2

Vous pouvez créer et gérer vos EC2 instances Amazon à l'aide des interfaces suivantes :

EC2Console Amazon

Une interface Web simple pour créer et gérer des EC2 instances et des ressources Amazon. Si vous avez créé un AWS compte, vous pouvez accéder à la EC2 console Amazon en vous connectant à la page d'accueil de la console AWS Management Console et en la sélectionnant sur la page EC2d'accueil de la console.

AWS Command Line Interface

Vous permet d'interagir avec les AWS services à l'aide des commandes de votre interface de ligne de commande. Elle est prise en charge sur Windows, Mac et Linux. Pour plus d'informations sur l' AWS CLI , consultez le Guide de l'utilisateur AWS Command Line Interface. Vous trouverez les EC2 commandes Amazon dans la référence des AWS CLI commandes.

AWS CloudFormation

Amazon EC2 prend en charge la création de ressources à l'aide de AWS CloudFormation. Vous créez un modèle, au YAML format JSON ou au format, qui décrit vos AWS ressources, et AWS CloudFormation qui fournit et configure ces ressources pour vous. Vous pouvez réutiliser vos CloudFormation modèles pour fournir les mêmes ressources plusieurs fois, que ce soit dans la même région et le même compte ou dans plusieurs régions et comptes. Pour plus d'informations sur les types de ressources et les propriétés pris en charge par AmazonEC2, consultez la référence aux types de EC2 ressources dans le guide de AWS CloudFormation l'utilisateur.

AWS SDKs

Si vous préférez créer des applications en utilisant un langage spécifique APIs au lieu de soumettre une demandeHTTPS, HTTP ou si vous fournissez AWS des bibliothèques, des exemples de code, des didacticiels et d'autres ressources aux développeurs de logiciels. Ces bibliothèques offrent des fonctions de base qui automatisent les tâches telles que la signature cryptographique des demandes, les nouvelles tentatives de demande et la gestion des réponses

d'erreur. Vous pouvez ainsi démarrer plus facilement. Pour en savoir plus, consultez la section Outils pour créer sur AWS.

AWS Tools for PowerShell

Un ensemble de PowerShell modules basés sur les fonctionnalités exposées par le AWS SDK for .NET. Les outils vous PowerShell permettent de scripter des opérations sur vos AWS ressources à partir de la ligne de PowerShell commande. Consultez le AWS Tools for Windows PowerShell Guide de l'utilisateur pour démarrer. Vous trouverez les applets de commande pour Amazon dans la référence EC2 des AWS Tools for PowerShell applets de commande.

Requête API

Amazon EC2 fournit une requêteAPI. Ces demandes sont des HTTP HTTPS requêtes qui utilisent les HTTP verbes GET ou un paramètre POST de requête nomméAction. Pour plus d'informations sur les API actions pour AmazonEC2, consultez la section Actions du manuel Amazon EC2 API Reference.

Tarification pour Amazon EC2

Amazon EC2 propose les options tarifaires suivantes :

Offre gratuite

Vous pouvez commencer à utiliser Amazon EC2 gratuitement. Pour découvrir les options du niveau gratuit, consultez Niveau gratuit d'AWS.

On-Demand instances

Payez les instances que vous utilisez à la seconde, avec un minimum de 60 secondes, sans engagement à long terme ou paiement initial.

Savings Plans

Vous pouvez réduire vos EC2 coûts Amazon en vous engageant à utiliser régulièrement, USD par heure, pour une durée de 1 ou 3 ans.

Instances réservées

Vous pouvez réduire vos EC2 coûts Amazon en vous engageant à utiliser une configuration d'instance spécifique, y compris le type d'instance et la région, pour une durée de 1 ou 3 ans.

Spot instances

Demandez EC2 des instances non utilisées, ce qui peut réduire considérablement vos EC2 coûts Amazon.

Hôtes dédiés

Réduisez les coûts en utilisant un EC2 serveur physique entièrement dédié à votre usage, que ce soit à la demande ou dans le cadre d'un Savings Plan. Vous pouvez utiliser vos licences logicielles existantes liées au serveur et obtenir de l'aide pour répondre aux exigences de conformité.

On-Demand Capacity Reservations

Réservez de la capacité de calcul pour vos EC2 instances dans une zone de disponibilité spécifique, quelle que soit la durée.

Facturation à la seconde

Supprime de votre facture le coût des minutes et des secondes inutilisées.

Pour obtenir la liste complète des frais et des prix pour Amazon EC2 et plus d'informations sur les modèles d'achat, consultez EC2les tarifs Amazon.

Estimations, facturation et optimisation des coûts

Pour créer des estimations pour vos cas AWS d'utilisation, utilisez le AWS Pricing Calculator.

Pour estimer le coût de la transformation des charges de travail Microsoft vers une architecture moderne utilisant des services open source et cloud natifs déployés AWS, utilisez le calculateur de AWS modernisation pour les charges de travail Microsoft.

Pour consulter votre facture, dirigez-vous vers le Tableau de bord de gestion des coûts et de la facturation dans la console AWS Billing and Cost Management. Votre facture contient des liens vers les rapports d'utilisation qui fournissent des détails sur votre facture. Pour en savoir plus sur la facturation des AWS comptes, consultez le guide de l'utilisateur AWS de Billing and Cost Management.

Si vous avez des questions concernant la AWS facturation, les comptes et les événements, contactez le AWS Support.

Pour calculer le coût d'un exemple d'environnement alloué, consultez le Centre d'optimisation des coûts du Cloud. Lorsque vous calculez le coût d'un environnement provisionné, n'oubliez pas d'inclure les coûts accessoires tels que le stockage des instantanés pour les EBS volumes.

Vous pouvez optimiser le coût, la sécurité et les performances de votre AWS environnement en utilisant AWS Trusted Advisor.

Vous pouvez l'utiliser AWS Cost Explorer pour analyser le coût et l'utilisation de vos EC2 instances. Vous pouvez consulter les données des 13 derniers mois et prévoir le montant que vous êtes susceptible de dépenser au cours des 12 prochains mois. Pour plus d'informations, consultez la section Analyse de vos coûts AWS Cost Explorer dans le guide de AWS Cost Management l'utilisateur.

Ressources

- EC2Fonctionnalités d'Amazon
- AWS Re : Publier
- AWS Générateur de compétences
- AWS Support
- Tutoriels pratiques
- Hébergement Web
- Windows activé AWS

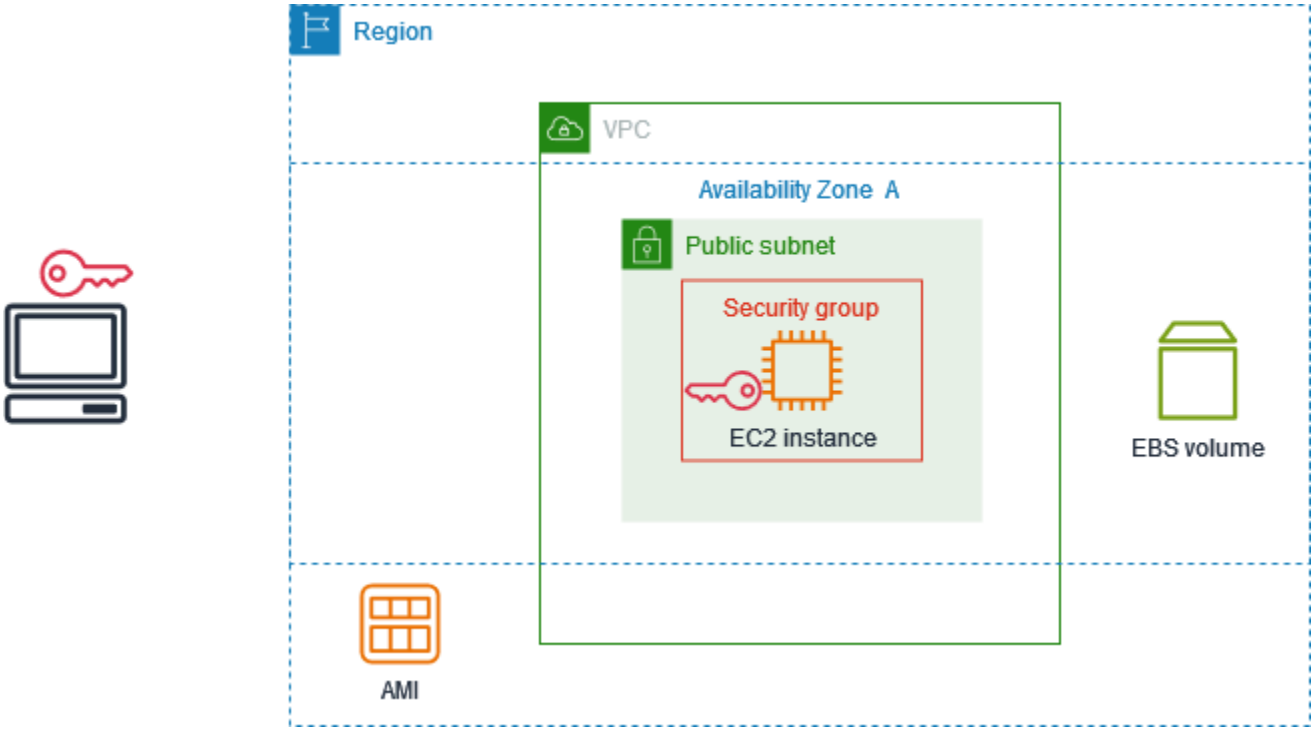
Commencez avec Amazon EC2

Utilisez ce didacticiel pour démarrer avec Amazon Elastic Compute Cloud (AmazonEC2). Vous allez apprendre à lancer une EC2 instance et à vous y connecter. Une instance est un serveur virtuel dans le AWS Cloud. Avec AmazonEC2, vous pouvez configurer le système d'exploitation et les applications qui s'exécutent sur votre instance.

Présentation

Le schéma suivant montre les principaux composants que vous allez utiliser dans ce didacticiel :

- Une image : modèle contenant le logiciel à exécuter sur votre instance, tel que le système d'exploitation.
- Une paire de clés : ensemble d'informations d'identification de sécurité que vous utilisez pour prouver votre identité lorsque vous vous connectez à votre instance. La clé publique se trouve sur votre instance et la clé privée sur votre ordinateur.
- Un réseau — Un cloud privé virtuel (VPC) est un réseau virtuel dédié à votre Compte AWS. Pour vous aider à démarrer rapidement, votre compte est doté d'une valeur par défaut VPC dans chaque zone de disponibilité Région AWS, et chaque valeur par défaut VPC possède un sous-réseau par défaut dans chaque zone de disponibilité.
- Un groupe de sécurité : agit comme un pare-feu virtuel pour contrôler le trafic entrant et sortant.
- Un EBS volume — Nous avons besoin d'un volume racine pour l'image. Vous pouvez éventuellement ajouter des volumes de données.



Coût de ce didacticiel

Lorsque vous vous inscrivez à AWS, vous pouvez commencer à EC2 utiliser Amazon en utilisant le Niveau gratuit d'AWS. Si vous avez créé le vôtre il y a Compte AWS moins de 12 mois et que vous n'avez pas encore dépassé les avantages du niveau gratuit pour AmazonEC2, suivre ce didacticiel ne vous coûtera rien, car nous vous aidons à sélectionner les options incluses dans les avantages du niveau gratuit. Dans le cas contraire, vous devrez payer les frais EC2 d'utilisation standard d'Amazon à partir du moment où vous lancerez l'instance et jusqu'à sa résiliation (dernière étape de ce didacticiel), même si elle reste inactive.

Pour obtenir des instructions permettant de déterminer si vous êtes éligible au niveau gratuit, consultezthe section called "Suivi de votre utilisation de l'offre gratuite ".

Tâches

- Étape 1 : Lancer une instance
- Étape 2 : Connexion à l'instance
- Étape 3 : Nettoyage de votre instance
- Étapes suivantes

Étape 1 : Lancer une instance

Vous pouvez lancer une EC2 instance à l'aide de la procédure AWS Management Console décrite dans la procédure suivante. Ce didacticiel a pour but de vous aider à lancer rapidement votre première instance. Il ne couvrira donc pas toutes les options possibles.

Pour lancer une instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation en haut de l'écran, nous affichons le courant Région AWS , par exemple l'Ohio. Vous pouvez utiliser la région sélectionnée ou éventuellement sélectionner une région plus proche de vous.
3. Dans le tableau de bord de la EC2 console, dans le volet Launch instance, choisissez Launch instance.
4. Sous Name and tags (Noms et identifications), pour Name (Nom), saisissez un nom descriptif pour votre instance.
5. Sous Application and OS Images (Amazon Machine Image) (Images d'application et de système d'exploitation [Amazon Machine Image]), procédez comme suit :

   a. Choisissez Quick Start, puis choisissez le système d'exploitation (OS) de votre instance. Pour votre première instance Linux, nous vous recommandons de choisir Amazon Linux.

   b. Dans Amazon Machine Image (AMI), sélectionnez un produit AMI marqué comme éligible au niveau gratuit.
6. Sous Type d'instance, dans Type d'instance **`t2.micro`**, choisissez laquelle est éligible au niveau gratuit. Dans les régions où `t2.micro` il n'est pas disponible, `t3.micro` est éligible au niveau gratuit.
7. Sous Paire de clés (connexion), pour Nom de la paire de clés, choisissez une paire de clés existante ou choisissez Créer une nouvelle paire de clés pour créer votre première paire de clés.

   > ⚠ Warning
   >
   > Si vous choisissez Proceed without a key pair (non recommandé), vous ne pourrez pas vous connecter à votre instance à l'aide des méthodes décrites dans ce didacticiel.
8. Sous Paramètres réseau, notez que nous avons sélectionné votre valeur par défautVPC, que nous avons sélectionné l'option permettant d'utiliser le sous-réseau par défaut dans une zone

de disponibilité que nous avons choisie pour vous et que nous avons configuré un groupe de sécurité avec une règle autorisant les connexions à votre instance depuis n'importe où. Pour votre première instance, nous vous recommandons d'utiliser les paramètres par défaut. Sinon, vous pouvez mettre à jour vos paramètres réseau comme suit :

- (Facultatif) Pour utiliser un sous-réseau par défaut spécifique, choisissez Modifier, puis choisissez un sous-réseau.
- (Facultatif) Pour en utiliser un autreVPC, choisissez Modifier, puis choisissez un existantVPC. Si le VPC n'est pas configuré pour un accès public à Internet, vous ne pourrez pas vous connecter à votre instance.
- (Facultatif) Pour restreindre le trafic de connexion entrant vers un réseau spécifique, choisissez Personnalisé au lieu de Anywhere, puis entrez le CIDR bloc correspondant à votre réseau.
- (Facultatif) Pour utiliser un autre groupe de sécurité, choisissez Sélectionner un groupe de sécurité existant, puis choisissez un groupe de sécurité existant. Si le groupe de sécurité n'a pas de règle autorisant le trafic de connexion depuis votre réseau, vous ne pourrez pas vous connecter à votre instance. Pour une instance Linux, vous devez autoriser SSH le trafic. Pour une instance Windows, vous devez autoriser RDP le trafic.

9. Sous Configurer le stockage, notez que nous avons configuré un volume racine mais aucun volume de données. Cela est suffisant à des fins de test.
10. Consultez un résumé de la configuration de votre instance dans le panneau Summary (Récapitulatif) et, lorsque vous êtes prêt, choisissez Launch instance (Lancer l'instance).
11. Si le lancement est réussi, choisissez l'ID de l'instance dans la notification de réussite pour ouvrir la page Instances et surveiller l'état du lancement.
12. Cochez la case correspondant à l'instance. L'état initial de l'instance est`pending`. Lorsque l'instance démarre, son statut passe à `running`. Choisissez l'onglet État et alarmes. Une fois que votre instance a passé ses vérifications d'état, elle est prête à recevoir des demandes de connexion.

Étape 2 : Connexion à l'instance

La procédure que vous utilisez dépend du système d'exploitation de l'instance. Si vous ne pouvez pas vous connecter à votre instance, consultez Résoudre les problèmes de connexion à votre instance Amazon EC2 Linux pour obtenir de l'aide.

Instances Linux

Vous pouvez vous connecter à votre instance Linux à l'aide de n'importe quel SSH client. Si vous utilisez Windows sur votre ordinateur, ouvrez un terminal et exécutez la `ssh` commande pour vérifier qu'un SSH client est installé. Si la commande est introuvable, installez Open SSH pour Windows.

Pour vous connecter à votre instance à l'aide de SSH

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance, puis choisissez Connecter.
4. Sur la page Connect to instance, sélectionnez l'onglet SSHclient.
5. (Facultatif) Si vous avez créé une paire de clés lorsque vous avez lancé l'instance et téléchargé la clé privée (fichier .pem) sur un ordinateur exécutant Linux ou macOS, exécutez l'exemple de chmod commande pour définir les autorisations associées à votre clé privée.
6. Copiez l'exemple de SSH commande. Voici un exemple, où *key-pair-name*.pem est le nom de votre fichier de clé privée, *ec2-user* est le nom d'utilisateur associé à l'image, et la chaîne après le symbole @ est le DNS nom public de l'instance.

   ```
   ssh -i key-pair-name.pem ec2-user@ec2-198-51-100-1.us-east-2.compute.amazonaws.com
   ```

7. Dans une fenêtre de terminal de votre ordinateur, exécutez la ssh commande que vous avez enregistrée à l'étape précédente. Si le fichier de clé privée ne se trouve pas dans le répertoire actuel, vous devez spécifier le chemin complet vers le fichier clé dans cette commande.

   Voici un exemple de réponse :

   ```
   The authenticity of host 'ec2-198-51-100-1.us-east-2.compute.amazonaws.com
    (198-51-100-1)' can't be established.
   ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
   Are you sure you want to continue connecting (yes/no)?
   ```

8. (Facultatif) Vérifiez que l'empreinte de l'alerte de sécurité correspond à l'empreinte de l'instance contenue dans la sortie de la console lorsque vous démarrez une instance pour la première fois. Pour obtenir le résultat de la console, choisissez Actions, Surveiller et dépanner, puis Obtenir le journal du système. Si les empreintes digitales ne correspondent pas, quelqu'un est peut-être en train de tenter une man-in-the-middle attaque. Si elles correspondent, passez à l'étape suivante.
9. Saisissez **`yes`**.

Voici un exemple de réponse :

```
Warning: Permanently added 'ec2-198-51-100-1.us-
east-2.compute.amazonaws.com' (ECDSA) to the list of known hosts.
```

instances Windows

Pour vous connecter à une instance Windows à l'aide deRDP, vous devez récupérer le mot de passe administrateur initial, puis saisir ce mot de passe lorsque vous vous connectez à votre instance. Il faut quelques minutes après le lancement de l'instance pour que ce mot de passe soit disponible.

Le nom d'utilisateur par défaut du compte administrateur dépend de la langue du système d'exploitation (OS) contenu dans leAMI. Pour déterminer le nom d'utilisateur correct, identifiez la langue AMI de votre système d'exploitation, puis choisissez le nom d'utilisateur correspondant. Par exemple, pour un système d'exploitation anglais, le nom d'utilisateur est`Administrator`, pour un système d'exploitation français, c'est le cas`Administrateur`, et pour un système d'exploitation portugais, c'est le cas`Administrador`. Si une version linguistique du système d'exploitation ne possède pas de nom d'utilisateur dans la même langue, choisissez-le`Administrator (Other)`. Pour plus d'informations, consultez la section Noms localisés du compte administrateur sous Windows sur le Microsoft TechNet Wiki.

Pour récupérer le mot de passe administrateur initial

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance, puis choisissez Connecter.
4. Sur la page Connect to instance, sélectionnez l'onglet RDPclient.
5. Dans Nom d'utilisateur, choisissez le nom d'utilisateur par défaut pour le compte administrateur. Le nom d'utilisateur que vous choisissez doit correspondre à la langue du système d'exploitation (OS) contenu dans celui AMI que vous avez utilisé pour lancer votre instance. S'il n'existe aucun nom d'utilisateur dans la même langue que votre système d'exploitation, choisissez Administrator (Other).
6. Choisissez Obtenir le mot de passe.
7. Sur la page Obtenir le mot de passe Windows, procédez comme suit :

a. Choisissez Télécharger le fichier de clé privée et accédez au fichier de clé privée (`.pem`) que vous avez spécifié lors du lancement de l'instance. Sélectionnez le fichier, puis choisissez Open (Ouvrir) pour copier tout le contenu du fichier dans cette page.

b. Choisissez Déchiffrer le mot de passe. La page Obtenir le mot de passe Windows se ferme et le mot de passe administrateur par défaut de l'instance apparaît sous Mot de passe, en remplacement du lien Obtenir le mot de passe affiché précédemment.

c. Copiez le mot de passe et enregistrez-le en lieu sûr. Vous en aurez besoin pour vous connecter à l'instance.

La procédure suivante utilise le client Remote Desktop Connection pour Windows (MSTSC). Si vous utilisez un autre RDP client, téléchargez le RDP fichier, puis consultez la documentation du RDP client pour connaître les étapes à suivre pour établir la RDP connexion.

Pour vous connecter à une instance Windows à l'aide d'un RDP client

1. Sur la page Connect to instance, choisissez Download remote desktop file. Lorsque le téléchargement du fichier est terminé, choisissez Annuler pour revenir à la page Instances. Le RDP fichier est téléchargé `Downloads` dans votre dossier.
2. Exécutez `mstsc.exe` pour ouvrir le RDP client.
3. Développez les options Afficher, choisissez Ouvrir, puis sélectionnez le fichier .rdp dans votre `Downloads` dossier.
4. Par défaut, Ordinateur est le IPv4 DNS nom public de l'instance et Nom d'utilisateur est le compte administrateur. Pour vous connecter à l'instance en utilisant IPv6 plutôt, remplacez le IPv4 DNS nom public de l'instance par son IPv6 adresse. Vérifiez les paramètres par défaut et modifiez-les si nécessaire.
5. Choisissez Se connecter. Si vous recevez un avertissement indiquant que l'éditeur de la connexion à distance est inconnu, choisissez Connect pour continuer.
6. Entrez le mot de passe que vous avez enregistré précédemment, puis cliquez sur OK.
7. En raison de la nature des certificat auto-signés, vous pouvez obtenir un avertissement indiquant que le certificat de sécurité ne peut pas être authentifié. Effectuez l'une des actions suivantes :
   - Si vous faites confiance au certificat, choisissez Oui pour vous connecter à votre instance.
   - [Windows] Avant de continuer, comparez l'empreinte numérique du certificat avec la valeur du journal système pour confirmer l'identité de l'ordinateur distant. Choisissez Afficher le certificat, puis sélectionnez Thumbprint dans l'onglet Détails. Comparez cette valeur à celle

de `RDPCERTIFICATE-THUMBPRINT` la section Actions, Surveillance et résolution des problèmes, Obtenir le journal du système.

- [Mac OS X] Avant de continuer, comparez l'empreinte digitale du certificat avec la valeur du journal système pour confirmer l'identité de l'ordinateur distant. Choisissez Afficher le certificat, développez les détails, puis choisissez SHA1Empreintes digitales. Comparez cette valeur à celle de `RDPCERTIFICATE-THUMBPRINT` la section Actions, Surveillance et résolution des problèmes, Obtenir le journal du système.

8. Si la RDP connexion est établie, le RDP client affiche l'écran de connexion Windows, puis le bureau Windows. Si vous recevez plutôt un message d'erreur, consultezthe section called "Le service Bureau à distance ne peut pas se connecter à l'ordinateur distant". Lorsque vous avez terminé la RDP connexion, vous pouvez fermer le RDP client.

Étape 3 : Nettoyage de votre instance

Une fois que vous avez fini avec l'instance que vous avez créée pour ce tutoriel, vous devez effectuer un nettoyage en mettant fin à l'instance. Si vous souhaitez exécuter d'autres opérations avec cette instance avant le nettoyage, consultez Étapes suivantes.

> **Important**
>
> Mettre fin à une instance la supprime ; vous ne pouvez pas vous reconnecter à une instance une fois que vous y avez mis fin.

Vous cesserez de payer des frais pour cette instance ou cette utilisation qui sont pris en compte dans les limites de votre niveau gratuit dès que le statut de l'instance deviendra ou. `shutting down` `terminated` Pour conserver votre instance pour plus tard, sans encourir de frais ou d'utilisation entrant en ligne de compte dans les limites du niveau gratuit, vous pouvez arrêter l'instance maintenant, puis la redémarrer ultérieurement. Pour de plus amples informations, veuillez consulter Arrêtez et démarrez les EC2 instances Amazon.

Pour mettre fin à une instance

1. Dans le panneau de navigation, choisissez Instances. Sélectionnez l'instance dans la liste des instances.
2. Choisissez État de l'instance, Résilier l'instance.
3. Choisissez Résilier lorsque vous êtes invité à confirmer.

Amazon EC2 arrête et met fin à votre instance. Après que votre instance a pris fin, elle reste visible sur la console pendant un court instant, puis l'entrée est supprimée automatiquement. Vous ne pouvez pas supprimer vous-même l'instance résiliée de l'affichage de la console.

Étapes suivantes

Après avoir démarré votre instance, vous souhaiterez peut-être explorer les étapes suivantes :

- Découvrez comment suivre votre utilisation d'Amazon EC2 Free Tier à l'aide de la console. Pour de plus amples informations, veuillez consulter the section called "Suivi de votre utilisation de l'offre gratuite ".
- Configurez une CloudWatch alarme pour vous avertir si votre utilisation dépasse le niveau gratuit. Pour plus d'informations, consultez la section Suivi de votre Niveau gratuit d'AWS utilisation dans le guide de AWS Billing l'utilisateur.
- Ajoutez un EBS volume. Pour plus d'informations, consultez la section Créer un EBS volume Amazon dans le guide de EBS l'utilisateur Amazon.
- Découvrez comment gérer votre EC2 instance à distance à l'aide de la Run commande. Pour plus d'informations, consultez AWS Systems Manager Run Command dans le AWS Systems Manager Guide de l'utilisateur.
- En savoir plus sur les options d'achat d'instances. Pour de plus amples informations, veuillez consulter Options EC2 de facturation et d'achat Amazon.
- Obtention de conseils sur les types d'instances Pour de plus amples informations, veuillez consulter Obtenez des recommandations depuis l'outil de recherche de types d'EC2instance.

Bonnes pratiques pour Amazon EC2

Pour tirer le meilleur parti d'AmazonEC2, nous vous recommandons de suivre les meilleures pratiques suivantes.

Sécurité

- Gérez l'accès aux AWS ressources et APIs utilisez la fédération d'identité avec un fournisseur d'identité et IAM des rôles dans la mesure du possible. Pour plus d'informations, consultez la section Création IAM de politiques dans le guide de IAM l'utilisateur.
- Implémentez les règles les moins permissives pour votre groupe de sécurité.
- Corrigez, mettez à jour et sécurisez régulièrement le système d'exploitation et les applications de votre instance. Pour plus d'informations, consultez Gestion des mises à jour. Pour les directives spécifiques aux systèmes d'exploitation Windows, voirBonnes pratiques de sécurité pour les instances Windows.
- Utilisez Amazon Inspector pour détecter et analyser automatiquement les EC2 instances Amazon afin de détecter les vulnérabilités logicielles et les risques d'exposition involontaire au réseau. Pour plus d'informations, consultez le Guide de l'utilisateur Amazon Inspector.
- Utilisez AWS Security Hub des contrôles pour surveiller vos EC2 ressources Amazon par rapport aux meilleures pratiques de sécurité et aux normes de sécurité. Pour plus d'informations sur l'utilisation de Security Hub, veuillez consulter la rubrique Contrôles Amazon Elastic Compute Cloud dans le Guide de l'utilisateur AWS Security Hub .

Stockage

- Maîtrisez les implications du type de périphérique racine pour la persistance, la sauvegarde et la récupération des données. Pour plus d'informations, consultez Root device type.
- Utilisez des EBS volumes Amazon distincts pour le système d'exploitation et pour vos données. Assurez-vous que le volume avec vos données persiste après la fin de l'instance. Pour plus d'informations, veuillez consulter Conservation des données lors de la résiliation d'une instance.
- Utilisez le stockage d'instance disponible pour que votre instance stocke les données temporaires. Souvenez-vous que les données stockées dans un stockage d'instance sont supprimées quand vous arrêtez, mettez en veille prolongée ou résiliez votre instance. Si vous utilisez le stockage d'instance pour le stockage de base de données, assurez-vous d'avoir un cluster avec un facteur de réplication qui garantit la tolérance aux pannes.

- Chiffrez les EBS volumes et les instantanés. Pour plus d'informations, consultez Amazon EBS Encryption dans le guide de EBS l'utilisateur Amazon.

Gestion des ressources

- Utilisez les métadonnées d'instances et les balises de ressource personnalisées pour suivre et identifier vos ressources AWS . Pour plus d'informations, consultez Utiliser les métadonnées de l'instance pour gérer votre EC2 instance et Marquez vos EC2 ressources Amazon.
- Consultez vos limites actuelles pour AmazonEC2. Prévoyez de demander les augmentations de limite avant le moment où vous en aurez besoin. Pour plus d'informations, consultez Quotas EC2 de service Amazon.
- Utilisez-le AWS Trusted Advisor pour inspecter votre AWS environnement, puis formuler des recommandations lorsque des opportunités se présentent pour économiser de l'argent, améliorer la disponibilité et les performances du système ou contribuer à combler les failles de sécurité. Pour plus d'informations, consultez AWS Trusted Advisor dans le Guide de l'utilisateur AWS Support .

Sauvegarde et restauration

- Sauvegardez régulièrement vos EBS volumes à l'aide de EBSsnapshots Amazon et créez une Amazon Machine Image (AMI) à partir de votre instance pour enregistrer la configuration en tant que modèle pour le lancement de futures instances. Pour plus d'informations sur AWS les services permettant de réaliser ce cas d'utilisation, consultez AWS BackupAmazon Data Lifecycle Manager.
- Déployez les composants critiques de votre application à travers plusieurs zones de disponibilité et répliquez vos données de manière appropriée.
- Concevez vos applications pour gérer l'adressage IP dynamique au redémarrage de votre instance. Pour plus d'informations, veuillez consulter Adressage IP de l'EC2instance Amazon.
- Surveillez les événements et répondez-y. Pour plus d'informations, veuillez consulter Surveillez les EC2 ressources Amazon.
- Vérifiez bien que vous êtes prêt à gérer le failover (basculement). Pour une solution de base, vous pouvez attacher manuellement une interface réseau ou une adresse IP Elastic à une instance de remplacement. Pour plus d'informations, consultez Interfaces réseau Elastic. Pour une solution automatisée, vous pouvez utiliser Amazon EC2 Auto Scaling. Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon EC2 Auto Scaling.
- Testez régulièrement le processus de restauration de vos instances et de vos EBS volumes Amazon pour vous assurer que les données et les services sont correctement restaurés.

Réseaux

- Définissez la valeur time-to-live (TTL) pour vos applications sur 255, pour IPv4 etIPv6. Si vous utilisez une valeur inférieure, elle risque d'expirer pendant que le TTL trafic de l'application est en transit, ce qui entraîne des problèmes d'accessibilité pour vos instances.

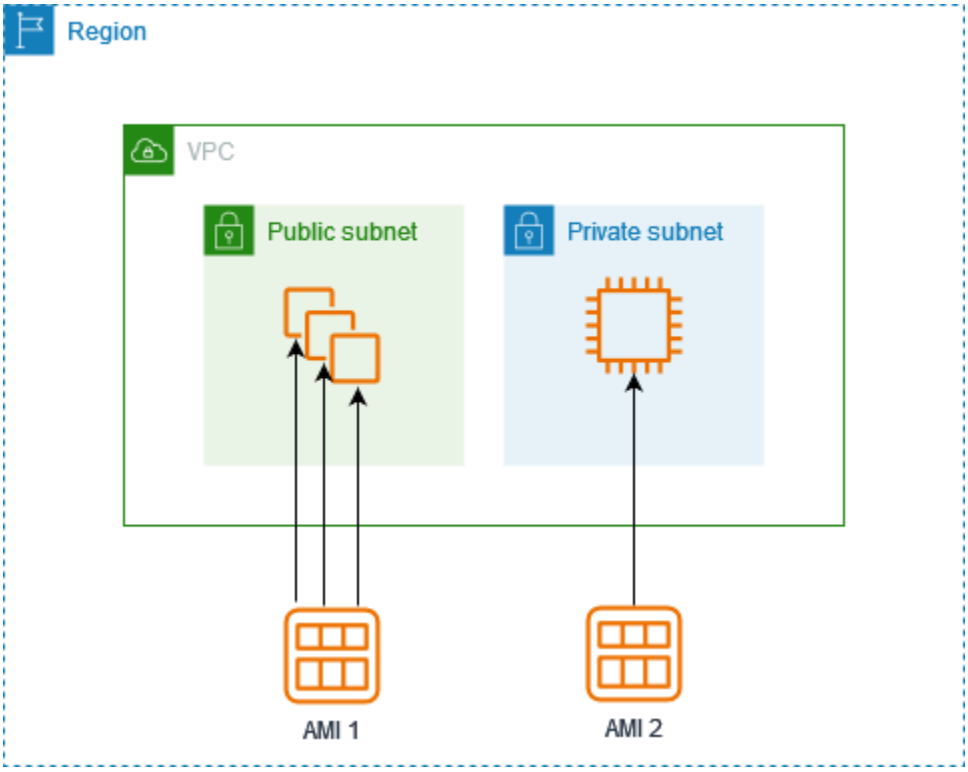
Amazon Machine Images sur Amazon EC2

Une Amazon Machine Image (AMI) est une image qui fournit le logiciel requis pour configurer et démarrer une EC2 instance Amazon. Chacun contient AMI également un mappage de périphériques en mode bloc qui spécifie les périphériques en mode bloc à associer aux instances que vous lancez. Vous devez spécifier un AMI moment où vous lancez une instance. Le AMI doit être compatible avec le type d'instance que vous avez choisi pour votre instance. Vous pouvez utiliser un produit AMI fourni par AWS, un publicAMI, un message AMI que quelqu'un d'autre a partagé avec vous, ou un produit AMI que vous avez acheté auprès d'eux AWS Marketplace.

An AMI est spécifique aux éléments suivants :

- Région
- Système d’exploitation
- Architecture du processeur
- Root device type
- Type de virtualisation

Vous pouvez lancer plusieurs instances à partir d'une seule instance AMI lorsque vous avez besoin de plusieurs instances avec la même configuration. Vous pouvez utiliser différents AMIs pour lancer des instances lorsque vous avez besoin d'instances avec des configurations différentes, comme le montre le schéma suivant.



Vous pouvez créer une instance AMI à partir de vos EC2 instances Amazon, puis l'utiliser pour lancer des instances avec la même configuration. Vous pouvez copier un AMI dans une autre AWS région, puis l'utiliser pour lancer des instances dans cette région. Vous pouvez également partager un compte AMI que vous avez créé avec d'autres comptes afin qu'ils puissent lancer des instances avec la même configuration. Vous pouvez vendre votre produit AMI en utilisant le AWS Marketplace.

Table des matières

AMItypes et caractéristiques sur Amazon EC2

Lorsque vous lancez une instance, celle AMI que vous choisissez doit être compatible avec le type d'instance que vous choisissez. Vous pouvez sélectionner celui AMI à utiliser en fonction des caractéristiques suivantes :

- Région
- Système d'exploitation
- Architecture du processeur
- Autorisations de lancement
- Root device type
- Types de virtualisation

Autorisations de lancement

Le propriétaire d'un AMI détermine sa disponibilité en spécifiant les autorisations de lancement. Les autorisations de lancement sont réparties en plusieurs catégories.

Autorisation de lancement	Description
public	Le propriétaire accorde des autorisations de lancement à tous les AWS comptes.
explicite	Le propriétaire accorde des autorisations de lancement à AWS des comptes, organisations ou unités organisationnelles spécifiques (OUs).
implicite	Le propriétaire dispose d'autorisations de lancement implicites pour unAMI.

Amazon et la EC2 communauté Amazon proposent un large choix de publicsAMIs. Pour de plus amples informations, veuillez consulter Comprendre AMI l'utilisation partagée sur Amazon EC2. Les développeurs peuvent facturer leurAMIs. Pour de plus amples informations, veuillez consulter AMIsPayé dans le AWS Marketplace cadre des EC2 instances Amazon.

Root device type

Tous AMIs sont classés comme étant soutenus par Amazon EBS ou soutenus par un magasin d'instances.

- EBSSauvegardé par Amazon AMI — Le périphérique racine d'une instance lancée depuis le AMI est un volume Amazon Elastic Block Store (AmazonEBS) créé à partir d'un EBS instantané Amazon. Compatible avec Linux et WindowsAMIs.
- Sauvegardé par une instance Amazon AMI : le périphérique racine d'une instance lancée depuis le AMI est un volume de stockage d'instance créé à partir d'un modèle stocké dans Amazon S3. Pris en charge AMIs uniquement pour Linux. Windows AMIs ne prend pas en charge le stockage d'instance pour le périphérique racine.

Pour de plus amples informations, veuillez consulter Volumes root pour vos EC2 instances Amazon.

Le tableau suivant résume les différences importantes entre les deux types deAMIs.

Caractéristiques	Soutenu EBS par Amazon AMI	Sauvegardé par une instance Amazon AMI
volume du périphéri que racine	EBSvolume	Volume de stockage d'instance
Temps de démarrage pour une instance	Généralement inférieur à 1 minute	Généralement inférieur à 5 minutes
Persistance des données	Par défaut, le volume racine est supprimé lorsque l'instanc e se termine.* Par défaut, les données de tous les autres EBS volumes sont conservées après la fermeture de l'instance.	Les données des volumes de stockage d'instances sont conservées uniquement pendant la durée de vie de l'instance.
État d'arrêt	Peut être à l'état arrêté. Même lorsque l'instance est arrêtée et ne	Ne peut pas être dans un état arrêté, les instances sont en cours d'exécution ou hors service

Caractéristiques	Soutenu EBS par Amazon AMI	Sauvegardé par une instance Amazon AMI
	fonctionne pas, le volume racine est conservé dans Amazon EBS	
Modifications	Le type d'instance, le noyau, RAM le disque et les données utilisateur peuvent être modifiés lorsque l'instance est arrêtée.	Les attributs de l'instance restent les mêmes pendant la durée de vie de l'instance.
Frais	Vous êtes facturé pour l'utilisation de l'instance, l'utilisation EBS du volume et le stockage de vos AMI données sous forme d'EBSinstantané.	L'utilisation de l'instance et le stockage de celle-ci AMI dans Amazon S3 vous sont facturés.
AMIcréation/regroupement	Utilise une seule commande/un seul appel	Nécessite l'installation et l'utilisation d'AMIoutils

* Par défautEBS, l'`DeleteOnTermination`indicateur est défini sur`true`. Pour plus d'informations sur la modification de cet indicateur afin que le volume soit conservé après la mise hors service, consultez Conserver un volume EBS racine Amazon après la résiliation d'une EC2 instance Amazon.

** Compatible uniquement avec `io2` EBS Block Express. Pour plus d'informations, consultez la section sur les volumes IOPS SSD Block Express provisionnés dans le guide de EBS l'utilisateur Amazon.

Déterminez le type de périphérique racine de votre AMI

Le volume AMI que vous utilisez pour lancer une EC2 instance détermine le type du volume racine. Le volume racine d'une EC2 instance est soit un EBS volume, soit un volume de stockage d'instance. Les types d'instances de la génération actuelle ne prennent en charge que les volumes EBS racine. Les seuls types d'instance qui prennent en charge les volumes racine de stockage d'instance sont C1, C3, D2, I2, M1, M2, M3, R3 et X1.

Pour déterminer le type de périphérique racine d'un utilisateur AMI utilisant la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez AMIs, puis sélectionnez leAMI.
3. Vérifiez la valeur de Root Device Type (Type de périphérique racine) sous l'onglet Details (Détails) comme suit :
   - `ebs`— Ceci est EBS soutenu par AMI un.
   - `instance store`— Il s'agit d'une instance sauvegardée en magasinAMI.

Pour déterminer le type de périphérique racine d'un à AMI l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes.

- describe-images (AWS CLI)
- Get-EC2Image (AWS Tools for Windows PowerShell)

Types de virtualisation

Amazon Machine Images utilise l'un des deux types de virtualisation suivants : machine virtuelle paravirtuelle (PV) ou machine virtuelle matérielle (HVM). Les principales différences entre les systèmes photovoltaïques HVM AMIs sont la manière dont ils démarrent et la possibilité de tirer parti d'extensions matérielles spéciales (CPUréseau et stockage) pour de meilleures performances. AMIsLes fenêtres le sont HVMAMIs.

Le tableau suivant compare avec HVM PVAMIs.

Caractéristiques	HVM	Virtualisation paravirtuelle
Description	HVMAMIssont présentés avec un ensemble de matériel entièrement virtualisé et démarrent en exécutant l'enregistrement de démarrage principal du périphérique root de votre image. Ce type de virtualisation permet d'exécute	AMIsDémarrez le PV avec un chargeur de démarrage spécial appelé PV-GRUB, qui démarre le cycle de démarrage puis charge en chaîne le noyau spécifié dans le `menu.lst` fichier sur votre image. Les invités de virtualis

Caractéristiques	HVM	Virtualisation paravirtuelle
	r un système d'exploitation directement par-dessus une machine virtuelle sans aucune modification, comme si elle était exécutée sur le matériel bare-metal. Le système EC2 hôte Amazon émule tout ou partie du matériel sous-jacent présenté à l'invité.	ation paravirtuelle peuvent s'exécuter sur du matériel hôte qui ne prend pas explicitement en charge la virtualisation. Pour plus d'informations sur le PV- GRUB et son utilisati on sur AmazonEC2, consultez la section Noyaux fournis par l'utilisateur.
Types d'instance pris en charge	Tous les types d'instances de la génération actuelle sont pris en charge HVMAMIs.	Les types d'instances de la génération précédente suivants prennent en charge le PV AMIs : C1, C3, M1, M3, M2 et T1. Les types d'instanc es de la génération actuelle ne prennent pas en charge le PVAMIs.

Caractéristiques	HVM	Virtualisation paravirtuelle
Prise en charge des extensions matérielles	HVMles clients peuvent tirer parti des extensions matérielles qui fournissent un accès rapide au matériel sous-jacent du système hôte. Ils sont tenus d'utiliser une mise en réseau et un GPU traitement améliorés. Pour transmettre des instructions à un réseau et à GPU des appareils spécialisés, le système d'exploitation doit avoir accès à la plate-forme matérielle native, et HVM la virtualisation fournit cet accès. Pour de plus amples informations, veuillez consulter Mise en réseau améliorée sur les EC2 instances Amazon.	Non, ils ne peuvent pas tirer parti d'extensions matérielles spéciales telles que la mise en réseau ou GPU le traitement améliorés.
Comment trouver	Vérifiez que le type de virtualisation de AMI est défini sur`hvm`, à l'aide de la console ou de la commande describe-images.	Vérifiez que le type de virtualisation de AMI est défini sur`paravirtual` , à l'aide de la console ou de la commande describe-images.

PV activé HVM

Les clients paravirtuels étaient traditionnellement plus HVM performants que les invités en matière de stockage et de réseau, car ils pouvaient tirer parti de pilotes spéciaux pour les E/S, ce qui leur évitait les frais liés à l'émulation du matériel réseau et disque, alors que HVM les invités devaient traduire ces instructions en matériel émulé. Les pilotes photovoltaïques sont désormais disponibles pour les HVM clients, de sorte que les systèmes d'exploitation qui ne peuvent pas être portés pour fonctionner dans un environnement paravirtualisé peuvent toujours bénéficier d'avantages en termes de performances en termes de stockage et d'E/S réseau grâce à leur utilisation. Grâce à ces HVM

pilotes photovoltaïques, les HVM clients peuvent obtenir des performances identiques ou supérieures à celles des clients paravirtuels.

Trouvez AMI celui qui répond aux exigences de votre EC2 instance

An AMI inclut les composants et les applications, tels que le système d'exploitation et le type de volume racine, nécessaires au lancement d'une instance. Pour lancer une instance, vous devez en trouver une AMI qui répond à vos besoins.

Lorsque vous sélectionnez unAMI, tenez compte des exigences suivantes que vous pourriez avoir pour les instances que vous souhaitez lancer :

- Les AWS régions des AMI as AMI IDs sont uniques à chaque région.
- Le système d'exploitation (par exemple, Linux ou Windows).
- L'architecture (par exemple, 32 bits, 64 bits ou 64 bitsARM).
- Type d'appareil racine (par exemple, Amazon EBS ou magasin d'instance).
- Le fournisseur (par exemple, Amazon Web Services).
- Logiciel supplémentaire (SQLserveur, par exemple).

Pour trouver un Amazon Linux 2023AMI, consultez la section AL2023 sur Amazon EC2 dans le guide de l'utilisateur Amazon Linux 2023.

Pour trouver un UbuntuAMI, consultez Amazon EC2 AMI Locator sur le site Web de Canonical Ubuntu.

Pour en trouver une RHELAMI, consultez les images Red Hat Enterprise Linux (AMI) disponibles sur Amazon Web Services (AWS) sur le site Web de Red Hat.

Il existe différentes manières de trouver AMI celui qui répond à vos besoins. Vous pouvez en trouver un AMI en utilisant la EC2 console Amazon, AWS CLI, AWS Tools for Windows PowerShell, et AWS Systems Manager.

Rechercher et AMI utiliser la EC2 console Amazon

Vous pouvez le trouver AMIs à l'aide de la EC2 console Amazon. Vous pouvez sélectionner dans la liste les cas AMIs où vous utilisez l'assistant de lancement d'instance pour lancer une instance, ou vous pouvez effectuer une recherche parmi toutes les options disponibles à AMIs l'aide de la page Images.

Pour en trouver un à AMI l'aide de l'assistant de lancement d'instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation, sélectionnez la région dans laquelle lancer vos instances. Vous pouvez sélectionner n'importe quelle région disponible, quel que soit votre emplacement. AMIIDssont propres à chaque AWS région.
3. Sur le tableau de bord de la console, sélectionnez Launch instance (Lancer une instance).
4. (Nouvelle console) Sous Images de l'application et du système d'exploitation (Amazon Machine Image), choisissez Quick Start, choisissez le système d'exploitation (OS) de votre instance, puis, dans Amazon Machine Image (AMI), sélectionnez l'un des systèmes couramment utilisés AMIs dans la liste. Si vous ne trouvez pas celui AMI que vous souhaitez utiliser, choisissez Parcourir davantage AMIs pour parcourir le AMI catalogue complet. Pour de plus amples informations, veuillez consulter Images d'applications et de systèmes d'exploitation (Amazon Machine Image).

   (Ancienne console) Dans l'onglet Démarrage rapide, sélectionnez l'une des options les plus fréquemment utilisées AMIs dans la liste. Si vous ne trouvez pas celui AMI que vous souhaitez utiliser, cliquez sur l'AMIsonglet Mon AMIs ou Communauté pour en trouver d'autresAMIs. AWS Marketplace

Pour trouver un utilisateur AMI de la AMIs page

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation, sélectionnez la région dans laquelle lancer vos instances. Vous pouvez sélectionner n'importe quelle région disponible, quel que soit votre emplacement. AMIIDssont propres à chaque AWS région.
3. Dans le volet de navigation, choisissez AMIs.
4. (Facultatif) Utilisez le filtre et les options de recherche pour élargir la liste des options affichées AMIs afin de ne voir AMIs que celles qui correspondent à vos critères.

   Par exemple, pour répertorier toutes les AMIs informations fournies par AWS, choisissez Images publiques. Utilisez ensuite les options de recherche pour élargir la liste des objets affichésAMIs. Cliquez dans la barre Search (Rechercher) et, dans le menu, choisissez Owner alias (Alias du propriétaire), puis l'opérateur =, et enfin la valeur amazon. Pour trouver AMIs celle qui correspond à une plate-forme spécifique, par exemple Linux ou Windows, cliquez à nouveau sur la barre de recherche pour sélectionner Plate-forme, puis l'opérateur =, puis le système d'exploitation dans la liste fournie.

5. (Facultatif) Cliquez sur l'icône Préférences pour sélectionner les attributs d'image à afficher, comme le type de périphérique racine. Vous pouvez également en sélectionner un AMI dans la liste et afficher ses propriétés dans l'onglet Détails.
6. Avant de sélectionner unAMI, il est important de vérifier s'il est soutenu par un magasin d'instances ou par Amazon EBS et de connaître les effets de cette différence. Pour de plus amples informations, veuillez consulter Root device type.
7. Pour lancer une instance à partir de cette optionAMI, sélectionnez-la, puis choisissez Launch instance from image. Pour plus d'informations sur le lancement d'une instance à l'aide de la console, consultez Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console. Si vous n'êtes pas prêt à lancer l'instance maintenant, notez l'AMIID pour plus tard.

Trouvez et AMI utilisez le AWS CLI

Vous pouvez utiliser la AWS CLI commande describe-images pour répertorier uniquement celles AMIs qui correspondent à vos besoins. Après avoir trouvé un fichier AMI correspondant à vos besoins, notez son identifiant afin de pouvoir l'utiliser pour lancer des instances. Pour plus d'informations, consultez Lancer votre instance dans le Guide de l'utilisateur AWS Command Line Interface .

La commande describe-images prend en charge les paramètres de filtrage. Par exemple, utilisez le `--owners` paramètre pour afficher le public AMIs appartenant à Amazon.

```
aws ec2 describe-images --owners amazon
```

Vous pouvez ajouter le filtre suivant à la commande précédente pour afficher uniquement WindowsAMIs.

```
--filters "Name=platform,Values=windows"
```

Vous pouvez ajouter le filtre suivant à la commande précédente pour n'afficher que le AMIs produit soutenu par AmazonEBS.

```
--filters "Name=root-device-type,Values=ebs"
```

> **Important**
>
> Si vous omettez le `--owners` paramètre dans la `describe-images` commande, toutes les images sont renvoyées pour lesquelles vous disposez d'autorisations de lancement, quel que soit leur propriétaire.

Trouvez et AMI utilisez le AWS Tools for Windows PowerShell

Vous pouvez utiliser des PowerShell applets de commande pour répertorier uniquement les fenêtres AMIs qui répondent à vos besoins. Pour obtenir des informations et des exemples, consultez la section Trouver une image de machine Amazon à l'aide de Windows PowerShell dans le guide de AWS Tools for Windows PowerShell l'utilisateur.

Après avoir trouvé un fichier AMI correspondant à vos besoins, notez son identifiant afin de pouvoir l'utiliser pour lancer des instances. Pour plus d'informations, consultez la section Lancer une EC2 instance Amazon à l'aide de Windows PowerShell dans le guide de AWS Tools for Windows PowerShell l'utilisateur.

Rechercher un paramètre AMI à l'aide d'un paramètre Systems Manager

Lorsque vous lancez une instance à l'aide de l'assistant de EC2 lancement d'instance AMI de la EC2 console Amazon, vous pouvez soit en sélectionner une dans la liste (décrite dansRechercher et AMI utiliser la EC2 console Amazon), soit sélectionner un AWS Systems Manager paramètre pointant vers un AMI ID (décrit dans cette section). Si vous utilisez un code d'automatisation pour lancer vos instances, vous pouvez spécifier le paramètre Systems Manager au lieu de l'AMIID.

Un paramètre Systems Manager est une paire clé-valeur définie par le client que vous pouvez créer dans le stockage de paramètres Systems Manager. Le stockage de paramètres fournit un magasin central pour externaliser les valeurs de configuration de vos applications. Pour plus d'informations, consultez Stockage de paramètres AWS Systems Manager dans le AWS Systems Manager Guide de l'utilisateur.

Lorsque vous créez un paramètre qui pointe vers un AMI ID, assurez-vous de spécifier le type de données sous la forme`aws:ec2:image`. La spécification de ce type de données garantit que lorsque le paramètre est créé ou modifié, la valeur du paramètre est validée en tant qu'AMIID. Pour plus d'informations, consultez la section Prise en charge des paramètres natifs pour Amazon Machine Image IDs dans le guide de AWS Systems Manager l'utilisateur.

Rubriques

Cas d'utilisation

Lorsque vous utilisez les paramètres de Systems Manager pour pointer AMIIDs, il est plus facile pour vos utilisateurs de sélectionner les bons paramètres AMI lors du lancement des instances. Les paramètres Systems Manager peuvent également simplifier la maintenance du code d'automatisation.

Plus facile pour les utilisateurs

Si vous souhaitez que les instances soient lancées à l'aide d'un paramètre spécifique AMI et que celui-ci AMI est régulièrement mis à jour, nous vous recommandons de demander à vos utilisateurs de sélectionner un paramètre Systems Manager pour trouver leAMI. Le fait de demander à vos utilisateurs de sélectionner un paramètre Systems Manager garantit que le dernier AMI est utilisé pour lancer les instances.

Par exemple, chaque mois au sein de votre organisation, vous pouvez créer une nouvelle version de votre entreprise AMI contenant les derniers correctifs du système d'exploitation et des applications. Vous demandez également à vos utilisateurs de lancer des instances à l'aide de la dernière version de votreAMI. Pour vous assurer que vos utilisateurs utilisent la dernière version, vous pouvez créer un paramètre Systems Manager (par exemple,`golden-ami`) qui pointe vers le bon AMI ID. Chaque fois qu'une nouvelle version du AMI est créée, vous mettez à jour la valeur AMI d'ID dans le paramètre afin qu'elle pointe toujours vers la dernière versionAMI. Vos utilisateurs n'ont pas besoin de connaître les mises à jour périodiques du AMI car ils continuent à sélectionner le même paramètre Systems Manager à chaque fois. L'utilisation d'un paramètre Systems Manager vous AMI permet de sélectionner plus facilement le bon paramètre AMI pour le lancement d'une instance.

Simplifier la maintenance du code d'automatisation

Si vous utilisez un code d'automatisation pour lancer vos instances, vous pouvez spécifier le paramètre Systems Manager au lieu de l'AMIID. Si une nouvelle version du AMI est créée, vous pouvez modifier la valeur de l'AMIID dans le paramètre afin qu'elle pointe vers la dernière

versionAMI. Le code d'automatisation qui fait référence au paramètre n'a pas besoin d'être modifié à chaque fois qu'une nouvelle version du AMI est créée. Cela simplifie la maintenance de l'automatisation et réduit les coûts de déploiement.

> **Note**
>
> Les instances en cours d'exécution ne sont pas affectées lorsque vous modifiez l'AMIID indiqué par le paramètre Systems Manager.

Autorisations

Si vous utilisez les paramètres de Systems Manager qui pointent vers AMI IDs l'assistant de lancement de l'instance, vous devez ajouter les autorisations suivantes à votre IAM politique :

- `ssm:DescribeParameters`— Autorise l'affichage et la sélection des paramètres de Systems Manager.
- `ssm:GetParameters`— Accorde l'autorisation de récupérer les valeurs des paramètres de Systems Manager.

Vous pouvez également restreindre l'accès à des paramètres Systems Manager spécifiques. Pour plus d'informations et des exemples IAM de politiques, consultezExemple : utilisation de l'assistant de EC2 lancement d'instance.

Limites

AMIset les paramètres de Systems Manager sont spécifiques à la région. Pour utiliser le même nom de paramètre Systems Manager dans les régions, créez un paramètre Systems Manager dans chaque région avec le même nom (par exemple, `golden-ami`). Dans chaque région, pointez le paramètre Systems Manager sur un paramètre AMI de cette région.

Lancer une instance à l'aide d'un paramètre Systems Manager

Vous pouvez lancer une instance à l'aide de la console ou de l' AWS CLI. Au lieu de spécifier un AMI identifiant, vous pouvez spécifier un AWS Systems Manager paramètre qui pointe vers un AMI identifiant.

New console

Pour rechercher un paramètre à AMI l'aide d'un paramètre Systems Manager (console)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation, sélectionnez la région dans laquelle lancer vos instances. Vous pouvez sélectionner n'importe quelle région disponible, quel que soit votre emplacement.
3. Sur le tableau de bord de la console, sélectionnez Launch instance (Lancer une instance).
4. Sous Images de l'application et du système d'exploitation (Amazon Machine Image), sélectionnez Parcourir davantage AMIs.
5. Sélectionnez le bouton fléché à droite de la barre de recherche, puis choisissez Search by Systems Manager parameter (Rechercher par paramètre Systems Manager).
6. Pour Paramètre Systems Manager, sélectionnez un paramètre. L'AMIID correspondant apparaît ci-dessous. Actuellement résolu à.
7. Choisissez Rechercher. AMIsCelles qui correspondent à l'AMIidentifiant apparaissent dans la liste.
8. Sélectionnez-le dans AMI la liste, puis sélectionnez Sélectionner.

Pour plus d'informations sur le lancement d'une instance à l'aide de l'assistant de lancement d'instance, consultez Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console.

Old console

Pour rechercher un paramètre à AMI l'aide d'un paramètre Systems Manager (console)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation, sélectionnez la région dans laquelle lancer vos instances. Vous pouvez sélectionner n'importe quelle région disponible, quel que soit votre emplacement.
3. Sur le tableau de bord de la console, sélectionnez Launch instance (Lancer une instance).
4. Choisissez Rechercher par paramètre Systems Manager (en haut à droite).
5. Pour Paramètre Systems Manager, sélectionnez un paramètre. L'AMIID correspondant apparaît à côté de Actuellement résolu à.
6. Choisissez Rechercher. AMIsCelles qui correspondent à l'AMIidentifiant apparaissent dans la liste.
7. Sélectionnez-le dans AMI la liste, puis sélectionnez Sélectionner.

Pour lancer une instance à l'aide d'un AWS Systems Manager paramètre au lieu d'un AMI ID (AWS CLI)

L'exemple suivant utilise le paramètre Systems Manager `golden-ami` pour lancer une instance `m5.xlarge`. Le paramètre pointe vers un AMI identifiant.

Pour spécifier le paramètre dans la commande, utilisez la syntaxe suivante : `resolve:ssm:/parameter-name`, où `resolve:ssm` est le préfixe standard et `parameter-name` est le nom du paramètre unique. Notez que le nom du paramètre est sensible à la casse. Les barres obliques inverses pour le nom du paramètre ne sont nécessaires que si le paramètre fait partie d'une hiérarchie, par exemple `/amis/production/golden-ami`. Vous pouvez omettre la barre oblique inverse si le paramètre ne fait pas partie d'une hiérarchie.

Dans l'exemple, les paramètres `--count` et `--security-group` ne sont pas inclus. Pour `--count`, la valeur par défaut est 1. Si vous avez un groupe de sécurité par défaut VPC et un groupe de sécurité par défaut, ils sont utilisés.

```
aws ec2 run-instances
    --image-id resolve:ssm:/golden-ami
    --instance-type m5.xlarge
    ...
```

Pour lancer une instance à l'aide d'une version spécifique d'un AWS Systems Manager paramètre (AWS CLI)

Les paramètres Systems Manager ont la prise en charge de la version. Chaque itération d'un paramètre se voit attribuer un numéro de version unique. Vous pouvez référencer la version du paramètre comme suit : `resolve:ssm:parameter-name:version`, où `version` est le numéro de version unique. Par défaut, la dernière version du paramètre est utilisée lorsqu'aucune version n'est spécifiée.

L'exemple suivant utilise la version 2 du paramètre.

Dans l'exemple, les paramètres `--count` et `--security-group` ne sont pas inclus. Car`--count`, la valeur par défaut est 1 Si vous avez un groupe de sécurité par défaut VPC et un groupe de sécurité par défaut, ils sont utilisés.

```
aws ec2 run-instances
    --image-id resolve:ssm:/golden-ami:2
```

```
    --instance-type m5.xlarge
    ...
```

Pour lancer une instance à l'aide d'un paramètre public fourni par AWS

Systems Manager fournit des paramètres publics pour le public AMIs fourni par AWS. Vous pouvez utiliser les paramètres publics lorsque vous lancez des instances afin de vous assurer que vous utilisez les dernières versionsAMIs.

Pour de plus amples informations, veuillez consulter Trouvez les dernières nouveautés AMIs à l'aide d'un paramètre public de Systems Manager.

Trouvez les dernières nouveautés AMIs à l'aide d'un paramètre public de Systems Manager

AWS Systems Manager fournit des paramètres publics pour le public AMIs gérés par AWS. Vous pouvez utiliser les paramètres publics lorsque vous lancez des instances afin de vous assurer que vous utilisez les dernières versionsAMIs. Par exemple, le paramètre public `/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-arm64` est disponible dans toutes les régions et pointe toujours vers la dernière version de l'architecture Amazon Linux 2023 AMI pour arm64 dans une région donnée.

Les paramètres publics sont disponibles à partir des chemins suivants :

- Linux : `/aws/service/ami-amazon-linux-latest`
- Windows – `/aws/service/ami-windows-latest`

Pour afficher la liste de tous les systèmes Linux ou Windows AMIs de la AWS région actuelle

Utilisez la get-parameters-by-path AWS CLI commande suivante pour afficher la liste de tous les systèmes Linux ou Windows AMIs de la AWS région actuelle. La valeur du `--path` paramètre est différente pour Linux et Windows.

Pour Linux :

```
aws ssm get-parameters-by-path \
    --path /aws/service/ami-amazon-linux-latest \
    --query "Parameters[].Name"
```

Pour Windows :

```
aws ssm get-parameters-by-path \
    --path /aws/service/ami-windows-latest \
    --query "Parameters[].Name"
```

Pour lancer une instance à l'aide d'un paramètre public

L'exemple suivant spécifie un paramètre public de Systems Manager pour l'ID d'image permettant de lancer une instance à l'aide de la dernière version d'Amazon Linux 2023AMI.

Pour spécifier le paramètre dans la commande, utilisez la syntaxe suivante : `resolve:ssm:`*`public-parameter`*, où `resolve:ssm` est le préfixe standard et *`public-parameter`* le chemin et le nom du paramètre public.

Dans l'exemple, les paramètres `--count` et `--security-group` ne sont pas inclus. Pour `--count`, la valeur par défaut est 1. Si vous avez un groupe de sécurité par défaut VPC et un groupe de sécurité par défaut, ils sont utilisés.

```
aws ec2 run-instances \
    --image-id resolve:ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-x86_64 \
    --instance-type m5.xlarge \
    --key-name MyKeyPair
```

Pour plus d'informations, veuillez consulter Utilisation de paramètres publics dans le Guide de l'utilisateur AWS Systems Manager .

Pour des exemples utilisant les paramètres de Systems Manager, consultez Query for the latest Amazon Linux AMI IDs Using AWS Systems Manager Parameter Store et Query for the Latest Windows AMI Using AWS Systems Manager Parameter Store.

AMIsPayé dans le AWS Marketplace cadre des EC2 instances Amazon

Un payant AMI est un AMI produit mis en vente dans le AWS Marketplace. AWS Marketplace Il s'agit d'une boutique en ligne où vous pouvez acheter des logiciels qui s' AWS exécutent, y compris ceux AMIs que vous pouvez utiliser pour lancer votre EC2 instance. Ils AWS Marketplace AMIs

sont organisés en catégories, telles que les outils de développement, pour vous permettre de trouver des produits adaptés à vos besoins. Pour plus d'informations AWS Marketplace, consultez le AWS Marketplacesite Web.

Vous pouvez l'acheter AWS Marketplace auprès d'un tiers, y compris AMIs AMIs dans le cadre de contrats de service auprès d'organisations telles que Red Hat. Vous pouvez également en créer un AMI et le vendre AWS Marketplace à d'autres EC2 utilisateurs d'Amazon. Construire un produit sûr, sécurisé et utilisable AMI pour la consommation publique est un processus assez simple, si vous suivez quelques directives simples. Pour plus d'informations sur la création et l'utilisation du partageAMIs, consultezComprendre AMI l'utilisation partagée sur Amazon EC2.

Lancer une instance à partir d'une instance payante AMI revient à lancer une instance à partir de n'importe quelle autre instanceAMI. Aucun paramètre supplémentaire n'est obligatoire. L'instance est facturée en fonction des tarifs fixés par le propriétaire duAMI, ainsi que des frais d'utilisation standard pour les services Web associés, par exemple le taux horaire pour l'exécution d'un type d'instance m5.small sur Amazon. EC2 Des taxes supplémentaires peuvent également être appliquées. Le propriétaire du paiement AMI peut confirmer si une instance spécifique a été lancée à l'aide de ce paiementAMI.

> **Important**
>
> Amazon DevPay n'accepte plus de nouveaux vendeurs ni de nouveaux produits. AWS Marketplace est désormais la plateforme de commerce électronique unique et unifiée pour la vente de logiciels et de services via AWS. Pour plus d'informations sur le déploiement et la vente de logiciels depuis AWS Marketplace, consultez Selling in AWS Marketplace. AWS Marketplace supports AMIs soutenus par AmazonEBS.

Table des matières

Vendez votre AMI place dans le AWS Marketplace

Vous pouvez vendre votre AMI usage AWS Marketplace. AWS Marketplace propose une expérience d'achat organisée. En outre, il prend AWS Marketplace également en charge des AWS fonctionnalités telles que les instances réservéesAMIs, EBS soutenues par Amazon et les instances ponctuelles.

Pour plus d'informations sur la manière de vendre votre produit AMI sur le AWS Marketplace, consultez Selling in AWS Marketplace.

Trouvez un payant AMI

Vous pouvez trouver plusieurs méthodes AMIs d'achat disponibles. Par exemple, vous pouvez utiliser AWS Marketplacela EC2 console Amazon ou la ligne de commande. Un développeur peut également vous informer de l'existence d'un paiement AMI lui-même.

Trouvez une personne payante AMI à l'aide de la console

Pour trouver une personne payante AMI à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez AMIs.
3. Choisissez Images publiques comme premier filtre.
4. Dans la barre de recherche, sélectionnez Owner alias (Alias du propriétaire), puis =, et ensuite aws-marketplace.
5. Si vous connaissez le code produit, choisissez Code Produit, puis =, et entrez ensuite le code produit.

Trouvez une solution payante AMI en utilisant AWS Marketplace

Pour trouver une solution payante AMI en utilisant AWS Marketplace

1. Ouvrir AWS Marketplace.
2. Saisissez le nom du système d'exploitation dans le champ de recherche, puis choisissez le bouton de recherche (loupe).
3. Pour affiner la recherche, utilisez l'une des catégories ou l'un des filtres.
4. Chaque produit est identifié par son type de produit : `AMI` ou `Software as a Service`.

Trouvez une personne payante AMI à l'aide du AWS CLI

Vous pouvez trouver un AMI payant en utilisant la commande describe-images ()AWS CLI suivante.

```
aws ec2 describe-images
    --owners aws-marketplace
```

Cette commande renvoie de nombreux détails décrivant chacune d'entre ellesAMI, y compris le code produit d'une commande payanteAMI. Le résultat de `describe-images` comprend une entrée pour le code produit, illustrée ici :

```
"ProductCodes": [
    {
        "ProductCodeId": "product_code",
        "ProductCodeType": "marketplace"
    }
],
```

Si vous connaissez le code produit, vous pouvez filtrer les résultats par code produit. Cet exemple renvoie le plus récent AMI avec le code produit spécifié.

```
aws ec2 describe-images
    --owners aws-marketplace \
    --filters "Name=product-code,Values=product_code" \
    --query "sort_by(Images, &CreationDate)[-1].[ImageId]"
```

Trouvez un payeur AMI à l'aide des outils pour Windows PowerShell

Vous pouvez trouver un payant AMI en utilisant la Get-EC2Imagecommande suivante.

```
PS C:\> Get-EC2Image -Owner aws-marketplace
```

La sortie pour un produit payant AMI inclut le code du produit.

```
ProductCodeId           ProductCodeType
-------------           ---------------
product_code            marketplace
```

Si vous connaissez le code produit, vous pouvez filtrer les résultats par code produit. Cet exemple renvoie le plus récent AMI avec le code produit spécifié.

```
PS C:\> (Get-EC2Image -Owner aws-marketplace -Filter @{"Name"="product-
code";"Value"="product_code"} | sort CreationDate -Descending | Select-Object -First
 1).ImageId
```

Achetez un produit payé AMI dans le AWS Marketplace

Vous devez vous inscrire pour (acheter) une instance payante AMI avant de pouvoir lancer une EC2 instance Amazon à l'aide duAMI.

Généralement, le vendeur d'un produit payant vous AMI présente des informations à son sujetAMI, notamment son prix et un lien vers lequel vous pouvez l'acheter. Lorsque vous cliquez sur le lien, vous êtes d'abord invité à vous connecter AWS, puis vous pouvez acheter leAMI.

Achetez un produit payant à AMI l'aide de la console

Vous pouvez en acheter un payant à AMI l'aide de l'assistant de EC2 lancement d'Amazon. Pour de plus amples informations, veuillez consulter Lancez une EC2 instance Amazon à partir d'un AWS Marketplace AMI.

Abonnez-vous à un produit en utilisant AWS Marketplace

Pour utiliser le AWS Marketplace, vous devez avoir un Compte AWS. Pour lancer des instances à partir de AWS Marketplace produits, vous devez être inscrit pour utiliser le EC2 service Amazon et vous devez être abonné au produit à partir duquel vous souhaitez lancer l'instance. Vous pouvez utiliser l'une des méthodes suivantes pour vous abonner à des produits dans le AWS Marketplace :

- AWS Marketplace site Web : vous pouvez lancer rapidement des logiciels préconfigurés grâce à la fonction de déploiement en 1 clic. Pour plus d'informations, voir les produits AMI à base de AWS Marketplace.
- Assistant de EC2 lancement Amazon : vous pouvez rechercher AMI et lancer une instance directement depuis l'assistant. Pour de plus amples informations, veuillez consulter Lancez une EC2 instance Amazon à partir d'un AWS Marketplace AMI.

Récupérez le code AWS Marketplace produit depuis votre instance

Vous pouvez récupérer le code AWS Marketplace produit de votre instance à l'aide de ses métadonnées. Si l'instance possède un code produit, Amazon le EC2 renvoie. Pour obtenir plus d'informations sur la récupération des métadonnées, consultez Accéder aux métadonnées d'une EC2 instance.

Pour récupérer un code produit, utilisez la commande correspondant au système d'exploitation de votre instance.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/product-codes
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/product-codes
```

Windows

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/product-codes
```

Utiliser le support payant pour les AWS Marketplace offres prises en charge

Amazon permet EC2 également aux développeurs de proposer une assistance pour les logiciels (ou dérivésAMIs). Les développeurs peuvent créer des produits de support que vous pouvez utiliser en vous y inscrivant. Lors de l'inscription au produit de support, le développeur vous fournit un code produit, que vous devez ensuite associer au vôtre. AMI Le développeur est ainsi en mesure de confirmer que votre instance peut bénéficier du support. Cela garantit également que, lorsque vous exécutez des instances du produit, le tarif appliqué correspond aux conditions définies pour le produit par le développeur.

> **Important**
>
> Vous ne pouvez pas utiliser un produit de support avec les instances réservées. Le tarif appliqué est toujours défini par le vendeur du produit de support.

Pour associer un code produit à votreAMI, utilisez l'une des commandes suivantes, où ami_id est l'ID du produit AMI et product_code est le code du produit :

- modify-image-attribute (AWS CLI)

```
aws ec2 modify-image-attribute --image-id ami_id --product-codes "product_code"
```

- Edit-EC2ImageAttribute (AWS Tools for Windows PowerShell)

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami_id -ProductCode product_code
```

Une fois que vous avez défini l'attribut du code produit, il ne peut pas être modifié ni supprimé.

Factures payées et prises en charge AMIs

À la fin de chaque mois, vous recevez un e-mail indiquant le montant débité de votre carte de crédit pour toute utilisation payée ou prise en charge AMIs au cours du mois. Cette facture est distincte de votre EC2 facture Amazon normale. Pour plus d'informations, consultez la section Paiement des produits dans le AWS Marketplace Guide de l'acheteur.

Gérer vos abonnements AWS Marketplace

Sur le AWS Marketplace site Web, vous pouvez vérifier les détails de votre abonnement, consulter les instructions d'utilisation du fournisseur, gérer vos abonnements, etc.

Pour vérifier les informations concernant votre abonnement

1. Connectez-vous à AWS Marketplace.
2. Choisissez Your Marketplace Account (Votre compte Marketplace).
3. Choisissez Manage your software subscriptions (Gérer vos abonnements logiciels).
4. Tous vos abonnements actuels sont répertoriés. Choisissez Instructions d'utilisation pour afficher les instructions spécifiques relatives à l'utilisation du produit, par exemple un nom d'utilisateur pour vous connecter à votre instance en cours d'exécution.

Pour annuler un AWS Marketplace abonnement

1. Vérifiez que vous avez mis fin à toutes les instances en cours d'exécution à partir de l'abonnement.
   a. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
   b. Dans le panneau de navigation, choisissez Instances.

c. Sélectionnez l'instance, puis choisissez État de l'instance, Terminer (supprimer) l'instance.

d. Choisissez Terminate (supprimer) lorsque vous êtes invité à confirmer.

2. Connectez-vous à AWS Marketplace, puis choisissez Your Marketplace Account (Votre compte Marketplace) et Manage your software subscriptions (Gérer vos abonnements logiciels).

3. Choisissez Cancel subscription (Annuler l'abonnement). Vous êtes invité à confirmer l'annulation.

> **Note**
>
> Une fois que vous avez annulé votre abonnement, vous ne pouvez plus lancer d'instances à partir de celui-ciAMI. Pour l'utiliser à AMI nouveau, vous devez vous y réabonner, soit sur le AWS Marketplace site Web, soit via l'assistant de lancement de la EC2 console Amazon.

EC2AMICycle de vie d'Amazon

Une Amazon Machine Image (AMI) est une image qui fournit le logiciel requis pour configurer et démarrer une instance. Vous devez spécifier un AMI moment où vous lancez une instance.

Amazon vous AMIs permet de les utiliser pour lancer vos instances ou de créer les vôtresAMIs. Par exemple, vous pouvez lancer une instance à partir d'une instance existanteAMI, personnaliser l'instance (par exemple, installer un logiciel et configurer les paramètres du système d'exploitation), puis enregistrer cet environnement mis à jour en tant que nouvel environnementAMI. Toutes les personnalisations d'instance sont enregistrées dans leAMI, de sorte que les instances que vous lancez à partir de votre nouvelle instance AMI incluent ces personnalisations.

Vous ne pouvez utiliser un AMI que dans celui Région AWS dans lequel il a été créé. Si vous devez lancer des instances avec la même configuration dans plusieurs régions, vous pouvez en créer une AMI dans une région, puis les copier dans AMI d'autres régions.

Pour empêcher l'utilisation temporaire d'une instance, vous pouvez désactiver leAMI. Une fois que vous avez désactivé unAMI, vous ne pouvez pas l'utiliser pour lancer de nouvelles instances. Après avoir activé leAMI, vous pouvez l'utiliser pour relancer les instances. Notez que le désenregistrement d'un n'AMIaffecte pas les instances que vous avez déjà lancées depuis le. AMI

Lorsque vous n'en avez plus besoinAMI, vous pouvez le désenregistrer. Une fois que vous avez désenregistré unAMI, vous ne pouvez pas l'utiliser pour lancer de nouvelles instances. Notez que le désenregistrement d'un n'AMIaffecte pas les instances que vous avez déjà lancées depuis le. AMI

Vous pouvez utiliser Amazon Data Lifecycle Manager pour automatiser la création, la conservation, la copie, la dépréciation et la désinscription des instantanés sauvegardés par EBS Amazon AMIs et de leurs instantanés de sauvegarde. Pour plus d'informations, consultez Amazon Data Lifecycle Manager.

Table des matières

Créez un compte soutenu EBS par Amazon AMI

Vous pouvez créer votre propre support Amazon EBS à AMI partir d'une EC2 instance Amazon ou d'un instantané du périphérique racine d'une EC2 instance Amazon.

Pour créer une instance basée sur Amazon EBS à AMI partir d'une instance, commencez par lancer une instance en utilisant une instance basée sur Amazon EBS existante. AMI Il AMI peut s'agir de celui que vous avez obtenu auprès du AWS Marketplace, créé à l'aide de VM Import/Export, ou de tout autre AMI auquel vous pouvez accéder. Après avoir personnalisé l'instance pour répondre à vos besoins spécifiques, créez-en une nouvelle et enregistrez-en une nouvelleAMI. Vous pouvez ensuite utiliser le nouveau AMI pour lancer de nouvelles instances avec vos personnalisations.

Les procédures décrites ci-dessous fonctionnent pour les EC2 instances Amazon soutenues par des volumes Amazon Elastic Block Store (AmazonEBS) chiffrés (y compris le volume racine) ainsi que pour les volumes non chiffrés.

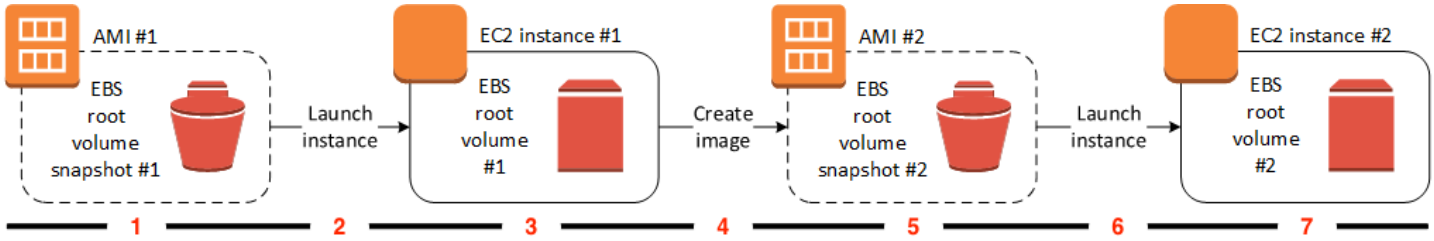
Le processus AMI de création est différent, par exemple en magasinAMIs. Pour de plus amples informations, veuillez consulter Création d'une instance sauvegardée en magasin AMI.

Table des matières

- Vue d'ensemble de AMI la création à partir d'une instance
- Créer et à AMI partir d'une instance
- Création d'un instantané AMI à partir d'un instantané

Vue d'ensemble de AMI la création à partir d'une instance

Le schéma suivant résume le processus de création d'une instance basée sur Amazon AMI à partir EBS d'une EC2 instance en cours d'exécution : commencez par une instance existanteAMI, lancez une instance, personnalisez-la, créez-en une nouvelle AMI à partir de celle-ci et lancez enfin une instance de votre nouvelle instance. AMI Les chiffres du diagramme correspondent à ceux de la description qui suit.



1 — AMI #1 : Commencez par un existant AMI

Trouvez un existant AMI similaire à celui AMI que vous souhaitez créer. Il peut s'agir d'un fichier que AMI vous avez obtenu auprès d'eux AWS Marketplace, d'un AMI que vous avez créé à l'aide de VM Import/Export, ou de tout autre outil AMI auquel vous pouvez accéder. Vous allez le personnaliser en fonction AMI de vos besoins.

Dans le diagramme, l'instantané du volume EBS racine #1 indique qu'il AMI s'agit d'un fichier EBS sauvegardé par Amazon AMI et que les informations relatives au volume racine sont stockées dans cet instantané.

2 — Lancer une instance à partir d'une instance existante AMI

La façon de configurer une AMI consiste à lancer une instance à partir de AMI laquelle vous souhaitez baser votre nouvelle instanceAMI, puis à personnaliser l'instance (indiquée au point 3 dans le schéma). Ensuite, vous allez en créer un nouveau AMI qui inclut les personnalisations (indiquées au point 4 dans le schéma).

3 — EC2 instance #1 : Personnaliser l'instance

Connectez-vous à votre instance et personnalisez-la selon vos besoins. Votre nouveau AMI inclura ces personnalisations.

Vous pouvez effectuer toutes les actions suivantes sur votre instance pour la personnaliser :

- Installer les logiciels et les applications
- Copier les données
- Réduire le temps de démarrage en supprimant les fichiers temporaires et en défragmentant le disque dur
- Attacher des volumes EBS supplémentaires

4 – Créer une image

Lorsque vous créez une instance AMI à partir d'une instance, Amazon EC2 met l'instance hors tension avant de la créer AMI afin de garantir que tout ce qui se trouve sur l'instance est arrêté et dans un état constant pendant le processus de création. Si vous êtes certain que votre instance est dans un état cohérent adapté à sa AMI création, vous pouvez demander à Amazon de EC2 ne pas l'éteindre et de ne pas la redémarrer. Certains systèmes de fichiers, tels queXFS, peuvent geler ou dégeler l'activité, ce qui permet de créer l'image en toute sécurité sans redémarrer l'instance.

Au cours du processus de AMI création, Amazon EC2 crée des instantanés du volume racine de votre instance et de tous les autres EBS volumes attachés à votre instance. Les instantanés vous sont facturés jusqu'à ce que vous les désenregistriez AMI et que vous les supprimiez. Si des volumes attachés à l'instance sont chiffrés, le nouveau AMI ne démarre correctement que sur les instances qui prennent en charge le EBS chiffrement Amazon.

Selon la taille des volumes, le processus de AMI création peut prendre plusieurs minutes (parfois jusqu'à 24 heures). Vous trouverez peut-être plus efficace de créer des instantanés de vos volumes avant de créer votreAMI. Ainsi, seuls de petits instantanés incrémentiels doivent être créés lors de la création, et le processus AMI se termine plus rapidement (le temps total de création des instantanés reste le même).

5 — AMI #2 : Nouveau AMI

Une fois le processus terminé, un nouvel AMI instantané (snapshot #2) est créé à partir du volume racine de l'instance. Si vous avez ajouté des volumes de stockage d'instance ou EBS des volumes à l'instance, en plus du volume du périphérique racine, le mappage du périphérique en mode bloc pour le nouveau AMI contient des informations relatives à ces volumes.

Amazon les enregistre EC2 automatiquement AMI pour vous.

6 — Lancer une instance depuis une nouvelle version AMI

Vous pouvez utiliser le nouveau AMI pour lancer une instance.

7 — EC2 instance #2 : nouvelle instance

Lorsque vous lancez une instance à l'aide du nouveau volumeAMI, Amazon EC2 crée un nouveau EBS volume pour le volume racine de l'instance à l'aide de l'instantané. Si vous avez ajouté des volumes de stockage d'instance ou des EBS volumes lorsque vous avez personnalisé l'instance, le mappage des périphériques par blocs pour les nouveaux AMI contient des informations relatives à ces volumes, et les mappages des périphériques par blocs pour les instances que vous lancez à partir de la nouvelle contiennent AMI automatiquement des informations pour ces volumes. Les volumes de stockage d'instance spécifiés dans le mappage des périphériques par blocs pour la nouvelle instance sont nouveaux et ne contiennent aucune donnée provenant des volumes de stockage d'instance de l'instance que vous avez utilisée pour créer le. AMI Les données relatives aux EBS volumes sont conservées. Pour de plus amples informations, veuillez consulter Bloquer les mappages d'appareils pour les volumes sur les instances Amazon EC2.

Lorsque vous créez une nouvelle instance à partir d'une instance EBS sauvegardée par - backedAMI, vous devez initialiser à la fois son volume racine et tout espace de EBS stockage supplémentaire avant de la mettre en production. Pour plus d'informations, consultez Initialiser les EBS volumes Amazon dans le guide de l'EBSutilisateur Amazon.

Créer et à AMI partir d'une instance

Si vous avez une instance existante, vous pouvez en créer une AMI à partir de cette instance.

Console

Pour créer un AMI

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance à partir de laquelle vous souhaitez créer leAMI, puis choisissez Actions, Image et modèles, puis Créer une image.

   > **Tip**
   >
   > Si cette option est désactivée, votre instance n'est pas une instance EBS soutenue par Amazon.

4. Sur la page Create image (Créer une image), spécifiez les informations suivantes :

a. Pour Image name (Nom de l'image), saisissez un nom unique pour l'image de 127 caractères au maximum.

b. Pour Image description (Description de l'image), saisissez une description facultative de l'image de 255 caractères au maximum.

c. Pour Redémarrer l'instance, maintenez la case à cocher sélectionnée (par défaut) ou désactivez-la.

- Si Redémarrer l'instance est sélectionné, lorsqu'Amazon EC2 crée la nouvelle instanceAMI, il redémarre l'instance afin qu'elle puisse prendre des instantanés des volumes attachés lorsque les données sont au repos, afin de garantir un état cohérent.
- Si l'option Redémarrer l'instance est désactivée, lorsqu'Amazon EC2 crée la nouvelleAMI, il ne l'arrête pas et ne redémarre pas l'instance.

> **Warning**
>
> Si vous effacez l'instance Reboot, nous ne pouvons pas garantir l'intégrité du système de fichiers de l'image créée.

d. Volumes d'instance : vous pouvez modifier le volume racine et ajouter des volumes Amazon EBS et de stockage d'instance supplémentaires, comme suit :

i. Le volume racine est défini dans la première ligne.

- Pour modifier la taille du volume racine, saisissez la valeur requise dans Size (Taille).
- Si vous sélectionnez Supprimer à la résiliation, lorsque vous mettez fin à l'instance créée à partir de cette optionAMI, le EBS volume est supprimé. Si vous désactivez l'option Supprimer à la résiliation, le EBS volume n'est pas supprimé lorsque vous arrêtez l'instance. Pour de plus amples informations, veuillez consulter Conservation des données lors de la résiliation d'une instance.

ii. Pour ajouter un EBS volume, choisissez Ajouter un volume (qui ajoute une nouvelle ligne). Pour Type de stockage EBS, choisissez et remplissez les champs de la ligne. Lorsque vous lancez une instance à partir de votre nouvelle instanceAMI, des volumes supplémentaires sont automatiquement attachés à l'instance. Les volumes vides doivent être formatés et montés. Les volumes basés sur un instantané doivent être montés.

iii. Pour ajouter un volume de stockage d'instance, consultez Ajouter des volumes de stockage d'instance à un Amazon EC2 AMI. Lorsque vous lancez une instance à partir de votre nouvelle instanceAMI, des volumes supplémentaires sont automatiquement initialisés et montés. Ces volumes ne contiennent pas de données provenant des volumes de stockage d'instance de l'instance en cours d'exécution sur laquelle vous avez basé votreAMI.

e. Balises — Vous pouvez étiqueter AMI et les instantanés avec les mêmes balises, ou vous pouvez les étiqueter avec des balises différentes.

- Pour étiqueter les instantanés AMI et les instantanés avec les mêmes balises, choisissez Marquer ensemble l'image et les instantanés. Les mêmes balises sont appliquées AMI à chaque instantané créé.
- Pour étiqueter les instantanés AMI et les instantanés avec des balises différentes, choisissez Marquer l'image et les instantanés séparément. Différentes balises sont appliquées aux instantanés créés AMI et aux instantanés créés. Cependant, tous les instantanés obtiennent les mêmes balises ; vous ne pouvez pas baliser chaque instantané avec une balise différente.

(Facultatif) Pour ajouter une balise, sélectionnez Add tag (Ajouter une balise) et saisissez la clé et la valeur de la balise. Répétez l'opération pour chaque étiquette.

f. Lorsque vous êtes prêt à créer votreAMI, choisissez Créer une image.

5. Pour consulter le statut de votre compte AMI lors de sa création :

a. Dans le volet de navigation, choisissez AMIs.

b. Réglez le filtre sur Owned by me et trouvez votre nom AMI dans la liste.

À l'origine, le statut est `pending` mais il doit être remplacé par `available` après quelques minutes.

6. (Facultatif) Pour afficher l'instantané créé pour le nouveau AMI :

a. Notez l'identifiant AMI que vous avez trouvé à l'étape précédente.

b. Dans le panneau de navigation, choisissez Snapshots.

c. Définissez le filtre sur Owned by me, puis recherchez l'instantané avec le nouvel AMI identifiant dans la colonne Description.

Lorsque vous lancez une instance à partir de celui-ciAMI, Amazon EC2 utilise cet instantané pour créer le volume de son appareil racine.

AWS CLI

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez Accédez à Amazon EC2.

- create-image (AWS CLI)
- New-EC2Image (AWS Tools for Windows PowerShell)

Création d'un instantané AMI à partir d'un instantané

Si vous avez un instantané du volume du périphérique racine d'une instance, vous pouvez en créer un AMI à partir de cet instantané.

> **Note**
>
> Dans la plupart des cas, AMIs pour Windows RedHat,SUSE, et SQL Server, les informations de licence correctes doivent figurer sur leAMI. Pour de plus amples informations, veuillez consulter Comprendre les informations de facturation d'AMI. Lors de la création AMI d'un instantané, l'`RegisterImage`opération extrait les informations de facturation correctes à partir des métadonnées du cliché, mais cela nécessite la présence des métadonnées appropriées. Pour vérifier si les informations de facturation correctes ont été appliquées, consultez le champ Détails de la plateforme sur le nouveauAMI. Si le champ est vide ou ne correspond pas au code du système d'exploitation attendu (par exemple, WindowsRedHat,SUSE, ouSQL), la AMI création a échoué. Vous devez le supprimer AMI et suivre les instructions indiquées dansCréer et à AMI partir d'une instance.

Console

Pour créer et à AMI partir d'un instantané

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Snapshots.

3. Sélectionnez l'instantané à partir duquel vous souhaitez créer leAMI, puis choisissez Actions, Créer une image à partir d'un instantané.
4. Sur la page Créer une image à partir d'un instantané, spécifiez les informations suivantes :

   a. Pour Image name (Nom de l'image), saisissez un nom descriptif pour l'image.

   b. Pour Description, saisissez une brève description pour l'image.

   c. Pour Architecture, choisissez l'architecture de l'image. Choisissez i386 pour 32 bits, x86_64 pour 64 bits, arm64 pour 64 bits ARM ou x86_64 pour macOS 64 bits.

   d. Pour Root device name (Nom du périphérique racine), saisissez le nom du périphérique à utiliser pour le volume du périphérique racine. Pour de plus amples informations, veuillez consulter Noms des appareils pour les volumes sur les EC2 instances Amazon.

   e. Pour le type de virtualisation, choisissez le type de virtualisation à utiliser par les instances lancées à partir de celui-ciAMI. Pour de plus amples informations, veuillez consulter Types de virtualisation.

   f. (Pour la virtualisation paravirtuelle uniquement) Pour Kernel ID (ID du noyau), sélectionnez le noyau du système d'exploitation pour l'image. Si vous utilisez un instantané du volume du périphérique racine d'une instance, sélectionnez le même ID du noyau que celui de l'instance d'origine. Si vous avez un doute, utilisez le noyau par défaut.

   g. (Pour la virtualisation paravirtuelle uniquement) Pour l'ID RAM du disque, sélectionnez le RAM disque pour l'image. Si vous sélectionnez un noyau spécifique, vous devrez peut-être sélectionner un RAM disque spécifique avec les pilotes nécessaires.

   h. Pour le mode de démarrage, choisissez le mode de démarrage de l'image ou choisissez Utiliser par défaut afin que, lorsqu'une instance est lancée avec ce modeAMI, elle démarre avec le mode de démarrage pris en charge par le type d'instance. Pour de plus amples informations, veuillez consulter Définir le mode de démarrage d'un Amazon EC2 AMI.

   i. (Facultatif) Sous Bloquer les mappages de périphériques, personnalisez le volume racine et ajoutez des volumes de données supplémentaires.

      Pour chaque volume, vous pouvez spécifier la taille, le type, les caractéristiques de performance, le comportement de la suppression lors de la résiliation et le statut de chiffrement. Pour le volume racine, la taille ne peut pas être inférieure à celle de l'instantané. Pour le type de volume, General Purpose SSD gp3 est la sélection par défaut.

j. (Facultatif) Sous Balises, vous pouvez ajouter une ou plusieurs balises à la nouvelleAMI. (Facultatif) Pour ajouter une balise, sélectionnez Add tag (Ajouter une balise) et saisissez la clé et la valeur de la balise. Répétez l'opération pour chaque étiquette.

k. Lorsque vous êtes prêt à créer votreAMI, choisissez Créer une image.

5. (Windows, RedHatSUSE, et SQL Server uniquement) Pour vérifier si les informations de facturation correctes ont été appliquées, vérifiez le champ Détails de la plateforme sur le nouveauAMI. Si le champ est vide ou ne correspond pas au code du système d'exploitation attendu (par exemple, Windows ou RedHat), la AMI création a échoué. Vous devez le supprimer AMI et suivre les instructions indiquées dansCréer et à AMI partir d'une instance.

AWS CLI

Pour créer un à AMI partir d'un instantané à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- register-image (AWS CLI)
- Register-EC2Image (AWS Tools for Windows PowerShell)

Création d'une instance sauvegardée en magasin AMI

Le volume AMI que vous spécifiez lorsque vous lancez votre instance détermine le type de volume du périphérique racine.

Pour créer une instance Linux basée sur le stockageAMI, commencez par une instance que vous avez lancée à partir d'une instance Linux basée sur le stockage d'instance existante. AMI Après avoir personnalisé l'instance en fonction de vos besoins, regroupez le volume et enregistrez-en un nouveauAMI, que vous pourrez utiliser pour lancer de nouvelles instances avec ces personnalisations.

Vous ne pouvez pas créer un système Windows basé sur un magasin d'instances, AMI car Windows AMIs ne prend pas en charge le stockage d'instance pour le périphérique racine.

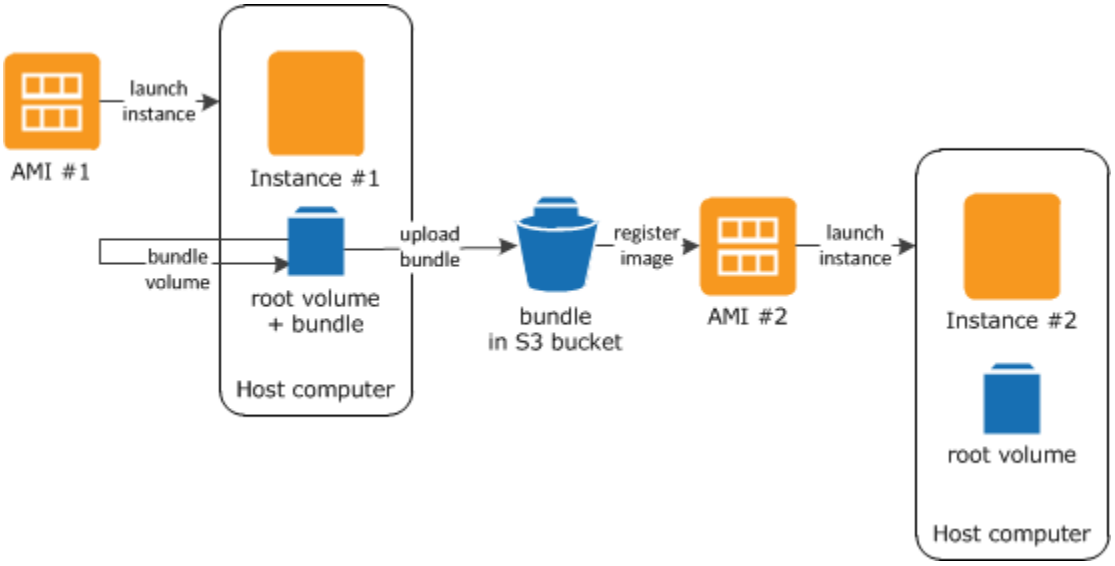
> **Important**
>
> Seuls les types d'instance suivants prennent en charge un volume de stockage d'instance en tant que périphérique racine et nécessitent une instance sauvegardée AMI : C1, C3, D2, I2, M1, M2, M3, R3 et X1.

Le processus AMI de création est différent pour Amazon EBS -backedAMIs. Pour de plus amples informations, veuillez consulter Créez un compte soutenu EBS par Amazon AMI.

Table des matières

Vue d'ensemble de AMI la création

Le schéma suivant résume le processus de création d'une instance AMI à partir d'une instance sauvegardée en magasin.



Commencez par lancer une instance à partir d'une AMI instance similaire à celle AMI que vous souhaitez créer. Vous pouvez vous connecter à votre instance et la personnaliser. Lorsque l'instance est configurée comme vous le voulez, vous pouvezen créer un bundle. Le processus de création d'un bundle peut prendre plusieurs minutes. Après la fin du processus, vous avez un groupe qui se compose d'un manifeste d'image (`image.manifest.xml`) et de fichiers (`image.part.xx`) contenant un modèle pour le volume racine. Ensuite, vous chargez le bundle dans votre compartiment Amazon S3, puis vous enregistrez votreAMI.

> **Note**
>
> Pour télécharger des objets dans un compartiment S3 pour votre instance Linux basée sur le stockageAMI, vous ACLs devez activer le compartiment. Dans le cas contraire, Amazon ne EC2 sera pas en mesure ACLs de définir les objets à télécharger. Si votre compartiment de destination utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, cela ne fonctionnera pas car ils ACLs sont désactivés. Pour plus d'informations, consultez la section Contrôle de la propriété des objets chargés à l'aide de la propriété de l'objet S3.

Lorsque vous lancez une instance à l'aide du nouveau volumeAMI, nous créons le volume racine de l'instance à l'aide du bundle que vous avez chargé sur Amazon S3. L'espace de stockage utilisé par le bundle dans Amazon S3 entraîne des frais sur votre compte jusqu'à ce que vous le supprimiez. Pour de plus amples informations, veuillez consulter Désenregistrer un Amazon EC2 AMI.

Si vous ajoutez des volumes de stockage d'instance à votre instance en plus du volume du périphérique racine, le mappage des périphériques par blocs pour les nouveaux AMI contient des informations relatives à ces volumes, et les mappages des périphériques par blocs pour les instances que vous lancez à partir du nouveau contiennent AMI automatiquement des informations pour ces volumes. Pour de plus amples informations, veuillez consulter Bloquer les mappages d'appareils pour les volumes sur les instances Amazon EC2.

Prérequis

Avant de pouvoir créer unAMI, vous devez effectuer les tâches suivantes :

- Installez les AMI outils. Pour de plus amples informations, veuillez consulter Configurer les EC2 AMI outils Amazon.

- Installez le AWS CLI. Pour plus d'informations, consultez la page Préparation de l'installation de l' AWS Command Line Interface.
- Assurez-vous que vous disposez d'un compartiment S3 pour le bundle et que votre compartiment est ACLs activé. Pour plus d'informations sur la configurationACLs, consultez la section Configuration ACLs.
  - Pour créer un compartiment S3 à l'aide de AWS Management Console, ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/et choisissez Create Bucket.
  - Pour créer un compartiment S3 avec le AWS CLI, vous pouvez utiliser la commande mb. Si la version installée des AMI outils est 1.5.18 ou ultérieure, vous pouvez également utiliser la `ec2-upload-bundle` commande pour créer le compartiment S3. Pour de plus amples informations, veuillez consulter ec2-upload-bundle.
- Assurez-vous que les fichiers de votre bundle ne sont pas chiffrés dans le compartiment S3. Si vous avez besoin d'un cryptage pour votreAMI, vous pouvez utiliser un EBS -backed à la AMI place. Pour de plus amples informations, veuillez consulter Utiliser le chiffrement avec des AMI basées sur EBS.
- Assurez-vous d'avoir votre identifiant de AWS compte. Pour plus d'informations, consultez la section Afficher les Compte AWS identifiants dans le Guide de référence AWS sur la gestion des comptes.
- Assurez-vous de disposer des informations d'identification nécessaires pour utiliser l' AWS CLI. Pour plus d'informations, consultez la section Meilleures pratiques relatives aux AWS comptes dans le Guide de AWS Account Management référence.
- Assurez-vous d'avoir un certificat X.509 et la clé privée correspondante.
  - Si vous avez besoin créer un certificat X.509, consultez la section Gérer les certificats de signature. Le certificat X.509 et la clé privée sont utilisés pour chiffrer et déchiffrer votre. AMI
  - [Chine (Pékin)] Utilisez le certificat `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-cn-north-1.pem`.
  - [AWS GovCloud (US-West)] Utilisez le `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-gov.pem` certificat.
- Connectez-vous à votre instance et personnalisez-la. Par exemple, vous pouvez installer des logiciels et des applications, copier des données, supprimer des fichiers temporaires et modifier la configuration Linux.

Création et AMI depuis une instance Amazon Linux

Les procédures suivantes décrivent comment créer une instance basée sur le stockage d'instance exécutant Amazon Linux 1 à AMI partir d'une instance. Ils risquent de ne pas fonctionner pour les instances exécutant d'autres distributions Linux.

Pour préparer l'utilisation des AMI outils (HVMinstances uniquement)

1. Les AMI outils nécessitent GRUB Legacy pour démarrer correctement. Utilisez la commande suivante pour installer GRUB :

   ```
   [ec2-user ~]$ sudo yum install -y grub
   ```

2. Installez les packages de gestion de partition à l'aide de la commande suivante :

   ```
   [ec2-user ~]$ sudo yum install -y gdisk kpartx parted
   ```

Pour créer une AMI instance Amazon Linux sauvegardée dans un magasin d'instance

Cette procédure part du principe que vous avez respecté les prérequis dans Prérequis.

Dans les commandes suivantes, remplacez chaque *user input placeholder* avec vos propres informations.

1. Chargez vos informations d'identification sur votre instance. Nous utilisons ces informations d'identification pour garantir que vous et Amazon êtes les seuls à EC2 pouvoir accéder à votreAMI.

   a. Créez un répertoire temporaire sur votre instance pour vos informations d'identification en suivant ce qui suit :

      ```
      [ec2-user ~]$ mkdir /tmp/cert
      ```

      Ceci vous permet d'exclure vos informations d'identification de l'image créée.

   b. Copiez votre certificat X.509 et votre clé privée correspondante depuis votre ordinateur vers le répertoire `/tmp/cert` de votre instance en utilisant un outil de copie sécurisé tel que scp. L'`-i` *my-private-key*`.pem`option de la scp commande suivante est la clé privée que vous utilisez pour vous connecter à votre instanceSSH, et non la clé privée X.509. Par exemple :

```
you@your_computer:~ $ scp -i my-private-key.pem /
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem /
path/to/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  685     0.7KB/s   00:00
```

Sinon, étant donné qu'il s'agit de fichiers de texte brut, vous pouvez ouvrir le certificat et la clé dans un éditeur de texte et copier leur contenu dans de nouveaux fichiers dans le répertoire `/tmp/cert`.

2. Préparez le bundle à charger sur Amazon S3 en exécutant la commande ec2-bundle-vol depuis votre instance. Assurez-vous de spécifier l'option `-e` pour exclure le répertoire où vos informations d'identification sont stockées. Par défaut, la création d'un bundle exclut les fichiers qui peuvent contenir des informations sensibles. Ces fichiers incluent `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` et `*/.bash_history`. Pour inclure tous ces fichiers, utilisez l'option `--no-filter`. Pour inclure certains de ces fichiers, utilisez l'option `--include`.

   > **Important**
   >
   > Par défaut, le processus de AMI regroupement crée une collection de fichiers compressés et chiffrés dans le `/tmp` répertoire qui représente votre volume racine. Si vous n'avez pas suffisamment d'espace disque libre dans `/tmp` pour stocker le groupe, vous devez spécifier un emplacement différent pour qu'il soit stocké avec l'option `-d` *`/path/to/bundle/storage`*. Certaines instances disposent d'un stockage éphémère installé sur `/mnt` ou `/media/ephemeral0` que vous pouvez utiliser, ou vous pouvez également créer, joindre et monter un nouveau volume EBS (Amazon) pour stocker le bundle. Pour plus d'informations, consultez la section Créer un EBS volume Amazon dans le guide de EBS l'utilisateur Amazon.

   a. Vous devez exécuter la commande ec2-bundle-vol en tant que racine. Pour la plupart des commandes, vous pouvez utiliser sudo afin d'obtenir des autorisations d'un niveau élevé, mais dans ce cas, vous devriez exécuter sudo -E su pour conserver vos variables d'environnement.

```
[ec2-user ~]$ sudo -E su
```

Notez que l'invite de commande de Bash vous identifie maintenant en tant qu'utilisateur racine, et que le signe dollar a été remplacé par un hashtag, ce qui indique que vous êtes dans un shell racine :

```
[root ec2-user]#
```

b. Pour créer le AMI bundle, exécutez la ec2-bundle-vol commande comme suit :

```
[root ec2-user]# ec2-bundle-vol -k /tmp/cert/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 123456789012 -r x86_64 -e /tmp/cert --
partition gpt
```

> **Note**
>
> Pour les régions de Chine (Pékin) et AWS GovCloud (ouest des États-Unis), utilisez le `--ec2cert` paramètre et spécifiez les certificats conformément aux prérequis.

La création de l'image peut prendre quelques minutes. Lorsque cette commande est terminée, votre répertoire `/tmp` (ou un répertoire autre que celui par défaut) contient le bundle (`image.manifest.xml`, plus multiple `image.part.xx` fichiers).

c. Quittez le shell racine.

```
[root ec2-user]# exit
```

3. (Facultatif) Pour ajouter d'autres volumes de stockage d'instance, modifiez les mappages de périphériques par blocs dans le `image.manifest.xml` fichier correspondant à votreAMI. Pour de plus amples informations, veuillez consulter Bloquer les mappages d'appareils pour les volumes sur les instances Amazon EC2.

   a. Créez une sauvegarde de votre fichier `image.manifest.xml`.

```
[ec2-user ~]$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
```

   b. Reformatez le fichier `image.manifest.xml` pour qu'il soit plus facile à lire et à modifier.

```
[ec2-user ~]$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/
image.manifest.xml
```

c. Modifiez les mappages de périphérique de stockage en mode bloc dans `image.manifest.xml` avec un éditeur de texte. L'exemple ci-dessous montre une nouvelle entrée pour le volume de stockage d'instance `ephemeral1`.

> **Note**
>
> Pour obtenir la liste des fichiers exclus, consultez ec2-bundle-vol.

```
<block_device_mapping>
  <mapping>
    <virtual>ami</virtual>
    <device>sda</device>
  </mapping>
  <mapping>
    <virtual>ephemeral0</virtual>
    <device>sdb</device>
  </mapping>
  <mapping>
    <virtual>ephemeral1</virtual>
    <device>sdc</device>
  </mapping>
  <mapping>
    <virtual>root</virtual>
    <device>/dev/sda1</device>
  </mapping>
</block_device_mapping>
```

d. Enregistrez le fichier `image.manifest.xml` et quittez votre éditeur de texte.

4. Pour charger votre bundle sur Amazon S3, exécutez la commande ec2-upload-bundle comme suit.

```
[ec2-user ~]$ ec2-upload-bundle -b amzn-s3-demo-bucket/bundle_folder/bundle_name -
m /tmp/image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

> **Important**
>
> Pour vous inscrire AMI dans une région autre que l'est des États-Unis (Virginie du Nord), vous devez spécifier à la fois la région cible avec l'`--region`option et un chemin de compartiment qui existe déjà dans la région cible ou un chemin de compartiment unique qui peut être créé dans la région cible.

5. (Facultatif) Une fois que le groupe est chargé sur Amazon S3, vous pouvez le supprimer du répertoire `/tmp` sur l'instance en utilisant la commande rm suivante :

```
[ec2-user ~]$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

> **Important**
>
> Si vous avez spécifié un chemin avec l'option `-d` *`/path/to/bundle/storage`* dans Step 2, utilisez ce chemin à la place de `/tmp`.

6. Pour enregistrer votreAMI, exécutez la commande register-image comme suit.

```
[ec2-user ~]$ aws ec2 register-image --image-location amzn-s3-demo-
bucket/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --
virtualization-type hvm
```

> **Important**
>
> Si vous avez précédemment spécifié une région pour la commande ec2-upload-bundle, spécifiez de nouveau cette région pour cette commande.

Configurer les EC2 AMI outils Amazon

Vous pouvez utiliser les AMI outils pour créer et gérer un système Linux basé sur le stockage d'instances. AMIs Pour utiliser ces outils, vous devez les installer sur votre instance Linux. Les AMI outils sont disponibles sous forme de fichier .zip RPM et sous forme de fichier .zip pour les distributions Linux qui ne sont pas prises en chargeRPM.

Pour configurer les AMI outils à l'aide du RPM

1. Installez Ruby en utilisant le gestionnaire de package pour votre distribution de Linux, par exemple yum. Par exemple :

```
[ec2-user ~]$ sudo yum install -y ruby
```

2. Téléchargez le RPM fichier à l'aide d'un outil tel que wget ou curl. Par exemple :

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.noarch.rpm
```

3. Vérifiez la signature du RPM fichier à l'aide de la commande suivante :

```
[ec2-user ~]$ rpm -K ec2-ami-tools.noarch.rpm
```

   La commande ci-dessus doit indiquer que le fichier SHA1 et les MD5 hachages sont. `OK`. Si la commande indique que les hachages le sont`NOT OK`, utilisez la commande suivante pour afficher l'en-tête SHA1 et MD5 les hachages du fichier :

```
[ec2-user ~]$ rpm -Kv ec2-ami-tools.noarch.rpm
```

   Comparez ensuite l'en-tête SHA1 et les hachages de votre fichier avec MD5 les hachages AMI des outils vérifiés suivants pour confirmer l'authenticité du fichier :

   - En-tête SHA1 : a1f662d6f25f69871104e6a62187fa4df508f880
   - MD5: 9faff05258064e2f7909b66142de6782

   Si l'en-tête SHA1 et les MD5 hachages de votre fichier correspondent aux hachages vérifiés AMI des outils, passez à l'étape suivante.

4. Installez le à RPM l'aide de la commande suivante :

```
[ec2-user ~]$ sudo yum install ec2-ami-tools.noarch.rpm
```

5. Vérifiez l'installation de vos AMI outils à l'aide de la ec2- ami-tools-version commande.

```
[ec2-user ~]$ ec2-ami-tools-version
```

> **Note**
>
> Si vous recevez une erreur de chargement du type « impossible de charger ce fichier -- ec2/amitools/version (LoadError) », passez à l'étape suivante pour ajouter l'emplacement de l'installation de vos outils à votre AMI chemin. `RUBYLIB`

6. (Facultatif) Si vous avez reçu une erreur à l'étape précédente, ajoutez l'emplacement de l'installation de vos AMI outils à votre `RUBYLIB` chemin.

   a. Exécutez la commande suivante afin de déterminer les chemins à ajouter.

   ```
   [ec2-user ~]$ rpm -qil ec2-ami-tools | grep ec2/amitools/version
   /usr/lib/ruby/site_ruby/ec2/amitools/version.rb
   /usr/lib64/ruby/site_ruby/ec2/amitools/version.rb
   ```

   Dans l'exemple ci-dessus, le fichier manquant à partir de l'erreur de chargement précédente est situé aux emplacements `/usr/lib/ruby/site_ruby` et `/usr/lib64/ruby/site_ruby`.

   b. Ajoutez les emplacements à partir de l'étape précédente pour votre chemin d'accès. `RUBYLIB`

   ```
   [ec2-user ~]$ export RUBYLIB=$RUBYLIB:/usr/lib/ruby/site_ruby:/usr/lib64/ruby/site_ruby
   ```

   c. Vérifiez l'installation de vos AMI outils à l'aide de la ec2- ami-tools-version commande.

   ```
   [ec2-user ~]$ ec2-ami-tools-version
   ```

Pour configurer les AMI outils à l'aide du fichier .zip

1. Installez Ruby et décompressez en utilisant le gestionnaire de package pour votre distribution de Linux, comme apt-get. Exemples :

   ```
   [ec2-user ~]$ sudo apt-get update -y && sudo apt-get install -y ruby unzip
   ```

2. Téléchargez le fichier .zip à l'aide d'un outil tel que wget ou curl. Exemples :

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.zip
```

3. Décompressez les fichiers dans un répertoire d'installation approprié, tel que `/usr/local/ec2`.

```
[ec2-user ~]$ sudo mkdir -p /usr/local/ec2
$ sudo unzip ec2-ami-tools.zip -d /usr/local/ec2
```

   Notez que le fichier .zip contient un dossier ec2-ami-tools-*x.x.x*Où : *x.x.x* est le numéro de version des outils (par exemple,`ec2-ami-tools-1.5.7`).

4. Définissez la variable d'environnement `EC2_AMITOOL_HOME` sur le répertoire d'installation des outils. Exemples :

```
[ec2-user ~]$ export EC2_AMITOOL_HOME=/usr/local/ec2/ec2-ami-tools-x.x.x
```

5. Ajoutez les outils à votre variable d'environnement `PATH`. Par exemple :

```
[ec2-user ~]$ export PATH=$EC2_AMITOOL_HOME/bin:$PATH
```

6. Vous pouvez vérifier l'installation de vos AMI outils à l'aide de la ec2- ami-tools-version commande.

```
[ec2-user ~]$ ec2-ami-tools-version
```

Gérer les certificats de signature

Certaines commandes des AMI outils nécessitent un certificat de signature (également appelé certificat X.509). Vous devez créer le certificat, puis le télécharger sur AWS. Par exemple, vous pouvez utiliser un outil tiers tel qu'Open SSL pour créer le certificat.

Pour créer un certificat de signature

1. Installez et configurez OpenSSL.
2. Créez une clé privée à l'aide de la commande `openssl genrsa` et enregistrez la sortie dans un fichier `.pem`. Nous vous recommandons de créer une clé de 2048 ou 4096 bitsRSA.

```
openssl genrsa 2048 > private-key.pem
```

3. Générez un certificat à l'aide de la commande `openssl req`.

```
openssl req -new -x509 -nodes -sha256 -days 365 -key private-key.pem -outform PEM -
out certificate.pem
```

Pour télécharger le certificat sur AWS, utilisez la upload-signing-certificatecommande.

```
aws iam upload-signing-certificate --user-name user-name --certificate-body
 file://path/to/certificate.pem
```

Pour répertorier les certificats d'un utilisateur, utilisez la list-signing-certificatescommande :

```
aws iam list-signing-certificates --user-name user-name
```

Pour désactiver ou réactiver un certificat de signature pour un utilisateur, utilisez la update-signing-certificatecommande. La commande suivante désactive le certificat :

```
aws iam update-signing-certificate --certificate-id OFHPLP4ZULTHYPMSYEX7O4BEXAMPLE --
status Inactive --user-name user-name
```

Pour supprimer un certificat, utilisez la delete-signing-certificatecommande suivante :

```
aws iam delete-signing-certificate --user-name user-name --certificate-
id OFHPLP4ZULTHYPMSYEX7O4BEXAMPLE
```

Référence EC2 AMI des outils Amazon

Vous pouvez utiliser les commandes AMI tools pour créer et gérer un système Linux basé sur le stockage d'instances. AMIs Pour installer les outils, consultez Configurer les EC2 AMI outils Amazon.

Pour plus d'informations sur vos clés d'accès, consultez la section Gestion des clés d'accès pour IAM les utilisateurs dans le Guide de IAM l'utilisateur.

Commandes

- ec2- ami-tools-version
- ec2-bundle-image
- ec2-bundle-vol
- ec2-delete-bundle

- ec2-download-bundle
- ec2-migrate-manifest
- ec2-unbundle
- ec2-upload-bundle
- Options courantes pour les AMI outils

ec2- ami-tools-version

Description

Décrit la version des AMI outils.

Syntaxe

ec2-ami-tools-version

Sortie

Informations de version.

Exemple

Cet exemple de commande affiche les informations de version des AMI outils que vous utilisez.

```
[ec2-user ~]$ ec2-ami-tools-version
1.5.2 20071010
```

ec2-bundle-image

Description

Crée une instance Linux sauvegardée en magasin AMI à partir d'une image de système d'exploitation créée dans un fichier de boucle.

Syntaxe

ec2-bundle-image -c *path* -k *path* -u *account* -i *path* [-d *path*] [--ec2cert *path*] [-r *architecture*] [--productcodes *code1*,*code2*,...] [-B *mapping*] [-p *prefix*]

Options

`-c, --cert` chemin

Le fichier de certificat de clé RSA publique PEM codé de l'utilisateur.

Obligatoire : oui

`-k, --privatekey` chemin

Le chemin d'accès à un fichier RSA clé PEM codé. Vous devrez également spécifier cette clé pour dissocier ce groupe, conservez-la dans un endroit sûr. Notez qu'il n'est pas nécessaire que la clé soit enregistrée sur votre AWS compte.

Obligatoire : oui

`-u, --user` compte

L'identifiant du AWS compte de l'utilisateur, sans tirets.

Obligatoire : oui

`-i, --image` chemin

Chemin d'accès à l'image à grouper.

Obligatoire : oui

`-d, --destination` chemin

Répertoire dans lequel vous créez le groupe.

Par défaut: `/tmp`

Obligatoire : non

`--ec2cert` chemin

Le chemin d'accès au certificat de clé publique Amazon EC2 X.509 utilisé pour chiffrer le manifeste d'image.

Les régions `us-gov-west-1`et `cn-north-1` utilisent un certificat de clé publique par défaut. Le chemin d'accès à ce certificat doit être spécifié avec cette option. Le chemin d'accès au certificat varie en fonction de la méthode d'installation des AMI outils. Pour Amazon Linux, les certificats se

trouvent à l'adresse `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Si vous avez installé les AMI outils depuis le ZIP fichier RPM ouConfigurer les EC2 AMI outils Amazon, les certificats se trouvent à l'adresse`$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obligatoire : uniquement pour les régions `us-gov-west-1` et `cn-north-1`.

`-r, --arch` architecture

Architecture d'image. Si vous ne fournissez pas l'architecture dans la ligne de commande, vous serez invité à la saisir au début de la création du bundle.

Valeurs valides : `i386` | `x86_64`

Obligatoire : non

`--productcodes` code1,code2,...

Codes de produit à attacher à l'image au moment de l'inscription, séparé par des virgules.

Obligatoire : non

`-B, --block-device-mapping` mappage

Définit la manière dont les périphériques en mode bloc sont exposés à une instance de ce type AMI si son type d'instance prend en charge le périphérique spécifié.

Spécifiez une liste séparée par des virgules de paires clé-valeur, où chaque clé est un nom virtuel et chaque valeur le nom de périphérique correspondant. Les noms virtuels incluent les éléments suivants :

- `ami`— Périphérique du système de fichiers racine, tel qu'il est vu par l'instance
- `root`— Périphérique du système de fichiers racine, tel qu'il est vu par le noyau
- `swap`— Périphérique d'échange, tel qu'il est vu par l'instance
- `ephemeralN`—Volume de stockage de la nième instance

Obligatoire : non

`-p, --prefix` prefix

Le préfixe du nom de fichier pour les fichiers groupésAMI.

Par défaut : nom du fichier image. Par exemple, si le chemin d'accès de l'image est `/var/spool/my-image/version-2/debian.img`, le préfixe par défaut est `debian.img`.

Obligatoire : non

`--kernel` kernel_id

Obsolète. Utilisez register-image pour définir le noyau.

Obligatoire : non

`--ramdisk` ramdisk_id

Obsolète. Utilisez register-image pour configurer le RAM disque si nécessaire.

Obligatoire : non

Sortie

Messages d'état décrivant les étapes et le statut du processus de groupement.

Exemple

Cet exemple crée un bundle AMI à partir d'une image de système d'exploitation créée dans un fichier de boucle.

```
[ec2-user ~]$ ec2-bundle-image -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -i image.img -d bundled/ -r x86_64
Please specify a value for arch [i386]:
Bundling image file...
Splitting bundled/image.gz.crypt...
Created image.part.00
Created image.part.01
Created image.part.02
Created image.part.03
Created image.part.04
Created image.part.05
Created image.part.06
Created image.part.07
Created image.part.08
Created image.part.09
Created image.part.10
Created image.part.11
Created image.part.12
Created image.part.13
Created image.part.14
Generating digests for each part...
```

```
Digests generated.
Creating bundle manifest...
ec2-bundle-image complete.
```

ec2-bundle-vol

Description

Crée une instance Linux basée sur le stockage AMI en compressant, en chiffrant et en signant une copie du volume du périphérique racine de l'instance.

Amazon EC2 tente d'hériter des codes produits, des paramètres du noyau, des paramètres RAM du disque et de bloquer les mappages de périphériques de l'instance.

Par défaut, la création d'un bundle exclut les fichiers qui peuvent contenir des informations sensibles. Ces fichiers incluent `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` et `*/.bash_history`. Pour inclure tous ces fichiers, utilisez l'option `--no-filter`. Pour inclure certains de ces fichiers, utilisez l'option `--include`.

Pour plus d'informations, consultez Création d'une instance sauvegardée en magasin AMI.

Syntaxe

ec2-bundle-vol -c *path* -k *path* -u *account* [-d *path*] [--ec2cert *path*] [-r *architecture*] [--productcodes *code1*,*code2*,...] [-B *mapping*] [--all] [-e *directory1*,*directory2*,...] [-i *file1*,*file2*,...] [--no-filter] [-p *prefix*] [-s *size*] [--[no-]inherit] [-v *volume*] [-P *type*] [-S *script*] [--fstab *path*] [--generate-fstab] [--grub-config *path*]

Options

`-c, --cert` chemin

Le fichier de certificat de clé RSA publique PEM codé de l'utilisateur.

Obligatoire : oui

`-k, --privatekey` chemin

Le chemin d'accès au fichier RSA clé PEM codé de l'utilisateur.

Obligatoire : oui

`-u, --user` compte

L'identifiant du AWS compte de l'utilisateur, sans tirets.

Obligatoire : oui

`-d, --destination` destination

Répertoire dans lequel vous créez le groupe.

Par défaut: `/tmp`

Obligatoire : non

`--ec2cert` chemin

Le chemin d'accès au certificat de clé publique Amazon EC2 X.509 utilisé pour chiffrer le manifeste d'image.

Les régions `us-gov-west-1`et `cn-north-1` utilisent un certificat de clé publique par défaut. Le chemin d'accès à ce certificat doit être spécifié avec cette option. Le chemin d'accès au certificat varie en fonction de la méthode d'installation des AMI outils. Pour Amazon Linux, les certificats se trouvent à l'adresse `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Si vous avez installé les AMI outils depuis le ZIP fichier RPM ouConfigurer les EC2 AMI outils Amazon, les certificats se trouvent à l'adresse`$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obligatoire : uniquement pour les régions `us-gov-west-1` et `cn-north-1`.

`-r, --arch` architecture

Architecture de l'image. Si vous ne fournissez pas cette ligne de commande, vous serez invité à la saisir au début de la création du bundle.

Valeurs valides : `i386` | `x86_64`

Obligatoire : non

`--productcodes` code1,code2,...

Codes de produit à attacher à l'image au moment de l'inscription, séparé par des virgules.

Obligatoire : non

`-B, --block-device-mapping` mappage

Définit la manière dont les périphériques en mode bloc sont exposés à une instance de ce type AMI si son type d'instance prend en charge le périphérique spécifié.

Spécifiez une liste séparée par des virgules de paires clé-valeur, où chaque clé est un nom virtuel et chaque valeur le nom de périphérique correspondant. Les noms virtuels incluent les éléments suivants :

- `ami`— Périphérique du système de fichiers racine, tel qu'il est vu par l'instance
- `root`— Périphérique du système de fichiers racine, tel qu'il est vu par le noyau
- `swap`— Périphérique d'échange, tel qu'il est vu par l'instance
- `ephemeralN`—Volume de stockage de la nième instance

Obligatoire : non

`-a, --all`

Groupez tous les répertoires, y compris ceux contenus dans les systèmes de fichiers montés à distance.

Obligatoire : non

`-e, --exclude` directory1,directory2,...

Liste des chemins absolus de répertoires et fichiers à exclure de l'opération de groupement. Ce paramètre remplace l'option `--all`. Lorsque la commande exclude est spécifié, les répertoires et sous-répertoires répertoriés avec le paramètre ne sont pas groupés avec le volume.

Obligatoire : non

`-i, --include` file1,file2,...

Liste des fichiers à inclure dans l'opération de groupement. Les fichiers spécifiés seraient sinon exclus du AMI car ils peuvent contenir des informations sensibles.

Obligatoire : non

`--no-filter`

Si cela est spécifié, nous n'en exclurons pas les fichiers AMI car ils peuvent contenir des informations sensibles.

Obligatoire : non

`-p, --prefix` prefix

Le préfixe du nom de fichier pour les fichiers groupésAMI.

Par défaut: `image`

Obligatoire : non

`-s, --size` taille

Taille, en Mo (1024 * 1024 octets), du fichier image à créer. La taille maximale est 10 240 Mo.

Par défaut: 10240

Obligatoire : non

`--[no-]inherit`

Indique si l'image doit hériter des métadonnées de l'instance (la valeur par défaut consiste à hériter). Le groupement échoue si vous activez `--inherit`, mais les métadonnées d'instance ne sont pas accessibles.

Obligatoire : non

`-v, --volume` volume

Chemin d'accès absolu au volume monté à partir duquel créer le groupe.

Par défaut : le répertoire racine (/)

Obligatoire : non

`-P, --partition` type

Indique si l'image de disque doit utiliser une table de partition. Si vous ne spécifiez pas de type de table de partition, la valeur par défaut est le type utilisé sur le périphérique de stockage en mode bloc parent du volume, le cas échéant. Dans le cas contraire, la valeur par défaut est `gpt`.

Valeurs valides : `mbr` | `gpt` | `none`

Obligatoire : non

`-S, --script` script

Script de personnalisation à exécuter juste avant de procéder à la création du bundle. Le script doit attendre un seul argument, le point de montage du volume.

Obligatoire : non

`--fstab` chemin

Chemin d'accès au fichier fstab à grouper dans l'image. Si cela n'est pas spécifié, Amazon EC2 regroupe /etc/fstab.

Obligatoire : non

`--generate-fstab`

Regroupe le volume à l'aide d'un fichier fstab EC2 fourni par Amazon.

Obligatoire : non

`--grub-config`

Chemin d'accès à un autre fichier de configuration grub à grouper dans l'image. Par défaut, `ec2-bundle-vol` attend `/boot/grub/menu.lst` ou `/boot/grub/grub.conf` pour exister sur l'image clonée. Cette option vous permet de spécifier un chemin d'accès à un autre fichier de configuration grub, qui sera ensuite copié par-dessus les valeurs par défaut (le cas échéant).

Obligatoire : non

`--kernel` kernel_id

Obsolète. Utilisez register-image pour définir le noyau.

Obligatoire : non

`--ramdisk`ramdisk_id

Obsolète. Utilisez register-image pour configurer le RAM disque si nécessaire.

Obligatoire : non

Sortie

Messages d'état décrivant les étapes et le statut de la création du bundle.

Exemple

Cet exemple crée un bundle AMI en compressant, chiffrant et signant un instantané du système de fichiers racine de la machine locale.

```
[ec2-user ~]$ ec2-bundle-vol -d /mnt -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c
 cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -r x86_64
  Copying / into the image file /mnt/image...
```

```
  Excluding:
       sys
       dev/shm
       proc
       dev/pts
       proc/sys/fs/binfmt_misc
       dev
       media
       mnt
       proc
       sys
       tmp/image
       mnt/img-mnt
  1+0 records in
  1+0 records out
  mke2fs 1.38 (30-Jun-2005)
  warning: 256 blocks unused.

  Splitting /mnt/image.gz.crypt...
  Created image.part.00
  Created image.part.01
  Created image.part.02
  Created image.part.03
  ...
  Created image.part.22
  Created image.part.23
  Generating digests for each part...
  Digests generated.
  Creating bundle manifest...
  Bundle Volume complete.
```

ec2-delete-bundle

Description

Supprime le groupe spécifié du stockage Amazon S3. Une fois que vous avez supprimé un bundle, vous ne pouvez pas lancer d'instances à partir du bundle correspondantAMI.

Syntaxe

ec2-delete-bundle -b *bucket* -a *access_key_id* -s *secret_access_key* [-t *token*] [--url *url*] [--region *region*] [--sigv *version*] [-m *path*] [-p *prefix*] [--clear] [--retry] [-y]

Options

`-b, --bucket` bucket

Le nom du compartiment Amazon S3 contenant le bundleAMI, suivi d'un préfixe de chemin facultatif délimité par «/»

Obligatoire : oui

`-a, --access-key` access_key_id

L'ID de la clé d' AWS accès.

Obligatoire : oui

`-s, --secret-key` secret_access_key

La clé d'accès AWS secrète.

Obligatoire : oui

`-t, --delegation-token` jeton

Le jeton de délégation à transmettre à la AWS demande. Pour plus d'informations, consultez Utilisation des autorisations de sécurité temporaires.

Requis : uniquement lorsque vous utilisez des informations d'identification de sécurité temporaires.

Par défaut : valeur de la variable d'environnement `AWS_DELEGATION_TOKEN` (si elle est définie).

`--region`region

Région à utiliser dans la signature de la demande.

Par défaut : `us-east-1`

Requis : requis si vous utilisez Signature Version 4

`--sigv`Version

Version de signature à utiliser lors de la signature de la demande.

Valeurs valides : `2` | `4`

Par défaut: `4`

Obligatoire : non

`-m, --manifest`chemin

Chemin d'accès au fichier manifeste.

Requis : vous devez spécifier `--prefix` ou `--manifest`.

`-p, --prefix` prefix

Préfixe du nom de fichier AMI groupé. Fournissez le préfixe entier. Par exemple, si le préfixe est image.img, utilisez `-p image.img`, non `-p image`.

Requis : vous devez spécifier `--prefix` ou `--manifest`.

`--clear`

Supprime le compartiment Amazon S3 s'il est vide après la suppression du groupe spécifié.

Obligatoire : non

`--retry`

Refait automatiquement des tentatives sur toutes les erreurs Amazon S3, jusqu'à cinq fois par opération.

Obligatoire : non

`-y, --yes`

Suppose automatiquement que la réponse à toutes les invites est oui.

Obligatoire : non

Sortie

Amazon EC2 affiche des messages d'état indiquant les étapes et le statut du processus de suppression.

Exemple

Cet exemple supprime un groupe de Amazon S3.

```
[ec2-user ~]$ ec2-delete-bundle -b amzn-s3-demo-bucket -a your_access_key_id -
s your_secret_access_key
Deleting files:
amzn-s3-demo-bucket/image.manifest.xml
amzn-s3-demo-bucket/image.part.00
```

```
amzn-s3-demo-bucket/image.part.01
amzn-s3-demo-bucket/image.part.02
amzn-s3-demo-bucket/image.part.03
amzn-s3-demo-bucket/image.part.04
amzn-s3-demo-bucket/image.part.05
amzn-s3-demo-bucket/image.part.06
Continue? [y/n]
y
Deleted amzn-s3-demo-bucket/image.manifest.xml
Deleted amzn-s3-demo-bucket/image.part.00
Deleted amzn-s3-demo-bucket/image.part.01
Deleted amzn-s3-demo-bucket/image.part.02
Deleted amzn-s3-demo-bucket/image.part.03
Deleted amzn-s3-demo-bucket/image.part.04
Deleted amzn-s3-demo-bucket/image.part.05
Deleted amzn-s3-demo-bucket/image.part.06
ec2-delete-bundle complete.
```

ec2-download-bundle

Description

Télécharge l'instance Linux spécifiée basée sur le stockage AMIs depuis le stockage Amazon S3.

Syntaxe

ec2-download-bundle -b *bucket* -a *access_key_id* -s *secret_access_key* -k *path* [--url *url*] [--region *region*] [--sigv *version*] [-m *file*] [-p *prefix*] [-d *directory*] [--retry]

Options

`-b, --bucket` bucket

Nom du compartiment Amazon S3 où se trouve le groupe, suivi d'un préfixe de chemin séparé par des « / »-facultatif.

Obligatoire : oui

`-a, --access-key` access_key_id

L'ID de la clé d' AWS accès.

Obligatoire : oui

`-s, --secret-key` secret_access_key

La clé d'accès AWS secrète.

Obligatoire : oui

`-k, --privatekey` chemin

Clé privée utilisée pour déchiffrer le manifeste.

Obligatoire : oui

`--url` url

Le service Amazon S3URL.

Par défaut: `https://s3.amazonaws.com/`

Obligatoire : non

`--region` région

Région à utiliser dans la signature de la demande.

Par défaut : `us-east-1`

Requis : requis si vous utilisez Signature Version 4

`--sigv` version

Version de signature à utiliser lors de la signature de la demande.

Valeurs valides : `2` | `4`

Par défaut: `4`

Obligatoire : non

`-m, --manifest` file

Nom du fichier manifeste (sans le chemin d'accès). Nous vous recommandons de spécifier soit le manifeste (`-m`) soit un préfixe (`-p`).

Obligatoire : non

`-p, --prefix` prefix

Le préfixe du nom de fichier pour les fichiers groupésAMI.

Par défaut: `image`

Obligatoire : non

`-d, --directory` directory

Répertoire dans lequel le groupe téléchargé est enregistré. Le répertoire doit exister.

Par défaut : le répertoire de travail actuel.

Obligatoire : non

`--retry`

Refait automatiquement des tentatives sur toutes les erreurs Amazon S3, jusqu'à cinq fois par opération.

Obligatoire : non

Sortie

Les messages d'état indiquant les différentes étapes du processus de téléchargement s'affichent.

Exemple

Cet exemple crée le répertoire `bundled` (à l'aide de la commande Linux mkdir) et télécharge le groupe depuis le compartiment Amazon S3 `amzn-s3-demo-bucket`.

```
[ec2-user ~]$ mkdir bundled
[ec2-user ~]$ ec2-download-bundle -b amzn-s3-demo-bucket/bundles/bundle_name
 -m image.manifest.xml -a your_access_key_id -s your_secret_access_key -k pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d mybundle
Downloading manifest image.manifest.xml from amzn-s3-demo-bucket to mybundle/
image.manifest.xml ...
Downloading part image.part.00 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.00 ...
Downloaded image.part.00 from amzn-s3-demo-bucket
Downloading part image.part.01 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.01 ...
Downloaded image.part.01 from amzn-s3-demo-bucket
Downloading part image.part.02 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.02 ...
Downloaded image.part.02 from amzn-s3-demo-bucket
```

```
Downloading part image.part.03 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.03 ...
Downloaded image.part.03 from amzn-s3-demo-bucket
Downloading part image.part.04 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.04 ...
Downloaded image.part.04 from amzn-s3-demo-bucket
Downloading part image.part.05 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.05 ...
Downloaded image.part.05 from amzn-s3-demo-bucket
Downloading part image.part.06 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.06 ...
Downloaded image.part.06 from amzn-s3-demo-bucket
```

ec2-migrate-manifest

Description

Modifie une instance Linux sauvegardée en stockage AMI (par exemple, son certificat, son noyau et son RAM disque) afin qu'elle prenne en charge une autre région.

Syntaxe

ec2-migrate-manifest -c *path* -k *path* -m *path* {(-a *access_key_id* -s *secret_access_key* --region *region*) | (--no-mapping)} [--ec2cert *ec2_cert_path*] [--kernel *kernel-id*] [--ramdisk *ramdisk_id*]

Options

`-c, --cert` chemin

Le fichier de certificat de clé RSA publique PEM codé de l'utilisateur.

Obligatoire : oui

`-k, --privatekey` chemin

Le chemin d'accès au fichier RSA clé PEM codé de l'utilisateur.

Obligatoire : oui

`--manifest` chemin

Chemin d'accès au fichier manifeste.

Obligatoire : oui

`-a, --access-key` access_key_id

L'ID de la clé d' AWS accès.

Requis : requis si vous utilisez le mappage automatique.

`-s, --secret-key` secret_access_key

La clé d'accès AWS secrète.

Requis : requis si vous utilisez le mappage automatique.

`--region` région

Région à rechercher dans le fichier de mappage.

Requis : requis si vous utilisez le mappage automatique.

`--no-mapping`

Désactive le mappage automatique des noyaux et des disques. RAM

Pendant la migration, Amazon EC2 remplace le noyau et le RAM disque du fichier manifeste par un noyau et un RAM disque conçus pour la région de destination. Si le paramètre `--no-mapping` n'est pas fourni, `ec2-migrate-bundle` peut utiliser les opérations `DescribeRegions` et `DescribeImages` pour effectuer les mappages automatiques.

Requis : requis si vous ne fournissez pas les options `-a`, `-s` et `--region` utilisées pour le mappage automatique.

`--ec2cert` chemin

Le chemin d'accès au certificat de clé publique Amazon EC2 X.509 utilisé pour chiffrer le manifeste d'image.

Les régions `us-gov-west-1`et `cn-north-1` utilisent un certificat de clé publique par défaut. Le chemin d'accès à ce certificat doit être spécifié avec cette option. Le chemin d'accès au certificat varie en fonction de la méthode d'installation des AMI outils. Pour Amazon Linux, les certificats se trouvent à l'adresse `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Si vous avez installé les AMI outils à partir du ZIP fichierConfigurer les EC2 AMI outils Amazon, les certificats se trouvent à l'adresse`$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obligatoire : uniquement pour les régions `us-gov-west-1` et `cn-north-1`.

`--kernel` kernel_id

ID du noyau à sélectionner.

> **Important**
>
> Nous vous recommandons d'utiliser PV- GRUB plutôt que des noyaux et des RAM disques. Pour plus d'informations, consultez la section Noyaux fournis par l'utilisateur dans le guide de l'utilisateur Amazon Linux 2.

Obligatoire : non

`--ramdisk` ramdisk_id

ID du RAM disque à sélectionner.

> **Important**
>
> Nous vous recommandons d'utiliser PV- GRUB plutôt que des noyaux et des RAM disques. Pour plus d'informations, consultez la section Noyaux fournis par l'utilisateur dans le guide de l'utilisateur Amazon Linux 2.

Obligatoire : non

Sortie

Messages d'état décrivant les étapes et le statut du processus de groupement.

Exemple

Cet exemple copie les AMI informations spécifiées dans le `my-ami.manifest.xml` manifeste des États-Unis vers l'UE.

```
[ec2-user ~]$ ec2-migrate-manifest --manifest my-ami.manifest.xml
 --cert cert-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --privatekey pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --region eu-west-1
```

```
Backing up manifest...
Successfully migrated my-ami.manifest.xml It is now suitable for use in eu-west-1.
```

ec2-unbundle

Description

Recrée le bundle à partir d'un système Linux basé sur le stockage d'instance. AMI

Syntaxe

ec2-unbundle -k *path* -m *path* [-s *source_directory*] [-d *destination_directory*]

Options

`-k, --privatekey` chemin

Le chemin d'accès à votre fichier RSA clé PEM codé.

Obligatoire : oui

`-m, --manifest` chemin

Chemin d'accès au fichier manifeste.

Obligatoire : oui

`-s, --source` source_directory

Répertoire contenant le groupe.

Par défaut : le répertoire actuel.

Obligatoire : non

`-d, --destination` destination_directory

Le répertoire dans lequel dégrouper leAMI. Le répertoire de destination doit exister.

Par défaut : le répertoire actuel.

Obligatoire : non

Exemple

Cet UNIX exemple de Linux déregroupe les informations AMI spécifiées dans le `image.manifest.xml` fichier.

```
[ec2-user ~]$ mkdir unbundled
$ ec2-unbundle -m mybundle/image.manifest.xml -k pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -s mybundle -d unbundled
$ ls -l unbundled
total 1025008
-rw-r--r-- 1 root root 1048578048 Aug 25 23:46 image.img
```

Sortie

Les messages d'état indiquant les différentes étapes du processus de dégroupement s'affichent.

ec2-upload-bundle

Description

Télécharge le bundle pour une instance Linux basée sur le stockage sur Amazon AMI S3 et définit les listes de contrôle d'accès (ACLs) appropriées sur les objets chargés. Pour de plus amples informations, veuillez consulter Création d'une instance sauvegardée en magasin AMI.

> **Note**
>
> Pour télécharger des objets dans un compartiment S3 pour votre instance Linux basée sur le stockageAMI, vous ACLs devez activer le compartiment. Dans le cas contraire, Amazon ne EC2 sera pas en mesure ACLs de définir les objets à télécharger. Si votre compartiment de destination utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, cela ne fonctionnera pas car ils ACLs sont désactivés. Pour plus d'informations, consultez la section Contrôle de la propriété des objets chargés à l'aide de la propriété de l'objet S3.

Syntaxe

```
ec2-upload-bundle -b bucket -a access_key_id -s secret_access_key [-t
token] -m path [--url url] [--region region] [--sigv version] [--acl acl]
[-d directory] [--part part] [--retry] [--skipmanifest]
```

Options

`-b, --bucket` bucket

Nom du compartiment Amazon S3 dans lequel stocker le groupe, suivi d'un préfixe de chemin séparé par des « / » facultatif. Si le compartiment n'existe pas, il est créé si le nom de compartiment est disponible. En outre, si le bucket n'existe pas et que la version AMI des outils est 1.5.18 ou ultérieure, cette commande définit le ACLs bucket.

Obligatoire : oui

`-a, --access-key` access_key_id

L'identifiant de votre clé d' AWS accès.

Obligatoire : oui

`-s, --secret-key` secret_access_key

Votre clé d'accès AWS secrète.

Obligatoire : oui

`-t, --delegation-token` jeton

Le jeton de délégation à transmettre à la AWS demande. Pour plus d'informations, consultez Utilisation des autorisations de sécurité temporaires.

Requis : uniquement lorsque vous utilisez des informations d'identification de sécurité temporaires.

Par défaut : valeur de la variable d'environnement `AWS_DELEGATION_TOKEN` (si elle est définie).

`-m, --manifest` chemin

Chemin d'accès au fichier manifeste. Le fichier manifeste est créé pendant la création d'un bundle ; il est disponible dans le répertoire contenant le groupe.

Obligatoire : oui

`--url` url

Obsolète. Utilisez plutôt l'option `--region`, sauf si votre compartiment est limité à l'emplacement `EU` (et pas `eu-west-1`). L'indicateur `--location` est le seul moyen de cibler cette restriction d'emplacement spécifique.

Le service de point de terminaison Amazon S3URL.

Par défaut: `https://s3.amazonaws.com/`

Obligatoire : non

`--region` région

Région à utiliser dans la signature de la demande pour le compartiment de destination S3.

- Si le compartiment n'existe pas et que vous ne spécifiez pas une région, l'outil crée le compartiment sans contrainte d'emplacement (dans `us-east-1`).
- Si le compartiment n'existe pas et que vous spécifiez une région, l'outil crée le compartiment dans la région spécifiée.
- Si le compartiment existe et que vous ne spécifiez pas une région, l'outil utilise emplacement du compartiment.
- Si le compartiment existe et que vous spécifiez `us-east-1` comme région, l'outil utilise l'emplacement du compartiment sans aucun message d'erreur, tous les fichiers correspondants existants sont écrasés.
- Si le compartiment existe et que vous spécifiez une région (autre que `us-east-1`) qui ne correspond pas à l'emplacement du compartiment, l'outil se termine avec une erreur.

Si votre compartiment est limité à l'emplacement `EU` (et pas `eu-west-1`), utilisez plutôt l'indicateur `--location`. L'indicateur `--location` est le seul moyen de cibler cette restriction d'emplacement spécifique.

Par défaut : `us-east-1`

Requis : requis si vous utilisez Signature Version `4`

`--sigv` version

Version de signature à utiliser lors de la signature de la demande.

Valeurs valides : `2` | `4`

Par défaut: `4`

Obligatoire : non

`--acl` acl

Stratégie de liste de contrôle des accès de l'image groupée.

Valeurs valides : `public-read` | `aws-exec-read`

Par défaut: `aws-exec-read`

Obligatoire : non

`-d, --directory` directory

Le répertoire contenant les AMI pièces groupées.

Par défaut : le répertoire contenant le fichier manifeste (cf. l'option `-m`).

Obligatoire : non

`--part` part

Commence le chargement de la partie spécifiée et de toutes les parties suivantes. Par exemple, `--part 04`.

Obligatoire : non

`--retry`

Refait automatiquement des tentatives sur toutes les erreurs Amazon S3, jusqu'à cinq fois par opération.

Obligatoire : non

`--skipmanifest`

Ne charge pas le fichier manifeste.

Obligatoire : non

`--location` location

Obsolète. Utilisez plutôt l'option `--region`, sauf si votre compartiment est limité à l'emplacement EU (et pas `eu-west-1`). L'indicateur `--location` est le seul moyen de cibler cette restriction d'emplacement spécifique.

Contrainte d'emplacement du compartiment Amazon S3 de destination. Si le compartiment existe et que vous spécifiez un emplacement qui ne correspond pas à l'emplacement du compartiment, l'outil se termine avec une erreur. Si le compartiment existe et que vous ne spécifiez pas d'emplacement, l'outil utilise emplacement du compartiment. Si le compartiment n'existe pas et que vous spécifiez un emplacement, l'outil crée le compartiment dans l'emplacement spécifié.

Si le compartiment n'existe pas et que vous ne spécifiez pas d'emplacement, l'outil crée le compartiment sans contrainte d'emplacement (dans `us-east-1`).

Par défaut : si `--region` est spécifié, l'emplacement est défini sur cette région spécifiée. Si `--region`n'est pas spécifié, l'emplacement par défaut est `us-east-1`.

Obligatoire : non

Sortie

Amazon EC2 affiche des messages d'état indiquant les étapes et le statut du processus de téléchargement.

Exemple

Cet exemple télécharge le groupe spécifié par le fichier manifeste `image.manifest.xml`.

```
[ec2-user ~]$ ec2-upload-bundle -b amzn-s3-demo-bucket/bundles/bundle_name -m
 image.manifest.xml -a your_access_key_id -s your_secret_access_key
Creating bucket...
Uploading bundled image parts to the S3 bucket amzn-s3-demo-bucket ...
Uploaded image.part.00
Uploaded image.part.01
Uploaded image.part.02
Uploaded image.part.03
Uploaded image.part.04
Uploaded image.part.05
Uploaded image.part.06
Uploaded image.part.07
Uploaded image.part.08
Uploaded image.part.09
Uploaded image.part.10
Uploaded image.part.11
Uploaded image.part.12
Uploaded image.part.13
Uploaded image.part.14
Uploading manifest ...
Uploaded manifest.
Bundle upload completed.
```

Options courantes pour les AMI outils

La plupart des AMI outils acceptent les paramètres facultatifs suivants.

`--help, -h`

Affiche le message d'aide.

`--version`

Affiche la version et l'avis de droit d'auteur.

`--manual`

Affiche l'entrée manuelle.

`--batch`

S'exécute en mode de traitement par lots et supprime les invites interactives.

`--debug`

Affiche les informations qui peuvent être utiles pour la résolution de problèmes.

Convertissez votre instance sauvegardée par le stockage en une instance sauvegardée par -backed AMI EBS AMI

Vous pouvez convertir un système Linux basé sur un stockage d'instance AMI que vous possédez en un système Linux soutenu par AmazonEBS. AMI

> **Important**
>
> Vous ne pouvez pas convertir une AMI personne que vous ne possédez pas.

Pour convertir une instance sauvegardée en stockage en instance soutenue par AMI Amazon EBS AMI

1. Lancez une instance Amazon Linux à partir d'une instance EBS soutenue par AMI Amazon. Pour de plus amples informations, veuillez consulter Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console. Les AMI outils AWS CLI et sont préinstallés sur les instances Amazon Linux.
2. Téléchargez la clé privée X.509 que vous avez utilisée pour regrouper votre instance sauvegardée en magasin AMI dans votre instance. Nous utilisons cette clé pour garantir que vous et Amazon êtes les seuls à EC2 pouvoir accéder à votreAMI.

a. Créez un répertoire temporaire sur votre instance pour votre clé privée X.509 en suivant ce qui suit :

```
[ec2-user ~]$ mkdir /tmp/cert
```

b. Copiez votre clé privée X.509 depuis votre ordinateur vers le répertoire `/tmp/cert` de votre instance en utilisant un outil de copie sécurisé comme scp. Le *my-private-key* Le paramètre de la commande suivante est la clé privée que vous utilisez pour vous connecter à votre instanceSSH. Par exemple :

```
you@your_computer:~ $ scp -i my-private-key.pem /
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
```

3. Configurez vos variables d'environnement pour utiliser l' AWS CLI. Pour plus d'informations, consultez la section Variables d'environnement.

a. (Recommandé) Définissez des variables d'environnement pour votre clé AWS d'accès, votre clé secrète et votre jeton de session.

```
[ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
[ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
[ec2-user ~]$ export AWS_SESSION_TOKEN=your_session_token
```

b. Définissez des variables d'environnement pour votre clé AWS d'accès et votre clé secrète.

```
[ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
[ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
```

4. Préparez un volume Amazon Elastic Block Store (AmazonEBS) pour votre nouveauAMI.

a. Créez un EBS volume vide dans la même zone de disponibilité que votre instance à l'aide de la commande create-volume. Notez l'ID du volume dans la sortie de la commande.

> **Important**
>
> Ce EBS volume doit être de taille identique ou supérieure à celle du volume racine de stockage de l'instance d'origine.

```
[ec2-user ~]$ aws ec2 create-volume --size 10 --region us-west-2 --
availability-zone us-west-2b
```

b. Attachez le volume à votre instance basée sur Amazon EBS à l'aide de la commande attach-volume.

```
[ec2-user ~]$ aws ec2 attach-volume --volume-id volume_id --instance-
id instance_id --device /dev/sdb --region us-west-2
```

5. Créez un dossier pour votre groupe.

```
[ec2-user ~]$ mkdir /tmp/bundle
```

6. Téléchargez le bundle pour votre instance basée sur le magasin AMI à `/tmp/bundle` l'aide de la ec2-download-bundle commande.

```
[ec2-user ~]$ ec2-download-bundle -b amzn-s3-demo-bucket/bundle_folder/bundle_name
 -m image.manifest.xml -a $AWS_ACCESS_KEY_ID -s $AWS_SECRET_ACCESS_KEY --
privatekey /path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d /tmp/bundle
```

7. Reconstituez le fichier image à partir du groupe en utilisant la commande ec2-unbundle.

a. Déplacez les répertoires vers le dossier du groupe.

```
[ec2-user ~]$ cd /tmp/bundle/
```

b. Exécutez la commande ec2-unbundle.

```
[ec2-user bundle]$ ec2-unbundle -m image.manifest.xml --privatekey /path/to/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem
```

8. Copiez les fichiers de l'image dégroupée vers le nouveau EBS volume.

```
[ec2-user bundle]$ sudo dd if=/tmp/bundle/image of=/dev/sdb bs=1M
```

9. Examinez le volume pour voir si de nouvelles partitions ont été dégroupées.

```
[ec2-user bundle]$ sudo partprobe /dev/sdb1
```

10. Affichez les périphériques de stockage en mode bloc pour trouver le nom du périphérique à monter.

```
[ec2-user bundle]$ lsblk
NAME         MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
/dev/sda    202:0    0   8G  0 disk
##/dev/sda1 202:1    0   8G  0 part /
/dev/sdb    202:80   0  10G  0 disk
##/dev/sdb1 202:81   0  10G  0 part
```

Dans cet exemple, la partition à monter est `/dev/sdb1`, mais le nom de votre périphérique sera probablement différent. Si votre volume n'est pas partitionné, l'appareil à monter sera similaire à `/dev/sdb` (sans chiffre de fin de partition de périphérique).

11. Créez un point de montage pour le nouveau EBS volume et montez le volume.

```
[ec2-user bundle]$ sudo mkdir /mnt/ebs
[ec2-user bundle]$ sudo mount /dev/sdb1 /mnt/ebs
```

12. Ouvrez le `/etc/fstab` fichier sur le EBS volume avec votre éditeur de texte préféré (tel que vim ounano) et supprimez toutes les entrées, par exemple stocker des volumes (éphémères). Le EBS volume étant monté dessus`/mnt/ebs`, le `fstab` fichier se trouve à l'emplacement`/mnt/ebs/etc/fstab`.

```
[ec2-user bundle]$ sudo nano /mnt/ebs/etc/fstab
#
LABEL=/     /           ext4    defaults,noatime  1   1
tmpfs       /dev/shm    tmpfs   defaults        0   0
devpts      /dev/pts    devpts  gid=5,mode=620  0   0
sysfs       /sys        sysfs   defaults        0   0
proc        /proc       proc    defaults        0   0
/dev/sdb        /media/ephemeral0       auto    defaults,comment=cloudconfig    0
     2
```

Dans cet exemple, la dernière ligne devrait être supprimée.

13. Démontez le volume et détachez-le de l'instance.

```
[ec2-user bundle]$ sudo umount /mnt/ebs
[ec2-user bundle]$ aws ec2 detach-volume --volume-id volume_id --region us-west-2
```

14. Créez et AMI à partir du nouveau EBS volume comme suit.

a. Créez un instantané du nouveau EBS volume.

```
[ec2-user bundle]$ aws ec2 create-snapshot --region us-west-2 --description
 "your_snapshot_description" --volume-id volume_id
```

b. Vérifiez si votre instantané est terminé.

```
[ec2-user bundle]$ aws ec2 describe-snapshots --region us-west-2 --snapshot-
id snapshot_id
```

c. Identifiez l'architecture du processeur, le type de virtualisation et l'image du noyau (`aki`) utilisés sur l'original à l'AMIaide de la describe-images commande. Pour cette étape, vous avez besoin de l'AMIID de l'instance d'origine sauvegardée AMI en magasin.

```
[ec2-user bundle]$ aws ec2 describe-images --region us-west-2 --image-id ami-id
 --output text
IMAGES x86_64 amazon/amzn-ami-pv-2013.09.2.x86_64-s3 ami-8ef297be amazon
 available public machine aki-fc8f11cc instance-store paravirtual xen
```

Dans cet exemple, l'architecture est `x86_64` et l'ID de l'image noyau est `aki-fc8f11cc`. Utilisez ces valeurs dans l'étape suivante. Si le résultat de la commande ci-dessus liste aussi un ID `ari`, prenez également note de cela.

d. Enregistrez votre nouveau volume AMI avec l'ID instantané de votre nouveau EBS volume et les valeurs de l'étape précédente. Si la sortie de la commande précédente a répertorié un ID `ari`, incluez-le dans la commande suivante avec `--ramdisk-id` *`ari_id`*.

```
[ec2-user bundle]$ aws ec2 register-image --region us-west-2 --
name your_new_ami_name --block-device-mappings DeviceName=device-
name,Ebs={SnapshotId=snapshot_id} --virtualization-type paravirtual --
architecture x86_64 --kernel-id aki-fc8f11cc --root-device-name device-name
```

15. (Facultatif) Après avoir vérifié que vous pouvez lancer une instance à partir de votre nouvelle instanceAMI, vous pouvez supprimer le EBS volume que vous avez créé pour cette procédure.

```
aws ec2 delete-volume --volume-id volume_id
```

Créez un Amazon à EC2 AMI l'aide de Windows Sysprep

L'outil Microsoft System Preparation (Windows Sysprep) crée une version généralisée du système d'exploitation, la configuration système spécifique à l'instance étant supprimée avant de capturer une nouvelle image.

Nous vous recommandons d'utiliser EC2Image Builder pour automatiser la création, la gestion et le déploiement d'images de serveur personnalisées, sécurisées et up-to-date « dorées », préinstallées et préconfigurées avec des logiciels et des paramètres.

Vous pouvez également utiliser Windows Sysprep pour créer une norme à AMI l'aide des agents de lancement Windows. Pour de plus amples informations, veuillez consulter the section called “Utiliser Windows Sysprep avec un agent de lancement”.

> **Important**
>
> N'utilisez pas Windows Sysprep pour créer une sauvegarde d'instance. Windows Sysprep supprime les informations spécifiques au système ; la suppression de ces informations peut avoir des conséquences imprévues sur la sauvegarde d'une instance.

Pour résoudre les problèmes liés à Windows Sysprep, consultez. Résoudre les problèmes liés à Sysprep avec les instances Amazon Windows EC2

Table des matières

Phases de Windows Sysprep

Windows Sysprep exécute les phases suivantes :

- Généraliser : l'outil Sysprep supprime les informations et les configurations spécifiques à l'image. Par exemple, Windows Sysprep supprime l'identifiant de sécurité (SID), le nom de l'ordinateur, les journaux d'événements et des pilotes spécifiques, pour n'en citer que quelques-uns. Une fois cette phase terminée, le système d'exploitation (OS) est prêt à créer unAMI.

> **Note**
>
> Lorsque vous exécutez Windows Sysprep avec les agents de lancement Windows, le système empêche la suppression des pilotes car il `PersistAllDeviceInstalls` est défini sur true par défaut.

- Specialize : la fonctionnalité Plug and Play analyse l'ordinateur et installe les pilotes de tous les périphériques détectés. L'outil Sysprep génère les exigences du système d'exploitation, telles que le nom de l'ordinateur et. SID Vous pouvez éventuellement exécuter des commandes dans cette phase.
- Expérience prête à l'emploi (OOBE) : le système exécute une version abrégée du programme d'installation de Windows et vous demande de saisir des informations telles que la langue du système, le fuseau horaire et l'organisation enregistrée. Lorsque vous exécutez Windows Sysprep avec des agents de lancement Windows, le fichier de réponses automatise cette phase.

Avant de commencer

- Avant d'exécuter Windows Sysprep, nous vous recommandons de supprimer tous les comptes d'utilisateurs locaux et tous les profils de compte autres qu'un compte administrateur unique sous lequel Windows Sysprep sera exécuté. Si vous exécutez Windows Sysprep avec des comptes et des profils supplémentaires, il peut en résulter un comportement inattendu, notamment la perte de données de profil ou l'échec de l'exécution de Windows Sysprep.
- En savoir plus sur Sysprep Overview.
- Découvrez quel support Sysprep prend en charge les rôles de serveur.

Utiliser Windows Sysprep avec un agent de lancement

Vous pouvez utiliser Windows Sysprep pour créer une Amazon Machine Image (AMI) standardisée lorsque vous démarrez avec une image sur AMI laquelle l'un des agents de lancement Windows est installé.

Utiliser Windows Sysprep avec la version v2 EC2Launch

Cette section contient des détails sur les tâches effectuées par le service EC2Launch v2 lors de la préparation de l'image. Il inclut également les étapes de création d'une norme à AMI l'aide de Windows Sysprep avec le EC2Launch service v2.

Windows Sysprep avec rubriques relatives à la version v2 EC2Launch

- Actions Windows Sysprep
- Étapes post-actions Sysprep
- Exécutez Windows Sysprep avec v2 EC2Launch

Actions Windows Sysprep

Windows Sysprep et EC2Launch v2 exécutent les actions suivantes lors de la préparation d'une image.

1. Lorsque vous sélectionnez Arrêter avec Sysprep dans la boîte de dialogue des EC2Launchparamètres, le système exécute la commande. `ec2launch sysprep`
2. EC2Launchv2 modifie le contenu du `unattend.xml` fichier en lisant la valeur de registre àHKEY_USERS\.DEFAULT\Control Panel\International\LocaleName. Ce fichier se trouve dans le répertoire suivant : `C:\ProgramData\Amazon\EC2Launch\sysprep`.
3. Le système exécute `BeforeSysprep.cmd`. Cette commande crée une clé de registre comme suit :

   reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 1 /f

   La clé de registre désactive les RDP connexions jusqu'à ce qu'elles soient réactivées. La désactivation RDP des connexions est une mesure de sécurité nécessaire car, lors de la première session de démarrage suivant l'exécution de Windows Sysprep, les connexions sont autorisées pendant une courte période et le mot de passe administrateur est vide. RDP
4. Le service EC2Launch v2 appelle Windows Sysprep en exécutant la commande suivante :

   sysprep.exe /oobe /generalize /shutdown /unattend: "C:\ProgramData\Amazon\EC2Launch \sysprep\unattend.xml"

Phase de généralisation

- EC2Launchv2 supprime les informations et les configurations spécifiques à l'image, telles que le nom de l'ordinateur et le. SID Si l'instance est membre d'un domaine, elle est supprimée du domaine. Le fichier de réponses `unattend.xml` inclut les paramètres suivants qui affectent cette phase :

  - PersistAllDeviceInstalls: ce paramètre empêche le programme d'installation de Windows de supprimer et de reconfigurer des appareils, ce qui accélère le processus de préparation des images, car Amazon a AMIs besoin de certains pilotes pour fonctionner et la redétection de ces pilotes prendrait du temps.
  - DoNotCleanUpNonPresentDevices: ce paramètre conserve les informations Plug-and-Play pour les appareils actuellement absents.
- Windows Sysprep arrête le système d'exploitation alors qu'il s'apprête à créer le. AMI Le système lance une nouvelle instance ou démarre l'instance originale.

Phase de spécialisation

Le système génère des exigences spécifiques au système d'exploitation, telles qu'un nom d'ordinateur et un. SID Le système exécute également les actions suivantes en fonction des configurations que vous spécifiez dans le fichier de réponses `unattend.xml`.

- CopyProfile: Windows Sysprep peut être configuré pour supprimer tous les profils utilisateur, y compris le profil administrateur intégré. Ce paramètre conserve le compte d'administrateur intégré afin que les personnalisations que vous effectuez sur ce compte soient transmises à la nouvelle image. La valeur par défaut est `True`.

  CopyProfileremplace le profil par défaut par le profil d'administrateur local existant. Tous les comptes auxquels vous vous connectez après avoir exécuté Windows Sysprep reçoivent une copie de ce profil et de son contenu lors de la première connexion.

  Si vous ne disposez pas de personnalisations de profil utilisateur spécifiques que vous souhaitez reporter à la nouvelle image, définissez ce paramètre sur `False`. Windows Sysprep supprimera tous les profils utilisateur (cela permet d'économiser du temps et de l'espace disque).
- TimeZone: le fuseau horaire est défini sur Temps universel coordonné (UTC) par défaut.
- Synchronous command with order 1 : le système exécute la commande suivante, qui active le compte administrateur et spécifie le mot de passe requis :

  ```
  net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER /
  PASSWORDREQ:YES
  ```
- Synchronous command with order 2 : le système brouille le mot de passe administrateur. Cette mesure de sécurité est conçue pour empêcher l'accès à l'instance une fois Windows Sysprep terminé si vous n'avez pas configuré la tâche. `setAdminAccount`

Le système exécute la commande suivante depuis le répertoire de votre agent de lancement local (`C:\Program Files\Amazon\EC2Launch\`).

```
EC2Launch.exe internal randomize-password --username Administrator
```

- Pour activer les connexions aux postes de travail à distance, le système définit la clé de `fDenyTSConnections` registre Terminal Server sur false.

OOBEphase

1. Le système spécifie les configurations suivantes à l'aide du fichier de réponses EC2Launch v2 :
   - `<InputLocale>en-US</InputLocale>`
   - `<SystemLocale>en-US</SystemLocale>`
   - `<UILanguage>en-US</UILanguage>`
   - `<UserLocale>en-US</UserLocale>`
   - `<HideEULAPage>true</HideEULAPage>`
   - `<HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>`
   - `<ProtectYourPC>3</ProtectYourPC>`
   - `<BluetoothTaskbarIconEnabled>false</BluetoothTaskbarIconEnabled>`
   - `<TimeZone>UTC</TimeZone>`
   - `<RegisteredOrganization>Amazon.com</RegisteredOrganization>`
   - `<RegisteredOwner>EC2</RegisteredOwner>`

   > **Note**
   >
   > Pendant les phases de généralisation et de spécialisation, la EC2Launch v2 surveille l'état du système d'exploitation. Si la EC2Launch version v2 détecte que le système d'exploitation est en phase Sysprep, elle publie le message suivant dans le journal système :
   > Windows est en cours de configuration. SysprepState= IMAGE _ STATE _ UNDEPLOYABLE

2. Le système exécute la EC2Launch v2.

Étapes post-actions Sysprep

Une fois Windows Sysprep terminé, la EC2Launch version v2 envoie le message suivant à la sortie de la console :

```
Windows sysprep configuration complete.
```

EC2LaunchLa v2 effectue ensuite les actions suivantes :

1. Lit le contenu du fichier `agent-config.yml` et exécute les tâches configurées.
2. Exécute toutes les tâches de l'étape `preReady`.
3. Une fois qu'il a terminé, envoie un message `Windows is ready` aux journaux du système d'instance.
4. Exécute toutes les tâches de l'étape `PostReady`.

Pour plus d'informations sur la EC2Launch version 2, consultezUtiliser l'agent EC2Launch v2 pour effectuer des tâches lors du lancement de l'instance EC2 Windows.

Exécutez Windows Sysprep avec v2 EC2Launch

Utilisez la procédure suivante pour créer une norme à AMI l'aide de Windows Sysprep avec v2. EC2Launch

1. Dans la EC2 console Amazon, recherchez AMI celui que vous souhaitez dupliquer.
2. Lancez et connectez-vous à votre instance Windows.
3. Personnalisez-la.
4. Dans le menu Démarrer de Windows, recherchez et choisissez EC2Launchles paramètres Amazon. Pour plus d'informations sur les options et les paramètres de la boîte de dialogue des EC2Launchparamètres Amazon, consultezConfigurer les paramètres EC2Launch v2 pour les instances Windows.
5. Sélectionnez Arrêter avec Sysprep ou Arrêter sans Sysprep.

Lorsque vous êtes invité à confirmer que vous souhaitez exécuter Windows Sysprep et arrêter l'instance, cliquez sur Oui. EC2LaunchLa v2 exécute Windows Sysprep. Ensuitez, vous êtes déconnecté de l'instance et l'instance est arrêtée. Si vous consultez la page Instances dans la EC2

console Amazon, l'état de l'instance passe de `Running` `Stopping` à`Stopped`. À ce stade, vous pouvez créer un à AMI partir de cette instance en toute sécurité.

Vous pouvez appeler manuellement l'outil Windows Sysprep depuis la ligne de commande à l'aide de la commande suivante :

```
"%programfiles%\amazon\ec2launch\ec2launch.exe" sysprep --shutdown=true
```

Utilisez Windows Sysprep avec EC2Launch

EC2Launchpropose un fichier de réponses par défaut et des fichiers batch pour Windows Sysprep qui automatisent et sécurisent le processus de préparation des images sur votre. AMI La modification de ces fichiers est facultative. Par défaut, ces fichiers se trouvent dans le répertoire suivant : `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.

> **Important**
>
> N'utilisez pas Windows Sysprep pour créer une sauvegarde d'instance. Windows Sysprep supprime les informations spécifiques au système. Si vous supprimez ces informations, les conséquences peuvent être néfastes pour une sauvegarde d'instance.

Windows Sysprep avec rubriques EC2Launch

- EC2Launchfichiers de réponses et de commandes pour Windows Sysprep
- Exécutez Windows Sysprep avec EC2Launch
- Mettre à jour les KMS métadonnées/routes pour Server 2016 et versions ultérieures lors du lancement d'une version personnalisée AMI

EC2Launchfichiers de réponses et de commandes pour Windows Sysprep

Le fichier de EC2Launch réponses et les fichiers batch pour Windows Sysprep sont les suivants :

`Unattend.xml`

Il s'agit du fichier de réponse par défaut. Si vous exécutez `SysprepInstance.ps1` ou choisissez ShutdownWithSysprepdans l'interface utilisateur, le système lit le paramètre à partir de ce fichier.

`BeforeSysprep.cmd`

Personnalisez ce fichier batch pour exécuter des commandes avant d'exécuter EC2Launch Windows Sysprep.

`SysprepSpecialize.cmd`

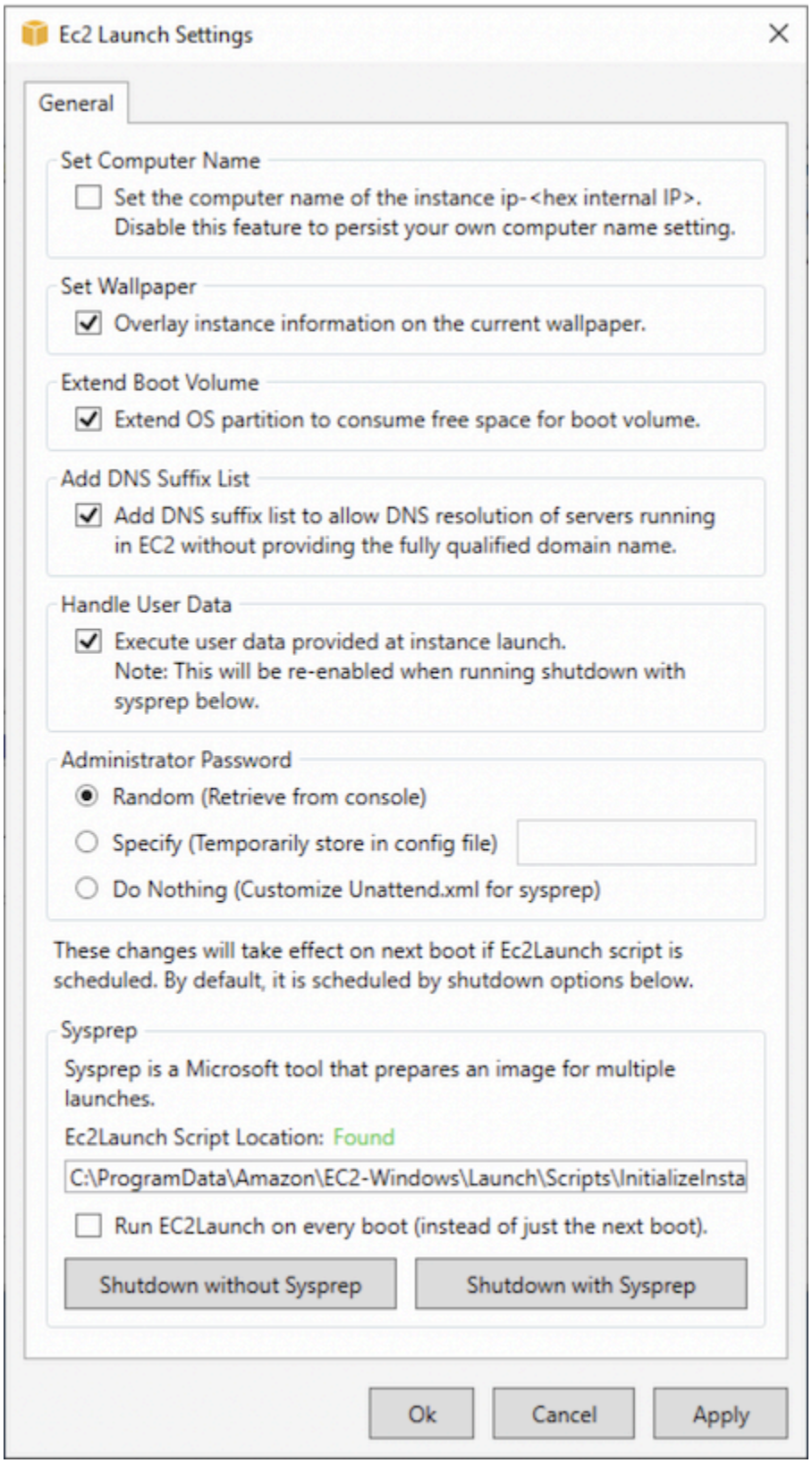
Personnalisez ce fichier batch pour exécuter des commandes pendant la phase de spécialisation de Windows Sysprep.

Exécutez Windows Sysprep avec EC2Launch

Lors de l'installation complète de Windows Server 2016 et versions ultérieures (avec une expérience de bureau), vous pouvez exécuter Windows Sysprep EC2Launch manuellement ou à l'aide de l'application Paramètres de EC2lancement.

Pour exécuter Windows Sysprep à l'aide de l'application Paramètres EC2Launch

1. Dans la EC2 console Amazon, recherchez ou créez un Windows Server 2016 ou version ultérieureAMI.
2. Lancez une instance Windows à partir duAMI.
3. Connectez-vous à votre instance Windows et personnalisez-la.
4. Recherchez et exécutez l'EC2LaunchSettingsapplication. Par défaut, le fichier se trouve dans le répertoire suivant : `C:\ProgramData\Amazon\EC2-Windows\Launch\Settings`.



5. Activez ou désactivez les options au besoin. Ces paramètres sont stockés dans le fichier `LaunchConfig.json`.

6. Pour Mot de passe administrateur, choisissez l'une des options suivantes :

   - Choisissez Random (Aléatoire). EC2Launchgénère un mot de passe et le chiffre à l'aide de la clé de l'utilisateur. Le système désactive ce paramètre après le lancement de l'instance afin que ce mot de passe persiste si l'instance est redémarrée, arrêtée ou démarrée.
   - Choisissez Specify (Spécifier) et saisissez un mot de passe conforme aux exigences de votre système. Le mot de passe est stocké `LaunchConfig.json` en texte clair et est supprimé une fois que Windows Sysprep a défini le mot de passe administrateur. Si vous arrêtez maintenant, le mot de passe est défini immédiatement. EC2Launchchiffre le mot de passe à l'aide de la clé de l'utilisateur.
   - Choisissez DoNothinget spécifiez un mot de passe dans le `unattend.xml` fichier. Si vous ne spécifiez pas de mot de passe dans `unattend.xml`, le compte d'administrateur est désactivé.

7. Choisissez Shutdown with Sysprep (Arrêter avec Sysprep).

Pour exécuter manuellement Windows Sysprep à l'aide de EC2Launch

1. Dans la EC2 console Amazon, recherchez ou créez une édition Windows Server 2016 ou ultérieure de Datacenter AMI que vous souhaitez dupliquer.
2. Lancez et connectez-vous à votre instance Windows.
3. Personnalisez l'instance.
4. Spécifiez les paramètres dans le fichier `LaunchConfig.json`. Par défaut, le fichier se trouve dans le répertoire `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

   Pour `adminPasswordType`, spécifiez l'une des valeurs suivantes :

   `Random`

   EC2Launchgénère un mot de passe et le chiffre à l'aide de la clé de l'utilisateur. Le système désactive ce paramètre après le lancement de l'instance afin que ce mot de passe persiste si l'instance est redémarrée, arrêtée ou démarrée.

   `Specify`

   EC2Launchutilise le mot de passe que vous spécifiez dans`adminPassword`. Si le mot de passe ne répond pas aux exigences du système, EC2Lauch génère un mot de passe aléatoire à la place. Le mot de passe est stocké `LaunchConfig.json` en texte clair

et est supprimé une fois que Windows Sysprep a défini le mot de passe administrateur. EC2Launchchiffre le mot de passe à l'aide de la clé de l'utilisateur.

`DoNothing`

EC2Launchutilise le mot de passe que vous avez indiqué dans le `unattend.xml` fichier. Si vous ne spécifiez pas de mot de passe dans `unattend.xml`, le compte d'administrateur est désactivé.

5. (Facultatif) Spécifiez les paramètres dans le fichier `unattend.xml` et autres fichiers de configuration. Si vous prévoyez une installation avec assistance, vous n'avez pas besoin d'apporter des modifications à ces fichiers. Par défaut, les fichiers se trouvent dans le répertoire suivant : `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.
6. Dans Windows PowerShell, exécutez`./InitializeInstance.ps1 -Schedule`. Par défaut, le script se trouve dans le répertoire suivant : `C:\ProgramData\Amazon\EC2-Windows \Launch\Scripts`. Ce script programme l'instance pour s'initialiser lors du démarrage suivant. Vous devez exécuter ce script avant d'exécuter le script `SysprepInstance.ps1` à l'étape suivante.
7. Dans Windows PowerShell, exécutez`./SysprepInstance.ps1`. Par défaut, le script se trouve dans le répertoire suivant : `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`.

Vous êtes déconnecté de l'instance et l'instance est arrêtée. Si vous consultez la page Instances dans la EC2 console Amazon, l'état de l'instance passe de `Running` à`Stopping`, puis de à`Stopped`. À ce stade, vous pouvez créer un à AMI partir de cette instance en toute sécurité.

Mettre à jour les KMS métadonnées/routes pour Server 2016 et versions ultérieures lors du lancement d'une version personnalisée AMI

Pour mettre à jour les KMS métadonnées/routes pour Server 2016 et versions ultérieures lors du lancement d'une personnalisationAMI, effectuez l'une des opérations suivantes :

- Exécutez le EC2LaunchSettings GUI (C : \ \ Amazon ProgramData \ EC2 -Windows \ Launch \ Settings \ Ec2 LaunchSettings .exe) et sélectionnez l'option permettant de l'arrêter avec Windows Sysprep.
- Exécutez EC2LaunchSettings et arrêtez sans Windows Sysprep avant de créer le. AMI Cela définit les tâches EC2 Launch Initialize à exécuter au prochain démarrage, qui définiront les itinéraires en fonction du sous-réseau de l'instance.

- Replanifiez manuellement EC2 Launch et initialisez les tâches avant de créer un formulaire. AMI PowerShell

> **Important**
>
> Prenez note du comportement de réinitialisation du mot de passe par défaut avant de replanifier les tâches.

- Pour mettre à jour les routes sur une instance en cours d'exécution qui rencontre des échecs d'activation de Windows ou de communication avec les métadonnées de l'instance, consultez « L'activation de Windows est impossible ».

Utilisez Windows Sysprep avec EC2Config

Cette section contient des détails sur les tâches effectuées par le EC2Config service lors de la préparation de l'image. Il inclut également les étapes de création d'une norme à AMI l'aide de Windows Sysprep avec le service. EC2Config

Windows Sysprep avec rubriques EC2Config

- Actions Windows Sysprep
- Étapes post-actions Sysprep
- Exécutez Windows Sysprep avec le service EC2Config

Actions Windows Sysprep

Windows Sysprep et le EC2Config service exécutent les actions suivantes lors de la préparation d'une image.

1. Lorsque vous sélectionnez Arrêter avec Sysprep dans la boîte de dialogue Propriétés du EC2 service, le système exécute la commande ec2config.exe -sysprep.
2. Le EC2Config service lit le contenu du `BundleConfig.xml` fichier. Ce fichier se trouve dans le répertoire suivant par défaut : `C:\Program Files\Amazon\Ec2ConfigService\Settings`.

   Le fichier `BundleConfig.xml` contient les paramètres suivants. Vous pouvez modifier les paramètres suivants :

- AutoSysprep: indique s'il faut utiliser Windows Sysprep automatiquement. Il n'est pas nécessaire de modifier cette valeur si vous exécutez Windows Sysprep à partir de la boîte de dialogue Propriétés du EC2 service. La valeur par défaut est `No`.
- S etRDPCertificate : définit un certificat auto-signé pour le serveur Remote Desktop. Cela vous permet d'utiliser en toute sécurité le protocole Remote Desktop (RDP) pour vous connecter à l'instance. Modifiez la valeur sur `Yes` si de nouvelles instances doivent utiliser un certificat. Ce paramètre n'est pas utilisé avec les instances de Windows Server 2012 car ces systèmes d'exploitation peuvent générer leurs propres certificats. La valeur par défaut est `No`.
- SetPasswordAfterSysprep: définit un mot de passe aléatoire sur une instance récemment lancée, la chiffre avec la clé de lancement de l'utilisateur et transmet le mot de passe chiffré à la console. Modifiez la valeur sur `No` si de nouvelles instances ne doivent pas être définies sur un mot de passe chiffré aléatoire. La valeur par défaut est `Yes`.
- PreSysprepRunCmd: emplacement de la commande à exécuter. La commande se trouve dans le répertoire suivant, par défaut : `C:\Program Files\Amazon\Ec2ConfigService\Scripts\BeforeSysprep.cmd`

3. Le système exécute `BeforeSysprep.cmd`. Cette commande crée une clé de registre comme suit :

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
 fDenyTSConnections /t REG_DWORD /d 1 /f
```

   La clé de registre désactive les RDP connexions jusqu'à ce qu'elles soient réactivées. La désactivation RDP des connexions est une mesure de sécurité nécessaire car, lors de la première session de démarrage suivant l'exécution de Windows Sysprep, les connexions sont autorisées pendant une courte période et le mot de passe administrateur est vide. RDP

4. Le EC2Config service appelle Windows Sysprep en exécutant la commande suivante :

```
sysprep.exe /unattend: "C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml" /
oobe /generalize /shutdown
```

Phase de généralisation

- L'outil supprime les informations et les configurations spécifiques à l'image, telles que le nom de l'ordinateur et le. SID Si l'instance est membre d'un domaine, elle est supprimée du domaine. Le fichier de réponses `sysprep2008.xml` inclut les paramètres suivants qui affectent cette phase :

  - PersistAllDeviceInstalls: ce paramètre empêche le programme d'installation de Windows de supprimer et de reconfigurer des appareils, ce qui accélère le processus de préparation des images, car Amazon a AMIs besoin de certains pilotes pour fonctionner et la redétection de ces pilotes prendrait du temps.
  - DoNotCleanUpNonPresentDevices: ce paramètre conserve les informations Plug-and-Play pour les appareils actuellement absents.
- Windows Sysprep arrête le système d'exploitation alors qu'il s'apprête à créer le. AMI Le système lance une nouvelle instance ou démarre l'instance originale.

Phase de spécialisation

Le système génère des exigences spécifiques au système d'exploitation, telles qu'un nom d'ordinateur et unSID. Le système exécute également les actions suivantes en fonction des configurations que vous spécifiez dans le fichier de réponses sysprep2008.xml.

- CopyProfile: Windows Sysprep peut être configuré pour supprimer tous les profils utilisateur, y compris le profil administrateur intégré. Ce paramètre conserve le compte d'administrateur intégré afin que les personnalisations que vous effectuez sur ce compte soient transmises à la nouvelle image. La valeur par défaut est True.

  CopyProfileremplace le profil par défaut par le profil d'administrateur local existant. Tous les comptes connectés après avoir exécuté Windows Sysprep recevront une copie de ce profil et de son contenu lors de la première connexion.

  Si vous ne disposez pas de personnalisations de profil utilisateur spécifiques que vous souhaitez reporter à la nouvelle image, définissez ce paramètre sur False. Windows Sysprep supprime tous les profils utilisateur, ce qui permet d'économiser du temps et de l'espace disque.
- TimeZone: le fuseau horaire est défini sur Temps universel coordonné (UTC) par défaut.
- Synchronous command with order 1 : le système exécute la commande suivante qui active le compte d'administrateur et spécifie l'exigence d'un mot de passe.

  net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER / PASSWORDREQ:YES
- Synchronous command with order 2 : le système brouille le mot de passe administrateur. Cette mesure de sécurité est conçue pour empêcher l'accès à l'instance une fois Windows Sysprep terminé si vous n'avez pas activé le paramètre ec2setpassword.

Administrateur C:\Program Files \ Amazon \ Ec2 ConfigService \ ScramblePassword .exe » -u

- Synchronous command with order 3 : le système exécute la commande suivante :

  C:\Program Files \ Amazon \ Ec2 \ Scripts ConfigService \ .cmd SysprepSpecializePhase

  Cette commande ajoute la clé de registre suivante, qui permet de réactiver RDP :

  reg add « HKEY _ LOCAL _ MACHINE \ \ SYSTEM \ Control CurrentControlSet \ Terminal Server » /v fDeny TSConnections /t REG _ /d 0 DWORD /f

OOBEphase

1. À l'aide du fichier de réponses du EC2Config service, le système définit les configurations suivantes :
   - < InputLocale InputLocale >fr-FR</ >
   - < SystemLocale SystemLocale >fr-FR</ >
   - < UILanguage UILanguage >fr-FR</ >
   - < UserLocale UserLocale >fr-FR</ >
   - <H ideEULAPage >Vrai</h > ideEULAPage
   - < HideWirelessSetupIn OOBE HideWirelessSetupIn OOBE >vrai</ >
   - < NetworkLocation NetworkLocation >Autres</ >
   - < ProtectYour PC>3</ PC> ProtectYour
   - < BluetoothTaskbarIconEnabled BluetoothTaskbarIconEnabled >fauss</ >
   - <TimeZone>UTC</TimeZone>
   - < RegisteredOrganization RegisteredOrganization >Amazon.com</ >
   - < RegisteredOwner RegisteredOwner >Amazon</ >

   > **Note**
   >
   > Pendant les phases de généralisation et de spécialisation, le EC2Config service surveille l'état du système d'exploitation. S'il EC2Config détecte que le système d'exploitation est en phase Sysprep, il publie le message suivant dans le journal système : EC2ConfigMonitorState: 0 Windows est en cours de configuration. SysprepState= IMAGE _ STATE _ UNDEPLOYABLE

2. Une fois la OOBE phase terminée, le système s'exécute `SetupComplete.cmd` à partir de l'emplacement suivant :`C:\Windows\Setup\Scripts\SetupComplete.cmd`. Dans Amazon public, AMIs avant avril 2015, ce fichier était vide et n'exécutait rien sur l'image. En public AMIs daté d'après avril 2015, le fichier inclut la valeur suivante :call "C:\Program Files\Amazon \Ec2ConfigService\Scripts\PostSysprep.cmd".
3. Le système exécute `PostSysprep.cmd`, qui effectue les opérations suivantes :
   - Permet de définir que le mot de passe d'administrateur local ne doit pas expirer. Si le mot de passe expirait, les administrateurs ne pourraient pas se connecter.
   - Définit le nom de la MSSQLServer machine (si elle est installée) afin qu'il soit synchronisé avec leAMI.

Étapes post-actions Sysprep

Une fois Windows Sysprep terminé, les EC2Config services envoient le message suivant à la sortie de la console :

```
Windows sysprep configuration complete.
   Message: Sysprep Start
   Message: Sysprep End
```

EC2Config effectue ensuite les actions suivantes :

1. Permet de lire le contenu du fichier config.xml et de répertorier tous les plugins activés.
2. Permet d'exécuter simultanément tous les plugins avant que Windows soit prêt.
   - Eco 2 SetPassword
   - Eco 2 SetComputerName
   - Eco 2 InitializeDrives
   - Eco 2 EventLog
   - Configuration d'Ec2 RDP
   - Eco 2 O utputRDPCert
   - Eco 2 SetDriveLetter
   - Eco 2 WindowsActivate
   - Eco 2 DynamicBootVolumeSize
3. Une fois terminé, il envoie un message « Windows is ready » aux journaux systèmes de l'instance.
4. Permet d'exécuter simultanément tous les plugins une fois que Windows est prêt.

- Amazon CloudWatch Logs
- UserData
- AWS Systems Manager (Systems Manager)

Pour plus d'informations sur les plugins Windows, consultez Utiliser le EC2Config service pour effectuer des tâches lors du lancement de EC2 l'ancienne instance du système d'exploitation Windows.

Exécutez Windows Sysprep avec le service EC2Config

Utilisez la procédure suivante pour créer une norme à AMI l'aide de Windows Sysprep et du service. EC2Config

1. Dans la EC2 console Amazon, recherchez ou créez AMI celui que vous souhaitez dupliquer.
2. Lancez et connectez-vous à votre instance Windows.
3. Personnalisez-la.
4. Spécifiez les paramètres de configuration dans le fichier EC2Config de réponses du service :

   ```
   C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml
   ```
5. Dans le menu Démarrer de Windows, sélectionnez Tous les programmes, puis EC2ConfigServiceParamètres.
6. Choisissez l'onglet Image dans la boîte de dialogue Ec2 Service Properties. Pour plus d'informations sur les options et les paramètres de la boîte de dialogue Ec2 Service Properties, consultez Propriétés du service EC2.
7. Sélectionnez une option pour le mot de passe de l'administrateur, puis choisissez Shutdown with Sysprep ou Shutdown without Sysprep. EC2Configmodifie les fichiers de paramètres en fonction de l'option de mot de passe que vous avez sélectionnée.
   - Aléatoire : EC2Config génère un mot de passe, le chiffre avec la clé de l'utilisateur et affiche le mot de passe chiffré sur la console. Nous désactivons ce paramètre après le premier lancement afin que ce mot de passe persiste si l'instance est redémarrée, arrêtée ou démarrée.
   - Spécifier : le mot de passe est enregistré dans le fichier de réponses Windows Sysprep sous forme non cryptée (texte clair). Lorsque Windows Sysprep s'exécute ensuite, il définit le mot de passe administrateur. Si vous arrêtez maintenant, le mot de passe est défini immédiatement. Lorsque le service redémarre, le mot de passe d'administrateur est supprimé. Il est important de vous rappeler ce mot de passe, car vous ne pourrez pas le récupérer ultérieurement.

- Continuer à exister : le mot de passe existant pour le compte administrateur ne change pas lorsque Windows Sysprep est exécuté ou EC2Config redémarré. Il est important de vous rappeler ce mot de passe, car vous ne pourrez pas le récupérer ultérieurement.

8. Choisissez OK.

Lorsque vous êtes invité à confirmer que vous souhaitez exécuter Windows Sysprep et arrêter l'instance, cliquez sur Oui. Vous remarquerez qu'il EC2Config exécute Windows Sysprep. Ensuite, vous êtes déconnecté de l'instance, et l'instance est arrêtée. Si vous consultez la page Instances dans la EC2 console Amazon, l'état de l'instance passe de `Running` à`Stopping`, puis enfin à`Stopped`. À ce stade, vous pouvez créer un à AMI partir de cette instance en toute sécurité.

Vous pouvez appeler manuellement l'outil Windows Sysprep depuis la ligne de commande à l'aide de la commande suivante :

```
"%programfiles%\amazon\ec2configservice\"ec2config.exe -sysprep""
```

> **Note**
>
> Les guillemets doubles dans la commande ne sont pas obligatoires si votre CMD shell se trouve déjà dans le répertoire C:\Program Files \ Amazon EC2ConfigService \ \.

Cependant, vous devez faire très attention à ce que les options de XML fichier spécifiées dans le `Ec2ConfigService\Settings` dossier soient correctes ; sinon, vous ne pourrez peut-être pas vous connecter à l'instance. Pour plus d'informations sur les fichiers de paramètres, consultez EC2Configfichiers de paramètres. Pour un exemple de configuration puis d'exécution de Windows Sysprep à partir de la ligne de commande, consultez. `Ec2ConfigService\Scripts\InstallUpdates.ps1`

Copier un Amazon EC2 AMI

Vous pouvez créer une copie d'une Amazon Machine Image (AMI) dans la même région ou entre les régions de la même partition. Pour copier un AMI vers une autre partition, reportez-vous à la sectionStockez et restaurez un AMI.

Table des matières

Considérations

- Autorisation de copie AMIs : vous pouvez utiliser des IAM politiques pour accorder ou refuser aux utilisateurs l'autorisation de copierAMIs. Les autorisations au niveau des ressources spécifiées pour l'`CopyImage`action s'appliquent uniquement aux nouvelles. AMI Vous ne pouvez pas spécifier d'autorisations au niveau des ressources pour la source. AMI
- Autorisations de lancement et autorisations de compartiment Amazon S3 : AWS ne copie pas les autorisations de lancement ou les autorisations de compartiment Amazon S3 de la source AMI vers la nouvelleAMI. Une fois l'opération de copie terminée, vous pouvez appliquer des autorisations de lancement et des autorisations de compartiment Amazon S3 au nouveauAMI.
- Balises : vous ne pouvez copier que les AMI balises définies par l'utilisateur que vous avez jointes à la sourceAMI. Les balises système (préfixées par `aws:`) et les balises qdéfinies par l'utilisateur qui sont attachées par d'autres Comptes AWS ne seront pas copiées. Lorsque vous copiez unAMI, vous pouvez associer de nouvelles balises à la cible AMI et à ses instantanés de sauvegarde.

Coûts

Il n'y a aucun frais pour copier unAMI. Toutefois, les taux standard de stockage et de transfert de données s'appliquent. Si vous copiez une copie EBS sauvegardéeAMI, des frais vous seront facturés pour le stockage de tout instantané supplémentaireEBS.

Accorder l'autorisation de copier Amazon EC2 AMIs

Pour copier une instance EBS sauvegardée par -back ou une instance sauvegardée par un stockageAMI, vous devez disposer des autorisations suivantes : IAM

- `ec2:CopyImage`— Pour copier leAMI. Pour EBS -backedAMIs, il autorise également la copie des instantanés AMI de sauvegarde.
- `ec2:CreateTags`— Pour étiqueter la cibleAMI. Pour EBS -backedAMIs, il autorise également à baliser les instantanés AMI de sauvegarde de la cible.

Si vous copiez une instance sauvegardéeAMI, vous devez disposer des autorisations supplémentaires IAM suivantes :

- `s3:CreateBucket`— Pour créer le compartiment S3 dans la région cible pour le nouveau AMI
- `s3:GetBucketAcl`— Pour lire les ACL autorisations associées au compartiment source
- `s3:ListAllMyBuckets`— Pour rechercher un compartiment S3 existant pour AMIs la région cible
- `s3:GetObject`— Pour lire les objets du bucket source
- `s3:PutObject`— Pour écrire les objets dans le compartiment cible
- `s3:PutObjectAcl`— Pour écrire les autorisations pour les nouveaux objets dans le compartiment cible

Exemple IAM de politique pour copier un fichier EBS sauvegardé AMI et baliser la cible AMI et les instantanés

L'exemple de politique suivant vous autorise à copier n'importe quel fichier EBS -backed AMI et à étiqueter la cible AMI et ses instantanés de sauvegarde.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "PermissionToCopyAllImages",
        "Effect": "Allow",
        "Action": [
            "ec2:CopyImage",
            "ec2:CreateTags"
        ],
        "Resource": "arn:aws:ec2:*::image/*"
    }]
}
```

Exemple IAM de politique pour copier un instantané EBS sauvegardé AMI mais refuser de baliser les nouveaux instantanés

L'`ec2:CopySnapshot`autorisation est automatiquement accordée lorsque vous l'`ec2:CopyImage`obtenez. Cela inclut l'autorisation de baliser les nouveaux instantanés de sauvegarde de la cibleAMI. L'autorisation de baliser les nouveaux instantanés de sauvegarde peut être explicitement refusée.

L'exemple de politique suivant vous autorise à copier n'importe quel EBS cliché sauvegardéAMI, mais vous interdit de baliser les nouveaux instantanés de sauvegarde de la cible. AMI

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        },
        {
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:::snapshot/*"
        }
    ]
}
```

Exemple IAM de politique pour copier une instance sauvegardée en magasin AMI et baliser la cible AMI

L'exemple de politique suivant vous autorise à copier toute instance sauvegardée AMI dans le compartiment source spécifié vers la région spécifiée et à étiqueter la cible. AMI

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "PermissionToCopyAllImages",
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": [
```

```
                "arn:aws:s3:::*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:PutObjectAcl",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amis-for-account-in-region-hash"
            ]
        }
    ]
}
```

Pour trouver le nom de ressource Amazon (ARN) du compartiment AMI source, ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/, dans le volet de navigation AMIs, sélectionnez et recherchez le nom du compartiment dans la colonne Source.

> **Note**
>
> L'`s3:CreateBucket`autorisation n'est requise que la première fois que vous copiez une instance sauvegardée en magasin dans une AMI région spécifique. Ensuite, le compartiment Amazon S3 déjà créé dans la région est utilisé pour stocker toutes les futures copies AMIs que vous copierez dans cette région.

Copier une AMI

Vous pouvez copier un AMI en utilisant les procédures suivantes.

Console

Pour copier un AMI

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation de la console, sélectionnez la région qui contient leAMI.
3. Dans le volet de navigation, choisissez AMIsd'afficher la liste des options AMIs disponibles dans la région.
4. Si le filtre que AMI vous souhaitez copier ne s'affiche pas, choisissez un autre filtre. Vous pouvez filtrer en fonction de mon AMIs propriétaire, d'images privées, d'images publiques et d'images désactivées.
5. Sélectionnez le AMI à copier, puis choisissez Actions, Copier AMI.
6. Sur la AMI page Copier, spécifiez les informations suivantes :

   a. AMIcopyname : nom du nouveauAMI. Vous pouvez inclure les informations du système d'exploitation dans le nom, car Amazon EC2 ne fournit pas ces informations lors de l'affichage des informations sur leAMI.

   b. AMIdescription de la copie : par défaut, la description inclut des informations sur la source AMI afin que vous puissiez distinguer une copie de son original. Vous pouvez modifier cette description si nécessaire.

   c. Région de destination : région dans laquelle copier leAMI. Pour de plus amples informations, veuillez consulter Copie entre régions.

   d. Copier les balises : cochez cette case pour inclure les AMI balises définies par l'utilisateur lorsque vous copiez leAMI. Les balises système (préfixées par `aws:`) et les balises qdéfinies par l'utilisateur qui sont attachées par d'autres Comptes AWS ne seront pas copiées.

   e. (EBS-backed AMIs uniquement) Chiffrer les EBS instantanés de AMI copie : cochez cette case pour chiffrer les instantanés cibles ou pour les rechiffrer à l'aide d'une autre clé. Si le chiffrement est activé par défaut, la case Chiffrer les EBS instantanés de AMI copie est cochée et ne peut pas être désactivée. Pour de plus amples informations, veuillez consulter Chiffrement et copie.

   f. clé (EBSsauvegardée AMIs uniquement) : KMSKMSclé à utiliser pour chiffrer les instantanés cibles.

   g. Balises : vous pouvez étiqueter les nouveaux AMI et les nouveaux instantanés avec les mêmes balises, ou vous pouvez les étiqueter avec des balises différentes.

- Pour étiqueter les nouveaux AMI et les nouveaux instantanés avec les mêmes balises, choisissez Marquer ensemble l'image et les instantanés. Les mêmes balises sont appliquées au nouveau cliché AMI et à chaque instantané créé.
- Pour étiqueter les nouveaux AMI et les nouveaux instantanés avec des balises différentes, choisissez Marquer l'image et les instantanés séparément. Différentes balises sont appliquées aux nouveaux instantanés AMI et aux instantanés créés. Notez toutefois que tous les nouveaux instantanés créés reçoivent les mêmes balises ; vous ne pouvez pas étiqueter chaque nouvel instantané avec une balise différente.

(Facultatif) Pour ajouter une balise, sélectionnez Add tag (Ajouter une balise) et saisissez la clé et la valeur de la balise. Répétez l'opération pour chaque étiquette.

h. Lorsque vous êtes prêt à copier leAMI, choisissez Copier AMI.

Le statut initial du nouveau AMI est`Pending`. L'opération de AMI copie est terminée lorsque le statut est défini`Available`.

AWS CLI

Pour copier et AMI utiliser le AWS CLI

Vous pouvez copier un à AMI l'aide de la commande copy-image. Vous devez indiquer les régions source et de destination. Vous spécifiez la région source à l'aide du paramètre `--source-region`. Vous pouvez spécifier la région de destination à l'aide du paramètre `--region` ou d'une variable d'environnement. Pour plus d'informations, voir Configuration de l'interface de ligne de AWS commande.

(EBS-backed AMIs uniquement) Lorsque vous chiffrez un instantané cible pendant la copie, vous devez spécifier les paramètres supplémentaires suivants : `--encrypted` et. `--kms-key-id`

Pour des exemples de commandes, veuillez consulter les exemples sous copy-image dans la référence des commandes AWS CLI .

PowerShell

Pour copier et AMI utiliser les Outils pour Windows PowerShell

Vous pouvez copier un à AMI l'aide de la Copy-EC2Imagecommande. Vous devez indiquer les régions source et de destination. Vous spécifiez la région source à l'aide du paramètre -

`SourceRegion`. Vous pouvez spécifier la région de destination à l'aide du paramètre `-Region` ou de la commande `Set-AWSDefaultRegion`. Pour plus d'informations, consultez la section Spécification AWS des régions.

(EBS-backed AMIs uniquement) Lorsque vous chiffrez un instantané cible pendant la copie, vous devez spécifier les paramètres supplémentaires suivants : `-Encrypted` et. `-KmsKeyId`

Arrêter la copie d'une AMI en attente

Vous pouvez arrêter une AMI copie en attente en suivant les procédures suivantes.

Console

Pour arrêter une opération de AMI copie à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation, sélectionnez la région de destination dans le sélecteur de régions.
3. Dans le volet de navigation, choisissez AMIs.
4. Sélectionnez le AMI pour arrêter la copie, puis choisissez Actions, Désenregistrer AMI.
5. Lorsque vous êtes invité à confirmer, choisissez Désenregistrer AMI.

Command line

Pour arrêter une opération de AMI copie à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez Accédez à Amazon EC2.

- deregister-image (AWS CLI)
- Unregister-EC2Image (AWS Tools for Windows PowerShell)

Comment fonctionne Amazon EC2 AMI Copy

La copie d'AMIune source produit une nouvelle source identique mais distincte AMI que nous appelons également la cibleAMI. La cible AMI possède son propre AMI identifiant unique. Vous pouvez modifier ou désenregistrer la source AMI sans aucun effet sur la cible. AMI L'inverse est également vrai.

Avec un EBS -backedAMI, chacun de ses instantanés de sauvegarde est copié sur un instantané cible identique mais distinct. Si vous copiez un AMI vers une nouvelle région, les instantanés sont des copies complètes (non incrémentielles). Si vous chiffrez des instantanés de sauvegarde non chiffrés ou si vous les chiffrez avec une nouvelle KMS clé, les instantanés sont des copies complètes (non incrémentielles). Les opérations de copie suivantes d'un AMI produisent des copies incrémentielles des instantanés de sauvegarde.

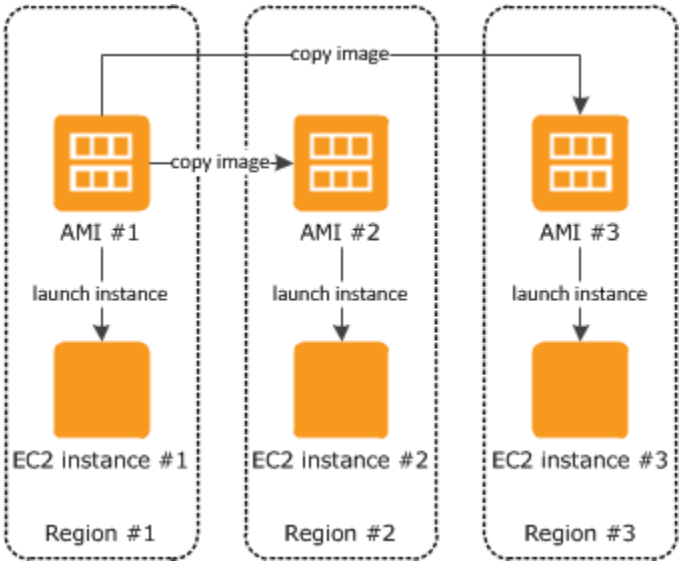
Table des matières

Copie entre régions

La copie d'une AMI région géographiquement diversifiée offre les avantages suivants :

- Déploiement mondial cohérent : le fait AMI de copier un fichier d'une région à l'autre vous permet de lancer des instances cohérentes dans différentes régions sur la base de la mêmeAMI.
- Évolutivité : vous pouvez plus facilement concevoir et créer des applications d'envergure internationale répondant aux besoins de vos utilisateurs, quel que soit l'emplacement.
- Performances : vous pouvez accroître les performances en distribuant votre application, ainsi qu'en recherchant les composants critiques de votre application plus près de vos utilisateurs. Vous pouvez également tirer parti des fonctionnalités spécifiques à la région, telles que les types d'instances ou d'autres AWS services.
- Disponibilité élevée : vous pouvez concevoir et déployer des applications dans différentes régions AWS afin d'accroître leur disponibilité.

Le schéma suivant montre la relation entre une source AMI et deux copies AMIs dans différentes régions, ainsi que les EC2 instances lancées à partir de chacune d'elles. Lorsque vous lancez une instance depuis unAMI, elle réside dans la même région que celle où elle AMI réside. Si vous apportez des modifications à la source AMI et souhaitez que ces modifications soient reflétées AMIs dans les régions cibles, vous devez recopier la source dans AMI les régions cibles.



Lorsque vous copiez AMI pour la première fois une instance sauvegardée en magasin dans une région, nous créons un compartiment Amazon S3 pour l'instance AMIs copiée dans cette région. Toutes les instances sauvegardées AMIs que vous copiez dans cette région sont stockées dans ce compartiment. Les noms des compartiments ont le format suivant : amis-for-*account*-dans-*region*-*hash*. Par exemple :`amis-for-123456789012-in-us-east-2-yhjmxvp6`.

Prérequis

Avant de copier uneAMI, vous devez vous assurer que le contenu de la source AMI est mis à jour pour permettre l'exécution dans une autre région. Par exemple, vous devez mettre à jour toutes les chaînes de connexion à la base de données ou des données de configuration d'application similaires de façon à ce qu'elles pointent vers les ressources appropriées. Dans le cas contraire, les instances lancées depuis la nouvelle instance AMI dans la région de destination peuvent toujours utiliser les ressources de la région source, ce qui peut avoir un impact sur les performances et les coûts.

Limites

- Les régions de destination sont limitées à 100 AMI copies simultanées.
- Vous ne pouvez pas copier un paravirtual (PV) AMI dans une région qui ne prend pas en charge le PV. AMIs Pour de plus amples informations, veuillez consulter Types de virtualisation.

Copie entre comptes

Si un message AMI provenant d'un autre utilisateur Compte AWS est partagé avec vous Compte AWS, vous pouvez le copierAMI. C'est ce que l'on appelle la copie entre comptes. AMICe

qui est partagé avec vous est la sourceAMI. Lorsque vous copiez la sourceAMI, vous en créez une nouvelleAMI. Le nouveau AMI est souvent appelé la cibleAMI.

AMIcoûts

- Pour un partageAMI, le compte du partage AMI est débité pour le stockage dans la Région.
- Si vous copiez un AMI message partagé avec votre compte, vous êtes le propriétaire de la cible AMI de votre compte.
  - Les frais de transfert standard d'Amazon EBS ou Amazon S3 sont facturés au propriétaire de la sourceAMI.
  - Le stockage de la cible AMI dans la région de destination vous est facturé.

Autorisations d'accès aux ressources

Pour copier un AMI fichier partagé avec vous depuis un autre compte, le propriétaire de la source AMI doit vous accorder des autorisations de lecture pour le stockage qui le sauvegardeAMI. Le stockage est soit le EBS snapshot associé (pour une instance EBS sauvegardée par AmazonAMI), soit un compartiment S3 associé (pour une instance sauvegardée en magasinAMI). Si le partage AMI contient des instantanés chiffrés, le propriétaire doit également partager la ou les clés avec vous. Pour plus d'informations sur l'octroi d'autorisations de ressources, pour les EBS instantanés, consultez Partager un EBS instantané Amazon dans le guide de EBS l'utilisateur Amazon, et pour les compartiments S3, voir Gestion des identités et des accès dans Amazon S3 dans le guide de l'utilisateur Amazon Simple Storage Service.

> **Note**
>
> Les balises associées à la source ne AMI sont pas copiées d'un compte à l'autre vers la cibleAMI.

Chiffrement et copie

Le tableau suivant indique la prise en charge du chiffrement pour différents scénarios de AMI copie. Bien qu'il soit possible de copier un instantané non chiffré pour créer un instantané chiffré, vous ne pouvez pas copier un instantané chiffré et en créer un qui ne soit pas chiffré.

Scénario	Description	Pris en charge
1	U nencrypted-to-unencrypted	Oui
2	E ncrypted-to-encrypted	Oui
3	U nencrypted-to-encrypted	Oui
4	E ncrypted-to-unencrypted	Non

> **Note**
>
> Le chiffrement effectué pendant l'`CopyImage`action s'applique uniquement aux applications soutenues EBS par AMIs Amazon. Comme une instance sauvegardée en stockage AMI ne repose pas sur des instantanés, vous ne pouvez pas utiliser la copie pour modifier son état de chiffrement.

Par défaut (c'est-à-dire sans spécifier de paramètres de chiffrement), l'instantané de sauvegarde d'un AMI est copié avec son état de chiffrement d'origine. La copie d'un instantané AMI sauvegardé par un instantané non chiffré permet d'obtenir un instantané cible identique qui est également déchiffré. Si la source AMI est sauvegardée par un instantané chiffré, sa copie permet d'obtenir un instantané cible identique qui est chiffré par la même AWS KMS clé. La copie d'un instantané AMI sauvegardé par plusieurs instantanés préserve, par défaut, l'état de chiffrement de la source dans chaque instantané cible.

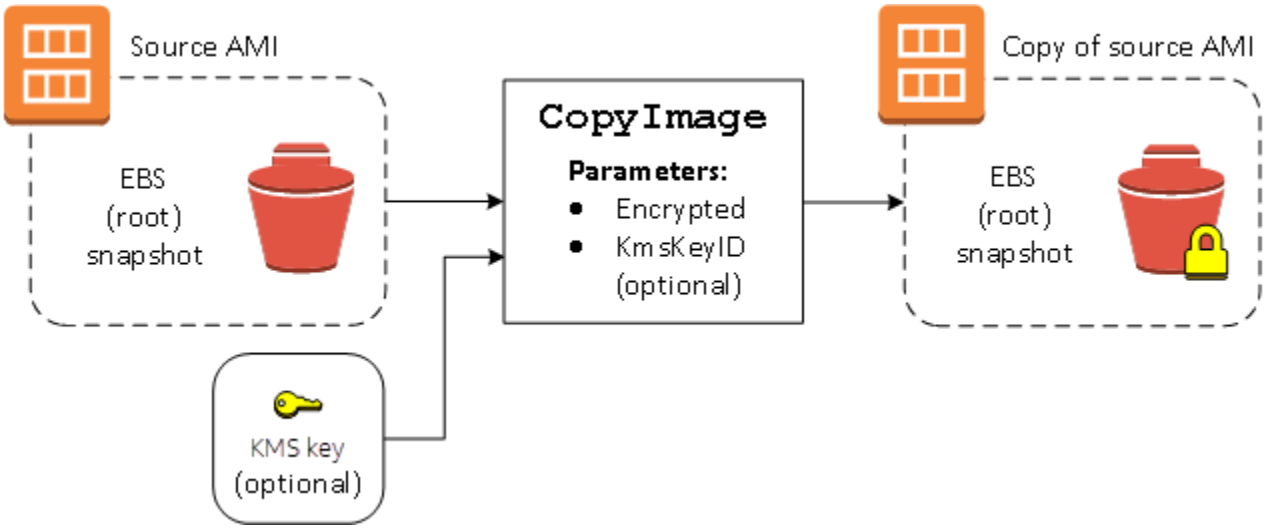
Si vous spécifiez des paramètres de chiffrement lors de la copie d'un fichierAMI, vous pouvez chiffrer ou rechiffrer ses instantanés de sauvegarde. L'exemple suivant montre un cas autre que celui par défaut qui fournit des paramètres de chiffrement à l'`CopyImage`action afin de modifier l'état AMI de chiffrement de la cible.

Copier une source non chiffrée AMI vers une cible chiffrée AMI

Dans ce scénario, un instantané racine AMI sauvegardé par un instantané non chiffré est copié vers un AMI instantané racine chiffré. L'action `CopyImage` est appelée avec deux paramètres de chiffrement, y compris une clé gérée par le client. Par conséquent, l'état de chiffrement de l'instantané racine change, de sorte que la cible AMI est soutenue par un instantané racine contenant les mêmes

données que le cliché source, mais chiffré à l'aide de la clé spécifiée. Vous devez payer des frais de stockage pour les instantanés dans les deux casAMIs, ainsi que des frais pour les instances que vous lancez à partir de l'un ou l'autre. AMI

> **Note**
>
> L'activation du chiffrement par défaut a le même effet que la définition du `Encrypted` paramètre sur `true` pour tous les instantanés duAMI.



Définir le paramètre `Encrypted` chiffre l'instantané unique de cette instance. Si vous ne spécifiez pas le paramètre `KmsKeyId`, la clé gérée par le client par défaut est utilisée pour chiffrer la copie de l'instantané.

Pour plus d'informations sur la copie AMIs avec des instantanés chiffrés, consultezUtiliser le chiffrement avec des AMI basées sur EBS.

Stockage et restauration à l'AMIaide de S3

Vous pouvez stocker une image machine Amazon (AMI) dans un compartiment Amazon S3, la AMI copier dans un autre compartiment S3, puis la restaurer à partir du compartiment S3. En stockant et en restaurant un compartiment S3 AMI en cours d'utilisation, vous pouvez copier AMIs d'une AWS partition à une autre, par exemple de la partition commerciale principale vers la AWS GovCloud (US) partition. Vous pouvez également créer des copies d'archives en les AMIs stockant dans un compartiment S3.

Les options prises en charge APIs pour le stockage et la restauration et AMI l'utilisation de S3 sont `CreateStoreImageTaskDescribeStoreImageTasks`, et`CreateRestoreImageTask`.

`CopyImage`est recommandé API pour copier AMIs au sein d'une AWS partition. Cependant, je ne `CopyImage` peux pas en AMI copier une sur une autre partition.

Pour plus d'informations sur les AWS partitions, voir *`partition`* sur la page Amazon Resource Names (ARNs) du guide de IAM l'utilisateur.

> **Warning**
>
> Assurez-vous de respecter toutes les lois et exigences commerciales applicables lorsque vous déplacez des données entre des AWS partitions ou des AWS régions, y compris, mais sans s'y limiter, les réglementations gouvernementales applicables et les exigences en matière de résidence des données.

Table des matières

Cas d'utilisation

Utilisez le magasin et la restauration APIs pour effectuer les opérations suivantes :

- Copier et AMI entre les AWS partitions
- Créez des copies d'archives de AMIs

Copier et AMI entre les AWS partitions

En stockant et en restaurant et AMI en utilisant des compartiments S3, vous pouvez les copier AMI d'une AWS partition à une autre ou d'une AWS région à une autre. Dans l'exemple suivant, vous copiez un AMI depuis la partition commerciale principale vers la AWS GovCloud (US) partition, en particulier depuis la `us-east-2` région vers la `us-gov-east-1` région.

Pour copier un fichier AMI d'une partition à une autre, procédez comme suit :

- AMIStockez-les dans un compartiment S3 de la région actuelle en utilisant`CreateStoreImageTask`. Dans cet exemple, le compartiment S3 se trouve dans `us-east-2`.
- Surveillez la progression de la tâche de stockage à l'aide de `DescribeStoreImageTasks`. L'objet devient visible dans le compartiment S3 lorsque la tâche est terminée.
- Copiez l'AMIobjet stocké dans un compartiment S3 de la partition cible à l'aide de la procédure de votre choix. Dans cet exemple, le compartiment S3 se trouve dans `us-gov-east-1`.

> **Note**
>
> Comme vous avez besoin AWS d'informations d'identification différentes pour chaque partition, vous ne pouvez pas copier un objet S3 directement d'une partition à l'autre. Le processus de copie d'un objet S3 d'une partition vers une autre n'entre pas dans le cadre de cette documentation. Les processus de copie suivants sont fournis à titre d'exemple uniquement. N'hésitez pas à utiliser celui qui répond le mieux à vos exigences de sécurité.
>
> - Pour en copier un AMI sur plusieurs partitions, le processus de copie peut être aussi simple que le suivant : téléchargez l'objet depuis le compartiment source vers un hôte intermédiaire (par exemple, une EC2 instance ou un ordinateur portable), puis téléchargez l'objet depuis l'hôte intermédiaire vers le compartiment cible. Pour chaque étape du processus, utilisez les AWS informations d'identification de la partition.
> - Pour une utilisation plus soutenue, n'hésitez pas à développer une application permettant de gérer les copies, en utilisant éventuellement des téléchargements et des chargements partitionnés S3.

- Restaurez le AMI depuis le compartiment S3 de la partition cible en utilisant`CreateRestoreImageTask`. Dans cet exemple, le compartiment S3 se trouve dans `us-gov-east-1`.
- Surveillez la progression de la tâche de restauration en décrivant le AMI pour vérifier quand son état sera disponible. Vous pouvez également suivre les pourcentages de progression des instantanés qui constituent les instantanés restaurés AMI en décrivant les instantanés.

Créez des copies d'archives de AMIs

Vous pouvez créer des copies d'archives en les AMIs stockant dans un compartiment S3. Le AMI est regroupé dans un seul objet dans S3, et toutes les AMI métadonnées (à l'exception des informations de partage) sont conservées dans le cadre du stockageAMI. Les AMI données sont compressées dans le cadre du processus de stockage. AMIsqui contiennent des données qui peuvent être facilement compressées se traduiront par des objets plus petits dans S3. Pour réduire les coûts, vous pouvez utiliser des niveaux de stockage S3 moins onéreux. Pour plus d'informations, consultez Classes de stockage Amazon S3 et les tarifs Amazon S3

Limites

- Pour stocker unAMI, vous Compte AWS devez soit posséder le AMI et ses instantanés, soit les AMI partager directement avec votre compte. Vous ne pouvez pas stocker un AMI s'il est uniquement partagé publiquement.
- Seul EBS -backed AMIs peut être stocké à l'aide de ceux-ciAPIs.
- Les systèmes paravirtuels (PV) ne AMIs sont pas pris en charge.
- La taille d'un AMI fichier (avant compression) pouvant être stocké est limitée à 5 000 Go.
- Quota sur les demandes d'image de stockage : tâche de stockage de 600 Go (données instantanées) en cours.
- Quota sur les demandes d'image de restauration : tâche de restauration de 300 Go (données d'instantanés) en cours.
- Pendant la durée de la tâche de stockage, les instantanés ne doivent pas être supprimés et le IAM principal responsable du stockage doit avoir accès aux instantanés, sinon le processus de stockage échouera.
- Vous ne pouvez pas créer plusieurs copies d'un AMI dans le même compartiment S3.
- Un AMI fichier stocké dans un compartiment S3 ne peut pas être restauré avec son AMI identifiant d'origine. Vous pouvez atténuer ce problème en utilisant l'AMIaliasing.
- Actuellement, le magasin et la restauration ne APIs sont pris en charge qu'à l'aide de AWS Command Line Interface AWS SDKs, et Amazon EC2API. Vous ne pouvez pas stocker et restaurer un fichier AMI à l'aide de la EC2 console Amazon.

Coûts

Lorsque vous stockez et restaurez AMIs à l'aide de S3, les services utilisés par le magasin et la restaurationAPIs, ainsi que le transfert de données, vous sont facturés. Ils APIs utilisent S3 et EBS

Direct API (utilisés en interne par ceux-ci APIs pour accéder aux données de capture instantanée). Pour plus d'informations, consultez les sections Tarification Amazon S3 et EBSTarification Amazon.

Comment fonctionnent AMI le stockage et la restauration

Pour stocker et restaurer un fichier à AMI l'aide de S3, vous devez utiliser ce qui suit APIs :

- `CreateStoreImageTask`— Stocke le AMI dans un compartiment S3
- `DescribeStoreImageTasks`— Indique la progression de la tâche de AMI stockage
- `CreateRestoreImageTask`— Restaure le AMI depuis un compartiment S3

Comment APIs fonctionne le travail

- CreateStoreImageTask
- DescribeStoreImageTasks
- CreateRestoreImageTask
- Chemins de fichier

CreateStoreImageTask

`CreateStoreImageTask`APIStocke un AMI en tant qu'objet unique dans un compartiment S3.

APIcrée une tâche qui lit toutes les données à partir de AMI ses instantanés, puis utilise un téléchargement partitionné S3 pour stocker les données dans un objet S3. APIIl prend tous les composants duAMI, y compris la plupart des AMI métadonnées non spécifiques à une région, et tous les EBS instantanés qu'il contientAMI, et les regroupe dans un seul objet dans S3. Les données sont compressées dans le cadre du processus de téléchargement afin de réduire l'espace utilisé dans S3. L'objet dans S3 peut donc être inférieur à la somme des tailles des instantanés duAMI.

Si des balises AMI de capture d'écran sont visibles par le compte qui l'appelleAPI, elles sont conservées.

L'objet dans S3 possède le même identifiant que leAMI, mais avec une `.bin` extension. Les données suivantes sont également stockées sous forme de balises de métadonnées S3 sur l'objet S3 : AMI nom, AMI description, date AMI d'enregistrement, compte AMI du propriétaire et horodatage du fonctionnement du magasin.

Le temps nécessaire pour terminer la tâche dépend de la taille duAMI. Il dépend également du nombre d'autres tâches en cours car les tâches sont mises en file d'attente. Vous pouvez suivre la progression de la tâche en appelant le `DescribeStoreImageTasks`API.

La somme des tailles de toutes les données AMIs en cours est limitée à 600 Go de données EBS instantanées par compte. La création d'autres tâches est rejetée jusqu'à ce que les tâches en cours soient inférieures à la limite. Par exemple, si une version AMI contenant 100 Go de données de capture instantanée et une autre AMI contenant 200 Go de données de capture sont actuellement stockées, une autre demande sera acceptée, car le total en cours est de 300 Go, ce qui est inférieur à la limite. Mais si un single AMI contenant 800 Go de données instantanées est actuellement stocké, les autres tâches sont rejetées jusqu'à ce qu'elles soient terminées.

DescribeStoreImageTasks

`DescribeStoreImageTasks`APIDécrit la progression des tâches du AMI magasin. Vous pouvez décrire les tâches pour des tâches spécifiéesAMIs. Si vous ne le spécifiez pasAMIs, vous obtenez une liste paginée de toutes les tâches liées aux images du magasin qui ont été traitées au cours des 31 derniers jours.

Pour chaque AMI tâche, la réponse indique si la tâche est `InProgress``Completed`, ou`Failed`. Pour les tâches `InProgress`, la réponse affiche une progression estimée en pourcentage.

Les tâches sont répertoriées dans l'ordre chronologique inverse.

Actuellement, seules les tâches du mois précédent peuvent être affichées.

CreateRestoreImageTask

`CreateRestoreImageTask`APIDémarre une tâche qui restaure un AMI objet S3 créé précédemment à l'aide d'une `CreateStoreImageTask` requête.

La tâche de restauration peut être exécutée dans la même région ou dans une autre région dans laquelle la tâche de stockage a été réalisée.

Le compartiment S3 à partir duquel l'AMIobjet sera restauré doit se trouver dans la même région que celle dans laquelle la tâche de restauration est demandée. Ils AMI seront restaurés dans cette région.

Le AMI est restauré avec ses métadonnées, telles que le nom, la description et les mappages de périphériques de blocs correspondant aux valeurs du périphérique stockéAMI. Le nom de ce compte doit être unique AMIs dans la région. Si vous ne fournissez pas de nom, le nouveau AMI prend le

même nom que l'originalAMI. AMIobtient un nouvel AMI identifiant généré au moment du processus de restauration.

Le temps nécessaire pour terminer la tâche de AMI restauration dépend de la taille duAMI. Il dépend également du nombre d'autres tâches en cours car les tâches sont mises en file d'attente. Vous pouvez visualiser la progression de la tâche en décrivant AMI (describe-images) ou ses EBS instantanés (describe-snapshots). Si la tâche échoue, les instantanés AMI et sont déplacés vers l'état d'échec.

La somme des tailles de tous les instantanés AMIs en cours est limitée à 300 Go (sur la base de la taille après restauration) de données EBS instantanées par compte. La création d'autres tâches est rejetée jusqu'à ce que les tâches en cours soient inférieures à la limite.

Chemins de fichier

Vous pouvez utiliser les chemins des fichiers lors du stockage et de la restaurationAMIs, de la manière suivante :

- Lorsque vous stockez un fichier AMI dans S3, le chemin du fichier peut être ajouté au nom du compartiment. En interne, le système sépare le chemin du nom du compartiment, puis ajoute le chemin à la clé d'objet générée pour stocker leAMI. Le chemin complet de l'objet est indiqué dans la réponse de l'APIappel.
- Lors de la restauration duAMI, étant donné qu'un paramètre de clé d'objet est disponible, le chemin peut être ajouté au début de la valeur de clé d'objet.

Exemple : utilisez un chemin de fichier lors du stockage et de la restauration d'un AMI (AWS CLI)

L'exemple suivant enregistre d'abord un AMI dans S3, avec le chemin du fichier ajouté au nom du compartiment. L'exemple restaure ensuite le fichier AMI à partir de S3, le chemin du fichier étant ajouté au paramètre clé de l'objet.

Lorsque vous stockez leAMI, spécifiez le chemin du fichier après le nom du bucket, comme suit :

```
aws ec2 create-store-image-task \
    --image-id ami-1234567890abcdef0 \
    --bucket amzn-s3-demo-bucket/path1/path2
```

Voici un exemple de sortie.

```
{
```

```
  "ObjectKey": "path1/path2/ami-1234567890abcdef0.bin"
}
```

Lorsque vous restaurez leAMI, spécifiez la valeur de la sortie de l'étape précédente, y compris le chemin du fichier.

```
aws ec2 create-restore-image-task \
    --object-key path1/path2/ami-1234567890abcdef0.bin \
    --bucket amzn-s3-demo-bucket \
    --name "New AMI Name"
```

Création d'une tâche d'imagerie de magasin

Lorsque vous stockez un AMI dans un compartiment S3, une tâche de stockage d'image est créée. Vous pouvez utiliser la tâche de stockage d'images pour suivre la progression et les résultats du processus.

Table des matières

Sécurisation de votre AMIs

Il est important de s'assurer que le compartiment S3 est configuré avec une sécurité suffisante pour sécuriser le contenu du AMI et que la sécurité est maintenue tant que les AMI objets restent dans le compartiment. Si cela n'est pas possible, leur utilisation n'APIsest pas recommandée. Assurez-vous qu'aucun accès public au compartiment S3 n'est autorisé. Nous recommandons d'activer le chiffrement côté serveur pour les compartiments S3 dans lesquels vous les stockezAMIs, bien que cela ne soit pas obligatoire.

Pour plus d'informations sur la définition des paramètres de sécurité appropriés pour vos compartiments S3, consultez les rubriques de sécurité suivantes :

- Blocage de l'accès public à votre stockage Amazon S3
- Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3

- Quelle politique de compartiment S3 puis-je utiliser pour me conformer à la AWS Config règle s3-bucket-ssl-requests-only ?
- Activation de la journalisation des accès au serveur Amazon S3

Lorsque les AMI instantanés sont copiés dans l'objet S3, les données sont ensuite copiées via des TLS connexions. Vous pouvez effectuer AMIs un stockage avec des instantanés chiffrés, mais ceux-ci sont déchiffrés dans le cadre du processus de stockage.

Autorisations de stockage et de restauration AMIs à l'aide de S3

Si vos IAM responsables souhaitent stocker ou restaurer à AMIs l'aide d'Amazon S3, vous devez leur accorder les autorisations requises.

L'exemple de politique suivant inclut toutes les actions requises pour permettre à un IAM mandant d'exécuter les tâches de stockage et de restauration.

Vous pouvez également créer des IAM politiques qui accordent aux principaux l'accès à des ressources spécifiques uniquement. Pour d'autres exemples de politiques, voir Gestion de l'accès aux AWS ressources dans le Guide de IAM l'utilisateur.

> **Note**
>
> Si les instantanés qui le constituent AMI sont chiffrés ou si le chiffrement est activé par défaut sur votre compte, votre IAM principal doit être autorisé à utiliser la KMS clé.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:PutObjectTagging",
                "s3:AbortMultipartUpload",
                "ebs:CompleteSnapshot",
```

```
                "ebs:GetSnapshotBlock",
                "ebs:ListChangedBlocks",
                "ebs:ListSnapshotBlocks",
                "ebs:PutSnapshotBlock",
                "ebs:StartSnapshot",
                "ec2:CreateStoreImageTask",
                "ec2:DescribeStoreImageTasks",
                "ec2:CreateRestoreImageTask",
                "ec2:GetEbsEncryptionByDefault",
                "ec2:DescribeTags",
                "ec2:CreateTags"
            ],
            "Resource": "*"
        }
    ]
}
```

Création de tâches de stockage et de restauration d'images

Pour stocker une image AMI dans un compartiment S3, commencez par créer une tâche d'image de stockage. Le temps nécessaire pour terminer la tâche dépend de la taille duAMI. Vous pouvez suivre la progression de la tâche jusqu'à ce qu'elle réussisse ou échoue.

Pour créer la tâche de stockage d'images

Utilisez la create-store-image-taskcommande. Spécifiez l'ID AMI et le nom du compartiment S3 dans lequel vous souhaitez stocker leAMI.

```
aws ec2 create-store-image-task \
    --image-id ami-1234567890abcdef0 \
    --bucket amzn-s3-demo-bucket
```

Voici un exemple de sortie.

```
{
  "ObjectKey": "ami-1234567890abcdef0.bin"
}
```

Pour décrire la progression de la tâche de stockage d'images

Utilisez la describe-store-image-taskscommande.

```
aws ec2 describe-store-image-tasks
```

Voici un exemple de sortie.

```
{
    "StoreImageTaskResults": [
        {
            "AmiId": "ami-1234567890abcdef0",
            "Bucket": "amzn-s3-demo-bucket",
            "ProgressPercentage": 17,
            "S3objectKey": "ami-1234567890abcdef0.bin",
            "StoreTaskState": "InProgress",
            "StoreTaskFailureReason": null,
            "TaskStartTime": "2022-01-01T01:01:01.001Z"
        }
    ]
}
```

Pour créer une tâche de restauration d'image

Utilisez la create-restore-image-taskcommande. À l'aide des valeurs pour `S3ObjectKey` et `Bucket` depuis la `describe-store-image-tasks` sortie, spécifiez la clé d'objet AMI et le nom du compartiment S3 dans lequel AMI elle a été copiée. Spécifiez également un nom pour la restaurationAMI. Le nom de ce compte doit être unique AMIs dans la région.

> **Note**
>
> La personne restaurée AMI reçoit un nouvel AMI identifiant.

```
aws ec2 create-restore-image-task \
    --object-key ami-1234567890abcdef0.bin \
    --bucket amzn-s3-demo-bucket \
    --name "New AMI Name"
```

Voici un exemple de sortie.

```
{
   "ImageId": "ami-0eab20fe36f83e1a8"
```

```
}
```

Vérifiez quand un Amazon EC2 AMI a été utilisé pour la dernière fois

Amazon EC2 enregistre la date et l'heure auxquelles vous avez AMI été utilisé pour la dernière fois pour lancer une instance. Si vous en avez un AMI qui n'a pas été utilisé pour lancer une instance depuis longtemps, déterminez s'il s'AMIagit d'un bon candidat à la désinscription ou à la dépréciation.

Considérations

- Lorsque le AMI est utilisé pour lancer une instance, il y a un délai de 24 heures avant que cette utilisation ne soit signalée.
- Vous devez être le propriétaire du AMI pour connaître l'heure du dernier lancement.
- Ces données AMI d'utilisation sont disponibles à partir d'avril 2017.

Console

Pour afficher l'heure du dernier lancement d'un AMI

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation de gauche, choisissez AMIs.
3. Dans la barre de filtre, choisissez Owned by me (M'appartenant).
4. Sélectionnez leAMI, puis cochez le champ Heure du dernier lancement (si vous avez coché la case à côté duAMI, elle se trouve dans l'onglet Détails). Le champ indique la date et l'heure auxquelles le AMI a été utilisé pour la dernière fois pour lancer une instance.

AWS CLI

Vous pouvez utiliser la commande describe-images ou la describe-image-attributecommande pour afficher l'heure du dernier lancement d'un fichier AMI que vous possédez.

Pour afficher l'heure du dernier lancement d'un à l'aide AMI de describe-images

Utilisez la commande describe-images et spécifiez l'ID du. AMI

```
aws ec2 describe-images --image-id ami-0123456789example --query
 "Images[*].LastLaunchedTime[].Value"
```

Voici un exemple de sortie.

```
[
    "2024-04-02T02:03:18Z"
]
```

S'il n'`LastLaunchedTime`est pas présent, vérifiez que vous êtes le propriétaire duAMI.

Pour afficher l'heure du dernier lancement d'un AMI

Utilisez la describe-image-attributecommande et spécifiez`--attribute lastLaunchedTime`. Vous devez être propriétaire du AMI pour exécuter cette commande.

```
aws ec2 describe-image-attribute \
    --image-id ami-0123456789example \
    --attribute lastLaunchedTime
```

Voici un exemple de sortie.

```
{
    "ImageId": "ami-1234567890example",
    "LastLaunchedTime": {
        "Value": "2022-02-10T02:03:18Z"
    }
}
```

Déprécier un Amazon EC2 AMI

Vous pouvez le déprécier AMI pour indiquer qu'il n'est pas à jour et ne doit pas être utilisé. Vous pouvez également spécifier une future date de dépréciation pour unAMI, en indiquant quand il AMI sera périmé. Par exemple, vous pouvez déprécier une AMI version qui n'est plus activement maintenue ou une version AMI qui a été remplacée par une version plus récente. Par défaut, les versions obsolètes n'apparaissent AMIs pas dans les AMI listes, ce qui empêche les nouveaux utilisateurs de les utiliser. out-of-date AMIs Toutefois, les utilisateurs existants et les services de lancement, tels que les modèles de lancement et les groupes Auto Scaling, peuvent continuer à utiliser un objet obsolète AMI en spécifiant son ID. Pour le supprimer AMI afin que les utilisateurs et les services ne puissent pas l'utiliser, vous devez le désenregistrer.

Une fois qu'un AMI est devenu obsolète :

- Pour AMI les utilisateurs, le terme obsolète n'apparaît AMI pas dans les DescribeImagesAPIappels, sauf si vous spécifiez son ID ou si vous ne spécifiez pas que le code obsolète doit AMIs apparaître. AMIles propriétaires continuent de voir les appels AMIs déconseillés. DescribeImagesAPI
- Pour AMI les utilisateurs, la version obsolète n'AMIest pas disponible à la sélection via la EC2 console. Par exemple, un objet obsolète n'apparaît AMI pas dans le AMI catalogue de l'assistant de lancement d'instance. AMIles propriétaires continuent d'être considérés comme obsolètes AMIs dans la EC2 console.
- Pour AMI les utilisateurs, si vous connaissez l'ID d'une instance obsolèteAMI, vous pouvez continuer à lancer des instances à l'aide de la version obsolète en AMI utilisant leAPI, CLI ou le. SDKs
- Les services de lancement, tels que les modèles de lancement et les groupes Auto Scaling, peuvent continuer à faire référence à des services obsolètesAMIs.
- EC2les instances lancées à l'aide d'une AMI instance devenue obsolète par la suite ne sont pas affectées et peuvent être arrêtées, démarrées et redémarrées.

Vous pouvez déprécier à la fois le privé et le public. AMIs

Vous pouvez également créer des politiques basées sur Amazon Data Lifecycle Manager pour automatiser la dépréciation des AMI politiques basées sur EBS -backed. EBS AMIs Pour plus d'informations, consultez Automatiser les AMI cycles de vie.

> **Note**
>
> Par défaut, la date d'obsolescence de tous les publics AMIs est fixée à deux ans à compter de la date de AMI création. Vous pouvez définir la date d'obsolescence à moins de deux ans. Pour annuler la date de dépréciation ou pour la déplacer à une date ultérieure, vous devez la rendre AMI privée en la partageant uniquement avec des comptes spécifiques. AWS

Table des matières

Coûts

Lorsque vous dépréciez unAMI, celui-ci n'AMIest pas supprimé. Le AMI propriétaire continue de payer pour les AMI instantanés. Pour arrêter de payer pour les instantanés, le AMI propriétaire doit les supprimer AMI en les désinscrivant.

Limites

- Pour déprécier unAMI, vous devez être le propriétaire du. AMI

Déprécier un AMI

Vous pouvez déprécier un à une AMI date et à une heure spécifiques. Vous devez être le AMI propriétaire pour effectuer cette procédure.

Console

Pour déprécier un à une AMI date précise

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le navigateur de gauche, choisissez AMIs.
3. Dans la barre de filtre, choisissez Owned by me (M'appartenant).
4. Sélectionnez leAMI, puis choisissez Actions, Gérer la AMI dépréciation. Vous pouvez en sélectionner plusieurs AMIs pour définir la même date d'obsolescence de plusieurs AMIs à la fois.
5. Cochez la case Enable (Activer), puis saisissez la date et l'heure d'obsolescence.

   La limite supérieure pour la date de dépréciation est fixée à 10 ans, sauf dans le cas du publicAMIs, où la limite supérieure est de 2 ans à compter de la date de création. Vous ne pouvez pas spécifier de date antérieure.
6. Choisissez Save (Enregistrer).

AWS CLI

Pour déprécier un à une AMI date précise

Utilisez la enable-image-deprecationcommande. Spécifiez l'ID du AMI ainsi que la date et l'heure auxquelles vous souhaitez désactiver le. AMI Si vous spécifiez une valeur pour les secondes, Amazon EC2 arrondit les secondes à la minute la plus proche.

La limite supérieure `deprecate-at` est fixée à 10 ans, sauf pour le secteur publicAMIs, où elle est fixée à 2 ans à compter de la date de création. Vous ne pouvez pas spécifier de date antérieure.

```
aws ec2 enable-image-deprecation \
    --image-id ami-1234567890abcdef0 \
    --deprecate-at "2021-10-15T13:17:12.000Z"
```

Sortie attendue

```
{
  "Return": "true"
}
```

Vérifiez quand un AMI a été utilisé pour la dernière fois

`LastLaunchedTime`est un horodatage qui indique la date à laquelle vous avez AMI été utilisé pour la dernière fois pour lancer une instance. AMIsqui n'ont pas été utilisés récemment pour lancer une instance peuvent être de bons candidats à la dépréciation ou au désenregistrement.

> **Note**
>
> - Lorsqu'un AMI est utilisé pour lancer une instance, il y a un délai de 24 heures avant que cette utilisation ne soit signalée.
> - `lastLaunchedTime`les données sont disponibles à partir d'avril 2017.

Console

Pour afficher l'heure du dernier lancement d'un AMI

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le navigateur de gauche, choisissez AMIs.
3. Dans la barre de filtre, choisissez Owned by me (M'appartenant).

4. Sélectionnez leAMI, puis cochez le champ Heure du dernier lancement (si vous avez coché la case à côté duAMI, elle se trouve dans l'onglet Détails). Le champ indique la date et l'heure auxquelles le AMI a été utilisé pour la dernière fois pour lancer une instance.

AWS CLI

Pour afficher l'heure du dernier lancement d'un AMI

Exécutez la describe-image-attributecommande et spécifiez`--attribute lastLaunchedTime`. Vous devez être le AMI propriétaire pour exécuter cette commande.

```
aws ec2 describe-image-attribute \
    --image-id ami-1234567890example \
    --attribute lastLaunchedTime
```

Exemple de sortie

```
{
    "LastLaunchedTime": {
        "Value": "2022-02-10T02:03:18Z"
    },
    "ImageId": "ami-1234567890example",
}
```

Décrire ce qui est obsolète AMIs

Vous pouvez afficher la date et l'heure de dépréciation d'unAMI, et les filtrer AMIs par date de dépréciation. Vous pouvez également utiliser le AWS CLI pour décrire tous ceux AMIs qui ont été déconseillés, dont la date de dépréciation est passée.

Console

Pour afficher la date de dépréciation d'un AMI

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le navigateur de gauche, choisissez AMIs, puis sélectionnez leAMI.
3. Cochez le champ Durée d'obsolescence (si vous avez coché la case à côté duAMI, elle se trouve dans l'onglet Détails). Le champ indique la date et l'heure de dépréciation du. AMI Si le champ est vide, AMI il n'est pas obsolète.

Pour filtrer AMIs par date de dépréciation

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le navigateur de gauche, choisissez AMIs.
3. Dans la barre de filtre, choisissez Posned by me ou Private images (les images privées incluent celles AMIs qui sont partagées avec vous et celles qui vous appartiennent).
4. Dans la barre de recherche, saisissez **`Deprecation time`** (lorsque vous saisissez les lettres, le filtre Deprecation time (Heure d'obsolescence) apparaît), puis choisissez un opérateur, une date et une heure.

AWS CLI

Lorsque vous décrivez tout AMIs à l'aide de la commande describe-images, les résultats sont différents selon que vous êtes un AMI utilisateur ou un propriétaire. AMI

- Si vous êtes un AMI utilisateur :

  Par défaut, lorsque vous décrivez tout à AMIs l'aide de la commande describe-images, les images obsolètes AMIs qui ne vous appartiennent pas, mais qui sont partagées avec vous, n'apparaissent pas dans les résultats. Cela est dû au fait que la valeur par défaut est `--no-include-deprecated`. Pour inclure les éléments obsolètes AMIs dans les résultats, vous devez spécifier le `--include-deprecated` paramètre.
- Si vous êtes AMI propriétaire :

  Lorsque vous décrivez tout AMIs à l'aide de la commande describe-images, tous ceux AMIs que vous possédez, y compris ceux qui sont obsolètesAMIs, apparaissent dans les résultats. Vous n'avez pas besoin de spécifier le paramètre `--include-deprecated`. De plus, vous ne pouvez pas exclure les objets obsolètes AMIs que vous possédez des résultats en utilisant. `--no-include-deprecated`

Si un AMI est obsolète, le `DeprecationTime` champ apparaît dans les résultats.

> **Note**
>
> Une personne obsolète AMI est une personne AMI dont la date d'obsolescence est passée. Si vous avez défini la date de dépréciation à une date future, elle n'AMIest pas encore obsolète.

Pour inclure tout ce qui est obsolète AMIs lors de la description de tout AMIs

Utilisez la commande describe-images et spécifiez le `--include-deprecated` paramètre pour inclure dans les résultats toutes les versions obsolètes AMIs qui ne vous appartiennent pas.

```
aws ec2 describe-images \
    --region us-east-1 \
    --owners 123456example
    --include-deprecated
```

Pour décrire la date de dépréciation d'un AMI

Utilisez la commande describe-images et spécifiez l'ID du. AMI

Notez que si vous le `--no-include-deprecated` spécifiez en même temps que l'AMIID, le code obsolète AMI sera renvoyé dans les résultats.

```
aws ec2 describe-images \
    --region us-east-1 \
    --image-ids ami-1234567890EXAMPLE
```

Sortie attendue

Le `DeprecationTime` champ affiche la date à laquelle AMI il est défini comme obsolète. Si le n'AMIest pas défini pour être obsolète, le `DeprecationTime` champ n'apparaît pas dans la sortie.

```
{
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "PlatformDetails": "Red Hat Enterprise Linux",
            "EnaSupport": true,
            "Hypervisor": "xen",
            "State": "available",
            "SriovNetSupport": "simple",
            "ImageId": "ami-1234567890EXAMPLE",
            "DeprecationTime": "2021-05-10T13:17:12.000Z"
            "UsageOperation": "RunInstances:0010",
            "BlockDeviceMappings": [
                {
```

```
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-111222333444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
            "Public": true,
            "ImageType": "machine",
            "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
        }
    ]
}
```

Annuler la AMI dépréciation

Vous pouvez annuler la dépréciation d'unAMI, ce qui supprime la date et l'heure du champ Heure d'obsolescence (console) ou le champ de la sortie `DeprecationTime` describe-images ().AWS CLI Vous devez être le AMI propriétaire pour effectuer cette procédure.

Console

Pour annuler la dépréciation d'un AMI

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le navigateur de gauche, choisissez AMIs.
3. Dans la barre de filtre, choisissez Owned by me (M'appartenant).
4. Sélectionnez leAMI, puis choisissez Actions, Gérer la AMI dépréciation. Vous pouvez en sélectionner plusieurs AMIs pour annuler la dépréciation de plusieurs d'un AMIs coup.
5. Décochez la case Enable (Activer), puis choisissez Save (Enregistrer).

AWS CLI

Pour annuler la dépréciation d'un AMI

Utilisez la disable-image-deprecationcommande et spécifiez l'ID duAMI.

```
aws ec2 disable-image-deprecation \
    --image-id ami-1234567890abcdef0
```

Sortie attendue

```
{
  "Return": "true"
}
```

Désactiver un Amazon EC2 AMI

Vous pouvez désactiver an AMI pour l'empêcher d'être utilisé pour les lancements d'instances. Vous ne pouvez pas lancer de nouvelles instances à partir d'une instance désactivéeAMI. Vous pouvez réactiver une instance désactivée AMI afin qu'elle puisse être réutilisée lors des lancements d'instances.

> **Warning**
>
> La désactivation et la AMI suppression de toutes ses autorisations de lancement.

Lorsqu'un AMI est désactivé :

- AMIL'état passe à`disabled`.
- Une personne handicapée ne AMI peut pas être partagée. Si une AMI information était publique ou partagée auparavant, elle devient privée. Si un AMI a été partagé avec une Compte AWS organisation ou une unité organisationnelle, ils n'ont plus accès aux personnes handicapéesAMI.
- Par défaut, le caractère désactivé AMI n'apparaît pas dans les DescribeImagesAPIappels.
- Un message désactivé AMI n'apparaît pas dans le filtre de console Owned by me. Pour trouver cette option désactivéeAMIs, utilisez le filtre de la console Images désactivées.

- AMIIl n'est pas possible de sélectionner une option désactivée, par exemple des lancements dans la EC2 console. Par exemple, une valeur désactivée AMI n'apparaît pas dans le AMI catalogue de l'assistant de lancement de l'instance ou lors de la création d'un modèle de lancement.
- Les services de lancement, tels que les modèles de lancement et les groupes Auto Scaling, peuvent continuer à faire référence à des services désactivésAMIs. Les lancements d'instance suivants à partir d'une instance désactivée AMI échoueront. Nous vous recommandons donc de mettre à jour les modèles de lancement et les groupes Auto Scaling pour qu'ils AMIs ne soient disponibles que pour les références disponibles.
- EC2les instances précédemment lancées à l'aide d'une AMI instance désactivée par la suite ne sont pas affectées et peuvent être arrêtées, démarrées et redémarrées.
- Vous ne pouvez pas supprimer les instantanés associés à une option désactivéeAMIs. Toute tentative de suppression d'un instantané associé entraîne l'erreur `snapshot is currently in use`.

Lorsqu'un AMI est réactivé :

- L'état AMI passe à`available`, et il peut être utilisé pour lancer des instances.
- Ils AMI peuvent être partagés.
- Comptes AWS, les organisations et les unités organisationnelles qui ont perdu l'accès au AMI lors de sa désactivation ne le retrouvent pas automatiquement, mais AMI peuvent être à nouveau partagés avec elles.

Vous pouvez désactiver à la fois le mode privé et le mode publicAMIs.

Vous pouvez archiver les instantanés associés à votre sauvegarde pour personnes désactivéesEBS. AMIs Cela peut vous aider à réduire les coûts de stockage associés aux objets rarement utilisés AMIs qui doivent être conservés pendant de longues périodes. Pour plus d'informations, consultez Archiver des EBS instantanés Amazon dans le guide de l'EBSutilisateur Amazon.

Table des matières

- Réactiver une personne handicapée AMI

Coûts

Lorsque vous désactivez unAMI, AMI il n'est pas supprimé. S'il s'AMIagit d'un EBS fichier sauvegardé par unAMI, vous continuez à payer pour les AMI EBS instantanés. Si vous souhaitez les conserverAMI, vous pouvez peut-être réduire vos coûts de stockage en archivant les instantanés. Pour plus d'informations, consultez Archiver des EBS instantanés Amazon dans le guide de l'EBSutilisateur Amazon. Si vous ne souhaitez pas conserver les instantanés AMI et leurs instantanés, vous devez les désenregistrer AMI et les supprimer. Pour de plus amples informations, veuillez consulter EBS-soutenu AMIs.

Prérequis

Pour désactiver ou réactiver unAMI, vous devez être le propriétaire duAMI.

IAMAutorisations requises

Pour désactiver et réactiver unAMI, vous devez disposer des IAM autorisations suivantes :

- `ec2:DisableImage`
- `ec2:EnableImage`

Désactiver un AMI

Vous pouvez désactiver un AMI en utilisant la EC2 console ou le AWS Command Line Interface (AWS CLI). Vous devez être le AMI propriétaire pour effectuer cette procédure.

Console

Pour désactiver un AMI

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation de gauche, choisissez AMIs.
3. Dans la barre de filtre, choisissez Owned by me (M'appartenant).
4. Sélectionnez leAMI, puis choisissez Actions, Désactiver AMI. Vous pouvez en sélectionner plusieurs AMIs à désactiver à la fois.
5. Dans la AMI fenêtre Désactiver, choisissez Désactiver AMI.

AWS CLI

Pour désactiver un AMI

Utilisez la disable-imagecommande et spécifiez l'ID duAMI.

```
aws ec2 disable-image --image-id ami-1234567890abcdef0
```

Sortie attendue

```
{
  "Return": "true"
}
```

Décrire les personnes handicapées AMIs

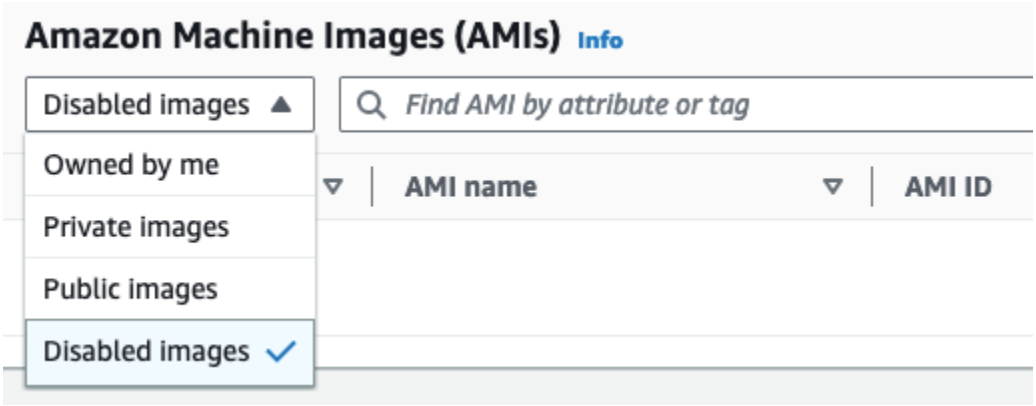
Vous pouvez afficher les informations désactivées AMIs dans la EC2 console et en utilisant le AWS CLI.

Vous devez être le AMI propriétaire pour que la vue soit désactivéeAMIs. Comme AMIs les personnes handicapées deviennent privées, vous ne pouvez pas afficher les options désactivées AMIs si vous n'en êtes pas le propriétaire.

Console

Pour afficher désactivé AMIs

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation de gauche, choisissez AMIs.
3. Dans la barre de filtre, choisissez Images désactivées.



AWS CLI

Par défaut, lorsque vous utilisez la describe-imagescommande pour tout décrireAMIs, les options désactivées AMIs n'apparaissent pas dans les résultats. Cela est dû au fait que la valeur par défaut est `--no-include-disabled`. Pour inclure les désactivés AMIs dans les résultats, vous devez spécifier le `--include-disabled` paramètre.

Pour inclure tous les désactivés AMIs lors de la description de tous AMIs

Utilisez la describe-imagescommande et spécifiez le `--include-disabled` paramètre à récupérer désactivé AMIs en plus de tous les autres paramètresAMIs. Vous pouvez éventuellement spécifier `--owners self` de ne récupérer que AMIs ce que vous possédez.

```
aws ec2 describe-images \
    --region us-east-1 \
    --owners self
    --include-disabled
```

Si vous spécifiez l'ID d'une personne désactivéeAMI, mais que vous ne le spécifiez pas`--include-disabled`, la personne désactivée AMI est renvoyée dans les résultats.

```
aws ec2 describe-images \
    --region us-east-1 \
    --image-ids ami-1234567890EXAMPLE
```

Pour récupérer uniquement, désactivé AMIs

Spécifiez `--filters Name=state,Values=disabled`. Vous devez également spécifier `--include-disabled`, sinon vous obtiendrez une erreur.

```
aws ec2 describe-images \
    --include-disabled \
    --filters Name=state,Values=disabled
```

Exemple de sortie

Le `State` champ affiche l'état d'unAMI. `disabled`indique que le AMI est désactivé.

```
{
```

```
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "PlatformDetails": "Red Hat Enterprise Linux",
            "EnaSupport": true,
            "Hypervisor": "xen",
            "State": "disabled",
            "SriovNetSupport": "simple",
            "ImageId": "ami-1234567890EXAMPLE",
            "DeprecationTime": "2023-05-10T13:17:12.000Z"
            "UsageOperation": "RunInstances:0010",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-111222333444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
            "Public": false,
            "ImageType": "machine",
            "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
        }
    ]
}
```

Réactiver une personne handicapée AMI

Vous pouvez réactiver une personne handicapéeAMI. Vous devez être le AMI propriétaire pour effectuer cette procédure.

Console

Pour réactiver une personne handicapée AMI

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation de gauche, choisissez AMIs.
3. Dans la barre de filtre, choisissez Images désactivées.
4. Sélectionnez leAMI, puis choisissez Actions, Activer AMI. Vous pouvez en sélectionner plusieurs AMIs pour en réactiver plusieurs AMIs à la fois.
5. Dans la AMI fenêtre Activer, choisissez Activer.

AWS CLI

Pour réactiver une personne handicapée AMI

Utilisez la enable-imagecommande et spécifiez l'ID duAMI.

```
aws ec2 enable-image --image-id ami-1234567890abcdef0
```

Sortie attendue

```
{
  "Return": "true"
}
```

Désenregistrer un Amazon EC2 AMI

Lorsque vous désenregistrez un, AMI Amazon le supprime EC2 définitivement. Une fois que vous avez désenregistré unAMI, vous ne pouvez pas l'utiliser pour lancer de nouvelles instances. Vous pourriez envisager de vous désinscrire une AMI fois que vous aurez fini de l'utiliser.

Pour vous protéger contre le désenregistrement accidentel ou malveillant d'unAMI, vous pouvez activer la protection contre le désenregistrement. Si vous annulez accidentellement l'enregistrement d'un fichier EBS -backedAMI, vous ne pouvez utiliser la corbeille pour le restaurer que si vous le restaurez dans le délai imparti avant qu'il ne soit définitivement supprimé.

La désinscription d'un n'AMIa aucun effet sur les instances lancées depuis le. AMI Vous pouvez continuer à utiliser ces instances. L'annulation de l'enregistrement n'a AMI également aucun effet

sur les instantanés créés au cours du processus de création. AMI Vous continuerez de devoir payer des frais d'utilisation pour ces instances et des coûts de stockage pour les instantanés. Par conséquent, pour éviter d'encourir des coûts inutiles, nous vous recommandons de mettre fin à toutes les instances et de supprimer les instantanés dont vous n'avez pas besoin. Pour de plus amples informations, veuillez consulter Évitez les coûts liés aux ressources inutilisées.

Table des matières

Considérations

- Vous ne pouvez pas annuler un enregistrement AMI qui n'appartient pas à votre compte.
- Vous ne pouvez pas utiliser Amazon EC2 pour annuler l'enregistrement d'un AMI site géré par le AWS Backup service. Utilisez-le plutôt AWS Backup pour supprimer les points de restauration correspondants dans le coffre de sauvegarde. Pour plus d'informations, consultez Suppression des sauvegardes dans le Guide du développeur AWS Backup .

Désenregistrer un AMI

Utilisez l'une des méthodes suivantes pour annuler l'enregistrement d'une instance sauvegardée par un stockage AMI ou une instance EBS sauvegardée par le stockage. AMI

> **Tip**
>
> Pour éviter d'encourir des coûts inutiles, vous devez supprimer toutes les ressources dont vous n'avez pas besoin. Par exemple, pour EBS -backedAMIs, si vous n'avez pas besoin des instantanés associés aux personnes désenregistréesAMI, vous devez les supprimer. Pour de plus amples informations, veuillez consulter Évitez les coûts liés aux ressources inutilisées.

Console

Pour annuler l'enregistrement d'une AMI

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez AMIs.
3. Dans la barre de filtre, choisissez Owned by me pour répertorier les images disponiblesAMIs, ou choisissez Disabled images pour répertorier vos images handicapéesAMIs.
4. Sélectionnez le AMI pour vous désinscrire.
5. Choisissez Actions, DeregisterAMI (Annuler l'enregistrement).
6. Lorsque vous êtes invité à confirmer, choisissez Désenregistrer AMI.

   Quelques minutes peuvent s'écouler avant que la console ne les supprime AMI de la liste. Choisissez Refresh pour actualiser le statut.

AWS CLI

Pour annuler l'enregistrement d'une AMI

Utilisez la commande deregister-image et spécifiez l'ID du à désenregistrer. AMI

```
aws ec2 deregister-image --image-id ami-0123456789example
```

PowerShell

Pour annuler l'enregistrement d'une AMI

Utilisez l'Unregister-EC2Imageapplet de commande et spécifiez l'ID du AMI pour annuler l'enregistrement.

```
Unregister-EC2Image -ImageId ami-0123456789example
```

Évitez les coûts liés aux ressources inutilisées

Lorsque vous désenregistrez unAMI, vous ne supprimez pas les ressources associées au. AMI Ces ressources incluent les instantanés pour EBS -backed AMIs et les fichiers dans Amazon S3, par

exemple sauvegardés en magasin. AMIs Lorsque vous désenregistrez unAMI, vous ne résiliez ni n'arrêtez aucune instance lancée depuis le. AMI

Vous continuerez à supporter des frais pour le stockage des instantanés et des fichiers, ainsi que pour toutes les instances en cours d'exécution.

Pour éviter ce type de coûts inutiles, nous vous recommandons de supprimer toutes les ressources dont vous n'avez pas besoin.

EBS-soutenu AMIs

Utilisez l'une des méthodes suivantes pour supprimer les ressources associées à votre EBS sauvegardeAMI.

Console

Pour supprimer les ressources associées à votre EBS sauvegarde AMI

1. Désenregistrer le. AMI

   Notez l'AMIidentifiant : cela peut vous aider à trouver les instantanés à supprimer à l'étape suivante.
2. Supprimez les instantanés dont vous n'avez pas besoin.

   L'ID de l'associé AMI est affiché dans la colonne Description de l'écran Instantanés.
3. Mettez fin aux instances dont vous n'avez pas besoin.

AWS CLI

Pour supprimer les ressources associées à votre EBS sauvegarde AMI

1. Désenregistrez-les à l'aide de AMI la commande deregister-image.

   ```
   aws ec2 deregister-image --image-id ami-0123456789example
   ```
2. Supprimez les instantanés dont vous n'avez pas besoin à l'aide de la commande delete-snapshot.

   ```
   aws ec2 delete-snapshot --snapshot-id snap-0123456789example
   ```

3. Mettez fin aux instances dont vous n'avez pas besoin à l'aide de la commande terminate-instances.

```
aws ec2 terminate-instances --instance-ids i-0123456789example
```

PowerShell

Pour supprimer les ressources associées à votre EBS sauvegarde AMI

1. Désenregistrez-les à l'aide de AMI l'applet de commande Unregister-EC2Image.

```
Unregister-EC2Image -ImageId ami-0123456789example
```

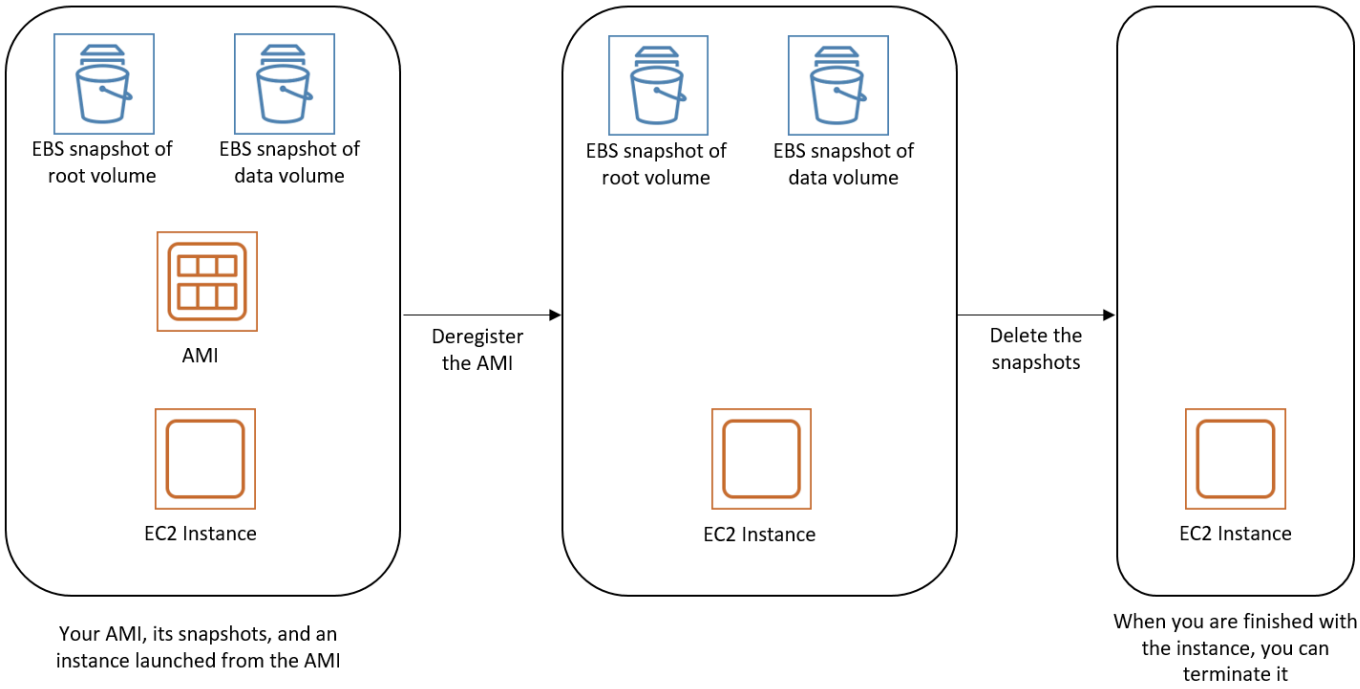
2. Supprimez les instantanés dont vous n'avez pas besoin à l'aide de l'Remove-EC2Snapshotapplet de commande.

```
Remove-EC2Snapshot -SnapshotId snap-0123456789example
```

3. Mettez fin aux instances dont vous n'avez pas besoin à l'aide de l'Remove-EC2Instanceapplet de commande.

```
Remove-EC2Instance -InstanceId i-0123456789example
```

Le schéma suivant illustre le flux qui vous permet de supprimer les ressources associées à un EBS - backedAMI.



Sauvegardé par instance AMI

Utilisez la méthode suivante pour supprimer les ressources associées à votre instance sauvegardée en magasinAMI.

Pour supprimer les ressources associées à votre instance sauvegardées en magasin AMI

1. Désenregistrez-les à l'aide de AMI la commande deregister-image.

```
aws ec2 deregister-image --image-id ami-0123456789example
```

2. Supprimez le bundle dans Amazon S3 à l'aide de la commande ec2-delete-bundle (AMItools).

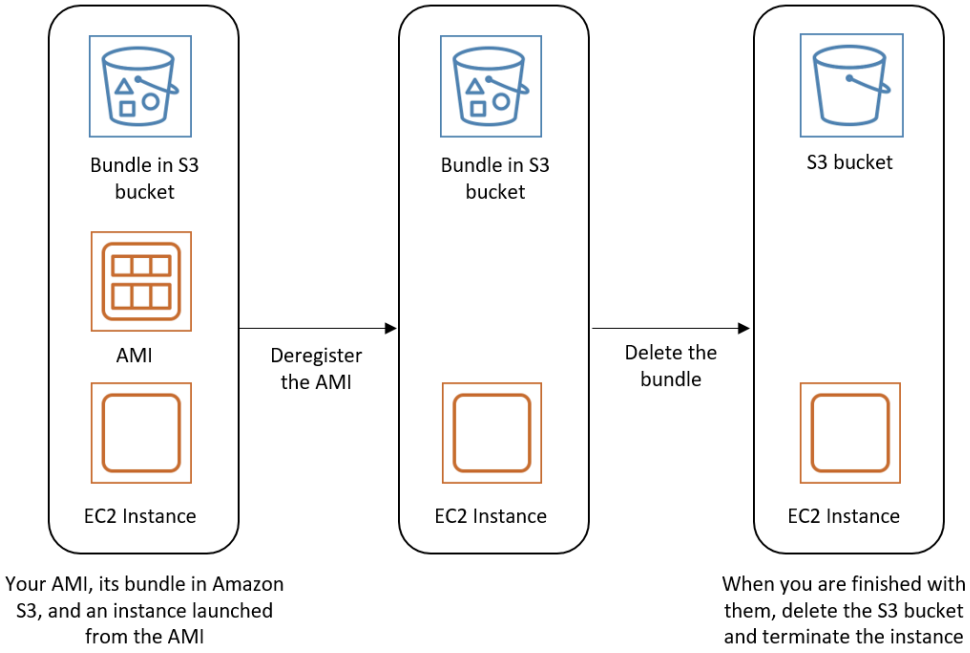
```
ec2-delete-bundle -b amzn-s3-demo-bucket/myami -a your_access_key_id -
s your_secret_access_key -p image
```

3. Mettez fin aux instances dont vous n'avez pas besoin à l'aide de la commande terminate-instances.

```
aws ec2 terminate-instances --instance-ids i-0123456789example
```

4. Si vous en avez terminé avec le compartiment Amazon S3 dans lequel vous avez chargé le bundle, vous pouvez le supprimer. Pour supprimer un compartiment Amazon S3, ouvrez la console Amazon S3, sélectionnez le compartiment, choisissez Actions, puis Delete.

Le schéma suivant illustre le flux de suppression des ressources associées à votre instance sauvegardée en magasinAMI.



Protéger un Amazon contre EC2 AMI la désinscription

Vous pouvez activer la protection de désinscription AMI pour empêcher toute suppression accidentelle ou malveillante. Lorsque vous activez la protection de désinscription, aucun utilisateur ne AMI peut le désenregistrer, quelles que soient ses autorisations. IAM Si vous souhaitez le désenregistrerAMI, vous devez d'abord désactiver la protection de désenregistrement.

Lorsque vous activez la protection de désenregistrement sur unAMI, vous avez la possibilité d'inclure une période de recharge de 24 heures. Cette période de recharge est la durée pendant laquelle la protection de désenregistrement reste active une fois que vous l'avez désactivée. Pendant cette période de recharge, il n'est pas AMI possible de le désenregistrer. À la fin de la période de recharge, l'enregistrement AMI peut être annulé.

La protection contre le désenregistrement est désactivée par défaut sur tous les appareils existants et nouveaux. AMIs

Activer la protection de désenregistrement

Suivez les procédures ci-dessous pour activer la protection de désenregistrement.

Console

Pour activer la protection de désinscription sur un AMI

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez AMIs.
3. Dans la barre de filtre, choisissez Owned by me pour répertorier les images disponiblesAMIs, ou choisissez Disabled images pour répertorier vos images handicapéesAMIs.
4. Sélectionnez celui AMI sur lequel vous souhaitez activer la protection de désenregistrement, puis choisissez Actions, Gérer AMI la protection de désenregistrement.
5. Dans la boîte de dialogue Gérer la protection contre le AMI désenregistrement, vous pouvez activer la protection contre le désenregistrement avec ou sans délai de recharge. Choisissez l'une des options suivantes :
   - Activez avec une période de recharge de 24 heures : avec une période de recharge, le désenregistrement ne AMI peut pas être annulé pendant 24 heures lorsque la protection de désenregistrement est désactivée.
   - Activer sans temps de recharge — Sans période de recharge, l'enregistrement AMI peut être annulé immédiatement lorsque la protection de désenregistrement est désactivée.
6. Choisissez Save (Enregistrer).

AWS CLI

Pour activer la protection de désinscription sur un AMI

Utilisez la enable-image-deregistration-protectioncommande et spécifiez l'AMIID. Pour inclure la période de recharge optionnelle de 24 heures, incluez `--with-cooldown` set to`true`. Pour exclure le délai de recharge, omettez le `--with-cooldown` paramètre.

```
aws ec2 enable-image-deregistration-protection \
    --image-id ami-0123456789example \
    --with-cooldown true
```

Désactiver la protection de désenregistrement

Suivez les procédures ci-dessous pour désactiver la protection de désenregistrement.

Si vous avez choisi d'inclure une période de recharge de 24 heures lorsque vous avez activé la protection de désenregistrement pour leAMI, alors, lorsque vous désactivez la protection de désenregistrement, vous ne pourrez pas le désenregistrer immédiatement. AMI La période de recharge est la période de 24 heures pendant laquelle la protection de désenregistrement reste en vigueur même après sa désactivation. Pendant cette période de recharge, il n'est pas AMI possible de le désenregistrer. Une fois la période de recharge terminée, l'enregistrement AMI peut être annulé.

Console

Pour désactiver la protection contre le désenregistrement sur un AMI

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez AMIs.
3. Dans la barre de filtre, choisissez Owned by me pour répertorier les images disponiblesAMIs, ou choisissez Disabled images pour répertorier vos images handicapéesAMIs.
4. Sélectionnez le AMI pour désactiver la protection de désenregistrement, puis choisissez Actions, Gérer AMI la protection de désenregistrement.
5. Dans la boîte de dialogue Gérer la protection contre le AMI désenregistrement, choisissez Désactiver.
6. Choisissez Save (Enregistrer).

AWS CLI

Pour désactiver la protection contre le désenregistrement sur un AMI

Utilisez la disable-image-deregistration-protectioncommande et spécifiez l'AMIID.

```
aws ec2 disable-image-deregistration-protection --image-id ami-0123456789example
```

Comportement de lancement de l'instance avec les modes de EC2 démarrage Amazon

Lorsqu'un ordinateur démarre, le premier logiciel qu'il exécute est responsable d'initialiser la plateforme et de fournir une interface permettant au système d'exploitation d'effectuer des opérations spécifiques à la plateforme.

Amazon prend EC2 en charge deux variantes du logiciel en mode de démarrage : Unified Extensible Microware Interface (UEFI) et LegacyBIOS.

Paramètres de mode de démarrage possibles sur un AMI

An AMI peut avoir l'une des valeurs de paramètre de mode de démarrage suivantes :`uefi`,`legacy-bios`, ou`uefi-preferred`. Le paramètre du mode de AMI démarrage est facultatif. En l'absence AMIs de paramètre de mode de démarrage, les instances lancées à partir de ces derniers AMIs utilisent la valeur du mode de démarrage par défaut du type d'instance.

Objectif du paramètre du mode de AMI démarrage

Le paramètre du mode de AMI démarrage indique à Amazon EC2 le mode de démarrage à utiliser lors du lancement d'une instance. Lorsque le paramètre du mode de démarrage est défini sur`uefi`, EC2 tente de lancer l'instance surUEFI. Si le système d'exploitation n'est pas configuré pour être compatibleUEFI, le lancement de l'instance échouera.

UEFIParamètre de mode de démarrage préféré

Vous pouvez créer AMIs ce support à la fois UEFI et Legacy BIOS en utilisant le paramètre de mode de `uefi-preferred` démarrage. Lorsque le paramètre du mode de démarrage est défini sur`uefi-preferred`, et si le type d'instance le prend en chargeUEFI, l'instance est lancée leUEFI. Si le type d'instance n'est pas compatibleUEFI, l'instance est lancée sur LegacyBIOS.

> **Warning**
>
> Certaines fonctionnalités, telles que le démarrage UEFI sécurisé, ne sont disponibles que sur les instances qui démarrentUEFI. Lorsque vous utilisez le paramètre de mode de `uefi-preferred` AMI démarrage avec un type d'instance non compatibleUEFI, l'instance sera lancée en tant que Legacy BIOS et la fonctionnalité UEFI dépendante sera désactivée.
> Si vous comptez sur la disponibilité d'une fonctionnalité UEFI dépendante, définissez le paramètre du mode de AMI démarrage sur`uefi`.

Modes de démarrage par défaut pour les types d'instance

- Types d'instances de Graviton : UEFI
- Intel et types d'AMDinstances : Legacy BIOS

Support de zone

UEFIle démarrage n'est pas pris en charge dans Local Zones, Wavelength Zones ou AWS Outposts.

Rubriques Mode de démarrage

- Conditions requises pour lancer une EC2 instance en mode de UEFI démarrage
- Déterminer le paramètre du mode de démarrage d'un Amazon EC2 AMI
- Déterminer les modes de démarrage pris en charge pour un type d'EC2instance
- Déterminer le mode de démarrage d'une EC2 instance
- Déterminez le mode de démarrage du système d'exploitation de votre EC2 instance
- Définir le mode de démarrage d'un Amazon EC2 AMI
- UEFIvariables pour les EC2 instances Amazon
- UEFIDémarrage sécurisé pour les EC2 instances Amazon

Conditions requises pour lancer une EC2 instance en mode de UEFI démarrage

Le mode de démarrage d'une instance est déterminé par la configuration duAMI, le système d'exploitation qu'elle contient et le type d'instance. Pour lancer une instance en mode de UEFI démarrage, vous devez satisfaire aux exigences suivantes.

AMI

AMIIl doit être configuré UEFI comme suit :

- Système d'exploitation : le système d'exploitation contenu dans le AMI doit être configuré pour être utilisé UEFI ; dans le cas contraire, le lancement de l'instance échouera. Pour de plus amples informations, veuillez consulter Déterminez le mode de démarrage du système d'exploitation de votre EC2 instance.

- AMIparamètre de mode de démarrage — Le paramètre de mode de démarrage du AMI doit être défini sur `uefi` ou`uefi-preferred`. Pour de plus amples informations, veuillez consulter Déterminer le paramètre du mode de démarrage d'un Amazon EC2 AMI.

Linux — Le AMIs support Linux suivant UEFI :

- Amazon Linux 2023
- Amazon Linux 2 (types d'instances Graviton uniquement)

Pour les autres systèmes LinuxAMIs, vous devez configurer le AMI, l'importer AMI via VM Import/Export ou l'AMIimporter via. CloudEndure

Windows : AMIs support Windows suivant UEFI :

- TPM-Windows_Server-2_Anglais-Base complète
- TPM-Windows_Server-2_Anglais-Core-Base
- TPM-Windows_Server-2019-Anglais-Base complète
- TPM-Windows_Server-2019-Anglais-Core-Base
- TPM-Windows_Server-2016-Anglais-Base complète
- TPM-Windows_Server-2016-Anglais-Core-Base

Type d'instance

Toutes les instances basées sur le système AWS Nitro sont compatibles à la fois UEFI avec LegacyBIOS, à l'exception des suivantes : instances bare metal, G4ad, P4DL1, u-3tb1, u-6tb1, u-9tb1, u-12tb1, u-18tb1, u-24tb1 et. VT1 Pour de plus amples informations, veuillez consulter the section called "Mode de démarrage du type d'instance".

Le tableau suivant montre que le mode de démarrage d'une instance (indiqué par la colonne Mode de démarrage de l'instance résultante) est déterminé par une combinaison du paramètre de mode de démarrage de la AMI (colonne 1), de la configuration du mode de démarrage du système d'exploitation contenue dans la AMI (colonne 2) et de la prise en charge du mode de démarrage du type d'instance (colonne 3).

AMIparamètre du mode de démarrage	Configuration du mode de démarrage du système d'exploitation	Prise en charge du mode de démarrage du type d'instance	Mode de démarrage de l'instance résultante
UEFI	UEFI	UEFI	UEFI
Héritage BIOS	Héritage BIOS	Héritage BIOS	Héritage BIOS
UEFIPréféré	UEFI	UEFI	UEFI
UEFIPréféré	UEFI	UEFIet Legacy BIOS	UEFI
UEFIPréféré	Héritage BIOS	Héritage BIOS	Héritage BIOS
UEFIPréféré	Héritage BIOS	UEFIet Legacy BIOS	Héritage BIOS
Aucun mode de démarrage spécifié - ARM	UEFI	UEFI	UEFI
Aucun mode de démarrage spécifié – x86	Héritage BIOS	UEFIet Legacy BIOS	Héritage BIOS

Déterminer le paramètre du mode de démarrage d'un Amazon EC2 AMI

Le paramètre du mode de AMI démarrage est facultatif. An AMI peut avoir l'une des valeurs de paramètre de mode de démarrage suivantes :`uefi`,`legacy-bios`, ou`uefi-preferred`.

Certains AMIs n'ont pas de paramètre de mode de démarrage. Lorsqu'un paramètre n'AMIa pas de mode de démarrage, les instances lancées à partir de celui-ci AMI utilisent la valeur par défaut du type d'instance, qui est `uefi` sur Graviton, Intel et `legacy-bios` les types d'AMDinstance.

Console

Pour déterminer le paramètre du mode de démarrage d'une AMI (console)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

2. Dans le volet de navigation, choisissez AMIs, puis sélectionnez leAMI.
3. Vérifiez le champ Mode de démarrage.

   - La valeur uefi indique que les AMI supports. UEFI
   - La valeur uefi-preferred indique qu'il AMI supporte à la fois UEFI Legacy et Legacy. BIOS
   - S'il n'y a aucune valeur, les instances lancées depuis le AMI utilisent la valeur par défaut du type d'instance.

Pour déterminer le paramètre de mode de démarrage d'une instance AMI lors du lancement d'une instance (console)

Lorsque vous lancez une instance à l'aide de l'assistant de lancement d'instanceAMI, inspectez le champ Mode de démarrage à l'étape de sélection d'une instance. Pour de plus amples informations, veuillez consulter Images d'applications et de systèmes d'exploitation (Amazon Machine Image).

AWS CLI

Pour déterminer le paramètre de mode de démarrage d'un AMI (AWS CLI)

Utilisez cette describe-imagesopération pour déterminer le mode de démarrage d'unAMI.

```
aws ec2 describe-images --region us-east-1 --image-id ami-0abcdef1234567890

{
    "Images": [
        {
         ...
            ],
            "EnaSupport": true,
            "Hypervisor": "xen",
            "ImageOwnerAlias": "amazon",
            "Name": "UEFI_Boot_Mode_Enabled-Windows_Server-2016-English-Full-
Base-2020.09.30",
            "RootDeviceName": "/dev/sda1",
            "RootDeviceType": "ebs",
            "SriovNetSupport": "simple",
            "VirtualizationType": "hvm",
            "BootMode":
 "uefi"
        }
```

```
    ]
}
```

Dans le résultat, le `BootMode` champ indique le mode de démarrage duAMI. Une valeur de `uefi` indique que les AMI supportsUEFI. Une valeur de `uefi-preferred` indique qu'il AMI prend en charge à la fois Legacy UEFI et LegacyBIOS. S'il n'y a aucune valeur, les instances lancées depuis le AMI utilisent la valeur par défaut du type d'instance.

PowerShell

Pour déterminer le paramètre du mode de démarrage d'un AMI (Outils pour PowerShell)

Utilisez l'Get-EC2Imageapplet de commande pour déterminer le mode de démarrage d'un. AMI

```
PS C:\> Get-EC2Image -Region us-east-1 -ImageId ami-0abcdef1234567890 | Format-List
 Name, BootMode, TpmSupport

Name       : TPM-Windows_Server-2016-English-Full-Base-2023.05.10
BootMode   : uefi
TpmSupport : v2.0
```

Dans le résultat, le `BootMode` champ indique le mode de démarrage duAMI. Une valeur de `uefi` indique que les AMI supportsUEFI. Une valeur de `uefi-preferred` indique qu'il AMI prend en charge à la fois Legacy UEFI et LegacyBIOS. S'il n'y a aucune valeur, les instances lancées depuis le AMI utilisent la valeur par défaut du type d'instance.

Déterminer les modes de démarrage pris en charge pour un type d'EC2instance

Vous pouvez utiliser le AWS CLI ou les outils PowerShell pour déterminer les modes de démarrage pris en charge pour un type d'instance.

Pour déterminer les modes de démarrage pris en charge d'un type d'instance

Vous pouvez utiliser les méthodes suivantes pour déterminer les modes de démarrage pris en charge d'un type d'instance.

AWS CLI

Utilisez la commande describe-instance-types pour déterminer les modes de démarrage pris en charge d'un type d'instance. Le `--query` paramètre filtre la sortie pour renvoyer uniquement les modes de démarrage pris en charge.

L'exemple suivant montre qu'il `m5.2xlarge` prend en charge les deux modes de BIOS démarrage UEFI et Legacy.

```
aws ec2 describe-instance-types --region us-east-1 --instance-types m5.2xlarge --
query "InstanceTypes[*].SupportedBootModes"
```

Voici un exemple de sortie.

```
[
    [
        "legacy-bios",
        "uefi"
    ]
]
```

L'exemple suivant montre que seul Legacy est pris `t2.xlarge` en chargeBIOS.

```
aws ec2 describe-instance-types --region us-east-1 --instance-types t2.xlarge --
query "InstanceTypes[*].SupportedBootModes"
```

Voici un exemple de sortie.

```
[
    [
        "legacy-bios"
    ]
]
```

PowerShell

Utilisez l'applet de commande Get-EC2InstanceType(Tools for PowerShell) pour déterminer les modes de démarrage pris en charge par un type d'instance.

L'exemple suivant montre qu'il `m5.2xlarge` prend en charge les deux modes de BIOS démarrage UEFI et Legacy.

```
Get-EC2InstanceType -Region us-east-1 -InstanceType m5.2xlarge | Format-List
 InstanceType, SupportedBootModes
```

Voici un exemple de sortie.

```
InstanceType       : m5.2xlarge
SupportedBootModes : {legacy-bios, uefi}
```

L'exemple suivant montre que seul Legacy est pris `t2.xlarge` en chargeBIOS.

```
Get-EC2InstanceType -Region us-east-1 -InstanceType t2.xlarge | Format-List
 InstanceType, SupportedBootModes
```

Voici un exemple de sortie.

```
InstanceType       : t2.xlarge
SupportedBootModes : {legacy-bios}
```

Pour déterminer les types d'instances qui prennent en charge UEFI

Vous pouvez utiliser les méthodes suivantes pour déterminer les types d'instances compatibles UEFI :

AWS CLI

Les types d'instance disponibles varient selon l' Région AWS. Pour voir les types d'instances disponibles qui sont pris UEFI en charge dans une région, utilisez la describe-instance-typescommande avec le `--region` paramètre. Si vous omettez le `--region` paramètre, la région par défaut configurée est utilisée dans la demande. Incluez le `--filters` paramètre pour étendre les résultats aux types d'instances pris en charge UEFI et le `--query` paramètre pour étendre la sortie à la valeur de`InstanceType`.

```
aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi --
query "InstanceTypes[*].[InstanceType]" --output text | sort
```

Voici un exemple de sortie.

```
a1.2xlarge
a1.4xlarge
a1.large
a1.medium
a1.metal
a1.xlarge
c5.12xlarge
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
 Where-Object {$_.SupportedBootModes -Contains "uefi"} | `
 Sort-Object InstanceType | `
 Format-Table InstanceType -GroupBy CurrentGeneration
```

Voici un exemple de sortie.

```
CurrentGeneration: False

InstanceType
------------
a1.2xlarge
a1.4xlarge
a1.large
a1.medium
a1.metal
a1.xlarge

CurrentGeneration: True

InstanceType
------------
c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
c5.4xlarge
c5.9xlarge
...
```

Pour déterminer les types d'instances qui prennent en charge le démarrage UEFI sécurisé et qui conservent les variables non volatiles

Les instances bare metal ne prennent pas en charge le démarrage UEFI sécurisé et les variables non volatiles. Ces exemples les excluent donc de la sortie. Pour plus d'informations sur le démarrage UEFI sécurisé, consultezUEFIDémarrage sécurisé pour les EC2 instances Amazon.

AWS CLI

Utilisez la describe-instance-typescommande et excluez les instances bare metal de la sortie en incluant le `Name=bare-metal,Values=false` filtre.

```
aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi
 Name=bare-metal,Values=false --query "InstanceTypes[*].[InstanceType]" --output
 text | sort
```

Voici un exemple de sortie.

```
a1.2xlarge
a1.4xlarge
a1.large
a1.medium
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
    Where-Object { `
        $_.SupportedBootModes -Contains "uefi" -and `
        $_.BareMetal -eq $False
        } | `
    Sort-Object InstanceType  | `
    Format-Table InstanceType, SupportedBootModes, BareMetal,
 @{Name="SupportedArchitectures";
 Expression={$_.ProcessorInfo.SupportedArchitectures}}
```

```
InstanceType     SupportedBootModes  BareMetal SupportedArchitectures
------------     ------------------  --------- ----------------------
a1.2xlarge       {uefi}                  False arm64
a1.4xlarge       {uefi}                  False arm64
```

```
a1.large          {uefi}                  False arm64
a1.medium         {uefi}                  False arm64
a1.xlarge         {uefi}                  False arm64
c5.12xlarge       {legacy-bios, uefi}     False x86_64
c5.18xlarge       {legacy-bios, uefi}     False x86_64
```

Déterminer le mode de démarrage d'une EC2 instance

Le mode de démarrage d'une instance est affiché dans le champ Mode de démarrage de la EC2 console Amazon et selon le `currentInstanceBootMode` paramètre du AWS CLI.

Lorsqu'une instance est lancée, la valeur de son paramètre de mode de démarrage est déterminée par la valeur du paramètre de mode de démarrage AMI utilisé pour la lancer, comme suit :

- Un AMI avec un paramètre de mode de démarrage de `uefi` crée une instance avec un `currentInstanceBootMode` paramètre de`uefi`.
- Un AMI avec un paramètre de mode de démarrage de `legacy-bios` crée une instance avec un `currentInstanceBootMode` paramètre de `legacy-bios`.
- Une instance AMI avec un paramètre de mode de démarrage de `uefi-preferred` crée une instance avec un `currentInstanceBootMode` paramètre de `uefi` si le type d'instance est compatible UEFI ; dans le cas contraire, elle crée une instance avec un `currentInstanceBootMode` paramètre de`legacy-bios`.
- Une AMI valeur de paramètre sans mode de démarrage crée une instance avec une valeur de `currentInstanceBootMode` paramètre qui dépend de l'AMIarchitecture x86 et du mode de démarrage pris en charge pour le type d'instance. ARM Le mode de démarrage par défaut est `uefi` celui des types d'instance Graviton, des types Intel et `legacy-bios` des types d'AMDinstance.

Console

Pour déterminer le mode de démarrage d'une instance (console)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez instances, puis sélectionnez votre instance.
3. Sous l'onglet Détails, vérifiez le champ Mode de démarrage.

AWS CLI

Pour déterminer le mode de démarrage d'une instance (AWS CLI)

Utilisez la commande describe-instances pour déterminer le mode de démarrage d'une instance. Vous pouvez également déterminer le mode de démarrage de celui AMI qui a été utilisé pour créer l'instance.

```
aws ec2 describe-instances --region us-east-1 --instance-ids i-1234567890abcdef0

{
    "Reservations": [
        {
            "Groups": [],
            "Instances": [
                {
                    "AmiLaunchIndex": 0,
                    "ImageId": "ami-0e2063e7f6dc3bee8",
                    "InstanceId": "i-1234567890abcdef0",
                    "InstanceType": "m5.2xlarge",
                    ...
                    },
                   "BootMode": "uefi",
                   "CurrentInstanceBootMode": "uefi"
                }
            ],
            "OwnerId": "1234567890",
            "ReservationId": "r-1234567890abcdef0"
        }
    ]
}
```

PowerShell

Pour déterminer le mode de démarrage d'une instance (Outils pour PowerShell)

Utilisez l'applet de commande Get-EC2Image pour déterminer le mode de démarrage d'une instance. Vous pouvez également déterminer le mode de démarrage de celui AMI qui a été utilisé pour créer l'instance.

Get-EC2Image (AWS Tools for Windows PowerShell)

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances | Format-List BootMode,
 CurrentInstanceBootMode, InstanceType, ImageId

BootMode                : uefi
CurrentInstanceBootMode : uefi
InstanceType            : c5a.large
ImageId                 : ami-0265446f88eb4021b
```

Dans la sortie, les paramètres suivants décrivent le mode de démarrage :

- `BootMode`— Le mode de démarrage du AMI qui a été utilisé pour créer l'instance.
- `CurrentInstanceBootMode` : le mode de démarrage utilisé pour démarrer l'instance au lancement ou au démarrage.

Déterminez le mode de démarrage du système d'exploitation de votre EC2 instance

Le mode de démarrage du AMI guide Amazon EC2 sur le mode de démarrage à utiliser pour démarrer une instance. Pour savoir si le système d'exploitation de votre instance est configuré pourUEFI, vous devez vous connecter à votre instance en utilisant SSH (instances Linux) ou RDP (instances Windows).

Utilisez les instructions fournies pour le système d'exploitation de votre instance.

Linux

Pour déterminer le mode de démarrage du système d'exploitation de l'instance

1. Connectez-vous à votre instance Linux à l'aide de SSH.
2. Pour afficher le mode de démarrage du système d'exploitation, essayez l'une des méthodes suivantes :

   - Exécutez la commande suivante.

     ```
     [ec2-user ~]$ sudo /usr/sbin/efibootmgr
     ```

     Résultat attendu d'une instance démarrée en UEFI mode de démarrage

     ```
     BootCurrent: 0001
     ```

```
Timeout: 0 seconds
BootOrder: 0000,0001
Boot0000* UiApp
Boot0001* UEFI Amazon Elastic Block Store vol-xyz
```

- Exécutez la commande suivante pour vérifier l'existence du répertoire `/sys/firmware/efi`. Ce répertoire n'existe que si l'instance démarre en utilisantUEFI. Si le répertoire n'existe pas, la commande renvoie `Legacy BIOS Boot Detected`.

  ```
  [ec2-user ~]$ [ -d /sys/firmware/efi ] && echo "UEFI Boot Detected" || echo
   "Legacy BIOS Boot Detected"
  ```

  Résultat attendu d'une instance démarrée en UEFI mode de démarrage

  ```
  UEFI Boot Detected
  ```

  Résultat attendu d'une instance démarrée en mode de BIOS démarrage Legacy

  ```
  Legacy BIOS Boot Detected
  ```

- Exécutez la commande suivante pour vérifier que cela EFI apparaît dans le `dmesg` résultat.

  ```
  [ec2-user ~]$ dmesg | grep -i "EFI"
  ```

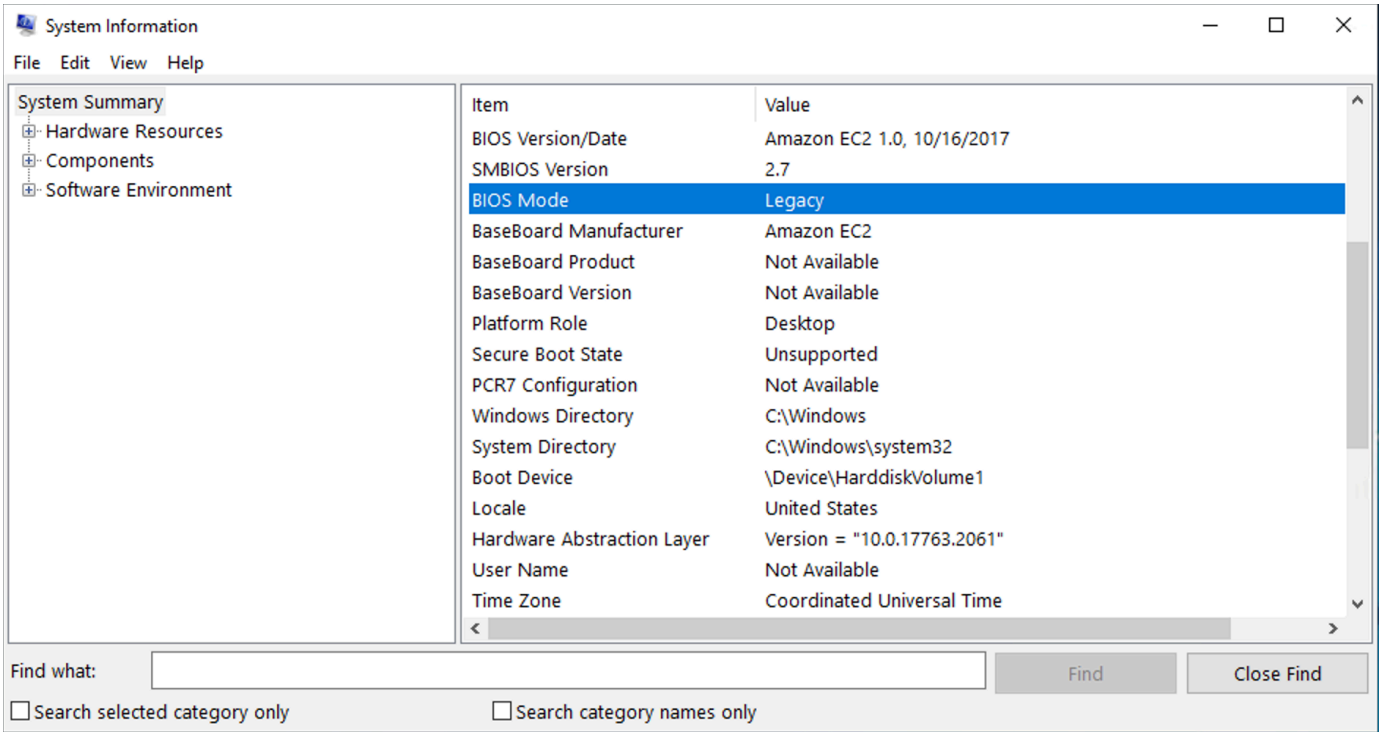
  Résultat attendu d'une instance démarrée en UEFI mode de démarrage

  ```
  [    0.000000] efi: Getting EFI parameters from FDT:
  [    0.000000] efi: EFI v2.70 by EDK II
  ```

Windows

Pour déterminer le mode de démarrage du système d'exploitation de l'instance

1. Connectez-vous à votre instance Windows à l'aide de RDP.
2. Accédez aux informations système et vérifiez la ligne BIOSMode.



Définir le mode de démarrage d'un Amazon EC2 AMI

Lorsque vous créez un AMI à l'aide de la register-imagecommande, vous pouvez définir le mode de démarrage du AMI à `uefilegacy-bios`, ou`uefi-preferred`.

Lorsque le mode de AMI démarrage est défini sur`uefi-preferred`, l'instance démarre comme suit :

- Pour les types d'instance qui prennent en charge les deux types UEFI et Legacy BIOS (par exemple,`m5.large`), l'instance démarre en utilisantUEFI.
- Pour les types d'instance qui ne prennent en charge que Legacy BIOS (par exemple,`m4.large`), l'instance démarre à l'aide de LegacyBIOS.

> **Note**
>
> Si vous définissez le mode de AMI démarrage sur`uefi-preferred`, le système d'exploitation doit prendre en charge le démarrage à la fois UEFI et le mode LegacyBIOS. Actuellement, vous ne pouvez pas utiliser la register-imagecommande pour créer une AMI annonce compatible à la fois avec Nitro TPM et UEFI Preferred.

> **Warning**
>
> Certaines fonctionnalités, telles que le démarrage UEFI sécurisé, ne sont disponibles que sur les instances qui démarrentUEFI. Lorsque vous utilisez le paramètre de mode de `uefi-preferred` AMI démarrage avec un type d'instance non compatibleUEFI, l'instance sera lancée en tant que Legacy BIOS et la fonctionnalité UEFI dépendante sera désactivée. Si vous comptez sur la disponibilité d'une fonctionnalité UEFI dépendante, définissez le paramètre du mode de AMI démarrage sur`uefi`.

Pour convertir une instance existante BIOS basée sur Legacy ou une instance existante UEFI en instance LegacyBIOS, vous devez effectuer un certain nombre d'étapes : tout d'abord, modifiez le volume et le système d'exploitation de l'instance pour qu'ils prennent en charge le mode de démarrage sélectionné. UEFI Créez ensuite un instantané du volume. Enfin, utilisez register-imagepour créer le à l'AMIaide de l'instantané.

Vous ne pouvez pas définir le mode de démarrage d'un AMI à l'aide de la create-imagecommande. Avec create-image, AMI hérite du mode de démarrage de l'EC2instance utilisée pour créer leAMI. Par exemple, si vous créez une instance AMI à partir d'une EC2 instance exécutée sur LegacyBIOS, le mode de AMI démarrage sera configuré comme`legacy-bios`. Si vous créez une instance AMI à partir d'une EC2 instance qui a été lancée à l'aide d'un AMI avec un mode de démarrage défini sur`uefi-preferred`, le AMI mode de démarrage créé sera également défini sur`uefi-preferred`.

> **Warning**
>
> La définition du paramètre du mode de AMI démarrage ne configure pas automatiquement le système d'exploitation pour le mode de démarrage spécifié. Avant de procéder à ces étapes, vous devez d'abord apporter les modifications appropriées au volume et au système d'exploitation de l'instance afin de permettre le démarrage à l'aide du mode de démarrage sélectionné ; sinon, le résultat ne AMI sera pas utilisable. Par exemple, si vous convertissez une instance Windows BIOS basée sur Legacy enUEFI, vous pouvez utiliser l'MBR2GPToutil de Microsoft pour convertir le disque système de MBR versGPT. Les modifications requises sont spécifiques au système d'exploitation. Pour plus d'informations, consultez le manuel de votre système d'exploitation.

Pour définir le mode de démarrage d'un AMI (AWS CLI)

1. Apporter des modifications appropriées au volume et au système d'exploitation de l'instance pour prendre en charge le démarrage via le mode de démarrage sélectionné. Les modifications requises sont spécifiques au système d'exploitation. Pour plus d'informations, consultez le manuel de votre système d'exploitation.

   > **Note**
   >
   > Si vous n'effectuez pas cette étape, ils ne AMI seront pas utilisables.

2. Pour trouver l'ID de volume de l'instance, utilisez la commande describe-instances. Vous allez créer un instantané de ce volume à l'étape suivante.

   ```
   aws ec2 describe-instances --region us-east-1 --instance-ids i-1234567890abcdef0
   ```

   Sortie attendue

   ```
   ...
               "BlockDeviceMappings": [
                           {
                               "DeviceName": "/dev/sda1",
                               "Ebs": {
                                   "AttachTime": "",
                                   "DeleteOnTermination": true,
                                   "Status": "attached",
                                   "VolumeId": "vol-1234567890abcdef0"
                               }
                           }
                           ...
   ```

3. Pour créer un instantané du volume, utilisez la commande create-snapshot. Utilisez l'ID de volume de l'étape précédente.

   ```
   aws ec2 create-snapshot --region us-east-1 --volume-id vol-1234567890abcdef0 --
   description "add text"
   ```

   Sortie attendue

   ```
   {
   ```

```
 "Description": "add text",
 "Encrypted": false,
 "OwnerId": "123",
 "Progress": "",
 "SnapshotId": "snap-01234567890abcdef",
 "StartTime": "",
 "State": "pending",
 "VolumeId": "vol-1234567890abcdef0",
 "VolumeSize": 30,
 "Tags": []
}
```

4. Notez l'ID d'instantané dans la sortie de l'étape précédente.
5. Attendez que la création de l'instantané soit `completed` avant de passer à l'étape suivante. Pour interroger l'état de l'instantané, utilisez la commande describe-snapshots.

```
aws ec2 describe-snapshots --region us-east-1 --snapshot-ids snap-01234567890abcdef
```

Exemple de sortie

```
{
    "Snapshots": [
        {
            "Description": "This is my snapshot",
            "Encrypted": false,
            "VolumeId": "vol-049df61146c4d7901",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2019-02-28T21:28:32.000Z",
            "Progress": "100%",
            "OwnerId": "012345678910",
            "SnapshotId": "snap-01234567890abcdef",
...
```

6. Pour en créer un nouveauAMI, utilisez la register-imagecommande. Utilisez l'ID d'instantané que vous avez noté à l'étape précédente.

   - Pour définir le mode de démarrage surUEFI, ajoutez le `--boot-mode` paramètre à la commande et `uefi` spécifiez-le comme valeur.

```
aws ec2 register-image \
   --region us-east-1 \
```

```
   --description "add description" \
   --name "add name" \
   --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-01234567890abcdef,DeleteOnTermination=true}" \
   --architecture x86_64 \
   --root-device-name /dev/sda1 \
   --virtualization-type hvm \
   --ena-support \
   --boot-mode uefi
```

- Pour définir le mode de démarrage sur `uefi-preferred`, ajoutez le paramètre `--boot-mode` à la commande et spécifiez `uefi-preferred` comme valeur.

```
aws ec2 register-image \
   --region us-east-1 \
   --description "add description" \
   --name "add name" \
   --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-01234567890abcdef,DeleteOnTermination=true}" \
   --architecture x86_64 \
   --root-device-name /dev/sda1 \
   --virtualization-type hvm \
   --ena-support \
   --boot-mode uefi-preferred
```

Sortie attendue

```
{
"ImageId": "ami-new_ami_123"
}
```

7. Pour vérifier que le nouveau modèle AMI possède le mode de démarrage que vous avez spécifié à l'étape précédente, utilisez la describe-imagescommande.

```
aws ec2 describe-images --region us-east-1 --image-id ami-new_ami_123
```

Sortie attendue

```
{
  "Images": [
   {
```

```
    "Architecture": "x86_64",
    "CreationDate": "2021-01-06T14:31:04.000Z",
    "ImageId": "ami-new_ami_123",
    "ImageLocation": "",
    ...
    "BootMode": "uefi"
    }
    ]
}
```

8. Lancez une nouvelle instance à l'aide de la nouvelle instance. AMI

   Si le mode de AMI démarrage est `uefi` ou`legacy-bios`, les instances créées à partir de celui-ci AMI auront le même mode de démarrage que leAMI. Si le mode de AMI démarrage est le cas`uefi-preferred`, l'instance démarrera en utilisant UEFI si le type d'instance est compatible UEFI ; sinon, l'instance démarrera en utilisant LegacyBIOS.

9. Pour vérifier que la nouvelle instance possède le mode de démarrage attendu, utilisez la commande describe-instances.

UEFIvariables pour les EC2 instances Amazon

Lorsque vous lancez une instance dont le mode de démarrage est défini surUEFI, un magasin de valeurs clés pour les variables est créé. Le magasin peut être utilisé par UEFI et par le système d'exploitation de l'instance pour stocker des UEFI variables.

UEFIles variables sont utilisées par le chargeur de démarrage et le système d'exploitation pour configurer le démarrage anticipé du système. Ils permettent au système d'exploitation de gérer certains paramètres du processus de démarrage, tels que l'ordre de démarrage ou la gestion des clés pour le démarrage UEFI sécurisé.

> **Warning**
>
> Toute personne capable de se connecter à l'instance (et potentiellement à tout logiciel exécuté sur l'instance), ou toute personne autorisée à l'utiliser GetInstanceUefiDataAPIsur l'instance, peut lire les variables. Vous ne devez jamais stocker de données sensibles, telles que des mots de passe ou des informations personnelles identifiables, dans le magasin UEFI variable.

UEFIpersistance variable

- Pour les instances lancées le 10 mai 2022 ou avant, les UEFI variables sont effacées au redémarrage ou à l'arrêt.
- Pour les instances lancées le 11 mai 2022 ou après cette date, les UEFI variables marquées comme non volatiles sont conservées au redémarrage et à l'arrêt/démarrage.
- Les instances bare metal ne préservent pas les variables UEFI non volatiles lors des opérations d'arrêt/démarrage des instances.

UEFIDémarrage sécurisé pour les EC2 instances Amazon

UEFISecure Boot s'appuie sur le processus de démarrage sécurisé de longue date d'Amazon EC2 et fournit des fonctionnalités supplémentaires defense-in-depth qui aident les clients à protéger leurs logiciels contre les menaces qui persistent après les redémarrages. Il garantit que l'instance démarre uniquement le logiciel signé avec des clés de chiffrement. Les clés sont stockées dans la base de données de clés du magasin de variables UEFI non volatiles. UEFILe démarrage sécurisé empêche toute modification non autorisée du flux de démarrage de l'instance.

Table des matières

Comment fonctionne UEFI Secure Boot avec les EC2 instances Amazon

UEFILe démarrage sécurisé est une fonctionnalité spécifiée dansUEFI, qui permet de vérifier l'état de la chaîne de démarrage. Il est conçu pour garantir que seuls les UEFI fichiers binaires vérifiés cryptographiquement sont exécutés après l'auto-initialisation du microprogramme. Ces fichiers binaires incluent les UEFI pilotes et le chargeur de démarrage principal, ainsi que les composants chargés en chaîne.

UEFISecure Boot spécifie quatre bases de données clés, qui sont utilisées dans une chaîne de confiance. Les bases de données sont stockées dans le magasin de UEFI variables.

La chaîne de confiance est la suivante :

Base de données de clés de plateforme (PK, Platform Key)

La base de données PK est la source de la confiance. Il contient une clé PK publique unique qui est utilisée dans la chaîne de confiance pour mettre à jour la base de données des clés d'échange de clés (KEK).

Pour modifier la base de données PK, vous devez disposer de la clé privée PK pour signer une demande de mise à jour. Cela inclut la suppression de la base de données PK en écrivant une clé PK vide.

Base de données de clés d'échange (KEK)

La KEK base de données est une liste de KEK clés publiques utilisées dans la chaîne de confiance pour mettre à jour les bases de données de signature (db) et de denylist (dbx).

Pour modifier la KEK base de données publique, vous devez disposer de la clé PK privée pour signer une demande de mise à jour.

Base de données de signature (db)

La base de données de base de données est une liste de clés publiques et de hachages utilisés dans la chaîne de confiance pour valider tous les binaires de UEFI démarrage.

Pour modifier la base de données de base de données, vous devez disposer de la clé PK privée ou de l'une des KEK clés privées pour signer une demande de mise à jour.

Base de données de liste d'exclusion de signature (dbx)

La base de données dbx est une liste de clés publiques et de hachages binaires qui ne sont pas fiables et sont utilisés dans la chaîne de confiance comme fichier de révocation.

La base de données dbx est toujours prioritaire sur toutes les autres bases de données clés.

Pour modifier la base de données dbx, vous devez disposer de la clé PK privée ou de l'une des KEK clés privées pour signer une demande de mise à jour.

Le UEFI Forum gère un dbx accessible au public pour de nombreux fichiers binaires et certificats connus comme défectueux à l'adresse https://uefi.org/revocationlistfile.

> **Important**
>
> UEFISecure Boot applique la validation des signatures à tous les UEFI fichiers binaires. Pour autoriser l'exécution d'un UEFI binaire dans UEFI Secure Boot, vous devez le signer avec l'une des clés de base de données privées décrites ci-dessus.

Par défaut, le démarrage UEFI sécurisé est désactivé et le système est activé`SetupMode`. Lorsque le système est en mode `SetupMode`, toutes les variables clés peuvent être mises à jour sans signature cryptographique. Lorsque le PK est défini, le démarrage UEFI sécurisé est activé et le SetupMode est quitté.

Lancez une EC2 instance Amazon avec le support UEFI Secure Boot

Lorsque vous lancez une EC2 instance Amazon avec un type d'instance pris en charge AMI et un type d'instance pris en charge, cette instance valide automatiquement les fichiers binaires de UEFI démarrage par rapport à sa base de données UEFI Secure Boot. Aucune configuration supplémentaire n'est requise. Vous pouvez également configurer le démarrage UEFI sécurisé sur une instance après son lancement.

> **Note**
>
> UEFISecure Boot protège votre instance et son système d'exploitation contre les modifications du flux de démarrage. Si vous en créez un nouveau AMI à partir d'une source sur AMI laquelle le démarrage UEFI sécurisé est activé et que vous modifiez certains paramètres pendant le processus de copie, par exemple en modifiant `UefiData` le démarrage sécuriséAMI, vous pouvez désactiver le démarrage UEFI sécurisé.

Table des matières

Soutenu AMIs

Linux AMIs

Pour lancer une instance Linux, le démarrage UEFI sécurisé AMI doit être activé sur Linux.

Amazon Linux prend en charge le démarrage UEFI sécurisé à partir de la version AL2 023 2023.1. Toutefois, le démarrage UEFI sécurisé n'est pas activé par défautAMIs. Pour plus d'informations, voir UEFISecure Boot dans le guide de l'utilisateur AL2 023. Les anciennes versions d'Amazon Linux AMIs ne sont pas activées pour le démarrage UEFI sécurisé. Pour utiliser un système compatibleAMI, vous devez effectuer un certain nombre d'étapes de configuration sur votre propre système LinuxAMI. Pour de plus amples informations, veuillez consulter Création d'un système Linux AMI avec des clés de démarrage UEFI sécurisées personnalisées.

Fenêtres AMIs

Pour lancer une instance Windows, le démarrage UEFI sécurisé AMI doit être activé sur Windows. Les fenêtres suivantes AMIs sont préconfigurées pour activer le démarrage UEFI sécurisé avec des clés Microsoft :

- TPM-Windows_Server-2_Anglais-Core-Base
- TPM-Windows_Server-2_Anglais-Base complète
- TPM-Windows_Server-2_Anglais-Complet- _2022_Enterprise SQL
- TPM-Windows_Server-2_Anglais-Complet- _2022_Standard SQL
- TPM-Windows_Server-2019-Anglais-Core-Base
- TPM-Windows_Server-2019-Anglais-Base complète
- TPM-Windows_Server-2019-Anglais-Complet- _2019_Enterprise SQL
- TPM-Windows_Server-2019-Anglais-Complet- _2019_Standard SQL
- TPM-Windows_Server-2016-Anglais-Core-Base
- TPM-Windows_Server-2016-Anglais-Base complète

À l'heure actuelle, nous ne prenons pas en charge l'importation de Windows avec UEFI Secure Boot à l'aide de la import-imagecommande.

Types d'instance pris en charge

Tous les types d'instances virtualisées compatibles prennent UEFI également en charge le démarrage UEFI sécurisé. Pour les types d'instances qui prennent en charge le démarrage UEFI sécurisé, consultezExigences relatives au mode de UEFI démarrage.

> **Note**
>
> Les types d'instances bare metal ne prennent pas en charge le démarrage UEFI sécurisé.

Vérifiez si une EC2 instance Amazon est activée pour le démarrage UEFI sécurisé

Vous pouvez utiliser les procédures suivantes pour déterminer si un Amazon EC2 est activé pour le démarrage UEFI sécurisé.

Instances Linux

Vous pouvez utiliser cet `mokutil` utilitaire pour vérifier si une instance Linux est activée pour le démarrage UEFI sécurisé. Si `mokutil` n'est pas installé sur votre instance, vous devez l'installer. Pour les instructions d'installation d'Amazon Linux 2, consultez Rechercher et installer des packages logiciels sur une instance Amazon Linux 2. Pour les autres distributions Linux, consultez leur documentation spécifique.

Pour vérifier si une instance Linux est activée pour le démarrage UEFI sécurisé

Connectez-vous à votre instance et exécutez la commande suivante comme `root` dans une fenêtre de terminal.

```
mokutil --sb-state
```

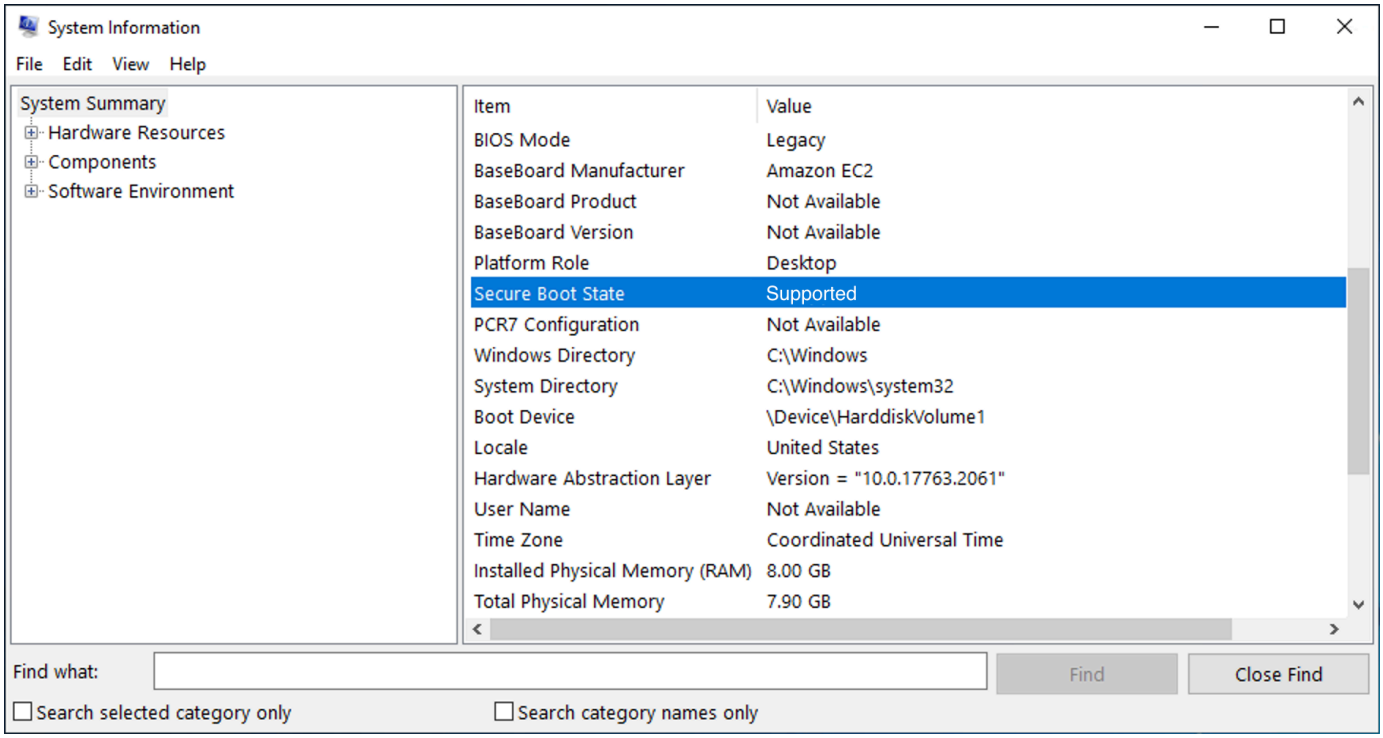
Voici un exemple de sortie.

- Si le démarrage UEFI sécurisé est activé, la sortie contient`SecureBoot enabled`.
- Si le démarrage UEFI sécurisé n'est pas activé, la sortie contient `SecureBoot disabled` ou`Failed to read SecureBoot`.

instances Windows

Pour vérifier si une instance Windows est activée pour le démarrage UEFI sécurisé

1. Connectez-vous à votre instance.
2. Ouvrez l'outil msinfo32.
3. Vérifiez le champ Secure Boot State (État du démarrage sécurisé). Si le démarrage UEFI sécurisé est activé, la valeur est Supported, comme indiqué dans l'image suivante.



Vous pouvez également utiliser l' PowerShell applet de commande Windows `Confirm-SecureBootUEFI` pour vérifier l'état du démarrage sécurisé. Pour plus d'informations sur l'applet de commande, consultez la section Confirm- SecureBoot UEFI dans la documentation Microsoft.

Création d'un système Linux AMI avec des clés de démarrage UEFI sécurisées personnalisées

Cette procédure explique comment créer un système Linux AMI avec UEFI Secure Boot et des clés privées personnalisées. Amazon Linux prend en charge le démarrage UEFI sécurisé à partir de la version AL2 023 2023.1. Pour plus d'informations, voir UEFISecure Boot dans le guide de l'utilisateur AL2 023.

> **Important**
>
> La procédure suivante s'adresse uniquement aux utilisateurs expérimentés. Vous devez avoir une connaissance suffisante du flux SSL de démarrage des distributions Linux pour utiliser ces procédures.

Prérequis

- Les outils suivants seront utilisés :
  - Ouvrez SSL — https://www.openssl.org/
  - éfivar — éfivar https://github.com/rhboot/
  - efitools : https://git.kernel.org/pub/scm/linux/kernel/git/jejb/efitools.git/
  - get-instance-uefi-data AWS CLI commande
- Votre instance Linux doit avoir été lancée avec un système Linux AMI compatible avec le mode de UEFI démarrage et contenir des données non volatiles.

Les instances nouvellement créées sans clés de démarrage UEFI sécurisé sont créées dans`SetupMode`, ce qui vous permet d'inscrire vos propres clés. Certaines AMIs sont préconfigurées avec UEFI Secure Boot et vous ne pouvez pas modifier les clés existantes. Si vous souhaitez modifier les clés, vous devez en créer une nouvelle sur la AMI base de l'originalAMI.

Vous pouvez propager les clés dans le magasin de variables de deux manières, décrites dans les options A et B suivantes. L'option A décrit comment le faire depuis l'instance, en imitant le flux de matériel réel. L'option B décrit comment créer un blob binaire, qui est ensuite transmis sous forme de fichier codé en base64 lorsque vous créez le. AMI Pour les deux options, vous devez d'abord créer les trois paires de clés utilisées pour la chaîne de confiance.

Étape 1 : Création de trois paires de clés

UEFISecure Boot est basé sur les trois bases de données clés suivantes, qui sont utilisées dans une chaîne de confiance : la clé de plate-forme (PK), la clé d'échange de clés (KEK) et la base de données de signatures (db) .[1]

Vous créez chaque clé sur l'instance. Pour préparer les clés publiques dans un format valide pour la norme UEFI Secure Boot, vous devez créer un certificat pour chaque clé. `DER`définit le SSL format (encodage binaire d'un format). Vous convertissez ensuite chaque certificat en une liste de UEFI signatures, qui est le format binaire compris par UEFI Secure Boot. Enfin, vous signez chaque certificat avec la clé correspondante.

Rubriques

- Préparez-vous à créer les paires de clés
- Paire de clés 1 : créer la clé de plateforme (PK)
- Paire de clés 2 : créer la clé d'échange de clés (KEK)

- Paire de clés 3 : créez la base de données de signatures (db)
- Signez l'image de démarrage (noyau) avec la clé privée

Préparez-vous à créer les paires de clés

Avant de créer les paires de clés, créez un identifiant unique global (GUID) à utiliser lors de la génération de clés.

1. Connectez-vous à l'instance.
2. Exécutez la commande suivante dans un shell.

```
uuidgen --random > GUID.txt
```

Paire de clés 1 : créer la clé de plateforme (PK)

Le PK est à l'origine de la confiance pour les instances UEFI Secure Boot. Le PK privé est utilisé pour mettre à jour leKEK, qui peut à son tour être utilisé pour ajouter des clés autorisées à la base de données de signatures (db).

La norme X.509 est utilisée pour créer la paire de clés. Pour plus d'informations sur la norme, veuillez consulter X.509 sur Wikipédia.

Pour créer la PK

1. Créez la clé. Vous devez nommer la variable PK.

```
openssl req -newkey rsa:4096 -nodes -keyout PK.key -new -x509 -sha256 -days 3650 -
subj "/CN=Platform key/" -out PK.crt
```

   Les paramètres suivants sont spécifiés :

   - `-keyout PK.key` : le fichier de clé privée.
   - `-days 3650` : le nombre de jours de validité du certificat.
   - `-out PK.crt`— Le certificat utilisé pour créer la UEFI variable.
   - `CN=Platform key` : le nom commun (CN) de la clé. Vous pouvez saisir le nom de votre propre organisation au lieu de *Platform key*.
2. Créez le certificat.

```
openssl x509 -outform DER -in PK.crt -out PK.cer
```

3. Convertissez le certificat en liste de UEFI signatures.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" PK.crt PK.esl
```

4. Signez la liste de UEFI signatures avec le PK privé (auto-signé).

```
sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt PK PK.esl PK.auth
```

Paire de clés 2 : créer la clé d'échange de clés (KEK)

Le private KEK est utilisé pour ajouter des clés à la base de données, qui est la liste des signatures autorisées pour démarrer sur le système.

Pour créer le KEK

1. Créez la clé.

```
openssl req -newkey rsa:4096 -nodes -keyout KEK.key -new -x509 -sha256 -days 3650 -
subj "/CN=Key Exchange Key/" -out KEK.crt
```

2. Créez le certificat.

```
openssl x509 -outform DER -in KEK.crt -out KEK.cer
```

3. Convertissez le certificat en liste de UEFI signatures.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" KEK.crt KEK.esl
```

4. Signez la liste de signatures avec la PK privée.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt KEK KEK.esl KEK.auth
```

Paire de clés 3 : créez la base de données de signatures (db)

La liste db contient des clés autorisées qui sont habilitées à être démarrées sur le système. Pour modifier la liste, le privé KEK est nécessaire. Les images de démarrage seront signées avec la clé privée créée au cours de cette étape.

Pour créer la db

1. Créez la clé.

```
openssl req -newkey rsa:4096 -nodes -keyout db.key -new -x509 -sha256 -days 3650 -
subj "/CN=Signature Database key/" -out db.crt
```

2. Créez le certificat.

```
openssl x509 -outform DER -in db.crt -out db.cer
```

3. Convertissez le certificat en liste de UEFI signatures.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" db.crt db.esl
```

4. Signez la liste de signatures avec le privéKEK.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k KEK.key -c KEK.crt db db.esl db.auth
```

Signez l'image de démarrage (noyau) avec la clé privée

Pour Ubuntu 22.04, les images suivantes nécessitent des signatures.

```
/boot/efi/EFI/ubuntu/shimx64.efi
/boot/efi/EFI/ubuntu/mmx64.efi
/boot/efi/EFI/ubuntu/grubx64.efi
/boot/vmlinuz
```

Pour signer une image

Utilisez la syntaxe suivante pour signer une image.

```
sbsign --key db.key --cert db.crt --output /boot/vmlinuz /boot/vmlinuz
```

> **Note**
>
> Vous devez signer tous les nouveaux noyaux. `/boot/vmlinuz` crée généralement un lien symbolique vers le dernier noyau installé.

Reportez-vous à la documentation de votre distribution pour connaître votre chaîne de démarrage et les images requises.

[1] Merci à la ArchWiki communauté pour tout le travail qu'elle a accompli. Les commandes permettant de créer le PK, de créer leKEK, de créer la base de données et de signer l'image proviennent de la section Création de clés, rédigée par l'équipe de ArchWiki maintenance et/ou les ArchWiki contributeurs.

Étape 2 (Option A) : ajouter des clés à la variable store depuis l'instance

Une fois que vous avez créé les trois paires de clés, vous pouvez vous connecter à votre instance et ajouter les clés au magasin de variables depuis l'instance en effectuant les étapes suivantes.

Étapes de l'option A :

- Étape 1 : Lancer une instance qui prendra en charge le démarrage UEFI sécurisé
- Étape 2 : configurer une instance pour prendre en charge le démarrage UEFI sécurisé
- Étape 3 : créer un AMI à partir de l'instance

Étape 1 : Lancer une instance qui prendra en charge le démarrage UEFI sécurisé

Lorsque vous lancez une instance avec les prérequis suivants, l'instance sera alors prête à être configurée pour prendre en charge le démarrage UEFI sécurisé. Vous ne pouvez activer la prise en charge du démarrage UEFI sécurisé sur une instance qu'au lancement ; vous ne pourrez pas l'activer ultérieurement.

Prérequis

- AMI— Le Linux AMI doit prendre en charge le mode de UEFI démarrage. Pour vérifier que le mode de UEFI démarrage est pris AMI en charge, le paramètre du mode de AMI démarrage doit être uefi. Pour de plus amples informations, veuillez consulter Déterminer le paramètre du mode de démarrage d'un Amazon EC2 AMI.

Notez que Linux est AWS uniquement AMIs configuré pour prendre en charge UEFI les types d'instances basés sur Graviton. AWS ne fournit actuellement pas de Linux x86_64 prenant en charge UEFI le mode de AMIs démarrage. Vous pouvez configurer le vôtre AMI pour prendre en charge le mode de UEFI démarrage pour toutes les architectures. Pour configurer le vôtre AMI afin de prendre en charge le mode de UEFI démarrage, vous devez effectuer vous-même un certain nombre d'étapes de configurationAMI. Pour de plus amples informations, veuillez consulter Définir le mode de démarrage d'un Amazon EC2 AMI.

- Type d'instance : tous les types d'instances virtualisées compatibles prennent UEFI également en charge le démarrage UEFI sécurisé. Les types d'instances bare metal ne prennent pas en charge le démarrage UEFI sécurisé. Pour les types d'instances qui prennent en charge le démarrage UEFI sécurisé, consultezExigences relatives au mode de UEFI démarrage.
- Lancez votre instance après la sortie de UEFI Secure Boot. Seules les instances lancées après le 10 mai 2022 (date de sortie de UEFI Secure Boot) peuvent prendre en charge le démarrage UEFI sécurisé.

Après avoir lancé votre instance, vous pouvez vérifier qu'elle est prête à être configurée pour prendre en charge le démarrage UEFI sécurisé (en d'autres termes, vous pouvez passer à l'étape 2) en vérifiant si UEFI des données sont présentes. La présence de UEFI données indique que les données non volatiles sont persistantes.

Pour vérifier si votre instance est prête pour l'étape 2

Utilisez la commande get-instance-uefi-data et spécifiez l'ID de l'instance.

```
aws ec2 get-instance-uefi-data --instance-id i-0123456789example
```

L'instance est prête pour l'étape 2 si UEFI des données sont présentes dans la sortie. Si la sortie est vide, l'instance ne peut pas être configurée pour prendre en charge le démarrage UEFI sécurisé. Cela peut se produire si votre instance a été lancée avant que le support UEFI Secure Boot ne soit disponible. Lancez une nouvelle instance et réessayez.

Étape 2 : configurer une instance pour prendre en charge le démarrage UEFI sécurisé

Inscrivez les paires de clés dans votre magasin de UEFI variables sur l'instance

> **Warning**
>
> Vous devez signer vos images de démarrage après avoir inscrit les clés, sinon vous ne pourrez pas démarrer votre instance.

Après avoir créé les listes de UEFI signatures signées (PKKEK,, etdb), elles doivent être inscrites dans le UEFI microprogramme.

Écriture dans la variable PK n'est possible que si :

- Aucune PK n'est encore inscrite, ce qui est indiqué si la variable `SetupMode` est `1`. Pour vérifier cela, utilisez la commande suivante. La sortie est soit `1`, soit `0`.

  ```
  efivar -d -n 8be4df61-93ca-11d2-aa0d-00e098032b8c-SetupMode
  ```

- La nouvelle PK est signée par la clé privée de la PK existante.

Pour enregistrer les clés dans votre magasin UEFI variable

Les commandes suivantes doivent être exécutées sur l'instance.

Si cette option SetupMode est activée (la valeur est1), les clés peuvent être inscrites en exécutant les commandes suivantes sur l'instance :

```
[ec2-user ~]$ efi-updatevar -f db.auth db
```

```
[ec2-user ~]$ efi-updatevar -f KEK.auth KEK
```

```
[ec2-user ~]$ efi-updatevar -f PK.auth PK
```

Pour vérifier que le démarrage UEFI sécurisé est activé

Pour vérifier que le démarrage UEFI sécurisé est activé, suivez les étapes décrites dansVérifiez si une EC2 instance Amazon est activée pour le démarrage UEFI sécurisé.

Vous pouvez désormais exporter votre répertoire de UEFI variables à l'aide de la get-instance-uefi-dataCLIcommande, ou vous pouvez passer à l'étape suivante et signer vos images de démarrage pour redémarrer sur une instance compatible UEFI Secure Boot.

Étape 3 : créer un AMI à partir de l'instance

Pour créer une instance AMI à partir de l'instance, vous pouvez utiliser la console ou le `CreateImage` APICLI, ouSDKs. Pour des instructions sur l'utilisation de la console, consultez Créez un compte soutenu EBS par Amazon AMI. Pour les API instructions, voir CreateImage.

> **Note**
>
> copie `CreateImage` API automatiquement le magasin de UEFI variables de l'instance dans leAMI. La console utilise le `CreateImage`API. Une fois que vous aurez lancé des instances à l'aide de cette optionAMI, les instances disposeront du même magasin de UEFI variables.

Étape 2 (Option B) : créer un blob binaire contenant un magasin de variables prérempli

Après avoir créé les trois paires de clés, vous pouvez créer un blob binaire contenant une banque de variables préremplie contenant les clés de démarrage UEFI sécurisé.

> **Warning**
>
> Vous devez signer vos images de démarrage avant d'inscrire les clés, sinon vous ne pourrez pas démarrer votre instance.

Étapes de l'option B :

- Étape 1 : créer un nouveau magasin de variables ou mettre à jour un stockage existant
- Étape 2 : Téléchargez le blob binaire lors AMI de sa création

Étape 1 : créer un nouveau magasin de variables ou mettre à jour un stockage existant

Vous pouvez créer le magasin de variables hors ligne sans instance en cours d'exécution à l'aide de l'outil python-uefivars. L'outil peut créer un nouveau magasin de variables à partir de vos clés. Le script prend actuellement en charge le EDK2 format, le AWS format et une JSON représentation qui est plus facile à modifier avec des outils de niveau supérieur.

Pour créer le magasin de variables hors ligne sans instance en cours d'exécution

1. Téléchargez l'outil en cliquant sur le lien suivant.

```
https://github.com/awslabs/python-uefivars
```

2. Créez un nouveau magasin de variables à partir de vos clés en exécutant la commande suivante. Cela créera un blob binaire codé en base64 dans *your_binary_blob*.bin. L'outil prend également en charge la mise à jour d'un blob binaire via le paramètre `-I`.

```
./uefivars.py -i none -o aws -O your_binary_blob.bin -P PK.esl -K KEK.esl --db
 db.esl --dbx dbx.esl
```

Étape 2 : Téléchargez le blob binaire lors AMI de sa création

register-imageÀ utiliser pour transmettre les données UEFI variables de votre magasin. Pour le paramètre `--uefi-data`, spécifiez votre blob binaire et pour le paramètre `--boot-mode`, spécifiez `uefi`.

```
aws ec2 register-image \
    --name uefi_sb_tpm_register_image_test \
    --uefi-data $(cat your_binary_blob.bin) \
    --block-device-mappings "DeviceName=/dev/sda1,Ebs=
 {SnapshotId=snap-0123456789example,DeleteOnTermination=true}" \
    --architecture x86_64 \
    --root-device-name /dev/sda1 \
    --virtualization-type hvm \
    --ena-support \
    --boot-mode uefi
```

Créez le blob AWS binaire pour UEFI Secure Boot

Vous pouvez suivre les étapes suivantes pour personnaliser les variables UEFI Secure Boot lors de leur AMI création. Le KEK qui est utilisé dans ces étapes est à jour en septembre 2021. Si Microsoft met à jour leKEK, vous devez utiliser la dernière versionKEK.

Pour créer le AWS blob binaire

1. Créez une liste de signatures PK vide.

```
touch empty_key.crt
cert-to-efi-sig-list empty_key.crt PK.esl
```

2. Téléchargez les KEK certificats.

```
https://go.microsoft.com/fwlink/?LinkId=321185
```

3. Enveloppez les KEK certificats dans une liste de UEFI signatures (`siglist`).

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_Win_KEK.esl MicCorKEKCA2011_2011-06-24.crt
```

4. Téléchargez les certificats db de Microsoft.

```
https://www.microsoft.com/pkiops/certs/MicWinProPCA2011_2011-10-19.crt
https://www.microsoft.com/pkiops/certs/MicCorUEFCA2011_2011-06-27.crt
```

5. Générez la liste de signatures db.

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_Win_db.esl MicWinProPCA2011_2011-10-19.crt
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_UEFI_db.esl MicCorUEFCA2011_2011-06-27.crt
cat MS_Win_db.esl MS_UEFI_db.esl > MS_db.esl
```

6. Téléchargez une demande de modification dbx mise à jour à partir du lien suivant.

```
https://uefi.org/revocationlistfile
```

7. La demande de modification dbx que vous avez téléchargée à l'étape précédente est déjà signée auprès de MicrosoftKEK. Vous devez donc la supprimer ou la déballer. Vous pouvez utiliser les liens suivants.

```
https://gist.github.com/out0xb2/f8e0bae94214889a89ac67fceb37f8c0
```

```
https://support.microsoft.com/en-us/topic/microsoft-guidance-for-applying-secure-
boot-dbx-update-e3b9e4cb-a330-b3ba-a602-15083965d9ca
```

8. Créez un magasin de UEFI variables à l'aide du `uefivars.py` script.

```
./uefivars.py -i none -o aws -O uefiblob-microsoft-keys-empty-pk.bin -P ~/PK.esl -K
 ~/MS_Win_KEK.esl --db ~/MS_db.esl  --dbx ~/dbx-2021-April.bin
```

9. Vérifiez le blob binaire et le magasin de UEFI variables.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o json | less
```

10. Vous pouvez mettre à jour le blob en le transmettant à nouveau au même outil.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o aws -O uefiblob-
microsoft-keys-empty-pk.bin -P ~/PK.esl -K ~/MS_Win_KEK.esl --db ~/MS_db.esl  --dbx
 ~/dbx-2021-April.bin
```

Sortie attendue

```
Replacing PK
Replacing KEK
Replacing db
Replacing dbx
```

Utiliser le chiffrement avec des AMI basées sur EBS

Les AMI basées sur des instantanés Amazon EBS peuvent tirer parti du chiffrement Amazon EBS. Les instantanés de volumes de données et racine peuvent être chiffrés et attachés à une AMI. Vous pouvez lancer des instances et copier des images avec une prise en charge complète du chiffrement EBS. Les paramètres de chiffrement pour ces opérations sont pris en charge dans toutes les régions où ils AWS KMS sont disponibles.

Les instances EC2 avec des volumes EBS chiffrés sont lancées à partir des AMIs de la même manière que les autres instances. De plus, lorsque vous lancez une instance à partir d'une AMI basée sur des instantanés EBS non chiffrés, vous pouvez chiffrer une partie ou l'ensemble des volumes pendant le lancement.

À l'instar des volumes EBS, les instantanés des AMI peuvent être chiffrés soit par défaut AWS KMS key, soit avec une clé gérée par le client que vous spécifiez. Dans tous les cas, vous devez être autorisé à utiliser la clé KMS sélectionnée.

Les AMI contenant des instantanés chiffrés peuvent être partagées entre les AWS comptes. Pour plus d'informations, consultez Comprendre AMI l'utilisation partagée sur Amazon EC2.

Rubriques relatives au chiffrement avec des AMI basées sur EBS

- Scénarios de lancement d'instances
- Scénarios de copie d'images

Scénarios de lancement d'instances

Les instances Amazon EC2 sont lancées à partir d'AMI à l'aide de l'`RunInstances`action avec des paramètres fournis par le biais du mappage de périphériques en mode bloc, soit au moyen de l'API ou de la CLI Amazon EC2, soit directement à l'aide de l'API AWS Management Console ou de la CLI Amazon EC2. Pour plus d'informations, consultez Bloquer les mappages d'appareils pour les volumes sur les instances Amazon EC2. Pour des exemples de contrôle du mappage des périphériques en mode bloc à partir du AWS CLI, voir Lancer, répertorier et résilier des instances EC2.

Par défaut, sans paramètres de chiffrement explicites, une action `RunInstances` conserve l'état de chiffrement existant des instantanés source d'une AMI lors de la restauration des volumes EBS à partir de ceux-ci. Si le chiffrement est activé par défaut, tous les volumes créés à partir de l'AMI (qu'ils soient issus de snapshots chiffrés ou non chiffrés) sont chiffrés. Si le chiffrement par défaut n'est pas activé, l'instance conserve l'état de chiffrement de l'AMI.

Vous pouvez également lancer une instance et, simultanément, appliquer un nouvel état de chiffrement aux volumes créés en spécifiant les paramètres de chiffrement. Dans un tel cas, les comportements suivants sont observés :

Lancement sans paramètres de chiffrement

- Un instantané non chiffré est restauré dans un volume non chiffré, sauf si le chiffrement par défaut est activé, auquel cas tous les volumes nouvellement créés seront chiffrés.
- Un instantané non chiffré que vous possédez est restauré dans un volume qui est chiffré avec la même clé KMS.
- Un instantané chiffré qui ne vous appartient pas (par exemple, l'AMI est partagée avec vous) est restauré sur un volume chiffré par la clé KMS par défaut de votre AWS compte.

Les comportements par défaut peuvent être ignorés en spécifiant les paramètres de chiffrement. Les paramètres disponibles sont `Encrypted` et `KmsKeyId`. La définition du seul paramètre `Encrypted` produit les effets suivants :

Comportements en cas de lancement d'instance avec le paramètre **`Encrypted`** défini, mais sans spécifier le paramètre **`KmsKeyId`**

- Un instantané non chiffré est restauré dans un volume EBS qui est chiffré avec la clé KMS par défaut de votre compte AWS .
- Un instantané chiffré que vous possédez est restauré dans un volume EBS qui est chiffré avec la même clé KMS. (En d'autres mots, le paramètre `Encrypted` est sans effet.)
- Un instantané chiffré qui ne vous appartient pas (c'est-à-dire que l'AMI est partagée avec vous) est restauré sur un volume chiffré à l'aide de la clé KMS par défaut de votre AWS compte. (En d'autres mots, le paramètre `Encrypted` est sans effet.)

La définition des paramètres `Encrypted` et `KmsKeyId` vous permet de spécifier une clé clé KMS autre que la clé par défaut pour une opération de chiffrement. Les comportements suivants sont observés :

Instance avec définition des paramètres **`Encrypted`** et **`KmsKeyId`**

- Un instantané non chiffré est restauré dans un volume EBS qui est chiffré avec la clé KMS spécifiée.
- Un instantané chiffré est restauré dans un volume EBS qui est chiffré non pas avec la clé KMS d'origine mais avec la clé KMS spécifiée.

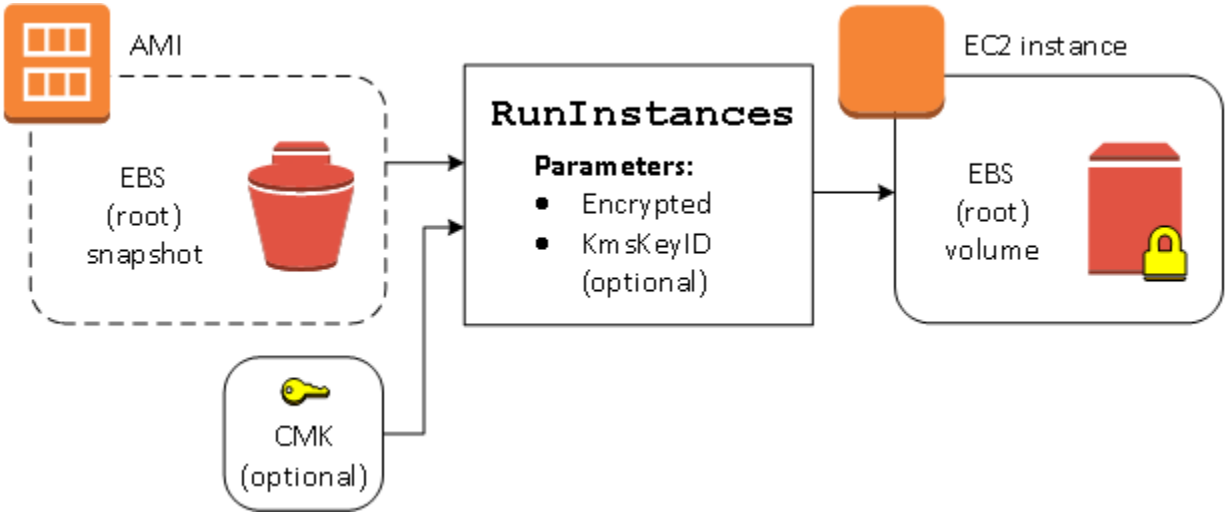
L'envoi de `KmsKeyId` sans définir également le paramètre `Encrypted` génère une erreur.

Les sections suivantes fournissent des exemples de lancement d'instances à partir d'AMI avec des paramètres de chiffrement autres que les paramètres par défaut. Dans chacun de ces scénarios, les paramètres fournis à l'action `RunInstances` entraînent un changement de l'état de chiffrement pendant la restauration d'un volume à partir d'un instantané.

Pour plus d'informations sur l'utilisation de la console pour lancer une instance à partir d'une AMI, consultez la section Lancer une EC2 instance Amazon.

Chiffrement d'un volume pendant le lancement

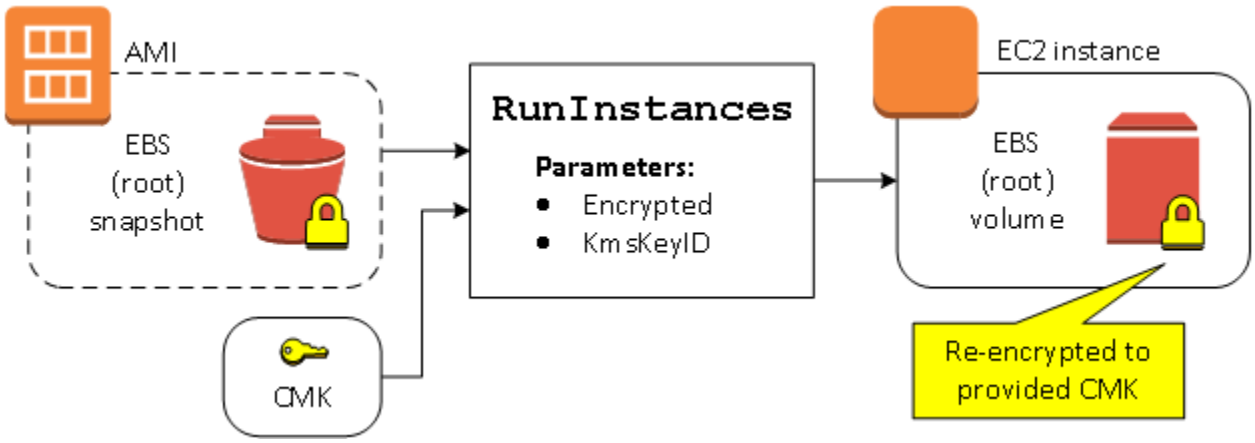
Dans cet exemple, une AMI basée sur un instantané non chiffré est utilisée pour lancer une instance EC2 avec un volume EBS chiffré.



Le paramètre `Encrypted` seul entraîne le chiffrement du volume pour cette instance. Le paramètre `KmsKeyId` est facultatif. Si aucun ID de clé KMS n'est spécifié, la clé KMS par défaut du AWS compte est utilisée pour chiffrer le volume. Pour chiffrer le volume avec une autre clé clé KMS que vous possédez, fournissez le paramètre `KmsKeyId`.

Rechiffrement d'un volume pendant le lancement

Dans cet exemple, une AMI basée sur un instantané chiffré est utilisée pour lancer une instance EC2 avec un volume EBS chiffré à l'aide d'une nouvelle clé KMS.

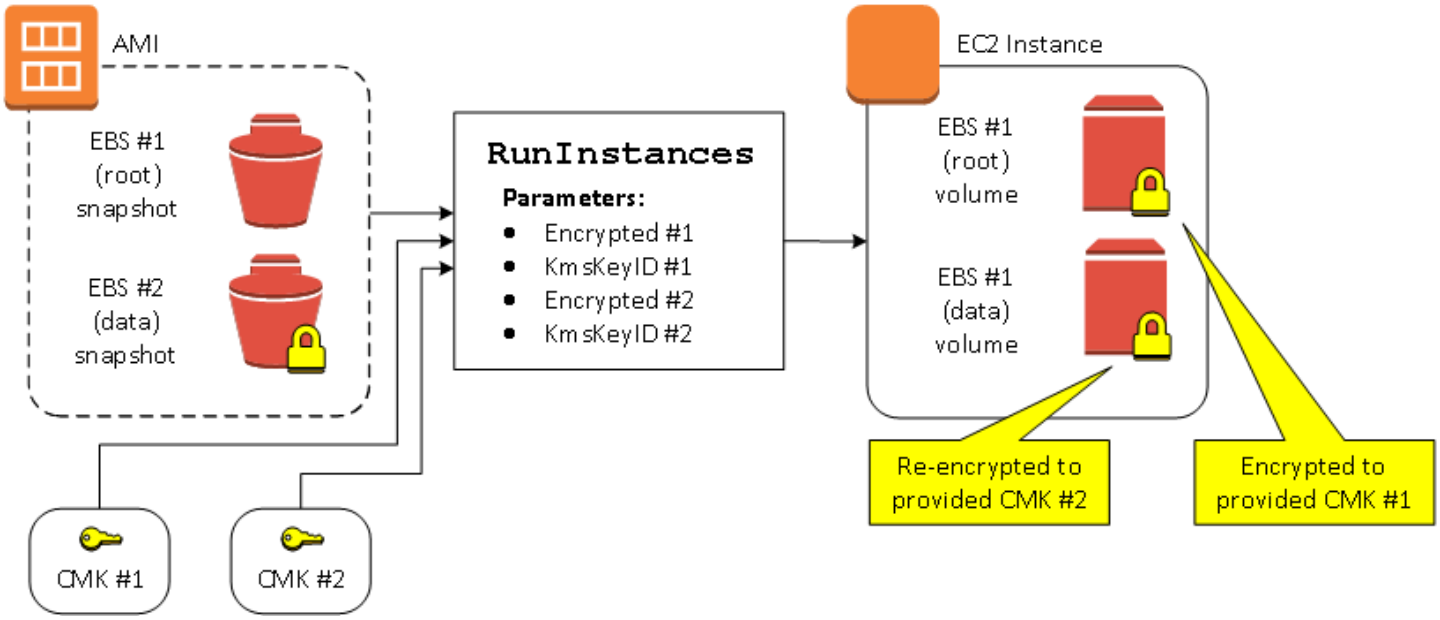


Si vous possédez l'AMI et que vous ne spécifiez pas de paramètres de chiffrement, l'instance obtenue dispose d'un volume chiffré avec la même clé KMS que l'instantané. Si l'AMI est partagée avec vous mais que vous n'en êtes pas propriétaire, et si vous ne spécifiez pas de paramètres de

chiffrement, le volume est chiffré avec votre clé KMS par défaut. Avec les paramètres de chiffrement fournis, comme illustré, le volume est chiffré avec la clé KMS spécifiée.

Modification de l'état de chiffrement de plusieurs volumes pendant le lancement

Dans cet exemple plus complexe, une AMI basée sur plusieurs instantanés (chacun avec son propre état de chiffrement) est utilisée pour lancer une instance EC2 avec un volume nouvellement chiffré et un volume rechiffré.



Dans ce scénario, l'action `RunInstances` reçoit des paramètres de chiffrement pour chacun des instantanés source. Lorsque tous les paramètres de chiffrement sont spécifiés, l'instance créée est la même, que vous possédiez ou non l'AMI.

Scénarios de copie d'images

Les AMI Amazon EC2 sont copiées au moyen de l'action `CopyImage`, soit via la AWS Management Console , soit directement avec l'API Amazon EC2 ou la CLI.

Par défaut, sans paramètres de chiffrement explicites, une action `CopyImage` conserve l'état de chiffrement existant des instantanés source d'une AMI lors de la copie. Vous pouvez également copier une AMI et, simultanément, appliquer un nouvel état de chiffrement à ses instantanés EBS associés en spécifiant les paramètres de chiffrement. Dans un tel cas, les comportements suivants sont observés :

Copie sans paramètres de chiffrement

- Un instantané non chiffré est copié dans un autre instantané non chiffré, sauf si le chiffrement par défaut est activé, auquel cas tous les instantanés nouvellement créés seront chiffrés.
- Un instantané chiffré que vous possédez est copié dans un instantané chiffré avec la même clé KMS.
- Un instantané chiffré qui ne vous appartient pas (c'est-à-dire que l'AMI est partagée avec vous) est copié dans un instantané chiffré par la clé KMS par défaut de votre AWS compte.

Tous ces comportements par défaut peuvent être ignorés en spécifiant les paramètres de chiffrement. Les paramètres disponibles sont `Encrypted` et `KmsKeyId`. La définition du seul paramètre `Encrypted` produit les effets suivants :

Comportements en cas de copie-image avec le paramètre **`Encrypted`** défini, mais pas le paramètre **`KmsKeyId`**

- Un instantané non chiffré est copié dans un instantané chiffré avec la clé KMS par défaut du compte AWS .
- Un instantané chiffré est copié dans un instantané chiffré avec la même clé KMS. (En d'autres mots, le paramètre `Encrypted` est sans effet.)
- Un instantané chiffré qui ne vous appartient pas (c'est-à-dire que l'AMI est partagée avec vous) est copié sur un volume chiffré à l'aide de la clé KMS par défaut de votre AWS compte. (En d'autres mots, le paramètre `Encrypted` est sans effet.)

La définition des paramètres `Encrypted` et `KmsKeyId` vous permet de spécifier une clé clé KMS gérée par le client pour une opération de chiffrement. Les comportements suivants sont observés :

Comportements en cas de copie-image avec les paramètres **`Encrypted`** et **`KmsKeyId`** définis

- Un instantané non chiffré est copié dans un instantané chiffré avec la clé KMS spécifiée.
- Un instantané chiffré est copié dans un instantané qui est chiffré non pas avec la clé KMS d'origine mais avec la clé KMS spécifiée.

L'envoi de `KmsKeyId` sans définir également le paramètre `Encrypted` génère une erreur.

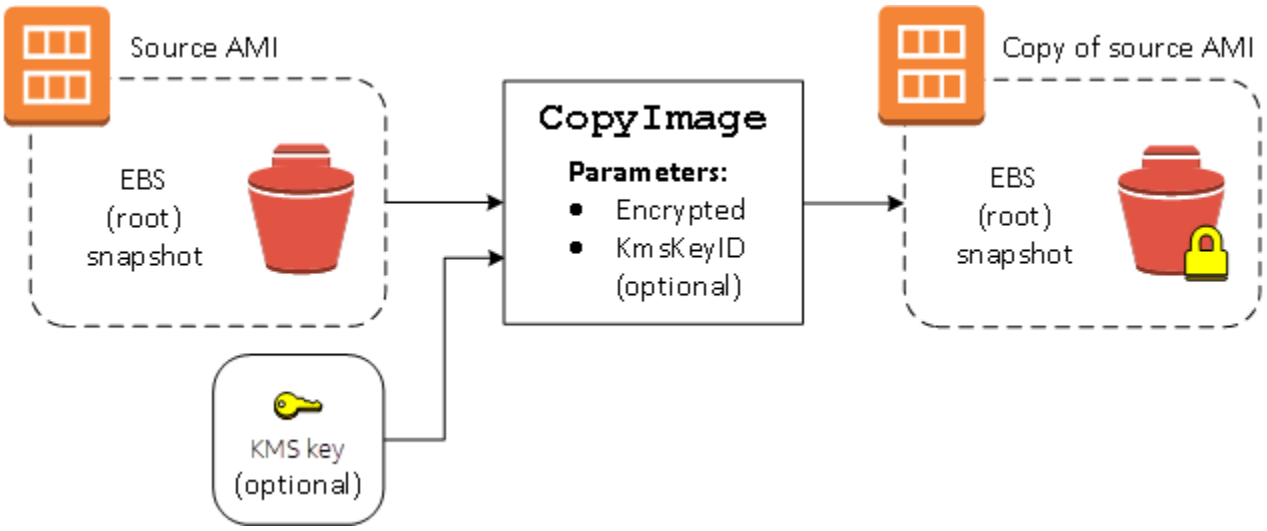
La section suivante fournit un exemple de copie d'une AMI avec des paramètres de chiffrement personnalisés, ce qui entraîne un changement de l'était de chiffrement.

Pour obtenir des instructions détaillées sur l'utilisation de la console, consultez la section Copier un Amazon EC2 AMI.

Chiffrement d'une image non chiffrée pendant la copie

Dans ce scénario, une AMI basée sur un instantané racine non chiffré est copiée sur une AMI avec un instantané racine chiffré. L'action `CopyImage` est appelée avec deux paramètres de chiffrement, y compris une clé gérée par le client. Par conséquent, l'état de chiffrement de l'instantané racine change, de sorte que l'AMI cible est basée sur un instantané racine contenant les mêmes données que l'instantané source, mais chiffrée à l'aide de la clé spécifiée. Vous supportez des coûts de stockage pour les instantanés dans les deux AMI, ainsi que des frais pour toutes les instances que vous lancez à partir de l'une ou l'autre AMI.

> **Note**
>
> L'activation du chiffrement par défaut a le même effet que la définition du `Encrypted` paramètre sur `true` pour tous les instantanés de l'AMI.



Définir le paramètre `Encrypted` chiffre l'instantané unique de cette instance. Si vous ne spécifiez pas le paramètre `KmsKeyId`, la clé gérée par le client par défaut est utilisée pour chiffrer la copie de l'instantané.

> **Note**
>
> Vous pouvez également copier une image avec plusieurs instantanés et configurer l'état de chiffrement de chacun individuellement.

Comprendre AMI l'utilisation partagée sur Amazon EC2

Un partage AMI est un fichier AMI créé par un développeur et mis à la disposition d'autres utilisateurs. L'un des moyens les plus simples de démarrer avec Amazon EC2 consiste à utiliser un partage AMI contenant les composants dont vous avez besoin, puis à ajouter du contenu personnalisé. Vous pouvez également créer les vôtres AMIs et les partager avec d'autres personnes.

Vous utilisez un partage AMI à vos risques et périls. Amazon ne peut garantir l'intégrité ou la sécurité des informations AMIs partagées par d'autres EC2 utilisateurs d'Amazon. Par conséquent, vous devez traiter le code partagé AMIs comme tout code étranger que vous pourriez envisager de déployer dans votre propre centre de données, et faire preuve de diligence raisonnable. Nous vous recommandons d'en obtenir une AMI auprès d'une source fiable, telle qu'un fournisseur vérifié.

Fournisseur vérifié

Dans la EC2 console Amazon, AMIs les entités publiques appartenant à Amazon ou à un partenaire Amazon vérifié sont marquées comme fournisseur vérifié.

Vous pouvez également utiliser la AWS CLI commande describe-images pour identifier le public provenant AMIs d'un fournisseur vérifié. Les images publiques détenues par Amazon ou par un propriétaire disposant d'un alias, qui est soit `amazon` soit `aws-marketplace`. Dans la CLI sortie, ces valeurs apparaissent pour`ImageOwnerAlias`. Les autres utilisateurs ne peuvent pas créer d'alias pour leurAMIs. Cela vous permet de trouver facilement des informations AMIs auprès d'Amazon ou de partenaires vérifiés.

Pour devenir un fournisseur vérifié, vous devez vous inscrire en tant que vendeur sur le AWS Marketplace. Une fois inscrit, vous pouvez inscrire votre nom AMI sur le AWS Marketplace. Pour plus d'informations, consultez la section Commencer en tant que vendeur et produits AMI dérivés dans le Guide du AWS Marketplace vendeur.

AMISujets partagés

- Rechercher un partage AMIs à utiliser pour les EC2 instances Amazon

- Préparez-vous à utiliser le partage AMIs pour Linux
- Rendez votre AMI document accessible au public pour une utilisation sur Amazon EC2
- Comprendre bloquer l'accès public pour AMIs
- AMIUtilisation partagée avec des organisations et des unités organisationnelles
- Partagez et AMI avec des AWS comptes spécifiques
- Annuler le AMI partage avec votre Compte AWS
- Recommandations pour créer un système Linux partagé AMIs

Si vous recherchez des informations sur d'autres sujets

- Pour plus d'informations sur la création d'unAMI, voir the section called "Création d'une instance sauvegardée en magasin AMI" outhe section called "Créez un AMI".
- Pour plus d'informations sur la création, la livraison et la maintenance de vos applications sur le AWS Marketplace, consultez la AWS Marketplace Documentation (Documentation de).

Rechercher un partage AMIs à utiliser pour les EC2 instances Amazon

Vous pouvez utiliser la EC2 console Amazon ou la ligne de commande pour trouver un partage public ou privé AMIs à utiliser avec vos EC2 instances Amazon.

AMIssont une ressource régionale. Lorsque vous recherchez un partage AMI (public ou privé), vous devez le rechercher dans la même région que celle à partir de laquelle il est partagé. Pour le rendre AMI disponible dans une autre région, copiez-le dans la région, puis partagez-le. AMI Pour de plus amples informations, veuillez consulter Copier un Amazon EC2 AMI.

Rechercher un partage AMI (console)

Pour rechercher un espace privé partagé AMI à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez AMIs.
3. Dans le premier filtre, choisissez Images privées. Toutes les AMIs informations qui ont été partagées avec vous sont répertoriées. Pour affiner votre recherche, cliquez dans la barre Search (Rechercher) et utilisez les options de filtre du menu.

Pour rechercher un public partagé à AMI l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez AMIs.
3. Dans le premier filtre, choisissez Images publiques. Pour affiner votre recherche, cliquez dans la barre Recherche et utilisez les options de filtre du menu.

Pour rechercher le public partagé d'Amazon à AMIs l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez AMIs.
3. Dans le premier filtre, choisissez Images publiques.
4. Cliquez sur l'onglet Recherche puis, dans les options de menu qui s'affichent, choisissez alias du propriétaire, puis=, et ensuite amazon pour afficher uniquement les images publiques d'Amazon.

Pour rechercher un public partagé AMI auprès d'un fournisseur vérifié à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez AMICatalog.
3. Choisissez Community AMIs.
4. L'étiquette Fournisseur vérifié indique AMIs qu'il provient d'Amazon ou d'un partenaire vérifié.

Trouver un partage AMI (AWS CLI)

Utilisez la commande describe-images (AWS CLI) pour créer une liste. AMIs Vous pouvez étendre la liste aux types AMIs qui vous intéressent, comme le montrent les exemples suivants.

Exemple : Répertorier tout le public AMIs

La commande suivante répertorie tous les publicsAMIs, y compris ceux AMIs que vous possédez.

```
aws ec2 describe-images --executable-users all
```

Exemple : liste AMIs avec autorisations de lancement explicites

La commande suivante répertorie celles AMIs pour lesquelles vous disposez d'autorisations de lancement explicites. Cette liste n'inclut aucun de ceux AMIs que vous possédez.

```
aws ec2 describe-images --executable-users self
```

Exemple : liste AMIs détenue par des fournisseurs vérifiés

La commande suivante répertorie les fournisseurs AMIs détenus par des fournisseurs vérifiés. Les fournisseurs publics AMIs détenus par des fournisseurs vérifiés (Amazon ou des partenaires vérifiés) ont un propriétaire alias, qui apparaît sous la forme `amazon` ou `aws-marketplace` dans le champ du compte. Cela vous permet de trouver facilement AMIs des fournisseurs vérifiés. Les autres utilisateurs ne peuvent pas créer d'alias pour leurAMIs.

```
aws ec2 describe-images \
    --owners amazon aws-marketplace \
    --query 'Images[*].[ImageId]' \
    --output text
```

Exemple : liste AMIs détenue par un compte

La commande suivante répertorie les AMIs propriétés détenues par le spécifié Compte AWS.

```
aws ec2 describe-images --owners 123456789012
```

Exemple : champ d'application AMIs à l'aide d'un filtre

Pour réduire le nombre d'affichagesAMIs, utilisez un filtre pour ne répertorier que les types AMIs qui vous intéressent. Par exemple, utilisez le filtre suivant pour afficher uniquement EBS -backedAMIs.

```
--filters "Name=root-device-type,Values=ebs"
```

Rechercher un partage AMI (Outils pour Windows PowerShell)

Utilisez la Get-EC2Imagecommande (Outils pour Windows PowerShell) pour créer une listeAMIs. Vous pouvez étendre la liste aux types AMIs qui vous intéressent, comme le montrent les exemples suivants.

Exemple : Répertorier tout le public AMIs

La commande suivante répertorie tous les publicsAMIs, y compris ceux AMIs que vous possédez.

```
PS C:\> Get-EC2Image -ExecutableUser all
```

Exemple : liste AMIs avec autorisations de lancement explicites

La commande suivante répertorie celles AMIs pour lesquelles vous disposez d'autorisations de lancement explicites. Cette liste n'inclut aucun de ceux AMIs que vous possédez.

```
PS C:\> Get-EC2Image -ExecutableUser self
```

Exemple : liste AMIs détenue par des fournisseurs vérifiés

La commande suivante répertorie les fournisseurs AMIs détenus par des fournisseurs vérifiés. Les fournisseurs publics AMIs détenus par des fournisseurs vérifiés (Amazon ou des partenaires vérifiés) ont un propriétaire alias, qui apparaît sous la forme `amazon` ou `aws-marketplace` dans le champ du compte. Cela vous permet de trouver facilement AMIs des fournisseurs vérifiés. Les autres utilisateurs ne peuvent pas créer d'alias pour leurAMIs.

```
PS C:\> Get-EC2Image -Owner amazon aws-marketplace
```

Exemple : liste AMIs détenue par un compte

La commande suivante répertorie les AMIs propriétés détenues par le spécifié Compte AWS.

```
PS C:\> Get-EC2Image -Owner 123456789012
```

Exemple : champ d'application AMIs à l'aide d'un filtre

Pour réduire le nombre d'affichagesAMIs, utilisez un filtre pour ne répertorier que les types AMIs qui vous intéressent. Par exemple, utilisez le filtre suivant pour afficher uniquement EBS -backedAMIs.

```
-Filter @{ Name="root-device-type"; Values="ebs" }
```

Préparez-vous à utiliser le partage AMIs pour Linux

Avant d'utiliser une instance partagée AMI pour Linux, suivez les étapes ci-dessous pour vérifier qu'aucune information d'identification préinstallée ne permet à un tiers d'accéder à votre instance de manière indésirable et qu'aucune journalisation à distance préconfigurée ne permet de transmettre des données sensibles à un tiers. Consultez la documentation de la distribution Linux utilisée par le AMI pour obtenir des informations sur l'amélioration de la sécurité du système.

Pour éviter de perdre accidentellement l'accès à votre instance, nous vous recommandons de lancer deux SSH sessions et de laisser la seconde ouverte jusqu'à ce que vous supprimiez les informations d'identification que vous ne reconnaissez pas et que vous confirmiez que vous pouvez toujours vous connecter à votre instanceSSH.

1. Identifiez et désactivez toutes les SSH clés publiques non autorisées. La seule clé du fichier doit être celle que vous avez utilisée pour lancer leAMI. La commande suivante localise les fichiers `authorized_keys` :

   ```
   [ec2-user ~]$ sudo find / -name "authorized_keys" -print -exec cat {} \;
   ```

2. Désactivez l'authentification basée sur mot de passe pour l'utilisateur racine. Ouvrez le fichier `sshd_config` et éditez la ligne `PermitRootLogin` de la façon suivante :

   ```
   PermitRootLogin without-password
   ```

   L'alternative est de désactiver la possibilité de se connecter à l'instance en tant qu'utilisateur racine :

   ```
   PermitRootLogin No
   ```

   Redémarrez le service sshd.

3. Vérifiez si d'autres utilisateurs peuvent se connecter à votre instance. Les utilisateurs disposant de privilèges de superutilisateur sont particulièrement dangereux. Supprimez ou verrouillez le mot de passe de tout compte inconnu.
4. Vérifiez s'il y a des ports ouverts que vous n'utilisez pas et des services de réseau en cours d'exécution en attente de connexions entrantes.
5. Pour empêcher la journalisation à distance préconfigurée, vous devez supprimer le fichier de configuration existant et redémarrer le service `rsyslog`. Par exemple :

   ```
   [ec2-user ~]$ sudo rm /etc/rsyslog.conf
   [ec2-user ~]$ sudo service rsyslog restart
   ```

6. Vérifiez que toutes les tâches cron sont légitimes.

Si vous découvrez un public AMI qui, selon vous, présente un risque de sécurité, contactez l'équipe AWS de sécurité. Pour plus d'informations, consultez le Centre de sécuritéAWS.

Rendez votre AMI document accessible au public pour une utilisation sur Amazon EC2

Vous pouvez rendre votre document AMI accessible au public en le partageant avec tout le monde Comptes AWS.

Si vous souhaitez empêcher le partage public de votreAMIs, vous pouvez activer le blocage de l'accès public pour AMIs. Cela bloque toute tentative de AMI publication, contribuant ainsi à empêcher tout accès non autorisé et toute utilisation abusive potentielle des AMI données. Notez que l'activation du blocage de l'accès public n'affecte pas AMIs ceux qui sont déjà accessibles au public ; ils restent accessibles au public. Pour de plus amples informations, veuillez consulter Comprendre bloquer l'accès public pour AMIs.

Pour autoriser uniquement des comptes spécifiques à utiliser votre compte AMI pour lancer des instances, consultezPartagez et AMI avec des AWS comptes spécifiques.

Table des matières

Considérations

Tenez compte des points suivants avant de rendre une AMI publication publique.

- Propriété — Pour rendre un AMI public, vous Compte AWS devez posséder leAMI.
- Région — AMIs sont une ressource régionale. Lorsque vous partagez unAMI, il n'est disponible que dans la région à partir de laquelle vous l'avez partagé. Pour le rendre AMI disponible dans une autre région, copiez-le dans la région, puis partagez-le. AMI Pour de plus amples informations, veuillez consulter Copier un Amazon EC2 AMI.
- Bloquer l'accès public — Pour partager publiquement unAMI, le blocage de l'accès public AMIs doit être désactivé dans chaque région dans laquelle il AMI sera partagé publiquement. Après avoir partagé publiquement leAMI, vous pouvez réactiver le blocage de l'accès public AMIs pour empêcher tout partage public ultérieur de votreAMIs.
- Certains ne AMIs peuvent pas être rendus publics — Si vous AMI incluez l'un des composants suivants, vous ne pouvez pas le rendre public (mais vous pouvez le partager AMI avec des personnes spécifiques Comptes AWS) :

  - Volumes chiffrés
  - Instantanés de volumes chiffrés
  - Codes produits
- Évitez d'exposer des données sensibles : pour éviter d'exposer des données sensibles lorsque vous partagez unAMI, lisez les considérations de sécurité Recommandations pour créer un système Linux partagé AMIs et suivez les actions recommandées.
- Utilisation — Lorsque vous partagez unAMI, les utilisateurs ne peuvent lancer des instances qu'à partir duAMI. Ils ne peuvent pas la supprimer, la partager ou la modifier. Cependant, une fois qu'ils ont lancé une instance à l'aide de votre instanceAMI, ils peuvent en créer une AMI à partir de l'instance qu'ils ont lancée.
- Obsolation automatique — Par défaut, la date d'obsolescence de tous les publics AMIs est fixée à deux ans à compter de la date de création. AMI Vous pouvez définir la date d'obsolescence à moins de deux ans. Pour annuler la date de dépréciation ou pour la déplacer à une date ultérieure, vous devez la rendre AMI privée en la partageant uniquement avec des personnes spécifiques. Comptes AWS
- Supprimer les éléments obsolètes AMIs : une fois qu'un public a AMI atteint sa date d'obsolescence, si aucune nouvelle instance n'a été lancée AMI depuis au moins six mois, la propriété de partage publique est AWS finalement supprimée afin que les entités obsolètes AMIs n'apparaissent pas dans les listes publiquesAMI.
- Facturation — Vous n'êtes pas facturé lorsque le vôtre AMI est utilisé par d'autres Comptes AWS pour lancer des instances. Les comptes qui lancent des instances à l'aide du AMI sont facturés pour les instances qu'ils lancent.

Partager et AMI avec tous les AWS comptes (partager publiquement)

Une fois que vous l'avez rendu AMI public, il est disponible dans Communauté AMIs dans la console, à laquelle vous pouvez accéder depuis le AMIcatalogue dans le navigateur de gauche de la EC2 console ou lorsque vous lancez une instance à l'aide de la console. Notez qu'une AMIs fois que vous l'avez rendue publique, son apparition dans la communauté peut prendre un AMI certain temps.

Console

Pour rendre AMI public

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez AMIs.

3. Sélectionnez votre dans AMI la liste, puis choisissez Actions, Modifier AMI les autorisations.
4. Dans AMIla section Disponibilité, sélectionnez Public.
5. Sélectionnez Enregistrer les modifications.

AWS CLI

Chacun AMI possède une `launchPermission` propriété qui contrôle qui Comptes AWS, outre celle du propriétaire, est autorisé à l'utiliser AMI pour lancer des instances. En modifiant la `launchPermission` propriété d'unAMI, vous pouvez le rendre AMI public (ce qui accorde des autorisations de lancement à tous Comptes AWS) ou le partager uniquement avec les personnes Comptes AWS que vous spécifiez.

Vous pouvez ajouter ou supprimer un compte IDs de la liste des comptes disposant d'autorisations de lancement pour unAMI. Pour rendre le AMI public, spécifiez le `all` groupe. Vous pouvez spécifier à la fois des autorisations de lancement publiques et explicites.

Pour rendre AMI public

1. Utilisez la modify-image-attributecommande suivante pour ajouter le `all` groupe à la `launchPermission` liste pour le groupe spécifiéAMI.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Add=[{Group=all}]"
```

2. Pour vérifier les autorisations de lancement duAMI, utilisez la describe-image-attributecommande.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

3. (Facultatif) Pour rendre le groupe à nouveau AMI privé, supprimez les autorisations de lancement du `all` groupe. Notez que le propriétaire du dispose AMI toujours des autorisations de lancement et n'est donc pas affecté par cette commande.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Remove=[{Group=all}]"
```

PowerShell

Chacun AMI possède une `launchPermission` propriété qui contrôle qui Comptes AWS, outre celle du propriétaire, est autorisé à l'utiliser AMI pour lancer des instances. En modifiant la `launchPermission` propriété d'unAMI, vous pouvez le rendre AMI public (ce qui accorde des autorisations de lancement à tous Comptes AWS) ou le partager uniquement avec les personnes Comptes AWS que vous spécifiez.

Vous pouvez ajouter ou supprimer un compte IDs de la liste des comptes disposant d'autorisations de lancement pour unAMI. Pour rendre le AMI public, spécifiez le `all` groupe. Vous pouvez spécifier à la fois des autorisations de lancement publiques et explicites.

Pour rendre AMI public

1. Utilisez la Edit-EC2ImageAttributecommande suivante pour ajouter le `all` groupe à la `launchPermission` liste pour le groupe spécifiéAMI.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType add -UserGroup all
```

2. Pour vérifier les autorisations de lancement duAMI, utilisez la Get-EC2ImageAttributecommande suivante.

```
PS C:\> Get-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission
```

3. (Facultatif) Pour rendre le groupe à nouveau AMI privé, supprimez les autorisations de lancement du `all` groupe. Notez que le propriétaire du dispose AMI toujours des autorisations de lancement et n'est donc pas affecté par cette commande.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType remove -UserGroup all
```

Comprendre bloquer l'accès public pour AMIs

Pour empêcher le partage public de votreAMIs, vous pouvez activer le blocage de l'accès public pour AMIs. Ce paramètre est activé au niveau du compte, mais vous devez l'activer dans chaque compte Région AWS dans lequel vous souhaitez empêcher le partage public de votreAMIs.

Lorsque le blocage de l'accès public est activé, toute tentative de rendre un accès AMI public est automatiquement bloquée. Toutefois, si vous en avez déjà unAMIs, il reste accessible au public.

Pour partager publiquementAMIs, vous devez désactiver le blocage de l'accès public. Lorsque vous avez terminé de partager, il est recommandé de réactiver le blocage de l'accès public afin d'empêcher tout partage public involontaire de votre compte. AMIs

Vous pouvez restreindre IAM les autorisations accordées à un utilisateur administrateur afin qu'il soit le seul à pouvoir activer ou désactiver le blocage de l'accès public pourAMIs.

Rubriques

Paramètres par défaut

Le AMIs paramètre Bloquer l'accès public est activé ou désactivé par défaut selon que votre compte est nouveau ou existant, et si vous êtes publicAMIs. Le tableau suivant répertorie les paramètres par défaut :

AWS compte	Bloquer l'accès public pour le paramètre AMIs par défaut
Nouveaux comptes	Activées
Comptes existants qui ne sont pas publics AMIs [1]	Activées
Comptes existants avec un ou plusieurs comptes publics AMIs	Désactivées

[1] Si un ou plusieurs comptes étaient publics AMIs le 15 juillet 2023 ou après cette date, le blocage de l'accès public AMIs est désactivé par défaut pour votre compte, même si vous les avez ensuite tous rendus AMIs privés.

Gérez le paramètre de blocage de l'accès public pour AMIs

Vous pouvez gérer le paramètre de blocage de l'accès public AMIs afin de contrôler s'ils peuvent être partagés publiquement. Vous pouvez activer, désactiver ou consulter l'état actuel de blocage de l'accès public pour vous à AMIs l'aide de la EC2 console Amazon ou du AWS CLI.

Afficher l'état du blocage de l'accès public pour AMIs

Pour savoir si le partage public de votre compte AMIs est bloqué, vous pouvez consulter l'état du blocage de l'accès public pourAMIs. Vous devez consulter l'état Région AWS dans lequel vous souhaitez voir si le partage public de votre compte AMIs est bloqué.

Autorisations nécessaires

Pour obtenir le paramètre actuel de blocage de l'accès public pourAMIs, vous devez avoir l'`GetImageBlockPublicAccessState`IAMautorisation.

Console

Pour afficher l'état du blocage de l'accès public AMIs dans la région spécifiée

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation (en haut de l'écran), sélectionnez la région pour laquelle vous souhaitez afficher l'état du blocage de l'accès publicAMIs.
3. Si le tableau de bord n'est pas affiché, dans le volet de navigation, sélectionnez EC2Tableau de bord.
4. Sous Attributs du compte, sélectionnez Protection et sécurité des données.
5. Sous Bloquer l'accès public pour AMIs, cochez le champ Accès public. La valeur est Nouveau partage public bloqué ou Nouveau partage public autorisé.

AWS CLI

Pour obtenir l'état de blocage de l'accès public pour AMIs

Utilisez la commande get-image-block-public-access-state.

- Pour une région spécifique

```
aws ec2 get-image-block-public-access-state --region us-east-1
```

Sortie attendue : la valeur est `block-new-sharing` ou `unblocked`.

```
{
    "ImageBlockPublicAccessState": "block-new-sharing"
}
```

- Pour toutes les régions de votre compte

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 get-image-block-public-access-state \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Sortie attendue : la valeur est `block-new-sharing` ou `unblocked`.

```
Region           Public Access State
--------------   ----------------------
ap-south-1       block-new-sharing
eu-north-1       unblocked
eu-west-3        block-new-sharing
...
```

PowerShell

Pour obtenir l'état de blocage de l'accès public pour AMIs

Utilisez l'Get-EC2ImageBlockPublicAccessStateapplet de commande.

- Pour une région spécifique

```
Get-EC2ImageBlockPublicAccessState -Region us-east-1
```

Sortie attendue

```
block-new-sharing
```

- Pour toutes les régions de votre compte

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
        [PSCustomObject]@{
            Region   = $_
            PublicAccessState = (Get-EC2ImageBlockPublicAccessState -Region $_)
        }
} | `
Format-Table -AutoSize
```

Sortie attendue

```
Region         PublicAccessState
------         -----------------
ap-south-1     block-new-sharing
eu-north-1     block-new-sharing
eu-west-3      block-new-sharing
…
```

Activer le blocage de l'accès public pour AMIs

Pour empêcher le partage public de votre compteAMIs, activez le blocage de l'accès public AMIs au niveau du compte. Vous devez activer le blocage de l'accès public pour AMIs chaque élément Région AWS dans lequel vous souhaitez empêcher le partage public de votreAMIs. Si vous en avez déjà unAMIs, il restera accessible au public.

Autorisations nécessaires

Pour activer le paramètre de blocage de l'accès public pourAMIs, vous devez disposer de l'`EnableImageBlockPublicAccess`IAMautorisation.

Console

Pour activer le blocage de l'accès public AMIs dans la région spécifiée

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation (en haut de l'écran), sélectionnez la région pour laquelle vous souhaitez activer le blocage de l'accès publicAMIs.
3. Si le tableau de bord n'est pas affiché, dans le volet de navigation, sélectionnez EC2Tableau de bord.
4. Sous Attributs du compte, sélectionnez Protection et sécurité des données.
5. Sous Bloquer l'accès public pour AMIs, choisissez Gérer.
6. Cochez la case Bloquer le partage public, puis sélectionnez Mettre à jour.

> **Note**
>
> La configuration de ce paramètre API peut prendre jusqu'à 10 minutes. Pendant ce temps, la valeur est Nouveau partage public autorisé. Lorsque la configuration API est terminée, la valeur passe automatiquement à Nouveau partage public bloqué.

AWS CLI

Pour activer le blocage de l'accès public pour AMIs

Utilisez la commande enable-image-block-public-access.

- Pour une région spécifique

```
aws ec2 enable-image-block-public-access \
--region us-east-1 \
--image-block-public-access-state block-new-sharing
```

Sortie attendue

```
{
    "ImageBlockPublicAccessState": "block-new-sharing"
}
```

- Pour toutes les régions de votre compte

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 enable-image-block-public-access \
            --region $region \
            --image-block-public-access-state block-new-sharing \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Sortie attendue

```
Region           Public Access State
--------------   ----------------------
ap-south-1       block-new-sharing
eu-north-1       block-new-sharing
eu-west-3        block-new-sharing
...
```

> **Note**
>
> La configuration de ce paramètre API peut prendre jusqu'à 10 minutes. Pendant ce temps, si vous exécutez la commande get-image-block-public-access-state, la réponse sera. `unblocked` Une fois la configuration API terminée, la réponse sera`block-new-sharing`.

PowerShell

Pour activer le blocage de l'accès public pour AMIs

Utilisez la Enable-EC2ImageBlockPublicAccesscommande.

- Pour une région spécifique

```
Enable-EC2ImageBlockPublicAccess `
    -Region us-east-1 `
    -ImageBlockPublicAccessState block-new-sharing
```

Sortie attendue

```
Value
-----
block-new-sharing
```

- Pour toutes les régions de votre compte

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (
        Enable-EC2ImageBlockPublicAccess `
         -Region $_ `
         -ImageBlockPublicAccessState block-new-sharing)
    }
} | `
Format-Table -AutoSize
```

Sortie attendue

```
Region         PublicAccessState
------         -----------------
ap-south-1     block-new-sharing
eu-north-1     block-new-sharing
eu-west-3      block-new-sharing
…
```

Désactiver le blocage de l'accès public pour AMIs

Pour permettre aux utilisateurs de votre compte de le partager publiquementAMIs, désactivez le blocage de l'accès public au niveau du compte. Vous devez désactiver le blocage de l'accès public

pour AMIs chaque élément Région AWS dans lequel vous souhaitez autoriser le partage public de votreAMIs.

Autorisations nécessaires

Pour désactiver le paramètre de blocage de l'accès public pourAMIs, vous devez avoir l'`DisableImageBlockPublicAccess`IAMautorisation.

Console

Pour désactiver le blocage de l'accès public AMIs dans la région spécifiée

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation (en haut de l'écran), sélectionnez la région pour laquelle vous souhaitez désactiver le blocage de l'accès publicAMIs.
3. Si le tableau de bord n'est pas affiché, dans le volet de navigation, sélectionnez EC2Tableau de bord.
4. Sous Attributs du compte, sélectionnez Protection et sécurité des données.
5. Sous Bloquer l'accès public pour AMIs, choisissez Gérer.
6. Décochez la case Bloquer le partage public, puis sélectionnez Mettre à jour.
7. Saisissez **`confirm`** lorsque vous êtes invité à confirmer, puis choisissez Autoriser le partage public.

> **Note**
>
> La configuration de ce paramètre API peut prendre jusqu'à 10 minutes. Pendant ce temps, la valeur est Nouveau partage public bloqué. Lorsque la configuration API est terminée, la valeur passe automatiquement à Nouveau partage public autorisé.

AWS CLI

Pour désactiver le blocage de l'accès public pour AMIs

Utilisez la commande disable-image-block-public-access.

- Pour une région spécifique

```
aws ec2 disable-image-block-public-access --region us-east-1
```

Sortie attendue

```
{
   "ImageBlockPublicAccessState": "unblocked"
}
```

- Pour toutes les régions de votre compte

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 disable-image-block-public-access \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Sortie attendue

```
Region           Public Access State
--------------   ----------------------
ap-south-1       unblocked
eu-north-1       unblocked
eu-west-3        unblocked
...
```

> **Note**
>
> La configuration de ce paramètre API peut prendre jusqu'à 10 minutes. Pendant ce temps, si vous exécutez la commande get-image-block-public-access-state, la

réponse sera. `block-new-sharing` Une fois la configuration API terminée, la réponse seraunblocked.

PowerShell

Pour désactiver le blocage de l'accès public pour AMIs

Utilisez l'Disable-EC2ImageBlockPublicAccessapplet de commande.

- Pour une région spécifique

```
Disable-EC2ImageBlockPublicAccess -Region us-east-1
```

Sortie attendue

```
Value
-----
unblocked
```

- Pour toutes les régions de votre compte

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (Disable-EC2ImageBlockPublicAccess -Region $_)
    }
} | `
Format-Table -AutoSize
```

Sortie attendue

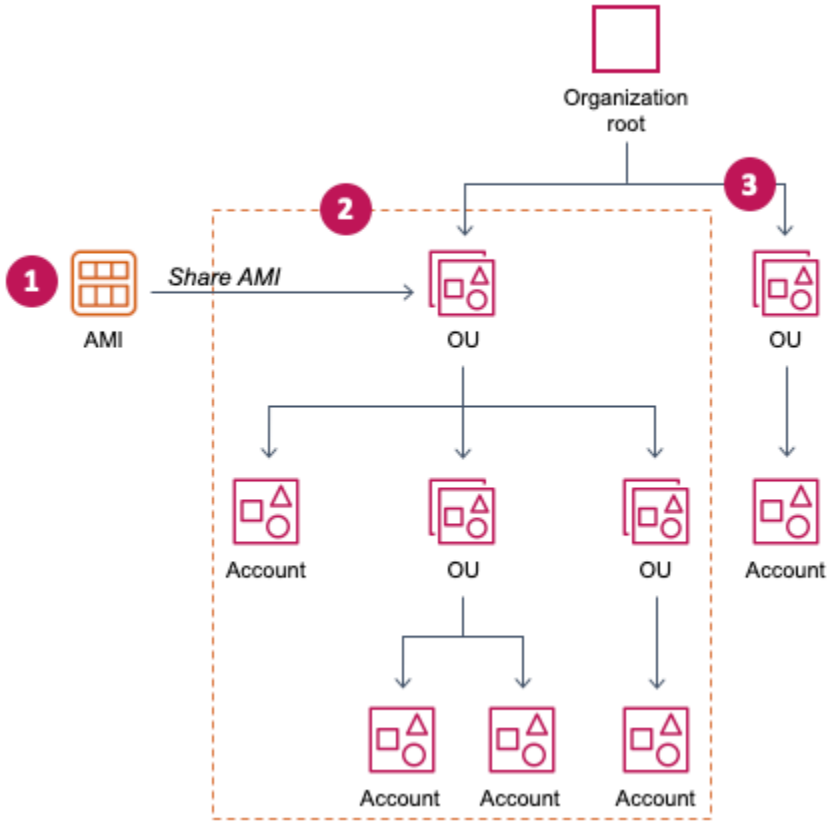
```
Region         PublicAccessState
------         -----------------
ap-south-1     unblocked
eu-north-1     unblocked
eu-west-3      unblocked
…
```

AMIUtilisation partagée avec des organisations et des unités organisationnelles

AWS Organizationsest un service de gestion de comptes qui vous permet de consolider plusieurs comptes au Comptes AWS sein d'une organisation que vous créez et gérez de manière centralisée. Vous pouvez partager un AMI avec une organisation ou une unité organisationnelle (UO) que vous avez créée, en plus de le partager avec des comptes spécifiques.

L'organisation est une entité que vous créez pour consolider et gérer vos Comptes AWS de manière centralisée. Vous pouvez organiser les comptes dans une structure arborescente hiérarchique, avec une racine au sommet et des unités organisationnelles imbriquées sous la racine de l'organisation. Chaque compte peut être ajouté directement à la racine ou placé dans l'un des comptes de la hiérarchie. OUs Pour en savoir plus, consultez la section Terminologie et concepts relatifs àAWS Organizations du Guide de l'utilisateur AWS Organizations .

Lorsque vous partagez un AMI avec une organisation ou une unité d'organisation, tous les comptes enfants ont accès auAMI. Par exemple, dans le schéma suivant, le AMI est partagé avec une unité d'organisation de niveau supérieur (indiquée par la flèche au numéro 1). Tous les comptes OUs et qui sont imbriqués sous cette unité d'organisation de premier niveau (indiqués par la ligne pointillée au numéro 2) ont également accès au. AMI Les comptes de l'organisation et de l'unité d'organisation situés en dehors de la ligne pointillée (indiqués par le chiffre 3) n'y ont pas accès AMI car ils ne sont pas des enfants de l'unité d'organisation avec laquelle ils AMI sont partagés.



Rubriques

- Obtenez le nom ARN d'une organisation ou d'une unité organisationnelle
- Considérations
- Autoriser les organisations et OUs utiliser une KMS clé
- Gérer AMI le partage avec une organisation ou une unité d'organisation

Obtenez le nom ARN d'une organisation ou d'une unité organisationnelle

L'organisation et l'unité organisationnelle ARNs contiennent le numéro de compte de gestion à 12 chiffres. Si vous ne connaissez pas le numéro de compte de gestion, vous pouvez décrire l'organisation et l'unité organisationnelle ARN pour obtenir le numéro correspondant à chacune d'entre elles. Dans les exemples suivants, `123456789012` est le numéro du compte de gestion.

Avant de pouvoir obtenir leARNs, vous devez être autorisé à décrire les organisations et les unités organisationnelles. La politique suivante fournit l'autorisation nécessaire.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour obtenir le nom ARN d'une organisation

Utilisez la describe-organizationcommande et le `--query` paramètre définis sur `'Organization.Arn'` pour renvoyer uniquement l'organisationARN.

```
aws organizations describe-organization --query 'Organization.Arn'
```

Exemple de réponse

```
"arn:aws:organizations::123456789012:organization/o-123example"
```

Pour obtenir le ARN nom d'une unité organisationnelle

Utilisez la describe-organizational-unitcommande, spécifiez l'ID de l'unité organisationnelle et définissez le `--query` paramètre `'OrganizationalUnit.Arn'` sur pour renvoyer uniquement l'unité organisationnelleARN.

```
aws organizations describe-organizational-unit --organizational-unit-
id ou-1234-5example --query 'OrganizationalUnit.Arn'
```

Exemple de réponse

```
"arn:aws:organizations::123456789012:ou/o-123example/ou-1234-5example"
```

Considérations

Tenez compte des points suivants lors du partage AMIs avec des organisations ou unités organisationnelles spécifiques.

- Propriété — Pour partager unAMI, vous Compte AWS devez posséder leAMI.

- Limites de partage : le AMI propriétaire peut partager un AMI avec n'importe quelle organisation ou unité d'organisation, y compris OUs les organisations dont il n'est pas membre.

  Pour connaître le nombre maximum d'entités avec lesquelles un identifiant AMI peut être partagé au sein d'une région, consultez les quotas EC2 de service Amazon.

- Balises : vous ne pouvez pas partager de balises définies par l'utilisateur (balises que vous attachez à unAMI). Lorsque vous partagez unAMI, vos tags définis par l'utilisateur ne sont accessibles Compte AWS à aucun membre d'une organisation ou d'une unité d'organisation avec laquelle ils AMI sont partagés.

- ARNformat — Lorsque vous spécifiez une organisation ou une unité d'organisation dans une commande, assurez-vous d'utiliser le ARN format correct. Vous obtiendrez une erreur si vous spécifiez uniquement l'ID, par exemple si vous spécifiez uniquement `o-123example` ou `ou-1234-5example`.

  ARNFormats corrects :

  - Organisation ARN : `arn:aws:organizations::`*`account-id`*`:organization/`*`organization-id`*
  - OU ARN : `arn:aws:organizations::`*`account-id`*`:ou/`*`organization-id`*`/`*`ou-id`*

  Où :

  - *`id-compte`* est le numéro de compte de gestion à 12 chiffres, par exemple,`123456789012`. Si vous ne connaissez pas le numéro de compte de gestion, vous pouvez décrire l'organisation ou l'unité organisationnelle qui l'obtientARN, y compris le numéro de compte de gestion. Pour de plus amples informations, veuillez consulter Obtenez le nom ARN d'une organisation ou d'une unité organisationnelle.
  - *`identifiant de l'organisation`* est l'identifiant de l'organisation, par exemple`o-123example`.
  - *`ou-id`* est l'ID de l'unité organisationnelle, par exemple,`ou-1234-5example`.

  Pour plus d'informations sur le format deARNs, consultez Amazon Resource Names (ARNs) dans le guide de IAM l'utilisateur.

- Chiffrement et clés : vous pouvez partager des AMIs données soutenues par des instantanés chiffrés et non chiffrés.

  - Les instantanés chiffrés doivent être chiffrés avec une clé gérée par le client. Vous ne pouvez pas partager ceux AMIs qui sont sauvegardés par des instantanés chiffrés à l'aide de la clé AWS gérée par défaut.

  - Si vous partagez un fichier AMI basé sur des instantanés chiffrés, vous devez autoriser les organisations OUs à utiliser les clés gérées par le client qui ont été utilisées pour chiffrer les instantanés. Pour de plus amples informations, veuillez consulter Autoriser les organisations et OUs utiliser une KMS clé.
- Région — AMIs sont une ressource régionale. Lorsque vous partagez unAMI, il n'est disponible que dans la région à partir de laquelle vous l'avez partagé. Pour le rendre AMI disponible dans une autre région, copiez-le dans la région, puis partagez-le. AMI Pour de plus amples informations, veuillez consulter Copier un Amazon EC2 AMI.
- Utilisation — Lorsque vous partagez unAMI, les utilisateurs ne peuvent lancer des instances qu'à partir duAMI. Ils ne peuvent pas la supprimer, la partager ou la modifier. Cependant, une fois qu'ils ont lancé une instance à l'aide de votre instanceAMI, ils peuvent en créer une AMI à partir de l'instance qu'ils ont lancée.
- Facturation — Vous n'êtes pas facturé lorsque le vôtre AMI est utilisé par d'autres Comptes AWS pour lancer des instances. Les comptes qui lancent des instances à l'aide du AMI sont facturés pour les instances qu'ils lancent.

Autoriser les organisations et OUs utiliser une KMS clé

Si vous partagez un AMI fichier basé sur des instantanés chiffrés, vous devez également autoriser les organisations OUs à utiliser ceux AWS KMS keys qui ont été utilisés pour chiffrer les instantanés.

Utilisez les `aws:PrincipalOrgPaths` touches `aws:PrincipalOrgID` et pour comparer le AWS Organizations chemin du principal qui fait la demande avec le chemin indiqué dans la politique. Ce principal peut être un utilisateur, un IAM rôle, un utilisateur fédéré ou un utilisateur Compte AWS root. Dans une politique, cette clé de condition garantit que le demandeur est membre du compte au sein de la racine ou OUs de l'organisation spécifiée. AWS Organizations Pour d'autres exemples d'énoncés de condition, consultez aws:PrincipalOrgIDet aws:PrincipalOrgPathsdans le Guide de IAM l'utilisateur.

Pour plus d'informations sur la modification d'une politique relative aux clés, voir Autoriser les utilisateurs d'autres comptes à utiliser une KMS clé dans le Guide du AWS Key Management Service développeur.

Pour autoriser une organisation ou une unité d'organisation à utiliser une KMS clé, ajoutez la déclaration suivante à la politique des clés.

```
{
```

```
    "Sid": "Allow access for organization root",
    "Effect": "Allow",
    "Principal": "*",
    "Action": [
        "kms:Describe*",
        "kms:List*",
        "kms:Get*",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "o-123example"
        }
    }
}
```

Pour partager une KMS clé avec plusieursOUs, vous pouvez utiliser une politique similaire à l'exemple suivant.

```
{
        "Sid": "Allow access for specific OUs and their descendants",
        "Effect": "Allow",
        "Principal": "*",
        "Action": [
            "kms:Describe*",
            "kms:List*",
            "kms:Get*",
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:ReEncrypt*",
            "kms:GenerateDataKey*"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:PrincipalOrgID": "o-123example"
            },
            "ForAnyValue:StringLike": {
                "aws:PrincipalOrgPaths": [
```

```
                    "o-123example/r-ab12/ou-ab12-33333333/*",
                    "o-123example/r-ab12/ou-ab12-22222222/*"
                ]
            }
        }
}
```

Gérer AMI le partage avec une organisation ou une unité d'organisation

Afficher les organisations et les organisations OUs avec lesquelles un AMI est partagé

Vous pouvez utiliser la EC2 console Amazon ou le AWS CLI pour vérifier avec quelles organisations OUs vous avez partagé le vôtreAMI.

Afficher les organisations OUs avec lesquelles un AMI est partagé (console)

Pour vérifier avec quelles organisations et OUs vous avez partagé votre AMI utilisation de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez AMIs.
3. Sélectionnez votre AMI dans la liste, cliquez sur l'onglet Autorisations et faites défiler l'écran vers le bas jusqu'à Organisations OUs partagées/.

   Pour découvrir AMIs ceux qui sont partagés avec vous, consultezRechercher un partage AMIs à utiliser pour les EC2 instances Amazon.

Afficher les organisations et OUs avec lesquelles un AMI est partagé (AWS CLI)

Vous pouvez vérifier AMI avec quelles organisations OUs vous avez partagé le vôtre en utilisant la describe-image-attributecommande (AWS CLI) et l'`launchPermission`attribut.

Pour vérifier avec quelles organisations et OUs vous avez partagé votre AMI utilisation du AWS CLI

La describe-image-attributecommande décrit l'`launchPermission`attribut du paramètre spécifié AMI et renvoie les organisations OUs avec lesquelles vous avez partagé leAMI.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

Exemple de réponse

```
{
    "ImageId": "ami-0abcdef1234567890",
    "LaunchPermissions": [
        {
            "OrganizationalUnitArn": "arn:aws:organizations::111122223333:ou/
o-123example/ou-1234-5example"
        }
    ]
}
```

Partager et AMI avec une organisation ou une unité d'organisation

Vous pouvez utiliser la EC2 console Amazon ou le AWS CLI pour partager un AMI avec une organisation ou une unité d'organisation.

Partager une AMI (console)

Pour partager un AMI avec une organisation ou une unité d'organisation à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez AMIs.
3. Sélectionnez votre AMI dans la liste, puis choisissez Actions, Modifier AMI les autorisations.
4. Dans AMIla liste des disponibilités, sélectionnez Privé.
5. À côté de Organisations partagées/ OUs, choisissez Ajouter une organisation/unité d'organisation. ARN
6. Dans Organisation/unité d'organisationARN, entrez l'organisation ARN ou l'unité d'organisation ARN avec laquelle vous souhaitez partagerAMI, puis choisissez Partager. AMI Notez que vous devez spécifier l'identifiant completARN, et pas uniquement l'identifiant.

   Pour le partager AMI avec plusieurs organisationsOUs, répétez cette étape jusqu'à ce que vous ayez ajouté toutes les organisations requises ouOUs.

   > **Note**
   >
   > Vous n'avez pas besoin de partager les EBS instantanés Amazon auxquels un AMI utilisateur fait référence pour partager leAMI. Seul le AMI fichier lui-même doit être partagé, et le système fournit automatiquement à l'instance l'accès aux EBS instantanés Amazon référencés pour le lancement. Cependant, vous devez partager les KMS clés

utilisées pour chiffrer les instantanés auxquels il fait référence. AMI Pour de plus amples informations, veuillez consulter Autoriser les organisations et OUs utiliser une KMS clé.

7. Lorsque vous avez terminé, sélectionnez Save Changes (Enregistrer les modifications).
8. (Facultatif) Pour afficher les organisations ou OUs avec lesquelles vous les avez partagéesAMI, sélectionnez-les AMI dans la liste, choisissez l'onglet Autorisations et faites défiler l'écran vers le bas jusqu'à Organisations OUs partagées/. Pour découvrir AMIs ceux qui sont partagés avec vous, consultezRechercher un partage AMIs à utiliser pour les EC2 instances Amazon.

Partagez un AMI (1 AWS CLI)

Utilisez la modify-image-attributecommande (AWS CLI) pour partager unAMI.

Pour partager un fichier AMI avec une organisation à l'aide du AWS CLI

La modify-image-attributecommande accorde des autorisations de lancement pour l'organisation spécifiée AMI à l'organisation spécifiée. Notez que vous devez spécifier l'identifiant completARN, et pas uniquement l'identifiant.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Add=[{OrganizationArn=arn:aws:organizations::123456789012:organization/
o-123example}]"
```

Pour partager un AMI avec une UO à l'aide du AWS CLI

La modify-image-attributecommande accorde des autorisations de lancement pour l'unité d'organisation spécifiée AMI à l'unité d'organisation spécifiée. Notez que vous devez spécifier l'identifiant completARN, et pas uniquement l'identifiant.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Add=[{OrganizationalUnitArn=arn:aws:organizations::123456789012:ou/o-123example/
ou-1234-5example}]"
```

> **Note**
>
> Vous n'avez pas besoin de partager les EBS instantanés Amazon auxquels un AMI utilisateur fait référence pour partager leAMI. Seul le AMI fichier lui-même doit être partagé, et le système fournit automatiquement à l'instance l'accès aux EBS instantanés Amazon référencés pour le lancement. Cependant, vous devez partager les KMS clés utilisées pour chiffrer les instantanés auxquels il fait référence. AMI Pour de plus amples informations, veuillez consulter Autoriser les organisations et OUs utiliser une KMS clé.

Partager un AMI (Outils pour Windows PowerShell)

Utilisez la Edit-EC2ImageAttributecommande (Outils pour Windows PowerShell) pour partager un AMI comme indiqué dans les exemples suivants.

Pour partager un AMI avec une organisation ou une UO

La commande suivante accorde des autorisations de lancement pour l'organisation spécifiée AMI à l'organisation spécifiée.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -
Attribute launchPermission -OperationType add -OrganizationArn
 "arn:aws:organizations::123456789012:organization/o-123example"
```

> **Note**
>
> Vous n'avez pas besoin de partager les EBS instantanés Amazon auxquels un AMI utilisateur fait référence pour partager leAMI. Seul le AMI fichier lui-même doit être partagé, et le système fournit automatiquement à l'instance l'accès aux EBS instantanés Amazon référencés pour le lancement. Cependant, vous devez partager les KMS clés utilisées pour chiffrer les instantanés auxquels il fait référence. AMI Pour de plus amples informations, veuillez consulter Autoriser les organisations et OUs utiliser une KMS clé.

Pour arrêter de partager un fichier AMI avec une organisation ou une unité d'organisation

La commande suivante supprime les autorisations AMI de lancement pour l'organisation spécifiée :

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -
Attribute launchPermission -OperationType remove -OrganizationArn
 "arn:aws:organizations::123456789012:organization/o-123example"
```

Pour arrêter de partager une AMI annonce avec toutes les organisationsOUs, et Comptes AWS

La commande suivante supprime toutes les autorisations de lancement publiques et explicites de celles spécifiéesAMI. Notez que le propriétaire du dispose AMI toujours des autorisations de lancement et n'est donc pas affecté par cette commande.

```
PS C:\> Reset-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission
```

Arrêter de partager une annonce AMI avec une organisation ou une unité d'organisation

Vous pouvez utiliser la EC2 console Amazon ou le AWS CLI pour arrêter de partager un AMI avec une organisation ou une unité d'organisation.

Arrêter de partager une AMI (console)

Pour arrêter de partager un AMI avec une organisation ou une unité d'organisation à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez AMIs.
3. Sélectionnez votre AMI dans la liste, puis choisissez Actions, Modifier AMI les autorisations.
4. Sous Organisations partagées/ OUs, sélectionnez les organisations ou OUs avec lesquelles vous souhaitez arrêter de partager lesAMI, puis choisissez Supprimer la sélection.
5. Lorsque vous avez terminé, sélectionnez Save Changes (Enregistrer les modifications).
6. (Facultatif) Pour confirmer que vous avez arrêté de partager le AMI avec les organisations ou sélectionnez-les AMI dans la listeOUs, choisissez l'onglet Autorisations et faites défiler la page vers le bas jusqu'à Organisations OUs partagées/.

Arrêtez de partager un AMI (AWS CLI)

Utilisez les reset-image-attributecommandes modify-image-attributeou (AWS CLI) pour arrêter de partager unAMI.

Pour arrêter de partager un fichier AMI avec une organisation ou une unité d'organisation à l'aide du AWS CLI

La modify-image-attributecommande supprime les autorisations AMI de lancement pour l'organisation spécifiée. Notez que vous devez spécifier leARN.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Remove=[{OrganizationArn=arn:aws:organizations::123456789012:organization/
o-123example}]"
```

Pour arrêter de partager un AMI fichier avec toutes les OUs organisations et Comptes AWS d'utiliser le AWS CLI

La reset-image-attributecommande supprime toutes les autorisations de lancement publiques et explicites de celles spécifiéesAMI. Notez que le propriétaire du dispose AMI toujours des autorisations de lancement et n'est donc pas affecté par cette commande.

```
aws ec2 reset-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

> **Note**
>
> Vous ne pouvez pas arrêter de partager un AMI fichier avec un compte spécifique s'il s'agit d'une organisation ou d'une unité d'organisation avec laquelle un compte AMI est partagé. Si vous essayez d'arrêter le partage AMI en supprimant les autorisations de lancement du compte, Amazon EC2 renvoie un message de réussite. Cependant, ils AMI continuent d'être partagés avec le compte.

Partagez et AMI avec des AWS comptes spécifiques

Vous pouvez partager un AMI avec en particulier Comptes AWS sans le rendre AMI public. Tout ce dont vous avez besoin, c'est du Compte AWS IDs.

Un Compte AWS identifiant est un numéro à 12 chiffres, par exemple`012345678901`, qui identifie de manière unique un Compte AWS. Pour plus d'informations, veuillez consulter la section Afficher les identifiants Compte AWS dans le Guide de référence AWS Account Management .

Considérations

Tenez compte des points suivants lorsque vous partagez AMIs avec des personnes spécifiques Comptes AWS.

- Propriété — Pour partager unAMI, vous Compte AWS devez posséder leAMI.
- Limites de partage : pour connaître le nombre maximum d'entités avec lesquelles l'ADN AMI peut être partagé au sein d'une région, consultez les quotas EC2 de service Amazon.
- Balises : vous ne pouvez pas partager de balises définies par l'utilisateur (balises que vous attachez à unAMI). Lorsque vous partagez unAMI, les balises définies par l'utilisateur ne sont pas accessibles aux personnes avec Compte AWS lesquelles AMI il est partagé.
- Chiffrement et clés : vous pouvez partager des AMIs données soutenues par des instantanés chiffrés et non chiffrés.
  - Les instantanés chiffrés doivent être chiffrés à l'aide d'une KMS clé. Vous ne pouvez pas partager ceux AMIs qui sont sauvegardés par des instantanés chiffrés à l'aide de la clé AWS gérée par défaut.
  - Si vous partagez un AMI fichier basé sur des instantanés chiffrés, vous devez Comptes AWS autoriser l'utilisation des KMS clés utilisées pour chiffrer les instantanés. Pour de plus amples informations, veuillez consulter Autoriser les organisations et OUs utiliser une KMS clé. Pour configurer la politique de clé dont vous avez besoin pour lancer des instances Auto Scaling lorsque vous utilisez une clé gérée par le client pour le chiffrement, consultez la section AWS KMS key Politique requise pour une utilisation avec des volumes chiffrés dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.
- Région — AMIs sont une ressource régionale. Lorsque vous partagez unAMI, il n'est disponible que dans cette région. Pour le rendre AMI disponible dans une autre région, copiez-le dans la région, puis partagez-le. AMI Pour de plus amples informations, veuillez consulter Copier un Amazon EC2 AMI.
- Utilisation — Lorsque vous partagez unAMI, les utilisateurs ne peuvent lancer des instances qu'à partir duAMI. Ils ne peuvent pas la supprimer, la partager ou la modifier. Cependant, une fois qu'ils ont lancé une instance à l'aide de votre instanceAMI, ils peuvent en créer une AMI à partir de leur instance.
- Copie partagée AMIs — Si les utilisateurs d'un autre compte souhaitent copier un partageAMI, vous devez leur accorder des autorisations de lecture pour le stockage qui sauvegarde leAMI. Pour de plus amples informations, veuillez consulter Copie entre comptes.

- Facturation — Vous n'êtes pas facturé lorsque le vôtre AMI est utilisé par d'autres Comptes AWS pour lancer des instances. Les comptes qui lancent des instances à l'aide du AMI sont facturés pour les instances qu'ils lancent.

Partager une AMI (console)

Pour donner des autorisations de lancement explicites à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez AMIs.
3. Sélectionnez votre AMI dans la liste, puis choisissez Actions, Modifier AMI les autorisations.
4. Choisissez Private (Privé).
5. Sous Shared accounts (Comptes partagés), choisissez Add account ID (Ajouter un ID de compte).
6. Pour Compte AWS ID, entrez l' Compte AWS ID avec lequel vous souhaitez partager leAMI, puis choisissez Partager AMI.

   Pour le partager AMI avec plusieurs comptes, répétez les étapes 5 et 6 jusqu'à ce que vous ayez ajouté tous les comptes requisIDs.

   > **Note**
   >
   > Vous n'avez pas besoin de partager les EBS instantanés Amazon auxquels un AMI utilisateur fait référence pour partager leAMI. Seul le AMI fichier lui-même doit être partagé ; le système fournit automatiquement à l'instance l'accès aux EBS instantanés Amazon référencés pour le lancement. Cependant, vous devez partager toutes les KMS clés utilisées pour chiffrer les instantanés auxquels il fait référence. AMI Pour plus d'informations, consultez Partager un EBS instantané Amazon dans le guide de EBS l'utilisateur Amazon.

7. Lorsque vous avez terminé, choisissez Save changes (Enregistrer les modifications).
8. (Facultatif) Pour afficher les Compte AWS IDs fichiers avec lesquels vous les avez partagésAMI, sélectionnez-les AMI dans la liste, puis cliquez sur l'onglet Autorisations. Pour découvrir AMIs ceux qui sont partagés avec vous, consultezRechercher un partage AMIs à utiliser pour les EC2 instances Amazon.

Partagez un AMI (1 AWS CLI)

Utilisez la modify-image-attributecommande (AWS CLI) pour partager un AMI comme indiqué dans les exemples suivants.

Pour donner des autorisations de lancement explicites

La commande suivante accorde des autorisations de lancement pour le fichier spécifié AMI à ce qui est spécifié Compte AWS. Dans l'exemple suivant, remplacez l'exemple d'AMIidentifiant par un AMI identifiant valide, puis remplacez-le *account-id* par un Compte AWS identifiant à 12 chiffres.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Add=[{UserId=account-id}]"
```

> **Note**
>
> Vous n'avez pas besoin de partager les EBS instantanés Amazon auxquels un AMI utilisateur fait référence pour partager leAMI. Seul le AMI fichier lui-même doit être partagé ; le système fournit automatiquement à l'instance l'accès aux EBS instantanés Amazon référencés pour le lancement. Cependant, vous devez partager toutes les KMS clés utilisées pour chiffrer les instantanés auxquels il fait référence. AMI Pour plus d'informations, consultez Partager un EBS instantané Amazon dans le guide de EBS l'utilisateur Amazon.

Pour supprimer des autorisations de lancement données à un compte

La commande suivante supprime les autorisations de lancement pour le fichier spécifié AMI par rapport à ce qui est spécifié Compte AWS. Dans l'exemple suivant, remplacez l'exemple d'AMIidentifiant par un AMI identifiant valide, puis remplacez-le *account-id* par un Compte AWS identifiant à 12 chiffres.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Remove=[{UserId=account-id}]"
```

Pour supprimer toutes les autorisations de lancement

La commande suivante supprime toutes les autorisations de lancement publiques et explicites de celles spécifiéesAMI. Notez que le propriétaire du dispose AMI toujours des autorisations de

lancement et n'est donc pas affecté par cette commande. Dans l'exemple suivant, remplacez l'exemple AMI d'ID par un AMI ID valide.

```
aws ec2 reset-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

Partager un AMI (Outils pour Windows PowerShell)

Utilisez la Edit-EC2ImageAttributecommande (Outils pour Windows PowerShell) pour partager un AMI comme indiqué dans les exemples suivants.

Pour donner des autorisations de lancement explicites

La commande suivante accorde des autorisations de lancement pour le fichier spécifié AMI à ce qui est spécifié Compte AWS. Dans l'exemple suivant, remplacez l'exemple d'AMIidentifiant par un AMI identifiant valide, puis remplacez-le *account-id* par un Compte AWS identifiant à 12 chiffres.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType add -UserId "account-id"
```

> **Note**
>
> Vous n'avez pas besoin de partager les EBS instantanés Amazon auxquels un AMI utilisateur fait référence pour partager leAMI. Seul le AMI fichier lui-même doit être partagé ; le système fournit automatiquement à l'instance l'accès aux EBS instantanés Amazon référencés pour le lancement. Cependant, vous devez partager toutes les KMS clés utilisées pour chiffrer les instantanés auxquels il fait référence. AMI Pour plus d'informations, consultez Partager un EBS instantané Amazon dans le guide de EBS l'utilisateur Amazon.

Pour supprimer des autorisations de lancement données à un compte

La commande suivante supprime les autorisations de lancement pour le fichier spécifié AMI par rapport à ce qui est spécifié Compte AWS. Dans l'exemple suivant, remplacez l'exemple d'AMIidentifiant par un AMI identifiant valide, puis remplacez-le *account-id* par un Compte AWS identifiant à 12 chiffres.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType remove -UserId "account-id"
```

Pour supprimer toutes les autorisations de lancement

La commande suivante supprime toutes les autorisations de lancement publiques et explicites de celles spécifiéesAMI. Notez que le propriétaire du dispose AMI toujours des autorisations de lancement et n'est donc pas affecté par cette commande. Dans l'exemple suivant, remplacez l'exemple AMI d'ID par un AMI ID valide.

```
PS C:\> Reset-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission
```

Annuler le AMI partage avec votre Compte AWS

Une Amazon Machine Image (AMI) peut être partagée avec des utilisateurs spécifiques en Comptes AWS ajoutant les comptes aux autorisations AMI de lancement. Si un compte AMI a été partagé avec vous Compte AWS et que vous ne souhaitez plus le partager avec votre compte, vous pouvez supprimer les autorisations de lancement AMI de votre compte. Pour ce faire, exécutez la `cancel-image-launch-permission` AWS CLI commande. Lorsque vous exécutez cette commande, vos autorisations de lancement Compte AWS sont supprimées pour les autorisations de lancement spécifiéesAMI. Pour trouver ceux AMIs qui sont partagés avec vous Compte AWS, consultezRechercher un partage AMIs à utiliser pour les EC2 instances Amazon.

Vous pouvez annuler le AMI partage d'une instance avec votre compte, par exemple, pour réduire la probabilité de lancer une instance avec une instance non utilisée ou obsolète AMI qui a été partagée avec vous. Lorsque vous annulez un AMI partage avec votre compte, il n'apparaît plus dans aucune AMI liste de la EC2 console ou dans la sortie pour describe-images.

Rubriques

- Limites
- Annuler un AMI partage avec votre compte

Limites

- Vous pouvez supprimer votre compte des autorisations de lancement d'un AMI compte partagé Compte AWS uniquement avec vous. Vous ne pouvez pas l'utiliser `cancel-image-launch-`

`permission` pour retirer votre compte des autorisations de lancement d'un compte AMIpartagé avec une organisation ou une unité organisationnelle (UO) ou pour supprimer l'accès au publicAMIs.

- Vous ne pouvez pas supprimer définitivement votre compte des autorisations de lancement d'unAMI. AMILe propriétaire peut à nouveau en partager un AMI avec votre compte.
- AMIssont une ressource régionale. Lors de l'exécution`cancel-image-launch-permission`, vous devez spécifier la région dans laquelle se AMI trouve le. Spécifiez la région dans la commande ou utilisez la variable d'REGIONenvironnement AWS DEFAULT _ _.
- Seul le SDKs support AWS CLI et la suppression de votre compte des autorisations de lancement d'unAMI. La EC2 console ne prend actuellement pas en charge cette action.

Annuler un AMI partage avec votre compte

> **Note**
>
> Une fois que vous avez annulé un AMI partage avec votre compte, vous ne pouvez pas l'annuler. Pour y accéder de nouveauAMI, le AMI propriétaire doit le partager avec votre compte.

AWS CLI

Pour annuler le AMI partage d'un message avec votre Compte AWS

Utilisez la cancel-image-launch-permissioncommande et spécifiez l'AMIID.

```
aws ec2 cancel-image-launch-permission \
    --image-id ami-0123456789example \
    --region us-east-1
```

Sortie attendue

```
{
    "Return": true
}
```

PowerShell

Pour annuler un AMI partage avec vous à Compte AWS l'aide du AWS Tools for PowerShell

Utilisez la Stop-EC2ImageLaunchPermissioncommande et spécifiez l'AMIID.

```
Stop-EC2ImageLaunchPermission `
    -ImageId ami-0123456789example `
    -Region us-east-1
```

Sortie attendue

```
True
```

Recommandations pour créer un système Linux partagé AMIs

Suivez les instructions suivantes pour réduire la surface d'attaque et améliorer la fiabilité de ce AMIs que vous créez.

> **Important**
>
> Aucune liste de consignes de sécurité ne peut être exhaustive. Créez votre partage AMIs avec soin et prenez le temps de réfléchir aux endroits où vous pourriez exposer des données sensibles.

Table des matières

Si vous créez AMIs pour cela AWS Marketplace, consultez la section Meilleures pratiques en matière de construction AMIs dans le Guide du AWS Marketplace vendeur pour connaître les directives, les politiques et les meilleures pratiques.

Pour plus d'informations sur le partage AMIs sécurisé, consultez les articles suivants :

- Comment partager et utiliser le public AMIs de manière sécurisée

- AMIPublication publique : exigences de renforcement et de nettoyage

Désactivation des connexions distantes basées sur un mot de passe pour l'utilisateur root

L'utilisation d'un mot de passe root fixe pour un public AMI constitue un risque de sécurité qui peut rapidement être connu. Même le fait de compter sur les utilisateurs pour changer le mot de passe après leur première connexion laisse une petite place à une opportunité d'abus potentiel.

Pour résoudre ce problème, désactivez les connexions à distance basées sur mot de passe pour l'utilisateur racine.

Pour désactiver les connexions à distance basées sur un mot de passe pour l'utilisateur root

1. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte et localisez la ligne suivante :

   ```
   #PermitRootLogin yes
   ```

2. Changez la ligne en :

   ```
   PermitRootLogin without-password
   ```

   L'emplacement de ce fichier de configuration peut être différent selon votre distribution ou si vous n'exécutez pas OpenSSH. Si tel est le cas, consultez la documentation appropriée.

Désactivation de l'accès local à la racine

Lorsque vous travaillez avec le partageAMIs, il est recommandé de désactiver les connexions root directes. Pour ce faire, connectez-vous à votre instance en cours d'exécution et entrez la commande suivante :

```
[ec2-user ~]$ sudo passwd -l root
```

> **Note**
>
> Cette commande n'a pas d'impact sur l'utilisation de `sudo`.

Supprimer les paires de clés d'SSHhôte

Si vous envisagez de partager un AMI dérivé d'un publicAMI, supprimez les paires de clés SSH d'hôte existantes qui se trouvent dans`/etc/ssh`. Cela oblige SSH à générer de nouvelles paires de SSH clés uniques lorsque quelqu'un lance une instance en utilisant la vôtreAMI, ce qui améliore la sécurité et réduit le risque man-in-the-middle d'attaques.

Supprimez tous les fichiers clés suivants présents dans votre système.

- ssh_host_dsa_key
- ssh_host_dsa_key.pub
- ssh_host_key
- ssh_host_key.pub
- ssh_host_rsa_key
- ssh_host_rsa_key.pub
- ssh_host_ecdsa_key
- ssh_host_ecdsa_key.pub
- ssh_host_ed25519_key
- ssh_host_ed25519_key.pub

Vous pouvez supprimer tous ces fichiers en toute sécurité avec la commande suivante.

```
[ec2-user ~]$ sudo shred -u /etc/ssh/*_key /etc/ssh/*_key.pub
```

> **Warning**
>
> Les utilitaires de suppression sécurisée tels que **`shred`** peuvent ne pas supprimer toutes les copies d'un fichier de vos supports de stockage. Des copies masquées de fichiers peuvent être créées en journalisant des systèmes de fichiers (y compris le fichier ext4 par défaut d'Amazon Linux), des instantanésRAID, des sauvegardes et une mise en cache temporaire. Pour plus d'informations, consultez la documentation **`shred`**.

> **Important**
>
> Si vous oubliez de supprimer les paires de clés SSH d'hôte existantes de votre publicAMI, notre processus d'audit de routine vous informe, ainsi que tous les clients utilisant vos instances, AMI du risque de sécurité potentiel. Après une courte période de grâce, nous marquons la AMI confidentialité.

Installation d'informations d'identification publiques

Après avoir configuré le AMI pour empêcher la connexion à l'aide d'un mot de passe, vous devez vous assurer que les utilisateurs peuvent se connecter à l'aide d'un autre mécanisme.

Amazon EC2 permet aux utilisateurs de spécifier un nom de paire de clés publique-privée lors du lancement d'une instance. Lorsqu'un nom de paire de clés valide est fourni à l'`RunInstances`APIappel (ou via les API outils de ligne de commande), la clé publique (la partie de la paire de clés qu'Amazon EC2 conserve sur le serveur après un appel à `CreateKeyPair` ou`ImportKeyPair`) est mise à la disposition de l'instance par le biais d'une HTTP requête portant sur les métadonnées de l'instance.

Pour vous connecterSSH, vous AMI devez récupérer la valeur de la clé au démarrage et l'ajouter `/root/.ssh/authorized_keys` (ou l'équivalent pour tout autre compte utilisateur sur leAMI). Les utilisateurs peuvent lancer vos instances à l'AMIaide d'une paire de clés et se connecter sans avoir besoin d'un mot de passe root.

De nombreuses distributions, dont Amazon Linux et Ubuntu, utilisent le package `cloud-init` pour injecter des informations d'identification de clé publiques pour un utilisateur configuré. Si votre distribution ne prend pas en charge `cloud-init`, vous pouvez ajouter le code suivant à un script de démarrage système (tel que `/etc/rc.local`) pour extraire la clé publique que vous avez spécifiée au lancement pour l'utilisateur racine.

> **Note**
>
> Dans l'exemple suivant, l'adresse IP http://169.254.169.254/ est une adresse lien-local et elle n'est valide que depuis l'instance.

IMDSv2

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

IMDSv1

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

Cela peut être appliqué à n'importe quel utilisateur. Il n'est pas nécessaire de la limiter à l'utilisateur `root`.

> **Note**
>
> Le regroupement d'une instance sur cette base AMI inclut la clé avec laquelle elle a été lancée. Pour éviter l'inclusion de la clé, vous devez vider (ou supprimer) le fichier `authorized_keys` ou exclure ce fichier du nouveau bundle.

Désactiver les DNS vérifications SSHD (facultatif)

La désactivation des DNS vérifications SSHD affaiblit légèrement votre sécurité SSHD. Toutefois, en cas d'échec de la DNS résolution, SSH les connexions fonctionnent toujours. Si vous ne désactivez pas les vérifications SSHD, les échecs de DNS résolution empêcheront toutes les connexions.

Pour désactiver les vérifications SSHD DNS

1. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte et localisez la ligne suivante :

```
#UseDNS yes
```

2. Changez la ligne en :

```
UseDNS no
```

> **Note**
>
> L'emplacement de ce fichier de configuration peut varier selon votre distribution ou si vous n'exécutez pas OpenSSH. Si tel est le cas, consultez la documentation appropriée.

Supprimer les données sensibles

Nous vous déconseillons de stocker des données ou des logiciels sensibles sur AMI ceux que vous partagez. Les utilisateurs qui lancent un partage AMI peuvent être en mesure de le regrouper et de l'enregistrer comme leur propre compte. Suivez ces consignes pour vous permettre d'éviter de vous exposer à des risques de sécurité facilement négligés :

- Nous recommandons d'utiliser l'option `--exclude` *`directory`* sur `ec2-bundle-vol` pour éviter tout répertoire et sous-répertoire contenant des informations secrètes que vous ne souhaiteriez pas inclure dans votre regroupement. En particulier, excluez toutes les paires de clés SSH publiques/privées et tous les SSH `authorized_keys` fichiers appartenant à l'utilisateur lors du regroupement de l'image. Le public Amazon les AMIs stocke `/root/.ssh` pour l'utilisateur root et /home/*`user_name`*`/.ssh/` pour les utilisateurs réguliers. Pour de plus amples informations, veuillez consulter ec2-bundle-vol.
- Supprimez toujours l'historique shell avant la création d'un bundle. Si vous tentez de télécharger plusieurs lots simultanémentAMI, l'historique du shell contient votre clé d'accès. L'exemple ci-

après devrait être la dernière commande que vous avez exécutée avant de créer un bundle depuis l'instance.

```
[ec2-user ~]$ shred -u ~/.*history
```

> **Warning**
>
> Les limites de **`shred`** décrites dans l'avertissement ci-dessus s'appliquent également ici. Ayez à l'esprit que bash inscrit l'historique de la session en cours sur le disque au moment de quitter. Si vous vous déconnectez de votre instance après avoir supprimé `~/.bash_history` et si vous vous reconnectez ensuite, vous constaterez que `~/.bash_history` a été recréé et contient toutes les commandes que vous avez exécutées durant votre session précédente.
> D'autres programmes en dehors de bash inscrivent les historiques sur le disque. Soyez prudent et retirez ou excluez tous les fichiers et répertoires dot superflus.

- La création d'une offre groupée pour une instance en cours d'exécution nécessite votre clé privée et un certificat X.509. Mettez ces éléments et toutes les autres informations d'identification dans un endroit qui n'est pas regroupé (comme par exemple le stockage d'instances).

Surveillez les AMI événements à l'aide d'Amazon EventBridge

Lorsque l'état d'une Amazon Machine Image (AMI) change, Amazon EC2 génère un événement qui est envoyé à Amazon EventBridge (anciennement Amazon CloudWatch Events). Les événements sont envoyés au bus d' EventBridge événements par défaut au JSON format. Vous pouvez utiliser Amazon EventBridge pour détecter ces événements et y réagir. Pour ce faire, vous devez créer des règles EventBridge qui déclenchent une action en réponse à un événement. Par exemple, vous pouvez créer une EventBridge règle qui détecte la fin du processus de AMI création, puis qui invoque un SNS sujet Amazon pour vous envoyer une notification par e-mail.

Amazon EC2 génère un `EC2 AMI State Change` événement lorsqu'un utilisateur AMI entre dans l'un des états suivants :

- `available`
- `failed`
- `deregistered`

- `disabled`

Les événements sont générés sur la base du meilleur effort.

Le tableau suivant répertorie les AMI opérations et les états qu'un homme AMI peut entrer. Dans le tableau, Oui indique les états qu'ils AMI peuvent entrer lors de l'exécution de l'opération correspondante.

AMIopérations	available	failed	deregistered	disabled
CopyImage	Oui	Oui		
CreateImage	Oui	Oui		
CreateRestoreImageTask	Oui	Oui		
DeregisterImage			Oui	
DisableImage				Oui
EnableImage	Oui			
RegisterImage	Oui	Oui		

Événements EC2 AMI State Change

- Détails de l'événement
- Événements available
- Événements failed
- Événements deregistered
- Événements disabled

Détails de l'événement

Vous pouvez utiliser les champs suivants lors de l'événement pour créer des règles qui déclenchent une action :

`"source": "aws.ec2"`

Indique que l'événement provient d'AmazonEC2.

`"detail-type": "EC2 AMI State Change"`

Identifie le nom de l'événement.

`"detail": { "ImageId": "ami-0123456789example", "State": "available", }`

Fournit l'AMIID et l'état du AMI (`available`failed,`deregistered`, ou`disabled`).

Pour plus d'informations, consultez les informations suivantes dans le guide de EventBridge l'utilisateur Amazon :

- EventBridge Événements Amazon
- Modèles d' EventBridge événements Amazon
- EventBridge Règles d'Amazon

Pour un didacticiel sur la création d'une fonction Lambda et d'une EventBridge règle qui exécute la fonction Lambda, consultez Tutoriel : enregistrez l'état d'une EC2 instance Amazon EventBridge à l'aide du manuel du développeur.AWS Lambda

Événements available

Voici un exemple d'événement EC2 généré par Amazon lorsqu'il AMI entre dans l'`available`état suite à une `EnableImage` opération `CreateImage`,`CopyImage`,`RegisterImage`,`CreateRestoreImageTask`, ou réussie.

`"State": "available"` indique que l'opération a réussi.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
```

```
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "available",
        "ErrorMessage": ""
    }
}
```

Événements failed

Voici un exemple d'événement EC2 généré par Amazon lorsqu'il AMI entre dans l'`failed`état suite à un échec `CreateImage` ou à une `CreateRestoreImageTask` opération. `CopyImage` `RegisterImage`

Les champs suivants fournissent des informations pertinentes :

- `"State": "failed"` : indique que l'opération a échoué.
- `"ErrorMessage": ""` : indique la raison de l'échec de l'opération.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "failed",
        "ErrorMessage": "Description of failure"
    }
}
```

Événements deregistered

Voici un exemple d'événement EC2 généré par Amazon lorsqu'il AMI entre dans l'`deregistered`état après une `DeregisterImage` opération réussie. Si l'opération échoue, aucun

événement n'est généré. Tout échec est immédiatement connu, car `DeregisterImage` est une opération synchrone.

`"State": "deregistered"` indique que l'opération `DeregisterImage` a réussi.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "deregistered",
        "ErrorMessage": ""
    }
}
```

Événements disabled

Voici un exemple d'événement EC2 généré par Amazon lorsqu'il AMI entre dans l'`disabled`état après une `DisableImage` opération réussie. Si l'opération échoue, aucun événement n'est généré. Tout échec est immédiatement connu, car `DisableImage` est une opération synchrone.

`"State": "disabled"` indique que l'opération `DisableImage` a réussi.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "disabled",
```

```
        "ErrorMessage": ""
    }
}
```

Comprendre les informations de facturation d'AMI

Il existe de nombreuses Amazon Machine Images (AMI) entre lesquelles choisir lorsque vous lancez vos instances, et celles-ci prennent en charge une variété de fonctionnalités et de plateformes du système d'exploitation. Pour comprendre l'impact de l'AMI que vous choisissez lors du lancement de votre instance sur le résultat net de votre AWS facture, vous pouvez rechercher la plate-forme du système d'exploitation et les informations de facturation associées. Faites ceci avant de lancer des instances Spot ou à la demande, ou d'acheter une Instance réservée.

Voici deux exemples qui illustrent en quoi une recherche préalable de votre AMI peut vous aider à choisir l'AMI qui correspond le mieux à vos besoins :

- Pour les Instances Spot, vous pouvez utiliser les détails de la plateforme sur l'AMI pour confirmer que l'AMI est prise en charge pour les Instances Spot.
- Lorsque vous achetez une Instance réservée, vous pouvez vous assurer que vous sélectionnez la plateforme du système d'exploitation (Platform) qui correspond aux détails de la plateforme sur l'AMI.

Pour plus d'informations sur la tarification des instances, consultez Tarification Amazon EC2.

Sommaire

Champs d'informations de facturation d'AMI

Les champs suivants fournissent les informations de facturation associées à une AMI :

Platform details (Détails de la plateforme)

> Détails de la plateforme associée au code de facturation de l'AMI. Par exemple, `Red Hat Enterprise Linux`.

Usage operation (Opération d'utilisation)

Opération de l'instance Amazon EC2 et code de facturation associé à l'AMI. Par exemple, `RunInstances:0010`. L'opération d'utilisation correspond à la colonne LineItem/Operation de votre rapport sur les AWS coûts et l'utilisation (CUR) et dans l'API AWS Price List.

Vous pouvez consulter ces champs sur la page Instances ou AMI de la console Amazon EC2, ou dans la réponse renvoyée par la commande describe-images. Get-EC2Image

Exemples de données : opération d'utilisation par plateforme

Le tableau suivant répertorie certains détails de la plateforme et les valeurs des opérations d'utilisation qui peuvent être affichés sur les pages Instances ou AMI de la console Amazon EC2, ou dans la réponse renvoyée par la commande describe-images. Get-EC2Image

Platform details (Détails de la plateforme)	Opération d'utilisation [2]
Linux/UNIX	RunInstances
Red Hat BYOL Linux	RunInstances:00g0[3]
Red Hat Enterprise Linux	RunInstances:0010
Red Hat Enterprise Linux with HA	RunInstances:1010
Red Hat Enterprise Linux with SQL Server Standard and HA	RunInstances:1014
Red Hat Enterprise Linux with SQL Server Enterprise and HA	RunInstances:1110
Red Hat Enterprise Linux with SQL Server Standard	RunInstances:0014
Red Hat Enterprise Linux with SQL Server Web	RunInstances:0210
Red Hat Enterprise Linux with SQL Server Enterprise	RunInstances:0110

Platform details (Détails de la plateforme)	Opération d'utilisation [2]
SQL Server Enterprise	RunInstances:0100
SQL Server Standard	RunInstances:0004
SQL Server Web	RunInstances:0200
SUSE Linux	RunInstances:000g
Ubuntu Pro	RunInstances:0g00
Windows	RunInstances:0002
Windows BYOL	RunInstances:0800
Windows with SQL Server Enterprise[1]	RunInstances:0102
Windows with SQL Server Standard[1]	RunInstances:0006
Windows with SQL Server Web[1]	RunInstances:0202

[1] Si deux licences logicielles sont associées à une AMI, le champ Détails de la plate-forme indique les deux.

[2] Si vous utilisez des instances Spot, la valeur de votre rapport lineitem/Operationsur les AWS coûts et l'utilisation peut être différente de la valeur de l'opération d'utilisation répertoriée ici. Par exemple, s'il s'`lineitem/Operation`affiche`RunInstances:0010:SV006`, cela signifie qu'Amazon EC2 exécute Red Hat Enterprise Linux Spot Instance-Hour dans l'est des États-Unis (Virginie du Nord) dans la zone 6.

[3] Cela apparaît comme RunInstances (Linux/UNIX) dans vos rapports d'utilisation.

Recherche des détails de facturation et d'utilisation d'AMI

Dans la console Amazon EC2, vous pouvez afficher les informations de facturation d'AMI à partir des pages AMI ou Instances. Vous pouvez également trouver des informations de facturation à l'aide du AWS CLI ou du service de métadonnées de l'instance.

Les champs suivants peuvent vous aider à vérifier les frais d'AMI sur votre facture :

- Platform details (Détails de la plateforme)
- Usage operation (Opération d'utilisation)
- ID D'AMI

Rechercher les informations de facturation d'AMI (console)

Procédez comme suit pour afficher les informations de facturation d'AMI dans la console Amazon EC2 :

Rechercher les informations de facturation d'AMI à partir de la page AMI

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez AMI, puis sélectionnez une AMI.
3. Sous l'onglet Details (Détails) vérifiez les valeurs de Platform details (Détails de la plateforme) et Usage operation (Opération d'utilisation).

Rechercher les informations de facturation d'AMI à partir de la page Instances

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances, puis sélectionnez l'instance.
3. Sous l'onglet Détails (ou l'onglet Description si vous utilisez la version antérieure de la console), examinez les valeurs pour Détails de la plateforme et Opération d'utilisation.

Rechercher les informations de facturation d'AMI (AWS CLI)

Pour trouver les informations de facturation de l'AMI à l'aide du AWS CLI, vous devez connaître l'ID de l'AMI. Si vous ne connaissez pas l'ID d'AMI, vous pouvez l'obtenir à partir de l'instance à l'aide de la commande describe-instances.

Pour trouver l'ID d'AMI

Si vous connaissez l'ID d'instance, vous pouvez obtenir l'ID d'AMI de l'instance à l'aide de la commande describe-instances.

```
aws ec2 describe-instances --instance-ids i-123456789abcde123
```

Dans la sortie, l'ID d'AMI est spécifié dans le champ `ImageId`.

```
..."Instances": [
{
    "AmiLaunchIndex": 0,
    "ImageId": "ami-0123456789EXAMPLE",
    "InstanceId": "i-123456789abcde123",
    ...
}]
```

Pour trouver les informations de facturation d'AMI

Si vous connaissez l'ID d'AMI, vous pouvez utiliser la commande describe-images pour obtenir les détails de la plateforme d'AMI et de l'opération d'utilisation.

```
$ aws ec2 describe-images --image-ids ami-0123456789EXAMPLE
```

L'exemple de sortie suivant montre les champs `PlatformDetails` et `UsageOperation`. Dans cet exemple, la plateforme ami-0123456789EXAMPLE est `Red Hat Enterprise Linux`, et la valeur de l'opération d'utilisation et du code de facturation est `RunInstances:0010`.

```
{
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "Hypervisor": "xen",
            "EnaSupport": true,
            "SriovNetSupport": "simple",
            "ImageId": "ami-0123456789EXAMPLE",
            "State": "available",
            "BlockDeviceMappings": [
                {
```

```
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-1112223334444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "PlatformDetails": "Red Hat Enterprise Linux",
            "UsageOperation": "RunInstances:0010",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
            "Public": true,
            "ImageType": "machine",
            "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
        }
    ]
}
```

Vérifier les frais d'AMI sur votre facture

Pour vous assurer de ne pas encourir de coûts imprévus, vous pouvez vérifier que les informations de facturation d'une instance figurant dans votre rapport sur les AWS coûts et l'utilisation (CUR) correspondent aux informations de facturation associées à l'AMI que vous avez utilisée pour lancer l'instance.

Pour vérifier les informations de facturation, recherchez l'ID d'instance dans votre rapport de coût et d'utilisation et vérifiez la valeur correspondante dans la colonne `lineitem/Operation`. La valeur doit correspondre à la valeur de Usage operation (Opération d'utilisation) associée à l'AMI.

Par exemple, l'AMI `ami-0123456789EXAMPLE` contient les informations de facturation suivantes :

- Platform details (Détails de la plateforme = `Red Hat Enterprise Linux`
- Opération d'utilisation = `RunInstances:0010`

Si vous avez lancé une instance à l'aide de cette AMI, vous pouvez trouver l'ID d'instance dans votre rapport d'utilisation et de coût et vérifier la valeur correspondante dans la colonne `lineitem/Operation`. Dans cet exemple. la valeur devrait être `RunInstances:0010`.

AMIquotas sur Amazon EC2

Les quotas suivants s'appliquent à la création et au partageAMIs. Les quotas s'appliquent par Région AWS.

Nom du quota	Description	Quota par défaut par région
AMIs	Le nombre maximum de sites publics et privés AMIs autorisés par région. Il s'agit notamment des produits disponibles, en attenteAMIs, désactivés et AMIs placés dans la corbeille.	50 000
Publique AMIs	Le nombre maximum de visiteurs autorisés par régionAMIs, y compris le public se trouvant AMIs dans la corbeille.	5
AMIpartage	Le nombre maximum d'entités (organisations, unités organisationnelles (OUs) et comptes) avec lesquelles il est AMI possible de partager dans une région. Notez que si vous partagez un AMI avec une organisation ou une unité d'organisation, le nombre de comptes de l'organisation ou de l'unité d'organisation n'est	1 000

Nom du quota	Description	Quota par défaut par région
	pas pris en compte dans le calcul du quota.	

Si vous dépassez vos quotas et que vous souhaitez en créer ou partager davantageAMIs, vous pouvez effectuer les opérations suivantes :

- Si vous dépassez votre AMIs quota total AMIs ou public, pensez à annuler l'enregistrement des images non utilisées.
- Si vous dépassez votre AMIs quota public, pensez à en rendre un ou plusieurs publics AMIs privés.
- Si vous dépassez votre quota de AMI partage, envisagez de le partager AMIs avec une organisation ou une unité d'organisation plutôt qu'avec des comptes séparés.
- Demandez une augmentation de quota pourAMIs.

Demandez une augmentation de quota pour AMIs

Si vous avez besoin d'un quota supérieur au quota par défaut pourAMIs, vous pouvez demander une augmentation de quota.

Pour demander une augmentation de quota pour AMIs

1. Ouvrez la console Service Quotas à l'adresse https://console.aws.amazon.com/servicequotas/.
2. Dans le panneau de navigation, choisissez Services AWS .
3. Choisissez Amazon Elastic Compute Cloud (AmazonEC2) dans la liste ou saisissez le nom du service dans le champ de recherche.
4. Choisissez le AMI quota pour demander une augmentation. Les AMI quotas que vous pouvez sélectionner sont les suivants :
   - AMIs
   - Publique AMIs
   - AMIpartage
5. Choisissez Request quota increase (Demander une augmentation de quota).
6. Pour Change quota value (Modifier la valeur du quota), saisissez la nouvelle valeur du quota, puis sélectionnez Request (Demander).

Pour afficher les demandes en attente ou récemment résolues, choisissez Dashboard (Tableau de bord) dans le volet de navigation. Pour les demandes en attente, choisissez l'état de la demande pour ouvrir le reçu de la demande. L'état initial d'une demande est Pending (En attente). Une fois que le statut est passé à Quota requested (Quota demandé), vous verrez le numéro du cas sous Support Center case number (Numéro de cas du centre de support). Choisissez le numéro de dossier pour ouvrir le billet pour votre demande.

Une fois la demande résolue, la Applied quota value (Valeur de quota appliquée) pour le quota est définie selon la nouvelle valeur.

Pour plus d'informations, consultez le Guide de l'utilisateur Service Quotas.

EC2Instances Amazon

Une EC2 instance Amazon est un serveur virtuel dans un environnement AWS cloud. Vous avez le contrôle total de votre instance, depuis le moment où vous la démarrez pour la première fois (lancement d'une instance) et jusqu'à ce que vous la supprimiez (arrêt d'une instance). Vous pouvez choisir parmi différents systèmes d'exploitation lorsque vous lancez votre instance. Vous pouvez vous connecter à votre instance et la personnaliser en fonction de vos besoins. Par exemple, vous pouvez configurer le système d'exploitation, installer des mises à jour du système d'exploitation et installer des applications sur votre instance.

Amazon EC2 propose un large éventail de types d'instances. Vous pouvez choisir un type d'instance qui fournit les ressources de calcul, la mémoire, le stockage et les performances réseau dont vous avez besoin pour exécuter vos applications.

Avec AmazonEC2, vous ne payez que pour ce que vous utilisez. La facturation de votre instance commence lorsque vous lancez votre instance et passe à l'état en cours d'exécution. La facturation s'arrête lorsque vous arrêtez votre instance et reprend lorsque vous démarrez votre instance. Lorsque vous mettez fin à votre instance, la facturation s'arrête lorsqu'elle passe à l'état d'arrêt.

Amazon EC2 fournit des fonctionnalités que vous pouvez utiliser pour optimiser les performances et le coût de vos instances. Par exemple, vous pouvez utiliser Amazon EC2 Fleet ou Amazon EC2 Auto Scaling pour augmenter ou diminuer votre capacité en fonction de l'évolution de l'utilisation de votre instance. Vous pouvez réduire les coûts de vos instances en utilisant des instances Spot ou des Savings Plans.

Fonctionnalités et tâches

- Types d'EC2instances Amazon
- Options EC2 de facturation et d'achat Amazon
- Stockez les paramètres de lancement de l'instance dans les modèles de EC2 lancement Amazon
- Lancer une EC2 instance Amazon
- Connect à votre EC2 instance
- Modifications de l'état de l'EC2instance Amazon
- Utiliser les métadonnées de l'instance pour gérer votre EC2 instance
- Détecter si un hôte est une EC2 instance
- Documents d'identité d'instance pour les EC2 instances Amazon
- Synchronisation précise de l'heure et de l'heure sur votre EC2 instance

- Gérez les pilotes de périphériques pour votre EC2 instance
- Configuration de votre instance Amazon EC2 Windows
- Mettre à niveau une instance EC2 Windows vers une version plus récente de Windows Server
- Tutoriel : Connecter une EC2 instance Amazon à une RDS base de données Amazon

Types d'EC2instances Amazon

Lorsque vous lancez une instance, le type d'instance que vous spécifiez détermine les capacités matérielles de l'ordinateur hôte utilisé pour votre instance. Chaque type d'instance propose différentes capacités de calcul, de mémoire et de stockage, et est regroupé dans une famille de·l'instance en fonction de ces capacités. Sélectionnez un type d'instance en fonction des exigences de l'application ou du logiciel que vous prévoyez d'exécuter sur votre instance.

Amazon EC2 consacre certaines ressources de l'ordinateur hôteCPU, telles que la mémoire et le stockage d'instance, à une instance particulière. Amazon EC2 partage d'autres ressources de l'ordinateur hôte, telles que le réseau et le sous-système de disque, entre les instances. Si chaque instance d'un ordinateur hôte essaie d'utiliser autant que possible de l'une de ces ressources partagées, chacun reçoit une part égale de cette ressource. Cependant, quand une ressource est sous-utilisée, une instance peut consommer une part plus important de cette ressource, tant qu'elle est disponible.

Chaque type d'instance offre des performances minimales plus ou moins élevées à partir d'une ressource partagée. Par exemple, les types d'instance avec des performances d'I/O élevées bénéficient d'une plus grande allocation de ressources partagées. L'allocation d'une plus grande part de ressources partagées réduit aussi les écarts de performances d'I/O. Pour la plupart des applications, des performances d'I/O modérées sont plus que suffisantes. Cependant, pour les applications qui requièrent des performances d'I/O plus élevées ou plus régulières, envisagez un type d'instance avec des performances d'I/O supérieures.

Sommaire

- Changements de type d'EC2instance Amazon
- Instances de performance à capacité extensible
- Accélération des performances grâce aux GPU instances
- Instances Amazon EC2 Mac
- Types d'instances EBS optimisés pour Amazon
- CPUoptions pour les EC2 instances Amazon
- AMDSEV- SNP pour les EC2 instances Amazon
- Contrôle de l'état du processeur pour les instances Amazon EC2 Linux

Types d'instance disponibles

Amazon EC2 propose une large sélection de types d'instances optimisés pour s'adapter à différents cas d'utilisation. Les types d'instances comprennent différentes combinaisons de mémoireCPU, de stockage et de capacité réseau et vous offrent la flexibilité de choisir la combinaison de ressources appropriée pour vos applications. Chaque type d'instance inclut une ou plusieurs tailles d'instance, ce qui vous permet d'adapter vos ressources aux exigences de votre charge de travail cible. Pour plus d'informations sur les fonctionnalités et les cas d'utilisation, consultez les détails des types d'EC2instances Amazon.

Conventions de dénomination des types d'instances

Les noms sont basés sur la famille d'instances, la génération, la famille de processeurs, les capacités et la taille. Pour plus d'informations, consultez les conventions de dénomination dans le guide des types d'EC2instances Amazon.

Rechercher un type d'instance

Pour déterminer quels types d'instances répondent à vos besoins, tels que les régions prises en charge, les ressources de calcul ou les ressources de stockage, consultez Rechercher un type d'EC2instance Amazon les spécifications relatives aux types d'EC2instances Amazon dans le guide des types d'EC2instances Amazon.

instances de la génération actuelle

- Usage général : M5 | M5a | M5ad | M5dn | M5n | M5zn | M6a | M6g | M6gd | M6i | M6id | M6idn | M6in | M7a | M7g | M7GD | M7i | M7i-Flex | Mac1 | Mac2 | Mac2-M1Ultra | Mac2-M2 | Mac2-M2Pro | T2 | T3 | T3a | T4g

- Optimisé pour le calcul : C5 | C5a | C5ad | C5d | C5n | C6a | C6g | C6gd | C6gn | C6i | C6id | C6in | C7a | C7g | C7gd | C7gn | C7i | C7i-Flex
- Mémoire optimisée : R5 | R5a | R5ad | R5b | R5d | R5dn | R5n | R6a | R6g | R6gd | R6i | R6idn | R6in | R6id | R7a | R7g | R7i | R8g | U-3tb1 | U-6TB1 | U-6TB1 | U-9b TB1 | U-12TB1 | U-18TB1 | U-24TB1 | U7i-12TB | U7in-16TB | U7in-24TB | U7in-32TB | X1 | x2GD | X2idn | X2iEDN | X2ieZN | X1e | z1d
- Stockage optimisé : D2 | D3 | D3en | H1 | I3 | i3EN | i4G | i4i | iM4GN | IS4gen
- Calcul accéléré : DL1 | | F1 DL2q | G4ad | G4dn | G5 | G5g | G6 | G6e | Gr6 | Inf1 | Inf2 | P2 | P3 | P3dn | P4d | P4de | P5 | Trn1 | Trn1n | VT1
- Calcul haute performance : HPC6a | HPC6id | HPC7a | HPC7g

instances de la génération précédente

- Usage général : A1 | M1 | M2 | M3 | M4 | T1
- Optimisé pour le calcul : C1 | C3 | C4
- Mémoire optimisée : R3 | R4
- Stockage optimisé : I2
- Calcul accéléré : G3

Spécifications matérielles

Pour les spécifications détaillées des types d'instance, consultez les spécifications dans le guide des types d'EC2instance Amazon. Pour plus d'informations sur les tarifs, consultez la section Tarification EC2 à la demande d'Amazon.

Pour que vous puissiez déterminer le type d'instance qui correspond le mieux à vos besoins, nous vous recommandons de lancer une instance et d'utiliser votre propre application de comparaison. Comme vous payez l'instance à la seconde, il est pratique et économique de tester plusieurs types d'instances avant de prendre une décision. Si vos besoins évoluent, même après avoir pris une décision, vous pouvez par la suite modifier le type d'instance. Pour de plus amples informations, veuillez consulter Changements de type d'EC2instance Amazon.

Fonctions du processeur Intel

EC2Les instances Amazon qui s'exécutent sur des processeurs Intel peuvent inclure les fonctionnalités suivantes. Toutes les fonctions de processeur suivantes ne sont pas prises en

charge par tous les types d'instance. Pour obtenir des informations détaillées sur les fonctionnalités disponibles pour chaque type d'instance, consultez la section Types d'EC2instances Amazon.

- AESNouvelles instructions Intel (AES-NI) — Le jeu d'instructions de chiffrement Intel AES -NI améliore l'algorithme original Advanced Encryption Standard (AES) afin de fournir une protection des données plus rapide et une sécurité accrue. Toutes les EC2 instances de la génération actuelle prennent en charge cette fonctionnalité de processeur.
- Extensions vectorielles avancées Intel (IntelAVX, Intel et Intel AVX2 AVX -512) : Intel et Intel AVX2 sont des extensions de 256 bits, AVX et Intel AVX -512 est une extension de jeu d'instructions de 512 bits conçue pour les applications gourmandes en virgule flottante (FP). AVXLes instructions Intel améliorent les performances d'applications telles que le traitement d'images et audio/vidéo, les simulations scientifiques, les analyses financières, ainsi que la modélisation et l'analyse 3D. Ces fonctionnalités ne sont disponibles que sur les instances lancées avec HVMAMIs.
- Technologie Intel Turbo Boost — Les processeurs à technologie Intel Turbo Boost exécutent automatiquement les cœurs plus rapidement que la fréquence de fonctionnement de base.
- Intel Deep Learning Boost (Intel DL Boost) — Accélère les cas d'utilisation du deep learning d'IA. Les processeurs Intel Xeon Scalable de 2e génération ajoutent à Intel AVX -512 une nouvelle instruction de réseau neuronal vectoriel (VNNI/INT8) qui augmente considérablement les performances d'inférence par apprentissage profond par rapport aux processeurs Intel Xeon Scalable de génération précédente (avecFP32) pour la reconnaissance/segmentation d'images, la détection d'objets, la reconnaissance vocale, la traduction linguistique, les systèmes de recommandation, l'apprentissage par renforcement, etc. VNNIpeut ne pas être compatible avec toutes les distributions Linux.

  Les instances suivantes prennent en charge VNNI : `M5n`R5n,`M5dn`,`M5zn`,`R5b`,`R5dn`,`D3`,`D3en`, et`C6i`. `C5`et prise en charge VNNI des `C5d` instances uniquement pour `12xlarge`24xlarge, et `metal` instances.

Les conventions de dénomination utilisées dans le secteur pour le 64 bits peuvent prêter à confusionCPUs. Le fabricant de puces Advanced Micro Devices (AMD) a présenté la première architecture 64 bits à succès commercial basée sur le jeu d'instructions Intel x86. Par conséquent, l'architecture est largement considérée comme AMD64 quel que soit le fabricant de la puce. C'est notamment le cas pour Windows et plusieurs distributions Linux. Cela explique pourquoi les informations système internes d'une instance exécutant Ubuntu ou Windows affichent l'CPUarchitecture comme AMD64 si les instances étaient exécutées sur du matériel Intel.

AWS Processeurs Graviton

AWS Graviton est une famille de processeurs conçus pour offrir le meilleur rapport prix/performances pour vos charges de travail exécutées sur des instances AmazonEC2.

Pour plus d'informations, consultez Getting started with Graviton.

AWS Trainium

Les instances alimentées par AWS Trainium sont spécialement conçues pour une formation en deep learning performante et rentable. Vous pouvez utiliser ces instances pour entraîner des modèles de traitement du langage naturel, de vision par ordinateur et de recommandation utilisés dans un large éventail d'applications, telles que la reconnaissance vocale, la recommandation, la détection des fraudes et la classification d'images et de vidéos. Utilisez vos flux de travail existants dans des frameworks ML courants, tels que PyTorch et TensorFlow.

AWS Inférentie

Les instances alimentées par AWS Inferentia sont conçues pour accélérer l'apprentissage automatique. Ils fournissent une inférence d'apprentissage automatique à haute performance et à faible latence. Ces instances sont optimisées pour déployer des modèles de Deep Learning (DL) pour des applications telles que le traitement du langage naturel, la détection et la classification des objets, la personnalisation et le filtrage du contenu et la reconnaissance vocale.

Il y a plusieurs façons de démarrer :

- Use SageMaker, un service entièrement géré qui constitue le moyen le plus simple de démarrer avec les modèles d'apprentissage automatique. Pour plus d'informations, consultez Get Started with SageMaker dans le manuel Amazon SageMaker Developer Guide.
- Lancez une instance Inf1 ou Inf2 à l'aide du Deep Learning. AMI Pour plus d'informations, consultez AWS Inferentia with DLAMI dans le guide du AWS Deep Learning AMIs développeur.
- Lancez une instance Inf1 ou Inf2 en utilisant la vôtre AMI et installez le AWS Neuron SDK, qui vous permet de compiler, d'exécuter et de profiler des modèles d'apprentissage profond pour Inferentia. AWS
- Lancez une instance de conteneur à l'aide d'une instance Inf1 ou Inf2 et d'une instance optimisée pour AmazonECS. AMI Pour plus d'informations, consultez Amazon Linux 2 (Inferentia) AMIs dans le manuel du développeur Amazon Elastic Container Service.
- Créez un EKS cluster Amazon avec des nœuds exécutant des instances Inf1. Pour plus d'informations, consultez le support d'Inferentia dans le guide de EKS l'utilisateur Amazon.

AMItypes de virtualisation

Le type de virtualisation de votre instance est déterminé par celui AMI que vous utilisez pour la lancer. Les types d'instances de la génération actuelle ne prennent en charge que les machines virtuelles matérielles (HVM). Certains types d'instances de la génération précédente prennent en charge les instances paravirtuelles (PV) et certaines AWS régions prennent en charge les instances PV. Pour de plus amples informations, veuillez consulter Types de virtualisation.

Pour de meilleures performances, nous vous recommandons d'utiliser un HVMAMI. En outre, HVM AMIs sont nécessaires pour tirer parti d'un réseau amélioré. HVMla virtualisation utilise la technologie d'assistance matérielle fournie par la plateforme. AWS Avec la HVM virtualisation, la machine virtuelle cliente fonctionne comme si elle se trouvait sur une plate-forme matérielle native, sauf qu'elle utilise toujours le réseau photovoltaïque et les pilotes de stockage pour améliorer les performances.

Rechercher un type d'EC2instance Amazon

Pour pouvoir lancer une instance, vous devez sélectionner un type d'instance à utiliser. Le type d'instance que vous choisissez peut dépendre des ressources requises par votre charge de travail, telles que les ressources de calcul, de mémoire ou de stockage. Il peut être utile d'identifier plusieurs types d'instance qui pourraient convenir à votre charge de travail et d'évaluer leurs performances dans un environnement de test. Rien ne remplace la mesure des performances de votre application sous charge.

Vous pouvez obtenir des suggestions et des conseils pour les types d'EC2instances à l'aide de l'outil de recherche de types d'EC2instance. Pour de plus amples informations, veuillez consulter the section called "EC2outil de recherche de type d'instance".

Si vous avez déjà des EC2 instances en cours d'exécution, vous pouvez AWS Compute Optimizer obtenir des recommandations sur les types d'instances à utiliser pour améliorer les performances, économiser de l'argent, ou les deux. Pour de plus amples informations, veuillez consulter the section called "Recommandations Compute Optimizer".

Tâches

- Rechercher un type d'instance à l'aide de la console
- Décrivez un type d'instance à l'aide du AWS CLI
- Trouvez un type d'instance à l'aide du AWS CLI

Rechercher un type d'instance à l'aide de la console

Vous pouvez trouver un type d'instance qui répond à vos besoins à l'aide de la EC2 console Amazon.

Recherche d'un type d'instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation, sélectionnez la région dans laquelle lancer vos instances. Vous pouvez sélectionner n'importe quelle région disponible, quel que soit votre emplacement.
3. Dans le volet de navigation, choisissez Types d'instances.
4. (Facultatif) Choisissez l'icône de préférences pour sélectionner les attributs de type d'instance à afficher, tels que la tarification Linux à la demande, puis choisissez Valider. Vous pouvez également sélectionner le nom d'un type d'instance pour ouvrir sa page de détails et afficher tous les attributs disponibles dans la console. La console n'affiche pas tous les attributs disponibles par le biais de la ligne de commande API ou de la ligne de commande.
5. Utilisez les attributs de type d'instance pour filtrer la liste des types d'instance affichés uniquement aux types d'instance qui répondent à vos besoins. Par exemple, vous pouvez filtrer sur les attributs suivants :
   - Zones de disponibilité : le nom de la zone de disponibilité, de la zone locale ou des zones Wavelength. Pour de plus amples informations, veuillez consulter the section called "Régions et zones".
   - vCPUsou cœurs : nombre de cœurs vCPUs ou.
   - Mémoire (Gio) : la taille de la mémoire, en Gio.
   - Performances réseau : la performance du réseau, en Gigabits.
   - Stockage d'instance locale : indique si le type d'instance a un stockage d'instance local (`true | false`).
6. (Facultatif) Pour voir une side-by-side comparaison, cochez la case correspondant à plusieurs types d'instances. La comparaison s'affiche au bas de l'écran.
7. (Facultatif) Pour enregistrer la liste des types d'instances dans un fichier de valeurs séparées par des virgules (.csv) pour un examen plus approfondi, choisissez Actions, Télécharger la liste. CSV Le fichier inclut tous les types d'instance qui correspondent aux filtres que vous avez définis.
8. (Facultatif) Pour lancer des instances en utilisant un type d'instance qui répond à vos besoins, cochez la case du type d'instance et choisissez Actions, Launch instance (Lancer l'instance). Pour de plus amples informations, veuillez consulter Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console.

Décrivez un type d'instance à l'aide du AWS CLI

Vous pouvez utiliser la describe-instance-typescommande pour décrire un type d'instance spécifique.

Pour décrire de manière complète un type d'instance

La commande suivante affiche tous les détails disponibles pour le type d'instance spécifié. La sortie est longue, elle est donc omise ici.

```
aws ec2 describe-instance-types \
    --instance-types t2.micro \
    --region us-east-2
```

Ensuite, décrivez un type d'instance et filtrez la sortie

La commande suivante affiche les détails du réseau pour le type d'instance spécifié.

```
aws ec2 describe-instance-types \
    --instance-types t2.micro \
    --region us-east-2 \
    --query "InstanceTypes[].NetworkInfo"
```

Voici un exemple de sortie.

```
[
    {
        "NetworkPerformance": "Low to Moderate",
        "MaximumNetworkInterfaces": 2,
        "MaximumNetworkCards": 1,
        "DefaultNetworkCardIndex": 0,
        "NetworkCards": [
            {
                "NetworkCardIndex": 0,
                "NetworkPerformance": "Low to Moderate",
                "MaximumNetworkInterfaces": 2,
                "BaselineBandwidthInGbps": 0.064,
                "PeakBandwidthInGbps": 1.024
            }
        ],
        "Ipv4AddressesPerInterface": 2,
        "Ipv6AddressesPerInterface": 2,
```

```
        "Ipv6Supported": true,
        "EnaSupport": "unsupported",
        "EfaSupported": false,
        "EncryptionInTransitSupported": false,
        "EnaSrdSupported": false
    }
]
```

La commande suivante affiche la mémoire disponible pour le type d'instance spécifié.

```
aws ec2 describe-instance-types \
    --instance-types t2.micro \
    --region us-east-2 \
    --query "InstanceTypes[].MemoryInfo"
```

Voici un exemple de sortie.

```
[
    {
        "SizeInMiB": 1024
    }
]
```

Trouvez un type d'instance à l'aide du AWS CLI

Vous pouvez utiliser les describe-instance-type-offeringscommandes describe-instance-typeset pour trouver les types d'instances qui répondent à vos besoins.

Exemples

- Exemple 1 : Rechercher un type d'instance par zone de disponibilité
- Exemple 2 : Rechercher un type d'instance en fonction de la taille de mémoire disponible
- Exemple 3 : Rechercher un type d'instance en fonction du stockage d'instance disponible
- Exemple 4 : trouver un type d'instance qui prend en charge l'hibernation

Exemple 1 : Rechercher un type d'instance par zone de disponibilité

L'exemple suivant affiche uniquement les types d'instances proposés dans la zone de disponibilité spécifiée.

```
aws ec2 describe-instance-type-offerings --location-type "availability-zone" \
    --filters "Name=location,Values=us-east-2a" \
    --region us-east-2 \
    --query "InstanceTypeOfferings[*].[InstanceType]" --output text | sort
```

Le résultat est une liste de types d'instances, triés par ordre alphabétique. Ce qui suit est le début de la sortie uniquement.

```
a1.2xlarge
a1.4xlarge
a1.large
a1.medium
a1.metal
a1.xlarge
c4.2xlarge
   ...
```

Exemple 2 : Rechercher un type d'instance en fonction de la taille de mémoire disponible

L'exemple suivant affiche uniquement les types d'instances de la génération actuelle avec 64 GiB (65536 MiB) de mémoire.

```
aws ec2 describe-instance-types \
    --filters "Name=current-generation,Values=true" "Name=memory-info.size-in-
mib,Values=65536" \
    --region us-east-2 \
    --query "InstanceTypes[*].[InstanceType]" --output text | sort
```

Le résultat est une liste de types d'instances, triés par ordre alphabétique. Ce qui suit est le début de la sortie uniquement.

```
c5a.8xlarge
c5ad.8xlarge
c6a.8xlarge
c6g.8xlarge
c6gd.8xlarge
c6gn.8xlarge
c6i.8xlarge
c6id.8xlarge
c6in.8xlarge
   ...
```

Exemple 3 : Rechercher un type d'instance en fonction du stockage d'instance disponible

L'exemple suivant affiche la taille totale du stockage d'instance pour toutes les instances R7 avec des volumes de stockage d'instance.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r7*" "Name=instance-storage-
supported,Values=true" \
    --region us-east-2 \
    --query "InstanceTypes[].[InstanceType, InstanceStorageInfo.TotalSizeInGB]" \
    --output table
```

Voici un exemple de sortie.

```
----------------------------
|  DescribeInstanceTypes   |
+----------------+---------+
|  r7gd.xlarge   |  237    |
|  r7gd.8xlarge  |  1900   |
|  r7gd.16xlarge |  3800   |
|  r7gd.medium   |  59     |
|  r7gd.4xlarge  |  950    |
|  r7gd.2xlarge  |  474    |
|  r7gd.metal    |  3800   |
|  r7gd.large    |  118    |
|  r7gd.12xlarge |  2850   |
+----------------+---------+
```

Exemple 4 : trouver un type d'instance qui prend en charge l'hibernation

L'exemple suivant montre les types d'instances qui prennent en charge l'hibernation.

```
aws ec2 describe-instance-types \
    --filters "Name=hibernation-supported,Values=true" \
    --region us-east-2 \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

Le résultat est une liste de types d'instances, triés par ordre alphabétique. Ce qui suit est le début de la sortie uniquement.

```
c4.2xlarge
```

```
c4.4xlarge
c4.8xlarge
c4.large
c4.xlarge
c5.12xlarge
c5.18xlarge
c5.2xlarge
c5.4xlarge
c5.9xlarge
...
```

Obtenez des recommandations depuis l'outil de recherche de types d'EC2instance

EC2Instance Type Finder prend en compte votre cas d'utilisation, le type de charge de travail, les préférences CPU du fabricant, la façon dont vous hiérarchisez le prix et les performances, ainsi que les paramètres supplémentaires que vous pouvez spécifier. Il utilise ensuite ces données pour fournir des suggestions et des conseils concernant les types d'EC2instances Amazon les mieux adaptés à vos nouvelles charges de travail.

Compte tenu du grand nombre de types d'instances disponibles, trouver les types d'instances adaptés à votre charge de travail peut s'avérer long et complexe. En utilisant l'outil de recherche de types d'EC2instance, vous pouvez rester à jour avec les derniers types d'instances et obtenir le meilleur rapport qualité-prix pour vos charges de travail.

Vous pouvez obtenir des suggestions et des conseils pour les types d'EC2instances à l'aide de la EC2 console Amazon. Vous pouvez également consulter directement Amazon Q pour demander des conseils sur le type d'instance. Pour plus d'informations, consultez le guide de l'utilisateur Amazon Q Developer.

Si vous recherchez des recommandations de type d'instance pour une charge de travail existante, utilisez AWS Compute Optimizer. Pour de plus amples informations, veuillez consulter Obtenez des recommandations EC2 d'instance auprès de Compute Optimizer.

Utiliser le moteur de recherche de type d'EC2instance

Dans la EC2 console Amazon, vous pouvez obtenir des suggestions de types d'instance à partir de l'outil de recherche des types d'EC2instance dans l'assistant de lancement d'instance, lors de la création d'un modèle de lancement ou sur la page des types d'instances.

Suivez les instructions suivantes pour obtenir des suggestions et des conseils sur les types d'EC2instances à l'aide de l'outil de recherche de types d'EC2instance dans la EC2 console Amazon. Pour visionner une animation des étapes, voirAfficher une animation : obtenir des suggestions de types d'instance à l'aide de l'outil de recherche de types d'EC2instance.

Pour obtenir des suggestions de types d'instance à l'aide de l'outil de recherche de types d'EC2instance

1. Démarrez votre processus en utilisant l'une des méthodes suivantes :

   - Suivez la procédure pour lancer une instance. À côté de Type d'instance, cliquez sur le lien Obtenir des conseils.
   - Suivez la procédure pour créer un modèle de lancement. À côté de Type d'instance, cliquez sur le lien Obtenir des conseils.
   - Dans le volet de navigation, choisissez Types d'instances, puis cliquez sur le bouton de recherche de types d'instances.
2. Dans l'écran Obtenir des conseils sur la sélection du type d'instance, procédez comme suit :

   a. Spécifiez vos exigences en matière de type d'instance en sélectionnant les options suivantes : type de charge de travail, cas d'utilisation, priorité et CPUfabricants.

   b. (Facultatif) Pour définir des exigences plus détaillées pour votre charge de travail, procédez comme suit :

      i. Développez les paramètres avancés.

      ii. Pour ajouter un paramètre, sélectionnez-le, choisissez Ajouter et spécifiez une valeur pour le paramètre. Répétez l'opération pour chaque paramètre supplémentaire que vous souhaitez ajouter. Pour n'indiquer aucune valeur minimale ou maximale, laissez le champ vide.

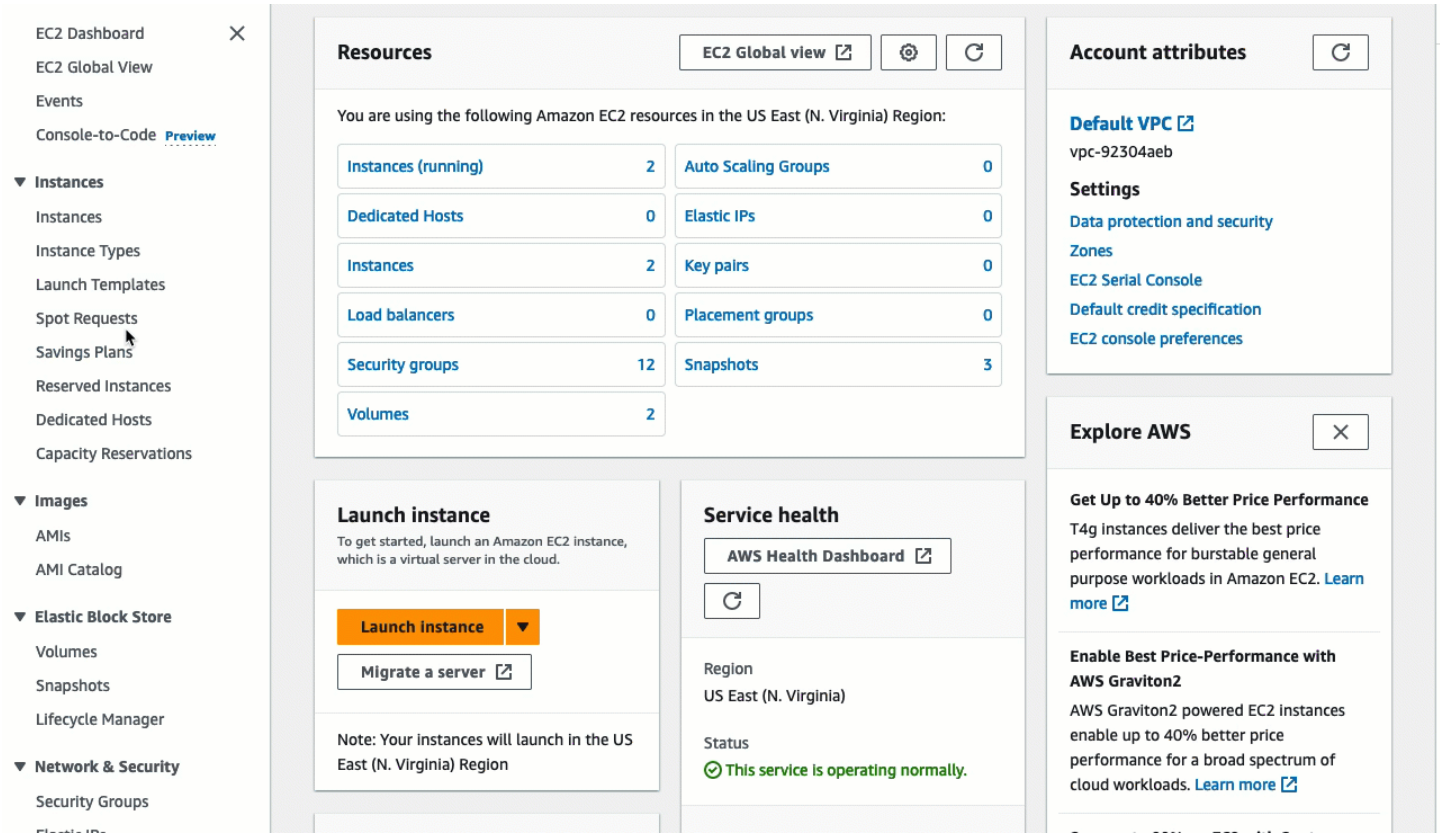
      iii. Pour supprimer un paramètre après l'avoir ajouté, cliquez sur le X à côté du paramètre.

   c. Choisissez Obtenir des conseils sur le type d'instance.

      Amazon vous EC2 propose, par exemple, des familles correspondant à vos besoins spécifiques.
3. Pour afficher les détails de chaque type d'instance au sein des familles d'instances suggérées, choisissez Afficher les détails de la famille d'instances recommandée.
4. Sélectionnez un type d'instance qui répond à vos besoins, puis choisissez Actions, Lancer une instance ou Actions, Créer un modèle de lancement.

Sinon, si vous avez lancé le processus dans l'assistant de lancement d'instance ou sur la page du modèle de lancement, et que vous préférez revenir à votre flux d'origine, notez le type d'instance que vous souhaitez utiliser. Ensuite, dans l'assistant de lancement d'instance ou le modèle de lancement, dans Type d'instance, choisissez le type d'instance et terminez la procédure de lancement d'une instance ou de création d'un modèle de lancement.

Afficher une animation : obtenir des suggestions de types d'instance à l'aide de l'outil de recherche de types d'EC2instance



Obtenez des recommandations EC2 d'instance auprès de Compute Optimizer

AWS Compute Optimizer fournit des EC2 recommandations Amazon pour vous aider à améliorer les performances, à économiser de l'argent, ou les deux. Vous pouvez utiliser ces recommandations pour décider de passer ou non à un nouveau type d'instance.

Pour formuler des recommandations, Compute Optimizer analyse les spécifications et les métriques d'utilisation de vos instances existantes. Les données compilées sont ensuite utilisées pour

recommander les types d'EC2instances Amazon les mieux à même de gérer la charge de travail existante. Les recommandations sont renvoyées avec la tarification horaire des instances. Pour plus d'informations, consultez les métriques relatives aux EC2 instances Amazon dans le guide de AWS Compute Optimizer l'utilisateur.

Table des matières

Prérequis

Pour obtenir des recommandations de Compute Optimizer, vous devez d'abord vous inscrire à Compute Optimizer. Pour plus d'informations, consultez Démarrer avec AWS Compute Optimizer dans le Guide de l'utilisateur AWS Compute Optimizer .

Compute Optimizer génère des recommandations pour certains types d'instances, mais pas pour tous les types d'instance. Si vous utilisez un type d'instance non pris en charge, Compute Optimizer ne générera pas de recommandations. Pour obtenir la liste des types d'instances pris en charge, consultez les exigences relatives aux EC2 instances Amazon dans le guide de AWS Compute Optimizer l'utilisateur.

Trouver des classifications

Compute Optimizer classe ses résultats pour les EC2 instances comme suit :

- Sous-provisionnée : une EC2 instance est considérée comme sous-provisionnée lorsqu'au moins une spécification de votre instance, telle que la mémoire ou le réseauCPU, ne répond pas aux exigences de performance de votre charge de travail. Des EC2 instances sous-provisionnées peuvent nuire aux performances des applications.
- Surprovisionnement : une EC2 instance est considérée comme surprovisionnée lorsqu'au moins une spécification de votre instance, telle que la mémoire ou le réseauCPU, peut être réduite tout en répondant aux exigences de performance de votre charge de travail, et lorsqu'aucune spécification n'est sous-provisionnée. Le surprovisionnement EC2 des instances peut entraîner des coûts d'infrastructure inutiles.

- Optimisée : une EC2 instance est considérée comme optimisée lorsque toutes les spécifications de votre instance, telles que CPU la mémoire et le réseau, répondent aux exigences de performance de votre charge de travail et que l'instance n'est pas surprovisionnée. Une EC2 instance optimisée exécute vos charges de travail avec des performances et des coûts d'infrastructure optimaux. Pour les instances optimisées, Compute Optimizer peut parfois recommander un type d'instance de nouvelle génération.
- None (Aucune) – Aucune recommandation n'est formulée pour cette instance. Cela peut se produire si vous êtes inscrit à Compute Optimizer depuis moins de 12 heures, ou lorsque l'instance s'exécute depuis moins de 30 heures, ou lorsque le type d'instance n'est pas pris en charge par Compute Optimizer.

Afficher les recommandations

Après avoir souscrit à Compute Optimizer, vous pouvez consulter les résultats générés par Compute Optimizer pour EC2 vos instances dans la console Amazon. EC2 Vous pouvez ensuite accéder à la console Compute Optimizer pour afficher les recommandations. Si vous vous êtes inscrit récemment, il est possible que les résultats ne soient pas reflétés dans la EC2 console avant 12 heures.

Pour consulter les recommandations relatives à une instance à l'aide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Choisissez l'ID de l'instance pour ouvrir la page détaillée de l'instance.
4. Sur la page détaillée de l'instance, dans la section récapitulative supérieure, localisez la AWS Compute Optimizer recherche. S'il y a un résultat, nous affichons la classification du résultat et un lien pour afficher les détails. Dans le cas contraire, aucune recommandation n'est disponible pour cette instance.
5. En cas de constatation, choisissez Afficher les détails. Cela ouvre la page Recommandations pour les EC2 instances dans la console Compute Optimizer. Le type d'instance actuel est intitulé Current. Il existe également jusqu'à trois recommandations de type d'instance, intitulées Option 1, Option 2 et Option 3. Cette page affiche également les données CloudWatch métriques récentes de l'instance.

Pour consulter les recommandations pour toutes les instances dans toutes les régions

Vous pouvez consulter les recommandations pour toutes vos EC2 instances Amazon dans toutes les régions à l'aide de la console Compute Optimizer. Pour plus d'informations, consultez les recommandations relatives à l'affichage des EC2 instances et à l'affichage des détails des EC2 instances dans le guide de AWS Compute Optimizer l'utilisateur.

Considérations relatives à l'évaluation des recommandations

Lorsque vous recevez une recommandation, vous devez décider si vous souhaitez y donner suite. Avant de modifier un type d'instance, tenez compte des éléments suivants :

- Les recommandations ne prévoient pas votre utilisation. Les recommandations sont basées sur votre historique d'utilisation au cours de la période de 14 jours la plus récente. Veillez à choisir un type d'instance censé répondre à vos futurs besoins en termes de ressources.
- Concentrez-vous sur le graphique des métriques pour déterminer si l'utilisation réelle est inférieure à la capacité d'instance. Vous pouvez également consulter les données métriques (moyenne, pic, percentile) afin d'évaluer plus en détail CloudWatch les recommandations relatives à votre EC2 instance. Par exemple, observez l'évolution des indicateurs en CPU pourcentage au cours de la journée et déterminez s'il y a des pics qui doivent être pris en compte. Pour plus d'informations, consultez la section Affichage des métriques disponibles dans le guide de CloudWatch l'utilisateur Amazon.
- Compute Optimizer peut fournir des recommandations pour les instances de performance à capacité extensible, à savoir les instances T3, T3a et T2. Si vous dépassez régulièrement la ligne de base, assurez-vous de pouvoir continuer à le faire en fonction vCPUs du nouveau type d'instance. Pour de plus amples informations, veuillez consulter Concepts clés pour les instances de performance éclatantes.
- Si vous avez acheté une Instance réservée, votre instance à la demande peut être facturée au prix d'une Instance réservée. Avant de modifier votre type d'instance actuel, commencez par évaluer l'impact sur l'utilisation et la couverture de l'Instance réservée.
- Dans la mesure du possible, envisagez des conversions vers des instances de nouvelle génération.
- Lors de la migration vers une autre famille d'instances, assurez-vous que le type d'instance actuel et le nouveau type d'instance sont compatibles, en termes de virtualisation, d'architecture ou de type de réseau par exemple. Pour plus d'informations, consultez Compatibilité pour modifier le type d'instance.
- Enfin, tenez compte de la note de risque de performances fournie pour chaque recommandation. Le risque de performances correspond à l'effort que vous pourriez avoir à consacrer pour valider si

le type d'instance recommandé répond aux exigences de performances de votre charge de travail. Nous recommandons également des tests rigoureux de charge et de performance avant et après toute modification.

Changements de type d'EC2instance Amazon

Au fur et à mesure que vos besoins évoluent, il se peut que vous constatiez que votre instance est sur-utilisée (le type d'instance est trop petit) ou sous-utilisée (le type d'instance est trop grand). Si tel est le cas, vous pouvez redimensionner votre instance en modifiant son type d'instance. Par exemple, si votre instance `t2.micro` est trop petite pour sa charge de travail, vous pouvez augmenter sa taille en la remplaçant par un type d'instance T2 plus volumineux, comme `t2.large`. Vous pouvez également la remplacer par un autre type d'instance, par exemple `m5.large`. Vous souhaiterez peut-être également passer d'un type d'instance de génération précédente à un type d'instance de génération actuelle afin de tirer parti de certaines fonctionnalités, telles que la prise en charge deIPv6.

Si vous souhaitez une recommandation du type d'instance le mieux à même de gérer votre charge de travail existante, vous pouvez utiliser AWS Compute Optimizer. Pour de plus amples informations, veuillez consulter Obtenez des recommandations EC2 d'instance auprès de Compute Optimizer.

Lorsque vous modifiez le type d'instance, vous commencez à payer le taux du nouveau type. Pour connaître les tarifs à la demande pour tous les types d'instances, consultez EC2la tarification Amazon On-Demand.

Pour ajouter de l'espace de stockage à votre instance sans modifier le type d'instance, ajoutez-y un EBS volume. Pour plus d'informations, consultez la section Attacher un EBS volume Amazon à une instance dans le guide de EBS l'utilisateur Amazon.

Quelles sont les instructions à suivre ?

Il existe différentes instructions pour la modification du type d'instance. Les instructions à suivre dépendent du volume racine de l'instance et de la compatibilité du type d'instance avec la configuration actuelle de l'instance. Pour en savoir plus sur la façon dont la compatibilité est déterminée, consultez Compatibilité pour modifier le type d'instance.

Utilisez le tableau suivant pour déterminer quelles instructions suivre.

Volume racine	Compatibilité	Suivez ces instructions
EBS	Compatible	Modifier le type d'instance
EBS	Non compatible	Migrer vers un nouveau type d'instance
Stockage d'instances	Ne s'applique pas	Migrer vers un nouveau type d'instance

Compatibilité pour modifier le type d'instance

Vous pouvez modifier le type d'instance uniquement si la configuration actuelle de l'instance est compatible avec le type d'instance souhaité. Si le type d'instance souhaité n'est pas compatible avec votre configuration actuelle d'instance, vous devez lancer une nouvelle instance dotée d'une configuration compatible avec le type d'instance, puis migrer votre application vers la nouvelle instance.

La compatibilité est déterminée de la manière suivante :

Type de virtualisation

Linux AMIs utilise l'un des deux types de virtualisation suivants : paravirtuelle (PV) ou machine virtuelle matérielle (HVM). Si une instance a été lancée à partir d'un PVAMI, vous ne pouvez pas passer à un type d'instance HVM uniquement. Pour de plus amples informations, veuillez consulter Types de virtualisation. Pour vérifier le type de virtualisation de votre instance, vérifiez la valeur de virtualisation dans le volet des détails de l'écran Instances de la EC2 console Amazon.

Architecture

AMIssont spécifiques à l'architecture du processeur. Vous devez donc sélectionner un type d'instance avec la même architecture de processeur que le type d'instance actuel. Par exemple :

- Si le type d'instance actuel est doté d'un processeur basé sur l'architecture Arm, vous êtes limité aux types d'instance qui prennent en charge un processeur basé sur l'architecture Arm, notamment C6g et M6g.
- Les types d'instance suivants sont les seuls à prendre en charge le 32 bits AMIs : `t2.nano`t2.micro,`t2.small`,`t2.medium`,`c3.large`,`t1.micro`, `m1.small`m1.medium, etc1.medium. Si vous modifiez le type d'une instance 32 bits, vous êtes limité à ces types d'instance.

Cartes réseau

Si vous passez d'un pilote d'une carte réseau à un autre, les paramètres de la carte réseau sont réinitialisés lorsque le système d'exploitation crée la nouvelle carte. Pour reconfigurer les paramètres, vous devrez peut-être accéder à un compte local doté d'autorisations d'administrateur. Voici des exemples de déplacement d'une carte réseau à une autre :

- AWS PV (instances T2) vers Intel 82599 VF (instances M4)
- Intel 82599 VF (la plupart des instances M4) à ENA (instances M5)
- ENA(instances M5) à bande passante élevée ENA (instances M5n)

Cartes réseau

Certains types d'instance prennent en charge plusieurs cartes réseau. Vous devez sélectionner un type d'instance prenant en charge le même nombre de cartes réseau que le type d'instance actuel.

Réseaux améliorés

Les types d'instance prenant en charge les réseaux améliorés nécessitent l'installation des pilotes requis. Par exemple, les instances créées sur le système AWS Nitro doivent être EBS sauvegardées AMIs avec les pilotes Elastic Network Adapter (ENA) installés. Pour passer d'un type d'instance qui ne prend pas en charge la mise en réseau améliorée à un type d'instance qui prend en charge la mise en réseau améliorée, vous devez installer les ENApilotes ou les pilotes ixgbevf sur l'instance, selon le cas.

> **Note**
>
> Lorsque vous redimensionnez une instance avec ENA Express activé, le nouveau type d'instance doit également prendre en charge ENA Express. Pour obtenir la liste des types d'instances compatibles avec ENA Express, consultezTypes d'instances pris en charge pour ENA Express.
> Pour passer d'un type d'instance compatible avec ENA Express à un type d'instance qui ne le prend pas en charge, assurez-vous qu'ENAExpress n'est pas activé actuellement avant de redimensionner l'instance.

NVMe

EBSles volumes sont exposés sous forme de NVMe blocs sur des instances créées sur le système AWS Nitro. Si vous passez d'un type d'instance non compatible NVMe à un type

d'instance compatibleNVMe, vous devez d'abord installer les NVMe pilotes sur votre instance. En outre, les noms des appareils que vous spécifiez dans le mappage des périphériques par blocs sont renommés à l'aide des noms de NVMe périphériques (`/dev/nvme[0-26]n1`).

[Instances Linux] Par conséquent, pour monter des systèmes de fichiers au démarrage à l'aide de /Label`/etc/fstab`, vous devez utiliser UUID /Label au lieu des noms de périphériques.

Limite de volume

Le nombre maximum de EBS volumes Amazon que vous pouvez attacher à une instance dépend du type et de la taille de l'instance. Pour de plus amples informations, veuillez consulter Limites EBS de volume Amazon pour les EC2 instances Amazon.

Vous pouvez uniquement passer à un type ou à une taille d'instance qui prend en charge le même nombre ou un plus grand nombre de volumes que celui qui est actuellement attaché à l'instance. Si vous optez pour un type d'instance ou une taille d'instance qui ne prend pas en charge le nombre de volumes actuellement attachés, la demande échoue. Par exemple, si vous passez d'une instance `m7i.4xlarge` avec 32 volumes attachés à une instance `m6i.4xlarge`, qui prend en charge un maximum de 27 volumes, la demande échoue.

Nitro TPM

Si vous avez lancé l'instance en utilisant un type d'instance AMI avec Nitro TPM activé et un type d'instance compatible avec NitroTPM, l'instance est lancée avec TPM Nitro activé. Vous ne pouvez passer qu'à un type d'instance qui prend également en charge NitroTPM.

Modifier le type d'instance de votre EC2 instance Amazon

Suivez les instructions suivantes pour modifier le type d'instance d'une instance basée sur Amazon EBS si le type d'instance dont vous avez besoin est compatible avec la configuration actuelle de votre instance. Pour de plus amples informations, veuillez consulter the section called "Compatibilité".

Considérations

- Vous devez arrêter votre instance avant de pouvoir modifier son type d'instance. Veillez à prévoir un temps d'arrêt pendant que votre instance est arrêtée. L'arrêt d'une instance et la modification de son type peuvent prendre quelques minutes, et la durée du redémarrage de votre instance peut varier en fonction des scripts de démarrage de votre application. Pour plus d'informations, consultez Arrêtez et démarrez les EC2 instances Amazon.

- Lorsque vous arrêtez et démarrez une instance, nous déplaçons l'instance vers un nouveau matériel. Si votre instance possède une IPv4 adresse publique qui n'est pas une adresse IP élastique, nous publions l'adresse et attribuons une nouvelle IPv4 adresse publique à votre instance. Pour plus d'informations sur le comportement des adresses IP tout au long du cycle de vie d'une instance, consultezDifférences entre les états des instances.
- Vous ne pouvez pas modifier le type d'instance d'une instance Spot.
- [Instances Windows] Nous vous recommandons de mettre à jour le package de pilotes AWS PV avant de modifier le type d'instance. Pour de plus amples informations, veuillez consulter the section called "Mettre à niveau les pilotes PV".
- Si votre instance fait partie d'un groupe Auto Scaling, le service Amazon EC2 Auto Scaling indique que l'instance arrêtée est défectueuse et peut la mettre hors service et lancer une instance de remplacement. Pour empêcher que cela ne se produise, vous pouvez suspendre les processus de mise à l'échelle pour le groupe pendant que vous modifiez le type d'instance. Pour plus d'informations, consultez la section Suspendre et reprise d'un processus pour un groupe Auto Scaling dans le guide de l'utilisateur d'Amazon EC2Auto Scaling.
- Lorsque vous modifiez le type d'instance d'une instance avec des volumes de stockage d'NVMeinstance, l'instance mise à jour peut avoir des volumes de stockage d'instance supplémentaires, car tous les volumes de stockage d'NVMeinstance sont disponibles même s'ils ne sont pas spécifiés dans le AMI mappage des périphériques par blocs d'instances. Autrement, l'instance mise à jour a le même nombre de volumes de stockage d'instances que celui spécifié lors du lancement de l'instance initiale.
- Le nombre maximum de EBS volumes Amazon que vous pouvez attacher à une instance dépend du type et de la taille de l'instance. Vous ne pouvez pas passer à un type ou à une taille d'instance qui ne prennent pas en charge le nombre de volumes déjà attachés à votre instance. Pour de plus amples informations, veuillez consulter Limites EBS de volume Amazon pour les EC2 instances Amazon.
- [Instances Linux] Vous pouvez utiliser le `AWSSupport-MigrateXenToNitroLinux` runbook pour migrer des instances Linux compatibles d'un type d'instance Xen vers un type d'instance Nitro. Pour plus d'informations, consultez AWSSupport-MigrateXenToNitroLinux runbook dans la référence AWS Systems Manager Automation runbook.
- [Instances Windows] Pour obtenir des conseils supplémentaires sur la migration d'instances Windows compatibles d'un type d'instance Xen vers un type d'instance Nitro, voir Migrer vers des types d'instances de dernière génération.

Pour modifier le type d'instance d'une instance basée sur Amazon EBS

1. (Facultatif) Si le nouveau type d'instance requiert des pilotes qui ne sont pas installés sur l'instance existante, vous devez vous connecter à votre instance et installer les pilotes. Pour de plus amples informations, veuillez consulter Compatibilité pour modifier le type d'instance.
2. [Instances Windows] Si vous avez configuré votre instance Windows pour utiliser l'adressage IP statique et que vous passez d'un type d'instance qui ne prend pas en charge la mise en réseau améliorée à un type d'instance prenant en charge la mise en réseau améliorée, vous pouvez recevoir un avertissement concernant un conflit d'adresses IP potentiel lorsque vous reconfigurez l'adressage IP statique. Pour éviter cela, activez-la DHCP sur l'interface réseau de votre instance avant de modifier le type d'instance. Depuis votre instance, ouvrez le Centre de réseau et de partage, ouvrez les propriétés du protocole Internet version 4 (TCP/IPv4) pour l'interface réseau, puis choisissez Obtenir une adresse IP automatiquement. Modifiez le type d'instance et reconfigurez l'adressage IP statique sur l'interface réseau.
3. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
4. Dans le panneau de navigation, choisissez Instances.
5. Sélectionnez l'instance et choisissez Instance state (État de l'instance), Stop instance (Arrêter l'instance). Lorsque vous êtes invité à confirmer l'opération, choisissez Stop (Arrêter). L'arrêt de l'instance peut prendre quelques minutes.
6. Tandis que l'instance est toujours sélectionnée, choisissez Actions, Instance settings (Paramètres de l'instance), puis Change instance type (Changer le type d'instance). Cette action est grisée si l'état de l'instance n'est pas `stopped`.
7. Sur la page Change instance type (Modifier le type d'instance), procédez comme suit :

   a. Dans Instance type (Type d'instance), sélectionnez le type d'instance souhaité.

      Si le type d'instance ne figure pas dans la liste, il n'est pas compatible avec la configuration de votre instance. Au lieu de cela, suivez les instructions suivantes : Migrer vers un nouveau type d'instance en lançant une nouvelle EC2 instance.

   b. (Facultatif) Si le type d'instance que vous avez sélectionné prend en charge EBS l'optimisation, sélectionnez EBS-optimized pour activer EBS l'optimisation ou désélectionnez EBS-optimized pour désactiver l'optimisation. EBS Si le type d'instance que vous avez sélectionné est EBS optimisé par défaut, EBS-optimized est sélectionné et vous ne pouvez pas le désélectionner.

   c. Choisissez Apply (Appliquer) pour accepter les nouveaux paramètres.

8. Pour démarrer l'instance, sélectionnez l'instance et choisissez Instance state (État de l'instance), Start instance (Démarrer l'instance). Il peut s'écouler quelques minutes avant que l'instance ne passe à l'état `running`. Si votre instance ne démarre pas, consultez la section Résoudre les problèmes de modification du type d'instance.
9. [Instances Windows] Si votre instance exécute Windows Server 2016 ou Windows Server 2019 avec EC2Launch v1, connectez-vous à votre instance Windows et exécutez le EC2Launch PowerShell script suivant pour configurer l'instance une fois le type d'instance modifié.

> **Important**
>
> Le mot de passe administrateur est réinitialisé lorsque vous activez le script de EC2 lancement de l'instance d'initialisation. Vous pouvez modifier le fichier de configuration pour désactiver la réinitialisation du mot de passe administrateur en le spécifiant dans les paramètres des tâches d'initialisation. Pour savoir comment désactiver la réinitialisation du mot de passe, voir Configurer les tâches d'initialisation (EC2Launch) ou Modifier les paramètres (EC2Launchv2).

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

Migrer vers un nouveau type d'instance en lançant une nouvelle EC2 instance

Vous ne pouvez modifier le type d'instance d'une EC2 instance que s'il s'agit d'une instance EBS basée sur un support dont la configuration est incompatible avec le nouveau type d'instance que vous souhaitez. Sinon, si la configuration ou votre instance n'est pas compatible avec le nouveau type d'instance, ou s'il s'agit d'une instance basée sur un magasin d'instances, vous devez lancer une instance de remplacement compatible avec le type d'instance que vous souhaitez. Pour plus d'informations sur la manière dont la compatibilité est déterminée, consultezCompatibilité pour modifier le type d'instance.

Présentation du processus de migration

- Sauvegardez les données de l'instance d'origine.
- Lancez une nouvelle instance avec une configuration compatible avec le nouveau type d'instance que vous souhaitez, en attachant tous les EBS volumes attachés à votre instance d'origine.

- Installez votre application sur votre nouvelle instance.
- Restaurez toutes les données.
- Si l'instance d'origine possède une adresse IP élastique, vous devez l'associer à votre nouvelle instance pour que vos utilisateurs puissent continuer à utiliser votre application sans interruption.

Pour migrer une instance vers une nouvelle instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Sauvegardez toutes les données dont vous avez encore besoin comme suit :
   - Connectez-vous à votre instance et copiez les données des volumes de stockage de votre instance vers un stockage persistant.
   - Créez des instantanés de vos EBS volumes afin de créer de nouveaux volumes avec les mêmes données, ou détachez les volumes de l'instance d'origine afin de pouvoir les associer à la nouvelle instance.
3. Dans le panneau de navigation, choisissez Instances.
4. Sélectionnez Launch instances (Lancer des instances). Lorsque vous configurez l'instance, procédez comme suit :
   a. Sélectionnez une AMI instance compatible avec le type d'instance que vous souhaitez. Par exemple, vous devez sélectionner un AMI processeur compatible avec le type de processeur du nouveau type d'instance. En outre, les types d'instances de la génération actuelle nécessitent un HVMAMI.
   b. Sélectionnez le nouveau type d'instance souhaité. Si le type d'instance que vous souhaitez n'est pas disponible, il n'est pas compatible avec la configuration de AMI celle que vous avez sélectionnée.
   c. Si vous souhaitez autoriser le même trafic à atteindre la nouvelle instance, sélectionnez le même groupe VPC de sécurité que celui utilisé avec l'instance d'origine.
   d. Une fois que vous avez terminé la configuration de votre nouvelle instance, effectuez les étapes pour sélectionner une paire de clés et lancer votre instance. Il peut s'écouler quelques minutes avant que l'instance ne passe à l'état `running`.
5. Si vous avez sauvegardé des données sur un EBS instantané, créez un volume à partir de cet instantané, puis attachez le volume à la nouvelle instance.

Pour déplacer un EBS volume de l'instance d'origine vers la nouvelle instance, détachez le volume de l'instance d'origine, puis attachez le volume à la nouvelle instance.

6. Installez votre application et les logiciels requis sur la nouvelle instance.
7. Restaurez les données que vous avez sauvegardées depuis les volumes de stockage d'instances de l'instance d'origine.
8. Si l'instance d'origine possède une adresse IP élastique, attribuez-la à la nouvelle instance comme suit :

   a. Dans le volet de navigation, sélectionnez Elastic IPs.

   b. Sélectionnez l'adresse IP Elastic associée à l'instance d'origine, choisissez Actions, puis Dissocier l'adresse IP Elastic. Sélectionnez Dissocier lorsque vous êtes invité à confirmer l'opération.

   c. L'adresse IP Elastic étant toujours sélectionnée, choisissez Actions, puis Associer l'adresse IP Elastic.

   d. Pour Resource type (Type de ressource), choisissez Instance.

   e. Par exemple, choisissez la nouvelle instance.

   f. (Facultatif) Pour Private IP address (Adresse IP privéeù), spécifiez une adresse IP privée à laquelle associer l'adresse IP Elastic.

   g. Choisissez Associate.

9. (Facultatif) Vous pouvez terminer l'instance d'origine si elle n'est plus nécessaire. Sélectionnez l'instance, vérifiez que vous êtes sur le point de résilier l'instance d'origine, et non la nouvelle instance (par exemple, vérifiez le nom ou l'heure du lancement), puis sélectionnez Instance state (État de l'instance), Terminate instance (Résilier l'instance).

Résoudre les problèmes de modification du type d'instance

Utilisez les informations suivantes pour identifier et résoudre les problèmes que vous pouvez rencontrer lorsque vous modifiez le type d'instance.

L'instance ne démarre pas après avoir modifié le type d'instance

Cause possible : les exigences relatives au nouveau type d'instance ne sont pas satisfaites

Si votre instance ne démarre pas, il est possible qu'une des exigences pour le nouveau type d'instance n'ait pas été respectée. Pour plus d'informations, consultez la section relative à la raison pour laquelle mon instance Linux ne démarre pas après que j'ai modifié son type.

Cause possible : AMI ne prend pas en charge le type d'instance

Si vous utilisez la EC2 console pour modifier le type d'instance, seuls les types d'instance pris en charge par l'instance sélectionnée AMI sont disponibles. Toutefois, si vous utilisez le AWS CLI pour lancer une instance, vous pouvez spécifier un type AMI d'instance incompatible. Si le type d'instance AMI et sont incompatibles, l'instance ne peut pas démarrer. Pour de plus amples informations, veuillez consulter Compatibilité pour modifier le type d'instance.

Cause possible : l'instance se trouve dans un groupe de placement du cluster

Si votre instance se trouve dans un groupe de placement du cluster et, qu'après avoir modifié le type d'instance, l'instance ne démarre pas, essayez ce qui suit :

1. Arrêtez toutes les instances du groupe de placement du cluster.
2. Modifiez le type de l'instance en question.
3. Démarrez toutes les instances du groupe de placement du cluster.

L'application ou le site web n'est pas accessible depuis Internet après avoir modifié le type d'instance

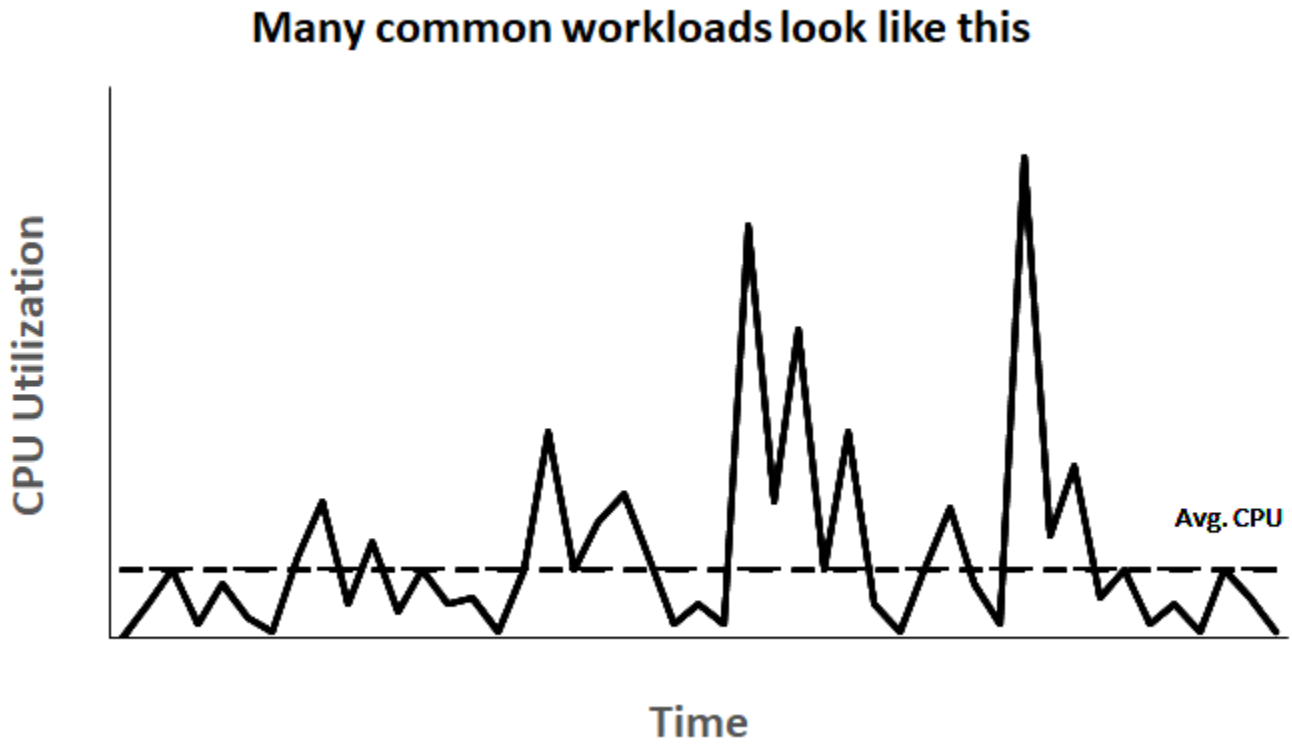
Cause possible : l'IPv4adresse publique est publiée

Lorsque vous modifiez le type d'instance, vous devez d'abord arrêter l'instance. Lorsque vous arrêtez une instance, nous publions l'IPv4adresse publique et attribuons une nouvelle IPv4 adresse publique à votre instance.

Pour conserver l'IPv4adresse publique entre les arrêts et les démarrages de l'instance, nous vous recommandons d'utiliser une adresse IP élastique, sans frais supplémentaires, à condition que votre instance soit en cours d'exécution. Pour de plus amples informations, veuillez consulter Adresses IP Elastic.

Instances de performance à capacité extensible

De nombreuses charges de travail à usage général ne sont en moyenne pas surchargées et ne nécessitent pas un niveau élevé de CPU performance soutenue. Le graphique suivant illustre l'CPUutilisation de nombreuses charges de travail courantes que les clients exécutent aujourd'hui dans le AWS cloud.



Ces charges de travail d' low-to-moderate CPUutilisation entraînent un gaspillage de CPU cycles et, par conséquent, vous payez plus que ce que vous utilisez. Pour surmonter ce problème, vous pouvez tirer parti des instances polyvalentes extensibles économiques que sont les instances T.

La famille d'instances T fournit des CPU performances de base avec la capacité de dépasser la ligne de base à tout moment et aussi longtemps que nécessaire. La base de référence CPU est définie pour répondre aux besoins de la majorité des charges de travail à usage général, notamment les microservices à grande échelle, les serveurs Web, les petites et moyennes bases de données, l'enregistrement des données, les référentiels de code, les bureaux virtuels, les environnements de développement et de test et les applications critiques pour l'entreprise. Les instances T offrent un équilibre entre les ressources de calcul, de mémoire et de réseau, et constituent le moyen le plus rentable d'exécuter un large éventail d'applications à usage général qui ont un low-to-moderate CPU usage. Elles peuvent vous faire économiser jusqu'à 15 % par rapport aux instances M, et peuvent

vous permettre de réaliser encore plus d'économies grâce à des tailles d'instance plus petites vCPUs et plus économiques, offrant seulement 2 ou 0,5 GiB de mémoire. Les plus petites tailles d'instance T, telles que nano, micro, petite et moyenne, conviennent parfaitement aux charges de travail qui nécessitent une petite quantité de mémoire et ne prévoient pas une CPU utilisation élevée.

> **Note**
>
> Cette rubrique décrit Burstable. CPU Pour plus d'informations sur les performances réseau extensibles, consultez Bande passante réseau des EC2 instances Amazon.

EC2types d'instances éclatables

Les instances EC2 burstables se composent des types d'instances T4g, T3a et T3, ainsi que des types d'instances T2 de la génération précédente.

Les types d'instances T4g sont la dernière génération d'instances extensibles. Ils offrent le meilleur rapport qualité-prix en termes de performances et vous offrent le coût le plus bas de tous les types d'EC2instances. Les types d'instances T4g sont alimentés par des processeurs AWS Graviton2 basés sur ARM bénéficiant d'une prise en charge complète de l'écosystème par des fournisseurs de systèmes d'exploitation, des fournisseurs de logiciels indépendants et des services et applications populaires AWS .

Le tableau suivant récapitule les principales différences entre les types d'instances extensibles.

Type	Description	Famille de processeurs
Dernière génération		
T4g	Type d'EC2instance le moins coûteux avec un rapport prix/performances jusqu'à 40 % plus élevé et des coûts inférieurs de 20 % par rapport à l'instance T3	AWS Processeurs Graviton2 avec cœurs Arm Neoverse N1
T3a	instances basées sur x86 les moins coûteuses à des coûts	AMDEPYCProcesseurs de 1re génération

Type	Description	Famille de processeurs
	inférieurs de 10 % par rapport à des instances T3	
T3	Meilleur rapport prix/performances maximales pour les charges de travail x86, jusqu'à 30 % inférieur à celui d'instances T2 de génération précédente	Intel Xeon Scalable (processeurs Skylake, Cascade Lake)
Génération précédente		
T2	instances extensibles de génération précédente	Processeurs Intel Xeon

Pour plus d'informations sur la tarification des instances et les spécifications supplémentaires, consultez Amazon EC2 Pricing et Amazon EC2 Instance Types. Pour plus d'informations sur les performances réseau extensibles, consultez Bande passante réseau des EC2 instances Amazon.

Si votre compte a moins de 12 mois, vous pouvez utiliser une instance `t2.micro` gratuitement (ou une instance `t3.micro` dans les régions où `t2.micro` n'est pas disponible) dans certaines limites d'utilisation. Pour de plus amples informations, veuillez consulter Niveau gratuit d'AWS.

Options d'achat prises en charge pour les instances T

- On-Demand instances
- Reserved instances
- instances dédiées (T3 uniquement)
- Hôtes dédiés (T3 uniquement, uniquement dans le mode `standard`)
- Spot instances

Pour plus d'informations, consultez Options EC2 de facturation et d'achat Amazon.

Sommaire

Bonnes pratiques

Suivez ces bonnes pratiques pour tirer le meilleur profit et la plus grande satisfaction des instances de performance à capacité extensible

- Assurez-vous que la taille d'instance que vous choisissez correspond à la configuration minimum requise en matière de mémoire par votre système d'exploitation et vos applications. Les systèmes d'exploitation dotés d'interfaces utilisateur graphiques consommant beaucoup de mémoire et de CPU ressources (par exemple, Windows) peuvent nécessiter une taille d'instance `t3.micro` ou plus grande dans de nombreux cas d'utilisation. À mesure que la mémoire et les CPU exigences de votre charge de travail augmentent au fil du temps, les instances T vous permettent de vous adapter à des tailles d'instance plus importantes du même type d'instance ou de sélectionner un autre type d'instance.
- Activez AWS Compute Optimizer pour votre compte, et consultez les recommandations de Compute Optimizer pour votre charge de travail. Compute Optimizer peut vous aider à évaluer l'opportunité d'augmenter la taille des instances pour améliorer les performances, ou de la diminuer pour réduire les coûts. Compute Optimizer peut également recommander un type d'instance différent en fonction de votre scénario. Pour plus d'informations, consultez la section Affichage des recommandations relatives aux EC2 instances dans le Guide de AWS Compute Optimizer l'utilisateur.

Concepts clés pour les instances de performance éclatantes

Les types d'EC2instances Amazon traditionnels fournissent des CPU ressources fixes, tandis que les instances à performances optimisées fournissent un niveau d'CPUutilisation de base avec la possibilité d'augmenter le CPU taux d'utilisation au-dessus du niveau de référence. Cela garantit que vous ne payez que pour la base de référence, CPU plus toute CPU utilisation supplémentaire en rafale, ce qui se traduit par une réduction des coûts de calcul. L'utilisation de base et la capacité à exploser sont régies par CPU des crédits. Les instances Burstable Performance sont les seuls types d'instances qui utilisent des crédits d'CPUutilisation.

Chaque instance de performance éclatante gagne continuellement des crédits lorsqu'elle reste en dessous du CPU niveau de référence, et dépense continuellement des crédits lorsqu'elle dépasse le niveau de référence. Le montant des crédits gagnés ou dépensés dépend de l'CPUutilisation de l'instance :

- Si l'CPUutilisation est inférieure au niveau de référence, les crédits gagnés sont supérieurs aux crédits dépensés.
- Si l'CPUutilisation est égale à la valeur de référence, les crédits gagnés sont égaux aux crédits dépensés.
- Si l'CPUutilisation est supérieure au niveau de référence, les crédits dépensés sont supérieurs aux crédits gagnés.

Lorsque les crédits gagnés sont supérieurs aux crédits dépensés, la différence est appelée crédits accumulés, qui peuvent être utilisés ultérieurement pour dépasser le taux d'utilisation de baseCPU. De même, quand les crédits dépensés sont supérieurs aux crédits gagnés, le comportement de l'instance dépend selon que le crédit est configuré en mode Standard ou Illimité.

En mode standard, lorsque les crédits dépensés sont supérieurs aux crédits gagnés, l'instance utilise les crédits accumulés pour dépasser le taux d'utilisation de baseCPU. S'il ne reste plus de crédits accumulés, l'instance revient progressivement à son niveau d'CPUutilisation de base et ne peut pas dépasser le niveau de référence tant qu'elle n'a pas accumulé plus de crédits.

En mode illimité, si l'instance dépasse le taux d'CPUutilisation de base, elle utilise d'abord les crédits accumulés pour exploser. S'il n'en reste pas, l'instance dépense des crédits excédentaires. Lorsque son CPU utilisation tombe en dessous du niveau de référence, elle utilise les CPU crédits qu'elle gagne pour rembourser les crédits excédentaires qu'elle a dépensés plus tôt. La possibilité de gagner des CPU crédits pour rembourser les crédits excédentaires permet EC2 à Amazon de calculer la moyenne d'CPUutilisation d'une instance sur une période de 24 heures. Si l'CPUutilisation moyenne sur une période de 24 heures dépasse le niveau de référence, l'instance est facturée pour l'utilisation supplémentaire à un par heureCPU.

Table des matières

- Durée de vie des CPU crédits accumulés
- Utilisation de référence

Concepts clés et définitions

Les concepts clés et définitions qui suivent s'appliquent aux instances de performance à capacité extensible.

CPUutilisation

CPUl'utilisation est le pourcentage d'unités de EC2 calcul allouées actuellement utilisées sur l'instance. Cette métrique mesure le pourcentage de CPU cycles alloués utilisés sur une instance. La CloudWatch métrique CPU d'utilisation indique CPU l'utilisation par instance et non CPU l'utilisation par cœur. La CPU spécification de base d'une instance est également basée sur l'CPUutilisation par instance. Pour mesurer CPU l'utilisation à l'aide du AWS Management Console ou du AWS CLI, voirObtenir les statistiques d'une instance spécifique.

CPUcrédit

Unité de v CPU -time.

Exemples :

1 CPU crédit = 1 v CPU * 100 % d'utilisation * 1 minute.

1 CPU crédit = 1 v CPU * 50 % d'utilisation * 2 minutes

1 CPU crédit = 2 v CPU * 25 % d'utilisation * 2 minutes

Utilisation de référence

L'utilisation de base est le niveau auquel le solde créditeur net CPU peut être égal à zéro, lorsque le nombre de CPU crédits gagnés correspond au nombre de CPU crédits utilisés. L'utilisation de référence est également appelée la référence. L'utilisation de base est exprimée en pourcentage de CPU l'utilisation de v, qui est calculé comme suit : % d'utilisation de référence = (nombre de crédits gagnés/nombre devCPUs) /60 minutes.

Pour connaître l'utilisation de référence de chaque type d'instance à capacité extensible, consultez le tableau des crédits.

Crédits gagnés

Crédits gagnés par une instance pendant son exécution.

Nombre de crédits gagnés par heure = % d'utilisation de base * nombre de vCPUs * 60 minutes

Exemple :

Un t3.nano avec 2 vCPUs et une utilisation de base de 5 % rapporte 6 crédits par heure, calculés comme suit :

2 vCPUs x 5 % de référence * 60 minutes = 6 crédits par heure

Crédits dépensés ou utilisés

Crédits utilisés par une instance pendant son exécution.

CPUcrédits dépensés par minute = Nombre de vCPUs * CPU utilisation * 1 minute

Crédits accumulés

CPUCrédits non dépensés lorsqu'une instance utilise moins de crédits que ce qui est requis pour l'utilisation de base. En d'autres termes, les crédits accumulés = (crédits gagnés - crédits utilisés) inférieurs à la base de référence.

Exemple :

Si un t3.nano fonctionne à 2 % d'CPUutilisation, ce qui est inférieur à sa valeur de référence de 5 % pendant une heure, les crédits accumulés sont calculés comme suit :

Crédits accumulés = (CPUcrédits gagnés par heure — crédits utilisés par heure) = 6 — 2 vCPUs * 2 % d'CPUutilisation * 60 minutes = 6 — 2,4 = 3,6 crédits accumulés par heure

Limite d'accumulation de crédit

Dépend de la taille de l'instance mais, en général, est égale au nombre maximum de crédits gagnés en 24 heures.

Exemple :

Pour t3.nano, la limite d'accumulation de crédit = 24 * 6 = 144 crédits

Crédits de lancement

Applicables uniquement pour des instances T2 configurées pour le mode Standard. Les crédits de lancement sont un nombre limité de CPU crédits alloués à une nouvelle instance T2 afin que, lorsqu'elle est lancée en mode Standard, elle puisse dépasser le niveau de référence.

Crédits excédentaires

Crédits dépensés par une instance après qu'elle a épuisé son solde de crédits accumulés. Les crédits excédentaires sont conçus pour permettre à des instances extensibles de soutenir des performances élevées pendant une période prolongée, et ne sont utilisés qu'en mode Illimité. Le solde de crédits excédentaires est utilisé pour déterminer combien de crédits l'instance a utilisés pour dépasser la ligne de référence en mode Illimité.

Mode Standard

Mode de configuration du crédit permettant à une instance de dépasser sa ligne de référence en dépensant les crédits accumulés dans son solde de crédit.

Mode Illimité

Mode de configuration du crédit, qui permet à une instance de dépasser le niveau de référence en maintenant un taux d'CPUutilisation élevé pendant n'importe quelle période, chaque fois que cela est nécessaire. Le prix horaire de l'instance couvre automatiquement tous les pics CPU d'utilisation si l'CPUutilisation moyenne de l'instance est égale ou inférieure à la valeur de référence sur une période continue de 24 heures ou sur la durée de vie de l'instance, la période la plus courte étant retenue. Si l'instance fonctionne à un taux d'CPUutilisation plus élevé pendant une période prolongée, elle peut le faire moyennant un par heure.

Le tableau suivant récapitule les principales différences de crédit entre les types d'instances extensibles.

Type	Type de CPU crédits pris en charge	Modes de configuration du crédit	Durée de vie des CPU crédits accumulés entre le démarrage et l'arrêt de l'instance
Dernière génération			
T4g	Crédits gagnés, Crédits accumulés, Crédits dépensés, Crédits excédentaires (mode illimité uniquement)	Standard, Illimité (par défaut)	7 jours (les crédits persistent pendant 7 jours après l'arrêt d'une instance)

Type	Type de CPU crédits pris en charge	Modes de configuration du crédit	Durée de vie des CPU crédits accumulés entre le démarrage et l'arrêt de l'instance
T3a	Crédits gagnés, Crédits accumulés, Crédits dépensés, Crédits excédentaires (mode illimité uniquement)	Standard, Illimité (par défaut)	7 jours (les crédits persistent pendant 7 jours après l'arrêt d'une instance)
T3	Crédits gagnés, Crédits accumulés, Crédits dépensés, Crédits excédentaires (mode illimité uniquement)	Standard, Illimité (par défaut)	7 jours (les crédits persistent pendant 7 jours après l'arrêt d'une instance)
Génération précédente			
T2	Crédits gagnés, Crédits accumulés, Crédits dépensés, Crédits de lancement (mode Standard uniquement), Crédits excédentaires (mode Illimité uniquement)	Standard (par défaut), Illimité	0 jour (les crédits sont perdus quand une instance s'arrête)

> **Note**
>
> Le mode illimité n'est pas pris en charge pour les instances T3 lancées sur un hôte dédié.

Gagnez des CPU crédits

Chaque instance de performance burstable gagne en permanence (à une résolution de l'ordre de la milliseconde) un taux fixe de CPU crédits par heure, en fonction de la taille de l'instance. Le processus comptable permettant de déterminer si les crédits sont accumulés ou dépensés se fait également à une résolution de l'ordre de la milliseconde. Vous n'avez donc pas à vous soucier des CPU crédits excessifs ; une courte période de crédit n'CPUutilise qu'une petite fraction d'un crédit. CPU

Si une instance de performance renforcée utilise moins de CPU ressources que ce qui est nécessaire pour une utilisation de base (par exemple lorsqu'elle est inactive), les CPU crédits non dépensés sont comptabilisés dans le solde créditeur. CPU Si une instance de performance à capacité extensible a besoin d'étendre l'utilisation au-dessus du niveau d'utilisation de référence, elle dépense les crédits accumulés. Plus le nombre de crédits accumulés par une instance de performance extensible augmente, plus elle peut dépasser sa valeur de référence lorsqu'une CPU utilisation accrue est nécessaire.

Le tableau suivant répertorie les types d'instances à performance maximale, le taux auquel les CPU crédits sont gagnés par heure, le nombre maximum de CPU crédits gagnés qu'une instance peut accumuler, le nombre de crédits vCPUs par instance et l'utilisation de base en pourcentage d'un cœur complet (en utilisant un seul vCPU).

Type d'instance	CPUcrédits gagnés par heure	Maximum de crédits gagnés pouvant être accumulés*	vCPUs***	Utilisation de référence par v CPU
T2				
`t2.nano`	3	72	1	5 %
`t2.micro`	6	144	1	10 %
`t2.small`	12	288	1	20 %
`t2.medium`	24	576	2	20%**
`t2.large`	36	864	2	30%**
`t2.xlarge`	54	1296	4	22,5%**

Type d'instance	CPUcrédits gagnés par heure	Maximum de crédits gagnés pouvant être accumulés*	vCPUs***	Utilisation de référence par v CPU
t2.2xlarge	81.6	1958.4	8	17%**
T3				
t3.nano	6	144	2	5%**
t3.micro	12	288	2	10%**
t3.small	24	576	2	20%**
t3.medium	24	576	2	20%**
t3.large	36	864	2	30%**
t3.xlarge	96	2304	4	40%**
t3.2xlarge	192	4608	8	40%**
T3a				
t3a.nano	6	144	2	5%**
t3a.micro	12	288	2	10%**
t3a.small	24	576	2	20%**
t3a.medium	24	576	2	20%**
t3a.large	36	864	2	30%**
t3a.xlarge	96	2304	4	40%**
t3a.2xlarge	192	4608	8	40%**
T4g				

Type d'instance	CPUcrédits gagnés par heure	Maximum de crédits gagnés pouvant être accumulés*	vCPUs***	Utilisation de référence par v CPU
t4g.nano	6	144	2	5%**
t4g.micro	12	288	2	10%**
t4g.small	24	576	2	20%**
t4g.medium	24	576	2	20%**
t4g.large	36	864	2	30%**
t4g.xlarge	96	2304	4	40%**
t4g.2xlarge	192	4608	8	40%**

* Le nombre de crédits pouvant être accumulés est équivalent au nombre de crédits pouvant être gagnés en 24 heures.

** Le pourcentage d'utilisation de référence indiqué dans le tableau est par CPU v. Dans CloudWatch, CPU l'utilisation est indiquée par CPU v. Par exemple, l'CPUutilisation d'une `t3.large` instance fonctionnant au niveau de référence est indiquée comme 30 % dans CloudWatch CPU les métriques. Pour plus d'informations sur le calcul de l'utilisation de référence, consultez Utilisation de référence.

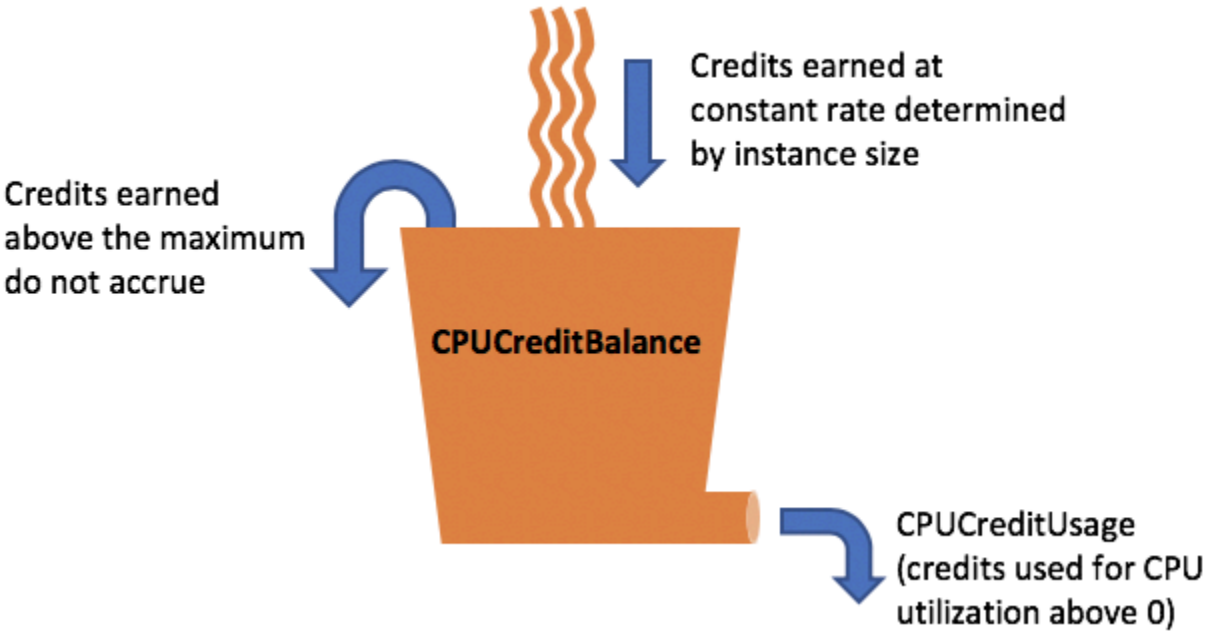
*** Chaque v CPU est un thread d'un cœur Intel Xeon ou d'un AMD EPYC cœur, à l'exception des instances T2 et T4g.

CPUtaux de gain de crédit

Le nombre de CPU crédits gagnés par heure est déterminé par la taille de l'instance. Par exemple, une instance `t3.nano` gagne six crédits par heure, tandis qu'une instance `t3.small` en gagne 24 par heure. Le tableau précédent répertorie le taux d'obtention de crédits pour l'ensemble des instances.

CPUlimite d'accumulation de crédit

Si les crédits gagnés n'expirent jamais sur une instance en cours d'exécution, il existe une limite pour le nombre de crédits gagnés pouvant être accumulés par une instance. La limite est déterminée par la limite du solde CPU créditeur. Une fois la limite atteinte, les nouveaux crédits gagnés sont rejetés, comme l'indique l'image suivante. Le compartiment plein indique la limite du solde CPU créditeur, et le solde indique les crédits nouvellement gagnés qui dépassent cette limite.



La limite du solde CPU créditeur varie en fonction de la taille de l'instance. Par exemple, une `t3.micro` instance peut accumuler un maximum de 288 CPU crédits gagnés dans le solde CPU créditeur. Le tableau précédent répertorie le nombre maximum de crédits gagnés pouvant être cumulés par instance

Les instances T2 standard gagnent également des crédits de lancement. Les crédits de lancement ne sont pas pris en compte dans la limite du solde CPU créditeur. Si une instance T2 n'a pas dépensé ses crédits de lancement et reste inactive pendant 24 heures tout en accumulant les crédits accumulés, son solde CPU créditeur apparaît comme étant dépassé. Pour de plus amples informations, veuillez consulter Crédits de lancement.

Les instances T4g, T3a et T3 instances ne gagnent pas de crédits de lancement. Ces instances sont lancées en mode `unlimited` par défaut et peuvent par conséquent s'exécuter en mode rafale immédiatement après leur démarrage, sans avoir besoin de crédits de lancement. Les instances T3 lancées sur un lancement d'hôte dédié `standard`by default ;`unlimited` (par défaut) ne sont pas prises en charge sur un Hôte Dédié pour les instances T3.

Durée de vie des CPU crédits accumulés

CPUles crédits d'une instance en cours d'exécution n'expirent pas.

Pour T2, le solde CPU créditeur ne persiste pas entre les arrêts et les démarrages de l'instance. Si vous arrêtez une instance T2, celle-ci perd tous ses crédits accumulés.

Pour T4g, T3a et T3, le solde CPU créditeur persiste pendant sept jours après l'arrêt d'une instance et les crédits sont perdus par la suite. Si vous démarrez l'instance dans les sept jours, aucun crédit n'est perdu.

Pour plus d'informations, consultez `CPUCreditBalance` le tableau CloudWatch des mesures.

Utilisation de référence

L'utilisation de base est le niveau auquel le solde créditeur net CPU peut être égal à zéro, lorsque le nombre de CPU crédits gagnés correspond au nombre de CPU crédits utilisés. L'utilisation de référence est également appelée la référence.

L'utilisation de référence est exprimée en pourcentage de CPU l'utilisation de v, qui est calculée comme suit :

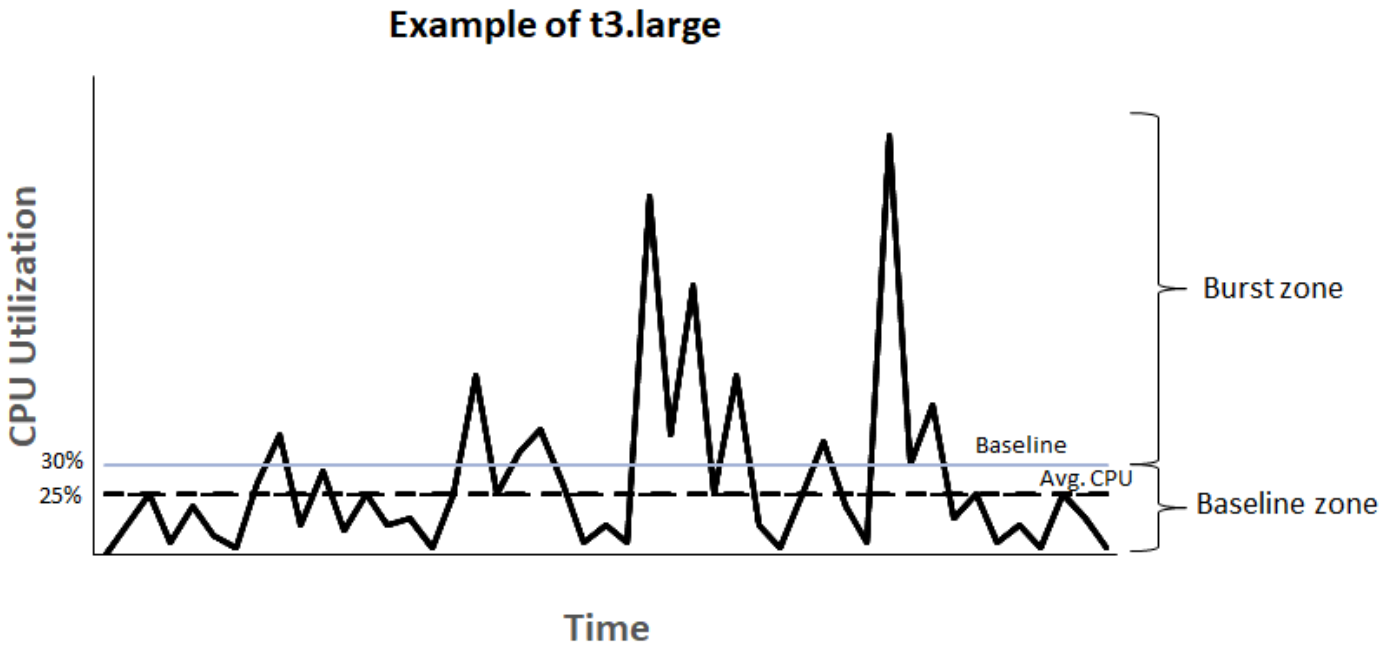
```
(number of credits earned/number of vCPUs)/60 minutes = % baseline
utilization
```

Par exemple, une `t3.nano` instance, avec 2vCPUs, gagne 6 crédits par heure, ce qui se traduit par une utilisation de base de 5 %, calculée comme suit :

```
(6 credits earned/2 vCPUs)/60 minutes = 5% baseline utilization
```

Une `t3.large` instance, avec 2vCPUs, génère 36 crédits par heure, soit une utilisation de base de 30 % (`(36/2)/60`).

Le graphique suivant fournit un exemple d'CPUutilisation moyenne inférieure à la base de référence. `t3.large`



Mode illimité pour les instances de performance à capacité extensible

Une instance de performance évolutive configurée de manière à `unlimited` pouvoir maintenir un taux d'CPUutilisation élevé pendant n'importe quelle période, chaque fois que cela est nécessaire. Le prix horaire de l'instance couvre automatiquement tous les pics CPU d'utilisation si l'CPUutilisation moyenne de l'instance est égale ou inférieure à la valeur de référence sur une période continue de 24 heures ou sur la durée de vie de l'instance, la période la plus courte étant retenue.

Pour la majorité des charges de travail à usage général, les instances configurées en mode `unlimited` fournissent d'excellentes performances sans frais supplémentaires. Si l'instance fonctionne à un CPU taux d'utilisation plus élevé pendant une période prolongée, elle peut le faire moyennant un tarif supplémentaire CPU forfaitaire par heure.

Si vous utilisez une `t3.micro` instance `t2.micro` ou dans le cadre de l'Niveau gratuit d'AWSoffre et que vous l'utilisez en `unlimited` mode, des frais peuvent s'appliquer si votre utilisation moyenne sur une période continue de 24 heures dépasse l'utilisation de base de l'instance.

Les instances T4g, T3a et T3 sont lancées `unlimited` par défaut (sauf si vous modifiez la valeur par défaut). Si l'CPUutilisation moyenne sur une période de 24 heures dépasse le niveau de référence, des frais vous seront facturés pour les crédits excédentaires. Si vous lancez des instances Spot en tant que `unlimited` et que vous prévoyez de les utiliser immédiatement et pendant une courte durée, sans aucune période d'inactivité pour accumuler des CPU crédits, des frais vous seront

facturés pour les crédits excédentaires. Nous vous recommandons de lancer vos instances Spot en mode standard pour éviter des coûts plus élevés. Pour plus d'informations, consultez Les crédits excédentaires peuvent occasionner des frais et Lancez des instances de performance éclatantes.

> **Note**
>
> Les instances T3 lancées sur un lancement d'hôte dédié `standard`by default ;`unlimited` (par défaut) ne sont pas prises en charge sur un Hôte Dédié pour les instances T3.

Table des matières

Concepts de mode illimités pour les instances éclatables

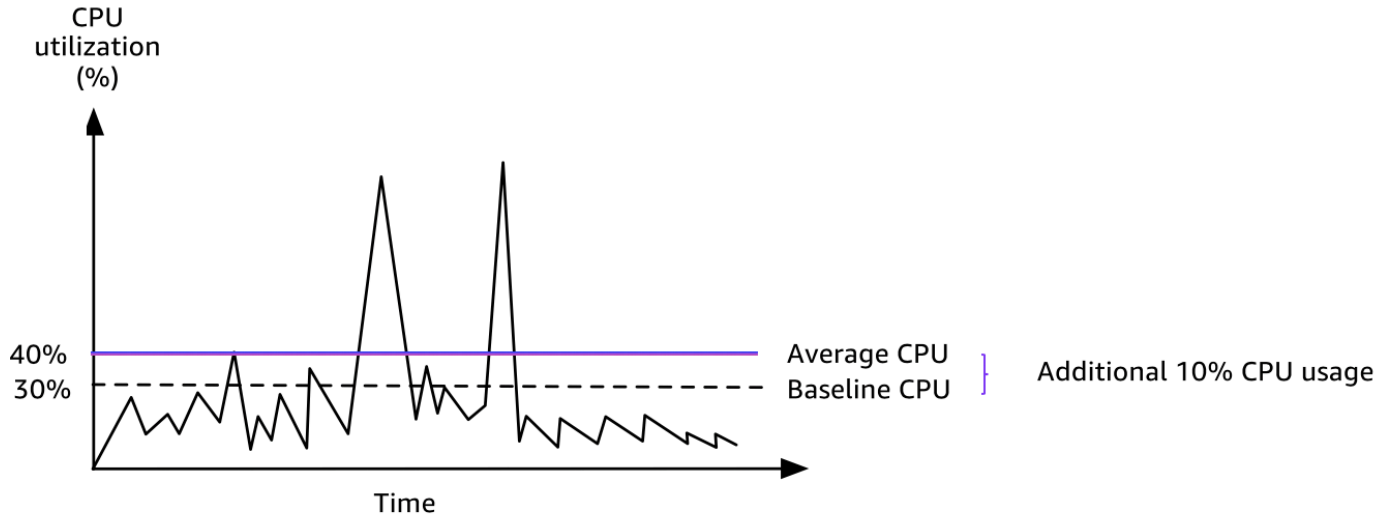
Le mode `unlimited` est une option de configuration de crédit pour les instances de performance à capacité extensible. Il peut être activé ou désactivé à tout moment pour une instance en cours d'exécution ou arrêtée. Vous pouvez la définir `unlimited` comme option de crédit par défaut au niveau du compte, par AWS région, par famille d'instances de performance éclatante, afin que toutes les nouvelles instances de performance actualisées du compte soient lancées à l'aide de l'option de crédit par défaut.

Fonctionnement des instances de performance à capacité extensible illimitées

Si une instance de performance évolutive configurée comme suit `unlimited` épuise son solde CPU créditeur, elle peut dépenser des crédits excédentaires pour dépasser le niveau de référence.

Lorsque son CPU utilisation tombe en dessous du niveau de référence, elle utilise les CPU crédits qu'elle gagne pour rembourser les crédits excédentaires qu'elle a dépensés plus tôt. La possibilité de gagner des CPU crédits pour rembourser les crédits excédentaires permet EC2 à Amazon de calculer la moyenne d'CPUutilisation d'une instance sur une période de 24 heures. Si l'CPUutilisation moyenne sur une période de 24 heures dépasse le niveau de référence, l'instance est facturée pour l'utilisation supplémentaire à un par heureCPU.

Le graphique suivant montre l'CPUutilisation d'un`t3.large`. L'CPUutilisation de référence pour a `t3.large` est de 30 %. Si l'instance fonctionne à un CPU taux d'utilisation de 30 % ou moins en moyenne sur une période de 24 heures, aucun frais supplémentaire n'est facturé car le coût est déjà couvert par le prix horaire de l'instance. Toutefois, si l'instance fonctionne à 40 % d'CPUutilisation en moyenne sur une période de 24 heures, comme le montre le graphique, l'instance est facturée pour les 10 % CPU d'utilisation supplémentaires à un par heureCPU.



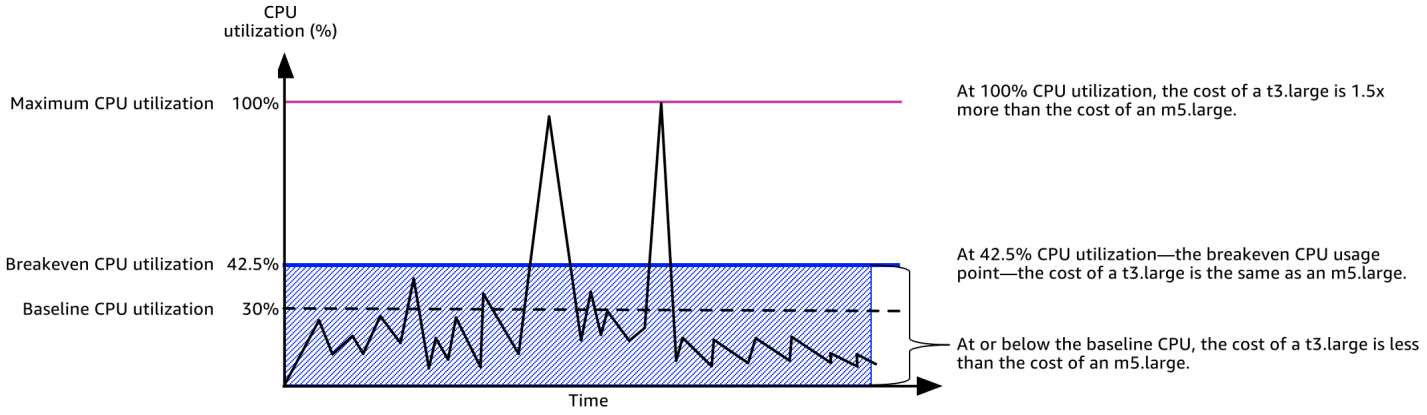
Pour plus d'informations sur l'utilisation de base par v CPU pour chaque type d'instance et le nombre de crédits gagnés par chaque type d'instance, consultez le tableau des crédits.

Quand utiliser le mode illimité plutôt que le mode fixe CPU

Lorsque vous déterminez si vous devez utiliser une instance de performance éclatante en `unlimited` mode, telle que T3, ou une instance de performance fixe, telle que M5, vous devez déterminer l'utilisation du seuil de rentabilité. CPU L'CPUutilisation du seuil de rentabilité d'une instance de performance éclatante est le point à partir duquel une instance de performance extensible coûte le même prix qu'une instance de performance fixe. L'CPUutilisation du seuil de rentabilité vous aide à déterminer les éléments suivants :

- Si l'CPUutilisation moyenne sur une période de 24 heures est égale ou inférieure au seuil de rentabilitéCPU, utilisez une instance de performance éclatante en `unlimited` mode afin de bénéficier du prix inférieur d'une instance de performance extensible tout en obtenant les mêmes performances qu'une instance à performance fixe.
- Si l'CPUutilisation moyenne sur une période de 24 heures est supérieure au seuil de rentabilité, CPU l'instance de performance éclatante coûtera plus cher que l'instance de performance fixe de taille équivalente. Si une instance T3 explose continuellement à 100 %CPU, vous finissez par payer environ 1,5 fois le prix d'une instance M5 de taille équivalente.

Le graphique suivant montre le seuil de CPU rentabilité où un `t3.large` coûte le même prix qu'un`m5.large`. Le seuil de rentabilité CPU pour a `t3.large` est de 42,5 %. Si l'CPUutilisation moyenne est de 42,5 %, le coût de fonctionnement `t3.large` est le même que celui d'un`m5.large`, et il est plus élevé si l'CPUutilisation moyenne est supérieure à 42,5 %. Si la charge de travail nécessite moins de 42,5 % CPU d'utilisation moyenne, vous pouvez bénéficier du prix inférieur du produit `t3.large` tout en obtenant les mêmes performances qu'un`m5.large`.



Le tableau suivant indique comment calculer le seuil CPU d'utilisation du seuil de rentabilité afin de déterminer quand il est moins coûteux d'utiliser une instance de performance en `unlimited` mode rafale ou une instance de performance fixe. Les colonnes du tableau sont étiquetées de A à K.

Type d'instance	vCPUs	T3 – Prix*/ heure	M5 – Prix*/ heure	Différence de prix	Utilisation de référence T3 par v CPU (%)	Facturer par CPU heure pour les crédits excédentaires	Charge par CPU minute	Minutes de rafale supplémentaires disponibles par v CPU	CPU % supplémentaire disponible	% d'équilibre CPU
A	B	C	D	E = D - C	F	G	H = G / 60	I = E / H	J = (I / 60) / B	K = F + J
t3.large	2	0,0835 US$	0,096 US$	0,0125 US$	30 %	0,05 US$	0,000833 US$	15	12,5%	42,5 %

* Le prix se rapporte à la région us-east-1 et au système d'exploitation Linux.

Le tableau fournit les informations suivantes :

- La colonne A indique le type d'instance, `t3.large`.
- La colonne B indique le nombre de vCPUs pour le`t3.large`.
- La colonne C indique le prix d'une instance `t3.large` par heure.
- La colonne D indique le prix d'une instance `m5.large` par heure.
- La colonne E indique la différence de prix entre l'instance `t3.large` et l'instance `m5.large`.
- La colonne F indique l'utilisation de base par v CPU de`t3.large`, qui est de 30 %. Au niveau de référence, le coût horaire de l'instance couvre le coût d'CPUutilisation.
- La colonne G indique le https://aws.amazon.com/ec2/pricing/on-demand/#T2.2FT3.2FT4g_Unlimited_Mode_Pricing par CPU heure auquel une instance est facturée si elle explose à 100 % CPU après épuisement des crédits accumulés.
- La colonne H indique le taux supplémentaire forfaitaire par CPU minute) auquel une instance est facturée si elle explose à 100 % CPU après avoir épuisé les crédits accumulés.

- La colonne I indique le nombre de minutes supplémentaires qu'ils `t3.large` peuvent parcourir par heure à 100 % CPU tout en payant le même prix par heure qu'un`m5.large`.
- La colonne J indique l'CPUutilisation supplémentaire (en %) par rapport à la valeur de référence que l'instance peut atteindre tout en payant le même prix horaire qu'un`m5.large`.
- La colonne K indique l'CPUutilisation du seuil de rentabilité (en %) qu'ils `t3.large` peuvent atteindre sans payer plus que le`m5.large`. Au dessus de ce seuil, l'instance `t3.large` coûte plus que l'instance `m5.large`.

Le tableau suivant montre l'CPUutilisation du seuil de rentabilité (en %) pour les types d'instances T3 par rapport aux types d'instances M5 de taille similaire.

Type d'instance T3	Taux CPU d'utilisation du seuil de rentabilité (en %) pour le T3 par rapport au M5
`t3.large`	42,5 %
`t3.xlarge`	52,5 %
`t3.2xlarge`	52,5 %

Les crédits excédentaires peuvent occasionner des frais

Si l'CPUutilisation moyenne d'une instance est égale ou inférieure à la valeur de référence, l'instance n'entraîne aucun frais supplémentaire. Comme une instance gagne un nombre maximum de crédits sur une période de 24 heures (par exemple, une instance `t3.micro` peut acquérir un maximum de 288 crédits sur une période de 24 heures), elle peut dépenser des crédits excédentaires jusqu'à ce maximum sans être facturée immédiatement.

Toutefois, si CPU l'utilisation reste supérieure à la valeur de référence, l'instance ne peut pas gagner suffisamment de crédits pour rembourser les crédits excédentaires qu'elle a dépensés. Les crédits excédentaires qui ne sont pas remboursés sont facturés à un taux supplémentaire CPU forfaitaire par heure. Pour en savoir plus sur les frais applicables, consultez Tarification des instances T2/T3/T4g en mode illimité.

Les crédits excédentaires qui ont été dépensés précédemment sont facturés lorsque l'une des situations suivantes se produit :

- Les crédits excédentaires dépensés dépassent le nombre maximum de crédits que l'instance peut gagner sur une période de 24 heures. Les crédits excédentaires dépensés au-dessus de ce maximum sont facturés à la fin de l'heure.
- L'instance est arrêtée ou résiliée.
- L'instance bascule du mode `unlimited` au mode `standard`.

Les crédits excédentaires dépensés sont suivis par la CloudWatch métrique`CPUSurplusCreditBalance`. Les crédits excédentaires facturés sont suivis selon la CloudWatch métrique`CPUSurplusCreditsCharged`. Pour de plus amples informations, veuillez consulter CloudWatch Mesures supplémentaires pour les instances de performance éclatantes.

Pas de crédit de lancement pour les instances T2 illimitées

Les instances T2 standard reçoivent des crédits de lancement, mais les instances T2 illimité n'en reçoivent pas. Une instance T2 Unlimited peut dépasser la valeur de référence à tout moment sans frais supplémentaires, à condition que son CPU utilisation moyenne soit égale ou inférieure à la valeur de référence sur une période continue de 24 heures ou pendant sa durée de vie, selon la période la plus courte. De ce fait, les instances T2 illimité ne nécessitent pas de crédits de lancement pour obtenir des performances élevées dès le lancement.

Si une instance T2 passe du mode `standard` au mode `unlimited`, tous les crédits de lancement accumulés sont supprimés de la métrique `CPUCreditBalance` avant que la métrique `CPUCreditBalance` restante soit reportée.

Les instances T4g, T3a et T3 ne reçoivent jamais de crédits de lancement parce qu'elles prennent en charge le mode Illimité. La configuration des crédits en mode illimité permet aux instances T4g, T3a et T3 d'en utiliser CPU autant que nécessaire pour dépasser le niveau de référence et aussi longtemps que nécessaire.

Activer le mode illimité

Vous pouvez passer du mode `unlimited` au mode `standard` et du mode `standard` au mode `unlimited` à tout moment sur une instance en cours d'exécution ou arrêtée. Pour plus d'informations, consultez Lancer une instance de performance à capacité extensible en mode Illimité ou Standard et Modifier la spécification de crédits d'une instance de performance à capacité extensible.

Vous pouvez la définir `unlimited` comme option de crédit par défaut au niveau du compte, par AWS région, par famille d'instances de performance éclatante, afin que toutes les nouvelles

instances de performance actualisées du compte soient lancées à l'aide de l'option de crédit par défaut. Pour de plus amples informations, veuillez consulter Définir la spécification de crédits par défaut pour le compte.

Vous pouvez vérifier si votre instance de performance burstable est configurée en tant que `unlimited` ou `standard` en utilisant la EC2 console Amazon ou le AWS CLI. Pour plus d'informations, consultez Afficher la spécification de crédits d'une instance de performance à capacité extensible et Afficher la spécification de crédits par défaut.

Comportement des crédits lors du basculement entre Illimité et Standard

`CPUCreditBalance`est une CloudWatch métrique qui suit le nombre de crédits accumulés par une instance. `CPUSurplusCreditBalance`est une CloudWatch métrique qui suit le nombre de crédits excédentaires dépensés par une instance.

Lorsque vous passez en mode `standard` une instance qui était configurée en mode `unlimited`, voici ce qui se produit :

- La valeur de `CPUCreditBalance` reste inchangée et est reportée.
- La valeur de `CPUSurplusCreditBalance` est immédiatement facturée.

Lorsqu'une instance `standard` passe à la configuration `unlimited`, la situation suivante se produit :

- La valeur de `CPUCreditBalance` contenant les crédits gagnés accumulés est reportée.
- Pour les instances T2 standard, tous les crédits de lancement sont supprimés de la valeur de `CPUCreditBalance` et la valeur de `CPUCreditBalance` restante contenant les crédits gagnés accumulés est reportée.

Surveiller l'utilisation du crédit

Pour savoir si votre instance dépense plus de crédits que ce que la base de référence fournit, vous pouvez utiliser CloudWatch des métriques pour suivre l'utilisation, et vous pouvez configurer des alarmes horaires pour être informé de l'utilisation des crédits. Pour de plus amples informations, veuillez consulter Surveillez les CPU crédits pour les instances instables.

Exemples de modes illimités pour les instances burstables

Les exemples suivants expliquent l'utilisation des crédits lorsque des instances sont configurées en mode `unlimited`.

Exemples

Exemple 1 : Expliquer l'utilisation des crédits avec T3 illimité

Dans cet exemple, vous pouvez voir l'CPUutilisation d'une `t3.nano` instance lancée en tant que`unlimited`, ainsi que la manière dont elle dépense les crédits gagnés et excédentaires pour maintenir CPU l'utilisation.

Une `t3.nano` instance gagne 144 CPU crédits sur une période continue de 24 heures, qu'elle peut échanger contre 144 minutes d'CPUutilisation. Lorsqu'elle épuise son solde CPU créditeur (représenté par la CloudWatch métrique`CPUCreditBalance`), elle peut dépenser les CPU crédits excédentaires, qu'elle n'a pas encore gagnés, pour augmenter aussi longtemps qu'elle en a besoin. Comme une instance `t3.nano` gagne un maximum de 144 crédits sur une période de 24 heures, elle peut dépenser des crédits excédentaires jusqu'à ce maximum sans être facturée immédiatement. S'il dépense plus de 144 CPU crédits, la différence lui est facturée à la fin de l'heure.

L'exemple illustré par le graphique suivant a pour but de montrer comment une instance peut passer en mode rafale à l'aide des crédits excédentaires, même après avoir épuisé son `CPUCreditBalance`. Le flux de travail suivant référence les points numérotés sur le graphique :

P1 – À 0 heure sur le graphe, l'instance est lancée en mode `unlimited` et commence immédiatement à gagner des crédits. L'instance reste inactive dès son lancement (le taux d'CPUutilisation est de 0 %) et aucun crédit n'est dépensé. Tous les crédits non dépensés sont accumulés dans le solde de crédits. Pendant les premières 24 heures, `CPUCreditUsage` est à 0 et la valeur de `CPUCreditBalance` atteint son maximum de 144.

P2 — Au cours des 12 prochaines heures, le CPU taux d'utilisation est de 2,5 %, ce qui est inférieur au niveau de référence de 5 %. L'instance gagne plus de crédits qu'elle n'en dépense, mais la valeur de `CPUCreditBalance` ne peut pas dépasser son maximum de 144 crédits.

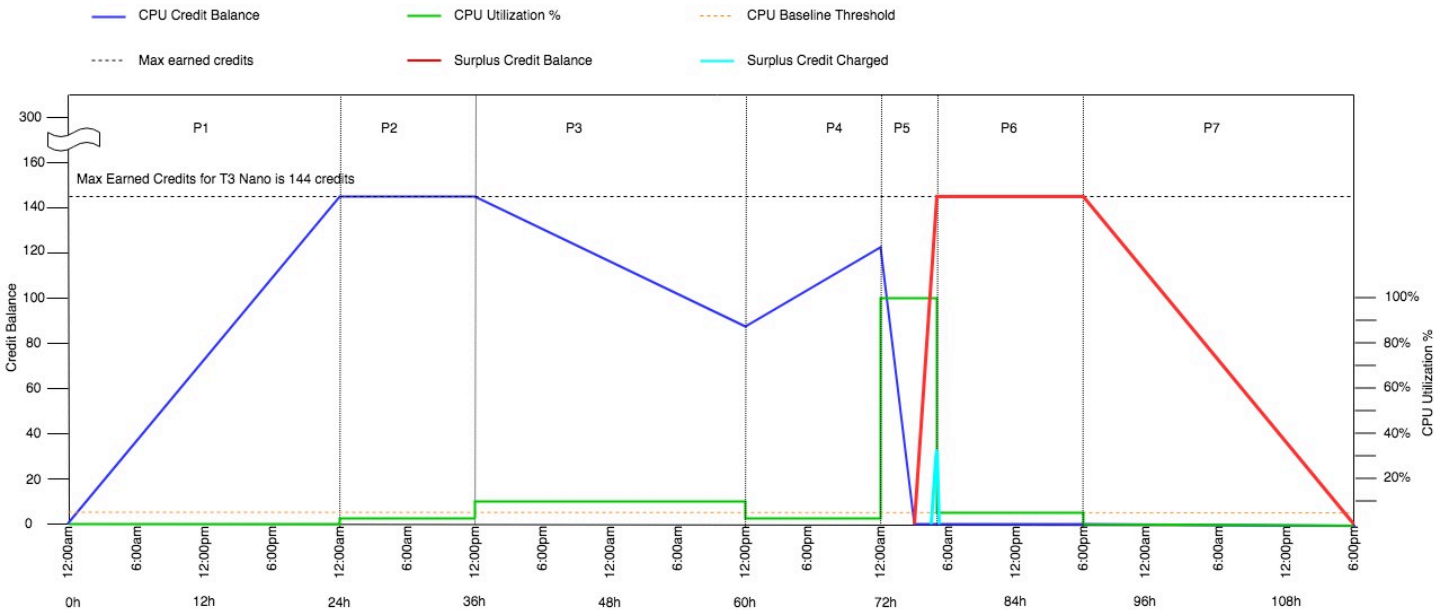
P3 — Au cours des prochaines 24 heures, le CPU taux d'utilisation est de 7 % (au-dessus de la base de référence), ce qui nécessite une dépense de 57,6 crédits. L'instance dépense plus de crédits qu'elle n'en gagne et la valeur de `CPUCreditBalance` baisse jusqu'à 86,4 crédits.

P4 — Au cours des 12 prochaines heures, le CPU taux d'utilisation diminue à 2,5 % (en dessous du niveau de référence), ce qui nécessite une dépense de 36 crédits. Au même moment, l'instance gagne 72 crédits. L'instance gagne plus de crédits qu'elle n'en dépense et la valeur `CPUCreditBalance` augmente jusqu'à 122 crédits.

P5 — Au cours des 5 prochaines heures, l'instance atteint 100 % d'CPUutilisation et dépense un total de 570 crédits pour maintenir la rafale. Environ une heure après le début de cette période, l'instance épuise la totalité `CPUCreditBalance` de ses 122 crédits et commence à dépenser des crédits excédentaires pour maintenir le taux d'CPUutilisation élevé, soit un total de 448 crédits excédentaires au cours de cette période (570-122 = 448). Lorsque la `CPUSurplusCreditBalance` valeur atteint 144 CPU crédits (le maximum qu'une `t3.nano` instance peut gagner sur une période de 24 heures), les crédits excédentaires dépensés par la suite ne peuvent pas être compensés par des crédits gagnés. Les crédits excédentaires dépensés par la suite s'élèvent à 304 crédits (448-144=304), ce qui entraîne de faibles frais supplémentaires à la fin de l'heure pour 304 crédits.

P6 — Pour les 13 prochaines heures, le CPU taux d'utilisation est de 5 % (valeur de référence). L'instance gagne autant de crédits qu'elle en dépense, sans excès pour rembourser progressivement le solde `CPUSurplusCreditBalance`. La valeur de `CPUSurplusCreditBalance` reste à 144 crédits.

P7 — Dans cet exemple, au cours des 24 dernières heures, l'instance est inactive et le taux d'CPUutilisation est de 0 %. Pendant ce temps, l'instance gagne 144 crédits, qu'elle utilise pour rembourser progressivement le solde `CPUSurplusCreditBalance`.



Exemple 2 : Expliquer l'utilisation des crédits avec T2 illimité

Dans cet exemple, vous pouvez voir l'CPUutilisation d'une `t2.nano` instance lancée en tant que`unlimited`, ainsi que la manière dont elle dépense les crédits gagnés et excédentaires pour maintenir CPU l'utilisation.

Une `t2.nano` instance gagne 72 CPU crédits sur une période continue de 24 heures, qu'elle peut échanger contre 72 minutes d'CPUutilisation. Lorsqu'elle épuise son solde CPU créditeur (représenté par la CloudWatch métrique`CPUCreditBalance`), elle peut dépenser les CPU crédits excédentaires, qu'elle n'a pas encore gagnés, pour augmenter aussi longtemps qu'elle en a besoin. Comme une instance `t2.nano` gagne un maximum de 72 crédits sur une période de 24 heures, elle peut dépenser des crédits excédentaires jusqu'à ce maximum sans être facturée immédiatement. S'il dépense plus de 72 CPU crédits, la différence lui est facturée à la fin de l'heure.

L'exemple illustré par le graphique suivant a pour but de montrer comment une instance peut passer en mode rafale à l'aide des crédits excédentaires, même après avoir épuisé son `CPUCreditBalance`. Vous pouvez supposer qu'au début de la ligne de temps du graphique, l'instance dispose d'un solde de crédits accumulés égal au nombre maximum de crédits qu'elle peut gagner en 24 heures. Le flux de travail suivant référence les points numérotés sur le graphique :

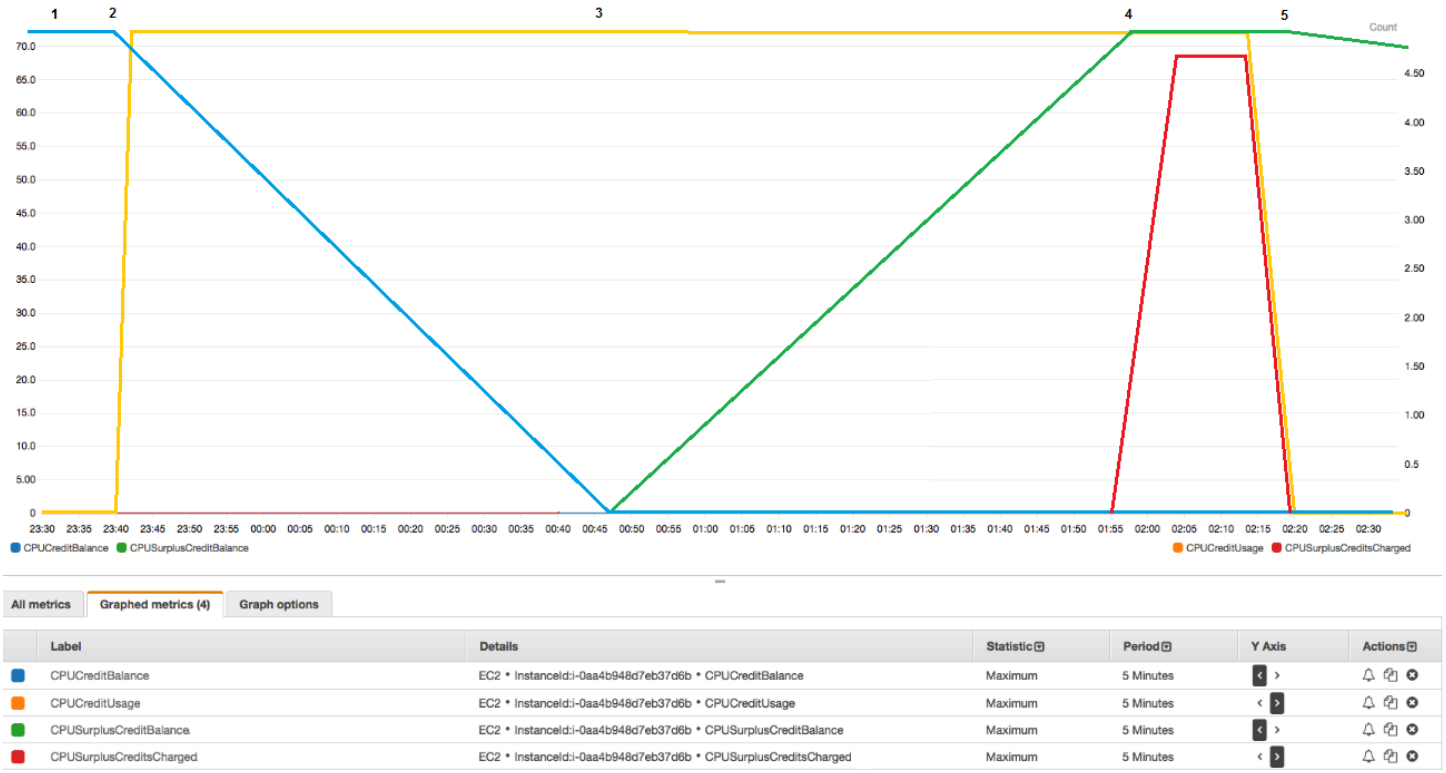
1 – Dans les 10 premières minutes, `CPUCreditUsage` est à 0, et la valeur de `CPUCreditBalance` reste à son maximum de 72.

2 — À 23 h 40, à mesure que CPU l'utilisation augmente, l'instance dépense des CPU crédits et la `CPUCreditBalance` valeur diminue.

3 — Vers 00h47, l'instance épuise son intégralité `CPUCreditBalance` et commence à dépenser des crédits excédentaires pour maintenir un taux d'utilisation élevé. CPU

4 — Les crédits excédentaires sont dépensés jusqu'à 01:55, date à laquelle la `CPUSurplusCreditBalance` valeur atteint 72 CPU crédits. Cela équivaut au nombre maximum de crédits qu'une instance `t2.nano` peut gagner sur une période de 24 heures. Les crédits excédentaires dépensés par la suite ne peuvent pas être compensés par les crédits gagnés au cours de la période de 24 heures, ce qui entraîne de faibles frais supplémentaires à la fin de l'heure.

5 – L'instance continue de dépenser les crédits excédentaires jusqu'à 02h20 environ. À ce stade, le CPU taux d'utilisation tombe en dessous du niveau de référence et l'instance commence à gagner des crédits à 3 crédits par heure (soit 0,25 crédit toutes les 5 minutes), qu'elle utilise pour rembourser le`CPUSurplusCreditBalance`. Une fois que la valeur de `CPUSurplusCreditBalance` est nulle, l'instance commence à accumuler les crédits gagnés dans son `CPUCreditBalance` à raison de 0,25 crédit toutes les 5 minutes.



Calcul de la facture (instance Linux)

Les crédits excédentaires coûtent 0,05$ par heureCPU. L'instance a dépensé environ 25 crédits excédentaires entre 01:55 et 02:20, ce qui équivaut à 0,42 v -heure. CPU Les frais supplémentaires pour cette instance sont de 0,42 v CPU -heure x 0,05 $/v CPU -heure = 0,021$, arrondis à 0,02$. Facture de fin de mois correspondant à cette instance T2 illimité :

Amazon Elastic Compute Cloud running Linux/UNIX		
$0.0058 per On Demand Linux t2.nano Instance Hour	720.000 Hrs	$4.18

Amazon Elastic Compute Cloud T2 CPU Credits		
$0.05 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	$0.02

Calcul de la facture (instance Windows)

Les crédits excédentaires coûtent 0,096$ par heure. CPU L'instance a dépensé environ 25 crédits excédentaires entre 01:55 et 02:20, ce qui équivaut à 0,42 v -heure. CPU Les frais supplémentaires pour cette instance sont de 0,42 v CPU -heure x 0,096 $/v CPU -heure = 0,04032$, arrondis à 0,04$. Facture de fin de mois correspondant à cette instance T2 illimité :

Amazon Elastic Compute Cloud running Windows		
$0.0081 per On Demand Windows t2.nano Instance Hour	720.000 Hrs	$5.83

Amazon Elastic Compute Cloud T2 CPU Credits		
$0.096 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	$0.04

Vous pouvez définir des alertes de facturation pour être notifié toutes les heures des frais accumulés, puis prendre des mesures au besoin.

Mode standard pour les instances de performance à capacité extensible

Une instance de performance évolutive configurée de manière `standard` adaptée aux charges de travail dont CPU l'utilisation moyenne est constamment inférieure à l'CPUutilisation de base de l'instance. Pour dépasser le niveau de référence, l'instance dépense les crédits qu'elle a accumulés dans son solde CPU créditeur. Si le nombre de crédits accumulés par l'instance est insuffisant, le taux d'CPUutilisation est progressivement abaissé jusqu'au niveau de référence, de sorte que l'instance ne subisse pas de forte baisse de performance lorsque son solde créditeur accumulé est épuiséCPU. Pour de plus amples informations, veuillez consulter Concepts clés pour les instances de performance éclatantes.

Table des matières

Concepts de mode standard pour les instances éclatables

Le mode `standard` est une option de configuration pour les instances de performance à capacité extensible. Il peut être activé ou désactivé à tout moment pour une instance en cours d'exécution ou arrêtée. Vous pouvez la définir `standard` comme option de crédit par défaut au niveau du compte, par AWS région, par famille d'instances de performance éclatante, afin que toutes les nouvelles instances de performance actualisées du compte soient lancées à l'aide de l'option de crédit par défaut.

Fonctionnement des instance de performance à capacité extensible standards

Lorsqu'une instance de performance à capacité extensible configurée en mode `standard` est en cours d'exécution, elle gagne continuellement (à une résolution de l'ordre de la milliseconde) un taux déterminé de crédits gagnés par heure. Lorsqu'une instance T2 Standard est arrêtée, elle perd tous ses crédits accumulés et le solde de crédits est remis à zéro. Lorsqu'elle est redémarrée, elle reçoit un nouveau jeu de crédits de lancement, et commence à accumuler des crédits gagnés. Pour les instances T4g, T3a et T3 Standard, le solde CPU créditeur persiste pendant sept jours après l'arrêt de l'instance et les crédits sont perdus par la suite. Si vous démarrez l'instance dans les sept jours, aucun crédit n'est perdu.

Les instances T2 Standard reçoivent deux types de CPUcrédits : les crédits gagnés et les crédits de lancement. Lorsqu'une instance T2 Standard est en cours d'exécution, elle gagne continuellement

(à une résolution de l'ordre de la milliseconde) un taux déterminé de crédits gagnés par heure. Au début, elle n'a pas de crédits gagnés pour une bonne expérience de démarrage ; elle reçoit donc, à cet effet, des crédits de lancement, qui sont dépensés pendant qu'elle accumule des crédits gagnés.

Les instances T4g, T3a et T3 ne reçoivent pas de crédits de lancement parce qu'elles prennent en charge le mode Illimité. La configuration des crédits en mode illimité permet aux instances T4g, T3a et T3 d'en utiliser CPU autant que nécessaire pour dépasser le niveau de référence et aussi longtemps que nécessaire.

Crédits de lancement

Les instances T2 Standard obtiennent 30 crédits de lancement par v CPU au lancement ou au démarrage, et les instances T1 Standard obtiennent 15 crédits de lancement. Par exemple, une `t2.micro` instance possède un v CPU et obtient 30 crédits de lancement, tandis qu'une `t2.xlarge` instance en possède quatre vCPUs et obtient 120 crédits de lancement. Les crédits de lancement sont conçus pour fournir une bonne expérience de démarrage et permettre aux instances de s'exécuter en mode rafale dès le lancement, avant qu'elles aient accumulé des crédits gagnés.

Les crédits de lancement sont dépensés en premier, avant les crédits gagnés. Les crédits de lancement non dépensés sont comptabilisés dans le solde CPU créditeur, mais ne sont pas pris en compte dans le calcul de la limite du solde CPU créditeur. Par exemple, le solde CPU créditeur d'une `t2.micro` instance est limité à 144 crédits gagnés. S'il est lancé et reste inactif pendant 24 heures, son solde CPU créditeur atteint 174 (30 crédits de lancement + 144 crédits gagnés), ce qui est supérieur à la limite. Toutefois, une fois que l'instance a dépensé les 30 crédits de lancement, le solde de crédits ne peut pas excéder 144. Pour plus d'informations sur la limite CPU de solde créditeur pour chaque taille d'instance, consultez le tableau des crédits.

Le tableau suivant répertorie l'allocation CPU de crédit initiale reçue au lancement ou au démarrage, ainsi que le nombre devCPUs.

Type d'instance	Crédits de lancement	vCPUs
`t1.micro`	15	1
`t2.nano`	30	1
`t2.micro`	30	1
`t2.small`	30	1

Type d'instance	Crédits de lancement	vCPUs
t2.medium	60	2
t2.large	60	2
t2.xlarge	120	4
t2.2xlarge	240	8

Limites de crédits de lancement

Le nombre de fois où les instances T2 Standard peuvent recevoir des crédits de lancement est limité. La limite par défaut est définie sur 100 lancements ou démarrages de toutes les instances T2 Standard combinées par compte, par région et par déploiement de 24 heures. Par exemple, la limite est atteinte lorsqu'une instance est arrêtée et démarrée 100 fois sur une période de 24 heures, ou lorsque 100 instances sont lancées sur une période de 24 heures, ou toute autre combinaison équivalente à 100 démarrages. Les nouveaux comptes peuvent présenter une limite inférieure qui augmentera au fil du temps en fonction de votre utilisation.

> **Tip**
>
> Pour vous assurer que vos charges de travail obtiennent toujours les performances nécessaires, passez à une instance Mode illimité pour les instances de performance à capacité extensible ou utilisez une taille d'instance supérieure.

Différences entre crédits de lancement et crédits gagnés

Le tableau suivant répertorie les différences entre les crédits de lancement et les crédits gagnés.

	Crédits de lancement	Crédits gagnés
Taux d'obtention de crédits	Les instances T2 Standard obtiennent 30 crédits de lancement par v CPU au lancement ou au démarrage.	Chaque instance T2 gagne en permanence (à une résolution de l'ordre de la milliseconde) un taux fixe de CPU crédits par heure, en fonction de la taille de l'instance. Pour plus

	Crédits de lancement	Crédits gagnés
	Si une instance T2 bascule du mode `unlimited` au mode `standard`, elle n'obtient pas de crédits de lancement au moment du basculement.	d'informations sur le nombre de CPU crédits obtenus par taille d'instance, consultez le tableau des crédits.
Limite d'obtention de crédits	La limite pour la réception de crédits de lancement est définie sur 100 lancements ou démarrages de toutes les instances T2 Standard combinées par compte, par région et par déploiement de 24 heures. Les nouveaux comptes peuvent présenter une limite inférieure qui augmentera au fil du temps en fonction de votre utilisation.	Une instance T2 ne peut pas accumuler plus de crédits que la limite du solde CPU créditeur. Si le solde CPU créditeur a atteint sa limite, tous les crédits accumulés après l'atteinte de la limite sont annulés. Les crédits de lancement ne sont pas comptés dans la limite. Pour plus d'informations sur la limite CPU de solde créditeur pour chaque taille d'instance T2, consultez le tableau des crédits.
Utilisation des crédits	Les crédits de lancement sont dépensés en premier, avant les crédits gagnés.	Les crédits gagnés sont dépensés uniquement lorsque tous les crédits de lancement ont été dépensés.
Expiration des crédits	Les crédits de lancement d'une instance T2 Standard en cours d'exécution n'expirent pas. Lorsqu'un e instance T2 Standard s'arrête ou passe à T2 illimité, tous les crédits de lancement sont perdus.	Lorsqu'une instance T2 est en cours d'exécution, les crédits gagnés qui ont été accumulés n'expirent pas. Lorsque l'instance T2 s'arrête, tous les crédits gagnés accumulés sont perdus.

Le nombre de crédits de lancement accumulés et de crédits accumulés est suivi par la métrique. CloudWatch `CPUCreditBalance` Pour plus d'informations, consultez `CPUCreditBalance` le tableau CloudWatch des mesures.

Exemples de mode standard pour les instances burstables

Les exemples suivants expliquent l'utilisation des crédits lorsque des instances sont configurées en mode `standard`.

Exemples

Exemple 1 : Expliquer l'utilisation des crédits avec T3 standard

Cet exemple vous montre comment une instance `t3.nano` lancée en mode `standard` gagne, accumule et dépense des crédits gagnés. Vous pouvez voir que le solde de crédits reflète les crédits gagnés accumulés.

Une instance `t3.nano` en cours d'exécution gagne 144 crédits toutes les 24 heures. Sa limite de solde de crédits est de 144 crédits gagnés. Une fois que la limite est atteinte, les nouveaux crédits gagnés sont rejetés. Pour plus d'informations sur le nombre de crédits pour l'UC pouvant être gagnés et accumulés, consultez le tableau des crédits.

Vous pouvez lancer une instance T3 Standard et l'utiliser immédiatement. Ou vous pouvez lancer une instance T3 Standard et la laisser inactive pendant quelques jours avant d'y exécuter des applications. L'utilisation ou l'inactivité d'une instance détermine si les crédits sont accumulés ou dépensés. Si une instance reste inactive pendant 24 heures après son lancement, le solde de crédits atteint sa limite, qui correspond au nombre maximal de crédits gagnés qui peuvent être accumulés.

Cet exemple décrit une instance qui reste inactive pendant 24 heures après son lancement, et explique sept périodes sur une plage de 96 heures. L'exemple illustre les taux d'obtention, d'accumulation, de dépense et de rejet de crédits, ainsi que la valeur du solde de crédits à la fin de chaque période.

Le flux de travail suivant référence les points numérotés sur le graphique :

P1 – À 0 heure sur le graphe, l'instance est lancée en mode `standard` et commence immédiatement à gagner des crédits. L'instance reste inactive dès son lancement (le taux d'CPUutilisation est de 0 %) et aucun crédit n'est dépensé. Tous les crédits non dépensés sont accumulés dans le solde de crédits. Pendant les premières 24 heures, `CPUCreditUsage` est à 0 et la valeur de `CPUCreditBalance` atteint son maximum de 144.

P2 — Au cours des 12 prochaines heures, le CPU taux d'utilisation est de 2,5 %, ce qui est inférieur au niveau de référence de 5 %. L'instance gagne plus de crédits qu'elle n'en dépense, mais la valeur de `CPUCreditBalance` ne peut pas dépasser son maximum de 144 crédits. Tous les crédits gagnés au-delà de cette limite sont rejetés.

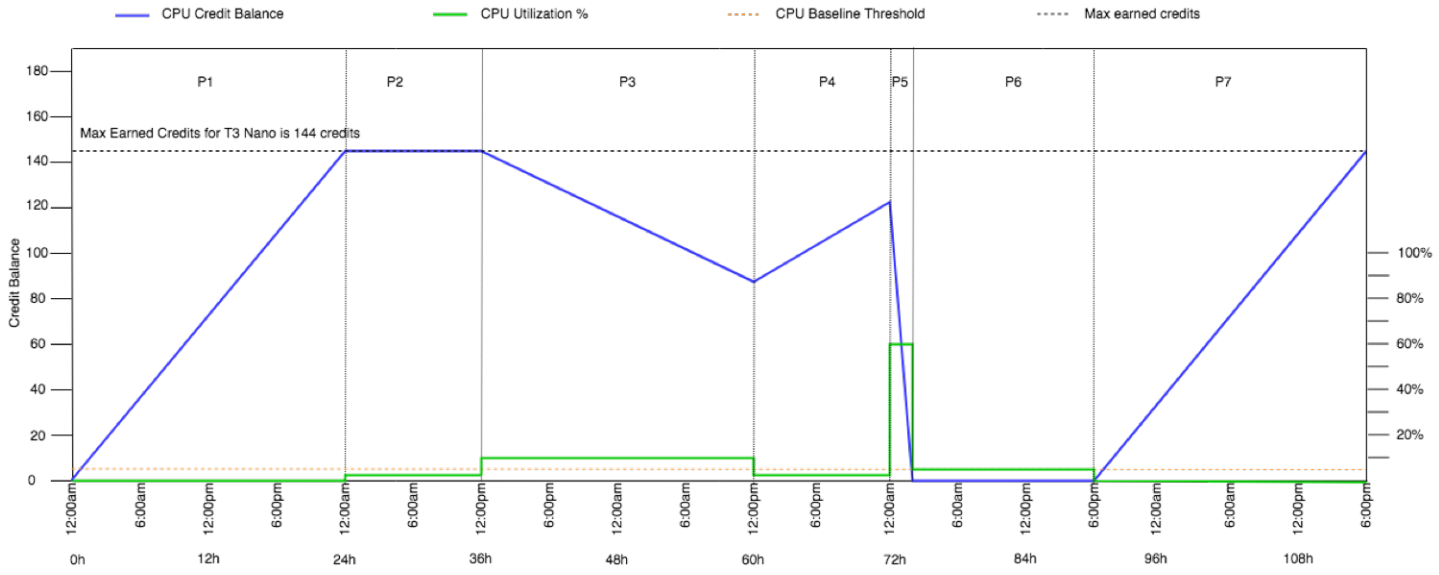
P3 — Au cours des prochaines 24 heures, le CPU taux d'utilisation est de 7 % (au-dessus de la base de référence), ce qui nécessite une dépense de 57,6 crédits. L'instance dépense plus de crédits qu'elle n'en gagne et la valeur de `CPUCreditBalance` baisse jusqu'à 86,4 crédits.

P4 — Au cours des 12 prochaines heures, le CPU taux d'utilisation diminue à 2,5 % (en dessous du niveau de référence), ce qui nécessite une dépense de 36 crédits. Au même moment, l'instance gagne 72 crédits. L'instance gagne plus de crédits qu'elle n'en dépense et la valeur `CPUCreditBalance` augmente jusqu'à 122 crédits.

P5 — Au cours des deux heures qui suivent, l'instance atteint 60 % d'CPUutilisation et épuise sa `CPUCreditBalance` valeur totale de 122 crédits. À la fin de cette période, lorsque le `CPUCreditBalance` taux d'utilisation est nul, le CPU taux d'utilisation est contraint de chuter au niveau d'utilisation de référence de 5 %. Au niveau de base, l'instance gagne autant de crédits qu'elle en dépense.

P6 — Au cours des 14 prochaines heures, le CPU taux d'utilisation est de 5 % (valeur de référence). L'instance gagne autant de crédits qu'elle en dépense. La valeur de `CPUCreditBalance` reste à 0.

P7 — Dans cet exemple, au cours des 24 dernières heures, l'instance est inactive et le taux d'CPUutilisation est de 0 %. Pendant ce temps, l'instance gagne 144 crédits, qu'elle accumule dans son solde `CPUCreditBalance`.



Exemple 2 : Expliquer l'utilisation des crédits avec T2 standard

Cet exemple vous montre comment une instance `t2.nano` lancée en tant que `standard` gagne, accumule et dépense des crédits de lancement et des crédits gagnés. Vous pouvez voir que le

solde de crédits reflète non seulement les crédits gagnés accumulés, mais également les crédits de lancement accumulés.

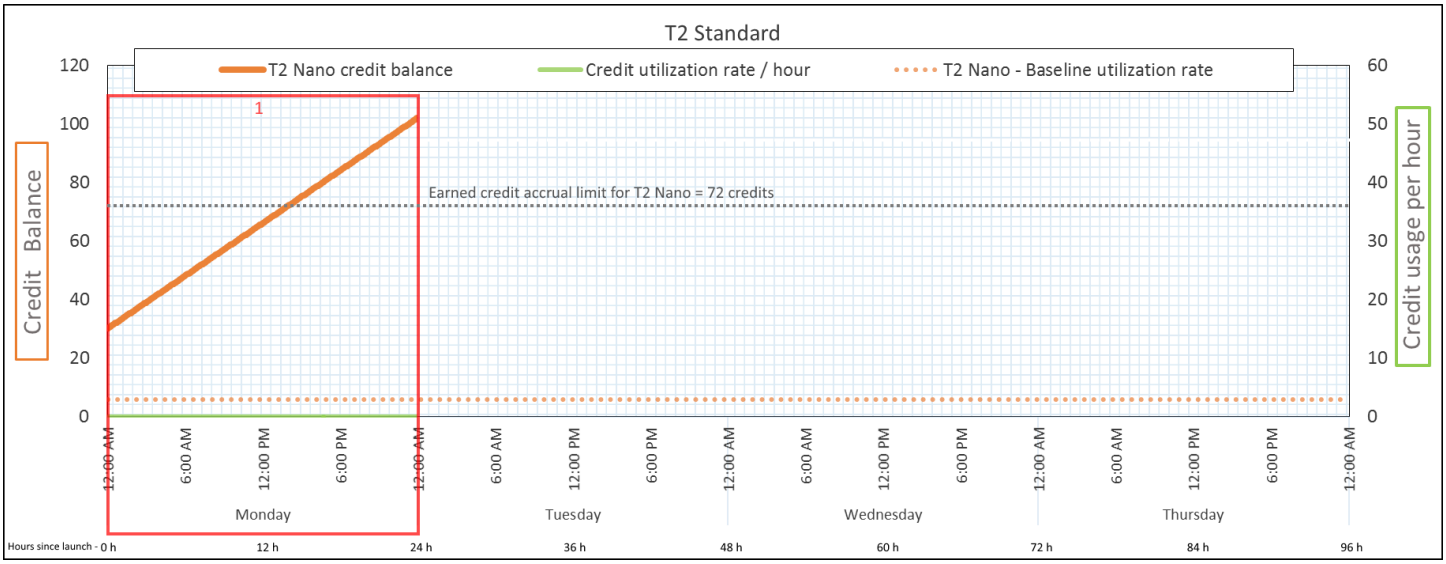
Une instance `t2.nano` obtient 30 crédits de lancement lorsqu'elle est lancée, et gagne 72 crédits par 24 heures. Sa limite du solde de crédits est de 72 crédit gagnés ; les crédits de lancement ne sont pas comptés dans la limite. Une fois que la limite est atteinte, les nouveaux crédits gagnés sont rejetés. Pour plus d'informations sur le nombre de crédits pour l'UC pouvant être gagnés et accumulés, consultez le tableau des crédits. Pour en savoir plus sur les limites, consultez Limites de crédits de lancement.

Vous pouvez lancer une instance T2 Standard et l'utiliser immédiatement. Ou vous pouvez lancer une instance T2 Standard et la laisser inactive pendant quelques jours avant d'y exécuter des applications. L'utilisation ou l'inactivité d'une instance détermine si les crédits sont accumulés ou dépensés. Si une instance reste inactive pendant 24 heurs après son lancement, le solde de crédits est affiché comme dépassant sa limite, car le solde reflète à la fois les crédits gagnés accumulés et les crédits de lancement accumulés. Cependant, une fois CPU utilisés, les crédits de lancement sont dépensés en premier. Par la suite, la limite reflète toujours le nombre maximum de crédits gagnés pouvant être accumulés.

Cet exemple décrit une instance qui reste inactive pendant 24 heures après son lancement, et explique sept périodes sur une plage de 96 heures. L'exemple illustre les taux d'obtention, d'accumulation, de dépense et de rejet de crédits, ainsi que la valeur du solde de crédits à la fin de chaque période.

Période 1 : 1 – 24 heures

À 0 heure sur le graphe, l'instance T2 est lancée en tant que `standard` et obtient immédiatement 30 crédits de lancement. Elle gagne des crédits lorsqu'elle s'exécute. L'instance reste inactive dès son lancement (le taux d'CPUutilisation est de 0 %) et aucun crédit n'est dépensé. Tous les crédits non dépensés sont accumulés dans le solde de crédits. Environ 14 heures après le lancement, le solde de crédits est de72 (30 crédits de lancement + 42 crédits gagnés), ce qui équivaut à ce que l'instance peut gagner en 24 heures. 24 heures après le lancement, le solde de crédits dépasse 72 crédits, car les crédits de lancement non dépensés sont inclus dans le —solde de crédits. Le solde de crédits est de 102 crédits : 30 crédits de lancement + 72 crédits gagnés.



Taux de dépense de crédits	0 crédits par 24 heures (0 % CPU d'utilisation)
Taux d'obtention de crédits	72 crédits par 24 heures
Taux de rejet de crédits	0 crédits par 24 heures
Solde de crédits	102 crédits (30 crédits de lancement + 72 crédits gagnés)

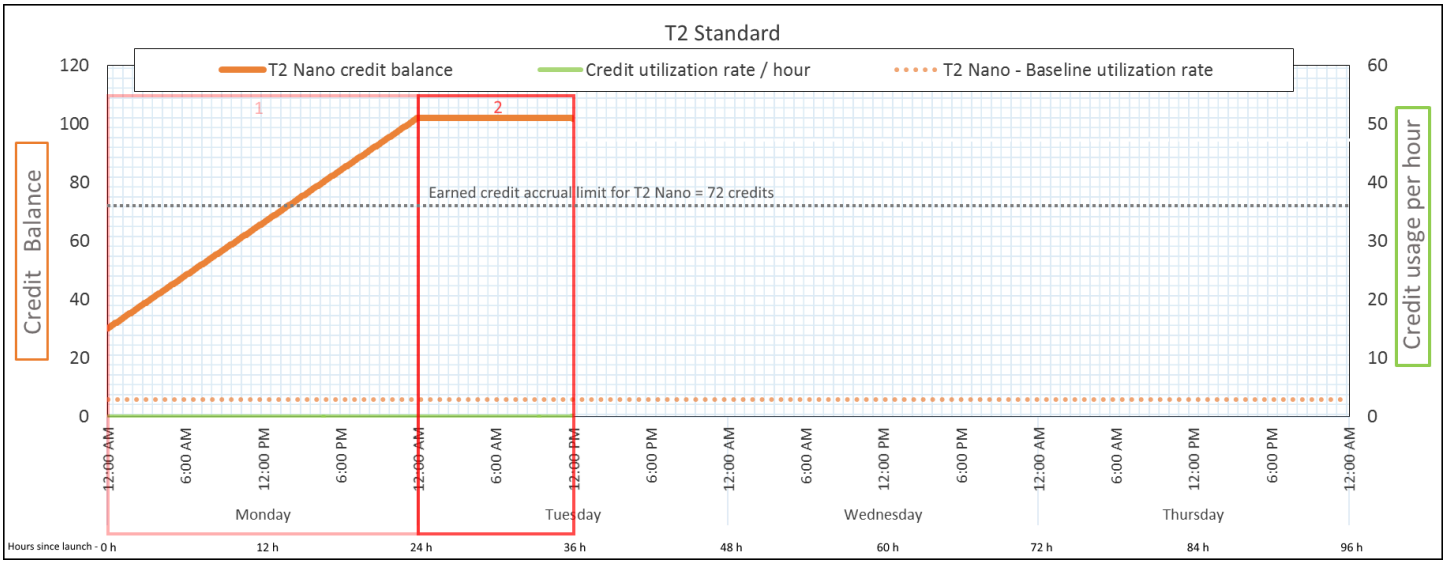
Conclusion

S'il n'y a aucune CPU utilisation après le lancement, l'instance accumule plus de crédits que ce qu'elle peut gagner en 24 heures (30 crédits de lancement + 72 crédits gagnés = 102 crédits).

Dans un scénario réel, une EC2 instance consomme un petit nombre de crédits lors de son lancement et de son exécution, ce qui empêche le solde d'atteindre la valeur théorique maximale dans cet exemple.

Période 2 : 25 – 36 heures

Pendant les 12 heures suivantes, l'instance reste encore inactive et gagne des crédits, mais le solde de crédits n'augmente pas. Il se stabilise à 102 crédits (30 crédits de lancement + 72 crédits gagnés). Le solde de crédits a atteint sa limite de 72 crédits gagnés accumulés. C'est pour cette raison que les nouveaux crédits gagnés sont rejetés.



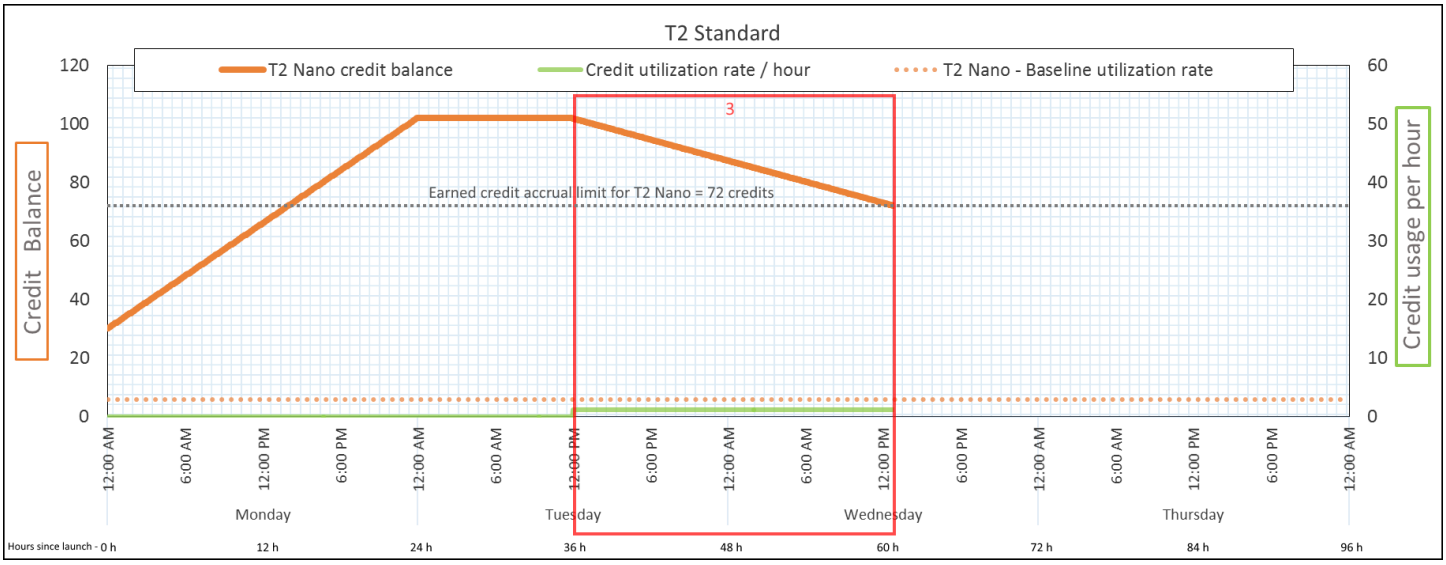
Taux de dépense de crédits	0 crédits par 24 heures (0 % CPU d'utilisation)
Taux d'obtention de crédits	72 crédits par 24 heures (3 crédits par heure)
Taux de rejet de crédits	72 crédits par 24 heures (100 % du taux d'obtention de crédits)
Solde de crédits	102 crédits (30 crédits de lancement + 72 crédits gagnés) — le solde est inchangé

Conclusion

Une instance gagne des crédits en permanence, mais elle ne peut pas accumuler des crédits gagnés au-delà de la limite du solde de crédits. Une fois que la limite est atteinte, les nouveaux crédits gagnés sont rejetés. Les crédits de lancement ne sont pas comptés dans la limite du solde de crédits. Si le solde comprend les crédits de lancement accumulés, il est affiché comme dépassant la limite.

Période 3 : 37 – 61 heures

Au cours des 25 prochaines heures, l'instance utilise 2 %CPU, ce qui nécessite 30 crédits. Pendant ce même laps de temps, elle gagne 75 crédits, mais le solde de crédits diminue. Le solde diminue car les crédits de lancement accumulés sont dépensés en premier, et les nouveaux crédits gagnés sont rejetés, car le solde de crédits a déjà atteint sa limite de 72 crédits gagnés.



Taux de dépense de crédits	28,8 crédits par 24 heures (1,2 crédit par heure, 2 % d'CPUutilisation, 40 % du taux d'accumulation de crédits) —30 crédits sur 25 heures
Taux d'obtention de crédits	72 crédits par 24 heures
Taux de rejet de crédits	72 crédits par 24 heures (100 % du taux d'obtention de crédits)
Solde de crédits	72 crédits (30 crédits de lancement ont été dépensés ; 72 crédits gagnés n'ont pas été dépensé)

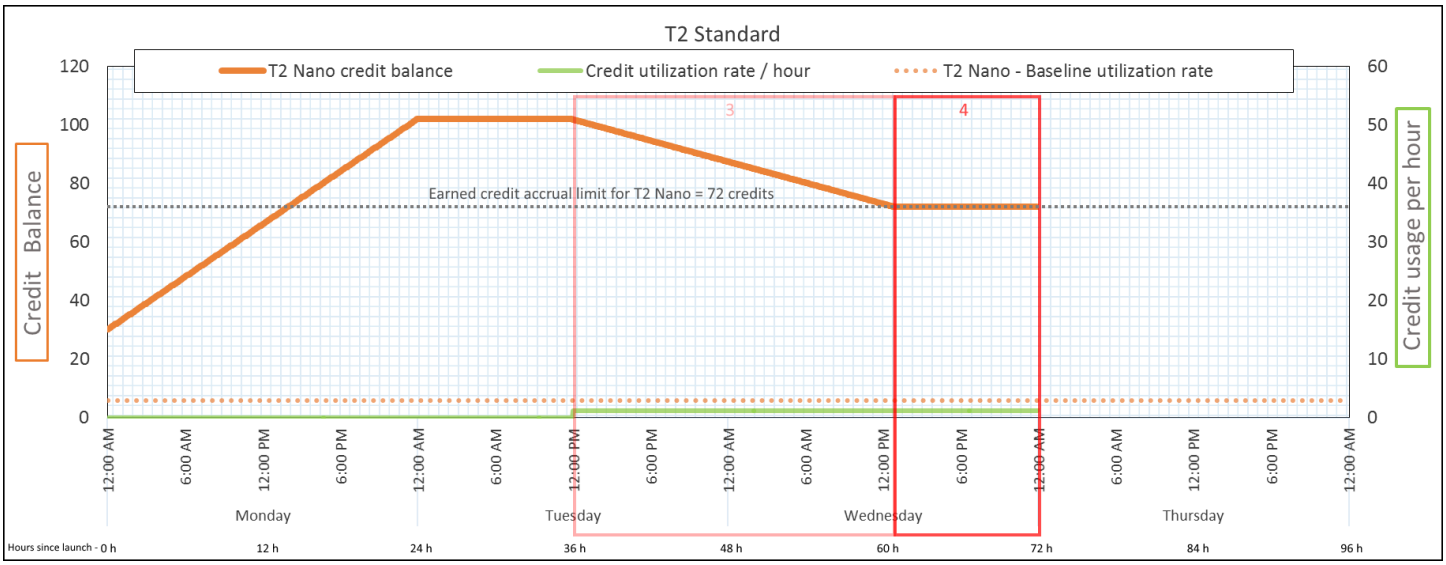
Conclusion

Une instance dépense les crédits de lancement en premier, avant les crédits gagnés. Les crédits de lancement ne sont pas comptés dans la limite de crédits. Lorsque les crédits de lancement sont dépensés, le solde ne peut pas être plus élevé que ce qui peut être gagné en l'espace de 24 heures. De plus, lorsqu'une instance s'exécute, elle ne peut pas obtenir de nouveaux crédits de lancement.

Période 4 : 62 – 72 heures

Au cours des 11 prochaines heures, l'instance utilise 2 %CPU, ce qui nécessite 13,2 crédits. Il s'agit de la même CPU utilisation que lors de la période précédente, mais le solde ne diminue pas. Il reste à 72 crédits.

Le solde ne diminue pas, car le taux d'obtention de crédits est supérieur à celui de dépense de crédits. Pendant que l'instance dépense 13.2 crédits, elle en gagne également 33. Cependant, la limite du solde étant de 72 crédits, les éventuels crédits gagnés au-delà de la limite sont rejetés. Le solde se stabilise à 72 crédits, et non à 102 crédits comme lors de la deuxième période, car il n'y a aucun crédit de lancement accumulé.



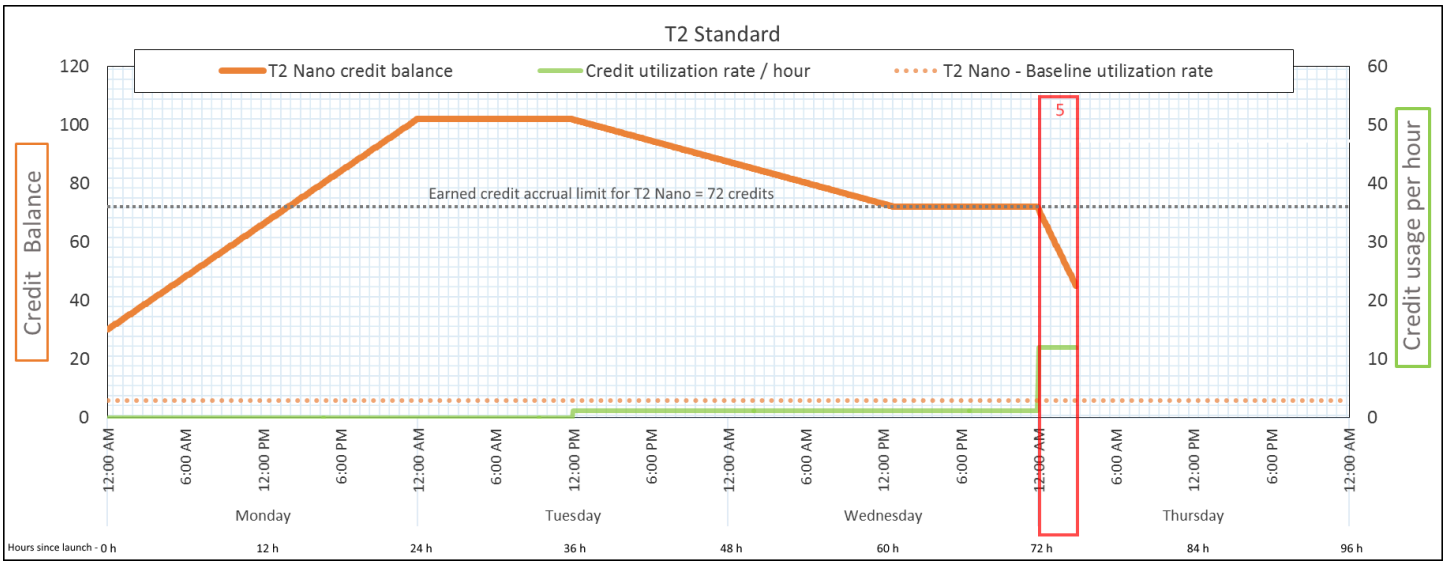
Taux de dépense de crédits	28,8 crédits par 24 heures (1,2 crédit par heure, 2 % d'CPUutilisation, 40 % du taux d'accumulation de crédits) —13,2 crédits sur 11 heures
Taux d'obtention de crédits	72 crédits par 24 heures
Taux de rejet de crédits	43.2 crédits par 24 heures (60 % du taux d'obtention de crédits)
Solde de crédits	72 crédits (0 crédit de lancement, 72 crédits gagnés) — le solde atteint sa limite

Conclusion

Une fois que les crédits de lancement sont dépensés, la limite du solde de crédits est déterminée par le nombre de crédits qu'une instance peut gagner en l'espace de 24 heures. Si l'instance gagne plus de crédits qu'elle n'en dépense, les nouveaux crédits gagnés au-delà de la limite sont rejetés.

Période 5 : 73 – 75 heures

Au cours des trois heures suivantes, l'instance atteint un taux d'CPUutilisation de 20 %, ce qui nécessite 36 crédits. L'instance gagne neuf crédits au cours de ces trois heures, ce qui entraîne une diminution du solde de 27 crédits. Au terme des trois heures, le solde de crédits est de 45 crédits gagnés accumulés.



Taux de dépense de crédits	288 crédits par 24 heures (12 crédits par heure, 20 % d'CPUutilisation, 400 % du taux d'accumulation de crédits) —36 crédits sur 3 heures
Taux d'obtention de crédits	72 crédits par 24 heures (9 crédits en 3 heures)
Taux de rejet de crédits	0 crédits par 24 heures
Solde de crédits	45 crédits (solde précédent (72) - crédits dépensés (36) + crédits gagnés (9)) — le solde diminue à 216 crédits par 24 heures (taux de dépense 288/24 + taux d'obtention 72/24 = taux de diminution du solde 216/24)

Conclusion

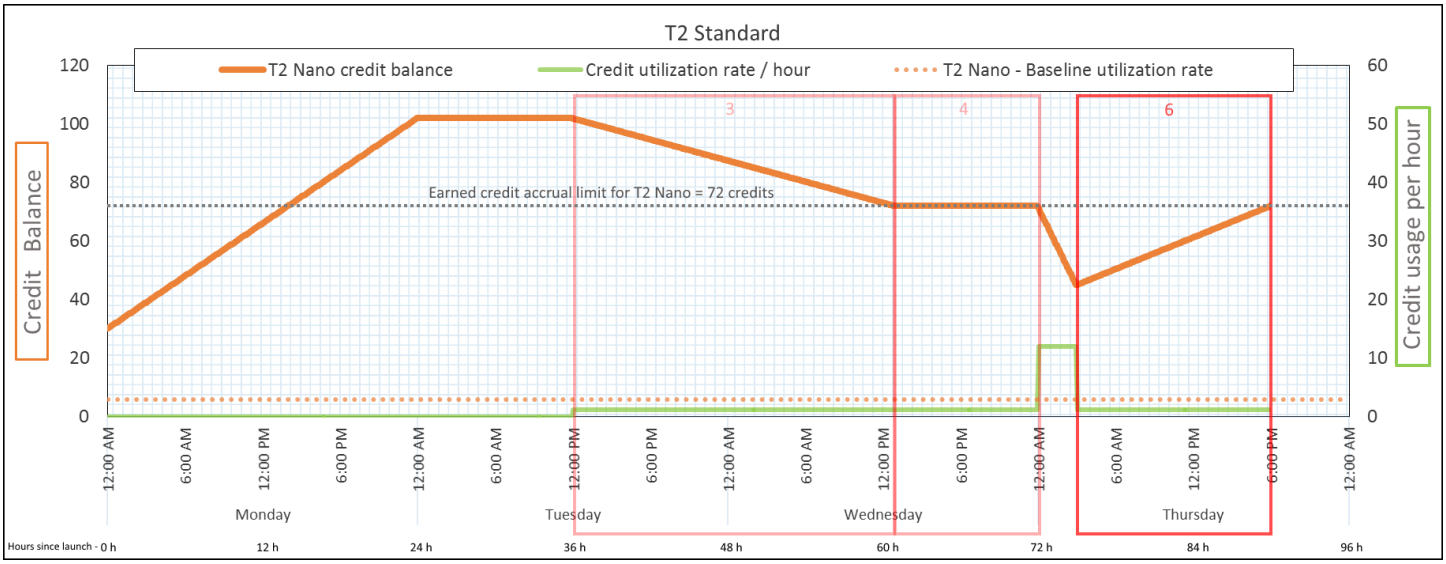
Si une instance dépense plus de crédits qu'elle n'en gagne, son solde de crédits diminue.

Période 6 : 76 – 90 heures

Au cours des 15 prochaines heures, l'instance utilise 2 %CPU, ce qui nécessite 18 crédits. Il s'agit de la même CPU utilisation qu'aux périodes 3 et 4. Cependant, le solde augmente au cours de cette période, alors qu'il avait diminué pendant la troisième période, et s'était stabilisé pendant la quatrième.

Pendant la troisième période, les crédits de lancement accumulés avaient été dépensés et les crédits gagnés au-delà de la limite de crédits avaient été rejetés, ce qui explique la diminution du solde de crédits. Pendant la quatrième période, l'instance avait dépensé moins de crédits qu'elle n'en avait gagné. Les crédits gagnés au-delà de la limite ont été rejetés, ce qui explique la stabilisation du solde à 72 crédits.

Au cours de cette nouvelle période, il n'y a aucun crédit de lancement accumulé, et le nombre de crédits gagnés accumulés du solde est inférieur à la limite. Aucun crédit gagné n'est rejeté. De plus, l'instance gagne plus de crédits qu'elle n'en dépense, ce qui entraîne une augmentation du solde de crédits.



Taux de dépense de crédits	28,8 crédits par 24 heures (1,2 crédit par heure, 2 % d'CPUutilisation, 40 % du taux d'accumulation de crédits) —18 crédits sur 15 heures
Taux d'obtention de crédits	72 crédits par 24 heures (45 crédits en 15 heures)
Taux de rejet de crédits	0 crédits par 24 heures

Solde de crédits	72 crédits (le solde augmente à un taux de 43,2 crédits par 24 heures — taux de variation = taux de dépense 28,8/24 + taux d'obtention 72/24)

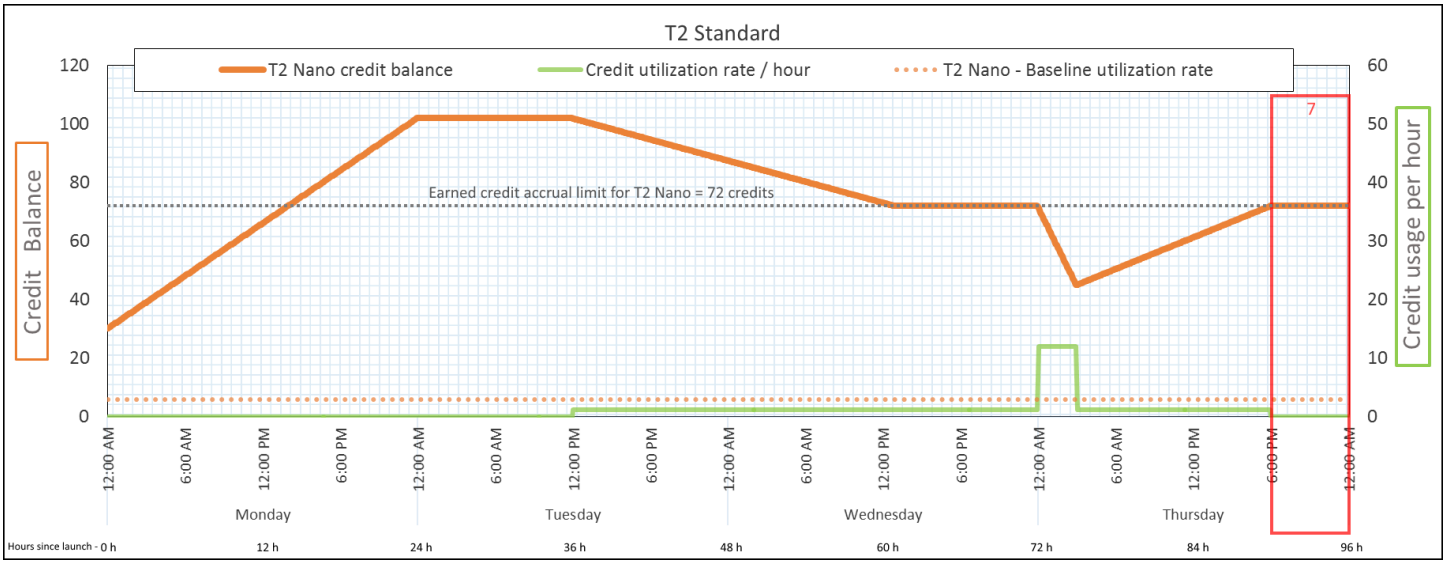
Conclusion

Si une instance dépense moins de crédits qu'elle n'en gagne, son solde de crédits augmente.

Période 7 : 91 – 96 heures

Pendant les six heures suivantes, l'instance reste inactive (le CPU taux d'utilisation est de 0 %) et aucun crédit n'est dépensé. Il s'agit de la même CPU utilisation qu'au cours de la période 2, mais le solde ne plafonne pas à 102 crédits ; il plafonne à 72 crédits, ce qui correspond à la limite du solde de crédit pour l'instance.

Au cours de la deuxième période, le solde de crédits comprenait 30 crédits de lancement accumulés. Les crédits de lancement ont été dépensés au cours de la troisième période. Une instance en cours d'exécution ne peut pas obtenir d'autres crédits de lancement. Lorsque la limite du solde de crédits est atteinte, les éventuels crédits gagnés au-delà de la limite sont rejetés.



Taux de dépense de crédits	0 crédits par 24 heures (0 % CPU d'utilisation)
Taux d'obtention de crédits	72 crédits par 24 heures

Taux de rejet de crédits	72 crédits par 24 heures (100 % du taux d'obtention de crédits)
Solde de crédits	72 crédits (0 crédit de lancement + 72 crédits gagnés)

Conclusion

Une instance gagne des crédits en permanence, mais ne peut pas accumuler des crédits gagnés si la limite du solde de crédits est atteinte. Une fois que la limite est atteinte, les nouveaux crédits gagnés sont rejetés. La limite du solde de crédits est déterminée par le nombre de crédits qu'une instance peut gagner en l'espace de 24 heures. Pour plus d'informations sur les limites du solde de crédits, consultez le tableau des crédits.

Utiliser des instance de performance à capacité extensible

Les étapes de lancement, de surveillance et de modification des instances de performance burstable (instances T) sont similaires. La différence clé est la spécification de crédits par défaut lors de leur lancement :

Chaque famille d'instances T est fournie avec la spécification de crédit par défaut suivante :

- Les instances T4g, T3a et T3 sont lancées en tant que `unlimited`
- Les instances T3 sur un hôte dédié ne peuvent être lancées qu'en tant que `standard`
- Instances T2 lancées en mode `standard`

Vous pouvez modifier la spécification de crédit par défaut pour le compte.

Table des matières

Lancer une instance de performance à capacité extensible en mode Illimité ou Standard

Vous pouvez lancer vos instances T en tant que `unlimited` ou `standard` à l'aide de la EC2 console Amazon AWS SDK, d'un outil de ligne de commande ou d'un groupe Auto Scaling.

Les procédures suivantes décrivent comment utiliser la EC2 console ou le AWS CLI. Pour plus d'informations sur l'utilisation d'un groupe Auto Scaling, consultezUtiliser un groupe Auto Scaling pour lancer une instance de performance à capacité extensible en mode Illimité.

Console

Pour lancer une instance T en tant que version illimitée ou standard

1. Suivez la procédure pour lancer une instance.
2. Pour Instance type (Type d'Instance), sélectionnez un type d'instance T.
3. Développez Advanced details (Détails avancés), et pour Credit specification (Spécification de crédit), sélectionnez une spécification de crédit. Si vous n'effectuez aucune sélection, la valeur par défaut est utilisée, c'est-à-dire `standard` pour T2, T4g, T3a et T3. `unlimited`
4. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance). Pour de plus amples informations, veuillez consulter Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console.

AWS CLI

Pour lancer une instance T en tant que version illimitée ou standard

Utilisez la commande run-instances pour lancer vos instances. Spécifiez la spécification de crédits à l'aide du paramètre `--credit-specification CpuCredits=`. Les spécifications de crédits valides sont `unlimited` et `standard`.

- Pour T4g, T3a et T3, si vous n'incluez pas le `--credit-specification` paramètre, l'instance se lance comme `unlimited` par défaut.
- Pour T2, si vous n'incluez pas le paramètre `--credit-specification`, l'instance est lancée en mode `standard` par défaut.

```
aws ec2 run-instances \
```

```
    --image-id ami-abc12345 \
    --count 1 \
    --instance-type t3.micro \
    --key-name MyKeyPair \
    --credit-specification "CpuCredits=unlimited"
```

Utiliser un groupe Auto Scaling pour lancer une instance de performance à capacité extensible en mode Illimité

Lorsque les instances T sont lancées ou démarrées, elles ont besoin de CPU crédits pour une bonne expérience de démarrage. Si vous utilisez un groupe Auto Scaling pour lancer vos instances, nous vous conseillons de configurer vos instances en mode `unlimited`. Dans ce cas, elles utilisent les crédits excédentaires en cas de lancement ou de redémarrage automatique par le groupe Auto Scaling. L'utilisation des crédits excédentaires empêche les restrictions de performances.

Créer un modèle de lancement

Vous devez utiliser un modèle de lancement pour lancer les instances en mode `unlimited` dans un groupe Auto Scaling. Une configuration de lancement ne prend pas en charge le lancement des instances en mode `unlimited`.

> **Note**
>
> Le mode `unlimited` n'est pas pris en charge pour les instances T3 lancées sur un hôte dédié.

Console

Pour créer un modèle de lancement des instances en mode Illimité

1. Suivez la procédure de création d'un modèle de lancement à l'aide des paramètres avancés du manuel Amazon EC2 Auto Scaling User Guide.
2. Dans Launch template contents (Contenu du modèle de lancement), pour Instance type (Type d'instance), choisissez une taille d'instance.
3. Pour lancer des instances en mode `unlimited` dans un groupe Auto Scaling, sous Advanced details (Détails avancés), pour la Credit specification (Spécification de crédits), choisissez Unlimited (Illimité).

4. Lorsque vous avez fini de définir les paramètres de modèle de lancement, choisissez Créer un modèle de lancement.

AWS CLI

Pour créer un modèle de lancement des instances en mode Illimité

Utilisez la create-launch-templatecommande et spécifiez `unlimited` comme spécification de crédit.

- Pour T4g, T3a et T3, si vous n'incluez pas la `CreditSpecification={CpuCredits=unlimited}` valeur, l'instance est lancée par défaut. `unlimited`
- Pour T2, si vous n'incluez pas la valeur `CreditSpecification={CpuCredits=unlimited}`, l'instance est lancée en mode `standard` par défaut.

```
aws ec2 create-launch-template \
    --launch-template-name MyLaunchTemplate \
    --version-description FirstVersion \
    --launch-template-data
 ImageId=ami-8c1be5f6,InstanceType=t3.medium,CreditSpecification={CpuCredits=unlimited}
```

Associer un groupe Auto Scaling avec un modèle de lancement

Pour associer le modèle de lancement à un groupe Auto Scaling, créez le groupe Auto Scaling à l'aide du modèle de lancement ou ajoutez le modèle de lancement à un groupe Auto Scaling existant.

Console

Pour créer un groupe Auto Scaling à l'aide d'un modèle de lancement

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation située en haut de l'écran, sélectionnez la même région que celle utilisée lorsque vous avez créé le modèle de lancement.
3. Dans le panneau de navigation, choisissez Groupes Auto Scaling, puis Créer le groupe Auto Scaling.

4. Choisissez Modèle de lancement, sélectionnez votre modèle de lancement, puis choisissez Étape suivante.
5. Complétez les champs pour le groupe Auto Scaling. Lorsque vous avez fini de passer en revue vos paramètres de configuration sur la page Vérification, choisissez Créer le groupe Auto Scaling. Pour plus d'informations, consultez Creating an Auto Scaling Group Using a Launch Template dans le manuel Amazon EC2 Auto Scaling User Guide.

AWS CLI

Pour créer un groupe Auto Scaling à l'aide d'un modèle de lancement

Utilisez la create-auto-scaling-group AWS CLI commande et spécifiez le `--launch-template` paramètre.

Console

Pour ajouter un modèle de lancement à un groupe Auto Scaling existant

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation située en haut de l'écran, sélectionnez la même région que celle utilisée lorsque vous avez créé le modèle de lancement.
3. Dans le panneau de navigation, choisissez Groupes Auto Scaling.
4. Dans la liste des groupes Auto Scaling, sélectionnez un groupe Auto Scaling et choisissez Actions, Modifier.
5. Sous l'onglet Détails, pour Modèle de lancement, choisissez un modèle de lancement, puis choisissez Enregistrer.

AWS CLI

Pour ajouter un modèle de lancement à un groupe Auto Scaling existant

Utilisez la update-auto-scaling-group AWS CLI commande et spécifiez le `--launch-template` paramètre.

Afficher la spécification de crédits d'une instance de performance à capacité extensible

Vous pouvez consulter la spécification de crédit (`unlimitedoustandard`) d'une instance T en cours d'exécution ou arrêtée.

Console

Pour afficher la spécification de crédit d'une instance T

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation de gauche, choisissez Instances.
3. Sélectionnez l'instance.
4. Choisissez Details (Détails) et affichez le champ Credit specification (Spécification de crédits). La valeur est `unlimited` ou `standard`.

AWS CLI

Pour décrire la spécification de crédit d'une instance T

Utilisez la describe-instance-credit-specifications commande. Si vous ne spécifiez pas une ou plusieurs instancesIDs, toutes les instances avec la spécification de crédit de `unlimited` sont renvoyées, ainsi que les instances précédemment configurées avec la spécification `unlimited` de crédit. Par exemple, si vous redimensionnez une instance T3 en instance M4, alors qu'elle est configurée comme telle, `unlimited` Amazon EC2 renvoie l'instance M4.

```
aws ec2 describe-instance-credit-specifications --instance-id i-1234567890abcdef0
```

Exemple de sortie

```
{
  "InstanceCreditSpecifications": [
    {
        "InstanceId": "i-1234567890abcdef0",
        "CpuCredits": "unlimited"
    }
  ]
}
```

Modifier la spécification de crédits d'une instance de performance à capacité extensible

Vous pouvez changer la spécification de crédit d'une instance T en cours d'exécution ou arrêtée à tout moment entre `unlimited` et`standard`.

Veuillez noter qu'en mode `unlimited`, une instance peut dépenser des crédits excédentaires, ce qui peut entraîner des frais supplémentaires. Pour de plus amples informations, veuillez consulter Les crédits excédentaires peuvent occasionner des frais.

Console

Pour modifier la spécification de crédit d'une instance T

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation de gauche, choisissez Instances.
3. Sélectionnez l'instance. Pour modifier la spécification de crédits pour plusieurs instances à la fois, sélectionnez toutes les instances applicables.
4. Choisissez Actions, Instance settings (Paramètres de l'instance), Change credit specification (Modifier la spécification de crédits). Cette option n'est activée que si vous avez sélectionné une instance T.
5. Pour remplacer le mode de spécification de crédits par `unlimited`, activez la case à cocher en regard de l'ID de l'instance. Pour remplacer le mode de spécification de crédits par `standard`, désactivez la case à cocher en regard de l'ID de l'instance.

AWS CLI

Pour modifier la spécification de crédit d'une instance T

Utilisez la modify-instance-credit-specificationcommande. Spécifiez l'instance et la spécification de crédits à l'aide du paramètre `--instance-credit-specification`. Les spécifications de crédits valides sont `unlimited` et `standard`.

```
aws ec2 modify-instance-credit-specification \
    --region us-east-1 \
    --instance-credit-specification
 "InstanceId=i-1234567890abcdef0,CpuCredits=unlimited"
```

Exemple de sortie

```
{
  "SuccessfulInstanceCreditSpecifications": [
    {
      "InstanceId": "i- 1234567890abcdef0"
    }
  ],
  "UnsuccessfulInstanceCreditSpecifications": []
}
```

Définir la spécification de crédits par défaut pour le compte

Chaque famille d'instances T est fournie avec une spécification de crédit par défaut. Vous pouvez modifier les spécifications de crédit par défaut pour chaque famille d'instances T au niveau du compte par AWS région.

Si vous utilisez l'assistant de lancement d'instance de la EC2 console pour lancer des instances, la valeur que vous sélectionnez pour la spécification de crédit remplace la spécification de crédit par défaut au niveau du compte. Si vous utilisez le AWS CLI pour lancer des instances, toutes les nouvelles instances T du compte sont lancées en utilisant la spécification de crédit par défaut. La spécification de crédits pour les instances existantes en cours d'exécution ou arrêtées n'est pas affectée.

Considération

La spécification de crédits par défaut pour une famille d'instances ne peut être modifiée qu'une seule fois au cours d'une période continue de 5 minutes, et jusqu'à quatre fois au cours d'une période continue de 24 heures.

Console

Pour définir la spécification de crédits par défaut au niveau du compte par région

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le volet de navigation de gauche, choisissez EC2Dashboard.
4. Dans Account attributes (Attributs de compte), sélectionnez Default credit specification (Spécification de crédits par défaut).
5. Choisissez Gérer.

6. Pour chaque famille de·l'instance, sélectionnez Unlimited (Illimité) ou Standard, puis sélectionnez Update (Mettre à jour).

AWS CLI

Pour définir la spécification de crédits par défaut au niveau du compte (AWS CLI)

Utilisez la modify-default-credit-specificationcommande. Spécifiez la Région AWS , la famille d'instances et la spécification de crédits par défaut à l'aide du paramètre `--cpu-credits`. Les spécifications de crédits par défaut valides sont `unlimited` et `standard`.

```
aws ec2 modify-default-credit-specification \
    --region us-east-1 \
    --instance-family t2 \
    --cpu-credits unlimited
```

Afficher la spécification de crédits par défaut

Vous pouvez consulter les spécifications de crédit par défaut d'une famille d'instances T au niveau du compte par AWS région.

Console

Pour consulter les spécifications de crédit par défaut au niveau du compte

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le volet de navigation de gauche, choisissez EC2Dashboard.
4. Dans Account attributes (Attributs de compte), sélectionnez Default credit specification (Spécification de crédits par défaut).

AWS CLI

Pour consulter les spécifications de crédit par défaut au niveau du compte

Utilisez la get-default-credit-specificationcommande. Spécifiez la Région AWS et la famille d'instances.

```
aws ec2 get-default-credit-specification --region us-east-1 --instance-family t2
```

Surveillez les CPU crédits pour les instances instables

EC2envoie des métriques à Amazon CloudWatch. Vous pouvez consulter les statistiques CPU de crédit dans les statistiques EC2 Amazon par instance de la CloudWatch console ou en utilisant le pour AWS CLI répertorier les mesures pour chaque instance. Pour de plus amples informations, veuillez consulter CloudWatch métriques disponibles pour vos instances.

Table des matières

CloudWatch Mesures supplémentaires pour les instances de performance éclatantes

Les instances de performance Burstable disposent des CloudWatch indicateurs supplémentaires suivants, qui sont mis à jour toutes les cinq minutes :

- `CPUCreditUsage`— Le nombre de CPU crédits dépensés pendant la période de mesure.
- `CPUCreditBalance`— Le nombre de CPU crédits accumulés par une instance. Ce solde est épuisé lorsque les CPU rafales et les CPU crédits sont dépensés plus rapidement qu'ils ne sont gagnés.
- `CPUSurplusCreditBalance`— Le nombre de CPU crédits excédentaires dépensés pour soutenir CPU l'utilisation lorsque la `CPUCreditBalance` valeur est nulle.
- `CPUSurplusCreditsCharged`— Le nombre de CPU crédits excédentaires dépassant le nombre maximum de CPU crédits pouvant être obtenus sur une période de 24 heures, et entraînant ainsi des frais supplémentaires.

Les deux dernières métriques s'appliquent uniquement aux instances configurées en mode `unlimited`.

Le tableau suivant décrit les CloudWatch mesures relatives aux instances de performance en rafale. Pour de plus amples informations, veuillez consulter CloudWatch métriques disponibles pour vos instances.

Métrique	Description
`CPUCreditUsage`	Le nombre de CPU crédits dépensés par l'instance pour être CPU utilisés. Un CPU crédit équivaut à un v CPU fonctionnant à 100 % d'utilisation pendant une minute ou une combinaison équivalente d'vCPUsutilisation et de temps (par exemple, un v CPU fonctionnant à 50 % d'utilisation pendant deux minutes ou deux vCPUs fonctionnant à 25 % d'utilisation pendant deux minutes). CPUles indicateurs de crédit ne sont disponibles qu'à une fréquence de cinq minutes. Si vous spécifiez une période supérieure à cinq minutes, utilisez la statistique `Sum` au lieu de la statistique `Average`. Unités : Crédits (v CPU -minutes)
`CPUCreditBalance`	Le nombre de CPU crédits accumulés par une instance depuis son lancement ou son démarrage. Pour les instances T2 Standard, le `CPUCreditBalance` inclut également le nombre de crédits de lancement qui ont été accumulés. Les crédits sont accumulés dans le solde de crédits quand ils sont gagnés et supprimés du solde de crédits lorsqu'ils sont dépensés. Le solde de crédits présente une limite maximum qui est déterminée par la taille de l'instance. Une fois que la limite est atteinte, tous les nouveaux crédits gagnés sont rejetés. Pour les instances T2 Standard, les crédits de lancement ne sont pas comptés dans la limite. Les crédits contenus dans le `CPUCreditBalance` sont disponibles pour que l'instance puisse les dépenser au-delà de son CPU utilisation de base. Les crédits figurant dans le `CPUCreditBalance` d'une instance en cours d'exécution n'expirent pas. Lorsqu'une instance T4g, T3a ou T3 s'arrête, la `CPUCreditBalance` valeur persiste pendant sept jours. Au-delà, tous les crédits

Métrique	Description
	accumulés sont perdus. Lorsqu'une instance T2 s'arrête, la valeur de `CPUCreditBalance` n'est pas conservée, et tous les crédits accumulés sont perdus. CPUles indicateurs de crédit ne sont disponibles qu'à une fréquence de cinq minutes. Unités : Crédits (v CPU -minutes)
`CPUSurplusCreditBalance`	Nombre de crédits excédentaires ayant été dépensés par une instance `unlimited` lorsque la valeur `CPUCreditBalance` est nulle. La `CPUSurplusCreditBalance` valeur est remboursée sous forme de CPU crédits gagnés. Si le nombre de crédits excédentaires dépasse le nombre maximum de crédits que l'instance peut gagner en 24 heures, les crédits excédentaires dépensés au-dessus du maximum génèrent des frais supplémentaires. Unités : Crédits (v CPU -minutes)

Métrique	Description
`CPUSurplusCreditsCharged`	Le nombre de crédits excédentaires dépensés qui ne sont pas remboursés par les CPU crédits gagnés et qui entraînent donc des frais supplémentaires. Les crédits excédentaires dépensés sont facturés lorsque l'une des situations suivantes se produit : • Les crédits excédentaires dépensés dépassent le nombre maximum de crédits que l'instance peut gagner sur une période de 24 heures. Les crédits excédentaires dépensés au-dessus de ce maximum sont facturés à la fin de l'heure. • L'instance est arrêtée ou résiliée. • L'instance bascule du mode `unlimited` au mode `standard`. Unités : Crédits (v CPU -minutes)

Calculer l'utilisation du CPU crédit

L'utilisation du CPU crédit des instances est calculée à l'aide CloudWatch des métriques d'instance décrites dans le tableau précédent.

Amazon EC2 envoie les statistiques CloudWatch toutes les cinq minutes. Une référence à la valeur antérieure d'une métrique à un moment donné désigne la valeur précédente de cette métrique, envoyée 5 minutes auparavant.

Calculer l'utilisation du CPU crédit pour les instances standard

- Le solde CPU créditeur augmente si CPU l'utilisation est inférieure au niveau de référence, lorsque les crédits dépensés sont inférieurs aux crédits gagnés au cours de l'intervalle de cinq minutes précédent.
- Le solde CPU créditeur diminue si CPU l'utilisation est supérieure au niveau de référence, lorsque les crédits dépensés sont supérieurs aux crédits gagnés au cours de l'intervalle de cinq minutes précédent.

Cette description est illustrée d'un point de vue mathématique par l'équation suivante:

Example

```
CPUCreditBalance = prior CPUCreditBalance + [Credits earned per hour * (5/60) -
 CPUCreditUsage]
```

La taille de l'instance détermine le nombre de crédits que l'instance peut gagner par heure, ainsi que le nombre de crédits gagnés qu'elle peut accumuler dans le solde de crédits. Pour plus d'informations sur le nombre de crédits gagnés par heure et la limite du solde de crédits pour chaque taille d'instance, consultez le tableau des crédits.

Exemple

Dans cet exemple, une instance `t3.nano` est utilisée. Pour calculer la valeur de `CPUCreditBalance` de l'instance, utilisez l'équation précédente comme suit :

- `CPUCreditBalance` – Solde de crédits actuel à calculer.
- `prior CPUCreditBalance` – Solde de crédits cinq minutes auparavant. Dans cet exemple, l'instance a accumulé deux crédits.
- `Credits earned per hour` – Une instance `t3.nano` gagne six crédits par heure.
- `5/60`— Représente l'intervalle de cinq minutes entre la publication des CloudWatch métriques. Multipliez les crédits gagnés par heure par 5/60 (cinq minutes) pour obtenir le nombre de crédits gagnés par l'instance au cours des cinq dernières minutes. Une instance `t3.nano` gagne 0,5 crédits toutes les cinq minutes.
- `CPUCreditUsage` – Nombre de crédits dépensés par l'instance au cours des cinq dernières minutes. Dans cet exemple, l'instance a dépensé un crédit au cours des cinq dernières minutes.

Vous pouvez calculer la valeur du `CPUCreditBalance` à l'aide de ces valeurs :

Example

```
CPUCreditBalance = 2 + [0.5 - 1] = 1.5
```

Calculer l'utilisation du CPU crédit pour un nombre illimité d'instances

Lorsqu'une instance de performance à capacité extensible doit dépasser le niveau de base, elle dépense toujours ses crédits accumulés avant de dépenser les crédits excédentaires. Lorsqu'elle

épuise son solde CPU créditeur accumulé, elle peut dépenser ses crédits excédentaires CPU pour augmenter aussi longtemps qu'elle en a besoin. Lorsque CPU l'utilisation tombe en dessous du niveau de référence, les crédits excédentaires sont toujours remboursés avant que l'instance n'accumule les crédits gagnés.

Nous employons le terme `Adjusted balance` dans les équations suivantes pour refléter l'activité qui se produit dans cet intervalle de cinq minutes. Nous utilisons cette valeur pour obtenir les valeurs des `CPUSurplusCreditBalance` CloudWatch métriques `CPUCreditBalance` et.

Example

```
Adjusted balance = [prior CPUCreditBalance - prior CPUSurplusCreditBalance] + [Credits
 earned per hour * (5/60) - CPUCreditUsage]
```

La valeur `0` du `Adjusted balance` indique que l'instance a dépensé l'ensemble de ses crédits gagnés pour une utilisation en mode rafale et qu'aucun crédit excédentaire n'a été dépensé. Le `CPUCreditBalance` et le `CPUSurplusCreditBalance` sont donc tous deux définis sur `0`.

Une valeur positive pour le `Adjusted balance` indique que l'instance a accumulé des crédits gagnés, et que les crédits excédentaires précédents, le cas échéant, ont été remboursés. En conséquence, la valeur du `Adjusted balance` est attribuée au `CPUCreditBalance`, et le `CPUSurplusCreditBalance` est défini sur `0`. La taille de l'instance détermine le nombre maximal de crédits qu'elle peut accumuler.

Example

```
CPUCreditBalance = min [max earned credit balance, Adjusted balance]
CPUSurplusCreditBalance = 0
```

Une valeur négative pour le `Adjusted balance` indique que l'instance a dépensé tous les crédits gagnés qu'elle a accumulés, ainsi que des crédits excédentaires pour une utilisation en mode rafale. En conséquence, la valeur de `Adjusted balance` est attribuée à `CPUSurplusCreditBalance` et le `CPUCreditBalance` est défini sur `0`. Là encore, la taille de l'instance détermine le nombre maximal de crédits qu'elle peut accumuler.

Example

```
CPUSurplusCreditBalance = min [max earned credit balance, -Adjusted balance]
```

```
CPUCreditBalance = 0
```

Si les crédits excédentaires dépensés dépassent le nombre maximal de crédits que l'instance peut accumuler, le solde de crédits excédentaires est défini sur le maximum, comme le montre l'équation précédente. Les crédits excédentaires restants représentés par la métrique `CPUSurplusCreditsCharged` sont facturés.

Example

```
CPUSurplusCreditsCharged = max [-Adjusted balance - max earned credit balance, 0]
```

Pour finir, lorsque l'instance est résiliée, les crédits excédentaires suivis par le `CPUSurplusCreditBalance` sont facturés. Si l'instance bascule du mode `unlimited` au mode `standard`, tout solde `CPUSurplusCreditBalance` restant éventuel est également facturé.

Accélération des performances grâce aux GPU instances

GPUles instances basées fournissent un accès à NVIDIA GPUs des milliers de cœurs de calcul. Vous pouvez utiliser ces instances pour accélérer les applications scientifiques, d'ingénierie et de rendu en tirant parti des frameworks CUDA de calcul parallèle OpenCL (Open Computing Language). Vous pouvez également les utiliser pour des applications graphiques, notamment les jeux en streaming, les applications 3D en streaming, et d'autres charges de travail graphiques.

Avant de pouvoir activer ou optimiser une instance GPU basée, vous devez installer les pilotes appropriés, comme suit :

- Pour installer des NVIDIA pilotes sur une instance associée NVIDIAGPU, telle qu'une instance P3 ou G4dn, consultez. NVIDIApilotes
- Pour installer des AMD pilotes sur une instance associée AMDGPU, telle qu'une instance G4ad, consultez. AMDpilotes

Table des matières

Activez des applications NVIDIA GRID virtuelles sur vos instances EC2 GPU basées sur Amazon

Pour activer les applications GRID virtuelles sur des GPU instances qui en ont NVIDIA GPUs (NVIDIAGRIDVirtual Workstation est activé par défaut), vous devez définir le type de produit pour le pilote. Le processus que vous utilisez dépend du système d'exploitation de votre instance.

Instances Linux

Pour activer les applications GRID virtuelles sur vos instances Linux

1. Créez le fichier `/etc/nvidia/gridd.conf` à partir du modèle de fichier fourni.

   ```
   [ec2-user ~]$ sudo cp /etc/nvidia/gridd.conf.template /etc/nvidia/gridd.conf
   ```

2. Ouvrez le fichier `/etc/nvidia/gridd.conf` dans votre éditeur de texte favori.
3. Trouvez la ligne `FeatureType` et affectez-lui la valeur `0`. Puis ajoutez une ligne avec `IgnoreSP=TRUE`.

   ```
   FeatureType=0 IgnoreSP=TRUE
   ```

4. Enregistrez le fichier et quittez l'éditeur.
5. Redémarrez l'instance pour récupérer la nouvelle configuration.

   ```
   [ec2-user ~]$ sudo reboot
   ```

instances Windows

Pour activer les applications GRID virtuelles sur vos instances Windows

1. Exécutez regedit.exe pour ouvrir l'éditeur de registre.
2. Accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global \GridLicensing`.
3. Ouvrez le menu contextuel (clic droit) dans le volet droit et choisissez Nouveau, DWORD.
4. Dans le champ Nom, entrez FeatureTypeet tapez`Enter`.
5. Ouvrez le menu contextuel (clic droit) FeatureTypeet choisissez Modifier.

6. Pour les données de valeur, entrez `0` pour Applications NVIDIA GRID virtuelles et cliquez sur OK.
7. Ouvrez le menu contextuel (clic droit) dans le volet droit et choisissez Nouveau, DWORD.
8. Pour Nom, saisissez IgnoreSP, puis tapez `Enter`.
9. Ouvrez le menu contextuel (clic droit) sur IgnoreSP et sélectionnez Modifier.
10. Pour Données de la valeur, tapez 1 et cliquez sur OK.
11. Fermez l'éditeur de registre.

Optimisation GPU des paramètres sur les EC2 instances Amazon

Il existe plusieurs optimisations de GPU paramètres que vous pouvez effectuer pour obtenir les meilleures performances sur NVIDIA GPU les instances. Avec certains de ces types d'instances, le NVIDIA pilote utilise une fonction d'accélération automatique, qui fait varier les vitesses d'GPUhorloge. En désactivant l'autoboost et en réglant les vitesses d'GPUhorloge sur leur fréquence maximale, vous pouvez toujours obtenir des performances maximales avec vos GPU instances.

Optimisation GPU des paramètres sous Linux

1. Configurez les GPU paramètres pour qu'ils soient persistants. L'exécution de cette commande peut prendre plusieurs minutes.

   ```
   [ec2-user ~]$ sudo nvidia-persistenced
   ```

2. [Instances G3 et P2 uniquement] Désactivez la fonction Autoboost pour tous les utilisateurs de GPUs l'instance.

   ```
   [ec2-user ~]$ sudo nvidia-smi --auto-boost-default=0
   ```

3. Réglez toutes les vitesses d'GPUhorloge sur leur fréquence maximale. Utilisez les vitesses d'horloge de mémoire et de graphiques spécifiées dans les commandes suivantes.

   Certaines versions du NVIDIA pilote ne prennent pas en charge le réglage de la vitesse d'horloge de l'application et affichent l'erreur"`Setting applications clocks is not supported for GPU...`", que vous pouvez ignorer.

   - instances G3 :

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 2505,1177
     ```

- instances G4dn :

```
[ec2-user ~]$ sudo nvidia-smi -ac 5001,1590
```

- Instances G5 :

```
[ec2-user ~]$ sudo nvidia-smi -ac 6250,1710
```

- Instances G6 et Gr6 :

```
[ec2-user ~]$ sudo nvidia-smi -ac 6251,2040
```

- Instances G6e :

```
[ec2-user ~]$ sudo nvidia-smi -ac 9001,2520
```

- instances P2 :

```
[ec2-user ~]$ sudo nvidia-smi -ac 2505,875
```

- instances P3 et P3dn :

```
[ec2-user ~]$ sudo nvidia-smi -ac 877,1530
```

- instances P4d :

```
[ec2-user ~]$ sudo nvidia-smi -ac 1215,1410
```

- Instances P4de :

```
[ec2-user ~]$ sudo nvidia-smi -ac 1593,1410
```

- Instances P5 :

```
[ec2-user ~]$ sudo nvidia-smi -ac 2619,1980
```

Optimisation GPU des paramètres sous Windows

1. Ouvrez une PowerShell fenêtre et accédez au dossier NVIDIA d'installation.

```
cd "C:\Windows\System32\DriverStore\FileRepository\nvgridsw_aws.inf_*\"
```

2. [Instances G3 et P2 uniquement] Désactivez la fonction Autoboost pour tous les utilisateurs de GPUs l'instance.

```
.\nvidia-smi --auto-boost-default=0
```

3. Réglez toutes les vitesses d'GPUhorloge sur leur fréquence maximale. Utilisez les vitesses d'horloge de mémoire et de graphiques spécifiées dans les commandes suivantes.

   Certaines versions du NVIDIA pilote ne prennent pas en charge le réglage de la vitesse d'horloge de l'application et affichent l'erreur"`Setting applications clocks is not supported for GPU...`", que vous pouvez ignorer.

   - instances G3 :

     ```
     .\nvidia-smi -ac "2505,1177"
     ```

   - instances G4dn :

     ```
     .\nvidia-smi -ac "5001,1590"
     ```

   - Instances G5 :

     ```
     .\nvidia-smi -ac "6250,1710"
     ```

   - Instances G6 et Gr6 :

     ```
     .\nvidia-smi -ac "6251,2040"
     ```

   - Instances G6e :

     ```
     .\nvidia-smi -ac "9001,2520"
     ```

   - instances P2 :

     ```
     .\nvidia-smi -ac "2505,875"
     ```

   - instances P3 et P3dn :

```
.\nvidia-smi -ac "877,1530"
```

Configuration de deux écrans 4K sur les instances G4ad Linux

Après avoir lancé une instance G4ad, vous pouvez configurer deux écrans 4K.

Pour installer les AMD pilotes et configurer les écrans doubles

1. Connectez-vous à votre instance Linux pour obtenir l'adresse du PCI bus que GPU vous souhaitez cibler pour la double résolution 4K (2 x 4 k) :

   ```
   lspci -vv | grep -i amd
   ```

   Vous obtenez une sortie similaire à ce qui suit :

   ```
   00:1e.0 Display controller: Advanced Micro Devices, Inc. [*AMD*/ATI] Device 7362 (rev
    c3)
   Subsystem: Advanced Micro Devices, Inc. [AMD/ATI] Device 0a34
   ```

2. Notez que l'adresse du PCI bus est 00:1 e.0 dans la sortie ci-dessus. Créez un fichier nommé `/etc/modprobe.d/amdgpu.conf` et ajoutez :

   ```
   options amdgpu virtual_display=0000:00:1e.0,2
   ```

3. Pour installer les AMD pilotes sous Linux, voirAMDpilotes pour votre EC2 instance. Si le AMD GPU pilote est déjà installé, vous devrez reconstruire les modules du noyau amdgpu via dkms.

4. Utilisez le fichier xorg.conf ci-dessous pour définir la topologie de l'écran double (2x4K) et enregistrez le fichier dans `/etc/X11/xorg.conf:`

   ```
   ~$ cat /etc/X11/xorg.conf
   Section "ServerLayout"
       Identifier     "Layout0"
       Screen          0 "Screen0"
       Screen        1 "Screen1"
       InputDevice     "Keyboard0" "CoreKeyboard"
       InputDevice     "Mouse0" "CorePointer"
       Option          "Xinerama" "1"
   EndSection
   Section "Files"
   ```

```
    ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
    ModulePath "/opt/amdgpu/lib/xorg/modules"
    ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
    ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
    ModulePath "/usr/lib64/xorg/modules"
    ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Mouse0"
    Driver         "mouse"
    Option         "Protocol" "auto"
    Option         "Device" "/dev/psaux"
    Option         "Emulate3Buttons" "no"
    Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Keyboard0"
    Driver         "kbd"
EndSection

Section "Monitor"
    Identifier     "Virtual"
    VendorName     "Unknown"
    ModelName      "Unknown"
    Option         "Primary" "true"
EndSection

Section "Monitor"
    Identifier     "Virtual-1"
    VendorName     "Unknown"
    ModelName      "Unknown"
    Option         "RightOf" "Virtual"
EndSection

Section "Device"
    Identifier     "Device0"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection
```

```
Section "Device"
    Identifier     "Device1"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection

Section "Extensions"
    Option         "DPMS" "Disable"
EndSection

Section "Screen"
    Identifier     "Screen0"
    Device         "Device0"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection

Section "Screen"
    Identifier     "Screen1"
    Device         "Device1"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection
```

5. Configurez DCV en suivant les instructions de la section Configuration d'un bureau interactif.
6. Une fois la DCV configuration terminée, redémarrez.
7. Confirmez que le pilote est fonctionnel :

```
dmesg | grep amdgpu
```

Les résultats doivent avoir l'aspect suivant :

```
Initialized amdgpu
```

8. Vous devriez voir dans la sortie pour `DISPLAY=:0 xrandr -q` que vous avez 2 écrans virtuels connectés :

```
~$ DISPLAY=:0 xrandr -q
Screen 0: minimum 320 x 200, current 3840 x 1080, maximum 16384 x 16384
Virtual connected primary 1920x1080+0+0 (normal left inverted right x axis y axis)
 0mm x 0mm
 4096x3112  60.00
 3656x2664  59.99
 4096x2160  60.00
 3840x2160  60.00
 1920x1200  59.95
 1920x1080  60.00
 1600x1200  59.95
 1680x1050  60.00
 1400x1050  60.00
 1280x1024  59.95
 1440x900 59.99
 1280x960 59.99
 1280x854 59.95
 1280x800 59.96
 1280x720 59.97
 1152x768 59.95
 1024x768 60.00 59.95
 800x600  60.32 59.96 56.25
 848x480  60.00 59.94
 720x480  59.94
 640x480  59.94 59.94
Virtual-1 connected 1920x1080+1920+0 (normal left inverted right x axis y axis) 0mm x
 0mm
 4096x3112  60.00
 3656x2664  59.99
 4096x2160  60.00
 3840x2160  60.00
 1920x1200  59.95
 1920x1080  60.00
 1600x1200  59.95
 1680x1050  60.00
```

```
 1400x1050  60.00
 1280x1024  59.95
 1440x900 59.99
 1280x960 59.99
 1280x854 59.95
 1280x800 59.96
 1280x720 59.97
 1152x768 59.95
 1024x768 60.00 59.95
 800x600  60.32 59.96 56.25
 848x480  60.00 59.94
 720x480  59.94
640x480  59.94 59.94
```

9. Lorsque vous vous connectezDCV, modifiez la résolution en 2x4K, en confirmant que la prise en charge du double moniteur est enregistrée parDCV.

Configuration d'un bureau interactif pour Linux

Après avoir confirmé que le AMD GPU pilote est installé sur votre instance Linux et qu'amdgpu est utilisé, vous pouvez installer un gestionnaire de bureau interactif. Nous recommandons l'environnement MATE de bureau pour une compatibilité et des performances optimales.

Prérequis

Lancez un éditeur de texte et enregistrez ce qui suit en tant que fichier nommé `xorg.conf`. Vous aurez besoin de ce fichier sur votre instance.

```
Section "ServerLayout"
Identifier     "Layout0"
Screen          0 "Screen0"
InputDevice     "Keyboard0" "CoreKeyboard"
InputDevice     "Mouse0" "CorePointer"
EndSection
Section "Files"
ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
ModulePath "/opt/amdgpu/lib/xorg/modules"
ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
```

```
ModulePath "/usr/lib64/xorg/modules"
ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
# generated from default
Identifier     "Mouse0"
Driver         "mouse"
Option         "Protocol" "auto"
Option         "Device" "/dev/psaux"
Option         "Emulate3Buttons" "no"
Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
# generated from default
Identifier     "Keyboard0"
Driver         "kbd"
EndSection
Section "Monitor"
Identifier     "Monitor0"
VendorName     "Unknown"
ModelName      "Unknown"
EndSection
Section "Device"
Identifier     "Device0"
Driver         "amdgpu"
VendorName     "AMD"
BoardName      "Radeon MxGPU V520"
BusID          "PCI:0:30:0"
EndSection
Section "Extensions"
Option         "DPMS" "Disable"
EndSection
Section "Screen"
Identifier     "Screen0"
Device         "Device0"
Monitor        "Monitor0"
DefaultDepth   24
Option         "AllowEmptyInitialConfiguration" "True"
SubSection "Display"
    Virtual    3840 2160
    Depth      32
EndSubSection
EndSection
```

Pour configurer un bureau interactif sur Amazon Linux 2

1. Installez le EPEL référentiel.

```
$ C:\> sudo amazon-linux-extras install epel -y
```

2. Installez le MATE bureau.

```
$ C:\> sudo amazon-linux-extras install mate-desktop1.x -y
$ C:\> sudo yum groupinstall "MATE Desktop" -y
$ C:\> sudo systemctl disable firewalld
```

3. Copiez le fichier `xorg.conf` dans `/etc/X11/xorg.conf`.
4. Redémarrez l'instance.

```
$ C:\> sudo reboot
```

5. (Facultatif) Installez le NICE DCV serveur à utiliser NICE DCV comme protocole d'affichage haute performance, puis connectez-vous à une NICE DCV session à l'aide de votre client préféré.

Pour configurer un bureau interactif sur Ubuntu

1. Installez le MATE bureau.

```
$ sudo apt install xorg-dev ubuntu-mate-desktop -y
$ C:\> sudo apt purge ifupdown -y
```

2. Copiez le fichier `xorg.conf` dans `/etc/X11/xorg.conf`.
3. Redémarrez l'instance.

```
$ sudo reboot
```

4. Installez l'AMFencodeur correspondant à la version appropriée d'Ubuntu.

```
$ sudo apt install ./amdgpu-pro-20.20-*/amf-amdgpu-pro_20.20-*_amd64.deb
```

5. (Facultatif) Installez le NICE DCV serveur à utiliser NICE DCV comme protocole d'affichage haute performance, puis connectez-vous à une NICE DCV session à l'aide de votre client préféré.

6. Après l'DCVinstallation, donnez à l'DCVutilisateur les autorisations vidéo :

```
$ sudo usermod -aG video dcv
```

Pour configurer un bureau interactif sur CentOS

1. Installez le EPEL référentiel.

```
$ sudo yum update -y
$ C:\> sudo yum install epel-release -y
```

2. Installez le MATE bureau.

```
$ sudo yum groupinstall "MATE Desktop" -y
$ C:\> sudo systemctl disable firewalld
```

3. Copiez le fichier `xorg.conf` dans `/etc/X11/xorg.conf`.
4. Redémarrez l'instance.

```
$ sudo reboot
```

5. (Facultatif) Installez le NICE DCV serveur à utiliser NICE DCV comme protocole d'affichage haute performance, puis connectez-vous à une NICE DCV session à l'aide de votre client préféré.

Démarrage avec les instances P5

Les instances P5 fournissent 8 NVIDIA H100 GPUs avec 640 Go de mémoire à bande passante élevéeGPU. Ils sont équipés de AMD EPYC processeurs de 3e génération et fournissent 2 To de mémoire système, 30 To de stockage d'NVMeinstance local, 3 200 Gbit/s de bande passante réseau agrégée et GPUDirect RDMA un support. Les instances P5 prennent également en charge EC2 UltraCluster la technologie Amazon, qui permet de réduire la latence et d'améliorer les performances du réseau. EFA

Le tableau suivant présente un résumé des spécifications `p5.48xlarge`.

vCPUs	Mémoire système	GPUs	GPUmémoire	Bande passante réseau	GPUDirect RDMA	GPUpair à pair	Stockage d'instances
192	2 Tio	8 NVIDIA H100 GPUs	640 Go HBM3	3200 Gbit/s avec EFAv2	Pris en charge	900 Gbit/s NVSw	8 volumes de 3 800 Go NVMe SSD

Configuration logicielle :

Le moyen le plus simple de démarrer avec les instances P5 est de lancer une instance à l'aide d'un AWS Deep Learning AMIs qui est préconfiguré avec tous les logiciels requis. Pour les dernières versions AWS Deep Learning AMIs à utiliser avec les instances P5, consultez la base d'apprentissage AWS profond GPU AMI (Ubuntu 20.04).

Si vous devez créer une version personnalisée à utiliser avec AMI les instances P5, nous vous recommandons d'installer les versions logicielles minimales suivantes :

- NVIDIApilote 535.54.03 ou version ultérieure
- CUDA12.1 ou version ultérieure
- NVIDIAGDRCopy2.3 ou version ultérieure
- EFAinstaller 1.24.1 ou version ultérieure
- NCCL2.18.3 ou version ultérieure
- aws-ofi-nccl plugin 1.7.2-aws ou version ultérieure

Nous vous recommandons également de configurer l'instance de façon à ne pas utiliser d'états C plus profonds. Pour plus d'informations, consultez la section Performances élevées et faible latence en limitant les états C plus profonds dans le guide de l'utilisateur Amazon Linux 2. La dernière base de AWS Deep Learning GPU AMI est préconfigurée pour ne pas utiliser d'états C plus profonds.

Recommandations spécifiques à Ubuntu 20.04

Les recommandations suivantes pour Ubuntu 20.04 permettent d'éviter les noms d'interface imprévisibles au démarrage :

- Assurez-vous que vous utilisez `systemd 245.4-4ubuntu3.19` ou une version ultérieure en exécutant la commande suivante :

```
systemd --version
```

- Assurez-vous d'avoir configuré GRUB :
  - Ouvrez le fichier de configuration `/etc/default/grub` dans un éditeur de texte.
  - Modifiez l'entrée `GRUB_CMDLINE_LINUX_DEFAULT` pour l'inclure `net.naming-scheme=v247`.
  - Redémarrez votre instance en exécutant `sudo update-grub`.

Mise en réseau et EFA configuration

Les instances P5 fournissent 3 200 Gbit/s de bande passante réseau en utilisant plusieurs interfaces. EFA Les instances P5 prennent en charge 32 cartes réseau. Nous vous recommandons de définir une seule interface EFA réseau par carte réseau. Pour configurer ces interfaces au lancement, nous vous recommandons d'utiliser les paramètres suivants :

- Pour l'interface réseau `0`, spécifiez l'index d'appareils `0`.
- Pour les interfaces réseaux `1` à `31`, spécifiez l'index d'appareils `1`.

Pour plus d'informations sur la configuration de vos instances P5, EFA consultezMaximisez la bande passante réseau sur les instances de calcul accéléré avec EFA.

Instances Amazon EC2 Mac

EC2Les instances Mac sont idéales pour développer, créer, tester et signer des applications pour les plateformes Apple iPhoneiPad, telles que Mac, Vision Pro, Apple Watch, Apple TV et Safari. Vous pouvez vous connecter à votre instance Mac à l'aide SSH d'Apple Remote Desktop (ARD).

> **Note**
>
> L'unité de facturation est l'hôte dédié. Les instances exécutées sur cet hôte n'engendrent pas de frais supplémentaires.

Les instances Amazon EC2 Mac prennent en charge de manière native le système d'exploitation macOS.

- EC2Les instances Mac x86 (`mac1.metal`) sont basées sur du matériel Mac mini 2018 alimenté par des GHz processeurs Intel Core i7 3.2 de huitième génération (Coffee Lake).
- EC2Les instances Mac M1 (`mac2.metal`) sont basées sur du matériel Mac mini 2020 alimenté par des processeurs Apple Silicon M1.
- EC2Les instances M1 Ultra Mac (`mac2-m1ultra.metal`) sont basées sur du matériel Mac Studio 2022 alimenté par des processeurs Apple Silicon M1 Ultra.
- EC2Les instances M2 Mac (`mac2-m2.metal`) sont basées sur du matériel Mac mini 2023 alimenté par des processeurs M2 au silicium Apple.
- EC2Les instances Mac M2 Pro (`mac2-m2pro.metal`) sont basées sur du matériel Mac mini 2023 alimenté par des processeurs Apple Silicon M2 Pro.

Table des matières

Considérations

Les considérations suivantes s'appliquent aux instances Mac :

- Les instances Mac ne sont disponibles qu'en tant qu'instances à matériel nu sur Hôtes dédiés, avec une période d'allocation minimale de 24 heures avant de pouvoir libérer l'Hôte dédié. Vous pouvez lancer une instance Mac par Hôte dédié. Vous pouvez partager l'hôte dédié avec les AWS comptes ou les unités organisationnelles de votre AWS organisation, ou avec l'ensemble de AWS l'organisation.
- Les instances Mac sont disponibles en différentes versions Régions AWS. Pour obtenir une liste de la disponibilité des instances Mac dans chacune des régions Régions AWS, consultez la section Types d'EC2instances Amazon par région.
- Les instances Mac ne sont disponibles qu'en tant que instances à la demande. Ils ne sont pas disponibles en tant que instances Spot ou instances réservées. Vous pouvez effectuer des économies sur les instances Mac en souscrivant à un Savings Plan.
- Les instances Mac peuvent exécuter l'un des systèmes d'exploitation suivants :
  - macOS Mojave (version 10.14) (instances Mac basées sur x86 uniquement)
  - macOS Catalina (version 10.15) (instances Mac basées sur x86 uniquement)
  - macOS Big Sur (version 11) (instances Mac basées sur x86 et M1)
  - macOS Monterey (version 12) (instances Mac basées sur x86 et M1)
  - macOS Ventura (version 13) (toutes les instances Mac, instances M2 et Mac M2 Pro compatibles avec macOS Ventura version 13.2 ou ultérieure)
  - macOS Sonoma (version 14) (toutes les instances Mac)
- EBSle hotplug est pris en charge.
- AWS ne gère ni ne prend en charge le matériel interne SSD d'Apple. Nous vous recommandons vivement d'utiliser plutôt EBS les volumes Amazon. EBSles volumes offrent les mêmes avantages en termes d'élasticité, de disponibilité et de durabilité sur les instances Mac que sur toute autre EC2 instance.
- Nous recommandons d'utiliser les instances General Purpose SSD (`gp2`et`gp3`) et Provisioned IOPS SSD (`io1`et`io2`) avec les instances Mac pour des EBS performances optimales.
- Les instances Mac sont compatibles avec Amazon EC2 Auto Scaling.
- Sur les instances Mac basées sur x86, les mises à jour logicielles automatiques sont désactivées. Nous vous recommandons d'appliquer les mises à jour et de les tester sur votre instance avant de mettre l'instance en production. Pour plus d'informations, consultez Mettre à jour le système d'exploitation et le logiciel sur les instances Mac.

- Lorsque vous arrêtez ou résiliez une instance Mac, un workflow de nettoyage est effectué sur Hôte dédié. Pour de plus amples informations, veuillez consulter Arrêtez ou mettez fin à votre instance Amazon EC2 Mac.

> **Warning**
>
> Ne pas utiliser FileVault. L'activation FileVault empêchera le démarrage de l'hôte en raison du verrouillage des partitions. Si le chiffrement des données est requis, utilisez le EBS chiffrement Amazon pour éviter les problèmes de démarrage et l'impact sur les performances. Avec Amazon EBS Encryption, les opérations de chiffrement sont effectuées sur les serveurs hébergeant les instances, garantissant ainsi la sécurité data-in-transit entre une instance data-at-rest et le EBS stockage qui lui est rattaché. Pour plus d'informations, consultez Amazon EBS Encryption dans le guide de EBS l'utilisateur Amazon

Préparation de l'instance

Après avoir lancé une instance Mac, vous devez attendre qu'elle soit prête avant de pouvoir vous y connecter. Pour un AWS appareil vendu AMI avec une instance Mac x86 ou une instance Apple Silicon Mac, le délai de lancement peut aller d'environ 6 minutes à 20 minutes. En fonction de la taille des EBS volumes Amazon choisie, de l'inclusion de scripts supplémentaires dans les données utilisateur ou de logiciels supplémentaires chargés sur un macOS personnaliséAMI, le délai de lancement peut augmenter.

Vous pouvez utiliser un petit script shell, comme celui ci-dessous, pour interroger le describe-instance-status API afin de savoir quand l'instance est prête à être connectée. Dans la commande suivante, remplacez l'exemple d'ID d'instance par le vôtre.

```
for i in $(seq 1 200); do aws ec2 describe-instance-status --instance-
ids=i-0123456789example \
    --query='InstanceStatuses[0].InstanceStatus.Status'; sleep 5; done;
```

EC2macOS AMIs

Amazon EC2 macOS est conçu pour fournir un environnement stable, sécurisé et performant pour les charges de travail des développeurs exécutées sur des instances Amazon EC2 Mac. EC2macOS AMIs inclut des packages qui permettent une intégration facile AWS, tels que les outils de configuration de lancement et les AWS bibliothèques et outils populaires.

Pour plus d'informations sur EC2 macOSAMIs, consultezNotes de AMIs mise à jour d'Amazon EC2 macOS.

AWS fournit régulièrement des mises à jour de EC2 macOSAMIs, notamment des mises à jour des packages appartenant à macOS AWS et de la dernière version entièrement testée de macOS. En outre, AWS fournit des mises à jour AMIs avec les dernières mises à jour des versions mineures ou majeures dès qu'elles peuvent être entièrement testées et approuvées. Si vous n'avez pas besoin de conserver les données ou de personnaliser vos instances Mac, vous pouvez obtenir les dernières mises à jour en lançant une nouvelle instance à l'aide de l'instance actuelle, AMI puis en mettant fin à l'instance précédente. Sinon, vous pouvez choisir les mises à jour à appliquer à vos instances Mac.

Pour plus d'informations sur la façon de s'abonner aux AMI notifications macOS, consultezS'abonner aux AMI notifications macOS.

EC2macOS Init

EC2macOS Init est utilisé pour initialiser les instances EC2 Mac au lancement. Il utilise des groupes de priorités pour exécuter des groupes logiques de tâches en même temps.

Le fichier launchd plist est `/Library/LaunchDaemons/com.amazon.ec2.macos-init.plist`. Les fichiers de EC2 macOS Init se trouvent dans`/usr/local/aws/ec2-macos-init`.

Pour plus d'informations, consultez https://github.com/aws/ec2-macos-init.

Amazon EC2 System Monitor pour macOS

Amazon EC2 System Monitor pour macOS fournit des statistiques CPU d'utilisation à Amazon CloudWatch. Il envoie ces métriques à CloudWatch un périphérique série personnalisé par périodes d'une minute. Vous pouvez activer ou désactiver cet agent comme suit. Il est activé par défaut.

```
sudo setup-ec2monitoring [enable | disable]
```

> **Note**
>
> Amazon EC2 System Monitor pour macOS n'est actuellement pas compatible avec les instances Apple Silicon Mac.

Ressources connexes

Pour plus d'informations sur la tarification, consultez Tarification .

Pour plus d'informations sur les instances Mac, consultez Amazon EC2 Mac Instances.

Pour plus d'informations sur les spécifications matérielles et les performances réseau des instances Mac, consultez la section Instances à usage général.

Lancez une instance Mac à l' AWS Management Console aide du AWS CLI

EC2Les instances Mac nécessitent un hôte dédié. Vous devez d'abord attribuer un hôte à votre compte, puis lancer l'instance sur cet hôte.

Vous pouvez lancer une instance Mac à l'aide du AWS Management Console ou du AWS CLI.

Lancer une instance Mac à l'aide de la console

Pour lancer une instance Mac sur un Hôte dédié

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Allouez l'hôte dédié, comme suit :
    a. Dans le volet de navigation, choisissez Hôtes dédiés.
    b. Choisissez Allouer Hôte dédié , puis procédez comme suit :
        i. Pour la famille d'instances, choisissez mac1, mac2, mac2-m2, mac2-m2pro ou mac2-m1ultra. Si la famille de·l'instance n'apparaît pas dans la liste, elle n'est pas prise en charge dans la région actuellement sélectionnée.
        ii. Pour le type d'instance, choisissez mac1.metal, mac2.metal, mac2-m2.metal, mac2-m2pro.metal ou mac2-m1ultra.metal en fonction de la famille d'instances choisie.
        iii. Pour Zone de disponibilité, choisissez la zone de disponibilité pour votre Hôte dédié.
        iv. Pour Quantity (Quantité), conservez 1.
        v. Choisissez Allouer.
3. Lancez l'instance sur l'hôte, comme suit :
    a. Sélectionnez le Hôte dédié que vous avez créé, puis procédez comme suit :
        i. Choisissez Actions, puis Launch instance(s) onto host (Lancer les instances sur l'hôte).
        ii. Sous Images de l'application et du système d'exploitation (Amazon Machine Image), sélectionnez un macOSAMI.
        iii. Sous Type d'instance, sélectionnez le type d'instance approprié (mac1.metal, mac2.metal, mac2-m2.metal, mac2-m2pro.metal ou mac2-m1ultra.metal).

iv. Sous Advanced details (Détails avancés), vérifiez que les paramètres Tenancy (Location), Tenancy host by (Hôte de location par) et Tenancy host ID (ID d'hôte de location) sont préconfigurés en fonction de l'hôte dédié que vous avez créé. Mettez à jour la valeur Tenancy affinity (Affinité de location), si nécessaire.

v. Complétez l'assistant en spécifiant EBS les volumes, les groupes de sécurité et les paires de clés selon vos besoins.

vi. Dans le panneau Summary (Récapitulatif), sélectionnez Launch instance (Lancer l'instance).

b. Une page de confirmation indique que l'instance est en cours de lancement. Sélectionnez View all instances (Afficher toutes les instances) pour fermer la page de confirmation et revenir à la console. L'état initial d'une instance est `pending`. L'instance est prête lorsque son état passe à `running` et qu'elle passe avec succès les vérifications de statut.

Lancez une instance Mac à l'aide du AWS CLI

Allouer l'hôte dédié

Utilisez la commande allocate-hosts suivante pour allouer un hôte dédié à votre instance Mac, en `instance-type` remplaçant le par `mac1.metalmac2.metal`,`mac2-m2.metal`, ou `mac2-m2pro.metalmac2-m1ultra.metal`, et par les `region` hôtes appropriés `availability-zone` à votre environnement.

```
aws ec2 allocate-hosts --region us-east-1 --instance-type mac1.metal --availability-
zone us-east-1b --auto-placement "on" --quantity 1
```

Lancer l'instance sur l'hôte

Utilisez la commande run-instances suivante pour lancer une instance Mac, en remplaçant à nouveau le `instance-type` par`mac1.metal`,`mac2.metal`, `mac2-m2.metalmac2-m2pro.metal`, ou`mac2-m1ultra.metal`, et le `region` et `availability-zone` par ceux utilisés précédemment.

```
aws ec2 run-instances --region us-east-1 --instance-type mac1.metal --placement
 Tenancy=host --image-id ami_id --key-name my-key-pair
```

L'état initial d'une instance est `pending`. L'instance est prête lorsque son état passe à `running` et qu'elle passe avec succès les vérifications de statut. Utilisez la describe-instance-statuscommande suivante pour afficher les informations d'état de votre instance.

```
aws ec2 describe-instance-status --instance-ids i-017f8354e2dc69c4f
```

Voici un exemple de sortie pour une instance qui est en cours d'exécution et qui a passé avec succès les contrôles de statut.


```
{
    "InstanceStatuses": [
        {
            "AvailabilityZone": "us-east-1b",
            "InstanceId": "i-017f8354e2dc69c4f",
            "InstanceState": {
                "Code": 16,
                "Name": "running"
            },
            "InstanceStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
                ],
                "Status": "ok"
            },
            "SystemStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
                ],
                "Status": "ok"
            }
        }
    ]
}
```


Connectez-vous à votre instance Mac à l'aide SSH d'un GUI

Vous pouvez vous connecter à votre instance Mac à l'aide SSH d'une interface utilisateur graphique (GUI).

Connexion à votre instance à l'aide d'SSH

> **Important**
>
> Plusieurs utilisateurs peuvent accéder simultanément au système d'exploitation. En général, il y a une GUI session utilisateur 1:1 en raison du service de partage d'écran intégré sur le port 5900. L'utilisation SSH dans macOS prend en charge plusieurs sessions jusqu'à la limite du « nombre maximum de sessions » indiquée dans le fichier sshd_config.

Les instances Amazon EC2 Mac n'autorisent pas le root à distance SSH par défaut. De plus, l'authentification par mot de passe est désactivée pour empêcher les attaques de force sur les mots de passe. Le compte ec2-user est configuré pour se connecter à distance à l'aide de. SSH Le compte ec2-user dispose également de privilèges sudo. Une fois que vous vous êtes connecté à votre instance, vous pouvez ajouter d'autres utilisateurs.

Pour faciliter la connexion à votre instanceSSH, lancez-la à l'aide d'une paire de clés et d'un groupe de sécurité autorisant SSH l'accès, et assurez-vous que l'instance dispose d'une connexion Internet. Vous fournissez le fichier `.pem` de la paire de clés lorsque vous vous connectez à l'instance.

Suivez la procédure ci-dessous pour vous connecter à votre instance Mac à l'aide d'un SSH client. Si vous recevez une erreur lors d'une tentative de connexion à votre instance, consultez Résoudre les problèmes de connexion à votre instance Amazon EC2 Linux.

Pour vous connecter à votre instance à l'aide de SSH

1. Vérifiez qu'un SSH client est installé sur votre ordinateur local en entrant ssh sur la ligne de commande. Si votre ordinateur ne reconnaît pas la commande, recherchez un SSH client pour votre système d'exploitation et installez-le.
2. Obtenez le DNS nom public de votre instance. À l'aide de la EC2 console Amazon, vous pouvez trouver le DNS nom public dans les onglets Détails et Mise en réseau. À l'aide de AWS CLI, vous pouvez trouver le DNS nom public à l'aide de la commande describe-instances.
3. Recherchez le fichier `.pem` pour la paire de clés que vous avez spécifiée lorsque vous avez lancé l'instance.
4. Connectez-vous à votre instance à l'aide de la ssh commande suivante, en spécifiant le DNS nom public de l'instance et du `.pem` fichier.

```
ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

Connectez-vous à l'interface utilisateur graphique de votre instance (GUI)

Suivez la procédure ci-dessous pour vous connecter à votre instance à l'GUIaide d'VNCApple Remote Desktop (ARD) ou de l'application de partage d'écran Apple (incluse dans macOS).

> **Note**
>
> macOS 10.14 et les versions ultérieures ne permettent le contrôle que si le partage d'écran est activé via Préférences système.

Pour vous connecter à votre instance à l'aide d'un ARD client ou d'un VNC client

1. Vérifiez que votre ordinateur local possède un ARD client ou qu'un VNC client compatible est ARD installé. Sur macOS, vous pouvez utiliser l'application Partage d'écran intégrée. Sinon, ARD recherchez votre système d'exploitation et installez-le.
2. Depuis votre ordinateur local, connectez-vous à votre instance à l'aide deSSH.
3. Configurez un mot de passe pour le compte ec2-user à l'aide de la commande passwd comme suit.

   ```
   [ec2-user ~]$ sudo passwd ec2-user
   ```

4. Installez et exécutez le partage d'écran macOS à l'aide de la commande suivante.

   ```
   [ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
   sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
   ```

5. Déconnectez-vous votre instance en saisissant exit et en appuyant sur la touche Entrée.
6. À partir de votre ordinateur, connectez-vous à votre instance à l'aide de la commande ssh suivante. Outre les options présentées dans la section précédente, utilisez l'-Loption permettant d'activer la redirection de port et de transférer tout le trafic sur le port local 5900 vers le ARD serveur de l'instance.

   ```
   ssh -L 5900:localhost:5900 -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
   ```

7. Depuis votre ordinateur local, utilisez le ARD client ou le VNC client qui prend ARD en charge la connexion`localhost:5900`. Par exemple, utilisez l'application Partage d'écran sur macOS comme suit :

a. Ouvrez le Finder et sélectionnez Aller.

b. Sélectionnez Se connecter au serveur.

c. Dans le champ Adresse du serveur, saisissez `vnc://localhost:5900`.

d. Connectez-vous comme demandé, en utilisant **`ec2-user`** le nom d'utilisateur et le mot de passe que vous avez créés pour le compte ec2-user.

Modifier la résolution d'écran macOS sur les instances Mac

Après vous être connecté à votre instance EC2 Mac à l'aide ARD d'un VNC client compatibleARD, vous pouvez modifier la résolution d'écran de votre environnement macOS à l'aide de l'un des outils ou utilitaires macOS accessibles au public, tels que Displayplacer.

Pour modifier la résolution d'écran à l'aide de displayplacer

1. Installez displayplacer.

```
[ec2-user ~]$ brew tap jakehilborn/jakehilborn && brew install displayplacer
```

2. Affichez les informations actuelles sur l'écran et les résolutions d'écran possibles.

```
[ec2-user ~]$ displayplacer list
```

3. Appliquez la résolution d'écran souhaitée.

```
[ec2-user ~]$ displayplacer "id:<screenID> res:<width>x<height> origin:(0,0)
 degree:0"
```

Par exemple :

```
RES="2560x1600"
displayplacer "id:69784AF1-CD7D-B79B-E5D4-60D937407F68 res:${RES} scaling:off
 origin:(0,0) degree:0"
```

Mettre à jour le système d'exploitation et le logiciel sur les instances Mac

> **Warning**
>
> L'installation des versions bêta ou préliminaires de macOS n'est disponible que sur les instances Apple Silicon Mac. Amazon EC2 ne qualifie pas les versions bêta ou préliminaires de macOS et ne garantit pas que les instances resteront fonctionnelles après la mise à jour d'une version de pré-production de macOS.
>
> Toute tentative d'installation de versions bêta ou de préversion de macOS sur des instances Mac Amazon EC2 x86 entraînera une dégradation de votre hôte dédié Amazon EC2 Mac lorsque vous arrêterez ou résilierez vos instances, et vous empêchera de démarrer ou de lancer une nouvelle instance sur cet hôte.

Étapes de mise à jour du logiciel sur les instances Mac x86 et les instances Apple Silicon Mac.

- Mettre à jour le logiciel sur les instances Mac x86
- Mettre à jour le logiciel sur les instances Apple Silicon Mac

Mettre à jour le logiciel sur les instances Mac x86

Sur les instances Mac basées sur x86, vous pouvez installer les mises à jour du système d'exploitation d'Apple à l'aide de la commande `softwareupdate`.

Pour installer les mises à jour du système d'exploitation d'Apple sur des instances Mac basées sur x86

1. Répertoriez les packages avec des mises à jour disponibles à l'aide de la commande suivante.

   ```
   [ec2-user ~]$ softwareupdate --list
   ```

2. Installez toutes les mises à jour ou uniquement des mises à jour spécifiques. Pour installer des mises à jour spécifiques, utilisez la commande suivante.

   ```
   [ec2-user ~]$ sudo softwareupdate --install label
   ```

   Pour installer toutes les mises à jour, utilisez la commande suivante.

   ```
   [ec2-user ~]$ sudo softwareupdate --install --all --restart
   ```

Les administrateurs système peuvent utiliser AWS Systems Manager pour déployer des mises à jour préapprouvées du système d'exploitation sur des instances Mac x86. Pour plus d'informations, consultez le AWS Systems Manager Guide de l'utilisateur .

Vous pouvez utiliser Homebrew pour installer des mises à jour de packages dans EC2 macOSAMIs, afin de disposer de la dernière version de ces packages sur vos instances. Vous pouvez également utiliser Homebrew pour installer et exécuter des applications macOS courantes sur Amazon EC2 macOS. Pour plus d'informations, consultez la documentation Homebrew.

Pour installer des mises à jour en utilisant Homebrew

1. Mettez à jour Homebrew en utilisant la commande suivante.

   ```
   [ec2-user ~]$ brew update
   ```

2. Répertoriez les packages avec des mises à jour disponibles à l'aide de la commande suivante.

   ```
   [ec2-user ~]$ brew outdated
   ```

3. Installez toutes les mises à jour ou uniquement des mises à jour spécifiques. Pour installer des mises à jour spécifiques, utilisez la commande suivante.

   ```
   [ec2-user ~]$ brew upgrade package name
   ```

   Pour installer toutes les mises à jour, utilisez la commande suivante.

   ```
   [ec2-user ~]$ brew upgrade
   ```

Mettre à jour le logiciel sur les instances Apple Silicon Mac

Considérations

pilote Elastic Network Adapter (ENA)

En raison d'une mise à jour de la configuration du pilote réseau, la version 1.0.2 du ENA pilote n'est pas compatible avec macOS 13.3 ou version ultérieure. Si vous souhaitez installer une version bêta, préliminaire ou de production de macOS version 13.3 ou ultérieure et que vous n'avez pas installé le dernier ENA pilote, suivez la procédure ci-dessous pour installer une nouvelle version du pilote.

Pour installer une nouvelle version du ENA pilote

1. Dans une fenêtre de terminal, connectez-vous à votre instance Apple Silicon Mac à l'aide de SSH.
2. Téléchargez l'ENAapplication dans le `Applications` fichier à l'aide de la commande suivante.

```
[ec2-user ~]$ brew install amazon-ena-ethernet-dext
```

> Conseil pour la résolution de problèmes
>
> Si vous recevez l'avertissement `No available formula with the name amazon-ena-ethernet-dext`, exécutez la commande suivante.
>
> ```
> [ec2-user ~]$ brew update
> ```

3. Déconnectez-vous votre instance en saisissant exit et en appuyant sur la touche Retour.
4. Utilisez le VNC client pour activer l'ENAapplication.
   a. Configurez le VNC client à l'aide deConnectez-vous à l'interface utilisateur graphique de votre instance (GUI).
   b. Une fois connecté à votre instance à l'aide de l'application de partage d'écran, accédez au dossier Applications et ouvrez l'ENAapplication.
   c. Choisissez Activer
   d. Pour vérifier que le pilote a été correctement activé, exécutez la commande suivante dans la fenêtre du terminal. La sortie de la commande indique que l'ancien pilote est arrêté et que le nouveau pilote est activé.

      ```
      systemextensionsctl list;
      ```

   e. Une fois l'instance redémarrée, seul le nouveau pilote est présent.

Mise à jour du logiciel sur les instances Apple Silicon Mac

Sur les instances Apple Silicon Mac, vous devez effectuer plusieurs étapes pour procéder à une mise à jour du système d'exploitation sur place. Accédez d'abord au disque interne de l'instance à l'aide du client GUI with a VNC (Virtual Network Computing). Cette procédure utilise le partage d'écran

macOS, le VNC client intégré. Déléguez ensuite la propriété à l'utilisateur administratif (`ec2-user`) en vous connectant comme `aws-managed-user` sur le EBS volume Amazon.

Au cours de cette procédure, vous créez deux mots de passe. Un mot de passe est destiné à l'utilisateur administratif (`ec2-user`) et l'autre est destiné à un utilisateur administratif spécial (`aws-managed-user`). N'oubliez pas ces mots de passe, car vous les utiliserez tout au long de la procédure.

> **Note**
>
> Avec cette procédure sur macOS Big Sur, vous ne pouvez effectuer que des mises à jour mineures, telles que la mise à jour de macOS Big Sur 11.7.3 vers macOS Big Sur 11.7.4. Pour macOS Monterey ou version ultérieure, vous pouvez effectuer des mises à jour logicielles majeures.

Accès au disque interne

1. Depuis votre ordinateur local, dans le Terminal, connectez-vous à votre instance Apple Silicon Mac à l'SSHaide de la commande suivante. Pour de plus amples informations, veuillez consulter Connexion à votre instance à l'aide d'SSH.

   ```
   ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
   ```

2. Installez et exécutez le partage d'écran macOS à l'aide de la commande suivante.

   ```
   [ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
   sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
   ```

3. Définissez un mot de passe pour `ec2-user` à l'aide de la commande suivante. N'oubliez pas le mot de passe, car vous l'utiliserez plus tard.

   ```
   [ec2-user ~]$ sudo /usr/bin/dscl . -passwd /Users/ec2-user
   ```

4. Déconnectez-vous de l'instance en saisissant exit et en appuyant sur la touche Retour.
5. Depuis votre ordinateur local, dans le terminal, reconnectez-vous à votre instance via un SSH tunnel vers le VNC port à l'aide de la commande suivante.

```
ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 ec2-user@instance-public-dns-name
```

> **Note**
>
> Ne quittez pas cette SSH session tant que la VNC connexion et les GUI étapes suivantes ne sont pas terminées. Lorsque l'instance est redémarrée, la connexion se ferme automatiquement.

6. À partir de votre ordinateur local, connectez-vous à `localhost:5900` en suivant les étapes ci-après :

   a. Ouvrez le Finder et sélectionnez Aller.

   b. Sélectionnez Se connecter au serveur.

   c. Dans le champ Adresse du serveur, saisissez `vnc://localhost:5900`.

7. Dans la fenêtre macOS, connectez-vous à la session distante de l'instance Apple Silicon Mac en tant qu'`ec2-user` à l'aide du mot de passe que vous avez créé à l'étape 3.

8. Accédez au disque interne, nommé InternalDisk, à l'aide de l'une des options suivantes.

   a. Pour macOS Ventura ou version ultérieure : ouvrez Réglages Système, sélectionnez Général dans le volet gauche, puis Disque de démarrage en bas à droite du volet.

   b. Pour macOS Monterey ou version antérieure : ouvrez les Préférences Système, sélectionnez Disque de démarrage, puis déverrouillez le volet en cliquant sur l'icône de verrouillage en bas à gauche de la fenêtre.

> **Conseil pour la résolution de problèmes**
>
> Si vous devez monter le disque interne, exécutez la commande suivante dans le terminal.
>
> ```
> APFSVolumeName="InternalDisk" ; SSDContainer=$(diskutil list | grep
>  "Physical Store disk0" -B 3 | grep "/dev/disk" | awk {'print $1'} ) ;
>  diskutil apfs addVolume $SSDContainer APFS $APFSVolumeName
> ```

9. Choisissez le disque interne, nommé InternalDisk, puis sélectionnez Redémarrer. Sélectionnez Redémarrer à nouveau lorsque vous y êtes invité.

> **Important**
>
> Si le disque interne est nommé Macintosh HD au lieu de InternalDisk, votre instance doit être arrêtée et redémarrée afin que l'hôte dédié puisse être mis à jour. Pour de plus amples informations, veuillez consulter Arrêtez ou mettez fin à votre instance Amazon EC2 Mac.

Utilisez la procédure suivante pour déléguer la propriété à l'utilisateur administratif. Lorsque vous vous reconnectez à votre instance avecSSH, vous démarrez à partir du disque interne à l'aide de l'utilisateur administratif spécial (`aws-managed-user`). Le mot de passe initial de `aws-managed-user` est vide, vous devez donc le remplacer lors de votre première connexion. Ensuite, répétez les étapes d'installation et de démarrage du partage d'écran macOS, car le volume de démarrage a changé.

Pour déléguer la propriété à l'administrateur d'un EBS volume Amazon

1. Depuis votre ordinateur local, dans le terminal, connectez-vous à votre instance Apple Silicon Mac à l'aide de la commande suivante.

```
ssh -i /path/key-pair-name.pem aws-managed-user@instance-public-dns-name
```

2. Lorsque vous recevez l'avertissement `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!`, exécutez l'une des commandes suivantes pour résoudre le problème.

   a. Supprimez les hôtes connus à l'aide de la commande suivante. Ensuite, répétez l'étape précédente.

   ```
   rm ~/.ssh/known_hosts
   ```

   b. Ajoutez ce qui suit à la SSH commande de l'étape précédente.

   ```
   -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no
   ```

3. Définissez le mot de passe pour `aws-managed-user` à l'aide de la commande suivante. Le mot de passe initial `aws-managed-user` est vide, vous devez donc le remplacer lors de votre première connexion.

   a.
   ```
   [aws-managed-user ~]$ sudo /usr/bin/dscl . -passwd /Users/aws-managed-user password
   ```

   b. Lorsque vous recevez le message `Permission denied. Please enter user's old password:`, appuyez sur Entrée.

   > **Conseil pour la résolution de problèmes**
   >
   > Si l'erreur `passwd: DS error: eDSAuthFailed` s'affiche, utilisez la commande suivante.
   >
   > ```
   > [aws-managed-user ~]$ sudo passwd aws-managed-user
   > ```

4. Installez et exécutez le partage d'écran macOS à l'aide de la commande suivante.

   ```
   [aws-managed-user ~]$ sudo launchctl enable system/com.apple.screensharing
   sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
   ```

5. Déconnectez-vous de l'instance en saisissant exit et en appuyant sur la touche Retour.

6. Depuis votre ordinateur local, dans le terminal, reconnectez-vous à votre instance via un SSH tunnel vers le VNC port à l'aide de la commande suivante.

   ```
   ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 aws-managed-user@instance-public-dns-name
   ```

7. À partir de votre ordinateur local, connectez-vous à `localhost:5900` en suivant les étapes ci-après :

   a. Ouvrez le Finder et sélectionnez Aller.

   b. Sélectionnez Se connecter au serveur.

   c. Dans le champ Adresse du serveur, saisissez `vnc://localhost:5900`.

8. Dans la fenêtre macOS, connectez-vous à la session distante de l'instance Apple Silicon Mac en tant qu'`aws-managed-user` à l'aide du mot de passe que vous avez créé à l'étape 3.

> **Note**
>
> Si un message vous invite à vous connecter avec votre identifiant Apple, sélectionnez Configurer plus tard.

9. Accédez au EBS volume Amazon à l'aide de l'une des options suivantes.

   a. Pour macOS Ventura ou version ultérieure : ouvrez Réglages Système, sélectionnez Général dans le volet gauche, puis Disque de démarrage en bas à droite du volet.

   b. Pour macOS Monterey ou version antérieure : ouvrez les Préférences Système, sélectionnez Disque de démarrage, puis déverrouillez le volet à l'aide de l'icône de verrouillage en bas à gauche de la fenêtre.

> **Note**
>
> En attendant le redémarrage, lorsqu'un message vous invite à saisir un mot de passe administrateur, utilisez celui que vous avez défini ci-dessus pour `aws-managed-user`. Ce mot de passe peut être différent de celui que vous avez défini pour `ec2-user` ou le compte administrateur par défaut de votre instance. Les instructions suivantes indiquent quand utiliser le mot de passe administrateur de votre instance.

10. Sélectionnez le EBS volume Amazon (le volume qui n'est pas nommé InternalDiskdans la fenêtre du disque de démarrage) et choisissez Redémarrer.

> **Note**
>
> Si plusieurs EBS volumes Amazon démarrables sont attachés à votre instance Apple Silicon Mac, veillez à utiliser un nom unique pour chaque volume.

11. Confirmez le redémarrage, puis choisissez Autoriser les utilisateurs lorsqu'un message vous y invite.
12. Dans le volet Autoriser l'utilisateur sur ce volume, vérifiez que l'utilisateur administratif (`ec2-user` par défaut) est sélectionné, puis sélectionnez Autoriser.
13. Saisissez le mot de passe `ec2-user` que vous avez créé à l'étape 3 de la procédure précédente, puis sélectionnez Continuer.

14. Saisissez le mot de passe de l'utilisateur administratif spécial (`aws-managed-user`) lorsqu'un message vous y invite.
15. Depuis votre ordinateur local, dans le Terminal, reconnectez-vous à votre instance en utilisant le nom SSH d'utilisateur`ec2-user`.

    > **Conseil pour la résolution de problèmes**
    >
    > Si l'avertissement s'affiche`WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!`, exécutez la commande suivante et reconnectez-vous à votre instance à l'aide SSH de.
    >
    > ```
    > rm ~/.ssh/known_hosts
    > ```

16. Pour effectuer la mise à jour logicielle, utilisez les commandes sous Mettre à jour le logiciel sur les instances Mac x86.

Augmenter la taille d'un EBS volume sur votre instance Mac

Vous pouvez augmenter la taille de vos EBS volumes Amazon sur votre instance Mac. Pour plus d'informations, consultez Amazon EBS Elastic Volumes dans le guide de EBS l'utilisateur Amazon.

Après avoir augmenté la taille du volume, vous devez augmenter la taille de votre APFS contenant comme suit.

Augmentez l'espace disque disponible à l'utilisation

1. Déterminez si un redémarrage est requis. Si vous avez redimensionné un EBS volume existant sur une instance Mac en cours d'exécution, vous devez redémarrer l'instance pour que la nouvelle taille soit disponible. Si la modification de l'espace disque a été effectuée pendant le lancement, le redémarrage n'est pas requis.

   Affichez l'état actuel des tailles de disque :

   ```
   [ec2-user ~]$  diskutil list external physical
   /dev/disk0 (external, physical):
      #:                       TYPE NAME                    SIZE       IDENTIFIER
      0:                 GUID_partition_scheme           *322.1 GB     disk0
      1:                 EFI EFI                          209.7 MB     disk0s1
   ```

```
   2:                 Apple_APFS Container disk2        321.9 GB     disk0s2
```

2. Copiez et collez la commande suivante.

```
[ec2-user ~]$ PDISK=$(diskutil list physical external | head -n1 | cut -d" " -f1)
APFSCONT=$(diskutil list physical external | grep "Apple_APFS" | tr -s " " | cut -
d" " -f8)
yes | sudo diskutil repairDisk $PDISK
```

3. Copiez et collez la commande suivante.

```
[ec2-user ~]$ sudo diskutil apfs resizeContainer $APFSCONT 0
```

Arrêtez ou mettez fin à votre instance Amazon EC2 Mac

Lorsque vous arrêtez une instance Mac, l'instance reste dans l'état `stopping` pendant environ 15 minutes avant de passer à l'état `stopped`.

Lorsque vous arrêtez ou mettez fin à une instance Mac, Amazon EC2 exécute un flux de travail de nettoyage sur l'hôte dédié sous-jacent afin d'effacer les données internesSSD, d'effacer les NVRAM variables persistantes et de mettre à jour le dernier microprogramme de l'appareil. Cela garantit que les instances Mac offrent la même sécurité et la même confidentialité des données que les autres instances EC2 Nitro. Il vous permet également d'exécuter la dernière version de macOSAMIs. Lors du workflow de nettoyage, l'hôte dédié entre temporairement dans l'état en attente. Sur les instances Mac basées sur x86, le flux de travail de nettoyage peut prendre jusqu'à 50 minutes. Sur les instances Apple Silicon Mac, le flux de travail de nettoyage peut prendre jusqu'à 110 minutes. En outre, sur les instances Mac basées sur x86, si le firmware de l'appareil doit être mis à jour, le flux de travail de nettoyage peut prendre jusqu'à 3 heures.

Vous ne pouvez pas démarrer l'instance Mac arrêtée ou lancer une nouvelle instance Mac avant la fin du workflow de nettoyage, moment où Hôte dédié entre dans l'état `available`.

La mesure et la facturation sont suspendues lorsque l'hôte dédié entre dans l'état `pending`. Vous n'êtes pas facturé pour la durée du workflow de nettoyage.

Libérez l'Hôte dédié pour votre instance Mac

Lorsque vous avez terminé avec votre instance Mac, vous pouvez libérer l'Hôte dédié. Avant de pouvoir libérer l'Hôte dédié, vous devez arrêter ou résilier l'instance Mac. Vous ne pouvez pas libérer l'hôte tant que la période d'allocation n'excède pas le minimum de 24 heures.

Pour libérer l'Hôte dédié

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance et État de l'instance, puis sélectionnez Arrêter l'instance ou Résilier l'instance.
4. Dans le volet de navigation, choisissez Hôtes dédiés.
5. Sélectionnez Hôte dédié puis Actions, Libérer l'hôte.
6. Lorsque vous êtes invité à confirmer l'opération, choisissez Release (Libérer).

Trouvez les versions de macOS prises en charge pour votre hôte dédié Amazon EC2 Mac

Vous pouvez consulter les dernières versions de macOS prises en charge par votre hôte dédié Amazon EC2 Mac. Grâce à cette fonctionnalité, vous pouvez vérifier si votre hôte dédié peut prendre en charge les lancements d'instances avec vos versions préférées de macOS.

Chaque version de macOS nécessite une version minimale du microprogramme sur le Mac Apple sous-jacent pour démarrer correctement. La version du microprogramme Apple Mac peut devenir obsolète si un hôte dédié Mac alloué est resté inactif pendant une période prolongée ou s'il contient une instance de longue date.

Pour garantir la compatibilité avec les dernières versions de macOS, vous pouvez arrêter ou résilier des instances sur l'hôte dédié Mac qui vous a été attribué. Cela déclenche le flux de travail de nettoyage de l'hôte et met à jour le microprogramme du Mac Apple sous-jacent pour qu'il soit compatible avec les dernières versions de macOS. Un hôte dédié doté d'une instance de longue durée sera automatiquement mis à jour lorsque vous arrêtez ou mettez fin à une instance en cours d'exécution.

Pour plus d'informations sur le flux de travail de nettoyage, consultezArrêtez ou mettez fin à votre instance Amazon EC2 Mac.

Pour plus d'informations sur le lancement d'instances Mac, consultezLancez une instance Mac à l' AWS Management Console aide du AWS CLI.

Vous pouvez consulter les informations relatives aux dernières versions de macOS prises en charge sur l'hôte dédié qui vous a été attribué à l'aide de la EC2 console Amazon ou du AWS CLI.

Console

Pour afficher les informations relatives au microprogramme de l'hôte dédié à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Sur la page de détails des hôtes dédiés, sous Dernières versions de macOS prises en charge, vous pouvez voir les dernières versions de macOS prises en charge par l'hôte.

AWS CLI

Pour consulter les informations relatives au microprogramme de l'hôte dédié à l'aide du AWS CLI

Utilisez la `describe-mac-hosts`commande en la `region` remplaçant par la commande appropriée Région AWS.

```
$ aws ec2 describe-mac-hosts --region us-east-1
  {
      "MacHosts": [
          {
              "HostId": "h-07879acf49EXAMPLE",
              "MacOSLatestSupportedVersions": [
                  "14.3",
                  "13.6.4",
                  "12.7.3"
              ]
          }
      ]
  }
```

S'abonner aux AMI notifications macOS

Pour être averti de la publication de nouvelles AMIs versions ou de la mise à jour de BridgeOS, abonnez-vous aux notifications via Amazon. SNS

Pour plus d'informations sur EC2 macOSAMIs, consultezNotes de AMIs mise à jour d'Amazon EC2 macOS.

Pour vous abonner aux AMI notifications macOS

1. Ouvrez la SNS console Amazon sur https://console.aws.amazon.com/sns/v3/home.
2. Dans la barre de navigation, changez la région en US Est (Virginie du Nord), si nécessaire. Vous devez utiliser cette région car les SNS notifications auxquelles vous êtes abonné ont été créées dans cette région.
3. Dans le panneau de navigation, sélectionnez Abonnements.
4. Choisissez Créer un abonnement.
5. Dans la boîte de dialogue Créer un abonnement, procédez comme suit :

   a. Pour le sujet ARN, copiez et collez l'un des noms de ressources Amazon suivants (ARNs) :

      - **`arn:aws:sns:us-east-1:898855652048:amazon-ec2-macos-ami-updates`**
      - **`arn:aws:sns:us-east-1:898855652048:amazon-ec2-bridgeos-updates`**

   b. Pour Protocole, sélectionnez l'une des options suivantes :

      - E-mail :

        Pour Endpoint (Point de terminaison), tapez une adresse e-mail que vous pouvez utiliser pour recevoir les notifications. Une fois votre abonnement créé, vous recevrez un message de confirmation avec la ligne d'objet `AWS Notification - Subscription Confirmation`. Ouvrez l'e-mail et choisissez Confirm subscription (Confirmer l'abonnement) pour terminer votre abonnement.

      - SMS:

        Pour Endpoint (Point de terminaison), tapez un numéro de téléphone que vous pouvez utiliser pour recevoir les notifications.

      - AWS Lambda, AmazonSQS, Amazon Data Firehose (les notifications sont disponibles sous forme de JSON format) :

        Pour Endpoint, entrez la ARN fonction Lambda, la SQS file d'attente ou le flux Firehose que vous pouvez utiliser pour recevoir les notifications.

   c. Choisissez Create subscription (Créer un abonnement).

Chaque fois AMIs que macOS est publié, nous envoyons des notifications aux abonnés du `amazon-ec2-macos-ami-updates` sujet. A chaque mise à jour de brifgeOS, nous envoyons des

notifications aux abonnés de la rubrique `amazon-ec2-bridgeos-updates`. Si vous ne souhaitez plus recevoir ces notifications, exécutez la procédure suivante pour annuler votre abonnement.

Pour vous désabonner des AMI notifications de macOS

1. Ouvrez la SNS console Amazon sur https://console.aws.amazon.com/sns/v3/home.
2. Dans la barre de navigation, changez la région en US Est (Virginie du Nord), si nécessaire. Vous devez utiliser cette région car les SNS notifications ont été créées dans cette région.
3. Dans le panneau de navigation, choisissez Abonnements.
4. Sélectionnez les abonnements, puis choisissez Actions, Delete subscriptions (Supprimer les abonnements). Lorsque vous êtes invité à confirmer, choisissez Delete (Supprimer).

Récupérez macOS AMI IDs à l'aide de AWS Systems Manager Parameter Store API

Vous devez spécifier un AMI moment où vous lancez une instance. An AMI est spécifique à un système Région AWS d'exploitation et à une architecture de processeur. Vous pouvez afficher tous les macOS contenus AMIs dans un Région AWS et récupérer la dernière version de macOS AMI en interrogeant le AWS Systems Manager Parameter StoreAPI. À l'aide de ces paramètres publics, vous n'avez pas besoin de rechercher manuellement macOS AMIIDs. Les paramètres publics sont disponibles à la fois pour ARM64 macOS x86 AMIs et peuvent être intégrés à vos AWS CloudFormation modèles existants.

Autorisations nécessaires

Pour effectuer cette action, le IAMprincipal doit être autorisé à lancer l'`ssm:GetParameter`APIaction.

Pour afficher la liste de tous les macOS actuels AMIs à l' Région AWS aide du AWS CLI

Utilisez la get-parameters-by-pathcommande suivante pour afficher la liste de tous les macOS AMIs de la région actuelle.

```
aws ssm get-parameters-by-path --path /aws/service/ec2-macos --recursive --query
 "Parameters[].Name"
```

Pour récupérer l'AMIidentifiant des derniers macOS majeurs à AMI l'aide du AWS CLI

Utilisez la commande get-parameter suivante avec le sous-paramètre. `image_id` Dans l'exemple suivant, remplacez-le `sonoma` par une version majeure prise en charge par macOS, `x86_64_mac`

par le processeur et `region-code` par une version compatible Région AWS pour laquelle vous souhaitez obtenir le dernier AMI identifiant macOS.

```
aws ssm get-parameter --name /aws/service/ec2-macos/sonoma/x86_64_mac/latest/image_id
 --region region-code
```

Pour plus d'informations, consultez la section Appeler les paramètres AMI publics pour macOS dans le guide de AWS Systems Manager l'utilisateur.

Notes de AMIs mise à jour d'Amazon EC2 macOS

Les informations suivantes fournissent des informations détaillées sur les packages inclus par défaut dans EC2 macOS AMIs et résument les modifications apportées à chaque AMI version de EC2 macOS.

Pour plus d'informations sur la façon de s'abonner aux AMI notifications macOS, consultezS'abonner aux AMI notifications macOS.

Packages par défaut inclus dans Amazon EC2 macOS AMIs

Le tableau suivant décrit les packages inclus par défaut dans les EC2 macOSAMIs.

Packages	Notes de mise à jour
EC2macOS Init	https://github.com/aws/ec2-macos-init/tags
EC2Utilitaires pour macOS	https://github.com/aws/ec2-macos-utils/tags
AmazonSSMAgent	https://github.com/aws/amazon-ssm-agent/releases
AWS Command Line Interface (AWS CLI) version 2	https://raw.githubusercontent.com/aws/aws-cli/v2/CHANGELOG.rst
Outils de ligne de commande pour Xcode	https://developer.apple.com/documentation/xcode-release-notes
Homebrew	https://github.com/Homebrew/brew/releases
EC2Instance Connect	https://github.com/aws/aws-ec2-instance-connect-config/releases

Packages	Notes de mise à jour
Safari	https://developer.apple.com/documentation/safari-release-notes

Mises à AMI jour d'Amazon EC2 macOS

Le tableau suivant décrit les modifications incluses dans les AMI versions de EC2 macOS. Notez que certaines modifications s'appliquent à tous les EC2 macOSAMIs, tandis que d'autres ne s'appliquent qu'à un sous-ensemble d'entre euxAMIs.

EC2Mises à AMI jour de macOS

Version	Modifications

2024,08,20	Tout AMIs
	• Homebrew mis à jour vers la version 4.3.14
	• Mise à jour `aws-cli` au format 2.17.29
	
	Sortie de macOS Sonoma 14.6.1 (toutes les instances Mac)
	• Aucune CVE entrée publiée.
	
	Sortie de macOS Ventura 13.6.9 (toutes les instances Mac)
	• Aucune CVE entrée publiée.
	• Safari mis à jour vers la version 17.6
	  • Consignes de sécurité de Safari 17.6
	
	Sortie de macOS Monterey 12.7.6 (toutes les instances Mac)
	• Consignes de sécurité de macOS Monterey 12.7.6
	• Safari mis à jour vers la version 17.6
	  • Consignes de sécurité de Safari 17.6

Version	Modifications

2024,06.07	Tout AMIs
	• Homebrew mis à jour vers la version 4.3.1-1
	• Mise à jour `aws-cli` au format 2.15.56
	• Mis à jour `amazon-ssm-agent` au code 3.3.380.0-1
	
	Sortie de macOS Sonoma 14.5 (toutes les instances Mac)
	• Consignes de sécurité de macOS Sonoma 14.5
	
	Sortie de macOS Ventura 13.6.7 (toutes les instances Mac)
	• Consignes de sécurité de macOS Ventura 13.6.7
	• Safari mis à jour vers la version 17.5
	  • Consignes de sécurité de Safari 17.5
	
	Sortie de macOS Monterey 12.7.5 (toutes les instances Mac)
	• Consignes de sécurité de macOS Monterey 12.7.5
	• Safari mis à jour vers la version 17.5
	  • Consignes de sécurité de Safari 17.5

Version	Modifications

2024,04.12	Tout AMIs
	• Homebrew mis à jour vers la version 4.2.16-1
	• Mise à jour `aws-cli` au format 2.15.36
	
	Sortie de macOS Sonoma 14.4.1 (toutes les instances Mac)
	• Consignes de sécurité de macOS Sonoma 14.4.1
	
	Sortie de macOS Ventura 13.6.6 (toutes les instances Mac)
	• Consignes de sécurité de macOS Ventura 13.6.6
	• Safari mis à jour vers la version 17.4.1
	  • Consignes de sécurité de Safari 17.4.1
	
	Pour macOS Monterey (toutes les instances Mac)
	• Safari mis à jour vers la version 17.4.1
	  • Consignes de sécurité de Safari 17.4.1

Types d'instances EBS optimisés pour Amazon

Les instances EBS optimisées pour Amazon utilisent une pile de configuration optimisée et fournissent une bande passante dédiée supplémentaire pour Amazon EBS I/O. Cette optimisation fournit les meilleures performances pour vos EBS volumes en minimisant les conflits entre Amazon EBS I/O et le reste du trafic provenant de votre instance.

Lorsqu'ils sont attachés à EBS une instance optimisée, les volumes à usage général SSD (`gp2`et`gp3`) sont conçus pour fournir au moins 90 % de leurs IOPS performances provisionnées 99 % du temps au cours d'une année donnée, et les volumes provisionnés IOPS SSD (`io1`et`io2`) sont conçus pour fournir au moins 90 % de leurs IOPS performances provisionnées 99,9 % du temps au cours d'une année donnée. Throughput Optimized HDD (`st1`) et Cold HDD (`sc1`) fournissent au moins 90 % des performances de débit attendues 99 % du temps au cours d'une année donnée. Les périodes non conformes sont assez uniformément réparties, en ciblant 99 % du débit total attendu

chaque heure. Pour plus d'informations, consultez les types de EBS volumes Amazon dans le guide de EBS l'utilisateur Amazon.

Certains types d'instances sont EBSoptimisés par défaut, il n'est pas nécessaire de les activer et aucun effet si vous essayez de les désactiver. D'autres types d'instances prennent éventuellement en charge EBS l'optimisation et vous pouvez l'activer pendant ou après le lancement moyennant un supplément horaire. Certains types d'instances ne prennent pas en charge EBS l'optimisation.

Pour connaître les spécifications et les fonctionnalités détaillées des types d'instance, consultez le guide des types d'EC2instance Amazon.

Rubriques

- EBS-optimisé par défaut
- EBSoptimisation prise en charge
- Profitez des performances EBS optimisées d'Amazon au maximum
- Trouvez les types d'EC2instances Amazon EBS optimisés pour Amazon
- Activer EBS l'optimisation Amazon pour une EC2 instance Amazon

EBS-optimisé par défaut

Les types d'instances suivants sont EBS optimisés par défaut. Il n'est pas nécessaire d'activer EBS l'optimisation et cela n'a aucun effet si vous la désactivezEBS.

> **Important**
>
> Les EBS performances d'une instance sont limitées par les limites de performance du type d'instance ou par les performances agrégées de ses volumes attachés, la valeur la plus faible étant retenue. Pour atteindre des EBS performances maximales, une instance doit être associée à des volumes qui fournissent des performances combinées égales ou supérieures aux performances maximales de l'instance. Par exemple, `80,000` IOPS pour atteindre cet objectif`r6i.16xlarge`, l'instance doit disposer d'au moins des `5` `gp3` volumes provisionnés avec `16,000` IOPS chacun d'entre eux (5volumes x `16,000` IOPS = `80,000`IOPS). Nous vous recommandons de choisir un type d'instance qui fournit un EBS débit Amazon dédié supérieur aux besoins de votre application ; sinon, la connexion entre Amazon EBS et Amazon EC2 peut devenir un goulot d'étranglement en termes de performances.

Note

[1] Ces instances peuvent maintenir les performances maximales pendant 30 minutes au moins une fois toutes les 24 heures, après quoi elles retrouvent leurs performances de base.
[2] Ces instances peuvent maintenir leurs performances déclarées indéfiniment. Si votre charge de travail nécessite des performances maximales soutenues pendant plus de 30 minutes, utilisez l'une de ces instances.

instances à usage général

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
a1.medium [1]	300	3500	37,50	437,50	2500	20 000
a1.large [1]	525	3500	65,62	437,50	4000	20 000
a1.xlarge [1]	800	3500	100,00	437,50	6 000	20 000
a1.2xlarge [1]	1750	3500	218,75	437,50	10 000	20 000
a1.4xlarge [2]	3500		437,5		20 000	
a1.metal [2]	3500		437,5		20 000	
m4.large [2]	450		56,25		3600	
m4.xlarge [2]	750		93,75		6 000	
m4.2xlarge [2]	1 000		125,0		8000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
m4.4xlarge [2]	2000		250,0		16000	
m4.10xlarge [2]	4000		500,0		32000	
m4.16xlarge [2]	10 000		1250,0		65000	
m5.large [1]	650	4750	81,25	593,75	3600	18750
m5.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
m5.2xlarge [1]	2300	4750	287,50	593,75	12 000	18750
m5.4xlarge [2]	4750		593,75		18750	
m5.8xlarge [2]	6800		850,0		30 000	
m5.12xlarge [2]	9500		1187,5		40 000	
m5.16xlarge [2]	13600		1700,0		60000	
m5.24xlarge [2]	19000		2375,0		80000	
m5.metal [2]	19000		2375,0		80000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
m5a.large [1]	650	2880	81,25	360,00	3600	16000
m5a.xlarge [1]	1085	2880	135,62	360,00	6 000	16000
m5a.2xlarge [1]	1580	2880	197,50	360,00	8333	16000
m5a.4xlarge [2]	2880		360,0		16000	
m5a.8xlarge [2]	4750		593,75		20 000	
m5a.12xlarge [2]	6780		847,5		30 000	
m5a.16xlarge [2]	9500		1187,5		40 000	
m5a.24xlarge [2]	13750		1718,75		60000	
m5ad.large [1]	650	2880	81,25	360,00	3600	16000
m5ad.xlarge [1]	1085	2880	135,62	360,00	6 000	16000
m5ad.2xlarge [1]	1580	2880	197,50	360,00	8333	16000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
m5ad.4xlarge [2]	2880		360,0		16000	
m5ad.8xlarge [2]	4750		593,75		20 000	
m5ad.12xlarge [2]	6780		847,5		30 000	
m5ad.16xlarge [2]	9500		1187,5		40 000	
m5ad.24xlarge [2]	13750		1718,75		60000	
m5d.large [1]	650	4750	81,25	593,75	3600	18750
m5d.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
m5d.2xlarge [1]	2300	4750	287,50	593,75	12 000	18750
m5d.4xlarge [2]	4750		593,75		18750	
m5d.8xlarge [2]	6800		850,0		30 000	
m5d.12xlarge [2]	9500		1187,5		40 000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
m5d.16xlarge [2]	13600		1700,0		60000	
m5d.24xlarge [2]	19000		2375,0		80000	
m5d.metal [2]	19000		2375,0		80000	
m5dn.large [1]	650	4750	81,25	593,75	3600	18750
m5dn.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
m5dn.2xlarge [1]	2300	4750	287,50	593,75	12 000	18750
m5dn.4xlarge [2]	4750		593,75		18750	
m5dn.8xlarge [2]	6800		850,0		30 000	
m5dn.12xlarge [2]	9500		1187,5		40 000	
m5dn.16xlarge [2]	13600		1700,0		60000	
m5dn.24xlarge [2]	19000		2375,0		80000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
m5dn.metal [2]	19000		2375,0		80000	
m5n.large [1]	650	4750	81,25	593,75	3600	18750
m5n.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
m5n.2xlarge [1]	2300	4750	287,50	593,75	12 000	18750
m5n.4xlarge [2]	4750		593,75		18750	
m5n.8xlarge [2]	6800		850,0		30 000	
m5n.12xlarge [2]	9500		1187,5		40 000	
m5n.16xlarge [2]	13600		1700,0		60000	
m5n.24xlarge [2]	19000		2375,0		80000	
m5n.metal [2]	19000		2375,0		80000	
m5zn.large [1]	800	3170	100,00	396,25	3333	13333

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
m5zn.xlarge [1]	1564	3170	195,50	396,25	6667	13333
m5zn.2xlarge [2]	3170		396,25		13333	
m5zn.3xlarge [2]	4750		593,75		20 000	
m5zn.6xlarge [2]	9500		1187,5		40 000	
m5zn.12xlarge [2]	19000		2375,0		80000	
m5zn.metal [2]	19000		2375,0		80000	
m6a.large [1]	650	10 000	81,25	1250,00	3600	40 000
m6a.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
m6a.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
m6a.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
m6a.8xlarge [2]	10 000		1250,0		40 000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
m6a.12xlarge [2]	15000		1875,0		60000	
m6a.16xlarge [2]	20 000		2500,0		80000	
m6a.24xlarge [2]	30 000		3750,0		120000	
m6a.32xlarge [2]	40 000		5000,0		160000	
m6a.48xlarge [2]	40 000		5000,0		240000	
m6a.metal [2]	40 000		5000,0		240000	
m6g.medium [1]	315	4750	39,38	593,75	2500	20 000
m6g.large [1]	630	4750	78,75	593,75	3600	20 000
m6g.xlarge [1]	1188	4750	148,50	593,75	6 000	20 000
m6g.2xlarge [1]	2375	4750	296,88	593,75	12 000	20 000
m6g.4xlarge [2]	4750		593,75		20 000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
m6g.8xlarge [2]	9500		1187,5		40 000	
m6g.12xlarge [2]	14250		1781,25		50000	
m6g.16xlarge [2]	19000		2375,0		80000	
m6g.metal [2]	19000		2375,0		80000	
m6gd.medium [1]	315	4750	39,38	593,75	2500	20 000
m6gd.large [1]	630	4750	78,75	593,75	3600	20 000
m6gd.xlarge [1]	1188	4750	148,50	593,75	6 000	20 000
m6gd.2xlarge [1]	2375	4750	296,88	593,75	12 000	20 000
m6gd.4xlarge [2]	4750		593,75		20 000	
m6gd.8xlarge [2]	9500		1187,5		40 000	
m6gd.12xlarge [2]	14250		1781,25		50000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
m6gd.16xlarge [2]	19000		2375,0		80000	
m6gd.metal [2]	19000		2375,0		80000	
m6i.large [1]	650	10 000	81,25	1250,00	3600	40 000
m6i.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
m6i.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
m6i.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
m6i.8xlarge [2]	10 000		1250,0		40 000	
m6i.12xlarge [2]	15000		1875,0		60000	
m6i.16xlarge [2]	20 000		2500,0		80000	
m6i.24xlarge [2]	30 000		3750,0		120000	
m6i.32xlarge [2]	40 000		5000,0		160000	
m6i.metal [2]	40 000		5000,0		160000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
m6id.large [1]	650	10 000	81,25	1250,00	3600	40 000
m6id.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
m6id.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
m6id.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
m6id.8xlarge [2]	10 000		1250,0		40 000	
m6id.12xlarge [2]	15000		1875,0		60000	
m6id.16xlarge [2]	20 000		2500,0		80000	
m6id.24xlarge [2]	30 000		3750,0		120000	
m6id.32xlarge [2]	40 000		5000,0		160000	
m6id.metal [2]	40 000		5000,0		160000	
m6idn.large [1]	1562	25000	195,31	3125,00	6250	100 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
m6idn.xlarge [1]	3125	25000	390,62	3125,00	12500	100 000
m6idn.2xlarge [1]	6250	25000	781,25	3125,00	25000	100 000
m6idn.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100 000
m6idn.8xlarge [2]	25000		3125,0		100 000	
m6idn.12xlarge [2]	37500		4687,5		150000	
m6idn.16xlarge [2]	50000		6250,0		200 000	
m6idn.24xlarge [2]	75000		9375,0		300 000	
m6idn.32xlarge [2]	100 000		12500,0		400 000	
m6idn.metal [2]	100 000		12500,0		400 000	
m6in.large [1]	1562	25000	195,31	3125,00	6250	100 000
m6in.xlarge [1]	3125	25000	390,62	3125,00	12500	100 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
m6in.2xlarge [1]	6250	25000	781,25	3125,00	25000	100 000
m6in.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100 000
m6in.8xlarge [2]	25000		3125,0		100 000	
m6in.12xlarge [2]	37500		4687,5		150000	
m6in.16xlarge [2]	50000		6250,0		200 000	
m6in.24xlarge [2]	75000		9375,0		300 000	
m6in.32xlarge [2]	100 000		12500,0		400 000	
m6in.metal [2]	100 000		12500,0		400 000	
m7a.medium [1]	325	10 000	40,62	1250,00	2500	40 000
m7a.large [1]	650	10 000	81,25	1250,00	3600	40 000
m7a.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
m7a.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
m7a.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
m7a.8xlarge [2]	10 000		1250,0		40 000	
m7a.12xlarge [2]	15000		1875,0		60000	
m7a.16xlarge [2]	20 000		2500,0		80000	
m7a.24xlarge [2]	30 000		3750,0		120000	
m7a.32xlarge [2]	40 000		5000,0		160000	
m7a.48xlarge [2]	40 000		5000,0		240000	
m7a.metal-48xl [2]	40 000		5000,0		240000	
m7g.medium [1]	315	10 000	39,38	1250,00	2500	40 000
m7g.large [1]	630	10 000	78,75	1250,00	3600	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
m7g.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
m7g.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
m7g.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
m7g.8xlarge [2]	10 000		1250,0		40 000	
m7g.12xlarge [2]	15000		1875,0		60000	
m7g.16xlarge [2]	20 000		2500,0		80000	
m7g.metal [2]	20 000		2500,0		80000	
m7gd.medium [1]	315	10 000	39,38	1250,00	2500	40 000
m7gd.large [1]	630	10 000	78,75	1250,00	3600	40 000
m7gd.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
m7gd.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
m7gd.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
m7gd.8xlarge [2]	10 000		1250,0		40 000	
m7gd.12xlarge [2]	15000		1875,0		60000	
m7gd.16xlarge [2]	20 000		2500,0		80000	
m7gd.metal 2	20 000		2500,0		80000	
m7i.large [1]	650	10 000	81,25	1250,00	3600	40 000
m7i.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
m7i.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
m7i.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
m7i.8xlarge [2]	10 000		1250,0		40 000	
m7i.12xlarge [2]	15000		1875,0		60000	
m7i.16xlarge [2]	20 000		2500,0		80000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
m7i.24xlarge [2]	30 000		3750,0		120000	
m7i.48xlarge [2]	40 000		5000,0		240000	
m7i.metal-24xl [2]	30 000		3750,0		120000	
m7i.metal-48xl [2]	40 000		5000,0		240000	
m7i-flex.large [1]	312	10 000	39,06	1250,00	2500	40 000
m7i-flex.xlarge [1]	625	10 000	78,12	1250,00	3600	40 000
m7i-flex.2xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
m7i-flex.4xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
m7i-flex.8xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
mac1.metal [2]	14000		1750,0		80000	
mac2.metal [2]	10 000		1250,0		55000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
mac2-m1 ultra metal 2	10 000		1250,0		55000	
mac2-m2.metal [2]	8000		1000,0		55000	
mac2-m2pro.metal [2]	8000		1000,0		55000	
t3.nano [1]	43	2085	5,38	260,62	250	11800
t3.micro [1]	87	2085	10,88	260,62	500	11800
t3.small [1]	174	2085	21,75	260,62	1 000	11800
t3.medium [1]	347	2085	43,38	260,62	2000	11800
t3.large [1]	695	2780	86,88	347,50	4000	15700
t3.xlarge [1]	695	2780	86,88	347,50	4000	15700
t3.2xlarge [1]	695	2780	86,88	347,50	4000	15700
t3a.nano [1]	45	2085	5,62	260,62	250	11800
t3a.micro [1]	90	2085	11.25	260,62	500	11800
t3a.small [1]	175	2085	21.88	260,62	1 000	11800
t3a.medium [1]	350	2085	43.75	260,62	2000	11800
t3a.large [1]	695	2780	86,88	347,50	4000	15700

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
t3a.xlarge [1]	695	2780	86,88	347,50	4000	15700
t3a.2xlarge [1]	695	2780	86,88	347,50	4000	15700
t4g.nano [1]	43	2085	5,38	260,62	250	11800
t4g.micro [1]	87	2085	10,88	260,62	500	11800
t4g.small [1]	174	2085	21,75	260,62	1 000	11800
t4g.medium [1]	347	2085	43,38	260,62	2000	11800
t4g.large [1]	695	2780	86,88	347,50	4000	15700
t4g.xlarge [1]	695	2780	86,88	347,50	4000	15700
t4g.2xlarge [1]	695	2780	86,88	347,50	4000	15700

Calcul optimisé

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
c4.large [2]	500		62,5		4000	
c4.xlarge [2]	750		93,75		6 000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
c4.2xlarge [2]	1 000		125,0		8000	
c4.4xlarge [2]	2000		250,0		16000	
c4.8xlarge [2]	4000		500,0		32000	
c5.large [1]	650	4750	81,25	593,75	4000	20 000
c5.xlarge [1]	1150	4750	143,75	593,75	6 000	20 000
c5.2xlarge [1]	2300	4750	287,50	593,75	10 000	20 000
c5.4xlarge [2]	4750		593,75		20 000	
c5.9xlarge [2]	9500		1187,5		40 000	
c5.12xlarge [2]	9500		1187,5		40 000	
c5.18xlarge [2]	19000		2375,0		80000	
c5.24xlarge [2]	19000		2375,0		80000	
c5.metal [2]	19000		2375,0		80000	
c5a.large [1]	200	3170	25,00	396,25	800	13300

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
c5a.xlarge [1]	400	3170	50,00	396,25	1600	13300
c5a.2xlarge [1]	800	3170	100,00	396,25	3200	13300
c5a.4xlarge [1]	1580	3170	197,50	396,25	6600	13300
c5a.8xlarge [2]	3170		396,25		13300	
c5a.12xlarge [2]	4750		593,75		20 000	
c5a.16xlarge [2]	6300		787,5		26700	
c5a.24xlarge [2]	9500		1187,5		40 000	
c5ad.large [1]	200	3170	25,00	396,25	800	13300
c5ad.xlarge [1]	400	3170	50,00	396,25	1600	13300
c5ad.2xlarge [1]	800	3170	100,00	396,25	3200	13300
c5ad.4xlarge [1]	1580	3170	197,50	396,25	6600	13300

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
c5ad.8xlarge [2]	3170		396,25		13300	
c5ad.12xlarge [2]	4750		593,75		20 000	
c5ad.16xlarge [2]	6300		787,5		26700	
c5ad.24xlarge [2]	9500		1187,5		40 000	
c5d.large [1]	650	4750	81,25	593,75	4000	20 000
c5d.xlarge [1]	1150	4750	143,75	593,75	6 000	20 000
c5d.2xlarge [1]	2300	4750	287,50	593,75	10 000	20 000
c5d.4xlarge [2]	4750		593,75		20 000	
c5d.9xlarge [2]	9500		1187,5		40 000	
c5d.12xlarge [2]	9500		1187,5		40 000	
c5d.18xlarge [2]	19000		2375,0		80000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
c5d.24xlarge [2]	19000		2375,0		80000	
c5d.metal [2]	19000		2375,0		80000	
c5n.large [1]	650	4750	81,25	593,75	4000	20 000
c5n.xlarge [1]	1150	4750	143,75	593,75	6 000	20 000
c5n.2xlarge [1]	2300	4750	287,50	593,75	10 000	20 000
c5n.4xlarge [2]	4750		593,75		20 000	
c5n.9xlarge [2]	9500		1187,5		40 000	
c5n.18xlarge [2]	19000		2375,0		80000	
c5n.metal [2]	19000		2375,0		80000	
c6a.large [1]	650	10 000	81,25	1250,00	3600	40 000
c6a.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
c6a.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
c6a.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
c6a.8xlarge [2]	10 000		1250,0		40 000	
c6a.12xlarge [2]	15000		1875,0		60000	
c6a.16xlarge [2]	20 000		2500,0		80000	
c6a.24xlarge [2]	30 000		3750,0		120000	
c6a.32xlarge [2]	40 000		5000,0		160000	
c6a.48xlarge [2]	40 000		5000,0		240000	
c6a.metal [2]	40 000		5000,0		240000	
c6g.medium [1]	315	4750	39,38	593,75	2500	20 000
c6g.large [1]	630	4750	78,75	593,75	3600	20 000
c6g.xlarge [1]	1188	4750	148,50	593,75	6 000	20 000
c6g.2xlarge [1]	2375	4750	296,88	593,75	12 000	20 000
c6g.4xlarge [2]	4750		593,75		20 000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
c6g.8xlarge [2]	9500		1187,5		40 000	
c6g.12xlarge [2]	14250		1781,25		50000	
c6g.16xlarge [2]	19000		2375,0		80000	
c6g.metal [2]	19000		2375,0		80000	
c6gd.medium [1]	315	4750	39,38	593,75	2500	20 000
c6gd.large [1]	630	4750	78,75	593,75	3600	20 000
c6gd.xlarge [1]	1188	4750	148,50	593,75	6 000	20 000
c6gd.2xlarge [1]	2375	4750	296,88	593,75	12 000	20 000
c6gd.4xlarge [2]	4750		593,75		20 000	
c6gd.8xlarge [2]	9500		1187,5		40 000	
c6gd.12xlarge [2]	14250		1781,25		50000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
c6gd.16xlarge [2]	19000		2375,0		80000	
c6gd.metal [2]	19000		2375,0		80000	
c6gn.medium [1]	760	9500	95,00	1187,50	2500	40 000
c6gn.large [1]	1235	9500	154,38	1187,50	5000	40 000
c6gn.xlarge [1]	2375	9500	296,88	1187,50	10 000	40 000
c6gn.2xlarge [1]	4750	9500	593,75	1187,50	20 000	40 000
c6gn.4xlarge [2]	9500		1187,5		40 000	
c6gn.8xlarge [2]	19000		2375,0		80000	
c6gn.12xlarge [2]	28500		3562,5		120000	
c6gn.16xlarge [2]	38000		4750,0		160000	
c6i.large [1]	650	10 000	81,25	1250,00	3600	40 000
c6i.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
c6i.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
c6i.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
c6i.8xlarge [2]	10 000		1250,0		40 000	
c6i.12xlarge [2]	15000		1875,0		60000	
c6i.16xlarge [2]	20 000		2500,0		80000	
c6i.24xlarge [2]	30 000		3750,0		120000	
c6i.32xlarge [2]	40 000		5000,0		160000	
c6i.metal [2]	40 000		5000,0		160000	
c6id.large [1]	650	10 000	81,25	1250,00	3600	40 000
c6id.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
c6id.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
c6id.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
c6id.8xlarge [2]	10 000		1250,0		40 000	
c6id.12xlarge [2]	15000		1875,0		60000	
c6id.16xlarge [2]	20 000		2500,0		80000	
c6id.24xlarge [2]	30 000		3750,0		120000	
c6id.32xlarge [2]	40 000		5000,0		160000	
c6id.metal [2]	40 000		5000,0		160000	
c6in.large [1]	1562	25000	195,31	3125,00	6250	100 000
c6in.xlarge [1]	3125	25000	390,62	3125,00	12500	100 000
c6in.2xlarge [1]	6250	25000	781,25	3125,00	25000	100 000
c6in.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100 000
c6in.8xlarge [2]	25000		3125,0		100 000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
c6in.12xlarge [2]	37500		4687,5		150000	
c6in.16xlarge [2]	50000		6250,0		200 000	
c6in.24xlarge [2]	75000		9375,0		300 000	
c6in.32xlarge [2]	100 000		12500,0		400 000	
c6in.metal [2]	100 000		12500,0		400 000	
c7a.medium [1]	325	10 000	40,62	1250,00	2500	40 000
c7a.large [1]	650	10 000	81,25	1250,00	3600	40 000
c7a.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
c7a.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
c7a.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
c7a.8xlarge [2]	10 000		1250,0		40 000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
c7a.12xlarge [2]	15000		1875,0		60000	
c7a.16xlarge [2]	20 000		2500,0		80000	
c7a.24xlarge [2]	30 000		3750,0		120000	
c7a.32xlarge [2]	40 000		5000,0		160000	
c7a.48xlarge [2]	40 000		5000,0		240000	
c7a.metal-48xl [2]	40 000		5000,0		240000	
c7g.medium [1]	315	10 000	39,38	1250,00	2500	40 000
c7g.large [1]	630	10 000	78,75	1250,00	3600	40 000
c7g.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
c7g.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
c7g.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
c7g.8xlarge [2]	10 000		1250,0		40 000	
c7g.12xlarge [2]	15000		1875,0		60000	
c7g.16xlarge [2]	20 000		2500,0		80000	
c7g.metal [2]	20 000		2500,0		80000	
c7gd.medium [1]	315	10 000	39,38	1250,00	2500	40 000
c7gd.large [1]	630	10 000	78,75	1250,00	3600	40 000
c7gd.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
c7gd.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
c7gd.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
c7gd.8xlarge [2]	10 000		1250,0		40 000	
c7gd.12xlarge [2]	15000		1875,0		60000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
c7gd.16xlarge [2]	20 000		2500,0		80000	
c7gd.metal 2	20 000		2500,0		80000	
c7gn.medium [1]	521	10 000	65,12	1250,00	2083	40 000
c7gn.large [1]	1042	10 000	130,25	1250,00	4167	40 000
c7gn.xlarge [1]	2083	10 000	260,38	1250,00	8333	40 000
c7gn.2xlarge [1]	4167	10 000	520,88	1250,00	16667	40 000
c7gn.4xlarge [1]	8333	10 000	1041,62	1250,00	33333	40 000
c7gn.8xlarge [1]	16667	20 000	2083,38	2500,00	66667	80000
c7gn.12xlarge [1]	25000	30 000	3125,00	3750,00	100 000	120000
c7gn.16xlarge [1]	33333	40 000	4166,62	5000,00	133333	160000
c7gn.metal 1	33333	40 000	4166,62	5000,00	133333	160000
c7i.large [1]	650	10 000	81,25	1250,00	3600	40 000
c7i.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
c7i.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
c7i.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
c7i.8xlarge [2]	10 000		1250,0		40 000	
c7i.12xlarge [2]	15000		1875,0		60000	
c7i.16xlarge [2]	20 000		2500,0		80000	
c7i.24xlarge [2]	30 000		3750,0		120000	
c7i.48xlarge [2]	40 000		5000,0		240000	
c7i.metal-24xl [2]	30 000		3750,0		120000	
c7i.metal-48xl [2]	40 000		5000,0		240000	
c7i-flex.large 1	312	10 000	39,06	1250,00	2500	40 000
c7i-flex.xlarge [1]	625	10 000	78,12	1250,00	3600	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
c7i-flex.2xlarge 1	1250	10 000	156,25	1250,00	6 000	40 000
c7i-flex.4xlarge 1	2500	10 000	312,50	1250,00	12 000	40 000
c7i-flex 8 x large 1	5000	10 000	625,00	1250,00	20 000	40 000

Optimisé pour la mémoire

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
r4.large [2]	425		53,125		3000	
r4.xlarge [2]	850		106,25		6 000	
r4.2xlarge [2]	1700		212,5		12 000	
r4.4xlarge [2]	3500		437,5		18750	
r4.8xlarge [2]	7000		875,0		37500	
r4.16xlarge [2]	14000		1750,0		75000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
r5.large [1]	650	4750	81,25	593,75	3600	18750
r5.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
r5.2xlarge [1]	2300	4750	287,50	593,75	12 000	18750
r5.4xlarge [2]	4750		593,75		18750	
r5.8xlarge [2]	6800		850,0		30 000	
r5.12xlarge [2]	9500		1187,5		40 000	
r5.16xlarge [2]	13600		1700,0		60000	
r5.24xlarge [2]	19000		2375,0		80000	
r5.metal [2]	19000		2375,0		80000	
r5a.large [1]	650	2880	81,25	360,00	3600	16000
r5a.xlarge [1]	1085	2880	135,62	360,00	6 000	16000
r5a.2xlarge [1]	1580	2880	197,50	360,00	8333	16000
r5a.4xlarge [2]	2880		360,0		16000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
r5a.8xlarge [2]	4750		593,75		20 000	
r5a.12xlarge [2]	6780		847,5		30 000	
r5a.16xlarge [2]	9500		1187,5		40 000	
r5a.24xlarge [2]	13570		1696,25		60000	
r5ad.large [1]	650	2880	81,25	360,00	3600	16000
r5ad.xlarge [1]	1085	2880	135,62	360,00	6 000	16000
r5ad.2xlarge [1]	1580	2880	197,50	360,00	8333	16000
r5ad.4xlarge [2]	2880		360,0		16000	
r5ad.8xlarge [2]	4750		593,75		20 000	
r5ad.12xlarge [2]	6780		847,5		30 000	
r5ad.16xlarge [2]	9500		1187,5		40 000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
r5ad.24xlarge [2]	13570		1696,25		60000	
r5b.large [1]	1250	10 000	156,25	1250,00	5417	43333
r5b.xlarge [1]	2500	10 000	312,50	1250,00	10833	43333
r5b.2xlarge [1]	5000	10 000	625,00	1250,00	21667	43333
r5b.4xlarge [2]	10 000		1250,0		43333	
r5b.8xlarge [2]	20 000		2500,0		86667	
r5b.12xlarge [2]	30 000		3750,0		130000	
r5b.16xlarge [2]	40 000		5000,0		173333	
r5b.24xlarge [2]	60000		7500,0		260000	
r5b.metal [2]	60000		7500,0		260000	
r5d.large [1]	650	4750	81,25	593,75	3600	18750
r5d.xlarge [1]	1150	4750	143,75	593,75	6 000	18750

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
r5d.2xlarge [1]	2300	4750	287,50	593,75	12 000	18750
r5d.4xlarge [2]	4750		593,75		18750	
r5d.8xlarge [2]	6800		850,0		30 000	
r5d.12xlarge [2]	9500		1187,5		40 000	
r5d.16xlarge [2]	13600		1700,0		60000	
r5d.24xlarge [2]	19000		2375,0		80000	
r5d.metal [2]	19000		2375,0		80000	
r5dn.large [1]	650	4750	81,25	593,75	3600	18750
r5dn.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
r5dn.2xlarge [1]	2300	4750	287,50	593,75	12 000	18750
r5dn.4xlarge [2]	4750		593,75		18750	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
r5dn.8xlarge [2]	6800		850,0		30 000	
r5dn.12xlarge [2]	9500		1187,5		40 000	
r5dn.16xlarge [2]	13600		1700,0		60000	
r5dn.24xlarge [2]	19000		2375,0		80000	
r5dn.metal [2]	19000		2375,0		80000	
r5n.large [1]	650	4750	81,25	593,75	3600	18750
r5n.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
r5n.2xlarge [1]	2300	4750	287,50	593,75	12 000	18750
r5n.4xlarge [2]	4750		593,75		18750	
r5n.8xlarge [2]	6800		850,0		30 000	
r5n.12xlarge [2]	9500		1187,5		40 000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
r5n.16xlarge [2]	13600		1700,0		60000	
r5n.24xlarge [2]	19000		2375,0		80000	
r5n.metal [2]	19000		2375,0		80000	
r6a.large [1]	650	10 000	81,25	1250,00	3600	40 000
r6a.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
r6a.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
r6a.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
r6a.8xlarge [2]	10 000		1250,0		40 000	
r6a.12xlarge [2]	15000		1875,0		60000	
r6a.16xlarge [2]	20 000		2500,0		80000	
r6a.24xlarge [2]	30 000		3750,0		120000	
r6a.32xlarge [2]	40 000		5000,0		160000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
r6a.48xlarge [2]	40 000		5000,0		240000	
r6a.metal [2]	40 000		5000,0		240000	
r6g.medium [1]	315	4750	39,38	593,75	2500	20 000
r6g.large [1]	630	4750	78,75	593,75	3600	20 000
r6g.xlarge [1]	1188	4750	148,50	593,75	6 000	20 000
r6g.2xlarge [1]	2375	4750	296,88	593,75	12 000	20 000
r6g.4xlarge [2]	4750		593,75		20 000	
r6g.8xlarge [2]	9500		1187,5		40 000	
r6g.12xlarge [2]	14250		1781,25		50000	
r6g.16xlarge [2]	19000		2375,0		80000	
r6g.metal [2]	19000		2375,0		80000	
r6gd.medium [1]	315	4750	39,38	593,75	2500	20 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
r6gd.large [1]	630	4750	78,75	593,75	3600	20 000
r6gd.xlarge [1]	1188	4750	148,50	593,75	6 000	20 000
r6gd.2xlarge [1]	2375	4750	296,88	593,75	12 000	20 000
r6gd.4xlarge [2]	4750		593,75		20 000	
r6gd.8xlarge [2]	9500		1187,5		40 000	
r6gd.12xlarge [2]	14250		1781,25		50000	
r6gd.16xlarge [2]	19000		2375,0		80000	
r6gd.metal [2]	19000		2375,0		80000	
r6i.large [1]	650	10 000	81,25	1250,00	3600	40 000
r6i.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
r6i.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
r6i.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
r6i.8xlarge [2]	10 000		1250,0		40 000	
r6i.12xlarge [2]	15000		1875,0		60000	
r6i.16xlarge [2]	20 000		2500,0		80000	
r6i.24xlarge [2]	30 000		3750,0		120000	
r6i.32xlarge [2]	40 000		5000,0		160000	
r6i.metal [2]	40 000		5000,0		160000	
r6idn.large [1]	1562	25000	195,31	3125,00	6250	100 000
r6idn.xlarge [1]	3125	25000	390,62	3125,00	12500	100 000
r6idn.2xlarge [1]	6250	25000	781,25	3125,00	25000	100 000
r6idn.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100 000
r6idn.8xlarge [2]	25000		3125,0		100 000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
r6idn.12xlarge [2]	37500		4687,5		150000	
r6idn.16xlarge [2]	50000		6250,0		200 000	
r6idn.24xlarge [2]	75000		9375,0		300 000	
r6idn.32xlarge [2]	100 000		12500,0		400 000	
r6idn.metal [2]	100 000		12500,0		400 000	
r6in.large [1]	1562	25000	195,31	3125,00	6250	100 000
r6in.xlarge [1]	3125	25000	390,62	3125,00	12500	100 000
r6in.2xlarge [1]	6250	25000	781,25	3125,00	25000	100 000
r6in.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100 000
r6in.8xlarge [2]	25000		3125,0		100 000	
r6in.12xlarge [2]	37500		4687,5		150000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
r6in.16xlarge [2]	50000		6250,0		200 000	
r6in.24xlarge [2]	75000		9375,0		300 000	
r6in.32xlarge [2]	100 000		12500,0		400 000	
r6in.metal [2]	100 000		12500,0		400 000	
r6id.large [1]	650	10 000	81,25	1250,00	3600	40 000
r6id.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
r6id.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
r6id.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
r6id.8xlarge [2]	10 000		1250,0		40 000	
r6id.12xlarge [2]	15000		1875,0		60000	
r6id.16xlarge [2]	20 000		2500,0		80000	
r6id.24xlarge [2]	30 000		3750,0		120000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
r6id.32xlarge [2]	40 000		5000,0		160000	
r6id.metal [2]	40 000		5000,0		160000	
r7a.medium [1]	325	10 000	40,62	1250,00	2500	40 000
r7a.large [1]	650	10 000	81,25	1250,00	3600	40 000
r7a.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
r7a.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
r7a.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
r7a.8xlarge [2]	10 000		1250,0		40 000	
r7a.12xlarge [2]	15000		1875,0		60000	
r7a.16xlarge [2]	20 000		2500,0		80000	
r7a.24xlarge [2]	30 000		3750,0		120000	
r7a.32xlarge [2]	40 000		5000,0		160000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
r7a.48xlarge [2]	40 000		5000,0		240000	
r7a.metal-48xl [2]	40 000		5000,0		240000	
r7g.medium [1]	315	10 000	39,38	1250,00	2500	40 000
r7g.large [1]	630	10 000	78,75	1250,00	3600	40 000
r7g.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
r7g.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
r7g.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
r7g.8xlarge [2]	10 000		1250,0		40 000	
r7g.12xlarge [2]	15000		1875,0		60000	
r7g.16xlarge [2]	20 000		2500,0		80000	
r7g.metal [2]	20 000		2500,0		80000	
r7gd.medium [1]	315	10 000	39,38	1250,00	2500	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
r7gd.large [1]	630	10 000	78,75	1250,00	3600	40 000
r7gd.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
r7gd.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
r7gd.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
r7gd.8xlarge [2]	10 000		1250,0		40 000	
r7gd.12xlarge [2]	15000		1875,0		60000	
r7gd.16xlarge [2]	20 000		2500,0		80000	
r7gd.metal 2	20 000		2500,0		80000	
r7i.large [1]	650	10 000	81,25	1250,00	3600	40 000
r7i.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
r7i.2xlarge [1]	2500	10 000	312,50	1250,00	12 000	40 000
r7i.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
r7i.8xlarge [2]	10 000		1250,0		40 000	
r7i.12xlarge [2]	15000		1875,0		60000	
r7i.16xlarge [2]	20 000		2500,0		80000	
r7i.24xlarge [2]	30 000		3750,0		120000	
r7i.48xlarge [2]	40 000		5000,0		240000	
r7i.metal-24xl [2]	30 000		3750,0		120000	
r7i.metal-48xl [2]	40 000		5000,0		240000	
r7iz.large [1]	792	10 000	99,00	1250,00	3600	40 000
r7iz.xlarge [1]	1584	10 000	198,00	1250,00	6667	40 000
r7iz.2xlarge [1]	3168	10 000	396,00	1250,00	13333	40 000
r7iz.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
r7iz.8xlarge [2]	10 000		1250,0		40 000	
r7iz.12xlarge [2]	19000		2375,0		76000	
r7iz.16xlarge [2]	20 000		2500,0		80000	
r7iz.32xlarge [2]	40 000		5000,0		160000	
r7iz.metal-16xl [2]	20 000		2500,0		80000	
r7iz.metal-32xl [2]	40 000		5000,0		160000	
r8g.medium 1	315	10 000	39,38	1250,00	2500	40 000
8 g .large 1	630	10 000	78,75	1250,00	3600	40 000
r8g.xlarge 1	1250	10 000	156,25	1250,00	6 000	40 000
r8g.2xlarge 1	2500	10 000	312,50	1250,00	12 000	40 000
r8g.4xlarge 1	5000	10 000	625,00	1250,00	20 000	40 000
8 g x 8 x large 2	10 000		1250,0		40 000	
8 g, 12 x large 2	15000		1875,0		60000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
8 g x 16 x large 2	20 000		2500,0		80000	
8 g, 24 x large 2	30 000		3750,0		120000	
8 g. 48 x large 2	40 000		5000,0		240000	
r8g.metal-24xl 2	30 000		3750,0		120000	
r8g.metal-48xl 2	40 000		5000,0		240000	
u-3tb1.56 xlarge [2]	19000		2375,0		80000	
u-6tb1.56 xlarge [2]	38000		4750,0		160000	
u-6tb1.11 2xlarge [2]	38000		4750,0		160000	
u-6tb1.me tal [2]	38000		4750,0		160000	
u-9tb1.11 2xlarge [2]	38000		4750,0		160000	
u-9tb1.me tal [2]	38000		4750,0		160000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
u-12tb1.112xlarge [2]	38000		4750,0		160000	
u-12tb1.metal [2]	38000		4750,0		160000	
u-18tb1.112xlarge [2]	38000		4750,0		160000	
u-18tb1.metal [2]	38000		4750,0		160000	
u-24tb1.112xlarge [2]	38000		4750,0		160000	
u-24tb1.metal [2]	38000		4750,0		160000	
u7i-12tb.224xlarge 2	60000		7500,0		420000	
u7in-16tb.224xlarge 2	100 000		12500,0		420000	
u7in-24tb.224xlarge 2	100 000		12500,0		420000	
u7in-32tb.224xlarge 2	100 000		12500,0		420000	
x1.16xlarge [2]	7000		875,0		40 000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
x1.32xlarge [2]	14000		1750,0		80000	
x2gd.medium [1]	315	4750	39,38	593,75	2500	20 000
x2gd.large [1]	630	4750	78,75	593,75	3600	20 000
x2gd.xlarge [1]	1188	4750	148,50	593,75	6 000	20 000
x2gd.2xlarge [1]	2375	4750	296,88	593,75	12 000	20 000
x2gd.4xlarge [2]	4750		593,75		20 000	
x2gd.8xlarge [2]	9500		1187,5		40 000	
x2gd.12xlarge [2]	14250		1781,25		60000	
x2gd.16xlarge [2]	19000		2375,0		80000	
x2gd.metal [2]	19000		2375,0		80000	
x2idn.16xlarge [2]	40 000		5000,0		173333	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
x2idn.24xlarge [2]	60000		7500,0		260000	
x2idn.32xlarge [2]	80000		10000,0		260000	
x2idn.metal [2]	80000		10000,0		260000	
x2iedn.xlarge [1]	2500	20 000	312,50	2500,00	8125	65000
x2iedn.2xlarge [1]	5000	20 000	625,00	2500,00	16250	65000
x2iedn.4xlarge [1]	10 000	20 000	1250,00	2500,00	32500	65000
x2iedn.8xlarge [2]	20 000		2500,0		65000	
x2iedn.16xlarge [2]	40 000		5000,0		130000	
x2iedn.24xlarge [2]	60000		7500,0		195 000	
x2iedn.32xlarge [2]	80000		10000,0		260000	
x2iedn.metal [2]	80000		10000,0		260000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
x2iezn.2xlarge [2]	3170		396,25		13333	
x2iezn.4xlarge [2]	4750		593,75		20 000	
x2iezn.6xlarge [2]	9500		1187,5		40 000	
x2iezn.8xlarge [2]	12 000		1500,0		55000	
x2iezn.12xlarge [2]	19000		2375,0		80000	
x2iezn.metal [2]	19000		2375,0		80000	
x1e.xlarge [2]	500		62,5		3700	
x1e.2xlarge [2]	1 000		125,0		7400	
x1e.4xlarge [2]	1750		218,75		10 000	
x1e.8xlarge [2]	3500		437,5		20 000	
x1e.16xlarge [2]	7000		875,0		40 000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
x1e.32xlarge [2]	14000		1750,0		80000	
z1d.large [1]	800	3170	100,00	396,25	3333	13333
z1d.xlarge [1]	1580	3170	197,50	396,25	6667	13333
z1d.2xlarge [2]	3170		396,25		13333	
z1d.3xlarge [2]	4750		593,75		20 000	
z1d.6xlarge [2]	9500		1187,5		40 000	
z1d.12xlarge [2]	19000		2375,0		80000	
z1d.metal [2]	19000		2375,0		80000	

Stockage optimisé

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
d2.xlarge [2]	750		93,75		6 000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
d2.2xlarge [2]	1 000		125,0		8000	
d2.4xlarge [2]	2000		250,0		16000	
d2.8xlarge [2]	4000		500,0		32000	
d3.xlarge [1]	850	2800	106,25	350,00	5000	15000
d3.2xlarge [1]	1700	2800	212,50	350,00	10 000	15000
d3.4xlarge [2]	2800		350,0		15000	
d3.8xlarge [2]	5000		625,0		30 000	
d3en.xlarge [1]	850	2800	106,25	350,00	5000	15000
d3en.2xlarge [1]	1700	2800	212,50	350,00	10 000	15000
d3en.4xlarge [2]	2800		350,0		15000	
d3en.6xlarge [2]	4000		500,0		25000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
d3en.8xlarge [2]	5000		625,0		30 000	
d3en.12xlarge [2]	7000		875,0		40 000	
h1.2xlarge [2]	1750		218,75		12 000	
h1.4xlarge [2]	3500		437,5		20 000	
h1.8xlarge [2]	7000		875,0		40 000	
h1.16xlarge [2]	14000		1750,0		80000	
i3.large [2]	425		53,125		3000	
i3.xlarge [2]	850		106,25		6 000	
i3.2xlarge [2]	1700		212,5		12 000	
i3.4xlarge [2]	3500		437,5		16000	
i3.8xlarge [2]	7000		875,0		32500	
i3.16xlarge [2]	14000		1750,0		65000	
i3.metal [2]	19000		2375,0		80000	
i3en.large [1]	576	4750	72,10	593,75	3000	20 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
i3en.xlarge [1]	1153	4750	144,20	593,75	6 000	20 000
i3en.2xlarge [1]	2307	4750	288.39	593,75	12 000	20 000
i3en.3xlarge [1]	3800	4750	475,00	593,75	15000	20 000
i3en.6xlarge [2]	4750		593,75		20 000	
i3en.12xlarge [2]	9500		1187,5		40 000	
i3en.24xlarge [2]	19000		2375,0		80000	
i3en.metal [2]	19000		2375,0		80000	
i4g.large [1]	625	10 000	78,12	1250,00	2500	40 000
i4g.xlarge [1]	1250	10 000	156,25	1250,00	5000	40 000
i4g.2xlarge [1]	2500	10 000	312,50	1250,00	10 000	40 000
i4g.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
i4g.8xlarge [2]	10 000		1250,0		40 000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
i4g.16xlarge [2]	20 000		2500,0		80000	
i4i.large [1]	625	10 000	78,12	1250,00	2500	40 000
i4i.xlarge [1]	1250	10 000	156,25	1250,00	5000	40 000
i4i.2xlarge [1]	2500	10 000	312,50	1250,00	10 000	40 000
i4i.4xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
i4i.8xlarge [2]	10 000		1250,0		40 000	
i4i.12xlarge [2]	15000		1875,0		60000	
i4i.16xlarge [2]	20 000		2500,0		80000	
i4i.24xlarge [2]	30 000		3750,0		120000	
i4i.32xlarge [2]	40 000		5000,0		160000	
i4i.metal [2]	40 000		5000,0		160000	
im4gn.large [1]	1250	10 000	156,25	1250,00	5000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
im4gn.xlarge [1]	2500	10 000	312,50	1250,00	10 000	40 000
im4gn.2xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
im4gn.4xlarge [2]	10 000		1250,0		40 000	
im4gn.8xlarge [2]	20 000		2500,0		80000	
im4gn.16xlarge [2]	40 000		5000,0		160000	
is4gen.medium [1]	625	10 000	78,12	1250,00	2500	40 000
is4gen.large [1]	1250	10 000	156,25	1250,00	5000	40 000
is4gen.xlarge [1]	2500	10 000	312,50	1250,00	10 000	40 000
is4gen.2xlarge [1]	5000	10 000	625,00	1250,00	20 000	40 000
is4gen.4xlarge [2]	10 000		1250,0		40 000	
is4gen.8xlarge [2]	20 000		2500,0		80000	

Calcul accéléré

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
dl1.24xlarge [2]	19000		2375,0		80000	
dl2q.24xlarge [2]	19000		2375,0		80000	
f1.2xlarge [2]	1700		212,5		12 000	
f1.4xlarge [2]	3500		437,5		44000	
f1.16xlarge [2]	14000		1750,0		75000	
g3.4xlarge [2]	3500		437,5		20 000	
g3.8xlarge [2]	7000		875,0		40 000	
g3.16xlarge [2]	14000		1750,0		80000	
g4ad.xlarge [1]	400	3170	50,00	396,25	1700	13333
g4ad.2xlarge [1]	800	3170	100,00	396,25	3400	13333
g4ad.4xlarge [1]	1580	3170	197,50	396,25	6700	13333

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
g4ad.8xlarge [2]	3170		396,25		13333	
g4ad.16xlarge [2]	6300		787,5		26667	
g4dn.xlarge [1]	950	3500	118.75	437,50	3000	20 000
g4dn.2xlarge [1]	1150	3500	143,75	437,50	6 000	20 000
g4dn.4xlarge [2]	4750		593,75		20 000	
g4dn.8xlarge [2]	9500		1187,5		40 000	
g4dn.12xlarge [2]	9500		1187,5		40 000	
g4dn.16xlarge [2]	9500		1187,5		40 000	
g4dn.metal [2]	19000		2375,0		80000	
g5.xlarge [1]	700	3500	87,50	437,50	3000	15000
g5.2xlarge [1]	850	3500	106,25	437,50	3500	15000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
g5.4xlarge [2]	4750		593,75		20 000	
g5.8xlarge [2]	16000		2000,0		65000	
g5.12xlarge [2]	16000		2000,0		65000	
g5.16xlarge [2]	16000		2000,0		65000	
g5.24xlarge [2]	19000		2375,0		80000	
g5.48xlarge [2]	19000		2375,0		80000	
g5g.xlarge [1]	1188	4750	148,50	593,75	6 000	20 000
g5g.2xlarge [1]	2375	4750	296,88	593,75	12 000	20 000
g5g.4xlarge [2]	4750		593,75		20 000	
g5g.8xlarge [2]	9500		1187,5		40 000	
g5g.16xlarge [2]	19000		2375,0		80000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
g5g.metal [2]	19000		2375,0		80000	
g6.xlarge [1]	1 000	5000	125,00	625,00	4000	20 000
g6,2 x large [1]	2000	5000	250,00	625,00	8000	20 000
g6,4xlarge [2]	8000		1000,0		32000	
g 6,8 x large [2]	16000		2000,0		64000	
g 6,12 x large [2]	20 000		2500,0		80000	
g 6,16 x large [2]	20 000		2500,0		80000	
g 6,24 x large [2]	30 000		3750,0		120000	
g 6,48 x large [2]	60000		7500,0		240000	
g6e.xlarge [1]	1 000	5000	125,00	625,00	4000	20 000
g6e.2xlarge [1]	2000	5000	250,00	625,00	8000	20 000
g6e.4xlarge [2]	8000		1000,0		32000	
6e.8xlarge [2]	16000		2000,0		64000	
g6e.12xlarge [2]	20 000		2500,0		80000	
g6e.16xlarge [2]	20 000		2500,0		80000	
g6e.24xlarge [2]	30 000		3750,0		120000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
g6e.48xlarge [2]	60000		7500,0		240000	
gr6,4xlarge [2]	8000		1000,0		32000	
gr6,8xlarge [2]	16000		2000,0		64000	
inf1.xlarge [1]	1190	4750	148.75	593,75	4000	20 000
inf1.2xlarge [1]	1190	4750	148.75	593,75	6 000	20 000
inf1.6xlarge [2]	4750		593,75		20 000	
inf1.24xlarge [2]	19000		2375,0		80000	
inf2.xlarge [1]	1250	10 000	156,25	1250,00	6 000	40 000
inf2.8xlarge [2]	10 000		1250,0		40 000	
inf2.24xlarge [2]	30 000		3750,0		120000	
inf2.48xlarge [2]	60000		7500,0		240000	
p2.xlarge [2]	750		93,75		6 000	
p2.8xlarge [2]	5000		625,0		32500	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
p2.16xlarge [2]	10 000		1250,0		65000	
p3.2xlarge [2]	1750		218,75		10 000	
p3.8xlarge [2]	7000		875,0		40 000	
p3.16xlarge [2]	14000		1750,0		80000	
p3dn.24xlarge [2]	19000		2375,0		80000	
p4d.24xlarge [2]	19000		2375,0		80000	
p4de.24xlarge [2]	19000		2375,0		80000	
p5.48xlarge [2]	80000		10000,0		260000	
trn1.2xlarge [1]	5000	20 000	625,00	2500,00	16250	65000
trn1.32xlarge [2]	80000		10000,0		260000	
trn1n.32xlarge [2]	80000		10000,0		260000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
vt1.3xlarge [1]	2375	4750	296,88	593,75	10 000	20 000
vt1.6xlarge [2]	4750		593,75		20 000	
vt1.24xlarge [2]	19000		2375,0		80000	

Calcul haute performance

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
hpc6a.48xlarge [1]	87	2085	10,88	260,62	500	11 000
hpc6id.32xlarge [1]	87	2085	10,88	260,62	500	11 000
hpc7a.12xlarge [1]	87	2085	10,88	260,62	500	11 000
hpc7a.24xlarge [1]	87	2085	10,88	260,62	500	11 000
hpc7a.48xlarge [1]	87	2085	10,88	260,62	500	11 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	Base de référence IOPS (16 Kio E/S)	Maximum IOPS (16 Kio E/S)
hpc7a.96xlarge [1]	87	2085	10,88	260,62	500	11 000
hpc7g.4xlarge [1]	87	2085	10,88	260,62	500	11 000
hpc7g.8xlarge [1]	87	2085	10,88	260,62	500	11 000
hpc7g.16xlarge [1]	87	2085	10,88	260,62	500	11 000

EBSoptimisation prise en charge

Les types d'instances suivants prennent en charge EBS l'EBSoptimisation, mais l'optimisation n'est pas activée par défaut. Vous devez activer EBS l'optimisation, moyennant un supplément horaire, pendant ou après le lancement pour atteindre le niveau de EBS performance décrit.

Taille d'instance	Bande passante maximum (Mbit/s)	Débit maximal (Mbit/s, I/O de 128 Kio)	Maximum IOPS (16 Kio E/S)
c1.xlarge	1 000	125,0	8000
c3.xlarge	500	62,5	4000
c3.2xlarge	1 000	125,0	8000
c3.4xlarge	2000	250,0	16000
i2.xlarge	500	62,5	4000
i2.2xlarge	1 000	125,0	8000

Taille d'instance	Bande passante maximum (Mbit/s)	Débit maximal (Mbit/s, I/O de 128 Kio)	Maximum IOPS (16 Kio E/S)
i2.4xlarge	2000	250,0	16000
m1.large	500	62,5	4000
m1.xlarge	1 000	125,0	8000
m2.2xlarge	500	62,5	4000
m2.4xlarge	1 000	125,0	8000
m3.xlarge	500	62,5	4000
m3.2xlarge	1 000	125,0	8000
r3.xlarge	500	62,5	4000
r3.2xlarge	1 000	125,0	8000
r3.4xlarge	2000	250,0	16000

> **Note**
>
> Les `r3.8xlarge` instances`i2.8xlarge`,`c3.8xlarge`, et ne disposent pas de EBS bande passante dédiée et ne proposent donc pas EBS d'optimisation. Dans ces instances, le trafic réseau et le EBS trafic Amazon partagent la même interface réseau 10 gigabits.

Profitez des performances EBS optimisées d'Amazon au maximum

Les EBS performances d'une instance sont limitées par les limites de performance du type d'instance ou par les performances agrégées de ses volumes attachés, la valeur la plus faible étant retenue. Pour atteindre des EBS performances maximales, une instance doit être associée à des volumes qui fournissent des performances combinées égales ou supérieures aux performances maximales de l'instance. Par exemple, `80,000` IOPS pour atteindre cet objectif`r6i.16xlarge`, l'instance doit disposer d'au moins des `5` `gp3` volumes provisionnés avec `16,000` IOPS chacun d'entre eux (`5`volumes x `16,000` IOPS = `80,000`IOPS). Nous vous recommandons de choisir un type

d'instance qui fournit un EBS débit Amazon dédié supérieur aux besoins de votre application ; sinon, la connexion entre Amazon EBS et Amazon EC2 peut devenir un goulot d'étranglement en termes de performances.

Vous pouvez utiliser les métriques `EBSIOBalance%` et `EBSByteBalance%` pour déterminer si vos instances sont dimensionnées correctement. Vous pouvez consulter ces mesures dans la CloudWatch console et définir une alarme qui sera déclenchée en fonction d'un seuil que vous spécifiez. Ces métriques sont exprimées sous forme de pourcentage. Les instances avec un pourcentage d'équilibre constamment faible sont candidates pour une augmentation de leur taille. Les instances pour lesquelles le pourcentage d'équilibre ne descend jamais sous 100 % sont candidates pour une diminution de leur taille. Pour de plus amples informations, veuillez consulter Surveillez vos instances à l'aide de CloudWatch.

Les instances à mémoire élevée sont conçues pour exécuter de grandes bases de données en mémoire, y compris des déploiements de production de la base de données SAP HANA en mémoire, dans le cloud. Pour optimiser les EBS performances, utilisez des instances à mémoire élevée avec un nombre pair `io1` ou des `io2` volumes avec des performances provisionnées identiques. Par exemple, pour les IOPS charges de travail importantes, utilisez quatre `io1` ou des `io2` volumes avec 40 000 instances provisionnées IOPS pour obtenir un maximum de 160 000 instances. IOPS De même, pour les charges de travail importantes, utilisez six `io2` volumes `io1` ou 48 000 provisionnés IOPS pour obtenir un débit maximal de 4 750 Mo/s. Pour des recommandations supplémentaires, consultez la section Configuration du stockage pour SAP HANA.

Considérations

- Les instances G4dn, i3en, Inf1, M5a, M5ad, R5a, R5ad, T3, T3a et Z1d lancées après le 26 février 2020 fournissent des performances optimisées maximales. EBS Pour obtenir les performances maximales d'une instance lancée avant le 26 février 2020, arrêtez-la et démarrez-la.
- Les instances C5, C5d, C5n, M5, M5d, M5n, M5dn, R5, R5d, R5n, R5dn et P3dn lancées après le 3 décembre 2019 fournissent des performances optimisées maximales. EBS Pour obtenir les performances maximales d'une instance lancée avant le 3 décembre 2019, arrêtez-la et démarrez-la.
- `u-6tb1.metalu-9tb1.metal`, et les `u-12tb1.metal` instances lancées après le 12 mars 2020 offrent des performances EBS optimisées maximales. Les instances de ce type lancées avant le 12 mars 2020 sont susceptibles de fournir des performances inférieures. Pour obtenir les performances maximales d'une instance lancée avant le 12 mars 2020, contactez votre équipe de compte pour mettre à niveau l'instance sans frais supplémentaires.

Trouvez les types d'EC2instances Amazon EBS optimisés pour Amazon

Vous pouvez utiliser le AWS CLI pour afficher les types d'instances de la région actuelle qui prennent en charge EBS l'optimisation.

Pour rechercher les types d'instances EBS optimisés par défaut pour Amazon

Utilisez la commande suivante de l' describe-instance-types. Si vous exécutez cette commande depuis une invite de commandes Windows, remplacez les caractères de suite \ line par le caractère ^.

```
aws ec2 describe-instance-types \
--query 'InstanceTypes[].{InstanceType:InstanceType,"MaxBandwidth(Mb/
s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIop
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--filters Name=ebs-info.ebs-optimized-support,Values=default --output=table
```

Exemple de sortie pour `eu-west-1` :

```
-------------------------------------------------------------------------------
|                            DescribeInstanceTypes                            |
+-------------------+---------------------+-----------+-----------------------+
|   InstanceType    | MaxBandwidth(Mb/s)  |  MaxIOPS  |  MaxThroughput(MB/s)  |
+-------------------+---------------------+-----------+-----------------------+
|  m5dn.8xlarge     |  6800               |  30000    |  850.0                |
|  m6gd.xlarge      |  4750               |  20000    |  593.75               |
|  c4.4xlarge       |  2000               |  16000    |  250.0                |
|  r4.16xlarge      |  14000              |  75000    |  1750.0               |
|  m5ad.large       |  2880               |  16000    |  360.0                |
...
```

Pour trouver les types d'instances qui prennent éventuellement en charge EBS l'optimisation Amazon

Utilisez la commande suivante de l' describe-instance-types.

```
aws ec2 describe-instance-types \
--query 'InstanceTypes[].{InstanceType:InstanceType,"MaxBandwidth(Mb/
s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIop
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--filters Name=ebs-info.ebs-optimized-support,Values=supported --output=table
```

Exemple de sortie pour `eu-west-1` :

```
-------------------------------------------------------------------------
|                        DescribeInstanceTypes                          |
+--------------+----------------------+----------+----------------------+
| InstanceType | MaxBandwidth(Mb/s)   | MaxIOPS  |  MaxThroughput(MB/s)  |
+--------------+----------------------+----------+----------------------+
|  i2.2xlarge  |  1000                |  8000    |  125.0                |
|  m2.4xlarge  |  1000                |  8000    |  125.0                |
|  m2.2xlarge  |  500                 |  4000    |  62.5                 |
|  c1.xlarge   |  1000                |  8000    |  125.0                |
|  i2.xlarge   |  500                 |  4000    |  62.5                 |
|  m3.xlarge   |  500                 |  4000    |  62.5                 |
|  m1.xlarge   |  1000                |  8000    |  125.0                |
|  r3.4xlarge  |  2000                |  16000   |  250.0                |
|  r3.2xlarge  |  1000                |  8000    |  125.0                |
|  c3.xlarge   |  500                 |  4000    |  62.5                 |
|  m3.2xlarge  |  1000                |  8000    |  125.0                |
|  r3.xlarge   |  500                 |  4000    |  62.5                 |
|  i2.4xlarge  |  2000                |  16000   |  250.0                |
|  c3.4xlarge  |  2000                |  16000   |  250.0                |
|  c3.2xlarge  |  1000                |  8000    |  125.0                |
|  m1.large    |  500                 |  4000    |  62.5                 |
+--------------+----------------------+----------+----------------------+
```

Activer EBS l'optimisation Amazon pour une EC2 instance Amazon

Vous pouvez activer manuellement EBS l'optimisation Amazon uniquement pour les types d'instances qui prennent éventuellement en charge EBS l'optimisation Amazon, mais qui ne sont pas EBS optimisés pour Amazon par défaut. Pour ces types d'instances, vous pouvez activer EBS l'optimisation d'Amazon pendant ou après le lancement moyennant un supplément horaire.

Console

Pour activer l'EBSoptimisation d'Amazon lors du lancement

Dans l'assistant de lancement d'instances, sélectionnez le type d'instance requis. Développez la section Détails avancés, puis pour l'instance EBS optimisée, sélectionnez Activer.

Si le type d'instance sélectionné ne prend pas en charge EBS l'optimisation Amazon, la liste déroulante est désactivée. Si le type d'instance est EBS optimisé pour Amazon par défaut, Enable est déjà sélectionné.

Pour activer l'EBSoptimisation d'Amazon après le lancement

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Instances, puis choisissez l'instance.
3. Arrêtez l'instance. Choisissez Actions, État de l'instance, Arrêter l'instance.

   > **Warning**
   >
   > Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instance sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

4. Tandis que l'instance est toujours sélectionnée, choisissez Actions, Paramètres de l'instance, puis Changer le type d'instance.
5. Sélectionnez EBS-optimized, puis choisissez Appliquer.

   Si le type d'instance est EBS optimisé pour Amazon par défaut, ou s'il ne prend pas en charge l'EBSoptimisation Amazon, la case à cocher est désactivée.
6. Redémarrez l'instance. Choisissez État de l'instance, Démarrer l'instance.

Command line

Pour activer l'EBSoptimisation d'Amazon lors du lancement

Vous pouvez utiliser l'une des commandes suivantes avec l'option correspondante.

- run-instances avec `--ebs-optimized` (AWS CLI)
- New-EC2Instanceavec `-EbsOptimized` (AWS Tools for Windows PowerShell)

Pour activer l'EBSoptimisation d'Amazon après le lancement

1. Si l'instance est en cours d'exécution, arrêtez-la à l'aide de l'une des commandes suivantes.
   - stop-instances (AWS CLI)
   - Stop-EC2Instance (AWS Tools for Windows PowerShell)

> **Warning**
>
> Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instance sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

2. Activez l'EBSoptimisation à l'aide de l'une des commandes suivantes avec l'option correspondante :

   - modify-instance-attributeavec `--ebs-optimized` (AWS CLI)
   - Edit-EC2InstanceAttributeavec `-EbsOptimized` (AWS Tools for Windows PowerShell)

CPUoptions pour les EC2 instances Amazon

De nombreuses EC2 instances Amazon prennent en charge le multithreading (SMT) simultané, ce qui permet à plusieurs threads de s'exécuter simultanément sur un même cœur. CPU Chaque thread est représenté sous la forme d'un virtuel CPU (vCPU) sur l'instance. Une instance possède un nombre de CPU cœurs par défaut, qui varie en fonction du type d'instance. Par exemple, un type d'`m5.xlarge`instance possède deux CPU cœurs et deux threads par cœur par défaut, soit quatre au total. vCPUs

> **Note**
>
> Chaque v CPU est le fil d'un CPU cœur, à l'exception des instances T2, des instances m7a, des instances Apple Silicon Mac et des ARM plateformes 64 bits telles que les instances alimentées par des processeurs AWS Graviton.

Dans la plupart des cas, il existe un type d'EC2instance Amazon qui possède une combinaison de mémoire et de nombre de mémoire adaptée vCPUs à vos charges de travail. Toutefois, vous pouvez spécifier les CPU options suivantes lors du lancement de l'instance afin d'optimiser votre instance en fonction de charges de travail ou de besoins commerciaux spécifiques :

- Nombre de CPU cœurs : vous pouvez personnaliser le nombre de CPU cœurs pour l'instance. Vous pouvez procéder ainsi pour optimiser les coûts de licence de votre logiciel avec une instance

dotée d'une quantité suffisante de ressources RAM pour les charges de travail gourmandes en mémoire, mais de moins de cœurs. CPU

- Threads par cœur : vous pouvez désactiver SMT en spécifiant un seul thread par CPU cœur. Vous pouvez le faire pour certaines charges de travail, telles que les charges de calcul haute performance (HPC).

Tarification

Il n'y a pas de frais supplémentaires ou réduits pour la spécification CPU des options. Vous êtes facturé de la même manière que les instances lancées avec les CPU options par défaut.

Table des matières

Règles de spécification CPU des options pour une EC2 instance Amazon

Pour définir les CPU options de votre instance, tenez compte des règles suivantes :

- Vous ne pouvez pas spécifier CPU d'options pour les instances bare metal.
- CPUles options ne peuvent être spécifiées que lors du lancement de l'instance et ne peuvent pas être modifiées après le lancement.
- Lorsque vous lancez une instance, vous devez spécifier à la fois le nombre de CPU cœurs et le nombre de threads par cœur dans la demande. Pour obtenir des exemples de requête, consultez Spécifier CPU les options pour une EC2 instance Amazon.
- Le nombre de vCPUs pour l'instance est le nombre de CPU cœurs multiplié par le nombre de threads par cœur. Pour spécifier un nombre personnalisé devCPUs, vous devez spécifier un nombre valide de CPU cœurs et de threads par cœur pour le type d'instance. Vous ne pouvez pas dépasser le nombre par défaut de vCPUs pour l'instance. Pour de plus amples informations, veuillez consulter CPUOptions prises en charge pour les types d'EC2instances Amazon.
- Pour désactiver le multithreading (SMT) simultané, également appelé hyperthreading, spécifiez un thread par cœur.

- Lorsque vous modifiez le type d'instance d'une instance existante, les CPU options sont automatiquement remplacées par les CPU options par défaut pour le nouveau type d'instance.
- Les CPU options spécifiées sont conservées après l'arrêt, le démarrage ou le redémarrage d'une instance.

CPUOptions prises en charge pour les types d'EC2instances Amazon

Les tableaux suivants répertorient les types d'instances qui prennent en charge la spécification CPU d'options.

Table des matières

instances à usage général

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
`m2.xlarge`	2	2	1	1, 2	1
`m2.2xlarge`	4	4	1	1, 2, 3, 4	1
`m2.4xlarge`	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
`m3.large`	2	1	2	1	1, 2
`m3.xlarge`	4	2	2	1, 2	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.large	2	1	2	1	1, 2
m4.xlarge	4	2	2	1, 2	1, 2
m4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m4.10xlarge	40	20	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20	1, 2
m4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5.large	2	1	2	1	1, 2
m5.xlarge	4	2	2	2	1, 2
m5.2xlarge	8	4	2	2, 4	1, 2
m5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5a.large	2	1	2	1	1, 2
m5a.xlarge	4	2	2	2	1, 2
m5a.2xlarge	8	4	2	2, 4	1, 2
m5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5ad.large	2	1	2	1	1, 2
m5ad.xlarge	4	2	2	2	1, 2
m5ad.2xlarge	8	4	2	2, 4	1, 2
m5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
m5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5d.large	2	1	2	1	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m5d.xlarge	4	2	2	2	1, 2
m5d.2xlarge	8	4	2	2, 4	1, 2
m5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5dn.large	2	1	2	1	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m5dn.xlarge	4	2	2	1, 2	1, 2
m5dn.2xlarge	8	4	2	2, 4	1, 2
m5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5n.large	2	1	2	1	1, 2
m5n.xlarge	4	2	2	1, 2	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m5n.2xlarge	8	4	2	2, 4	1, 2
m5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5zn.large	2	1	2	1	1, 2
m5zn.xlarge	4	2	2	1, 2	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m5zn.2xlarge	8	4	2	2, 4	1, 2
m5zn.3xlarge	12	6	2	2, 4, 6	1, 2
m5zn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
m5zn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6a.large	2	1	2	1	1, 2
m6a.xlarge	4	2	2	1, 2	1, 2
m6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
m6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
m6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
m6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
m6g.large	2	2	1	1, 2	1
m6g.xlarge	4	4	1	1, 2, 3, 4	1
m6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6gd.large	2	2	1	1, 2	1
m6gd.xlarge	4	4	1	1, 2, 3, 4	1
m6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6i.large	2	1	2	1	1, 2
m6i.xlarge	4	2	2	1, 2	1, 2
m6i.2xlarge	8	4	2	2, 4	1, 2
m6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6id.large	2	1	2	1	1, 2
m6id.xlarge	4	2	2	1, 2	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m6id.2xlarge	8	4	2	2, 4	1, 2
m6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6idn.large	2	1	2	1	1, 2
m6idn.xlarge	4	2	2	1, 2	1, 2
m6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m6idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6in.large	2	1	2	1	1, 2
m6in.xlarge	4	2	2	1, 2	1, 2
m6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m7a.large	2	2	1	1, 2	1
m7a.xlarge	4	4	1	1, 2, 3, 4	1
m7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
m7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
m7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
m7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
m7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
m7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
m7g.large	2	2	1	1, 2	1
m7g.xlarge	4	4	1	1, 2, 3, 4	1
m7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7gd.large	2	2	1	1, 2	1
m7gd.xlarge	4	4	1	1, 2, 3, 4	1
m7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7i.large	2	1	2	1	1, 2
m7i.xlarge	4	2	2	1, 2	1, 2
m7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
m7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
m7i-flex.large	2	1	2	1	1, 2
m7i-flex.xlarge	4	2	2	1, 2	1, 2
m7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
t3.nano	2	1	2	1	1, 2
t3.micro	2	1	2	1	1, 2
t3.small	2	1	2	1	1, 2
t3.medium	2	1	2	1	1, 2
t3.large	2	1	2	1	1, 2
t3.xlarge	4	2	2	2	1, 2
t3.2xlarge	8	4	2	2, 4	1, 2
t3a.nano	2	1	2	1	1, 2
t3a.micro	2	1	2	1	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
t3a.small	2	1	2	1	1, 2
t3a.medium	2	1	2	1	1, 2
t3a.large	2	1	2	1	1, 2
t3a.xlarge	4	2	2	2	1, 2
t3a.2xlarge	8	4	2	2, 4	1, 2
t4g.nano	2	2	1	1, 2	1
t4g.micro	2	2	1	1, 2	1
t4g.small	2	2	1	1, 2	1
t4g.medium	2	2	1	1, 2	1
t4g.large	2	2	1	1, 2	1
t4g.xlarge	4	4	1	1, 2, 3, 4	1
t4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

instances de calcul optimisé

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c3.large	2	1	2	1	1, 2
c3.xlarge	4	2	2	1, 2	1, 2
c3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c4.large	2	1	2	1	1, 2
c4.xlarge	4	2	2	1, 2	1, 2
c4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c4.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.large	2	1	2	1	1, 2
c5.xlarge	4	2	2	2	1, 2
c5.2xlarge	8	4	2	2, 4	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c5.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5a.large	2	1	2	1	1, 2
c5a.xlarge	4	2	2	1, 2	1, 2
c5a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5a.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c5a.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5a.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2
c5a.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5a.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5ad.large	2	1	2	1	1, 2
c5ad.xlarge	4	2	2	1, 2	1, 2
c5ad.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5ad.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2
c5ad.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5ad.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c5ad.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5ad.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5d.large	2	1	2	1	1, 2
c5d.xlarge	4	2	2	2	1, 2
c5d.2xlarge	8	4	2	2, 4	1, 2
c5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5d.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5d.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c5d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5n.large	2	1	2	1	1, 2
c5n.xlarge	4	2	2	2	1, 2
c5n.2xlarge	8	4	2	2, 4	1, 2
c5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5n.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5n.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c6a.large	2	1	2	1	1, 2
c6a.xlarge	4	2	2	1, 2	1, 2
c6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
c6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
c6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
c6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
c6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
c6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
c6g.large	2	2	1	1, 2	1
c6g.xlarge	4	4	1	1, 2, 3, 4	1
c6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gd.large	2	2	1	1, 2	1
c6gd.xlarge	4	4	1	1, 2, 3, 4	1
c6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gn.medium	1	1	1	1	1
c6gn.large	2	2	1	1, 2	1
c6gn.xlarge	4	4	1	1, 2, 3, 4	1
c6gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c6gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c6gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6i.large	2	1	2	1	1, 2
c6i.xlarge	4	2	2	1, 2	1, 2
c6i.2xlarge	8	4	2	2, 4	1, 2
c6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6id.large	2	1	2	1	1, 2
c6id.xlarge	4	2	2	1, 2	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c6id.2xlarge	8	4	2	2, 4	1, 2
c6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6in.large	2	1	2	1	1, 2
c6in.xlarge	4	2	2	1, 2	1, 2
c6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c7a.large	2	2	1	1, 2	1
c7a.xlarge	4	4	1	1, 2, 3, 4	1
c7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
c7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
c7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
c7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
c7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
c7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
c7g.large	2	2	1	1, 2	1
c7g.xlarge	4	4	1	1, 2, 3, 4	1
c7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gd.large	2	2	1	1, 2	1
c7gd.xlarge	4	4	1	1, 2, 3, 4	1
c7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gn.large	2	2	1	1, 2	1
c7gn.xlarge	4	4	1	1, 2, 3, 4	1
c7gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c7gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c7gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7i.large	2	1	2	1	1, 2
c7i.xlarge	4	2	2	1, 2	1, 2
c7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
c7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
c7i-flex.large	2	1	2	1	1, 2
c7i-flex.xlarge	4	2	2	1, 2	1, 2
c7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

instances de mémoire optimisée

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r3.large	2	1	2	1	1, 2
r3.xlarge	4	2	2	1, 2	1, 2
r3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r4.large	2	1	2	1	1, 2
r4.xlarge	4	2	2	1, 2	1, 2
r4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r4.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.large	2	1	2	1	1, 2
r5.xlarge	4	2	2	2	1, 2
r5.2xlarge	8	4	2	2, 4	1, 2
r5.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5a.large	2	1	2	1	1, 2
r5a.xlarge	4	2	2	2	1, 2
r5a.2xlarge	8	4	2	2, 4	1, 2
r5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5ad.large	2	1	2	1	1, 2
r5ad.xlarge	4	2	2	2	1, 2
r5ad.2xlarge	8	4	2	2, 4	1, 2
r5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5b.large	2	1	2	1	1, 2
r5b.xlarge	4	2	2	1, 2	1, 2
r5b.2xlarge	8	4	2	2, 4	1, 2
r5b.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5b.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5b.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5b.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5b.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r5d.large	2	1	2	1	1, 2
r5d.xlarge	4	2	2	2	1, 2
r5d.2xlarge	8	4	2	2, 4	1, 2
r5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5dn.large	2	1	2	1	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r5dn.xlarge	4	2	2	1, 2	1, 2
r5dn.2xlarge	8	4	2	2, 4	1, 2
r5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5n.large	2	1	2	1	1, 2
r5n.xlarge	4	2	2	1, 2	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r5n.2xlarge	8	4	2	2, 4	1, 2
r5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6a.large	2	1	2	1	1, 2
r6a.xlarge	4	2	2	1, 2	1, 2
r6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
r6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
r6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
r6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
r6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
r6g.large	2	2	1	1, 2	1
r6g.xlarge	4	4	1	1, 2, 3, 4	1
r6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6gd.large	2	2	1	1, 2	1
r6gd.xlarge	4	4	1	1, 2, 3, 4	1
r6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6i.large	2	1	2	1	1, 2
r6i.xlarge	4	2	2	1, 2	1, 2
r6i.2xlarge	8	4	2	2, 4	1, 2
r6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6idn.large	2	1	2	1	1, 2
r6idn.xlarge	4	2	2	1, 2	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r6idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r6idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6in.large	2	1	2	1	1, 2
r6in.xlarge	4	2	2	1, 2	1, 2
r6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6id.large	2	1	2	1	1, 2
r6id.xlarge	4	2	2	1, 2	1, 2
r6id.2xlarge	8	4	2	2, 4	1, 2
r6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r7a.large	2	2	1	1, 2	1
r7a.xlarge	4	4	1	1, 2, 3, 4	1
r7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
r7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
r7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
r7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
r7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
r7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
r7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r7g.large	2	2	1	1, 2	1
r7g.xlarge	4	4	1	1, 2, 3, 4	1
r7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7gd.large	2	2	1	1, 2	1
r7gd.xlarge	4	4	1	1, 2, 3, 4	1
r7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7i.large	2	1	2	1	1, 2
r7i.xlarge	4	2	2	1, 2	1, 2
r7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
r7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r7iz.large	2	1	2	1	1, 2
r7iz.xlarge	4	2	2	1, 2	1, 2
r7iz.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7iz.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r7iz.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7iz.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7iz.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r7iz.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r8g.large	2	2	1	1, 2	1
r8g.xlarge	4	4	1	1, 2, 3, 4	1
r8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
r8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96,, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164, 166,	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
				168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
u-3tb1.56xlarge	224	112	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112	1, 2
u-6tb1.56xlarge	224	224	1	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
u-6tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-9tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
u-12tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-18tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
u-24tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
u7i-12tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
u7in-16tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
u7in-24tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
u7in-32tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2
x1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
x1.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
x2gd.large	2	2	1	1, 2	1
x2gd.xlarge	4	4	1	1, 2, 3, 4	1
x2gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
x2gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
x2gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
x2gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
x2gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
x2idn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
x2idn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2idn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iedn.xlarge	4	2	2	1, 2	1, 2
x2iedn.2xlarge	8	4	2	2, 4	1, 2
x2iedn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iedn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
x2iedn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x2iedn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2iedn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iezn.2xlarge	8	4	2	2, 4	1, 2
x2iezn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iezn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
x2iezn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
x2iezn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
x1e.xlarge	4	2	2	1, 2	1, 2
x1e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
x1e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
x1e.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
x1e.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x1e.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
z1d.large	2	1	2	1	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
z1d.xlarge	4	2	2	1, 2	1, 2
z1d.2xlarge	8	4	2	2, 4	1, 2
z1d.3xlarge	12	6	2	2, 4, 6	1, 2
z1d.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
z1d.12xlarge	48	24	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

instances de stockage optimisé

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
d2.xlarge	4	2	2	1, 2	1, 2
d2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
d2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
d2.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
d3.xlarge	4	2	2	1, 2	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
d3.2xlarge	8	4	2	2, 4	1, 2
d3.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.xlarge	4	2	2	1, 2	1, 2
d3en.2xlarge	8	4	2	2, 4	1, 2
d3en.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
d3en.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
h1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
h1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
h1.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
h1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i2.xlarge	4	2	2	1, 2	1, 2
i2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i2.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
i3.large	2	1	2	1	1, 2
i3.xlarge	4	2	2	1, 2	1, 2
i3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
i3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i3en.large	2	1	2	1	1, 2
i3en.xlarge	4	2	2	1, 2	1, 2
i3en.2xlarge	8	4	2	2, 4	1, 2
i3en.3xlarge	12	6	2	2, 4, 6	1, 2
i3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
i3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
i3en.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
i4g.large	2	2	1	1, 2	1
i4g.xlarge	4	4	1	1, 2, 3, 4	1
i4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
i4g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
i4g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
i4g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
i4i.large	2	1	2	1	1, 2
i4i.xlarge	4	2	2	1, 2	1, 2
i4i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i4i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
i4i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i4i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
i4i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i4i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
i4i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
im4gn.large	2	2	1	1, 2	1
im4gn.xlarge	4	4	1	1, 2, 3, 4	1
im4gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
im4gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
im4gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
im4gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
is4gen.medium	1	1	1	1	1
is4gen.large	2	2	1	1, 2	1
is4gen.xlarge	4	4	1	1, 2, 3, 4	1
is4gen.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
is4gen.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
is4gen.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

instances à calcul accéléré

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
dl1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
dl2q.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28,	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
				30, 32, 34, 36, 38, 40, 42, 44, 46, 48	
f1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
f1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
f1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
g3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g4ad.xlarge	4	2	2	2	1, 2
g4ad.2xlarge	8	4	2	2, 4	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
g4ad.4xlarge	16	8	2	2, 4, 8	1, 2
g4ad.8xlarge	32	16	2	2, 4, 8, 16	1, 2
g4ad.16xlarge	64	32	2	2, 4, 8, 16, 32	1, 2
g4dn.xlarge	4	2	2	2	1, 2
g4dn.2xlarge	8	4	2	2, 4	1, 2
g4dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
g4dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
g4dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
g4dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g5g.xlarge	4	4	1	1, 2, 3, 4	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
g5g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
g5g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
g5g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
g5g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
g6.xlarge	4	2	2	1, 2	1, 2
g6.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
g6.12xlarge	48	24	2	1, 2, 3, 6, 9, 12, 15, 18, 21, 24	1, 2
g6.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
g6.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1, 2
g6.48xlarge	192	96	2	4, 6, 8, 10, 12, 24, 36, 48, 60, 72, 84, 96	1, 2
g6e.xlarge	4	2	2	1, 2	1, 2
g6e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g6e.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
g6e.12xlarge	48	24	2	3, 6, 9, 12, 15, 18, 21, 24	1, 2
g6e.16xlarge	64	32	2	4, 8, 12, 16, 20, 24, 28, 32	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
g6e.24xlarge	96	48	2	6, 12, 18, 24, 30, 36, 42, 48	1, 2
g6e.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2
gr6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
gr6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2
inf1.xlarge	4	2	2	2	1, 2
inf1.2xlarge	8	4	2	2, 4	1, 2
inf1.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
inf1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
inf2.xlarge	4	2	2	1, 2	1, 2
inf2.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
inf2.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
inf2.48xlarge	192	96	2	4, 8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
p2.xlarge	4	2	2	1, 2	1, 2
p2.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
p2.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
p3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
p3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
p3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
p3dn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p4d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p4de.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p5.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2
trn1.2xlarge	8	4	2	2, 4	1, 2

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
trn1.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
trn1n.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
vt1.3xlarge	12	6	2	6	1, 2
vt1.6xlarge	24	12	2	6, 12	1, 2
vt1.24xlarge	96	48	2	6, 12, 48	1, 2

Instances de calcul hautes performances

Type d'instance	Par défaut vCPUs	CPUNoyaux par défaut	Threads par défaut par cœur	CPUNoyaux valides	Threads valides par cœur
`hpc6id.32xlarge`	64	64	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1

Spécifier CPU les options pour une EC2 instance Amazon

Vous pouvez spécifier des CPU options lors du lancement de l'instance.

Les exemples suivants décrivent comment spécifier les CPU options lors de l'utilisation de l'assistant de lancement d'instance dans la EC2 console et de la AWS CLI commande run-instances, ainsi que de la page de création d'un modèle de lancement dans la EC2 console et de la create-launch-template AWS CLI commande. Pour EC2 Fleet ou Spot Fleet, vous devez spécifier les CPU options dans un modèle de lancement.

Les exemples suivants concernent un type d'instance `r5.4xlarge`, qui possède les valeurs par défaut suivantes :

- Nombre de CPU cœurs par défaut : 8
- Threads par défaut par cœur : 2
- Par défaut vCPUs : 16 (8 * 2)
- Nombre de CPU cœurs valide : 2, 4, 6, 8
- Nombre valide de threads par cœur : 1, 2

Désactiver le multithreading simultané

Pour désactiver le multithreading (SMT) simultané, également appelé hyper-threading, spécifiez 1 thread par cœur.

Console

Pour désactiver SMT lors du lancement de l'instance

1. Suivez la procédure Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console et configurez votre instance selon vos besoins.
2. Développez les détails avancés et cochez la case Spécifier les CPU options.
3. Pour Nombre de cœurs, choisissez le nombre de CPU cœurs requis. Dans cet exemple, pour spécifier le nombre de CPU cœurs par défaut pour une `r5.4xlarge` instance, choisissez8.
4. Pour désactiverSMT, pour Threads par cœur, choisissez 1.
5. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance). Pour de plus amples informations, veuillez consulter Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console.

AWS CLI

Pour désactiver SMT lors du lancement de l'instance

Utilisez la commande run-instances de l' AWS CLI et spécifiez la valeur 1 pour `ThreadsPerCore` pour le paramètre `--cpu-options`. Pour`CoreCount`, spécifiez le nombre de CPU cœurs. Dans cet exemple, pour spécifier le nombre de CPU cœurs par défaut pour une `r5.4xlarge` instance, spécifiez une valeur de8.

```
aws ec2 run-instances \
    --image-id ami-1a2b3c4d \
    --instance-type r5.4xlarge \
    --cpu-options "CoreCount=8,ThreadsPerCore=1" \
    --key-name MyKeyPair
```

Spécifiez un nombre personnalisé de vCPUs au lancement

Vous pouvez personnaliser le nombre de CPU cœurs et de threads par cœur pour l'instance.

L'exemple suivant lance une `r5.4xlarge` instance avec 4vCPUs.

Console

Pour spécifier un nombre personnalisé de vCPUs lors du lancement de l'instance

1. Suivez la procédure Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console et configurez votre instance selon vos besoins.
2. Développez les détails avancés et cochez la case Spécifier les CPU options.
3. Pour obtenir 4vCPUs, spécifiez 2 CPU cœurs et 2 threads par cœur, comme suit :
   - Pour Nombre de cœurs, choisissez 2.
   - Sous Threads per core (Threads par cœur), choisissez 2.
4. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance). Pour de plus amples informations, veuillez consulter Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console.

AWS CLI

Pour spécifier un nombre personnalisé de vCPUs lors du lancement de l'instance

Utilisez la AWS CLI commande run-instances et spécifiez le nombre de CPU cœurs et le nombre de threads dans le `--cpu-options` paramètre. Vous pouvez spécifier 2 CPU cœurs et 2 threads par cœur pour obtenir 4vCPUs.

```
aws ec2 run-instances \
    --image-id ami-1a2b3c4d \
    --instance-type r5.4xlarge \
    --cpu-options "CoreCount=2,ThreadsPerCore=2" \
    --key-name MyKeyPair
```

Vous pouvez également spécifier 4 CPU cœurs et 1 thread par cœur (désactiverSMT) pour obtenir 4 vCPUs :

```
aws ec2 run-instances \
    --image-id ami-1a2b3c4d \
    --instance-type r5.4xlarge \
```

```
    --cpu-options "CoreCount=4,ThreadsPerCore=1" \
    --key-name MyKeyPair
```

Spécifiez un numéro personnalisé de vCPUs dans un modèle de lancement

Vous pouvez personnaliser le nombre de CPU cœurs et de threads par cœur pour l'instance dans un modèle de lancement.

L'exemple suivant crée un modèle de lancement qui spécifie la configuration d'une `r5.4xlarge` instance avec 4vCPUs.

Console

Pour spécifier un nombre personnalisé de vCPUs dans un modèle de lancement

1. Suivez la procédure Création d'un modèle de lancement en spécifiant des paramètres et configurez votre modèle de lancement selon vos besoins.
2. Développez les détails avancés et cochez la case Spécifier les CPU options.
3. Pour obtenir 4vCPUs, spécifiez 2 CPU cœurs et 2 threads par cœur, comme suit :
   - Pour Nombre de cœurs, choisissez 2.
   - Sous Threads per core (Threads par cœur), choisissez 2.
4. Dans le panneau Résumé, vérifiez la configuration de votre instance, puis choisissez Créer un modèle de lancement. Pour de plus amples informations, veuillez consulter Stockez les paramètres de lancement de l'instance dans les modèles de EC2 lancement Amazon.

AWS CLI

Pour spécifier un nombre personnalisé de vCPUs dans un modèle de lancement

Utilisez la create-launch-template AWS CLI commande et spécifiez le nombre de CPU cœurs et le nombre de threads dans le `CpuOptions` paramètre. Vous pouvez spécifier 2 CPU cœurs et 2 threads par cœur pour obtenir 4vCPUs.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForCPUOptions \
    --version-description CPUOptionsVersion1 \
    --launch-template-data file://template-data.json
```

Voici un exemple de JSON fichier qui contient les données du modèle de lancement, y compris les CPU options, pour la configuration de l'instance dans cet exemple.

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-7b16de0c"
    }],
    "ImageId": "ami-8c1be5f6",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":2,
        "ThreadsPerCore":2
    }
}
```

Vous pouvez également spécifier 4 CPU cœurs et 1 thread par cœur (désactiverSMT) pour obtenir 4 vCPUs :

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-7b16de0c"
    }],
    "ImageId": "ami-8c1be5f6",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
```

```
    }],
    "CpuOptions": {
        "CoreCount":4,
        "ThreadsPerCore":1
    }
}
```

Afficher CPU les threads et les cœurs d'une EC2 instance Amazon

Vous pouvez consulter les CPU options d'une instance existante dans la EC2 console Amazon ou en décrivant l'instance à l'aide du AWS CLI.

Console

Pour afficher les CPU options d'une instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation sur la gauche, choisissez Instances, puis sélectionnez l'instance.
3. Dans l'onglet Détails, sous Hôte et groupe de placement, recherchez Nombre de vCPUs.

AWS CLI

Pour afficher les CPU options d'une instance (AWS CLI)

Utilisez la commande describe-instances.

```
aws ec2 describe-instances --instance-ids i-123456789abcde123
```

```
...
    "Instances": [
        {
            "Monitoring": {
                "State": "disabled"
            },
            "PublicDnsName": "ec2-198-51-100-5.eu-central-1.compute.amazonaws.com",
            "State": {
                "Code": 16,
                "Name": "running"
```

```
            },
            "EbsOptimized": false,
            "LaunchTime": "2018-05-08T13:40:33.000Z",
            "PublicIpAddress": "198.51.100.5",
            "PrivateIpAddress": "172.31.2.206",
            "ProductCodes": [],
            "VpcId": "vpc-1a2b3c4d",
            "CpuOptions": {
                "CoreCount": 34,
                "ThreadsPerCore": 1
            },
            "StateTransitionReason": "",
            ...
        }
    ]
...
```

Dans le résultat retourné, le champ `CoreCount` indique le nombre de cœurs pour l'instance. Le champ `ThreadsPerCore` indique le nombre de threads par cœur.

Pour consulter les CPU informations, vous pouvez également vous connecter à votre instance et utiliser l'un des outils système suivants :

- Windows `Task Manager` sur votre instance Windows
- La lscpu commande sur votre instance Linux

Vous pouvez l'utiliser AWS Config pour enregistrer, évaluer, auditer et évaluer les modifications de configuration des instances, y compris les instances résiliées. Pour plus d'informations, consultez Mise en route avec AWS Config dans le AWS Config Guide du développeur.

AMDSEV- SNP pour les EC2 instances Amazon

AMDVirtualisation cryptée sécurisée-pagination imbriquée sécurisée (AMDSEV-SNP) est une CPU fonctionnalité qui fournit les propriétés suivantes :

- Attestation — AMD SEV - vous SNP permet de récupérer un rapport d'attestation signé contenant une mesure cryptographique qui peut être utilisée pour valider l'état et l'identité de l'instance, et pour confirmer qu'elle s'exécute sur du AMD matériel authentique. Pour plus d'informations, consultez Tester une EC2 instance Amazon avec - AMD SEV SNP.

- Chiffrement de la mémoire : à partir des processeurs AMD EPYC (Milan), AWS Graviton2 et Intel Xeon Scalable (Ice Lake), la mémoire de l'instance est toujours chiffrée. Instances activées pour AMD SEV : SNP utilisent une clé spécifique à l'instance pour le chiffrement de leur mémoire.

Rubriques

Concepts et terminologie

Avant de commencer à utiliser AMD SEV -SNP, assurez-vous de connaître les concepts et la terminologie suivants.

AMDSEV- rapport SNP d'attestation

Le AMD SEV rapport SNP d'attestation est un document qu'une instance peut demander auCPU. Le AMD SEV rapport SNP d'attestation peut être utilisé pour valider l'état et l'identité d'une instance et pour vérifier qu'elle s'exécute dans un AMD environnement sanctionné. Le rapport inclut une mesure de lancement, qui est un hachage cryptographique de l'état de démarrage initial d'une instance, y compris le contenu de la mémoire initiale de l'instance et l'état initial du. vCPUs Le AMD SEV rapport SNP d'attestation est signé avec une VLEK signature qui remonte à une AMD source de confiance.

VLEK

La clé d'approbation chargée versionnée (VLEK) est une clé de signature versionnée qui est certifiée AMD et utilisée par le AMD CPU pour signer les AMD SEV rapports SNP d'attestation. VLEKles signatures peuvent être validées à l'aide des certificats fournis parAMD.

OVMFbinaire

Le microprogramme Open Virtual Machine (OVMF) est le code de démarrage anticipé utilisé pour fournir un UEFI environnement à l'instance. Le code de démarrage anticipé est exécuté avant le

démarrage du code contenu dans AMI le. OVMFIl trouve et exécute également le chargeur de démarrage fourni dans leAMI. Pour plus d'informations, consultez le OVMFréférentiel.

Prérequis

Pour utiliser AMD SEV -SNP, vous devez effectuer les opérations suivantes :

- Utilisez l'un des types d'instance pris en charge suivants :
  - Usage général : `m6a.large` | `m6a.xlarge` | `m6a.2xlarge` | `m6a.4xlarge` | `m6a.8xlarge`
  - Optimisées pour le calcul : `c6a.large` | `c6a.xlarge` | `c6a.2xlarge` | `c6a.4xlarge` | `c6a.8xlarge` | `c6a.12xlarge` | `c6a.16xlarge`
  - Mémoire optimisée : `r6a.large` | `r6a.xlarge` | `r6a.2xlarge` | `r6a.4xlarge`
- Lancez votre instance dans un environnement compatible Région AWS. À l'heure actuelle, seules les régions USA Est (Ohio) et Europe (Irlande) sont prises en charge.
- Utilisez un mode AMI avec `uefi` ou de `uefi-preferred` démarrage et un système d'exploitation compatible avec AMD SEV -SNP. Pour plus d'informations sur AMD SEV le SNP support de votre système d'exploitation, reportez-vous à la documentation du système d'exploitation correspondant. Car AWS, AMD SEV - SNP est pris en charge sur les AL2 versions 023, RHEL 9.3SP4, SLES 15 et Ubuntu 23.04 et versions ultérieures.

Considérations

Vous ne pouvez l'activer AMD SEV que SNP lorsque vous lancez une instance. Lorsque AMD SEV - SNP est activé pour le lancement de votre instance, les règles suivantes s'appliquent.

- Une fois activé, AMD SEV - ne SNP peut pas être désactivé. Il reste activé tout au long du cycle de vie de l'instance.
- Vous pouvez uniquement remplacer le type d'instance par un autre type d'instance prenant en charge AMD SEV -SNP.
- Hibernation et Nitro Enclaves ne sont pas pris en charge.
- Les hôtes dédiés ne sont pas pris en charge.
- Si la maintenance de l'hôte sous-jacent de votre instance est planifiée, vous recevrez une notification d'événement planifié 14 jours avant l'événement. Vous devez arrêter ou redémarrer manuellement votre instance pour la déplacer vers un nouvel hôte.

Tarification

Lorsque vous lancez une EC2 instance Amazon avec l'SNPoption AMD SEV - activée, des frais d'utilisation supplémentaires vous sont facturés, équivalant à 10 % du taux horaire à la demande du type d'instance sélectionné.

Ces AMD SEV frais SNP d'utilisation sont facturés séparément de l'utilisation de votre EC2 instance Amazon. Les instances réservées, les Savings Plans et l'utilisation du système d'exploitation n'ont aucune incidence sur ces frais.

Si vous configurez une instance Spot pour qu'elle soit lancée avec l'SNPoption AMDSEV- activé, des frais d'utilisation supplémentaires vous sont facturés, équivalant à 10 % du taux horaire à la demande du type d'instance sélectionné. Si la stratégie d'allocation utilise le prix comme entrée, le parc d'instances Spot n'inclut pas ces frais supplémentaires ; seul le prix au comptant est utilisé.

Vérifier AMD SEV : SNP assistance sur les EC2 instances Amazon

Rubriques

- Trouvez les types d'EC2instances Amazon compatibles avec AMD SEV - SNP
- Vérifiez si une EC2 instance Amazon est activée pour AMD SEV - SNP

Trouvez les types d'EC2instances Amazon compatibles avec AMD SEV - SNP

Vous pouvez utiliser le AWS CLI pour rechercher les types d'instances compatibles avec AMD SEV - SNP.

Pour trouver les types d'instances compatibles AMD SEV SNP avec le AWS CLI, utilisez la describe-instance-typescommande suivante.

```
$ aws ec2 describe-instance-types \
--filters Name=processor-info.supported-features,Values=amd-sev-snp \
--query 'InstanceTypes[*].InstanceType'
```

Exemple de sortie.

```
[
 "r6a.2xlarge",
 "m6a.large",
 "m6a.2xlarge",
 "r6a.xlarge",
```

```
 "c6a.16xlarge",
 "c6a.8xlarge",
 "m6a.4xlarge",
 "c6a.12xlarge",
 "r6a.4xlarge",
 "c6a.xlarge",
...
]
```

Vérifiez si une EC2 instance Amazon est activée pour AMD SEV - SNP

Vous pouvez utiliser l'une des méthodes suivantes pour vérifier le statut de AMD SEV -SNP.

AWS CLI

Pour vérifier si AMD SEV - SNP est activé pour une instance utilisant le AWS CLI, utilisez la describe-instancescommande. Pour `--instance-ids`, spécifiez l'ID de l'instance à vérifier.

```
$ aws ec2 describe-instances --instance-ids instance_id
```

Dans la sortie de commande, la valeur de `AmdSevSnp` in `CpuOptions` indique si AMD SEV - SNP est activé ou désactivé.

AWS CloudTrail

Dans le AWS CloudTrail cas d'une demande de lancement d'instance, une valeur de `"cpuOptions": {"AmdSevSnp": enabled}` indique que AMD SEV - SNP est activé pour l'instance.

Tester une EC2 instance Amazon avec - AMD SEV SNP

L'attestation est un processus qui permet à votre instance de prouver son état et son identité. Lorsque vous activez AMDSEV, SNP pour votre instance, vous pouvez demander un AMD SEV rapport SNP d'attestation au processeur sous-jacent. Le AMD SEV rapport SNP d'attestation contient un hachage cryptographique, appelé mesure de lancement, du contenu initial de la mémoire de l'invité et de l'état initial v. CPU Le rapport d'attestation est signé avec une VLEK signature qui remonte à une AMD source de confiance. Vous pouvez utiliser la mesure de lancement incluse dans le rapport d'attestation pour vérifier que l'instance s'exécute dans un AMD environnement authentique et pour valider le code de démarrage initial utilisé pour lancer l'instance.

Pour effectuer une attestation avec AMD SEV -SNP, procédez comme suit.

Rubriques

Étape 1 : Activer AMDSEV, SNP lors du lancement de l'instance

Vous pouvez utiliser le AWS CLI pour lancer une instance avec AMD SEV - SNP activé.

Pour lancer une instance avec AMD SEV - SNP activé, vous devez utiliser le AWS CLI. Utilisez la run-instancescommande et incluez l'`--cpu-options AmdSevSnp=enabled`option. Pour`--image-id`, spécifiez un mode de `uefi-prefered` démarrage AMI avec `uefi` ou et un système d'exploitation compatible avec AMD SEV -SNP. Pour `--instance-type`, spécifiez un type d'instance pris en charge.

```
$ aws ec2 run-instances \
--image-id supported_ami_id \
--instance-type supported_instance_type \
--key-name key_pair_name \
--subnet-id subnet_id \
--cpu-options AmdSevSnp=enabled
```

Étape 2 : Obtenir le rapport d'attestation

Au cours de cette étape, vous installez et compilez l'`snpguest`utilitaire, puis vous l'utilisez pour demander le AMD SEV rapport SNP d'attestation et les certificats.

1. Exécutez les commandes suivantes pour créer l'`snpguest`utilitaire à partir du snpguest repository.

   ```
   $ git clone https://github.com/virtee/snpguest.git
   $ cd snpguest
   $ cargo build -r
   $ cd target/release
   ```

2. Générez une demande pour le rapport d'attestation. L'utilitaire demande le rapport d'attestation à l'hôte et l'écrit dans un fichier binaire avec les données de demande fournies.

   L'exemple suivant crée une chaîne de requête aléatoire et l'utilise comme fichier de demande (`request-file.txt`). Lorsque la commande renvoie le rapport d'attestation, celui-ci est stocké

dans le chemin de fichier que vous spécifiez (`report.bin`). Dans ce cas, l'utilitaire enregistre le rapport dans le répertoire en cours.

```
$ ./snpguest report report.bin request-file.txt --random
```

3. Demandez les certificats à la mémoire de l'hôte et stockez-les sous forme de PEM fichiers. L'exemple suivant enregistre les fichiers dans le même répertoire que l'`snpguest`utilitaire. Si des certificats existent déjà dans le répertoire spécifié, ils sont remplacés.

```
$ ./snpguest certificates PEM ./
```

Étape 3 : Valider la signature du rapport d'attestation

Le rapport d'attestation est signé avec un certificat, appelé clé d'approbation chargée versionnée (VLEK), qui est émis par AMD for AWS. Au cours de cette étape, vous pouvez vérifier que le VLEK certificat est émis par AMD ce certificat et que le rapport d'attestation est signé par ce VLEK certificat.

1. Téléchargez la VLEK racine des certificats de confiance depuis le AMD site officiel vers le répertoire actuel.

```
$ sudo curl --proto '=https' --tlsv1.2 -sSf https://kdsintf.amd.com/vlek/v1/Milan/
cert_chain -o ./cert_chain.pem
```

2. `openssl`À utiliser pour vérifier que le VLEK certificat est signé par la AMD racine des certificats de confiance.

```
$ sudo openssl verify --CAfile ./cert_chain.pem vlek.pem
```

Sortie attendue :

```
certs/vcek.pem: OK
```

3. Utilisez l'`snpguest`utilitaire pour vérifier que le rapport d'attestation est signé par le VLEK certificat.

```
$ ./snpguest verify attestation ./ report.bin
```

Sortie attendue.

```
Reported TCB Boot Loader from certificate matches the attestation report.
Reported TCB TEE from certificate matches the attestation report.
Reported TCB SNP from certificate matches the attestation report.
Reported TCB Microcode from certificate matches the attestation report.
VEK signed the Attestation Report!
```

Contrôle de l'état du processeur pour les instances Amazon EC2 Linux

Les états C contrôlent les niveaux de sommeil dans lesquels un cœur peut entrer lorsqu'il est inactif. Les états « C-state » sont numérotés de C0 (l'état le plus superficiel lorsque le cœur est totalement éveillé et exécute les instructions) à C6 (l'état de veille le plus profond lorsqu'un cœur est arrêté).

Les états P contrôlent les performances souhaitées (en CPU fréquence) à partir d'un noyau. La numérotation des états « P-states » commence à P0 (paramètre de performance le plus élevé dans lequel le cœur peut utiliser la technologie Intel Turbo Boost pour améliorer la fréquence si possible) et va de P1 (état « P-state » qui demande la fréquence de base maximale) à P15 (fréquence la plus basse possible).

> **Note**
>
> AWS Les processeurs Graviton sont dotés de modes d'économie d'énergie intégrés et fonctionnent à une fréquence fixe. Par conséquent, ils ne permettent pas au système d'exploitation de contrôler les états « C-state » et les états « P-state ».

États C-state et P-state

Les types d'instance EC2 suivants permettent à un système d'exploitation de contrôler les états « C-state » et « P-state » des processeurs.

- Usage général : `m4.10xlarge` | `m4.16xlarge`
- Optimisé pour le calcul : `c4.8xlarge`
- Mémoire optimisée : `r4.8xlarge` | `r4.16xlarge` | `x1.16xlarge` | `x1.32xlarge` | `x1e.8xlarge` | `x1e.16xlarge` | `x1e.32xlarge`
- Stockage optimisé : `d2.8xlarge` | `i3.8xlarge` | `i3.16xlarge` | `i3en.24xlarge` | `h1.8xlarge` | `h1.16xlarge`

- Calcul accéléré : f1.16xlarge | g3.16xlarge | | p2.16xlarge | p3.16xlarge
- Bare metal : toutes les instances bare metal avec Intel et AMD processeurs

États C-state uniquement

Les types d'instance suivants permettent à un système d'exploitation de contrôler les états « C-state » des processeurs :

- Usage général : m5.12xlarge m5.24xlarge m5d.12xlarge | m5d.24xlarge | m5n.12xlarge | m5n.24xlarge | m5dn.12xlarge | m5dn.24xlarge | m5zn.6xlarge | m5zn.12xlarge | m6a.24xlarge m6a.48xlarge | m6i.16xlarge | m6i.32xlarge | m6id.16xlarge | m6id.32xlarge | m6idn.16xlarge | m6in.16xlarge | m6in.32xlarge | m7a.medium | m7a.large m7a.xlarge | m7a.2xlarge | m7a.4xlarge | m7a.8xlarge | m7a.12xlarge | m7a.16xlarge | m7a.24xlarge | m7a.32xlarge | m7a.48xlarge | m7i.large m7i.xlarge | m7i.2xlarge | m7i.4xlarge | m7i.8xlarge | m7i.12xlarge | m7i.16xlarge| m7i.24xlarge | m7i.48xlarge
- Optimisé pour le calcul : c5.9xlarge c5.12xlarge c5.18xlarge c5.24xlarge | c5a.24xlarge | c5ad.24xlarge | c5d.9xlarge | c5d.12xlarge | c5d.18xlarge | c5d.24xlarge | c5n.9xlarge | c5n.18xlarge | c6a.24xlarge | c6a.32xlarge | c6a.48xlarge | c6i.16xlarge | c6i.32xlarge | c6id.24xlarge | c6id.32xlarge | c6in.32xlarge | c7a.medium | c7a.large | c7a.xlarge | c7a.2xlarge | c7a.4xlarge | c7a.8xlarge | c7a.12xlarge | c7a.16xlarge | c7a.24xlarge | c7a.32xlarge | c7a.48xlarge | c7i.large | c7i.xlarge | c7i.2xlarge | c7i.4xlarge | c7i.8xlarge | c7i.12xlarge| c7i.16xlarge | c7i.24xlarge | c7i.48xlarge
- Mémoire optimisée : r5.12xlarge | r5.24xlarge | r5b.12xlarge | r5d.12xlarge | r5d.24xlarge | r5n.12xlarge | r5n.24xlarge | | r5dn.12xlarge | r5dn.24xlarge | r6a.24xlarge | r6a.48xlarge | r6i.16xlarge | r6i.32xlarge | r6id.16xlarge | r6id.32xlarge | r6in.16xlarge | r6in.32xlarge | r7a.medium | r7a.large | r7a.xlarge | r7a.2xlarge | r7a.4xlarge | r7a.8xlarge | r7a.12xlarge | r7a.16xlarge | r7a.24xlarge | | r7a.32xlarge | r7a.48xlarge | r7i.large | r7i.xlarge | r7i.2xlarge | r7i.4xlarge | r7i.8xlarge | r7i.12xlarge | r7i.16xlarge | r7i.24xlarge | r7i.48xlarge| r7iz.large | r7iz.xlarge r7iz.2xlarge | r7iz.4xlarge | r7iz.8xlarge | r7iz.12xlarge | r7iz.16xlarge | r7iz.32xlarge | u-3tb1.56xlarge | u-6tb1.56xlarge u-6tb1.112xlarge | u-9tb1.112xlarge | u-12tb1.112xlarge | u-18tb1.112xlarge | u-24tb1.112xlarge | u7i-12tb.224xlarge | u7in-16tb.224xlarge | u7in-24tb.224xlarge |

`u7in-32tb.224xlarge` `x2idn.32xlarge` | `x2iedn.16xlarge` | `x2iezn.12xlarge` | `z1d.6xlarge` | `z1d.12xlarge`

- Optimisées pour le stockage : `d3en.12xlarge` | `dl1.24xlarge` | `i3en.12xlarge` | `i3en.24xlarge` | `i4i.16xlarge` | `r5b.12xlarge` | `r5b.24xlarge`
- Calcul accéléré : `dl1.24xlarge` `g5.24xlarge` | `g5.48xlarge` | `g6.24xlarge` | `g6.48xlarge` `g6e.12xlarge` | `g6e.24xlarge` | `g6e.48xlarge` | `inf1.24xlarge` | `p3dn.24xlarge` | `p4d.24xlarge` | `p4de.24xlarge` | `p5.24xlarge` | `trn1.32xlarge` | `vt1.24xlarge`

Il se peut que vous vouliez changer les paramètres « C-state » ou « P-state » pour améliorer la cohérence des performances du processeur, réduire la latence ou ajuster votre instance pour une charge de travail spécifique. Les paramètres « C-state » ou « P-state » par défaut offre des performances maximales qui sont optimales pour la plupart des charges de travail. Cependant, si votre application tirerait avantage de la latence réduite pour un coût de fréquences simple ou double cœur plus hautes ou des performances cohérentes à des fréquences plus basses au lieu des fréquences Turbo Boost transmises en paquets, pensez à essayer les paramètres « C-state » ou « P-state » qui sont disponibles pour ces instances.

Pour plus d'informations sur les différentes configurations de processeur et sur la manière de surveiller les effets de votre configuration pour Amazon Linux, consultez la section Contrôle de l'état du processeur pour l'instance EC2 Amazon Amazon Linux dans le guide de l'utilisateur Amazon Linux 2. Ces procédures ont été écrites pour Amazon Linux et s'appliquent à celui-ci ; toutefois, elles peuvent également fonctionner pour d'autres distributions Linux avec un noyau Linux de version 3.9 ou ultérieure. Pour obtenir plus d'informations sur les autres distributions Linux et le contrôle des états du processeur, consultez la documentation spécifique à votre système.

Options EC2 de facturation et d'achat Amazon

Vous pouvez utiliser les options suivantes pour optimiser vos coûts pour Amazon EC2 :

- Instances à la demande – Payez à la seconde pour les instances que vous lancez.
- Savings Plans — Réduisez vos EC2 coûts Amazon en vous engageant à utiliser régulièrement, USD par heure, pour une durée d'un ou trois ans.
- Instances réservées : réduisez vos EC2 coûts Amazon en vous engageant à utiliser une configuration d'instance cohérente, y compris le type d'instance et la région, pour une durée de 1 ou 3 ans.

- Instances ponctuelles : demandez EC2 des instances non utilisées, ce qui peut réduire considérablement vos EC2 coûts Amazon.
- Hôtes dédiés – Paiement d'un hôte physique qui est entièrement dédié à l'exécution de vos instances et utilisation du modèle BYOL (Bring-Your-Own-License) pour vos licences logicielles par socket, par cœur ou par ordinateur virtuel afin de réduire les coûts.
- Instances dédiées – Payez à l'heure, pour les instances qui s'exécutent sur un matériel à client unique.
- Réservations de capacité : réservez de la capacité pour vos EC2 instances dans une zone de disponibilité spécifique.

Si vous ne pouvez pas vous engager sur une configuration d'instance spécifique, mais que vous pouvez vous engager sur un montant d'utilisation, achetez des Savings Plans pour réduire les coûts de vos instances à la demande.Si vous avez besoin d'une réservation de capacité, achetez des instances réservées ou des réservations de capacité pour une zone de disponibilité spécifique. Les blocs de capacité peuvent être utilisés pour réserver un cluster d'GPUinstances. Les instances Spot constituent un choix économique si vous êtes flexible quant au moment où vos applications s'exécutent et à la possibilité de les interrompre. Les hôtes dédiés ou les instances dédiées peuvent vous aider à satisfaire vos exigences en matière de conformité et à réduire les coûts en utilisant vos licences logicielles existantes liées au serveur.

Pour plus d'informations, consultez Amazon EC2 Pricing.

Achat d'instances à la demande pour Amazon EC2

Avec les instances à la demande, vous payez la capacité de calcul à la seconde, sans engagement à long terme. Vous bénéficiez d'un contrôle complet sur le cycle de vie de l'instance : vous décidez quand la lancer, l'arrêter, la mettre en veille prolongée, la démarrer, la redémarrer ou la résilier.

Aucun engagement à long terme n'est requis lorsque vous achetez des instances à la demande. Vous payez uniquement pour les secondes pendant lesquelles vos Instances à la demande sont à l'état `running`, avec un minimum de 60 secondes. Le prix par seconde pour une instance à la demande en cours d'exécution est fixe et est indiqué sur la page de EC2tarification Amazon et sur la page de tarification à la demande d'.

Nous vous recommandons d'utiliser des instances à la demande pour les applications avec des charges de travail irrégulières à court terme qui ne peuvent pas être interrompues.

Pour réaliser des économies importantes par rapport aux instances à la demande, utilisez AWS Savings Plans, Spot instances ou EC2Présentation des instances réservées pour Amazon.

Table des matières

Quotas des instances à la demande

Il existe des quotas pour le nombre d'instances à la demande en cours d'exécution Compte AWS par région. Les quotas d'instances à la demande sont gérés en fonction du nombre d'unités centrales virtuelles (vCPUs) utilisées par vos instances à la demande en cours d'exécution, quel que soit le type d'instance. Chaque type de quota indique le nombre maximum de vCPUs pour une ou plusieurs familles d'instances.

Votre compte inclut les quotas suivants pour les instances à la demande. Les instances en attente, en arrêt, en veille prolongée ou en veille prolongée ne sont pas prises en compte dans vos quotas d'instances à la demande. Les réservations de capacité sont prises en compte dans vos quotas d'instances à la demande, même si elles ne sont pas utilisées.

Nom	Par défaut	Ajustable
Les instances DL à la demande en cours d'exécution	0	Oui
Instances F à la demande en cours d'exécution	0	Oui
Les instances G et VT à la demande en cours d'exécution	0	Oui
Exécution d'HPCinstances à la demande	0	Oui
Toutes les instances mémoire élevée à la demande en cours d'exécution	0	Oui
Instances Inf à la demande en cours d'exécution	0	Oui

Nom	Par défaut	Ajustable
Instances P à la demande en cours d'exécution	0	Oui
Les instances standard à la demande (A, C, D, H, I, M, R, T, Z) en cours d'exécution	5	Oui
Les instances Trn à la demande en cours d'exécution	0	Oui
Instances X à la demande en cours d'exécution	0	Oui

Pour plus d'informations sur les différentes familles, générations et tailles d'instances, consultez le Amazon EC2 Instance Types Guide.

Vous pouvez lancer n'importe quelle combinaison de types d'instances répondant à l'évolution des besoins de vos applications, à condition que le nombre d'instances vCPUs ne dépasse pas le quota de votre compte. Par exemple, avec un quota d'instances standard de 256vCPUs, vous pouvez lancer 32 `m5.2xlarge` instances (32 x 8vCPUs) ou 16 `c5.4xlarge` instances (16 x 16vCPUs). Pour plus d'informations, consultez EC2la section Limites des instances à la demande.

Tâches

- Surveiller les quotas et l'utilisation des instances à la demande
- Demander une augmentation de quota

Surveiller les quotas et l'utilisation des instances à la demande

Vous pouvez afficher et gérer les quotas de vos instances à la demande pour chaque région en utilisant les méthodes suivantes.

Pour afficher vos quotas actuels à l'aide de la console Service Quotas

1. Ouvrez la console Service Quotas à l'adresse https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Dans la barre de navigation, sélectionnez une région.
3. Dans le champ de filtre, saisissez **`On-Demand`**.
4. La colonne Valeur du quota appliqué affiche le nombre maximum de quotas vCPUs pour chaque type d'instance à la demande pour votre compte.

Pour consulter vos quotas actuels à l'aide de la AWS Trusted Advisor console

Ouvrez la page des limites de service dans la AWS Trusted Advisor console.

Pour configurer les CloudWatch alarmes

Grâce à l'intégration CloudWatch des métriques Amazon, vous pouvez surveiller votre EC2 utilisation par rapport à vos quotas. Vous pouvez également configurer des alarmes pour vous avertir lorsque vous approchez des quotas. Pour plus d'informations, consultez les sections Service Quotas et Amazon CloudWatch alarmes dans le Guide de l'utilisateur de Service Quotas.

Demander une augmentation de quota

Même si Amazon augmente EC2 automatiquement les quotas de vos instances à la demande en fonction de votre utilisation, vous pouvez demander une augmentation de quota si nécessaire. Par exemple, si vous avez l'intention de lancer plus d'instances que celles autorisées par votre quota actuel, vous pouvez demander une augmentation de quota à l'aide du de la console Service Quotas, comme décrit dans Quotas EC2 de service Amazon.

Rechercher les prix des instances à la demande

Vous pouvez utiliser le service de liste de prix API ou la liste de AWS prix API pour demander les prix des instances à la demande. Pour plus d'informations, consultez la section Utilisation de la liste de AWS prix API dans le guide de AWS Billing l'utilisateur.

EC2Présentation des instances réservées pour Amazon

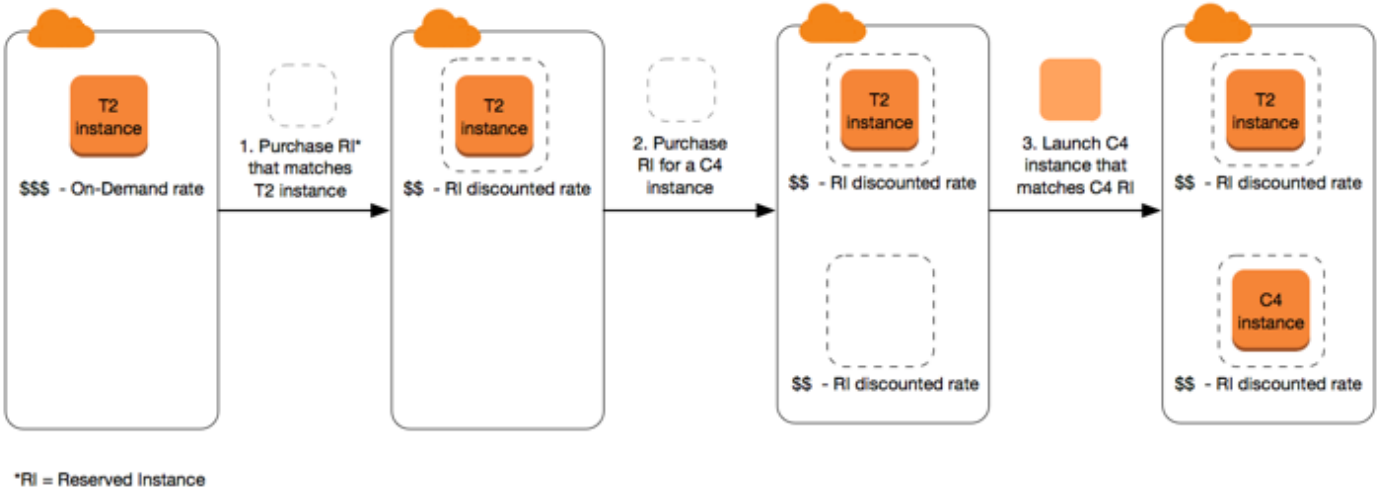
> **Important**
>
> Nous recommandons les Savings Plans plutôt que les instances réservées. Les plans d'épargne constituent le moyen le plus simple et le plus flexible d'économiser de l'argent sur vos coûts de AWS calcul et de proposer des prix plus bas (jusqu'à 72 % de réduction sur les prix à la demande), tout comme les instances réservées. Cependant, les Savings Plans sont différents des instances réservées. Avec les instances réservées, vous vous engagez à utiliser une configuration d'instance spécifique, tandis qu'avec Savings Plans, vous avez la possibilité d'utiliser les configurations d'instance qui répondent le mieux à vos besoins. Pour utiliser Savings Plans, vous vous engagez à utiliser un montant d'utilisation constant, mesuré USD par heure. Pour plus d'informations, consultez le Guide de l'utilisateur des AWS Savings Plans.

Les instances réservées vous permettent de réaliser des économies importantes sur vos EC2 coûts Amazon par rapport à la tarification des instances à la demande. Les instances réservées ne sont pas des instances physiques, mais correspondent à une remise de facturation appliquée à l'utilisation d'instances à la demande dans votre compte. Ces instances à la demande doivent correspondre à certains attributs, comme le type et la région de l'instance, afin d'entraîner une remise de facturation.

Rubriques instances réservées

Exemple de scénario d'instance réservée

Le schéma suivant montre un scénario de base d'achat et d'utilisation d'instances réservées.



Dans ce scénario, vous disposez dans votre compte d'une instance à la demande (T2) en cours d'exécution, qui vous est facturée au tarif à la demande. Vous achetez une Instance réservée qui correspond aux attributs de votre instance en cours d'exécution et l'avantage de facturation est immédiatement appliqué. Ensuite, vous achetez une Instance réservée pour une instance C4. Aucune instance en cours d'exécution dans votre compte ne correspond aux attributs de cette Instance réservée. Dans la dernière étape, vous lancez une instance qui correspond aux attributs de l'Instance réservée C4 et l'avantage de facturation est immédiatement appliqué.

Variables clés déterminant la tarification d'une Instance réservée

La tarification de Instance réservée est déterminée par les variables clés suivantes.

Attributs d'instance

Une instance réservée dispose de quatre attributs d'instance qui déterminent son prix.

- Type d'instance : par exemple, `m4.large`. Il est composé de la famille de·l'instance (par exemple, `m4`) et de la taille de l'instance (par exemple, `large`).
- Région : Région dans laquelle l'Instance réservée a été achetée.
- Location : si votre instance est exécutée sur un matériel partagé (par défaut) ou à client unique (dédié). Pour plus d'informations, consultez Instances EC2 dédiées Amazon.
- Plateforme : le système d'exploitation ; par exemple, Windows ou Linux/Unix. Pour plus d'informations, consultez Sélection d'une plateforme.

Engagement de durée

Vous pouvez acheter une Instance réservée pour un engagement d'un ou de trois ans, avec une remise plus importante pour l'engagement de trois ans.

- Un an : un an correspond à 31536000 secondes (365 jours).
- Trois ans : trois ans correspondent à 94608000 secondes (1095 jours).

Les instances réservées ne se renouvellent pas automatiquement ; lorsqu'elles expirent, vous pouvez continuer à utiliser l'EC2instance sans interruption, mais des tarifs à la demande vous sont facturés. Dans l'exemple ci-dessus, lorsque les instances réservées qui couvrent les instances T2 et C4 expirent, les tarifs à la demande vous sont à nouveaux appliqués jusqu'à ce que vous mettiez les instances hors service ou que vous achetiez de nouvelles instances réservées qui correspondent aux attributs de l'instance.

> **Important**
>
> Une fois que vous avez acheté une Instance réservée, vous ne pouvez pas annuler votre achat. Toutefois, vous pourrez probablement modifier, échanger ou vendre votre Instance réservée si vos besoins évoluent.

Options de paiement

Les options de paiement suivantes sont disponibles pour les instances réservées :

- Tous les frais initiaux : le paiement est effectué en totalité au début de la période, sans aucun autre coût ou frais horaires supplémentaires pour le reste de la réservation, quel que soit le nombre d'heures utilisé.
- Frais initiaux partiels : une partie du coût doit être payée au départ et les heures restantes pendant la période sont facturées à un tarif horaire réduit, que la Instance réservée soit utilisée ou non.
- Sans frais initiaux : vous devez régler un taux horaire avec remise pour chaque heure entrant dans le cadre de l'abonnement, que la Instance réservée soit utilisée ou non. Aucun paiement initial n'est requis.

> **Note**
>
> Les instances réservées sans frais initiaux sont basées sur une obligation contractuelle d'effectuer des paiements mensuels pendant toute la durée de la réservation. C'est la raison pour laquelle il est nécessaire de fournir un bon historique de facturation pour pouvoir acheter des instances réservées sans frais initiaux.

En règle générale, l'option la plus économique consiste à acheter des instances réservées en versant un paiement initial plus élevé. Vous pouvez aussi trouver des instances réservées proposées par des vendeurs tiers à des prix inférieurs avec des durées de paiement plus courtes sur la marketplace des instances réservées. Pour plus d'informations, consultez Vendez des instances réservées pour Amazon sur EC2 le Reserved Instance Marketplace.

Classe d'offre

Si vos besoins informatiques évoluent, vous pourrez probablement modifier ou échanger votre Instance réservée, en fonction de la classe d'offre.

- Standard : proposent la réduction la plus importante, mais ne peut que se modifier. Les instances réservées Standard ne peuvent pas être échangées.
- Convertible : proposent une réduction plus faible que les Instances réservées Standard, mais peut s'échanger contre une Instance réservée convertible avec différents attributs d'instance. Les instances réservées convertibles peuvent également être modifiées.

Pour plus d'informations, consultez Types d'instances réservées (classes d'offres).

> **Important**
>
> Une fois que vous avez acheté une Instance réservée, vous ne pouvez pas annuler votre achat. Toutefois, vous pourrez probablement modifier, échanger ou vendre votre Instance réservée si vos besoins évoluent.

Pour plus d'informations, consultez la page de tarification des instances EC2 réservées .

instances réservées régionales et zonales (portée)

Lorsque vous achetez une Instance réservée, vous déterminez la portée de la Instance réservée. La portée est régionale ou zonale.

- Régionale : lorsque vous achetez une Instance réservée pour une région, elle est appelée Instance réservée régionale.
- Zonale : lorsque vous achetez une Instance réservée pour une Zone de disponibilité spécifique, il s'agit d'une Instance réservée zonale.

L'étendue n'affecte pas le prix. Vous payez le même prix pour un Instance réservée régional ou zonal. Pour plus d'informations sur la tarification des instances réservées, consultez la section Variables clés déterminant la tarification d'une Instance réservée et la tarification des instances EC2 réservées Amazon.

Pour plus d'informations sur la façon de spécifier la portée d'une instance réservée, consultez Attributs RI, plus précisément le point Zone de disponibilité.

Différences entre les instances réservées régionales et zonales

Le tableau suivant souligne certaines différences essentielles entre les instances réservées zonales et les instances réservées régionales :

	instances réservées régionales	instances réservées zonales
Possibilité de réserver de la capacité	Une Instance réservée de région ne réserve pas de capacité.	Une Instance réservée de zone réserve de la capacité dans la zone de disponibilité spécifiée.
Flexibilité des zones de disponibilité	La remise de Instance réservée s'applique à l'utilisation d'une instance dans n'importe quelle zone de disponibilité de la région spécifiée.	Aucune flexibilité de zone de disponibilité—la remise de Instance réservée s'applique à l'utilisation d'instance uniquement dans la zone de disponibilité spécifiée.
Flexibilité de la taille de l'instance	La remise Instance réservée s'applique à une utilisation d'instance, quelle que soit la taille, au sein de cette famille d'instances. Prise en charge uniquement sur les instances réservées Amazon Linux/Unix avec location par défaut. Pour plus d'informations, consultez Flexibilité de taille d'instance déterminée par le facteur de normalisation.	Aucune flexibilité de taille d'instance—la remise de Instance réservée s'applique pour l'utilisation d'instance uniquement pour la taille et le type d'instance spécifiés.
Mise en file d'attente d'un achat	Vous pouvez mettre en file d'attente les achats pour les instances réservées régionales.	Vous ne pouvez pas mettre en file d'attente les achats pour les instances réservées zonales.

Pour plus d'informations et d'exemples, consultez Comment les remises sur les instances réservées sont appliquées.

Types d'instances réservées (classes d'offres)

La classe d'offre d'une Instance réservée est Standard ou Convertible. Une Instance réservée Standard offre un rabais plus important qu'une Instance réservée Convertible, mais vous ne pouvez pas échanger une Instance réservée Standard. Vous pouvez échanger les instances réservées Convertible. Vous pouvez modifier les instances réservées Standard et Convertible.

La configuration d'une Instance réservée comprend un type d'instance unique, une plateforme, une étendue et une location pendant une période donnée. Si vos besoins informatiques changent, vous pourriez être en mesure de modifier ou d'échanger votre Instance réservée.

Différences entre les instances réservées Standard et Convertible

Les différences entre les instances réservées Convertible et Standard sont les suivantes.

	Instance réservée standard	Instance réservée convertible
Modifier instances réservées	Certains attributs peuvent être modifiés. Pour plus d'informations, consultez Modifier instances réservées.	Certains attributs peuvent être modifiés. Pour plus d'informations, consultez Modifier instances réservées.
Échanger des instances réservées	Ne peut pas être échangée.	Peut être échangée, pendant la période de paiement, contre une autre Instance réservée convertible avec de nouveaux attributs tels que la famille de·l'instance, le type d'instance, la plateforme, l'étendue ou la location. Pour plus d'informations, consultez Échanger des instances réservées convertibles.

	Instance réservée standard	Instance réservée convertible
Vendre sur la marketplace des instances réservées	Peut être vendue sur la marketplace des instances réservées.	Ne peut pas être vendue sur la marketplace des instances réservées.
Acheter sur la marketplace des instances réservées	Peut être achetée sur la marketplace des instances réservées.	Ne peut pas être achetée sur la marketplace des instances réservées.

Comment les remises sur les instances réservées sont appliquées

Les instances réservées ne sont pas des instances physiques, mais correspondent à une remise de facturation appliquée à l'exécution d'instances à la demande dans votre compte. Les instances à la demande doivent correspondre à certains attributs des instances réservées pour bénéficier de la remise de facturation.

Si vous achetez une instance réservée et que vous avez déjà une instance à la demande en cours d'exécution qui correspond aux attributs de l'instance réservée, la remise de facturation est immédiatement et automatiquement appliquée. Vous n'avez pas besoin de redémarrer vos instances. Si vous n'avez pas d'instance à la demande éligible en cours d'exécution, lancez une instance à la demande ayant les mêmes attributs que votre instance réservée. Pour plus d'informations, consultez Utiliser votre instances réservées.

La classe d'offre (Standard ou Convertible) de l'instance réservée n'affecte pas la façon dont la remise de facturation est appliquée.

Rubriques

Application des instances réservées zonales

Une instance réservée achetée pour réserver une capacité dans une zone de disponibilité spécifique est appelée instance réservée de zone.

- La remise d'instance réservée s'applique à l'utilisation correspondante d'une instance dans cette zone de disponibilité.
- Les attributs (location, plateforme, zone de disponibilité, type d'instance et taille d'instance) des instances en cours d'exécution doivent correspondre à celles des instances réservées.

Par exemple, si vous achetez deux instances réservées standard Linux/Unix à location par défaut `c4.xlarge` dans la zone de disponibilité us-east-1a, jusqu'à deux instances Linux/Unix à location par défaut `c4.xlarge` s'exécutant dans la zone de disponibilité us-east-1a peuvent bénéficier de la remise d'instance réservée.

Application des instances réservées régionales

Une instance réservée achetée pour une région est appelée instance réservée régionale et assure une flexibilité de zone de disponibilité et de taille d'instance.

- La remise de Instance réservée s'applique à l'utilisation d'une instance dans n'importe quelle zone de disponibilité de la région spécifiée.
- La remise d'instance réservée s'applique à une utilisation d'instance, quelle que soit la taille, au sein de cette famille d'instances. Il s'agit de la flexibilité de la taille d'instance.

Flexibilité de la taille de l'instance

Avec la flexibilité de la taille d'instance, la remise d'instance réservée s'applique à une utilisation d'instances de la même famille, génération et du même attribut. L'instance réservée est appliquée de la taille d'instance la plus petite à la taille d'instance la plus grande au sein de la famille de·l'instance, en fonction du facteur de normalisation. Pour voir un exemple d'application de la réduction sur les instances réservées, consultez Scénario 2 : instances réservées dans un compte unique utilisant le facteur de normalisation.

Limites

- Prise en charge : la flexibilité de la taille des instances n'est prise en charge que pour les instances réservées régionales.
- Pas de prise en charge : la flexibilité de la taille des instances n'est pas prise en charge pour les instances réservées suivantes :
  - Les instances réservées achetées pour une Zone de disponibilité spécifique (instances réservées zonales)

- Instances réservées pour les instances G4ad, G4dn, G5, G5g, G6, G6e, Gr6, hpc7a, P5, Inf1 et Inf2
- Instances réservées pour Windows Server, Windows Server avec SQL Standard, Windows SQL Server avec Server Enterprise, Windows SQL Server avec Server Web et SUSE Linux Enterprise Server RHEL
- instances réservées avec location dédiée

Flexibilité de taille d'instance déterminée par le facteur de normalisation

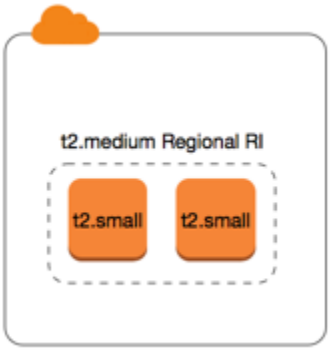
La flexibilité de la taille d'instance est déterminée par le facteur de normalisation de la taille d'instance. La remise s'applique complètement ou partiellement aux instances en cours d'exécution d'une même famille de·l'instance, en fonction de la taille d'instance de la réservation, dans n'importe quelle zone de disponibilité de la région. Les seuls attributs qui doivent correspondre sont la famille de·l'instance, la location et la plate-forme.

Le tableau suivant décrit les différentes tailles au sein d'une famille de·l'instance et le facteur de normalisation correspondant. Cette échelle est utilisée pour appliquer le taux avec remise des instances réservées à l'utilisation normalisée de la famille de·l'instance.

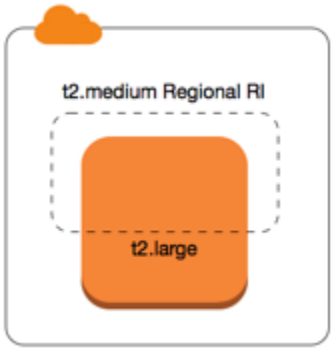
Taille d'instance	Facteur de normalisation
nano	0.25
micro	0.5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32

Taille d'instance	Facteur de normalisation
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256
48xlarge	384
56xlarge	448
112xlarge	896

Par exemple, le facteur de normalisation d'une instance `t2.medium` est 2. Si vous achetez une Instance réservée Amazon Linux/Unix `t2.medium` à location par défaut dans la région US East (N. Virginia) et que vous avez deux instances `t2.small` en cours d'exécution dans votre compte dans cette région, l'avantage de facturation est appliqué entièrement à ces deux instances.



Si vous avez une instance `t2.large` en cours d'exécution dans votre compte dans la région US East (N. Virginia), l'avantage de facturation est appliqué à 50 % de l'utilisation de l'instance.



Le facteur de normalisation est également appliqué lors de la modification d'instances réservées standard. Pour plus d'informations, consultez Modifier instances réservées.

Facteur de normalisation pour les instances matériel nu

La flexibilité de taille d'instance s'applique également aux instances à matériel nu dans la famille d'instances. Si vous disposez de instances réservées Amazon Linux/Unix régionales avec une location partagée sur des instances à matériel nu, vous pouvez profiter des économies Instance réservée avec la même famille d'instances. L'inverse est également vrai : si vous disposez de instances réservées Amazon Linux/Unix régionales avec une location partagée sur des instances de la même famille que l'instance à matériel nu, vous pouvez profiter des économies Instance réservée sur l'instance à matériel nu.

La taille d'instances `metal` ne dispose pas d'un seul et unique facteur de normalisation. Une instance bare metal a le même facteur de normalisation que la taille d'instance virtualisée équivalente au sein de la même famille de·l'instance. Par exemple, une instance `i3.metal` a le même facteur de normalisation qu'une instance `i3.16xlarge`.

Taille d'instance	Facteur de normalisation
`a1.metal`	32
`m5zn.metal` | `x2iezn.metal` `z1d.metal`	96
`c6g.metal` | `c6gd.metal` | `i3.metal` | `m6g.metal` | `m6gd.metal` | `r6g.metal` | `r6gd.metal` | `x2gd.metal`	128

Taille d'instance	Facteur de normalisation
c5n.metal	144
c5.metal | c5d.metal | i3en.metal | m5.metal | m5d.metal | m5dn.metal | m5n.metal | r5.metal | r5b.metal | r5d.metal | r5dn.metal | r5n.metal	192
c6i.metal | c6id.metal | m6i.metal | m6id.metal | r6d.metal | r6id.metal	256
u-*.metal	896

Par exemple, une instance i3.metal dispose d'un facteur de normalisation de 128. Si vous achetez un Instance réservée Amazon Linux/Unix à location par défaut i3.metal dans la US East (N. Virginia), l'avantage de facturation peut s'appliquer comme suit :

- Si vous disposez d'une i3.16xlarge en cours d'exécution dans votre compte pour cette région, l'avantage de facturation peut s'appliquer entièrement à l'instance i3.16xlarge (facteur de normalisation i3.16xlarge = 128).
- Sinon, si vous disposez de deux instances i3.8xlarge en cours d'exécution dans votre compte pour cette région, l'avantage de facturation peut s'appliquer entièrement aux deux instances i3.8xlarge (facteur de normalisation i3.8xlarge = 64).
- Sinon, si vous disposez de quatre instances i3.4xlarge en cours d'exécution dans votre compte pour cette région, l'avantage de facturation peut s'appliquer entièrement aux quatre instances i3.4xlarge (facteur de normalisation i3.4xlarge = 32).

L'inverse est également vrai. Par exemple, si vous achetez deux Instances réservées Amazon Linux/Unix à location par défaut i3.8xlarge dans la US East (N. Virginia) et que vous disposez d'une instance i3.metal dans cette région, l'avantage de facturation s'applique entièrement à l'instance i3.metal.

Exemples d'application des instances réservées

Les scénarios suivants couvrent les façons dont les instances réservées sont appliquées.

- Scénario 1 : instances réservées dans un compte unique

Scénario 1 : instances réservées dans un compte unique

Vous exécutez les instances à la demande suivantes dans le compte A :

- 4 instances `m3.large` Linux à location par défaut dans la zone de disponibilité us-east-1a
- 2 instances `m4.xlarge` Amazon Linux à location par défaut dans la zone de disponibilité us-east-1b
- 1 instance Amazon Linux `c4.xlarge` à location par défaut dans la zone de disponibilité us-east-1c

Vous achetez ensuite les instances réservées suivantes dans le compte A :

- 4 Instances réservées `m3.large` Linux à location par défaut dans la zone de disponibilité us-east-1a (la capacité est réservée)
- 4 Instances réservées Amazon Linux `m4.large` à location par défaut dans la région us-east-1
- 1 Instances réservées Amazon Linux `c4.large` à location par défaut dans la région us-east-1

Les avantages de l'Instance réservée sont appliqués de la façon suivante :

- La remise et la réservation de capacité des quatre Instances réservées zonales `m3.large` sont utilisées par les quatre instances `m3.large`, car leurs attributs (taille de l'instance, région, plateforme, location) correspondent.
- Les Instances réservées régionales `m4.large` fournissent une flexibilité de zone de disponibilité et de taille d'instance, car il s'agit d'Instances réservées Amazon Linux régionales à location par défaut.

  Une instance `m4.large` est équivalente à 4 unités normalisées/heure.

  Vous avez acheté quatre Instances réservées régionales `m4.large` et, au total, celles-ci sont égales à 16 unités normalisées/heure (4x4). Le compte A comporte deux instances `m4.xlarge` en cours d'exécution, ce qui est équivalant à 16 unités normalisées/heure (2x8). Dans ce cas, les quatre instances réservées régionales `m4.large` apportent l'avantage de facturation complet à l'utilisation des deux instances `m4.xlarge`.

- L'Instance réservée régionale `c4.large` dans la région us-east-1 fournit une flexibilité de zone de disponibilité et de taille d'instance, car il s'agit d'une Instance réservée régionale Amazon Linux à location par défaut et elle s'applique à l'instance `c4.xlarge`. Une instance `c4.large` est équivalente à 4 unités normalisées/heure et une instance `c4.xlarge` est équivalente à 8 unités normalisées/heure.

  Dans ce cas, l'Instance réservée régionale `c4.large` apporte un avantage partiel à l'utilisation de `c4.xlarge`. Cela est dû au fait qu'une Instance réservée `c4.large` est équivalente à 4 unités normalisées/heure d'utilisation, mais qu'une instance `c4.xlarge` requiert 8 unités normalisées/heure. Par conséquent, la remise de facturation de l'Instance réservée `c4.large` s'applique à 50 % de l'utilisation de `c4.xlarge`. L'utilisation `c4.xlarge` restante est facturée au taux à la demande.

Scénario 2 : instances réservées dans un compte unique utilisant le facteur de normalisation

Vous exécutez les instances à la demande suivantes dans le compte A :

- 2 instances `m3.xlarge` Amazon Linux à location par défaut dans la zone de disponibilité us-east-1a
- 2 instances `m3.large` Amazon Linux à location par défaut dans la zone de disponibilité us-east-1b

Vous achetez ensuite l'instance réservée suivante dans le compte A :

- 1 instance réservée Amazon Linux `m3.2xlarge` à location par défaut dans la région us-east-1

Les avantages de l'Instance réservée sont appliqués de la façon suivante :

- L'instance réservée régionale `m3.2xlarge` dans la région us-east-1 fournit une flexibilité de zone de disponibilité et de taille d'instance, car il s'agit d'une instance réservée régionale Amazon Linux à location par défaut. Elle s'applique d'abord aux instances `m3.large`, puis aux instances `m3.xlarge`, car elle s'applique de la taille d'instance la plus petite à la taille d'instance la plus grande au sein de la famille de·l'instance, en fonction du facteur de normalisation.

  Une instance `m3.large` est équivalente à 4 unités normalisées/heure.

  Une instance `m3.xlarge` est équivalente à 8 unités normalisées/heure.

  Une instance `m3.2xlarge` est équivalente à 16 unités normalisées/heure.

L'avantage est appliqué comme suit :

L'instance réservée régionale `m3.2xlarge` offre un avantage complet pour l'utilisation de deux instances `m3.large`, car ensemble, ces instances représentent 8 unités normalisées/heure. Ainsi, il reste 8 unités normalisées/heure à appliquer aux instances `m3.xlarge`.

Avec les 8 unités normalisées/heure restantes, l'instance réservée régionale `m3.2xlarge` offre un avantage complet pour l'utilisation d'une instance `m3.xlarge`, car chaque instance `m3.xlarge` est équivalente à 8 unités normalisées/heure. L'utilisation `m3.xlarge` restante est facturée au taux à la demande.

Scénario 3 : instances réservées régionales dans des comptes liés

Les instances réservées sont d'abord appliquées à une utilisation au sein du compte d'achat, puis à l'utilisation éligible dans tout autre compte au sein de l'organisation. Pour plus d'informations, consultez instances réservées et la facturation consolidée. Pour les instances réservées régionales qui offrent la flexibilité de la taille d'instance, l'avantage est appliqué de la taille d'instance la plus petite à la taille d'instance la plus grande au sein de la famille de·l'instance.

Vous exécutez les instances à la demande suivantes dans le compte A (le compte d'achat) :

- 2 instances `m4.xlarge` Linux à location par défaut dans la zone de disponibilité us-east-1a
- 1 instances `m4.2xlarge` Linux à location par défaut dans la zone de disponibilité us-east-1b
- 2 instances `c4.xlarge` Linux à location par défaut dans la zone de disponibilité us-east-1a
- 1 instances `c4.2xlarge` Linux à location par défaut dans la zone de disponibilité us-east-1b

Un autre client exécute les instances à la demande suivantes dans le compte B (un compte lié) :

- 2 instances `m4.xlarge` Linux à location par défaut dans la zone de disponibilité us-east-1a

Vous achetez ensuite les instances réservées régionales suivantes dans le compte A :

- 4 Instances réservées Linux `m4.xlarge` à location par défaut dans la région us-east-1
- 2 Instances réservées Linux `c4.xlarge` à location par défaut dans la région us-east-1

Les avantages de l'Instance réservée régionale sont appliqués de la façon suivante :

- La remise des quatre Instances réservées `m4.xlarge` est utilisée par les deux instances `m4.xlarge` et par l'instance `m4.2xlarge` unique dans le compte A (compte d'achat). Les trois instances correspondent toutes aux attributs (famille de·l'instance, région, plate-forme, location). La remise s'applique d'abord aux instances dans le compte d'achat (compte A), même si le compte B (compte lié) dispose de deux `m4.xlarge` qui correspondent également aux Instances réservées. Il n'y a pas de réservation de capacité, car les instances réservées sont des instances réservées régionales.
- La remise des deux Instances réservées `c4.xlarge` s'applique aux deux instances `c4.xlarge`, car elles ont une taille d'instance plus petite que l'instance `c4.2xlarge`. Il n'y a pas de réservation de capacité, car les instances réservées sont des instances réservées régionales.

Scénario 4 : instances réservées zonales dans un compte lié

En général, les instances réservées appartenant à un compte sont appliquées en premier à l'utilisation dans ce compte. Cependant, s'il existe des instances réservées éligibles non utilisées pour une zone de disponibilité spécifique (instances réservées zonales) dans d'autres comptes de l'organisation, elles sont appliquées au compte avant les instances réservées régionales appartenant au compte. Ceci vise à garantir une utilisation maximale des Instance réservée et une facture moins élevée. A des fins de facturation, tous les comptes de l'organisation sont traités comme s'il s'agissait d'un seul compte. L'exemple suivant peut contribuer à en apporter l'explication.

Vous exécutez l'instance à la demande suivante dans le compte A (le compte d'achat) :

- 1 instance `m4.xlarge` Linux à location par défaut dans la zone de disponibilité us-east-1a

Un client exécute l'instance à la demande suivante dans le compte B lié :

- 1 instance `m4.xlarge` Linux à location par défaut dans la zone de disponibilité us-east-1b

Vous achetez ensuite les instances réservées régionales suivantes dans le compte A :

- 1 Instance réservée Linux `m4.xlarge` à location par défaut dans la région us-east-1

Un client achète également les instances réservées zonales suivantes dans le compte C lié :

- 1 Instances réservées `m4.xlarge` Linux à location par défaut dans la zone de disponibilité us-east-1a

Les avantages de l'Instance réservée sont appliqués de la façon suivante :

- La remise de l'Instance réservée zonale `m4.xlarge` appartenant au compte C est appliquée à l'utilisation de `m4.xlarge` dans le compte A.
- La remise de l'Instance réservée régionale `m4.xlarge` appartenant au compte A est appliquée à l'utilisation de `m4.xlarge` dans le compte B.
- Si l'Instance réservée régionale appartenant au compte A est appliquée d'abord à l'utilisation dans le compte A, l'Instance réservée zonale appartenant au compte C reste inutilisée et l'utilisation dans le compte B est facturée aux tarifs à la demande.

Pour plus d'informations, consultez la section Comprendre vos réservations dans le AWS Cost and Usage Report.

> **Note**
>
> Les instances réservées zonales réservent de la capacité uniquement au compte propriétaire et ne peuvent pas être partagées avec d'autres Comptes AWS. Si vous devez partager de la capacité avec d'autres Comptes AWS, utilisez Réservez de la capacité de calcul grâce aux réservations de capacité à la demande.

Utiliser votre instances réservées

Les instances réservées sont appliquées automatiquement aux instances à la demande en cours d'exécution correspondant aux spécifications. Si vous n'avez pas d'instances à la demande en cours d'exécution qui correspond aux spécifications de votre Instance réservée, l'Instance réservée est inutilisée jusqu'à ce que vous lanciez une instance avec les spécifications requises.

Si vous lancez une instance à la demande pour bénéficier de l'avantage de facturation d'une instance réservée, veillez à spécifier les informations suivantes lors de la configuration.

Plateforme

Vous devez spécifier une Amazon Machine Image (AMI) correspondant à la plate-forme (description du produit) de votre instance réservée. Par exemple, si vous l'avez spécifié `Linux/UNIX` pour votre instance réservée, vous pouvez lancer une instance à partir d'un Amazon Linux AMI ou d'un UbuntuAMI.

Type d'instance

Si vous avez acheté une instance réservée zonale, vous devez spécifier le même type d'instance que pour votre instance réservée ; par exemple, `t3.large`. Pour plus d'informations, consultez Application des instances réservées zonales.

Si vous avez acheté une instance réservée régionale, vous devez spécifier un type d'instance de la même famille d'instances que le type d'instance de votre instance réservée. Par exemple, si vous avez spécifié `t3.xlarge` pour votre instance réservée, vous devez lancer votre instance à partir de la famille T3, mais vous pouvez spécifier n'importe quelle taille, par exemple, `t3.medium`. Pour plus d'informations, consultez Application des instances réservées régionales.

Zone de disponibilité

Si vous avez acheté une instance réservée zonale pour une zone de disponibilité spécifique, vous devez lancer l'instance dans la même zone de disponibilité.

Si vous avez acheté une instance réservée régionale, vous pouvez lancer l'instance dans n'importe quelle zone de disponibilité de la région spécifiée pour l'instance réservée.

Location

La location (`dedicated` ou `shared`) de votre instance doit correspondre à celle de l'instance réservée. Pour plus d'informations, consultez Instances EC2 dédiées Amazon.

Pour voir des exemples d'application des instances réservées à vos instances à la demande en cours d'exécution, consultez Comment les remises sur les instances réservées sont appliquées. Pour plus d'informations, consultez Pourquoi mes instances EC2 réservées Amazon ne s'appliquent-elles pas à ma AWS facturation de la manière prévue ?

Vous pouvez utiliser diverses méthodes pour lancer les instances à la demande qui utilisent votre remise d'instance réservée. Pour plus d'informations sur les différentes méthodes de lancement, consultez Lancer une EC2 instance Amazon. Vous pouvez également utiliser Amazon EC2 Auto Scaling pour lancer une instance. Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon EC2 Auto Scaling.

Comment fonctionne la facturation avec les instances réservées

Toutes les instances réservées vous permettent de bénéficier d'une remise par rapport à la tarification à la demande. Avec les instances réservées, vous payez pour toute la durée de

l'abonnement et non en fonction de l'utilisation réelle. Vous pouvez choisir d'effectuer un paiement initial ou un paiement initial partiel, ou mensuel pour votre Instance réservée, en fonction de l'option de paiement spécifiée pour l'Instance réservée.

Lorsque les instances réservées expirent, des tarifs à la demande vous sont facturés pour l'utilisation des EC2 instances. Vous pouvez mettre en file d'attente l'achat d'une Instance réservée jusqu'à trois ans en avance. Cela peut vous aider à garantir une couverture ininterrompue. Pour de plus amples informations, veuillez consulter Mettre votre achat en file d'attente.

Le Niveau gratuit d'AWS est disponible pour les neufs Comptes AWS. Si vous utilisez le Niveau gratuit d'AWS pour exécuter des EC2 instances Amazon et que vous achetez une instance réservée, le prix standard vous est facturé. Pour plus d'informations, veuillez consulter Niveau gratuit d'AWS.

Table des matières

Facturation de l'utilisation

Les instances réservées sont facturées toutes les heures d'horloge au cours de la réservation sélectionnée, que l'instance soit exécutée. Chaque heure d'horloge commence à l'heure (zéro minute et zéro seconde après l'heure) d'une horloge standard de 24 heures. Par exemple, 1:00:00 à 1:59:59 est une heure horloge. Pour plus d'informations sur les états de l'instance, consultez Modifications de l'état de l'EC2instance Amazon.

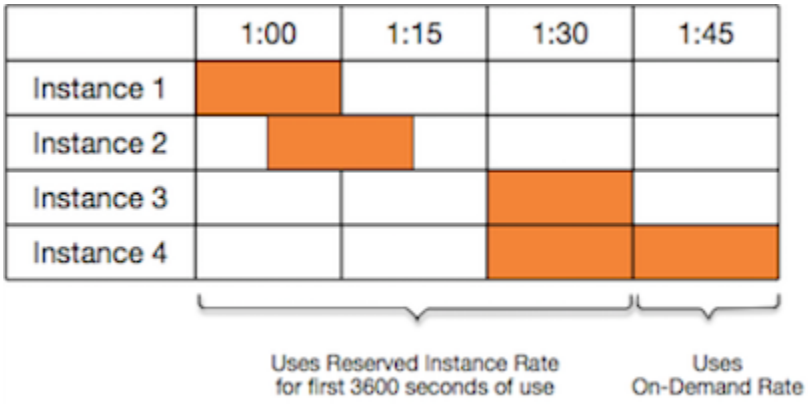
L'avantage de facturation d'une Instance réservée peut être appliqué à une instance en cours d'exécution sur une base par seconde. La facturation par seconde est disponible pour les instances qui utilisent une distribution Linux en open source, telle que Amazon Linux et Ubuntu. La facturation horaire est utilisée pour les distributions Linux commerciales, telles que Red Hat Enterprise Linux et SUSE Linux Enterprise Server.

L'avantage de facturation d'une Instance réservée peut s'appliquer à un maximum de 3 600 secondes (une heure) d'utilisation d'instance par heure d'horloge. Vous pouvez exécuter plusieurs instances simultanément, mais vous ne pouvez bénéficier de l'avantage de la remise d'Instance réservée que pour un total de 3600 secondes par heure d'horloge ; l'utilisation d'instance qui dépasse 3600 secondes dans une heure d'horloge est facturée au tarif à la demande.

Par exemple, si vous achetez une Instance réservée `m4.xlarge` et que vous exécutez simultanément quatre instances `m4.xlarge` pendant une heure, une instance est facturée au tarif d'une heure d'utilisation d'Instance réservée et les trois autres instances sont facturées au tarif de trois heures d'utilisation à la demande.

Par contre, si vous achetez une Instance réservée `m4.xlarge` et que vous exécutez simultanément quatre instances `m4.xlarge` pendant 15 minutes (900 secondes), chacune au cours de la même heure, la durée d'exécution totale pour les instances est d'une heure, ce qui se traduit par une heure d'utilisation d'Instance réservée et 0 heure d'utilisation à la demande.

Si plusieurs instances éligibles s'exécutent simultanément, l'avantage de facturation d'Instance réservée est appliqué à toutes les instances en même temps pour un maximum de 3600 secondes dans une heure d'horloge ; ensuite ce sont les tarifs à la demande qui s'appliquent.



Cost Explorer dans la console Billing and Cost Management vous permet d'analyser les économies réalisées par rapport à l'exécution d'Instances à la demande. Les instances réservées FAQ incluent un exemple de calcul de valeur de liste.

Si vous fermez votre AWS compte, la facturation à la demande de vos ressources cesse. Toutefois, si vous avez des instances réservées dans votre compte, vous continuez à recevoir une facture pour ces instances jusqu'à ce qu'elles expirent.

Affichage d'une facture

Vous pouvez consulter les frais et tarifs appliqués à votre compte sur la page de la console AWS Billing and Cost Management.

- Le Tableau de bord affiche un récapitulatif des dépenses de votre compte.
- Sur la page Factures, sous Détails, développez la section Elastic Compute Cloud et la région pour obtenir des informations de facturation sur vos Instances réservées.

Vous pouvez consulter les frais en ligne ou télécharger un CSV fichier.

Vous pouvez également suivre l'utilisation de vos instances réservées à l'aide du rapport sur les AWS coûts et l'utilisation. Pour plus d'informations, consultez Instances réservées dans le rapport d'utilisation et de coût du Guide de l'utilisateur AWS Billing .

instances réservées et la facturation consolidée

Les avantages de tarification des instances réservées sont partagés lorsque le compte d'achat fait partie d'un ensemble de comptes facturés réunis sous un même compte payeur de facturation consolidée. L'utilisation d'instance pour tous les comptes membres est regroupé dans le compte souscripteur tous les mois. Cette fonctionnalité est généralement utile dans le cadre des sociétés disposant de plusieurs équipes ou groupes fonctionnels. Ensuite, la logique standard des Instance réservées est appliquée pour calculer le montant de la facture. Pour plus d'informations, consultez Facturation consolidée dans le AWS Organizations.

Si vous fermez le compte qui a acheté l'Instance réservée, le compte payeur est débité pour l'Instance réservée jusqu'à ce que celle-ci expire. Le compte fermé est supprimé définitivement après 90 jours, et les comptes membres ne bénéficient plus de la réduction de facturation pour Instance réservée.

> **Note**
>
> Les instances réservées zonales réservent de la capacité uniquement au compte propriétaire et ne peuvent pas être partagées avec d'autres Comptes AWS. Si vous devez partager de la capacité avec d'autres Comptes AWS, utilisez Réservez de la capacité de calcul grâce aux réservations de capacité à la demande.

Niveaux de tarification avec remise d'Instance réservée

Si votre compte est éligible pour bénéficier d'un niveau de tarification avec remise, il bénéficie automatiquement des remises dès le départ et le tarif d'utilisation des instances pour tous les achats d'Instance réservée effectuées dans le cadre de ce niveau à partir de ce moment-là. Pour bénéficier d'une réduction, la valeur de liste de vos instances réservées dans la région doit être de 500 000$ USD ou plus.

Les règles suivantes s'appliquent :

- Les niveaux de tarification et les remises associées s'appliquent uniquement aux achats d'instances réservées Amazon EC2 Standard.
- Les niveaux de tarification ne s'appliquent pas aux instances réservées pour Windows avec SQL SQL Server Standard, Server Web et SQL Server Enterprise.
- Les niveaux de tarification ne s'appliquent pas aux instances réservées pour Linux avec SQL SQL Server Standard, Server Web et SQL Server Enterprise.
- Les remises tarifaires s'appliquent uniquement aux achats effectués auprès de AWS. Elles ne s'appliquent pas aux achats d'instances réservées tierces.
- Les achats d'Instance réservée convertible ne bénéficient pas actuellement de niveaux de tarification avec remise.

Rubriques

Calculer les remises de tarification d'une Instance réservée

Vous pouvez déterminer le niveau de tarification de votre compte en calculant la valeur de la liste répertoriant toutes vos instances réservées dans une région. Multipliez le taux horaire récurrent de chaque réservation par le nombre total d'heures pour l'abonnement et ajoutez le tarif initial avant remise (également connu sous le nom de tarif fixe) au moment de l'achat. Dans la mesure où la valeur de la liste repose sur le tarif avant remise (public), elle ne change pas si vous êtes éligible pour une remise sur le volume ou si le tarif chute une fois que vous avez acheté vos instances réservées.

```
List value = fixed price + (undiscounted recurring hourly price * hours in term)
```

Par exemple, pour une Instance réservée `t2.small` avec frais initiaux partiels d'une année, supposons que le prix initial est de 60,00 USD et que le tarif horaire est de 0,007 USD. Cela donne une valeur de liste de 121,32 USD.

```
121.32 = 60.00 + (0.007 * 8760)
```

New console

Pour consulter les valeurs des prix fixes pour les instances réservées à l'aide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Reserved Instances (Instances réservées).
3. Pour afficher la colonne du prix initial, choisissez settings () dans le coin supérieur droit, activez le prix initial et choisissez Confirmer.

Old console

Pour consulter les valeurs des prix fixes pour les instances réservées à l'aide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Reserved Instances (Instances réservées).
3. Pour afficher la colonne Prix initial, choisissez settings () dans le coin supérieur droit, sélectionnez Prix initial, puis cliquez sur Fermer.

Pour afficher les valeurs du tarif fixe des instances réservées à l'aide de la ligne de commande

- describe-reserved-instances (AWS CLI)
- Get-EC2ReservedInstance (AWS Tools for Windows PowerShell)
- DescribeReservedInstances(Amazon EC2API)

Acheter avec un niveau de remise

Lorsque vous achetez des instances réservées, Amazon applique EC2 automatiquement toutes les remises à la partie de votre achat correspondant à un niveau de prix réduit. Vous n'avez rien à faire différemment et vous pouvez acheter des instances réservées à l'aide de l'un des EC2 outils Amazon. Pour de plus amples informations, veuillez consulter Acheter des instances réservées pour Amazon EC2.

Une fois que la valeur de la liste répertoriant vos instances réservées actives dans une région a atteint le niveau de tarification avec remise, tous les achats suivants d'instances réservées dans cette région sont facturés au tarif réduit. Si un seul achat d'instances réservées dans une région vous permet de dépasser le seuil d'un niveau de remise, la partie de l'achat qui dépasse ce seuil est facturée au tarif réduit. Pour plus d'informations sur les instances IDs réservées temporaires créées au cours du processus d'achat, consultezChangement de niveau de tarification.

Si votre valeur de liste tombe en dessous du seuil minimum pour ce niveau de tarification avec remise (par exemple, lorsque certaines instances réservées arrivent à expiration), les achats suivants d'instances réservées dans la région ne sont pas facturés au tarif réduit. Toutefois, vous continuez à bénéficier de la remise appliquée aux instances réservées initialement achetées dans le cadre du niveau de tarification avec remise.

Lorsque vous achetez des instances réservées, quatre scénarios peuvent se produire :

- Aucune remise : votre achat dans une région se trouve toujours en dessous du seuil de remise.
- Remise partielle : votre achat dans une région dépasse le seuil du premier niveau de tarification avec remise. Aucune remise n'est appliquée à une ou plusieurs réservations et le taux avec remise est appliqué aux réservations restantes.
- Remise complète : tous vos achats au sein d'une région relèvent d'un niveau de tarification avec remise et sont en conséquence facturés au tarif réduit.
- Deux taux avec remise : votre achat dans une région vous permet de passer d'un niveau de tarification inférieur avec remise à un niveau de tarification supérieur avec remise. Deux taux différents sont facturés : une ou plusieurs réservations au taux avec remise inférieur et les réservations restantes au taux avec remise supérieur.

Changement de niveau de tarification

Si votre achat vous fait passer à un niveau de tarification avec remise, vous voyez plusieurs entrées pour cet achat : une première correspondant à la partie de l'achat facturée au prix standard et une deuxième correspondant à la partie de l'achat facturée au taux avec remise applicable.

Le service d'instance réservée génère plusieurs instances réservées IDs parce que votre achat est passé d'un niveau sans réduction ou d'un niveau réduit à un autre. Un ID est attribué à chaque ensemble de réservations d'un niveau. Par conséquent, l'identifiant renvoyé par votre CLI commande ou API action d'achat est différent de l'identifiant réel des nouvelles instances réservées.

Facturation consolidée pour les niveaux de tarification

Un compte de facturation consolidée regroupe la valeur de liste des comptes membres au sein d'une région. Lorsque la valeur de la liste de toutes les instances réservées actives du compte de facturation consolidée atteint un niveau de tarification avec remise, toute instances réservées achetée après ce stade par un membre du compte de facturation consolidée est facturée au tarif avec remise (tant que la valeur de la liste associée à ce compte consolidé reste au-dessus du seuil du niveau de tarification avec remise). Pour de plus amples informations, veuillez consulter instances réservées et la facturation consolidée.

Acheter des instances réservées pour Amazon EC2

Pour acheter une instance réservée pour AmazonEC2, vous pouvez utiliser la EC2 console Amazon, un outil de ligne de commande ou rechercher des offres d'SDKinstances réservées auprès de AWS vendeurs tiers, en ajustant vos paramètres de recherche jusqu'à ce que vous trouviez la correspondance exacte que vous recherchez.

Lorsque vous recherchez des instances réservées à acheter, vous recevez un devis avec le coût des offres renvoyées. Lorsque vous procédez à l'achat, place AWS automatiquement un prix limite sur le prix d'achat. Le coût total de vos instances réservées ne dépasse pas le montant du devis.

Si le tarif augmente ou change pour quelque raison que ce soit, l'achat n'est pas validé. Lorsque vous achetez l'instance réservée d'un vendeur tiers sur Amazon EC2 Reserved Instance Marketplace, s'il existe des offres similaires à votre choix mais à un prix initial inférieur, vous AWS vend les offres au prix initial le plus bas.

Avant de valider votre achat, vérifiez les détails des Instance réservées que vous avez l'intention d'acheter et veillez à ce que tous les paramètres soient exacts. Après avoir acheté une instance réservée (soit auprès d'un vendeur tiers sur le Reserved Instance Marketplace, soit auprès de AWS),

vous ne pouvez pas annuler votre achat. Vous pouvez mettre un achat en file d'attente pour une date future et annuler l'achat en attente avant l'heure prévue.

Pour acheter et modifier des instances réservées, assurez-vous que votre utilisateur dispose des autorisations appropriées, telles que la possibilité de décrire les zones de disponibilité. Pour plus d'informations, voir the section called "Utiliser instances réservées" (API) ou the section called "Utiliser instances réservées" (console).

Rubriques

Sélection d'une plateforme

Amazon EC2 prend en charge les plateformes suivantes pour les instances réservées :

- Linux/ UNIX
- Linux avec SQL Server Standard
- Linux avec SQL serveur Web
- Linux avec SQL Server Enterprise
- SUSELinux
- Utilisation de Red Hat Enterprise Linux
- Red Hat Enterprise Linux avec HA
- Windows
- Windows avec SQL Server Standard
- Windows avec SQL serveur Web
- Windows avec SQL Server Enterprise

Lorsque vous achetez une Instance réservée, vous devez choisir une offre pour une plateforme qui correspond au système d'exploitation de votre instance.

Instances Linux

- Pour SUSE Linux et les RHEL distributions, vous devez choisir des offres pour ces plateformes spécifiques, c'est-à-dire pour les plateformes SUSELinux ou Red Hat Enterprise Linux.
- Pour toutes les autres distributions Linux (y compris Ubuntu), choisissez une offre pour la plate-forme Linux/ UNIX.
- Si vous apportez votre RHEL abonnement existant, vous devez choisir une offre pour la UNIX plate-forme Linux/, et non une offre pour la plate-forme Red Hat Enterprise Linux.

instances Windows

- Pour Windows SQL Standard, Windows avec SQL Server Enterprise et Windows avec SQL Server Web, vous devez choisir des offres pour ces plateformes spécifiques.
- Pour toutes les autres versions Windows, choisissez une offre pour la plateforme Windows.

> **Note**
>
> Ubuntu Pro n'est pas disponible en tant qu'instance réservée. Pour réaliser des économies importantes par rapport à la tarification des instances à la demande, nous vous recommandons d'utiliser Ubuntu Pro avec Savings Plans. Pour plus d'informations, consultez le Guide de l'utilisateur des Savings Plans.

> **Important**
>
> Si vous envisagez d'acheter une instance réservée à appliquer à une instance à la demande lancée depuis un AWS Marketplace AMI, vérifiez d'abord le `PlatformDetails` champ duAMI. Le champ `PlatformDetails` indique quelle Instance réservée acheter. Les informations relatives à la plateforme AMI doivent correspondre à celles de l'instance réservée, sinon l'instance réservée ne sera pas appliquée à l'instance à la demande. Pour plus d'informations sur la façon de consulter les informations relatives à la plateformeAMI, consultezComprendre les informations de facturation d'AMI.

Mettre votre achat en file d'attente

Par défaut, lorsque vous achetez une Instance réservée, l'achat est effectué immédiatement. Vous pouvez également mettre vos achats en file d'attente pour une date et une heure futures. Par exemple, vous pouvez mettre un achat en file d'attente jusqu'à ce qu'une Instance réservée existante expire. Cela peut vous aider à garantir une couverture ininterrompue.

Vous pouvez mettre en file d'attente des achats pour une instances réservées régionale, mais pas pour une instances réservées de zone ou une instances réservées d'autres vendeurs. Vous pouvez mettre un achat en file d'attente jusqu'à trois ans en avance. À l'heure et la date prévues, l'achat est effectué à l'aide du mode de paiement par défaut. Une fois le paiement réussi, l'avantage de facturation est appliqué.

Vous pouvez définir une date pour vos achats en file d'attente dans la EC2 console Amazon, et l'achat est mis en file d'attente jusqu'à 00h00 UTC à cette date. Pour spécifier une autre heure pour l'achat en file d'attente, utilisez un outil de ligne de commande AWS SDK ou.

Vous pouvez consulter vos achats en file d'attente dans la console AmazonEC2. Le statut d'un achat mis en file d'attente est queued. Vous pouvez annuler un achat mis en file d'attente à tout moment avant son heure planifiée. Pour plus de détails, consultez Annuler un achat mis en file d'attente.

Acheter une instances réservées Standard

Vous pouvez acheter des instances réservées standard dans une zone de disponibilité spécifique et obtenir une réservation de capacité. Vous avez également la possibilité de renoncer à la réservation de capacité et d'acheter une Instance réservée standard régionale.

New console

Pour acheter des instances réservées standard à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances réservées, puis Acheter des Instances réservées.
3. Pour Offering class (Classe d'offre), sélectionnez Standard pour afficher les Instances réservées standard.
4. Pour acheter une réservation de capacité, basculez sur Only show offerings that reserve capacity (Ne montre que les offres réservant une capacité) dans le coin supérieur droit de l'écran d'achat. Lorsque vous basculez sur ce paramètre, le champ Availability Zone (Zone de disponibilité) apparaît.

Pour acheter une Instance réservée régionale, désactivez ce paramètre. Lorsque vous désactivez ce paramètre, le champ Availability Zone (Zone de disponibilité) disparaît.

5. Sélectionnez d'autres configurations en fonction de vos besoins, puis sélectionnez Search (Recherche).
6. Pour chaque Instance réservée que vous souhaitez acheter, saisissez la quantité désirée et sélectionnez Add to cart (Ajouter au panier).

   Pour acheter une instance réservée standard sur la marketplace des instances réservées, recherchez 3rd party (Tiers) dans la colonne Seller (Vendeur) des résultats de recherche. La colonne Durée affiche des durées non standard. Pour plus d'informations, consultez Acheter sur le Marketplace Instance réservée.
7. Pour afficher un récapitulatif des Instances réservées sélectionnées, sélectionnez View cart (Afficher le panier).
8. Si Order On (Commander le) correspond à Now (Maintenant), l'achat est terminé après que vous avez sélectionné Order all (Commander tout). Pour mettre un achat en file d'attente, choisissez Maintenant et sélectionnez une date. Vous pouvez sélectionner une date différente pour chaque offre éligible dans le panier. L'achat est mis en attente jusqu'à 00h00 à la UTC date sélectionnée.
9. Pour valider la commande, sélectionnez Order all (Commander tout).

   Si, au moment de passer la commande, il existe des offres similaires à votre choix mais à un prix inférieur, vous AWS vend les offres au prix inférieur.
10. Choisissez Fermer.

    L'état de votre commande figure dans la colonne État. Une fois votre commande terminée, la valeur État passe de `Payment-pending` à `Active`. Lorsque l'Instance réservée est `Active`, elle est prête à être utilisée.

> **Note**
>
> Si le statut passe à`Retired`, votre paiement n'a AWS peut-être pas été reçu.

Old console

Pour acheter des instances réservées standard à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances réservées, puis Acheter des Instances réservées.
3. Pour Offering class (Classe d'offre), sélectionnez Standard pour afficher les Instances réservées standard.
4. Pour acheter une réservation de capacité, choisissez Ne montre que les offres réservant une capacité dans le coin supérieur droit de l'écran d'achat. Pour acheter une Instance réservée régionale, laissez la case à cocher désactivée.
5. Sélectionnez d'autres configurations en fonction de vos besoins, puis choisissez Recherche.

   Pour acheter une instance réservée standard sur la marketplace des instances réservées, recherchez 3rd Party (Tiers) dans la colonne Seller (Vendeur) des résultats de recherche. La colonne Durée affiche des durées non standard.
6. Pour chaque Instance réservée que vous souhaitez acheter, saisissez la quantité et sélectionnez Add to Cart (Ajouter au panier).
7. Pour afficher un récapitulatif des Instances réservées sélectionnées, sélectionnez View cart (Afficher le panier).
8. Si Order On (Commander le) est Maintenant, l'achat est terminé immédiatement. Pour mettre un achat en file d'attente, choisissez Maintenant et sélectionnez une date. Vous pouvez sélectionner une date différente pour chaque offre éligible dans le panier. L'achat est mis en attente jusqu'à 00h00 à la UTC date sélectionnée.
9. Pour valider la commande, choisissez Order (Commander).

   Si, au moment de passer la commande, il existe des offres similaires à votre choix mais à un prix inférieur, vous AWS vend les offres au prix inférieur.
10. Choisissez Fermer.

    L'état de votre commande figure dans la colonne État. Une fois votre commande terminée, la valeur État passe de `payment-pending` à `active`. Lorsque l'Instance réservée est `active`, elle est prête à être utilisée.

> **Note**
>
> Si le statut passe à`retired`, votre paiement n'a AWS peut-être pas été reçu.

Pour acheter une instance réservée standard à l'aide du AWS CLI

1. Trouvez les instances réservées disponibles à l'aide de la describe-reserved-instances-offeringscommande. Spécifiez `standard` pour le paramètre `--offering-class` afin de renvoyer uniquement des Instances réservées standard. Vous pouvez appliquer des paramètres supplémentaires pour affiner vos résultats. Par exemple, si vous souhaitez acheter une Instance réservée `t2.large` régionale avec une location par défaut pour `Linux/UNIX` pour une durée d'un an seulement :

   ```
   aws ec2 describe-reserved-instances-offerings \
       --instance-type t2.large \
       --offering-class standard \
       --product-description "Linux/UNIX" \
       --instance-tenancy default \
       --filters Name=duration,Values=31536000 Name=scope,Values=Region
   ```

   Pour rechercher des instances réservées sur la marketplace des instances réservées uniquement, utilisez le filtre `marketplace` et ne spécifiez pas de durée dans la demande, puisque la durée peut être inférieure à 1 ou 3 ans.

   ```
   aws ec2 describe-reserved-instances-offerings \
       --instance-type t2.large \
       --offering-class standard \
       --product-description "Linux/UNIX" \
       --instance-tenancy default \
       --filters Name=marketplace,Values=true
   ```

   Lorsque vous trouvez une Instance réservée qui correspond à vos besoins, notez l'ID de l'offre. Par exemple :

   ```
   "ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
   ```

2. Utilisez la purchase-reserved-instances-offeringcommande pour acheter votre instance réservée. Vous devez spécifier l'ID d'offre d'Instance réservée que vous avez obtenu à l'étape précédente et indiquer le nombre d'instances pour la réservation.

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
    --instance-count 1
```

   Par défaut, l'achat est terminé immédiatement. Pour mettre l'achat en file d'attente, vous pouvez également ajouter le paramètre suivant à l'appel précédent.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Utilisez la describe-reserved-instancescommande pour obtenir le statut de votre instance réservée.

```
aws ec2 describe-reserved-instances
```

Vous pouvez également utiliser les AWS Tools for Windows PowerShell commandes suivantes :

- Get-EC2ReservedInstancesOffering
- New-EC2ReservedInstance
- Get-EC2ReservedInstance

Une fois l'achat terminé, si vous avez déjà une instance en cours d'exécution qui correspond aux attributs de l'Instance réservée, l'avantage de facturation est immédiatement appliqué. Vous n'avez pas besoin de redémarrer vos instances. Si vous n'avez pas d'instance en cours d'exécution adéquate, lancez une instance et veillez à respecter les mêmes critères que ceux spécifiés pour l'Instance réservée. Pour plus d'informations, consultez Utiliser votre instances réservées.

Pour des exemples de la façon dont les Instances réservées sont appliquées à vos instances en cours d'exécution, consultez Comment les remises sur les instances réservées sont appliquées.

Acheter instances réservées convertibles

Vous pouvez acheter des instances réservées convertibles dans une zone de disponibilité spécifique et obtenir une réservation de capacité. Vous avez également la possibilité de renoncer à la réservation de capacité et d'acheter une Instance réservée convertible régionale.

New console

Pour acheter des instances réservées convertibles à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances réservées, puis Acheter des Instances réservées.
3. Pour Offering class (Classe d'offre), sélectionnez Convertible pour afficher des Instances réservées convertibles.
4. Pour acheter une réservation de capacité, basculez sur Only show offerings that reserve capacity (Ne montre que les offres réservant une capacité) dans le coin supérieur droit de l'écran d'achat. Lorsque vous basculez sur ce paramètre, le champ Availability Zone (Zone de disponibilité) apparaît.

   Pour acheter une Instance réservée régionale, désactivez ce paramètre. Lorsque vous désactivez ce paramètre, le champ Availability Zone (Zone de disponibilité) disparaît.
5. Sélectionnez d'autres configurations en fonction de vos besoins, puis choisissez Recherche.
6. Pour chaque Instance réservée convertible que vous souhaitez acheter, saisissez la quantité et sélectionnez Add to cart (Ajouter au panier).
7. Pour afficher un résumé de votre sélection, sélectionnez View cart (Afficher le panier).
8. Si Order On (Commander le) correspond à Now (Maintenant), l'achat est terminé après que vous avez sélectionné Order all (Commander tout). Pour mettre un achat en file d'attente, choisissez Maintenant et sélectionnez une date. Vous pouvez sélectionner une date différente pour chaque offre éligible dans le panier. L'achat est mis en attente jusqu'à 00h00 à la UTC date sélectionnée.
9. Pour valider la commande, sélectionnez Order all (Commander tout).

   Si, au moment de passer la commande, il existe des offres similaires à votre choix mais à un prix inférieur, vous AWS vend les offres au prix inférieur.
10. Choisissez Fermer.

    L'état de votre commande figure dans la colonne État. Une fois votre commande terminée, la valeur État passe de `Payment-pending` à `Active`. Lorsque l'Instance réservée est `Active`, elle est prête à être utilisée.

> **Note**
>
> Si le statut passe à`Retired`, votre paiement n'a AWS peut-être pas été reçu.

Old console

Pour acheter des instances réservées convertibles à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances réservées, puis Acheter des Instances réservées.
3. Pour Offering class (Classe d'offre), sélectionnez Convertible pour afficher des Instances réservées convertibles.
4. Pour acheter une réservation de capacité, choisissez Ne montre que les offres réservant une capacité dans le coin supérieur droit de l'écran d'achat. Pour acheter une Instance réservée régionale, laissez la case à cocher désactivée.
5. Sélectionnez d'autres configurations en fonction de vos besoins, puis choisissez Recherche.
6. Pour chaque Instance réservée convertible que vous souhaitez acheter, saisissez la quantité et sélectionnez Add to Cart (Ajouter au panier).
7. Pour afficher un résumé de votre sélection, sélectionnez View cart (Afficher le panier).
8. Si Order On (Commander le) est Maintenant, l'achat est terminé immédiatement. Pour mettre un achat en file d'attente, choisissez Maintenant et sélectionnez une date. Vous pouvez sélectionner une date différente pour chaque offre éligible dans le panier. L'achat est mis en attente jusqu'à 00h00 à la UTC date sélectionnée.
9. Pour valider la commande, choisissez Order (Commander).

   Si, au moment de passer la commande, il existe des offres similaires à votre choix mais à un prix inférieur, vous AWS vend les offres au prix inférieur.
10. Choisissez Fermer.

    L'état de votre commande figure dans la colonne État. Une fois votre commande terminée, la valeur État passe de `payment-pending` à `active`. Lorsque l'Instance réservée est `active`, elle est prête à être utilisée.

> **Note**
>
> Si le statut passe à `retired`, votre paiement n'a AWS peut-être pas été reçu.

Pour acheter une instance réservée convertible à l'aide du AWS CLI

1. Trouvez les instances réservées disponibles à l'aide de la describe-reserved-instances-offeringscommande. Spécifiez `convertible` pour le paramètre `--offering-class` afin de renvoyer uniquement des Instances réservées convertibles. Vous pouvez appliquer des paramètres supplémentaires pour affiner vos résultats. Par exemple, si vous voulez acheter une Instance réservée `t2.large` régionale à location par défaut pour `Linux/UNIX` :

   ```
   aws ec2 describe-reserved-instances-offerings \
       --instance-type t2.large \
       --offering-class convertible \
       --product-description "Linux/UNIX" \
       --instance-tenancy default \
       --filters Name=scope,Values=Region
   ```

   Lorsque vous trouvez une Instance réservée qui correspond à vos besoins, notez l'ID de l'offre. Par exemple :

   ```
   "ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
   ```

2. Utilisez la purchase-reserved-instances-offeringcommande pour acheter votre instance réservée. Vous devez spécifier l'ID d'offre d'Instance réservée que vous avez obtenu à l'étape précédente et indiquer le nombre d'instances pour la réservation.

   ```
   aws ec2 purchase-reserved-instances-offering \
       --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
       --instance-count 1
   ```

   Par défaut, l'achat est terminé immédiatement. Pour mettre l'achat en file d'attente, vous pouvez également ajouter le paramètre suivant à l'appel précédent.

   ```
   --purchase-time "2020-12-01T00:00:00Z"
   ```

3. Utilisez la describe-reserved-instancescommande pour obtenir le statut de votre instance réservée.

```
aws ec2 describe-reserved-instances
```

Vous pouvez également utiliser les AWS Tools for Windows PowerShell commandes suivantes :

- Get-EC2ReservedInstancesOffering
- New-EC2ReservedInstance
- Get-EC2ReservedInstance

Si vous avez déjà une instance en cours d'exécution qui correspond aux attributs de l'Instance réservée, l'avantage de facturation est immédiatement appliqué. Vous n'avez pas besoin de redémarrer vos instances. Si vous n'avez pas d'instance en cours d'exécution adéquate, lancez une instance et veillez à respecter les mêmes critères que ceux spécifiés pour l'Instance réservée. Pour plus d'informations, consultez Utiliser votre instances réservées.

Pour des exemples de la façon dont les Instances réservées sont appliquées à vos instances en cours d'exécution, consultez Comment les remises sur les instances réservées sont appliquées.

Acheter sur le Marketplace Instance réservée

Vous pouvez acheter des instances réservées auprès de vendeurs tiers qui possèdent des instances réservées dont ils n'ont plus besoin sur la marketplace des instances réservées. Vous pouvez le faire à l'aide de la EC2 console Amazon ou d'un outil de ligne de commande. Le processus est similaire à l'achat d'instances réservées auprès de AWS. Pour de plus amples informations, veuillez consulter Acheter une instances réservées Standard.

Il existe quelques différences entre les instances réservées achetées sur le Reserved Instance Marketplace et les instances réservées achetées directement auprès de AWS :

- Durée – Les instances réservées que vous achetez auprès de tiers ont une durée inférieure à la durée standard complète. Conditions générales complètes à compter d' AWS une durée d'un an ou de trois ans.
- Prix initial – Les instances réservées tierces peuvent être vendues à différents prix initiaux. Les frais d'utilisation ou récurrents restent les mêmes que ceux déterminés lorsque les instances réservées ont été achetées initialement auprès d' AWS.

- Types d'instances réservées : seules les instances réservées Amazon EC2 Standard peuvent être achetées sur le Reserved Instance Marketplace. Les instances réservées convertiblesRDS, Amazon et Amazon ElastiCache ne sont pas disponibles à l'achat sur le Reserved Instance Marketplace.

Les informations de base vous concernant sont partagées avec le vendeur, par exemple votre ZIP code et les informations relatives à votre pays.

Ces informations permettent au vendeur de calculer toutes les taxes destinées au gouvernement qui sont susceptibles d'être appliquées aux transactions (par exemple, les taxes de vente ou la TVA). Elles sont communiquées sous la forme d'un rapport de décaissement. Dans de rares cas, vous devrez AWS peut-être fournir votre adresse e-mail au vendeur afin qu'il puisse vous contacter pour toute question relative à la vente (par exemple, des questions fiscales).

Pour des raisons similaires, AWS partage le nom de l'entité juridique du vendeur sur la facture d'achat de l'acheteur. Si vous avez besoin d'informations supplémentaires sur le vendeur pour des raisons fiscales ou autres, contactez AWS Support.

Afficher votre instances réservées

Vous pouvez consulter les instances réservées que vous avez achetées à l'aide de la EC2 console Amazon ou d'un outil de ligne de commande.

Pour afficher vos instances réservées sur la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances réservées.
3. Vos instances réservées mises en file d'attente, actives et mises hors service sont répertoriées. La colonne État indique l'état.
4. Si vous êtes vendeur sur la marketplace des instances réservées, l'onglet My Listings (Mes listes) indique le statut d'une réservation répertoriée sur la marketplace des instances réservées. Pour plus d'informations, consultez États de la liste des éléments Instance réservée.

Pour afficher vos instances réservées à l'aide de la ligne de commande

- describe-reserved-instances (AWS CLI)
- Get-EC2ReservedInstance(Outils pour Windows PowerShell)

Annuler un achat mis en file d'attente

Vous pouvez mettre un achat en file d'attente jusqu'à trois ans en avance. Vous pouvez annuler un achat mis en file d'attente à tout moment avant son heure planifiée.

Pour annuler un achat mis en file d'attente

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances réservées.
3. Sélectionnez une ou plusieurs instances réservées.
4. Sélectionnez Actions, Delete queued Reserved Instances (Supprimer les instances réservées mises en file d'attente).
5. Lorsque vous êtes invité à confirmer, sélectionnez Delete (Supprimer), puis sélectionnez Close (Fermer).

Pour annuler un achat en file d'attente à l'aide de la ligne de commande

- delete-queued-reserved-instances (AWS CLI)
- Remove-EC2QueuedReservedInstance(Outils pour Windows PowerShell)

Renouveler un Instance réservée

Vous pouvez renouveler une Instance réservée avant qu'elle n'entre en phase d'expiration. Le renouvellement d'une Instance réservée met en file d'attente l'achat d'une Instance réservée possédant la même configuration jusqu'à ce que l'Instance réservée actuelle expire.

Pour renouveler une instance réservée à l'aide d'un achat en file d'attente à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Reserved Instances (Instances réservées).
3. Sélectionnez l'instance réservée à renouveler.
4. Choisissez Actions, Renew Reserved Instances (Renouveler les instances réservées).
5. Pour valider la commande, sélectionnez Order all (Commander tout), puis Close (Fermer).

Vendez des instances réservées pour Amazon sur EC2 le Reserved Instance Marketplace

Amazon EC2 Reserved Instance Marketplace est une plateforme qui facilite la vente d'instances réservées standard non utilisées par des AWS clients et des vendeurs tiers. Ces instances réservées peuvent varier en termes de durée et d'options tarifaires. Vous souhaiterez peut-être vendre vos instances réservées lorsque vous n'en avez plus besoin, par exemple lorsque vous déplacez vos instances vers une nouvelle instance, que vous changez de type d'instance Région AWS, que vous terminez des projets avant l'expiration du terme des instances réservées, que les besoins de votre entreprise changent ou que vous avez une capacité excédentaire.

Dès que vous listez vos instances réservées sur la marketplace des instances réservées, elles deviennent disponibles et des acheteurs potentiels peuvent se les procurer. Toutes les instances réservées sont regroupées selon la durée de réservation restante et le taux horaire.

Pour répondre à la demande d'un acheteur d'acheter l'instance réservée d'un vendeur tiers via le Reserved Instance Marketplace, vendez d' AWS abord l'instance réservée au prix initial le plus bas dans le groupe spécifié. AWS Vend ensuite l'instance réservée au prix le plus bas suivant, jusqu'à ce que la totalité de la commande de l'acheteur soit exécutée. AWS traite ensuite les transactions et transfère la propriété des instances réservées à l'acheteur.

Vous êtes le propriétaire de l'Instance réservée jusqu'à ce qu'elle soit vendue. Une fois la vente conclue, vous ne disposez plus de la réservation de capacité et vous n'êtes plus soumis aux frais récurrents avec remise. Si vous continuez à utiliser votre instance, AWS vous facturera le tarif à la demande à partir du moment où l'instance réservée aura été vendue.

Si vous voulez vendre vos instances réservées inutilisées sur la marketplace des instances réservées, vous devez respecter certains critères d'éligibilité.

Pour plus d'informations sur l'achat d'instances réservées sur la marketplace des instances réservées, consultez Acheter sur le Marketplace Instance réservée.

Sommaire

- Lister votre instances réservées
- États de la liste des éléments Instance réservée
- Cycle de vie d'une liste
- Après la vente de votre Instance réservée
- Obtention du paiement
- Communication des informations à l'acheteur

Limites et restrictions

Avant de pouvoir vendre vos réservations inutilisées, vous devez vous inscrire en tant que vendeur sur la marketplace des instances réservées. Pour plus d'informations, consultez S'inscrire en tant que vendeur.

Les restrictions et restrictions suivantes s'appliquent à la vente d'instances réservées :

- Seules les instances réservées régionales et zonales Amazon EC2 Standard peuvent être vendues sur le Reserved Instance Marketplace.
- Les instances réservées EC2 convertibles Amazon ne peuvent pas être vendues sur le Reserved Instance Marketplace.
- Les instances réservées pour d'autres AWS services, tels qu'Amazon RDS et Amazon ElastiCache, ne peuvent pas être vendues sur le Reserved Instance Marketplace.
- L'Instance réservée standard doit être valable pendant encore au moins un mois.
- Vous ne pouvez pas vendre une instance réservée standard dans une région désactivée par défaut.
- Le tarif minimum autorisé sur la marketplace des instances réservées est de 0,00 USD.
- Vous pouvez vendre des instances réservées sans frais initiaux, avec frais initiaux partiels ou au paiement total anticipé sur le Marketplace des instances réservées, à condition qu'elles soient actives sur votre compte depuis au moins 30 jours. En outre, s'il y a un paiement initial sur une instance réservée, celle-ci ne peut être vendue AWS qu'après réception du paiement initial.
- Vous ne pouvez pas vendre une instance réservée sur le Reserved Instance Marketplace si vous l'avez achetée dans le cadre d'une réduction sur le volume.
- Vous ne pouvez pas modifier directement votre liste sur la marketplace des instances réservées. Toutefois, vous pouvez la changer en commençant par l'annuler, puis en créant une autre liste avec de nouveaux paramètres. Pour plus d'informations, consultez Définir le prix de votre instances

réservées. Vous pouvez également modifier vos instances réservées avant de les inclure dans votre liste. Pour plus d'informations, veuillez consulter Modifier instances réservées.

- AWS facture des frais de service de 12 % du prix initial total de chaque instance réservée standard que vous vendez sur le Reserved Instance Marketplace. Le prix initial correspond au prix demandé par le vendeur pour l'Instance réservée standard.
- Lorsque vous vous inscrivez en tant que vendeur, la banque que vous spécifiez doit avoir une adresse aux États-Unis. Pour plus d'informations, consultez Exigences supplémentaires du vendeur pour les produits payés dans le Guide du vendeur AWS Marketplace .
- Les clients d'Amazon Web Services India Private Limited (AWS Inde) ne peuvent pas vendre d'instances réservées sur le Reserved Instance Marketplace, même s'ils possèdent un compte bancaire américain. Pour plus d'informations, voir Quelles sont les différences entre les comptes AWS indiens Comptes AWS et les comptes indiens ?

S'inscrire en tant que vendeur

> **Note**
>
> Ils sont les seuls à Utilisateur racine d'un compte AWS pouvoir créer un compte en tant que vendeur.

Pour vendre sur la marketplace des instances réservées, vous devez tout d'abord vous inscrire comme vendeur. Lors de l'enregistrement, vous devez fournir les informations suivantes lors de l'enregistrement :

- Informations bancaires : vous AWS devez disposer de vos informations bancaires afin de décaisser les fonds collectés lorsque vous vendez vos réservations. La banque que vous spécifiez doit avoir une adresse aux États-Unis. Pour plus d'informations, consultez Compte bancaire pour les décaissements.
- Questionnaire fiscal : tous les vendeurs doivent répondre à un questionnaire fiscal afin de déterminer les obligations de déclaration fiscale éventuelles. Pour de plus amples informations, veuillez consulter Informations fiscales.

Après avoir AWS reçu votre inscription de vendeur terminée, vous recevez un e-mail confirmant votre inscription et vous informant que vous pouvez commencer à vendre sur le Reserved Instance Marketplace.

Compte bancaire pour les décaissements

AWS devez disposer de vos informations bancaires afin de débourser les fonds collectés lorsque vous vendez votre instance réservée. La banque que vous spécifiez doit avoir une adresse aux États-Unis. Pour plus d'informations, consultez Exigences supplémentaires du vendeur pour les produits payés dans le Guide du vendeur AWS Marketplace .

Pour enregistrer un compte par défaut destiné aux décaissements

1. Ouvrez la page Reserved Instance Marketplace Seller Registration (Inscription vendeur sur la marketplace des instances réservées) et connectez-vous à l'aide de vos informations d'identification AWS .
2. Sur la page Manage Bank Account (Gérer le compte bancaire), entrez les informations suivantes concernant la banque qui recevra vos paiements :

   - Nom du titulaire du compte bancaire
   - Code d'acheminement
   - Numéro de compte
   - Type de compte bancaire

   > **Note**
   >
   > Si vous utilisez le compte bancaire de votre société, vous êtes invité à envoyer les informations relatives au compte bancaire par télécopie au 1-206-765-3424.

Une fois l'enregistrement terminé, le compte bancaire spécifié est utilisé par défaut, dans l'attente d'une vérification auprès de la banque. Cette opération peut prendre jusqu'à deux semaines, une période au cours de laquelle vous ne pouvez pas recevoir de décaissements. Pour un compte établi, deux jours sont généralement nécessaires à l'exécution d'un décaissement.

Pour modifier le compte bancaire par défaut utilisé pour les décaissements

1. Sur la page Reserved Instance Marketplace Seller Registration (Inscription vendeur sur la marketplace des instances réservées), connectez-vous avec le compte utilisé pour l'inscription.
2. Sur la page Manage Bank Account (Gérer le compte bancaire), ajoutez un nouveau compte bancaire ou modifiez le compte défini par défaut.

Informations fiscales

Votre vente d'instances réservées peut être soumise à une taxe appliquée aux transactions, telle qu'une taxe de vente ou une TVA. Vérifiez auprès du service fiscal, juridique, financier ou comptable de votre entreprise afin de déterminer si des taxes sont applicables aux transactions concernées. Il vous incombe de collecter et d'envoyer les taxes applicables aux transactions à l'administration fiscale appropriée.

Dans le cadre du processus d'enregistrement du vendeur, vous devez remplir un questionnaire d'ordre fiscal dans le Seller Registration Portal. L'entretien recueille vos informations fiscales et remplit un IRS formulaire W-9, W-8 ou BEN W-8-EBEN, qui est utilisé pour déterminer les obligations de déclaration fiscale nécessaires.

Les informations fiscales que vous renseignez dans le questionnaire peuvent différer selon que vous œuvrez comme personne morale ou physique, et que votre entreprise est une entité ou personne américaine ou non. En remplissant ce questionnaire, gardez les points suivants à l'esprit :

- Les informations fournies par AWS, y compris les informations contenues dans cette rubrique, ne constituent pas des conseils fiscaux, juridiques ou autres conseils professionnels. Pour savoir comment les exigences en matière de IRS déclaration peuvent affecter votre entreprise, ou si vous avez d'autres questions, contactez votre conseiller fiscal, juridique ou autre conseiller professionnel.
- Pour répondre aux exigences en matière de IRS rapports le plus efficacement possible, répondez à toutes les questions et saisissez toutes les informations demandées lors de l'entretien.
- Vérifiez vos réponses. Évitez les fautes de frappe ou la saisie de numéros d'identification fiscale inexacts. Ces erreurs risqueraient d'entraîner le refus de votre formulaire fiscal.

Sur la base de vos réponses aux entretiens fiscaux et des seuils de IRS déclaration, Amazon peut déposer le formulaire 1099-K. Amazon envoie une copie de votre formulaire 1099-K par e-mail au plus tard le 31 janvier de l'année suivant l'année au cours de laquelle votre compte fiscal atteint les seuils. Par exemple, si votre compte fiscal atteint le seuil en 2018, vous recevrez le formulaire 1099-K le 31 janvier 2019 au plus tard.

Pour plus d'informations sur les IRS exigences et le formulaire 1099-K, consultez le IRSsite Web.

Définir le prix de votre instances réservées

Tenez compte des éléments suivants lorsque vous fixez le prix de vos instances réservées :

- Prix initial – Le prix initial est le seul prix que vous puissiez spécifier pour l'instance réservée que vous vendez. Le prix initial est le prix unique que l'acheteur paie lorsqu'il achète une instance réservée.

  Étant donné que la valeur des instances réservées diminue au fil du temps, AWS vous pouvez par défaut définir les prix pour qu'ils diminuent par tranches égales d'un mois à l'autre. Toutefois, vous pouvez définir des tarifs initiaux différents en fonction du moment de vente de votre réservation. Par exemple, si votre Instance réservée est encore valide pendant neuf mois, vous pouvez indiquer le montant que vous accepteriez si un client achetait cette Instance réservée au cours des neuf mois restants. Vous pouvez définir un autre prix avec cinq mois restants, et encore un autre avec un mois restant.

  Le tarif minimum autorisé sur la marketplace des instances réservées est de 0,00 USD.
- Limites – Les limites suivantes relatives pour la vente d'instances réservées s'appliquent à la durée de vie de votre Compte AWS. Il ne s'agit pas de limites annuelles.
  - Vous pouvez vendre jusqu'à 50 000 USD d'Instances réservées.
  - Vous pouvez vendre jusqu'à 5 000 Instances réservées.

  Ces limites ne peuvent généralement pas être augmentées, mais elles seront case-by-case évaluées sur demande. Pour demander une augmentation des limites, remplissez le formulaire de demande d'augmentation de limite de service. Pour Type de limite, choisissez EC2Reserved Instance Sales.
- Ne peut pas modifier – Vous ne pouvez pas modifier votre liste directement. Toutefois, vous pouvez la changer en commençant par l'annuler, puis en créant une autre liste avec de nouveaux paramètres.
- Peut annuler – Vous pouvez annuler votre liste à tout moment, tant qu'elle est dans l'état `active`. Vous ne pouvez pas annuler une liste si elle fait déjà l'objet d'une correspondance ou si sa vente est en cours de traitement. Si certaines instances de votre liste font l'objet d'une correspondance et que vous annulez la liste, seules les instances restantes qui ne font pas l'objet d'une correspondance sont supprimées de la liste.

Lister votre instances réservées

En tant que vendeur enregistré, vous pouvez choisir de vendre une ou plusieurs de vos instances réservées. Vous pouvez choisir de les vendre toutes sur une même liste ou par sections. En outre, vous pouvez ajouter à la liste les instances réservées avec n'importe quelle configuration de type d'instance, plateforme et portée.

La console détermine une suggestion de prix. Elle vérifie les offres qui correspondent à votre Instance réservée et sélectionne celle dont le prix est le plus bas. Sinon, elle calcule un prix suggéré basé sur le coût de l'Instance réservée pour le temps restant. Si la valeur calculée est inférieure à 1,01 USD, le prix suggéré est de 1,01 USD.

Si vous annulez votre liste et qu'une partie de celle-ci a déjà été vendue, l'annulation ne s'applique pas à la partie déjà vendue. Seule la partie de la liste non encore vendue n'est plus disponible sur la marketplace des instances réservées.

Pour répertorier une instance réservée sur le Reserved Instance Marketplace à l'aide du AWS Management Console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances réservées.
3. Sélectionnez les Instances réservées à répertorier, puis choisissez Actions, Vendre des Instances réservées.
4. Sur la page Configuration de votre liste d'Instance réservée définissez le nombre d'instances à vendre et le prix initial pour la durée restante dans les colonnes appropriées. Pour afficher l'évolution de la valeur de votre réservation au cours de la durée restante, sélectionnez la flèche en regard de la colonne Mois restant.
5. Si vous êtes un utilisateur avancé et que vous souhaitez personnaliser la tarification, vous pouvez entrer différentes valeurs pour les mois suivants. Pour revenir à la baisse de prix linéaire par défaut, choisissez Réinitialiser.
6. Choisissez Continuer une fois la configuration de la liste terminée.
7. Vérifiez les détails de votre liste sur la page Configuration de votre liste d'Instance réservée. Si vous n'avez rien à modifier, choisissez Répertorier l'instance réservée.

Pour afficher vos listes sur la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances réservées.
3. Sélectionnez l'Instance réservée que vous avez répertoriée et choisissez l'onglet Mes listes en bas de la page.

Pour gérer les instances réservées sur le Reserved Instance Marketplace à l'aide du AWS CLI

1. Obtenez la liste de vos instances réservées à l'aide de la describe-reserved-instancescommande.
2. Notez l'ID de l'instance réservée que vous souhaitez répertorier et appeler create-reserved-instances-listing. Vous devez spécifier l'ID de l'Instance réservée, le nombre d'instances et le barème de tarification.
3. Pour consulter votre annonce, utilisez la describe-reserved-instances-listingscommande.
4. Pour annuler votre annonce, utilisez la cancel-reserved-instances-listingscommande.

États de la liste des éléments Instance réservée

État de la liste de l'onglet Mes listes de la page des Instances réservées affiche le statut actuel de vos listes :

Les informations figurant dans Listing State (État de la liste) concernent l'état de votre liste sur la marketplace des instances réservées. Elles diffèrent des informations d'état affichées par la colonne État de la page Instances réservées. Ces informations d'État concernent votre réservation.

- active : la liste peut être achetée.
- canceled (annulée) : la liste a été annulée et ne peut plus être achetée sur la marketplace des instances réservées.
- closed (fermée) : l'Instance réservée figure pas sur la liste. Une Instance réservée peut être `closed` parce que la vente de la liste est terminée.

Cycle de vie d'une liste

Lorsque toutes les instances d'une liste correspondent aux besoins d'un acheteur et sont vendues, l'onglet Mes listes indique que votre Total instance count (Nombre total d'instances) correspond au nombre indiqué sous Vendue. Il n'y a plus aucune instance avec le statut Disponible pour votre liste dont le Statut est désormais `closed`.

Lorsqu'une partie seulement de votre annonce est vendue, AWS les instances réservées sont retirées de l'annonce et crée un nombre d'instances réservées égal au nombre d'instances réservées restant dans le décompte. Par conséquent, l'ID de liste et la liste qu'il représente, et qui a désormais moins de réservations en vente, restent actifs.

Toute vente ultérieure d'instances réservées figurant sur la liste est traitée de cette façon. Lorsque toutes les instances réservées de la liste sont vendues, AWS marque l'offre comme`closed`.

Par exemple, vous créez une liste ID de liste d'instances réservées 5ec28771-05ff-4b9b-aa31-9e57dexample. Cette liste comporte 5 instances.

L'onglet Mes listes de la page de console Instance réservée affiche la liste de cette façon :

ID de liste d'Instance réservée 5ec28771-05ff-4b9b-aa31-9e57dexample

- Total reservation count = 5
- Sold = 0
- Available = 5
- Status = active

Un acheteur achète deux de ces réservations, ce qui laisse trois réservations encore disponibles à la vente. En raison de cette vente partielle, AWS crée une nouvelle réservation avec un compte de trois pour représenter les réservations restantes encore en vente.

Voici comment votre liste apparaît sous l'onglet Mes listes :

ID de liste d'Instance réservée 5ec28771-05ff-4b9b-aa31-9e57dexample

- Total reservation count = 5
- Sold = 2
- Available = 3
- Status = active

Si vous annulez votre liste et qu'une partie de celle-ci a déjà été vendue, l'annulation ne s'applique pas à la partie déjà vendue. Seule la partie de la liste non encore vendue n'est plus disponible sur la marketplace des instances réservées.

Après la vente de votre Instance réservée

Lorsque votre instance réservée est vendue, vous AWS envoie une notification par e-mail. Vous êtes averti par e-mail de toutes les activités quotidiennes vous concernant. Les activités peuvent inclure la création ou la vente d'une annonce, ou l' AWS envoi de fonds sur votre compte.

Pour suivre le statut d'une liste d'Instance réservée dans la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances réservées.
3. Cliquez sur l'onglet Mes listes.

   L'onglet Mes listes contient la valeur État de la liste. Il contient aussi des informations sur la durée, le tarif et le nombre d'instances disponibles, en attente, vendues ou annulées.

Vous pouvez également utiliser la describe-reserved-instances-listingscommande avec le filtre approprié pour obtenir des informations sur vos annonces.

Obtention du paiement

Dès AWS réception des fonds de la part de l'acheteur, un message est envoyé à l'adresse e-mail du propriétaire enregistré pour l'instance réservée vendue.

AWS envoie un virement bancaire Automated Clearing House (ACH) sur le compte bancaire que vous avez indiqué. En règle générale, ce virement est effectué entre 1 à 3 jours après la vente de l'Instance réservée. Les décaissements se déroulent une fois par jour. Vous recevrez un e-mail avec un rapport de remboursement une fois que les fonds auront été débloqués. N'oubliez pas que vous ne pouvez pas recevoir de versements tant que vous n'avez pas AWS reçu de vérification de la part de votre banque. Cela peut prendre jusqu'à deux semaines.

L'Instance réservée que vous avez vendue continue à apparaître lorsque vous décrivez vos instances réservées.

Vous recevez un versement en espèces pour vos instances réservées par virement bancaire directement sur votre compte bancaire. AWS facture des frais de service de 12 % du prix initial total de chaque instance réservée que vous vendez sur le Reserved Instance Marketplace.

Communication des informations à l'acheteur

Lorsque vous vendez sur le Reserved Instance AWS Marketplace, indiquez le nom légal de votre entreprise sur la déclaration de l'acheteur conformément à la réglementation américaine. En outre, si l'acheteur appelle AWS Support parce qu'il a besoin de vous contacter au sujet d'une facture ou pour tout autre motif fiscal, AWS peut être amené à lui communiquer votre adresse e-mail afin qu'il puisse vous contacter directement.

Pour des raisons similaires, le ZIP code de l'acheteur et les informations relatives au pays sont fournis au vendeur dans le rapport de versement. En tant que vendeur, vous aurez parfois besoin de joindre ces informations aux taxes que vous remettez au gouvernement (par exemple, les taxes de vente ou la TVA) pour ces transactions.

AWS ne peut pas fournir de conseils fiscaux, mais si votre fiscaliste détermine que vous avez besoin d'informations supplémentaires spécifiques, contactez AWS Support.

Modifier instances réservées

Lorsque vos besoins évoluent, vous pouvez modifier vos instances réservées standards ou convertibles et continuer à bénéficier de votre avantage de facturation. Vous pouvez modifier des attributs tels que la zone de disponibilité, la taille d'instance (au sein de la même famille et génération d'instances) et la portée de votre instance réservée.

> **Note**
>
> Vous pouvez également échanger une Instance réservée convertible contre une autre Instance réservée convertible avec une configuration différente. Pour plus d'informations, consultez Échanger des instances réservées convertibles.

Vous pouvez modifier toutes vos instances réservées ou un sous-ensemble. Vous pouvez séparer les instances réservées initiales en deux nouvelles instances réservées ou plus. Par exemple, si vous avez une réservation pour 10 instances dans `us-east-1a` et que vous décidez de déplacer 5 instances vers `us-east-1b`, la demande de modification entraîne la création de deux réservations : une pour 5 instances dans `us-east-1a` et l'autre pour 5 instances dans `us-east-1b`.

Vous pouvez aussi fusionner deux Instances réservées ou plus dans une Instance réservée unique. Par exemple, si vous avez quatre Instances réservées `t2.small` d'une instance chacune, vous pouvez les fusionner pour créer une Instance réservée `t2.large`. Pour plus d'informations, consultez Prise en charge de la modification de tailles d'instances.

Après une modification, la tarification des instances réservées est appliquée uniquement aux instances qui correspondent aux nouveaux paramètres. Par exemple, si vous modifiez la zone de disponibilité d'une réservation, les avantages de réservation de capacité et de tarification sont appliqués automatiquement à l'utilisation d'instance dans la nouvelle zone de disponibilité. Les instances qui ne correspondent plus aux nouveaux paramètres sont facturées au taux à la demande à moins que votre compte n'ait d'autres réservations applicables.

Si votre demande de modification a été appliquée :

- La réservation modifiée devient effective immédiatement et l'avantage de tarification est appliqué aux nouvelles instances à partir de l'heure de la demande de modification. Par exemple, si vous avez modifié vos réservations à 21 h 15, l'avantage de tarification est appliqué à votre nouvelle instance à partir de 21 h 00. Vous pouvez obtenir la date d'entrée en vigueur des instances réservées modifiées à l'aide de la describe-reserved-instancescommande.
- La réservation initiale est mise hors service. Sa date de fin est la date de début de la nouvelle réservation et la date de fin de la nouvelle réservation est identique à la date de fin de l'Instance réservée initiale. Si vous modifiez une réservation d'une durée de trois ans avec 16 mois restants, la réservation modifiée a une durée de 16 mois, avec la même date de fin que la réservation initiale.
- La réservation modifiée indique un tarif fixe s'élevant à 0 USD et non le tarif fixe de la réservation initiale.
- Le tarif fixe de la réservation modifiée n'a aucune répercussion sur les calculs du niveau tarifaire avec remise appliqué à votre compte. Ces calculs reposent en effet sur le tarif fixe de la réservation initiale.

Si votre demande de modification échoue, vos instances réservées conservent leur configuration d'origine et sont immédiatement disponibles pour une autre demande de modification.

Il n'y a aucun frais pour les modifications et vous ne recevez pas de nouvelles factures.

Vous pouvez modifier vos réservations aussi souvent que vous le souhaitez. Toutefois, vous ne pouvez pas modifier ou annuler une demande de modification en attente une fois que vous l'avez envoyée. Une fois la modification appliquée, vous pouvez envoyer une autre demande de modification afin d'annuler des modifications précédentes, si nécessaire.

Sommaire

Conditions obligatoires et restrictions pour toute modification

Vous pouvez modifier ces attributs comme suit.

Attribut modifiable	Plateformes prises en charge	Limites et considérations
Changer de zones de disponibilité au sein de la même région	Linux et Windows	-
Modifier la portée pour passer de Zone de disponibilité à Région et inversement	Linux et Windows	Une instance réservée zonale est étendue à une zone de disponibilité et réserve la capacité dans cette zone de disponibilité. Si vous modifiez la portée de Zone de disponibilité à Région (en d'autres termes, de zonal à régional), vous ne bénéficiez plus de l'avantage de réserve de capacité. Une instance réservée régionale a une portée sur une région. Votre remise d'instance réservée peut s'appliquer aux instances exécutées dans n'importe quelle zone de disponibilité de cette Région. En outre, la remise d'instance réservée s'applique à l'utilisation d'instance de toutes les tailles de la famille d'instances sélectionnée. Si vous modifiez la portée de Région à Zone de disponibilité (en d'autres

Attribut modifiable	Plateformes prises en charge	Limites et considérations
		termes, de régional à zonal), vous perdez la flexibilité de la Zone de disponibilité et la flexibilité de la taille de l'instance (le cas échéant). Pour de plus amples informations, veuillez consulter Comment les remises sur les instances réservées sont appliquées.
Modification de la taille d'instance au sein de la même famille et génération d'instances	Linux/ uniquement UNIX La flexibilité de taille d'instance n'est pas disponible pour les instances réservées sur les autres plateformes, notamment Linux avec SQL Server Standard, Linux avec SQL Server Web, Linux avec SQL Server Enterprise, Red Hat Enterprise Linux, SUSE Linux, Windows, Windows, Windows avec SQL Standard, Windows avec SQL Server Enterprise et Windows avec SQL Server Web.	La réservation doit utiliser la location par défaut. Certaines familles d'instances ne sont pas prises en charge dans la mesure où aucune autre taille n'est disponible. Pour plus d'informations, consultez Prise en charge de la modification de tailles d'instances.

Prérequis

Amazon EC2 traite votre demande de modification si la capacité est suffisante pour votre nouvelle configuration (le cas échéant) et si les conditions suivantes sont remplies :

- Vous ne pouvez pas modifier la Instance réservée avant ou au moment même de son achat.

- La Instance réservée doit être active.
- Il ne peut pas y avoir de demande de modification en attente
- L'instance réservée n'est pas listée sur la marketplace des instances réservées.
- Il doit y avoir une correspondance entre la couverture de la taille de l'instance associée à la réservation initiale et la configuration cible. Pour plus d'informations, consultez Prise en charge de la modification de tailles d'instances.
- Les instances réservées d'origine sont toutes des instances réservées standard ou des instances réservées convertibles, non pas quelques-unes de chaque sorte.
- Les instances réservées d'origine doivent expirer dans la même heure si ce sont des instances réservées standard.
- L'instance réservée doit prendre en charge la flexibilité de la taille de l'instance. Pour obtenir la liste des instances réservées qui ne prennent pas en charge la flexibilité de taille d'instance, consultezFlexibilité de la taille de l'instance.

Prise en charge de la modification de tailles d'instances

Vous pouvez modifier la taille d'instance d'une Instance réservée si les conditions suivantes sont remplies.

Prérequis

- La plateforme est Linux/UNIX.
- Vous devez sélectionner une autre taille d'instance au sein de la même famille d'instances (indiquée par une lettre, par exemple T) et la même génération (indiquée par un chiffre, par exemple 2).

  Par exemple, vous pouvez modifier une instance réservée de `t2.small` à `t2.large` parce qu'elles appartiennent toutes deux à la même famille et génération T2. Cependant, vous ne pouvez pas modifier une instance réservée de T2 à M2 ou de T2 à T3, car dans ces deux exemples, la famille et la génération d'instance cible ne sont pas les mêmes que celles de l'instance réservée d'origine.
- Vous pouvez modifier la taille d'instance d'une instance réservée uniquement si elle permet une flexibilité de taille d'instance. Pour obtenir la liste des instances réservées qui ne prennent pas en charge la flexibilité de taille d'instance, consultezFlexibilité de la taille de l'instance.
- Vous ne pouvez pas modifier la taille des instances réservées pour les `t1.micro` instances, car elles n'`t1.micro`ont qu'une seule taille.

- Les Instance réservée nouvelle et d'origine doivent avoir la même couverture de taille d'instance.

Sommaire

Couverture de taille d'instance

Chaque Instance réservée a une couverture de taille d'instance qui est déterminée par le facteur de normalisation de taille d'instance et par le nombre d'instances dans la réservation. Lorsque vous modifiez les tailles des instances dans une Instance réservée, la couverture de la nouvelle configuration doit correspondre à celle de la configuration d'origine, sinon la demande de modification n'est pas traitée.

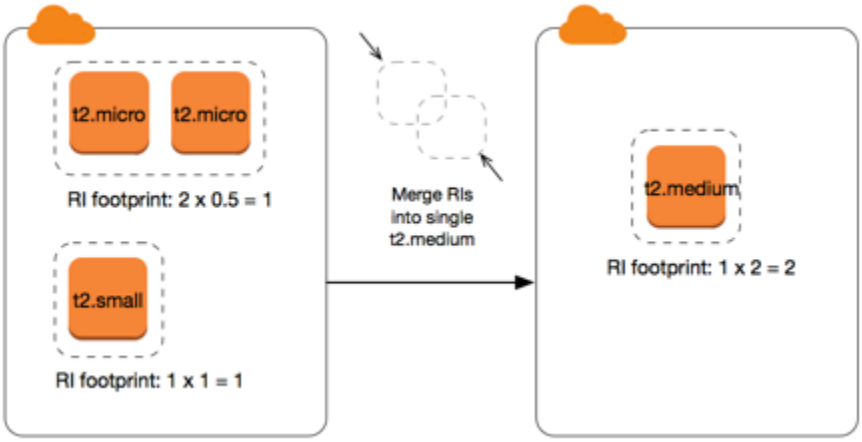
Pour calculer la couverture de la taille d'une Instance réservée, multipliez le nombre d'instances par le facteur de normalisation. Dans la EC2 console Amazon, le facteur de normalisation est mesuré en unités. Le tableau suivant décrit le facteur de normalisation pour les tailles d'instance dans une famille d'instances. Par exemple, une instance `t2.medium` dispose d'un facteur de normalisation de 2, ce qui implique qu'une réservation de 4 instances `t2.medium` dispose d'une couverture de 8 unités.

Taille d'instance	Facteur de normalisation
nano	0.25
micro	0.5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24

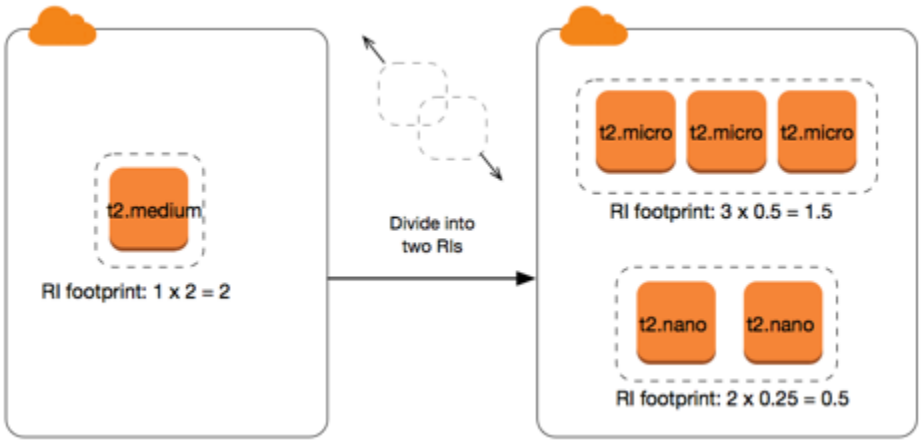
Taille d'instance	Facteur de normalisation
4xlarge	32
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256
48xlarge	384
56xlarge	448
112xlarge	896

Vous pouvez allouer vos réservations en utilisant différentes tailles d'instance sur la même famille de·l'instance tant que la couverture de taille d'instance de votre réservation reste la même. Par exemple, vous pouvez diviser une réservation pour une instance `t2.large` (1 @ 4 unités) en quatre instances `t2.small` (4 @ 1 unité). De même, vous pouvez combiner une réservation pour quatre instances `t2.small` en une seule instance `t2.large`. Toutefois, vous ne pouvez pas remplacer votre réservation de deux instances `t2.small` par une seule instance `t2.large`, car la couverture de la nouvelle réservation (4 unités) est plus grande que celle de la réservation d'origine (2 unités).

Dans l'exemple suivant, vous avez une réservation avec deux instances `t2.micro` (1 unité) et une réservation avec une instance `t2.small` (1 unité). Si vous fusionnez ces deux réservations en une seule avec une instance `t2.medium` (2 unités), la couverture de la nouvelle réservation est égale à la couverture des réservations combinées.



Vous pouvez aussi modifier une réservation pour la diviser en deux réservations ou plus. Dans l'exemple suivant, vous disposez d'une réservation avec une instance `t2.medium` (2 unités). Vous pouvez diviser la réservation en deux, l'une avec deux instances `t2.nano` (0,5 unités) et l'autre avec trois instances `t2.micro` (1,5 unité).



Facteur de normalisation pour les instances à matériel nu

Vous pouvez modifier une réservation avec des instances `metal` en utilisant d'autres tailles au sein de la même famille d'instances. De même, vous pouvez modifier une réservation avec des instances autres que des instances à matériel nu en utilisant la taille `metal` de la même famille d'instances. Généralement, une instance à matériel nu a la même taille que la plus grande taille d'instance disponible au sein de la même famille d'instances. Par exemple, une instance `i3.metal` a la même taille qu'une instance `i3.16xlarge`, de sorte qu'elles ont le même facteur de normalisation.

Le tableau suivant décrit le facteur de normalisation pour les tailles d'instance à matériel nu dans les familles d'instances qui ont des instances à matériel nu. Le facteur de normalisation des instances `metal` dépend de la famille d'instances, contrairement aux autres tailles d'instance.

Taille d'instance	Facteur de normalisation
a1.metal	32
m5zn.metal | x2iezn.metal z1d.metal	96
c6g.metal | c6gd.metal | i3.metal | m6g.metal | m6gd.metal | r6g.metal | r6gd.metal | x2gd.metal	128
c5n.metal	144
c5.metal | c5d.metal | i3en.metal | m5.metal | m5d.metal | m5dn.metal | m5n.metal | r5.metal | r5b.metal | r5d.metal | r5dn.metal | r5n.metal	192
c6i.metal | c6id.metal | m6i.metal | m6id.metal | r6d.metal | r6id.metal	256
u-*.metal	896

Par exemple, une instance `i3.metal` dispose d'un facteur de normalisation de 128. Si vous achetez une Instance réservée Amazon Linux/Unix à location par défaut `i3.metal`, vous pouvez diviser la réservation comme suit :

- Une `i3.16xlarge` fait toujours la même taille qu'une instance `i3.metal`. Il dispose donc d'un facteur de normalisation de 128 (128/1). La réservation pour une instance `i3.metal` peut être modifiée en une instance `i3.16xlarge`.
- Une `i3.8xlarge` fait toujours la moitié de la taille d'une instance `i3.metal`. Il dispose donc d'un facteur de normalisation de 64 (128/2). La réservation pour une instance `i3.metal` peut être divisée en deux instances `i3.8xlarge`.
- Une `i3.4xlarge` fait toujours le quart de la taille d'une instance `i3.metal`. Il dispose donc d'un facteur de normalisation de 32 (128/4). La réservation pour une instance `i3.metal` peut être divisée en quatre instances `i3.4xlarge`.

Soumettre des demandes de modification

Avant de modifier vos instances réservées, assurez-vous d'avoir lu les restrictions applicables. Avant de modifier la taille de l'instance, calculez la taille d'instance totale des réservations d'origine que vous souhaitez modifier et assurez-vous qu'elle correspond à la taille d'instance totale de vos nouvelles configurations.

Pour modifier vos instances réservées à l'aide du AWS Management Console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Sur la page Instances réservées, sélectionnez une ou plusieurs Instances réservées à modifier, puis choisissez Actions, Modifier des instances réservées.

   > **Note**
   >
   > Si vos Instances réservées ne sont pas actives ou si elles ne peuvent pas être modifiées, Modifier des Instances réservées est désactivé.

3. La première entrée du tableau de modification indique les attributs des instances réservées sélectionnées, et au moins une configuration cible en dessous. La colonne Unités indique la couverture de taille d'instance totale. Choisissez Ajouter pour chaque nouvelle configuration à ajouter. Modifiez les attributs de chaque configuration selon vos besoins.

   - Portée : indiquez si la configuration s'applique à une zone de disponibilité ou à l'ensemble de la région.
   - Zone de disponibilité : choisissez la zone de disponibilité requise. Ne s'applique pas aux instances réservées régionales.
   - Type d'instance : sélectionnez le type d'instance requis. Les configurations combinées doivent être égales à la couverture de taille d'instance de vos configurations d'origine.
   - Nombre : spécifiez le nombre d'instances. Pour fractionner les Instances réservées en plusieurs configurations, réduisez leur nombre, choisissez Ajouter et spécifiez un nombre pour la configuration supplémentaire. Par exemple, si vous disposez d'une configuration unique comportant 10 instances réservées, vous pouvez redéfinir ce nombre sur 6 et ajouter une configuration avec un nombre de 4. Ce processus supprime l'Instance réservée d'origine une fois les nouvelles instances réservées activées.

4. Choisissez Continue.

5. Pour valider vos choix de modification une fois que vous avez terminé la définition des configurations cibles, sélectionnez Submit modifications (Soumettre des modifications).
6. Vous pouvez consulter l'état de votre demande de modification en observant la colonne État de l'écran des Instances réservées. Les états possibles sont les suivants :

   - active (en attente de modification) : État de transition pour les Instances réservées initiales
   - hors service (en attente de modification) : État de transition pour les Instances réservées initiales pendant que les nouvelles Instances réservées sont créées
   - hors service : Instances réservées modifiées et remplacées avec succès.
   - active : L'un des statuts suivants :
     - Nouvelles instances réservées créées à la suite d'une demande de modification
     - instances réservées initiales après l'échec d'une demande de modification

Pour modifier vos instances réservées à l'aide de la ligne de commande

1. Pour modifier vos instances réservées, vous pouvez utiliser l'une des commandes suivantes :
   - modify-reserved-instances (AWS CLI)
   - Edit-EC2ReservedInstance (AWS Tools for Windows PowerShell)
2. Pour obtenir le statut de votre demande modification (`processing`, `fulfilled` ou `failed`), utilisez une des commandes suivantes :
   - describe-reserved-instances-modifications (AWS CLI)
   - Get-EC2ReservedInstancesModification (AWS Tools for Windows PowerShell)

Résoudre les problèmes liés aux demandes de modification

Si les paramètres que vous avez demandés pour la configuration cible sont uniques, vous recevez un message indiquant que votre demande est en cours de traitement. À ce stade, Amazon EC2 a uniquement déterminé que les paramètres de votre demande de modification sont valides. Votre demande de modification peut encore échouer au cours du traitement si la capacité nécessaire n'est pas disponible.

Dans certains cas, vous ne recevrez pas de confirmation, mais un message indiquant que la demande de modification a échoué ou est incomplète. Utilisez les informations de ces messages comme point de départ pour soumettre une nouvelle demande de modification. Veillez à lire les restrictions applicables avant d'envoyer la demande.

Certaines instances réservées sélectionnées ne peuvent pas faire l'objet d'une modification

Amazon EC2 identifie et répertorie les instances réservées qui ne peuvent pas être modifiées. Si vous recevez un tel message, rendez-vous sur la page des instances réservées de la EC2 console Amazon et vérifiez les informations relatives aux instances réservées.

Erreur lors du traitement de votre demande de modification

Vous avez demandé la modification d'une ou de plusieurs instances réservées, mais aucune de ces demandes ne peut être traitée. Selon le nombre de réservations que vous modifiez, vous pouvez obtenir différentes versions de ce message.

Amazon EC2 indique les raisons pour lesquelles votre demande ne peut pas être traitée. Par exemple, vous pouvez avoir spécifié la même configuration cible (une combinaison de zone de disponibilité et de plateforme) pour une ou plusieurs parties des instances réservées que vous modifiez. Essayez de soumettre à nouveau les demandes de modification, mais veillez à ce que les détails d'instance des réservations soient corrects et à ce que les configurations cibles pour toutes les parties modifiées soient uniques.

Échanger des instances réservées convertibles

Vous pouvez échanger une ou plusieurs instances réservées convertibles contre une autre Instance réservée convertible avec une configuration différente, y compris la famille de·l'instance, le système d'exploitation et la location. Il n'y a pas de limite au nombre d'échanges que vous pouvez effectuer, tant que l'Instance réservée convertible nouvelle est de valeur égale ou plus élevée que les instances réservées convertibles que vous échangez.

Lorsque vous échangez votre instance réservée convertible, le nombre d'instances de votre réservation actuelle est remplacé par un nombre d'instances qui couvre une valeur égale ou supérieure à celle de la configuration de la nouvelle instance réservée convertible. Amazon EC2 calcule le nombre d'instances réservées que vous pouvez recevoir à la suite de l'échange.

Vous ne pouvez pas échanger d'instances réservées standard, mais vous pouvez les modifier. Pour plus d'informations, consultez Modifier instances réservées.

Sommaire

- Échanger une partie d'une Instance réservée convertible
- Soumettre des demandes d'échange

Exigences pour l'échange d'instances réservées convertibles

Si les conditions suivantes sont remplies, Amazon EC2 traite votre demande d'échange. Votre Instance réservée convertible doit être :

- Actif
- Libre de toute demande d'échange précédente
- Il doit rester au moins 24 heures avant son expiration

Les règles suivantes s'appliquent :

- Les instances réservées convertibles ne peuvent être échangées que contre d'autres instances réservées convertibles actuellement proposées par AWS.
- Les instances réservées convertibles sont associées à une région spécifique, qui reste la même pendant la durée de la période de réservation. Vous ne pouvez pas échanger une Instance réservée convertible par une Instance réservée convertible d'une autre région.
- Vous pouvez échanger une ou plusieurs instances réservées convertibles à la fois contre une seule Instance réservée convertible.
- Pour échanger une partie d'une Instance réservée convertible, vous pouvez la modifier en deux réservations ou plus, avant d'en échanger une ou plusieurs contre une nouvelle Instance réservée convertible. Pour plus d'informations, consultez Échanger une partie d'une Instance réservée convertible. Pour plus d'informations sur la modification de vos Instances réservées, consultez Modifier instances réservées.
- Les instances réservées convertibles avec tous les frais initiaux peuvent être échangées contre des instances réservées convertibles avec frais initiaux partiels, et inversement.

> **Note**
>
> Si le paiement initial total requis pour l'échange (coût d'ajustement) est inférieur à 0,00 USD, vous obtenez AWS automatiquement un nombre d'instances dans l'instance réservée convertible qui garantit que le coût d'ajustement est égal ou supérieur à 0,00 USD.

> **Note**
>
> Si la valeur totale (prix initial + prix horaire* nombre d'heures restantes) de la nouvelle instance réservée convertible est inférieure à la valeur totale de l'instance réservée convertible échangée, vous obtenez AWS automatiquement une quantité d'instances dans l'instance réservée convertible qui garantit que la valeur totale est égale ou supérieure à celle de l'instance réservée convertible échangée.

- Pour bénéficier d'un meilleur tarif, vous pouvez échanger une Instance réservée convertible sans paiement initial pour une Instance réservée convertible avec tous les frais totaux ou avec frais initiaux partiels.
- Vous ne pouvez pas échanger de instances réservées convertibles avec tous les frais initiaux ou avec frais initiaux partiels contre des instances réservées convertibles. sans frais initiaux.
- Vous pouvez échanger une Instance réservée convertible sans frais initiaux pour une autre Instance réservée convertible sans frais initiaux uniquement si le tarif horaire de la nouvelle Instance réservée convertible est égal ou supérieur au prix horaire de la Instance réservée convertible échangée.

> **Note**
>
> Si la valeur totale (prix horaire * nombre d'heures restantes) de la nouvelle Instance réservée convertible est inférieure à la valeur totale de la Instance réservée convertible échangée, AWS vous attribue automatiquement une quantité d'instances parmi les instances réservées convertibles qui garantit que la valeur totale est égale ou supérieure à celle de l'instance réservée convertible échangée.

- Si vous échangez plusieurs instances réservées convertibles avec différentes dates d'expiration, la date d'expiration de la nouvelle instance réservée convertible est la plus lointaine dans le futur.
- Si vous échangez une Instance réservée convertible unique, elle doit avoir la même durée que la nouvelle Instance réservée convertible (1 an ou 3 ans). Si vous fusionnez plusieurs instances réservées convertibles avec différentes durées, la nouvelle Instance réservée convertible aura une durée de 3 ans. Pour de plus amples informations, veuillez consulter Fusionner des instances réservées convertibles.
- Lorsqu'Amazon EC2 échange une instance réservée convertible, il retire la réservation associée et transfère la date de fin à la nouvelle réservation. Après l'échange, Amazon EC2 fixe à la fois

la date de fin de l'ancienne réservation et la date de début de la nouvelle réservation à la date de l'échange. Par exemple, si vous échangez une réservation d'une durée de trois ans avec 16 mois restants, la nouvelle réservation a une durée de 16 mois, avec la même date de fin que la réservation de l'instance réservée convertible que vous avez échangée.

Calculer des échanges d'instances réservées convertibles

L'échange de instances réservées convertibles est gratuit. Toutefois, vous pouvez être tenu de payer des frais de régularisation calculés au prorata du paiement comptant de la différence entre les instances réservées convertibles que vous aviez et les nouvelles instances réservées convertibles que vous recevez de l'échange.

Chaque Instance réservée convertible dispose d'une liste de valeurs. Cette valeur de liste est comparée à la valeur de liste des instances réservées convertibles que vous voulez pour déterminer combien de réservations d'instances vous pouvez recevoir de l'échange.

Par exemple : vous avez une Instance réservée convertible avec une valeur de liste de 35 $ que vous voulez échanger contre un nouveau type d'instance avec une valeur de liste de 10 USD.

```
$35/$10 = 3.5
```

Vous pouvez échanger votre Instance réservée convertible contre trois instances réservées convertibles de 10 USD. Étant donné qu'il n'est pas possible d'acheter des moitiés de réservation, vous devez acheter une Instance réservée convertible supplémentaire pour couvrir le reste :

```
3.5 = 3 whole Convertible Reserved Instances + 1 additional Convertible Reserved
 Instance
```

La quatrième Instance réservée convertible a la même date de fin que les trois autres. Vous payez la régularisation correspondant à la quatrième réservation si vous échangez des instances réservées convertibles à paiement initial partiel ou comptant. Si le reste du paiement en amont de vos instances réservées convertibles est de 500 USD et que la nouvelle réservation coûterait normalement 600 USD au prorata, vous êtes facturé 100 USD.

```
$600 prorated upfront cost of new reservations - $500 remaining upfront cost of old
 reservations = $100 difference
```

Fusionner des instances réservées convertibles

Si vous fusionnez deux instances réservées convertibles ou plus, le terme de l'instance réservée convertible obtenue doit être le même que celui des instances réservées convertibles ou celui de la plus grande des instances réservées convertibles. La date d'expiration de la nouvelle Instance réservée convertible est la plus lointaine dans le futur.

Par exemple, si vous possédez les instances réservées convertibles suivantes sur votre compte :

ID Instance réservée	Durée	Date d'expiration
aaaa1111	1 an	31-12-2018
bbbb2222	1 an	31-07-2018
cccc3333	3 ans	30-06-2018
dddd4444	3 ans	31-12-2019

- Vous pouvez fusionner `aaaa1111` et `bbbb2222` et les échanger contre une Instance réservée convertible valable 1 an. Vous ne pouvez pas les échanger contre une Instance réservée convertible valable trois ans. La date d'expiration de la nouvelle Instance réservée convertible est 2018-12-31.
- Vous pouvez fusionner `bbbb2222` et `cccc3333` et les échanger contre une Instance réservée convertible valable 3 ans. Vous ne pouvez pas les échanger contre une Instance réservée convertible valable un an. La date d'expiration de la nouvelle Instance réservée convertible est 2018-07-31.
- Vous pouvez fusionner `cccc3333` et `dddd4444` et les échanger contre une Instance réservée convertible valable 3 ans. Vous ne pouvez pas les échanger contre une Instance réservée convertible valable un an. La date d'expiration de la nouvelle Instance réservée convertible est 2019-12-31.

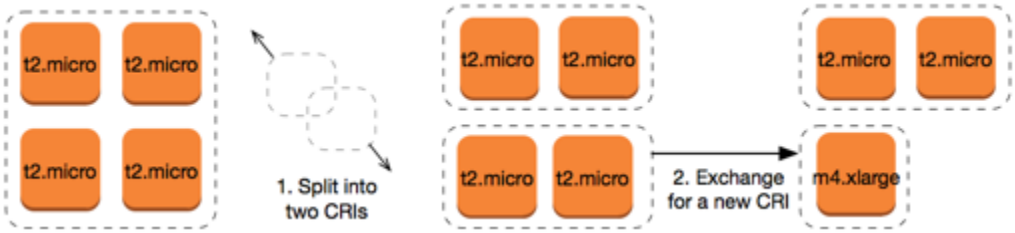
Échanger une partie d'une Instance réservée convertible

Vous pouvez utiliser le processus de modification pour diviser votre Instance réservée convertible en plus petites réservations, avant d'en échanger une ou plusieurs contre une nouvelle Instance réservée convertible. Les exemples suivant montrent comment procéder.

Example Exemple : Instance réservée convertible avec plusieurs instances

Dans cet exemple, vous disposez d'une Instance réservée convertible `t2.micro` avec quatre instances dans la réservation. Pour échanger deux instances `t2.micro` contre une instance `m4.xlarge` :

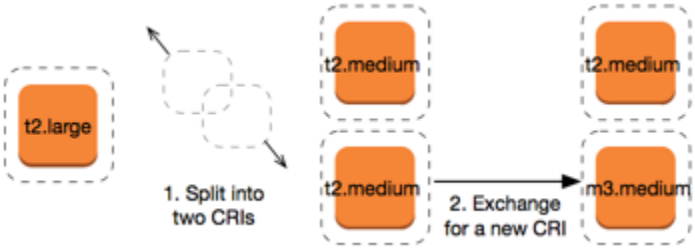
1. Modifiez la Instance réservée convertible `t2.micro` en la divisant en deux Instances réservées convertibles `t2.micro` avec deux instances chacune.
2. Échangez l'une des nouvelles Instances réservées convertibles `t2.micro` obtenues contre une Instance réservée convertible `m4.xlarge`.



Example Exemple : Instance réservée convertible avec une seule instance

Dans cet exemple, vous disposez d'une `t2.large` Instance réservée convertible. Pour la changer en une instance `t2.medium` plus petite et une instance `m3.medium` :

1. Modifiez l'Instance réservée convertible `t2.large` en la divisant en deux Instances réservées convertibles `t2.medium`. Une seule instance `t2.large` a la même couverture de taille d'instance que les deux instances `t2.medium`.
2. Échangez l'une des nouvelles Instances réservées convertibles `t2.medium` obtenues contre une Instance réservée convertible `m3.medium`.



Pour plus d'informations, consultez Prise en charge de la modification de tailles d'instances et Soumettre des demandes d'échange.

Soumettre des demandes d'échange

Vous pouvez échanger vos instances réservées convertibles à l'aide de la EC2 console Amazon ou d'un outil de ligne de commande.

Échanger une Instance réservée convertible à l'aide de la console

Vous pouvez rechercher des offres de instances réservées convertibles et sélectionner votre nouvelle configuration parmi les choix fournis.

Pour échanger des instances réservées convertibles à l'aide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Choisissez Instances réservées, sélectionnez les Instances réservées convertibles à échanger, puis choisissez Actions, Échange de l'Instance réservée.
3. Sélectionnez les attributs de la configuration souhaitée et sélectionnez Find offering (Trouver une offre).
4. Sélectionnez une nouvelle Instance réservée convertible. En bas de l'écran, vous pouvez consulter le nombre de instances réservées que vous recevez pour l'échange, ainsi que les éventuels coûts supplémentaires.
5. Lorsque vous avez sélectionné une Instance réservée convertible qui répond à vos besoins, sélectionnez Review (Vérifier).
6. Sélectionnez Exchange (Échange), puis Close (Fermer).

Les instances réservées qui ont été échangées sont retirées et les nouvelles instances réservées sont affichées dans la EC2 console Amazon. Ce processus peut prendre quelques minutes pour se propager.

Échanger une instance réservée convertible à l'aide de l'interface de la ligne de commande

Pour échanger une Instance réservée convertible, commencez par rechercher une nouvelle Instance réservée convertible qui répond à vos besoins :

- describe-reserved-instances-offerings (AWS CLI)
- Get-EC2ReservedInstancesOffering(Outils pour Windows PowerShell)

Obtenez un devis pour l'échange, qui inclut le nombre de instances réservées que vous obtenez lors de l'échange et les frais de régularisation pour l'échange :

- get-reserved-instances-exchange-citation ()AWS CLI
- Obtenir EC2 - ReservedInstancesExchangeQuote (Outils pour Windows PowerShell)

Enfin, effectuez l'échange :

- accept-reserved-instances-exchange-citation ()AWS CLI
- Approve-EC2ReservedInstancesExchangeQuote(Outils pour Windows PowerShell)

Quotas d'instances réservées

Vous pouvez acheter de nouvelles instances réservées chaque mois. Le nombre de nouvelles instances réservées que vous pouvez acheter chaque mois est déterminé par votre quota mensuel, comme indiqué ci-dessous :

Description du quota	Quota par défaut
Nouvelles instances réservées régionales	20 par région et par mois
Nouvelles instances réservées zonales	20 par zone de disponibilité et par mois

Par exemple, dans une région comportant trois zones de disponibilité, le quota par défaut est de 80 nouvelles instances réservées par mois, calculé comme suit :

- 20 instances réservées régionales pour la région
- Plus 60 instances réservées zonales (20 pour chacune des trois zones de disponibilité)

Les instances de l'`running`État sont prises en compte dans votre quota. Les instances situées dans les `hibernated` états`spending`, `stopping``stopped`, et ne sont pas prises en compte dans votre quota.

Afficher le nombre total d'instances réservées que vous avez achetées

Le nombre d'instances réservées que vous achetez est indiqué par le champ Instance count (Nombre d'instances, console) ou par le paramètre `InstanceCount` (AWS CLI). Lorsque vous achetez de nouvelles instances réservées, le quota est mesuré par rapport au nombre total d'instances. Par exemple, si vous achetez une configuration d'instance réservée unique avec un nombre d'instances de 10, l'achat compte dans votre quota à 10, et non à 1.

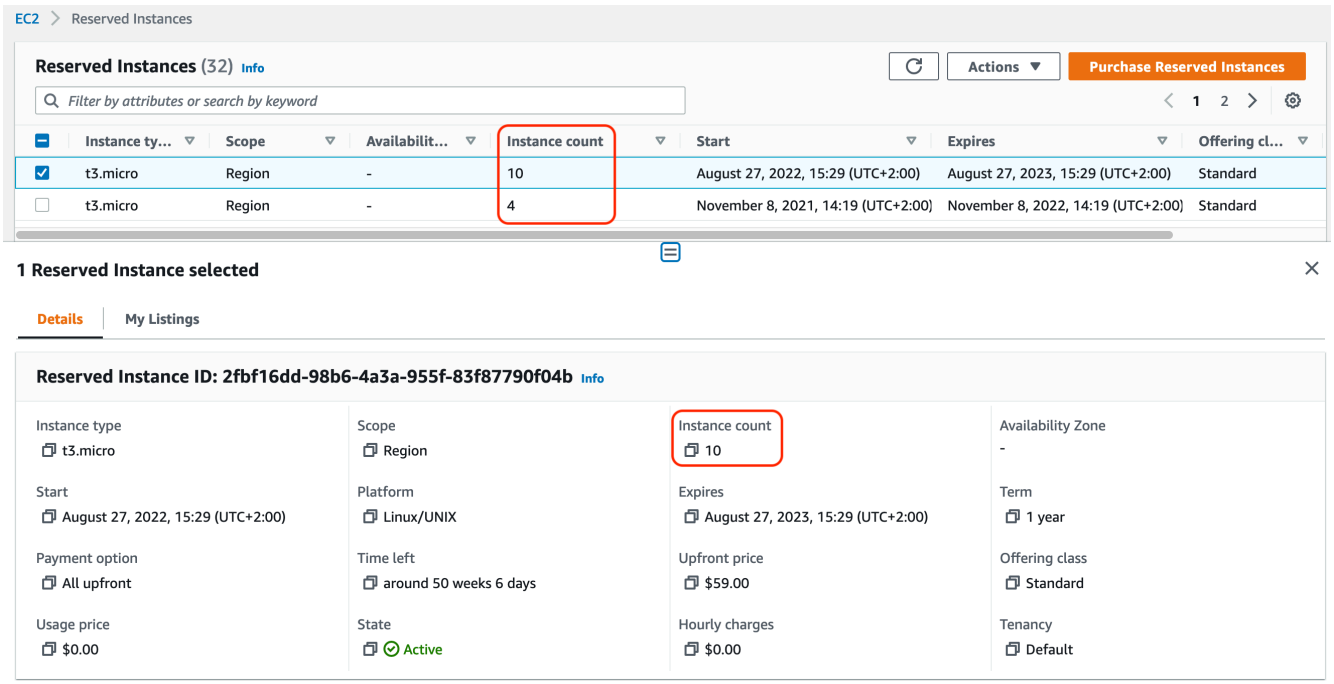
Vous pouvez consulter le nombre d'instances réservées que vous avez achetées en utilisant Amazon EC2 ou le AWS CLI.

Console

Pour afficher le nombre total d'instances réservées que vous avez achetées

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Reserved Instances (Instances réservées).
3. Sélectionnez une configuration d'instance réservée dans le tableau, puis vérifiez le champ Instance count (Nombre d'instances).

   Dans la capture d'écran suivante, la ligne sélectionnée représente une configuration d'instance réservée unique pour un type d'instance `t3.micro`. La colonne Instance count (Nombre d'instances) de la vue de table et le champ Instance count de la vue détaillée (mis en évidence dans la capture d'écran) indiquent qu'il existe 10 instances réservées pour cette configuration.



AWS CLI

Pour afficher le nombre total d'instances réservées que vous avez achetées

Utilisez la describe-reserved-instancesCLIcommande et spécifiez l'ID de la configuration de l'instance réservée.

```
aws ec2 describe-reserved-instances \
    --reserved-instances-ids a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --output table
```

Exemple de sortie : le champ `InstanceCount` indique qu'il existe 10 instances réservées pour cette configuration.

```
-------------------------------------------------------------------
|                    DescribeReservedInstances                    |
+-----------------------------------------------------------------+
||                       ReservedInstances                       ||
|+----------------------+----------------------------------------+|
||  CurrencyCode        |  USD                                   ||
||  Duration            |  31536000                              ||
||  End                 |  2023-08-27T13:29:44+00:00             ||
||  FixedPrice          |  59.0                                  ||
||  InstanceCount       |  10                                    ||
||  InstanceTenancy     |  default                               ||
||  InstanceType        |  t3.micro                              ||
||  OfferingClass       |  standard                              ||
||  OfferingType        |  All Upfront                           ||
||  ProductDescription  |  Linux/UNIX                            ||
||  ReservedInstancesId |  a1b2c3d4-5678-90ab-cdef-EXAMPLE11111  ||
||  Scope               |  Region                                ||
||  Start               |  2022-08-27T13:29:45.938000+00:00      ||
||  State               |  active                                ||
||  UsagePrice          |  0.0                                   ||
|+----------------------+----------------------------------------+|
|||                      RecurringCharges                       |||
||+---------------------------------+--------------------------+||
|||  Amount                         |  0.0                     |||
|||  Frequency                      |  Hourly                  |||
||+---------------------------------+--------------------------+||
```

PowerShell

Pour afficher le nombre total d'instances réservées que vous avez achetées

Utilisez l'Get-EC2ReservedInstanceapplet de commande et spécifiez l'ID de la configuration de l'instance réservée.

```
Get-EC2ReservedInstance -ReservedInstancesId a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Exemple de sortie : le champ `InstanceCount` indique qu'il existe 10 instances réservées pour cette configuration.

```
AvailabilityZone    :
CurrencyCode        : USD
Duration            : 31536000
End                 : 1/12/2017 8:57:08 PM
FixedPrice          : 0
InstanceCount       : 10
InstanceTenancy     : default
InstanceType        : t3.medium
OfferingClass       : standard
OfferingType        : All Upfront
ProductDescription  : Windows
RecurringCharges    : {}
ReservedInstancesId : a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
Scope               : Region
Start               : 10/12/2016 4:00:00 PM
State               : active
Tags                : {}
UsagePrice          : 0
```

Considérations

Une Instance réservée régionale applique une remise à une instance à la demande en cours d'exécution. La limite d'instance à la demande par défaut est de 20. Vous ne pouvez pas dépasser votre limite d'instance à la demande en cours d'exécution en achetant des instances réservées régionales. Par exemple, si vous avez déjà 20 instances à la demande en cours d'exécution, et que vous achetez 20 instances réservées régionales, les 20 instances réservées régionales sont utilisées pour appliquer une remise aux 20 instances à la demande en cours d'exécution. Si vous achetez plus d'instances réservées régionales, vous ne pourrez pas lancer plus d'instances flottee que vous avez atteint votre limite d'instance à la demande.

Avant d'acheter des instances réservées régionales, assurez-vous que votre limite d'instance à la demande atteint ou dépasse le nombre d'instances réservées régionales que vous comptez posséder. Si nécessaire, assurez-vous de demander une augmentation de votre limite d'instance à la demande avant d'acheter des Instances réservées régionales supplémentaires.

Une instance réservée zonale, c'est-à-dire une instance réservée achetée pour une zone de disponibilité spécifique, offre une réserve de capacité ainsi qu'une remise. Vous pouvez dépasser votre limite d'instance à la demande en cours d'exécution en achetant des Instances réservées zonales. Par exemple, si vous avez déjà 20 instances à la demande en cours d'exécution et que vous achetez 20 instances réservées zonales, vous pouvez lancer 20 instances à la demande supplémentaires qui correspondent aux spécifications de vos instances réservées zonales, ce qui vous donne un total de 40 instances en cours d'exécution.

Afficher vos quotas d'instances réservées et demander une augmentation de quota

La EC2 console Amazon fournit des informations sur les quotas. Vous pouvez également demander une augmentation de vos quotas. Pour plus d'informations, consultez Afficher vos quotas actuels et Demander une augmentation.

Spot instances

Une instance Spot est une instance qui utilise de la EC2 capacité inutilisée disponible à un prix inférieur au prix à la demande. Dans la mesure où les instances Spot vous permettent de demander des EC2 instances non utilisées à des remises importantes, vous pouvez réduire considérablement vos EC2 coûts Amazon. Le prix horaire d'une instance Spot est appelé prix spot. Le prix spot de chaque type d'instance dans chaque zone de disponibilité est fixé par Amazon EC2 et est ajusté progressivement en fonction de l'offre et de la demande à long terme d'instances ponctuelles. Votre instance Spot s'exécute chaque fois que la capacité est disponible.

Les instances Spot constituent un choix économique si vous êtes flexible quant au moment où vos applications s'exécutent et à la possibilité de les interrompre. Par exemple, les instances Spot sont particulièrement adaptées à l'analyse de données, aux travaux par lots, au traitement en arrière-plan et aux tâches facultatives. Pour plus d'informations, consultez Amazon EC2 Spot Instances.

Pour une comparaison des différentes options d'achat par EC2 exemple, voirOptions EC2 de facturation et d'achat Amazon.

Concepts

Avant de commencer à utiliser les instances Spot, vous devez connaître les concepts suivants :

- Pool de capacité ponctuelle : ensemble d'EC2instances inutilisées ayant le même type d'instance (par exemple`m5.large`) et la même zone de disponibilité.
- Prix Spot – Prix horaire actuel d'une instance Spot.

- Demande d'instance Spot – Demande d'une instance Spot. Lorsque la capacité est disponible, Amazon EC2 répond à votre demande. Une demande d'instance Spot est soit One-time (Unique) soit Persistent (Persistante). Amazon soumet EC2 automatiquement à nouveau une demande d'instance ponctuelle persistante après l'interruption de l'instance ponctuelle associée à la demande.
- EC2recommandation de rééquilibrage d'instance : Amazon EC2 émet un signal de recommandation de rééquilibrage d'instance pour vous informer qu'une instance Spot présente un risque élevé d'interruption. Ce signal vous donne la possibilité de rééquilibrer de manière proactive vos charges de travail entre les instances Spot existantes ou nouvelles sans avoir à attendre l'avis d'interruption d'instance Spot deux minutes avant celle-ci.
- Interruption de l'instance Spot : Amazon EC2 met fin à votre instance Spot, l'arrête ou la met en veille prolongée lorsqu'Amazon EC2 a besoin de récupérer sa capacité. Amazon EC2 fournit un avis d'interruption de l'instance Spot, qui donne à l'instance un avertissement de deux minutes avant son interruption.

Différences entre les instances ponctuelles et les instances à la demande

Le tableau suivant répertorie les principales différences entre les instances Spot et les instances à la demande.

	Spot instances	On-Demand instances
Heure de lancement	Ne peut être lancée immédiatement que si la demande d'instance Spot est active et la capacité disponible.	Peut uniquement être lancé immédiate ment si vous émettez une demande de lancement manuel et que la capacité est disponible.
Capacité disponible	Si la capacité n'est pas disponible, la demande d'instance Spot continue à effectuer automatiquement la demande de lancement jusqu'à ce que la capacité devienne disponible.	Si la capacité n'est pas disponible lorsque vous faites une demande de lancement, une erreur de capacité insuffisante s'affiche (ICE).
Tarif horaire		Le prix horaire pour les instances à la demande est statique.

	Spot instances	On-Demand instances
	Le prix horaire pour les instances Spot varie en fonction de l'offre et de la demande à long terme.	
Recommandation de rééquilibrage	Signal émis par EC2 Amazon pour une instance Spot en cours d'exécution lorsque celle-ci présente un risque élevé d'interruption.	Vous déterminez le moment où une instance à la demande est interrompue (arrêtée, mise en veille prolongée ou résiliée).
Interruption d'instance	Vous pouvez arrêter et démarrer une instance Spot EBS soutenue par Amazon. En outre, Amazon EC2 peut interrompre une instance Spot individuelle si la capacité n'est plus disponible.	Vous déterminez le moment où une instance à la demande est interrompue (arrêtée, mise en veille prolongée ou résiliée).

Tarification et économies

Vous payez le prix Spot pour les instances Spot, qui est fixé par Amazon EC2 et ajusté progressivement en fonction de l'offre et de la demande à long terme d'instances Spot. Vos instances Spot fonctionnent jusqu'à ce que vous les résiliiez, que la capacité ne soit plus disponible ou que votre groupe Amazon EC2 Auto Scaling les mette hors service pendant le dimensionnement.

Si vous ou Amazon EC2 interrompez une instance Spot en cours d'exécution, vous êtes facturé pour les secondes utilisées ou pour l'heure complète, ou vous ne recevez aucun frais, selon le système d'exploitation utilisé et la personne qui a interrompu l'instance Spot. Pour de plus amples informations, veuillez consulter Facturation des instances Spot interrompues.

Les instances Spot ne sont pas couvertes par Savings Plans. Si vous avez un Savings Plan, celui-ci ne vous permet pas de réaliser des économies supplémentaires en plus des économies déjà réalisées en utilisant les instances Spot. De plus, vos dépenses pour les instances Spot n'appliquent pas les engagements de vos Compute Savings Plans.

Consulter les tarifs

Pour connaître le prix spot le plus bas actuel (mis à jour toutes les cinq minutes) par Région AWS type d'instance, consultez la page de tarification des instances Amazon EC2 Spot.

Pour consulter l'historique des prix au comptant des trois derniers mois, utilisez la EC2 console Amazon ou la describe-spot-price-historycommande (AWS CLI). Pour de plus amples informations, veuillez consulter Historique de tarification d'instances Spot.

Nous mappons indépendamment les zones de disponibilité aux codes de chacune d'entre elles Compte AWS. Par conséquent, vous pouvez obtenir des résultats variables pour un même code de zone de disponibilité (par exemple, `us-west-2a`) entre différents comptes.

Consulter les économies

Vous pouvez afficher les économies réalisées grâce à l'utilisation d'instances Spot pour un seul parc d'instances Spot ou pour toutes les instances Spot. Vous pouvez consulter les économies réalisées au cours de la dernière heure ou des trois derniers jours, ainsi que le coût moyen par CPU heure et par heure de mémoire (GiB). Les économies sont des estimations et peuvent différer de vos économies réelles, car elles ne tiennent pas compte des ajustements de facturation en fonction de votre utilisation. Pour plus d'informations sur la consultation des informations sur les économies, consultez Économies réalisées grâce à l'achat d'instances Spot.

Consulter les factures

Votre facture fournit des détails sur votre utilisation du service. Pour plus d'informations, consultez la section Viewing your bill (Affichage d'une facture) dans le Guide de l'utilisateur AWS Billing .

Bonnes pratiques pour Amazon EC2 Spot

Amazon EC2 fournit un accès à de la capacité de EC2 calcul inutilisée dans le AWS Cloud cadre d'instances Spot via des instances ponctuelles, ce qui permet de réaliser des économies allant jusqu'à 90 % par rapport aux prix à la demande. La seule différence entre les instances à la demande et les instances ponctuelles est que les instances ponctuelles peuvent être interrompues par AmazonEC2, moyennant un préavis de deux minutes, si Amazon EC2 a besoin de récupérer la capacité. Pour garantir la meilleure expérience possible avec les instances Spot, il est important de comprendre et d'appliquer les meilleures pratiques relatives à leur utilisation.

Les instances Spot sont recommandés pour les applications flexibles sans état, tolérantes aux pannes. Par exemple, les instances Spot fonctionnent bien pour les mégadonnées, les charges de travail conteneurisées, les CI/CD, les serveurs Web apatrides, le calcul haute performance () HPC et les charges de travail de rendu.

En cours d'exécution, les instances Spot sont exactement les mêmes que instances à la demande. Toutefois, Spot ne garantit pas que vous pouvez conserver vos instances en cours d'exécution

suffisamment longtemps pour terminer vos charges de travail. Spot ne garantit pas non plus que vous pouvez obtenir la disponibilité immédiate des instances que vous recherchez, ou que vous pouvez toujours obtenir la capacité globale que vous avez demandée. De plus, les interruptions et la capacité des instances Spot peuvent changer au fil du temps, car leur disponibilité varie en fonction de l'offre et de la demande, et les performances passées ne sont pas une garantie de résultats futurs.

Les instances Spot ne conviennent pas aux charges de travail inflexibles, dynamiques, intolérantes aux pannes ou étroitement couplées entre des nœuds d'instance. Nous ne recommandons pas les instances Spot pour les charges de travail qui ne tolèrent pas les périodes occasionnelles pendant lesquelles la totalité de la capacité cible n'est pas entièrement disponible. Bien que le respect des meilleures pratiques Spot en matière de flexibilité en ce qui concerne les types d'instances et les zones de disponibilité offre les meilleures chances d'obtenir une haute disponibilité, rien ne garantit que la capacité sera disponible, car l'augmentation de la demande d'instances à la demande peut perturber les charges de travail sur les instances ponctuelles.

Nous vous déconseillons vivement d'utiliser des instances ponctuelles pour ces charges de travail ou de tenter de passer à des instances à la demande pour gérer les interruptions ou les périodes d'indisponibilité. Le passage à des instances à la demande peut entraîner des interruptions par inadvertance pour vos autres instances ponctuelles. En outre, si les instances ponctuelles correspondant à une combinaison de type d'instance et de zone de disponibilité sont interrompues, il peut s'avérer difficile pour vous d'obtenir des instances à la demande avec cette même combinaison.

Que vous soyez un utilisateur Spot expérimenté ou un nouvel utilisateur des instances Spot, si vous rencontrez actuellement des problèmes avec les interruptions ou la disponibilité des instances Spot, nous vous recommandons de suivre ces bonnes pratiques pour bénéficier de la meilleure expérience d'utilisation du service Spot.

Bonnes pratiques en matière d'instances Spot

- Préparer des instances individuelles pour les interruptions
- Soyez flexible en ce qui concerne les types d'instance et les zones de disponibilité
- Utilisation d'une sélection de type d'instance basée sur des attributs
- Utilisez les scores de placement Spot pour identifier les régions et les zones de disponibilité optimales
- Utilisez les groupes EC2 Auto Scaling ou EC2 Fleet pour gérer votre capacité globale
- Utiliser la stratégie d'allocation optimisée pour le prix et la capacité
- Utilisez AWS des services intégrés pour gérer vos instances Spot
- Quelle est la meilleure méthode de demande Spot à utiliser ?

Préparer des instances individuelles pour les interruptions

La meilleure façon pour vous de gérer fluidement les interruptions d'instance Spot consiste à concevoir votre application pour qu'elle soit tolérante aux pannes. Pour ce faire, vous pouvez tirer parti des recommandations de rééquilibrage des EC2 instances et des avis d'interruption des instances ponctuelles.

Une recommandation de rééquilibrage d'EC2instance est un signal qui vous avertit lorsqu'une instance Spot présente un risque élevé d'interruption. Le signal vous donne la possibilité de gérer de manière proactive l'instance Spot avant son avis d'interruption à deux minutes. Vous pouvez décider de rééquilibrer votre charge de travail en une instances Spot nouvelle ou existante qui ne présente pas un risque élevé d'interruption. Nous vous avons facilité l'utilisation de ce signal en utilisant la fonction de rééquilibrage de capacité dans les groupes et les EC2 flottes Auto Scaling.

Un avis d'interruption d'une instance Spot est un avertissement émis deux minutes avant qu'Amazon n'EC2interrompe une instance Spot. Si votre charge de travail est « flexible dans le temps », vous pouvez configurer vos instances Spot pour qu'elles soient arrêtées ou mises en veille prolongée plutôt que résiliées lorsqu'elles sont interrompues. Amazon arrête ou met EC2 automatiquement en veille prolongée vos instances Spot en cas d'interruption, et les reprend automatiquement lorsque la capacité est disponible.

Nous vous recommandons de créer une règle dans Amazon EventBridge qui capture les recommandations de rééquilibrage et les notifications d'interruption, puis déclenche un point de contrôle pour suivre l'évolution de votre charge de travail ou gère correctement l'interruption. Pour de plus amples informations, veuillez consulter Surveiller les signaux de recommandation de rééquilibrage. Pour un exemple détaillé expliquant comment créer et utiliser des règles relatives aux événements, consultez Taking Advantage of Amazon EC2 Spot Instance Interruption Notices.

Pour plus d'informations, consultez EC2recommandations de rééquilibrage des instances et Interruptions d'instance Spot.

Soyez flexible en ce qui concerne les types d'instance et les zones de disponibilité

Un pool de capacité Spot est un ensemble d'EC2instances inutilisées ayant le même type d'instance (par exemple`m5.large`) et la même zone de disponibilité (par exemple, us-east-1a). Vous devez être flexible quant aux types d'instance que vous demandez et aux zones de disponibilité dans lesquelles vous pouvez déployer votre charge de travail. Cela donne à Spot une meilleure chance de trouver et d'allouer la quantité requise de capacité de calcul. Par exemple, ne demandez pas simplement `c5.large` si vous seriez prêt à utiliser des larges des familles c4, m5 et m4.

En fonction de vos besoins spécifiques, vous pouvez évaluer les types d'instance que vous pouvez utiliser pour répondre à vos besoins de calcul. Si une charge de travail peut être redimensionnée verticalement, vous devez inclure des types d'instances plus importants (plus de volume vCPUs et de mémoire) dans vos demandes. Si vous ne pouvez évoluer qu'horizontalement, vous devez inclure des types d'instance de génération plus ancienne car ils sont moins demandés par les clients à la demande.

Une bonne règle générale est d'être flexible sur au moins 10 types d'instance pour chaque charge de travail. En outre, assurez-vous que toutes les zones de disponibilité sont configurées pour être utilisées dans votre charge de travail VPC et qu'elles sont sélectionnées en fonction de votre charge de travail.

Utilisation d'une sélection de type d'instance basée sur des attributs

Grâce à la sélection du type d'instance basée sur les attributs, vous pouvez spécifier des attributs d'instance, tels que la mémoire et le stockagevCPUs, pour la charge de travail que vous souhaitez exécuter. EC2Auto Scaling ou EC2 Fleet identifieront et lanceront ensuite automatiquement les instances correspondant aux attributs que vous avez spécifiés. Cela élimine les efforts nécessaires pour sélectionner manuellement des types d'instances spécifiques, ce qui nécessite une compréhension approfondie de l'offre de chaque type d'instance.

De plus, la sélection du type d'instance basée sur les attributs vous permet d'utiliser automatiquement les nouveaux types d'instance dès qu'ils sont disponibles. Cela garantit un accès fluide à une gamme de plus en plus large de capacités d'instances Spot.

La sélection du type d'instance basée sur les attributs est idéale pour les charges de travail et les frameworks qui peuvent être flexibles quant aux types d'instances sur lesquels ils s'exécutent, tels que le calcul haute performance (HPC) et les charges de travail Big Data.

Pour plus d'informations, consultez Créer un groupe d'instances mixtes à l'aide de la sélection du type d'instance basée sur les attributs dans le guide de l'utilisateur Amazon EC2 Auto Scaling et Spécifiez les attributs pour la sélection du type d'instance pour EC2 Fleet ou Spot Fleet dans ce guide.

Utilisez les scores de placement Spot pour identifier les régions et les zones de disponibilité optimales

Les instances ponctuelles sont des EC2 capacités inutilisées, et cette capacité fluctue en fonction de l'EC2offre et de la demande. Par conséquent, il se peut que vous n'obteniez pas toujours la capacité Spot exacte dont vous avez besoin à un endroit précis et à un moment précis. Pour atténuer cette

imprévisibilité, vous pouvez utiliser la fonction Spot placement score. Cette fonctionnalité fournit des recommandations pour les régions ou les zones de disponibilité les plus susceptibles de disposer d'une capacité suffisante pour répondre à vos besoins en matière de capacité Spot sans que vous ayez à lancer d'abord des instances Spot dans ces zones.

Il est préférable d'utiliser le score de placement ponctuel pour les charges de travail qui peuvent être flexibles quant aux types d'instances et à la région ou à la zone de disponibilité qu'elles peuvent utiliser. Il vous suffit de spécifier la capacité Spot dont vous avez besoin, les exigences relatives au type d'instance et si vous souhaitez des recommandations pour les régions ou les zones de disponibilité. En retour, vous recevez un score allant de 1 à 10 pour chaque région ou zone de disponibilité, indiquant la probabilité de fournir avec succès la capacité Spot demandée dans cette région. Un score de 10 indique que votre demande Spot a de fortes chances d'aboutir.

Il est important de noter qu'un score de placement Spot est une point-in-time recommandation, car la capacité peut varier au fil du temps. Il ne garantit pas la capacité disponible et ne prévoit pas le risque d'interruption.

Vous pouvez utiliser la fonction de score de placement Spot dans la EC2 console Amazon AWS CLI, ou unSDK. Pour de plus amples informations, veuillez consulter Score de placement Spot.

Utilisez les groupes EC2 Auto Scaling ou EC2 Fleet pour gérer votre capacité globale

Spot vous permet de penser en termes de capacité globale (en unités incluant la mémoirevCPUs, le stockage ou le débit du réseau) plutôt que de penser en termes d'instances individuelles. Les groupes Auto Scaling et EC2 Fleet vous permettent de lancer et de maintenir une capacité cible, et de demander automatiquement des ressources pour remplacer celles qui sont perturbées ou arrêtées manuellement. Lorsque vous configurez un groupe ou un EC2 parc Auto Scaling, il vous suffit de spécifier les types d'instances et la capacité cible en fonction des besoins de votre application. Pour plus d'informations, consultez les groupes Auto Scaling dans le guide de l'utilisateur Amazon EC2 Auto Scaling et Création d'une EC2 flotte dans ce guide de l'utilisateur.

Utiliser la stratégie d'allocation optimisée pour le prix et la capacité

Les stratégies d'allocation dans les groupes Auto Scaling vous aident à provisionner votre capacité cible sans avoir à rechercher manuellement des groupes de capacités Spot avec une capacité de réserve. Nous vous recommandons d'utiliser la stratégie `price-capacity-optimized`, car elle alloue automatiquement les instances des groupes de capacités Spot les plus disponibles qui présentent également le prix le plus bas. Vous pouvez également tirer parti de la stratégie d'`price-capacity-optimized`allocation dans EC2 Fleet. Étant donné que votre capacité d'instance Spot provient de pools avec une capacité optimale, cela réduit la possibilité que vos instances Spot soient

demandées. Pour plus d'informations sur les stratégies d'allocation, consultez Spot Instances dans le guide de l'utilisateur Amazon EC2 Auto Scaling et Lorsque les charges de travail ont un coût d'interruption élevé dans ce guide de l'utilisateur.

Utilisez AWS des services intégrés pour gérer vos instances Spot

D'autres AWS services s'intègrent à Spot pour réduire les coûts de calcul globaux sans qu'il soit nécessaire de gérer les instances ou les flottes individuelles. Nous vous recommandons d'envisager les solutions suivantes pour vos charges de travail applicables : AmazonEMR, Amazon Elastic Container Service AWS Batch, Amazon Elastic Kubernetes Service, Amazon et SageMaker Amazon AWS Elastic Beanstalk. GameLift Pour en savoir plus sur les meilleures pratiques de Spot relatives à ces services, consultez le site Web Amazon EC2 Spot Instances Workshops.

Quelle est la meilleure méthode de demande Spot à utiliser ?

Utilisez le tableau suivant pour déterminer laquelle API utiliser lorsque vous demandez des instances Spot.

API	Quand l'utiliser ?	Cas d'utilisation	Dois-je l'utiliser API ?
CreateAutoScalingGroup	• Vous avez besoin de plusieurs instances avec une configuration unique ou une configuration mixte. • Vous souhaitez automatiser la gestion du cycle de vie par le biais d'un outil configurableAPI.	Créez un groupe Auto Scaling qui gère le cycle de vie de vos instances tout en gardant le nombre d'instances souhaité. Prend en charge la mise à l'échelle horizontale (ajout d'instances supplémentaires) entre les limites minimale et maximale spécifiées.	Oui
CreateFleet	• Vous avez besoin de plusieurs	Créez un parc d'instances à la	Oui – en mode `instant` si vous

API	Quand l’utiliser ?	Cas d’utilisation	Dois-je l'utiliser API ?
	instances avec une configuration unique ou une configuration mixte. • Vous voulez gérer vous-même le cycle de vie de vos instances. • Si vous n’avez pas besoin de scalabilité automatique, nous vous recommandons d’utiliser une flotte de type `instant`.	demande et d'instances ponctuelles en une seule demande, avec plusieurs spécifications de lancement qui varient en fonction du type d'instance AMI, de la zone de disponibilité ou du sous-réseau. La stratégie d’allocation d’instances Spot est définie par défaut sur `lowest-price` par unité, mais vous pouvez la modifier en `price-capacity-optimized` , `capacity-optimized` ou `diversified` .	n’avez pas besoin de scalabilité automatique

API	Quand l’utiliser ?	Cas d’utilisation	Dois-je l'utiliser API ?
RunInstances	• Vous utilisez déjà le RunInstances API pour lancer des instances à la demande, et vous souhaitez simplement passer au lancement d'instances ponctuelles en modifiant un seul paramètre. • Vous n’avez pas besoin de plusieurs instances avec des types d’instance différents.	Lancez un nombre spécifié d'instances à l'aide d'un AMI et d'un type d'instance.	Non, car il RunInstances n'autorise pas les types d'instances mixtes dans une seule demande

API	Quand l'utiliser ?	Cas d'utilisation	Dois-je l'utiliser API ?
RequestSpotFleet	• Nous vous déconseillons vivement d'utiliser le RequestSpotFleet API car il s'agit d'un héritage API sans investissement prévu. • Si vous souhaitez gérer le cycle de vie de votre instance, utilisez le CreateFleet API. • Si vous ne souhaitez pas gérer le cycle de vie de votre instance, utilisez le CreateAutoScalingGroup API.	FAIRE NOTUSE. RequestSpotFleet est API un héritage sans investissement prévu.	Non

API	Quand l'utiliser ?	Cas d'utilisation	Dois-je l'utiliser API ?
RequestSpotInstances	• Nous vous déconseillons vivement d'utiliser le RequestSpotInstances API car il s'agit d'un héritage API sans investissement prévu.	FAIRE NOTUSE. RequestSpotInstances est API un héritage sans investissement prévu.	Non

Fonctionnement des instances Spot

Pour lancer une instance Spot, soit vous créez une demande d'instance Spot, soit Amazon EC2 crée une demande d'instance Spot en votre nom. L'instance Spot se lance lorsque la demande d'instance Spot est remplie.

Vous pouvez lancer une instance Spot en utilisant plusieurs services différents. Pour plus d'informations, consultez Getting Started with Amazon EC2 Spot Instances. Dans ce guide de l'utilisateur, nous décrivons les méthodes suivantes pour lancer une instance Spot en utilisant EC2 :

- Vous pouvez créer une demande d'instance Spot à l'aide de l'assistant de lancement d'instance de la EC2 console Amazon ou de la commande run-instances AWS CLI . Pour de plus amples informations, veuillez consulter Gérez vos instances Spot.
- Vous pouvez créer une EC2 flotte dans laquelle vous spécifiez le nombre souhaité d'instances Spot. Amazon EC2 crée une demande d'instance Spot en votre nom pour chaque instance Spot spécifiée dans le EC2 parc. Pour de plus amples informations, veuillez consulter Création d'une EC2 flotte.
- Vous pouvez créer une demande de parc d'instances Spot dans laquelle vous spécifiez le nombre d'instances Spot souhaité. Amazon EC2 crée une demande d'instance Spot en votre nom pour chaque instance Spot spécifiée dans la demande Spot Fleet. Pour de plus amples informations, veuillez consulter Créer une flotte Spot.

Votre instance Spot est lancée si la capacité est disponible. Votre instance Spot fonctionne jusqu'à ce que vous l'arrêtiez ou que vous la résiliiez, ou jusqu'à ce qu'Amazon l'EC2interrompe (c'est ce que l'on appelle une interruption d'instance Spot). Amazon EC2 peut arrêter, résilier ou mettre en veille prolongée une instance Spot lorsqu'elle l'interrompt.

Lorsque vous utilisez des instances Spot, vous devez être prêt à des interruptions. Amazon EC2 peut interrompre votre instance Spot lorsque la demande d'instances Spot augmente ou lorsque l'offre d'instances Spot diminue. Lorsqu'Amazon EC2 interrompt une instance Spot, il fournit un avis d'interruption, qui donne à l'instance un avertissement de deux minutes avant qu'Amazon ne l'EC2interrompe. Vous ne pouvez pas activer la protection de la résiliation pour les instances Spot. Pour de plus amples informations, veuillez consulter Interruptions d'instance Spot.

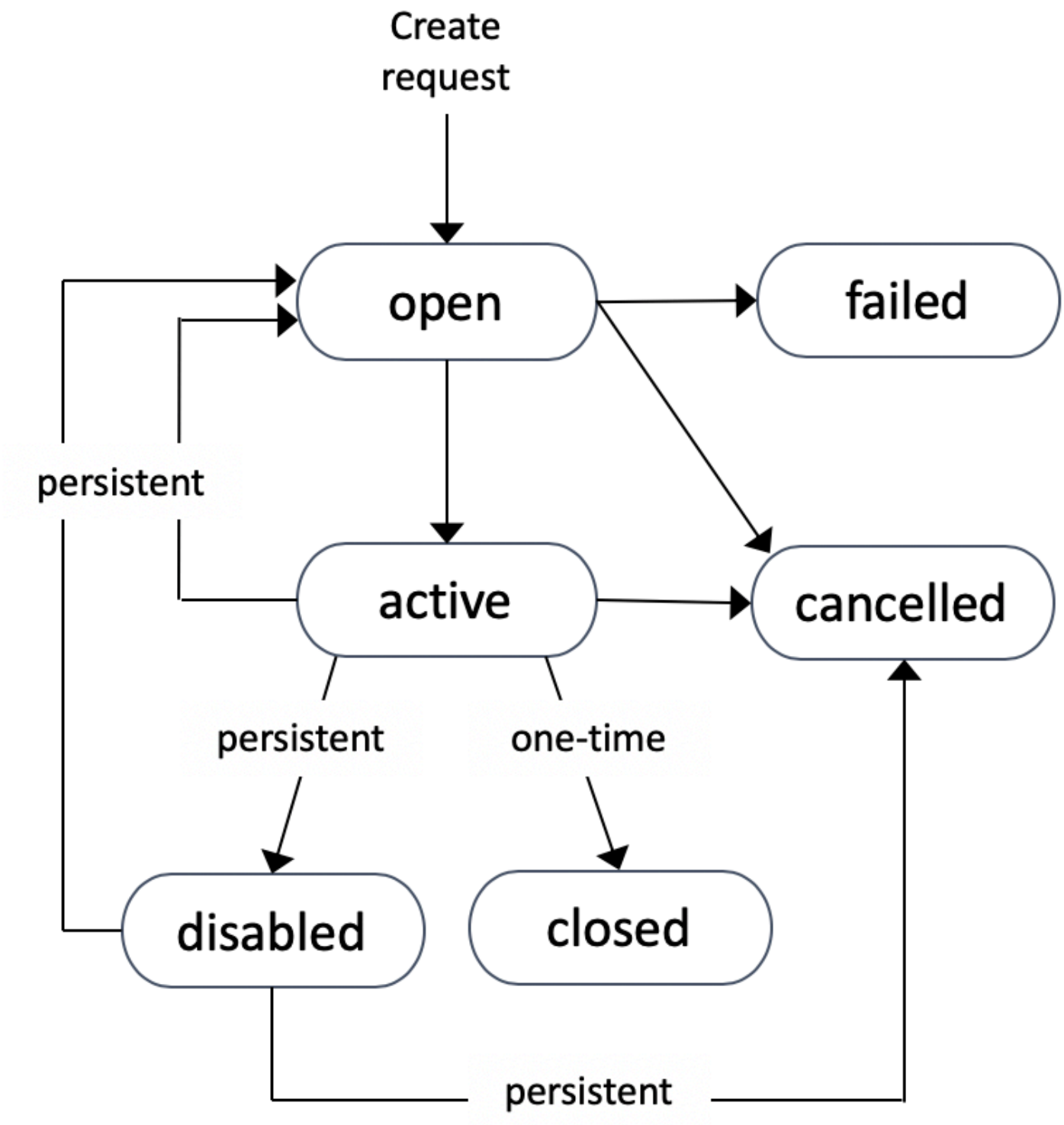
Table des matières

États des demandes d'instance Spot

Une demande d'instance Spot peut avoir l'un des états suivants :

- `open` – La demande est en attente d'exécution.
- `active` – La demande a été exécutée et est associée à une instance Spot.
- `failed` – La demande a un ou plusieurs paramètres erronés.
- `closed` – L'instance Spot a été interrompue ou résiliée.
- `disabled` – Vous avez arrêté l'instance Spot.
- `cancelled` – Vous avez annulé la demande ou elle est arrivée à expiration.

L'illustration suivante représente les transitions entre les états de la demande. Remarquez que les transitions dépendent du type de demande (unique ou persistante).



Une demande d'instance ponctuelle unique reste active jusqu'à ce qu'Amazon EC2 lance l'instance ponctuelle, que la demande expire ou que vous l'annuliez. Si la capacité n'est pas disponible, votre instance Spot est résiliée et la demande d'instance Spot est close.

Une demande d'instance Spot persistante reste active jusqu'à ce qu'elle arrive à expiration ou que vous l'annuliez, même si la demande est satisfaite. Si la capacité n'est pas disponible, votre instance Spot est interrompue. Une fois que votre instance a été interrompue, lorsque la capacité redevient disponible, l'instance Spot est démarrée si elle a été arrêtée, ou reprise si elle a été mise en veille prolongée. Vous pouvez arrêter une instance Spot et la redémarrer si la capacité est disponible. Si l'instance Spot est résiliée (qu'elle soit arrêtée ou en cours d'exécution), la demande d'instance Spot est à nouveau ouverte et Amazon EC2 lance une nouvelle instance Spot. Pour plus d'informations, consultez Arrêt d'une instance Spot, Démarrer une instance Spot et Résilier une instance Spot.

Vous pouvez effectuer le suivi du statut de vos demandes d'instance Spot, ainsi que celui des instances Spot lancées, via le statut. Pour de plus amples informations, veuillez consulter Obtenir le statut d'une demande d'instance Spot.

Lancer une instances Spot dans un groupe de lancement

Spécifiez un groupe de lancement dans votre demande d'instance Spot pour demander EC2 à Amazon de lancer un ensemble d'instances Spot uniquement s'il peut toutes les lancer. De plus, si le service Spot doit résilier l'une des instances du groupe de lancement, il doit toutes les résilier. Toutefois, si vous mettez fin à une ou plusieurs instances d'un groupe de lancement, Amazon EC2 ne met pas fin aux instances restantes du groupe de lancement.

Même si cette option peut être utile, l'ajout d'une contrainte de ce type peut réduire les chances de voir votre demande d'instance Spot satisfaite et accroître les risques de suppression de vos instances Spot. Par exemple, votre groupe de lancement inclut des instances figurant dans plusieurs zones de disponibilité. Si la capacité de l'une de ces zones de disponibilité diminue et n'est plus disponible, Amazon EC2 met fin à toutes les instances du groupe de lancement.

Si vous créez une autre demande d'instance Spot réussie qui spécifie le même groupe de lancement (existant) qu'une demande précédente réussie, les nouvelles instances sont ajoutées au groupe de lancement. Par conséquent, si une instance de ce groupe de lancement est mise hors service, toutes les instances du groupe de lancement sont également mises hors service, ce qui inclut les instances lancées par les première et deuxième demandes.

Lancer une instances Spot dans un groupe de zone de disponibilité

Spécifiez un groupe de zones de disponibilité dans votre demande d'instance Spot pour demander EC2 à Amazon de lancer un ensemble d'instances Spot dans la même zone de disponibilité. Amazon n'a pas EC2 besoin d'interrompre simultanément toutes les instances d'un groupe de zones de disponibilité. Si Amazon EC2 doit interrompre l'une des instances d'un groupe de zones de disponibilité, les autres restent actives.

Même si cette option peut s'avérer utile, l'ajout d'une contrainte de ce type peut réduire les chances de voir votre demande d'instance Spot satisfaite.

Si vous spécifiez un groupe de zone de disponibilité, mais que vous n'indiquez aucune zone de disponibilité dans la demande d'instance Spot, le résultat dépend du réseau que vous avez spécifié.

Par défaut VPC

Amazon EC2 utilise la zone de disponibilité pour le sous-réseau spécifié. Si vous ne spécifiez pas de sous-réseau, le service sélectionne une zone de disponibilité et son sous-réseau par défaut, mais pas nécessairement la zone ayant le prix le plus bas. Si vous avez supprimé le sous-réseau par défaut pour une zone de disponibilité, vous devez spécifier un autre sous-réseau.

Non par défaut VPC

Amazon EC2 utilise la zone de disponibilité pour le sous-réseau spécifié.

Lancez des instances ponctuelles dans un VPC

Vous spécifiez un sous-réseau pour vos instances Spot de la même façon que vous spécifiez un sous-réseau pour vos instances à la demande.

- [Par défautVPC] Si vous souhaitez que votre instance Spot soit lancée dans une zone de disponibilité à bas prix spécifique, vous devez spécifier le sous-réseau correspondant dans votre demande d'instance Spot. Si vous ne spécifiez aucun sous-réseau, Amazon en EC2 sélectionne un pour vous, et il est possible que la zone de disponibilité de ce sous-réseau ne propose pas le prix spot le plus bas.
- [Non défini par défautVPC] Vous devez spécifier le sous-réseau de votre instance Spot.

Lancez des instances de performance éclatantes

Les types d'instances T sont des instances à capacité extensible. Si vous lancez vos instances Spot à l'aide d'un type d'instance à performances évolutives, et si vous prévoyez d'utiliser vos instances Spot à performances évolutives immédiatement et pendant une courte durée, sans aucune période d'inactivité pour accumuler des CPU crédits, nous vous recommandons de les lancer en mode Standard pour éviter de payer des coûts plus élevés. Si vous lancez des instances Spot aux performances exceptionnelles en mode illimité et que vous les explosez CPU immédiatement, vous dépenserez des crédits excédentaires pour le bursting. Si vous utilisez l'instance pendant une courte période, l'instance n'a pas le temps d'accumuler des CPU crédits pour rembourser les crédits excédentaires, et les crédits excédentaires vous sont facturés lorsque vous mettez fin à l'instance.

Le mode illimité convient aux instances Spot aux performances élevées uniquement si l'instance fonctionne suffisamment longtemps pour accumuler des CPU crédits en cas d'éclatement. Sinon, payer des crédits excédentaires rend les instances Spot de performance à capacité extensible plus coûteuses que les autres instances. Pour de plus amples informations, veuillez consulter Quand utiliser le mode illimité plutôt que le mode fixe CPU.

Les instances T2, lorsqu'elles sont configurées en mode Standard, obtiennent des crédits de lancement. Les instances T2 sont les seules instances à capacité extensible qui obtiennent des crédits de lancement. Les crédits de lancement visent à optimiser la productivité du lancement initial des instances T2 en leur fournissant suffisamment de ressources de calcul pour pouvoir configurer l'instance. Il est interdit de procéder à des lancements répétés d'instances T2 pour bénéficier de nouveaux crédits de lancement. Si vous avez besoin d'une instance prolongéeCPU, vous pouvez gagner des crédits (en restant inactifs pendant un certain temps), utiliser le mode illimité pour les instances ponctuelles T2 ou utiliser un type d'instance dédiéeCPU.

Lancement sur du matériel à locataire unique

Vous pouvez exécuter une instance Spot sur du matériel à client unique. Les instances Spot dédiées sont physiquement isolées des instances appartenant à d'autres AWS comptes. Pour plus d'informations, consultez Instances EC2 dédiées Amazon et les instances EC2 dédiées Amazon.

Pour exécuter une instance Spot dédiée, effectuez l'une des actions suivantes :

- Spécifiez une location de `dedicated` au moment de créer la demande d'instance Spot. Pour de plus amples informations, veuillez consulter Gérez vos instances Spot.
- Demandez une instance Spot dans un VPC avec une location d'instance de`dedicated`. Pour de plus amples informations, veuillez consulter Lancer des instances dédiées dans un environnement VPC avec location par défaut. Vous ne pouvez pas demander une instance Spot avec une location de `default` si vous la demandez dans une instance VPC avec une location d'instance de. `dedicated`

Toutes les familles d'instances prennent en charge les instances Spot dédiées sauf les instances T. Pour chaque famille d'instances prise en charge, seule la plus grande taille d'instance ou taille de métal prend en charge les instances Spot dédiées.

Historique de tarification d'instances Spot

Les prix des instances Spot sont fixés par Amazon EC2 et s'ajustent progressivement en fonction des tendances à long terme de l'offre et de la demande de capacité des instances Spot.

Lorsque votre demande d'instance Spot est satisfaite, vos instances Spot se lancent au prix Spot actuel, sans dépasser le prix à la demande. Vous pouvez consulter l'historique des prix Spot pour les 90 derniers jours en filtrant par type d'instance, système d'exploitation et zone de disponibilité.

Pour afficher les prix Spot actuels

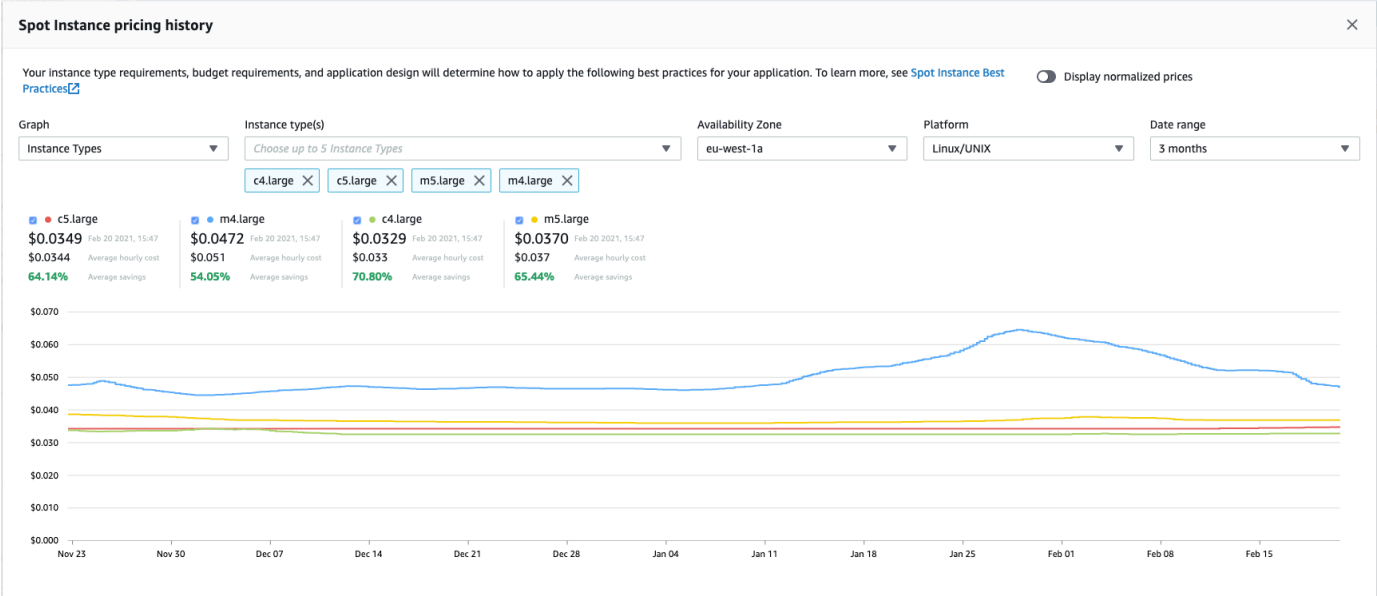
Pour connaître les prix actuels des instances Spot, consultez la tarification des instances EC2 Spot Amazon.

Pour consulter l'historique des prix au comptant à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez Historique de tarification.
4. Pour Graph (Graphique), choisissez de comparer l'historique des prix par Availability Zones (Zones de disponibilité) ou par Instance Types (Types d'instance).

   - Si vous choisissez Availability Zones (Zones de disponibilité), alors sélectionnez le Instance type (Type d'instance), le système d'exploitation (Platform (Plateforme)) et la Date range (Plage de dates) pour lesquels afficher l'historique des prix.
   - Si vous sélectionnez Instance Types (Types d'instance), alors choisissez jusqu'à 5 Instance type(s) (Type(s) d'instance), la Availability Zone (Zone de disponibilité), le système d'exploitation (Platform (Plateforme)) et la Date range (Plage de dates) pour lesquels afficher l'historique des prix.

   La capture d'écran suivante présente une comparaison de prix pour différents types d'instance.



5. Survolez le graphique avec le pointeur de la souris pour afficher les prix à des moments donnés dans la plage de dates sélectionnée. Les prix sont affichés dans les blocs d'informations au-dessus du graphique. Le prix affiché dans la ligne supérieure indique le prix à une date spécifique. Le prix affiché sur la deuxième ligne indique le prix moyen sur la plage de dates sélectionnée.
6. Pour afficher le prix au vCPU, activez Afficher les prix normalisés. Pour afficher le prix du type d'instance, désactivez Display normalized prices (Afficher les prix normalisés).

Pour afficher l'historique des prix Spot à l'aide de la ligne de commande

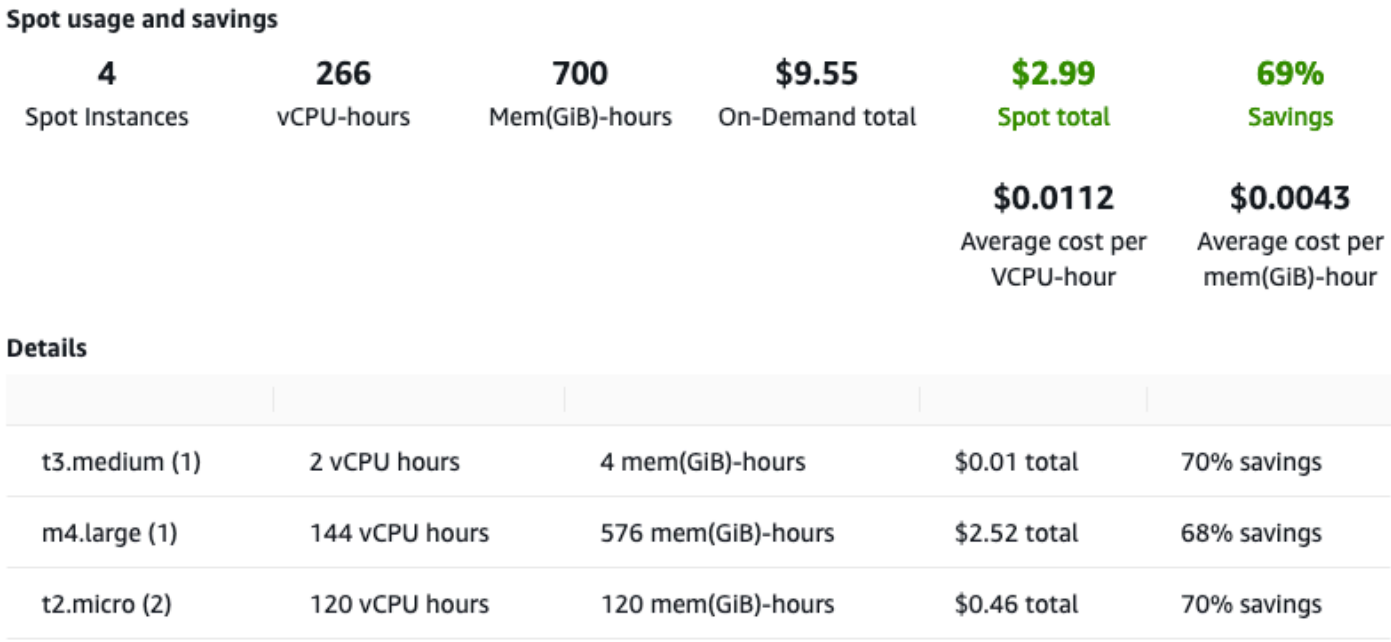
Vous pouvez utiliser l'une des commandes suivantes. Pour de plus amples informations, veuillez consulter Accédez à Amazon EC2.

- describe-spot-price-history (AWS CLI)
- Get-EC2SpotPriceHistory (AWS Tools for Windows PowerShell)

Économies réalisées grâce à l'achat d'instances Spot

Vous pouvez visualiser les informations relatives à l'utilisation et aux économies réalisées grâce aux instances Spot pour chaque flotte ou pour l'ensemble des instances Spot en cours d'exécution. Les informations relatives à l'utilisation et aux économies pour chaque flotte incluent l'ensemble des instances lancées et résiliées par la flotte. Ces informations peuvent être consultées pour la dernière heure ou pour les trois derniers jours.

La capture d'écran suivante de la section Economie illustre les informations relatives à l'utilisation d'instances Spot et aux économies associées pour un parc d'instances Spot.



Les informations suivantes relatives à l'utilisation et aux économies sont disponibles :

- Instances Spot – Nombre d'instances. Spot lancées et terminées par le parc d'instances Spot. Le nombre qui apparaît dans le récapitulatif des économies représente l'ensemble de vos instances Spot en cours d'exécution.
- v CPU -hours — Le nombre de v CPU heures utilisées sur toutes les instances ponctuelles pendant la période sélectionnée.
- Mem(GiB)-hours (Heures de mémoire (Gio)) : nombre d'heures Gio utilisées pour l'ensemble des Instances Spot sur la période sélectionnée.
- On-Demand total (Total à la demande) : montant total que vous auriez payé pour la période sélectionnée si vous aviez lancé ces instances en tant qu'Instances à la demande.
- Spot total (Total Spot) : montant total à payer pour la période sélectionnée.
- Économie : pourcentage que vous économisez en ne payant pas le prix à la demande.
- Coût moyen par CPU heure v — Le coût horaire moyen de l'utilisation de vCPUs toutes les instances ponctuelles pendant la période sélectionnée, calculé comme suit : coût moyen par CPU heure v = total ponctuel/v CPU -heures.

- Coût moyen par mém (GiB) par heure — Le coût horaire moyen de l'utilisation de toutes GiBs les instances ponctuelles pendant la période sélectionnée, calculé comme suit : coût moyen par mém (GiB) -heure = total spot/Mem (GiB) -heures.
- Tableau Détails – Les différents types d'instances (le nombre d'instances par type d'instance est placé entre parenthèses) qui composent le parc d'instances Spot. Le récapitulatif des économies comprend l'ensemble de vos instances Spot en cours d'exécution.

Les informations relatives aux économies ne peuvent être consultées qu'à l'aide de la EC2 console Amazon.

Pour consulter les informations relatives aux économies réalisées sur un parc Spot à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez l'ID d'une demande de parc d'instances Spot et faites défiler jusqu'à la section Economie.

   Vous pouvez également cocher la case en regard de l'ID de demande de parc d'instances Spot, puis choisir l'onglet Economie.
4. Par défaut, la page affiche les informations relatives à l'utilisation et aux économies de ces trois derniers jours. Vous pouvez choisir last hour (dernière heure) ou last three days (trois derniers jours). Pour les Parcs d'instances Spot qui ont été lancés il y a moins d'une heure, la page affiche une estimation des économies réalisées sur cette heure.

Pour consulter les informations relatives aux économies réalisées pour toutes les instances Spot en cours d'exécution à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Choisissez Savings Summary (Récapitulatif des économies).

Créer une demande d'instance Spot

Pour utiliser des instances Spot, vous créez une demande d'instance Spot qui inclut le nombre d'instances souhaité, le type d'instance et la zone de disponibilité. Si la capacité est disponible,

Amazon EC2 répond immédiatement à votre demande. Dans le cas contraire, Amazon EC2 attend que votre demande soit traitée ou que vous l'annuliez.

Vous pouvez utiliser l'assistant de lancement d'instance de la EC2 console Amazon ou la AWS CLI commande run-instances pour demander une instance Spot de la même manière que vous pouvez lancer une instance à la demande. Cette méthode n'est recommandée que pour les raisons suivantes :

- Vous utilisez déjà l'assistant de lancement d'instance ou la commande run-instances pour lancer des instances à la demande, et vous voulez simplement passer au lancement d'instances Spot en modifiant un seul paramètre.
- Vous n'avez pas besoin de plusieurs instances avec des types d'instance différents.

Cette méthode n'est généralement pas recommandée pour le lancement d'instances Spot car vous ne pouvez pas spécifier plusieurs types d'instance et vous ne pouvez pas lancer d'instances Spot et d'instances à la demande dans la même requête. Pour connaître les méthodes préférées pour lancer des instances Spot, notamment le lancement d'une flotte qui inclut des instances Spot et des instances à la demande avec plusieurs types d'instance, veuillez consulter la rubrique Quelle est la meilleure méthode de demande Spot à utiliser ?

Si vous demandez plusieurs instances ponctuelles à la fois, Amazon EC2 crée des demandes d'instances ponctuelles distinctes afin que vous puissiez suivre le statut de chaque demande séparément. Pour plus d'informations sur le suivi des demandes d'instance Spot, consultez Obtenir le statut d'une demande d'instance Spot.

Console

Pour créer une demande d'Instance Spot à l'aide de l'assistant de lancement d'instance

Les étapes 1 à 9 sont les mêmes que celles que vous utiliseriez pour lancer une instance à la demande. À l'étape 10, vous configurez la demande d'instance Spot.

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation, en haut de l'écran, sélectionnez une région.
3. Dans le tableau de bord de EC2 la console Amazon, choisissez Launch instance.
4. (Facultatif) Sous Name and tags (Noms et identifications), vous pouvez nommer votre instance et étiqueter la demande d'instance Spot, l'instance, les volumes et les Elastic

Graphics. Pour plus d'informations sur les balises, consultez Marquez vos EC2 ressources Amazon.

a. Pour Name (Nom), saisissez un nom descriptif pour votre instance.

   Le nom de l'instance est une identification, où la clé est Name (Nom), et la valeur est le nom que vous spécifiez. Si vous ne spécifiez pas de nom, l'instance peut être identifiée par son ID, qui est automatiquement généré lorsque vous lancez l'instance.

b. Pour étiqueter la demande d'instance Spot, l'instance, les volumes et les Elastic Graphics, choisissez Add additional tags (Ajouter de identifications supplémentaires). Choisissez Add tag (Ajouter une identification), saisissez une clé et une valeur, puis sélectionnez le type de ressource à étiqueter. Choisissez Add tag (Ajouter une identification) pour chaque étiquette supplémentaire.

5. Sous Images de l'application et du système d'exploitation (Amazon Machine Image), choisissez le système d'exploitation (OS) de votre instance, puis sélectionnez unAMI. Pour de plus amples informations, veuillez consulter Images d'applications et de systèmes d'exploitation (Amazon Machine Image).
6. Sous Instance type (Type d'instance), sélectionnez le type d'instance qui répond à vos exigences en ce qui concerne la configuration matérielle et la taille de votre instance. Pour de plus amples informations, veuillez consulter Type d'instance.
7. Sous Key pair (login) (Paire de clés [connexion]), choisissez une paire de clés existante ou choisissez Create new key pair (Créer une paire de clés) pour en créer une. Pour de plus amples informations, veuillez consulter Paires de EC2 clés Amazon et EC2 instances Amazon.

   > **Important**
   >
   > Si vous choisissez l'option Proceed without key pair (non recommandé), vous ne pourrez pas vous connecter à l'instance sauf si vous en choisissez une AMI configurée pour autoriser les utilisateurs à se connecter d'une autre manière.

8. Sous Network settings (Paramètres réseau), utilisez les paramètres par défaut ou choisissez Edit (Modifier) pour configurer les paramètres réseau selon les besoins.

   Les groupes de sécurité font partie des paramètres réseau et définissent les règles de pare-feu pour votre instance. Ces règles déterminent le trafic réseau entrant acheminé vers votre instance.

Pour de plus amples informations, veuillez consulter Paramètres réseau.

9. Le volume AMI que vous avez sélectionné inclut un ou plusieurs volumes de stockage, y compris le volume du périphérique racine. Sous Configure storage (Configurer le stockage), vous pouvez spécifier des volumes supplémentaires à attacher à l'instance en choisissant Add new volume (Ajouter un nouveau volume). Pour de plus amples informations, veuillez consulter Configurer le stockage.
10. Sous Advanced details (Détails avancés), configurez la demande d'instance Spot comme suit :

    a. Sous Purchasing option (Option d'achat), cochez la case Request Spot Instances (Demander des instances Spot).

    b. Vous pouvez soit conserver la configuration par défaut de la demande d'instance Spot, soit choisir Customize (Personnaliser), à droite, pour spécifier des paramètres personnalisés pour votre demande d'instance Spot.

    Lorsque vous choisissez Customize (Personnaliser), les champs suivants s'affichent.

    i. Maximum price (Prix maximal) : vous pouvez demander des instances Spot au prix Spot, plafonné au prix À la demande, ou spécifier le montant maximum que vous êtes prêt à payer.

    > **Warning**
    >
    > Si vous spécifiez un prix maximum, vos instances seront interrompues plus fréquemment que si vous choisissez No maximum price (Pas de prix maximal).

    - No maximum price (Pas de prix maximal) : votre instance Spot sera lancée au prix Spot en vigueur. Le prix ne dépassera jamais le prix À la demande. (Recommandé)
    - Set your maximum price (per instance/hour) (Définir votre prix maximal, par instance/heure) : vous pouvez spécifier le montant maximum que vous êtes prêt à payer.
      - Si vous spécifiez un prix maximum inférieur au prix Spot, votre instance Spot n'est pas lancée.

- Si vous spécifiez un prix maximum supérieur au prix Spot actuel, votre Instance Spot sera lancée et facturée au prix Spot actuel. Une fois votre instance Spot en cours d'exécution, si le prix Spot dépasse votre prix maximum, Amazon EC2 interrompt votre instance Spot.
- Quel que soit le prix maximum que vous spécifiez, vous serez toujours facturé au prix Spot actuel.

Pour passer en revue les tendances de prix Spot, consultez Historique de tarification d'instances Spot.

ii. Request type (Type de demande) : le type de demande d'instance spot que vous choisissez détermine ce qui se passe si votre instance spot est interrompue.

- Unique : Amazon EC2 fait une demande unique pour votre instance Spot. Si votre instance Spot est interrompue, la demande n'est pas soumise à nouveau.
- Demande persistante : Amazon EC2 place une demande persistante pour votre instance Spot. Si votre instance spot est interrompue, la demande est soumise à nouveau afin de réapprovisionner l'instance spot résiliée.

Si vous ne spécifiez pas de valeur, la valeur par défaut est une demande unique.

iii. Valid to (Valide jusqu'au) : date d'expiration d'une demande persistante d'instance Spot.

Ce champ n'est pas pris en charge pour les demandes uniques. Une demande d'unique reste active jusqu'à ce que toutes les instances de la demande soient lancées ou que vous annuliez la demande.

- No request expiry date (Pas de date d'expiration de la demande) : la demande reste active jusqu'à ce que vous l'annuliez.
- Set your request expiry date (Définir la date d'expiration de votre demande) : la demande persistante reste active jusqu'à la date spécifiée ou jusqu'à ce que vous l'annuliez.

iv. Interruption behavior (Comportement d'interruption) : le comportement que vous choisissez détermine ce qui se passe lorsqu'une instance spot est interrompue.

- Pour les demandes persistantes, les valeurs valides sont Stop (Arrêter) et Hibernate (Mettre en veille prolongée). Lorsqu'une instance est arrêtée, des frais de stockage en EBS volume s'appliquent.

  > **Note**
  >
  > Les instances Spot utilisent désormais la même fonctionnalité de mise en veille prolongée que les instances à la demande. Pour activer la mise en veille prolongée, vous pouvez soit choisir Mise en veille prolongée ici, soit sélectionner Activer dans le champ Comportement d'arrêt – mise en veille prolongée, qui apparaît plus bas dans l'assistant de lancement d'instance. Pour les prérequis de mise en veille prolongée, consultez Conditions préalables à l'hibernation des EC2 instances Amazon.

- Pour les demandes uniques, seule la valeur Terminate (Résilier) est valide.

Si vous ne spécifiez pas de valeur, la valeur par défaut est Terminate (Résilier), laquelle n'est pas valide pour une demande d'instance Spot persistante. Si vous conservez la valeur par défaut et tentez de lancer une demande d'instance Spot persistante, une erreur s'affiche.

Pour de plus amples informations, veuillez consulter Comportement des interruptions des instances Spot.

11. Sur le panneau Summary (Récapitulatif), pour Number of instances (Nombre d'instances), saisissez le nombre d'instances à lancer.

    > **Note**
    >
    > Amazon EC2 crée une demande distincte pour chaque instance Spot.

12. Sur le panneau Summary (Récapitulatif), vérifiez les détails de votre instance et effectuez toute modification nécessaire. Après avoir soumis votre demande d'instance Spot, vous ne pouvez plus modifier les paramètres de la demande. Vous pouvez accéder directement à une section dans l'assistant de lancement d'instance en sélectionnant son lien dans le panneau Summary (Récapitulatif). Pour de plus amples informations, veuillez consulter Récapitulatif.

13. Lorsque vous êtes prêt à lancer votre instance , choisissez Launch instance (Lancer l'instance).

    Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez Résoudre les problèmes de lancement des EC2 instances Amazon.

AWS CLI

Pour créer une demande d'instance Spot à l'aide de run-instances

Utilisez la commande run-instances et spécifiez les options de l'instance Spot dans le paramètre `--instance-market-options`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --count 5 \
    --subnet-id subnet-08fc749671b2d077c \
    --key-name MyKeyPair \
    --security-group-ids sg-0b0384b66d7d692f9 \
    --instance-market-options file://spot-options.json
```

La structure de données à spécifier dans le JSON fichier est la suivante`--instance-market-options`. Vous pouvez également spécifier `ValidUntil` et `InstanceInterruptionBehavior`. Si vous ne spécifiez pas de champ dans la structure de données, la valeur par défaut est utilisée.

L'exemple suivant crée une demande `persistent`.

```
{
  "MarketType": "spot",
  "SpotOptions": {
    "SpotInstanceType": "persistent"
  }
}
```

Pour créer une demande d'instance Spot à l'aide de request-spot-instances

> **Note**
>
> Nous vous déconseillons vivement d'utiliser cette request-spot-instancescommande pour demander une instance Spot, car il s'agit d'une ancienne instance API sans investissement planifié. Pour plus d'informations, consultez Quelle est la meilleure méthode de demande Spot à utiliser ?.

Utilisez la request-spot-instancescommande pour créer une demande unique.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json
```

Utilisez la request-spot-instancescommande pour créer une demande persistante.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "persistent" \
    --launch-specification file://specification.json
```

Pour accéder à des exemples de fichiers de spécification à utiliser avec ces commandes, consultez Exemple de spécifications de lancement d'une demande d'instance Spot. Si vous téléchargez un fichier de spécification de lancement depuis la console Spot Requests, vous devez utiliser la request-spot-fleetcommande à la place (la console Spot Requests spécifie une demande d'instance Spot à l'aide d'un parc Spot).

Exemple de spécifications de lancement d'une demande d'instance Spot

Les exemples suivants montrent les configurations de lancement que vous pouvez utiliser avec la request-spot-instancescommande pour créer une demande d'instance Spot. Pour de plus amples informations, veuillez consulter Gérez vos instances Spot.

> **Important**
>
> Nous vous déconseillons vivement d'utiliser cette request-spot-instancescommande pour demander une instance Spot, car il s'agit d'une ancienne instance API sans investissement

planifié. Pour plus d'informations, consultez Quelle est la meilleure méthode de demande Spot à utiliser ?.

Exemples

- Exemple 1 : Lancement d'instances Spot
- Exemple 2 : Lancement d'instances Spot dans la zone de disponibilité spécifiée
- Exemple 3 : Lancement d'instances Spot dans le sous-réseau spécifié
- Exemple 4 : Lancement d'une instance Spot dédiée

Exemple 1 : Lancement d'instances Spot

L'exemple suivant n'inclut aucune zone de disponibilité ou sous-réseau. Amazon EC2 sélectionne une zone de disponibilité pour vous. Amazon EC2 lance les instances dans le sous-réseau par défaut de la zone de disponibilité sélectionnée.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Exemple 2 : Lancement d'instances Spot dans la zone de disponibilité spécifiée

L'exemple suivant inclut une zone de disponibilité. Amazon EC2 lance les instances dans le sous-réseau par défaut de la zone de disponibilité spécifiée.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "Placement": {
    "AvailabilityZone": "us-west-2a"
```

```
  },
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Exemple 3 : Lancement d'instances Spot dans le sous-réseau spécifié

L'exemple suivant inclut un sous-réseau. Amazon EC2 lance les instances dans le sous-réseau spécifié. S'il ne s'VPCagit pas d'une adresse par défautVPC, l'instance ne reçoit pas d'IPv4adresse publique par défaut.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "SubnetId": "subnet-1a2b3c4d",
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Pour attribuer une IPv4 adresse publique à une instance dans une valeur autre que celle par défautVPC, spécifiez le `AssociatePublicIpAddress` champ comme indiqué dans l'exemple suivant. Lorsque vous spécifiez une interface réseau, vous devez inclure l'ID du sous-réseau et l'ID du groupe de sécurité à l'aide de l'interface réseau au lieu d'utiliser les champs `SubnetId` et `SecurityGroupIds` illustrés dans le bloc de code précédent.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "InstanceType": "m5.medium",
  "NetworkInterfaces": [
    {
      "DeviceIndex": 0,
      "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
      "Groups": [ "sg-1a2b3c4d5e6f7g8h9" ],
      "AssociatePublicIpAddress": true
    }
  ],
  "IamInstanceProfile": {
```

```
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Exemple 4 : Lancement d'une instance Spot dédiée

L'exemple suivant demande une instance Spot avec une location de `dedicated`. Une instance Spot dédiée doit être lancée dans unVPC.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "c5.8xlarge",
  "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
  "Placement": {
    "Tenancy": "dedicated"
  }
}
```

Obtenir le statut d'une demande d'instance Spot

Pour vous aider à suivre vos demandes d'instances Spot et à planifier votre utilisation des instances Spot, utilisez le statut des demandes fourni par AmazonEC2. Par exemple, le statut de la demande peut indiquer pourquoi votre demande d'instance Spot n'a pas encore été satisfaite, ou répertorier les contraintes qui empêchent l'exécution de votre demande d'instance Spot.

À chaque étape du processus, c'est-à-dire au cours du cycle de vie d'une demande Spot, des événements spécifiques déterminent les états successifs de la demande.

L'illustration suivante présente le fonctionnement des demandes d'instances Spot. Notez que le type de demande (ponctuelle ou persistante) détermine si la demande est à nouveau ouverte lorsqu'Amazon EC2 interrompt une instance Spot ou si vous arrêtez une instance Spot. Si la demande est persistante, elle est rouverte après que votre instance Spot soit interrompue. Si la demande est persistante et que vous arrêtez votre instance Spot, la demande s'ouvre seulement après que vous ayez démarré votre instance Spot.

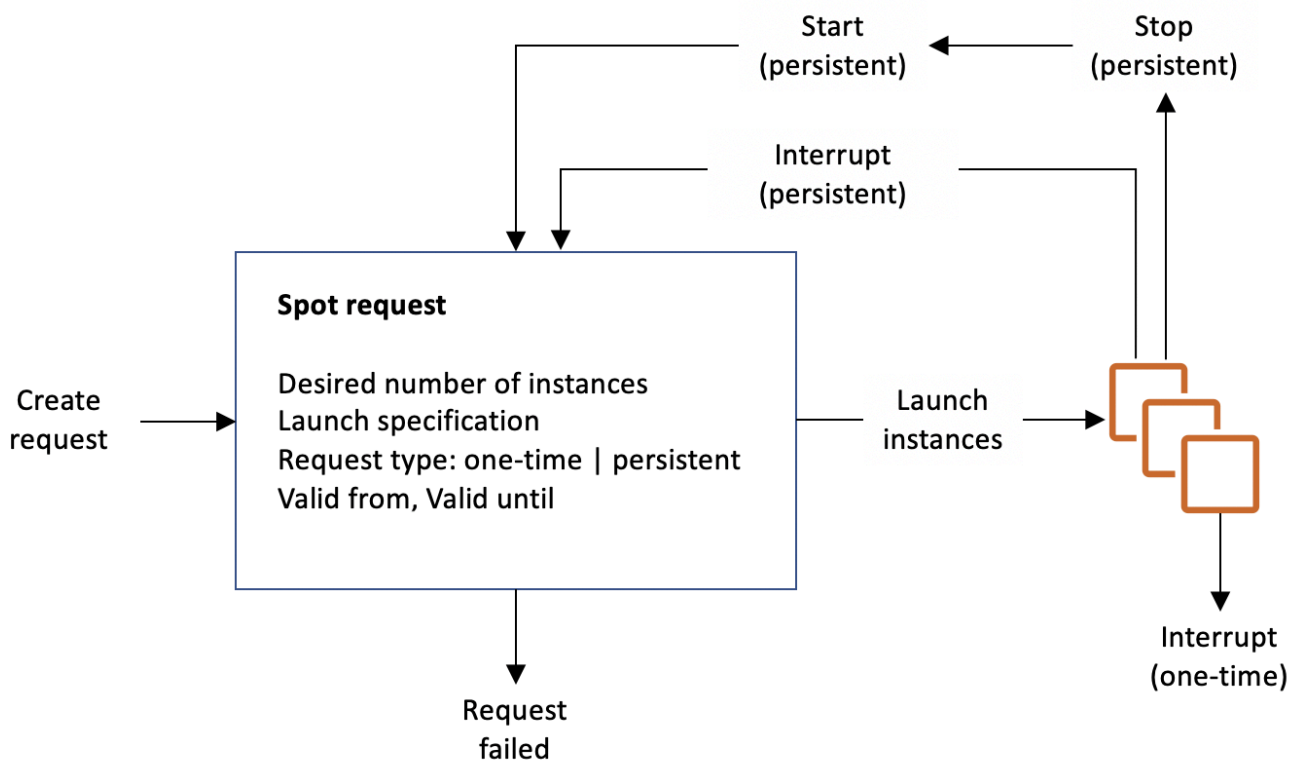


Table des matières

Obtenir des informations sur le statut d'une demande

Vous pouvez obtenir des informations sur l'état de la demande à l'aide de l'outil AWS Management Console ou en ligne de commande.

Pour obtenir des informations sur le statut d'une demande à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Demandes Spot et sélectionnez la demande d'instance Spot.
3. Pour vérifier l'état, sous l'onglet Description, cochez le champ Statut.

Pour obtenir des informations sur le statut de la demande à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- describe-spot-instance-requests (AWS CLI)
- Get-EC2SpotInstanceRequest (AWS Tools for Windows PowerShell)

Codes de statut des demandes Spot

Les informations sur le statut des demandes Spot sont composées d'un code de statut, de l'heure de mise à jour et d'un message de statut. Toutes ces informations vous permettent de savoir où en est votre demande d'instance Spot.

Voici les codes de statut des demandes Spot :

`az-group-constraint`

Amazon EC2 ne peut pas lancer toutes les instances que vous avez demandées dans la même zone de disponibilité.

`bad-parameters`

Un ou plusieurs paramètres de votre demande Spot ne sont pas valides (par exemple, ceux AMI que vous avez spécifiés n'existent pas). Le message de statut indique quel paramètre n'est pas valide.

`canceled-before-fulfillment`

L'utilisateur a annulé la demande d'instance Spot avant son exécution.

`capacity-not-available`

Il n'y a pas suffisamment de capacité disponible pour les instances que vous avez demandées.

`constraint-not-fulfillable`

La demande d'instance Spot ne peut pas être satisfaite dans la mesure où une ou plusieurs contraintes ne sont pas valides (par exemple, la zone de disponibilité n'existe pas). Le message de statut indique quelle contrainte n'est pas valide.

`fulfilled`

La demande Spot est`active`, et Amazon EC2 lance vos instances Spot.

`instance-stopped-by-price`

Votre instance a été arrêtée car le prix Spot a dépassé votre prix maximum.

`instance-stopped-by-user`

Votre instance a été arrêtée car un utilisateur l'a arrêtée ou a exécuté la commande shutdown à partir de l'instance.

`instance-stopped-no-capacity`

Votre instance a été arrêtée pour des raisons EC2 de gestion des capacités.

`instance-terminated-by-price`

Votre instance a été supprimée car le prix Spot a dépassé votre prix maximum. Si votre demande est une offre persistante, le processus redémarre et votre demande se retrouve en attente d'évaluation.

`instance-terminated-by-schedule`

Votre instance Spot a été résiliée à la fin de sa durée planifiée.

`instance-terminated-by-service`

Votre instance a été mise hors service à partir d'un état d'arrêt.

`instance-terminated-by-user` ou `spot-instance-terminated-by-user`

Étant donné que vous avez résilié une instance Spot qui a été exécutée, l'état de la demande est `closed` (sauf s'il s'agit d'une demande persistante) et l'état de l'instance est `terminated`.

`instance-terminated-launch-group-constraint`

Une ou plusieurs instances de votre groupe de lancement ont été mises hors service, c'est pourquoi la contrainte du groupe de lancement n'est plus respectée.

`instance-terminated-no-capacity`

Votre instance a été résiliée en raison de processus standard de gestion de la capacité.

`launch-group-constraint`

Amazon EC2 ne peut pas lancer toutes les instances que vous avez demandées en même temps. Toutes les instances d'un groupe de lancement sont démarrées et mises hors service ensemble.

`limit-exceeded`

La limite du nombre de EBS volumes ou du volume total de stockage a été dépassée. Pour plus d'informations, consultez la section Quotas pour Amazon EBS dans le guide de EBS l'utilisateur Amazon.

`marked-for-stop`

L'instance Spot est marquée pour être arrêtée.

`marked-for-termination`

L'instance Spot est marquée pour être résiliée.

`not-scheduled-yet`

La demande d'instance Spot n'est pas évaluée avant la date prévue.

`pending-evaluation`

Une fois que vous avez effectué une demande d'instance Spot, elle passe à l'état `pending-evaluation` le temps que le système évalue les paramètres de votre demande.

`pending-fulfillment`

Amazon EC2 essaie de mettre en service vos instances Spot.

`placement-group-constraint`

La demande Spot ne peut pas encore être satisfaite, car une instance Spot ne peut pas être ajoutée au groupe de placement à ce stade.

`price-too-low`

La demande ne peut pas encore être exécutée, car le prix maximum est inférieur au prix Spot. Dans le cas présent, aucune instance n'est lancée et votre demande reste à l'état `open`.

`request-canceled-and-instance-running`

Vous avez annulé la demande Spot alors que les instances Spot sont toujours en cours d'exécution. La demande est `cancelled`, tandis que les instances conservent l'état `running`.

`schedule-expired`

La demande d'instance Spot est arrivée à expiration car elle n'a pas été exécutée avant la date spécifiée.

`system-error`

Il y a eu une erreur système inattendue. S'il s'agit d'un problème récurrent, veuillez nous contacter AWS Support pour obtenir de l'aide.

EC2Événement de traitement des demandes d'instance Spot

Lorsqu'une demande d'instance Spot est traitée, Amazon EC2 envoie un événement de traitement de demande d'instance EC2 Spot à Amazon EventBridge. Vous pouvez créer une règle pour effectuer une action chaque fois que cet événement se produit, par exemple en invoquant une fonction Lambda ou en notifiant un SNS sujet Amazon.

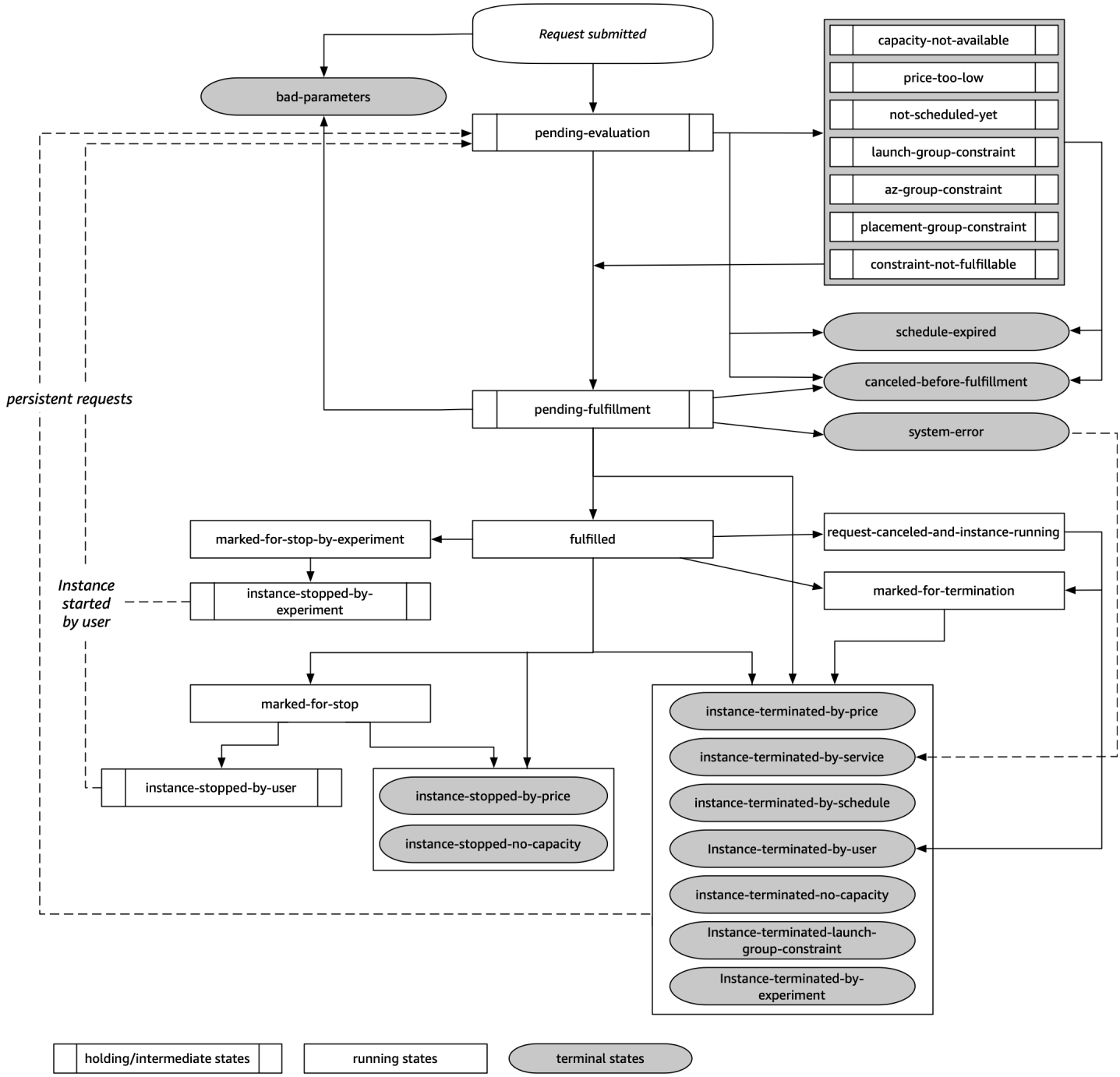
Voici un exemple de données pour cet événement.

```
{
    "version": "0",
    "id": "01234567-1234-0123-1234-012345678901",
    "detail-type": "EC2 Spot Instance Request Fulfillment",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "spot-instance-request-id": "sir-1a2b3c4d",
        "instance-id": "i-1234567890abcdef0"
    }
}
```

Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.

Changements d'état pour une demande Spot

Le diagramme suivant illustre les étapes suivies par votre demande d'instance Spot au cours de son cycle de vie, de la soumission à la mise hors service. Chaque étape est représentée sous forme d'un nœud et le code de statut de chaque nœud décrit le statut de la demande d'instance Spot et de l'instance Spot.



Évaluation en attente

Dès que vous créez une demande d'instance Spot, celle-ci passe à l'état `pending-evaluation` à moins qu'un ou plusieurs paramètres de demande ne soient pas valides (`bad-parameters`).

Code d'état	État de la demande	État de l'instance
`pending-evaluation`	`open`	Ne s'applique pas
`bad-parameters`	`closed`	Ne s'applique pas

En attente

Si une ou plusieurs contraintes de demande sont valides mais ne peuvent pas encore être respectées ou s'il n'y a pas suffisamment de capacité, la demande se voit attribuer l'état En attente jusqu'à ce que les contraintes soient respectées. Les options de la demande ont un impact sur les possibilités d'exécution de la demande. Par exemple, si la capacité n'est pas disponible, votre demande reste à l'état en attente jusqu'à ce que la capacité devienne disponible. Si vous spécifiez un groupe de zone de disponibilité, la demande conserve l'état En attente jusqu'à ce que la contrainte de zone de disponibilité soit respectée.

En cas de panne de l'une des zones de disponibilité, il est possible que la EC2 capacité inutilisée disponible pour les demandes d'instance ponctuelle dans d'autres zones de disponibilité soit affectée.

Code d'état	État de la demande	État de l'instance
`capacity-not-available`	`open`	Ne s'applique pas
`price-too-low`	`open`	Ne s'applique pas
`not-scheduled-yet`	`open`	Ne s'applique pas
`launch-group-constraint`	`open`	Ne s'applique pas
`az-group-constraint`	`open`	Ne s'applique pas
`placement-group-constraint`	`open`	Ne s'applique pas

Code d'état	État de la demande	État de l'instance
`constraint-not-fulfillable`	`open`	Ne s'applique pas

Fin de l'évaluation/exécution-terminal

Votre demande d'instance Spot peut passer à l'état `terminal` si vous créez une demande valide uniquement pendant une durée spécifique et que cette durée arrive à expiration avant que votre demande atteigne la phase d'exécution en attente. Cela peut également se produire si vous annulez la demande ou si une erreur système se produit.

Code d'état	État de la demande	État de l'instance
`schedule-expired`	`cancelled`	Ne s'applique pas
`canceled-before-fulfillment` [1]	`cancelled`	Ne s'applique pas
`bad-parameters`	`failed`	Ne s'applique pas
`system-error`	`closed`	Ne s'applique pas

[1] Si vous annulez la demande.

Exécution en attente

Lorsque les contraintes que vous avez spécifiées (le cas échéant) sont respectées, votre demande Spot passe à l'état `pending-fulfillment`.

À ce stade, Amazon s'EC2apprête à fournir les instances que vous avez demandées. Si le processus s'arrête à ce stade, il a probablement été annulé par l'utilisateur avant le lancement d'une instance Spot. Cela peut aussi être dû à une erreur système inattendue.

Code d'état	État de la demande	État de l'instance
`pending-fulfillment`	`open`	Ne s'applique pas

Exécutée

Lorsque toutes les caractéristiques de vos instances Spot sont respectées, votre demande d'instance Spot est satisfaite. Amazon EC2 lance les instances Spot, ce qui peut prendre quelques minutes. Si une instance Spot est mise en veille prolongée ou arrêtée lorsqu'elle est interrompue, elle reste dans cet état jusqu'à ce que la demande puisse être de nouveau satisfaite ou qu'elle soit annulée.

Code d'état	État de la demande	État de l'instance
`fulfilled`	`active`	`pending` → `running`
`fulfilled`	`active`	`stopped` → `running`

Si vous arrêtez une instance Spot, votre demande Spot passe à l'état `marked-for-stop` ou `instance-stopped-by-user` jusqu'à ce que l'instance Spot puisse être redémarrée ou que la demande soit annulée.

Code d'état	État de la demande	État de l'instance
`marked-for-stop`	`active`	`stopping`
`instance-stopped-by-user`[1]	`disabled` ou `cancelled` [2]	`stopped`

[1] Une instance Spot passe à l'état `instance-stopped-by-user` si vous arrêtez l'instance ou si vous exécutez la commande shutdown à partir de l'instance. Une fois l'instance arrêtée, vous pouvez la redémarrer. Au redémarrage, la demande d'instance Spot revient à son `pending-evaluation` état, puis Amazon EC2 lance une nouvelle instance Spot lorsque les contraintes sont satisfaites.

[2] L'état de la demande Spot est `disabled` si vous arrêtez l'instance Spot sans annuler la demande. L'état de la demande est `cancelled` si votre instance Sport est arrêtée et que la demande expire.

Exécuté-terminal

Vos instances Spot continuent de s'exécuter tant qu'il existe de la capacité pour votre type d'instance et que vous ne résiliez pas l'instance. Si Amazon EC2 doit résilier vos instances Spot, la demande Spot passe à l'état terminal. Une demande se voit attribuer l'état terminal si vous annulez la demande Spot ou si vous résiliez les instances Spot.

Code d'état	État de la demande	État de l'instance
`request-canceled-and-instance-running`	`cancelled`	`running`
`marked-for-stop`	`active`	`running`
`marked-for-termination`	`active`	`running`
`instance-stopped-by-price`	`disabled`	`stopped`
`instance-stopped-by-user`	`disabled`	`stopped`
`instance-stopped-no-capacity`	`disabled`	`stopped`
`instance-terminated-by-price`	`closed` (exceptionnelle), `open` (persistante)	`terminated`
`instance-terminated-by-schedule`	`closed`	`terminated`
`instance-terminated-by-service`	`cancelled`	`terminated`
`instance-terminated-by-user`	`closed` ou `cancelled` [1]	`terminated`
`instance-terminated-no-capacity`	`closed` (exceptionnelle), `open` (persistante)	`running` †

Code d'état	État de la demande	État de l'instance
`instance-terminated-no-capacity`	`closed` (exceptionnelle), `open` (persistante)	`terminated`
`instance-terminated-launch-group-constraint`	`closed` (exceptionnelle), `open` (persistante)	`terminated`

¹ L'état de la demande est `closed` si vous résiliez l'instance, mais que vous n'annulez pas la demande. L'état de la demande est `cancelled` si vous mettez l'instance hors service et que vous annulez la demande. Même si vous résiliez une instance Spot avant d'annuler sa demande, Amazon peut attendre un certain temps avant qu'Amazon ne EC2 détecte que votre instance Spot a été résiliée. Le cas échéant, l'état `closed` ou `cancelled` est attribué à la demande.

† Lorsqu'Amazon EC2 interrompt une instance Spot si elle a besoin de retrouver sa capacité et que l'instance est configurée pour s'arrêter en cas d'interruption, le statut est immédiatement défini sur `instance-terminated-no-capacity` (il n'est pas défini sur`marked-for-termination`). Toutefois, l'instance reste dans à l'état `running` pendant 2 minutes pour refléter la période de 2 minutes pendant laquelle elle reçoit l'avis d'interruption de l'instance Spot. Au bout de 2 minutes, l'état de l'instance est défini sur `terminated`.

Expériences d'interruption

Vous pouvez l'utiliser AWS Fault Injection Service pour déclencher une interruption d'instance Spot afin de tester la façon dont les applications de vos instances Spot répondent. Si AWS FIS une instance Spot est arrêtée, votre demande Spot entre dans l'`marked-for-stop-by-experiment`état puis dans l'`instance-stopped-by-experiment`état. En cas de AWS FIS résiliation d'une instance Spot, votre demande Spot entre dans l'`instance-terminated-by-experiment`état. Pour de plus amples informations, veuillez consulter the section called "Initier une interruption".

Code d'état	État de la demande	État de l'instance
`marked-for-stop-by-experiment`	`active`	`running`

Code d'état	État de la demande	État de l'instance
`instance-stopped-by-experiment`	`disabled`	`stopped`
`instance-terminated-by-experiment`	`closed`	`terminated`

Demandes persistantes

Lorsque vos instances Spot sont résiliées (par vous ou par AmazonEC2), si la demande Spot est une demande persistante, elle revient à l'`pending-evaluation`état et Amazon EC2 peut alors lancer une nouvelle instance Spot lorsque les contraintes sont satisfaites.

Marquer les demandes d'instance Spot

Pour vous aider à classer et à gérer vos demandes d'instance Spot, vous pouvez les marquer avec des métadonnées personnalisées. Vous pouvez affecter une balise à une demande d'instance Spot lorsque vous la créez, ou après. Vous pouvez attribuer des balises à l'aide de la EC2 console Amazon ou d'un outil de ligne de commande.

Lorsque vous balisez une demande d'instance Spot, les instances et les volumes lancés par la demande d'instance Spot ne sont pas automatiquement balisés. Vous devez baliser explicitement les instances et les volumes lancés par la demande d'instance Spot. Vous pouvez affecter une balise à une instance Spot et à des volumes pendant le lancement, ou après.

Pour plus d'informations sur le fonctionnement des balises, consultez Marquez vos EC2 ressources Amazon.

Table des matières

Prérequis

Octroyez à l'utilisateur l'autorisation de baliser les ressources. Pour plus d'informations sur IAM les politiques et des exemples de politiques, consultezExemple : Baliser des ressources.

La IAM politique que vous créez est déterminée par la méthode que vous utilisez pour créer une demande d'instance Spot.

- Si vous utilisez l'assistant de lancement d'instance ou `run-instances` pour demander Instances Spot, consultez To grant a user the permission to tag resources when using the launch instance wizard or run-instances.
- Si vous utilisez la commande `request-spot-instances` pour demander des instances Spot, consultez To grant a user the permission to tag resources when using request-spot-instances.

Pour accorder à un utilisateur l'autorisation de baliser des ressources lors de l'utilisation de l'assistant de lancement d'instance ou de run-instances

Créez une IAM politique qui inclut les éléments suivants :

- L'action `ec2:RunInstances`. Cela accorde à l'utilisateur l'autorisation de lancer une instance.
- Pour `Resource`, spécifiez `spot-instances-request`. Cela permet aux utilisateurs de créer des demandes d'instance Spot, qui demandent des instances Spot.
- L'action `ec2:CreateTags`. Celle-ci accorde à l'utilisateur l'autorisation de créer des balises.
- Pour `Resource`, spécifiez `*`. Cela permet aux utilisateurs de baliser toutes les ressources créées lors du lancement de l'instance.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowLaunchInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
```

```
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagSpotInstanceRequests",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Lorsque vous utilisez cette RunInstances action pour créer des demandes d'instance ponctuelle et que vous balisez les demandes d'instance ponctuelle lors de la création, vous devez savoir comment Amazon EC2 évalue la `spot-instances-request` ressource dans la RunInstances déclaration selon laquelle elle est évaluée dans la IAM politique comme suit :

- Si vous ne balisez pas une demande d'instance Spot lors de la création, Amazon EC2 n'évalue pas la `spot-instances-request` ressource dans la RunInstances déclaration.
- Si vous balisez une demande d'instance Spot lors de la création, Amazon EC2 évalue la `spot-instances-request` ressource dans le RunInstances relevé.

Par conséquent, pour la `spot-instances-request` ressource, les règles suivantes s'appliquent à la IAM politique :

- Si vous avez l' RunInstances habitude de créer une demande d'instance ponctuelle et que vous n'avez pas l'intention de baliser la demande d'instance ponctuelle lors de la création, vous n'avez pas besoin d'autoriser explicitement la `spot-instances-request` ressource ; l'appel aboutira.
- Si vous avez l' RunInstances habitude de créer une demande d'instance Spot et que vous avez l'intention de baliser la demande d'instance Spot lors de sa création, vous devez inclure la `spot-instances-request` ressource RunInstances dans l'instruction d'autorisation, sinon l'appel échouera.
- Si vous avez l' RunInstances habitude de créer une demande d'instance Spot et que vous avez l'intention de baliser la demande d'instance Spot lors de sa création, vous devez spécifier la

`spot-instances-request` ressource ou inclure un `*` caractère générique dans CreateTags l'instruction d'autorisation, sinon l'appel échouera.

Par exemple, IAM les politiques, y compris les politiques qui ne sont pas prises en charge pour les demandes d'instance Spot, voirUtiliser instances Spot.

Pour accorder à un utilisateur l'autorisation de baliser des ressources lorsqu'il utilise request-spot-instances

Créez une IAM politique qui inclut les éléments suivants :

- L'action `ec2:RequestSpotInstances`. Cela accorde à l'utilisateur l'autorisation de créer une demande d'instance Spot.
- L'action `ec2:CreateTags`. Celle-ci accorde à l'utilisateur l'autorisation de créer des balises.
- Pour `Resource`, spécifiez `spot-instances-request`. Cela permet aux utilisateurs de baliser uniquement la demande d'instance Spot.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotInstanceRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:RequestSpotInstances",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-instances-request/*"
}
```

Baliser une nouvelle demande d'instance Spot

Console

Pour baliser une nouvelle demande d'instance Spot à l'aide de la console

1. Suivez la procédure Gérez vos instances Spot.

2. Pour ajouter une balise, sur la page Ajouter des balises , choisissez Ajouter une balise, puis entrez la clé et la valeur de la balise. Choisissez Ajouter une autre balise pour chaque balise supplémentaire.

   Pour chaque balise, vous pouvez baliser la demande d'instance Spot, les instances Spot et les volumes avec la même balise. Pour baliser les trois, assurez-vous que instances, Volumes, et Demandes d'instance Spot sont sélectionnés. Pour n'en baliser qu'une ou deux, assurez-vous que les ressources que vous souhaitez baliser sont sélectionnées et que les autres ressources sont effacées.

3. Remplissez les champs obligatoires pour créer une demande d'instance Spot, puis choisissez Lancer. Pour de plus amples informations, veuillez consulter Gérez vos instances Spot.

AWS CLI

Pour étiqueter une nouvelle demande d'instance Spot à l'aide du AWS CLI

Pour étiqueter une demande d'instance Spot lors de sa création, configurez la demande d'instance Spot comme suit :

- Spécifiez les balises de la demande d'instance Spot à l'aide du paramètre `--tag-specification`.
- Pour `ResourceType`, spécifiez `spot-instances-request`. Si vous indiquez une autre valeur, la demande d'instance Spot échouera.
- Pour `Tags`, spécifiez la paire clé-valeur. Vous pouvez définir plus d'une paire clé-valeur.

Dans l'exemple suivant, la demande d'instance Spot est marquée par deux balises : Key=Environment et Value=Production, ainsi que Key=Cost-Center et Value=123.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json \
    --tag-specification 'ResourceType=spot-instances-
request,Tags=[{Key=Environment,Value=Production},{Key=Cost-Center,Value=123}]'
```

Baliser une demande d'instance Spot existante

Console

Pour baliser une demande d'instance Spot existante à l'aide de la console

Après avoir créé une demande d'instance Spot, vous pouvez ajouter des balises à la demande d'instance Spot à l'aide de la console.

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande d'instance Spot.
4. Choisissez l'onglet Tags (Balises), puis Create Tag (Créer une balise).

Pour baliser une instance Spot existante à l'aide de la console

Une fois que votre demande d'instance Spot a lancé votre instance Spot, vous pouvez ajouter des balises à l'instance à l'aide de la console. Pour de plus amples informations, veuillez consulter Ajouter et supprimer des tags à l'aide de la console.

AWS CLI

Pour baliser une demande d'instance Spot ou une instance Spot existante à l'aide du AWS CLI

Utilisez la commande create-tags pour baliser les ressources existantes. Dans l'exemple suivant, la demande d'instance Spot existante et l'instance Spot sont balisées avec Key=purpose et Value=test.

```
aws ec2 create-tags \
    --resources sir-08b93456 i-1234567890abcdef0 \
    --tags Key=purpose,Value=test
```

Afficher les balises de demande d'instance Spot

Console

Pour afficher les balises d'une demande d'instance Spot à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.

3. Sélectionnez votre demande d'instance Spot et choisissez l'onglet Balises.

AWS CLI

Pour décrire les balises de demande d'instance Spot

Vous pouvez consulter les balises d'une demande d'instance Spot en décrivant la demande d'instance Spot. Utilisez la describe-spot-instance-requestscommande pour afficher la configuration de la demande d'instance Spot spécifiée, qui inclut toutes les balises spécifiées pour la demande.

```
aws ec2 describe-spot-instance-requests \
    --spot-instance-request-ids sir-EXAMPLE1 \
    --query "SpotInstanceRequests[*].Tags"
```

Voici un exemple de sortie.

```
[
    [
        {
            "Key": "Environment",
            "Value": "Production"
        },
        {
            "Key": "Department",
            "Value": "101"
        }
    ]
]
```

Annuler une demande d'instance Spot

Si vous n'avez plus besoin de votre demande d'instance Spot, vous pouvez l'annuler. Vous pouvez ne pouvez annuler que les demandes d'instances Spot qui sont `open`, `active`, ou `disabled`.

- Votre demande d'instance Spot est `open` lorsqu'elle n'a pas encore été exécutée et si aucune instance n'a été lancée.
- Votre demande d'instance Spot est `active` lorsqu'elle a été satisfaite et que les instances Spot ont été lancées en conséquence.

- Votre demande d'instance Spot est `disabled` lorsque vous arrêtez votre instance Spot.

Si votre demande d'instance Spot est `active` et qu'elle est associée à une instance Spot en cours d'exécution, l'annulation de la demande ne résilie pas l'instance. Pour plus d'informations sur la résiliation d'une instance Spot, consultez Résilier une instance Spot.

Console

Pour annuler une demande d'instance Spot à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez la demande d'instance Spot.
4. Choisissez Actions, Annuler la demande.
5. (Facultatif) Si vous n'avez plus besoin d'utiliser les instances Spot associées, vous pouvez les résilier. Dans la boîte de dialogue Annuler la demande Spot sélectionnez Terminer les instances, puis choisissez Confirmer.

AWS CLI

Pour annuler une demande d'instance Spot à l'aide du AWS CLI

Utilisez la cancel-spot-instance-requestscommande pour annuler la demande d'instance Spot spécifiée.

```
aws ec2 cancel-spot-instance-requests --spot-instance-request-ids sir-08b93456
```

Gérez vos instances Spot

Amazon EC2 lance une instance Spot lorsque la capacité est disponible. Une instance Spot s'exécute jusqu'à ce qu'elle soit interrompue ou que vous la résiliiez.

Table des matières

- Résilier une instance Spot

Trouvez vos instances Spot

Une instance Spot apparaît sur la page Instances de la console, avec les instances à la demande. Utilisez la procédure suivante pour trouver vos instances Spot.

Console

Pour trouver vos instances Spot à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Pour trouver toutes les instances Spot, dans le volet de recherche, choisissez Instance lifecycle=spot.
4. Pour vérifier qu'une instance est une instance ponctuelle, sélectionnez l'instance, cliquez sur l'onglet Détails et vérifiez la valeur de Lifecycle. La valeur d'une instance ponctuelle est `spot` et celle d'une instance à la demande est`normal`.

AWS CLI

Pour trouver vos instances Spot à l'aide du AWS CLI

Utilisez la commande describe-instances avec l'`--filters`option.

```
aws ec2 describe-instances \
    --filters "Name=instance-lifecycle,Values=spot"
```

Pour déterminer si une instance est une instance ponctuelle

Utilisez la commande describe-instances, en utilisant l'`--query`option permettant de vérifier la valeur du cycle de vie.

```
aws ec2 describe-instances \
    --instance-ids i-0123a456700123456 \
    --query "Reservations[*].Instances[*].InstanceLifecycle" \
    --output text
```

Si le résultat est le cas`spot`, l'instance est une instance Spot. S'il n'y a aucune sortie, l'instance est une instance à la demande.

Utilisez la procédure suivante pour rechercher les instances Spot lancées à partir d'une demande d'instance Spot ou de flotte Spot spécifique.

Console

Pour trouver les instances Spot pour une demande à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot. La liste contient à la fois les demandes d'instance Spot et les demandes de parc Spot.
3. Si une demande d'instance Spot est satisfaite, Capacity est l'ID de l'instance Spot. Pour un parc d'instances Spot, le champ Capacité indique la part de la capacité demandée qui a été satisfaite. Pour afficher les instances IDs d'un parc ponctuel, cliquez sur la flèche d'extension ou sélectionnez le parc et choisissez Instances.
4. Pour une flotte ponctuelle, la capacité indique la quantité de capacité demandée qui est atteinte. Pour afficher les instances IDs d'un parc Spot, choisissez l'ID du parc pour ouvrir sa page de détails et localiser le volet Instances.

AWS CLI

Pour trouver les instances ponctuelles pour une demande à l'aide du AWS CLI

Utilisez la describe-spot-instance-requestscommande avec l'`--query`option.

```
aws ec2 describe-spot-instance-requests \
    --query "SpotInstanceRequests[*].{ID:InstanceId}"
```

Voici un exemple de sortie :

```
[
    {
        "ID": "i-1234567890abcdef0"
    },
    {
        "ID": "i-0598c7d356eba48d7"
```

```
    }
]
```

Arrêt d'une instance Spot

Si vous n'avez pas besoin de vos instances Spot pour le moment, mais que vous souhaitez les redémarrer ultérieurement sans perdre les données conservées dans le EBS volume Amazon, vous pouvez les arrêter. Les étapes d'arrêt d'une instance Spot sont similaires à celles de l'arrêt d'une instance à la demande.

> **Note**
>
> Pendant qu'une instance Spot est arrêtée, vous pouvez modifier certains de ses attributs, mais pas le type d'instance.
> Nous ne facturons pas l'utilisation d'une instance Spot arrêtée, ni les frais de transfert de données, mais nous facturons le stockage pour tous les EBS volumes Amazon.

Limites

- Vous ne pouvez arrêter une instance Spot que si elle a été lancée à partir d'une demande d'instance Spot `persistent`.
- Vous ne pouvez pas arrêter une instance Spot si la demande d'instance Spot associée est annulée. Lorsque la demande d'instance Spot est annulée, vous ne pouvez que résilier l'instance Spot.
- Vous ne pouvez pas arrêter une instance Spot si elle fait partie d'une flotte, d'un groupe de lancement ou d'un groupe de zone de disponibilité.

Console

Pour arrêter une instance Spot à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance Spot. Si vous n'avez pas enregistré l'ID d'instance de l'instance Spot, consultezthe section called "Trouvez vos instances Spot".
4. Choisissez État de l'instance, Arrêter l'instance.

5. Lorsque vous êtes invité à confirmer l'opération, choisissez Arrêter.

AWS CLI

Pour arrêter une instance Spot à l'aide du AWS CLI

Utilisez la commande stop-instances pour arrêter manuellement vos instances Spot.

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

Démarrer une instance Spot

Vous pouvez démarrer une instance Spot que vous avez précédemment arrêtée.

Prérequis

Vous pouvez démarrer une instance Spot uniquement si :

- Vous avez manuellement arrêté l'instance Spot.
- L'instance Spot est une instance EBS sauvegardée.
- La capacité d'instance Spot est disponible.
- Le prix Spot est inférieur à votre prix maximum.

Limites

- Vous ne pouvez pas démarrer une instance Spot qui fait partie d'une flotte, d'un groupe de lancement ou d'un groupe de zone de disponibilité.

Les étapes du démarrage d'une instance Spot sont similaires à celles du démarrage d'une instance à la demande.

Console

Pour démarrer une instance Spot à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.

3. Sélectionnez l'instance Spot. Si vous n'avez pas enregistré l'ID d'instance de l'instance Spot, consultezthe section called "Trouvez vos instances Spot".
4. Choisissez État de l'instance, Démarrer l'instance.

AWS CLI

Pour démarrer une instance Spot, AWS CLI

Utilisez la commande start-instances pour démarrer manuellement vos instances Spot.

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

Résilier une instance Spot

Si vous résiliez une instance Spot en cours d'exécution ou arrêtée qui a été lancée par une demande d'instance Spot persistante, la demande d'instance Spot passe à l'état `open` pour qu'une nouvelle instance Spot puisse être lancée. Pour vous assurer qu'aucune nouvelle instance Spot ne soit lancée, vous devez d'abord annuler la demande d'instance Spot.

Si vous annulez une demande d'instance Spot `active` qui comporte une instance Spot en cours d'exécution, celle-ci n'est pas résiliée automatiquement. Vous devez la résilier manuellement.

Si vous annulez une demande d'instance `disabled` Spot dont une instance Spot est arrêtée, l'instance Spot arrêtée est automatiquement résiliée par le service Amazon EC2 Spot. Il peut y avoir un bref décalage entre le moment où vous annulez la demande d'instance Spot et celui où le service Spot résilie l'instance Spot.

Pour de plus amples informations, veuillez consulter Annuler une demande d'instance Spot.

Console

Pour résilier manuellement une instance Spot à l'aide de la console

1. Avant de mettre fin à une instance, vérifiez que vous ne perdrez aucune donnée en vérifiant que vos EBS volumes Amazon ne seront pas supprimés lors de la résiliation et que vous avez copié toutes les données dont vous avez besoin depuis les volumes de stockage de votre instance vers un stockage persistant, tel qu'Amazon EBS ou Amazon S3.
2. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

3. Dans le panneau de navigation, choisissez Instances.
4. Sélectionnez l'instance Spot. Si vous n'avez pas enregistré l'ID d'instance de l'instance Spot, consultezthe section called "Trouvez vos instances Spot".
5. Choisissez État de l'instance, puis Terminer (supprimer) l'instance.
6. Choisissez Terminate (supprimer) lorsque vous êtes invité à confirmer.

AWS CLI

Pour mettre fin manuellement à une instance Spot à l'aide du AWS CLI

Utilisez la commande terminate-instances pour mettre fin manuellement à vos instances Spot.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7
```

Interruptions d'instance Spot

Vous pouvez lancer des instances Spot sur de la EC2 capacité inutilisée pour bénéficier de remises importantes en échange de leur retour lorsqu'Amazon EC2 a besoin de récupérer la capacité. Lorsqu'Amazon EC2 récupère une instance Spot, nous appelons cet événement une interruption d'instance Spot.

La demande d'instances ponctuelles peut varier considérablement d'un moment à l'autre, et la disponibilité des instances ponctuelles peut également varier considérablement en fonction du nombre d'EC2instances non utilisées disponibles. Il est toujours possible que votre instance Spot soit interrompue. Voici les raisons possibles pour lesquelles Amazon EC2 peut interrompre vos instances Spot :

Capacité

Amazon EC2 peut interrompre votre instance Spot lorsqu'elle a besoin de la récupérer. EC2récupère votre instance principalement pour réutiliser la capacité, mais cela peut également se produire pour d'autres raisons, telles que la maintenance de l'hôte ou la mise hors service du matériel.

Prix

Le prix Spot est supérieur à votre prix maximum.

Vous pouvez spécifier le prix maximum dans votre demande Spot. Cependant, si vous spécifiez un prix maximal, vos instances seront interrompues plus fréquemment que si vous ne le spécifiez pas.

Contraintes

Si votre demande comprend une exigence telle qu'un groupe de lancement ou un groupe de zone de disponibilité, les instances Spot sont résiliées en tant que groupe lorsque l'exigence n'est plus respectée.

Lorsqu'Amazon EC2 interrompt une instance Spot, il met fin à l'instance, l'arrête ou la met en veille prolongée, selon le comportement d'interruption que vous avez spécifié lors de la création de la demande Spot.

Table des matières

Comportement des interruptions des instances Spot

Lorsque vous créez une demande Spot, vous pouvez spécifier le comportement d'interruption. Les comportements d'interruption possibles sont les suivants :

- Arrêter
- Mise en veille prolongée
- Terminer

Le comportement par défaut est qu'Amazon EC2 met fin aux instances Spot lorsqu'elles sont interrompues.

Arrêter l'instances Spot interrompue

Vous pouvez spécifier qu'Amazon EC2 arrête vos instances Spot lorsqu'elles sont interrompues. Le type de la demande d'instance Spot doit être `persistent`. Vous ne pouvez pas spécifier de groupe de lancement dans la demande d'instance Spot. Pour EC2 Fleet ou Spot Fleet, le type de demande doit être`maintain`.

Considérations

- Seul Amazon EC2 peut redémarrer une instance Spot interrompue.
- Pour une instance ponctuelle lancée par une demande d'instance `persistent` ponctuelle : Amazon EC2 redémarre l'instance arrêtée lorsque la capacité est disponible dans la même zone de disponibilité et pour le même type d'instance que l'instance arrêtée (les mêmes spécifications de lancement doivent être utilisées).
- Pendant qu'une instance Spot est arrêtée, vous pouvez modifier certains de ses attributs, mais pas le type d'instance. Si vous détachez ou supprimez un EBS volume, il n'est pas attaché au démarrage de l'instance Spot. Si vous détachez le volume racine et qu'Amazon EC2 tente de démarrer l'instance Spot, celle-ci ne démarrera pas et Amazon EC2 mettra fin à l'instance arrêtée.
- Vous pouvez résilier une instance Spot pendant qu'elle est arrêtée.
- Si vous annulez une demande d'instance ponctuelle, un EC2 parc ou un parc d'instances ponctuelles, Amazon EC2 met fin à toutes les instances ponctuelles associées qui sont arrêtées.
- Lorsqu'une instance Spot interrompue est arrêtée, seuls les EBS volumes conservés vous sont facturés. Avec EC2 Fleet et Spot Fleet, si vous avez de nombreuses instances arrêtées, vous pouvez dépasser la limite du nombre de EBS volumes pour votre compte. Pour plus d'informations sur la facturation lorsqu'une instance Spot est interrompue, consultez Facturation des instances Spot interrompues.
- Assurez-vous de bien savoir ce que l'arrêt d'une instance implique. Pour des informations sur ce qui se produit lors de l'arrêt d'une instance, consultez Différences entre les états des instances.

Mettre les instances Spot interrompues en veille prolongée

Vous pouvez spécifier qu'Amazon EC2 met en veille prolongée vos instances Spot lorsqu'elles sont interrompues. Pour de plus amples informations, veuillez consulter Hibernez votre instance Amazon EC2.

Amazon propose EC2 désormais la même expérience d'hibernation pour les instances Spot que celle actuellement disponible pour les instances à la demande. Cette expérience offre une prise en charge

complète, les éléments suivants étant désormais pris en charge pour la mise en veille prolongée des instances Spot :

- Plus pris en charge AMIs
- Plus de familles d'instances prises en charge
- Mise en veille prolongée à l'initiative de l'utilisateur

Résilier les instances Spot interrompues

Lorsqu'Amazon EC2 interrompt une instance Spot, il met fin à l'instance par défaut, sauf si vous spécifiez un comportement d'interruption différent, tel que stop ou hibernation. Pour de plus amples informations, veuillez consulter Mettre fin aux EC2 instances Amazon.

Préparez-vous aux interruptions des instances Spot

La demande d'instances ponctuelles peut varier considérablement d'un moment à l'autre, et la disponibilité des instances ponctuelles peut également varier considérablement en fonction du nombre d'EC2instances non utilisées disponibles. Il est toujours possible que votre instance Spot soit interrompue. Par conséquent, vous devez veiller à ce que votre application soit préparée à une interruption d'instance Spot.

Nous vous recommandons de suivre ces bonnes pratiques afin de vous préparer à subir une interruption d'instance Spot.

- Créez votre demande Spot à l'aide d'un groupe Auto Scaling. Si vos instances Spot sont interrompues, le groupe Auto Scaling lancera automatiquement les instances de remplacement. Pour plus d'informations, consultez la section Groupes Auto Scaling avec plusieurs types d'instances et options d'achat dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.
- Assurez-vous que votre instance est prête à fonctionner dès que la demande est traitée en utilisant une Amazon Machine Image (AMI) contenant la configuration logicielle requise. Vous pouvez également utiliser les données utilisateur afin d'exécuter les commandes lors du démarrage.
- Les données stockées sur des volumes de stockage d'instance sont perdues lorsque l'instance est arrêtée ou résiliée. Sauvegardez toutes les données importantes relatives aux volumes de stockage d'instance vers un stockage plus persistant, tel qu'Amazon S3EBS, Amazon ou Amazon DynamoDB.
- Stockez les données importantes régulièrement à un emplacement qui n'est pas touché par la résiliation de l'instance Spot. Par exemple, vous pouvez utiliser Amazon S3EBS, Amazon ou DynamoDB.

- Divisez le travail en petites tâches (à l'aide d'une architecture Grid, Hadoop ou reposant sur les files d'attente) ou utilisez des points de contrôle afin de pouvoir enregistrer votre travail fréquemment.
- Amazon EC2 envoie un signal de recommandation de rééquilibrage à l'instance Spot lorsque celle-ci présente un risque élevé d'interruption. Vous pouvez vous fier à la recommandation de rééquilibrage pour gérer de manière proactive les interruptions d'instance Spot sans avoir à attendre l'avis d'interruption d'instance Spot à deux minutes. Pour plus d'informations, consultez EC2recommandations de rééquilibrage des instances.
- Utilisez les avis d'interruption d'instance Spot à deux minutes pour surveiller le statut de vos instances Spot. Pour plus d'informations, consultez Avis d'interruption d'instance Spot..
- Même si nous nous efforçons de vous communiquer ces avertissements dès que possible, il se peut que votre instance Spot soit interrompue avant que les avertissements puissent être mis à disposition. Testez votre application afin de vous assurer qu'elle peut gérer correctement une interruption inattendue d'une instance, même si vous surveillez les signaux de recommandation de rééquilibrage et les avis d'interruption. Pour cela, exécutez l'application en utilisant une instance à la demande, puis résiliez vous-même cette instance à la demande.
- Exécutez une expérience d'injection de pannes contrôlée AWS Fault Injection Service pour tester la façon dont votre application réagit lorsque votre instance Spot est interrompue. Pour plus d'informations, consultez le Tutorial: Test Spot Instance interruptions using AWS FIS dans le Guide de l'utilisateur AWS Fault Injection Service .

Lancement d'une interruption d'instance Spot

Vous pouvez sélectionner une demande d'instance Spot ou une demande de parc Spot dans la EC2 console Amazon et lancer une interruption d'instance Spot afin de tester la façon dont les applications de vos instances Spot gèrent les interruptions. Lorsque vous initiez une interruption d'instance Spot, Amazon vous EC2 informe que votre instance Spot sera interrompue dans deux minutes, puis qu'elle sera interrompue au bout de deux minutes.

Le service sous-jacent qui effectue l'interruption de l'instance Spot est AWS Fault Injection Service (AWS FIS). Pour plus d'informations sur AWS FIS, voir AWS Fault Injection Service.

> **Note**
>
> Les comportements d'interruption sont `terminate`, `stop`, et `hibernate`. Si le comportement d'interruption défini est `hibernate`, lorsque vous lancez l'interruption d'une instance Spot, le processus de mise en veille commence immédiatement.

Le lancement d'une interruption d'instance Spot est pris en charge dans tous les pays Régions AWS sauf en Asie-Pacifique (Jakarta), en Asie-Pacifique (Osaka), en Chine (Pékin), en Chine (Ningxia) et au Moyen-Orient (UAE).

Table des matières

Lancer une interruption d'instance Spot

Vous pouvez utiliser la EC2 console pour déclencher rapidement une interruption d'instance Spot. Lorsque vous sélectionnez une demande d'instance Spot, vous pouvez lancer l'interruption d'une instance Spot. Lorsque vous sélectionnez une demande de parc d'instances Spot, vous pouvez lancer l'interruption de plusieurs instances Spot à la fois.

Pour des tests plus avancés visant à tester les interruptions des instances Spot, vous pouvez créer vos propres tests à l'aide de la AWS FIS console.

Pour initier l'interruption d'une instance Spot dans une demande d'instance Spot à l'aide de la EC2 console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Spot Requests (Demandes Spot).
3. Sélectionnez une demande d'instance Spot, puis sélectionnez Actions, Initiate interruption (Lancer une interruption). Vous ne pouvez pas sélectionner plusieurs demandes d'instance Spot pour lancer une interruption.
4. Dans la boîte de dialogue Initiate Spot Instance interruption (Lancer une interruption d'instance Spot), sous Service access (Accès à un service), utilisez le rôle par défaut ou sélectionnez un

rôle existant. Pour choisir un rôle existant, choisissez Utiliser un rôle de service existant, puis, pour IAMrôle, sélectionnez le rôle à utiliser.

5. Lorsque vous êtes prêt à lancer l'interruption de l'instance Spot, sélectionnez Initiate interruption (Lancer l'interruption).

Pour initier l'interruption d'une ou de plusieurs instances Spot dans une demande de parc Spot à l'aide de la EC2 console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Spot Requests (Demandes Spot).
3. Sélectionnez une demande de parc d'instances Spot, puis sélectionnez Actions, Lancer une interruption. Vous ne pouvez pas sélectionner plusieurs demandes de parc d'instances Spot pour lancer une interruption.
4. Dans la boîte de dialogue Spécifier le nombre d'instances Spot, dans le champ Nombre d'instances à interrompre, saisissez le nombre d'instances Spot à interrompre, puis choisissez Confirmer.

> **Note**
>
> Le nombre ne peut pas dépasser le nombre d'instances ponctuelles du parc ou votre quota pour le nombre d'instances ponctuelles AWS FIS pouvant être interrompues par expérience.

5. Dans la boîte de dialogue Initiate Spot Instance interruption (Lancer une interruption d'instance Spot), sous Service access (Accès à un service), utilisez le rôle par défaut ou sélectionnez un rôle existant. Pour choisir un rôle existant, choisissez Utiliser un rôle de service existant, puis, pour IAMrôle, sélectionnez le rôle à utiliser.
6. Lorsque vous êtes prêt à lancer l'interruption de l'instance Spot, sélectionnez Initiate interruption (Lancer l'interruption).

Pour créer des expériences plus avancées afin de tester les interruptions d'instances Spot à l'aide de la console AWS FIS

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Spot Requests (Demandes Spot).
3. Sélectionnez Actions, Create advanced experiments (Créer des expériences avancées).

La AWS FIS console s'ouvre. Pour plus d'informations, consultez Didacticiel : tester les interruptions d'instance Spot à l'aide de AWS FIS dans le Guide de l'utilisateur AWS Fault Injection Service .

Vérifier l'interruption d'instance Spot

Après avoir lancé l'interruption, les événements suivants se produisent :

- L'instance Spot reçoit une recommandation de rééquilibrage d'instance.
- Un avis d'interruption d'instance Spot est émis deux minutes avant l' AWS FIS interruption de votre instance.
- Après deux minutes, l'instance Spot est interrompue.
- Une instance Spot arrêtée par le AWS FIS reste jusqu'à ce que vous la redémarriez.

Pour vérifier que l'instance a été interrompue après le lancement de l'interruption

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Depuis le panneau de navigation, ouvrez Demandes Spot et Instances dans des onglets ou des fenêtres de navigateur distincts.
3. Pour les demandes Spot, sélectionnez la demande d'instance Spot ou la demande de parc d'instances Spot. L'état initial est `fulfilled`. Une fois l'instance interrompue, le statut change comme suit, en fonction du comportement d'interruption :
   - `terminate` – Le statut passe à `instance-terminated-by-experiment`.
   - `stop` – Le statut de l'instance passe à `marked-for-stop-by-experiment`, puis à `instance-stopped-by-experiment`.
4. Pour Instances, sélectionnez l'instance Spot. L'état initial est `Running`. Deux minutes après réception de l'avis d'interruption de l'instance Spot, le statut change comme suit, en fonction du comportement d'interruption :
   - `stop` – Le statut de l'instance passe à `Stopping`, puis à `Stopped`.
   - `terminate` – Le statut de l'instance passe à `Shutting-down`, puis à `Terminated`.

Quotas

Vous Compte AWS avez le quota par défaut suivant pour le nombre d'instances ponctuelles AWS FIS pouvant être interrompues par expérience.

Nom	Par défaut	Ajustable	Description
Cible SpotInstances pour aws:ec2 : send-spot-instance-interruptions	Chaque Région prise en charge : 5	Oui	Le nombre maximum d'instances ponctuelles que aws:ec2 : send-spot-instance-interruptions peut cibler lorsque vous identifiez des cibles à l'aide de balises, par expérience.

Vous pouvez demander une augmentation de quota. Pour de plus amples informations, veuillez consulter Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas.

Pour afficher tous les quotas pour AWS FIS, ouvrez la console Service Quotas. Dans le panneau de navigation, sélectionnez Services AWS , puis AWS Fault Injection Service. Vous pouvez également consulter tous les quotas pour AWS Fault Injection Service dans le guide de l'utilisateur AWS Fault Injection Service .

Avis d'interruption d'instance Spot.

Un avis d'interruption d'une instance Spot est un avertissement émis deux minutes avant qu'Amazon n'EC2arrête ou ne mette fin à votre instance Spot. Lorsque vous spécifiez la mise en veille comme comportement d'interruption, vous recevez un avis d'interruption, mais vous ne recevez pas d'avertissement de deux minutes car le processus de mise en veille commence immédiatement.

La meilleure façon pour vous de gérer fluidement les interruptions d'instance Spot consiste à concevoir votre application pour qu'elle soit tolérante aux pannes. Pour ce faire, vous pouvez vous servir des avis d'interruption d'instance Spot. Nous vous recommandons de vérifier ces avis d'interruption toutes les 5 secondes.

Les avis d'interruption sont mis à disposition en tant qu' EventBridge événement et en tant qu'éléments dans les métadonnées de l'instance Spot. Les avis d'interruption sont créés sur la base du meilleur effort.

EC2 Spot Instance Interruption Warning event

Lorsqu'Amazon EC2 va interrompre votre instance Spot, elle émet un événement deux minutes avant l'interruption effective (sauf pour l'hibernation, qui reçoit l'avis d'interruption, mais pas deux minutes à l'avance, car l'hibernation commence immédiatement). Cet événement peut être détecté par Amazon EventBridge. Pour plus d'informations sur EventBridge les événements, consultez le guide de EventBridge l'utilisateur Amazon. Pour un exemple détaillé expliquant comment créer et utiliser des règles relatives aux événements, consultez Taking Advantage of Amazon EC2 Spot Instance Interruption Notices.

Vous trouverez ci-dessous un exemple d'événement pour une interruption d'instance Spot. Les valeurs possibles pour `instance-action` sont `hibernate`, `stop` ou `terminate`.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Spot Instance Interruption Warning",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2a:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0",
        "instance-action": "action"
    }
}
```

> **Note**
>
> Le ARN format de l'événement d'interruption de l'instance Spot est`arn:aws:ec2:availability-zone:instance/instance-id`. Ce format est différent du ARNformat de EC2 ressource.

instance-action

L'`instance-action`élément indique l'action et l'heure approximative à UTC laquelle l'action aura lieu.

Si votre instance Spot est marquée comme devant être arrêtée ou résiliée par AmazonEC2, l'`instance-action`élément est présent dans les métadonnées de votre instance. Sinon, il n'est pas présent. Vous pouvez les récupérer `instance-action` à l'aide du service de métadonnées d'instance version 2 (IMDSv2) comme suit.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/spot/instance-action
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/instance-action
```

L'exemple de sortie suivant indique la date et l'heure auxquelles cette instance sera arrêtée.

```
{"action": "stop", "time": "2017-09-18T08:22:00Z"}
```

L'exemple de sortie suivant indique la date et l'heure auxquelles cette instance sera résiliée.

```
{"action": "terminate", "time": "2017-09-18T08:22:00Z"}
```

Si Amazon ne s'EC2apprête pas à arrêter ou à mettre fin à l'instance, ou si vous l'avez résiliée vous-même, `instance-action` cela ne figure pas dans les métadonnées de l'instance et vous recevez une erreur HTTP 404 lorsque vous essayez de la récupérer.

termination-time

L'`termination-time`élément indique l'heure approximative à UTC laquelle l'instance recevra le signal d'arrêt.

> **Note**
>
> Cet élément est conservé à des fins de compatibilité descendante ; nous vous invitons à utiliser `instance-action` à la place.

Si votre instance Spot est marquée comme devant être résiliée par Amazon EC2 (soit en raison d'une interruption d'instance ponctuelle pour laquelle le comportement d'interruption est défini sur`terminate`, soit en raison de l'annulation d'une demande d'instance ponctuelle persistante), l'`termination-time`élément est présent dans les métadonnées de votre instance. Sinon, il n'est pas présent. Vous pouvez récupérer l'`termination-time`utilisation IMDSv2 comme suit.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`
[ec2-user ~]$ if curl -H "X-aws-ec2-metadata-token: $TOKEN" -s
 http://169.254.169.254/latest/meta-data/spot/termination-time | grep -q .*T.*Z;
 then echo termination_scheduled; fi
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/termination-time
```

Voici un exemple de sortie.

```
2015-01-05T18:02:00Z
```

Si Amazon ne EC2 se prépare pas à mettre fin à l'instance (soit parce qu'il n'y a pas d'interruption de l'instance Spot, soit parce que votre comportement d'interruption est défini sur `stop` ou`hibernate`), soit si vous avez résilié l'instance Spot vous-même, l'`termination-time`élément n'est pas présent dans les métadonnées de l'instance (vous recevez donc une erreur HTTP 404) ou contient une valeur qui n'est pas une valeur temporelle.

Si Amazon EC2 ne parvient pas à mettre fin à l'instance, le statut de la demande est défini sur`fulfilled`. La valeur `termination-time` reste dans les métadonnées de l'instance avec l'heure approximative initiale, qui se trouve maintenant dans le passé.

Identifier des instances Spot interrompues

Dans la console, le volet Instances affiche toutes les instances, y compris Instances Spot. Le cycle de vie d'une instance Spot est `spot`. L'état de l'instance d'une instance Spot est soit `stopped` ou `terminated`, en fonction du comportement d'interruption que vous avez configuré. Pour une instance Spot mise en veille de manière prolongée, l'état de l'instance est `stopped`.

Pour rechercher une instance Spot interrompue à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Appliquez le filtre suivant : Instance lifecycle=spot.
4. Appliquez le filtre Instance state=stopped ou Instance state=terminated en fonction du comportement d'interruption que vous avez configuré.
5. Pour chaque instance Spot, dans l'onglet Détails, sous Détails de l'instance, recherchez le message de transition d'état. Les codes suivants indiquent que l'instance Spot a été interrompue.
   - `Server.SpotInstanceShutdown`
   - `Server.SpotInstanceTermination`
6. Pour plus d'informations sur la raison de l'interruption, consultez le code d'état de la demande Spot. Pour de plus amples informations, veuillez consulter the section called "Obtenir le statut d'une demande d'instance Spot".

Pour rechercher des instances Spot interrompues à l'aide du AWS CLI

Vous pouvez répertorier les Instances Spot interrompues à l'aide de la commande describe-instances avec le paramètre `--filters`. Pour répertorier uniquement l'instance IDs dans la sortie, incluez le `--query` paramètre.

Si le comportement d'interruption de l'instance consiste à résilier les instances Spot, utilisez la commande suivante :

```
aws ec2 describe-instances \
```

```
    --filters Name=instance-lifecycle,Values=spot Name=instance-state-
name,Values=terminated Name=state-reason-code,Values=Server.SpotInstanceTermination \
    --query "Reservations[*].Instances[*].InstanceId"
```

Si le comportement d'interruption de l'instance consiste à arrêter les instances Spot, utilisez la commande suivante :

```
aws ec2 describe-instances \
    --filters Name=instance-lifecycle,Values=spot Name=instance-state-
name,Values=stopped Name=state-reason-code,Values=Server.SpotInstanceShutdown \
    --query "Reservations[*].Instances[*].InstanceId"
```

Déterminer si Amazon EC2 a résilié une instance Spot

Une instance Spot fonctionne jusqu'à ce qu'Amazon y mette EC2 fin en réponse à une interruption, ou jusqu'à ce que vous la résiliiez vous-même. Pour de plus amples informations, veuillez consulter the section called "Comportement d'interruption".

Après la résiliation d'une instance Spot, vous pouvez l'utiliser AWS CloudTrail pour voir si Amazon l'EC2a résiliée. Si le CloudTrail journal inclut un`BidEvictedEvent`, cela indique qu'Amazon a EC2 résilié l'instance Spot. Si au contraire vous voyez un `TerminateInstances` événement, cela indique qu'un utilisateur a résilié l'instance Spot.

Sinon, si vous souhaitez recevoir une notification indiquant qu'Amazon EC2 va interrompre votre instance Spot, utilisez Amazon EventBridge pour répondre à l'événement d'avertissement d'interruption d'instance EC2 Spot.

Pour consulter les BidEvictedEvent événements dans CloudTrail

1. Ouvrez la CloudTrail console à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sélectionnez Historique des événements.
3. Dans la liste des filtres, choisissez Nom de l'événement, puis entrez dans le champ de filtre à droite**`BidEvictedEvent`**.
4. (Facultatif) Sélectionnez une plage horaire.
5. Si la liste n'est pas vide, choisissez BidEvictedEventl'entrée qui en résulte pour ouvrir sa page de détails. Vous pouvez trouver des informations sur l'instance Spot dans le volet d'enregistrement des événements, y compris l'ID de l'instance Spot. Voici un exemple d'enregistrement d'événement.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "ec2.amazonaws.com"
    },
    "eventTime": "2016-08-16T22:30:00Z",
    "eventSource": "ec2.amazonaws.com",
    "userAgent": "ec2.amazonaws.com",
    "sourceIPAddress": "ec2.amazonaws.com",
    "eventName": "BidEvictedEvent",
    "awsRegion": "us-east-2",
    "eventID": "d27a6096-807b-4bd0-8c20-a33a83375054",
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "123456789012",
    "RequestParameters": null,
    "ResponseElements": null,
    "serviceEventDetails": {
        "instanceIdSet": [
          "i-1eb2ac8eEXAMPLE"
        ]
    }
}
```


6. Si vous n'avez pas trouvé d'entrée pour l'`BidEvictedEvent`événement, entrez le **`TerminateInstances`** nom de l'événement. Pour plus d'informations sur l'enregistrement d'événements pour`TerminateInstances`, consultezthe section called “Exemples d'EC2APIévénements Amazon”.

Facturation des instances Spot interrompues

Lorsqu'une instance Spot est interrompue, l'utilisation de l'instance et EBS du volume vous est facturée, et d'autres frais peuvent vous être facturés, comme suit.

Utilisation de l'instance

Qui interrompt l'instance Spot	Système d'exploitation	Interrompue au cours de la première heure	Interrompue au cours de toute heure après la première heure
Si vousArrêtez ou résiliez l'instance Spot	Windows et Linux (saufSUSE)	Les secondes utilisées sont facturées	Les secondes utilisées sont facturées
	SUSE	L'heure complète est facturée même si vous n'en avez utilisé qu'une partie	Les heures complètes utilisées sont facturées, et une heure complète est facturée pour l'heure partielle interrompue
Si Amazon EC2 interrompt l'instance Spot	Windows et Linux (saufSUSE)	Aucuns frais.	Les secondes utilisées sont facturées
	SUSE	Aucuns frais.	Les heures complètes utilisées sont facturées, mais l'heure partielle interrompue n'est pas facturée

EBSutilisation du volume

Lorsqu'une instance Spot interrompue est arrêtée, seuls les EBS volumes conservés vous sont facturés.

Avec EC2 Fleet et Spot Fleet, si vous avez de nombreuses instances arrêtées, vous pouvez dépasser la limite du nombre de EBS volumes pour votre compte.

EC2recommandations de rééquilibrage des instances

Une recommandation de rééquilibrage d'EC2instance est un signal qui vous avertit lorsqu'une instance Spot présente un risque élevé d'interruption. Le signal peut arriver plus tôt que l'avis d'interruption d'instance Spot à deux minutes, ce qui vous donne la possibilité de gérer l'instance Spot de manière proactive. Vous pouvez décider de rééquilibrer votre charge de travail en une instances Spot nouvelle ou existante qui ne présente pas un risque élevé d'interruption.

Il n'est pas toujours possible pour Amazon d'EC2envoyer le signal de recommandation de rééquilibrage avant l'avis d'interruption de deux minutes de l'instance Spot. Par conséquent, le signal de recommandation de rééquilibrage peut arriver avec l'avis d'interruption de deux minutes.

Les recommandations de rééquilibrage sont mises à disposition sous forme d' EventBridge événement et d'élément dans les métadonnées de l'instance Spot. Les événements sont générés dans la mesure du possible.

> **Note**
>
> Les recommandations de rééquilibrage ne sont prises en charge que pour les instances ponctuelles lancées après le 5 novembre 2020 à 00h00UTC.

Table des matières

Actions de rééquilibrage que vous pouvez effectuer

Voici quelques-unes des actions de rééquilibrage possibles que vous pouvez effectuer :

Arrêt normal

Lorsque vous recevez le signal de recommandation de rééquilibrage pour une instance Spot, vous pouvez démarrer vos procédures d'arrêt d'instance, ce qui peut inclure la garantie que les processus sont terminés avant de les arrêter. Par exemple, vous pouvez télécharger les journaux du système ou des applications vers Amazon Simple Storage Service (Amazon S3), vous pouvez arrêter SQS Amazon Workers ou vous pouvez annuler l'enregistrement auprès du système de

noms de domaine (). DNS Vous pouvez également enregistrer votre travail sur un stockage externe et le reprendre ultérieurement.

Empêcher la planification d'une nouvelle tâche

Lorsque vous recevez le signal de recommandation de rééquilibrage pour une instance Spot, vous pouvez empêcher la planification d'une nouvelle tâche sur l'instance, tout en continuant à utiliser l'instance jusqu'à ce que les tâches planifiées soient terminées.

Lancer de manière proactive de nouvelles instances de remplacement

Vous pouvez configurer les groupes Auto Scaling, EC2 Fleet ou Spot Fleet pour lancer automatiquement des instances Spot de remplacement lorsqu'un signal de recommandation de rééquilibrage est émis. Pour plus d'informations, consultez la section Utiliser le rééquilibrage de capacité pour gérer les interruptions d'Amazon EC2 Spot dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling et Utilisez le rééquilibrage des capacités dans le EC2 parc et le parc ponctuel pour remplacer les instances ponctuelles à risque dans ce guide de l'utilisateur.

Surveiller les signaux de recommandation de rééquilibrage

Vous pouvez surveiller le signal de recommandation de rééquilibrage afin que vous puissiez effectuer les actions spécifiées dans la section précédente lorsqu'il est émis. Le signal de recommandation de rééquilibrage est mis à disposition sous forme d'événement envoyé à Amazon EventBridge (anciennement Amazon CloudWatch Events) et sous forme de métadonnées d'instance sur l'instance Spot.

Surveiller les signaux de recommandation de rééquilibrage :

- Utilisez Amazon EventBridge
- Utiliser les métadonnées d'instance

Utilisez Amazon EventBridge

Lorsque le signal de recommandation de rééquilibrage est émis pour une instance Spot, l'événement correspondant au signal est envoyé à Amazon EventBridge. S'il EventBridge détecte un modèle d'événement correspondant à un modèle défini dans une règle, EventBridge invoque une cible (ou des cibles) spécifiée dans la règle.

Voici un exemple d'événement pour le signal de recommandation de rééquilibrage.

```
{
```

```
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Instance Rebalance Recommendation",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0"
    }
}
```

Les champs suivants forment le modèle d'événement défini dans la règle :

`"detail-type": "EC2 Instance Rebalance Recommendation"`

Identifie que l'événement est un événement de recommandation de rééquilibrage

`"source": "aws.ec2"`

Identifie que l'événement provient d'Amazon EC2

Création d'une EventBridge règle

Vous pouvez écrire une EventBridge règle et automatiser les actions à effectuer lorsque le modèle d'événement correspond à la règle.

L'exemple suivant crée une EventBridge règle pour envoyer un e-mail, un SMS ou une notification push mobile chaque fois qu'Amazon EC2 émet un signal de recommandation de rééquilibrage. Le signal est émis en tant qu'événement de `EC2 Instance Rebalance Recommendation`, ce qui déclenche l'action définie par la règle.

Avant de créer la EventBridge règle, vous devez créer le SNS sujet Amazon pour l'e-mail, le message texte ou la notification push mobile.

Pour créer une EventBridge règle pour un événement de recommandation de rééquilibrage

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Choisissez Créer une règle.
3. Pour Define rule detail (Définir les détails de la règle), procédez comme suit :

a. Entrez un nom et éventuellement une description pour la règle.

   Une règle ne peut pas avoir le même nom qu'une autre règle de la même région et sur le même bus d'événement.

b. Pour Event bus (Bus d'événement), choisissez default (défaut). Lorsqu'un service AWS de votre compte génère un événement, il accède toujours au bus d'événement par défaut de votre compte.

c. Pour Rule type (Type de règle), choisissez Rule with an event pattern (Règle avec un modèle d'événement).

d. Choisissez Suivant.

4. Pour Build event pattern (Créer un modèle d'événement), procédez comme suit :

   a. Dans Source de l'événement, sélectionnez AWS événements ou événements EventBridge partenaires.

   b. Pour le Event pattern (Modèle d'événement), dans cet exemple, spécifiez le modèle d'événement suivant pour correspondre à l'événement `EC2 Instance Rebalance Recommendation`, puis choisissez Save (Enregistrer).

```
{
 "source": ["aws.ec2"],
 "detail-type": ["EC2 Instance Rebalance Recommendation"]
}
```

      Pour ajouter le modèle d'événement, vous pouvez soit utiliser un modèle en choisissant Formulaire de modèle d'événement, soit spécifier votre propre modèle en choisissant Modèle personnalisé (JSONéditeur), comme suit :

      i. Pour utiliser un modèle pour créer le modèle d'événement, procédez comme suit :

         A. Sélectionnez Event pattern form (Formulaire de modèle d'événement).

         B. Pour Event source (Origine de l'événement), choisissez AWS services (Services).

         C. Pour le AWS service, choisissez EC2Spot Fleet.

         D. Pour Type d'événement, choisissez EC2Instance Rebalance Recommendation.

         E. Pour personnaliser le modèle, choisissez Edit pattern (Modifier le modèle) et apportez vos modifications pour correspondre à l'exemple de modèle d'événement.

ii. (Alternative) Pour spécifier un modèle d'événement personnalisé, procédez comme suit :

A. Choisissez Motif personnalisé (JSONéditeur).

B. Dans la boîte de dialogue Event pattern (Modèle d'événement), ajoutez le modèle d'événement pour cet exemple.

c. Choisissez Next (Suivant).

5. Pour Select target(s) (Sélectionner la ou les cibles), procédez comme suit :

a. Pour Types de cibles, choisissez service AWS .

b. Pour Sélectionner une cible, choisissez le SNSsujet pour envoyer un e-mail, un SMS ou une notification push mobile lorsque l'événement se produit.

c. Pour Topic (Rubrique), sélectionnez une rubrique existante. Vous devez d'abord créer un SNS sujet Amazon à l'aide de la SNS console Amazon. Pour plus d'informations, consultez la section Utilisation d'Amazon SNS pour la messagerie application-to-person (A2P) dans le manuel du développeur Amazon Simple Notification Service.

d. (Facultatif) Sous Additional settings (Paramètres supplémentaires), vous pouvez configurer des paramètres supplémentaires. Pour plus d'informations, consultez la section Création de EventBridge règles Amazon réagissant aux événements (étape 16) dans le guide de EventBridge l'utilisateur Amazon.

e. Choisissez Suivant.

6. (Facultatif) Pour Tags (Identifications), vous pouvez également attribuer une ou plusieurs identifications à votre règle, puis choisir Next (Suivant).

7. Pour Review and create (Vérifier et créer), procédez comme suit :

a. Consultez les détails de la règle et modifiez-les si nécessaire.

b. Choisissez Créer une règle.

Pour plus d'informations, consultez les EventBridge règles Amazon et les modèles d' EventBridge événements Amazon dans le guide de EventBridge l'utilisateur Amazon

Utiliser les métadonnées d'instance

La catégorie de métadonnées d'instance `events/recommendations/rebalance` fournit l'heure approximative, enUTC, à laquelle le signal de recommandation de rééquilibrage a été émis pour une instance Spot.

Nous vous recommandons de vérifier la présence de signaux de recommandation de rééquilibrage toutes les 5 secondes afin de ne pas manquer l'occasion de donner suite à la recommandation de rééquilibrage.

Si une instance Spot reçoit une recommandation de rééquilibrage, l'heure à laquelle le signal a été émis est présente dans les métadonnées de l'instance. Vous pouvez retrouver l'heure à laquelle le signal a été émis comme suit.

cURL

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

Voici un exemple de sortie, qui indique l'heure à UTC laquelle le signal de recommandation de rééquilibrage a été émis pour l'instance Spot.

```
{"noticeTime": "2020-10-27T08:22:00Z"}
```

Si le signal n'a pas été émis pour l'instance, `events/recommendations/rebalance` s'il n'est pas présent et que vous recevez une erreur HTTP 404 lorsque vous essayez de le récupérer.

Services utilisant le signal de recommandation de rééquilibrage

Amazon EC2 Auto Scaling, EC2 Fleet et Spot Fleet utilisent le signal de recommandation de rééquilibrage pour vous permettre de maintenir facilement la disponibilité de la charge de travail en

augmentant de manière proactive votre flotte avec une nouvelle instance Spot avant qu'une instance en cours d'exécution ne reçoive l'avis d'interruption de deux minutes de l'instance Spot. Vous pouvez demander à ces services de surveiller et de répondre de manière proactive aux changements affectant la disponibilité de votre instances Spot. Pour plus d'informations, consultez les ressources suivantes :

- Utilisez le rééquilibrage de capacité pour gérer les interruptions d'Amazon EC2 Spot dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling
- Utilisez le rééquilibrage des capacités dans le EC2 parc et le parc ponctuel pour remplacer les instances ponctuelles à risquedans les rubriques EC2 Fleet et Spot Fleet de ce guide de l'utilisateur

Score de placement Spot

La fonction de score de placement des Spot peut recommander une AWS région ou une zone de disponibilité en fonction de vos besoins en matière de capacité de Spot. La capacité Spot fluctue et vous ne pouvez pas être sûr d'obtenir toujours la capacité dont vous avez besoin. Un score de placement Spot indique la probabilité qu'une demande Spot soit effectuée avec succès dans une région ou une zone de disponibilité.

> **Note**
>
> Un score de placement Spot ne fournit aucune garantie en termes de capacité disponible ou de risque d'interruption. Un score de placement Spot sert uniquement de recommandation.

Cas d'utilisation

Vous pouvez utiliser la fonction de score de placement Spot pour les éléments suivants :

- Pour relocaliser et mettre à l'échelle la capacité de calcul Spot dans une autre région, le cas échéant, en réponse à des besoins accrus en capacité ou à une diminution de la capacité disponible dans la région actuelle.
- Pour identifier la zone de disponibilité la plus optimale dans laquelle exécuter les charges de travail de zone de disponibilité unique.
- Pour simuler les besoins futurs en capacité Spot afin de pouvoir choisir une région optimale pour l'expansion de vos charges de travail basées sur Spot.

- Pour trouver une combinaison optimale de types d'instances pour répondre à vos besoins en capacité Spot.

Table des matières

Limites

- Limite de capacité cible : la limite de capacité cible de votre score de placement Spot est basée sur votre récente utilisation Spot, tout en tenant compte de la croissance potentielle de l'utilisation. Si vous n'avez pas récemment utilisé Spot, nous vous fournissons une limite par défaut faible alignée sur votre limite de demande Spot.
- Limite des configurations de demande : nous pouvons limiter le nombre de nouvelles configurations de demande sur une période de 24 heures si nous détectons des modèles non associés à l'utilisation prévue de la fonction de score de placement Spot. Si vous atteignez la limite, vous pouvez réessayer les configurations de demande que vous avez déjà utilisées, mais vous ne pouvez pas spécifier de nouvelles configurations de demande avant les prochaines 24 heures.
- Nombre minimum de types d'instances — Si vous spécifiez des types d'instances, vous devez spécifier au moins trois types d'instances différents, sinon Amazon EC2 affichera un faible score de placement Spot. De même, si vous spécifiez des attributs d'instance, ils doivent être résolus à au moins trois types d'instance différents. Les types d'instance sont considérés comme différents s'ils portent un nom différent. Par exemple, m5.8xlarge, m5a.8xlarge et m5.12xlarge sont tous considérés comme différents.

Coûts

L'utilisation de la fonction de score de placement Spot n'implique aucun coût supplémentaire.

Fonctionnement du score de placement Spot

Lorsque vous utilisez la fonctionnalité de score de placement Spot, vous spécifiez d'abord vos besoins en calcul pour vos instances Spot, puis Amazon EC2 renvoie aux 10 meilleures régions ou

les zones de disponibilité dans lesquelles votre demande Spot est susceptible de réussir. Chaque région ou zone de disponibilité est évaluée sur une échelle de 1 à 10, 10 indiquant que votre demande Spot est très susceptible de réussir, et 1 indiquant que votre demande Spot n'est pas susceptible de réussir.

Pour utiliser la fonction de score de placement Spot, procédez comme suit :

- Étape 1 : indiquer vos exigences Spot
- Étape 2 : filtrer la réponse du score de placement Spot
- Étape 3 : examiner les recommandations
- Étape 4 : utiliser les recommandations

Étape 1 : indiquer vos exigences Spot

Tout d'abord, vous spécifiez la capacité Spot cible souhaitée et vos exigences de calcul, comme suit :

1. Spécifiez la capacité Spot cible et éventuellement l'unité de capacité cible.

   Vous pouvez spécifier la capacité Spot cible souhaitée en termes de nombre d'instances ou vCPUs de quantité de mémoire en MiB. Pour spécifier la capacité cible en nombre vCPUs ou en quantité de mémoire, vous devez spécifier l'unité de capacité cible sous la forme `vcpu` ou`memory-mib`. Sinon, le nombre d'instances est défini par défaut.

   En spécifiant votre capacité cible en termes de nombre vCPUs ou de quantité de mémoire, vous pouvez utiliser ces unités pour compter la capacité totale. Par exemple, si vous souhaitez utiliser une combinaison d'instances de différentes tailles, vous pouvez spécifier la capacité cible sous la forme d'un nombre total devCPUs. La fonction de score de placement ponctuel prend ensuite en compte chaque type d'instance de la demande en fonction de son nombre devCPUs, et compte le nombre total d'instances vCPUs plutôt que le nombre total d'instances pour totaliser la capacité cible.

   Supposons, par exemple, que vous spécifiez une capacité cible totale de 30 vCPUs et que votre liste de types d'instances soit composée de c5.xlarge (4vCPUs), m5.2xlarge (8) et r5.large (2vCPUs). vCPUs Pour obtenir un total de 30vCPUs, vous pouvez obtenir un mélange de 2 c5.xlarge (2*4vCPUs), 2 m5.2xlarge (2*8) et 3 r5.large (vCPUs3*2). vCPUs
2. Spécifiez les types d'instance ou les attributs d'instance.

   Vous pouvez soit spécifier les types d'instances à utiliser, soit spécifier les attributs d'instance dont vous avez besoin pour vos besoins de calcul, puis laisser Amazon EC2 identifier les types

d'instances dotés de ces attributs. C'est ce qu'on appelle la sélection de type d'instance basée sur des attributs.

Vous ne pouvez pas spécifier à la fois les types d'instance et les attributs d'instance dans la même demande de score de placement Spot.

Si vous spécifiez des types d'instances, vous devez spécifier au moins trois types d'instances différents, sinon Amazon EC2 affichera un faible score de placement Spot. De même, si vous spécifiez des attributs d'instance, ils doivent être résolus à au moins trois types d'instance différents.

Pour obtenir des exemples de différentes manières de spécifier vos exigences Spot, consultez Exemples de configuration.

Étape 2 : filtrer la réponse du score de placement Spot

Amazon EC2 calcule le score de placement ponctuel pour chaque région ou zone de disponibilité, et renvoie soit les 10 principales régions, soit les 10 principales zones de disponibilité dans lesquelles votre demande de places est susceptible d'être acceptée. Le procédé par défaut consiste à renvoyer une liste de régions évaluées. Si vous envisagez de lancer toute votre capacité Spot dans une seule zone de disponibilité, il est utile de demander une liste de zones de disponibilité évaluées.

Vous pouvez spécifier un filtre de région pour affiner les régions qui seront renvoyées dans la réponse.

Vous pouvez combiner le filtre Région et une demande de zones de disponibilité évaluées. De cette façon, les zones de disponibilité évaluées sont limitées aux régions filtrées. Pour trouver la zone de disponibilité la mieux notée dans une région, spécifiez uniquement cette région, et la réponse renvoie une liste notée de toutes les zones de disponibilité de cette région.

Étape 3 : examiner les recommandations

Le score de placement Spot pour chaque région ou zone de disponibilité est calculé en fonction de la capacité cible, de la composition des types d'instance, des tendances historiques et actuelles de l'utilisation Spot et de l'heure de la demande. Étant donné que la capacité Spot fluctue constamment, la même demande de score de placement Spot peut générer des scores différents lorsqu'elle est calculée à des moments différents.

Les régions et les zones de disponibilité sont évaluées sur une échelle de 1 à 10. Un score de 10 indique que votre demande Spot est très susceptible, mais non garantie, d'aboutir. Un score de 1

indique que votre demande Spot a peu de chances d'aboutir. Le même score peut être renvoyé pour différentes régions ou zones de disponibilité.

Si des scores faibles sont renvoyés, vous pouvez modifier vos exigences de calcul et recalculer le score. Vous pouvez également demander des recommandations de score de placement Spot pour les mêmes exigences de calcul à différents moments de la journée.

Étape 4 : utiliser les recommandations

Un score de placement Spot n'est pertinent que si votre demande Spot a exactement la même configuration que celle du score de placement Spot (capacité cible, unité de capacité cible, types d'instance ou attributs d'instance) et est configurée pour utiliser la stratégie d'allocation `capacity-optimized`. Sinon, la probabilité d'obtenir une capacité Spot disponible ne sera pas alignée sur le score.

Bien qu'un score de placement Spot serve de directive et qu'aucun score ne garantit que votre demande Spot sera entièrement ou partiellement satisfaite, vous pouvez utiliser les informations suivantes pour obtenir les meilleurs résultats :

- Utilisez la même configuration — Le score de placement Spot n'est pertinent que si la configuration de la demande Spot (capacité cible, unité de capacité cible et types d'instances ou attributs d'instance) dans votre groupe Auto Scaling, votre EC2 flotte ou votre parc Spot est identique à celle que vous avez saisie pour obtenir le score de placement Spot.

  Si vous avez utilisé la sélection du type d'instance basée sur les attributs dans votre demande de score de placement Spot, vous pouvez utiliser la sélection du type d'instance basée sur les attributs pour configurer votre groupe, votre EC2 flotte ou votre parc d'instances Auto Scaling. Pour plus d'informations, consultez Création d'un groupe Auto Scaling avec un ensemble d'exigences relatives aux types d'instances utilisés etSpécifiez les attributs pour la sélection du type d'instance pour EC2 Fleet ou Spot Fleet.

  > **Note**
  >
  > Si vous avez spécifié votre capacité cible en termes de nombre vCPUs ou de quantité de mémoire, et que vous avez spécifié des types d'instances dans la configuration de votre score de placement Spot, notez que vous ne pouvez actuellement pas créer cette configuration dans votre groupe Auto Scaling, votre EC2 flotte ou votre flotte Spot. À la place, vous devez définir manuellement la pondération de l'instance à l'aide du paramètre `WeightedCapacity`.

- Utiliser la stratégie d'allocation **`capacity-optimized`** : tout score suppose que votre demande de flotte sera configurée pour utiliser toutes les zones de disponibilité (pour demander de la capacité dans toutes les régions) ou une seule zone de disponibilité (si vous demandez une capacité dans une zone de disponibilité) et la stratégie d'allocation Spot `capacity-optimized` pour que votre demande de capacité Spot aboutisse. Si vous utilisez d'autres stratégies d'allocation, telles que `lowest-price`, la probabilité d'obtenir une capacité Spot disponible ne sera pas alignée sur le score.
- Agir immédiatement après l'obtention du score : la recommandation de score de placement Spot reflète la capacité Spot disponible au moment de la demande, et la même configuration peut générer des scores différents lorsqu'elle est calculée à des moments différents en raison des fluctuations de capacité Spot. Bien qu'un score de 10 signifie que votre demande de capacité Spot est très susceptible, mais non garantie, d'aboutir, pour obtenir de meilleurs résultats, nous vous recommandons d'agir immédiatement après l'obtention du score. Nous vous recommandons également d'obtenir un nouveau score chaque fois que vous tentez une demande de capacité.

Autorisations requises pour le score de placement dans Spot

Par défaut, les IAM identités (utilisateurs, rôles ou groupes) ne sont pas autorisées à être utiliséesthe section called "Score de placement Spot". Pour autoriser IAM les identités à utiliser le score de placement Spot, vous devez créer une IAM politique autorisant l'utilisation de l'`ec2:GetSpotPlacementScores`EC2APIaction. Vous associez ensuite la politique aux IAM identités qui nécessitent cette autorisation.

Voici un exemple de IAM politique qui autorise l'utilisation de l'`ec2:GetSpotPlacementScores`EC2APIaction.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:GetSpotPlacementScores",
            "Resource": "*"
        }
    ]
}
```

Pour plus d'informations sur la modification d'une IAM politique, consultez la section Modification IAM des politiques dans le Guide de IAM l'utilisateur.

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .
- Utilisateurs gérés IAM par le biais d'un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Suivez les instructions de la section Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le guide de IAM l'utilisateur.
- IAMutilisateurs :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la section Création d'un rôle pour un IAM utilisateur dans le Guide de IAM l'utilisateur.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la section Ajouter des autorisations à un utilisateur (console) dans le guide de IAM l'utilisateur.

Calculez le score de placement Spot

Vous pouvez calculer un score de placement ponctuel en fonction de la capacité cible et des exigences de calcul. Pour de plus amples informations, veuillez consulter the section called "Fonctionnement du score de placement Spot".

Autorisations nécessaires

Vérifiez que vous disposez des autorisations requises. Pour de plus amples informations, veuillez consulter the section called "Autorisations nécessaires".

Options

- Calculer à l'aide des attributs d'instance
- Calculer à l'aide des types d'instances
- Calculez à l'aide du AWS CLI

Calculer à l'aide des attributs d'instance

Pour calculer un score de placement Spot en spécifiant des attributs d'instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Choisissez Spot placement score (Score de placement Spot).
4. Choisissez Enter requirements (Saisir les exigences).
5. Pour Capacité cible, entrez la capacité souhaitée en termes de nombre d'instances ou vCPUsde quantité de mémoire (MiB).
6. Pour les exigences relatives aux types d'instance, pour définir vos exigences en matière de calcul et laisser Amazon EC2 identifier les types d'instance optimaux en fonction de ces exigences, choisissez Spécifier les attributs d'instance correspondant à vos exigences de calcul.
7. Pour vCPUs, entrez le nombre minimum et maximum souhaités devCPUs. Pour ne spécifier aucune limite, sélectionnez No minimum (Pas de minimum), No maximum (Pas de maximum), ou les deux.
8. Pour Memory (GiB) (Mémoire (Gio)), saisissez la quantité minimale et maximale de mémoire souhaitée. Pour ne spécifier aucune limite, sélectionnez No minimum (Pas de minimum), No maximum (Pas de maximum), ou les deux.
9. Pour CPUl'architecture, sélectionnez l'architecture d'instance requise.
10. (Facultatif) Pour Additional instance attributes (Attributs d'instance supplémentaires), vous pouvez éventuellement spécifier un ou plusieurs attributs pour exprimer vos exigences de calcul plus en détail. Chaque attribut supplémentaire ajoute une contrainte supplémentaire à votre demande. Vous pouvez omettre les attributs supplémentaires. Lorsque ces attributs sont omis, les valeurs par défaut sont utilisées. Pour une description de chaque attribut et de leurs valeurs par défaut, consultez le get-spot-placement-scoresmanuel Amazon EC2 Command Line Reference.
11. (Facultatif) Pour afficher les types d'instance avec vos attributs spécifiés, développez Preview matching instance types (Aperçu des types d'instance correspondants). Pour empêcher des types d'instances d'être utilisés dans l'évaluation du placement, sélectionnez les instances, puis choisissez Eclude selected instance types (Exclure les types d'instances sélectionnés).
12. Choisissez Load placement scores (Charger les scores de placement) et vérifiez les résultats.
13. (Facultatif) Pour afficher le score de placement Spot pour des régions spécifiques, pour Regions to evaluate (Régions à évaluer), sélectionnez les régions à évaluer, puis choisissez Calculate placement scores (Calculer les scores de placement).
14. (Facultatif) Pour afficher le score de placement Spot pour les zones de disponibilité dans les régions affichées, cochez la case Provide placement scores per Availability Zone (Fournir des scores de placement par zone de disponibilité). Une liste de zones de disponibilité évaluées est utile si vous souhaitez lancer toute votre capacité Spot dans une seule zone de disponibilité.

15. (Facultatif) Pour modifier vos exigences de calcul et obtenir un nouveau score de placement, choisissez Edit (Modifier), effectuez les ajustements nécessaires, puis choisissez Calculate placement scores (Calculer les scores de placement).

Calculer à l'aide des types d'instances

Pour calculer un score de placement Spot en spécifiant des types d'instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Choisissez Spot placement score (Score de placement Spot).
4. Choisissez Enter requirements (Saisir les exigences).
5. Pour Capacité cible, entrez la capacité souhaitée en termes de nombre d'instances ou vCPUsde quantité de mémoire (MiB).
6. Pour Instance type requirements (Exigences de type d'instance), afin de spécifier les types d'instance à utiliser, choisissez Manually select instance types (Sélection manuelle des types d'instance).
7. Choisissez Select instance types (Sélectionner les types d'instance), sélectionnez les types d'instance à utiliser, puis choisissez Select (Sélectionner). Pour trouver rapidement des types d'instance, vous pouvez utiliser la barre de filtre afin de filtrer les types d'instance selon différentes propriétés.
8. Choisissez Load placement scores (Charger les scores de placement) et vérifiez les résultats.
9. (Facultatif) Pour afficher le score de placement Spot pour des régions spécifiques, pour Regions to evaluate (Régions à évaluer), sélectionnez les régions à évaluer, puis choisissez Calculate placement scores (Calculer les scores de placement).
10. (Facultatif) Pour afficher le score de placement Spot pour les zones de disponibilité dans les régions affichées, cochez la case Provide placement scores per Availability Zone (Fournir des scores de placement par zone de disponibilité). Une liste de zones de disponibilité évaluées est utile si vous souhaitez lancer toute votre capacité Spot dans une seule zone de disponibilité.
11. (Facultatif) Pour modifier la liste des types d'instance et obtenir un nouveau score de placement, choisissez Edit (Modifier), effectuez les ajustements nécessaires, puis choisissez Calculate placement scores (Calculer les scores de placement).

Calculez à l'aide du AWS CLI

Pour calculer le score de placement Spot

1. (Facultatif) Pour générer tous les paramètres possibles pouvant être spécifiés pour la configuration du score de placement Spot, utilisez la get-spot-placement-scorescommande et le `--generate-cli-skeleton` paramètre.

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
    --generate-cli-skeleton
```

Voici un exemple de sortie.

```
{
    "InstanceTypes": [
        ""
    ],
    "TargetCapacity": 0,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "RegionNames": [
        ""
    ],
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": [
            "x86_64_mac"
        ],
        "VirtualizationTypes": [
            "hvm"
        ],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 0,
                "Max": 0
            },
            "MemoryMiB": {
                "Min": 0,
                "Max": 0
            },
            "CpuManufacturers": [
                "amd"
```

```
            ],
            "MemoryGiBPerVCpu": {
                "Min": 0.0,
                "Max": 0.0
            },
            "ExcludedInstanceTypes": [
                ""
            ],
            "InstanceGenerations": [
                "previous"
            ],
            "SpotMaxPricePercentageOverLowestPrice": 0,
            "OnDemandMaxPricePercentageOverLowestPrice": 0,
            "BareMetal": "excluded",
            "BurstablePerformance": "excluded",
            "RequireHibernateSupport": true,
            "NetworkInterfaceCount": {
                "Min": 0,
                "Max": 0
            },
            "LocalStorage": "included",
            "LocalStorageTypes": [
                "hdd"
            ],
            "TotalLocalStorageGB": {
                "Min": 0.0,
                "Max": 0.0
            },
            "BaselineEbsBandwidthMbps": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorTypes": [
                "fpga"
            ],
            "AcceleratorCount": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorManufacturers": [
                "amd"
            ],
            "AcceleratorNames": [
                "vu9p"
```

```
            ],
            "AcceleratorTotalMemoryMiB": {
                "Min": 0,
                "Max": 0
            }
        }
    },
    "DryRun": true,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Créez un fichier JSON de configuration à l'aide du résultat de l'étape précédente et configurez-le comme suit :

   a. Pour`TargetCapacity`, entrez la capacité Spot souhaitée en termes de nombre d'instances ou vCPUs de quantité de mémoire (MiB).

   b. Pour `TargetCapacityUnitType`, saisissez l'unité correspondant à la capacité cible. Si vous omettez ce paramètre, `units` est utilisé par défaut.

      Valeurs valides : `units` (qui se traduit par le nombre d'instances) | `vcpu` | `memory-mib`

   c. Pour `SingleAvailabilityZone`, spécifiez `true` pour une réponse qui renvoie une liste de zones de disponibilité évaluées. Une liste de zones de disponibilité évaluées est utile si vous souhaitez lancer toute votre capacité Spot dans une seule zone de disponibilité. Si vous omettez ce paramètre, `false` est utilisé par défaut et la réponse renvoie une liste des régions notées.

   d. (Facultatif) Pour `RegionNames`, spécifiez les régions à utiliser comme filtre. Vous devez spécifier le code de région, par exemple, `us-east-1`.

      Avec un filtre de région, la réponse renvoie uniquement les régions que vous spécifiez. Si vous avez spécifié `true` pour `SingleAvailabilityZone`, la réponse renvoie uniquement les zones de disponibilité dans les régions spécifiées.

   e. Vous pouvez inclure `InstanceTypes` ou `InstanceRequirements`, mais pas les deux dans la même configuration.

      Spécifiez l'une des options suivantes dans votre JSON configuration :

      - Pour spécifier une liste de types d'instances, spécifiez les types d'instances dans le paramètre `InstanceTypes`. Spécifiez au moins trois types d'instance différents. Si vous

ne spécifiez qu'un ou deux types d'instance, le score de placement Spot renvoie un score faible. Pour la liste des types d'instances, consultez Amazon EC2 Instance Types.

- Pour spécifier les attributs de l'instance afin EC2 qu'Amazon identifie les types d'instances correspondant à ces attributs, spécifiez les attributs situés dans la `InstanceRequirements` structure.

  Vous devez fournir des valeurs pour `VCpuCount`, `MemoryMiB` et `CpuManufacturers`. Vous pouvez omettre les autres attributs. Lorsqu'ils sont omis, les valeurs par défaut sont utilisées. Pour une description de chaque attribut et de leurs valeurs par défaut, consultez le get-spot-placement-scoresmanuel Amazon EC2 Command Line Reference.

Pour obtenir des exemples de configuration, consultez Exemples de configuration.

3. Pour obtenir le score de placement Spot correspondant aux exigences que vous avez spécifiées dans le JSON fichier, utilisez la get-spot-placement-scorescommande et spécifiez le nom et le chemin d'accès à votre JSON fichier à l'aide du `--cli-input-json` paramètre.

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
    --cli-input-json file://file_name.json
```

Exemple de sortie si la valeur `SingleAvailabilityZone` est définie `false` ou omise (si cette valeur est omise, la valeur par défaut est définie sur`false`) : une liste de régions pour lesquelles est renvoyée.

```
"SpotPlacementScores": [
    {
        "Region": "us-east-1",
        "Score": 7
    },
    {
        "Region": "us-west-1",
        "Score": 5
    },
   ...
```

Exemple de sortie si le paramètre `SingleAvailabilityZone` est défini sur `true` : une liste notée de zones de disponibilité est renvoyée.

```
"SpotPlacementScores": [
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "use1-az1",
        "Score": 8
    },
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "usw2-az3",
        "Score": 6
    },
   ...
```

Exemples de configuration

Lorsque vous utilisez le AWS CLI, vous pouvez utiliser les exemples de configuration suivants.

Exemples de configuration

- Exemple : spécifier les types d'instance et la capacité cible
- Exemple : spécifier les types d'instance et la capacité cible en termes de mémoire
- Exemple : spécifier des attributs pour la sélection du type d'instance basée sur des attributs
- Exemple : spécifier des attributs pour la sélection du type d'instance basée sur des attributs et renvoyer une liste de zones de disponibilité évaluées

Exemple : spécifier les types d'instance et la capacité cible

L'exemple de configuration suivant spécifie trois types d'instance différents et une capacité Spot cible de 500 instances Spot.

```
{
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
    ],
    "TargetCapacity": 500
}
```

Exemple : spécifier les types d'instance et la capacité cible en termes de mémoire

L'exemple de configuration suivant spécifie trois types d'instance différents et une capacité Spot cible de 500 000 Mio de mémoire, où le nombre d'instances Spot à lancer doit fournir un total de 500 000 Mio de mémoire.

```
{
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
    ],
    "TargetCapacity": 500000,
    "TargetCapacityUnitType": "memory-mib"
}
```

Exemple : spécifier des attributs pour la sélection du type d'instance basée sur des attributs

L'exemple de configuration suivant est configuré pour la sélection du type d'instance basé sur des attributs et est suivi d'une explication textuelle.

```
{
    "TargetCapacity": 5000,
    "TargetCapacityUnitType": "vcpu",
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

`InstanceRequirementsWithMetadata`

Pour utiliser la sélection du type d'instance basée sur les attributs, vous devez inclure la structure `InstanceRequirementsWithMetadata` dans votre configuration et spécifier les attributs souhaités pour les instances Spot.

Dans l'exemple précédent, les attributs d'instance obligatoires suivants sont spécifiés :

- `ArchitectureTypes` – le type d'architecture des types d'instance doit être `arm64`.
- `VirtualizationTypes` – le type de virtualisation des types d'instance doit être `hvm`.
- `VCpuCount`— Les types d'instance doivent avoir un minimum de 1 et un maximum de 12vCPUs.
- `MemoryMiB` : les types d'instance doivent avoir un minimum de 512 Mio de mémoire. En omettant le paramètre `Max`, vous indiquez qu'il n'y a pas de limite maximale.

Notez qu'il existe plusieurs autres attributs facultatifs que vous pouvez spécifier. Pour la liste des attributs, reportez-vous get-spot-placement-scoresà la référence des AWS CLI commandes.

`TargetCapacityUnitType`

Le paramètre `TargetCapacityUnitType` spécifie l'unité de la capacité cible. Dans l'exemple, la capacité cible est `5000` et le type d'unité de capacité cible est`vcpu`, ce qui indique ensemble une capacité cible souhaitée de 5 000vCPUs, le nombre d'instances ponctuelles à lancer devant fournir un total de 5 000vCPUs.

Exemple : spécifier des attributs pour la sélection du type d'instance basée sur des attributs et renvoyer une liste de zones de disponibilité évaluées

L'exemple de configuration suivant est configuré pour la sélection du type d'instance basée sur des attributs. En spécifiant `"SingleAvailabilityZone": true`, la réponse renverra une liste des zones de disponibilité évaluées.

```
{
    "TargetCapacity": 1000,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 1,
                "Max": 12
```

```
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

Suivez les coûts de votre instance Spot à l'aide du flux de données de l'instance Spot

Pour vous aider à comprendre les frais liés à vos instances Spot, Amazon EC2 fournit un flux de données qui décrit l'utilisation et les prix de vos instances Spot. Ce flux de données est envoyé vers un compartiment Amazon S3 que vous spécifiez lorsque vous vous abonnez au flux de données.

Les fichiers de flux de données arrivent généralement dans votre compartiment une fois par heure. Si vous n'avez aucune instance Spot en cours d'exécution à une certaine heure, vous ne recevez pas de fichier de flux de données pour cette heure.

Chaque heure d'utilisation d'une instance Spot est généralement couverte dans un seul fichier de données. Ces fichiers sont compressés (gzip) avant qu'ils ne soient livrés à votre compartiment. Amazon EC2 peut écrire plusieurs fichiers pour une heure d'utilisation donnée lorsque les fichiers sont volumineux (par exemple, lorsque le contenu du fichier pour l'heure dépasse 50 Mo avant compression).

> **Note**
>
> Vous ne pouvez créer qu'un seul flux de données d'instance Spot par Compte AWS.

Le flux de données des instances Spot est pris en charge dans toutes les AWS régions à l'exception de la Chine (Pékin), de la Chine AWS GovCloud (Ningxia), (États-Unis) et des régions qui sont désactivées par défaut.

Table des matières

Nom et format du fichier de flux de données

Le nom du fichier de flux de données de l'instance Spot utilise le format suivant (date et heure indiquéesUTC) :

```
bucket-name.s3.amazonaws.com/optional-prefix/aws-account-id.YYYY-MM-DD-HH.n.unique-id.gz
```

Par exemple, si le nom de votre compartiment est **amzn-s3-demo-bucket** et que votre préfixe est **my-prefix**, vos noms de fichier ont le format suivant :

```
amzn-s3-demo-bucket.s3.amazonaws.com/my-prefix/111122223333.2023-12-09-07.001.b959dbc6.gz
```

Pour plus d'informations sur les noms de compartiment, veuillez consulter la rubrique Règles de dénomination de compartiment dans le Guide de l'utilisateur Amazon S3.

Les fichiers de flux de données d'instance Spot sont délimités par des tabulations. Chaque ligne du fichier de données correspond à une heure d'instance et contient les champs répertoriés dans le tableau suivant.

Champ	Description
`Timestamp`	Horodatage utilisé pour déterminer le prix facturé pour cette utilisation d'instance.
`UsageType`	Type d'utilisation et type d'instance associés à la facturation. Pour `m1.small` Instances Spot, ce champ est défini sur `SpotUsage` . Pour tous les autres types d'instance, ce champ est défini sur `SpotUsage:` {instance-type}. Par exemple, `SpotUsage:c1.medium` .
`Operation`	Le produit faisant l'objet d'une facturation. Pour les Instances Spot Linux, ce champ est défini sur `RunInstances` . Pour les Instances Spot Windows, ce champ est défini sur `RunInstances:0002` . L'utilisation des instances Spot est regroupée par zone de disponibilité.

Champ	Description
`InstanceID`	L'ID de l'instance Spot qui a généré cette utilisation d'instance.
`MyBidID`	L'ID de la demande d'instance Spot qui a généré cette utilisation d'instance.
`MyMaxPrice`	Prix maximum spécifié pour cette demande Spot.
`MarketPrice`	Prix Spot au moment spécifié dans le champ `Timestamp` .
`Charge`	Prix facturé pour cette utilisation d'instance.
`Version`	Version du flux de données. La version disponible est la version 1.0.

Conditions requises pour le compartiment Amazon S3

Lorsque vous vous abonnez au flux de données, vous devez spécifier un compartiment Amazon S3 afin de stocker les fichiers de flux de données.

Avant de choisir un compartiment Amazon S3 pour le flux de données, tenez compte des points suivants :

- Vous devez bénéficier d'une autorisation `FULL_CONTROL` sur le compartiment. Si vous êtes le propriétaire du compartiment, vous disposez de cette autorisation par défaut. Dans le cas contraire, le propriétaire du bucket doit vous accorder Compte AWS cette autorisation.
- Lorsque vous vous abonnez à un flux de données, ces autorisations sont utilisées pour mettre à jour le compartiment ACL afin d'`FULL_CONTROL`autoriser le compte du flux de AWS données. Le compte AWS de flux de données écrit des fichiers de flux de données dans le compartiment. Si votre compte ne dispose pas des autorisations nécessaires, les fichiers de flux de données ne peuvent pas être écrits dans le compartiment. Pour plus d'informations, consultez la section Logs envoyés à Amazon S3 dans le guide de l'utilisateur Amazon CloudWatch Logs.

  Si vous mettez à jour le compte de flux de AWS données ACL et que vous en supprimez les autorisations, les fichiers du flux de données ne peuvent pas être écrits dans le bucket. Vous devez vous réabonner au flux de données pour recevoir les fichiers de flux de données.

- Chaque fichier de flux de données possède son propre fichier ACL (distinct ACL de celui du bucket). Le propriétaire du compartiment bénéficie de l'autorisation `FULL_CONTROL` pour les fichiers de données. Le compte du flux de AWS données dispose d'autorisations de lecture et d'écriture.
- Si vous supprimez votre abonnement au flux de données, Amazon EC2 ne supprime pas les autorisations de lecture et d'écriture du compte du flux de AWS données, que ce soit sur le bucket ou sur les fichiers de données. Vous devez supprimer ces autorisations vous-même.
- Si vous chiffrez votre compartiment Amazon S3 à l'aide du chiffrement côté serveur avec une AWS KMS clé stockée dans AWS Key Management Service (SSE-KMS), vous devez utiliser une clé gérée par le client. Pour plus d'informations, consultez la section Chiffrement du compartiment Amazon S3 côté serveur dans le guide de l'utilisateur Amazon CloudWatch Logs.

S'abonner à votre flux de données d'instance Spot

Pour vous abonner à votre flux de données, utilisez la create-spot-datafeed-subscription AWS CLI commande.

```
aws ec2 create-spot-datafeed-subscription \
    --bucket amzn-s3-demo-bucket \
    [--prefix my-prefix]
```

Ce qui suit est un exemple de sortie.

```
{
    "SpotDatafeedSubscription": {
        "OwnerId": "111122223333",
        "Bucket": "amzn-s3-demo-bucket",
        "Prefix": "my-prefix",
        "State": "Active"
    }
}
```

Si vous recevez un message d'erreur indiquant que le bucket ne dispose pas d'autorisations suffisantes, consultez l'article suivant pour obtenir des informations de dépannage : Résoudre les problèmes liés au flux de données pour les instances Spot.

Afficher les données dans votre flux de données

Dans le AWS Management Console, ouvrez AWS CloudShell. Utilisez la commande de synchronisation s3 suivante pour obtenir les fichiers .gz du compartiment S3 pour votre flux de données et les stocker dans le dossier que vous spécifiez.

```
aws s3 sync s3://amzn-s3-demo-bucket ./data-feed
```

Pour afficher le contenu d'un fichier .gz, accédez au dossier dans lequel vous avez stocké le contenu du compartiment S3.

```
cd data-feed
```

Utilisez la commande ls pour afficher les noms des fichiers. Utilisez la commande zcat avec le nom du fichier pour afficher le contenu du fichier compressé. Voici un exemple de commande.

```
zcat  111122223333.2023-12-09-07.001.b959dbc6.gz
```

Voici un exemple de sortie.

```
#Version: 1.0
#Fields: Timestamp UsageType Operation InstanceID MyBidID MyMaxPrice MarketPrice Charge
 Version
2023-12-09 07:13:47 UTC USE2-SpotUsage:c7a.medium       RunInstances:SV050
 i-0c3e0c0b046e050df     sir-pwq6nmfp    0.0510000000 USD        0.0142000000 USD
  0.0142000000 USD        1
```

Supprimer votre flux de données d'instance Spot

Pour supprimer votre flux de données, utilisez la delete-spot-datafeed-subscription AWS CLI commande.

```
aws ec2 delete-spot-datafeed-subscription
```

Rôle lié à un service pour les demandes d'instance Spot

Amazon EC2 utilise des rôles liés à un service pour obtenir les autorisations dont il a besoin pour appeler d'autres AWS services en votre nom. Un rôle lié à un service est un type unique de IAM

rôle directement lié à un. service AWS Les rôles liés à un service constituent un moyen sécurisé de déléguer des autorisations, services AWS car seul le service lié peut assumer un rôle lié au service. Pour plus d'informations, consultez la section Rôles liés aux services dans le Guide de l'IAMutilisateur.

Amazon EC2 utilise le rôle lié au service nommé AWSServiceRoleForEC2Spotpour lancer et gérer les instances Spot en votre nom.

Autorisations octroyées par AWSServiceRoleForEC2Spot

Amazon EC2 utilise AWSServiceRoleForEC2Spotpour effectuer les actions suivantes :

- `ec2:DescribeInstances` – Décrire les instances Spot
- `ec2:StopInstances` – Arrêter les instances Spot
- `ec2:StartInstances` – Démarrer les instances Spot

Création du rôle lié à un service

Dans la plupart des cas, vous n'avez pas besoin de créer manuellement un rôle lié à un service. Amazon EC2 crée le rôle AWSServiceRoleForEC2Spotlié au service la première fois que vous demandez une instance Spot à l'aide de la console.

Si vous avez reçu une demande d'instance Spot active avant octobre 2017, date à laquelle Amazon EC2 a commencé à prendre en charge ce rôle lié à un service, Amazon EC2 a créé le AWSServiceRoleForEC2Spotrôle dans votre AWS compte. Pour plus d'informations, voir Un nouveau rôle est apparu dans Mon compte dans le guide de IAM l'utilisateur.

Si vous utilisez le AWS CLI ou API pour demander une instance Spot, vous devez d'abord vous assurer que ce rôle existe.

Pour créer AWSServiceRoleForEC2Spot à l'aide de la console

1. Ouvrez la IAM console à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Roles (Rôles).
3. Sélectionnez Create role (Créer un rôle).
4. Sur la page Sélectionner le type d'entité de confiance EC2, choisissez EC2- Spot Instances, Next : Permissions.
5. Sur la page suivante, choisissez Suivant : Vérification.

6. Sur la page Vérification, choisissez Create Role (Créer un rôle).

Pour créer à AWSServiceRoleForEC2Spotl'aide du AWS CLI

Utilisez la commande create-service-linked-role comme suit.

```
aws iam create-service-linked-role --aws-service-name spot.amazonaws.com
```

Si vous n'avez plus besoin d'utiliser des instances Spot, nous vous recommandons de supprimer le AWSServiceRoleForEC2Spotrôle. Une fois ce rôle supprimé de votre compte, Amazon le EC2 créera à nouveau si vous demandez des instances Spot.

Accordez l'accès aux clés gérées par le client pour les utiliser avec le chiffrement AMIs et les EBS instantanés

Si vous spécifiez un EBS instantané Amazon chiffré AMI ou chiffré pour vos instances Spot et que vous utilisez une clé gérée par le client pour le chiffrement, vous devez accorder au AWSServiceRoleForEC2Spotrôle l'autorisation d'utiliser la clé gérée par le client afin qu'Amazon EC2 puisse lancer des instances Spot en votre nom. Pour cela, vous devez ajouter une autorisation à la clé gérée par le client, comme indiqué dans la procédure suivante.

Lorsque vous définissez les autorisations, les octrois constituent une alternative aux politiques de clé. Pour de plus amples informations, veuillez consulter Utilisation des octrois et Utilisation des stratégies de clé dans AWS KMS dans le Guide du développeur AWS Key Management Service .

Pour autoriser le rôle AWSServiceRoleForEC2Spot à utiliser la clé gérée par le client

- Utilisez la commande create-grant pour ajouter une autorisation à la clé gérée par le client et pour spécifier le principal (le rôle AWSServiceRoleForEC2Spotlié au service) autorisé à effectuer les opérations autorisées par l'autorisation. La clé gérée par le client est spécifiée par le `key-id` paramètre et le ARN de la clé gérée par le client. Le principal est spécifié par le `grantee-principal` paramètre et le ARN rôle AWSServiceRoleForEC2Spotlié au service.

  ```
  aws kms create-grant \
      --region us-east-1 \
      --key-id arn:aws:kms:us-
  east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
      --grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
  spot.amazonaws.com/AWSServiceRoleForEC2Spot \
  ```

```
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
"GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
"ReEncryptTo"
```

Quotas d'instances Spot

Il existe des quotas pour le nombre d'instances Spot en cours d'exécution et les demandes d'instances Spot en attente par Compte AWS et par région. Une fois qu'une demande d'instance Spot en attente est traitée, elle n'est plus prise en compte dans le quota car l'instance en cours d'exécution est prise en compte dans le quota.

Les quotas d'instances Spot sont gérés en fonction du nombre d'unités centrales virtuelles (vCPUs) que vos instances Spot en cours d'exécution utilisent ou utiliseront en attendant le traitement des demandes d'instances Spot ouvertes. Si vous résiliez vos instances Spot mais que vous n'annulez pas les demandes d'instances Spot, les demandes sont prises en compte dans votre CPU quota d'instances Spot v jusqu'à ce qu'Amazon EC2 détecte les résiliations d'instances Spot et ferme les demandes.

Nous proposons les types de quotas suivants pour les instances Spot.

Nom	Par défaut	Ajustable
Toutes les demandes d'instance Spot DL	0	Oui
Toutes les demandes d'instance Spot F	0	Oui
Toutes les demandes d'instance Spot G et VT	0	Oui
Toutes les demandes d'instance Spot Inf	0	Oui
Toutes les demandes d'instances ponctuelles P4, P3 et P2	0	Oui
Toutes les demandes d'instance P5 Spot	0	Oui
Toutes les demandes d'instance Spot standard (A, C, D, H, I, M, R, T, Z)	5	Oui
Toutes les demandes d'instance Spot Trn	0	Oui

Nom	Par défaut	Ajustable
Toutes les demandes d'instance Spot X	0	Oui

Même si Amazon augmente EC2 automatiquement les quotas de vos instances Spot en fonction de votre utilisation, vous pouvez demander une augmentation de quota si nécessaire. Par exemple, si vous avez l'intention de lancer plus d'instances Spot que celles autorisées par votre quota actuel, vous pouvez demander une augmentation de quota. Vous pouvez aussi demander une augmentation de quota si vous soumettez une demande d'instance Spot et que vous recevez l'erreur `Max spot instance count exceeded`. Pour demander une augmentation de quota, utilisez la console Service Quotas, comme décrit dans Quotas EC2 de service Amazon.

Vous pouvez lancer toute combinaison de types d'instance qui répond à l'évolution de vos besoins en termes d'applications. Par exemple, avec un quota de 256 demandes d'instances ponctuelles standardvCPUs, vous pouvez demander 32 instances `m5.2xlarge` ponctuelles (32 x 8vCPUs) ou 16 instances `c5.4xlarge` ponctuelles (16 x 16vCPUs).

Grâce à l'intégration CloudWatch des métriques Amazon, vous pouvez surveiller EC2 l'utilisation par rapport à vos quotas. Vous pouvez également configurer des alarmes pour vous avertir lorsque vous approchez des quotas. Pour plus d'informations, consultez la section Quotas de service et CloudWatch alarmes Amazon dans le guide de l'utilisateur des quotas de service. .

Hôtes EC2 dédiés Amazon

Un hôte EC2 dédié Amazon est un serveur physique entièrement dédié à votre usage. Vous pouvez éventuellement choisir de partager la capacité de l'instance avec d'autres AWS comptes. Pour de plus amples informations, veuillez consulter Partage d'hôtes Amazon EC2 Dedicated Host entre comptes.

Les hôtes dédiés offrent une visibilité et un contrôle sur le placement des instances et favorisent l'affinité entre les hôtes. Cela signifie que vous pouvez lancer et exécuter des instances sur des hôtes spécifiques, et vous pouvez vous assurer que les instances ne s'exécutent que sur des hôtes spécifiques. Pour de plus amples informations, veuillez consulter Placement automatique et affinité d'hôte Amazon EC2 Dedicated Host.

Les hébergeurs dédiés fournissent un support complet avec la licence Bring Your Own License (BYOL). Ils vous permettent d'utiliser vos licences logicielles existantes par socket, par cœur ou par machine virtuelle, y compris Windows Server, SQL Server, SUSE Linux Enterprise Server, Red Hat

Enterprise Linux, ou d'autres licences logicielles liées à des sockets ou à VMs des cœurs physiques, sous réserve de vos conditions de licence.

Si vous souhaitez que vos instances s'exécutent sur du matériel dédié, mais que vous n'avez pas besoin de visibilité ou de contrôle sur le placement des instances, et que vous n'avez pas besoin d'utiliser des licences logicielles par socket ou par cœur, vous pouvez envisager d'utiliser des instances dédiées à la place. Les instances dédiées et les hôtes dédiés peuvent tous deux être utilisés pour lancer EC2 des instances Amazon sur des serveurs physiques dédiés. Il n'existe pas de différence physique, de sécurité ou de performance entre les instances dédiées et les instances des Hôtes dédiés. Cependant, il existe des différences majeures entre eux. Le tableau suivant met en valeur quelques-unes des principales différences entre les Hôtes dédiés et les instances dédiées :

	Dedicated Host	Dedicated Instance
Serveur physique dédié	Serveur physique avec une capacité d'instance entièrement dédiée à votre utilisation.	Serveur physique dédié à un seul compte client.
Partage de capacité d'instance	Peut partager la capacité de l'instance avec d'autres comptes.	Non pris en charge
Facturation	Facturation par hôte	Facturation par instance
Visibilité des sockets, cœurs et ID d'hôte	Offre une visibilité sur le nombre de sockets et de cœurs physiques	Aucune visibilité
Affinité de l'hôte et de l'instance	Permet de déployer vos instances de façon cohérente sur le même serveur physique au fil du temps	Non pris en charge
Placement ciblé d'instances	Offre une visibilité supplémentaire et un contrôle sur la façon dont les instances sont placées sur un serveur physique	Non pris en charge

	Dedicated Host	Dedicated Instance
Récupération automatique des instances	Pris en charge. Pour plus d'informations, consultez Restauration d'EC2un hôte dédié Amazon.	Pris en charge
Apportez votre propre licence (BYOL)	Pris en charge	Support partiel*
Réserve de capacité	Non pris en charge	Pris en charge

* Les licences Microsoft SQL Server with License Mobility through Software Assurance et Windows Virtual Desktop Access (VDA) peuvent être utilisées avec une instance dédiée.

Pour plus d'informations sur les instances dédiées, veuillez consulter la rubrique Instances EC2 dédiées Amazon.

Restrictions Hôtes dédiés

Avant d'allouer des Hôtes dédiés, prenez note des restrictions suivantes :

- Pour exécuter RHEL SUSE Linux et SQL Server sur des hôtes dédiés, vous devez apporter le vôtreAMIs. RHEL, SUSE Linux et AMIs les SQL serveurs proposés par AWS ou sur lesquels ils sont disponibles ne AWS Marketplace peuvent pas être utilisés avec des hôtes dédiés. Pour plus d'informations sur la façon de créer le vôtreAMI, consultezApportez vos propres licences logicielles à Amazon EC2 Dedicated Hosts.

  Cette restriction ne s'applique pas aux hôtes alloués aux instances de mémoire élevée (`u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` et `u-24tb1.metal`). RHELet AMIs les SUSE systèmes Linux proposés par AWS ou disponibles sur ces hôtes AWS Marketplace peuvent être utilisés avec ces hôtes.
- Le nombre d'hôtes dédiés exécutés par famille d'instances, par compte AWS et par région est limité. Les quotas s'appliquent uniquement aux instances en cours d'exécution. Si votre instance est en attente, en cours d'arrêt ou arrêtée, elle n'est pas prise en compte dans votre quota. Pour

consulter les quotas s'appliquant à votre compte, ou pour demander une augmentation de quota, utilisez la console Service Quotas.

- Les instances qui s'exécutent sur un hôte dédié ne peuvent être lancées que dans unVPC.
- Les groupes Auto Scaling sont pris en charge lors de l'utilisation d'un modèle de lancement qui spécifie un groupe de ressources hôte. Pour plus d'informations, consultez la section Créer un modèle de lancement à l'aide des paramètres avancés dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.
- Les RDS instances Amazon ne sont pas prises en charge.
- Le niveau d'utilisation AWS gratuite n'est pas disponible pour les hôtes dédiés.
- Le contrôle de placement d'instance fait référence à la gestion du lancement d'instances sur les Hôtes dédiés. Vous ne pouvez pas lancer Hôtes dédiés dans des groupes de placement.
- Si vous allouez un hôte pour un type d'instance virtualisée, vous ne pouvez pas modifier le type d'instance en un type d'instance `.metal` après l'allocation de l'hôte. Par exemple, si vous allouez un hôte pour le type d'instance `m5.large`, vous ne pouvez pas modifier le type d'instance en `m5.metal`.

  De même, si vous allouez un hôte pour un type d'instance `.metal`, vous ne pouvez pas modifier le type d'instance en un type d'instance virtualisée après l'allocation de l'hôte. Par exemple, si vous allouez un hôte pour le type d'instance `m5.metal`, vous ne pouvez pas modifier le type d'instance en `m5.large`.

Table des matières

- Modifier la location et l'affinité d'un hôte EC2 dédié Amazon pour une instance Amazon EC2
- Libérez un hôte EC2 dédié Amazon
- Achetez des réservations d'hôtes dédiés pour bénéficier de remises sur la facturation des hôtes dédiés
- Partage d'hôtes Amazon EC2 Dedicated Host entre comptes
- Amazon EC2 Dedicated Hosts sur AWS Outposts
- Restauration d'EC2un hôte dédié Amazon
- Maintenance de l'hôte pour Amazon EC2 Dedicated Host
- Surveillez l'état de vos hôtes Amazon EC2 Dedicated
- Suivez les modifications de configuration d'Amazon EC2 Dedicated Host à l'aide de AWS Config

Tarification et facturation d'Amazon EC2 Dedicated Host

Le prix d'un Hôte dédié varie selon l'option de paiement.

Options de paiement

- Hôtes dédiés à la demande
- Dedicated Host Reservations
- Savings Plans
- Tarification pour Windows Server sur les Hôtes dédiés

Hôtes dédiés à la demande

La facturation à la demande est automatiquement activée lorsque vous allouez un Hôte dédié à votre compte.

Le prix à la demande pour un Hôte dédié varie par famille de·l'instance et par région. Vous payez par seconde (avec un minimum de 60 secondes) pour l'Hôte dédié actif, quelle que soit la quantité ou la taille des instances que vous choisissez de lancer dessus. Pour plus d'informations sur la tarification à la demande, consultez la section Tarification à la demande d'Amazon EC2 Dedicated Hosts.

Vous pouvez libérer un Hôte dédié à la demande à tout moment pour arrêter d'accumuler des frais dessus. Pour plus d'informations sur la libération d'un Hôte dédié, consultez Libérez un hôte EC2 dédié Amazon.

Dedicated Host Reservations

Les réservations d'hôtes dédiés permettent de bénéficier d'une remise sur la facturation par rapport à l'exécution d'Hôtes dédiés à la demande. Trois options de paiement sont disponibles pour les réservations :

- Aucun paiement initial — Les réservations sans aucun paiement initial vous offrent une remise sur votre utilisation d'un Hôte dédié pendant une période donnée et ne nécessitent aucun paiement initial. Disponible pour une période d'un an ou de trois ans. Seules certaines familles d'instance prennent en charge le délai de trois ans pour les réservations sans aucun paiement initial.
- Paiement initial partiel — Une partie de la réservation doit être payée au départ et les heures restantes pendant la période sont facturées à un tarif réduit. Disponible pour une période d'un an ou de trois ans.
- Paiement initial complet — Offre le coût effectif le plus bas. Disponible pour une période d'un an et de trois ans et couvre le coût intégral de la période à l'avance, sans plus aucuns frais supplémentaire futurs.

Vous devez disposer d'un Hôtes dédiés actif sur votre compte pour pouvoir acheter des réservations. Chaque réservation peut couvrir un ou plusieurs hôtes prenant en charge la même famille de·l'instance dans une seule zone de disponibilité. Les réservations sont appliquées à la famille de·l'instance sur l'hôte, et non à la taille de l'instance. Si vous avez trois Hôtes dédiés avec des tailles d'instance différentes (`m4.xlarge`, `m4.medium` et `m4.large`), vous pouvez associer une même réservation `m4` à tous ces Hôtes dédiés. La famille de·l'instance et la zone de disponibilité doivent correspondre à celles des hôtes dédiés que vous souhaitez leur associer.

Lorsqu'une réservation est associée à un Hôte dédié, cet Hôte dédié ne peut pas être libéré avant la fin de la période de la réservation.

Pour plus d'informations sur les tarifs de réservation, consultez les tarifs Amazon EC2 Dedicated Hosts.

Savings Plans

Les Savings Plans sont un modèle de tarification flexible qui offre des économies importantes par rapport aux instances à la demande. Avec Savings Plans, vous vous engagez à utiliser une quantité constante, exprimée USD par heure, pour une durée d'un ou trois ans. Cela vous donne la flexibilité d'utiliser le Hôtes dédiés répondant le mieux à vos besoins et de continuer à économiser de l'argent

au lieu de vous engager pour un Hôte dédié spécifique. Pour plus d'informations, consultez le Guide de l'utilisateur des AWS Savings Plans.

> **Note**
>
> Les Savings Plans (Plans d'épargne) ne sont pas pris en charge par `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal`, et `u-24tb1.metal` Hôtes dédiés.

Tarification pour Windows Server sur les Hôtes dédiés

Sous réserve des conditions de licence Microsoft, vous pouvez transférer vos licences Windows Server et SQL Server existantes vers des hôtes dédiés. Aucuns frais supplémentaires ne s'applique à l'utilisation du logiciel si vous choisissez de réutiliser vos licences.

En outre, vous pouvez également utiliser Windows Server AMIs fourni par Amazon pour exécuter les dernières versions de Windows Server sur des hôtes dédiés. Cela est courant dans les scénarios dans lesquels vous disposez de licences de SQL serveur existantes pouvant être exécutées sur des hôtes dédiés, mais que vous avez besoin de Windows Server pour exécuter la charge de travail SQL du serveur. Les serveurs Windows AMIs fournis par Amazon ne sont pris en charge que sur les types d'instances de la génération actuelle. Pour plus d'informations, consultez les tarifs d'Amazon EC2 Dedicated Hosts.

Configurations de capacité des instances Amazon EC2 Dedicated Host

Les hôtes dédiés prennent en charge différentes configurations (cœurs physiques, sockets, VCPUs etc.) qui vous permettent d'exécuter des instances de différentes familles et tailles.

Lorsque vous attribuez un hôte dédié à votre compte, vous pouvez choisir une configuration qui prend en charge soit un type d'instance unique ou plusieurs types d'instances au sein de la même famille d'instances. Le nombre d'instances que vous pouvez exécuter sur un hôte dépend de la configuration que vous choisissez.

Table des matières

Prise en charge d'un seul type d'instance

Vous pouvez allouer un hôte dédié qui ne prend en charge qu'un seul type d'instance. Avec cette configuration, chaque instance que vous lancez sur l'hôte dédié doit être du même type d'instance, que vous spécifiez lors de l'allocation de l'hôte.

Par exemple, vous pouvez allouer un hôte qui prend uniquement en charge le type d'instance `m5.4xlarge`. Dans ce cas, vous pouvez exécuter uniquement des instances `m5.4xlarge` sur cet hôte.

Le nombre d'instances que vous pouvez lancer sur l'hôte dépend du nombre de cœurs physiques fournis par l'hôte et du nombre de cœurs utilisés par le type d'instance spécifié. Par exemple, si vous attribuez un hôte à des instances `m5.4xlarge`, l'hôte fournit 48 cœurs physiques, et chaque instance `m5.4xlarge` consomme 8 cœurs physiques. Cela signifie que vous pouvez lancer jusqu'à 6 instances sur cet hôte (48 cœurs physiques/8 cœurs par instance = 6 instances).

Prise en charge de plusieurs types d'instances

Vous pouvez allouer un hôte dédié qui prend en charge plusieurs types d'instances au sein de la même famille d'instances. Cela vous permet d'exécuter différents types d'instances sur le même hôte, à condition qu'ils appartiennent à la même famille d'instances et que l'hôte dispose d'une capacité d'instance suffisante.

Par exemple, vous pouvez allouer un hôte qui prend en charge différents types d'instances au sein de la famille d'instances `R5`. Dans ce cas, vous pouvez lancer n'importe quelle combinaison de types d'instances `R5`, tels que `r5.large`, `r5.xlarge`, `r5.2xlarge` et `r5.4xlarge`, sur cet hôte, jusqu'à la capacité de cœur physique de l'hôte.

Les familles d'instances suivantes prennent en charge les hôtes dédiés et plusieurs types d'instances :

- Usage général : A1, M5, M5n, M6i et T3
- Optimisées pour le calcul : C5, C5n et C6i
- Mémoire optimisée : R5, R5n et R6i

Le nombre d'instances que vous pouvez exécuter sur l'hôte dépend du nombre de cœurs physiques fournis par l'hôte et du nombre de cœurs utilisés par chaque type d'instance exécuté sur l'hôte. Par exemple, si vous allouez un hôte `R5`, qui fournit 48 cœurs physiques, et que vous exécutez

2 instances `r5.2xlarge` (4 cœurs x 2 instances) et 3 instances `r5.4xlarge` (8 cœurs x 3 instances), ces instances utilisent au total 32 cœurs et vous pouvez exécuter n'importe quelle combinaison d'instances R5 tant qu'elles ne dépassent pas les 16 cœurs restants.

Cependant, pour chaque famille de·l'instance, le nombre d'instances pouvant être exécutées pour chaque taille d'instance est limité. Par exemple, un hôte dédié R5 prend en charge jusqu'à 2 instances `r5.8xlarge`, ce qui utilise 32 des cœurs physiques. Dans ce cas, des instances R5 supplémentaires de tailles inférieures peuvent ensuite être utilisées pour remplir la capacité de l'hôte à la capacité cœur. Pour connaître le nombre de tailles d'instance prises en charge pour chaque famille d'instance, veuillez consulter la rubrique Tableau de configuration des hôtes dédiés.

Le tableau suivant présente des exemples de combinaison de types d'instances :

Famille d'instances	Exemples de combinaisons de tailles d'instances
R5	• Exemple 1 : 4 x `r5.4xlarge` + 4 x `r5.2xlarge` • Exemple 2 : 1 x `r5.12xlarge` + 1 x `r5.4xlarge` + 1 x `r5.2xlarge` + 5 x `r5.xlarge` + 2 x `r5.large`
C5	• Exemple 1 : 1 x `c5.9xlarge` + 2 x `c5.4xlarge` + 1 x `c5.xlarge` • Exemple 2 : 4 x `c5.4xlarge` + 1 x `c5.xlarge` + 2 x `c5.large`
M5	• Exemple 1 : 4 x `m5.4xlarge` + 4 x `m5.2xlarge` • Exemple 2 : 1 x `m5.12xlarge` + 1 x `m5.4xlarge` + 1 x `m5.2xlarge` + 5 x `m5.xlarge` + 2 x `m5.large`

Considérations

Gardez les points suivants à l'esprit lorsque vous travaillez avec des hôtes dédiés qui prennent en charge plusieurs types d'instances :

- Avec les hôtes dédiés de type N, tels que C5n, M5n et R5n, vous ne pouvez pas mélanger des tailles d'instance inférieures (`2xlarge` et inférieures) avec des tailles d'instance supérieures (`4xlarge` et supérieures, y compris `metal`). Si vous avez besoin d'utiliser simultanément des tailles d'instance inférieures et supérieures sur des hôtes dédiés de type N, vous devez allouer des hôtes distincts pour les tailles d'instance inférieures et supérieures.
- Nous vous recommandons de lancer d'abord les types d'instance supérieurs, puis de remplir la capacité d'instance restante avec les types d'instance inférieurs, si nécessaire.

Instances T3 éclatables sur les hôtes dédiés Amazon EC2

Les hôtes dédiés prennent en charge les instances T3 à performance modulable. Les instances T3 constituent un moyen rentable d'utiliser votre logiciel de BYOL licence éligible sur du matériel dédié. L'CPUencombrement réduit des instances T3 vous permet de consolider vos charges de travail sur un nombre réduit d'hôtes et d'optimiser l'utilisation de vos licences par cœur.

Les hôtes dédiés T3 sont particulièrement adaptés à l'exécution de BYOL logiciels dont l'CPUutilisation est faible à modérée. Cela inclut les licences logicielles éligibles par socket, par cœur ou par machine virtuelle, telles que Windows Server, Windows Desktop, SQL Server, SUSE Enterprise Linux Server, Red Hat Enterprise Linux et Oracle Database. Parmi les exemples des charges de travail adaptées aux Hôtes dédiés T3 se trouvent les petites et moyennes bases de données, les postes de travail virtuels, les environnements de développement et de test, les référentiels de code et les prototypes de produits. Les hôtes dédiés T3 ne sont pas recommandés pour les charges de travail présentant un taux d'CPUutilisation élevé soutenu ou pour les charges de travail qui subissent simultanément des pics corrélésCPU.

Les instances T3 sur les hôtes dédiés utilisent le même modèle de crédit que les instances T3 sur le matériel de location partagé. Cependant, elles prennent uniquement en charge le mode de crédit `standard` ; le mode de crédit `unlimited` n'est pas pris en charge. Dans le mode `standard`, les instances T3 sur les hôtes dédiés gagnent, dépensent et accumulent des crédits de la même manière que les instances extensibles sur le matériel de location partagé. Ils fournissent des CPU performances de base avec la capacité de dépasser le niveau de référence. Pour dépasser le niveau de référence, l'instance dépense les crédits qu'elle a accumulés dans son solde CPU créditeur. Lorsque les crédits accumulés sont épuisés, CPU l'utilisation est abaissée au niveau de référence.

Pour plus d'informations sur le mode `standard`, consultez Fonctionnement des instance de performance à capacité extensible standards.

Les hôtes dédiés T3 prennent en charge toutes les fonctionnalités proposées par Amazon EC2 Dedicated Hosts, y compris plusieurs tailles d'instance sur un seul hôte, les groupes de ressources d'hôtes etBYOL.

Tailles et configurations d'instance T3 prises en charge

Les hôtes dédiés T3 exécutent des instances T3 généralistes qui partagent les CPU ressources de l'hôte en fournissant des CPU performances de référence et en permettant d'atteindre un niveau supérieur en cas de besoin. Cela permet aux hôtes dédiés T3, qui ont 48 cœurs, de prendre en charge un maximum de 192 instances par hôte. Afin d'utiliser efficacement les ressources de l'hôte et de fournir les meilleures performances d'instance, l'algorithme de placement d'EC2instance Amazon calcule automatiquement le nombre d'instances pris en charge et les combinaisons de tailles d'instance pouvant être lancées sur l'hôte.

Les hôtes dédiés T3 prennent en charge plusieurs types d'instance sur le même hôte. Les hôtes dédiés ne prennent pas en charge toutes les tailles d'instances T3. Vous pouvez exécuter différentes combinaisons d'instances T3 dans la CPU limite de l'hôte.

Le tableau suivant répertorie les types d'instances pris en charge, résume les performances de chaque type d'instance et indique le nombre maximal d'instances pour chaque taille pouvant être lancées.

Type d'instance	vCPUs	Mémoire (Gio)	CPUUtilisation de référence par v CPU	Bande passante d'éclatement du réseau (Gbit/s)	Bande passante Amazon EBS Burst (Mbits/s)	Nombre maximal d'instances par hôte dédié
t3.na	2	0.5	5 %	5	Jusqu'à 2 085	192
t3.m	2	1	10 %	5	Jusqu'à 2 085	192
t3.sn	2	2	20 %	5	Jusqu'à 2 085	192
t3.m	2	4	20 %	5	Jusqu'à 2 085	192

Type d'instance	vCPUs	Mémoire (Gio)	CPUUtilisation de référence par v CPU	Bande passante d'éclatement du réseau (Gbit/s)	Bande passante Amazon EBS Burst (Mbits/s)	Nombre maximal d'instances par hôte dédié
t3.la	2	8	30 %	5	2 780	96
t3.xl	4	16	40 %	5	2 780	48
t3.2x e	8	32	40 %	5	2 780	24

Surveillez CPU l'utilisation des hôtes dédiés T3

Vous pouvez utiliser la CloudWatch métrique `DedicatedHostCPUUtilization` Amazon pour surveiller le CPU taux d'utilisation d'un hôte dédié. La métrique est disponible dans l'espace de noms `EC2` et dans la dimension `Per-Host-Metrics`. Pour de plus amples informations, veuillez consulter Métriques d'hôte dédié.

Apportez vos propres licences logicielles à Amazon EC2 Dedicated Hosts

Les Hôtes dédiés vous permettent d'utiliser vos licences logicielles existantes par socket, par cœur ou par machine virtuelle. Lorsque vous utilisez vos propres licences, vous êtes responsable de leur gestion. Amazon EC2 possède toutefois des fonctionnalités qui vous aident à garantir la conformité des licences, telles que l'affinité entre les instances et le placement ciblé.

Voici les étapes générales à suivre pour importer votre propre image de machine sous licence en volume sur AmazonEC2.

1. Assurez-vous que les termes du contrat de licence régissant l'utilisation de vos images de machine permettent l'utilisation dans un environnement cloud virtualisé. Pour de plus amples informations sur les licences Microsoft, consultez Amazon Web Services et licences Microsoft.
2. Après avoir vérifié que l'image de votre machine peut être utilisée dans AmazonEC2, importez-la à l'aide de VM Import/Export. Pour plus d'informations sur la procédure à suivre pour importer votre image de machine, consultez le Guide de l'utilisateur VM Import/Export.
3. Une fois votre image de machine importée, vous pouvez lancer des instances depuis cette image sur des Hôtes dédiés actifs de votre compte.

4. Lorsque vous exécutez ces instances, selon le système d'exploitation, il peut vous être demandé de les activer sur votre propre KMS serveur (par exemple, Windows Server ou Windows SQL Server). Vous ne pouvez pas activer votre Windows importé AMI sur le KMS serveur Amazon Windows.

> **Note**
>
> Pour suivre la façon dont vos images sont utilisées AWS, activez l'enregistrement par l'hôte dans AWS Config. Vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées à un hôte dédié et utiliser la sortie comme source de données pour les rapports sur les licences. Pour de plus amples informations, veuillez consulter Suivez les modifications de configuration d'Amazon EC2 Dedicated Host à l'aide de AWS Config.

Placement automatique et affinité d'hôte Amazon EC2 Dedicated Host

Le contrôle de placement pour l'Hôtes dédiés est effectué au niveau de l'instance et au niveau de l'hôte.

Placement automatique

Le placement automatique est configuré au niveau de l'hôte. Il vous permet de définir si les instances que vous lancez le sont sur un hôte spécifique ou sur n'importe quel hôte disponible doté de configurations correspondantes.

Lorsque le placement automatique est désactivé pour un hôte dédié, celui-ci n'accepte que les lancements d'instances de location d'hôte qui spécifient son identifiant d'hôte unique. Il s'agit du paramètre par défaut pour un nouvel Hôtes dédiés.

Lorsque le placement automatique est activé pour un hôte dédié, celui-ci accepte tout lancement d'instance de location d'hôte non ciblé correspondant à la configuration de son type d'instance.

Lors du lancement d'une instance, vous devez configurer sa location. Le lancement d'une instance sur un Hôte dédié sans indiquer un `HostId` spécifique permet de la lancer sur n'importe quel Hôte dédié sur lequel le placement automatique est activé et qui correspond à son type d'instance.

Affinité de l'hôte

L'affinité de l'hôte est configurée au niveau de l'instance. Elle établit une relation de lancement entre une instance et un Hôte dédié.

Lorsque l'affinité a pour valeur `Host`, une instance lancée sur un hôte spécifique redémarre toujours sur le même hôte si elle est arrêtée. Cela s'applique aussi bien aux lancements ciblés qu'aux lancements non-ciblés.

Lorsque l'affinité a pour valeur `Default` et que vous arrêtez et redémarrez l'instance, cette dernière peut être redémarrée sur tout hôte disponible. Toutefois, elle essaie de se relancer sur le dernier Hôte dédié sur lequel elle s'est exécutée (dans la mesure du possible).

Attribuez un hôte EC2 dédié Amazon à utiliser sur votre compte

Pour commencer à utiliser un hôte dédié, vous devez d'abord l'attribuer à votre compte. Lorsque vous allouez l'Hôte dédié, la capacité de l'Hôte dédié est immédiatement mise à disposition dans votre compte et vous pouvez commencer à lancer des instances sur l'Hôte dédié.

Lorsque vous attribuez un hôte dédié à votre compte, vous pouvez choisir une configuration qui prend en charge soit un type d'instance unique ou plusieurs types d'instances au sein de la même famille d'instances. Le nombre d'instances que vous pouvez exécuter sur l'hôte dépend de la configuration que vous choisissez. Pour plus d'informations, voir Configurations de capacité des instances Amazon EC2 Dedicated Host.

Console

Pour allouer un Hôte dédié

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Hôtes dédiés, puis Allouer un Hôte dédié.
3. Pour Famille d'instances, choisissez la famille de·l'instance de l'Hôte dédié.
4. Indiquez si l'Hôte dédié prend en charge plusieurs types d'instances dans la famille d'instances sélectionnée ou uniquement un type d'instance spécifique. Effectuez l'une des actions suivantes :

   - Pour configurer l'Hôte dédié afin qu'il prenne en charge plusieurs types d'instances dans la famille d'instances sélectionnée, pour Support multiple instance types (Prendre en charge plusieurs types d'instances), choisissez Activer. La sélection de cette option vous permet de lancer différentes tailles d'instances d'une même famille d'instances sur l'Hôte dédié. Par exemple, si vous choisissez la famille d'instances `m5` et que vous choisissez cette option, vous pouvez lancer les instances `m5.xlarge` et `m5.4xlarge` sur l'Hôte dédié.
   - Pour configurer l'hôte dédié afin qu'il prenne en charge un type d'instance spécifique dans la famille d'instances sélectionnée, désélectionnez Support multiple instance

types (Prendre en charge plusieurs types d'instances), puis, dans Instance type (Type d'instance), choisissez le type d'instance à prendre en charge. Cette action vous permet de lancer un seul type d'instance sur l'Hôte dédié. Par exemple, si vous choisissez cette option et spécifiez `m5.4xlarge` comme type d'instance pris en charge, vous pouvez uniquement lancer des instances `m5.4xlarge` sur l'Hôte dédié.

5. Pour Zone de disponibilité, choisissez la zone de disponibilité dans laquelle allouer l'Hôte dédié.
6. Pour autoriser l'Hôte dédié à accepter les lancements d'instance non ciblés correspondant à son type d'instance, pour Instance auto-placement (Placement automatique d'instance), choisissez Enable (Autoriser). Pour en savoir plus sur le placement automatique, consultez Placement automatique et affinité d'hôte Amazon EC2 Dedicated Host.
7. Pour autoriser la récupération d'hôte pour l'Hôte dédié, pour Host recovery (Récupération de l'hôte), choisissez Activer. Pour plus d'informations, consultez Restauration d'EC2un hôte dédié Amazon.
8. Pour Quantité, entrez le nombre d'Hôtes dédiés à allouer.
9. (Facultatif) Sélectionnez Ajouter une nouvelle balise et saisissez une clé et une valeur de balise.
10. Choisissez Allocate.

AWS CLI

Pour allouer un Hôte dédié

Utilisez la commande allocate-hosts AWS CLI . La commande suivante alloue un Hôte dédié qui prend en charge plusieurs types d'instances de la famille d'instances `m5` dans la zone de disponibilité `us-east-1a`. La fonction de récupération de l'hôte est activée et la fonction de placement automatique est désactivée sur l'hôte.

```
aws ec2 allocate-hosts --instance-family "m5" --availability-zone "us-east-1a" --
auto-placement "off" --host-recovery "on" --quantity 1
```

La commande suivante alloue un Hôte dédié qui prend en charge des lancements d'instance `m4.large` non ciblés dans la zone de disponibilité `eu-west-1a`, autorise la récupération de l'hôte et applique une balise avec une clé `purpose` et une valeur `production`.

```
aws ec2 allocate-hosts --instance-type "m4.large" --availability-zone "eu-west-1a"
 --auto-placement "on" --host-recovery "on" --quantity 1 --tag-specifications
 'ResourceType=dedicated-host,Tags=[{Key=purpose,Value=production}]'
```

PowerShell

Pour allouer un Hôte dédié

Utilisez la New-EC2Host AWS Tools for Windows PowerShell commande. La commande suivante alloue un Hôte dédié qui prend en charge plusieurs types d'instances de la famille d'instances `m5` dans la zone de disponibilité `us-east-1a`. La fonction de récupération de l'hôte est activée et la fonction de placement automatique est désactivée sur l'hôte.

```
PS C:\> New-EC2Host -InstanceFamily m5 -AvailabilityZone us-east-1a -
AutoPlacement Off -HostRecovery On -Quantity 1
```

Les commandes suivantes allouent un Hôte dédié qui prend en charge des lancements d'instance non ciblés `m4.large` dans la zone de disponibilité `eu-west-1a` et appliquent une balise avec une clé `purpose` et une valeur `production`.

Le paramètre `TagSpecification` utilisé pour baliser un Hôte dédié à la création requiert un objet qui spécifie le type de ressource à baliser, ainsi que la clé et la valeur de balise. Les commandes suivantes permettent de créer l'objet requis.

```
PS C:\> $tag = @{ Key="purpose"; Value="production" }
PS C:\> $tagspec = new-object Amazon.EC2.Model.TagSpecification
PS C:\> $tagspec.ResourceType = "dedicated-host"
PS C:\> $tagspec.Tags.Add($tag)
```

La commande suivante alloue le Hôte dédié et applique la balise spécifiée dans l'objet `$tagspec`.

```
PS C:\> New-EC2Host -InstanceType m4.large -AvailabilityZone eu-west-1a -
AutoPlacement On -HostRecovery On -Quantity 1 -TagSpecification $tagspec
```

Lancer EC2 des instances Amazon sur un hôte EC2 dédié Amazon

Une fois que vous avez alloué un Hôte dédié, vous pouvez lancer des instances sur cet hôte. Vous ne pouvez pas lancer des instances avec la location `host` si vous n'avez pas d'Hôtes dédiés actifs avec suffisamment de capacité disponible pour le type d'instance que vous lancez.

> **Tip**
>
> Pour les hôtes dédiés qui prennent en charge plusieurs tailles d'instance, nous vous recommandons de lancer d'abord les instances de plus grande taille, puis de remplir la capacité d'instance restante avec les instances de plus petite taille, si nécessaire.

Avant de lancer vos instances, prenez note des restrictions. Pour plus d'informations, consultez Restrictions Hôtes dédiés.

Vous pouvez lancer une instance dans un Hôte dédié à l'aide des méthodes suivantes.

Console

Pour lancer une instance sur un Hôte dédié spécifique depuis la page Hôtes dédiés

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Choisissez Hôtes dédiés dans le volet de navigation.
3. Dans la page Dedicated Hosts (Hôtes dédiés), sélectionnez un hôte et choisissez Actions, Launch Instance(s) onto host (Lancer une ou plusieurs instances sur l'hôte).
4. Dans la section Images de l'application et du système d'exploitation, sélectionnez-en un AMI dans la liste.

   > **Note**
   >
   > SQLLe serveur et RHEL AMIs fourni par Amazon ne EC2 peuvent pas être utilisés avec des hôtes dédiés. SUSE

5. Dans la section Instance type (Type d'instance), sélectionnez le type d'instance à lancer.

   > **Note**
   >
   > Si l'Hôte dédié ne prend en charge qu'un seul type d'instance, ce type est sélectionné par défaut et ne peut pas être modifié.
   > Si l'Hôte dédié prend en charge plusieurs types d'instances, vous devez sélectionner un type d'instance dans la famille d'instances prise en charge en fonction de la capacité d'instance disponible de l'Hôte dédié. Nous vous recommandons de lancer

d'abord les tailles d'instance plus grandes, puis de remplir la capacité d'instance restante avec les tailles d'instance plus petites, si nécessaire.

6. Dans la section Key pair (Paire de clés), sélectionnez la paire de clés à associer à l'instance.
7. Dans la section Détails avancés, pour Affinité de location, choisissez l'une des options suivantes :

   - Désactivé : affinité avec l'hôte désactivée. L'instance est lancée sur l'hôte spécifié, mais il n'est pas garanti qu'elle redémarrera sur le même hôte dédié en cas d'arrêt.
   - Un identifiant d'hôte dédié : affinité d'hôte activée. En cas d'arrêt, l'instance redémarre toujours sur cet hôte spécifié s'il a de la capacité. Si l'hôte n'a pas de capacité, l'instance ne peut pas être redémarrée ; vous devez établir une affinité avec un autre hôte.

   Pour en savoir plus sur l'affinité, consultez Placement automatique et affinité d'hôte Amazon EC2 Dedicated Host.

   > **Note**
   >
   > Les options Location et Hôte sont préconfigurées en fonction de l'hôte que vous avez sélectionné.

8. Configurez les options d'instance restantes selon les besoins. Pour de plus amples informations, veuillez consulter Référence pour les paramètres de configuration des EC2 instances Amazon.
9. Sélectionnez Launch instance (Lancer une instance).

Pour lancer une instance sur un Hôte dédié à l'aide de l'assistant de lancement d'instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Instances, Launch instance (Lancer une instance).
3. Dans la section Images de l'application et du système d'exploitation, sélectionnez-en un AMI dans la liste.

> **Note**
>
> SQLLe serveur et RHEL AMIs fourni par Amazon ne EC2 peuvent pas être utilisés avec des hôtes dédiés. SUSE

4. Dans la section Instance type (Type d'instance), sélectionnez le type d'instance à lancer.
5. Dans la section Key pair (Paire de clés), sélectionnez la paire de clés à associer à l'instance.
6. Dans la section Advanced details (Détails avancés), procédez comme suit :

   a. Pour Tenancy (Location), sélectionnez Dedicated Host (Hôte dédié).

   b. Pour Target host by (Cibler l'hôte par), sélectionnez Host ID (ID de l'hôte).

   c. Pour Target host ID (ID de l'hôte cible), sélectionnez l'hôte sur lequel lancer l'instance.

   d. Pour Affinité de location, choisissez l'une des options suivantes :

   - Désactivé : affinité avec l'hôte désactivée. L'instance est lancée sur l'hôte spécifié, mais il n'est pas garanti qu'elle redémarrera sur le même hôte dédié en cas d'arrêt.
   - Un identifiant d'hôte dédié : affinité d'hôte activée. En cas d'arrêt, l'instance redémarre toujours sur cet hôte spécifié s'il a de la capacité. Si l'hôte n'a pas de capacité, l'instance ne peut pas être redémarrée ; vous devez établir une affinité avec un autre hôte.

   Pour en savoir plus sur l'affinité, consultez Placement automatique et affinité d'hôte Amazon EC2 Dedicated Host.
7. Configurez les options d'instance restantes selon les besoins. Pour de plus amples informations, veuillez consulter Référence pour les paramètres de configuration des EC2 instances Amazon.
8. Sélectionnez Launch instance (Lancer une instance).

AWS CLI

Pour lancer une instance dans un Hôte dédié

Utilisez la AWS CLI commande run-instances et spécifiez l'affinité, la location et l'hôte de l'instance dans le `Placement` paramètre de requête.

PowerShell

Pour lancer une instance dans un Hôte dédié

Utilisez la New-EC2Instance AWS Tools for Windows PowerShell commande et spécifiez l'affinité, la location et l'hôte de l'instance dans le paramètre de `Placement` demande.

Lancer EC2 des instances Amazon dans un groupe de ressources hôte

Les hôtes dédiés sont également intégrés à AWS License Manager. Grâce à License Manager, vous pouvez créer un groupe de ressources hôte, qui est un ensemble d'Hôtes dédiés gérés en tant qu'entité unique. Lors de la création d'un groupe de ressources hôte, vous spécifiez les préférences de gestion de l'hôte, telles que l'allocation automatique et la libération automatique, pour les Hôtes dédiés. Vous pouvez ainsi lancer des instances sur les Hôtes dédiés sans allouer ni gérer manuellement ces hôtes. Pour plus d'informations, consultez Groupes de ressources hôte dans le Guide de l'utilisateur AWS License Manager .

Lorsque vous lancez une instance dans un groupe de ressources hôte doté d'un hôte dédié avec une capacité d'instance disponible, Amazon EC2 lance l'instance sur cet hôte. Si le groupe de ressources d'hôtes ne dispose pas d'un hôte disposant d'une capacité d'instance disponible, Amazon alloue EC2 automatiquement un nouvel hôte dans le groupe de ressources d'hôtes, puis lance l'instance sur cet hôte. Pour plus d'informations, consultez Groupes de ressources hôte dans le Guide de l'utilisateur AWS License Manager .

Exigences et limites

- Vous devez associer une configuration de licence basée sur le noyau ou le socket au. AMI
- Vous ne pouvez pas utiliser le SQL SUSE serveur ou RHEL AMIs les hôtes dédiés fournis EC2 par Amazon.
- Vous ne pouvez pas cibler un hôte spécifique en choisissant un ID d'hôte et vous ne pouvez pas activer l'affinité d'instance lors du lancement d'une instance dans un groupe de ressources hôte.

Vous pouvez lancer une instance dans un groupe de ressources hôte à l'aide des méthodes suivantes.

Console

Pour lancer une instance dans un groupe de ressources hôte

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Instances, Launch instance (Lancer une instance).
3. Dans la section Images de l'application et du système d'exploitation, sélectionnez-en un AMI dans la liste.

   > **Note**
   >
   > SQLLe serveur et RHEL AMIs fourni par Amazon ne EC2 peuvent pas être utilisés avec des hôtes dédiés. SUSE

4. Dans la section Instance type (Type d'instance), sélectionnez le type d'instance à lancer.
5. Dans la section Key pair (Paire de clés), sélectionnez la paire de clés à associer à l'instance.
6. Dans la section Advanced details (Détails avancés), procédez comme suit :

   a. Pour Tenancy (Location), sélectionnez Dedicated Host (Hôte dédié).

   b. Pour Target host by (Cibler l'hôte par), sélectionnez Host resource group (Groupe de ressources hôte).

   c. Pour Host resource group name (Groupe de ressources hôte de location), sélectionnez le groupe de ressources hôte dans lequel lancer l'instance.

   d. Pour Tenancy affinity (Affinité de location), sélectionnez l'une des options suivantes :

      - Sélectionnez Off (Désactivé) — L'instance est lancée sur l'hôte spécifié, mais il n'est pas garanti qu'elle redémarre sur le même hôte dédié si elle est arrêtée.
      - Sélectionnez l'ID de l'hôte dédié — Si l'instance est arrêtée, elle redémarre toujours sur cet hôte spécifique.

   Pour en savoir plus sur l'affinité, consultez Placement automatique et affinité d'hôte Amazon EC2 Dedicated Host.

7. Configurez les options d'instance restantes selon les besoins. Pour de plus amples informations, veuillez consulter Référence pour les paramètres de configuration des EC2 instances Amazon.

8. Sélectionnez Launch instance (Lancer une instance).

AWS CLI

Pour lancer une instance dans un groupe de ressources hôte

Utilisez la AWS CLI commande run-instances et, dans le paramètre de `Placement` requête, omettez l'option Tenancy et spécifiez le groupe de ressources hôte. ARN

PowerShell

Pour lancer une instance dans un groupe de ressources hôte

Utilisez la New-EC2Instance AWS Tools for Windows PowerShell commande et, dans le paramètre de `Placement` requête, omettez l'option Tenancy et spécifiez le groupe de ressources hôte. ARN

Modifier le paramètre de placement automatique pour un hôte Amazon EC2 Dedicated Host existant

Vous pouvez modifier les paramètres de placement automatique d'un hôte dédié après l'avoir attribué à votre AWS compte, en utilisant l'une des méthodes suivantes.

Console

Pour modifier le placement automatique d'un Hôte dédié

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Sélectionnez un hôte et choisissez Actions, Modify host (Modifier l'hôte).
4. Pour Instance auto-placement (Placement automatique de l'instance), choisissez Activer pour activer le placement automatique ou Désactiver pour désactiver le placement automatique. Pour plus d'informations, consultez Placement automatique et affinité d'hôte Amazon EC2 Dedicated Host.
5. Choisissez Enregistrer.

AWS CLI

Pour modifier le placement automatique d'un Hôte dédié

Utilisez la commande modify-hosts AWS CLI . Les exemples suivants activent le placement automatique pour l'Hôte dédié spécifié.

```
aws ec2 modify-hosts --auto-placement on --host-ids h-012a3456b7890cdef
```

PowerShell

Pour modifier le placement automatique d'un Hôte dédié

Utilisez la Edit-EC2Host AWS Tools for Windows PowerShell commande. Les exemples suivants activent le placement automatique pour l'Hôte dédié spécifié.

```
PS C:\> Edit-EC2Host --AutoPlacement 1 --HostId h-012a3456b7890cdef
```

Modifier les types d'instances pris en charge pour un hôte Amazon EC2 Dedicated Host existant

Vous pouvez modifier un Hôte dédié afin de modifier les types d'instances qu'il prend en charge. S'il prend actuellement en charge un seul type d'instance, vous pouvez le modifier afin qu'il en prenne en charge plusieurs dans cette famille d'instances. De même, s'il prend en charge plusieurs types d'instances, vous pouvez le modifier afin qu'il n'en prenne plus qu'un seul.

Pour modifier un Hôte dédié afin qu'il prenne en charge plusieurs types d'instances, vous devez d'abord arrêter toutes les instances en cours d'exécution sur l'hôte. Cette modification prend effet au bout d'environ 10 minutes. L'Hôte dédié passe à l'état `pending` pendant que la modification est en cours. Vous ne pouvez pas démarrer les instances arrêtées ou lancer de nouvelles instances sur l'Hôte dédié lorsqu'il est à l'état `pending`.

Pour qu'il soit possible de modifier un Hôte dédié prenant en charge plusieurs types d'instances afin qu'il n'en prenne plus qu'un seul, l'hôte ne doit avoir aucune instance en cours d'exécution ou les instances en cours d'exécution doivent être du type qui devra être pris en charge par l'hôte. Par exemple, pour modifier un hôte prenant en charge plusieurs types d'instances dans la famille d'instances `m5` afin qu'il ne prenne plus en charge que les instances `m5.large`, il faut que l'Hôte dédié n'ait aucune instance en cours d'exécution ou que seules des instances `m5.large` soient en cours d'exécution sur l'hôte.

Si vous allouez un hôte pour un type d'instance virtualisée, vous ne pouvez pas modifier le type d'instance en un type d'instance `.metal` après l'allocation de l'hôte. Par exemple, si vous allouez un hôte pour le type d'instance `m5.large`, vous ne pouvez pas modifier le type d'instance en

`m5.metal`. De même, si vous allouez un hôte pour un type d'instance `.metal`, vous ne pouvez pas modifier le type d'instance en un type d'instance virtualisée après l'allocation de l'hôte. Par exemple, si vous allouez un hôte pour le type d'instance `m5.metal`, vous ne pouvez pas modifier le type d'instance en `m5.large`.

Vous pouvez modifier les types d'instance pris en charge à l'aide de l'une des méthodes suivantes.

Console

Pour modifier les types d'instance pris en charge pour un Hôte dédié

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Dedicated Host (Hôte dédié).
3. Sélectionnez l'Hôte dédié à modifier et choisissez Actions, Modify host (Modifier l'hôte).
4. Selon la configuration actuelle de l'Hôte dédié, procédez comme indiqué ci-après.

   - Si l'Hôte dédié prend actuellement en charge un type d'instance spécifique, l'option Support multiple instance types (Prendre en charge plusieurs types d'instance) n'est pas activée et la liste Type d'instance répertorie le type d'instance pris en charge. Pour modifier l'hôte afin qu'il prenne en charge plusieurs types d'instances dans la famille d'instances actuelle, pour Support multiple instance types (Prendre en charge plusieurs types d'instances), choisissez Activer.

     Pour modifier un hôte afin qu'il prenne en charge plusieurs types d'instances, vous devez d'abord arrêter toutes les instances en cours d'exécution sur l'hôte.
   - Si l'Hôte dédié prend actuellement en charge plusieurs types d'instances d'une famille, Activé est sélectionné pour Support multiple instance types (Prendre en charge plusieurs types d'instances). Pour modifier l'hôte afin qu'il prenne en charge un type d'instance spécifique, pour Support multiple instance types (Prendre en charge plusieurs types d'instances), décochez Activer, puis pour Type d'instance, sélectionnez le type d'instance spécifique à prendre en charge.

     Vous ne pouvez pas modifier la famille d'instances prise en charge par l'Hôte dédié.
5. Choisissez Enregistrer.

AWS CLI

Pour modifier les types d'instance pris en charge pour un Hôte dédié

Utilisez la commande modify-hosts AWS CLI .

La commande suivante modifie un Hôte dédié afin qu'il prenne en charge plusieurs types d'instances au sein de la famille d'instances `m5`.

```
aws ec2 modify-hosts --instance-family m5 --host-ids h-012a3456b7890cdef
```

La commande suivante modifie un Hôte dédié afin qu'il prenne uniquement en charge les instances `m5.xlarge`.

```
aws ec2 modify-hosts --instance-type m5.xlarge --instance-family --host-
ids h-012a3456b7890cdef
```

PowerShell

Pour modifier les types d'instance pris en charge pour un Hôte dédié

Utilisez la Edit-EC2Host AWS Tools for Windows PowerShell commande.

La commande suivante modifie un Hôte dédié afin qu'il prenne en charge plusieurs types d'instances au sein de la famille d'instances `m5`.

```
PS C:\> Edit-EC2Host --InstanceFamily m5 --HostId h-012a3456b7890cdef
```

La commande suivante modifie un Hôte dédié afin qu'il prenne uniquement en charge les instances `m5.xlarge`.

```
PS C:\> Edit-EC2Host --InstanceType m5.xlarge --HostId h-012a3456b7890cdef
```

Modifier la location et l'affinité d'un hôte EC2 dédié Amazon pour une instance Amazon EC2

Vous pouvez modifier la location d'une instance après l'avoir lancée. Vous pouvez également modifier l'affinité de votre instance afin de cibler un hôte spécifique ou de l'autoriser à être lancée sur n'importe quel hôte dédié disponible avec les attributs correspondants dans votre compte. Pour qu'il soit possible de modifier l'affinité ou la location de l'instance, il faut que l'instance soit à l'état `stopped`.

Les informations relatives au système d'exploitation de votre instance, et le fait que le SQL serveur soit installé ou non, ont une incidence sur les conversions prises en charge. Pour plus d'informations sur les chemins de conversion de location disponibles pour votre instance, consultez la section Tenancy conversion dans le Guide de l'utilisateur de License Manager.

> **Note**
>
> Pour les instances T3, vous devez lancer l'instance sur un hôte dédié pour utiliser une location `host`. Pour les instances T3, vous ne pouvez pas modifier la location de `host` à `dedicated` ou `default`. Si vous tentez d'effectuer l'une de ces modifications de location non prises en charge, vous obtiendrez un code d'erreur `InvalidRequest`.

Vous pouvez modifier la location et l'affinité d'une instance à l'aide des méthodes suivantes.

Console

Pour modifier la location d'instance ou l'affinité

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Choisissez Instances, puis sélectionnez l'instance à modifier.
3. Choisissez État de l'instance, Arrêter.
4. Tandis que l'instance est toujours sélectionnée, choisissez Actions, Paramètres de l'instance, puis Changer le placement d'instance.
5. Sur la page Modifier le placement de l'instance, configurez les éléments suivants :
   - Location — Choisissez l'une des options suivantes :
     - Exécuter une instance matérielle dédiée — Lance l'instance en tant qu'Instance dédiée. Pour plus d'informations, consultez Instances EC2 dédiées Amazon.
     - Launch the instance on a Hôte dédié — Lance l'instance sur un Hôte dédié avec une affinité configurable.
   - Affinité — Choisissez l'une des options suivantes :
     - Cette instance peut être exécutée sur un de mes hôtes — L'instance est lancée sur n'importe quel Hôte dédié disponible de votre compte prenant en charge son type d'instance.
     - Cette instance ne peut être exécutée que sur l'hôte sélectionné — L'instance ne peut s'exécuter que sur l'Hôte dédié sélectionné pour Hôte cible.

- Hôte cible — Sélectionnez l'Hôte dédié sur lequel l'instance doit s'exécuter. Si aucun hôte cible n'est répertorié, cela signifie que vous n'avez peut-être aucun Hôtes dédiés compatible disponible dans votre compte.

Pour plus d'informations, consultez Placement automatique et affinité d'hôte Amazon EC2 Dedicated Host.

6. Choisissez Enregistrer.

AWS CLI

Pour modifier la location d'instance ou l'affinité

Utilisez la modify-instance-placement AWS CLI commande. Les exemples suivants remplacent l'affinité de l'instance spécifiée `default` par `host` et indiquent l'Hôte dédié avec lequel l'instance a une affinité.

```
aws ec2 modify-instance-placement --instance-id i-1234567890abcdef0 --affinity host
 --tenancy host --host-id h-012a3456b7890cdef
```

PowerShell

Pour modifier la location d'instance ou l'affinité

Utilisez la Edit-EC2InstancePlacement AWS Tools for Windows PowerShell commande. Les exemples suivants remplacent l'affinité de l'instance spécifiée `default` par `host` et indiquent l'Hôte dédié avec lequel l'instance a une affinité.

```
PS C:\> Edit-EC2InstancePlacement -InstanceId i-1234567890abcdef0 -Affinity host -
Tenancy host -HostId h-012a3456b7890cdef
```

Libérez un hôte EC2 dédié Amazon

Si vous n'avez plus besoin d'un hôte dédié, vous pouvez arrêter l'exécution des instances sur l'hôte, leur demander de se lancer sur un autre hôte, puis libérer l'hôte.

Pour pouvoir libérer l'Hôte dédié, vous devez arrêter toutes les instances exécutées sur ce dernier. Ces instances peuvent être migrées vers un autre Hôtes dédiés de votre compte afin que vous puissiez continuer à les utiliser. Ces étapes ne concernent que les Hôtes dédiés à la demande.

Vous pouvez libérer un Hôte dédié à l'aide des méthodes suivantes.

Console

Pour libérer un Hôte dédié

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Sur la page Hôtes dédiés, sélectionnez le Hôte dédié à libérer.
4. Sélectionnez Actions, puis Libérer des hôtes.
5. Choisissez Libérer pour confirmer.

AWS CLI

Pour libérer un Hôte dédié

Utilisez la commande release-hosts AWS CLI .

```
aws ec2 release-hosts --host-ids h-012a3456b7890cdef
```

PowerShell

Pour libérer un Hôte dédié

Utilisez la Remove-EC2Hosts AWS Tools for Windows PowerShell commande.

```
PS C:\> Remove-EC2Hosts -HostId h-012a3456b7890cdef
```

Une fois que vous avez libéré un Hôte dédié, vous ne pouvez plus réutiliser le même hôte ou ID d'hôte et la facturation à la demande pour cet hôte cesse. L'état de l'Hôte dédié devient `released` et vous ne pouvez plus lancer aucune instance sur cet hôte.

> **Note**
>
> Si vous avez récemment libéré des Hôtes dédiés, il peut s'écouler un peu de temps avant qu'ils cessent d'être comptabilisés dans le cadre de votre limite. Pendant ce temps, vous pouvez recevoir des erreurs `LimitExceeded` lorsque vous essayez d'allouer de nouveaux Hôtes dédiés. Dans ce cas, réessayez d'allouer ces nouveaux hôtes après quelques minutes.

Les instances qui ont été arrêtées peuvent toujours être utilisées et sont répertoriées à la page Instances. Elles conservent leur paramètre de location `host`.

Achetez des réservations d'hôtes dédiés pour bénéficier de remises sur la facturation des hôtes dédiés

Les réservations d'hôtes dédiés vous permettent de bénéficier d'une réduction allant jusqu'à 70 % par rapport à la tarification des hôtes dédiés à la demande. Vous devez disposer d'hôtes dédiés actifs sur votre compte avant de pouvoir acheter des réservations d'hôtes dédiés. Pour de plus amples informations, veuillez consulter Dedicated Host Reservations.

Vous pouvez acheter des réservations d'hôtes dédiés en utilisant les méthodes suivantes :

Console

Pour acheter des réservations

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Choisissez Hôtes dédiés, Réservations d'hôtes dédiés, Purchase Réservation d'hôtes dédiés (Acheter un hôte dédié).
3. Sur l'écran Rechercher des offres, procédez comme suit :
   a. Dans Famille d'instances, sélectionnez la famille d'instances de l'hôte dédié pour lequel vous souhaitez acheter la réservation d'hôte dédié.
   b. Pour l'option de paiement, sélectionnez et configurez votre option de paiement préférée.
4. Choisissez Suivant.
5. Sélectionnez les hôtes dédiés auxquels associer la réservation d'hôte dédié, puis choisissez Next.
6. (Facultatif) Attribuez des tags à la réservation d'hôte dédié.
7. Vérifiez votre commande et choisissez Acheter.

AWS CLI

Pour acheter des réservations

1. Utilisez la describe-host-reservation-offerings AWS CLI commande pour répertorier les offres disponibles qui répondent à vos besoins. L'exemple suivant répertorie les offres qui prennent en charge des instances dans la famille d'instances `m4` et ont une durée d'un an.

> **Note**
>
> La durée est indiquée en secondes. Une période d'un an comporte 31 536 000 secondes, tandis qu'une période de trois ans comporte 94 608 000 secondes.

```
aws ec2 describe-host-reservation-offerings --filter Name=instance-family,Values=m4 --max-duration 31536000
```

Les deux commandes renvoient une liste d'offres qui correspondent à vos critères de recherche. Notez l'`offeringId` de l'offre à acheter.

2. Utilisez la purchase-host-reservation AWS CLI commande pour acheter l'offre et fournissez les informations `offeringId` indiquées à l'étape précédente. L'exemple suivant achète la réservation spécifiée et l'associe à un hôte dédié spécifique qui est déjà attribué dans le AWS compte, et il applique une balise avec une clé `purpose` et une valeur de`production`.

```
aws ec2 purchase-host-reservation --offering-id hro-03f707bf363b6b324 --host-id-set h-013abcd2a00cbd123 --tag-specifications 'ResourceType=host-reservation,Tags={Key=purpose,Value=production}'
```

PowerShell

Pour acheter des réservations

1. Utilisez la Get-EC2HostReservationOffering AWS Tools for Windows PowerShell commande pour répertorier les offres disponibles qui répondent à vos besoins. Les exemples suivants répertorient les offres qui prennent en charge des instances dans la famille d'instances `m4` et ont une durée d'un an.

> **Note**
>
> La durée est indiquée en secondes. Une période d'un an comporte 31 536 000 secondes, tandis qu'une période de trois ans comporte 94 608 000 secondes.

```
PS C:\> $filter = @{Name="instance-family"; Value="m4"}
```

```
PS C:\> Get-EC2HostReservationOffering -filter $filter -MaxDuration 31536000
```

Les deux commandes renvoient une liste d'offres qui correspondent à vos critères de recherche. Notez l'`offeringId` de l'offre à acheter.

2. Utilisez la New-EC2HostReservation AWS Tools for Windows PowerShell commande pour acheter l'offre et fournissez les informations `offeringId` indiquées à l'étape précédente. L'exemple suivant achète la réservation spécifiée et l'associe à un hôte dédié spécifique déjà attribué dans le AWS compte.

```
PS C:\> New-EC2HostReservation -OfferingId hro-03f707bf363b6b324 -
HostIdSet h-013abcd2a00cbd123
```

Partage d'hôtes Amazon EC2 Dedicated Host entre comptes

Le partage d'hôtes dédiés permet aux propriétaires d'hôtes dédiés de partager leurs hôtes dédiés avec d'autres AWS comptes ou au sein d'une AWS organisation. Cela vous permet de créer et de gérer des hôtes dédiés de manière centralisée, et de partager l'hôte dédié entre plusieurs AWS comptes ou au sein de votre AWS organisation.

Dans ce modèle, le AWS compte propriétaire de l'hôte dédié (propriétaire) le partage avec d'autres AWS comptes (consommateurs). Les consommateurs peuvent lancer des instances sur des Hôtes dédiés partagés avec eux comme ils le feraient sur des Hôtes dédiés qu'ils alloueraient dans leur propre compte. Le propriétaire est responsable de la gestion de l'Hôte dédié et des instances lancées sur celui-ci. Les propriétaires ne peuvent pas modifier les instances que les consommateurs lancent sur les Hôtes dédiés partagés. Les consommateurs sont responsables de la gestion des instances qu'ils lancent sur les Hôtes dédiés partagés avec eux. Les consommateurs ne peuvent ni afficher ni modifier les instances détenues par d'autres consommateurs ou par le propriétaire de l'Hôte dédié, et ils ne peuvent pas modifier les Hôtes dédiés qui sont partagés avec eux.

Un propriétaire d'Hôte dédié peut partager un Hôte dédié avec :

- AWS Comptes spécifiques à l'intérieur ou à l'extérieur de son AWS organisation
- Une unité organisationnelle au sein de son AWS organisation

- Toute son AWS organisation

Table des matières

Conditions préalables au partage d'Hôtes dédiés

- Pour partager un hôte dédié, vous devez le posséder dans votre AWS compte. Vous ne pouvez pas partager un hôte dédié qui a été partagé avec vous.
- Pour partager un hôte dédié avec votre AWS organisation ou une unité organisationnelle de votre AWS organisation, vous devez activer le partage avec AWS Organizations. Pour plus d'informations, consultez Activation du partage avec AWS Organizations dans le Guide de l'utilisateur AWS RAM .

Limites pour le partage des Hôte dédiés

Vous ne pouvez pas partager les Hôtes dédiés qui ont été alloués pour les types d'instance suivants : `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` et `u-24tb1.metal`.

Services connexes

AWS Resource Access Manager

Le partage d'hôtes dédiés s'intègre à AWS Resource Access Manager (AWS RAM). AWS RAM est un service qui vous permet de partager vos AWS ressources avec n'importe quel AWS compte

ou via AWS Organizations. Avec AWS RAM, vous partagez les ressources que vous possédez en créant un partage de ressources. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées. Les consommateurs peuvent être AWS des comptes individuels, des unités organisationnelles ou l'ensemble d'une organisation AWS Organizations.

Pour plus d'informations AWS RAM, consultez le guide de AWS RAM l'utilisateur.

Partager sur plusieurs zones de disponibilité

Pour garantir que les ressources sont réparties entre les zones de disponibilité d'une région, nous mappons indépendamment les zones de disponibilité aux noms de chaque compte. Cela peut entraîner des différences de nom de zone de disponibilité entre les comptes. Par exemple, il est possible que la zone `us-east-1a` de disponibilité de votre AWS compte ne soit pas la même que celle `us-east-1a` d'un autre AWS compte.

Pour identifier l'emplacement de vos Hôtes dédiés par rapport à vos comptes, vous devez utiliser l'ID de zone de disponibilité. L'ID de zone de disponibilité est un identifiant unique et cohérent pour une zone de disponibilité sur tous les AWS comptes. Par exemple, `use1-az1` est un ID de zone de disponibilité pour la région `us-east-1`, qui correspond au même emplacement dans chaque compte AWS .

Pour consulter la zone de disponibilité IDs correspondant aux zones de disponibilité de votre compte

1. Ouvrez la AWS RAM console à l'adresse https://console.aws.amazon.com/ram.
2. La zone de disponibilité IDs de la région actuelle est affichée dans le panneau Your AZ ID sur le côté droit de l'écran.

Autorisations relatives à un Hôte dédié partagé

Autorisations accordées aux propriétaires

Les propriétaires sont responsables de la gestion de leurs Hôtes dédiés partagés et des instances qu'ils lancent sur eux. Les propriétaires peuvent afficher toutes les instances s'exécutant sur l'Hôte dédié partagé, y compris celles lancées par les consommateurs. Toutefois, les propriétaires ne peuvent effectuer aucune action sur les instances en cours d'exécution lancées par les consommateurs.

Autorisations accordées aux consommateurs

Les consommateurs sont responsables de la gestion des instances qu'ils lancent sur un Hôte dédié partagé. Les consommateurs ne peuvent en aucun cas modifier l'Hôte dédié partagé. Ils ne peuvent pas non plus afficher ou modifier les instances qui ont été lancées par d'autres consommateurs ou par le propriétaire de l'Hôte dédié.

Facturation et mesures

Le partage d'Hôtes dédiés n'entraîne pas de frais supplémentaires.

Les propriétaires sont facturés pour les Hôtes dédiés qu'ils partagent. Les consommateurs ne sont pas facturés pour les instances qu'ils lancent sur des Hôtes dédiés partagés.

Les réservations d'hôtes dédiés continuent à fournir des remises de facturation pour les Hôtes dédiés partagés. Seuls les propriétaires d'Hôte dédié peuvent acheter des réservations d'hôtes dédiés pour les Hôtes dédiés partagés qu'ils possèdent.

Limites Hôte dédié

Les Hôtes dédiés partagés sont uniquement pris en compte dans les limites d'Hôtes dédiés du propriétaire. Les limites d'Hôtes dédiés du consommateur ne sont pas affectées par les Hôtes dédiés qui ont été partagés avec lui. De même, les instances que les consommateurs lancent sur les Hôtes dédiés partagés ne sont pas pris en compte dans leurs limites d'instance.

Récupération d'hôte et partage d'Hôte dédié

La récupération d'hôte permet de récupérer les instances lancées par le propriétaire d'un Hôte dédié et par les consommateurs avec qui ce dernier a été partagé. L'Hôte dédié de remplacement est alloué au compte du propriétaire. Il est ajouté aux mêmes partages de ressources que l'Hôte dédié d'origine, et il est partagé avec les mêmes consommateurs.

Pour de plus amples informations, veuillez consulter Restauration d'EC2un hôte dédié Amazon.

Partagez un hôte EC2 dédié Amazon sur plusieurs AWS comptes

Lorsqu'un propriétaire partage un Hôte dédié, il permet aux consommateurs de lancer des instances sur l'hôte. Les consommateurs peuvent lancer autant d'instances sur l'hôte partagé que sa capacité disponible le permet.

> **Important**
>
> Notez qu'il vous incombe de vous assurer que vous disposez des droits de licence appropriés pour partager les BYOL licences sur vos hôtes dédiés.

Si vous partagez un Hôte dédié en ayant activé le placement automatique, gardez ce qui suit à l'esprit car cela pourrait conduire à une utilisation involontaire de l'Hôte dédié :

- Si les consommateurs lancent des instances avec location d'Hôte dédié et qu'ils n'ont pas de capacité sur un Hôte dédié qu'ils possèdent dans leur compte, l'instance est automatiquement lancée sur l'Hôte dédié partagé.

Pour partager un Hôte dédié, vous devez l'ajouter à un partage de ressources. Un partage de ressources est une AWS RAM ressource qui vous permet de partager vos ressources entre différents AWS comptes. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées. Vous pouvez ajouter l'Hôte dédié à une ressource existante ou l'ajouter à un nouveau partage de ressources.

Si vous faites partie d'une organisation AWS Organizations et que le partage au sein de votre organisation est activé, les clients de votre organisation ont automatiquement accès à l'hôte dédié partagé. Dans le cas contraire, les consommateurs reçoivent une invitation à rejoindre le partage de ressources et bénéficient d'un accès à l'Hôte dédié partagé après avoir accepté l'invitation.

> **Note**
>
> Après avoir partagé un Hôte dédié, les consommateurs peuvent y avoir accès en quelques minutes.

Vous pouvez partager un Hôte dédié que vous possédez à l'aide de l'une des méthodes suivantes.

Amazon EC2 console

Pour partager un hôte dédié dont vous êtes propriétaire à l'aide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Hôtes dédiés.

3. Choisissez le Hôte dédié à partager, puis choisissez Actions, Partager l'hôte.
4. Sélectionnez le partage de ressources auquel vous souhaitez ajouter le Hôte dédié, puis choisissez Partager l'hôte.

   Les consommateurs peuvent avoir accès à l'hôte partagé en quelques minutes.

AWS RAM console

Pour partager un hôte dédié dont vous êtes propriétaire à l'aide de la AWS RAM console

Consultez Création d'un partage de ressources dans le Guide de l'utilisateur AWS RAM .

AWS CLI

Pour partager un hôte dédié dont vous êtes le propriétaire à l'aide du AWS CLI

Utilisez la create-resource-sharecommande.

Annuler le partage d'un hôte dédié partagé avec d'autres comptes AWS

Le propriétaire d'un Hôte dédié peut annuler le partage d'un Hôte dédié partagé à tout moment. Lorsque vous annulez le partage d'un Hôte dédié partagé, les règles suivantes s'appliquent :

- Les consommateurs avec qui l'Hôte dédié a été partagé ne peuvent plus lancer de nouvelles instances sur celui-ci.
- Les instances appartenant à des consommateurs qui s'exécutaient sur l'Hôte dédié au moment de l'annulation du partage continuent de s'exécuter, mais sont programmées pour être mises hors service. Les consommateurs reçoivent des notifications de mise hors service pour les instances, et disposent de deux semaines pour prendre les mesures nécessaires. Toutefois, si l'Hôte dédié est à nouveau partagé avec le consommateur au cours de la période de préavis de mise hors service, les mises hors service d'instance sont annulées.

Pour annuler le partage d'un Hôte dédié partagé qui vous appartient, vous devez le supprimer du partage de ressources. Pour ce faire, utilisez l'une des méthodes suivantes :

Amazon EC2 console

Pour annuler le partage d'un hôte dédié partagé dont vous êtes propriétaire à l'aide de la console Amazon EC2

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Choisissez le Hôte dédié dont vous voulez annuler le partage et choisissez l'onglet Partage.
4. L'onglet Partage affiche la liste des partages de ressources auxquels le Hôte dédié a été ajouté. Sélectionnez le partage de ressources duquel vous souhaitez supprimer le Hôte dédié, puis choisissez Supprimer l'hôte du partage de ressources.

AWS RAM console

Pour annuler le partage d'un hôte dédié partagé qui vous appartient à l'aide de la console AWS RAM

Consultez Mise à jour d'un partage de ressources dans le Guide de l'utilisateur AWS RAM .

Command line

Pour annuler le partage d'un hôte dédié partagé dont vous êtes le propriétaire à l'aide du AWS CLI

Utilisez la disassociate-resource-sharecommande.

Afficher les hôtes Amazon EC2 Dedicated Hosts partagés sur votre AWS compte

Vous pouvez consulter les hôtes dédiés que vous partagez avec d'autres comptes, ainsi que les hôtes dédiés partagés avec vous. Si vous êtes propriétaire de l'hôte dédié, vous pouvez voir toutes les instances exécutées sur l'hôte, y compris les instances lancées par des clients. Si l'hôte dédié est partagé avec vous, vous ne pouvez voir que les instances que vous avez lancées sur l'hôte partagé, et non celles lancées par d'autres consommateurs.

Les propriétaires et les consommateurs peuvent identifier les Hôtes dédiés partagés à l'aide de l'une des méthodes suivantes.

Amazon EC2 console

Pour identifier un hôte dédié partagé à l'aide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Hôtes dédiés. L'écran affiche la liste des Hôtes dédiés qui vous appartiennent et des Hôtes dédiés qui sont partagés avec vous. La colonne Propriétaire affiche l'ID du compte AWS du propriétaire de l'hôte dédié. Pour afficher les instances exécutées sur les hôtes, sélectionnez l'onglet Instances.

Command line

Pour identifier un hôte dédié partagé à l'aide du AWS CLI

Utilisez la commande describe-hosts. La commande renvoie les Hôtes dédiés qui vous appartiennent et les Hôtes dédiés qui sont partagés avec vous.

Amazon EC2 Dedicated Hosts sur AWS Outposts

AWS Outposts est un service entièrement géré qui étend AWS l'infrastructureAPIs, les services et les outils à vos locaux. En fournissant un accès local à l'infrastructure AWS gérée, vous AWS Outposts pouvez créer et exécuter des applications sur site en utilisant les mêmes interfaces de programmation que dans AWS les régions, tout en utilisant les ressources de calcul et de stockage locales pour réduire la latence et les besoins de traitement des données locaux.

Un avant-poste est un pool de capacités de AWS calcul et de stockage déployé sur le site d'un client. AWS exploite, surveille et gère cette capacité dans le cadre d'une AWS région.

Vous pouvez allouer des hôtes dédiés à des Outposts que vous possédez dans votre compte. Cela vous permet d'apporter plus facilement vos licences logicielles existantes et vos charges de travail nécessitant un serveur physique dédié à AWS Outposts. Vous pouvez également cibler des actifs matériels spécifiques sur un Outpost afin de minimiser la latence entre vos charges de travail.

Les hébergeurs dédiés vous permettent d'utiliser vos licences logicielles éligibles sur AmazonEC2, afin que vous puissiez bénéficier de la flexibilité et de la rentabilité liées à l'utilisation de vos propres licences. D'autres licences logicielles liées à des machines virtuelles, des sockets ou des cœurs physiques peuvent également être utilisées sur des hôtes dédiés, sous réserve de leurs conditions de licence. Bien que les Outposts aient toujours été des environnements à locataire unique éligibles aux

BYOL charges de travail, les hôtes dédiés vous permettent de limiter les licences nécessaires à un seul hôte plutôt qu'à l'ensemble du déploiement d'Outpost.

En outre, l'utilisation d'hôtes dédiés sur un Outpost vous offre une plus grande flexibilité dans le déploiement de type d'instance et un contrôle plus précis du placement des instances. Vous pouvez cibler un hôte spécifique pour les lancements d'instances et utiliser l'affinité de l'hôte pour garantir que l'instance s'exécute toujours sur cet hôte, ou vous pouvez utiliser le placement automatique pour lancer une instance sur n'importe quel hôte disponible disposant de configurations et de capacités disponibles correspondantes.

Table des matières

Prérequis

Vous devez avoir un outpost installé sur votre site. Pour plus d'informations, consultez Créer un outpost et commander une capacité outpost dans le Guide de l'utilisateur AWS Outposts .

Fonctionnalités prises en charge

- Les familles d'instances suivantes sont prises en charge : `C5`, `M5`, `R5`, `C5d`, `M5d`, `R5d`, `G4dn` et `i3en`.
- Les hôtes dédiés sur Outposts peuvent être configurés pour prendre en charge plusieurs tailles d'instance. La prise en charge de plusieurs tailles d'instance est disponible pour les familles d'instances suivantes : `C5`, `M5`, `R5`, `C5d`, `M5d`, et `R5d`. Pour de plus amples informations, veuillez consulter Configurations de capacité des instances Amazon EC2 Dedicated Host.
- Les hôtes dédiés sur Outposts prennent en charge le placement automatique et les lancements d'instances ciblées. Pour de plus amples informations, veuillez consulter Placement automatique et affinité d'hôte Amazon EC2 Dedicated Host.
- Les hôtes dédiés sur Outposts prennent en charge l'affinité de l'hôte. Pour de plus amples informations, veuillez consulter Placement automatique et affinité d'hôte Amazon EC2 Dedicated Host.

- Les hôtes dédiés sur Outposts prennent en charge le partage avec. AWS RAM Pour de plus amples informations, veuillez consulter Partage d'hôtes Amazon EC2 Dedicated Host entre comptes.

Considérations

- Les réservations d'hôtes dédiés ne sont pas prises en charge sur Outposts.
- Hébergez des groupes de ressources AWS License Manager qui ne sont pas pris en charge sur Outposts.
- Les hôtes dédiés sur Outposts ne prennent pas en charge les instances T3 burstable.
- Les hôtes dédiés sur Outposts ne prennent pas en charge la récupération de l'hôte.
- La restauration automatique simplifiée n'est pas prise en charge pour les instances dotées d'une location d'hôte dédié sur Outposts.

Allouez un hôte EC2 dédié Amazon sur AWS Outposts

Vous allouez et utilisez des hôtes dédiés sur des Outposts de la même manière que pour les hôtes dédiés dans une Région AWS .

Prérequis

Créez un sous-réseau sur l'outpost. Pour plus d'informations, consultez Créer un sous-réseau dans le Guide de l'utilisateur AWS Outposts .

Pour allouer un hôte dédié à un Outpost, utilisez l'une des méthodes suivantes :

AWS Outposts console

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Dans le panneau de navigation, choisissez Outposts. Sélectionnez l'Outpost, puis choisissez Actions, Allocate Dedicated Host (Allouer un hôte dédié).
3. Configurez l'hôte dédié selon les besoins. Pour de plus amples informations, veuillez consulter Attribuez un hôte EC2 dédié Amazon à utiliser sur votre compte.

> **Note**
>
> La zone de disponibilité et l'avant-poste ARN doivent être préremplis avec la zone de disponibilité et ARN l'avant-poste sélectionné.

4. Choisissez Allouer.

Amazon EC2 console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Hôtes dédiés, puis Allouer un Hôte dédié.
3. Pour Zone de disponibilité, sélectionnez la zone de disponibilité associée à l'avant-poste.
4. Dans le champ Outpost ARN, saisissez le ARN de l'Outpost.
5. Pour cibler des actifs matériels spécifiques sur l'Outpost, pour Cibler des actifs matériels spécifiques sur l'Outpost, sélectionnez Activer. Pour chaque actif matériel à cibler, sélectionnez Ajouter un identifiant d'actif, puis saisissez l'identifiant d'actif matériel.

> **Note**
>
> La valeur que vous spécifiez pour Quantité doit être égale au nombre d'actifs IDs que vous spécifiez. Par exemple, si vous spécifiez 3 actifsIDs, la quantité doit également être égale à 3.

6. Configurez les paramètres de l'hôte dédié restant selon les besoins. Pour de plus amples informations, veuillez consulter Attribuez un hôte EC2 dédié Amazon à utiliser sur votre compte.
7. Choisissez Allouer.

AWS CLI

Utilisez la commande allocate-hosts AWS CLI . Pour `--availability-zone`, spécifiez la zone de disponibilité associée à l'avant-poste. Pour`--outpost-arn`, spécifiez le ARN de l'avant-poste. Le cas échéant, pour`--asset-ids`, spécifiez les actifs matériels IDs de l'Outpost à cibler.

```
aws ec2 allocate-hosts --availability-zone "us-east-1a" --outpost-arn
 "arn:aws:outposts:us-east-1a:111122223333:outpost/op-4fe3dc21baEXAMPLE" --asset-
ids asset_id --instance-family "m5" --auto-placement "off" --quantity 1
```

Pour lancer une instance dans un Hôte dédié sur un avant-poste

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Hôtes dédiés. Sélectionnez l'hôte dédié que vous avez alloué à l'étape précédente et choisissez Actions, Launch instance onto host (Lancer une instance sur l'hôte).
3. Configurez l'instance selon les besoins, puis lancez l'instance. Pour de plus amples informations, veuillez consulter Lancer EC2 des instances Amazon sur un hôte EC2 dédié Amazon.

Restauration d'EC2un hôte dédié Amazon

La fonction de récupération automatique de l'hôte dédie redémarre vos instances sur un nouvel hôte de remplacement lorsque certaines conditions problématiques sont détectées sur votre hôte dédié. La fonction de récupération de l'hôte permet de réduire les interventions manuelles et de diminuer la charge de travail opérationnelle en cas d'incident inattendu lié à l'alimentation système ou à des événements de connectivité réseau sur un hôte dédié. Les autres problèmes liés à l'hôte dédié nécessiteront une intervention manuelle pour être résolus.

Table des matières

Comment fonctionne Amazon EC2 Dedicated Host

Les hôtes dédiés et la fonction de récupération des groupes de ressource d'hôtes font intervenir des surveillances de l'état au niveau de l'hôte pour évaluer la disponibilité de l'hôte dédié et détecter les

pannes système sous-jacentes. Le type de défaillance de l'hôte dédié détermine si la récupération automatique de l'hôte dédié est possible. Voici quelques exemples de problèmes pouvant entraîner l'échec des vérifications de l'état au niveau de l'hôte :

- Perte de connectivité réseau
- Perte d'alimentation système
- Problèmes logiciels ou matériels sur l'hôte physique

> **Important**
>
> La récupération automatique de l'hôte dédié n'a pas lieu lorsque la mise hors service de l'hôte est prévue.

Récupération automatique de l'hôte dédié

Lorsqu'une panne d'alimentation du système ou de connectivité réseau est détectée sur votre hôte dédié, la restauration automatique de l'hôte dédié est lancée et Amazon alloue EC2 automatiquement un hôte dédié de remplacement dans la même zone de disponibilité que l'hôte dédié d'origine. L'Hôte dédié de remplacement reçoit un nouvel ID d'hôte, mais conserve les mêmes attributs que l'Hôte dédié d'origine, en particulier :

- Zone de disponibilité
- Type d'instance
- Balises
- Paramètres de placement automatique
- Réservation

Une fois l'hôte dédié de remplacement alloué, les instances sont récupérées sur l'hôte dédié de remplacement. Les instances récupérées conservent les mêmes attributs que les instances d'origine, en particulier :

- ID d'instance
- Adresses IP privées
- Adresses IP élastiques
- EBSpièces jointes aux volumes

- Toutes les métadonnées d'instance

En outre, l'intégration intégrée à AWS License Manager automatise le suivi et la gestion de vos licences.

> **Note**
>
> AWS L'intégration de License Manager n'est prise en charge que dans les régions dans lesquelles AWS License Manager est disponible.

Si des instances ont des relations d'affinité avec l'Hôte dédié déficient, les instances récupérées établissent une relation d'affinité avec l'Hôte dédié de remplacement.

Une fois que toutes les instances ont été récupérées sur l'Hôte dédié de remplacement, l'Hôte dédié déficient est libéré et l'Hôte dédié de remplacement devient disponible.

Lorsque la restauration de l'hôte est lancée, le propriétaire du AWS compte est averti par e-mail et par un AWS Health Dashboard événement. Une seconde notification est envoyée une fois la récupération de l'hôte réalisée avec succès.

Si vous utilisez AWS License Manager pour suivre vos licences, AWS License Manager alloue de nouvelles licences à l'hôte dédié de remplacement en fonction des limites de configuration des licences. Si la configuration de la licence comporte des limites strictes qui seront dépassées à la suite de la restauration de l'hôte, le processus de restauration n'est pas autorisé et vous êtes informé de l'échec de la restauration de l'hôte par le biais d'une SNS notification Amazon (si les paramètres de notification ont été configurés pour AWS License Manager). Si la configuration de licence comporte des limites souples qui seront dépassées à la suite de la restauration de l'hôte, la restauration est autorisée à se poursuivre et vous êtes informé du non-respect des limites par le biais d'une SNS notification Amazon. Pour plus d'informations, consultez Configurations de licences dans License Manager et Paramètres dans License Manager dans le Guide de l'utilisateur AWS License Manager.

États de la récupération de l'hôte

Lorsqu'une déficience d'Hôte dédié est détectée, l'Hôte dédié déficient passe à l'état `under-assessment` et toutes les instances passent à l'état `impaired`. Vous ne pouvez pas lancer des instances sur l'Hôte dédié déficient tant qu'il est à l'état `under-assessment`.

Une fois l'Hôte dédié de remplacement alloué, il passe à l'état `pending`. Il reste dans cet état jusqu'à ce que le processus de récupération de l'hôte soit terminé. Vous ne pouvez pas lancer des instances

sur l'Hôte dédié de remplacement tant qu'il est à l'état `pending`. Les instances récupérées situées sur l'Hôte dédié de remplacement restent à l'état `impaired` durant le processus de récupération.

Une fois la récupération de l'hôte terminée, l'Hôte dédié de remplacement passe à l'état `available` et les instances récupérées repassent à l'état `running`. Vous pouvez lancer des instances sur l'Hôte dédié de remplacement une fois qu'il est à l'état `available`. L'Hôte dédié déficient d'origine est libéré de façon permanente et il passe à l'état `released-permanent-failure`.

Si l'Hôte dédié déficient possède des instances qui ne prennent pas en charge la récupération de l'hôte, telles que les instances comportant des volumes basés sur le stockage d'instances, l'Hôte dédié n'est pas libéré. Il est marqué comme devant être mis hors service et passe à l'état `permanent-failure`.

Scénarios sans récupération automatique d'hôte dédié

La récupération automatique de l'hôte dédié n'a pas lieu lorsque la mise hors service de l'hôte est prévue. Vous recevrez une notification de retrait lors d'un CloudWatch événement Amazon AWS Health Dashboard, et l'adresse e-mail du propriétaire du AWS compte recevra un message concernant la défaillance de l'hôte dédié. Suivez les étapes correctives décrites dans la notification de mise hors service dans le temps imparti pour récupérer manuellement les instances sur l'hôte qui est mis hors service.

Les instances arrêtées ne sont pas récupérées sur l'Hôte dédié de remplacement. Si vous tentez de démarrer une instance arrêtée qui cible l'Hôte dédié déficient, son démarrage échoue. Nous vous recommandons de modifier l'instance arrêtée afin qu'elle cible un autre Hôte dédié ou de la lancer sur tout Hôte dédié disponible ayant des caractéristiques de configuration et de remplacement automatique correspondantes.

Les instances avec stockage d'instance ne sont pas récupérées sur l'Hôte dédié de remplacement. Afin de remédier à ce problème, l'Hôte dédié déficient est marqué comme devant être mis hors service et vous recevez une notification de mise hors service une fois la récupération de l'hôte terminée. Suivez les étapes correctives décrites dans la notification de mise hors service dans le temps imparti pour récupérer manuellement les instances restantes sur l'Hôte dédié déficient.

Types d'instance pris en charge

La restauration de l'hôte est prise en charge pour les familles d'instances suivantes : A1, C3, C4, C5, C5n, C6a, C6g, C6i, Inf1, G3, G5g, M3, M4, M5, M5n, M5zn, M6a, M6g, M6i, P2, P3, R3, R4, R5, R5b, R5n, R6g, R6i, T3, X1, X1e, X2iezn, u-6tb1, u-9tb1, u-12tb1, u-18tb1 et u-24tb1.

Pour récupérer des instances qui ne sont pas prises en charge, consultez Restaurez manuellement les instances qui ne sont pas prises en charge par Amazon EC2 Dedicated Host Recovery.

> **Note**
>
> La récupération automatique de l'hôte dédié pour les types d'instance métalliques pris en charge prendra plus de temps à détecter et à récupérer que pour les types d'instance non métalliques.

Tarification

Il n'y a pas de facturation supplémentaire pour l'utilisation de la fonction de récupération de l'hôte, mais les frais habituellement appliqués pour l'Hôte dédié vous seront facturés. Pour plus d'informations, consultez les tarifs d'Amazon EC2 Dedicated Hosts.

Dès que la fonction de récupération de l'hôte est lancée, vous n'êtes plus facturé pour l'Hôte dédié déficient. La facturation relative à l'hôte dédié de remplacement commence uniquement une fois qu'il est passé à l'état `available`.

Si l'Hôte dédié déficient était facturé au tarif à la demande, l'Hôte dédié de remplacement est également facturé au tarif à la demande. Si l'Hôte dédié déficient possédait une Réservation d'hôtes dédiés, elle est transférée à l'Hôte dédié de remplacement.

Gérez la restauration d'Amazon EC2 Dedicated Host

La fonction de récupération automatique de l'hôte dédie redémarre vos instances sur un nouvel hôte de remplacement lorsque certaines conditions problématiques sont détectées sur votre hôte dédié. Vous pouvez activer la restauration de l'hôte lorsque vous allouez l'hôte dédié ou après l'allocation.

Utilisez les procédures suivantes pour activer la restauration de l'hôte lors de l'allocation de l'hôte.

Console

Pour activer la restauration de l'hôte lors de l'allocation

Lorsque vous allouez un hôte dédié à l'aide de la EC2 console Amazon, pour la restauration de l'hôte, choisissez Enable. Pour de plus amples informations, veuillez consulter Attribuez un hôte EC2 dédié Amazon à utiliser sur votre compte.

AWS CLI

Pour activer la restauration de l'hôte lors de l'allocation

Utilisez la commande allocate-hosts et spécifiez le paramètre. `host-recovery`

```
$ aws ec2 allocate-hosts \
    --instance-type m5.large \
    --availability-zone eu-west-1a \
    --auto-placement on \
    --host-recovery on \
    --quantity 1
```

Utilisez les procédures suivantes pour gérer la restauration d'un hôte dédié.

Console

Pour gérer la restauration de l'hôte après l'allocation

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Sélectionnez l'hôte dédié.
4. Choisissez Actions, Modifier l'hôte.
5. Pour la restauration de l'hôte, sélectionnez ou décochez Activer.
6. Choisissez Save (Enregistrer).

AWS CLI

Pour activer la restauration de l'hôte après allocation

Utilisez la commande modify-hosts et spécifiez le `host-recovery` paramètre avec une valeur de. `on`

```
$ aws ec2 modify-hosts --host-recovery on --host-ids h-012a3456b7890cdef
```

Pour désactiver la restauration de l'hôte après l'allocation

Utilisez la commande modify-hosts et spécifiez le `host-recovery` paramètre avec une valeur de. `off`

```
$ aws ec2 modify-hosts --host-recovery off --host-ids h-012a3456b7890cdef
```

Afficher le paramètre de restauration de l'hôte pour votre hôte Amazon EC2 Dedicated Host

Vous pouvez afficher la configuration de récupération de l'hôte d'un Hôte dédié à tout moment.

Pour afficher la configuration de récupération de l'hôte d'un Hôte dédié à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Sélectionnez l'Hôte dédié, puis, dans l'onglet Description, passez en revue le champ Host Recovery (Récupération de l'hôte).

Pour afficher la configuration de récupération de l'hôte d'un hôte dédié à l'aide de la AWS CLI

Utilisez la commande describe-hosts.

```
$ aws ec2 describe-hosts --host-ids h-012a3456b7890cdef
```

L'élément de réponse `HostRecovery` indique si la récupération de l'hôte est activée ou désactivée.

Restaurez manuellement les instances qui ne sont pas prises en charge par Amazon EC2 Dedicated Host Recovery

La fonction de récupération de l'hôte ne prend pas en charge la récupération des instances qui utilisent des volumes de stockage d'instances. Suivez les instructions ci-après pour récupérer manuellement les instances qui n'ont pas pu être récupérées automatiquement.

> **Warning**
>
> Les données stockées sur des volumes de stockage d'instances sont perdues lorsqu'une instance est arrêtée, mise en veille prolongée ou résiliée. Cela inclut les volumes de stockage d'instance attachés à une instance dont le périphérique racine est un EBS volume. Pour protéger les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent avant l'arrêt ou la résiliation de l'instance.

Restaurez manuellement les EBS instances sauvegardées

Pour les instances EBS sauvegardées qui n'ont pas pu être restaurées automatiquement, nous vous recommandons d'arrêter et de démarrer manuellement les instances afin de les récupérer sur un nouvel hôte dédié. Pour plus d'informations sur l'arrêt de votre instance, ainsi que sur les changements apportés à la configuration de votre instance lorsque celle-ci est arrêtée, consultez Arrêtez et démarrez les EC2 instances Amazon.

Récupérer manuellement les instances basées sur le stockage d'instances

Pour les instances basées sur le stockage d'instances qui n'ont pas pu être récupérées automatiquement, nous vous recommandons de procéder comme suit :

1. Lancez une instance de remplacement sur un nouvel hôte dédié à partir de votre dernière instanceAMI.
2. Migrez toutes les données nécessaires vers l'instance de remplacement.
3. Résiliez l'instance d'origine sur l'Hôte dédié déficient.

Maintenance de l'hôte pour Amazon EC2 Dedicated Host

Dans le cadre de la maintenance de l'hôte, vos EC2 instances Amazon sur l'hôte dédié dégradé sont automatiquement redémarrées sur un hôte dédié de remplacement lors d'un événement de maintenance planifié. Cela permet de réduire les temps d'arrêt des applications et de déléguer à AWS la lourdeur indifférenciée de la maintenance. La maintenance de l'hôte est également effectuée pour la EC2 maintenance planifiée et de routine d'Amazon.

La maintenance de l'hôte est prise en charge sur toutes les nouvelles allocations d'hôtes dédiés effectuées via EC2 la console Amazon. Vous pouvez configurer la maintenance de l'hôte pour les hôtes dédiés pris en charge pour tout hôte dédié de votre choix Compte AWS ou pour tout nouvel hôte dédié attribué par votre intermédiaire AllocateHostsAPI. Pour de plus amples informations, veuillez consulter the section called "Configuration de la maintenance de l'hôte".

Table des matières

- Comment fonctionne la maintenance des hôtes Amazon EC2 Dedicated Hosts
- Configurer le paramètre de maintenance de l'hôte pour un hôte Amazon EC2 Dedicated Host

Maintenance d'hôte versus récupération d'hôte

Le tableau suivant présente les principales différences entre la récupération d'hôte et la maintenance d'hôte.

	Resturation de l'hôte	Maintenance de l'hôte
Accessibilité	Injoignable	Joignable
État	`under-assessment`	`permanent-failure`
Action	La récupération est immédiate	La maintenance est planifiée
Flexibilité de la planification	Ne peut être planifié à nouveau	Peut être planifié à nouveau
Groupe de ressources hôte	Pris en charge	Non pris en charge

Pour plus d'informations sur la restauration de l'hôte, consultez Restauration de l'hôte.

Types d'instance pris en charge

La maintenance de l'hôte est prise en charge pour les familles d'instances suivantes :

- Usage général : `A1` | `M4` | `M5` | `M5a` | `M5n` | `M5zn` | `M6a` | `M6g` | `M6i` | `M6in` | `M7a` | `M7g` | `M7i` | `T3`
- Calcul optimisé : `C4` | `C5` | `C5a` | `C5n` | `C6a` | `C6g` | `C6gn` | `C6i` | `C6in` | `C7g` | `C7gn` | `C7i`
- Mémoire optimisée : `R4` | `R5` | `R5a` | `R5b` | `R5n` | `R6a` | `R6g` | `R6i` | `R6in` | `R7a` | `R7g` | `R7iz` | `u-12tb1` | `u-18tb1` | `u-24tb1` | `u-3tb1` | `u-6tb1` | `u-9tb1` | `X2iezn`
- Calcul accéléré: `G3` | `G5g` | `Inf1` | `P2` | `P3`

Limites

- La maintenance de l'hôte n'est pas prise en charge dans AWS Outposts les zones AWS Local et les zones AWS Wavelength.

- La maintenance des hôtes ne peut pas être activée ou désactivée pour les hôtes déjà présents dans un groupe de ressources hôte. Les hôtes ajoutés à un groupe de ressources hôte conservent leur paramètre de maintenance d'hôte. Pour plus d'informations, consultez Groupes de ressources hôte.
- La maintenance d'hôte n'est prise en charge que sur des types d'instance spécifiques. Pour de plus amples informations, veuillez consulter the section called "Types d'instance pris en charge".

Services connexes

Dedicated Host s'intègre à AWS License Manager : suit les licences sur vos Amazon EC2 Dedicated Hosts (pris en charge uniquement dans les régions dans lesquelles AWS License Manager est disponible). Pour plus d'informations, consultez le Guide de l'utilisateur AWS License Manager.

Vous devez disposer de suffisamment de licences Compte AWS pour votre nouvel hôte dédié. Les licences associées à votre hôte dégradé sont libérées lorsque l'hôte est libéré après la fin de l'événement de maintenance planifié.

Tarification

Il n'y a pas de facturation supplémentaire pour l'utilisation de la fonction de maintenance de l'hôte, mais les frais habituellement appliqués pour l'Hôte dédié vous seront facturés. Pour plus d'informations, consultez les tarifs d'Amazon EC2 Dedicated Hosts.

Dès que la fonction de maintenance de l'hôte est lancée, vous n'êtes plus facturé pour l'Hôte dédié dégradé. La facturation relative à l'hôte dédié de remplacement commence uniquement une fois qu'il est passé à l'état `available`.

Si l'hôte dédié dégradé a été facturé au tarif à la demande, l'hôte dédié de remplacement est également facturé au tarif à la demande. Si l'hôte dédié dégradé avait une réservation d'hôte dédié active, celle-ci est transférée au nouvel hôte dédié.

Comment fonctionne la maintenance des hôtes Amazon EC2 Dedicated Hosts

Lorsqu'une dégradation est détectée sur un hôte dédié, un nouvel hôte dédié est alloué. La dégradation peut être causée par la dégradation du matériel sous-jacent ou par la détection de certaines conditions problématiques. Vos instances sur l'hôte dédié dégradé sont programmées pour être automatiquement redémarrées sur l'hôte dédié de remplacement.

L'hôte dédié de remplacement reçoit un nouvel ID d'hôte, mais conserve les mêmes attributs que l'hôte dédié d'origine. Ces attributs sont les suivants.

- Paramètres de placement automatique
- Zone de disponibilité
- Réservation
- Affinité de l'hôte
- Paramètres de maintenance de l'hôte
- Paramètres de récupération de l'hôte
- Type d'instance
- Balises

La maintenance de l'hôte est disponible dans tous les Régions AWS cas pour tous les hôtes dédiés pris en charge. Pour plus d'informations sur les hôtes dédiés pour lesquels la maintenance de l'hôte n'est pas prise en charge, consultez the section called "Limites".

Votre hôte dédié dégradé est libéré une fois que toutes vos instances ont été redémarrées sur un nouvel hôte dédié ou arrêtées. Vous pouvez accéder à vos instances sur l'hôte dédié dégradé avant l'événement de maintenance programmé, mais le lancement d'instances sur l'hôte dédié dégradé n'est pas pris en charge.

Vous pouvez utiliser l'hôte dédié de remplacement pour lancer de nouvelles instances sur l'hôte avant l'événement de maintenance planifié. Toutefois, une partie de la capacité d'instance de l'hôte de remplacement est réservée aux instances qui doivent être migrées depuis l'hôte dégradé. Vous ne pouvez pas lancer de nouvelles instances dans cette capacité réservée. Pour de plus amples informations, veuillez consulter the section called "Instances sur hôte dédié".

Instances sur hôte dédié

Amazon réserve EC2 automatiquement de la capacité sur l'hôte de remplacement pour les instances qui seront automatiquement migrées depuis l'hôte dégradé. Amazon EC2 ne réserve pas de capacité sur l'hôte de remplacement pour les instances qui ne peuvent pas être migrées automatiquement, telles que les instances avec des volumes racine de stockage d'instance. La capacité réservée ne peut pas être utilisée pour lancer de nouvelles instances.

> **Note**
>
> La EC2 console Amazon indique la capacité réservée en tant que capacité utilisée. Il peut sembler que les instances s'exécutent à la fois sur l'hôte dégradé et sur l'hôte de

remplacement. Toutefois, les instances continueront de fonctionner uniquement sur l'hôte dégradé jusqu'à ce qu'elles soient arrêtées ou qu'elles soient migrées vers la capacité réservée sur l'hôte de remplacement.

Si vous arrêtez manuellement une instance sur l'hôte dégradé qui peut être migrée automatiquement, la capacité réservée à cette instance sur l'hôte de remplacement est libérée et peut être utilisée.

Au cours de l'événement de maintenance planifié, les instances de l'hôte dégradé sont redémarrées et migrées vers la capacité réservée sur l'hôte dédié de remplacement. Les instances migrées conservent les mêmes attributs que ceux de votre hôte dégradé, notamment les suivants.

- Pièces jointes au EBS volume Amazon
- Adresses IP Elastic
- ID d'instance
- Métadonnées de l'instance
- Adresse IP privée

Vous pouvez arrêter et démarrer une instance sur l'hôte dégradé à tout moment avant le début de l'événement de maintenance planifiée. Ce faisant, vous redémarrez votre instance sur un autre hôte, et votre instance ne subira pas la maintenance planifiée. Vous devez mettre à jour l'affinité d'hôte de votre instance avec le nouvel hôte sur lequel vous voulez redémarrer votre instance. Si vous arrêtez toutes les instances de l'hôte dégradé avant le lancement de l'événement de maintenance, l'hôte dégradé est libéré et l'événement de maintenance est annulé. Pour de plus amples informations, veuillez consulter Arrêtez et démarrez les EC2 instances Amazon.

Note

Les données d'un volume de stockage d'instances ne sont pas conservées lorsque vous arrêtez et démarrez votre instance.

Les instances dont le périphérique racine est un volume de stockage d'instances sont résiliées après la date de résiliation spécifiée. Toutes les données des volumes de stockage d'instances sont supprimées lorsque les instances sont résiliées. Les instances résiliées sont définitivement supprimées et ne peuvent pas être redémarrées. Pour les instances dont les volumes de stockage

d'instances sont le périphérique racine, nous vous recommandons de lancer des instances de remplacement sur un hôte dédié différent en utilisant l'Amazon Machine Image la plus récente, et de migrer toutes les données disponibles vers les instances de remplacement avant la date de résiliation spécifiée. Pour plus d'informations, voir Mesures à prendre, par exemple, le départ à la retraite.

Les instances qui ne peuvent pas être redémarrées automatiquement sont arrêtées après la date spécifiée. Vous pouvez redémarrer ces instances sur un autre hôte. Les instances utilisant un EBS volume Amazon comme périphérique racine continuent d'utiliser le même EBS volume Amazon après avoir été démarrées sur un nouvel hôte.

Vous pouvez définir l'ordre du redémarrage de l'instance en reprogrammant l'heure de début du redémarrage d'une instance dans. https://console.aws.amazon.com/ec2/

Événement de maintenance

En cas de détection d'une dégradation, un événement de maintenance est planifié 14 jours plus tard, afin de redémarrer vos instances sur un nouvel hôte dédié. Vous recevez une notification par e-mail fournissant des informations sur l'hôte endommagé, l'événement de maintenance planifié et les plages horaires de maintenance. Pour plus d'informations, consultez Affichage des événements planifiés.

Vous pouvez replanifier l'événement de maintenance pour n'importe quel jour jusqu'à sept jours après la date de l'événement planifié. Pour plus d'informations sur la replanification, consultez Replanification d'un événement planifié.

L'événement de maintenance dure généralement quelques minutes. Dans les rares cas d'échec, vous recevez une notification par e-mail vous demandant d'expulser les instances de l'hôte endommagé dans un délai spécifié.

États de la maintenance de l'hôte

Votre hôte dédié est configuré sur l'état `permanent-failure` lorsqu'une dégradation est détectée. Vous ne pouvez pas lancer d'instances sur un hôte dédié dont l'état est `permanent-failure`. À la fin de l'événement de maintenance, l'hôte dégradé est libéré et placé dans l'état `released, permanent-failure`.

Après avoir détecté une dégradation sur un hôte dédié et avant de planifier un événement de maintenance, le service de maintenance de l'hôte alloue automatiquement un hôte dédié de remplacement sur votre compte. Cet hôte de remplacement reste en `pending` état jusqu'à ce qu'un

événement de maintenance soit planifié. Une fois l'événement de maintenance planifié, l'hôte dédié de remplacement passe à l'`available`état.

Vous pouvez utiliser l'hôte dédié de remplacement pour lancer de nouvelles instances sur l'hôte avant l'événement de maintenance planifié. Toutefois, une partie de la capacité d'instance de l'hôte de remplacement est réservée aux instances qui doivent être migrées depuis l'hôte dégradé. Vous ne pouvez pas lancer de nouvelles instances dans cette capacité réservée. Pour de plus amples informations, veuillez consulter the section called “Instances sur hôte dédié”.

Configurer le paramètre de maintenance de l'hôte pour un hôte Amazon EC2 Dedicated Host

Vous pouvez configurer la maintenance de l'hôte pour tous les hôtes dédiés pris en charge via AWS Management Console ou AWS CLI. Consultez le tableau suivant pour plus de détails.

AWS Management Console

Pour activer la maintenance de l'hôte pour votre hôte dédié à l'aide de AWS Management Console.

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Sélectionnez l'hôte dédié > Actions > Modifier l'hôte.
4. Sélectionnez Activé dans le champ Maintenance de l'hôte.

Pour désactiver la maintenance de l'hôte pour votre hôte dédié en utilisant la AWS Management Console.

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Sélectionnez l'hôte dédié > Actions > Modifier l'hôte.
4. Sélectionnez Désactivé dans le champ Maintenance de l'hôte.

Pour afficher la configuration de maintenance de l'hôte d'un hôte dédié à l'aide de la AWS Management Console.

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Hôtes dédiés.

3. Sélectionnez l'Hôte dédié, puis, dans l'onglet Description, passez en revue le champ Maintenance de l'hôte.

AWS CLI

Pour activer ou désactiver la maintenance de l'hôte pour votre nouvel hôte dédié pendant l'allocation en utilisant l' AWS CLI.

Utilisez la commande allocate-hosts.

Activer

```
aws ec2 allocate-hosts --region us-east-1 --quantity 1 --instance-type m3.large --
availability-zone us-east-1b --host-maintenance on
```

Désactiver

```
aws ec2 allocate-hosts --region us-east-1 --quantity 1 --instance-type m3.large --
availability-zone us-east-1b --host-maintenance off
```

Pour activer ou désactiver la maintenance de l'hôte pour votre hôte dédié existant en utilisant l' AWS CLI.

Utilisez la commande modify-hosts.

Activer

```
aws ec2 modify-hosts --region us-east-1 --host-maintenance on --host-
ids h-0d123456bbf78910d
```

Désactiver

```
aws ec2 modify-hosts --region us-east-1 --host-maintenance off --host-
ids h-0d123456bbf78910d
```

Pour afficher la configuration de maintenance de l'hôte d'un hôte dédié à l'aide de la AWS CLI.

Utilisez la commande describe-hosts.

```
aws ec2 describe-hosts --region us-east-1 --host-ids h-0d123456bbf78910d
```

> **Note**
>
> Si vous désactivez la maintenance de l'hôte, vous recevez une notification par e-mail vous demandant d'expulser l'hôte endommagé et de migrer manuellement vos instances vers un autre hôte dans les 28 jours. Un hôte de remplacement est attribué si vous avez réservé un hôte dédié. Après 28 jours, les instances exécutées sur l'hôte dégradé sont résiliées et l'hôte est libéré automatiquement.

Surveillez l'état de vos hôtes Amazon EC2 Dedicated

Amazon surveille EC2 en permanence l'état de vos hôtes dédiés. Les mises à jour sont communiquées sur la EC2 console Amazon. Vous pouvez afficher des informations sur un Hôte dédié à l'aide des méthodes suivantes.

Console

Pour afficher l'état d'un Hôte dédié

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Recherchez l'Hôte dédié dans la liste et consultez la valeur située dans la colonne État.

AWS CLI

Pour afficher l'état d'un Hôte dédié

Utilisez la AWS CLI commande describe-hosts, puis examinez la `state` propriété dans l'élément de `hostSet` réponse.

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

PowerShell

Pour afficher l'état d'un Hôte dédié

Utilisez la Get-EC2Host AWS Tools for Windows PowerShell commande, puis passez en revue la `state` propriété dans l'élément de `hostSet` réponse.

```
PS C:\> Get-EC2Host -HostId h-012a3456b7890cdef
```

Le tableau suivant explique les états possibles pour l'Hôte dédié.

État	Description
`available`	AWS n'a détecté aucun problème avec l'hôte dédié. Aucune maintenan ce ni réparation n'est programmée. Les instances peuvent être lancées sur cet hôte dédié.
`released`	L'Hôte dédié a été libéré. l'ID de l'hôte n'est plus utilisé. Les hôtes libérés ne peuvent pas être réutilisés.
`under-ass essment`	AWS explore un éventuel problème avec l'hôte dédié. Si des mesures doivent être prises, vous en êtes informé par e-mail. AWS Management Console Aucune instance ne peut être lancée sur un Hôte dédié dans cet état.
`pending`	L'Hôte dédié ne peut pas être utilisé le lancement de nouvelles instances . Soit il est en cours de modification afin de prendre en charge plusieurs types d'instances, soit une récupération d'hôte est en cours.
`permanent- failure`	Une défaillance irrécupérable a été détectée. Vous recevez une notice d'expulsion par l'intermédiaire de vos instances et par e-mail. Vos instances peuvent continuer à s'exécuter. Si vous arrêtez ou mettez fin à toutes les instances d'un hôte dédié présentant cet état, l'hôte AWS est retiré. AWS ne redémarre pas les instances dans cet état. Aucune instance ne peut être lancée sur un Hôtes dédiés dans cet état.
`released- permanent- failure`	AWS libère définitivement les hôtes dédiés en panne et sur lesquels aucune instance n'est en cours d'exécution. L'ID de l'Hôte dédié ne peut plus être utilisé.

Suivez les modifications de configuration d'Amazon EC2 Dedicated Host à l'aide de AWS Config

Vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration pour les hôtes dédiés et pour les instances lancées, arrêtées ou résiliées sur ces hôtes. Vous pouvez utiliser les informations capturées par AWS Config comme source de données pour les rapports d'utilisation des licences.

AWS Config enregistre les informations de configuration pour les hôtes dédiés et les instances individuellement, et associe ces informations par le biais de relations. Il y a trois conditions pour la création de rapports :

- AWS Config état de l'enregistrement : lorsque cette option AWS Config est activée, elle enregistre un ou plusieurs types de AWS ressources, notamment des hôtes dédiés et des instances dédiées. Pour capturer les informations requises pour les rapports d'utilisation des licences, vérifiez que les hôtes et les instances sont enregistrés avec les champs suivants.
- Statut de l'enregistrement de l'hôte — Lorsque ce paramètre a la valeur Activé, les informations de configuration concernant les Hôtes dédiés sont enregistrées.
- Statut de l'enregistrement de l'instance : lorsque ce paramètre est défini sur Activé, les informations de configuration concernant les Instances dédiées sont enregistrées.

Si l'une de ces trois conditions est désactivée, l'icône du bouton Edit Config Recording est rouge. Afin de tirer pleinement profit de cet outil, assurez-vous que les trois méthodes d'enregistrement soient activées. Lorsqu'elles sont toutes les trois activées, l'icône est verte. Pour modifier les paramètres, choisissez Edit Config Recording. Vous êtes dirigé vers la AWS Config page de configuration de la AWS Config console, où vous pouvez configurer AWS Config et démarrer l'enregistrement pour vos hôtes, instances et autres types de ressources pris en charge. Pour plus d'informations, consultez la section Configuration à AWS Config l'aide de la console dans le guide du AWS Config développeur.

> **Note**
>
> AWS Config enregistre vos ressources après les avoir découvertes, ce qui peut prendre plusieurs minutes.

Après avoir AWS Config commencé à enregistrer les modifications de configuration de vos hôtes et instances, vous pouvez obtenir l'historique de configuration de tout hôte que vous avez alloué ou

publié et de toute instance que vous avez lancée, arrêtée ou arrêtée. Par exemple, à tout moment dans l'historique de configuration d'un Hôte dédié, vous pouvez rechercher combien d'instances sont lancées sur cet hôte, ainsi que le nombre de sockets et de cœurs sur l'hôte. Pour chacune de ces instances, vous pouvez également rechercher l'ID de son Amazon Machine Image (AMI). Vous pouvez utiliser ces informations pour les rapports de licences portant sur vos propres licences logicielles liées au serveur par socket ou par cœur.

Vous pouvez accéder aux historiques de configuration de l'une des façons suivantes :

- À l'aide de la AWS Config console. Pour chaque ressource enregistrée, vous pouvez visualiser une page chronologique fournissant une historique des détails de configuration. Pour visualiser cette page, choisissez l'icône grise dans la colonne Chronologie de configuration de la page Hôtes dédiés. Pour plus d'informations, consultez la section Affichage des détails de configuration dans la AWS Config console dans le guide du AWS Config développeur.
- En exécutant AWS CLI des commandes. Tout d'abord, vous pouvez utiliser la list-discovered-resourcescommande pour obtenir une liste de tous les hôtes et instances. Vous pouvez ensuite utiliser la get-resource-config-historycommande pour obtenir les détails de configuration d'un hôte ou d'une instance pour un intervalle de temps spécifique. Pour plus d'informations, voir Afficher les détails de configuration CLI à l'aide du manuel du AWS Config développeur.
- En utilisant le AWS Config API dans vos applications. Tout d'abord, vous pouvez utiliser l'ListDiscoveredResourcesaction pour obtenir une liste de tous les hôtes et instances. Vous pouvez ensuite utiliser l'GetResourceConfigHistoryaction pour obtenir les détails de configuration d'un hôte ou d'une instance pour un intervalle de temps spécifique.

Par exemple, pour obtenir la liste de tous vos hôtes dédiés AWS Config, exécutez une CLI commande telle que la suivante.

```
aws configservice list-discovered-resources --resource-type AWS::EC2::Host
```

Pour obtenir l'historique de configuration d'un hôte dédié auprès de AWS Config, exécutez une CLI commande telle que la suivante.

```
aws configservice get-resource-config-history --resource-type AWS::EC2::Instance --
resource-id i-1234567890abcdef0
```

Pour gérer les AWS Config paramètres à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Sur la page Hôtes dédiés, sélectionnez Modifier l'enregistrement de la configuration.
3. Dans la AWS Config console, suivez les étapes indiquées pour activer l'enregistrement. Pour plus d'informations, consultez la section Configuration à AWS Config l'aide de la console.

Pour plus d'informations, consultez la section Affichage des détails de configuration dans la AWS Config console.

Pour l'activer à AWS Config l'aide de la ligne de commande ou API

- AWS CLI: affichage des détails de configuration (AWS CLI) dans le guide du AWS Config développeur.
- Amazon EC2 API : GetResourceConfigHistory.

Instances EC2 dédiées Amazon

Par défaut, les EC2 instances s'exécutent sur du matériel à location partagée. Cela signifie que plusieurs AWS comptes peuvent partager le même matériel physique.

Les instances dédiées sont EC2 des instances qui s'exécutent sur du matériel dédié à un seul AWS compte. Cela signifie que les instances dédiées sont physiquement isolées au niveau du matériel hôte des instances appartenant à d'autres instances Comptes AWS, même si ces comptes sont liés à un compte payeur unique. Toutefois, les instances dédiées peuvent partager du matériel avec d'autres instances de la même instance Compte AWS qui ne sont pas des instances dédiées.

Les instances dédiées n'offrent aucune visibilité ni aucun contrôle sur le placement des instances, et elles ne prennent pas en charge l'affinité avec l'hôte. Si vous arrêtez et démarrez une instance dédiée, elle risque de ne pas s'exécuter sur le même hôte. De même, vous ne pouvez pas cibler un hôte spécifique sur lequel lancer ou exécuter une instance. En outre, les instances dédiées fournissent un support limité pour Bring Your Own License (BYOL).

Si vous avez besoin de visibilité et de contrôle sur le placement des instances et d'un BYOL support plus complet, pensez plutôt à utiliser un hôte dédié. Les instances dédiées et les hôtes dédiés peuvent tous deux être utilisés pour lancer EC2 des instances Amazon sur des serveurs physiques dédiés. Il n'existe pas de différence physique, de sécurité ou de performance entre les instances

dédiées et les instances des Hôtes dédiés. Cependant, il existe des différences majeures entre eux. Le tableau suivant met en valeur quelques-unes des principales différences entre les Hôtes dédiés et les instances dédiées :

	Dedicated Host	Dedicated Instance
Serveur physique dédié	Serveur physique avec une capacité d'instance entièrement dédiée à votre utilisation.	Serveur physique dédié à un seul compte client.
Partage de capacité d'instance	Peut partager la capacité de l'instance avec d'autres comptes.	Non pris en charge
Facturation	Facturation par hôte	Facturation par instance
Visibilité des sockets, cœurs et ID d'hôte	Offre une visibilité sur le nombre de sockets et de cœurs physiques	Aucune visibilité
Affinité de l'hôte et de l'instance	Permet de déployer vos instances de façon cohérente sur le même serveur physique au fil du temps	Non pris en charge
Placement ciblé d'instances	Offre une visibilité supplémentaire et un contrôle sur la façon dont les instances sont placées sur un serveur physique	Non pris en charge
Récupération automatique des instances	Pris en charge. Pour plus d'informations, consultez Restauration d'EC2un hôte dédié Amazon.	Pris en charge
Apportez votre propre licence (BYOL)	Pris en charge	Support partiel*

	Dedicated Host	Dedicated Instance
Réserve de capacité	Non pris en charge	Pris en charge

* Les licences Microsoft SQL Server with License Mobility through Software Assurance et Windows Virtual Desktop Access (VDA) peuvent être utilisées avec une instance dédiée.

Pour plus d'informations sur les instances dédiées, veuillez consulter la rubrique Hôtes EC2 dédiés Amazon.

Rubriques

- Principes de base de Instance dédiée
- Fonctionnalités prises en charge
- Limites de instances dédiées
- Tarification des instances dédiées
- Lancer des instances dédiées dans un environnement VPC avec location par défaut
- Modifier la location d'une instance Amazon EC2
- Modifier la location d'instance d'un VPC

Principes de base de Instance dédiée

A VPC peut avoir une location de l'un `default` ou `dedicated` de l'autre. Par défaut, vous VPCs avez une `default` location et les instances lancées dans une `default` location VPC ont `default` une location. Pour lancer des instances dédiées, procédez comme suit :

- Créez un VPC avec une location de`dedicated`, afin que toutes les instances s'VPCexécutent en tant qu'instances dédiées. Pour de plus amples informations, veuillez consulter Lancer des instances dédiées dans un environnement VPC avec location par défaut.
- Créez un VPC avec une location de `default` et spécifiez manuellement une location de `dedicated` pour que les instances s'exécutent en tant qu'instances dédiées. Pour de plus amples informations, veuillez consulter Lancer des instances dédiées dans un environnement VPC avec location par défaut.

Fonctionnalités prises en charge

Les instances dédiées prennent en charge les fonctionnalités et intégrations AWS de services suivantes :

Rubriques

- Instances réservées
- Dimensionnement automatique
- Récupération automatique
- instances Spot dédiées
- Instances de performance à capacité extensible

Instances réservées

Pour réserver de la capacité pour vos instances dédiées, vous pouvez acheter des instances réservées dédiées ou des réservations de capacité. Pour plus d'informations, consultez EC2Présentation des instances réservées pour Amazon et Réservez de la capacité de calcul grâce aux réservations de capacité à la demande.

Lorsque vous achetez une instance réservée dédiée, vous achetez la capacité de lancer une instance dédiée vers une instance dédiée VPC à un prix d'utilisation très réduit ; la réduction des frais d'utilisation ne s'applique que si vous lancez une instance avec une location dédiée. Lorsque vous achetez une Instance réservée avec une location par défaut, celle-ci s'applique uniquement à une instance en cours d'exécution dotée d'un location `default`. Elle ne s'appliquerait pas à une instance en cours d'exécution dotée d'une location `dedicated`.

Vous ne pouvez pas utiliser le processus de modification pour modifier la location d'une Instance réservée après l'avoir achetée. Par contre, vous pouvez échanger une Instance réservée convertible contre une nouvelle Instance réservée convertible avec une autre location.

Dimensionnement automatique

Vous pouvez utiliser Amazon EC2 Auto Scaling pour lancer des instances dédiées. Pour plus d'informations, consultez Launching Auto Scaling Instances in a VPC dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.

Récupération automatique

Vous pouvez configurer la restauration automatique pour une instance dédiée si celle-ci est altérée en raison d'une défaillance matérielle sous-jacente ou d'un problème nécessitant une AWS intervention pour être réparé. Pour de plus amples informations, veuillez consulter Résilience des instances.

instances Spot dédiées

Vous pouvez exécuter une instance Spot dédiée en spécifiant une location `dedicated` lorsque vous créez une demande d'instance Spot. Pour plus d'informations, consultez Lancement sur du matériel à locataire unique.

Instances de performance à capacité extensible

Vous pouvez tirer parti des avantages liés à une exécution sur du matériel à location dédiée avec the section called "Instances de performance à capacité extensible". Les instances dédiées T3 sont lancées en mode illimité par défaut et fournissent un niveau de CPU performance de référence avec la possibilité d'atteindre un CPU niveau supérieur lorsque votre charge de travail l'exige. Les performances de base du T3 et la capacité à exploser sont régies par des CPU crédits. En raison de la nature évolutive des types d'instances T3, nous vous recommandons de surveiller la manière dont vos instances T3 utilisent les CPU ressources du matériel dédié pour obtenir les meilleures performances. Les instances dédiées T3 sont destinées aux clients ayant des charges de travail diverses qui présentent un CPU comportement aléatoire, mais dont l'CPUutilisation moyenne est idéalement égale ou inférieure aux utilisations de base. Pour de plus amples informations, veuillez consulter the section called "Concepts clés".

Amazon EC2 a mis en place des systèmes pour identifier et corriger la variabilité des performances. Cependant, il est toujours possible de connaître une variabilité à court terme si vous lancez plusieurs instances dédiées T3 présentant des modèles CPU d'utilisation corrélés. Pour les charges de travail plus exigeantes ou corrélées, nous recommandons d'utiliser des instances dédiées M5 ou M5 plutôt que des instances dédiées T3.

Limites de instances dédiées

Gardez les points suivants à l'esprit lorsque vous utilisez des instances dédiées :

- Certains AWS services ou leurs fonctionnalités ne sont pas pris en charge VPC avec une location d'instance définie sur. `dedicated` Vérifiez la documentation du service pour confirmer s'il existe des restrictions.

- Certains types d'instances ne peuvent pas être lancés dans un VPC si la location d'instance est définie sur. `dedicated` Pour plus d'informations sur les types d'instances pris en charge, consultez Amazon EC2 Dedicated Instances.
- Lorsque vous lancez une instance dédiée soutenue par AmazonEBS, le EBS volume ne s'exécute pas sur du matériel à locataire unique.

Tarification des instances dédiées

La tarification des instances dédiées est différente de celle des instances à la demande. Pour plus d'informations, consultez les instances EC2 dédiées Amazon.

Lancer des instances dédiées dans un environnement VPC avec location par défaut

Lorsque vous créez une instanceVPC, vous avez la possibilité de spécifier la location de son instance. Si vous lancez une instance dans une instance VPC dont la location est égale à`dedicated`, l'instance fonctionnera toujours en tant qu'instance dédiée sur du matériel dédié à votre usage.

Pour plus d'informations sur la création d'un VPC et le choix des options de location, consultez Create a VPC dans le guide de l'VPCutilisateur Amazon.

Vous pouvez lancer une instance dédiée à l'aide de l'assistant de EC2 lancement d'instance Amazon.

Console

Pour lancer une instance dédiée dans une location par défaut à VPC l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Instances, Launch instance (Lancer une instance).
3. Dans la section Images de l'application et du système d'exploitation, sélectionnez-en un AMI dans la liste.
4. Dans la section Instance type (Type d'instance), sélectionnez le type d'instance à lancer.

> **Note**
>
> Veillez à choisir un type d'instance pris en charge en tant qu'Instance dédiée. Pour plus d'informations, consultez Amazon EC2 Dedicated Instances.

5. Dans la section Key pair (Paire de clés), sélectionnez la paire de clés à associer à l'instance.
6. Dans la section Advanced details, pour Tenancy (Location), sélectionnez Dedicated (Dédié).
7. Configurez les options d'instance restantes selon les besoins. Pour de plus amples informations, veuillez consulter Référence pour les paramètres de configuration des EC2 instances Amazon.
8. Sélectionnez Launch instance (Lancer une instance).

AWS CLI

Pour définir l'option de location d'une instance lors du lancement à l'aide du AWS CLI

Utilisez la commande run-instances et incluez dans `Tenancy` l'`--placement`option.

PowerShell

Pour définir l'option de location d'une instance lors du lancement à l'aide des outils pour PowerShell

Utilisez l'New-EC2Instanceapplet de commande avec le `-Placement_Tenancy` paramètre.

Pour plus d'informations sur le lancement d'une instance avec une location `host`, consultez Lancer EC2 des instances Amazon sur un hôte EC2 dédié Amazon.

Modifier la location d'une instance Amazon EC2

Vous pouvez modifier la location d'une instance arrêtée après l'avoir lancée. Les modifications que vous apportez prennent effet au prochain démarrage de l'instance.

Les informations relatives au système d'exploitation de votre instance, et le fait que le SQL serveur soit installé ou non, ont une incidence sur les conversions prises en charge. Pour plus d'informations sur les chemins de conversion de location disponibles pour votre instance, consultez la section Tenancy conversion dans le Guide de l'utilisateur de License Manager.

Vous pouvez également modifier la location de votre cloud privé virtuel (VPC). Pour de plus amples informations, veuillez consulter the section called "Modifier le bail d'un VPC".

Limites

- Pour les instances T3, vous devez lancer l'instance sur un hôte dédié pour utiliser une location `host`. Vous ne pouvez pas modifier la location de `host` à `dedicated` ou `default`. Si vous tentez

d'effectuer l'une de ces modifications de location non prises en charge, vous obtiendrez un code d'erreur `InvalidRequest`.

Console

Pour modifier la location d'une instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Instances, puis choisissez votre instance.
3. Sélectionnez Instance state (État de l'instance), Stop instance (Arrêter l'instance), Stop (Arrêter).
4. Choisissez Actions, Paramètres de l'instance, puis Modifier le placement d'instance.
5. Pour Tenancy (Location), choisissez d'exécuter votre instance sur un matériel dédié ou sur un Hôte dédié. Choisissez Save (Enregistrer).

AWS CLI

Pour modifier la valeur de location d'une instance à l'aide du AWS CLI

Utilisez la modify-instance-placementcommande.

```
aws ec2 modify-instance-placement --instance-id i-1234567890abcdef0 --
tenancy dedicated
```

PowerShell

Pour modifier la valeur de location d'une instance à l'aide du AWS CLI

Utilisez l'Edit-EC2InstancePlacementapplet de commande.

```
Edit-EC2InstancePlacement -InstanceId i-1234567890abcdef0 -Tenancy Dedicated
```

Modifier la location d'instance d'un VPC

Vous pouvez modifier la location d'instance d'un cloud privé virtuel (VPC) de `dedicated` à `default` après l'avoir créé. La modification de la location d'instance d'un n'VPCaffecte pas la location des instances existantes dans le. VPC La prochaine fois que vous lancerez une instance dans leVPC, elle sera louée`default`, sauf indication contraire lors du lancement de l'instance.

Vous pouvez également modifier la location d'instances spécifiques. Pour de plus amples informations, veuillez consulter the section called "Modifier la location d'une instance".

Limites

- Vous ne pouvez pas modifier la location d'instance VPC `default` d'un formulaire `dedicated` après sa création.
- Vous ne pouvez pas modifier la location d'une instance VPC en utilisant le AWS Management Console Vous pouvez la modifier en utilisant le AWS CLI, un AWS SDK, ou Amazon EC2API.

AWS CLI

Pour modifier l'attribut de location d'instance d'un à l'VPCaide du AWS CLI

Utilisez la modify-vpc-tenancycommande et spécifiez l'ID de la valeur de location de l'instance VPC et. La seule valeur prise en charge est `default`.

```
aws ec2 modify-vpc-tenancy --vpc-id vpc-1a2b3c4d --instance-tenancy default
```

PowerShell

Pour modifier l'attribut de location d'instance d'un à VPC l'aide des outils pour PowerShell

Utilisez l'Edit-EC2VpcTenancyapplet de commande et spécifiez l'ID de la valeur de location de l'instance VPC et. La seule valeur prise en charge est `Default`.

```
Edit-EC2VpcTenancy -VpcId vpc-1a2b3c4d -InstanceTenancy Default
```

Réservations de capacité à la demande et blocs de capacité pour le ML

Les réservations de capacité vous permettent de réserver de la capacité de calcul pour EC2 les instances Amazon dans une zone de disponibilité spécifique. Il existe deux types de réserve de capacité qui répondent à différents cas d'utilisation.

Types de réserve de capacité

- Réservations de capacité à la demande
- Blocs de capacité pour ML

Voici quelques cas d'utilisation courants de la réserve de capacité à la demande :

- Événements de mise à l'échelle : créez une réserve de capacité avant les événements stratégiques afin de pouvoir effectuer une mise à l'échelle lorsque vous en avez besoin.
- Exigences réglementaires et reprise après sinistre : utilisez la réservation de capacité à la demande pour satisfaire aux exigences réglementaires en matière de haute disponibilité, et effectuez une réserve de capacité dans une zone de disponibilité ou une région différente pour la reprise après sinistre.

Voici quelques cas d'utilisation courants des blocs de capacité pour ML :

- Entraînement et réglage précis des modèles de machine learning (ML) : bénéficiez d'un accès ininterrompu aux GPU instances que vous avez réservées pour terminer la formation et le réglage des modèles de machine learning.
- Expériences et prototypes de machine learning : exécutez des expériences et créez des prototypes qui nécessitent GPU des instances de courte durée.

Quand utiliser la réserve de capacité à la demande

Utilisez la réserve de capacité à la demande si vous avez des exigences de capacité strictes et si vous exécutez des charges de travail critiques qui nécessitent une garantie de capacité. Avec les réservations de capacité à la demande, vous pouvez vous assurer que vous aurez toujours accès à la EC2 capacité Amazon que vous avez réservée aussi longtemps que vous en aurez besoin.

Quand utiliser les blocs de capacité pour ML

Utilisez les blocs de capacité pour le ML lorsque vous devez vous assurer de disposer d'un accès ininterrompu aux GPU instances pendant une période définie à compter d'une date future. Les blocs de capacité conviennent parfaitement à l'entraînement et à l'optimistion des modèles de machine learning, aux expérimentations de courte durée et à la gestion des augmentations temporaires de la demande d'inférence à avenir. Avec les blocs de capacité, vous pouvez vous assurer que vous aurez accès aux GPU ressources à une date précise pour exécuter vos charges de travail de machine learning.

Réservez de la capacité de calcul grâce aux réservations de capacité à la demande

Les réservations de capacité à la demande vous permettent de réserver de la capacité de calcul pour vos EC2 instances Amazon dans une zone de disponibilité spécifique, quelle que soit la durée. Si

vous avez des exigences de capacité strictes et que vous exécutez des charges de travail critiques qui nécessitent un certain niveau d'assurance de capacité à long ou à court terme, nous vous recommandons de créer une réservation de capacité afin de vous assurer de toujours avoir accès aux EC2 capacités d'Amazon quand vous en avez besoin, aussi longtemps que vous en avez besoin.

Vous pouvez créer des réserves de capacité à tout moment, sans avoir à vous engager pour une durée de 1 à 3 ans. La capacité devient disponible et la facturation démarre dès que la réserve de capacité est allouée dans votre compte. Lorsque vous n'avez plus besoin de la garantie de capacité, annulez la réserve de capacité pour libérer de la capacité et ne plus encourir de frais. Vous pouvez également utiliser les remises de facturation proposées par les Savings Plans et les instances réservées régionales pour réduire le coût d'une réserve de capacité.

Lorsque vous créez un Réservation de capacité, vous spécifiez :

- Zone de disponibilité dans laquelle la capacité est réservée
- Nombre d'instances pour lesquelles vous souhaitez réserver la capacité
- Les attributs de l'instance, y compris le type d'instance, la plate-forme, la zone de disponibilité et la location

Réservations de capacité peut uniquement être utilisé par les instances correspondant aux attributs. Par défaut, les réservations de capacité correspondent automatiquement aux nouvelles instances et aux instances en cours d'exécution dont les attributs correspondent (type d'instance, plateforme, zone de disponibilité et location). Cela signifie que toute instance avec des attributs correspondants est exécutée automatiquement dans la Réservation de capacité. Cependant, vous pouvez également cibler une Réservation de capacité pour des charges de travail spécifiques. Cela vous permet de contrôler explicitement quelles instances sont autorisées à s'exécuter dans cette capacité réservée.

Vous pouvez spécifiez comment votre réservation prend fin. Vous pouvez choisir d'annuler la Réservation de capacité ou de la terminer automatiquement à une date et une heure spécifiées. Si vous spécifiez une date et une heure de fin, la Réservation de capacité est annulée dans l'heure du moment spécifié. Par exemple, si vous spécifiez la date du 31/5/2019 à 13:30:55, la Réservation de capacité est assurée de prendre fin le 31/5/2019, entre 13:30:55 et 14:30:55.

Lorsque la réservation prend fin, vous ne pouvez plus cibler d'instances sur la Réservation de capacité. Les instances en cours d'exécution dans la capacité réservée continuent à s'exécuter sans interruption. Si des instances ciblant une Réservation de capacité sont arrêtées, vous ne pouvez pas les redémarrer avant de supprimer leur préférence de ciblage de Réservation de capacité ou

de les configurer de manière à cibler une Réservation de capacité différente. Pour de plus amples informations, veuillez consulter Modifier les paramètres de réservation de capacité de votre instance.

Sommaire

Différences entre les réservations de capacité, les instances réservées et les Savings Plans

Le tableau suivant met en évidence les principales différences entre les réservations de capacité, les instances réservées et les Savings Plans :

	Capacity Reservations	instances réservées zonales	instances réservées régionales	Savings Plans
Durée	Aucun engagement requis. Peuvent être créées et annulées selon les besoins.	Exige un engagement d'un an ou de trois ans		
Avantage de capacité	Capacité réservée dans une zone de disponibilité spécifique.		Aucune capacité réservée.	
Remise de facturation	Pas de remise de facturation. †	Fournit une remise de facturation.		
Limites d'instance	Vos limites instance à la demande par région s'appliquent.	La valeur par défaut est de 20 par zone de disponibilité. Vous pouvez demander une augmentation de limite.	La valeur par défaut est de 20 par région. Vous pouvez demander une augmentation de limite.	Aucune limite.

† Vous pouvez combiner les réservations de capacité avec des Savings Plans ou des instances réservées régionales pour bénéficier d'une remise.

Pour plus d'informations, consultez les ressources suivantes :

- EC2Présentation des instances réservées pour Amazon
- Guide de l'utilisateur Savings Plans

Plateformes prises en charge

Vous devez créer la réservation de capacité avec la plateforme appropriée pour vous assurer qu'elle correspond à vos instances. Les réservations de capacité prennent en charge les plateformes suivantes :

- Linux/ UNIX
- Linux avec SQL Server Standard
- Linux avec SQL serveur Web
- Linux avec SQL Server Enterprise
- SUSELinux
- Utilisation de Red Hat Enterprise Linux
- RHELavec SQL Server Standard
- RHELavec SQL Server Enterprise
- RHELavec SQL Server Web
- RHELavec HA
- RHELavec HA et SQL Server Standard
- RHELavec HA et SQL Server Enterprise
- Ubuntu Pro
- Windows
- Windows avec SQL serveur
- Windows avec SQL serveur Web
- Windows avec SQL Server Standard
- Windows avec SQL Server Enterprise

Lorsque vous achetez une Réservation de capacité, vous devez spécifier la plateforme qui correspond au système d'exploitation de votre instance.

- Pour SUSE Linux et les RHEL distributions, à l'exceptionBYOL, vous devez choisir la plate-forme spécifique. Par exemple, la plateforme SUSELinux ou Red Hat Enterprise Linux.
- Pour toutes les autres distributions Linux (y compris Ubuntu), choisissez la plate-forme Linux/ UNIX.

- Si vous apportez votre RHEL abonnement existant (BYOL), vous devez choisir la plateforme Linux/UNIX.
- Pour Windows SQL Standard, Windows avec SQL Server Enterprise et Windows avec SQL Server Web, vous devez choisir la plate-forme spécifique.
- Pour toutes les autres versions de Windows, à l'exception de BYOL celles qui ne sont pas prises en charge, choisissez la plate-forme Windows.

Quotas

Le nombre d'instances pour lesquelles vous êtes autorisé à réserver de la capacité est basé sur le quota d'instances à la demande de votre compte. Vous pouvez réserver de la capacité pour autant d'instances que ce quota le permet, moins le nombre d'instances que vous exécutez déjà.

Les quotas s'appliquent uniquement aux instances en cours d'exécution. Si votre instance est en attente, en arrêt, arrêtée ou mise en veille prolongée, elle n'est pas prise en compte dans votre quota.

Limites

Avant de créer des réservations de capacité, prenez note des limitations et restrictions suivantes.

- Les réservations de capacité actifs et non utilisés sont pris en compte dans vos limites d'instance à la demande.
- Les réservations de capacité ne sont pas transférables d'un AWS compte à un autre. Toutefois, vous pouvez partager les réservations de capacité avec d'autres AWS comptes. Pour de plus amples informations, veuillez consulter Réservations de capacité partagée.
- Les remises de facturation sur les Instance réservée par zone ne s'appliquent pas aux réservations de capacité.
- Les réserves de capacité ne peuvent pas être créées dans des groupes de placement de cluster. Les groupes de placement par répartition et par partition ne sont pas pris en charge.
- Les réservations de capacité ne peuvent pas être utilisés avec des Hôtes dédiés. Les réserves de capacité peuvent être utilisées avec les instances dédiées.
- [Instances Windows] Les réservations de capacité ne peuvent pas être utilisées avec Bring Your Own License (BYOL).
- Les réservations de capacité ne vous assurent pas qu'une instance en veille prolongée peut reprendre après avoir essayé de la démarrer.

Tarification et facturation d'une Réservation de capacité

Les rubriques de cette section fournissent un aperçu de la tarification et de la facturation pour les réservations de capacité.

Rubriques

Tarification

Les réserves de capacité sont facturées au tarif à la demande équivalent, que vous exécutiez des instances dans la capacité réservée ou non. Si vous n'utilisez pas la réservation, cela apparaît comme une réservation non utilisée sur votre EC2 facture Amazon. Lorsque vous exécutez une instance qui correspond aux attributs d'une réservation, vous payez seulement pour l'instance, vous ne payez rien pour la réservation. Il n'y a aucun frais anticipé ou additionnel.

Par exemple, si vous créez une Réservation de capacité pour 20 instances Linux `m4.large` et que vous exécutez 15 instances Linux `m4.large` dans la même zone de disponibilité, vous serez facturé pour 15 instances actives et pour 5 instances non utilisées dans la réservation.

Les remises de facturation pour les Savings Plans et les Instances réservées régionales s'appliquent aux Réservations de capacité. Pour de plus amples informations, veuillez consulter Remises de facturation.

Pour plus d'informations, consultez Amazon EC2 Pricing.

Facturation

La facturation commence dès que la réserve de capacité est allouée dans votre compte, et elle se poursuit tant que la réserve de capacité reste allouée dans votre compte.

Les réservations de capacité sont facturées à la seconde. Cela signifie que vous êtes facturé pour les heures partielles. Par exemple, si une réserve de capacité reste active dans votre compte pendant `24` heures et `15` minutes, vous serez facturé pour `24.25` heures de réservation.

L'exemple suivant présente la manière dont une Réservation de capacité est facturée. La Réservation de capacité est créée pour une instance Linux `m4.large`, dont le tarif à la demande

est de 0,10 USD par heure d'utilisation. Dans cet exemple, la réserve de capacité est allouée dans le compte pendant cinq heures. La Réservation de capacité n'étant pas utilisée la première heure, elle est facturée en tant qu'heure non utilisée au tarif à la demande standard du type d'instance `m4.large`. De la deuxième à la cinquième heure, la Réservation de capacité est occupée par une instance `m4.large`. Pendant ce laps de temps, la Réservation de capacité n'engendre pas de frais, et le compte est facturé pour l'instance `m4.large` qui l'occupe. Pour la sixième heure, la Réservation de capacité est annulée et l'instance `m4.large` s'exécute normalement en dehors de la capacité réservée. Cette heure est facturée selon le tarif à la demande du type d'instance `m4.large`.

Hour	1	2	3	4	5	6	Total cost
Unused Capacity Reservation	$0.10	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.10**
On-demand Instance Usage	$0.00	$0.10	$0.10	$0.10	$0.10	$0.10	**$0.50**
Hourly cost	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.60**

Remises de facturation

Les remises de facturation pour les Savings Plans et les instances réservées régionales s'appliquent aux réservations de capacité. AWS applique automatiquement ces remises aux réservations de capacité dont les attributs correspondent. Lorsqu'un Réservation de capacité est utilisé par une instance, la remise est appliquée à cette instance. Les remises sont prioritairement appliquées à des instances en cours d'exécution avant de couvrir les réservations de capacité inutilisées.

Les remises de facturation sur les instances réservées zonales ne s'appliquent pas aux réservations de capacité.

Pour plus d'informations, consultez les ressources suivantes :

- EC2Présentation des instances réservées pour Amazon
- Guide de l'utilisateur Savings Plans
- Options de facturation et d'achat

Affichage d'une facture

Vous pouvez consulter les frais et les frais associés à votre compte sur la AWS Billing and Cost Management console.

- Le Tableau de bord affiche un récapitulatif des dépenses de votre compte.

- Sur la page Factures, sous Détails, développez la section Elastic Compute Cloud et la région pour obtenir des informations de facturation sur vos Réservations de capacité.

Vous pouvez consulter les frais en ligne ou télécharger un CSV fichier. Pour plus d'informations, consultez Éléments de ligne de réservation de capacité dans le Guide de l'utilisateur AWS Billing and Cost Management .

Créer une Réservation de capacité

Vous pouvez créer une réservation de capacité pour vous assurer que vous disposez d'une capacité de calcul disponible dans une zone de disponibilité spécifique. Si votre demande de création d'une réserve de capacité aboutit, la capacité est disponible immédiatement. La capacité demeure réservée pour votre utilisation tant que la Réservation de capacité est active. Vous pouvez y lancer des instances à tout moment. Si la Réservation de capacité est ouverte, les nouvelles instances et les instances existantes dont les attributs correspondent s'exécutent automatiquement dans la capacité de la Réservation de capacité. Si la Réservation de capacité est `targeted`, les instances doivent la cibler spécifiquement pour s'exécuter dans la capacité réservée.

Votre demande de création d'une Réservation de capacité peut échouer si l'une des situations suivantes se produit :

- Amazon EC2 ne dispose pas de capacités suffisantes pour répondre à la demande. Réessayez ultérieurement, essayez une zone de disponibilité différente ou essayez une demande moins importante. Si votre application tolère plusieurs types et tailles d'instance, essayez des attributs d'instance différents.
- La quantité demandée dépasse votre limite d'instance à la demande pour la famille de·l'instance sélectionnée. Augmentez votre limite d'instance à la demande pour la famille de·l'instance requise et réessayez. Pour plus d'informations, consultez Quotas des instances à la demande.

Pour créer une Réservation de capacité à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Choisissez Réservations de capacité, puis Créer Réservation de capacité.
3. Sur la page Create a Réservation de capacité (Créer une capacité de réservation), configurez les paramètres suivants dans la section Instance details (Détails de l'instance). Le type d'instance, la plateforme, la zone de disponibilité et la location des instances que vous lancez doivent correspondre au type d'instance, à la plateforme, à la zone de disponibilité et à la location

que vous spécifiez ici, sinon la réservation de capacité n'est pas appliquée. Par exemple, si un Réservation de capacité ouvert ne correspond pas, un lancement d'instance ciblant ce Réservation de capacité explicitement échouera.

a. Type d'instance : type d'instance à lancer dans la capacité réservée.

b. Lancer des instances EBS optimisées : spécifiez si vous souhaitez réserver la capacité aux instances EBS optimisées. Cette option est sélectionnée par défaut pour certains types d'instances. Pour de plus amples informations, veuillez consulter the section called "EBSoptimisation".

c. Plateforme : système d'exploitation pour vos instances. Pour de plus amples informations, veuillez consulter Plateformes prises en charge.

d. Zone de disponibilité : zone de disponibilité dans laquelle réserver la capacité.

e. Emplacement : spécifiez si vous voulez exécuter sur un matériel partagé (par défaut) ou une instance dédiée.

f. (Facultatif) Groupe ARN ARN de placement : du groupe de placement du cluster dans lequel créer la réservation de capacité.

   Pour de plus amples informations, veuillez consulter Création de réservations de capacité dans des groupes de placement de clusters.

g. Quantité : nombre d'instances pour lesquelles vous souhaitez réserver la capacité. Si vous spécifiez une quantité qui dépasse votre limite d'instance à la demande restante pour le type d'instance sélectionné, la demande est refusée.

4. Configurez les paramètres suivants dans la section Reservation details (Détails de la réservation) :

   a. Reservation Ends (Fins de réservation) : choisissez une des options suivantes :

      - Manually (Manuellement) : réservez la capacité jusqu'à ce que vous l'annuliez de manière explicite.
      - Specific time (Date et heure spécifiques) : annule la réservation de capacité automatiquement à la date et à l'heure spécifiées.

   b. Instance eligibility (Éligibilité de l'instance) : choisissez une des options suivantes :

      - open — (Par défaut) La réservation de capacité correspond à toute instance dont les attributs correspondent (type d'instance, plateforme, zone de disponibilité et location).

Si vous lancez une instance avec les attributs correspondants, celle-ci est placée automatiquement dans la capacité réservée.

- ciblé : la réservation de capacité accepte uniquement les instances dont les attributs correspondent (type d'instance, plateforme, zone de disponibilité et location) et qui ciblent explicitement la réservation.

5. Choisissez Request reservation (Demander une réservation).

Pour créer une réservation de capacité à l'aide du AWS CLI

Utilisez la create-capacity-reservationcommande. Pour de plus amples informations, veuillez consulter Plateformes prises en charge.

La commande suivante crée une réservation de capacité qui réserve de la capacité à trois `m5.2xlarge` instances exécutant Red Hat Enterprise Linux AMIs dans la zone de `us-east-1a` disponibilité.

```
aws ec2 create-capacity-reservation --instance-type m5.2xlarge --instance-platform Red
 Hat Enterprise Linux --availability-zone us-east-1a --instance-count 3
```

La commande suivante crée une réservation de capacité qui réserve de la capacité à trois `m5.2xlarge` instances exécutant Windows avec un SQL serveur AMIs dans la zone de `us-east-1a` disponibilité.

```
aws ec2 create-capacity-reservation --instance-type m5.2xlarge --instance-
platform Windows with SQL Server --availability-zone us-east-1a --instance-count 3
```

Afficher l'état d'une réservation de capacité

Amazon surveille EC2 en permanence l'état de vos réservations de capacité. Les mises à jour sont communiquées sur la EC2 console Amazon. Vous pouvez consulter les informations relatives à une réservation de capacité en utilisant l'une des méthodes suivantes.

Pour afficher vos réservations de capacité à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Choisissez Réservations de capacité puis sélectionnez une Réservation de capacité à afficher.

Pour consulter vos réservations de capacité à l'aide du AWS CLI

Utilisez la describe-capacity-reservationscommande :

Par exemple, la commande suivante décrit toutes les réservations de capacité.

```
aws ec2 describe-capacity-reservations
```

Exemple de sortie.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1234abcd56EXAMPLE ",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-16T09:03:18.000Z",
            "AvailableInstanceCount": 1,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 1,
            "State": "active",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "a1.medium",
            "PlacementGroupArn": "arn:aws:ec2:us-east-1:123456789012:placement-group/
MyPG"
        },
        {
            "CapacityReservationId": "cr-abcdEXAMPLE9876ef ",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-07T11:34:19.000Z",
            "AvailableInstanceCount": 3,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 3,
            "State": "cancelled",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "m5.large"
```

```
        }
    ]
}
```

Réservations de capacité peut avoir les états suivants :

- `active` : la capacité peut être utilisée.
- `expired` : la Réservation de capacité a expiré automatiquement à la date et à l'heure spécifiées dans votre demande de réservation. La capacité réservée n'est plus disponible pour utilisation.
- `cancelled` : la Réservation de capacité a été annulée. La capacité réservée n'est plus disponible pour utilisation.
- `pending` : la demande de Réservation de capacité a abouti, mais la mise en service de la capacité est toujours en attente.
- `failed` : la demande de Réservation de capacité a échoué. Une demande peut échouer en raison de paramètres de demande qui ne sont pas valides, de contraintes de capacité ou de contraintes de limite d'instance. Vous pouvez afficher une demande qui a échoué pendant 60 minutes.

> **Note**
>
> En raison de l'éventuel modèle de cohérence suivi par Amazon EC2APIs, une fois que vous avez créé une réservation de capacité, la console et la describe-capacity-reservationsréponse peuvent prendre jusqu'à 5 minutes pour indiquer que la réservation de capacité est en bon `active` état. Pendant ce temps, la console et la réponse `describe-capacity-reservations` peuvent indiquer que la réserve de capacité se trouve dans l'état `pending`. Toutefois, la réserve de capacité peut déjà être utilisée et vous pouvez tenter d'y lancer des instances.

Lancer des instances dans une Réservation de capacité existante

Lorsque vous lancez une instance, vous pouvez spécifier si elle doit être lancée dans n'importe quel Réservation de capacité `open`, dans une Réservation de capacité spécifique, ou dans un groupe de Réservations de capacité. Vous ne pouvez lancer une instance que dans le cadre d'une réservation de capacité qui possède les attributs correspondants (type d'instance, plateforme, zone de disponibilité et location) et une capacité suffisante. Vous pouvez également configurer l'instance pour éviter qu'elle s'exécute dans une Réservation de capacité, même si vous avez une Réservation de capacité `open` qui a des attributs correspondants et la capacité disponible.

Le lancement d'une instance dans une Réservation de capacité réduit sa capacité disponible du nombre d'instances lancées. Par exemple, si vous lancez trois instances, la capacité disponible de la Réservation de capacité est réduite de trois.

Pour lancer des instances dans une Réservation de capacité existante à l'aide de la console

1. Suivez la procédure pour lancer une instance, mais ne lancez pas l'instance tant que vous n'avez pas effectué les étapes suivantes pour spécifier les paramètres du groupe de placement et de la réservation de capacité.
2. Développez les informations avancées et procédez comme suit :

   a. Pour Groupe de placement, sélectionnez le groupe de placement du cluster dans lequel vous souhaitez lancer l'instance.

   b. Pour Capacity Reservation (Réserve de capacité), choisissez l'une des options suivantes en fonction de la configuration de la réserve de capacité :

      - Aucune : empêche les instances de se lancer dans une réservation de capacité. Les instances s'exécutent dans une capacité à la demande.
      - Ouvert — Lance les instances dans n'importe quelle réservation de capacité dont les attributs correspondent et une capacité suffisante pour le nombre d'instances que vous avez sélectionné. Si vous n'avez pas de Réservation de capacité correspondante avec une capacité suffisante, l'instance utilise une capacité à la demande.
      - Cibler par ID — Lance les instances dans la réservation de capacité sélectionnée. Si la Réservation de capacité sélectionnée ne dispose pas d'une capacité suffisante pour le nombre d'instances que vous avez sélectionnées, le lancement de l'instance échoue.
      - Cibler par groupe : lance les instances dans n'importe quelle réservation de capacité avec les attributs correspondants et la capacité disponible dans le groupe de réservation de capacité sélectionné. Si le groupe sélectionné ne dispose pas d'une Réservation de capacité avec les attributs correspondants et de la capacité disponible, les instances s'exécutent à l'aide de la capacité à la demande.
3. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance). Pour de plus amples informations, veuillez consulter Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console.

Pour lancer une instance dans une réservation de capacité existante à l'aide du AWS CLI

Utilisez la commande run-instances et spécifiez le paramètre `--capacity-reservation-specification`.

L'exemple suivant lance une instance `t2.micro` dans toute Réservation de capacité ouverte disposant des attributs correspondants et de la capacité disponible :

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro
 --key-name MyKeyPair --subnet-id subnet-1234567890abcdef1 --capacity-reservation-
specification CapacityReservationPreference=open
```

L'exemple suivant lance une instance `t2.micro` dans un `targeted` Réservation de capacité :

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro
 --key-name MyKeyPair --subnet-id subnet-1234567890abcdef1 --capacity-reservation-
specification CapacityReservationTarget={CapacityReservationId=cr-a1234567}
```

L'exemple suivant lance une instance `t2.micro` dans un groupe Réservation de capacité :

```
aws ec2 run-instances --image-id ami-abc12345 --count 1
 --instance-type t2.micro --key-name MyKeyPair --subnet-
id subnet-1234567890abcdef1 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-1:123456789012:group/my-cr-group}
```

Modifier une réservation de capacité active

Si vous avez une réservation de capacité existante qui ne correspond pas à la charge de travail nécessitant cette capacité, vous pouvez modifier le nombre d'instances, l'éligibilité des instances (`open`ou`targeted`) et l'heure de fin (`At specific time`ou`Manually`). Vous ne pouvez pas modifier une réservation de capacité après son expiration ou après l'avoir explicitement annulée. Si vous spécifiez une nouvelle quantité d'instances qui dépasse la limite d'instances à la demande restante pour le type d'instance sélectionné, la mise à jour échoue.

Vous ne pouvez pas modifier le type d'instance, EBS l'optimisation, la plateforme, la zone de disponibilité ou la location d'une réservation de capacité existante. Si vous devez modifier un de ces attributs, nous vous recommandons d'annuler la réservation, puis d'en créer une nouvelle avec les attributs requis.

Si vous modifiez une réservation de capacité existante en faisant passer l'éligibilité de l'instance `targeted` à à`open`, toutes les instances en cours d'exécution qui correspondent aux attributs de

la réservation de capacité, dont le `CapacityReservationPreference` paramètre est défini sur et qui ne sont pas encore exécutées dans le cadre d'une réservation de capacité utiliseront automatiquement la réservation de capacité modifiée. `open`

> **Note**
>
> Pour modifier l'éligibilité des instances, la réservation de capacité doit être complètement inactive (aucune utilisation) car Amazon ne EC2 peut pas modifier l'éligibilité des instances lorsque des instances sont exécutées dans le cadre de la réservation.

Pour modifier une Réservation de capacité à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Choisissez Réservations de capacité, sélectionnez la Réservation de capacité à modifier, puis choisissez Modifier.
3. Modifiez les options de capacité totale, de fin de réservation de capacité ou d'éligibilité de l'instance selon vos besoins, puis choisissez Enregistrer.

Pour modifier une réservation de capacité à l'aide du AWS CLI

Utilisez la modify-capacity-reservationcommande. Par exemple, la commande suivante modifie une Réservation de capacité pour réserver la capacité pour huit instances.

```
aws ec2 modify-capacity-reservation --capacity-reservation-id cr-1234567890abcdef0 --
instance-count 8
```

Modifier les paramètres de réservation de capacité de votre instance

Vous pouvez modifier les paramètres de Réservation de capacité pour une instance arrêtée à tout moment :

- Commencez par n'importe quelle réservation de capacité dont les attributs (type d'instance, plate-forme, zone de disponibilité et location) et la capacité disponible correspondent.
- Démarrez l'instance dans une Réservation de capacité spécifique.
- Démarrez dans n'importe quelle Réservation de capacité qui dispose des attributs correspondants et de la capacité disponible dans un groupe Réservation de capacité

- Empêchez l'instance de démarrer dans une Réservation de capacité.

Pour modifier les paramètres de la Réservation de capacité d'une instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Choisissez Instances, puis sélectionnez l'instance à modifier. Arrêtez l'instance, si elle ne l'est pas déjà.
3. Choisissez Actions, Paramètres de l'instance, Modifier les paramètres de réservation de capacité.
4. Pour Réservation de capacité, choisissez l'une des options suivantes :

   - Open (Ouvrir) : lance les instances dans toute Réservation de capacité comportant des attributs correspondants et une capacité suffisante pour le nombre d'instances que vous avez sélectionnées. Si vous n'avez pas de Réservation de capacité correspondante avec une capacité suffisante, l'instance utilise une capacité à la demande.
   - None (Aucune) : empêche les instances de se lancer dans une Réservation de capacité. Les instances s'exécutent dans une capacité à la demande.
   - Spécifier la réservation de capacité — Lance les instances dans la Réservation de capacité sélectionnée. Si la Réservation de capacité sélectionnée ne dispose pas d'une capacité suffisante pour le nombre d'instances que vous avez sélectionnées, le lancement de l'instance échoue.
   - Spécifier le groupe de réservation de capacité — Lance les instances dans n'importe quelle Réservation de capacité avec les attributs correspondants et la capacité disponible dans le groupe Réservation de capacité sélectionné. Si le groupe sélectionné ne dispose pas d'une Réservation de capacité avec les attributs correspondants et de la capacité disponible, les instances s'exécutent à l'aide de la capacité à la demande.

Pour modifier les paramètres de réservation de capacité d'une instance à l'aide du AWS CLI

Utilisez la commande modify-instance-capacity-reservation-attributes.

Par exemple, la commande suivante change le paramètre Réservation de capacité d'une instance pour `open` ou `none`.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-
id i-1234567890abcdef0 --capacity-reservation-specification
 CapacityReservationPreference=none|open
```

Par exemple, la commande suivante modifie une instance pour cibler une Réservation de capacité spécifique.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-
id i-1234567890abcdef0 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=cr-1234567890abcdef0}
```

Par exemple, la commande suivante modifie une instance pour cibler un groupe Réservation de capacité spécifique.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-
id i-1234567890abcdef0 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-1:123456789012:group/my-cr-group}
```

Déplacer la capacité entre les réservations de capacité

Si vous avez plusieurs réservations de capacité, vous pouvez déplacer la capacité disponible d'une réservation à l'autre. Par exemple, si vous avez besoin de capacités supplémentaires dans le cadre d'une réservation de capacité dont l'utilisation augmente et que vous avez une autre réservation de capacité avec une capacité disponible, vous pouvez réaffecter la capacité entre les deux réservations.

La réservation de capacité de destination doit correspondre aux propriétés suivantes de la réservation de capacité source :

- Type d'instance
- Plateforme
- Zone de disponibilité
- Location
- Groupe de placement
- L'heure de fin

L'éligibilité (`openoutargeted`) de l'instance de réservation de capacité de destination et les balises ne doivent pas nécessairement correspondre à la réservation de capacité source. La configuration de la réservation de capacité source et de destination reste la même, à l'exception de la capacité disponible réduite dans la réservation source et de l'augmentation de la capacité disponible dans la réservation de destination.

Si toute la capacité disponible est déplacée depuis la réservation de capacité source et qu'aucune capacité n'est utilisée, la réservation de capacité sera automatiquement annulée. Si vous essayez de déplacer une capacité supérieure à la capacité disponible dans la réservation de capacité source, vous recevrez un message d'erreur.

> **Note**
>
> Le déplacement de la capacité disponible des blocs de capacité n'est pas pris en charge.

Pour déplacer la capacité disponible d'une réservation de capacité source vers une réservation de capacité de destination, vous pouvez utiliser la EC2 console Amazon ou le AWS CLI.

Console

Pour déplacer la capacité disponible à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation de gauche, choisissez Capacity Reservations.
3. Sélectionnez un numéro de réservation de capacité à la demande qui dispose de la capacité disponible pour le déménagement.
4. Sous Actions, Gérer la capacité, choisissez Déplacer.
5. Sur la page Capacité de transfert, sous Réservation de capacité de destination, sélectionnez une réservation dans la liste.
6. Sous Quantité à déplacer, utilisez le curseur ou saisissez le nombre d'instances à déplacer de la réservation de capacité source à la réservation de capacité de destination.
7. Passez en revue le résumé, puis lorsque vous êtes prêt, choisissez Déplacer.

AWS CLI

Pour déplacer la capacité disponible à l'aide du AWS CLI

Utilisez la commande `move-capacity-reservation-instances`. L'exemple suivant déplace 10 instances de la réservation de capacité source avec un ID de `cr-1234567890abcdef0` vers la réservation de capacité de destination avec un ID de`cr-021345abcdef56789`.

```
aws ec2 move-capacity-reservation-instances --source-capacity-reservation-
id cr-1234567890abcdef0 --destination-capacity-reservation-id cr-021345abcdef56789
 --instance-count 10
```

Séparer la capacité disponible d'une réservation de capacité existante

Si vous disposez d'une capacité disponible dans une réservation de capacité existante que vous souhaitez affecter à une charge de travail spécifique ou utiliser pour effectuer une action spécifique, vous pouvez diviser la capacité disponible dans une nouvelle réservation de capacité. Par exemple, pour partager partiellement une réservation de capacité avec un autre compte, vous pouvez diviser une partie de la capacité disponible pour créer une réservation de capacité plus petite. La réservation de capacité de plus petite taille peut ensuite être partagée avec l'autre compte en utilisant AWS Resource Access Manager (AWS RAM).

Lorsque vous divisez la capacité disponible d'une réservation de capacité existante, une nouvelle réservation de capacité est automatiquement créée. La réservation de capacité existante restera inchangée, à l'exception de la capacité totale réduite due au nombre d'instances séparées. Les instances qui s'exécutent dans le cadre de la réservation de capacité existante ne sont pas affectées. Vous pouvez diviser la réservation de capacité existante en une seule nouvelle réservation de capacité. Afin de répartir la capacité disponible, la réservation de capacité existante doit être active et détenue par votre AWS compte.

La nouvelle réservation de capacité aura la même configuration que la réservation de capacité existante, à l'exception des balises. Par défaut, la nouvelle réservation de capacité ne comporte aucune étiquette. Vous pouvez spécifier de nouvelles balises lors de l'opération de fractionnement. La nouvelle réservation de capacité peut également être modifiée après sa création, si nécessaire.

Le nombre maximum d'instances à séparer d'une réservation de capacité existante est le montant de la réservation moins une. Par exemple, si une réservation de capacité a une capacité réservée de 10 emplacements, vous pouvez séparer un maximum de neuf emplacements si les neuf emplacements sont disponibles.

Considérations

- Groupes de ressources — Si la réservation de capacité existante appartient à un groupe de ressources, la nouvelle réservation de capacité ne sera pas automatiquement ajoutée au groupe de ressources. Vous pouvez ajouter la nouvelle réservation de capacité à un groupe de ressources après sa création, si nécessaire.
- Partage — Si la réservation de capacité existante est partagée avec un compte client, la nouvelle réservation de capacité ne sera pas automatiquement partagée avec le compte client. Vous pouvez partager la nouvelle réservation de capacité après sa création, si nécessaire.
- Groupe de placement de cluster — Si la réservation de capacité existante fait partie d'un groupe de placement de cluster, la nouvelle réservation de capacité sera créée dans le même groupe de placement de cluster.

> **Note**
>
> La division de la capacité d'un bloc de capacité n'est pas prise en charge.

Contrôlez l'accès pour diviser les réservations de capacité à l'aide de balises

Vous pouvez utiliser des balises pour contrôler l'accès aux EC2 ressources Amazon, notamment en séparant la capacité disponible d'une réservation de capacité existante pour créer une nouvelle réservation de capacité. Pour plus d'informations, consultez la section Contrôle de l'accès aux AWS ressources à l'aide de balises dans le Guide de IAM l'utilisateur.

Pour contrôler l'accès lors du fractionnement d'une réservation de capacité à l'aide de balises, assurez-vous de spécifier les balises de ressource et de demande dans la déclaration de politique, car IAM les politiques sont évaluées à la fois par rapport à la réservation de capacité source et à la réservation de capacité nouvellement créée. L'exemple de politique suivant inclut la clé de `ec2:ResourceTag` condition avec la balise `Owner=ExampleDepartment1` pour la réservation de capacité source et la clé de `ec2:RequestTag` condition avec la balise `stack=production` pour la réservation de capacité nouvellement créée.

```
{
  "Statement": [
    {
      "Sid": "AllowSourceCapacityReservation",
```

```
      "Effect": "Allow",
      "Action": "ec2:CreateCapacityReservationBySplitting",
      "Resource": "arn:aws:ec2:region:account:capacity-reservation/
cr-1234567890abcdef0",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Owner": "ExampleDepartment1"
        }
      }
    },
    {
      "Sid": "AllowNewlyCreatedCapacityReservation",
      "Effect": "Allow",
      "Action": ["ec2:CreateCapacityReservationBySplitting", "ec2:CreateTags"],
      "Resource": "arn:aws:ec2:region:account:capacity-reservation/*",
      "Condition": {
        "StringEquals": {
          "ec2:RequestTag/stack": "production"
        }
      }
    }
  ]
}
```

Répartissez la capacité disponible à l'aide de la EC2 console Amazon ou du AWS CLI

Pour séparer la capacité disponible d'une réservation de capacité existante et créer une nouvelle réservation de capacité, vous pouvez utiliser la EC2 console Amazon ou le AWS CLI.

Console

Pour répartir la capacité disponible à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation de gauche, choisissez Capacity Reservations.
3. Sélectionnez un numéro de réservation de capacité à la demande qui dispose d'une capacité disponible à diviser.
4. Sous Actions, Gérer la capacité, choisissez Split.
5. Sur la page Réservation de capacité partagée, sous Quantité à diviser, utilisez le curseur ou saisissez le nombre d'instances disponibles à séparer de la réservation en cours.
6. (Facultatif) Ajoutez des balises pour la nouvelle réservation de capacité.

7. Passez en revue le résumé et lorsque vous êtes prêt, choisissez Split.

AWS CLI

Pour répartir la capacité disponible à l'aide du AWS CLI

Utilisez la commande `create-capacity-reservation-by-splitting`. L'exemple suivant crée une nouvelle réservation de capacité en séparant 10 instances de la réservation de capacité avec un ID de`cr-1234567890abcdef0`.

```
aws ec2 create-capacity-reservation-by-splitting --source-capacity-reservation-
id cr-1234567890abcdef0 --instance-count 10
```

Annuler une Réservation de capacité

Vous pouvez annuler une Réservation de capacité à tout moment si vous n'avez plus besoin de la capacité réservée. Lorsque vous annulez une Réservation de capacité, la capacité est immédiatement libérée et n'est plus réservée pour votre utilisation.

Vous pouvez annuler des réservations de capacité vides et des réservations de capacité ayant des instances en cours d'exécution. Si vous annulez une Réservation de capacité avec des instances en cours d'exécution, les instances continuent leur exécution normale en dehors de la réservation de capacité aux tarifs standard instance à la demande ou à un tarif réduit si vous avez un Savings Plans ou une Instance réservée régionale correspondant.

Une fois que vous avez annulé une Réservation de capacité, les instances la ciblant ne peuvent plus être lancées. Modifiez ces instances de sorte qu'elles ciblent une autre Réservation de capacité, lancez-les dans une Réservation de capacité « open » disposant des attributs correspondants et d'une capacité suffisante ou évitez de les lancer dans une Réservation de capacité. Pour plus d'informations, consultez Modifier les paramètres de réservation de capacité de votre instance.

Pour annuler une Réservation de capacité à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Choisissez Réservations de capacité et sélectionnez la Réservation de capacité à annuler.
3. Choisissez Cancel réservation (Annuler la réservation), Cancel réservation (Annuler la réservation).

Pour annuler une réservation de capacité à l'aide du AWS CLI

Utilisez la cancel-capacity-reservationcommande :

Par exemple, la commande suivante annule une Réservation de capacité avec un ID de `cr-1234567890abcdef0`.

```
aws ec2 cancel-capacity-reservation --capacity-reservation-id cr-1234567890abcdef0
```

Groupes de réserve de capacité

Vous pouvez l'utiliser AWS Resource Groups pour créer des ensembles logiques de réservations de capacité, appelés groupes de ressources. Un groupe de ressources est un regroupement logique de AWS ressources qui se trouvent toutes dans la même AWS région. Pour plus d'informations sur les groupes de ressources, consultez Que sont les groupes de ressources ? dans le Guide de l'utilisateur AWS Resource Groups .

Vous pouvez inclure les réservations de capacité que vous possédez dans votre compte et les réservations de capacité partagées avec vous par d'autres AWS comptes dans un seul groupe de ressources. Vous pouvez également inclure des réservations de capacité ayant différents attributs (type d'instance, plate-forme, zone de disponibilité et location) dans un seul groupe de ressources.

Lorsque vous créez des groupes de ressources pour des réserves de capacité, vous pouvez cibler des instances vers un groupe de réserves de capacité au lieu d'une réserve de capacité seule. Les instances qui ciblent un groupe de réservations de capacité correspondent à toutes les réservations de capacité du groupe dont les attributs (type d'instance, plate-forme, zone de disponibilité et location) et la capacité disponible correspondent. Si le groupe ne dispose pas d'une Réservation de capacité avec les attributs correspondants et de la capacité disponible, les instances s'exécutent à l'aide de la capacité à la demande. Si une Réservation de capacité adéquate est ajoutée au groupe cible à un stade ultérieur, l'instance est automatiquement mise en correspondance et déplacée vers sa capacité réservée.

Pour empêcher une utilisation non prévue des réservations de capacité dans un groupe, configurez la réservations de capacité dans le groupe pour accepter uniquement les instances qui ciblent explicitement la réserve de capacité. Pour ce faire, définissez l'éligibilité de l'instance sur les instances ciblées (ancienne console) ou uniquement sur les instances qui spécifient cette réservation (nouvelle console) lors de la création de la réservation de capacité à l'aide de la EC2 console Amazon. Lorsque vous utilisez le AWS CLI, spécifiez-le `--instance-match-criteria targeted` lors de la création de la réservation de capacité. On s'assure ainsi que seules les

instances qui ciblent explicitement le groupe, ou une Réservation de capacité dans le groupe, peuvent s'exécuter dans le groupe.

Si une Réservation de capacité dans un groupe est annulée ou expire alors qu'elle a des instances en cours d'exécution, des dernières sont automatiquement déplacées vers une autre Réservation de capacité dans le groupe qui a des attributs correspondants et la capacité disponible. S'il ne reste pas de réservations de capacité dans le groupe avec les attributs et la capacité disponible correspondants, les instances s'exécutent à l'aide de la capacité à la demande. Si une Réservation de capacité adéquate est ajoutée au groupe cible à un stade ultérieur, l'instance est automatiquement déplacée dans sa capacité réservée.

Rubriques

- Création d'un groupe de réserves de capacité
- Ajout d'une réserve de capacité à un groupe
- Suppression d'une réserve de capacité d'un groupe
- Suppression d'un groupe de réserves de capacité

Création d'un groupe de réserves de capacité

Vous pouvez utiliser les informations suivantes pour créer un groupe de ressources pour les réservations de capacité.

Pour créer un groupe de réserves de capacité

Utilisez la commande create-group AWS CLI . Pour `name`, indiquez un nom descriptif pour le groupe et pour `configuration`, spécifiez deux paramètres de `Type` demande :

- `AWS::EC2::CapacityReservationPool` pour s'assurer que le groupe de ressources peut être ciblé pour les lancements d'instances
- `AWS::ResourceGroups::Generic` avec `allowed-resource-types` définie sur `AWS::EC2::CapacityReservation` pour s'assurer que le groupe de ressources accepte uniquement les réserves de capacité

Par exemple, la commande suivante crée un groupe nommé `MyCRGroup`.

```
aws resource-groups create-group --name MyCRGroup --configuration
 '{"Type":"AWS::EC2::CapacityReservationPool"}'
```

```
 '{"Type":"AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-resource-
types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

Voici un exemple de sortie.

```
{
    "GroupConfiguration": {
        "Status": "UPDATE_COMPLETE",
        "Configuration": [
            {
                "Type": "AWS::EC2::CapacityReservationPool"
            },
            {
                "Type": "AWS::ResourceGroups::Generic",
                "Parameters": [
                    {
                        "Values": [
                            "AWS::EC2::CapacityReservation"
                        ],
                        "Name": "allowed-resource-types"
                    }
                ]
            }
        ]
    },
    "Group": {
        "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup",
        "Name": "MyCRGroup"
    }
}
```

Ajout d'une réserve de capacité à un groupe

Si vous ajoutez une réserve de capacité qui est partagée avec vous à un groupe et que le partage est annulé, la réserve est automatiquement supprimée du groupe.

Pour ajouter une Réservation de capacité à un groupe

Utilisez la commande AWS CLI group-resources. Pour`group`, spécifiez le nom du groupe auquel ajouter les réservations de capacité, et pour`resources`, spécifiez les réservations ARNs de capacité à ajouter. Pour ajouter plusieurs réservations de capacité, ARNs séparez-les par un espace. Pour

obtenir les réservations ARNs de capacité à ajouter, utilisez la describe-capacity-reservations AWS CLI commande et spécifiez les réservations IDs de capacité.

Par exemple, la commande suivante ajoute deux Réservations de capacité à un groupe nommé `MyCRGroup`.

```
aws resource-groups group-resources --group MyCRGroup --resource-arns arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Voici un exemple de sortie.

```
{
    "Failed": [],
    "Succeeded": [
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
    ]
}
```

Suppression d'une réserve de capacité d'un groupe

Pour supprimer une Réservation de capacité d'un groupe

Utilisez la commande ungroup-resources AWS CLI . Pour`group`, spécifiez le ARN groupe dont vous souhaitez supprimer la réservation de capacité, et pour `resources` spécifier les réservations ARNs de capacité à supprimer. Pour supprimer plusieurs réservations de capacité, ARNs séparez-les par un espace.

L'exemple suivant montre comment supprimer deux Réservations de capacité d'un groupe nommé `MyCRGroup`.

```
aws resource-groups ungroup-resources --group MyCRGroup --resource-arns arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Voici un exemple de sortie.

```
{
    "Failed": [],
```

```
    "Succeeded": [
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd",
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
    ]
}
```

Suppression d'un groupe de réserves de capacité

Vous pouvez utiliser les informations suivantes pour supprimer un groupe de réservation de capacité.

Pour supprimer un groupe

Utilisez la commande delete-group AWS CLI . Pour `group` fournissez le nom du groupe à supprimer.

Par exemple, la commande suivante supprime un groupe appelé `MyCRGroup`.

```
aws resource-groups delete-group --group MyCRGroup
```

Voici un exemple de sortie.

```
{
    "Group": {
        "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup",
        "Name": "MyCRGroup"
    }
}
```

Création de réservations de capacité dans des groupes de placement de clusters

Vous pouvez créer des réservations de capacité dans un groupe de placement de clusters afin de réserver la capacité de EC2 calcul d'Amazon pour vos charges de travail. Les groupes de placement du cluster offrent l'avantage d'une faible latence réseau et d'un débit réseau élevé.

La création d'une réserve de capacité dans un groupe de placement du cluster garantit que vous avez accès à la capacité de calcul dans vos groupes de placement du cluster lorsque vous en avez besoin, aussi longtemps que nécessaire. C'est la solution idéale pour réserver de la capacité aux charges de travail à hautes performances (HPC) nécessitant une mise à l'échelle du calcul. Vous pouvez réduire votre cluster tout en veillant à ce que la capacité reste disponible pour votre utilisation afin que vous puissiez la remettre à l'échelle en cas de besoin.

Rubriques

Limites

Gardez les éléments suivants à l'esprit lorsque vous créez des réserves de capacité dans des groupes de placement du cluster :

- Si une réservation de capacité existante ne se trouve pas dans un groupe de placement, vous ne pouvez pas modifier la réservation de capacité pour réserver de la capacité dans un groupe de placement. Pour réserver une capacité dans un groupe de placement, vous devez créer la réserve de capacité dans le groupe de placement.
- Une fois que vous avez créé une réserve de capacité dans un groupe de placement, vous ne pouvez pas la modifier pour réserver la capacité en dehors du groupe de placement.
- Vous pouvez augmenter votre capacité réservée dans un groupe de placement en modifiant une réserve de capacité existante dans le groupe de placement ou en créant des réserves de capacité supplémentaires dans le groupe de placement. Toutefois, vous augmentez vos chances d'obtenir une erreur de capacité insuffisante.
- Vous ne pouvez pas partager de réserves de capacité qui ont été créées dans un groupe de placement du cluster.
- Vous ne pouvez pas supprimer un groupe de placement du cluster qui a des réserves de capacité `active`. Vous devez annuler toutes les réserves de capacité du groupe de placement du cluster avant de pouvoir les supprimer.

Utiliser les réserves de capacité dans des groupes de placement de cluster

Pour commencer à utiliser les réserves de capacité avec des groupes de placement de cluster, effectuez les opérations suivantes.

> **Note**
>
> Si vous souhaitez créer une réserve de capacité dans un groupe de placement de cluster existant, ignorez l'étape 1. Ensuite, pour les étapes 2 et 3, spécifiez le groupe ARN de placement du cluster existant.

Rubriques

Étape 1 : (Conditionnelle) Créer un groupe de placement du cluster pour l'utiliser avec une réserve de capacité

Effectuez cette étape uniquement si vous devez créer un groupe de placement du cluster. Pour utiliser un groupe de placement de clusters existant, ignorez cette étape, puis pour les étapes 2 et 3, utilisez le groupe ARN de placement de clusters de ce groupe.

Vous pouvez créer le groupe de placement du cluster en employant l'une des méthodes suivantes.

Console

Pour créer un groupe de placement du cluster à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Placement Groups Groupes de placement, puis Create placement group (Créer un groupe de placement).
3. Pour Name (Nom), spécifiez un nom descriptif pour le groupe de placement.
4. Pour Placement strategy (Stratégie de placement), choisissez Cluster.
5. Choisissez Créer un groupe.
6. Dans le tableau Groupes de placement, dans la ARN colonne Groupe, notez le groupe ARN de placement de clusters que vous avez créé. Vous en aurez besoin pour la prochaine étape.

AWS CLI

Pour créer un groupe de placement de clusters à l'aide du AWS CLI

Utilisez la create-placement-groupcommande. Pour `--group-name`, spécifiez un nom descriptif pour le groupe de placement et pour `--strategy`, spécifiez `cluster`.

L'exemple suivant crée un groupe de placement nommé `MyPG` qui utilise la stratégie de placement `cluster`.

```
aws ec2 create-placement-group \
```

```
    --group-name MyPG \
    --strategy cluster
```

Notez le groupe de placement ARN renvoyé dans la sortie de commande, car vous en aurez besoin pour l'étape suivante.

Étape 2 : Créer une réserve de capacité dans un groupe de placement du cluster

Vous créez une réserve de capacité dans un groupe de placement du cluster de la même manière que vous créez n'importe quelle réserve de capacité. Cependant, vous devez également spécifier le groupe ARN de placement du cluster dans lequel créer la réservation de capacité. Pour de plus amples informations, veuillez consulter Créer une Réservation de capacité.

Considérations

- Le groupe de placement du cluster spécifié doit être en état `available`. Si le groupe de placement du cluster se trouve en état `pending`, `deleting` ou `deleted`, la demande échoue.
- La réserve de capacité et le groupe de placement du cluster doivent se trouver dans la même zone de disponibilité. Si la demande de création de la réserve de capacité spécifie une zone de disponibilité différente de celle du groupe de placement du cluster, la demande échoue.
- Vous pouvez créer des réserves de capacité uniquement pour les types d'instance pris en charge par les groupes de placement du cluster. Si vous spécifiez un type d'instance non pris en charge, la demande échoue.
- Si vous créez une réservation de `open` capacité dans un groupe de placement de cluster et que certaines instances en cours d'exécution possèdent des attributs correspondants (groupe de placementARN, type d'instance, zone de disponibilité, plate-forme et location), ces instances s'exécutent automatiquement dans la réservation de capacité.
- Votre demande de création d'une Réservation de capacité peut échouer si l'une des situations suivantes se produit :
  - Amazon EC2 ne dispose pas de capacités suffisantes pour répondre à la demande. Réessayez ultérieurement, essayez une zone de disponibilité différente ou essayez une capacité moins importante. Si votre charge de travail tolère plusieurs types et tailles d'instance, essayez des attributs d'instance différents.
  - La quantité demandée dépasse votre limite d'instance à la demande pour la famille de·l'instance sélectionnée. Augmentez votre limite d'instance à la demande pour la famille de·l'instance requise et réessayez. Pour plus d'informations, consultez Quotas des instances à la demande.

Vous pouvez créer la réserve de capacité dans le groupe de placement du cluster en employant l'une des méthodes suivantes.

Console

Pour créer une Réservation de capacité à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Choisissez Réserves de capacité, puis Créer Réserve de capacité.
3. Sur la page Créer une réservation de capacité, spécifiez le type d'instance, la plate-forme, la zone de disponibilité, la location, la quantité et la date de fin selon les besoins.
4. Pour Groupe de placement, sélectionnez le groupe ARN de placement du cluster dans lequel vous souhaitez créer la réservation de capacité.
5. Sélectionnez Create (Créer).

Pour de plus amples informations, veuillez consulter Créer une Réservation de capacité.

AWS CLI

Pour créer une réservation de capacité à l'aide du AWS CLI

Utilisez la create-capacity-reservationcommande. Pour`--placement-group-arn`, spécifiez le groupe ARN de placement du cluster dans lequel créer la réservation de capacité.

```
$ aws ec2 create-capacity-reservation \
    --instance-type instance_type \
    --instance-platform platform \
    --availability-zone az \
    --instance-count quantity \
    --placement-group-arn placement_group_ARN
```

Pour de plus amples informations, veuillez consulter Créer une Réservation de capacité.

Étape 3 : Lancer des instances dans un groupe de placement du cluster

Vous lancez une instance dans une réserve de capacité dans un groupe de placement de cluster de la même manière que vous lancez une instance dans n'importe quelle réserve de capacité. Cependant, vous devez également spécifier le groupe ARN de placement du cluster dans lequel

lancer l'instance. Pour de plus amples informations, veuillez consulter Créer une Réservation de capacité.

Considérations

- Si la réserve de capacité est open, vous n'avez pas besoin de spécifier la réserve de capacité dans la demande de lancement de l'instance. Si l'instance possède des attributs (groupe de placementARN, type d'instance, zone de disponibilité, plateforme et location) qui correspondent à une réservation de capacité dans le groupe de placement spécifié, l'instance s'exécute automatiquement dans la réservation de capacité.
- Si la réserve de capacité accepte uniquement les lancements d'instances ciblées, vous devez spécifier la réserve de capacité cible en plus du groupe de placement du cluster dans la demande.
- Si la réserve de capacité fait partie d'un groupe de réserve de capacité, vous devez spécifier le groupe de réserve de capacité cible en plus du groupe de placement du cluster dans la demande. Pour plus d'informations, consultez Groupes de réserve de capacité.

Vous pouvez lancer une instance dans une réserve de capacité d'un groupe de placement du cluster en employant l'une des méthodes suivantes.

Console

Pour lancer des instances dans une Réservation de capacité existante à l'aide de la console

1. Suivez la procédure pour lancer une instance, mais ne lancez pas l'instance tant que vous n'avez pas effectué les étapes suivantes pour spécifier les paramètres du groupe de placement et de la réservation de capacité.
2. Développez les informations avancées et procédez comme suit :

   a. Pour Groupe de placement, sélectionnez le groupe de placement du cluster dans lequel vous souhaitez lancer l'instance.

   b. Pour Capacity Reservation (Réserve de capacité), choisissez l'une des options suivantes en fonction de la configuration de la réserve de capacité :

      - Ouvert : pour lancer les instances dans n'importe quelle réservation de open capacité du groupe de placement du cluster qui possède les attributs correspondants et une capacité suffisante.
      - Cibler par ID : pour lancer les instances dans une réservation de capacité qui n'accepte que les lancements d'instances ciblés.

- Cibler par groupe — Pour lancer les instances dans n'importe quelle réservation de capacité avec les attributs correspondants et la capacité disponible dans le groupe de réservation de capacité sélectionné.

3. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance). Pour de plus amples informations, veuillez consulter Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console.

Pour de plus amples informations, veuillez consulter Lancer des instances dans une Réservation de capacité existante.

AWS CLI

Pour lancer des instances dans une réservation de capacité existante à l'aide du AWS CLI

Utilisez la commande run-instances. Si vous devez cibler une réserve de capacité spécifique ou un groupe réserve de capacité spécifique, spécifiez le paramètre `--capacity-reservation-specification`. Pour `--placement`, spécifiez le paramètre `GroupName`, puis indiquez le nom du groupe de placement que vous avez créé lors des étapes précédentes.

La commande suivante lance une instance dans une réserve de capacité `targeted` d'un groupe de placement du cluster.

```
$ aws ec2 run-instances \
    --image-id ami_id \
    --count quantity \
    --instance-type instance_type \
    --key-name key_pair_name \
    --subnet-id subnetid \
    --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=capacity_reservation_id} \
    --placement "GroupName=cluster_placement_group_name"
```

Pour plus d'informations, consultez Lancer des instances dans une Réservation de capacité existante.

Réservations de capacité dans Local Zones

Une zone locale est une extension d'une AWS région géographiquement proche de vos utilisateurs. Ainsi, les ressources créées dans une zone locale peuvent servir les utilisateurs locaux avec des communications à très faible latence. Pour plus d'informations, consultez Local Zones AWS.

Vous pouvez étendre une zone VPC depuis sa AWS région parente vers une zone locale en créant un nouveau sous-réseau dans cette zone locale. Lorsque vous créez un sous-réseau dans une zone locale, le vôtre VPC est étendu à cette zone locale. Le sous-réseau de la zone locale fonctionne de la même manière que les autres sous-réseaux de votre. VPC

En utilisant des Local Zones, vous pouvez placer des réservations de capacité dans plusieurs emplacements qui sont plus proches de vos utilisateurs. Vous créez et utilisez des réservations de capacité dans Local Zones de la même manière que vous créez et utilisez des réservations de capacité dans les zones de disponibilité standard. Les fonctionnalités et le comportement de correspondance d'instance sont les mêmes. Pour plus d'informations sur les modèles de tarification pris en charge dans les zones locales, consultez la section Zones AWS locales FAQs.

Considérations

Vous ne pouvez pas utiliser de groupes de réservation de capacité dans une zone locale.

Pour utiliser une réservation de capacité dans une zone locale

1. Activez la zone locale pour l'utiliser dans votre AWS compte. Pour plus d'informations, consultez la section Getting Started with AWS Local Zones dans le guide de l'utilisateur des zones AWS locales.
2. Créez une réservation de capacité dans la zone locale. Pour Zone de disponibilité, sélectionnez la zone locale. La zone locale est représentée par un code de AWS région suivi d'un identifiant indiquant l'emplacement, par exemple`us-west-2-lax-1a`. Pour de plus amples informations, veuillez consulter Créer une Réservation de capacité.
3. Créez un sous-réseau dans la zone locale. Pour Zone de disponibilité, sélectionnez la zone locale. Pour plus d'informations, consultez la section Créer un sous-réseau VPC dans votre manuel Amazon VPC User Guide.
4. Lancez une instance. Pour Sous-réseau, sélectionnez le sous-réseau dans la zone locale (par exemple, `subnet-123abc | us-west-2-lax-1a`) et, pour Réservation de capacité, sélectionnez la spécification (`open` ou ciblez-la par ID) requise pour la réservation de capacité que vous avez créée dans la zone locale. Pour plus d'informations, consultez Lancer des instances dans une Réservation de capacité existante.

Réservations de capacité dans les zones Wavelength

AWS Wavelength permet aux développeurs de créer des applications qui offrent des latences ultra-faibles aux appareils mobiles et aux utilisateurs finaux. Wavelength déploie des services de calcul et de stockage AWS standard à la périphérie des réseaux 5G des opérateurs de télécommunications. Vous pouvez étendre un Amazon Virtual Private Cloud (VPC) à une ou plusieurs zones de Wavelength. Vous pouvez ensuite utiliser AWS des ressources telles que EC2 les instances Amazon pour exécuter des applications nécessitant une latence très faible et une connexion aux AWS services de la région. Pour plus d'informations, consultez la section Zones AWS Wavelength.

Lorsque vous créez des réservations de capacité à la demande, vous pouvez choisir la zone Wavelength et lancer des instances Réservation de capacité dans une zone Wavelength en spécifiant le sous-réseau associé à la zone Wavelength. Une zone Wavelength est représentée par un code de Région AWS suivi d'un identifiant qui indique l'emplacement, par exemple, `us-east-1-wl1-bos-wlz-1`.

Les zones Wavelength ne sont pas disponibles dans toutes les régions. Pour plus d'informations sur les régions qui prennent en charge les zones Wavelength, consultez Zones Wavelength disponibles dans le Guide du développeur AWS Wavelength .

Considérations

Vous ne pouvez pas utiliser de groupes de Réservation de capacité dans une zone Wavelength.

Pour utiliser une Réservation de capacité dans une zone Wavelength

1. Activez la Wavelength Zone pour l'utiliser dans votre AWS compte. Pour plus d'informations, consultez Mise en route avec AWS Wavelength dans le Guide du développeur AWS Wavelength .
2. Créez une Réservation de capacité dans la zone Wavelength. Pour Zone de disponibilité, sélectionnez une Wavelength. La Wavelength est représentée par un code de AWS région suivi d'un identifiant indiquant l'emplacement, par exemple`us-east-1-wl1-bos-wlz-1`. Pour de plus amples informations, veuillez consulter Créer une Réservation de capacité.
3. Créez un sous-réseau dans la zone Wavelength. Pour Zone de disponibilité, sélectionnez une zone Wavelength. Pour plus d'informations, consultez la section Créer un sous-réseau VPC dans votre manuel Amazon VPC User Guide.
4. Lancez une instance. Pour Sous-réseau, sélectionnez le sous-réseau dans la zone Wavelength (par exemple, `subnet-123abc | us-east-1-wl1-bos-wlz-1`) et, pour Réservation de

capacité, sélectionnez la spécification (open ou ciblez-la par ID) requise pour la Réservation de capacité que vous avez créée dans Wavelength. Pour de plus amples informations, veuillez consulter Lancer des instances dans une Réservation de capacité existante.

Réservations de capacité sur AWS Outposts

AWS Outposts est un service entièrement géré qui étend AWS l'infrastructureAPIs, les services et les outils aux locaux du client. En fournissant un accès local à l'infrastructure AWS gérée, il AWS Outposts permet aux clients de créer et d'exécuter des applications sur site en utilisant les mêmes interfaces de programmation que dans AWS les régions, tout en utilisant les ressources de calcul et de stockage locales pour réduire la latence et les besoins de traitement des données locaux.

Un avant-poste est un pool de capacités de AWS calcul et de stockage déployé sur le site d'un client. AWS exploite, surveille et gère cette capacité dans le cadre d'une AWS région.

Vous pouvez créer des réservations de capacité sur les Outposts que vous avez créés dans votre compte. Cela vous permet de réserver une capacité de calcul sur un outpost de votre site. Vous créez et utilisez des réservations de capacité dans Outposts de la même manière que vous créez et utilisez des réservations de capacité dans les zones de disponibilité standard. Les fonctionnalités et le comportement de correspondance d'instance sont les mêmes.

Vous pouvez également partager les réservations de capacité sur les Outposts avec d'autres AWS comptes de votre organisation à l'aide de. AWS Resource Access Manager Pour plus d'informations sur le partage des réserves de capacité, consultez Réservations de capacité partagée.

Prérequis

Vous devez avoir un outpost installé sur votre site. Pour plus d'informations, consultez Créer un outpost et commander une capacité outpost dans le Guide de l'utilisateur AWS Outposts .

Considérations

- Vous ne pouvez pas utiliser les groupes de réservation de capacité sur un Outpost.

Pour utiliser une réservation de capacité sur un Outpost.

1. Créez un sous-réseau sur l'outpost. Pour plus d'informations, consultez Créer un sous-réseau dans le Guide de l'utilisateur AWS Outposts .
2. Créez une réservation de capacité sur l'outpost.

a. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.

b. Dans le volet de navigation, choisissez Outposts, puis choisissez Actions, Créer une réservation de capacité.

c. Configurez la réservation de capacité selon vos besoins, puis choisissez Créer. Pour plus d'informations, consultez Créer une Réservation de capacité.

> **Note**
>
> La liste déroulante Type d'instance répertorie uniquement les types d'instance pris en charge par l'outpost sélectionné, et la liste déroulante Zone de disponibilité répertorie uniquement la zone de disponibilité à laquelle l'outpost sélectionné est associé.

3. Lancer une instance dans la réservation de capacité. Pour Sous-réseau choisissez le sous-réseau que vous avez créé à l'étape 1 et pour Réservation de capacité, sélectionnez la réservation de capacité que vous avez créée à l'étape 2. Pour plus d'informations, consultez la section Lancer une instance sur votre Outpost du Guide de l'utilisateur AWS Outposts .

Réservations de capacité partagée

Le partage des réservations de capacité permet aux propriétaires des réservations de capacité de partager leur capacité réservée avec d'autres AWS comptes ou au sein d'une AWS organisation. Cela vous permet de créer et de gérer les réservations de capacité de manière centralisée, et de partager la capacité réservée entre plusieurs AWS comptes ou au sein de votre AWS organisation.

Dans ce modèle, le AWS compte propriétaire de la réservation de capacité (propriétaire) la partage avec d'autres AWS comptes (consommateurs). Les consommateurs peuvent lancer des instances dans des réservations de capacité partagées avec eux comme ils le feraient avec des réservations de capacité qu'ils possèderaient dans leur propre compte. Le propriétaire d'une Réservation de capacité est responsable de la gestion de la Réservation de capacité et des instances lancées dans celle-ci. Les propriétaires ne peuvent pas modifier les instances lancées par les consommateurs dans des réservations de capacité qu'ils ont partagées. Les consommateurs sont responsables de la gestion des instances qu'ils lancent dans des réservations de capacité partagées avec eux. Les consommateurs ne peuvent pas voir ou modifier les instances appartenant à d'autres consommateurs ou au propriétaire de la Réservation de capacité.

Un propriétaire de Réservation de capacité peut partager une Réservation de capacité avec :

- AWS Comptes spécifiques à l'intérieur ou à l'extérieur de son AWS organisation
- Une unité organisationnelle au sein de son AWS organisation
- Toute son AWS organisation

Conditions préalables au partage de réservations de capacité

- Pour partager une réservation de capacité, vous devez la posséder dans votre AWS compte. Vous ne pouvez pas partager une Réservation de capacité qui a été partagée avec vous.
- Vous pouvez uniquement partager des réservations de capacité pour les instances de locations partagées. Vous ne pouvez pas partager de réservations de capacité pour les instances de locations dédiées.
- Le partage des réservations de capacité n'est pas disponible pour AWS les nouveaux AWS comptes ou les comptes dont l'historique de facturation est limité.
- Pour partager une réservation de capacité avec votre AWS organisation ou une unité organisationnelle de votre AWS organisation, vous devez activer le partage avec AWS Organizations. Pour plus d'informations, consultez Activation du partage avec AWS Organizations dans le Guide de l'utilisateur AWS RAM .

Services connexes

Le partage des réservations de capacité s'intègre à AWS Resource Access Manager (AWS RAM). AWS RAM est un service qui vous permet de partager vos AWS ressources avec n'importe quel AWS compte ou via AWS Organizations. Avec AWS RAM, vous partagez les ressources que vous possédez en créant un partage de ressources. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées. Les consommateurs peuvent être AWS des comptes individuels, des unités organisationnelles ou l'ensemble d'une organisation AWS Organizations.

Pour plus d'informations AWS RAM, consultez le guide de AWS RAM l'utilisateur.

Partager sur plusieurs zones de disponibilité

Pour garantir que les ressources sont réparties entre les zones de disponibilité d'une région, nous mappons indépendamment les zones de disponibilité aux noms de chaque compte. Cela peut entraîner des différences de nom de zone de disponibilité entre les comptes. Par exemple, il est possible que la zone `us-east-1a` de disponibilité de votre AWS compte ne soit pas la même que celle `us-east-1a` d'un autre AWS compte.

Pour identifier l'emplacement de vos Réservations de capacité par rapport à vos comptes, vous devez utiliser l'ID de zone de disponibilité. L'AZ ID est un identifiant unique et cohérent pour une zone de disponibilité pour tous les AWS comptes. Par exemple, `use1-az1` il s'agit d'un identifiant AZ pour la `us-east-1` région et il s'agit du même emplacement dans tous les AWS comptes.

Pour consulter l'AZ IDs des zones de disponibilité de votre compte

1. Ouvrez la AWS RAM console à l'adresse https://console.aws.amazon.com/ram.
2. L'AZ IDs de la région actuelle s'affiche dans le panneau Your AZ ID sur le côté droit de l'écran.

Partager une Réservation de capacité

Lorsque vous partagez une réservation de capacité dont vous êtes propriétaire avec d'autres personnes Comptes AWS, vous leur permettez de lancer des instances dans la capacité que vous avez réservée. Si vous partagez une Réservation de capacité ouverte, gardez présent à l'esprit les points suivants, car cela pourrait entraîner une utilisation indésirable de la Réservation de capacité :

- Si des consommateurs disposent d'instances en cours d'exécution correspondant aux attributs de la Réservation de capacité, du paramètre `CapacityReservationPreference` défini sur `open` et qu'ils ne procèdent pas à l'exécution dans une capacité réservée, ils utilisent automatiquement la Réservation de capacité partagée.
- Si les consommateurs lancent des instances dont les attributs correspondent (type d'instance, plateforme, zone de disponibilité et location) et dont le `CapacityReservationPreference` paramètre est défini sur`open`, ils se lancent automatiquement dans la réservation de capacité partagée.

Pour partager une Réservation de capacité, vous devez l'ajouter à un partage de ressources. Un partage de ressources est une AWS RAM ressource qui vous permet de partager vos ressources entre différents AWS comptes. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées. Lorsque vous partagez une réservation de capacité à l'aide de la EC2 console Amazon, vous l'ajoutez à un partage de ressources existant. Pour ajouter une réservation de capacité à un nouveau partage de ressources, vous devez créer le partage de ressources avec la console AWS RAM.

Si vous faites partie d'une organisation AWS Organizations et que le partage au sein de votre organisation est activé, les clients de votre organisation ont accès à la réservation de capacité partagée si les conditions préalables au partage sont remplies. Si la réserve de capacité est partagée

avec des comptes externes, ils reçoivent une invitation à rejoindre le partage de ressources et bénéficient d'un accès à la réserve de capacité partagée après avoir accepté l'invitation.

> **Important**
>
> Avant de lancer des instances dans une réservation de capacité partagée avec vous, vérifiez que vous avez accès à la réservation de capacité partagée en la consultant dans la console ou en la décrivant à l'aide de la describe-capacity-reservations AWS CLI commande. Si vous pouvez consulter la réservation de capacité partagée dans la console ou la décrire à l'aide du AWS CLI, elle est disponible pour votre usage et vous pouvez y lancer des instances. Si vous tentez de lancer des instances dans la réserve de capacité et qu'elle n'est pas accessible en raison d'un échec de partage, les instances seront lancées dans la capacité à la demande.

Vous pouvez partager une réservation de capacité dont vous êtes propriétaire à l'aide de la EC2 console Amazon, de la AWS RAM console ou du AWS CLI.

Pour partager une réservation de capacité dont vous êtes propriétaire à l'aide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Réservations de capacité.
3. Choisissez la Réservation de capacité à partager, puis choisissez Actions, Share reservation (Partager une réservation).
4. Sélectionnez le partage de ressources auquel vous souhaitez ajouter la Réservation de capacité, puis choisissez Share Réservation de capacité (Partager la réservation de capacité).

   Les consommateurs peuvent avoir accès à la Réservation de capacité partagée en quelques minutes.

Pour partager une réservation de capacité dont vous êtes propriétaire à l'aide de la AWS RAM console

Consultez Création d'un partage de ressources dans le Guide de l'utilisateur AWS RAM .

Pour partager une réservation de capacité dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez la create-resource-sharecommande.

Arrêter de partager une Réservation de capacité

Le propriétaire d'une Réservation de capacité peut cesser de partager une Réservation de capacité à tout moment. Les règles suivantes s'appliquent :

- Les instances détenues par des clients qui fonctionnaient dans la capacité partagée au moment de l'arrêt du partage continuent de fonctionner normalement en dehors de la capacité réservée, et la capacité est rétablie conformément à la réservation de capacité sous réserve de la disponibilité des EC2 capacités Amazon.
- Les consommateurs avec lesquels la Réservation de capacité était partagée ne peuvent plus lancer de nouvelles instances dans la capacité réservée.

Pour arrêter de partager une Réservation de capacité que vous possédez, vous devez la supprimer du partage de ressources. Vous pouvez le faire à l'aide de la EC2 console Amazon, de la AWS RAM console ou du AWS CLI.

Pour arrêter de partager une réservation de capacité dont vous êtes propriétaire à l'aide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Réservations de capacité.
3. Sélectionnez la Réservation de capacité et choisissez l'onglet Sharing (Partage).
4. L'onglet Sharing (Partage) affiche la liste des partages de ressources auxquels la Réservation de capacité a été ajoutée. Sélectionnez le partage de ressources duquel vous souhaitez supprimer la Réservation de capacité, puis choisissez Remove from resource share (Supprimer du partage de ressources).

Pour arrêter de partager une réservation de capacité dont vous êtes propriétaire à l'aide de la AWS RAM console

Consultez Mise à jour d'un partage de ressources dans le Guide de l'utilisateur AWS RAM .

Pour arrêter de partager une réservation de capacité dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez la disassociate-resource-sharecommande.

Autorisations relatives à une Réservation de capacité partagée

Autorisations accordées aux propriétaires

Les propriétaires sont responsables de la gestion et de l'annulation de leurs réservations de capacité partagées. Les propriétaires ne peuvent pas modifier des instances appartenant à d'autres comptes et en cours d'exécution dans la Réservation de capacité. Les propriétaires sont responsables de la gestion des instances qu'ils lancent dans la Réservation de capacité partagée.

Autorisations accordées aux consommateurs

Les consommateurs sont responsables de la gestion de leurs instances exécutées dans la Réservation de capacité partagée. Les consommateurs ne peuvent pas modifier la Réservation de capacité partagée. Ils ne peuvent pas non plus afficher ou modifier des instances qui appartiennent à d'autres consommateurs ou au propriétaire de la Réservation de capacité.

Facturation et mesures

Le partage de réservations de capacité n'entraîne pas de frais supplémentaires.

Le propriétaire de la Réservation de capacité est facturé pour les instances qu'il exécute dans la Réservation de capacité et pour la capacité réservée non utilisée. Les consommateurs sont facturés pour les instances qu'ils exécutent dans la Réservation de capacité partagée.

Si le propriétaire de la réserve de capacité appartient à un autre compte payeur et que la réserve de capacité est couverte par une instance régionale réservée ou un Savings Plan, le propriétaire de la réserve de capacité continue d'être facturé pour l'instance régionale réservée ou le Savings Plan. Dans ces cas, le propriétaire de la réserve de capacité paie pour l'instance réservée régionale ou le Savings Plan et les consommateurs sont facturés pour les instances qu'ils exécutent dans la réserve de capacité partagée.

Limites d'instance

Toute utilisation d'une Réservation de capacité est prise en compte par rapport aux limites instance à la demande du propriétaire de la Réservation de capacité. Cela comprend :

- La capacité réservée non utilisée
- L'utilisation par des instances qui appartiennent au propriétaire de la Réservation de capacité
- L'utilisation par des instances qui appartiennent aux consommateurs

Les instances lancées dans la capacité partagée par des consommateurs sont prises en compte par rapport à la limite instance à la demande du propriétaire de la Réservation de capacité. Les limites d'instance des consommateurs sont égales à la somme de leurs propres limites instance à la demande et de la capacité disponible dans les réservations de capacité partagées auxquelles ils ont accès.

Flottes de réservation de capacité

Une flotte de réservation de capacité à la demande est un groupe de réservations de capacité.

Une demande de flotte de réservation de capacité contient toutes les informations de configuration nécessaires pour lancer une flotte de réservation de capacité. À l'aide d'une seule demande, vous pouvez réserver de grandes quantités de EC2 capacité Amazon pour votre charge de travail sur plusieurs types d'instances, jusqu'à une capacité cible que vous spécifiez.

Après avoir créé une flotte de réservation de capacité, vous pouvez gérer collectivement les réservations de capacité de la flotte en modifiant ou en annulant la flotte de réservation de capacité.

Rubriques

Fonctionnement de flottes de réservation de capacité

Lorsque vous créez une flotte de réservation de capacité, celle-ci tente de créer des réservations de capacité individuelles pour atteindre la capacité cible totale que vous avez spécifiée dans la demande de la flotte.

Le nombre d'instances pour lesquelles la flotte réserve de la capacité dépend de la capacité cible totale et des pondérations du type d'instance que vous spécifiez. Le type d'instance pour lequel il réserve la capacité dépend de la stratégie d'allocation et des priorités de type d'instance que vous utilisez.

Si la capacité est insuffisante au moment de la création de la flotte et qu'elle n'est pas en mesure d'atteindre immédiatement sa capacité cible totale, elle tente de manière asynchrone de créer des réservations de capacité jusqu'à ce qu'elle ait réservé la quantité de capacité demandée.

Lorsque la flotte atteint sa capacité cible totale, elle tente de maintenir cette capacité. Si une réservation de capacité de la flotte est annulée, celle-ci crée automatiquement une ou plusieurs réservations de capacité, selon la configuration de votre flotte, pour remplacer la capacité perdue et maintenir sa capacité cible totale.

Les réservations de capacité dans la flotte ne peuvent pas être gérées individuellement. Elles doivent être gérées collectivement en modifiant la flotte. Lorsque vous modifiez une flotte, les réservations de capacité de celle-ci sont automatiquement mises à jour pour refléter les changements.

Actuellement, les flottes de réservation de capacité prennent en charge le critère de correspondance d'instance `open`, et toutes les réservations de capacité lancées par une flotte utilisent automatiquement ce critère de correspondance d'instance. Avec ce critère, les nouvelles instances et les instances existantes dont les attributs correspondent (type d'instance, plateforme, zone de disponibilité et location) s'exécutent automatiquement dans les réservations de capacité créées par une flotte. Les flottes de réservation de capacité ne prennent pas en charge les critères de correspondance des instances `target`.

Considérations

Gardez les points suivants à l'esprit lorsque vous travaillez avec des flottes de réservation de capacité :

- Une flotte de réservation de capacité peut être créée, modifiée, consultée et annulée à l'aide du AWS CLI et AWS API.
- Les réservations de capacité dans une flotte ne peuvent pas être gérées individuellement. Elles doivent être gérées collectivement en modifiant ou en annulant la flotte.
- Une flotte de réservation de capacité ne peut pas s'étendre sur plusieurs régions.
- Une flotte de réservation de capacité ne peut pas s'étendre sur plusieurs zones de disponibilité.
- Les réservations de capacité créées par une flotte de réservation de capacité sont automatiquement étiquetées avec le tag AWS généré suivant :

- Clé : `aws:ec2-capacity-reservation-fleet`
- Valeur : *`fleet_id`*

Vous pouvez utiliser cette identification pour identifier les réservations de capacité qui ont été créées par une flotte de réservation de capacité.

Tarification

L'utilisation des flottes de réservation de capacité ne donne lieu à aucun frais supplémentaire. Vous êtes facturé pour les réservations de capacité individuelles créées par vos flottes de réservation de capacité. Pour plus d'informations sur la façon dont les réservations de capacité sont facturées, consultez Tarification et facturation d'une Réservation de capacité.

Réservation de capacité : concepts et planification de la flotte

Les informations suivantes décrivent comment planifier une flotte de réservation de capacité et décrivent les concepts de flotte de réservation de capacité, notamment la capacité cible totale, la stratégie d'allocation, le poids du type d'instance et la priorité du type d'instance.

Rubriques

- Planifier une flotte de réservation de capacité
- Capacité cible totale
- Stratégie d'allocation
- Pondération du type d'instance
- Priorité de type d'instance

Planifier une flotte de réservation de capacité

Lorsque vous planifiez votre flotte de réservation de capacité, nous vous recommandons de procéder comme suit :

1. Déterminez la quantité de capacité de calcul nécessaire à votre charge de travail.
2. Décidez des types d'instance et des zones de disponibilité que vous voulez utiliser.
3. Attribuez à chaque type d'instance une priorité en fonction de vos besoins et de vos préférences. Pour plus d'informations, consultez Priorité de type d'instance.

4. Créez un système de pondération de la capacité qui a du sens pour votre charge de travail. Attribuez un poids à chaque type d'instance et déterminez votre capacité cible totale. Pour plus d'informations, consultez Pondération du type d'instance et Capacité cible totale.
5. Déterminez si vous avez besoin de la réservation de capacité indéfiniment ou seulement pour une période de temps spécifique.

Capacité cible totale

La capacité cible totale définit la quantité totale de capacité de calcul que la flotte de réservation de capacité réserve. Vous spécifiez la capacité cible totale lorsque vous créez la flotte de réservation de capacité. Une fois la flotte créée, Amazon crée EC2 automatiquement des réservations de capacité pour réserver des capacités jusqu'à la capacité cible totale.

Le nombre d'instances pour lesquelles la flotte de réservation de capacité réserve de la capacité est déterminé par la capacité cible totale et la pondération du type d'instance que vous spécifiez pour chaque type d'instance dans la flotte de réservation de capacité (`total target capacity/instance type weight=number of instances`).

Vous pouvez attribuer une capacité cible totale en fonction d'unités significatives pour votre charge de travail. Par exemple, si votre charge de travail nécessite un certain nombre devCPUs, vous pouvez attribuer la capacité cible totale en fonction du nombre de capacités vCPUs requises. Si votre charge de travail l'exige `2048`vCPUs, spécifiez une capacité cible totale de, `2048` puis attribuez des pondérations aux types d'instance en fonction du nombre de types d'instances vCPUs fournis par les types d'instances de la flotte. Pour obtenir un exemple, consultez Pondération du type d'instance.

Stratégie d'allocation

La stratégie d'allocation de votre flotte de réservation de capacité détermine comment elle répond à votre demande de capacité réservée à partir des spécifications du type d'instance dans la configuration de la flotte de réservation de capacité.

Actuellement, seule la stratégie d'allocation `prioritized` est prise en charge. Avec cette stratégie, la flotte de réservation de capacité crée des réservations de capacité en utilisant les priorités que vous avez assignées à chacune des spécifications de type d'instance dans la configuration de la flotte de réservation de capacité. Les valeurs de priorité inférieures indiquent une priorité d'utilisation plus élevée. Par exemple, supposons que vous créez une flotte de réservation de capacité qui utilise les types d'instance et les priorités suivants :

- `m4.16xlarge` — priorité = 1

- m5.16xlarge — priorité = 3
- m5.24xlarge — priorité = 2

La flotte tente d'abord de créer des réservations de capacité pour m4.16xlarge. Si la m4.16xlarge capacité EC2 d'Amazon est insuffisante, la flotte tente de créer des réservations de capacité pourm5.24xlarge. Si la m5.24xlarge capacité EC2 d'Amazon est insuffisante, la flotte crée des réservations de capacité pourm5.16xlarge.

Pondération du type d'instance

La pondération du type d'instance est une pondération que vous attribuez à chaque type d'instance dans la flotte de réservation de capacité. La pondération détermine combien d'unités de capacité chaque instance de ce type d'instance spécifique compte pour la capacité cible totale de la flotte.

Vous pouvez attribuer des pondérations en fonction des unités qui sont significatives pour votre charge de travail. Par exemple, si votre charge de travail nécessite un certain nombre devCPUs, vous pouvez attribuer des pondérations en fonction du nombre vCPUs fourni par chaque type d'instance dans le parc de réservations de capacité. Dans ce cas, si vous créez une flotte de réservation de capacité à l'aide d'm5.24xlargeinstances m4.16xlarge et, vous devez attribuer des pondérations correspondant au nombre de vCPUs pour chaque instance comme suit :

- m4.16xlarge— 64vCPUs, poids = 64 unités
- m5.24xlarge— 96vCPUs, poids = 96 unités

La pondération du type d'instance détermine le nombre d'instances pour lesquelles la flotte de réservation de capacité réserve de la capacité. Par exemple, si une flotte de réservation de capacité ayant une capacité cible totale de 384 unités utilise les types d'instance et les pondérations de l'exemple précédent, la flotte pourrait réserver une capacité pour 6 m4.16xlarge instances (384 capacité cible totale/64 pondération du type d'instance=6 instances), ou 4 m5.24xlarge instances (384 / 96 = 4).

Si vous n'attribuez pas de pondération aux types d'instance, ou si vous attribuez une pondération de type d'instance de 1, la capacité cible totale est basée uniquement sur le nombre d'instances. Par exemple, si une flotte de réservation de capacité ayant une capacité cible totale de 384 unités utilise les types d'instances de l'exemple précédent, mais omet les pondérations ou spécifie une pondération de 1 pour les deux types d'instances, la flotte pourrait réserver une capacité pour 384 m4.16xlarge instances ou 384 m5.24xlarge instances.

Priorité de type d'instance

La priorité de type d'instance est une valeur que vous attribuez aux types d'instance de la flotte. Les priorités sont utilisées pour déterminer lequel des types d'instance spécifiés pour la flotte doit être utilisé en priorité.

Les valeurs de priorité inférieures indiquent une priorité d'utilisation plus élevée.

Création d'une flotte de réservation de capacité

Lorsque vous créez une flotte de réservation de capacité, elle crée automatiquement des réservations de capacité pour les types d'instance spécifiés dans la demande de flotte, jusqu'à la capacité cible totale spécifiée. Le nombre d'instances pour lesquelles la flotte de réservation de capacité réserve de la capacité dépend de la capacité cible totale et des pondérations de type d'instance que vous spécifiez dans la demande. Pour plus d'informations, consultez Pondération du type d'instance et Capacité cible totale.

Lorsque vous créez la flotte, vous devez spécifier les types d'instance à utiliser et une priorité pour chacun de ces types d'instance. Pour plus d'informations, consultez Stratégie d'allocation et Priorité de type d'instance.

> **Note**
>
> Le rôle AWSServiceRoleForEC2CapacityReservationFleetlié au service est automatiquement créé dans votre compte la première fois que vous créez une flotte de réservation de capacité. Pour de plus amples informations, veuillez consulter Utilisation des rôles liés à un service pour la flotte de réserve de capacité.

Actuellement, les flottes de réservation de capacité ne prennent en charge que les critères de correspondance de l'instance `open`.

Pour créer une flotte de réservation de capacité

Utilisez la create-capacity-reservation-fleet AWS CLI commande.

```
aws ec2 create-capacity-reservation-fleet \
--total-target-capacity capacity_units \
--allocation-strategy prioritized \
--instance-match-criteria open \
--tenancy dedicated|default \
```

```
--end-date yyyy-mm-ddThh:mm:ss.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

Voici le contenu de `instanceTypeSpecification.json`.

```
[
    {
        "InstanceType": "instance_type",
        "InstancePlatform":"platform",
        "Weight": instance_type_weight,
        "AvailabilityZone":"availability_zone",
        "AvailabilityZoneId" : "az_id",
        "EbsOptimized": true|false,
        "Priority" : instance_type_priority
    }
]
```

Sortie attendue.

```
{
    "Status": "status",
    "TotalFulfilledCapacity": fulfilled_capacity,
    "CapacityReservationFleetId": "cr_fleet_id",
    "TotalTargetCapacity": capacity_units
}
```

Exemple

```
aws ec2 create-capacity-reservation-fleet \
--total-target-capacity 24 \
--allocation-strategy prioritized \
--instance-match-criteria open \
--tenancy default \
--end-date 2021-12-31T23:59:59.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

`instanceTypeSpecification.json`

```
[
  {
    "InstanceType": "m5.xlarge",
    "InstancePlatform": "Linux/UNIX",
```

```
    "Weight": 3.0,
    "AvailabilityZone":"us-east-1a",
    "EbsOptimized": true,
    "Priority" : 1
  }
]
```

Exemple de sortie.

```
{
    "Status": "submitted",
    "TotalFulfilledCapacity": 0.0,
    "CapacityReservationFleetId": "crf-abcdef01234567890",
    "TotalTargetCapacity": 24
}
```

Affichage d'une flotte de réservation de capacité

Vous pouvez afficher les informations de configuration et de capacité d'une flotte de réservation de capacité à tout moment. L'affichage d'une flotte fournit également des détails sur les réservations de capacité individuelles qui se trouvent dans la flotte.

Pour afficher une flotte de réservation de capacité

Utilisez la describe-capacity-reservation-fleets AWS CLI commande.

```
aws ec2 describe-capacity-reservation-fleets \
--capacity-reservation-fleet-ids cr_fleet_ids
```

Voici un exemple de sortie.

```
{
    "CapacityReservationFleets": [
        {
            "Status": "status",
            "EndDate": "yyyy-mm-ddThh:mm:ss.000Z",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "CapacityReservationFleetId": "cr_fleet_id",
            "Tenancy": "dedicated|default",
            "InstanceTypeSpecifications": [
                {
                    "CapacityReservationId": "cr1_id",
```

```
                    "AvailabilityZone": "cr1_availability_zone",
                    "FulfilledCapacity": cr1_used_capacity,
                    "Weight": cr1_instance_type_weight,
                    "CreateDate": "yyyy-mm-ddThh:mm:ss.000Z",
                    "InstancePlatform": "cr1_platform",
                    "TotalInstanceCount": cr1_number of instances,
                    "Priority": cr1_instance_type_priority,
                    "EbsOptimized": true|false,
                    "InstanceType": "cr1_instance_type"
                },
    {
                    "CapacityReservationId": "cr2_id",
                    "AvailabilityZone": "cr2_availability_zone",
                    "FulfilledCapacity": cr2_used_capacity,
                    "Weight": cr2_instance_type_weight,
                    "CreateDate": "yyyy-mm-ddThh:mm:ss.000Z",
                    "InstancePlatform": "cr2_platform",
                    "TotalInstanceCount": cr2_number of instances,
                    "Priority": cr2_instance_type_priority,
                    "EbsOptimized": true|false,
                    "InstanceType": "cr2_instance_type"
                },
            ],
            "TotalTargetCapacity": total_target_capacity,
            "TotalFulfilledCapacity": total_target_capacity,
            "CreateTime": "yyyy-mm-ddThh:mm:ss.000Z",
            "AllocationStrategy": "prioritized"
        }
    ]
}
```

Exemple

```
aws ec2 describe-capacity-reservation-fleets \
--capacity-reservation-fleet-ids crf-abcdef01234567890
```

Voici un exemple de sortie.

```
{
    "CapacityReservationFleets": [
        {
            "Status": "active",
            "EndDate": "2021-12-31T23:59:59.000Z",
```

```
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "CapacityReservationFleetId": "crf-abcdef01234567890",
            "Tenancy": "default",
            "InstanceTypeSpecifications": [
                {
                    "CapacityReservationId": "cr-1234567890abcdef0",
                    "AvailabilityZone": "us-east-1a",
                    "FulfilledCapacity": 5.0,
                    "Weight": 1.0,
                    "CreateDate": "2021-07-02T08:34:33.398Z",
                    "InstancePlatform": "Linux/UNIX",
                    "TotalInstanceCount": 5,
                    "Priority": 1,
                    "EbsOptimized": true,
                    "InstanceType": "m5.xlarge"
                }
            ],
            "TotalTargetCapacity": 5,
            "TotalFulfilledCapacity": 5.0,
            "CreateTime": "2021-07-02T08:34:33.397Z",
            "AllocationStrategy": "prioritized"
        }
    ]
}
```

États des flottes de réservation de capacité

Une flotte de réservation de capacité peut se trouver dans l'un des états suivants :

- `submitted`— La demande de flotte de réservation de capacité a été soumise et Amazon EC2 se prépare à créer les réservations de capacité.
- `modifying` — La flotte de réservation de capacité est en cours de modification. La flotte reste dans cet état jusqu'à ce que la modification soit terminée.
- `active` — La flotte de réservation de capacité a atteint sa capacité cible totale et tente de maintenir cette capacité. La flotte reste dans cet état jusqu'à ce qu'elle soit modifiée ou supprimée.
- `partially_fulfilled` — La flotte de réservation de capacité a partiellement atteint sa capacité cible totale. La EC2 capacité Amazon est insuffisante pour atteindre la capacité cible totale. La flotte tente de remplir de manière asynchrone sa capacité cible totale.
- `expiring` — La flotte de réservation de capacité a atteint sa date de fin et est en train d'expirer. Une ou plusieurs de ses réservations de capacité peuvent encore être actives.

- `expired` — La flotte de réservation de capacité a atteint sa date d'expiration. La flotte et ses réservations de capacité sont expirées. La flotte ne peut pas créer de nouvelles réservations de capacité.
- `cancelling` — La flotte de réservation de capacité est en cours d'annulation. Une ou plusieurs de ses réservations de capacité peuvent encore être actives.
- `cancelled` — La flotte de réservation de capacité a été annulée manuellement. La flotte et ses réservations de capacité sont annulées et la flotte ne peut pas créer de nouvelles réservations de capacité.
- `failed` — La flotte de réservation de capacité n'a pas réussi à réserver de la capacité pour les types d'instance spécifiés.

Modification d'une flotte de réservation de capacité

Vous pouvez modifier la capacité cible totale et la date d'une flotte de réservation de capacité à tout moment. Lorsque vous modifiez la capacité totale cible d'une flotte de réservation de capacité, la flotte crée automatiquement de nouvelles réservations de capacité, ou modifie ou annule les réservations de capacité existantes dans la flotte pour répondre à la nouvelle capacité totale cible. Lorsque vous modifiez la date de fin de la flotte, les dates de fin de toutes les réservations de capacité individuelles sont mises à jour en conséquence.

Après avoir modifié une flotte, son statut passe à `modifying`. Vous ne pouvez pas tenter d'apporter d'autres modifications à une flotte lorsqu'elle se trouve dans l'état `modifying`.

Vous ne pouvez pas modifier la location, la zone de disponibilité, les types d'instance, les plateformes d'instance, les priorités ou les pondérations utilisées par une flotte de réservation de capacité. Si vous devez modifier l'un de ces paramètres, vous devrez peut-être annuler la flotte existante et en créer une nouvelle avec les paramètres requis.

Pour modifier une flotte de réservation de capacité

Utilisez la modify-capacity-reservation-fleet AWS CLI commande.

> **Note**
>
> Vous ne pouvez pas spécifier `--end-date` et `--remove-end-date` dans la même commande.

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id cr_fleet_ids \
--total-target-capacity capacity_units \
--end-date yyyy-mm-ddThh:mm:ss.000Z \
--remove-end-date
```

Voici un exemple de sortie.

```
{
    "Return": true
}
```

Exemple : Modifier la capacité cible totale

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id crf-01234567890abcedf \
--total-target-capacity 160
```

Exemple : Modifier la date de fin

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id crf-01234567890abcedf \
--end-date 2021-07-04T23:59:59.000Z
```

Exemple : Supprimer la date de fin

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id crf-01234567890abcedf \
--remove-end-date
```

Voici un exemple de sortie.

```
{
    "Return": true
}
```

Annulation d'une flotte de réservation de capacité

Lorsque vous n'avez plus besoin d'une flotte de réservation de capacité et de la capacité qu'elle réserve, vous pouvez l'annuler. Lorsque vous annulez une flotte, son statut passe à `cancelled` et

elle ne peut plus créer de nouvelles réservations de capacité. De plus, toutes les réservations de capacité individuelles de la flotte sont annulées. Les instances qui s'exécutaient auparavant dans la capacité réservée continuent de fonctionner normalement dans la capacité partagée.

Pour annuler une flotte de réservation de capacité

Utilisez la cancel-capacity-reservation-fleets AWS CLI commande.

```
aws ec2 cancel-capacity-reservation-fleets \
--capacity-reservation-fleet-ids cr_fleet_ids
```

Voici un exemple de sortie.

```
{
    "SuccessfulFleetCancellations": [
        {
            "CurrentFleetState": "state",
            "PreviousFleetState": "state",
            "CapacityReservationFleetId": "cr_fleet_id_1"
        },
        {
            "CurrentFleetState": "state",
            "PreviousFleetState": "state",
            "CapacityReservationFleetId": "cr_fleet_id_2"
        }
    ],
    "FailedFleetCancellations": [
        {
         "CapacityReservationFleetId": "cr_fleet_id_3",
         "CancelCapacityReservationFleetError": [
             {
              "Code": "code",
                    "Message": "message"
          }
         ]
     }
    ]
}
```

Exemple : Annulation réussie

```
aws ec2 cancel-capacity-reservation-fleets \
```

```
--capacity-reservation-fleet-ids crf-abcdef01234567890
```

Voici un exemple de sortie.

```
{
    "SuccessfulFleetCancellations": [
        {
            "CurrentFleetState": "cancelling",
            "PreviousFleetState": "active",
            "CapacityReservationFleetId": "crf-abcdef01234567890"
        }
    ],
    "FailedFleetCancellations": []
}
```

Exemples de configurations de flotte de réservation de capacité

L'exemple suivant crée une flotte de réservation de capacité qui utilise deux types d'instance : `m5.4xlarge` et `m5.12xlarge`.

Il utilise un système de pondération basé sur le nombre de types d'instance vCPUs fournis par les types d'instances spécifiés. La capacité cible totale est de `480`vCPUs. Il en `m5.4xlarge` fournit 16 vCPUs et prend un poids de16, tandis qu'il en `m5.12xlarge` fournit 48 vCPUs et obtient un poids de48. Ce système de pondération configure la flotte de réservation de capacité pour réserver la capacité soit pour 30 instances `m5.4xlarge` (480/16=30), soit pour 10 instances `m5.12xlarge` (480/48=10).

La flotte est configurée pour donner la priorité à la capacité de `m5.12xlarge` et obtient la priorité de 1, tandis que `m5.4xlarge` obtient une priorité inférieure de 2. Cela signifie que la flotte essaiera d'abord de réserver la `m5.12xlarge` capacité, et ne tentera de réserver la `m5.4xlarge` capacité que si Amazon ne EC2 dispose pas d'une `m5.12xlarge` capacité suffisante.

La flotte réserve la capacité pour `Windows` les instances et la réservation expire automatiquement `October 31, 2021` à `23:59:59`UTC.

```
aws ec2 create-capacity-reservation-fleet \
--total-target-capacity 480 \
--allocation-strategy prioritized \
--instance-match-criteria open \
--tenancy default \
--end-date 2021-10-31T23:59:59.000Z \
```

```
--instance-type-specifications file://instanceTypeSpecification.json
```

Voici le contenu de `instanceTypeSpecification.json`.

```
[
    {
        "InstanceType": "m5.4xlarge",
        "InstancePlatform":"Windows",
        "Weight": 16,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 2
    },
    {
        "InstanceType": "m5.12xlarge",
        "InstancePlatform":"Windows",
        "Weight": 48,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 1
 }
]
```

Utilisation des rôles liés à un service pour la flotte de réserve de capacité

La flotte de réservation de capacité à la demande utilise AWS Identity and Access Management (IAM) des rôles liés au service. Un rôle lié à un service est un type unique de IAM rôle directement lié à la flotte de réservation de capacités. Les rôles liés au service sont prédéfinis par Capacity Reservation Fleet et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration de la flotte de réservation de capacité, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. La flotte de réservation de capacité définit les autorisations de ses rôles liés à un service et, sauf définition contraire, seule la flotte de réservation de capacité peut endosser ses rôles. Les autorisations définies incluent la politique de confiance et la politique d'autorisations, et cette politique d'autorisations ne peut être attachée à aucune autre IAM entité.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Vos ressources de la flotte de réservation de capacité sont ainsi protégées, car vous ne pouvez pas supprimer par inadvertance les autorisations d'accès aux ressources.

Autorisations de rôles liés à un service pour la flotte de réserve de capacité

La flotte de réservation de capacité utilise le rôle lié au service nommé AWSServiceRoleForEC2CapacityReservationFleetpour créer, décrire, modifier et annuler les réservations de capacité précédemment créées par une flotte de réservation de capacité, en votre nom.

Le rôle AWSServiceRoleForEC2CapacityReservationFleet lié au service fait confiance à l'entité suivante pour assumer le rôle :. `capacity-reservation-fleet.amazonaws.com`

Le rôle utilise la AWSEC2CapacityReservationFleetRolePolicypolitique, qui inclut les autorisations suivantes :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeCapacityReservations",
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateCapacityReservation",
                "ec2:CancelCapacityReservation",
                "ec2:ModifyCapacityReservation"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:capacity-reservation/*"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:CapacityReservationFleet": "arn:aws:ec2:*:*:capacity-
reservation-fleet/crf-*"
                }
            }
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:capacity-reservation/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateCapacityReservation"
                }
            }
        }
    ]
}
```

Vous devez configurer les autorisations pour autoriser une IAM entité (telle qu'un utilisateur, un groupe ou un rôle) à créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez la section Autorisations relatives aux rôles liés à un service dans le Guide de l'IAMutilisateur.

Création d'un rôle lié à un service pour la flotte de réserve de capacité

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez une flotte de réservation de capacité à l'aide de la `create-capacity-reservation-fleet` AWS CLI commande ou du `CreateCapacityReservationFleet`API, le rôle lié au service est automatiquement créé pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez une flotte de réservation de capacité, elle crée à nouveau le rôle lié à un service pour vous.

Modification d'un rôle lié à un service pour la flotte de réserve de capacité

La flotte de réservation de capacité ne vous permet pas de modifier le rôle AWSServiceRoleForEC2CapacityReservationFleet lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Vous pouvez toutefois modifier la description du rôle à l'aide deIAM. Pour plus d'informations, consultez la section Modification d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Suppression d'un rôle lié à un service pour la flotte de réserve de capacité

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez supprimer les ressources de votre rôle lié à un service avant de pouvoir le supprimer manuellement.

> **Note**
>
> Si le service de la flotte de réservation de capacité utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression peut échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer le rôle lié à AWSServiceRoleForEC2CapacityReservationFleet un service

1. Utilisez la `delete-capacity-reservation-fleet` AWS CLI commande ou le `DeleteCapacityReservationFleet` API pour supprimer les flottes de réservation de capacité de votre compte.
2. Utilisez la IAM console AWS CLI, le ou le AWS API pour supprimer le rôle AWSServiceRoleForEC2CapacityReservationFleet lié au service. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Régions prises en charge pour les rôles liés à un service de la flotte de réserve de capacité de capacité

La flotte de réservation de capacité prend en charge l'utilisation des rôles liés à un service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Régions et Points de terminaison AWS.

Surveillez l'utilisation des réservations de capacité à l'aide de CloudWatch métriques

Grâce aux CloudWatch métriques, vous pouvez surveiller efficacement vos réservations de capacité et identifier les capacités inutilisées en configurant des CloudWatch alarmes pour vous avertir lorsque les seuils d'utilisation sont atteints. Cela peut vous aider à maintenir un volume de Réservation de capacité constant et à atteindre un niveau d'utilisation plus élevé.

Les réservations de capacité à la demande envoient des données métriques CloudWatch toutes les cinq minutes. Les métriques ne sont pas prises en charge pour des réservations de capacité qui sont actives pendant moins de cinq minutes.

Pour plus d'informations sur l'affichage des métriques dans la CloudWatch console, consultez la section Utilisation d'Amazon CloudWatch Metrics. Pour plus d'informations sur la création d'alarmes, consultez Creating Amazon CloudWatch Alarms.

Table des matières

Métriques d'utilisation Réservation de capacité

L'espace de nom `AWS/EC2CapacityReservations` inclut les mesures d'utilisation suivantes que vous pouvez employer pour surveiller et maintenir la capacité à la demande à l'intérieur des seuils que vous spécifiez pour votre réservation.

Métrique	Description
`UsedInstanceCount`	Nombre d'instances actuellement utilisées. Unité : nombre
`AvailableInstanceCount`	Nombre d'instances qui sont disponibles. Unité : nombre
`TotalInstanceCount`	Nombre total d'instances que vous avez réservées. Unité : nombre
`InstanceUtilization`	Pourcentage d'instances de capacité réservées qui sont actuellement utilisées. Unité : pourcentage

Métrique	Description

Dimensions de métriques Réservation de capacité

Vous pouvez utiliser les dimensions suivantes pour affiner les mesures répertoriées dans le tableau précédent au sein de la région et du compte sélectionnés.

Dimension	Description
(Aucune dimension)	Cette dimension filtre la métrique spécifiée pour toutes les réservations de capacité.
`CapacityReservationId`	Cette dimension filtre la métrique spécifiée pour la réservation de capacité identifiée.
`InstanceType`	Cette dimension filtre la métrique spécifiée pour le type d'instance identifié.
`AvailabilityZone`	Cette dimension filtre la métrique spécifiée pour la zone de disponibilité identifiée.
`InstanceMatchCriteria`	Cette dimension filtre la métrique spécifiée pour les critères de correspondance d'instance identifiés (`openoutargeted`).
`InstancePlatform`	Cette dimension filtre les données métriques spécifiées pour la plate-forme identifiée.
`Tenancy`	Cette dimension filtre la métrique spécifiée pour la location identifiée.

Afficher CloudWatch les statistiques relatives aux réservations de capacité

Les métriques sont d'abord regroupées par espaces de noms de service, puis par dimensions prises en charge. Vous pouvez utiliser les procédures ci-dessous pour afficher les métriques pour vos réservations de capacité.

Pour consulter les statistiques de réservation de capacité à l'aide de la CloudWatch console

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Si nécessaire, changez la région. Dans la barre de navigation, sélectionnez la région où réside la Réservation de capacité. Pour plus d'informations, consultez Régions et points de terminaison.
3. Dans le panneau de navigation, sélectionnez Metrics (Métriques).
4. Pour Toutes les statistiques, choisissez EC2Capacity Reservations.
5. Choisissez parmi les dimensions métriques précédentes pour toutes les réservations de capacité, par réservation de capacité, par type d'instance, par zone de disponibilité, par plate-forme, par critère de correspondance d'instance ou par location et les métriques seront regroupées par Aucune dimension`CapacityReservationId`,`InstanceType`,`AvailabilityZone`,, `PlatformInstanceMatchCriteria`, et `Tenancy` respectivement.
6. Pour trier les métriques, utilisez l'en-tête de colonne. Pour représenter graphiquement une métrique, cochez la case en regard de la métrique.

Pour afficher les métriques de réserve de capacité (AWS CLI)

Utilisez la commande list-metrics suivante :

```
aws cloudwatch list-metrics --namespace "AWS/EC2CapacityReservations"
```

Surveillez l'utilisation des réservations de capacité à l'aide EventBridge

AWS Health envoie des événements à Amazon EventBridge lorsqu'une réservation de capacité enregistrée sur votre compte est inférieure à 20 % d'utilisation sur certaines périodes. Avec EventBridge, vous pouvez établir des règles qui déclenchent des actions programmatiques en réponse à de tels événements. Par exemple, vous pouvez créer une règle qui annule automatiquement une réserve de capacité lorsque son taux d'utilisation passe en dessous de 20 % sur une période de 7 jours.

Les événements de EventBridge sont représentés sous forme JSON d'objets. Les champs propres à l'événement sont contenus dans la section « détail » de l'JSONobjet. Le champ « événement » contient le nom de l'événement. Le champ « résultat » contient l'état terminé de l'action qui déclenche l'événement. Pour plus d'informations, consultez les modèles EventBridge d'événements Amazon dans le guide de EventBridge l'utilisateur Amazon.

Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.

Cette fonctionnalité n'est pas prise en charge dans AWS GovCloud (US).

Table des matières

Événements

AWS Health envoie les événements suivants lorsque l'utilisation de la capacité pour une réservation de capacité est inférieure à 20 %.

Événements

- AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION
- AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY

AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION

Voici un exemple d'événement généré lorsqu'une réserve de capacité nouvellement créée a un taux d'utilisation de la capacité inférieur à 20 % sur une période de 24 heures.


```
{
    "version": "0",
    "id": "b3e00086-f271-12a1-a36c-55e8ddaa130a",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-03-10T12:03:38Z",
    "region": "ap-south-1",
    "resources": [
        "cr-01234567890abcdef"
```

```
    ],
    "detail": {
        "eventArn": "arn:aws:health:ap-south-1::event/EC2/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_cr-01234567890abcdef-6211-4d50-9286-0c9fbc243f04",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION",
        "eventTypeCategory": "accountNotification",
        "startTime": "Fri, 10 Mar 2023 12:03:38 GMT",
        "endTime": "Fri, 10 Mar 2023 12:03:38 GMT",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided here"
            }
        ],
        "affectedEntities": [
            {
                "entityValue": "cr-01234567890abcdef"
            }
        ]
    }
    }
```

AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY

Voici un exemple d'événement généré lorsqu'une ou plusieurs réserves de capacité nouvellement créées ont un taux d'utilisation de la capacité inférieur à 20 % sur une période de 7 jours.

```
{
    "version": "0", "id":"7439d42b-3c7f-ad50-6a88-25e2a70977e2",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-03-07T06:06:01Z",
    "region": "us-east-1",
    "resources": [
        "cr-01234567890abcdef | us-east-1b | t3.medium | Linux/UNIX | 0.0%",
        "cr-09876543210fedcba | us-east-1a | t3.medium | Linux/UNIX | 0.0%"
    ],
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/EC2/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY/
```

```
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY_726c1732-d6f6-4037-b9b8-
bec3c2d3ba65",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY",
        "eventTypeCategory": "accountNotification",
        "startTime": "Tue, 7 Mar 2023 06:06:01 GMT",
        "endTime": "Tue, 7 Mar 2023 06:06:01 GMT",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided
 here"
            }
        ],
        "affectedEntities": [
            {
                "entityValue": "cr-01234567890abcdef | us-east-1b | t3.medium | Linux/
UNIX | 0.0%"
            },
            {
                "entityValue": "cr-09876543210fedcba | us-east-1a | t3.medium | Linux/
UNIX | 0.0%"
            }
        ]
    }
}
```

Création d'une EventBridge règle

Pour recevoir des notifications par e-mail lorsque le taux d'utilisation de votre réservation de capacité tombe en dessous de 20 %, créez un SNS sujet Amazon, puis une EventBridge règle pour l'`AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION`événement.

Pour créer le SNS sujet Amazon

1. Ouvrez la SNS console Amazon sur https://console.aws.amazon.com/sns/v3/home.
2. Dans le panneau de navigation, choisissez Rubriques, puis Créer une rubrique.
3. Pour Type, choisissez Standard.
4. Pour Nom, attribuez un nom à la nouvelle rubrique.
5. Choisissez Créer une rubrique.
6. Choisissez Create subscription (Créer un abonnement).

7. Pour Protocole, choisissez E-mail, puis pour Point de terminaison, saisissez l'adresse e-mail qui reçoit les notifications.
8. Choisissez Create subscription (Créer un abonnement).
9. L'adresse e-mail saisie ci-dessus recevra un e-mail avec l'objet suivant : `AWS Notification - Subscription Confirmation`. Suivez les instructions pour confirmer votre abonnement.

Pour créer la EventBridge règle

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Dans le volet de navigation, sélectionnez Rules (Règles), puis Create rule (Créer une règle).
3. Pour Nom, attribuez un nom à la nouvelle règle.
4. Pour Rule type (Type de règle), choisissez Rule with an event pattern (Règle avec un modèle d'événement).
5. Choisissez Suivant.
6. Pour Modèle d'événement, procédez comme suit :
    a. Pour Event source (Origine de l'événement), choisissez AWS services (Services).
    b. Pour Service AWS , choisissez AWS Health.
    c. Pour Type d'événement, choisissez Notification de EC2 ODCR sous-utilisation.
7. Choisissez Suivant.
8. Pour Cible 1, procédez comme suit :
    a. Pour Types de cibles, choisissez service AWS .
    b. Pour Sélectionner une cible, choisissez un SNSsujet.
    c. Pour Rubrique, choisissez la rubrique que vous avez créée précédemment.
9. Choisissez Suivant, puis de nouveau Suivant.
10. Choisissez Créer une règle.

Notifications d'utilisation des réservations de capacité provenant de AWS Health

AWS Health envoie l'e-mail et les AWS Health Dashboard notifications suivants lorsque le taux d'utilisation des capacités pour les réservations de capacité de votre compte tombe en dessous de 20 %.

- Notifications individuelles pour chaque réserve de capacité nouvellement créée dont le taux d'utilisation a été inférieur à 20 % au cours des dernières 24 heures.
- Une notification récapitulative pour toutes les réserves de capacité dont le taux d'utilisation a été inférieur à 20 % au cours des 7 derniers jours.

Les notifications par e-mail et les AWS Health Dashboard notifications sont envoyées à l'adresse e-mail associée au AWS compte propriétaire des réservations de capacité. Les notifications comprennent les informations suivantes :

- L'ID de la capacité de réservation.
- Zone de disponibilité de la réserve de capacité.
- Taux d'utilisation moyen de la réserve de capacité.
- Type d'instance et plateforme (système d'exploitation) de la réserve de capacité.

En outre, lorsque le taux d'utilisation de la capacité pour une réservation de capacité de votre compte tombe en dessous de 20 % sur une période de 24 heures et 7 jours, AWS Health envoie des événements à EventBridge. Avec EventBridge, vous pouvez créer des règles qui activent des actions automatiques, telles que l'envoi de notifications par e-mail ou le déclenchement de AWS Lambda fonctions, en réponse à de tels événements. Pour de plus amples informations, veuillez consulter Surveillez l'utilisation des réservations de capacité à l'aide EventBridge.

Blocs de capacité pour ML

Les blocs de capacité pour le machine learning vous permettent de réserver des GPU instances très recherchées à une date future afin de prendre en charge vos charges de travail d'apprentissage automatique (ML) de courte durée. Les instances qui s'exécutent dans un bloc de capacité sont automatiquement placées à proximité les unes des autres dans Amazon EC2 UltraClusters, pour une mise en réseau non bloquante à faible latence, à l'échelle du pétaoctet.

Avec les blocs de capacité, vous pouvez voir quand la capacité de l'GPUinstance sera disponible à des dates futures, et vous pouvez planifier le démarrage d'un bloc de capacité à l'heure qui vous convient le mieux. Lorsque vous réservez un bloc de capacité, vous bénéficiez d'une assurance de capacité prévisible pour les GPU instances, tout en ne payant que pour le temps dont vous avez besoin. Nous recommandons les blocs de capacité lorsque vous devez GPUs prendre en charge vos charges de travail ML pendant des jours ou des semaines d'affilée et que vous ne souhaitez pas payer pour une réservation lorsque vos GPU instances ne sont pas utilisées.

Voici quelques cas d'utilisation courants des blocs de capacité.

- Entraînement et mise au point du modèle ML : accédez sans interruption aux GPU instances que vous avez réservées pour terminer la formation et le réglage du modèle ML.
- Expériences et prototypes de machine learning : exécutez des expériences et créez des prototypes qui nécessitent GPU des instances de courte durée.

Les blocs de capacité sont actuellement disponibles pour `p5.48xlarge` et pour `p4d.24xlarge` les instances. Les `p5.48xlarge` instances sont disponibles dans les régions de l'est des États-Unis (Ohio) et de l'est des États-Unis (Virginie du Nord). Les `p4d.24xlarge` instances sont disponibles dans les régions de l'est des États-Unis (Ohio) et de l'ouest des États-Unis (Oregon). Vous pouvez réserver un bloc de capacité avec un démarrage ultérieur, jusqu'à huit semaines plus tard.

Vous pouvez utiliser les blocs de capacité pour réserver `p5` des `p4d` instances avec les options de durée de réservation et de quantité d'instances suivantes.

- Durées de réservation par tranches d'un jour jusqu'à 14 jours et par tranches de 7 jours jusqu'à 28 jours au total
- Options de quantité d'instances des réservations pour 1, 2, 4, 8, 16, 32 ou 64 instances

Pour réserver un bloc de capacité, vous devez commencer par spécifier vos besoins en matière de capacité, notamment le type d'instance, le nombre d'instances, la durée, la date de début la plus ancienne et la dernière date de fin dont vous avez besoin. Ensuite, vous pouvez voir une offre de blocs de capacité disponible qui répond à vos spécifications. L'offre de bloc de capacité inclut des informations telles que l'heure de début, la zone de disponibilité et le prix de réservation. Le prix d'une offre de bloc de capacité dépend de l'offre et de la demande au moment où l'offre est proposée. Une fois que vous avez réservé un bloc de capacité, le prix ne change pas. Pour de plus amples informations, veuillez consulter Tarification et facturation des blocs de capacité.

Lorsque vous achetez un bloc de capacité, votre réservation est créée pour la date et le nombre d'instances que vous avez sélectionnés. Lorsque votre réservation de bloc de capacité commence, vous pouvez cibler les lancements d'instances en spécifiant l'ID de réservation dans vos demandes de lancement.

Vous pouvez utiliser toutes les instances que vous avez réservées jusqu'à 30 minutes avant la fin du bloc de capacité. Lorsqu'il ne reste que 30 minutes de réservation à votre bloc de capacité, nous commençons à mettre fin à toutes les instances en cours d'exécution dans le bloc de capacité.

Nous utilisons ce temps pour nettoyer vos instances avant de livrer le bloc de capacité au client suivant. Les 30 dernières minutes de la réservation ne sont pas incluses dans le prix du bloc de capacité. Nous émettons un événement EventBridge 10 minutes avant le début du processus de résiliation. Pour de plus amples informations, veuillez consulter Surveillez les blocs de capacité à l'aide EventBridge.

Rubriques

Plateformes prises en charge

Les blocs de capacité pour le ML sont actuellement pris en charge `p5.48xlarge` et `p4d.24xlarge` les instances sont louées par défaut. Lorsque vous utilisez le AWS Management Console pour acheter un bloc de capacité, l'option de plateforme par défaut est Linux/UNIX. Lorsque vous utilisez le AWS Command Line Interface (AWS CLI) ou que AWS SDK vous achetez un bloc de capacité, les options de plateforme suivantes sont disponibles :

- Linux/Unix
- Utilisation de Red Hat Enterprise Linux
- RHELavec HA
- SUSELinux
- Ubuntu Pro

Considérations

Avant d'utiliser les blocs de capacité, tenez compte des informations et des limites suivantes.

- Les blocs de capacité commencent et se terminent à 11 h 30, temps universel coordonné (UTC).

- Le processus de résiliation pour les instances exécutées dans un bloc de capacité commence à 11 h 00, heure universelle coordonnée (UTC), le dernier jour de la réservation.
- Les blocs de capacité peuvent être réservés avec un démarrage ultérieur, jusqu'à huit semaines plus tard.
- Vous n'êtes pas autorisé à modifier ou annuler les blocs de capacité.
- Les blocs de capacité ne peuvent pas être partagés entre les AWS comptes ou au sein de votre AWS organisation.
- Les blocs de capacité ne peuvent pas être utilisés dans un groupe de réserve de capacité.
- Le nombre total d'instances pouvant être réservées dans les blocs de capacité pour tous les comptes de votre AWS organisation ne peut pas dépasser 64 instances à une date donnée.
- Pour utiliser un bloc de capacité, les instances doivent cibler spécifiquement l'ID de réservation.
- Les instances d'un bloc de capacité ne sont pas prises en compte dans vos limites d'instances à la demande.
- Pour les instances P5 utilisant une configuration personnaliséeAMI, assurez-vous de disposer du logiciel et de la configuration requis pour EFA.
- Pour les groupes de nœuds EKS gérés par Amazon, consultez Créer un groupe de nœuds gérés avec Amazon EC2 Capacity Blocks for ML. Pour les groupes de nœuds EKS autogérés par Amazon, consultez Utiliser des blocs de capacité pour le machine learning avec des nœuds autogérés.

Ressources connexes

Après avoir créé un bloc de capacité, vous pouvez effectuer les opérations suivantes avec le bloc de capacité :

- Lancez des instances dans le bloc de capacité. Pour de plus amples informations, veuillez consulter Lancer des instances dans des blocs de capacité.
- Créez un groupe Amazon EC2 Auto Scaling. Pour plus d'informations, consultez la section Utiliser les blocs de capacité pour les charges de travail d'apprentissage automatique dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.

> **Note**
>
> Si vous utilisez Amazon EC2 Auto Scaling ou AmazonEKS, vous pouvez planifier le dimensionnement pour qu'il soit exécuté au début de la réservation du Capacity Block.

Grâce au dimensionnement planifié, il gère AWS automatiquement les nouvelles tentatives pour vous. Vous n'avez donc pas à vous soucier de la mise en œuvre d'une logique de nouvelles tentatives pour gérer les échecs transitoires.

- Améliorez les flux de travail ML avec AWS ParallelCluster. Pour plus d'informations, consultez Enhancing ML Workflows with AWS ParallelCluster et Amazon EC2 Capacity Blocks for ML.

Pour plus d'informations AWS ParallelCluster, voir Qu'est-ce que AWS ParallelCluster.

Tarification et facturation des blocs de capacité

Avec Amazon EC2 Capacity Blocks for ML, vous ne payez que pour ce que vous réservez. Le prix d'un bloc de capacité dépend de l'offre et de la demande des blocs de capacité au moment de l'achat. Vous pouvez afficher le prix d'une offre de bloc de capacité avant de la réserver. Le prix du bloc de capacité est facturé d'avance au moment de la réservation. Lorsque vous recherchez un bloc de capacité sur une plage de dates, nous vous renvoyons l'offre de bloc de capacité la moins chère disponible. Une fois que vous avez réservé un bloc de capacité, le prix ne change pas.

Lorsque vous utilisez un bloc de capacité, vous payez pour le système d'exploitation que vous utilisez lorsque vos instances sont exécutées. Pour plus d'informations sur les prix des systèmes d'exploitation, consultez Amazon EC2 Capacity Blocks for ML Pricing.

Facturation

Le prix d'une offre de bloc de capacité est facturé d'avance. Le paiement est facturé sur votre compte AWS dans les 12 heures qui suivent l'achat d'un bloc de capacité. Pendant le traitement de votre paiement, votre ressource de réservation de bloc de capacité reste en état d'`payment-pending`. Si votre paiement ne peut pas être traité dans un délai de 12 heures, votre bloc de capacité est libéré et l'état de la réservation passe à `payment-failed`.

Une fois votre paiement traité avec succès, l'état de la ressource de bloc de capacité passe de `payment-pending` à `scheduled`. Vous recevez une facture qui reflète le paiement initial unique. Dans la facture, vous pouvez associer le montant payé à l'identifiant de réservation de bloc de capacité.

Lorsque votre réservation de bloc de capacité commence, vous êtes facturé uniquement en fonction du système d'exploitation que vous utilisez pendant que vos instances sont exécutées dans le cadre de la réservation. Vous pouvez consulter votre utilisation et les frais associés sur votre facture anniversaire pour le mois d'utilisation de votre AWS Cost and Usage Report.

> **Note**
>
> Les remises sur les Savings Plans et les instances réservées ne s'appliquent pas aux blocs de capacité.

Affichage d'une facture

Vous pouvez consulter votre facture dans la AWS Billing and Cost Management console. Le paiement initial de votre bloc de capacité apparaît le mois au cours duquel vous avez acheté la réservation.

Après le début de votre réservation, votre facture indique des lignes distinctes pour le temps de réservation du bloc utilisé et le temps non utilisé. Vous pouvez utiliser ces lignes pour voir combien de temps a été utilisé pour votre réservation. Vous ne verrez des frais d'utilisation dans la ligne correspondant au temps utilisé que si vous utilisez un système d'exploitation premium. Pour de plus amples informations, veuillez consulter Tarification et facturation des blocs de capacité. Le temps non utilisé n'entraîne aucuns frais supplémentaires.

Pour plus d'informations, consultez la section Viewing your bill (Affichage d'une facture) dans le Guide de l'utilisateur AWS Billing and Cost Management .

Si votre bloc de capacité commence à un mois différent de celui au cours duquel vous avez acheté votre réservation, le prix initial et l'utilisation de la réservation apparaissent sous des mois de facturation distincts. Dans votre AWS Cost and Usage Report, le numéro de réservation Capacity Block est indiqué dans la ARN rubrique Réservation/réservation de vos frais initiaux et dans le LineItem/ResourceID sur votre facture anniversaire afin que vous puissiez associer l'utilisation au prix initial correspondant.

Utiliser des blocs de capacité

Pour commencer à utiliser les blocs de capacité, vous devez d'abord rechercher et acheter un bloc de capacité disponible qui correspond à la taille, à la durée et au calendrier de votre réservation. Ensuite, lorsque la réservation commence, vous pouvez utiliser le bloc de capacité en lançant des instances qui ciblent l'ID de réservation. Trente minutes avant l'expiration de la réservation, nous commençons à mettre fin à toutes les instances encore en cours d'exécution dans le bloc de capacité.

Les blocs de capacité sont fournis sous forme de réserve de capacité `targeted` dans une seule zone de disponibilité. Pour exécuter des instances dans un bloc de capacité, vous devez spécifier

l'ID de réservation lors du lancement de vos instances. Si vous arrêtez vous-même des instances et que le bloc de capacité expire, vous ne pouvez pas les redémarrer tant que vous n'avez pas ciblé un autre bloc de capacité à l'état `active`.

Par défaut, les blocs de capacité fournissent une connectivité réseau à faible latence et à haut débit entre les instances du bloc de capacité. Il n'est donc pas nécessaire d'utiliser un groupe de placement du cluster avec un bloc de capacité.

Rubriques

Prérequis

Vous devez utiliser le Région AWS correspondant au type d'instance que vous souhaitez utiliser. Pour de plus amples informations, veuillez consulter Régions.

Les blocs de capacité avec `p5.48xlarge` instances sont disponibles ci-dessous Régions AWS.

Nom de la région	Code région
USA Est (Ohio)	us-east-2
USA Est (Virginie du Nord)	us-east-1

Les blocs de capacité avec `p4d.24xlarge` instances sont disponibles ci-dessous Régions AWS.

Nom de la région	Code région
USA Est (Ohio)	us-east-2
USA Ouest (Oregon)	us-west-2

> **Note**
>
> Les tailles de bloc de capacité de 64 instances ne sont pas prises en charge pour tous les types d'instances Régions AWS.

Rechercher et acheter des blocs de capacité

Pour réserver un bloc de capacité, vous devez d'abord rechercher un intervalle de temps pendant lequel la capacité est disponible et qui correspond à vos besoins. Pour trouver un bloc de capacité disponible à la réservation, vous devez spécifier les éléments suivants.

- Le nombre d'instances dont vous avez besoin
- La durée pendant laquelle vous avez besoin des instances
- La plage de dates pour laquelle vous avez besoin de votre réservation

Pour rechercher une offre de bloc de capacité disponible, vous devez spécifier une durée de réservation et un nombre d'instances. Vous devez sélectionner l'une des options suivantes.

- Pour la durée de la réservation : jusqu'à 14 jours par tranches d'un jour ou jusqu'à 28 jours par tranches de 7 jours
- Par nombre d'instances : 1, 2, 4, 8, 16, 32 ou 64 instances

Si un bloc de capacité correspondant à vos spécifications est disponible, nous vous renvoyons les détails d'une seule offre de bloc de capacité. Les détails de l'offre incluent l'heure de début de la réservation, la zone de disponibilité de la réservation et le prix de la réservation. Pour de plus amples informations, veuillez consulter Tarification et facturation des blocs de capacité.

Vous pouvez acheter l'offre de bloc de capacité qui vous est présentée, ou vous pouvez modifier vos critères de recherche pour voir les autres options disponibles. Il n'y a pas de date d'expiration prédéfinie pour l'offre, mais les offres sont disponibles uniquement sur le principe du premier arrivé, premier servi.

Lorsque vous achetez une offre de bloc de capacité, vous recevez une réponse immédiate confirmant que votre bloc de capacité a été réservé. Après confirmation, vous verrez une nouvelle réserve de capacité sur votre compte avec un type de réservation `capacity-block` et une `start-date` définie pour l'offre que vous avez achetée. Votre réservation de bloc de capacité est créée avec l'état

`payment-pending`. Une fois le paiement initial traité avec succès, l'état de la réservation passe à `scheduled`. Pour de plus amples informations, veuillez consulter Facturation.

Vous pouvez utiliser l'une des méthodes suivantes pour rechercher et acheter un bloc de capacité.

Console

Pour rechercher et acheter un bloc de capacité à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation en haut de l'écran, sélectionnez un Région AWS. Ce choix est important car les tailles de blocs de capacité de 64 instances ne sont pas prises en charge pour tous les types d'instances dans toutes les régions.
3. Dans le volet de navigation, choisissez Réserve de capacité, Acheter des blocs de capacité.
4. Sous Attributs de capacité, vous pouvez définir les paramètres de recherche de votre bloc de capacité. Par défaut, la plateforme est Linux. Si vous souhaitez sélectionner un autre système d'exploitation, utilisez l' AWS CLI. Pour de plus amples informations, veuillez consulter Plateformes prises en charge.
5. Sous Capacité totale, sélectionnez le nombre d'instances que vous souhaitez réserver.
6. Sous Durée, saisissez le nombre de jours pour lesquels vous avez besoin de la réservation.
7. Sous Plage de dates pour rechercher des blocs de capacité, entrez la date la plus proche à laquelle vous souhaitez que votre réservation commence.
8. Choisissez Rechercher des blocs de capacité.
9. Si un bloc de capacité répondant à vos spécifications est disponible, une offre s'affiche sous Blocs de capacité recommandés. Si plusieurs offres répondent à vos spécifications, la plus ancienne offre de blocs de capacité disponible est affichée. Pour consulter les autres offres de blocs de capacité, ajustez vos critères de recherche et sélectionnez à nouveau Rechercher des blocs de capacité.
10. Lorsque vous trouvez une offre de bloc de capacité que vous souhaitez acheter, choisissez Suivant.
11. (Facultatif) Sur la page Ajouter des balises, choisissez Ajouter une nouvelle balise.
12. La page Vérifier et acheter répertorie les dates de début et de fin, la durée, le nombre total d'instances et le prix.

> **Note**
>
> Les blocs de capacité ne peuvent être ni modifiés ni annulés une fois que vous les avez réservés.

13. Dans la fenêtre contextuelle Acheter un bloc de capacité, saisissez « confirm », puis choisissez Acheter.

AWS CLI

Pour trouver un bloc de capacité à l'aide du AWS CLI

Utilisez la commande `describe-capacity-block-offerings`.

L'exemple suivant recherche un bloc de capacité comportant 16 instances `p5.48xlarge`, dont la plage de dates commence le `2023-08-14` et se termine le `2023-10-22` avec une durée de 48 heures. Le nombre d'instances doit être un entier provenant d'un ensemble prédéfini d'options 1, 2, 4, 8, 16, 32 ou 64. La durée de la capacité doit être un entier multiple de 24 compris entre 24 et 336 indiquant le nombre de jours en heures.

```
aws ec2 describe-capacity-block-offerings --instance-type p5.48xlarge \
  --instance-count 16 --start-date-range 2023-08-14T00:00:00Z \
  --end-date-range 2023-10-22-T00:00:00Z --capacity-duration 48
```

Pour acheter un bloc de capacité à l'aide du AWS CLI

Utilisez la commande `purchase-capacity-block` et spécifiez l'ID de l'offre de bloc de capacité que vous souhaitez acheter et la plateforme de l'instance.

```
aws ec2 purchase-capacity-block \
  --capacity-block-offering-id cbr-0123456789abcdefg \
  --instance-platform Linux/UNIX
```

Lancer des instances dans des blocs de capacité

Pour utiliser votre bloc de capacité, vous devez spécifier l'ID de réservation de bloc de capacité lors du lancement des instances. Le lancement d'une instance dans un bloc de capacité réduit la capacité disponible du nombre d'instances lancées. Par exemple, si la capacité d'instance que vous avez

achetée est de huit instances et que vous lancez quatre instances, la capacité disponible est réduite de quatre.

Si vous mettez fin à une instance exécutée dans le bloc de capacité avant la fin de la réservation, vous pouvez lancer une nouvelle instance à sa place. Lorsque vous arrêtez ou mettez fin à une instance dans un bloc de capacité, le nettoyage de votre instance prend plusieurs minutes avant de pouvoir lancer une autre instance pour la remplacer. Pendant ce temps, votre instance sera à l'état Arrêt ou `shutting-down`. Une fois ce processus terminé, l'état de votre instance deviendra `stopped` ou `terminated`. Ensuite, la capacité disponible dans votre bloc de capacité sera mise à jour pour afficher une autre instance disponible à utiliser.

Pour plus d'informations sur la configuration d'un groupe de nœuds EKS gérés avec un bloc de capacité, consultez la section Créer un groupe de nœuds gérés avec des blocs de capacité pour le ML dans le guide de EKS l'utilisateur Amazon.

Pour plus d'informations sur la configuration à AWS ParallelCluster l'aide d'un bloc de capacité, voir ML on AWS ParallelCluster.

Pour plus d'informations sur la façon de lancer des instances dans un bloc de capacité à l'aide de EC2 Fleet, consultezTutoriel : configurez votre EC2 flotte pour lancer des instances dans des blocs de capacité.

Pour plus d'informations sur la création d'un modèle de lancement ciblant un bloc de capacité, consultez la rubrique Stockez les paramètres de lancement de l'instance dans les modèles de EC2 lancement Amazon.

Les étapes suivantes expliquent comment lancer des instances dans un bloc de capacité dans l'`active`état à l'aide du AWS Management Console ou du AWS CLI.

Console

Pour lancer des instances dans un bloc de capacité à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation, en haut de l'écran, sélectionnez la région de votre réservation de bloc de capacité.
3. Dans le tableau de bord de EC2 la console Amazon, choisissez Launch instance.
4. (Facultatif) Sous Nom et balises, vous pouvez nommer et baliser votre instance. Pour plus d'informations sur les balises, consultez Marquez vos EC2 ressources Amazon

5. Sous Images de l'application et du système d'exploitation, sélectionnez une image de machine Amazon (AMI).
6. Sous Type d'instance, sélectionnez le type d'instance qui correspond à votre réservation de bloc de capacité.
7. Sous Paire de clés (connexion), choisissez une paire de clés existante ou choisissez Créer une paire de clés pour en créer une. Pour de plus amples informations, veuillez consulter Paires de EC2 clés Amazon et EC2 instances Amazon.
8. Sous Network settings (Paramètres réseau), utilisez les paramètres par défaut ou choisissez Edit (Modifier) pour configurer les paramètres réseau selon les besoins.

   > **Important**
   >
   > Votre instance ne peut pas être lancée dans un sous-réseau situé dans une zone de disponibilité différente de celle dans laquelle se trouve votre bloc de capacité.

9. Sous Détails avancés, configurez l'instance Spot comme suit.
   a. Sous Option d'achat (type de marché), sélectionnez Bloc de capacité.
   b. Sous Réserve de capacité, sélectionnez Cible par ID.
   c. Sélectionnez l'ID de réserve de capacité de votre réservation de bloc de capacité.
10. Sur le panneau Summary (Récapitulatif), pour Number of instances (Nombre d'instances), saisissez le nombre d'instances à lancer.
11. Choisissez Launch instance (Lancer une instance).

AWS CLI

Pour lancer des instances dans un bloc de capacité à l'aide du AWS CLI

- Utilisez la commande `run-instances` et spécifiez un `MarketType` de `capacity-block` dans la structure `instance-market-options`. Vous devez également spécifier le paramètre `capacity-reservation-specification`.

  L'exemple suivant lance une instance `p5.48xlarge` unique dans un bloc de capacité actif disposant des attributs correspondants et de la capacité disponible.

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 \
  --instance-type p5.48xlarge --key-name MyKeyPair \
```

```
  --subnet-id subnet-1234567890abcdef1 \
  --instance-market-options MarketType='capacity-block'
  --capacity-reservation-specification
CapacityReservationTarget={CapacityReservationId=cr-a1234567}
```

Afficher les blocs de capacité

Après avoir réservé un bloc de capacité, vous pouvez consulter la réservation du bloc de capacité dans votre compte AWS . Vous pouvez consulter la `start-date` et la `end-date` pour savoir quand votre réservation débute et se termine. Avant le début d'une réservation de bloc de capacité, la capacité disponible apparaît comme nulle. Vous pouvez voir combien d'instances seront disponibles dans votre bloc de capacité en fonction de la valeur de balise associée à la clé de balise `aws:ec2capacityreservation:incrementalRequestedQuantity`.

Lorsqu'une réservation de bloc de capacité commence, l'état de la réservation passe de `scheduled` à `active`. Nous émettons un événement via Amazon EventBridge pour vous informer que le Capacity Block est prêt à être utilisé. Pour de plus amples informations, veuillez consulter Surveillez les blocs de capacité à l'aide EventBridge.

Les états des blocs de capacité sont les suivants :

- `payment-pending` : le paiement initial n'a pas encore été traité.
- `payment-failed` : le paiement n'a pas pu être traité dans un délai prévu des 12 heures. Votre bloc de capacité a été libéré.
- `scheduled` : le paiement a été traité et la réservation du bloc de capacité n'a pas encore commencé.
- `active` : la capacité réservée peut être utilisée.
- `expired` : la réservation de bloc de capacité a expiré automatiquement à la date et à l'heure spécifiées dans votre demande de réservation. La capacité réservée n'est plus disponible pour utilisation.

Vous pouvez utiliser l'une des méthodes ci-dessous pour afficher votre réservation de bloc de capacité.

Console

Pour afficher les blocs de capacité à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Réservations de capacité.
3. Sur la page Aperçu des réservations de capacité, vous pouvez voir un table des ressources contenant des détails sur toutes vos ressources de réserve de capacité. Pour trouver vos réservations de blocs de capacité, sélectionnez les blocs de capacité dans la liste déroulante située au-dessus de l'ID de réserve de capacité. Dans la table, vous pouvez consulter des informations sur vos blocs de capacité, telles que les dates de début et de fin, la durée et le statut.
4. Pour plus de détails sur un bloc de capacité, sélectionnez l'ID de réservation de bloc de capacité que vous souhaitez consulter. La page Détails de réserve de capacité affiche toutes les propriétés de la réservation ainsi que le nombre d'instances utilisées et disponibles dans le bloc de capacité.

> **Note**
>
> Avant le début d'une réservation de bloc de capacité, la capacité disponible apparaît comme nulle. Vous pouvez voir combien d'instances seront disponibles lorsque la réservation du bloc de capacité commence à l'aide de la valeur de balise suivante associée à la clé de balise : `aws:ec2capacityreservation:incrementalRequestedQuantity`.

AWS CLI

Pour afficher les blocs de capacité à l'aide du AWS CLI

Par défaut, lorsque vous utilisez la describe-capacity-reservationscommande, les réservations de capacité à la demande et les réservations par blocs de capacité sont répertoriées. Pour afficher uniquement vos réservations de blocs de capacité, filtrez le paramètre `capacity-reservation-type` à l'aide de `capacity-block`.

Par exemple, la commande suivante décrit une ou plusieurs de vos réservations Capacity Block dans votre compte actuel Région AWS.

```
aws ec2 describe-capacity-reservations -reservation-type capacity-block
```

Exemple de sortie.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-12345678",
            "EndDateType": "limited",
            "ReservationType": "capacity-block"
            "AvailabilityZone": "eu-east-2a",
            "InstanceMatchCriteria": "targeted",
            "EphemeralStorage": false,
            "CreateDate": "2023-11-29T14:22:45Z",
            "StartDate": "2023-12-15T12:00:00Z",
            "EndDate": "2023-08-19T12:00:00Z",
            "AvailableInstanceCount": 0,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 16,
            "State": "payment-pending",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "p5.48xlarge"
        },
        ...
```

Surveillez les blocs de capacité à l'aide EventBridge

Lorsque votre réservation de Capacity Block commence, Amazon EC2 émet un événement indiquant EventBridge que votre capacité est prête à être utilisée. Quarante minutes avant la fin de votre réservation Capacity Block, vous recevez un autre EventBridge événement vous indiquant que toutes les instances incluses dans la réservation commenceront à se terminer dans 10 minutes. Pour plus d'informations sur EventBridge les événements, consultez Amazon EventBridge Events.

Les structures d'événements suivantes pour les événements émis pour les blocs de capacité :

Bloc de capacité remis

L'exemple suivant présente un événement pour un bloc de capacité remis.

```
{
```

```
  "customer_event_id": "[Capacity Reservation Id]-delivered",
  "detail_type": "Capacity Block Reservation Delivered",
  "source": "aws.ec2",
  "account": "[Customer Account ID]",
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

Avertissement d'expiration du bloc de capacité

L'exemple suivant présente un événement pour un avertissement d'expiration d'un bloc de capacité.

```
{
  "customer_event_id": "[Capacity Reservation Id]-approaching-expiry",
  "detail_type": "Capacity Block Reservation Expiration Warning",
  "source": "aws.ec2",
  "account": "[Customer Account ID]",
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

Capacité de journalisation : bloque API les appels avec AWS CloudTrail

Capacity Blocks est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Capacity Blocks. CloudTrail capture les API appels aux blocs de capacité sous forme d'événements. Les appels capturés incluent des appels provenant de la console Capacity Blocks et des appels de code vers les API opérations Capacity Blocks. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour les blocs de capacité. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les

plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Capacity Blocks, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations sur les blocs de capacité dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans des blocs de capacité, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements qui se produisent dans votre environnement Compte AWS, y compris les événements liés aux blocs de capacité, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- CloudTrail services et intégrations pris en charge
- Configuration des SNS notifications Amazon pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les actions des Capacity Blocks sont enregistrées CloudTrail et documentées dans le Amazon EC2 API Reference. Par exemple, les appels au`CapacityBlockScheduled`, et les `CapacityBlockActive` actions génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'CloudTrail userIdentity élément.

Présentation des entrées des fichiers journaux des blocs de capacité

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des API appels publics, ils n'apparaissent donc pas dans un ordre spécifique.

Les exemples suivants montrent les entrées du CloudTrail journal pour :

- TerminateCapacityBlocksInstances
- CapacityBlockPaymentFailed
- CapacityBlockScheduled
- CapacityBlockActive
- CapacityBlockFailed
- CapacityBlockExpired

> **Note**
>
> Certains champs qui ont été supprimés des exemples relatifs à la confidentialité des données.

TerminateCapacityBlocksInstances

```
{
```

```
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "TerminateCapacityBlockInstances",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:instance/
i-1234567890abcdef0"
    }
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws::ec2:US East (N. Virginia):123456789012:instance/
i-0598c7d356eba48d7"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      }
}
```


CapacityBlockPaymentFailed


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
```

```
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockPaymentFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "payment-failed"
      }
}
```


CapacityBlockScheduled


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockScheduled",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
```

```
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "scheduled"
      }
}
```


CapacityBlockActive


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockActive",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
```

```
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "active"
      }
 }
```

CapacityBlockFailed

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "failed"
      }
 }
```

CapacityBlockExpired


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockExpired",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "expired"
      }
 }
```


Stockez les paramètres de lancement de l'instance dans les modèles de EC2 lancement Amazon

Vous pouvez utiliser un modèle de EC2 lancement Amazon pour stocker les paramètres de lancement d'une instance afin de ne pas avoir à les spécifier à chaque fois que vous lancez une EC2 instance Amazon. Par exemple, vous pouvez créer un modèle de lancement qui stocke l'AMIID, le type d'instance et les paramètres réseau que vous utilisez généralement pour lancer des instances.

Lorsque vous lancez une instance à l'aide de la EC2 console Amazon AWS SDK, d'un outil de ligne de commande ou d'un outil de ligne de commande, vous pouvez spécifier le modèle de lancement au lieu de saisir à nouveau les paramètres.

Pour chaque modèle de lancement, vous pouvez créer une ou plusieurs versions de modèle de lancement numérotées. Chaque version peut comporter différents paramètres de lancement. Lorsque vous lancez une instance à partir d'un modèle de lancement, vous pouvez utiliser une version quelconque du modèle de lancement. Si vous ne spécifiez pas de version, la version par défaut est utilisée. Vous pouvez définir n'importe quelle version du modèle de lancement comme version par défaut. Par défaut, il s'agit de la première version du modèle de lancement.

Le schéma suivant présente trois versions d'un modèle de lancement. La première version spécifie le type d'instance, l'AMIID, le sous-réseau et la paire de clés à utiliser pour lancer l'instance. La deuxième version est basée sur la première et spécifie également un groupe de sécurité pour l'instance. La troisième version utilise différentes valeurs pour certains des paramètres. La version 2 est définie comme version par défaut. Si vous avez lancé une instance à partir de ce modèle de lancement, les paramètres de lancement de la version 2 sont utilisés si aucune autre version n'a été spécifiée.

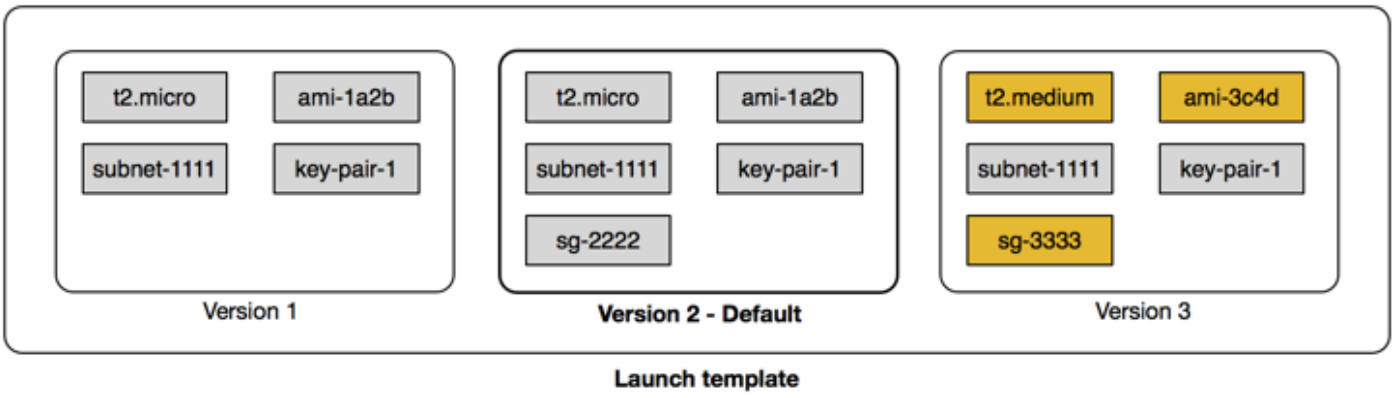


Table des matières

Restrictions relatives aux modèles EC2 de lancement Amazon

Les restrictions suivantes s'appliquent aux modèles de lancement et aux versions des modèles de lancement :

- Quotas : pour consulter les quotas de vos modèles de lancement et des versions de vos modèles de lancement, ouvrez la console Service Quotas ou utilisez la list-service-quotas AWS CLI commande. Chaque AWS compte peut avoir jusqu'à 5 000 modèles de lancement par région et jusqu'à 10 000 versions par modèle de lancement. Vos comptes peuvent avoir des quotas différents en fonction de leur ancienneté et de leur historique d'utilisation.
- Les paramètres sont facultatifs : les paramètres du modèle de lancement sont facultatifs. Cependant, vous devez vous assurer que votre demande de lancement d'instance inclut tous les paramètres requis. Par exemple, si votre modèle de lancement n'inclut pas d'AMIidentifiant, vous devez le spécifier lorsque vous lancez une instance avec ce modèle de lancement. AMI
- Les paramètres ne sont pas validés : les paramètres du modèle de lancement ne sont pas entièrement validés lorsque vous créez le modèle de lancement. Si vous spécifiez des valeurs incorrectes ou si vous utilisez des combinaisons de paramètres non prises en charge, les instances ne pourront pas être lancées à l'aide de ce modèle de lancement. Pour éviter tout problème, assurez-vous de spécifier les valeurs correctes et d'utiliser les combinaisons de paramètres prises en charge. Par exemple, pour lancer une instance dans un groupe de placement, vous devez spécifier un type d'instance pris en charge.
- Balises : vous pouvez baliser un modèle de lancement, mais pas une version du modèle de lancement.
- Immutable : les modèles de lancement sont immuables. Pour modifier un modèle de lancement, vous devez créer une nouvelle version du modèle de lancement.
- Numéros de version : les versions de modèles de lancement sont numérotées dans l'ordre de leur création. Lorsque vous créez une version du modèle de lancement, vous ne pouvez pas spécifier vous-même le numéro de version.

IAMautorisations requises pour les modèles de EC2 lancement Amazon

Vous pouvez utiliser IAM les autorisations pour contrôler si les utilisateurs peuvent répertorier, afficher, créer ou supprimer des modèles de lancement ou des versions de modèles de lancement.

> **Important**
>
> Vous ne pouvez pas utiliser les autorisations au niveau des ressources pour restreindre les ressources que les utilisateurs peuvent spécifier dans un modèle de lancement lorsqu'ils créent un modèle de lancement ou une version de modèle de lancement. Par conséquent, assurez-vous que seuls les administrateurs de confiance sont autorisés à créer des modèles de lancement et des versions de modèles de lancement.

Vous devez accorder à toute personne qui utilisera un modèle de lancement les autorisations nécessaires pour créer et accéder aux ressources spécifiées dans le modèle de lancement. Par exemple :

- Pour lancer une instance à partir d'une Amazon Machine Image privée partagée (AMI), l'utilisateur doit disposer de l'autorisation de lancement pourAMI.
- Pour créer des EBS volumes avec des balises à partir d'instantanés existants, l'utilisateur doit disposer d'un accès en lecture aux instantanés et des autorisations nécessaires pour créer et étiqueter des volumes.

Table des matières

EC2 : CreateLaunchTemplate

Pour créer un modèle de lancement dans la console ou à l'aide duAPIs, le principal doit avoir l'`ec2:CreateLaunchTemplate`autorisation requise dans une IAM politique. Dans la mesure du possible, utilisez des balises pour contrôler l'accès aux modèles de lancement de votre compte.

Par exemple, la déclaration de IAM politique suivante donne au principal l'autorisation de créer des modèles de lancement uniquement si le modèle utilise la balise spécifiée (*`objectif`*=*`test`*).

```
{
    "Sid": "IAMPolicyForCreatingTaggedLaunchTemplates",
    "Action": "ec2:CreateLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/purpose": "testing"
        }
    }
}
```

Les principaux qui créent des clés peuvent avoir besoin de certaines autorisations associées, telles que :

- ec2 : CreateTags — Pour ajouter des balises au modèle de lancement pendant l'`CreateLaunchTemplate`opération, l'`CreateLaunchTemplate`appelant doit avoir l'`ec2:CreateTags`autorisation spécifiée dans une IAM politique.
- ec2 : RunInstances — Pour lancer des EC2 instances à partir du modèle de lancement qu'ils ont créé, le principal doit également disposer de l'`ec2:RunInstances`autorisation spécifiée dans une IAM politique.

Pour les actions de création de ressources qui appliquent des balises, les utilisateurs doivent être autorisés à effectuer l'action `ec2:CreateTags`. La déclaration IAM de politique suivante utilise la clé de `ec2:CreateAction` condition pour permettre aux utilisateurs de créer des balises uniquement dans le contexte de`CreateLaunchTemplate`. Les utilisateurs ne peuvent pas étiqueter les modèles de lancement existants ou d'autres ressources. Pour de plus amples informations, veuillez consulter Accorder l'autorisation de baliser les EC2 ressources Amazon lors de la création.

```
{
    "Sid": "IAMPolicyForTaggingLaunchTemplatesOnCreation",
    "Action": "ec2:CreateTags",
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction": "CreateLaunchTemplate"
        }
    }
```

```
}
```

L'IAMutilisateur qui crée un modèle de lancement n'est pas automatiquement autorisé à utiliser le modèle de lancement qu'il a créé. Comme tout autre responsable, le créateur du modèle de lancement doit obtenir une autorisation par le biais d'une IAM politique. Si un IAM utilisateur souhaite lancer une EC2 instance à partir d'un modèle de lancement, il doit en avoir l'`ec2:RunInstances`autorisation. Lorsque vous accordez ces autorisations, vous pouvez spécifier que les utilisateurs ne peuvent utiliser que des modèles de lancement dotés de balises spécifiques ou spécifiquesIDs. Vous pouvez également contrôler les ressources AMI et les autres ressources auxquelles toute personne utilisant des modèles de lancement peut faire référence et utiliser lors du lancement d'instances en spécifiant des autorisations au niveau des ressources pour l'`RunInstances`appel. Pour obtenir des exemples de politiques, consultez Modèles de lancement.

EC2 : DescribeLaunchTemplates

Pour répertorier et afficher les modèles de lancement dans le compte, le principal doit avoir l'`ec2:DescribeLaunchTemplates`autorisation requise dans une IAM politique. Parce que les actions `Describe` ne prennent pas en charge les autorisations au niveau des ressources, vous devez les spécifier sans condition et la valeur de l'élément de ressource dans la politique doit être `"*"`.

Par exemple, la déclaration de IAM politique suivante donne au principal l'autorisation de répertorier et d'afficher tous les modèles de lancement du compte.

```
{
    "Sid": "IAMPolicyForDescribingLaunchTemplates",
    "Action": "ec2:DescribeLaunchTemplates",
    "Effect": "Allow",
    "Resource": "*"
}
```

EC2 : DescribeLaunchTemplateVersions

Les responsables qui répertorient et consultent les modèles de lancement doivent également être `ec2:DescribeLaunchTemplateVersions` autorisés à récupérer l'ensemble complet des attributs qui constituent les modèles de lancement.

Pour répertorier et afficher les versions des modèles de lancement dans le compte, le principal doit avoir l'`ec2:DescribeLaunchTemplateVersions`autorisation requise dans une IAM politique. Parce que les actions `Describe` ne prennent pas en charge les autorisations au niveau des

ressources, vous devez les spécifier sans condition et la valeur de l'élément de ressource dans la politique doit être `"*"`.

Par exemple, la déclaration de IAM politique suivante donne au principal l'autorisation de répertorier et d'afficher toutes les versions des modèles de lancement dans le compte.

```
{
    "Sid": "IAMPolicyForDescribingLaunchTemplateVersions",
    "Effect": "Allow",
    "Action": "ec2:DescribeLaunchTemplateVersions",
    "Resource": "*"
}
```

EC2 : DeleteLaunchTemplate

> **Important**
>
> Soyez prudent lorsque vous donnez aux principaux l'autorisation de supprimer une ressource. La suppression d'un modèle de lancement peut entraîner une défaillance d'une AWS ressource qui repose sur le modèle de lancement.

Pour supprimer un modèle de lancement, le principal doit avoir l'`ec2:DeleteLaunchTemplate`autorisation requise dans une IAM politique. Dans la mesure du possible, utilisez des clés de condition basées sur des balises pour limiter les autorisations.

Par exemple, la déclaration de IAM politique suivante donne au principal l'autorisation de supprimer des modèles de lancement uniquement si le modèle possède la balise spécifiée (*`objectif`*=*`test`*).

```
{
    "Sid": "IAMPolicyForDeletingLaunchTemplates",
    "Action": "ec2:DeleteLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/purpose": "testing"
        }
    }
}
```

Vous pouvez également l'utiliser ARNs pour identifier le modèle de lancement auquel s'applique la IAM politique.

Un modèle de lancement présente les caractéristiques suivantesARN.

```
"Resource": "arn:aws:ec2:region:account-id:launch-template/lt-09477bcd97b0d310e"
```

Vous pouvez en spécifier plusieurs ARNs en les plaçant dans une liste, ou vous pouvez spécifier une `Resource` valeur égale à `"*"` sans l'`Condition`élément pour permettre au principal de supprimer tout modèle de lancement du compte.

Contrôler les autorisations de gestion des versions

Pour les administrateurs fiables, vous pouvez accorder l'accès pour créer et supprimer des versions d'un modèle de lancement, et pour modifier la version par défaut d'un modèle de lancement, en utilisant des IAM politiques similaires aux exemples suivants.

> **Important**
>
> Soyez prudent lorsque vous autorisez les principaux à créer des versions de modèles de lancement ou à modifier des modèles de lancement.
>
> - Lorsque vous créez une version du modèle de lancement, vous affectez toutes AWS les ressources qui permettent EC2 à Amazon de lancer des instances en votre nom avec `Latest` cette version.
> - Lorsque vous modifiez un modèle de lancement, vous pouvez changer de version `Default` et, par conséquent, affecter les AWS ressources qui permettent EC2 à Amazon de lancer des instances en votre nom avec cette version modifiée.
>
> Vous devez également faire preuve de prudence dans la manière dont vous gérez les AWS ressources qui interagissent avec la version modèle `Latest` ou qui `Default` lancent une version, telles que EC2 Fleet et Spot Fleet. Lorsqu'une version différente du modèle de lancement est utilisée pour `Latest` ou`Default`, Amazon EC2 ne revérifie pas les autorisations des utilisateurs pour les actions à effectuer lors du lancement de nouvelles instances afin d'atteindre la capacité cible du parc, car il n'y a aucune interaction de l'utilisateur avec la AWS ressource. En accordant à un utilisateur l'autorisation d'appeler le `CreateLaunchTemplateVersion` et `ModifyLaunchTemplate`APIs, l'utilisateur obtient également cette `iam:PassRole` autorisation s'il oriente le parc vers une autre version du

modèle de lancement contenant un profil d'instance (un conteneur pour un IAM rôle). Cela signifie qu'un utilisateur peut potentiellement mettre à jour un modèle de lancement pour transmettre un IAM rôle à une instance même s'il n'en a pas l'`iam:PassRole`autorisation. Vous pouvez gérer ce risque en faisant preuve de prudence lorsque vous accordez des autorisations aux personnes habilitées à créer et à gérer les versions des modèles de lancement.

EC2 : CreateLaunchTemplateVersion

Pour créer une nouvelle version d'un modèle de lancement, le principal doit avoir l'`ec2:CreateLaunchTemplateVersion`autorisation d'utiliser le modèle de lancement dans une IAM politique.

Par exemple, la déclaration de IAM politique suivante donne au principal l'autorisation de créer des versions de modèles de lancement uniquement si la version utilise la balise spécifiée (*`environment`*=*`production`*). Vous pouvez également spécifier un ou plusieurs modèles de lancementARNs, ou vous pouvez spécifier une `Resource` valeur égale à `"*"` sans l'`Condition`élément pour permettre au principal de créer des versions de n'importe quel modèle de lancement dans le compte.

```
{
    "Sid": "IAMPolicyForCreatingLaunchTemplateVersions",
    "Action": "ec2:CreateLaunchTemplateVersion",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

EC2 : DeleteLaunchTemplateVersion

Important

Comme toujours, vous devez faire preuve de prudence lorsque vous autorisez les principaux à supprimer une ressource. La suppression d'une version du modèle de lancement peut

entraîner une défaillance d'une AWS ressource qui repose sur la version du modèle de lancement.

Pour supprimer une version du modèle de lancement, le principal doit avoir l'`ec2:DeleteLaunchTemplateVersion`autorisation d'utiliser le modèle de lancement dans une IAM politique.

Par exemple, la déclaration de IAM politique suivante donne au principal l'autorisation de supprimer les versions du modèle de lancement uniquement si la version utilise la balise spécifiée (*`environment`*=*`production`*). Vous pouvez également spécifier un ou plusieurs modèles de lancementARNs, ou vous pouvez spécifier une `Resource` valeur égale à `"*"` sans l'`Condition`élément pour permettre au principal de supprimer les versions de n'importe quel modèle de lancement dans le compte.

```
{
    "Sid": "IAMPolicyForDeletingLaunchTemplateVersions",
    "Action": "ec2:DeleteLaunchTemplateVersion",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

EC2 : ModifyLaunchTemplate

Pour modifier la `Default` version associée à un modèle de lancement, le principal doit avoir l'`ec2:ModifyLaunchTemplate`autorisation d'utiliser le modèle de lancement dans une IAM politique.

Par exemple, la déclaration de IAM politique suivante donne au principal l'autorisation de modifier les modèles de lancement uniquement si le modèle de lancement utilise la balise spécifiée (*`environment`*=*`production`*). Vous pouvez également spécifier un ou plusieurs modèles de lancementARNs, ou vous pouvez spécifier une `Resource` valeur égale à `"*"` sans l'`Condition`élément pour permettre au principal de modifier n'importe quel modèle de lancement du compte.

```
{
    "Sid": "IAMPolicyForModifyingLaunchTemplates",
    "Action": "ec2:ModifyLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

Contrôler l'accès aux balises sur les modèles de lancement

Vous pouvez utiliser des clés de condition pour limiter les autorisations d'étiquetage lorsque la ressource est un modèle de lancement. Par exemple, la IAM politique suivante permet de supprimer uniquement le tag contenant la *temporary* clé des modèles de lancement dans le compte et la région spécifiés.

```
{
    "Sid": "IAMPolicyForDeletingTagsOnLaunchTemplates",
    "Action": "ec2:DeleteTags",
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
    "Condition": {
        "ForAllValues:StringEquals": {
            "aws:TagKeys": ["temporary"]
        }
    }
}
```

Pour plus d'informations sur les clés de conditions que vous pouvez utiliser pour contrôler les clés de balise et les valeurs qui peuvent être appliquées aux EC2 ressources Amazon, consultezContrôler l'accès à des balises spécifiques.

Utilisez les modèles de EC2 lancement Amazon pour contrôler le lancement EC2 des instances Amazon

Vous pouvez contrôler la configuration de vos EC2 instances Amazon en spécifiant que les utilisateurs ne peuvent lancer des instances que s'ils utilisent un modèle de lancement, et qu'ils

ne peuvent utiliser qu'un modèle de lancement spécifique. Vous pouvez également contrôler qui peut créer, modifier, décrire et supprimer les modèles de lancement et les versions du modèle de lancement.

Utiliser des modèles de lancement pour contrôler les paramètres de lancement

Un modèle de lancement peut contenir tout ou partie des paramètres permettant de configurer une instance au lancement. Toutefois, lorsque vous lancez une instance à l'aide d'un modèle de lancement, vous pouvez remplacer les paramètres spécifiés dans le modèle de lancement. Vous pouvez également spécifier d'autres paramètres qui ne figurent pas dans le modèle de lancement.

> **Note**
>
> Vous ne pouvez pas supprimer les paramètres du modèle de lancement lors du lancement (par exemple, vous ne pouvez pas spécifier de valeur nulle pour le paramètre). Pour supprimer un paramètre, créez une nouvelle version du modèle de lancement sans ce paramètre, puis utilisez cette version pour lancer l'instance.

Pour lancer des instances, les utilisateurs doivent être autorisés à utiliser l'`ec2:RunInstances`action. Les utilisateurs doivent également être autorisés à créer ou à utiliser les ressources créées ou associées à l'instance. Vous pouvez utiliser des autorisations au niveau des ressources pour l'action `ec2:RunInstances` afin de contrôler les paramètres de lancement pouvant être spécifiés par les utilisateurs. Vous pouvez également autoriser les utilisateurs à lancer une instance à l'aide d'un modèle de lancement. Cela vous permet de gérer les paramètres de lancement dans un modèle de lancement plutôt que dans une IAM politique, et d'utiliser un modèle de lancement comme véhicule d'autorisation pour le lancement d'instances. Par exemple, vous pouvez spécifier que les utilisateurs peuvent uniquement lancer des instances à l'aide d'un modèle de lancement et qu'ils peuvent uniquement utiliser un modèle de lancement spécifique. Vous pouvez également contrôler les paramètres de lancement que les utilisateurs peuvent remplacer dans le modèle de lancement. Pour obtenir des exemples de politiques, consultez Modèles de lancement.

Contrôler l'utilisation des modèles de lancement

Par défaut, les utilisateurs d' ne sont pas autorisés à utiliser des modèles de lancement. Vous pouvez créer une stratégie qui autorise les utilisateurs à créer, modifier, décrire et supprimer des modèles de lancement et leurs versions. Vous pouvez également appliquer des autorisations au niveau des ressources à certaines actions de modèle de lancement pour contrôler la capacité d'un utilisateur à

utiliser des ressources spécifiques pour ces actions. Pour plus d'informations, consultez Exemple : Utiliser des modèles de lancement.

Soyez vigilant lorsque vous autorisez des utilisateurs à effectuer les actions `ec2:CreateLaunchTemplate` et `ec2:CreateLaunchTemplateVersion`. Vous ne pouvez pas utiliser les autorisations au niveau des ressources pour contrôler les ressources que les utilisateurs peuvent spécifier dans le modèle de lancement. Pour limiter les ressources utilisées pour lancer une instance, veillez à autoriser uniquement les administrateurs appropriés à créer des modèles de lancement et des versions de modèles de lancement.

Problèmes de sécurité importants lors de l'utilisation de modèles de lancement avec EC2 Fleet ou Spot Fleet

Pour utiliser les modèles de lancement, vous devez accorder à vos utilisateurs des autorisations pour créer, modifier, décrire et supprimer des modèles de lancement et leurs versions. Vous pouvez contrôler qui peut créer des modèles de lancement et des versions de modèles en contrôlant l'accès aux actions `ec2:CreateLaunchTemplate` et `ec2:CreateLaunchTemplateVersion`. Vous pouvez également contrôler qui peut modifier les modèles de lancement en contrôlant l'accès à l'action `ec2:ModifyLaunchTemplate`.

> **Important**
>
> Si une EC2 flotte ou une flotte ponctuelle est configurée pour utiliser la version la plus récente ou la version par défaut du modèle de lancement, la flotte ne sait pas si la version la plus récente ou la version par défaut sont modifiées ultérieurement pour pointer vers une autre version du modèle de lancement. Lorsqu'une version différente du modèle de lancement est utilisée pour Latest ou Default, Amazon EC2 ne revérifie pas les autorisations relatives aux actions à effectuer lors du lancement de nouvelles instances afin d'atteindre la capacité cible de la flotte. Il s'agit d'une considération importante lorsque vous accordez des autorisations aux personnes qui peuvent créer et gérer des versions de modèles de lancement, en particulier l'action `ec2:ModifyLaunchTemplate` qui permet à un utilisateur de modifier la version de modèle de lancement « Par défaut ».

En accordant à un utilisateur l'autorisation d'utiliser les EC2 actions du modèle de lancementAPIs, l'utilisateur obtient également l'`iam:PassRole`autorisation s'il crée ou met à jour une EC2 flotte ou une flotte ponctuelle afin de pointer vers une autre version du modèle de lancement contenant un profil d'instance (un conteneur pour un IAM rôle). Cela signifie qu'un utilisateur peut potentiellement

mettre à jour un modèle de lancement pour transmettre un IAM rôle à une instance même s'il n'en a pas l'`iam:PassRole`autorisation. Pour plus d'informations et un exemple de IAM politique, consultez la section Utilisation d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le Guide de IAM l'utilisateur.

Pour plus d'informations, consultez Contrôler l'utilisation des modèles de lancement et Exemple : Utiliser des modèles de lancement.

Création d'un modèle de EC2 lancement Amazon

Vous pouvez créer un modèle de EC2 lancement Amazon en spécifiant vos propres valeurs pour les paramètres de configuration de l'instance, ou en obtenant les valeurs d'un modèle de lancement ou d'une EC2 instance Amazon existant.

Il n'est pas nécessaire de spécifier une valeur pour chaque paramètre du modèle de lancement ; il suffit de spécifier un paramètre de configuration d'instance pour créer un modèle de lancement. Pour indiquer les paramètres que vous choisissez de ne pas spécifier, sélectionnez Ne pas inclure dans le modèle de lancement lorsque vous utilisez la console. Lorsque vous utilisez un outil de ligne de commande, n'incluez pas les paramètres pour indiquer que vous choisissez de ne pas les spécifier dans le modèle de lancement.

Si vous souhaitez en spécifier un AMI dans le modèle de lancement, vous pouvez soit sélectionner unAMI, soit spécifier un paramètre Systems Manager qui pointera vers un lancement AMI sur instance.

Lorsqu'une instance est lancée avec un modèle de lancement, les valeurs spécifiées dans le modèle de lancement sont utilisées pour configurer les paramètres d'instance correspondants. Si aucune valeur n'est spécifiée dans le modèle de lancement, la valeur par défaut du paramètre d'instance correspondant est utilisée.

Tâches

- Création d'un modèle de lancement en spécifiant des paramètres
- Créer un modèle de lancement à partir d'un modèle de lancement existant
- Créer un modèle de lancement à partir d'une instance
- Utiliser un paramètre Systems Manager au lieu d'un AMI ID

Création d'un modèle de lancement en spécifiant des paramètres

Pour créer un modèle de lancement, vous devez spécifier son nom et au moins un paramètre de configuration d'instance.

Pour une description de chaque paramètre, voirRéférence pour les paramètres de configuration des EC2 instances Amazon.

Console

Pour créer un modèle de lancement à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Modèles de lancement, puis Créer un modèle de lancement.
3. Sous Nom et description du modèle de lancement, procédez comme suit :
   a. Pour Nom du modèle de lancement, entrez un nom descriptif pour le modèle.
   b. Pour Description de la version du modèle, fournissez une brève description de cette version du modèle de lancement.
   c. Pour étiqueter le modèle de lancement lors de sa création, développez les balises du modèle, choisissez Ajouter une nouvelle balise, puis entrez une clé de balise et une paire de valeurs. Choisissez à nouveau Ajouter une nouvelle balise pour chaque balise supplémentaire à ajouter.

   > **Note**
   >
   > Pour étiqueter les ressources créées lors du lancement d'une instance, vous devez spécifier les identifications sous Resource tags (Identifications de ressource). Pour plus d'informations, reportez-vous à l'étape 9 de cette procédure.

4. Sous Images de l'application et du système d'exploitation (Amazon Machine Image), vous pouvez soit garder Ne pas inclure dans le modèle de lancement sélectionné, soit choisir le système d'exploitation (OS) de l'instance, puis en choisir unAMI. Vous pouvez également spécifier un paramètre Systems Manager au lieu de spécifier unAMI. Pour de plus amples informations, veuillez consulter Utiliser un paramètre Systems Manager au lieu d'un AMI ID.

An AMI est un modèle qui contient le système d'exploitation et le logiciel requis pour lancer une instance.

5. Sous Type d'instance, vous pouvez soit conserver la case Ne pas inclure dans le modèle de lancement sélectionnée, soit sélectionner un type d'instance, soit spécifier les attributs de l'instance et laisser Amazon EC2 identifier les types d'instance avec ces attributs.

> **Note**
>
> La spécification des attributs d'instance n'est prise en charge que lorsque le modèle de lancement est utilisé par les groupes Auto Scaling, EC2 Fleet et Spot Fleet pour lancer des instances. Pour plus d'informations, consultez Création d'un groupe Auto Scaling à l'aide de la sélection du type d'instance basée sur les attributs et. Spécifiez les attributs pour la sélection du type d'instance pour EC2 Fleet ou Spot Fleet
> Si vous prévoyez d'utiliser le modèle de lancement dans l'assistant de lancement d'instance ou avec le RunInstances API, vous ne pouvez pas spécifier d'attributs de type d'instance.

Le type d'instance détermine la configuration matérielle (mémoireCPU, stockage et capacité réseau) et la taille de l'ordinateur hôte utilisé pour une instance.

Si vous ne savez pas quel type d'instance choisir, vous pouvez effectuer les opérations suivantes :

- Choisissez Comparer les types d'instances pour comparer différents types d'instances en fonction des attributs suivants : nombre devCPUs, architecture, quantité de mémoire (GiB), quantité de stockage (Go), type de stockage et performances du réseau.
- Choisissez Obtenir des conseils pour obtenir des conseils et des suggestions concernant les types d'instances à partir de l'outil de recherche de types d'EC2instance. Pour de plus amples informations, veuillez consulter Obtenez des recommandations depuis l'outil de recherche de types d'EC2instance.

> **Note**
>
> Si vous avez moins de 12 mois, vous pouvez utiliser Amazon EC2 dans le cadre du niveau gratuit en choisissant le type d'instance t2.micro ou le type d'instance t3.micro

dans les régions où t2.micro Compte AWS n'est pas disponible. Sachez que lorsque vous lancez une instance t3.micro, elle passe par défaut en mode illimité, ce qui peut entraîner des frais supplémentaires en fonction de l'utilisation. CPU Si un type d'instance est éligible dans le cadre du niveau gratuit, il est étiqueté Free tier eligible (Éligible à l'offre gratuite).

6. Sous Paire de clés (connexion), pour le nom de la paire de clés, maintenez la case Ne pas inclure dans le modèle de lancement sélectionnée, choisissez une paire de clés existante ou créez-en une nouvelle.
7. Sous Paramètres réseau, vous pouvez soit conserver l'option Ne pas inclure dans le modèle de lancement sélectionnée, soit spécifier des valeurs pour les différents paramètres réseau.
8. Sous Configurer le stockage, si vous avez spécifié un AMI dans le modèle de lancement, celui-ci AMI inclut un ou plusieurs volumes de stockage, y compris le volume racine (volume 1 (AMIracine)). Vous pouvez éventuellement spécifier des volumes supplémentaires à associer à l'instance. Pour ajouter un nouveau volume, choisissez Ajouter un volume.
9. Sous Balises de ressources, pour étiqueter les ressources créées lors du lancement d'une instance, choisissez Ajouter une balise, puis entrez une clé de balise et une paire de valeurs. Pour Resource types (Types de ressource), spécifiez les ressources à étiqueter lors de la création. Vous pouvez spécifier la même identification pour toutes les ressources ou spécifier des identifications différentes pour différentes ressources. Choisissez Add tag (Ajouter une identification) pour chaque étiquette supplémentaire.

   Vous pouvez spécifier des identifications pour les ressources suivantes qui sont créées lorsqu'un modèle de lancement est utilisé :

   - instances
   - Volumes
   - Elastic Graphics
   - Demandes d'instance Spot
   - Interfaces réseau

> **Note**
>
> Pour étiqueter le modèle de lancement lui-même, vous devez spécifier les identifications sous Template tags (Identifications de modèle). Pour plus d'informations, reportez-vous à l'étape 3 de cette procédure.

10. Pour les informations avancées, développez la section pour afficher les champs et spécifiez éventuellement des paramètres supplémentaires pour votre instance.
11. Utilisez le panneau Résumé pour vérifier la configuration de votre modèle de lancement. Vous pouvez accéder à n'importe quelle section en choisissant son lien, puis en apportant les modifications nécessaires.
12. Lorsque vous êtes prêt à créer votre modèle de lancement, choisissezCreate launch template (Créer un modèle de lancement).

AWS CLI

L'exemple suivant utilise la create-launch-templatecommande pour créer un modèle de lancement avec le nom et la configuration d'instance spécifiés.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --version-description WebVersion1 \
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

L'exemple suivant JSON indique les données du modèle de lancement pour la configuration de l'instance. Enregistrez le JSON dans un fichier et incluez-le dans le `--launch-template-data` paramètre, comme indiqué dans l'exemple de commande.

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-7b16de0c"
    }],
```

```
    "ImageId": "ami-8c1be5f6",
    "InstanceType": "r4.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":4,
        "ThreadsPerCore":2
    }
}
```

Voici un exemple de sortie.

```
{
    "LaunchTemplate": {
        "LatestVersionNumber": 1,
        "LaunchTemplateId": "lt-01238c059e3466abc",
        "LaunchTemplateName": "TemplateForWebServer",
        "DefaultVersionNumber": 1,
        "CreatedBy": "arn:aws:iam::123456789012:root",
        "CreateTime": "2017-11-27T09:13:24.000Z"
    }
}
```

PowerShell

L'exemple suivant utilise l'New-EC2LaunchTemplateapplet de commande pour créer un modèle de lancement avec le nom et la configuration d'instance spécifiés.

```
$launchTemplateData = [Amazon.EC2.Model.RequestLaunchTemplateData]@{
    ImageId = 'ami-8c1be5f6'
    InstanceType = 'r4.4xlarge'
    NetworkInterfaces = @(

 [Amazon.EC2.Model.LaunchTemplateInstanceNetworkInterfaceSpecificationRequest]@{
            AssociatePublicIpAddress = $true
            DeviceIndex = 0
            Ipv6AddressCount = 1
            SubnetId = 'subnet-7b16de0c'
```

```
        }
    )
    TagSpecifications = @(
        [Amazon.EC2.Model.LaunchTemplateTagSpecificationRequest]@{
            ResourceType = 'instance'
            Tags = [Amazon.EC2.Model.Tag]@{
                Key = 'Name'
                Value = 'webserver'
            }
        }
    )
    CpuOptions = [Amazon.EC2.Model.LaunchTemplateCpuOptionsRequest]@{
        CoreCount = 4
        ThreadsPerCore = 2
    }
}
$tagSpecificationData = [Amazon.EC2.Model.TagSpecification]@{
    ResourceType = 'launch-template'
    Tags = [Amazon.EC2.Model.Tag]@{
        Key = 'purpose'
        Value = 'production'
    }
}
New-EC2LaunchTemplate -LaunchTemplateName 'TemplateForWebServer' -VersionDescription
 'WebVersion1' -LaunchTemplateData $launchTemplateData -TagSpecification
 $tagSpecificationData
```

Voici un exemple de sortie.

```
CreatedBy            : arn:aws:iam::123456789012:root
CreateTime           : 9/19/2023 16:57:55
DefaultVersionNumber : 1
LatestVersionNumber  : 1
LaunchTemplateId     : lt-01238c059eEXAMPLE
LaunchTemplateName   : TemplateForWebServer
Tags                 : {purpose}
```

Créer un modèle de lancement à partir d'un modèle de lancement existant

Vous pouvez cloner un modèle de lancement existant, puis ajuster les paramètres pour créer un modèle de lancement. Toutefois, vous ne pouvez le faire que lorsque vous utilisez la EC2 console

Amazon. Le AWS CLI ne prend pas en charge le clonage d'un modèle. Pour une description de chaque paramètre, voirRéférence pour les paramètres de configuration des EC2 instances Amazon.

Console

Pour créer un modèle de lancement à partir d'un modèle de lancement existant

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Modèles de lancement, puis Créer un modèle de lancement.
3. Pour Nom du modèle de lancement, entrez un nom descriptif pour le modèle.
4. Pour Description de la version du modèle, fournissez une brève description de cette version du modèle de lancement.
5. Pour étiqueter le modèle de lancement lors de sa création, développez les balises du modèle, choisissez Ajouter une nouvelle balise, puis entrez une clé de balise et une paire de valeurs.
6. Développez Modèle source, et, pour Nom du modèle de lancement, choisissez un modèle de lancement sur lequel baser le nouveau modèle.
7. Pour Version du modèle source, choisissez la version du modèle de lancement sur laquelle baser le nouveau modèle de lancement.
8. Ajustez les paramètres de lancement si nécessaire, puis choisissez Créer un modèle de lancement.

Créer un modèle de lancement à partir d'une instance

Vous pouvez cloner les paramètres d'une EC2 instance Amazon existante, puis les ajuster pour créer un modèle de lancement. Pour une description de chaque paramètre, voirRéférence pour les paramètres de configuration des EC2 instances Amazon.

Console

Pour créer un modèle de lancement à partir d'une instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance, puis choisissez Actions, Image et modèles, puis Créer un modèle à partir de l'instance.

4. Indiquez un nom, une description eet des balises, puis ajustez les paramètres de lancement si nécessaire.

> **Note**
>
> Lorsque vous créez un modèle de lancement à partir d'une instance, l'interface réseau IDs et les adresses IP de l'instance ne sont pas incluses dans le modèle.

5. Choisissez Créer un modèle de lancement.

AWS CLI

Vous pouvez utiliser le AWS CLI pour créer un modèle de lancement à partir d'une instance existante en obtenant d'abord les données du modèle de lancement à partir d'une instance, puis en créant un modèle de lancement à l'aide des données du modèle de lancement.

Pour obtenir des données de modèle de lancement à partir d'une instance

- Utilisez la get-launch-template-datacommande et spécifiez l'ID de l'instance. Vous pouvez utiliser la sortie comme base pour créer un modèle de lancement ou une version de modèle de lancement. Par défaut, la sortie contient un objet `LaunchTemplateData` de niveau supérieur qui ne peut pas être spécifié dans les données de modèle de lancement. Excluez cet objet à l'aide de l'option `--query`.

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData"
```

Voici un exemple de sortie.

```
    {
        "Monitoring": {},
        "ImageId": "ami-8c1be5f6",
        "BlockDeviceMappings": [
            {
                "DeviceName": "/dev/xvda",
                "Ebs": {
                    "DeleteOnTermination": true
                }
            }
```

```
        ],
        "EbsOptimized": false,
        "Placement": {
            "Tenancy": "default",
            "GroupName": "",
            "AvailabilityZone": "us-east-1a"
        },
        "InstanceType": "t2.micro",
        "NetworkInterfaces": [
            {
                "Description": "",
                "NetworkInterfaceId": "eni-35306abc",
                "PrivateIpAddresses": [
                    {
                        "Primary": true,
                        "PrivateIpAddress": "10.0.0.72"
                    }
                ],
                "SubnetId": "subnet-7b16de0c",
                "Groups": [
                    "sg-7c227019"
                ],
                "Ipv6Addresses": [
                    {
                        "Ipv6Address": "2001:db8:1234:1a00::123"
                    }
                ],
                "PrivateIpAddress": "10.0.0.72"
            }
        ]
    }
```

Par exemple, vous pouvez écrire directement la sortie dans un fichier :

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData" >> instance-data.json
```

Pour créer un modèle de lancement à l'aide des données du modèle de lancement

- Utilisez la create-launch-templatecommande pour créer un modèle de lancement en utilisant le résultat de la procédure précédente. Pour plus d'informations sur la création d'un

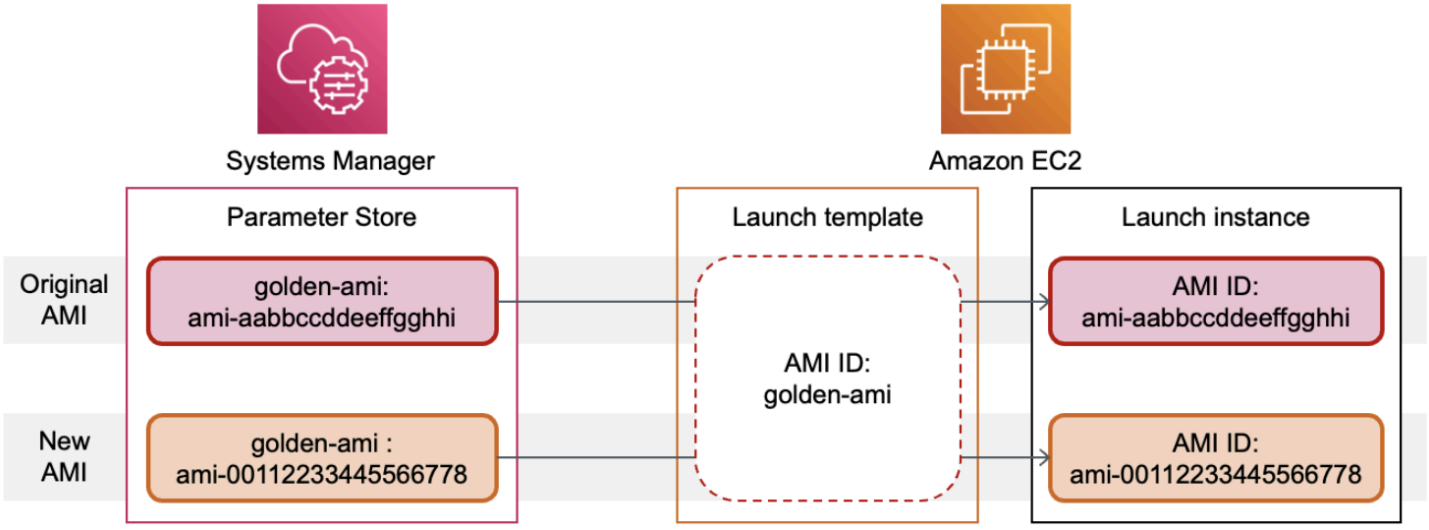
modèle de lancement à l'aide du AWS CLI, consultezCréation d'un modèle de lancement en spécifiant des paramètres.

Utiliser un paramètre Systems Manager au lieu d'un AMI ID

Au lieu de spécifier un AMI identifiant dans vos modèles de lancement, vous pouvez spécifier un AWS Systems Manager paramètre. Si l'AMIidentifiant change, vous pouvez le AMI mettre à jour en un seul endroit en mettant à jour le paramètre Systems Manager dans le magasin de paramètres Systems Manager. Les paramètres peuvent également être partagés avec d'autres Comptes AWS. Vous pouvez stocker et gérer les AMI paramètres de manière centralisée dans un seul compte et les partager avec tous les autres comptes qui ont besoin de les référencer. En utilisant un paramètre Systems Manager, tous vos modèles de lancement peuvent être mis à jour en une seule action.

Un paramètre Systems Manager est une paire clé-valeur définie par l'utilisateur que vous créez dans le AWS Systems Manager Parameter Store. Le stockage de paramètres est un endroit central où vous pouvez stocker les valeurs de configuration de votre application.

Dans le schéma suivant, le `golden-ami` paramètre est d'abord mappé à l'original AMI `ami-aabbccddeeffgghhi` dans le Parameter Store. Dans le modèle de lancement, la valeur de l'AMIID est`golden-ami`. Lorsqu'une instance est lancée à l'aide de ce modèle de lancement, l'AMIID devient`ami-aabbccddeeffgghhi`. Plus tard, AMI il est mis à jour, ce qui entraîne un nouvel AMI identifiant. Dans le stockage de paramètres, le paramètre `golden-ami` est mappé au nouveau `ami-00112233445566778`. Le modèle de lancement reste inchangé. Lorsqu'une instance est lancée à l'aide de ce modèle de lancement, l'AMIID est remplacé par le nouveau`ami-00112233445566778`.



Format des paramètres de Systems Manager pour AMI IDs

Les modèles de lancement nécessitent que les paramètres de Systems Manager définis par l'utilisateur respectent le format suivant lorsqu'ils sont utilisés à la place d'un AMI identifiant :

- Type de paramètre : `String`
- Type de données de paramètre : `aws:ec2:image` — Cela garantit que Parameter Store valide que la valeur que vous entrez est au format approprié pour un AMI ID.

Pour plus d'informations sur la création d'un paramètre valide pour un AMI ID, consultez la section Création des paramètres de Systems Manager dans le guide de AWS Systems Manager l'utilisateur.

Format des paramètres Systems Manager dans les modèles de lancement

Pour utiliser un paramètre Systems Manager à la place d'un AMI identifiant dans un modèle de lancement, vous devez utiliser l'un des formats suivants lorsque vous spécifiez le paramètre dans le modèle de lancement :

Pour référencer un paramètre public :

- `resolve:ssm:`*`public-parameter`*

Pour référencer un paramètre stocké dans le même compte :

- `resolve:ssm:`*`parameter-name`*
- `resolve:ssm:`*`parameter-name`*`:`*`version-number`* – Le numéro de version lui-même est une étiquette par défaut
- `resolve:ssm:`*`parameter-name`*`:`*`label`*

Pour référencer un paramètre partagé par un autre Compte AWS :

- `resolve:ssm:`*`parameter-ARN`*
- `resolve:ssm:`*`parameter-ARN`*`:`*`version-number`*
- `resolve:ssm:`*`parameter-ARN`*`:`*`label`*

Versions des paramètres

Les paramètres Systems Manager sont des ressources versionnées. Lorsque vous mettez à jour un paramètre, vous créez de nouvelles versions successives du paramètre. Systems Manager prend en charge les étiquettes de paramètres que vous pouvez associer à des versions spécifiques d'un paramètre.

Par exemple, le paramètre `golden-ami` peut avoir trois versions : `1`, `2` et `3`. Vous pouvez créer une étiquette de paramètre `beta` qui correspond à la version `2` et une étiquette de paramètre `prod` qui correspond à la version `3`.

Dans un modèle de lancement, vous pouvez spécifier la version 3 du paramètre `golden-ami` en utilisant l'un des formats suivants :

- `resolve:ssm:golden-ami:3`
- `resolve:ssm:golden-ami:prod`

La spécification de la version ou de l'étiquette est facultative. Si aucune version ou étiquette n'est spécifiée, c'est la dernière version du paramètre qui est utilisée.

Spécifier un paramètre Systems Manager dans un modèle de lancement

Vous pouvez spécifier un paramètre Systems Manager dans un modèle de lancement au lieu d'un AMI ID lorsque vous créez un modèle de lancement ou une nouvelle version d'un modèle de lancement.

Console

Pour spécifier un paramètre Systems Manager dans un modèle de lancement

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Modèles de lancement, puis Créer un modèle de lancement.
3. Pour Nom du modèle de lancement, entrez un nom descriptif pour le modèle.
4. Sous Images de l'application et du système d'exploitation (Amazon Machine Image), sélectionnez Parcourir davantage AMIs.
5. Sélectionnez le bouton fléché à droite de la barre de recherche, puis choisissez Spécifier une valeur personnalisée/un paramètre Systems Manager.
6. Dans la boîte de dialogue Spécifier une valeur personnalisée ou un paramètre Systems Manager, procédez comme suit :

a. Pour la chaîne de paramètres AMI ID ou Systems Manager, entrez le nom du paramètre Systems Manager en utilisant l'un des formats suivants :

   Pour référencer un paramètre public :

   - **resolve:ssm:*public-parameter***

   Pour référencer un paramètre stocké dans le même compte :

   - **resolve:ssm:*parameter-name***
   - **resolve:ssm:*parameter-name*:*version-number***
   - **resolve:ssm:*parameter-name*:*label***

   Pour référencer un paramètre partagé par un autre Compte AWS :

   - **resolve:ssm:*parameter-ARN***
   - **resolve:ssm:*parameter-ARN*:*version-number***
   - **resolve:ssm:*parameter-ARN*:*label***

b. Choisissez Save (Enregistrer).

7. Spécifiez tout autre paramètre de modèle de lancement selon vos besoins, puis choisissez Créer un modèle de lancement.

Pour de plus amples informations, veuillez consulter Création d'un modèle de lancement en spécifiant des paramètres.

AWS CLI

Pour spécifier un paramètre Systems Manager dans un modèle de lancement

- Utilisez la create-launch-templatecommande pour créer le modèle de lancement. Pour spécifier le paramètre AMI à utiliser, entrez le nom du paramètre Systems Manager en utilisant l'un des formats suivants :

  Pour référencer un paramètre public :

  - **resolve:ssm:*public-parameter***

Pour référencer un paramètre stocké dans le même compte :

- **resolve:ssm:*parameter-name***
- **resolve:ssm:*parameter-name*:*version-number***
- **resolve:ssm:*parameter-name*:*label***

Pour référencer un paramètre partagé par un autre Compte AWS :

- **resolve:ssm:*parameter-ARN***
- **resolve:ssm:*parameter-ARN*:*version-number***
- **resolve:ssm:*parameter-ARN*:*label***

L'exemple suivant crée un modèle de lancement qui spécifie ce qui suit :

- Nom du modèle de lancement (*TemplateForWebServer*)
- Une balise pour le modèle de lancement (*purpose*=*production*)
- Les données pour la configuration de l'instance, spécifiées dans un JSON fichier :
  - Le AMI à utiliser (`resolve:ssm:`*golden-ami*)
  - Le type d'instance à lancer (*m5.4xlarge*)
  - Une balise pour l'instance (*Name*=*webserver*)

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

Voici un exemple de JSON fichier contenant les données du modèle de lancement pour la configuration de l'instance. La valeur pour `ImageId` est le nom du paramètre Systems Manager, saisi au format requis `resolve:ssm:`*golden-ami*.

```
{"LaunchTemplateData": {
    "ImageId": "resolve:ssm:golden-ami",
    "InstanceType": "m5.4xlarge",
```

```
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }]
  }
}
```

Vérifiez qu'un modèle de lancement reçoit le bon AMI identifiant

Pour convertir le paramètre Systems Manager à l'AMIID réel

Utilisez la describe-launch-template-versionscommande et incluez le `--resolve-alias` paramètre.

```
aws ec2 describe-launch-template-versions \
    --launch-template-name my-launch-template \
    --versions $Default \
    --resolve-alias
```

La réponse inclut l'AMIidentifiant de`ImageId`. Dans cet exemple, lorsqu'une instance est lancée à l'aide de ce modèle de lancement, l'AMIID est converti en`ami-0ac394d6a3example`.

```
{
    "LaunchTemplateVersions": [
        {
            "LaunchTemplateId": "lt-089c023a30example",
            "LaunchTemplateName": "my-launch-template",
            "VersionNumber": 1,
            "CreateTime": "2022-12-28T19:52:27.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Bob",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0ac394d6a3example",
                "InstanceType": "t3.micro",
            }
        }
    ]
}
```

Ressources connexes

Pour plus d'informations sur l'utilisation des paramètres de Systems Manager, consultez les documents de référence suivants dans la documentation de Systems Manager.

- Pour plus d'informations sur la manière de rechercher les paramètres AMI publics pris en charge par AmazonEC2, consultez la section Paramètres AMI publics des appels.
- Pour plus d'informations sur le partage de paramètres avec d'autres AWS comptes ou via d'autres comptes AWS Organizations, consultez la section Utilisation de paramètres partagés.
- Pour plus d'informations sur le suivi de la création réussie de vos paramètres, consultez la section Prise en charge des paramètres natifs pour Amazon Machine Image IDs.

Limites

- Seules EC2 les flottes de type Fleets `instant` prennent en charge l'utilisation d'un modèle de lancement dont le paramètre Systems Manager est spécifié à la place d'un AMI ID.
- EC2Les flottes de type `maintain` et`request`, et les flottes ponctuelles ne prennent pas en charge l'utilisation d'un modèle de lancement dont le paramètre Systems Manager est spécifié à la place d'un AMI identifiant. Pour les EC2 flottes de type A `maintain` et`request`, et pour les flottes ponctuelles, si vous spécifiez un AMI dans le modèle de lancement, vous devez spécifier l'AMIID.
- Si vous utilisez la sélection d'instance basée sur les attributs dans votre EC2 flotte, vous ne pouvez pas spécifier de paramètre Systems Manager à la place d'un AMI ID. Lorsque vous utilisez la sélection d'instance basée sur les attributs, vous devez spécifier l'AMIID.
- Amazon EC2 Auto Scaling propose d'autres restrictions. Pour plus d'informations, consultez la section Utiliser AWS Systems Manager les paramètres plutôt que AMI IDs dans les modèles de lancement dans le manuel Amazon EC2 Auto Scaling User Guide.

Modifier un modèle de lancement (gérer les versions du modèle de lancement)

Les modèles de lancement sont inaltérables ; une fois que vous avez créé un modèle de lancement, vous ne pouvez plus le modifier. Au lieu de cela, vous pouvez créer une nouvelle version du modèle de lancement qui inclut toutes les modifications nécessaires.

Vous pouvez créer différentes versions d'un modèle de lancement, définir la version par défaut, décrire une version du modèle de lancement et supprimer les versions dont vous n'avez plus besoin.

Tâches

- Créer une version d'un modèle de lancement
- Définir la version par défaut du modèle de lancement
- Décrire une version du modèle de lancement

Créer une version d'un modèle de lancement

Lorsque vous créez une version d'un modèle de lancement, vous pouvez spécifier de nouveaux paramètres de lancement ou utiliser une version existante comme base de la nouvelle version. Pour une description de chaque paramètre, voirRéférence pour les paramètres de configuration des EC2 instances Amazon.

Console

Pour créer une version d'un modèle de lancement

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Modèles de lancement.
3. Sélectionnez un modèle de lancement, puis choisissez Actions, Modify template (Create new version) (Modifier le modèle (Créer une nouvelle version)).
4. Pour Description de la version du modèle, saisissez une description pour cette version du modèle de lancement.
5. (Facultatif) Développez Modèle source et sélectionnez une version du modèle de lancement à utiliser comme base pour la nouvelle version du modèle. La nouvelle version de modèle de lancement hérite des paramètres de lancement de cette version.
6. Modifiez les paramètres de lancement selon vos besoins.
7. Choisissez Créer un modèle de lancement.

AWS CLI

Pour créer une version d'un modèle de lancement

- Utilisez la create-launch-template-versioncommande. Vous pouvez spécifier une version source sur laquelle baser la nouvelle version. La nouvelle version hérite des paramètres de lancement de cette version et vous pouvez les remplacer en utilisant `--launch-template-`

`data`. L'exemple suivant crée une nouvelle version basée sur la version 1 du modèle de lancement et spécifie un AMI identifiant différent.

```
aws ec2 create-launch-template-version \
    --launch-template-id lt-0abcd290751193123 \
    --version-description WebVersion2 \
    --source-version 1 \
    --launch-template-data "ImageId=ami-c998b6b2"
```

PowerShell

Utilisez l'New-EC2LaunchTemplateVersionapplet de commande. Vous pouvez spécifier une version source sur laquelle baser la nouvelle version. La nouvelle version hérite des paramètres de lancement de cette version et vous pouvez les remplacer en utilisant `LaunchTemplateData`. L'exemple suivant crée une nouvelle version basée sur la version 1 du modèle de lancement et spécifie un AMI identifiant différent.

```
New-EC2LaunchTemplateVersion `
    -LaunchTemplateId lt-0abcd290751193123 `
    -VersionDescription WebVersion2 `
    -SourceVersion 1 `
    -LaunchTemplateData (
        New-Object `
            -TypeName Amazon.EC2.Model.RequestLaunchTemplateData `
            -Property @{ImageId = 'ami-c998b6b2'}
    )
```

Définir la version par défaut du modèle de lancement

Vous pouvez définir la version par défaut du modèle de lancement. Si vous lancez une instance à partir d'un modèle de lancement sans spécifier de version, le lancement est effectué à l'aide des paramètres de la version par défaut.

Console

Pour définir la version par défaut du modèle de lancement

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Modèles de lancement.

3. Sélectionnez le modèle de lancement et choisissez Actions, Définir la version par défaut.
4. Pour Version du modèle, sélectionnez le numéro de la version à définir par défaut et choisissez Définir comme version par défaut.

AWS CLI

Pour définir la version par défaut du modèle de lancement

- Utilisez la modify-launch-templatecommande et spécifiez la version que vous souhaitez définir comme version par défaut.

```
aws ec2 modify-launch-template \
    --launch-template-id lt-0abcd290751193123 \
    --default-version 2
```

PowerShell

Utilisez l'Edit-EC2LaunchTemplateapplet de commande et spécifiez la version que vous souhaitez définir par défaut.

```
Edit-EC2LaunchTemplate `
    -LaunchTemplateId lt-0abcd290751193123 `
    -DefaultVersion 2
```

Décrire une version du modèle de lancement

À l'aide de la console, vous pouvez afficher toutes les versions du modèle de lancement sélectionné ou obtenir une liste des modèles de lancement dont la version la plus récente ou par défaut correspond à un numéro de version spécifique. À l'aide du AWS CLI, vous pouvez décrire toutes les versions, les versions individuelles ou une série de versions d'un modèle de lancement spécifique. Vous pouvez également décrire toutes les dernières versions ou toutes les versions par défaut de tous les modèles de lancement de votre compte.

Console

Pour décrire une version du modèle de lancement

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

2. Dans le panneau de navigation, choisissez Modèles de lancement.
3. Vous pouvez afficher une version d'un modèle de lancement spécifique ou obtenir une liste des modèles de lancement dont la version la plus récente ou par défaut correspond à un numéro de version spécifique.
   - Pour afficher une version d'un modèle de lancement : sélectionnez le modèle de lancement. Sous l'onglet Versions dans Version, sélectionnez une version pour afficher ses détails.
   - Pour obtenir une liste de tous les modèles de lancement dont la dernière version correspond à un numéro de version spécifique : dans la barre de recherche, choisissez Dernière version, puis sélectionnez un numéro de version.
   - Pour obtenir la liste de tous les modèles de lancement dont la version par défaut correspond à un numéro de version spécifique : dans la barre de recherche, choisissez Version par défaut, puis sélectionnez un numéro de version.

AWS CLI

Pour décrire une version du modèle de lancement

- Utilisez la describe-launch-template-versionscommande et spécifiez les numéros de version. Dans l'exemple suivant, les versions *1* et *3* sont spécifiés.

```
aws ec2 describe-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1 3
```

Pour décrire toutes les versions du modèle de lancement les plus récentes et par défaut de votre compte

- Utilisez la describe-launch-template-versionscommande et spécifiez `$Latest``$Default`, ou les deux. Vous devez omettre l'ID et le nom du modèle de lancement dans l'appel. Vous ne pouvez pas spécifier de numéros de version.

```
aws ec2 describe-launch-template-versions \
    --versions "$Latest,$Default"
```

PowerShell

Pour décrire une version du modèle de lancement

- Utilisez l'Get-EC2TemplateVersionapplet de commande et spécifiez les numéros de version. Dans l'exemple suivant, les versions *1* et *3* sont spécifiés.

```
Get-EC2TemplateVersion `
    -LaunchTemplateId lt-0abcd290751193123 `
    -Version 1,3
```

Pour décrire toutes les versions du modèle de lancement les plus récentes et par défaut de votre compte

- Utilisez l'Get-EC2TemplateVersionapplet de commande et spécifiez `$Latest$Default`, ou les deux. Vous devez omettre l'ID et le nom du modèle de lancement dans l'appel. Vous ne pouvez pas spécifier de numéros de version.

```
Get-EC2TemplateVersion `
    -Version '$Latest','$Default'
```

Supprimer un modèle de lancement ou une version du modèle de lancement

Si vous n'avez plus besoin d'un modèle de lancement, vous pouvez le supprimer. La suppression d'un modèle de lancement entraîne celle de toutes ses versions. Si vous souhaitez uniquement supprimer une version spécifique d'un modèle de lancement, vous pouvez le faire tout en conservant les autres versions du modèle de lancement.

La suppression d'un modèle de lancement ou d'une version de modèle de lancement n'a aucune incidence sur les instances que vous avez lancées à partir du modèle de lancement.

Supprimer un modèle de lancement et toutes ses versions

Si vous n'avez plus besoin d'un modèle de lancement, y compris de toutes ses versions, vous pouvez le supprimer. La suppression d'un modèle de lancement entraîne celle de toutes ses versions.

Console

Pour supprimer un modèle de lancement et toutes ses versions

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Modèles de lancement.
3. Sélectionnez le modèle de lancement et choisissez Actions, Supprimer le modèle.
4. Entrez **`Delete`** pour confirmer la suppression, puis choisissez Supprimer.

AWS CLI

Pour supprimer un modèle de lancement et toutes ses versions

Utilisez la commande delete-launch-template(AWS CLI) et spécifiez le modèle de lancement.

```
aws ec2 delete-launch-template --launch-template-id lt-01238c059e3466abc
```

PowerShell

Pour supprimer un modèle de lancement et toutes ses versions

Utilisez la commande Remove-EC2LaunchTemplate(AWS Tools for PowerShell) et spécifiez le modèle de lancement. S'il `-Force` n'est pas indiqué PowerShell , demande une confirmation.

```
Remove-EC2LaunchTemplate -LaunchTemplateId lt-0123456789example -Force
```

Supprimer une version d'un modèle de lancement

Si vous n'avez plus besoin d'une version du modèle de lancement, vous pouvez la supprimer.

Considérations

- Vous ne pouvez pas remplacer le numéro d'une version après l'avoir supprimée.
- Vous ne pouvez pas supprimer la version par défaut du modèle de lancement et devez d'abord attribuer une autre version comme version par défaut. Si la version par défaut est la seule version du modèle de lancement, vous devez supprimer la totalité du modèle de lancement.
- Lorsque vous utilisez la console, vous pouvez supprimer une version du modèle de lancement à la fois. Lorsque vous utilisez le AWS CLI, vous pouvez supprimer jusqu'à 200 versions de modèles de

lancement en une seule demande. Pour supprimer plus de 200 versions en une seule demande, vous pouvez supprimer le modèle de lancement, ce qui supprime également toutes ses versions.

Console

Pour supprimer une version du modèle de lancement

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Modèles de lancement.
3. Sélectionnez le modèle de lancement et choisissez Actions, Supprimer la version du modèle.
4. Sélectionnez la version à supprimer et choisissez Supprimer.

AWS CLI

Pour supprimer une version du modèle de lancement

- Utilisez la delete-launch-template-versionscommande et spécifiez les numéros de version à supprimer. Vous pouvez spécifier jusqu'à 200 versions de modèles de lancement à supprimer en une seule demande.

```
aws ec2 delete-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1
```

PowerShell

Utilisez l'Remove-EC2TemplateVersionapplet de commande et spécifiez les numéros de version à supprimer. Vous pouvez spécifier jusqu'à 200 versions de modèles de lancement à supprimer en une seule demande.

```
Remove-EC2TemplateVersion `
    -LaunchTemplateId lt-0abcd290751193123 `
    -Version 1
```

Lancer une EC2 instance Amazon

Une instance est un serveur virtuel dans le AWS Cloud. Vous lancez une instance à partir d'une Amazon Machine Image (AMI). AMIfournit le système d'exploitation, le serveur d'applications et les applications de votre instance.

Lorsque vous vous inscrivez à AWS, vous pouvez commencer à utiliser Amazon EC2 gratuitement en utilisant le Niveau gratuit d'AWS. Vous pouvez utiliser le niveau gratuit pour lancer et utiliser une `t2.micro` instance gratuitement pendant 12 mois (dans les régions où elle n'`t2.micro`est pas disponible, vous pouvez utiliser une `t3.micro` instance dans le cadre du niveau gratuit).Vous devez payer des frais pour votre instance ou son utilisation qui sont pris en compte dans les limites de votre niveau gratuit pendant que l'instance est en cours d'exécution, même si elle reste inactive. Pour plus d'informations, consultez les EC2tarifs Amazon.

Lorsque vous lancez votre instance, vous pouvez le faire dans un sous-réseau associé à l'une des ressources suivantes :

- Une zone de disponibilité : cette option est la valeur par défaut.
- Une zone locale : pour lancer une instance dans une zone locale, vous devez vous connecter à la zone locale, puis créer un sous-réseau dans la zone. Pour plus d'informations, voir Commencer avec les zones locales.
- Une zone de longueur d'onde : pour lancer une instance dans une zone de longueur d'onde, vous devez opter pour la zone de longueur d'onde, puis créer un sous-réseau dans la zone. Pour plus d'informations sur le lancement d'une instance dans une zone Wavelength, consultez Get started with AWS Wavelength.
- Un avant-poste — Pour lancer une instance dans un avant-poste, vous devez créer un avant-poste. Pour plus d'informations sur la création d'un avant-poste, voir Commencer avec AWS Outposts.

Une fois que vous avez lancé votre instance, vous pouvez la connecter et l'utiliser. Au début, l'état de l'instance est `pending`. Lorsque l'état de l'instance indique `running`, cela signifie que le démarrage de l'instance a commencé. Il peut y avoir un bref délai avant que vous puissiez vous connecter à l'instance. Notez que le lancement de types d'instances de matériel nu peut prendre plus de temps.

L'instance reçoit un DNS nom public que vous pouvez utiliser pour contacter l'instance depuis Internet. L'instance reçoit également un DNS nom privé que les autres instances de la même instance VPC peuvent utiliser pour contacter l'instance.

Lorsque vous en avez terminé avec une instance, pour éviter d'encourir des coûts inutiles, veillez à la résilier. Pour de plus amples informations, veuillez consulter Mettre fin aux EC2 instances Amazon.

Les méthodes suivantes vous permettent de lancer une instance.

Méthode	Outil	Documentation
Utilisez l'assistant de lancement d'instance pour spécifier les paramètres de lancement.	EC2Console Amazon	Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console
Créez un modèle de lancement et lancez l'instanc e à partir du modèle de lancement.	EC2Console Amazon	Lancer EC2 des instances à l'aide d'un modèle de lancement
Utilisez une instance existante comme base.	EC2Console Amazon	Lancer une EC2 instance en utilisant les détails d'une instance existante
Utilisez un AMI que vous avez acheté auprès du AWS Marketplace.	EC2Console Amazon	Lancez une EC2 instance Amazon à partir d'un AWS Marketplace AMI
Utilisez AMI celui que vous spécifiez.	AWS CLI	Lancez, listez et fermez EC2 les instances Amazon pour AWS CLI
Utilisez AMI celui que vous spécifiez.	AWS Tools for Windows PowerShell	Lancer une EC2 instance Amazon à l'aide de Windows PowerShell
Utilisez EC2 Fleet pour fournir de la capacité entre différents types d'EC2instances et zones de disponibilité, ainsi qu'entre les options d'achat d'instanc es à la demande, d'instanc	AWS CLI	EC2Fleet et Spot Fleet

Méthode	Outil	Documentation
e réservée et d'instance ponctuelle.		
Utilisez un AWS CloudFormation modèle pour spécifier une instance.	AWS CloudFormation	AWS: : EC2 : :Instance dans le guide de l'AWS CloudFormation utilisateur
Utilisez une langue spécifique AWS SDK pour lancer une instance.	AWS SDK	AWS SDKpour. NET AWS SDKpour C++ AWS SDKpour Go AWS SDKpour Java AWS SDKpour JavaScript AWS SDKpour PHP V3 AWS SDKpour Python AWS SDKpour Ruby V3

Référence pour les paramètres de configuration des EC2 instances Amazon

L'assistant de lancement d'instance et le modèle de lancement de la EC2 console Amazon fournissent tous les paramètres nécessaires à la configuration d'une EC2 instance Amazon.

À l'exception de la paire de clés, l'assistant de lancement d'instance fournit une valeur par défaut pour chaque paramètre. Vous pouvez accepter tout ou partie des valeurs par défaut, ou configurer une instance avec vos propres valeurs. Lors de la création d'un modèle de lancement, les paramètres sont facultatifs. Si vous utilisez un modèle de lancement pour lancer une instance, les paramètres spécifiés dans le modèle de lancement remplacent les valeurs par défaut de l'assistant de lancement d'instance. Tout paramètre non spécifié dans le modèle de lancement prendra par défaut la valeur fournie par l'assistant de lancement de l'instance.

Les paramètres sont regroupés dans l'assistant de lancement d'instance et le modèle de lancement. Les descriptions suivantes sont présentées en fonction des groupements de paramètres dans la console.

Paramètres pour la configuration d'instance

- Noms et identifications
- Images d'applications et de systèmes d'exploitation (Amazon Machine Image)
- Type d'instance
- Paire de clés (connexion)
- Paramètres réseau
- Configurer le stockage
- Détails avancés
- Récapitulatif

Noms et identifications

Le nom de l'instance est une identification, où la clé est Name (Nom), et la valeur est le nom que vous spécifiez. Vous pouvez étiqueter l'instance, les volumes et les interfaces réseau. Pour les instances Spot, vous pouvez baliser uniquement la demande d'instance Spot. Pour plus d'informations sur les balises, consultez Marquez vos EC2 ressources Amazon.

La spécification d'un nom d'instance et d'identifications supplémentaires est facultative.

- Pour Name (Nom), saisissez un nom descriptif pour l'instance. Si vous ne spécifiez pas de nom, l'instance peut être identifiée par son ID, qui est automatiquement généré lorsque vous lancez l'instance.
- Pour ajouter des identifications supplémentaires, sélectionnez Add additional tags (Ajouter des identifications supplémentaires). Choisissez Add tag (Ajouter une identification), saisissez une clé et une valeur, puis sélectionnez le type de ressource à étiqueter. Choisissez Add tag (Ajouter une identification) pour chaque étiquette supplémentaire.

Vous ne pouvez spécifier le nom de l'instance que lorsque vous lancez une instance. Vous ne pouvez pas nommer l'instance lorsque vous créez un modèle de lancement, mais vous pouvez ajouter des balises pour les ressources créées lors du lancement de l'instance.

Images d’applications et de systèmes d’exploitation (Amazon Machine Image)

Une Amazon Machine Image (AMI) contient les informations requises pour créer une instance. Par exemple, un AMI peut contenir le logiciel requis pour agir en tant que serveur Web, tel que Linux, Apache et votre site Web.

Vous pouvez en trouver un approprié AMI comme suit. Pour chaque option permettant de trouver unAMI, vous pouvez choisir Annuler (en haut à droite) pour revenir à l'assistant de lancement d'instance sans en choisir unAMI.

Barre de recherche

Pour effectuer une recherche parmi toutes les AMIs options disponibles, entrez un mot clé dans la barre AMI de recherche, puis appuyez sur Entrée. Pour en sélectionner unAMI, choisissez Sélectionner.

Recents (Récentes)

Celui AMIs que vous avez récemment utilisé.

Choisissez Lancé récemment ou Actuellement utilisé, puis, dans Amazon Machine Image (AMI), sélectionnez unAMI.

Mon AMIs

Les informations privées AMIs que vous possédez ou celles AMIs qui ont été partagées avec vous.

Choisissez Owned by me ou Shared with me, puis, dans Amazon Machine Image (AMI), sélectionnez unAMI.

Quick Start

AMIssont regroupés par système d'exploitation (OS) pour vous aider à démarrer rapidement.

Sélectionnez d'abord le système d'exploitation dont vous avez besoin, puis, dans Amazon Machine Image (AMI), sélectionnez unAMI. Pour sélectionner un AMI niveau éligible au niveau gratuit, assurez-vous qu'il AMI est marqué comme éligible au niveau gratuit.

En savoir plus AMIs

Choisissez Parcourir davantage AMIs pour parcourir le AMI catalogue complet.

- Pour effectuer une recherche parmi toutes les AMIs options disponibles, entrez un mot clé dans la barre de recherche, puis appuyez sur Entrée.

- Pour rechercher un en AMI utilisant un paramètre de Systems Manager, cliquez sur le bouton fléché situé à droite de la barre de recherche, puis choisissez le paramètre Search by Systems Manager. Pour de plus amples informations, veuillez consulter Rechercher un paramètre AMI à l'aide d'un paramètre Systems Manager.
- Pour effectuer une recherche par catégorie, sélectionnez Quickstart AMIs AMIs AWS Marketplace AMIs, My ou Community AMIs.

  AWS Marketplace Il s'agit d'une boutique en ligne où vous pouvez acheter des logiciels qui fonctionnent AWS, notammentAMIs. Pour plus d'informations sur le lancement d'une instance depuis le AWS Marketplace, consultezLancez une EC2 instance Amazon à partir d'un AWS Marketplace AMI. Dans Communauté AMIs, vous pouvez constater AMIs que les membres de AWS la communauté ont mis à la disposition d'autres utilisateurs. AMIsauprès d'Amazon ou d'un partenaire vérifié sont marqués comme fournisseur vérifié.
- Pour filtrer la listeAMIs, cochez une ou plusieurs cases sous Affiner les résultats sur la gauche de l'écran. Les options de filtre sont différentes selon la catégorie de recherche sélectionnée.
- Vérifiez le type de périphérique racine répertorié pour chacun d'entre euxAMI. Notez le type dont AMIs vous avez besoin : ebs (soutenu par AmazonEBS) ou instance-store (soutenu par instance store). Pour de plus amples informations, veuillez consulter Root device type.
- Vérifiez le type de virtualisation répertorié pour chacun d'entre euxAMI. Notez quels AMIs sont les types dont vous avez besoin : hvm ou paravirtual. Par exemple, certains types d'instances nécessitentHVM. Pour plus d'informations sur les types de virtualisation Linux, consultezTypes de virtualisation.
- Vérifiez le mode de démarrage répertorié pour chacun d'entre euxAMI. Notez qu'ils AMIs utilisent le mode de démarrage dont vous avez besoin : legacy-bios, uefi ou uefi-preferred. Pour de plus amples informations, veuillez consulter Comportement de lancement de l'instance avec les modes de EC2 démarrage Amazon.
- Choisissez AMI celui qui répond à vos besoins, puis sélectionnez Sélectionner.

Avertissement lors de la modification du AMI

Lorsque vous lancez une instance, si vous modifiez la configuration de volumes ou de groupes de sécurité associés à l'instance sélectionnéeAMI, puis que vous en choisissez un autreAMI, une fenêtre s'ouvre pour vous avertir que certains de vos paramètres actuels seront modifiés ou supprimés. Vous pouvez consulter les modifications apportées aux groupes de sécurité et aux volumes. En outre, vous pouvez soit afficher quels volumes seront ajoutés et supprimés, soit afficher uniquement les volumes qui seront ajoutés. Cet avertissement ne s'affiche pas lors de la création d'un modèle de lancement.

Type d'instance

Le type d'instance définit la configuration matérielle et la taille de l'instance. Les types d'instances de grande taille disposent de plus de mémoire CPU et de mémoire. Pour plus d'informations, consultez la section Types d'EC2instances Amazon.

- Type d'instance : assurez-vous que le type d'instance est compatible avec celui AMI que vous avez spécifié. Pour de plus amples informations, veuillez consulter Types d'EC2instances Amazon.

  Niveau gratuit : si vous avez moins de 12 mois, vous pouvez utiliser Amazon EC2 dans le cadre du niveau gratuit en sélectionnant le type d'instance t2.micro ou le type d'instance t3.micro dans les régions où t2.micro Compte AWS n'est pas disponible. Sachez que lorsque vous lancez une instance t3.micro, elle passe par défaut en mode illimité, ce qui peut entraîner des frais supplémentaires en fonction de l'utilisation. CPU Si un type d'instance est éligible dans le cadre du niveau gratuit, il est étiqueté Free tier eligible (Éligible à l'offre gratuite).
- Comparez les types d'instances : vous pouvez comparer différents types d'instances en fonction des attributs suivants : nombre devCPUs, architecture, quantité de mémoire (GiB), quantité de stockage (Go), type de stockage et performances du réseau.
- Obtenir des conseils : vous pouvez obtenir des conseils et des suggestions pour les types d'instances à partir de l'outil de recherche de types d'EC2instance. Pour de plus amples informations, veuillez consulter Obtenez des recommandations depuis l'outil de recherche de types d'EC2instance.
- (Modèles de lancement uniquement) Avancé : pour spécifier les attributs d'instance et laisser Amazon EC2 identifier les types d'instance dotés de ces attributs, choisissez Avancé, puis choisissez Spécifier les attributs du type d'instance.
  - Nombre de vCPUs : Entrez le nombre minimum et maximum correspondant vCPUs à vos besoins de calcul. Pour n'indiquer aucune limite, saisissez un minimum de **0** et laissez le champ maximum vide.
  - Quantité de mémoire (MiB) : saisissez la quantité minimale et maximale de mémoire, en MiB, pour vos besoins en calcul. Pour n'indiquer aucune limite, saisissez un minimum de **0** et laissez le champ maximum vide.
  - Développez Attributs de type d'instance facultatifs et choisissez Add attribute (Ajouter un attribut) pour exprimer plus en détail vos besoins en matière de calcul. Pour plus d'informations sur chaque attribut, consultez InstanceRequirementsRequestla EC2APIréférence Amazon.
  - Resulting instance types (Types d'instance obtenus) : vous pouvez prévisualiser les types d'instance qui correspondent aux attributs spécifiés. Pour exclure des types d'instance,

choisissez Add attribute (Ajouter un attribut), et depuis la liste Attribute (Attribut), choisissez Excluded instance types (Types d'instance exclus). À partir de la liste Attribute value (Valeur d'attribut), sélectionnez les types d'instances à exclure.

Paire de clés (connexion)

Pour Key pair name (Nom de la paire de clés), choisissez une paire de clés existante ou choisissez Create new key pair (Créer une nouvelle paire de clés) pour en créer une nouvelle. Pour de plus amples informations, veuillez consulter Paires de EC2 clés Amazon et EC2 instances Amazon.

> **Important**
>
> Si vous choisissez l'option Proceed without key pair (non recommandé), vous ne pourrez pas vous connecter à l'instance sauf si vous en choisissez une AMI configurée pour autoriser les utilisateurs à se connecter d'une autre manière.

Paramètres réseau

Configurez les paramètres réseau, le cas échéant.

- (Assistant de lancement d'instance uniquement) VPC: Choisissez une instance existante VPC pour votre instance. Vous pouvez choisir la valeur par défaut VPC ou VPC celle que vous avez créée. Pour de plus amples informations, veuillez consulter the section called "Clouds privés virtuels".
- Sous-réseau : vous pouvez lancer une instance dans un sous-réseau associé à une zone de disponibilité, une zone locale, une zone Wavelength ou un Outpost.

  Pour lancer l'instance dans une zone de disponibilité, sélectionnez le sous-réseau dans lequel lancer votre instance. Pour créer un nouveau sous-réseau, choisissez Create new subnet pour accéder à la console AmazonVPC. Une fois que vous avez terminé, revenez dans l'assistant de lancement d'instance et choisissez l'icône Refresh (Actualiser) afin de charger votre sous-réseau dans la liste.

  Pour lancer l'instance dans un sous-réseau IPv6 réservé, l'instance doit être créée sur le système Nitro.

  Pour lancer l'instance dans une zone locale, sélectionnez un sous-réseau que vous avez créé dans la zone locale.

Pour lancer une instance dans un avant-poste, sélectionnez un sous-réseau VPC que vous avez associé à l'avant-poste.

- (Lancer l'assistant d'instance uniquement) Attribuer automatiquement une adresse IP publique : Spécifiez si votre instance reçoit une IPv4 adresse publique. Par défaut, les instances d'un sous-réseau par défaut reçoivent une IPv4 adresse publique, contrairement aux instances d'un sous-réseau autre que celui par défaut. Vous pouvez sélectionner Activer ou Désactiver pour remplacer la configuration par défaut du sous-réseau. Pour plus d'informations, consultez IPv4Adresses publiques.
- Firewall (security groups) (Pare-feu (groupes de sécurité)) : utilisez un groupe de sécurité afin de définir les règles de pare-feu de votre instance. Ces règles déterminent le trafic réseau entrant acheminé vers votre instance. Le reste du trafic est ignoré. Pour plus d'informations sur les groupes de sécurité, consultez Groupes EC2 de sécurité Amazon pour vos EC2 instances.

  Si vous ajoutez une interface réseau, vous devez indiquer le même groupe de sécurité dans l'interface réseau.

  Sélectionnez ou créez un groupe de sécurité de la façon suivante :

  - Pour sélectionner un groupe de sécurité existant pour vousVPC, choisissez Sélectionner un groupe de sécurité existant, puis sélectionnez votre groupe de sécurité dans Groupes de sécurité communs.
  - Pour créer un nouveau groupe de sécurité pour votreVPC, choisissez Create security group. L'assistant de lancement d'instance définit automatiquement le groupe de sécurité launch-wizard-x et fournit les cases à cocher suivantes pour ajouter rapidement des règles de groupe de sécurité :

    (Linux) Autoriser SSH le trafic en provenance : crée une règle entrante pour vous permettre de vous connecter à votre instance SSH via le port 22.

    (Windows) Autoriser RDP le trafic en provenance : crée une règle entrante pour vous permettre de vous connecter à votre instance via RDP le port 3389.

    Spécifiez si le trafic provient de Anywhere (N'importe où), Custom (Personnalisée), ou My IP (Mon IP).

    Autoriser le HTTPs trafic en provenance d'Internet : crée une règle entrante qui ouvre le port 443 (HTTPS) pour autoriser le trafic Internet en provenance de n'importe où. Si votre instance est un serveur web, vous aurez besoin de cette règle.

Autoriser le HTTP trafic en provenance d'Internet : crée une règle entrante qui ouvre le port 80 (HTTP) pour autoriser le trafic Internet en provenance de n'importe où. Si votre instance est un serveur web, vous aurez besoin de cette règle.

Vous pouvez modifier ces règles et ajouter des règles en fonction de vos besoins.

Pour modifier ou ajouter une règle, choisissez Edit (Modifier) (en haut à droite). Pour ajouter une règle, choisissez Add security group rule (Ajouter une règle de groupe de sécurité). Pour Type, sélectionnez le type de trafic réseau. Le champ Protocol (Protocole) est automatiquement rempli avec le protocole pour s'ouvrir au trafic réseau. Pour Source type (Type de source), sélectionnez le type de source. Pour permettre à l'assistant de lancement d'instance ou au modèle de lancement d'ajouter l'adresse IP publique de votre ordinateur, choisissez My IP. Toutefois, si vous vous connectez via ISP ou depuis un pare-feu sans adresse IP statique, vous devez connaître la plage d'adresses IP utilisée par les ordinateurs clients.

> **Warning**
>
> Les règles qui permettent à toutes les adresses IP (`0.0.0.0/0`) d'accéder à votre instance SSH ou RDP sont acceptables si vous lancez brièvement une instance de test et que vous allez bientôt l'arrêter ou y mettre fin, mais elles ne sont pas sûres pour les environnements de production. Veillez à autoriser une seule adresse IP ou plage d'adresses à accéder à votre instance.

- Advanced network configuration (Configuration réseau avancée) : disponible uniquement si vous choisissez un sous-réseau.

  Interface réseau

  - Device index (Index de périphérique) : l'index de la carte réseau. L'interface réseau principale doit être affectée à l'index de carte réseau 0. Certains types d'instance prennent en charge plusieurs cartes réseau.
  - Interface réseau : sélectionnez Nouvelle interface pour permettre à Amazon de EC2 créer une nouvelle interface, ou sélectionnez une interface réseau existante et disponible.
  - Description : (facultatif) description de la nouvelle interface réseau.
  - Subnet (Sous-réseau) : sous-réseau dans lequel créer une nouvelle interface réseau. Pour l'interface réseau principale (`eth0`), il s'agit du sous-réseau dans lequel l'instance est lancée. Si

vous avez indiqué une interface réseau existante pour `eth0`, l'instance est lancée dans le sous-réseau dans lequel l'interface réseau est située.

> **Note**
>
> Pour lancer une EC2 instance dans un sous-réseau IPv6 réservé uniquement, vous devez utiliser des instances basées sur le système AWS Nitro.

> **Note**
>
> Lors du lancement d'une instance IPv6 réservée, il est DHCPv6 possible que le serveur de IPv6 DNS noms ne soit pas immédiatement fourni à l'instance. Au cours de ce délai initial, l'instance peut ne pas être en mesure de résoudre les domaines publics.
> Pour les instances exécutées sur Amazon Linux 2, si vous souhaitez mettre à jour immédiatement le fichier /etc/resolv.conf avec le serveur de IPv6 DNS noms, exécutez la directive cloud-init suivante au lancement :
>
> ```
> #cloud-config
> bootcmd:
> - /usr/bin/sed -i -E 's,^nameserver\s+[\.[:digit:]]+$,nameserver
>  fd00:ec2::253,' /etc/resolv.conf
> ```
>
> Une autre option consiste à modifier le fichier de configuration et à créer une nouvelle image AMI pour que le fichier contienne l'adresse du serveur de IPv6 DNS noms dès le démarrage.

- Groupes de sécurité : un ou plusieurs groupes de sécurité à associer à l'interface réseau.
- (Modèles de lancement uniquement) Attribuer automatiquement une adresse IP publique : Spécifiez si votre instance reçoit une IPv4 adresse publique. Par défaut, les instances d'un sous-réseau par défaut reçoivent une IPv4 adresse publique, ce qui n'est pas le cas des instances d'un sous-réseau autre que le sous-réseau par défaut. Vous pouvez sélectionner Activer ou Désactiver pour remplacer la configuration par défaut du sous-réseau. Pour de plus amples informations, veuillez consulter IPv4Adresses publiques.
- IP principale : IPv4 adresse privée comprise dans la plage de votre sous-réseau. Laissez ce champ vide pour permettre à Amazon de EC2 choisir une IPv4 adresse privée pour vous.

- IP secondaire : IPv4 adresses privées supplémentaires de la plage de votre sous-réseau. Choisissez Attribuer manuellement et entrez une IPv4 adresse. Choisissez Ajouter une adresse IP pour ajouter une autre IPv4 adresse. Vous pouvez également choisir Attribuer automatiquement et saisir une valeur indiquant le nombre d'IPv4adresses qu'Amazon EC2 choisit pour vous.
- (IPv6-only) IPv6IPs: IPv6 adresses issues de la plage du sous-réseau. Choisissez Attribuer manuellement et entrez une IPv6 adresse. Choisissez Ajouter une adresse IP pour ajouter une autre IPv6 adresse. Vous pouvez également choisir Attribuer automatiquement et saisir une valeur indiquant le nombre d'IPv6adresses qu'Amazon EC2 choisit pour vous.
- IPv4Préfixes : IPv4 préfixes de l'interface réseau. Choisissez Attribuer manuellement et entrez un IPv4 préfixe. Vous pouvez également choisir Attribuer automatiquement et saisir une valeur indiquant le nombre de IPv4 préfixes qu'Amazon EC2 choisit pour vous.
- IPv6Préfixes : IPv6 préfixes de l'interface réseau. Choisissez Attribuer manuellement et entrez un IPv6 préfixe. Vous pouvez également choisir Attribuer automatiquement et saisir une valeur indiquant le nombre de IPv6 préfixes qu'Amazon EC2 choisit pour vous.
- (Double pile et IPv6 uniquement) Attribuer une IPv6 adresse IP principale : lorsque vous lancez une instance dans un sous-réseau à double pile ou IPv6 uniquement, vous pouvez indiquer si elle doit avoir une adresse principale. IPv6 Cela permet d'éviter les perturbations du trafic vers l'instance ou l'interface réseau. Choisissez Oui si vous comptez sur le IPv6 fait que l'adresse de cette instance ne change pas et qu'Amazon EC2 choisit une IPv6 adresse associée à l'interface réseau comme IPv6 adresse principale. Vous ne pourrez pas supprimer l'IPv6adresse principale ultérieurement. Lorsque vous activez une IPv6 GUA adresse comme adresse principaleIPv6, la première IPv6 GUA devient l'IPv6adresse principale jusqu'à ce que l'instance soit résiliée ou que l'interface réseau soit détachée. Si plusieurs IPv6 adresses sont associées à une interface réseau attachée à votre instance et que vous EC2 autorisez Amazon à attribuer une IPv6 adresse principale, la première IPv6 GUA adresse associée à l'interface réseau devient l'IPv6adresse principale.
- Supprimer à l'arrêt : indique si l'interface réseau est supprimée lors de la suppression de l'instance.
- Elastic Fabric Adapter (EFA) : Indique si l'interface réseau est une Elastic Fabric Adapter (EFA). Pour de plus amples informations, veuillez consulter Adaptateur Elastic Fabric pour les charges de travail ML HPC et ML sur Amazon EC2.
- Index de carte réseau : l'index de la carte réseau. L'interface réseau principale doit être affectée à l'index de carte réseau 0. Certains types d'instance prennent en charge plusieurs cartes réseau.

- ENAExpress : ENA Express est alimenté par la technologie AWS Scalable Reliable Datagram (SRD). SRDla technologie utilise un mécanisme de pulvérisation de paquets pour répartir la charge et éviter la congestion du réseau. L'activation d'ENAExpress permet aux instances prises en charge de communiquer SRD en plus du TCP trafic normal lorsque cela est possible. L'assistant ou le modèle de lancement de l'instance n'inclut pas la configuration ENA express de l'instance, sauf si vous sélectionnez Activer ou Désactiver dans la liste.
- ENAExpress UDP : si vous avez activé ENA Express, vous pouvez éventuellement l'utiliser pour le UDP trafic. L'assistant ou le modèle de lancement de l'instance n'inclut pas la configuration ENA express de l'instance, sauf si vous sélectionnez Activer ou Désactiver.

Choisissez Ajouter une interface réseau pour ajouter des interfaces réseau supplémentaires. Le nombre d'interfaces réseau que vous pouvez ajouter dépend du nombre pris en charge par le type d'instance sélectionné. Des interfaces réseau supplémentaires peuvent résider dans un sous-réseau différent du même VPC ou dans un sous-réseau appartenant à un autre VPC que vous possédez (à condition que le sous-réseau se trouve dans la même zone de disponibilité que votre instance). Si vous choisissez d'ajouter une interface réseau supplémentaire résidant dans un autre VPC sous-réseau, l'option VPCSous-réseaux multiples apparaît lorsque vous sélectionnez un sous-réseau. Si vous sélectionnez un sous-réseau dans un autreVPC, le VPC label multiple apparaît à côté de l'interface réseau que vous avez ajoutée. Cela vous permet de créer des instances multihébergées VPCs avec différentes configurations réseau et de sécurité. Notez que si vous joignez un élément supplémentaire ENI provenant d'un autreVPC, vous devez choisir un groupe ENI de sécurité pour celui-ciVPC.

Pour de plus amples informations, veuillez consulter Interfaces réseau Elastic. Si vous spécifiez plusieurs interfaces réseau, votre instance ne peut pas recevoir d'IPv4adresse publique. En outre, si vous spécifiez une interface réseau existante pour eth0, vous ne pouvez pas remplacer le IPv4 paramètre public du sous-réseau à l'aide de l'attribution automatique d'une adresse IP publique. Pour de plus amples informations, veuillez consulter Attribuer une IPv4 adresse publique lors du lancement de l'instance.

Configurer le stockage

Le volume AMI que vous avez sélectionné inclut un ou plusieurs volumes de stockage, y compris le volume racine. Vous pouvez spécifier d'autres volumes à attacher à l'instance.

(Assistant de lancement d'instance uniquement) Vous pouvez utiliser la vue simple ou la vue avancée. Avec la vue Simple, vous spécifiez la taille et le type du volume. Pour spécifier tous les paramètres de volume, choisissez la vue Advanced (Avancée) (en haut à droite de la carte).

En utilisant la vue Advanced (Avancée), vous pouvez configurer chaque volume comme suit :

- Type de stockage : sélectionnez Amazon EBS ou les volumes de stockage d'instance à associer à votre instance. Les types de volumes disponibles dans la liste dépendent du type d'instance que vous avez sélectionné. Pour plus d'informations, consultez Stockage d'instances Stockage par blocs temporaire pour les EC2 instances et Amazon EBS Volumes.
- Device name (Nom du dispositif) : sélectionnez le périphérique dans la liste des noms de périphériques disponibles pour le volume.
- Snapshot (Instantané) : saisissez l'instantané à partir duquel vous souhaitez restaurer le volume. Vous pouvez rechercher les instantanés partagés et publics disponibles en saisissant un texte dans le champ Snapshot (Instantané).
- Taille (GiB) : pour les EBS volumes, vous pouvez spécifier une taille de stockage. Si vous avez sélectionné une AMI instance éligible au niveau gratuit, n'oubliez pas que pour rester dans les limites du niveau gratuit, vous devez disposer d'un espace de stockage total inférieur à 30 GiB.
- Type de volume : pour les EBS volumes, sélectionnez un type de volume. Pour plus d'informations, consultez les types de EBS volumes Amazon dans le guide de EBS l'utilisateur Amazon.
- IOPS: Si vous avez sélectionné un type de IOPS SSD volume provisionné, vous pouvez saisir le nombre d'opérations d'E/S par seconde (IOPS) que le volume peut prendre en charge.
- Supprimer en cas de résiliation : pour les EBS volumes Amazon, choisissez Oui pour supprimer le volume lorsque l'instance est résiliée, ou cliquez sur Non pour conserver le volume. Pour de plus amples informations, veuillez consulter Conservation des données lors de la résiliation d'une instance.
- Chiffré : si le type d'instance prend en charge le EBS chiffrement, vous pouvez choisir Oui pour activer le chiffrement du volume. Si vous avez activé le chiffrement par défaut dans cette région, le chiffrement est activé automatiquement. Pour plus d'informations, consultez Amazon EBS Encryption dans le guide de EBS l'utilisateur Amazon.
- KMSclé : si vous avez sélectionné Oui pour Encrypté, vous devez sélectionner une clé gérée par le client à utiliser pour chiffrer le volume. Si vous avez activé le chiffrement par défaut dans cette région, la clé gérée par le client par défaut est sélectionnée pour vous. Vous pouvez sélectionner une autre clé ou spécifier celle ARN de toute clé gérée par le client que vous avez créée.

- Systèmes de fichiers : montez un système de FSx fichiers Amazon EFS ou Amazon sur l'instance. Pour plus d'informations sur le montage d'un système de EFS fichiers Amazon, consultezUtiliser Amazon EFS avec des instances Amazon EC2 Linux. Pour plus d'informations sur le montage d'un système de FSx fichiers Amazon, consultez Utiliser Amazon FSx avec des EC2 instances Amazon

Détails avancés

Développez la section Détails avancés pour afficher les champs et spécifier des paramètres supplémentaires pour l'instance.

- (Assistant de lancement d'instance uniquement) Répertoire de jointure de domaines : sélectionnez le AWS Directory Service répertoire (domaine) auquel votre instance est jointe après le lancement. Si vous sélectionnez un domaine, vous devez sélectionner un IAM rôle doté des autorisations requises. Pour plus d'informations sur la jonction de domaines, consultez Joindre de manière fluide une instance Amazon EC2 Linux à votre répertoire Microsoft AD AWS géré (instances Linux) et Joindre facilement une instance Amazon EC2 Windows à votre répertoire Microsoft AD AWS géré (instances Windows).
- IAMprofil d'instance : sélectionnez un profil d'IAMinstance à associer à l'instance. Il s'agit d'un conteneur pour un IAM rôle. Pour de plus amples informations, veuillez consulter IAMrôles pour Amazon EC2.
- Hostname type(Type de nom d'hôte) : sélectionnez si le nom d'hôte du système d'exploitation hôte de l'instance inclura le nom de la ressource ou le nom de l'adresse IP. Pour de plus amples informations, veuillez consulter Types de noms EC2 d'hôte des instances Amazon.
- DNSNom d'hôte : détermine si les DNS requêtes portant sur le nom de la ressource ou sur le nom IP (selon le type de nom d'hôte que vous avez sélectionné) répondront par l'IPv4adresse (enregistrement A), l'IPv6adresse (AAAAenregistrement) ou les deux. Pour de plus amples informations, veuillez consulter Types de noms EC2 d'hôte des instances Amazon.
- Restauration automatique de l'instance : lorsque cette option est activée, elle restaure votre instance si les vérifications de l'état du système échouent. Ce paramètre est activé par défaut au lancement pour les types d'instances pris en charge. Pour de plus amples informations, veuillez consulter Configuration d'une restauration automatique simplifiée.
- Comportement d'arrêt : indiquez si l'instance doit s'arrêter ou être résiliée lorsque vous arrêtez l'ordinateur. Pour plus d'informations, consultez Modifier le comportement d'arrêt lancé de l'instance.
- Stop - Hibernate behavior (Comportement d'arrêt - mise en veille prolongée) : pour activer la mise en veille prolongée, sélectionnez Enable (Activer). Ce champ est uniquement disponible si votre

instance satisfait les conditions préalables à la mise en veille prolongée. Pour plus d'informations, consultez Hibernez votre instance Amazon EC2.

- Termination protection (Protection de la résilitation) : pour éviter toute mise hors service accidentelle, sélectionnez Enable (Activer). Pour de plus amples informations, veuillez consulter Activer la protection de la résiliation.
- Stop protection (Protection contre l'arrêt) : pour éviter tout arrêt accidentel, choisissez Enable (Activer). Pour de plus amples informations, veuillez consulter Activer la protection contre l'arrêt.
- CloudWatch Surveillance détaillée : choisissez Activer pour activer la surveillance détaillée de votre instance à l'aide d'Amazon CloudWatch. Des frais supplémentaires seront facturés. Pour de plus amples informations, veuillez consulter Surveillez vos instances à l'aide de CloudWatch.
- Elastic GPU : Amazon Elastic Graphics a atteint sa fin de vie le 8 janvier 2024. Pour les charges de travail nécessitant une accélération graphique, nous vous recommandons d'utiliser des instances Amazon EC2 G4ad, G4dn ou G5.
- Inférence élastique : accélérateur d'inférence élastique à associer à votre EC2 CPU instance. Pour plus d'informations, consultez Utilisation d'Amazon Elastic Inference dans le Guide du développeur Amazon Elastic Inference.

> **Note**
>
> À compter du 15 avril 2023, AWS nous n'intégrerons pas de nouveaux clients à Amazon Elastic Inference (EI) et nous aiderons les clients actuels à migrer leurs charges de travail vers des options offrant un meilleur prix et de meilleures performances. Après le 15 avril 2023, les nouveaux clients ne pourront plus lancer d'instances avec les accélérateurs Amazon EI sur Amazon SageMakerECS, Amazon ou AmazonEC2. Toutefois, les clients qui ont utilisé Amazon EI au moins une fois au cours des 30 derniers jours sont considérés comme des clients actuels et pourront continuer à utiliser le service.

- Credit specification (Spécification de crédit) : sélectionnez Unlimited (Non limité) pour permettre aux applications de s'exécuter au-delà du niveau de référence aussi longtemps que nécessaire. Ce champ est valable uniquement pour les instances T. Des frais supplémentaires peuvent être facturés. Pour de plus amples informations, veuillez consulter Instances de performance à capacité extensible.
- Groupe de placement : Spécifiez le groupe de placement dans lequel lancer l'instance. Vous pouvez sélectionner un groupe de placement existant ou en créer un nouveau. Le lancement dans un groupe de placement n'est pas possible pour tous les types d'instance. Pour de plus amples informations, veuillez consulter Groupes de placement pour vos EC2 instances Amazon.

- EBS-instance optimisée : une instance optimisée pour Amazon EBS utilise une pile de configuration optimisée et fournit une capacité dédiée supplémentaire pour Amazon EBS I/O. Si le type d'instance prend en charge cette fonctionnalité, choisissez Enable pour l'activer. Des frais supplémentaires seront facturés. Pour de plus amples informations, veuillez consulter the section called "EBSoptimisation".
- Option d'achat : Choisissez les instances Spot pour demander des instances Spot au prix Spot, plafonné au prix à la demande, et choisissez les options Personnaliser les instances Spot pour modifier les paramètres par défaut des instances Spot. Vous pouvez définir votre prix maximum (non recommandé) et modifier le type de demande, la durée de la demande et le comportement d'interruption. Si vous ne demandez pas d'instance ponctuelle, Amazon EC2 lance une instance à la demande par défaut. Pour de plus amples informations, veuillez consulter Gérez vos instances Spot.
- Capacity Reservation (Réserve de capacité) : indiquez s'il convient de lancer l'instance dans une réserve de capacité (Open (Ouvrir)), dans une réserve de capacité spécifique (Target by ID (Cibler par ID)) ou dans un groupe de réserve de capacité (Target by group (Cibler par groupe)). Pour spécifier qu'il ne faut pas utiliser de réserve de capacité, choisissez None (Aucune). Pour plus d'informations, consultez Lancer des instances dans une Réservation de capacité existante.
- Location : indiquez s'il convient d'exécuter votre instance sur un matériel partagé (Partagé), isolé, dédié (Dédié) ou sur un Hôte dédié (Hôte dédié). Si vous choisissez de lancer l'instance sur un Hôte dédié, vous pouvez spécifier si l'instance doit être lancée dans un groupe de ressources hôte ou vous pouvez cibler un Hôte dédié spécifique. Des frais supplémentaires peuvent être facturés. Pour plus d'informations, consultez Instances EC2 dédiées Amazon et Hôtes EC2 dédiés Amazon.
- RAMID de disque : (Valable uniquement pour le paravirtual (PV)AMIs) Sélectionnez un RAM disque pour l'instance. Si vous avez sélectionné un noyau, vous devrez peut-être sélectionner un RAM disque spécifique avec les pilotes nécessaires.
- ID du noyau : (Valable uniquement pour le paravirtual (PV)AMIs) Sélectionnez un noyau pour l'instance.
- Nitro Enclave : vous permet de créer des environnements d'exécution isolés, appelés enclaves, à partir d'instances AmazonEC2. Sélectionnez Activer pour activer l'instance pour AWS Nitro Enclaves. Pour plus d'informations, consultez Qu'est-ce que AWS Nitro Enclaves ? dans le guide de l'utilisateur de AWS Nitro Enclaves.
- Configurations de licence : vous pouvez lancer des instances sur la configuration de licence spécifiée pour suivre l'utilisation de votre licence. Pour plus d'informations, consultez Create a License Configuration (Création d'une configuration de licence) dans le Guide de l'utilisateur AWS License Manager.

- Spécifier CPU les options : dans l'assistant de lancement d'instance, ce champ n'est visible que si le type d'instance sélectionné prend en charge la spécification CPU d'options. Choisissez Spécifier CPU les options pour spécifier un nombre personnalisé de vCPUs lors du lancement. Définissez le nombre de CPU cœurs et de threads par cœur. Pour de plus amples informations, veuillez consulter CPUoptions pour les EC2 instances Amazon.
- Métadonnées accessibles : vous pouvez activer ou désactiver l'accès au service de métadonnées d'instance (IMDS). Pour de plus amples informations, veuillez consulter Configurer les options de métadonnées d'instance pour les nouvelles instances.
- Point de IPv6terminaison des métadonnées : vous pouvez autoriser l'instance à utiliser l'IMDSIPv6adresse `[fd00:ec2::254]` pour récupérer les métadonnées de l'instance. Cette option n'est disponible que si vous lancez des instances basées sur le système AWS Nitro dans un sous-réseau IPv6 compatible (double pile ou IPv6 uniquement). Pour plus d'informations sur la récupération des métadonnées d'instance, consultez Accéder aux métadonnées d'une EC2 instance.
- Version des métadonnées : si vous activez l'accès auIMDS, vous pouvez choisir d'exiger l'utilisation de la version 2 du service de métadonnées d'instance lorsque vous demandez des métadonnées d'instance. Pour de plus amples informations, veuillez consulter Configurer les options de métadonnées d'instance pour les nouvelles instances.
- Limite de sauts de réponse aux métadonnées : si vous activez leIMDS, vous pouvez définir le nombre de sauts réseau autorisés pour le jeton de métadonnées. Pour de plus amples informations, veuillez consulter Configurer les options de métadonnées d'instance pour les nouvelles instances.
- Allow tags in metadata (Autoriser les balises dans les métadonnées) : si vous sélectionnez Enable (Activer), l'instance autorise l'accès à toutes ses balises à partir de ses métadonnées. Si aucune valeur n'est spécifiée, l'accès aux identifications dans les métadonnées de l'instance est désactivé par défaut. Pour plus d'informations, consultez Autoriser l'accès aux identifications dans les métadonnées d'instance.
- Données utilisateur : vous pouvez spécifier les données utilisateur pour configurer une instance lors du lancement ou pour exécuter un script de configuration. Pour plus d'informations sur les données utilisateur pour les instances Linux, consultezExécuter des commandes lorsque vous lancez une EC2 instance avec saisie de données utilisateur. Pour plus d'informations sur les données utilisateur pour les instances Windows, consultezComment Amazon EC2 gère les données utilisateur pour les instances Windows.

Récapitulatif

Utilisez le panneau Summary (Récapitulatif) pour spécifier le nombre d'instances à lancer, vérifier la configuration de votre instance et lancer vos instances.

- Nombre d'instances : entrez le nombre d'instances à lancer. Toutes les instances seront lancées avec la même configuration.

  > **Tip**
  >
  > Pour accélérer les lancements d'instances, divisez les demandes volumineuses en lots plus petits. Par exemple, créez cinq demandes de lancement distinctes pour 100 instances au lieu d'un lancement pour 500 instances.

- (Facultatif) Si vous spécifiez plusieurs instances, afin de vous assurer de maintenir le nombre correct d'instances pour gérer la demande de votre application, vous pouvez choisir d'utiliser EC2Auto Scaling pour créer un modèle de lancement et un groupe Auto Scaling. La fonctionnalité Auto Scaling fait évoluer le nombre d'instances du groupe en fonction de vos spécifications. Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon EC2 Auto Scaling.

  > **Note**
  >
  > Si Amazon EC2 Auto Scaling indique qu'une instance appartenant à un groupe Auto Scaling est défectueuse, le remplacement de l'instance est automatiquement programmé pour être résiliée et une autre est lancée, et vous perdez vos données sur l'instance d'origine. Une instance est marquée comme non saine si vous arrêtez ou redémarrez l'instance, ou si un autre événement marque l'instance comme non saine. Pour plus d'informations, consultez la section Contrôles de santé des instances d'un groupe Auto Scaling dans le manuel Amazon EC2 Auto Scaling User Guide.

- Vérifiez les détails de votre instance et effectuez les modifications nécessaires. Vous pouvez accéder directement à une section en sélectionnant son lien dans le panneau Summary (Récapitulatif).
- Lorsque vous êtes prêt à lancer votre instance , choisissez Launch instance (Lancer l'instance).

Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console

Vous pouvez lancer une EC2 instance Amazon à l'aide de l'assistant de lancement d'instance de la EC2 console Amazon. L'assistant fournit des valeurs par défaut pour les paramètres de lancement, que vous pouvez accepter ou modifier en fonction de vos besoins. Le seul paramètre non spécifié est la paire de clés. Si vous choisissez d'accepter les valeurs par défaut, vous pouvez lancer rapidement une instance en sélectionnant uniquement une paire de clés.

> **Important**
>
> Vous devez payer des frais pour l'instance tant qu'elle est en `running` état, même si elle reste inactive. Toutefois, si vous êtes éligible au niveau gratuit, il se peut que vous n'ayez pas à payer de frais. Pour de plus amples informations, veuillez consulter Suivez votre utilisation du niveau gratuit pour Amazon EC2.

Pour obtenir une description de chaque paramètre de l'assistant de lancement d'instance, consultezRéférence pour les paramètres de configuration des EC2 instances Amazon.

Rubriques

- Lancer rapidement une instance
- Lancer une instance à l'aide de paramètres définis

Lancer rapidement une instance

Pour configurer une instance rapidement à des fins de test, procédez comme suit. Vous allez sélectionner le système d'exploitation et votre paire de clés et accepter les valeurs par défaut. À l'exception de la paire de clés, l'assistant de lancement d'instance fournit des valeurs par défaut pour tous les paramètres. Vous pouvez accepter la totalité ou une partie des valeurs par défaut, ou configurer une instance en spécifiant vos propres valeurs pour chaque paramètre.

Pour obtenir une description de chaque paramètre de l'assistant de lancement d'instance, consultezRéférence pour les paramètres de configuration des EC2 instances Amazon.

Pour lancer rapidement une instance à l'aide de l'assistant de lancement d'instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

2. Dans la barre de navigation en haut de l'écran, la AWS région actuelle est affichée (par exemple, USA East (Ohio)). Si nécessaire, sélectionnez une autre région dans laquelle vous souhaitez lancer l'instance.
3. Dans le tableau de bord de EC2 la console Amazon, choisissez Launch instance.
4. (Facultatif) Sous Name and tags (Noms et identifications), pour Name (Nom), saisissez un nom descriptif pour votre instance.
5. Sous Application and OS Images (Amazon machine Image) (Images d'applications et de systèmes d'exploitation (Amazon machine Image)), choisissez Quick Start (Démarrage rapide), puis choisissez le système d'exploitation de votre instance.
6. Sous Key pair (login) (Paire de clés (connexion)), pour Key pair name (Nom de la paire de clés), choisissez une paire de clés existante ou créez-en une.
7. Dans le panneau Summary (Récapitulatif), sélectionnez Launch instance (Lancer l'instance).

Lancer une instance à l'aide de paramètres définis

Si vous lancez une instance que vous utiliserez en production, vous devrez la configurer en fonction de vos besoins. Pour obtenir une description de chaque paramètre de l'assistant de lancement d'instance, consultezRéférence pour les paramètres de configuration des EC2 instances Amazon.

Pour lancer une instance en définissant tous les paramètres de lancement à l'aide de l'assistant de lancement d'instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation en haut de l'écran, la AWS région actuelle est affichée (par exemple, USA East (Ohio)). Si nécessaire, sélectionnez une autre région dans laquelle vous souhaitez lancer l'instance.
3. Dans le tableau de bord de EC2 la console Amazon, choisissez Launch instance.
4. (Facultatif) Sous Nom et balises, dans Nom, entrez un nom descriptif pour votre instance afin de pouvoir facilement en assurer le suivi.

   Le nom de l'instance est une identification, où la clé est Name (Nom), et la valeur est le nom que vous spécifiez.
5. Sous Images de l'application et du système d'exploitation (Amazon Machine Image), choisissez le système d'exploitation (OS) de votre instance, puis choisissez unAMI.

An AMI est un modèle qui contient le système d'exploitation et le logiciel requis pour lancer votre instance.

6. Pour Instance type (Type d'Instance), choisissez un type d'instance.

   Le type d'instance détermine la configuration matérielle (mémoireCPU, capacité de stockage et de réseau) et la taille de l'ordinateur hôte utilisé pour votre instance.

   Si vous ne savez pas quel type d'instance choisir, vous pouvez effectuer les opérations suivantes :

   - Choisissez Comparer les types d'instances pour comparer différents types d'instances en fonction des attributs suivants : nombre devCPUs, architecture, quantité de mémoire (GiB), quantité de stockage (Go), type de stockage et performances du réseau.
   - Choisissez Obtenir des conseils pour obtenir des conseils et des suggestions concernant les types d'instances à partir de l'outil de recherche de types d'EC2instance. Pour de plus amples informations, veuillez consulter Obtenez des recommandations depuis l'outil de recherche de types d'EC2instance.

   > **Note**
   >
   > Si vous avez moins de 12 mois, vous pouvez utiliser Amazon EC2 dans le cadre du niveau gratuit en choisissant le type d'instance t2.micro ou le type d'instance t3.micro dans les régions où t2.micro Compte AWS n'est pas disponible. Sachez que lorsque vous lancez une instance t3.micro, elle passe par défaut en mode illimité, ce qui peut entraîner des frais supplémentaires en fonction de l'utilisation. CPU Si un type d'instance est éligible dans le cadre du niveau gratuit, il est étiqueté Free tier eligible (Éligible à l'offre gratuite).

7. Sous Key pair (login) (Paire de clés (connexion)), pour Key pair name (Nom de la paire de clés), choisissez une paire de clés existante ou créez-en une. Si vous n'avez pas besoin d'une paire de clés pour vous connecter à votre instance, vous pouvez choisir Proceed without a key pair (ce n'est pas recommandé).
8. Sous Paramètres réseau, vous pouvez conserver les valeurs par défaut si vous lancez une instance de test. Si vous lancez une instance de production, il est recommandé de contrôler le trafic entrant et sortant de votre instance à l'aide des paramètres réseau et des groupes de sécurité que vous définissez.

9. Sous Configurer le stockage, vous pouvez conserver les valeurs par défaut ou spécifier un espace de stockage supplémentaire. Le volume AMI que vous avez sélectionné inclut un ou plusieurs volumes de stockage, y compris le volume racine. Vous pouvez spécifier d'autres volumes à attacher à l'instance.

   Vous pouvez utiliser la vue Simple ou Advanced (Avancée). Avec la vue Simple, vous spécifiez la taille et le type du volume. Pour spécifier tous les paramètres de volume, choisissez la vue Advanced (Avancée) (en haut à droite de la carte).

10. Pour les informations avancées, développez la section pour afficher les champs et spécifier les éventuels paramètres supplémentaires pour votre instance.
11. Dans le panneau Résumé, vous pouvez effectuer les opérations suivantes :

    a. Spécifiez le nombre d'instances à lancer.

    b. Passez en revue la configuration de votre instance et accédez directement à une section en choisissant son lien.

    c. Lorsque vous êtes prêt à lancer votre instance , choisissez Launch instance (Lancer l'instance).

    Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez Résoudre les problèmes de lancement des EC2 instances Amazon.

12. (Facultatif) Vous pouvez créer une alerte de facturation pour l'instance. Sur l'écran de confirmation, sous Next Steps (Étapes suivantes), choisissez Create billing alerts (Créer des alarmes de contrôle de facturation) et suivez les instructions. Des alertes de facturation peuvent également être créées après le lancement de l'instance. Pour plus d'informations, consultez la section Création d'une alarme de facturation pour surveiller vos AWS frais estimés dans le guide de CloudWatch l'utilisateur Amazon.

Lancer EC2 des instances à l'aide d'un modèle de lancement

Un modèle de EC2 lancement Amazon stocke les paramètres de lancement d'une instance afin que vous n'ayez pas à les spécifier à chaque fois que vous lancez une instance.

Plusieurs services de lancement d'instance peuvent éventuellement utiliser des modèles de lancement lors du lancement d'instances, tandis que pour d'autres services, tels que EC2 Fleet, les instances ne peuvent être lancées que si un modèle de lancement est utilisé. Cette rubrique décrit

comment utiliser un modèle de lancement lors du lancement d'une instance à l'aide de l'assistant de EC2 lancement d'instance, Amazon EC2 Auto Scaling, EC2 Fleet et Spot Fleet.

Pour plus d'informations sur les modèles de lancement, notamment sur la façon de créer un modèle de lancement, consultezStockez les paramètres de lancement de l'instance dans les modèles de EC2 lancement Amazon.

Rubriques

- Lancer une EC2 instance Amazon à l'aide d'un modèle de lancement
- Lancer des instances dans un groupe Amazon EC2 Auto Scaling à l'aide d'un modèle de lancement
- Lancer une EC2 flotte à l'aide d'un modèle de lancement
- Lancez une flotte de spots à l'aide d'un modèle de lancement

Lancer une EC2 instance Amazon à l'aide d'un modèle de lancement

Vous pouvez utiliser les paramètres contenus dans un modèle de lancement pour lancer une EC2 instance Amazon. Après avoir sélectionné le modèle de lancement, mais avant de lancer l'instance, vous pouvez modifier les paramètres de lancement.

Deux balises accompagnées des clés `aws:ec2launchtemplate:id` et `aws:ec2launchtemplate:version` sont attribuées automatiquement aux instances lancées à l'aide d'un modèle de lancement. Vous ne pouvez ni supprimer ni modifier ces balises.

Console

Pour lancer une instance à l'aide d'un modèle de lancement

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Utilisez l'une des options suivantes pour sélectionner le modèle de lancement :
   - Dans le tableau de bord de la EC2 console Amazon, cliquez sur la flèche vers le bas à côté de Launch instance, choisissez Launch instance from template, puis pour Source template, sélectionnez un modèle de lancement.
   - Dans le volet de navigation, choisissez Launch Templates, sélectionnez le modèle de lancement, puis choisissez Actions, Launch instance from template.
3. Pour Version du modèle source, sélectionnez la version du modèle de lancement à utiliser.

4. (Facultatif) Vous pouvez modifier les valeurs de tous les paramètres de lancement. Si vous ne modifiez aucune valeur, la valeur définie par le modèle de lancement est utilisée. Si aucune valeur n'a été spécifiée dans le modèle de lancement, la valeur par défaut du paramètre est utilisée.
5. Dans le panneau Résumé, pour Nombre d'instances, spécifiez le nombre d'instances à lancer.
6. Choisissez Launch instance (Lancer une instance).

   Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez Résoudre les problèmes de lancement des EC2 instances Amazon.

AWS CLI

Pour lancer une instance à partir d'un modèle de lancement

- Utilisez la commande run-instances et spécifiez le paramètre `--launch-template`. Spécifiez éventuellement la version du modèle de lancement à utiliser. Si vous ne la spécifiez pas, c'est la version par défaut qui est utilisée.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123,Version=1
```

- Pour remplacer un paramètre du modèle de lancement, spécifiez-le dans la commande run-instances. Dans l'exemple suivant, le type d'instance spécifié dans le modèle de lancement (le cas échéant) est remplacé.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --instance-type t2.small
```

- Si vous spécifiez un paramètre imbriqué faisant partie d'une structure complexe, l'instance est lancée à l'aide de la structure complexe spécifiée dans le modèle de lancement et des éventuels paramètres imbriqués supplémentaires définis.

  Dans l'exemple suivant, l'instance est lancée avec la balise *Owner*=*TeamA* et toute autre balise spécifiée dans le modèle de lancement. Si le modèle de lancement comporte une balise avec une clé *Owner*, la valeur est remplacée par *TeamA*.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --tag-specifications "ResourceType=instance,Tags=[{Key=Owner,Value=TeamA}]"
```

Dans l'exemple suivant, l'instance est lancée avec un volume portant le nom de l'appareil */dev/xvdb* ainsi que tout autre mappage de périphériques en mode bloc spécifié dans le modèle de lancement. Si le modèle de lancement possède un volume existant défini pour */dev/xvdb*, ses valeurs sont remplacées par les valeurs spécifiées.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --block-device-mappings "DeviceName=/dev/
xvdb,Ebs={VolumeSize=20,VolumeType=gp2}"
```

Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez Résoudre les problèmes de lancement des EC2 instances Amazon.

PowerShell

Pour lancer une instance à partir d'un modèle de lancement à l'aide de l' AWS Tools for PowerShell

- Utilisez la New-EC2Instancecommande et spécifiez le `-LaunchTemplate` paramètre. Spécifiez éventuellement la version du modèle de lancement à utiliser. Si vous ne la spécifiez pas, c'est la version par défaut qui est utilisée.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
)
```

- Pour remplacer un paramètre du modèle de lancement, spécifiez-le dans la New-EC2Instancecommande. Dans l'exemple suivant, le type d'instance spécifié dans le modèle de lancement (le cas échéant) est remplacé.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
)
```

- Si vous spécifiez un paramètre imbriqué faisant partie d'une structure complexe, l'instance est lancée à l'aide de la structure complexe spécifiée dans le modèle de lancement et des éventuels paramètres imbriqués supplémentaires définis.

  Dans l'exemple suivant, l'instance est lancée avec la balise *Owner*=*TeamA* et toute autre balise spécifiée dans le modèle de lancement. Si le modèle de lancement comporte une balise avec une clé *Owner*, la valeur est remplacée par *TeamA*.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small  `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
        }
) `
    -TagSpecification (
        New-Object -TypeName Amazon.EC2.Model.TagSpecification -Property @{
            ResourceType = 'instance';
            Tags         = @(
                @{key = "Owner"; value = "TeamA" },
                @{key = "Department"; value = "Operations" }
            )
        }
)
```

  Dans l'exemple suivant, l'instance est lancée avec un volume portant le nom de l'appareil */dev/xvdb* ainsi que tout autre mappage de périphériques en mode bloc spécifié dans le

modèle de lancement. Si le modèle de lancement possède un volume existant défini pour */dev/xvdb*, ses valeurs sont remplacées par les valeurs spécifiées.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small  `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
) `
    -BlockDeviceMapping  (
        New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping -Property @{
            DeviceName = '/dev/xvdb';
            EBS        = (
                New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property @{
                    VolumeSize = 25;
                    VolumeType = 'gp3'
                }
            )
        }
)
```

Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez Résoudre les problèmes de lancement des EC2 instances Amazon.

Lancer des instances dans un groupe Amazon EC2 Auto Scaling à l'aide d'un modèle de lancement

Vous pouvez créer un groupe Auto Scaling et spécifier un modèle de lancement à utiliser pour le groupe. Lorsqu'Amazon EC2 Auto Scaling lance des instances dans le groupe Auto Scaling, il utilise les paramètres de lancement définis dans le modèle de lancement associé.

Avant de créer un groupe Auto Scaling à l'aide d'un modèle de lancement, vous devez d'abord créer un modèle de lancement qui inclut les paramètres requis pour lancer une instance dans un groupe Auto Scaling. Certains paramètres sont obligatoires, tels que l'ID duAMI, et certains paramètres ne

peuvent pas être utilisés avec un groupe Auto Scaling. La console fournit des conseils pour vous aider à créer un modèle que vous pouvez utiliser avec Amazon EC2 Auto Scaling.

Pour créer un groupe Auto Scaling avec un modèle de lancement à l'aide de la console

- Pour les instructions, consultez Create an Auto Scaling group using a launch template dans le manuel Amazon EC2 Auto Scaling User Guide.

Pour créer ou mettre à jour un groupe Auto Scaling avec un modèle de lancement à l'aide du AWS CLI

- Utilisez la update-auto-scaling-groupcommande create-auto-scaling-groupou et spécifiez le `--launch-template` paramètre.

Pour plus d'informations, consultez les rubriques suivantes dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling :

- Création d'un modèle de lancement pour un groupe Auto Scaling
- Création d'un modèle de lancement à l'aide des paramètres avancés
- Exemples de création et de gestion de modèles de lancement avec le AWS Command Line Interface (AWS CLI) — Fournit des exemples qui montrent comment créer des modèles de lancement avec différentes combinaisons de paramètres.
- Créez des groupes Auto Scaling à l'aide de modèles de lancement
- Mettre à jour un groupe Auto Scaling

Lancer une EC2 flotte à l'aide d'un modèle de lancement

Un modèle de lancement est obligatoire lors de la création d'une demande EC2 de flotte. Lorsqu'Amazon EC2 répond à la demande EC2 Fleet, il utilise les paramètres de lancement définis dans le modèle de lancement associé. Vous pouvez remplacer certains des paramètres spécifiés dans le modèle de lancement. Pour de plus amples informations, veuillez consulter Création d'une EC2 flotte.

Pour créer une EC2 flotte avec un modèle de lancement à l'aide du AWS CLI

- Utilisez la commande create-fleet. Utilisez le paramètre `--launch-template-configs` pour spécifier le modèle de lancement et tous les remplacements de celui-ci.

Lancez une flotte de spots à l'aide d'un modèle de lancement

Un modèle de lancement est facultatif lors de la création d'une demande Spot Fleet. Si vous n'utilisez pas de modèle de lancement, vous pouvez définir manuellement les paramètres de lancement. Si vous utilisez un modèle de lancement, lorsqu'Amazon EC2 répond à la demande Spot Fleet, il utilise les paramètres de lancement définis dans le modèle de lancement associé. Vous pouvez remplacer certains des paramètres spécifiés dans le modèle de lancement. Pour de plus amples informations, veuillez consulter Créer une flotte Spot.

Pour créer une demande Spot Fleet à l'aide d'un modèle de lancement

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Choisissez Demander des instances ponctuelles.
4. Sous Launch parameters (Paramètres de lancement), choisissez Use a launch template (Utiliser un modèle de lancement).
5. Pour Launch template (Modèle de lancement), choisissez un modèle de lancement, puis, dans le champ de droite, choisissez la version du modèle de lancement.
6. Configurez votre parc d'instances Spot en sélectionnant différentes options sur cet écran. Pour plus d'informations sur ces options, consultez Création d'une demande de parc d'instances Spot à l'aide des paramètres définis (console).
7. Lorsque vous êtes prêt à créer votre parc d'instances Spot, choisissez Launch (Lancer).

Pour créer une demande Spot Fleet à l'aide d'un modèle de lancement

- Utilisez la request-spot-fleetcommande. Utilisez le paramètre `LaunchTemplateConfigs` pour spécifier le modèle de lancement et tous les remplacements de celui-ci.

Lancer une EC2 instance en utilisant les détails d'une instance existante

La EC2 console Amazon propose une option de lancement similaire à celle-ci qui vous permet d'utiliser une instance actuelle comme base pour lancer d'autres instances. Cette option renseigne automatiquement l'assistant de EC2 lancement d'instance Amazon avec certains détails de configuration de l'instance sélectionnée.

Considérations

- Nous ne clonons pas vos instances ; nous ne répliquons que certains détails de configuration. Pour créer une copie de votre instance, créez-en d'abord une AMI à partir de celle-ci, puis lancez d'autres instances à partir deAMI. Créez un modèle de lancement pour vous assurer de lancer vos instances en utilisant les mêmes informations de lancement.
- L'instance doit être dans l'état `running`.

Détails copiés

Les détails de configuration suivants sont copiés de l'instance sélectionnée vers l'assistant de lancement d'instance :

- AMIID
- Type d'instance
- Zone de disponibilité, ou sous-réseau VPC et dans lequel se trouve l'instance sélectionnée
- IPv4Adresse publique Si l'instance sélectionnée possède actuellement une IPv4 adresse publique, la nouvelle instance reçoit une IPv4 adresse publique, quel que soit le paramètre d'IPv4adresse publique par défaut de l'instance sélectionnée. Pour plus d'informations sur les IPv4 adresses publiques, consultezIPv4Adresses publiques.
- Groupe de placement, le cas échéant
- IAMrôle associé à l'instance, le cas échéant
- Paramètre du comportement lors de la mise hors tension (arrêt ou mise hors service)
- Paramètre de protection de mise hors service de l'instance (vrai ou faux)
- CloudWatch surveillance (activée ou désactivée)
- Amazon EBS -paramètre d'optimisation (vrai ou faux)
- Paramètre de location, en cas de lancement dans un VPC (partagé ou dédié)
- ID du noyau et ID RAM du disque, le cas échéant
- Données utilisateur, le cas échéant
- Balises associées à l'instance, le cas échéant
- Groupes de sécurité associés à l'instance
- [Instances Windows] Informations d'association. Si l'instance sélectionnée est associée à un fichier de configuration, le même fichier est automatiquement associé à la nouvelle instance. Si le fichier de configuration comprend une configuration de domaine joint, la nouvelle instance est jointe au

même domaine. Pour plus d'informations sur l'adhésion à un domaine, voir Joindre facilement une EC2 instance Windows à votre annuaire Microsoft AD Active Directory AWS géré dans le Guide d'AWS Directory Service administration.

Détails non copiés

Les détails de configuration suivants ne sont pas copiés à partir de l'instance sélectionnée. Au lieu de cela, l'assistant applique leurs paramètres ou leur comportement par défaut :

- Nombre d'interfaces réseau : par défaut, il y a une interface réseau, qui est l'interface réseau principale (eth0).
- Stockage : la configuration de stockage par défaut est déterminée par AMI et par le type d'instance.

Lancement de plus d'instances similaires à une instance existante

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez une instance, puis choisissez Actions, Images et modèles, puis En lancer plus comme ceci.
4. L'assistant de lancement d'instance s'ouvre. Vous pouvez apporter toutes les modifications nécessaires à la configuration de l'instance en sélectionnant différentes options sur cet écran.

   Lorsque vous êtes prêt à lancer votre instance, choisissez Launch instance (Lancer l'instance).
5. Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez Résoudre les problèmes de lancement des EC2 instances Amazon.

Lancez une EC2 instance Amazon à partir d'un AWS Marketplace AMI

Vous pouvez vous abonner à une instance AWS Marketplace AMI et lancer une instance à partir de celle-ci à l'aide de la EC2 console Amazon ou d'un outil de ligne de commande. Pour plus d'informations sur AWS Marketplace AMIs, voirAMIsPayé dans le AWS Marketplace cadre des EC2 instances Amazon.

Pour annuler votre abonnement à AMI After Launch, vous devez d'abord résilier toutes les instances lancées depuis leAMI. Pour de plus amples informations, veuillez consulter Gérer vos abonnements AWS Marketplace.

New console

Pour lancer une instance depuis ou à l' AWS Marketplace AMIaide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le tableau de bord de EC2 la console Amazon, choisissez Launch instance.
3. (Facultatif) Sous Name and tags (Noms et identifications), pour Name (Nom), saisissez un nom descriptif pour votre instance.
4. Sous Images de l'application et du système d'exploitation (Amazon Machine Image)AMIs, choisissez Parcourir davantage, puis sélectionnez l'AWS Marketplace AMIsonglet. Trouvez un produit qui vous convient AMI en parcourant les catégories ou en utilisant la fonctionnalité de recherche. Pour choisir un produit, choisissez Select (Sélectionner).
5. Une fenêtre s'ouvre avec un aperçu du produit que vous avez sélectionné. Vous pouvez afficher les informations de tarification, ainsi que toute autre information communiquée par le fournisseur. Lorsque vous êtes prêt, cliquez sur l'un des boutons suivants :

   - S'abonner au lancement de l'instance : votre abonnement commence lorsque vous choisissez Launch instance (à l'étape 10).
   - Abonnez-vous maintenant — Votre abonnement commence immédiatement. Pendant que l'abonnement est en cours, vous pouvez configurer l'instance en suivant les étapes de cette procédure. En cas de problème avec les informations de votre carte bancaire, vous serez invité à mettre à jour les coordonnées de votre compte.

   > **Note**
   >
   > L'utilisation du produit ne vous est pas facturée tant que vous n'avez pas lancé une instance avec leAMI. Prenez note de la tarification pour chaque type d'instance pris en charge lorsque vous sélectionnez un type d'instance. Des taxes supplémentaires peuvent également s'appliquer au produit.

6. Pour Instance type (Type d'instance), sélectionnez un type d'instance pour votre instance. Le type d'instance définit la configuration matérielle et la taille de l'instance à lancer.
7. Sous Key pair (login) (Paire de clés (connexion)), pour Key pair name (Nom de la paire de clés), choisissez une paire de clés existante ou créez-en une.
8. Sous Paramètres réseau, pour Pare-feu (groupes de sécurité), prenez note du nouveau groupe de sécurité créé conformément aux spécifications du fournisseur pour le produit.

Le groupe de sécurité peut inclure des règles permettant à toutes les IPv4 adresses (`0.0.0.0/0`) d'accéder au SSH (port 22) sous Linux ou au RDP (port 3389) sous Windows. Il est recommandé d'ajuster ces règles pour n'autoriser qu'une adresse ou plage d'adresses spécifiques à accéder à votre instance sur ces ports.

9. Vous pouvez utiliser les autres champs sur l'écran pour configurer votre instance, ajouter du stockage et ajouter des identifications. Pour plus d'informations sur les différentes options que vous pouvez configurer, consultez Référence pour les paramètres de configuration des EC2 instances Amazon.
10. Dans le panneau Résumé, sous Image logicielle (AMI), vérifiez les détails de l'instance AMI à partir de laquelle vous êtes sur le point de lancer l'instance. Vérifiez également les autres détails de configuration que vous avez spécifiés. Lorsque vous êtes prêt à lancer votre instance , choisissez Launch instance (Lancer l'instance).
11. Selon le produit auquel vous êtes abonné, le lancement de l'instance peut prendre quelques minutes, voire plus. Si vous avez choisi S'abonner au lancement de l'instance à l'étape 5, vous êtes d'abord abonné au produit avant le lancement de votre instance. En cas de problème avec les informations de votre carte bancaire, vous serez invité à mettre à jour les coordonnées de votre compte. Lorsque la page de confirmation de lancement s'affiche, choisissez View all instances (Afficher toutes les instances) pour accéder à la page Instances.

> **Note**
>
> Le prix de l'abonnement vous est facturé aussi longtemps que votre instance est dans l'état `running`, même si elle est inactive. Si votre instance est arrêtée, il se peut que vous continuiez à être facturé pour le stockage.

12. Lorsque votre instance est à l'état `running`, vous pouvez vous y connecter. Pour ce faire, sélectionnez votre instance dans la liste, choisissez Connect (Connecter), puis choisissez une option de connexion. Pour plus d'informations sur la connexion à votre instance, consultez Connect à votre EC2 instance.

> **Important**
>
> Vérifiez attentivement les instructions d'utilisation du fournisseur, car vous devrez peut-être utiliser un nom d'utilisateur spécifique pour vous connecter à votre instance.

Pour plus d'informations sur l'accès aux détails de votre abonnement, consultez Gérer vos abonnements AWS Marketplace.

13. Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez Résoudre les problèmes de lancement des EC2 instances Amazon.

Old console

Pour lancer une instance depuis ou à l' AWS Marketplace AMIaide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le tableau de EC2 bord Amazon, choisissez Launch instance.
3. Sur la page Choisissez une image Amazon Machine (AMI), choisissez la AWS Marketplacecatégorie sur la gauche. Trouvez un produit qui vous convient AMI en parcourant les catégories ou en utilisant la fonctionnalité de recherche. Sélectionnez Select pour choisir votre produit.
4. Une présentation du produit sélectionné s'affiche dans une boîte de dialogue. Vous pouvez afficher les informations de tarification, ainsi que toute autre information communiquée par le fournisseur. Lorsque vous êtes prêt, sélectionnez Continue.

> **Note**
>
> L'utilisation du produit ne vous est pas facturée tant que vous n'avez pas lancé une instance avec leAMI. Notez la tarification de chaque type d'instance pris en charge, car vous allez être invité à sélectionner un type d'instance sur la page suivante de l'Assistant. Des taxes supplémentaires peuvent également être appliquées au produit.

5. Sur la page Choisir un type d'instance, sélectionnez la configuration matérielle et la taille de l'instance à lancer. Lorsque vous avez terminé, sélectionnez Next: Configure Instance Details.
6. Sur les pages suivantes de l'Assistant, vous pouvez configurer votre instance et ajouter du stockage, ainsi que des balises. Pour plus d'informations sur les différentes options que vous pouvez configurer, consultez Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console. Choisissez Next jusqu'à la page Configure Security Group.

L'Assistant crée un groupe de sécurité conforme aux spécifications du fournisseur pour le produit. Le groupe de sécurité peut inclure des règles permettant à toutes les IPv4 adresses (`0.0.0.0/0`) d'accéder au SSH (port 22) sous Linux ou au RDP (port 3389) sous Windows. Il est recommandé d'ajuster ces règles pour n'autoriser qu'une adresse ou plage d'adresses spécifiques à accéder à votre instance sur ces ports.

Lorsque vous êtes prêt, sélectionnez Review and Launch.

7. Sur la page Vérifier le lancement de l'instance, vérifiez les détails de l'instance à AMI partir de laquelle vous êtes sur le point de lancer l'instance, ainsi que les autres détails de configuration que vous avez définis dans l'assistant. Lorsque vous êtes prêt, sélectionnez Launch pour choisir ou créer une paire de clés, et démarrez votre instance.
8. Selon le produit auquel vous êtes abonné, le lancement de l'instance peut prendre quelques minutes, voire plus. Vous devez vous abonner au produit avant de pouvoir lancer une instance. En cas de problème avec les informations de votre carte bancaire, vous serez invité à mettre à jour les coordonnées de votre compte. Lorsque la page de confirmation de lancement s'affiche, sélectionnez View Instances pour accéder à la page Instances.

> **Note**
>
> Vous êtes facturé pour le prix de l'abonnement aussi longtemps que votre instance s'exécute, même si elle est inactive. Si votre instance est arrêtée, il se peut que vous continuiez à être facturé pour le stockage.

9. Lorsque votre instance est à l'état `running`, vous pouvez vous y connecter. Pour ce faire, sélectionnez votre instance dans la liste et choisissez Connect. Suivez les instructions de la boîte de dialogue. Pour plus d'informations sur la connexion à votre instance, consultez Connect à votre EC2 instance.

> **Important**
>
> Vérifiez attentivement les instructions d'utilisation du fournisseur, car vous devrez peut-être utiliser un nom d'utilisateur spécifique pour vous connecter à l'instance. Pour plus d'informations sur l'accès aux détails de votre abonnement, consultez Gérer vos abonnements AWS Marketplace.

10. Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez Résoudre les problèmes de lancement des EC2 instances Amazon.

Pour lancer une instance à partir d'un AWS Marketplace AMI outil de ligne de commande

Pour lancer des instances à partir de AWS Marketplace produits à l'aide d'un outil de ligne de commande, assurez-vous d'abord que vous êtes abonné au produit. Vous pouvez ensuite lancer une instance avec l'AMIID du produit en utilisant les méthodes suivantes :

Méthode	Documentation
AWS CLI	Utilisez la commande run-instances ou consultez la rubrique suivante pour plus d'informations : Lancez votre instance.
AWS Tools for Windows PowerShell	Utilisez la New-EC2Instancecommande ou consultez la rubrique suivante pour plus d'informations : Lancer une EC2 instance Amazon à l'aide de Windows PowerShell
Requête API	Utilisez la RunInstancesdemande.

Connect à votre EC2 instance

Votre EC2 instance Amazon est un serveur virtuel dans le AWS cloud. Pour vous connecter à votre instance, vous devez établir une connexion avec l'instance. La façon dont vous vous connectez à votre instance dépend du système d'exploitation de l'instance et du système d'exploitation de l'ordinateur que vous utilisez pour vous connecter à l'instance. Choisissez parmi les options décrites ci-dessous.

Options de connexion

- Connectez-vous à votre instance Linux à l'aide d'un SSH client
- Connectez-vous à votre instance Linux à l'aide de Pu TTY
- Connectez-vous à votre instance Windows à l'aide d'un RDP client
- Se connecter à une instance Windows à l'aide de Fleet Manager
- Connexion à l'aide du Gestionnaire de session

- Connectez-vous à l'aide d'EC2Instance Connect
- Connectez-vous à l'aide du point de terminaison EC2 Instance Connect

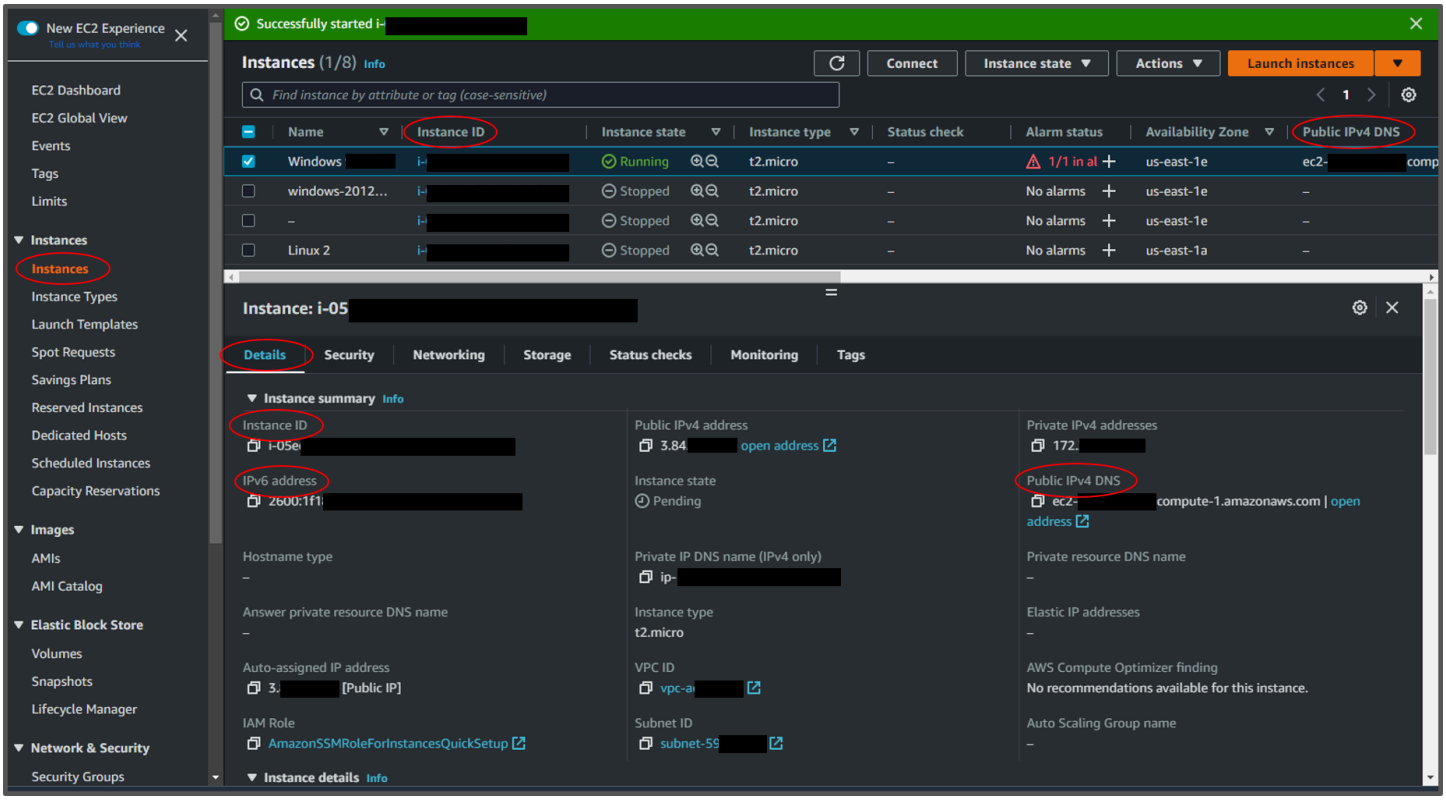
Les prérequis généraux sont les suivants. Notez que des prérequis supplémentaires peuvent être spécifiques à l'option de connexion que vous choisissez.

Prérequis généraux

- Vérifiez que votre instance a réussi les contrôles de statut. Quelques minutes peuvent être nécessaires pour qu'une instance soit prête à accepter les demandes de connexion. Pour de plus amples informations, veuillez consulter Afficher les vérifications de statut.
- Obtenez les informations requises sur l'instance.
- Localisation de la clé privée et définition des autorisations.
- (Facultatif) Obtenez l'empreinte digitale de l'instance.

Obtenez les informations requises sur l'instance

Pour préparer la connexion à votre instance, obtenez les informations suivantes depuis la EC2 console Amazon ou en utilisant la ligne de commande.



- Obtenez le DNS nom public de l'instance.

  Vous pouvez obtenir le public DNS de votre instance depuis la EC2 console Amazon. Consultez la IPv4 DNS colonne Public du volet Instances. Si cette colonne est masquée, choisissez l'icône des paramètres () dans le coin supérieur droit de l'écran, puis sélectionnez Public IPv4 DNS. Vous pouvez également trouver le public DNS dans la section des informations sur les instances du volet Instances. Lorsque vous sélectionnez l'instance dans le volet Instances de la EC2 console Amazon, les informations relatives à cette instance apparaissent dans la partie inférieure de la page. Dans l'onglet Détails, recherchez Public IPv4 DNS.

  Si vous préférez, vous pouvez utiliser les commandes describe-instances (AWS CLI) ou Get-EC2Instance(AWS Tools for Windows PowerShell).

  Si aucun message public n'IPv4DNSest affiché, vérifiez que l'état de l'instance est en cours d'exécution et que vous n'avez pas lancé l'instance dans un sous-réseau privé. Si vous avez lancé votre instance à l'aide de l'assistant de lancement d'instance, vous avez peut-être modifié le champ Attribuer automatiquement une adresse IP publique sous Paramètres réseau et changé la valeur sur Désactiver. Si vous désactivez l'option Attribuer automatiquement une adresse IP publique, aucune adresse IP publique n'est attribuée à l'instance lors de son lancement.

- (instances IPv6 uniquement) Obtenez l'IPv6adresse de l'instance.

  Si vous avez attribué une IPv6 adresse à votre instance, vous pouvez éventuellement vous connecter à l'instance en utilisant son IPv6 adresse plutôt qu'une IPv4 adresse publique ou un IPv4 DNS nom d'hôte public. Votre ordinateur local doit avoir une IPv6 adresse et doit être configuré pour être utiliséIPv6. Vous pouvez obtenir l'IPv6adresse de votre instance depuis la EC2 console Amazon. Vérifiez la IPv6IPscolonne du volet Instances. Vous pouvez également trouver l'IPv6adresse dans la section des informations sur l'instance. Lorsque vous sélectionnez l'instance dans le volet Instances de la EC2 console Amazon, les informations relatives à cette instance apparaissent dans la partie inférieure de la page. Dans l'onglet Détails, recherchez l'IPv6adresse.

  Si vous préférez, vous pouvez utiliser les commandes describe-instances (AWS CLI) ou Get-EC2Instance(AWS Tools for Windows PowerShell). Pour plus d'informations surIPv6, voirIPv6adresses.

- (Instances Linux) Obtenez le nom d'utilisateur de votre instance.

Vous pouvez vous connecter à votre instance en utilisant le nom d'utilisateur de votre compte utilisateur ou le nom d'utilisateur par défaut de AMI celui que vous avez utilisé pour lancer votre instance.

- Obtenez le nom d'utilisateur de votre compte utilisateur.

  Pour plus d'informations sur la création d'un compte utilisateur, consultez Gérez les utilisateurs du système sur votre instance Amazon EC2 Linux.
- Obtenez le nom d'utilisateur par défaut pour celui AMI que vous avez utilisé pour lancer votre instance.
  - CentOS — ou `centos` `ec2-user`
  - Debian — `admin`
  - Fedora — ou `fedora` `ec2-user`
  - RHEL— `ec2-user` ou `root`
  - SUSE— `ec2-user` ou `root`
  - Ubuntu — `ubuntu`
  - Oracle – `ec2-user`
  - Bitnami — `bitnami`
  - Rocky Linux — `rocky`
  - Autre — Vérifiez auprès du AMI fournisseur

Localisation de la clé privée et définition des autorisations

Vous devez connaître l'emplacement de votre fichier de clé privée pour établir la connexion initiale à une instance Linux SSH ou à une instance Windows utilisantRDP. Pour SSH les connexions, vous devez définir les autorisations des fichiers afin que vous soyez le seul à pouvoir lire la clé privée.

Pour plus d'informations sur le fonctionnement des paires de clés lors de l'utilisation d'AmazonEC2, consultezPaires de EC2 clés Amazon et EC2 instances Amazon.

- Localisez la clé privée.

  Vous aurez besoin du chemin d'accès qualifié complet à l'emplacement sur votre ordinateur du fichier `.pem` pour la paire de clés que vous avez spécifiée lorsque vous avez lancé l'instance. Pour de plus amples informations, veuillez consulter the section called "Identifier la clé publique spécifiée au lancement".

Si vous ne trouvez pas votre fichier de clé privée, consultez J'ai perdu ma clé privée. Comment puis-je me connecter à mon instance ?

(Instances Linux) Si vous vous connectez à votre instance via Pu TTY et que vous devez convertir le `.pem` fichier enConvertissez votre clé privée en utilisant P uTTYgen. `.ppk`

- (Instances Linux) Définissez les autorisations de votre clé privée afin que vous soyez le seul à pouvoir la lire.
  - Connexion à partir de macOS ou Linux

    Si vous envisagez d'utiliser un SSH client sur un ordinateur macOS ou Linux pour vous connecter à votre instance Linux, utilisez la commande suivante pour définir les autorisations de votre fichier de clé privée afin que vous soyez le seul à pouvoir le lire.

    ```
    chmod 400 key-pair-name.pem
    ```

    Si vous ne définissez pas ces autorisations, vous ne pouvez pas vous connecter à votre instance à l'aide de cette paire de clés. Pour de plus amples informations, veuillez consulter Erreur : fichier de clé privée non protégé.
  - Connexion à partir de Windows

    Ouvrez l'Explorateur de fichiers et cliquez avec le bouton droit sur le fichier `.pem`. Sélectionnez Propriétés > l'onglet Sécurité et choisissez Avancé. Choisissez Désactiver l'héritage. Supprimez l'accès à tous les utilisateurs à l'exception de l'utilisateur actuel.

(Facultatif) Obtenez l'empreinte digitale de l'instance

Pour vous protéger des man-in-the-middle attaques, vous pouvez vérifier l'authenticité de l'instance à laquelle vous êtes sur le point de vous connecter en vérifiant l'empreinte digitale affichée. La vérification de l'empreinte digitale est utile si vous avez lancé votre instance à partir d'un public AMI fourni par un tiers.

Présentation de la tâche

Tout d'abord, récupérez l'empreinte digitale de l'instance. Ensuite, lorsque vous vous connectez à l'instance et que vous êtes invité à vérifier l'empreinte digitale, comparez l'empreinte que vous avez obtenue au cours de cette procédure avec l'empreinte digitale affichée. Si les empreintes digitales ne

correspondent pas, quelqu'un est peut-être en train de tenter une man-in-the-middle attaque. Si elles correspondent, vous pouvez vous connecter à votre instance en toute confiance.

Conditions préalables pour obtenir l'empreinte digitale de l'instance

- L'instance ne doit pas être dans l'état `pending`. L'empreinte digitale n'est disponible qu'une fois le premier démarrage de l'instance terminé.
- Vous devez être le propriétaire de l'instance pour obtenir la sortie de la console.
- Il existe différentes manières d'obtenir l'empreinte digitale de l'instance. Si vous souhaitez utiliser le AWS CLI, il doit être installé sur votre ordinateur local. Pour plus d'informations sur l'installation du AWS CLI, reportez-vous à la section Installation du AWS Command Line Interface dans le guide de AWS Command Line Interface l'utilisateur.

Pour obtenir l'empreinte digitale de l'instance

À l'étape 1, vous obtenez la sortie de console, qui inclut l'empreinte digitale de l'instance. À l'étape 2, vous trouverez l'empreinte de l'instance dans la sortie de la console.

1. Obtenez le résultat de la console à l'aide de l'une des méthodes suivantes.

   Console

   1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
   2. Dans le navigateur de gauche, sélectionnez Instances.
   3. Sélectionnez votre instance, puis choisissez Actions, Surveiller et dépanner, puis Obtenir le journal du système.

   AWS CLI

   Sur votre ordinateur local (et non sur l'instance à laquelle vous vous connectez), utilisez la commande get-console-output(AWS CLI). Si la sortie est volumineuse, vous pouvez la diriger vers un fichier texte où elle sera peut-être plus facile à lire. Notez que vous devez spécifier un Région AWS lorsque vous utilisez le AWS CLI, soit explicitement, soit en définissant une région par défaut. Pour plus d'informations sur la façon de définir ou de spécifier une région, consultez la section Configurer le AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

```
aws ec2 get-console-output --instance-id instance_id --query Output --output
 text > temp.txt
```

2. Dans la sortie de console, recherchez l'empreinte digitale de l'instance (hôte) située sous`BEGIN SSH HOST KEY FINGERPRINTS`. Il peut y avoir plusieurs exemples d'empreintes digitales. Lorsque vous vous connectez à votre instance, celle-ci n'affiche qu'une seule des empreintes digitales.

   Le résultat exact peut varier en fonction du système d'exploitation, de AMI la version et de la AWS création ou non des paires de clés. Voici un exemple de sortie.

```
ec2:#############################################################
ec2: -----BEGIN SSH HOST KEY FINGERPRINTS-----
ec2: 256 SHA256:l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY no comment (ECDSA)
ec2: 256 SHA256:kpEa+rw/Uq3zxaYZN8KT501iBtJOIdHG52dFi66EEfQ no comment (ED25519)
ec2: 2048 SHA256:L8l6pepcA7iqW/jBecQjVZClUrKY+o2cHLI0iHerbVc no comment (RSA)
ec2: -----END SSH HOST KEY FINGERPRINTS-----
ec2: #############################################################
```

> **Note**
>
> Vous ferez référence à cette empreinte lorsque vous vous connecterez à l'instance.

Connectez-vous à votre instance Linux à l'aide de SSH

Vous pouvez vous connecter à votre instance Linux de plusieurs manières à l'aide deSSH. Certaines méthodes dépendent du système d'exploitation de l'ordinateur local à partir duquel vous vous connectez. D'autres méthodes sont basées sur un navigateur, telles que Instance EC2 Connect ou AWS Systems Manager Session Manager, et peuvent être utilisées depuis n'importe quel ordinateur. Vous pouvez l'utiliser SSH pour vous connecter à votre instance Linux et exécuter des commandes, ou SSH pour transférer des fichiers entre votre ordinateur local et votre instance.

Avant de vous connecter à votre instance Linux à l'aide deSSH, remplissez les conditions préalables suivantes :

- Vérifiez que votre instance a réussi les contrôles de statut. Quelques minutes peuvent être nécessaires pour qu'une instance soit prête à accepter les demandes de connexion. Pour de plus amples informations, veuillez consulter Afficher les vérifications de statut.
- Assurez-vous que le groupe de sécurité associé à votre instance autorise le SSH trafic entrant depuis votre adresse IP. Pour de plus amples informations, veuillez consulter Règles pour la connexion à des instances à partir de votre ordinateur.
- Obtenez les informations requises sur l'instance.
- Localisation de la clé privée et définition des autorisations.
- (Facultatif) Obtenez l'empreinte digitale de l'instance.

Choisissez ensuite l'une des options suivantes pour vous connecter à votre instance Linux à l'aide deSSH.

- Connect à l'aide d'un SSH client
- Connectez-vous à l'aide de Pu TTY
- Transférez des fichiers en utilisant SCP

Si vous ne parvenez pas à vous connecter à votre instance et que vous avez besoin d'aide pour résoudre les problèmes, consultezRésoudre les problèmes de connexion à votre instance Amazon EC2 Linux.

Connectez-vous à votre instance Linux à l'aide d'un SSH client

Vous pouvez utiliser Secure Shell (SSH) pour vous connecter à votre instance Linux depuis votre ordinateur local. Pour plus d'informations sur les autres options, consultezConnect à votre EC2 instance.

> **Note**
>
> Si vous recevez un message d'erreur lorsque vous tentez de vous connecter à votre instance, assurez-vous que celle-ci répond à toutes les SSHprérequis de connexion. Si elle répond à toutes les conditions préalables et que vous ne parvenez toujours pas à vous connecter à votre instance Linux, veuillez consulter la rubrique Résoudre les problèmes de connexion à votre instance Amazon EC2 Linux.

Table des matières

SSHprérequis de connexion

Avant de pouvoir vous connecter à votre instance Linux à l'aide deSSH, effectuez les tâches suivantes.

Complétez les prérequis généraux.

- Vérifiez que votre instance a réussi les contrôles de statut. Quelques minutes peuvent être nécessaires pour qu'une instance soit prête à accepter les demandes de connexion. Pour de plus amples informations, veuillez consulter Afficher les vérifications de statut.
- Obtenez les informations requises sur l'instance.
- Localisation de la clé privée et définition des autorisations.
- (Facultatif) Obtenez l'empreinte digitale de l'instance.

Autorisez le SSH trafic entrant depuis votre adresse IP.

Assurez-vous que le groupe de sécurité associé à votre instance autorise le SSH trafic entrant depuis votre adresse IP. Pour de plus amples informations, veuillez consulter Règles pour la connexion à des instances à partir de votre ordinateur.

Installez un SSH client sur votre ordinateur local (si nécessaire).

Un SSH client est peut-être installé par défaut sur votre ordinateur local. Vous pouvez le vérifier en saisissant la commande suivante dans une fenêtre de terminal. Si votre ordinateur ne reconnaît pas la commande, vous devez installer un SSH client.

```
ssh
```

Voici quelques-unes des options possibles pour Windows. Si votre ordinateur exécute un autre système d'exploitation, consultez la documentation de ce système d'exploitation pour connaître les options SSH du client.

Installer Open SSH sous Windows

Après avoir installé Open SSH sous Windows, vous pouvez vous connecter à votre instance Linux depuis votre ordinateur Windows à l'aide deSSH. Avant de commencer, assurez-vous que vous répondez aux exigences suivantes.

Version Windows

La version de Windows installée sur votre ordinateur doit être Windows Server 2019 ou une version ultérieure.

Pour les versions antérieures de Windows, téléchargez et installez Win32-Open SSH à la place.

PowerShell exigences

Pour installer Open SSH sur votre système d'exploitation Windows à l'aide de PowerShell, vous devez exécuter la PowerShell version 5.1 ou ultérieure et votre compte doit être membre du groupe d'administrateurs intégré. Exécutez PowerShell à `$PSVersionTable.PSVersion` partir de pour vérifier votre PowerShell version.

Pour vérifier si vous êtes membre du groupe d'administrateurs intégré, exécutez la PowerShell commande suivante :

```
(New-Object
 Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())).Is
```

Si vous êtes membre du groupe d'administrateurs intégré, le résultat est `True`.

Pour installer Open SSH pour Windows à l'aide de PowerShell, exécutez la PowerShell commande suivante.

```
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Voici un exemple de sortie.

```
Path          :
Online        : True
RestartNeeded : False
```

Pour désinstaller Open SSH de Windows à l'aide de PowerShell, exécutez la PowerShell commande suivante.

```
Remove-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Voici un exemple de sortie.

```
Path          :
Online        : True
RestartNeeded : True
```

Installer le sous-système Windows pour Linux () WSL

Après l'installation WSL sous Windows, vous pouvez vous connecter à votre instance Linux depuis votre ordinateur Windows à l'aide d'outils de ligne de commande Linux, tels qu'un SSH client.

Suivez les instructions de la section Installez le sous-système Windows pour Linux sur votre instance EC2 Windows. Si vous suivez les instructions du guide d'installation de Microsoft, ils installent la distribution Ubuntu de Linux. Vous pouvez installer une autre distribution Linux si vous le souhaitez.

Dans une fenêtre de WSL terminal, copiez le `.pem` fichier (pour la paire de clés que vous avez spécifiée pour votre instance au lancement) de Windows versWSL. Notez le chemin complet vers le `.pem` fichier WSL à utiliser lors de la connexion à votre instance. Pour plus d'informations sur la façon de spécifier le chemin vers votre disque dur Windows, consultez How do I access my C drive ?.

```
cp /mnt/<Windows drive letter>/path/my-key-pair.pem ~/WSL-path/my-key-pair.pem
```

Pour plus d'informations sur la désinstallation du sous-système Windows pour Linux, consultez Comment désinstaller une WSL distribution ? .

Connectez-vous à votre instance Linux à l'aide d'un SSH client

Suivez la procédure ci-dessous pour vous connecter à votre instance Linux à l'aide d'un SSH client.

Pour vous connecter à votre instance à l'aide d'un SSH client

1. Ouvrez une fenêtre de terminal sur votre ordinateur.
2. Utilisez la ssh commande pour vous connecter à l'instance. Vous avez besoin des informations relatives à votre instance que vous avez collectées dans le cadre des prérequis. Par exemple, vous avez besoin de l'emplacement de la clé privée (`.pem`fichier), du nom d'utilisateur et du DNS nom ou de l'IPv6adresse publics. Voici des exemples de commandes.
   - (PublicDNS) Pour utiliser le DNS nom public, entrez la commande suivante.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-dns-name
```

- (IPv6) Sinon, si votre instance possède une IPv6 adresse, entrez la commande suivante pour utiliser l'IPv6adresse.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-IPv6-address
```

Voici un exemple de réponse.

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (198-51-100-1)'
 can't be established.
ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
Are you sure you want to continue connecting (yes/no)?
```

3. (Facultatif) Vérifiez que l'empreinte de l'alerte de sécurité correspond à l'empreinte digitale. Si ces empreintes ne correspondent pas, il se peut que quelqu'un tente une man-in-the-middle attaque. Si elles correspondent, passez à l'étape suivante. Pour plus d'informations, consultez Obtenir l'empreinte digitale de l'instance.
4. Saisissez **yes**.

   Vous verrez une réponse telle que celle ci-après:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (ECDSA) to
 the list of known hosts.
```

Connectez-vous à votre instance Linux à l'aide de Pu TTY

Vous pouvez vous connecter à votre instance Linux à l'aide de PuTTY, un SSH client gratuit pour Windows.

Si vous utilisez Windows Server 2019 ou une version ultérieure, nous vous recommandons d'utiliser OpenSSH, un outil de connectivité open source pour la connexion à distance à l'aide du SSH protocole.

> **Note**
>
> Si vous recevez un message d'erreur lorsque vous tentez de vous connecter à votre instance, assurez-vous que celle-ci répond à toutes les SSHprérequis de connexion. Si elle répond à

toutes les conditions préalables et que vous ne parvenez toujours pas à vous connecter à votre instance Linux, veuillez consulter la rubrique Résoudre les problèmes de connexion à votre instance Amazon EC2 Linux.

Table des matières

Prérequis

Avant de vous connecter à votre instance Linux à l'aide de PuTTY, effectuez les tâches suivantes.

Complétez les prérequis généraux.

- Vérifiez que votre instance a réussi les contrôles de statut. Quelques minutes peuvent être nécessaires pour qu'une instance soit prête à accepter les demandes de connexion. Pour plus d'informations, consultez Afficher les vérifications de statut.
- Obtenez les informations requises sur l'instance.
- Localisation de la clé privée et définition des autorisations.
- (Facultatif) Obtenez l'empreinte digitale de l'instance.

Autorisez le SSH trafic entrant depuis votre adresse IP.

Assurez-vous que le groupe de sécurité associé à votre instance autorise le SSH trafic entrant depuis votre adresse IP. Pour plus d'informations, consultez Règles pour la connexion à des instances à partir de votre ordinateur.

Installez Pu TTY sur votre ordinateur local (si nécessaire).

Téléchargez et installez Pu TTY depuis la page de TTY téléchargement de Pu. Si vous avez déjà TTY installé une version antérieure de Pu, nous vous recommandons de télécharger la dernière version. Assurez-vous d'installer toute la suite.

Convertissez votre clé privée au PPK format P uTTYgen

Vous devez spécifier la clé privée pour la paire de clés que vous avez spécifiée lorsque vous avez lancé l'instance. Si vous avez créé la clé privée au format .pem, vous devez la convertir en PPK

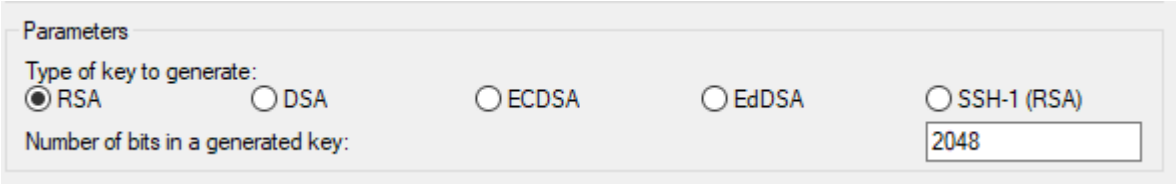
fichier à utiliser avec Pu. TTY Localisez la clé privée (fichier .pem), puis suivez les étapes décrites dans. Convertissez votre clé privée en utilisant P uTTYgen

(Facultatif) Convertissez votre clé privée en utilisant P uTTYgen

Pu TTY ne prend pas en charge nativement le PEM format des SSH clés. Pu TTY fournit un outil nommé PuTTYgen, qui convertit PEM les clés au PPK format requis pour PuTTY. Si vous avez créé la clé en utilisant le PEM format plutôt que le PPK format, vous devez convertir votre clé privée (fichier .pem) dans ce format (fichier .ppk) pour l'utiliser avec Pu. TTY

Pour convertir votre clé privée du PPK format PEM au format

1. Dans le menu Démarrer, choisissez Tous les programmes, Pu TTY, uTTYgenP.
2. Sous Type de clé à générer, sélectionnez RSA. Si votre version de P uTTYgen n'inclut pas cette option, choisissez SSH-2 RSA.



3. Choisissez Load (Charger). Par défaut, P uTTYgen affiche uniquement les fichiers portant l'extension `.ppk`. Pour trouver votre fichier `.pem`, choisissez l'option permettant d'afficher tous les types de fichiers.

4. Sélectionnez votre fichier `.pem` pour la paire de clés que vous avez spécifiée lorsque vous avez lancé votre instance, puis choisissez Ouvrir. P uTTYgen affiche une notification indiquant que le `.pem` fichier a été importé avec succès. Choisissez OK.
5. Pour enregistrer la clé dans le format que Pu TTY peut utiliser, choisissez Enregistrer la clé privée. P uTTYgen affiche un avertissement concernant l'enregistrement de la clé sans phrase secrète. Choisissez Oui.

> **Note**
>
> La phrase secrète d'une clé privée constitue une couche supplémentaire de protection. Même si votre clé privée est découverte, elle ne peut pas être utilisée sans la phrase

secrète. Le désavantage d'une phrase secrète est qu'elle rend l'automatisation plus difficile, car l'intervention humaine est nécessaire pour se connecter à une instance, ou copier des fichiers vers une instance.

6. Spécifiez le même nom pour la clé que celui que vous avez utilisé pour la paire de clés (par exemple, `key-pair-name`) et choisissez Enregistrer. Pu ajoute TTY automatiquement l'extension `.ppk` du fichier.

Votre clé privée est désormais au bon format pour une utilisation avec PuTTY. Vous pouvez désormais vous connecter à votre instance à l'aide TTY du SSH client de Pu.

Connectez-vous à votre instance Linux

Utilisez la procédure suivante pour vous connecter à votre instance Linux à l'aide de PuTTY. Vous aurez besoin du fichier `.ppk` que vous avez créé pour votre clé privée. Pour plus d'informations, consultez (Facultatif) Convertissez votre clé privée en utilisant P uTTYgen dans la section précédente. Si vous recevez une erreur lors d'une tentative de connexion à votre instance, consultez Résoudre les problèmes de connexion à votre instance Amazon EC2 Linux.

Dernière version testée — Pu TTY 7.8

Pour vous connecter à votre instance à l'aide de Pu TTY

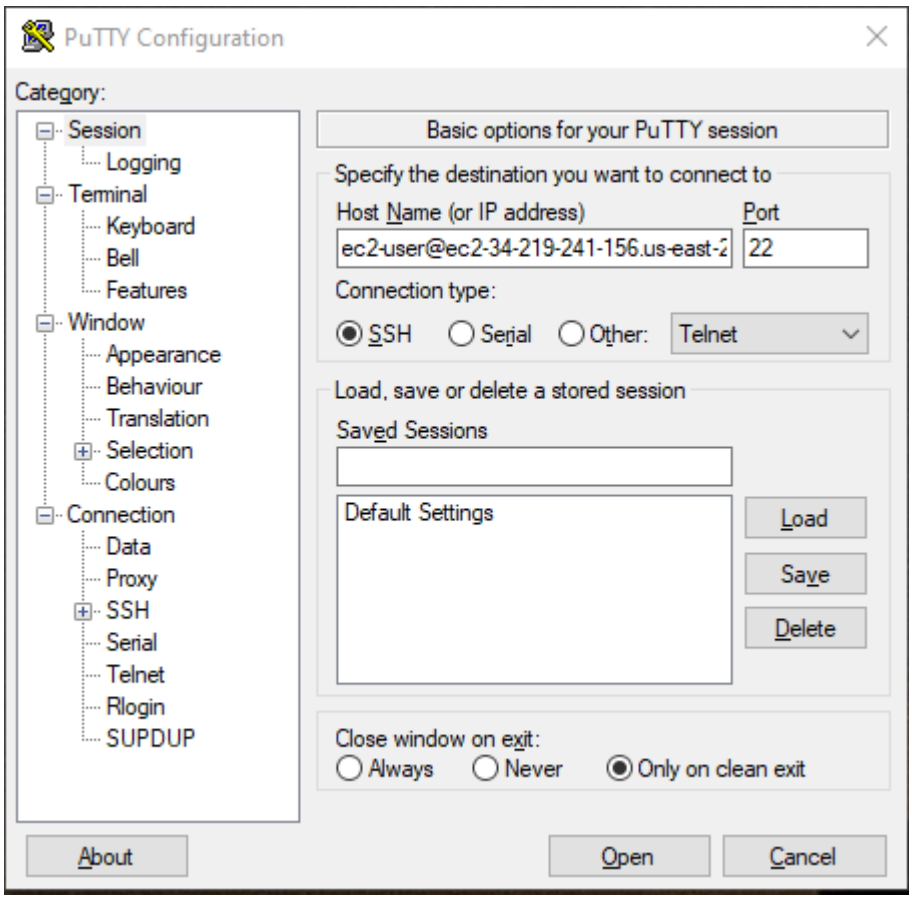
1. Démarrez Pu TTY (dans le menu Démarrer, recherchez Pu, TTY puis choisissez Ouvrir).
2. Dans le volet Catégorie, Choisissez Session et complétez les champs suivants :

   a. Dans la zone Host Name (Nom d'hôte), effectuez l'une des opérations suivantes :
      - (PublicDNS) Pour vous connecter en utilisant le DNS nom public de votre instance, entrez *instance-user-name*@*instance-public-dns-name*.
      - (IPv6) Sinon, si votre instance possède une IPv6 adresse, pour vous connecter à l'aide de l'IPv6adresse de votre instance, entrez *instance-user-name*@*instance-IPv6-address*.

      Pour plus d'informations sur la façon d'obtenir le nom d'utilisateur de votre instance, ainsi que le DNS nom ou l'IPv6adresse publics de votre instance, consultezObtenez les informations requises sur l'instance.

   b. Vérifiez que Port a pour valeur 22.

   c. Sous Type de connexion, sélectionnez SSH.



3. (Facultatif) Vous pouvez configurer Pu TTY pour qu'il envoie automatiquement des données « keepalive » à intervalles réguliers afin de maintenir la session active. Cela est particulièrement utile et vous évite de vous déconnecter de votre instance en raison de l'inactivité de la session. Dans le volet Catégorie, choisissez Connexion, puis entrez l'intervalle requis dans le champ Secondes écoulées entre les paquets keepalive. Par exemple, si votre session se déconnecte après 10 minutes d'inactivité, entrez 180 pour configurer Pu TTY afin qu'il envoie des données keepalive toutes les 3 minutes.
4. Dans le volet Catégorie, développez Connection et Auth. SSH Choisissez Informations d'identification.
5. À côté de Fichier de clé privée pour l'authentification, choisissez Parcourir. Dans la boîte de dialogue Sélectionner le fichier de clé privée, sélectionnez le fichier `.ppk` que vous avez généré pour votre paire de clés. Vous pouvez soit double-cliquer sur le fichier, soit choisir Ouvrir dans la boîte de dialogue Sélectionner un fichier de clé privée.
6. (Facultatif) Si vous comptez vous reconnecter à cette instance après cette session, vous pouvez enregistrer les informations correspondantes pour les utiliser à l'avenir. Dans le volet Catégorie,

choisissez Session. Saisissez un nom pour la session dans Sessions enregistrées, puis choisissez Enregistrer.

7. Pour vous connecter à l'instance, choisissez Ouvrir.
8. Si c'est la première fois que vous vous connectez à cette instance, Pu TTY affiche une boîte de dialogue d'alerte de sécurité qui vous demande si vous faites confiance à l'hôte auquel vous vous connectez.

   a. (Facultatif) Vérifiez que l'empreinte dans la boîte de dialogue d'alerte de sécurité correspond à l'empreinte que vous avez obtenue précédemment dans (Facultatif) Obtenez l'empreinte digitale de l'instance. Si ces empreintes ne correspondent pas, quelqu'un est peut-être en train de tenter une attaque « man-in-the-middle ». Si elles correspondent, passez à l'étape suivante.

   b. Choisissez Accepter. Une fenêtre s'ouvre et vous êtes connecté à votre instance.

> **Note**
>
> Si vous avez spécifié un mot de passe lorsque vous avez converti votre clé privée au TTY format Pu, vous devez fournir ce mot de passe lorsque vous vous connectez à l'instance.

Si vous recevez une erreur lors d'une tentative de connexion à votre instance, consultez Résoudre les problèmes de connexion à votre instance Amazon EC2 Linux.

Transférez des fichiers vers une instance Linux à l'aide de SCP

L'un des moyens de transférer des fichiers entre votre ordinateur local et une instance Linux consiste à utiliser le protocole de copie sécurisée (SCP). Cette section décrit comment transférer des fichiers avecSCP. La procédure est similaire à la procédure de connexion à une instance avecSSH.

Avant de vous connecter à votre instance Linux à l'aide deSCP, effectuez les tâches suivantes :

- Complétez les prérequis généraux.
  - Vérifiez que votre instance a réussi les contrôles de statut. Quelques minutes peuvent être nécessaires pour qu'une instance soit prête à accepter les demandes de connexion. Pour de plus amples informations, veuillez consulter Afficher les vérifications de statut.
  - Obtenez les informations requises sur l'instance.
  - Localisation de la clé privée et définition des autorisations.

  - (Facultatif) Obtenez l'empreinte digitale de l'instance.
- Autorisez le SSH trafic entrant depuis votre adresse IP.

  Assurez-vous que le groupe de sécurité associé à votre instance autorise le SSH trafic entrant depuis votre adresse IP. Pour de plus amples informations, veuillez consulter Règles pour la connexion à des instances à partir de votre ordinateur.
- Installez un SCP client.

  La plupart des ordinateurs Linux, Unix et Apple incluent un SCP client par défaut. Si le vôtre ne le fait pas, le SSH projet Open fournit une implémentation gratuite de la suite complète d'SSHoutils, y compris un SCP client. Pour plus d'informations, consultez https://www.openssh.com.

La procédure suivante vous explique comment SCP transférer un fichier en utilisant le DNS nom public de l'instance, ou l'IPv6adresse si votre instance en possède une.

À utiliser SCP pour transférer des fichiers entre votre ordinateur et votre instance

1. Déterminez l'emplacement du fichier source sur votre ordinateur et le chemin d'accès de destination sur l'instance. Dans les exemples suivants, le nom du fichier de clé privée est`key-pair-name.pem`, le fichier à transférer est`my-file.txt`, le nom d'utilisateur de l'instance estec2-user, le DNS nom public de l'instance est `instance-public-dns-name` et l'IPv6adresse de l'instance est`instance-IPv6-address`.
   - (PublicDNS) Pour transférer un fichier vers la destination sur l'instance, entrez la commande suivante depuis votre ordinateur.

     ```
     scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@instance-public-dns-name:path/
     ```
   - (IPv6) Pour transférer un fichier vers la destination sur l'instance si celle-ci possède une IPv6 adresse, entrez la commande suivante depuis votre ordinateur. L'IPv6adresse doit être placée entre crochets (`[ ]`), qui doivent être exclus (\).

     ```
     scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@\[instance-IPv6-address\]:path/
     ```
2. Si vous n'êtes pas encore connecté à l'instance en utilisantSSH, vous voyez une réponse comme celle-ci :

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

(Facultatif) Vous pouvez vérifier si l'empreinte digitale de l'alerte de sécurité correspond à l'empreinte digitale de l'instance. Pour plus d'informations, consultez (Facultatif) Obtenez l'empreinte digitale de l'instance.

Saisissez **`yes`**.

3. Si le transfert réussit, la réponse est semblable à la suivante :

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
my-file.txt                                   100%   480     24.4KB/s   00:00
```

4. Pour transférer un fichier dans l'autre sens (de votre EC2 instance Amazon vers votre ordinateur), inversez l'ordre des paramètres de l'hôte. Par exemple, vous pouvez effectuer un transfert `my-file.txt` de votre EC2 instance vers une destination sur votre ordinateur local`my-file2.txt`, comme indiqué dans les exemples suivants.

   - (PublicDNS) Pour transférer un fichier vers une destination sur votre ordinateur, entrez la commande suivante depuis votre ordinateur.

     ```
     scp -i /path/key-pair-name.pem ec2-user@instance-public-dns-name:path/my-file.txt path/my-file2.txt
     ```

   - (IPv6) Pour transférer un fichier vers une destination sur votre ordinateur si l'instance possède une IPv6 adresse, entrez la commande suivante depuis votre ordinateur. L'IPv6adresse doit être placée entre crochets (`[ ]`), qui doivent être exclus (`\`).

     ```
     scp -i /path/key-pair-name.pem ec2-user@\[instance-IPv6-address\]:path/my-file.txt path/my-file2.txt
     ```

Gérez les utilisateurs du système sur votre instance Amazon EC2 Linux

Chaque type d'instance Linux est lancé avec un utilisateur du système Linux par défaut. Vous pouvez ajouter et supprimer des utilisateurs de votre instance.

Pour l'utilisateur par défaut, le nom d'utilisateur par défaut est déterminé par celui AMI qui a été spécifié lorsque vous avez lancé l'instance.

> **Note**
>
> Par défaut, l'authentification par mot de passe et la connexion racine sont désactivées, et sudo est activé. Pour vous connecter à votre instance, vous devez utiliser une paire de clés. Pour plus d'informations sur la connexion, consultez Connectez-vous à votre instance Linux à l'aide de SSH.
> Vous pouvez autoriser l'authentification par mot de passe et la connexion racine pour votre instance. Pour plus d'informations, consultez la documentation de votre système d'exploitation.

> **Note**
>
> Les utilisateurs du système Linux ne doivent pas être confondus avec IAM les utilisateurs. Pour plus d'informations, consultez le Guide de l'IAMutilisateur pour les IAMutilisateurs.

Table des matières

Noms d'utilisateur par défaut

Le nom d'utilisateur par défaut de votre EC2 instance est déterminé par celui AMI qui a été spécifié lors du lancement de l'instance.

Les noms d'utilisateur par défaut sont les suivants :

- Pour un Amazon LinuxAMI, le nom d'utilisateur est`ec2-user`.
- Pour un CentOSAMI, le nom d'utilisateur est `centos` ou. `ec2-user`
- Pour une DebianAMI, le nom d'utilisateur est`admin`.
- Pour un FedoraAMI, le nom d'utilisateur est `fedora` ou`ec2-user`.

- Pour un RHELAMI, le nom d'utilisateur est `ec2-user` ou`root`.
- Pour un SUSEAMI, le nom d'utilisateur est `ec2-user` ou`root`.
- Pour un UbuntuAMI, le nom d'utilisateur est`ubuntu`.
- Pour un OracleAMI, le nom d'utilisateur est`ec2-user`.
- Pour un BitnamiAMI, le nom d'utilisateur est. `bitnami`

> **Note**
>
> Pour trouver le nom d'utilisateur par défaut pour les autres distributions Linux, contactez le AMI fournisseur.

Considérations

L'utilisation de l'utilisateur par défaut convient à de nombreuses applications. Toutefois, vous pouvez décider d'ajouter des utilisateurs afin que les individus puissent disposer de leurs propres fichiers et espaces de travail. Par ailleurs, la création d'utilisateurs pour de nouveaux utilisateurs est beaucoup plus sécurisée que l'octroi à plusieurs utilisateurs (probablement inexpérimentés) de l'accès à l'utilisateur par défaut, car l'utilisateur par défaut peut engendrer beaucoup de dommages à un système lorsqu'il est mal utilisé. Pour plus d'informations, consultez la section Conseils pour sécuriser votre EC2 instance.

Pour permettre SSH aux utilisateurs d'accéder à votre EC2 instance à l'aide d'un utilisateur du système Linux, vous devez partager la SSH clé avec l'utilisateur. Vous pouvez également utiliser EC2 Instance Connect pour fournir un accès aux utilisateurs sans qu'il soit nécessaire de partager et de gérer les SSH clés. Pour de plus amples informations, veuillez consulter Connectez-vous à votre instance Linux à l'aide d'EC2Instance Connect.

Créez un utilisateur

Créez d'abord l'utilisateur, puis ajoutez la clé SSH publique qui permet à l'utilisateur de se connecter et de se connecter à l'instance.

> **Important**
>
> À l'étape 1 de cette procédure, vous allez créer une nouvelle paire de clés. Comme une paire de clés fonctionne comme un mot de passe, il est essentiel de la gérer en toute sécurité. Si vous créez une paire de clés pour un utilisateur, vous devez vous assurer que la clé privée

lui est envoyée de manière sécurisée. L'utilisateur peut également effectuer les étapes 1 et 2 en créant sa propre paire de clés, en sécurisant la clé privée sur son ordinateur, puis en vous envoyant la clé publique pour terminer la procédure de l'étape 3.

Pour créer un utilisateur

1. Créez une nouvelle paire de clés. Vous devez fournir le fichier `.pem` à l'utilisateur pour lequel vous créez l'utilisateur. Ils doivent utiliser ce fichier pour se connecter à l'instance.
2. Récupérez la clé publique de la paire de clés que vous avez créée à l'étape précédente.

   ```
   $ ssh-keygen -y -f /path_to_key_pair/key-pair-name.pem
   ```

   La commande renvoie la clé publique, comme indiqué dans l'exemple suivant.

   ```
   ssh-rsa
    AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6Vhz2ItxCih
   +PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/
   d6RJhJOI0iBXrlsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/
   i8SeJtjnV3iAoG/cQk+0FzZqaeJAAHco
   +CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi
   +z7wB3RbBQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
   ```

3. Connectez-vous à l'instance.
4. Utilisez la commande adduser pour créer l'utilisateur et l'ajouter au système (avec une entrée dans le fichier `/etc/passwd`). Cette commande crée également un groupe et un répertoire de base pour l'utilisateur. Dans cet exemple, l'utilisateur est nommé *`newuser`*.

   - AL2023 et Amazon Linux 2

     Avec AL2 023 et Amazon Linux 2, l'utilisateur est créé avec l'authentification par mot de passe désactivée par défaut.

     ```
     [ec2-user ~]$ sudo adduser newuser
     ```

   - Ubuntu

     Incluez le paramètre `--disabled-password` pour créer l'utilisateur avec l'authentification par mot de passe désactivée.

```
[ubuntu ~]$ sudo adduser newuser --disabled-password
```

5. Passez au nouvel utilisateur afin que le répertoire et le fichier que vous créez aient le droit de propriété approprié.

```
[ec2-user ~]$ sudo su - newuser
```

L'invite passe de `ec2-user` à *`newuser`* pour indiquer que vous avez basculé de la session shell au nouvel utilisateur.

6. Ajoutez la clé SSH publique à l'utilisateur. Créez d'abord un répertoire dans le répertoire personnel de l'utilisateur pour le fichier SSH clé, puis créez le fichier clé et collez enfin la clé publique dans le fichier clé, comme décrit dans les sous-étapes suivantes.

   a. Créez un répertoire `.ssh` dans le répertoire de base *`newuser`* et modifiez ses autorisations de fichier en `700` (seul le propriétaire peut ouvrir le répertoire et y lire ou y écrire).

```
[newuser ~]$ mkdir .ssh
```

```
[newuser ~]$ chmod 700 .ssh
```

> **Important**
>
> Sans les autorisations de fichier exactes, l'utilisateur ne pourra pas se connecter.

   b. Créez un fichier nommé `authorized_keys` dans le répertoire `.ssh` et modifiez ses autorisations de fichier en `600` (seul le propriétaire peut lire le fichier ou y écrire).

```
[newuser ~]$ touch .ssh/authorized_keys
```

```
[newuser ~]$ chmod 600 .ssh/authorized_keys
```

> **Important**
>
> Sans les autorisations de fichier exactes, l'utilisateur ne pourra pas se connecter.

c. Ouvrez le fichier `authorized_keys` avec votre éditeur de texte préféré (comme vim ou nano).

```
[newuser ~]$ nano .ssh/authorized_keys
```

Collez la clé publique que vous avez récupérée à l' étape 2 dans le fichier et enregistrez les modifications.

> **Important**
>
> Assurez-vous que vous collez la clé publique dans une ligne continue. La clé publique ne doit pas être divisée sur plusieurs lignes.

L'utilisateur doit pouvoir se connecter à l'utilisateur *`newuser`* de votre instance à l'aide de la clé privée qui correspond à la clé publique que vous avez ajoutée au fichier `authorized_keys`. Pour plus d'informations sur les différentes méthodes de connexion à une instance Linux, consultez Connectez-vous à votre instance Linux à l'aide de SSH.

Supprimer un utilisateur

Si un utilisateur n'est plus nécessaire, vous pouvez supprimer cet utilisateur pour qu'il ne puisse plus être utilisé.

Utilisez la commande userdel pour supprimer l'utilisateur du système. Quand vous spécifiez le paramètre `-r`, le répertoire de base et le fichier temporaire des e-mails de l'utilisateur sont supprimés. Pour conserver le répertoire de base et le fichier temporaire des e-mails de l'utilisateur, omettez le paramètre `-r`.

```
[ec2-user ~]$ sudo userdel -r olduser
```

Connectez-vous à votre instance Windows à l'aide de RDP

Vous pouvez vous connecter aux EC2 instances Amazon créées à partir de la plupart des Amazon Machine Images (AMIs) Windows à l'aide de Remote Desktop. Remote Desktop utilise le protocole Remote Desktop (RDP) pour se connecter à votre instance et l'utiliser de la même manière que vous utilisez un ordinateur situé devant vous (ordinateur local). Il est disponible sur la plupart des éditions de Windows et disponible pour Mac OS.

La licence pour le système d'exploitation Windows Server autorise deux connexions à distance simultanées à des fins administratives. La licence pour Windows Server est incluse dans le prix de votre instance Windows. Si vous avez besoin de plus de deux connexions à distance simultanées, vous devez acheter une licence Remote Desktop Services (RDS). Si vous tentez une troisième connexion, une erreur se produit.

> **Tip**
>
> Si vous devez vous connecter à votre instance afin de résoudre les problèmes de démarrage, de configuration réseau et d'autres problèmes liés aux instances créées sur le système Nitro AWS, vous pouvez utiliser la EC2Console série pour instances.

Table des matières

Connectez-vous à votre instance Windows à l'aide d'un RDP client

Vous pouvez vous connecter à votre instance Windows à l'aide d'un RDP client comme suit.

> **Tip**
>
> Vous pouvez également vous connecter à votre instance Windows à l'aide de Systems Manager Fleet Manager ou EC2Instance Connect Endpoint.

Prérequis

Vous devez remplir les conditions préalables suivantes pour vous connecter à votre instance Windows à l'aide d'un RDP client.

- Complétez les prérequis généraux.
  - Vérifiez que votre instance a réussi les contrôles de statut. Quelques minutes peuvent être nécessaires pour qu'une instance soit prête à accepter les demandes de connexion. Pour de plus amples informations, veuillez consulter Afficher les vérifications de statut.

  - Obtenez les informations requises sur l'instance.
  - Localisation de la clé privée et définition des autorisations.
  - (Facultatif) Obtenez l'empreinte digitale de l'instance.
- Installez un RDP client.
  - (Windows) Windows inclut un RDP client par défaut. Pour vérifier, tapez mstsc dans une fenêtre d'invite de commande. Si votre ordinateur ne reconnaît pas cette commande, consultez la page d'accueil Microsoft Windows et recherchez la page de téléchargement de l'application Bureau à distance Microsoft.
  - (macOS X) Téléchargez l'application Microsoft Remote Desktop depuis le Mac App Store.
  - (Linux) Utilisez Remmina.
- Autorisez le RDP trafic entrant depuis votre adresse IP.

  Assurez-vous que le groupe de sécurité associé à votre instance autorise le RDP trafic entrant depuis votre adresse IP. Pour de plus amples informations, veuillez consulter Règles pour la connexion à des instances à partir de votre ordinateur.

Récupérez le mot de passe administrateur

Si vous avez joint votre instance à un domaine, vous pouvez vous y connecter à l'aide des informations d'identification du domaine provenant de AWS Directory Service. Sur l'écran de connexion à Remote Desktop, au lieu d'utiliser le nom de l'ordinateur local et le mot de passe généré, utilisez le nom d'utilisateur complet de l'administrateur (par exemple,**`corp.example.com\Admin`**) et le mot de passe de ce compte.

Pour vous connecter à une instance Windows à l'aide deRDP, vous devez récupérer le mot de passe administrateur initial, puis saisir ce mot de passe lorsque vous vous connectez à votre instance. Il faut quelques minutes après le lancement de l'instance pour que ce mot de passe soit disponible.

Le nom d'utilisateur par défaut du compte administrateur dépend de la langue du système d'exploitation (OS) contenu dans leAMI. Pour déterminer le nom d'utilisateur correct, identifiez la langue AMI de votre système d'exploitation, puis choisissez le nom d'utilisateur correspondant. Par exemple, pour un système d'exploitation anglais, le nom d'utilisateur est`Administrator`, pour un système d'exploitation français, c'est le cas`Administrateur`, et pour un système d'exploitation portugais, c'est le cas`Administrador`. Si une version linguistique du système d'exploitation ne possède pas de nom d'utilisateur dans la même langue, choisissez-le`Administrator (Other)`.

Pour plus d'informations, consultez la section Noms localisés du compte administrateur sous Windows sur le Microsoft TechNet Wiki.

Pour récupérer le mot de passe administrateur initial

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance, puis choisissez Connecter.
4. Sur la page Connect to instance, sélectionnez l'onglet RDPclient.
5. Dans Nom d'utilisateur, choisissez le nom d'utilisateur par défaut pour le compte administrateur. Le nom d'utilisateur que vous choisissez doit correspondre à la langue du système d'exploitation (OS) contenu dans celui AMI que vous avez utilisé pour lancer votre instance. S'il n'existe aucun nom d'utilisateur dans la même langue que votre système d'exploitation, choisissez Administrator (Other).
6. Choisissez Obtenir le mot de passe.
7. Sur la page Obtenir le mot de passe Windows, procédez comme suit :

    a. Choisissez Télécharger le fichier de clé privée et accédez au fichier de clé privée (`.pem`) que vous avez spécifié lors du lancement de l'instance. Sélectionnez le fichier, puis choisissez Open (Ouvrir) pour copier tout le contenu du fichier dans cette page.

    b. Choisissez Déchiffrer le mot de passe. La page Obtenir le mot de passe Windows se ferme et le mot de passe administrateur par défaut de l'instance apparaît sous Mot de passe, en remplacement du lien Obtenir le mot de passe affiché précédemment.

    c. Copiez le mot de passe et enregistrez-le en lieu sûr. Vous en aurez besoin pour vous connecter à l'instance.

Connexion à votre instance Windows

La procédure suivante utilise le client Remote Desktop Connection pour Windows (MSTSC). Si vous utilisez un autre RDP client, téléchargez le RDP fichier, puis consultez la documentation du RDP client pour connaître les étapes à suivre pour établir la RDP connexion.

Pour vous connecter à une instance Windows à l'aide d'un RDP client

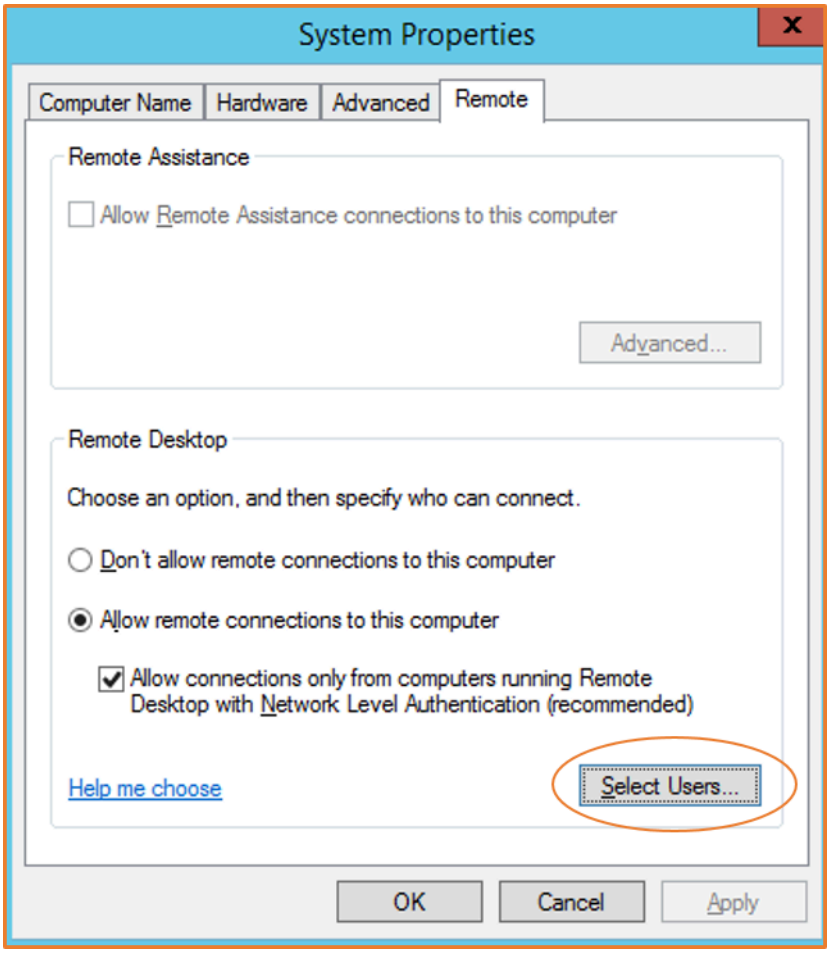
1. Sur la page Connect to instance, choisissez Download remote desktop file. Lorsque le téléchargement du fichier est terminé, choisissez Annuler pour revenir à la page Instances. Le RDP fichier est téléchargé `Downloads` dans votre dossier.

2. Exécutez `mstsc.exe` pour ouvrir le RDP client.
3. Développez les options Afficher, choisissez Ouvrir, puis sélectionnez le fichier .rdp dans votre `Downloads` dossier.
4. Par défaut, Ordinateur est le IPv4 DNS nom public de l'instance et Nom d'utilisateur est le compte administrateur. Pour vous connecter à l'instance en utilisant IPv6 plutôt, remplacez le IPv4 DNS nom public de l'instance par son IPv6 adresse. Vérifiez les paramètres par défaut et modifiez-les si nécessaire.
5. Choisissez Se connecter. Si vous recevez un message d'avertissement indiquant que l'éditeur de la connexion à distance est inconnu, choisissez Connect pour continuer.
6. Entrez le mot de passe que vous avez enregistré précédemment, puis cliquez sur OK.
7. En raison de la nature des certificat auto-signés, vous pouvez obtenir un avertissement indiquant que le certificat de sécurité ne peut pas être authentifié. Effectuez l'une des actions suivantes :
   - Si vous faites confiance au certificat, choisissez Oui pour vous connecter à votre instance.
   - [Windows] Avant de continuer, comparez l'empreinte numérique du certificat avec la valeur du journal système pour confirmer l'identité de l'ordinateur distant. Choisissez Afficher le certificat, puis sélectionnez Thumbprint dans l'onglet Détails. Comparez cette valeur à celle de `RDPCERTIFICATE-THUMBPRINT` la section Actions, Surveillance et résolution des problèmes, Obtenir le journal du système.
   - [Mac OS X] Avant de continuer, comparez l'empreinte digitale du certificat avec la valeur du journal système pour confirmer l'identité de l'ordinateur distant. Choisissez Afficher le certificat, développez les détails, puis choisissez SHA1Empreintes digitales. Comparez cette valeur à celle de `RDPCERTIFICATE-THUMBPRINT` la section Actions, Surveillance et résolution des problèmes, Obtenir le journal du système.
8. Si la RDP connexion est établie, le RDP client affiche l'écran de connexion Windows, puis le bureau Windows. Si vous recevez plutôt un message d'erreur, consultezthe section called "Le service Bureau à distance ne peut pas se connecter à l'ordinateur distant". Lorsque vous avez terminé la RDP connexion, vous pouvez fermer le RDP client.

Configuration des comptes utilisateurs

Après vous être connecté à votre instanceRDP, nous vous recommandons d'effectuer les tâches suivantes :

- Modifiez la valeur entrée par défaut pour le mot de passe administrateur. Il vous suffit de modifier le mot de passe lorsque vous êtes connecté à l'instance elle-même, comme avec n'importe quel autre Windows Server s'exécutant sur votre ordinateur.
- Créez un autre utilisateur avec des privilèges d'administrateur sur l'instance. Il s'agit d'une protection si vous oubliez le mot de passe administrateur ou si vous rencontrez un problème avec le compte administrateur. Le nouvel utilisateur doit avoir l'autorisation d'accéder à l'instance à distance. Ouvrez Propriétés en faisant un clic droit sur l'icône Ce PC dans votre bureau Windows ou en ouvrant l'explorateur de fichiers et en sélectionnant Propriétés. Choisissez Paramètres d'utilisation à distance, puis Sélectionnez des utilisateurs pour ajouter l'utilisateur au groupe Remote Desktop Users (Utilisateurs du bureau à distance).



Se connecter à une instance Windows à l'aide de Fleet Manager

Vous pouvez utiliser Fleet Manager, une fonctionnalité de AWS Systems Manager, pour vous connecter à des instances Windows à l'aide du protocole Remote Desktop (RDP) et afficher jusqu'à quatre instances Windows sur la même page dans le AWS Management Console. Vous pouvez

vous connecter à la première instance dans le Fleet Manager Remote Desktop directement depuis la page Instances de la EC2 console Amazon. Pour plus d'informations sur Fleet Manager, consultez la section Connexion à un nœud géré à l'aide de Remote Desktop dans le Guide de l'utilisateur AWS Systems Manager .

Il n'est pas nécessaire d'autoriser spécifiquement le RDP trafic entrant depuis votre adresse IP si vous utilisez Fleet Manager pour vous connecter. Fleet Manager s'en charge pour vous.

Prérequis

Avant de tenter de vous connecter à une instance à l'aide de Fleet Manager, vous devez configurer votre environnement. Pour plus d'informations, consultez la section Configuration de votre environnement dans le guide de AWS Systems Manager l'utilisateur.

Pour vous connecter à une instance Windows à l'aide de Fleet Manager

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation de gauche, choisissez Instances.
3. Sélectionnez l'instance, puis choisissez Connecter.
4. Dans l'onglet RDPclient, pour Type de connexion, choisissez Connect using Fleet Manager.
5. Choisissez Bureau à distance Fleet Manager. Cela ouvre la page Fleet Manager Remote Desktop (Bureau à distance Fleet Manager) dans la console AWS Systems Manager .
6. Entrez vos informations d'identification, puis choisissez Connect.
7. Si la RDP connexion est établie, Fleet Manager affiche le bureau Windows. Lorsque vous avez terminé la session, choisissez Actions, Terminer la session.

Pour plus d'informations, consultez la section Connexion à une instance gérée Windows Server à l'aide de Remote Desktop dans le Guide de AWS Systems Manager l'utilisateur.

Transférez des fichiers vers une instance Windows à l'aide de RDP

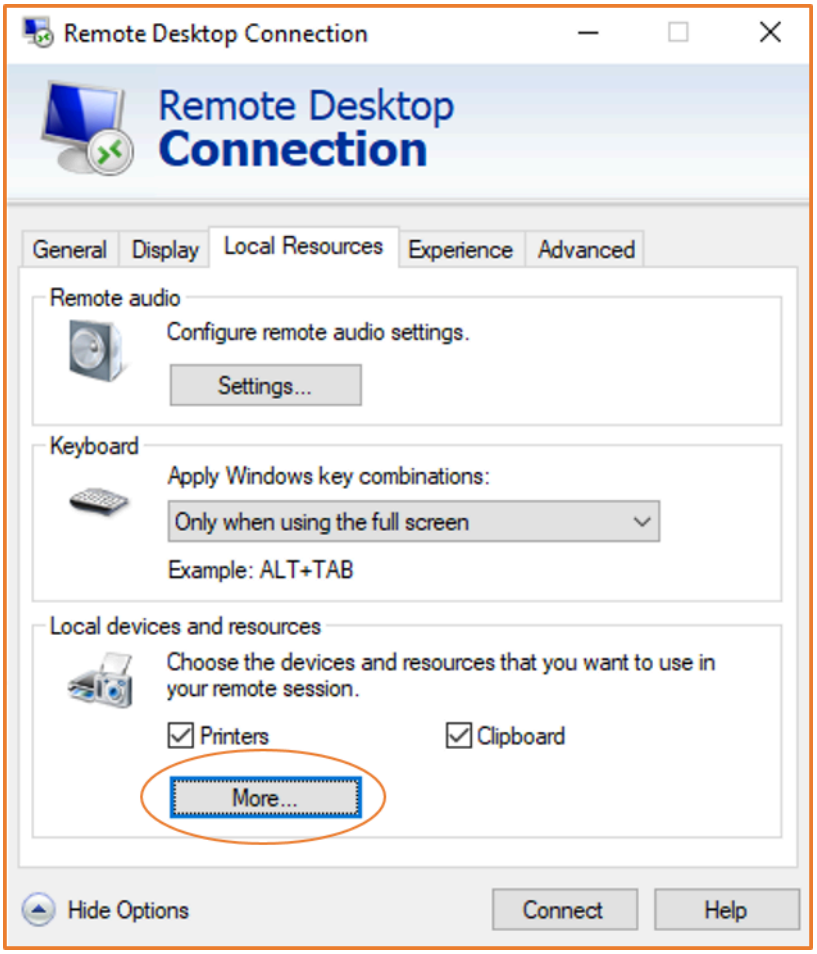
Votre instance Windows vous permet d'effectuer les mêmes opérations que n'importe quel serveur Windows. Par exemple, vous pouvez transférer des fichiers entre une instance Windows et votre ordinateur local à l'aide de la fonctionnalité de partage de fichiers local du logiciel Microsoft Remote Desktop Connection (RDP). Vous pouvez accéder aux fichiers locaux sur des disques durs, des DVD lecteurs, des lecteurs multimédias portables et des lecteurs réseau mappés.

Pour accéder à vos fichiers locaux à partir de vos instances Windows, vous devez activer la fonction de partage de fichiers locaux en mappant le lecteur de session à distance à votre lecteur local. Les étapes sont légèrement différentes selon que le système d’exploitation de votre ordinateur local est Windows ou macOS X.

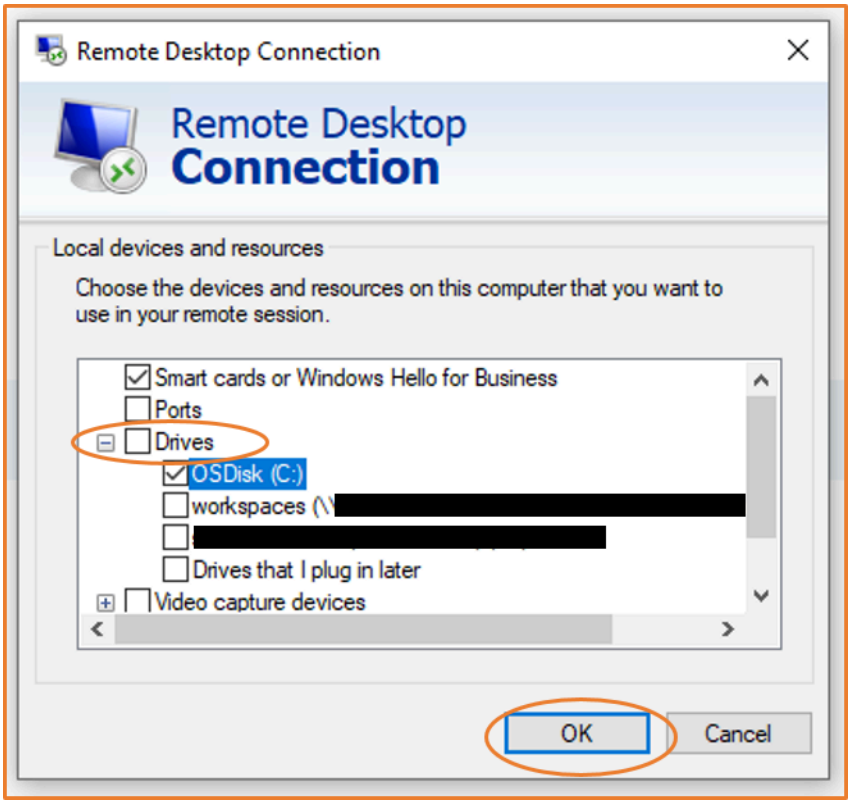
Windows

Pour mapper le lecteur de session à distance à votre lecteur local sur votre ordinateur Windows local

1. Ouvrez le client Connexion Bureau à distance.
2. Choisissez Show Options.
3. Ajoutez le nom d'hôte de l'instance dans le champ Ordinateur et le nom d'utilisateur dans le champ Nom d'utilisateur, comme suit :
   a. Sous Paramètres de connexion, choisissez Ouvrir... , puis accédez au fichier de RDP raccourci que vous avez téléchargé depuis la EC2 console Amazon. Le fichier contient le nom IPv4 DNS d'hôte public, qui identifie l'instance, et le nom d'utilisateur de l'administrateur.
   b. Sélectionnez le fichier, puis choisissez Open (Ouvrir). Les champs Ordinateur et Nom d'utilisateur sont remplis avec les valeurs du fichier de RDP raccourcis.
   c. Choisissez Save (Enregistrer).
4. Sélectionnez l’onglet Local Resources (Ressources locales).
5. Sous Local Devices and resources (Périphériques et ressources locaux), choisissez More... (Plus…).



6. Développez Lecteurs et sélectionnez le lecteur local auquel mapper l'instance Windows.
7. Choisissez OK.

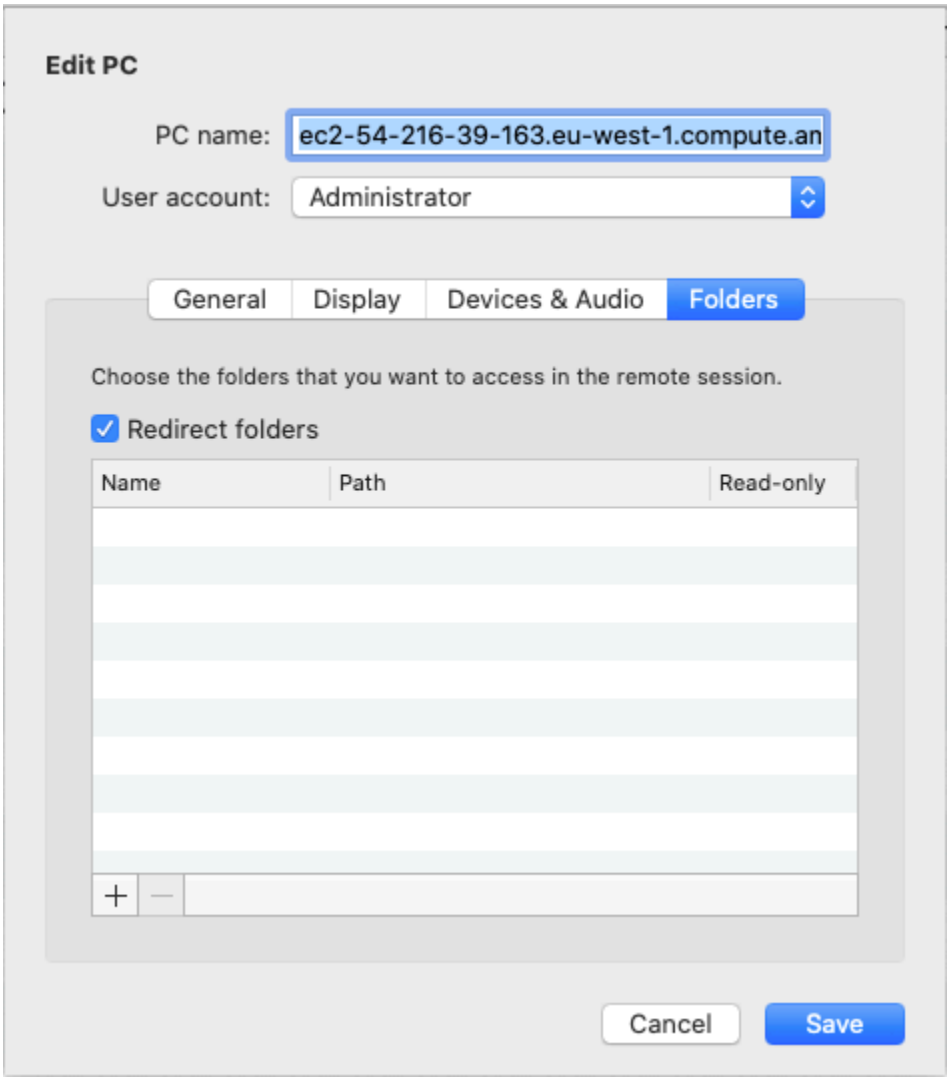


8. Choisissez Connect (Connexion) pour établir la connexion à votre instance Windows.

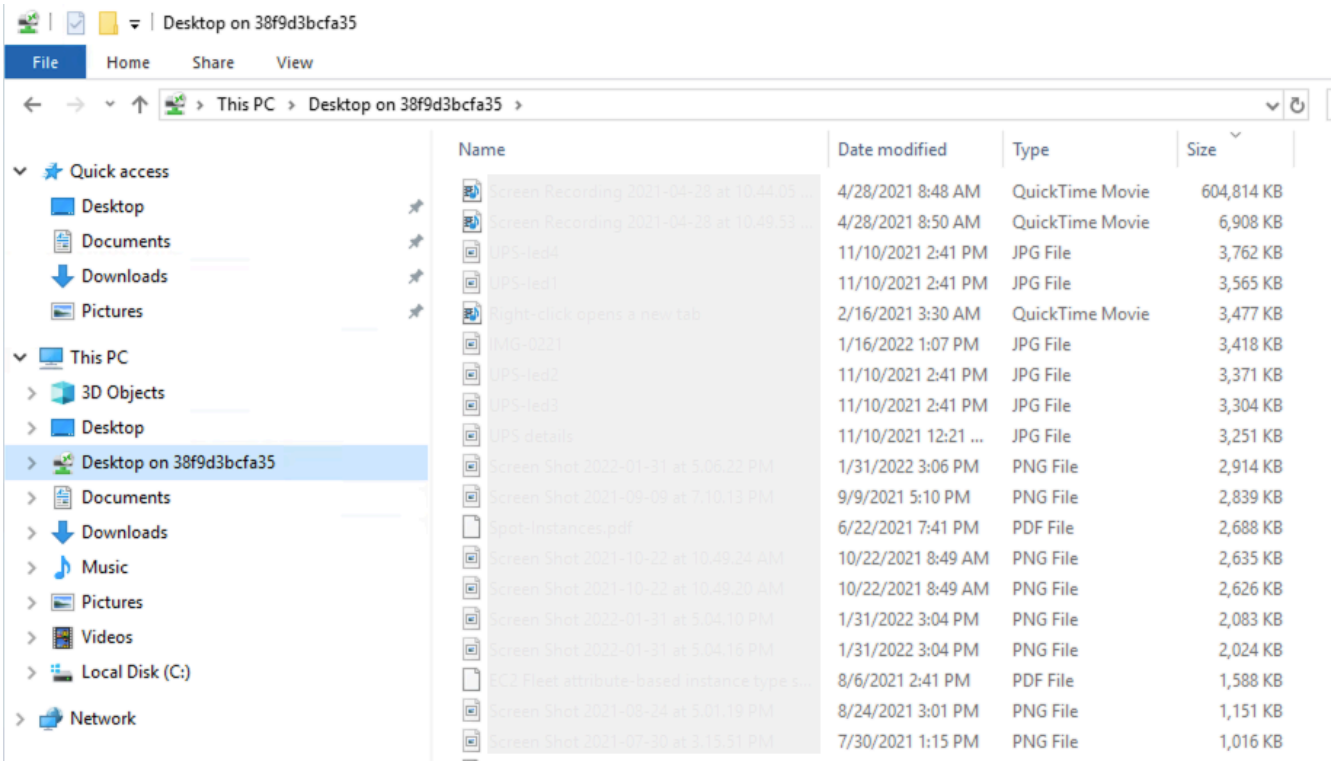
macOS X

Pour mapper le lecteur de session à distance à votre dossier local sur votre ordinateur macOS X local

1. Ouvrez le client Connexion Bureau à distance.
2. Accédez au RDP fichier que vous avez téléchargé depuis la EC2 console Amazon (lorsque vous vous êtes connecté initialement à l'instance) et faites-le glisser sur le client Remote Desktop Connection.
3. Cliquez avec le bouton droit sur RDP le fichier, puis sélectionnez Modifier.
4. Cliquez sur l'onglet Folders (Dossiers), puis cochez la case Redirect folders (Rediriger les dossiers).



5. Cliquez sur l'icône + en bas à gauche, accédez au dossier pour mapper, puis choisissez Open (Ouvrir). Répétez cette étape pour chaque dossier à mapper.
6. Choisissez Save (Enregistrer).
7. Choisissez Connect (Connexion) pour établir la connexion à votre instance Windows. Vous serez invité à saisir le mot de passe.
8. Sur l'instance, dans l'Explorateur de fichiers, développez This PC (Ce PC), et recherchez le dossier partagé à partir duquel vous pouvez accéder à vos fichiers locaux. Dans la capture d'écran suivante, le dossier Desktop (Bureau) sur l'ordinateur local a été mappé au lecteur de session à distance de l'instance.



Pour plus d'informations sur la mise à disposition de périphériques locaux pour une session à distance sur un ordinateur Mac, consultez Bien démarrer avec le client macOS.

Connectez-vous à votre EC2 instance Amazon à l'aide du gestionnaire de session

Le gestionnaire de session est une AWS Systems Manager fonctionnalité entièrement gérée permettant de gérer vos EC2 instances Amazon via un shell interactif basé sur un navigateur en un clic, ou via le. AWS CLI Vous pouvez utiliser le Gestionnaire de session pour démarrer une session avec une instance dans votre compte. Une fois la session démarrée, vous pouvez exécuter des commandes interactives sur l'instance comme vous le feriez pour tout autre type de connexion. Pour plus d'informations sur le Gestionnaire de session, consultez Gestionnaire de sessions AWS Systems Manager dans le Guide de l'utilisateur AWS Systems Manager .

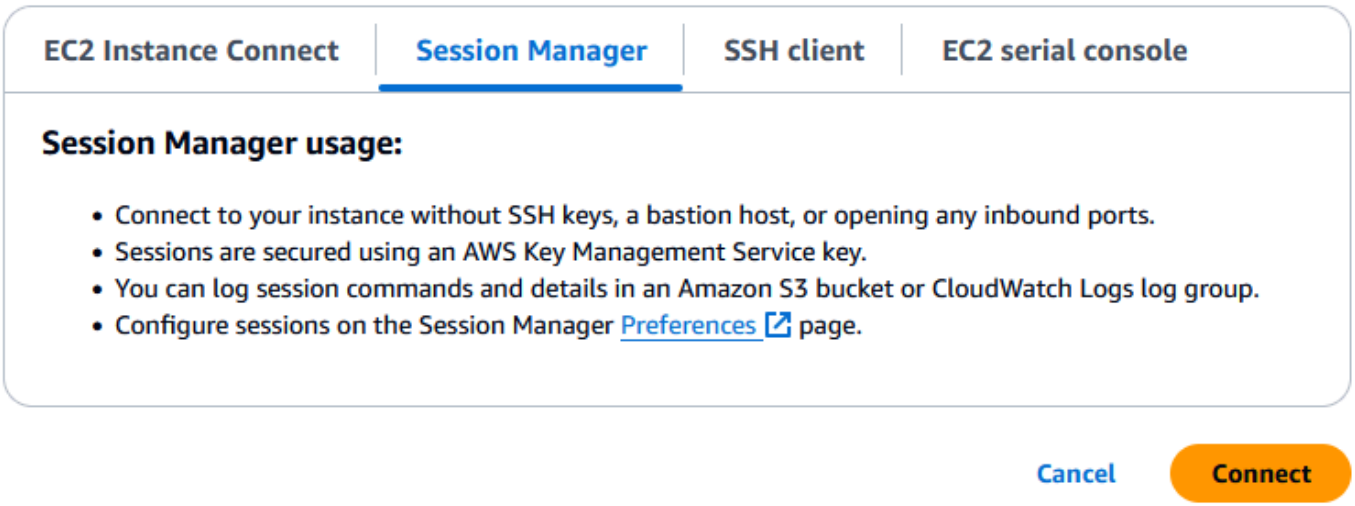
Prérequis

Avant de tenter de vous connecter à une instance à l'aide du Gestionnaire de session, vous devez effectuer les étapes de configuration requises. Par exemple, l'instance doit être gérée par SSM la

mazonSSMManaged InstanceCore politique A. Elle doit y être associée à un IAM rôle. Pour plus d'informations, consultez Configuration de Session Manager.

Pour vous connecter à une EC2 instance Amazon à l'aide du gestionnaire de session sur la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance, puis choisissez Connect (Connexion).
4. Pour la méthode de connexion, choisissez Session Manager.
5. Choisissez Connect pour démarrer la session.



Résolution des problèmes

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer une ou plusieurs actions de Systems Manager (`ssm:command-name`), vous devez mettre à jour vos politiques pour vous permettre de démarrer des sessions depuis la EC2 console Amazon. Pour plus d'informations et d'instructions, consultez la section IAMPolitiques par défaut de Quickstart pour le gestionnaire de session dans le guide de AWS Systems Manager l'utilisateur.

Connectez-vous à votre instance Linux à l'aide d'EC2Instance Connect

Amazon EC2 Instance Connect fournit un moyen sécurisé de se connecter à vos instances Linux via Secure Shell (SSH). Avec EC2 Instance Connect, vous utilisez des politiques et des principes AWS Identity and Access Management (IAM) pour contrôler l'SSHaccès à vos instances, éliminant

ainsi le besoin de partager et de gérer les SSH clés. Toutes les demandes de connexion utilisant EC2 Instance Connect sont enregistrées AWS CloudTrail afin que vous puissiez auditer les demandes de connexion.

Vous pouvez utiliser EC2 Instance Connect pour vous connecter à vos instances à l'aide de la EC2 console Amazon ou du SSH client de votre choix.

Lorsque vous vous connectez à une instance à l'aide d'EC2Instance Connect, Instance API Connect envoie une clé SSH publique aux métadonnées de l'instance, où elle reste pendant 60 secondes. Une IAM politique attachée à votre utilisateur autorise celui-ci à transmettre la clé publique aux métadonnées de l'instance. Le SSH démon utilise `AuthorizedKeysCommand` et`AuthorizedKeysCommandUser`, qui sont configurés lors de l'installation d'Instance Connect, pour rechercher la clé publique dans les métadonnées de l'instance à des fins d'authentification, et vous connecte à l'instance.

> **Tip**
>
> EC2Instance Connect est l'une des options permettant de se connecter à votre instance Linux. Pour d'autres options, veuillez consulter la rubrique Connectez-vous à votre instance Linux à l'aide de SSH. Pour vous connecter à une instance Windows, consultezConnectez-vous à votre instance Windows à l'aide de RDP.

Tarification

EC2Instance Connect est disponible sans frais supplémentaires.

Disponibilité dans les Régions

EC2Instance Connect est disponible dans tous les pays Régions AWS. Il n'est pas pris en charge dans les Zones Locales.

Table des matières

- Désinstallez EC2 Instance Connect

Pour consulter un article de blog expliquant comment améliorer la sécurité de vos hôtes bastion à l'aide d'EC2Instance Connect, consultez la section Sécurisation de vos hôtes bastion avec Amazon Instance EC2 Connect.

Tutoriel : complétez la configuration requise pour vous connecter à votre instance à l'aide d'EC2Instance Connect

Pour vous connecter à votre instance à l'aide d'EC2Instance Connect dans la EC2 console Amazon, vous devez d'abord effectuer la configuration préalable qui vous permettra de vous connecter correctement à votre instance. Le but de ce didacticiel est de vous guider à travers les tâches nécessaires à la réalisation de la configuration préalable.

Aperçu du didacticiel

Dans ce didacticiel, vous allez effectuer les quatre tâches suivantes :

- Tâche 1 : accorder les autorisations requises pour utiliser EC2 Instance Connect

  Vous allez d'abord créer une IAM politique contenant les IAM autorisations vous permettant d'envoyer une clé publique aux métadonnées de l'instance. Vous allez associer cette politique à votre IAM identité (utilisateur, groupe d'utilisateurs ou rôle) afin que votre IAM identité obtienne ces autorisations.
- Tâche 2 : Autoriser le trafic entrant du service EC2 Instance Connect vers votre instance

  Vous allez ensuite créer un groupe de sécurité qui autorise le trafic du service EC2 Instance Connect vers votre instance. Cela est nécessaire lorsque vous utilisez EC2 Instance Connect dans la EC2 console Amazon pour vous connecter à votre instance.
- Tâche 3 : Lancer votre instance

  Vous lancerez ensuite une EC2 instance à l'aide d'une AMI EC2 instance préinstallée avec Instance Connect et vous ajouterez le groupe de sécurité que vous avez créé à l'étape précédente.
- Tâche 4 : Se connecter à votre instance

  Enfin, vous utiliserez EC2 Instance Connect dans la EC2 console Amazon pour vous connecter à votre instance. Si vous pouvez vous connecter, vous pouvez être sûr que la configuration préalable que vous avez effectuée dans les tâches 1, 2 et 3 a été effectuée avec succès.

Tâche 1 : accorder les autorisations requises pour utiliser EC2 Instance Connect

Lorsque vous vous connectez à une instance à l'aide d'EC2Instance Connect, EC2 Instance API Connect envoie une clé SSH publique aux métadonnées de l'instance, où elle reste pendant 60 secondes. Vous avez besoin d'une IAM politique associée à votre IAM identité (utilisateur, groupe d'utilisateurs ou rôle) pour vous accorder l'autorisation requise pour transmettre la clé publique aux métadonnées de l'instance.

Objectif de la tâche

Vous allez créer la IAM politique qui autorise l'envoi de la clé publique à l'instance. L'action spécifique à autoriser est`ec2-instance-connect:SendSSHPublicKey`. Vous devez également autoriser l'`ec2:DescribeInstances`action afin de pouvoir afficher et sélectionner votre instance dans la EC2 console Amazon.

Après avoir créé la politique, vous l'associerez à votre IAM identité (utilisateur, groupe d'utilisateurs ou rôle) afin que votre IAM identité obtienne les autorisations.

Vous allez créer une politique configurée comme suit :

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeInstances",
            "Resource": "*"
        }
    ]
}
```

Important

La IAM politique créée dans ce didacticiel est très permissive ; elle vous permet de vous connecter à n'importe quelle instance en utilisant n'importe quel nom d'utilisateur. AMI Nous utilisons cette politique hautement permissive pour que le didacticiel reste simple et se concentre sur les configurations spécifiques enseignées dans ce didacticiel. Toutefois, dans

un environnement de production, nous recommandons que votre IAM politique soit configurée de manière à fournir des autorisations de moindre privilège. Pour des exemples IAM de politiques, voirAccorder IAM des autorisations pour EC2 Instance Connect.

Pour créer et associer une IAM politique vous permettant d'utiliser EC2 Instance Connect pour vous connecter à vos instances

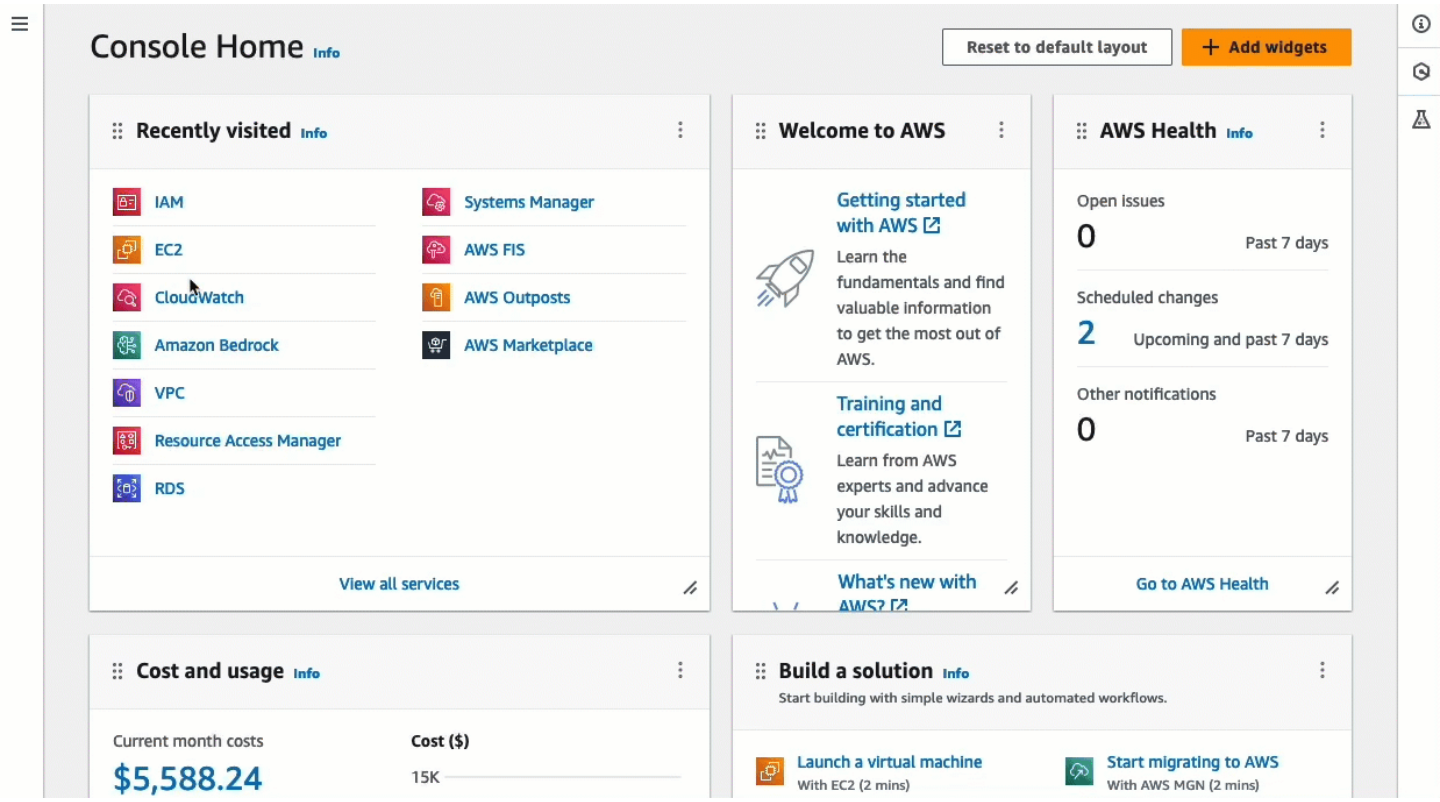
1. Créez d'abord la IAM politique
   a. Ouvrez la IAM console à l'adresse https://console.aws.amazon.com/iam/.
   b. Dans le panneau de navigation, choisissez Politiques.
   c. Sélectionnez Create policy (Créer une politique).
   d. Sur la page Spécifier l'autorisation, procédez comme suit :
      i. Pour Service, choisissez EC2Instance Connect.
      ii. Sous Actions autorisées, dans le champ de recherche, commencez **`send`** à taper pour afficher les actions pertinentes, puis sélectionnez S endSSHPublic Key.
      iii. Sous Ressources, sélectionnez Tout. Pour un environnement de production, nous vous recommandons de spécifier l'instance par son ARN nom, mais pour ce didacticiel, vous autorisez toutes les instances.
      iv. Choisissez Ajouter d'autres autorisations.
      v. Pour Service , choisissez EC2.
      vi. Sous Actions autorisées, dans le champ de recherche, commencez **`describein`** à taper pour afficher les actions pertinentes, puis sélectionnez DescribeInstances.
      vii. Choisissez Suivant.
   e. Sur la page Réviser et créer, procédez comme suit :
      i. Pour Policy name (Nom de la stratégie), attribuez un nom à cette stratégie.
      ii. Choisissez Create Policy (Créer une politique).
2. Attachez ensuite la politique à votre identité
   a. Dans le volet de navigation de la IAM console, sélectionnez Policies.
   b. Dans la liste des politiques, sélectionnez le bouton d'option à côté du nom de la politique que vous avez créée. Vous pouvez utiliser la zone de recherche pour filtrer la liste des politiques.

c. Sélectionnez Actions, puis Attach (Attacher).

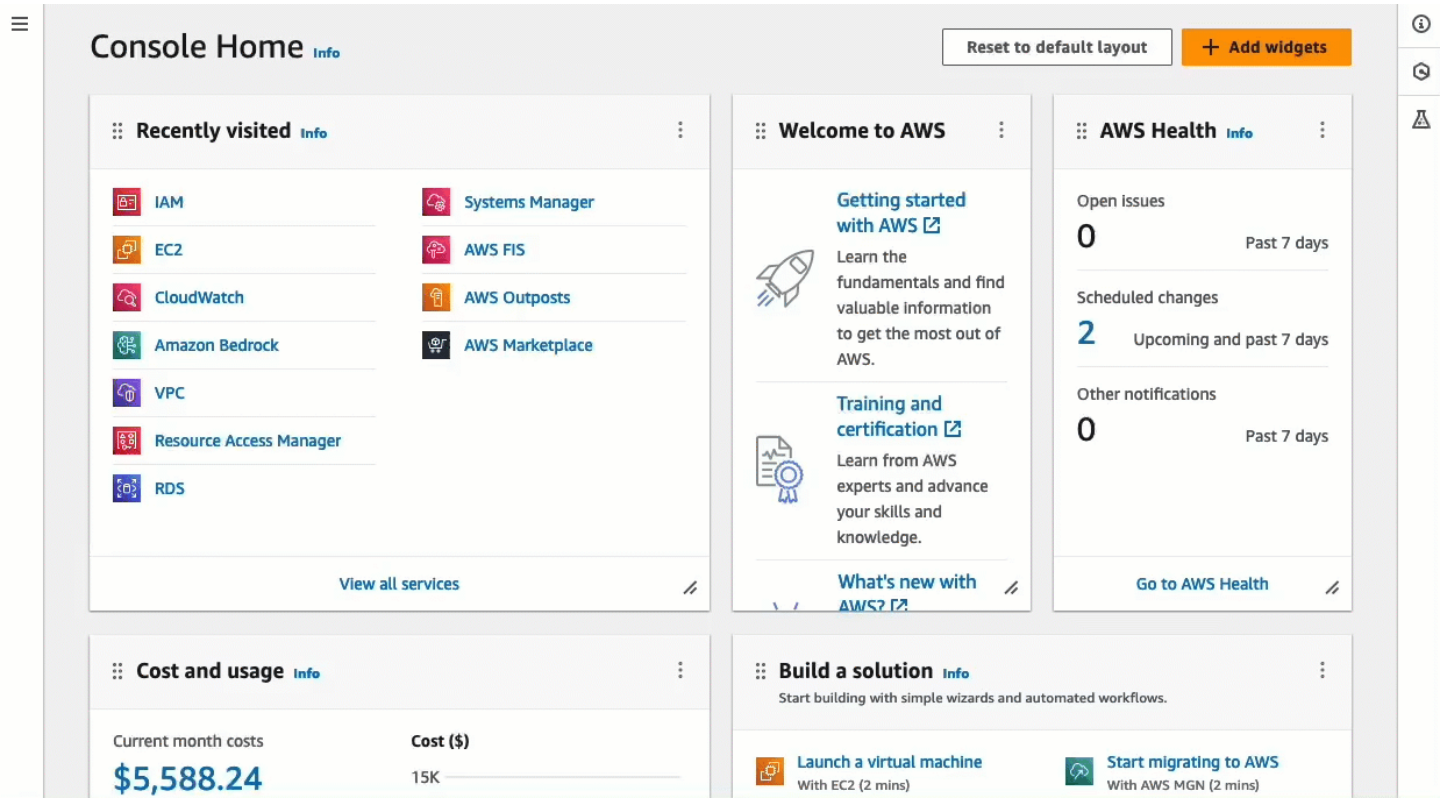
d. Sous IAMentités, cochez la case à côté de votre identité (utilisateur, groupe d'utilisateurs ou rôle). Vous pouvez utiliser le champ de recherche pour filtrer la liste des entités.

e. Choisissez Attach policy (Attacher une politique).

Afficher une animation : créer une IAM politique



Afficher une animation : joindre une IAM politique



Tâche 2 : Autoriser le trafic entrant du service EC2 Instance Connect vers votre instance

Lorsque vous utilisez EC2 Instance Connect dans la EC2 console Amazon pour vous connecter à une instance, le trafic qui doit être autorisé à atteindre l'instance est le trafic provenant du service EC2 Instance Connect. Cela est différent de la connexion de votre ordinateur local à une instance ; dans ce cas, vous devez autoriser le trafic entre votre ordinateur local et votre instance. Pour autoriser le trafic provenant du service EC2 Instance Connect, vous devez créer un groupe de sécurité qui autorise le SSH trafic entrant depuis la plage d'adresses IP du service EC2 Instance Connect.

Les plages d'adresses IP pour les AWS services sont disponibles sur https://ip-ranges.amazonaws.com/ip-ranges.json. Les plages d'adresses IP d'EC2Instance Connect sont identifiées par`"service": "EC2_INSTANCE_CONNECT"`.

Objectif de la tâche

Vous trouverez d'abord la plage d'adresses IP `EC2_INSTANCE_CONNECT` Région AWS dans laquelle se trouve votre instance. Vous allez ensuite créer un groupe de sécurité qui autorise le SSH trafic entrant sur le port 22 à partir de cette plage d'adresses IP.

Pour créer un groupe de sécurité qui autorise le trafic entrant du service EC2 Instance Connect vers votre instance

1. Obtenez d'abord la plage d'adresses IP pour le service EC2 Instance Connect

   a. Ouvrez le JSON fichier de plages d'adresses AWS IP dans https://ip-ranges.amazonaws.com/ip-ranges.json.

   b. Choisissez Raw Data.

   c. Trouvez la plage d'adresses IP correspondant `EC2_INSTANCE_CONNECT` à celle Région AWS dans laquelle se trouve votre instance. Vous pouvez utiliser le champ de recherche du navigateur pour rechercher le service `EC2_INSTANCE_CONNECT` et poursuivre votre recherche jusqu'à ce que vous trouviez la région dans laquelle se trouve votre instance.

      Par exemple, si votre instance est située dans la région USA Est (Virginie du Nord`us-east-1`) (), la plage d'adresses IP pour `EC2_INSTANCE_CONNECT` cette région est`18.206.107.24/29`.

      > **Note**
      >
      > Les plages d'adresses IP sont différentes pour chacune d'entre elles Région AWS.

   d. Copiez la plage d'adresses IP qui apparaît à côté de`ip_prefix`. Vous utiliserez cette plage d'adresses IP ultérieurement dans cette procédure.

   Pour plus d'informations sur le téléchargement du JSON fichier de plages d'adresses AWS IP et le filtrage par service, consultez la section Plages d'adresses AWS IP dans le guide de VPC l'utilisateur Amazon.

2. Créez ensuite le groupe de sécurité avec une règle entrante pour autoriser le trafic provenant de la plage d'adresses IP copiée

   a. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

   b. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité).

   c. Sélectionnez Create security group (Créer un groupe de sécurité).

   d. Sous Basic details (Détails de base), procédez comme suit :

      i. Dans Nom du groupe de sécurité, entrez un nom significatif pour votre groupe de sécurité.

ii. Dans Description, entrez une description significative pour votre groupe de sécurité.

e. Sous Règles de trafic entrant, procédez comme suit :

i. Choisissez Ajouter une règle.

ii. Pour Type, choisissez SSH.

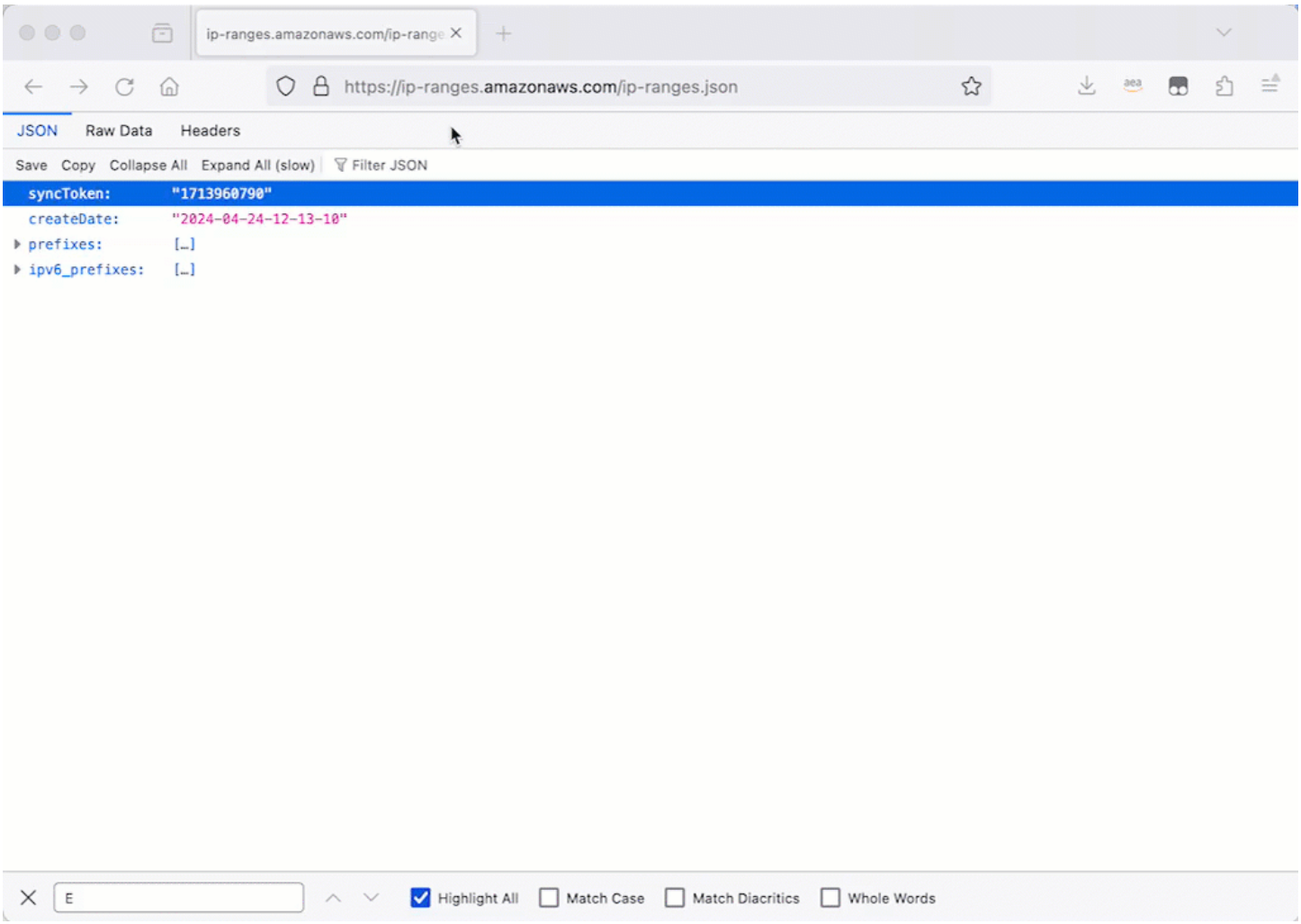
iii. Pour Source, laissez Personnalisé.

iv. Dans le champ situé à côté de Source, collez la plage d'adresses IP du service EC2 Instance Connect que vous avez copiée plus tôt dans cette procédure.

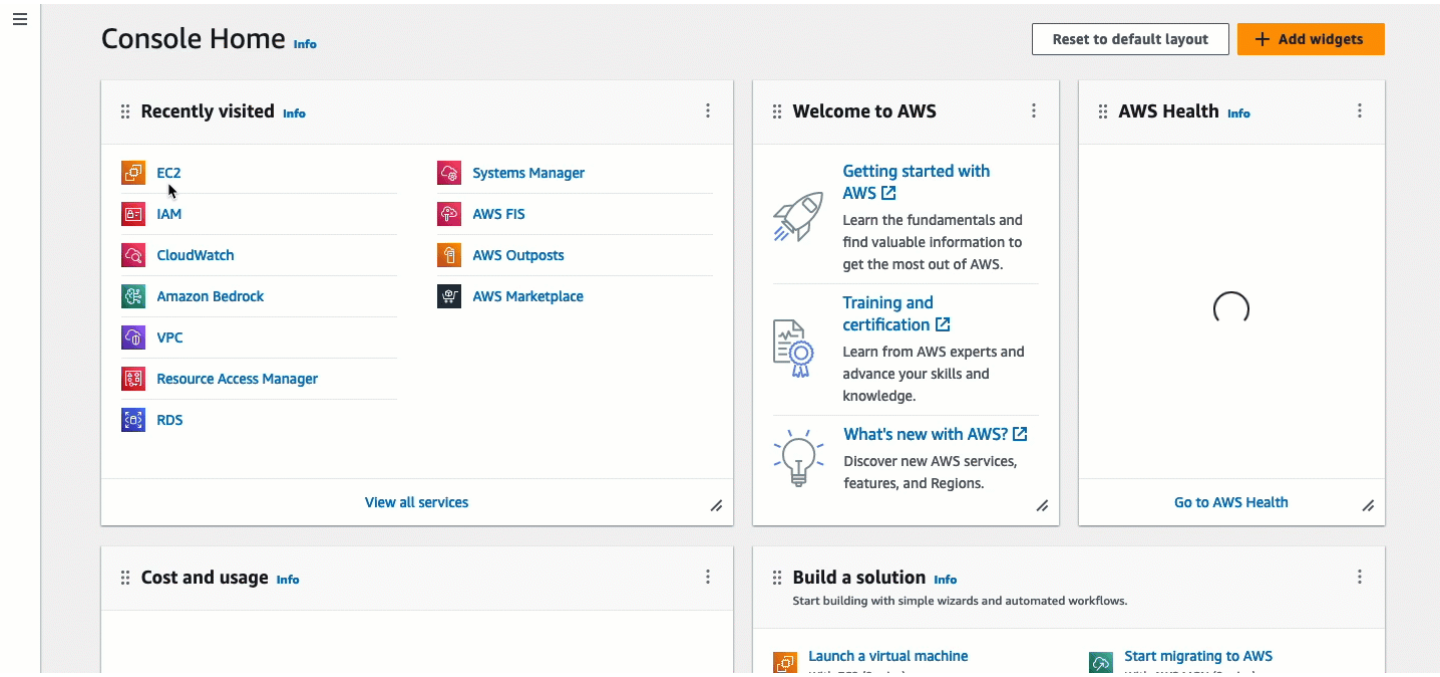
Par exemple, si votre instance est située dans la région USA Est (Virginie du Nord) (`us-east-1`), collez la plage d'adresses IP suivante dans le champ : `18.206.107.24/29`

f. Sélectionnez Create security group (Créer un groupe de sécurité).

Afficher une animation : obtenir la plage d'adresses IP pour EC2 Instance Connect pour une région spécifique



Afficher une animation : Configuration d'un groupe de sécurité



Tâche 3 : Lancer votre instance

Lorsque vous lancez une instance, vous devez en spécifier une AMI contenant les informations requises pour lancer l'instance. Vous pouvez choisir de lancer une instance avec ou sans EC2 Instance Connect préinstallé. Dans cette tâche, nous indiquons un AMI préinstallé avec EC2 Instance Connect.

Si vous lancez votre EC2 instance sans Instance Connect préinstallé et que vous souhaitez utiliser EC2 Instance Connect pour vous connecter à votre instance, vous devrez effectuer des étapes de configuration supplémentaires. Ces étapes n'entrent pas dans le cadre de ce didacticiel.

Objectif de la tâche

Vous allez lancer une instance avec Amazon Linux 2023AMI, qui est préinstallé avec EC2 Instance Connect. Vous allez également spécifier le groupe de sécurité que vous avez créé précédemment afin de pouvoir utiliser EC2 Instance Connect dans la EC2 console Amazon pour vous connecter à votre instance. Comme vous utiliserez EC2 Instance Connect pour vous connecter à votre instance, ce qui envoie une clé publique aux métadonnées de votre instance, vous n'aurez pas besoin de spécifier de SSH clé lorsque vous lancerez votre instance.

Pour lancer une instance qui peut utiliser EC2 Instance Connect dans la EC2 console Amazon pour la connexion

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation en haut de l'écran, la AWS région actuelle est affichée (par exemple, l'Irlande). Sélectionnez la région dans laquelle vous souhaitez lancer votre instance. Ce choix est important car vous avez créé un groupe de sécurité qui autorise le trafic pour une région spécifique. Vous devez donc sélectionner la même région dans laquelle lancer votre instance.
3. Dans le tableau de bord de EC2 la console Amazon, choisissez Launch instance.
4. (Facultatif) Sous Name and tags (Noms et identifications), pour Name (Nom), saisissez un nom descriptif pour votre instance.
5. Sous Images de l'application et du système d'exploitation (Amazon Machine Image), choisissez Quick Start. Amazon Linux est sélectionné par défaut. Sous Amazon Machine Image (AMI), Amazon Linux 2023 AMI est sélectionné par défaut. Conservez la sélection par défaut pour cette tâche.
6. Sous Type d'instance, pour Type d'instance, conservez la sélection par défaut ou choisissez un autre type d'instance.
7. Sous Paire de clés (connexion), pour Nom de la paire de clés, choisissez Procéder sans paire de clés (Non recommandé). Lorsque vous utilisez EC2 Instance Connect pour vous connecter à une EC2 instance, Instance Connect envoie une paire de clés aux métadonnées de l'instance, et c'est cette paire de clés qui est utilisée pour la connexion.
8. Sous Network settings (Paramètres réseau), effectuez les opérations suivantes :

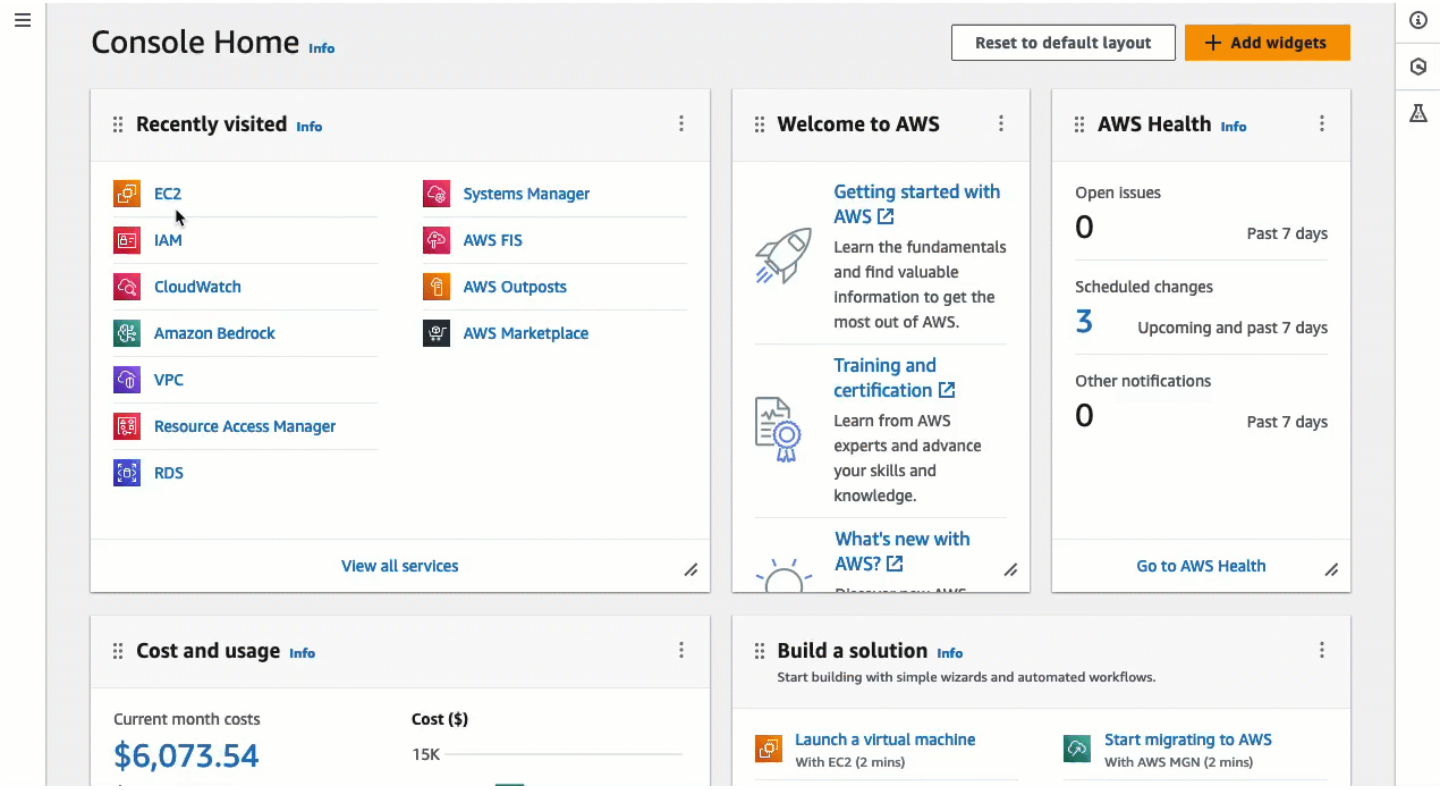
   a. Pour Attribuer automatiquement une adresse IP publique, laissez Activer.

   > **Note**
   >
   > Pour utiliser EC2 Instance Connect dans la EC2 console Amazon afin de se connecter à une instance, celle-ci doit avoir une IPv4 adresse publique.

   b. Pour Pare-feu (groupes de sécurité), choisissez Sélectionner un groupe de sécurité existant.

   c. Sous Groupes de sécurité communs, choisissez le groupe de sécurité que vous avez créé précédemment.
9. Dans le panneau Summary (Récapitulatif), sélectionnez Launch instance (Lancer l'instance).

Afficher une animation : lancez votre instance



Tâche 4 : Se connecter à votre instance

Lorsque vous vous connectez à une instance à l'aide d'EC2Instance Connect, EC2 Instance API Connect envoie une clé SSH publique aux métadonnées de l'instance, où elle reste pendant 60 secondes. Le SSH démon utilise `AuthorizedKeysCommand` et `AuthorizedKeysCommandUser` pour rechercher la clé publique dans les métadonnées de l'instance à des fins d'authentification, puis vous connecte à l'instance.

Objectif de la tâche

Dans cette tâche, vous allez vous connecter à votre instance à l'aide d'EC2Instance Connect dans la EC2 console Amazon. Si vous avez effectué les tâches 1, 2 et 3 requises, la connexion devrait réussir.

Étapes pour vous connecter à votre instance

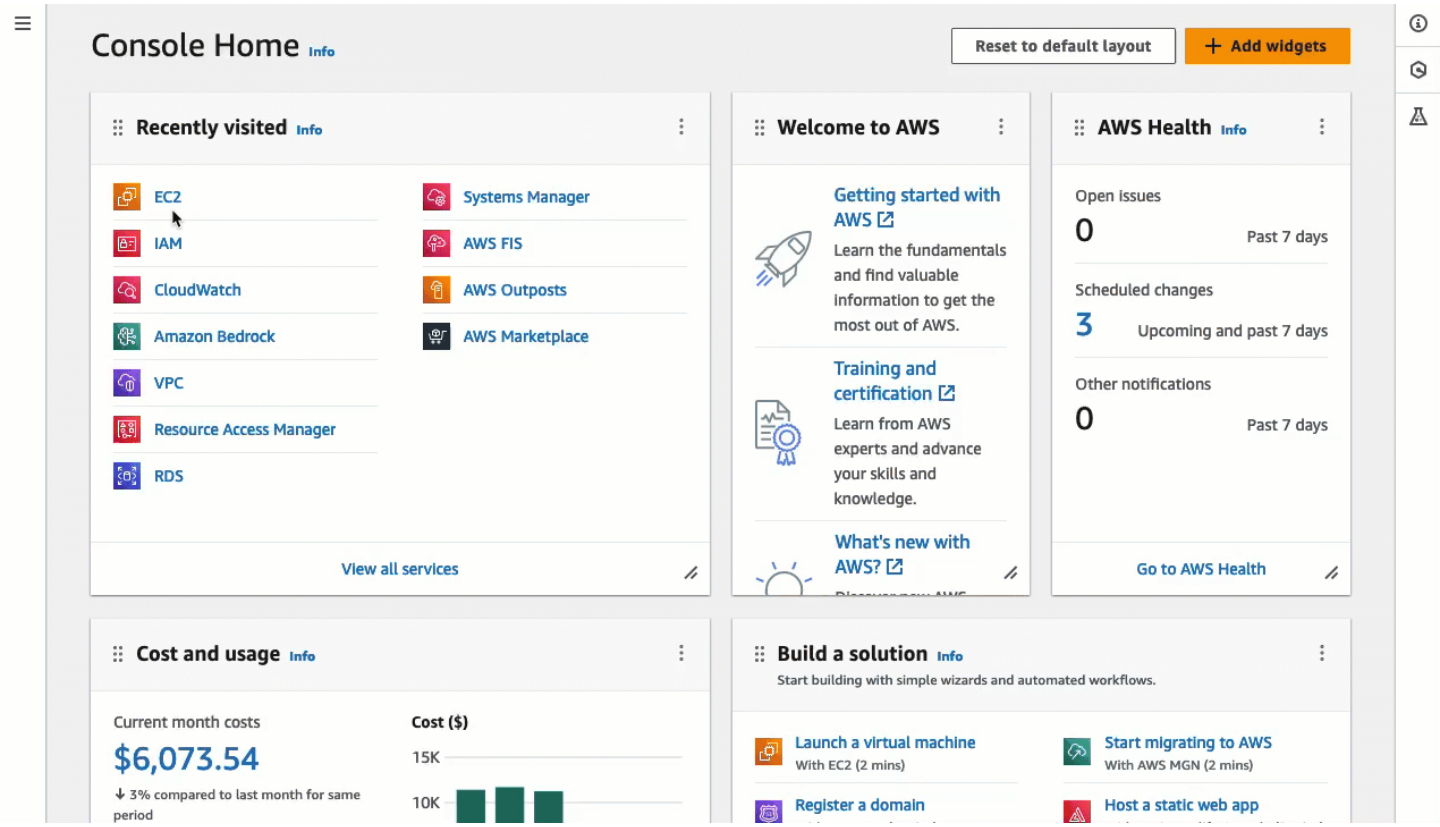
Suivez les étapes ci-dessous pour vous connecter à votre instance. Pour visionner une animation des étapes, voirAfficher une animation : Connectez-vous à votre instance.

Pour connecter une instance à l'aide d'EC2Instance Connect dans la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation en haut de l'écran, la AWS région actuelle est affichée (par exemple, l'Irlande). Sélectionnez la région dans laquelle se trouve votre instance.
3. Dans le panneau de navigation, choisissez Instances.
4. Sélectionnez votre instance, puis choisissez Connect.
5. Choisissez l'onglet EC2Instance Connect.
6. Pour le type de connexion, choisissez Connect using EC2 Instance Connect.
7. Choisissez Se connecter.

   Une fenêtre de terminal s'ouvre dans le navigateur et vous êtes connecté à votre instance.

Afficher une animation : Connectez-vous à votre instance



Conditions requises pour EC2 Instance Connect

Les conditions préalables à l'installation et à l'utilisation d'EC2Instance Connect sont les suivantes :

- Installez EC2 Instance Connect
- Garantir la connectivité réseau
- Autoriser le trafic entrant SSH
- Accorder des autorisations
- Installation d'un SSH client sur votre ordinateur local
- Répondre aux exigences en matière de nom

Installez EC2 Instance Connect

Pour utiliser EC2 Instance Connect pour se connecter à une instance, Instance Connect doit être installée sur l'EC2instance. Vous pouvez soit lancer l'instance à l'aide AMI d'une EC2 instance préinstallée avec Instance Connect, soit installer EC2 Instance Connect sur des instances lancées avec supportAMIs. Pour de plus amples informations, veuillez consulter Installez EC2 Instance Connect sur vos EC2 instances.

Garantir la connectivité réseau

Les instances peuvent être configurées pour permettre aux utilisateurs de se connecter à votre instance via Internet ou via l'adresse IP privée de l'instance. En fonction de la manière dont vos utilisateurs se connecteront à votre instance à l'aide d'EC2Instance Connect, vous devez configurer l'accès réseau suivant :

- Si vos utilisateurs se connecteront à votre instance via internet, votre instance doit alors avoir une adresse IP publique et se trouver dans un sous-réseau public. Pour plus d'informations, consultez Activer l'accès à Internet dans le guide de VPC l'utilisateur Amazon.
- Si vos utilisateurs se connectent à votre instance via l'adresse IP privée de l'instance, vous devez établir une connectivité réseau privée avec la vôtreVPC, par exemple en utilisant AWS Direct Connect ou en VPC peering, afin que vos utilisateurs puissent accéder à l'adresse IP privée de l'instance. AWS Site-to-Site VPN

Si votre instance ne possède pas d'IPv4adresse publique et que vous préférez ne pas configurer l'accès au réseau comme décrit ci-dessus, vous pouvez envisager EC2 Instance Connect Endpoint comme alternative à EC2 Instance Connect. Avec EC2 Instance Connect Endpoint, vous pouvez vous connecter à une instance en utilisant SSH ou RDP même si l'instance ne possède pas d'IPv4adresse publique. Pour de plus amples informations, veuillez consulter Connectez-vous à votre instance Linux à l'aide de la EC2 console Amazon.

Autoriser le trafic entrant SSH

Assurez-vous que le groupe de sécurité associé à votre instance autorise le SSH trafic entrant sur le port 22 en provenance de votre adresse IP ou de votre réseau. Le groupe de sécurité par défaut pour le VPC n'autorise pas le SSH trafic entrant par défaut. Le groupe de sécurité créé par l'assistant de lancement d'instance autorise SSH le trafic entrant par défaut. Pour de plus amples informations, veuillez consulter Règles pour la connexion à des instances à partir de votre ordinateur.

EC2Instance Connect utilise des plages d'adresses IP spécifiques pour les SSH connexions basées sur un navigateur à votre instance (lorsque les utilisateurs utilisent la EC2 console Amazon pour se connecter à une instance). Si vos utilisateurs doivent utiliser la EC2 console Amazon pour se connecter à une instance, assurez-vous que le groupe de sécurité associé à votre instance autorise le SSH trafic entrant depuis la plage d'adresses IP pour`EC2_INSTANCE_CONNECT`. Pour identifier la plage d'adresses, téléchargez le JSON fichier fourni par AWS et filtrez le sous-ensemble pour EC2 Instance Connect, en utilisant `EC2_INSTANCE_CONNECT` comme valeur de service. Ces plages d'adresses IP diffèrent entre les deux Régions AWS. Pour plus d'informations sur le téléchargement du JSON fichier et le filtrage par service, consultez les plages d'adresses AWS IP dans le guide de VPC l'utilisateur Amazon.

Accorder des autorisations

Vous devez accorder les autorisations requises à chaque IAM utilisateur qui utilisera EC2 Instance Connect pour se connecter à une instance. Pour de plus amples informations, veuillez consulter Accorder IAM des autorisations pour EC2 Instance Connect.

Installation d'un SSH client sur votre ordinateur local

Si vos utilisateurs veulent se connecter en utilisantSSH, ils doivent s'assurer que leur ordinateur local possède un SSH client.

Un SSH client est probablement installé par défaut sur l'ordinateur local d'un utilisateur. Ils peuvent vérifier la présence d'un SSH client en tapant ssh sur la ligne de commande. Si leur ordinateur local ne reconnaît pas la commande, ils peuvent installer un SSH client. Pour plus d'informations sur l'installation d'un SSH client sous Linux ou macOS X, consultez http://www.openssh.com. Pour plus d'informations sur l'installation d'un SSH client sous Windows 10, voir Ouvrir SSH sous Windows.

Il n'est pas nécessaire d'installer un SSH client sur un ordinateur local si vos utilisateurs utilisent uniquement la EC2 console Amazon pour se connecter à une instance.

Répondre aux exigences en matière de nom

Lorsque vous utilisez EC2 Instance Connect pour vous connecter à une instance, le nom d'utilisateur doit répondre aux exigences suivantes :

- Premier caractère : doit être une lettre (`A-Z`,`a-z`), un chiffre (`0-9`) ou un trait de soulignement (`_`)
- Caractères suivants : il peut s'agir de lettres (`A-Z`, `a-z`), de chiffres (`0-9`) ou des caractères suivants : `@ . _ -`
- Longueur minimale : 1 caractère
- Longueur maximale : 31 caractères

Accorder IAM des autorisations pour EC2 Instance Connect

Pour vous connecter à une instance à l'aide d'EC2Instance Connect, vous devez créer une IAM politique qui accorde à vos utilisateurs des autorisations pour les actions et conditions suivantes :

- Action `ec2-instance-connect:SendSSHPublicKey` – Accorde l'autorisation d'envoyer la clé publique en mode push à une instance.
- Condition `ec2:osuser` – Spécifie le nom de l'utilisateur du système d'exploitation qui peut envoyer la clé publique en mode push à une instance. Utilisez le nom d'utilisateur par défaut pour celui AMI que vous avez utilisé pour lancer l'instance. Le nom d'utilisateur par défaut pour AL2 023 et Amazon Linux 2 est`ec2-user`, et pour Ubuntu, c'`ubuntu`est le cas.
- `ec2:DescribeInstances`action — Obligatoire lors de l'utilisation de la EC2 console car le wrapper appelle cette action. Les utilisateurs peuvent déjà disposer de l'autorisation d'appeler cette action à partir d'une autre politique.

Envisagez de restreindre l'accès à des EC2 instances spécifiques. Dans le cas contraire, tous IAM les principaux autorisés à effectuer l'`ec2-instance-connect:SendSSHPublicKey`action peuvent se connecter à toutes les EC2 instances. Vous pouvez restreindre l'accès en spécifiant une ressource ARNs ou en utilisant des balises de ressource comme clés de condition.

Pour plus d'informations, consultez Actions, ressources et clés de condition pour Amazon EC2 Instance Connect.

Pour plus d'informations sur la création de IAM politiques, voir Création de IAM politiques dans le Guide de IAM l'utilisateur.

Autoriser les utilisateurs à se connecter à des instances spécifiques

La IAM politique suivante autorise la connexion à des instances spécifiques, identifiées par leur ressourceARNs.

Dans l'exemple de IAM politique suivant, les actions et conditions suivantes sont spécifiées :

- L'`ec2-instance-connect:SendSSHPublicKey`action autorise les utilisateurs à se connecter à deux instances, spécifiées par la ressourceARNs. Pour autoriser les utilisateurs à se connecter à toutes les EC2 instances, remplacez la ressource ARNs par le `*` caractère générique.
- La `ec2:osuser` condition accorde l'autorisation de se connecter aux instances uniquement si *`ami-username`* est spécifié lors de la connexion.
- L'action `ec2:DescribeInstances` est spécifiée pour accorder l'autorisation aux utilisateurs qui utiliseront la console pour se connecter à vos instances. Si vos utilisateurs n'utilisent un SSH client que pour se connecter à vos instances, vous pouvez l'omettre`ec2:DescribeInstances`. Notez que les `ec2:Describe*` API actions ne prennent pas en charge les autorisations au niveau des ressources. Par conséquent, le caractère générique `*` est nécessaire dans l'élément `Resource`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": [
                "arn:aws:ec2:region:account-id:instance/i-1234567890abcdef0",
                "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeInstances",
            "Resource": "*"
        }
    ]
```

```
}
```

Autoriser les utilisateurs à se connecter à des instances avec des balises spécifiques

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction de balises pouvant être associées aux utilisateurs et AWS aux ressources. Vous pouvez utiliser des balises de ressources pour contrôler l'accès à une instance. Pour plus d'informations sur l'utilisation de balises pour contrôler l'accès à vos AWS ressources, consultez la section Contrôle de l'accès aux AWS ressources dans le Guide de IAM l'utilisateur.

Dans l'exemple de IAM politique suivant, l'`ec2-instance-connect:SendSSHPublicKey`action autorise les utilisateurs à se connecter à n'importe quelle instance (indiquée par le * caractère générique dans la ressourceARN) à condition que l'instance possède une balise de ressource avec key= `tag-key` et value=. `tag-value`

L'action `ec2:DescribeInstances` est spécifiée pour accorder l'autorisation aux utilisateurs qui utiliseront la console pour se connecter à vos instances. Si vos utilisateurs n'utilisent qu'un SSH client pour se connecter à vos instances, vous pouvez l'omettre`ec2:DescribeInstances`. Notez que les `ec2:Describe*` API actions ne prennent pas en charge les autorisations au niveau des ressources. Par conséquent, le caractère générique * est nécessaire dans l'élément `Resource`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "arn:aws:ec2:region:account-id:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/tag-key": "tag-value"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeInstances",
            "Resource": "*"
        }
    ]
}
```

Installez EC2 Instance Connect sur vos EC2 instances

Pour se connecter à une instance Linux à l'aide d'EC2Instance Connect, Instance Connect doit être installée sur l'EC2instance. L'installation d'EC2Instance Connect configure le SSH daemon sur l'instance.

Pour plus d'informations sur le package EC2 Instance Connect, consultez aws/aws-ec2 - sur le site Web. instance-connect-config GitHub

> **Note**
>
> Si vous avez configuré les `AuthorizedKeysCommandUser` paramètres `AuthorizedKeysCommand` et pour SSH l'authentification, l'installation d'EC2Instance Connect ne les mettra pas à jour. Par conséquent, vous ne pouvez pas utiliser EC2 Instance Connect.

Installer les prérequis

Avant d'installer EC2 Instance Connect, assurez-vous de respecter les conditions préalables suivantes.

- Vérifiez que l'instance utilise l'un des éléments suivants :
  - Amazon Linux 2 avant la version 2.0.20190618
  - AL2023 minimal AMI ou optimisé pour Amazon ECS AMI
  - CentOS Stream 8 et 9
  - macOS Sonoma avant 14.2.1, Ventura avant 13.6.3 et Monterey avant 12.7.2
  - Red Hat Enterprise Linux (RHEL) 8 et 9
  - Ubuntu 16.04 et 18.04

  > **Tip**
  >
  > Si vous avez lancé votre instance à l'aide d'une version ultérieure d'Amazon Linux, de macOS Sonoma, Ventura ou Monterey, ou d'Ubuntu, Instance EC2 Connect est préinstallée. Vous n'avez donc pas besoin de l'installer vous-même.

- Vérifiez les conditions générales requises pour EC2 Instance Connect.

Pour de plus amples informations, veuillez consulter Conditions requises pour EC2 Instance Connect.

- Vérifiez les conditions requises pour vous connecter à votre instance à l'aide d'un SSH client sur votre machine locale.

  Pour de plus amples informations, veuillez consulter Connectez-vous à votre instance Linux à l'aide de SSH.

- Obtenez l'ID de l'instance.

  Vous pouvez obtenir l'ID de votre instance à l'aide de la EC2 console Amazon (dans la colonne Instance ID). Si vous préférez, vous pouvez utiliser la commande describe-instances (AWS CLI) ou Get-EC2Instance(AWS Tools for Windows PowerShell).

Installation manuelle d'EC2Instance Connect

> **Note**
>
> Si vous avez lancé votre instance à l'aide de l'une des AMIs méthodes suivantes, EC2 Instance Connect est préinstallé et vous pouvez ignorer cette procédure :
>
> - AL2023 normale AMI
> - Amazon Linux 2 2.0.20190618 ou version ultérieure
> - macOS Sonoma 14.2.1 ou version ultérieure
> - macOS Ventura 13.6.3 ou version ultérieure
> - macOS Monterey 12.7.2 ou version ultérieure
> - Ubuntu 20.04 ou version ultérieure

Utilisez l'une des procédures suivantes pour installer EC2 Instance Connect, en fonction du système d'exploitation de votre instance.

Amazon Linux 2

Pour installer EC2 Instance Connect sur une instance lancée avec Amazon Linux 2

1. Connectez-vous à votre instance à l'aide deSSH.

Remplacez les valeurs de l'exemple dans la commande suivante par vos propres valeurs. Utilisez la paire de SSH clés attribuée à votre instance lorsque vous l'avez lancée et le nom d'utilisateur par défaut AMI que vous avez utilisé pour lancer votre instance. Pour Amazon Linux 2, le nom d'utilisateur par défaut est`ec2-user`.

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Pour plus d'informations sur la connexion à votre instance, consultez Connectez-vous à votre instance Linux à l'aide d'un SSH client.

2. Installez le package EC2 Instance Connect sur votre instance.

```
[ec2-user ~]$ sudo yum install ec2-instance-connect
```

Trois nouveaux scripts doivent apparaître dans le dossier `/opt/aws/bin/` :

```
eic_curl_authorized_keys
eic_parse_authorized_keys
eic_run_authorized_keys
```

3. (Facultatif) Vérifiez qu'EC2Instance Connect a été correctement installé sur votre instance.

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config
```

EC2Instance Connect a été correctement installée si les `AuthorizedKeysCommandUser` lignes `AuthorizedKeysCommand` et contiennent les valeurs suivantes :

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` définit le script `eic_run_authorized_keys` pour rechercher les clés à partir des métadonnées de l'instance.
- `AuthorizedKeysCommandUser` définit l'utilisateur système comme `ec2-instance-connect`.

> **Note**
>
> Si vous avez déjà configuré `AuthorizedKeysCommand` et`AuthorizedKeysCommandUser`, l'installation d'EC2Instance Connect ne modifiera pas les valeurs et vous ne pourrez pas utiliser EC2 Instance Connect.

CentOS

Pour installer EC2 Instance Connect sur une instance lancée avec CentOS

1. Connectez-vous à votre instance à l'aide deSSH.

   Remplacez les valeurs de l'exemple dans la commande suivante par vos propres valeurs. Utilisez la paire de SSH clés attribuée à votre instance lorsque vous l'avez lancée et le nom d'utilisateur par défaut AMI que vous avez utilisé pour lancer votre instance. Pour CentOS, le nom d'utilisateur par défaut est `centos` ou. `ec2-user`

   ```
   $ ssh -i my_ec2_private_key.pem centos@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Pour plus d'informations sur la connexion à votre instance, consultez Connectez-vous à votre instance Linux à l'aide d'un SSH client.

2. Si vous utilisez un HTTPS proxy HTTP ou, vous devez définir les variables d'`https_proxy`environnement `http_proxy` or dans la session shell en cours.

   Si vous n'utilisez pas de proxy, vous pouvez ignorer cette étape.

   - Pour un serveur HTTP proxy, exécutez les commandes suivantes :

     ```
     $ export http_proxy=http://hostname:port
     $ export https_proxy=http://hostname:port
     ```

   - Pour un serveur HTTPS proxy, exécutez les commandes suivantes :

     ```
     $ export http_proxy=https://hostname:port
     $ export https_proxy=https://hostname:port
     ```

3. Installez le package EC2 Instance Connect sur votre instance en exécutant les commandes suivantes.

   Les fichiers de configuration EC2 Instance Connect pour CentOS sont fournis dans un package Red Hat Package Manager (RPM), avec différents RPM packages pour CentOS 8 et CentOS 9 et pour les types d'instances qui s'exécutent sur Intel/ AMD (x86_64) ou (). ARM AArch64

   Utilisez le bloc de commandes correspondant à votre système d'exploitation et à votre CPU architecture.

   - CentOS 8

     Intel/ AMD (x86_64)

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rhel8.rpm -o /
     tmp/ec2-instance-connect/ec2-instance-connect.rpm
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
     selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
     selinux.rpm
     [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
     connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
     ```

     ARM (AArch64)

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rhel8.rpm -o /
     tmp/ec2-instance-connect/ec2-instance-connect.rpm
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
     selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
     selinux.rpm
     [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
     connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
     ```

   - CentOS 9

     Intel/ AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rpm -o /tmp/ec2-
instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rpm -o /tmp/ec2-
instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

Vous devriez voir ce nouveau script dans le dossier `/opt/aws/bin/` :

```
eic_run_authorized_keys
```

4. (Facultatif) Vérifiez qu'EC2Instance Connect a été correctement installé sur votre instance.

   - Pour CentOS 8 :

     ```
     [ec2-user ~]$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-
     connect.conf
     ```

   - Pour CentOS 9 :

     ```
     [ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
     ```

EC2Instance Connect a été correctement installée si les `AuthorizedKeysCommandUser` lignes `AuthorizedKeysCommand` et contiennent les valeurs suivantes :

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` définit le script `eic_run_authorized_keys` pour rechercher les clés à partir des métadonnées de l'instance.
- `AuthorizedKeysCommandUser` définit l'utilisateur système comme `ec2-instance-connect`.

> **Note**
>
> Si vous avez déjà configuré `AuthorizedKeysCommand` et`AuthorizedKeysCommandUser`, l'installation d'EC2Instance Connect ne modifiera pas les valeurs et vous ne pourrez pas utiliser EC2 Instance Connect.

macOS

Pour installer EC2 Instance Connect sur une instance lancée avec macOS

1. Connectez-vous à votre instance à l'aide de`SSH`.

   Remplacez les valeurs de l'exemple dans la commande suivante par vos propres valeurs. Utilisez la paire de SSH clés attribuée à votre instance lorsque vous l'avez lancée et le nom d'utilisateur par défaut AMI que vous avez utilisé pour lancer votre instance. Pour les instances de macOS, le nom d'utilisateur par défaut est`ec2-user`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Pour plus d'informations sur la connexion à votre instance, consultez Connectez-vous à votre instance Linux à l'aide d'un SSH client.

2. Mettez à jour Homebrew en utilisant la commande suivante. La mise à jour listera les logiciels que Homebrew connaît. Le package EC2 Instance Connect est fourni via Homebrew sur les

instances de macOS. Pour de plus amples informations, veuillez consulter Mettre à jour le système d'exploitation et le logiciel sur les instances Mac.

```
[ec2-user ~]$ brew update
```

3. Installez le package EC2 Instance Connect sur votre instance. Cela installera le logiciel et configurera sshd pour l'utiliser.

```
[ec2-user ~]$ brew install ec2-instance-connect
```

Vous devriez voir ce nouveau script dans le dossier `/opt/aws/bin/` :

```
eic_run_authorized_keys
```

4. (Facultatif) Vérifiez qu'EC2Instance Connect a été correctement installé sur votre instance.

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
```

EC2Instance Connect a été correctement installée si les `AuthorizedKeysCommandUser` lignes `AuthorizedKeysCommand` et contiennent les valeurs suivantes :

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` définit le script `eic_run_authorized_keys` pour rechercher les clés à partir des métadonnées de l'instance.
- `AuthorizedKeysCommandUser` définit l'utilisateur système comme `ec2-instance-connect`.

> **Note**
>
> Si vous avez déjà configuré `AuthorizedKeysCommand` et`AuthorizedKeysCommandUser`, l'installation d'EC2Instance Connect ne modifiera pas les valeurs et vous ne pourrez pas utiliser EC2 Instance Connect.

RHEL

Pour installer EC2 Instance Connect sur une instance lancée avec Red Hat Enterprise Linux (RHEL)

1. Connectez-vous à votre instance à l'aide deSSH.

   Remplacez les valeurs de l'exemple dans la commande suivante par vos propres valeurs. Utilisez la paire de SSH clés attribuée à votre instance lorsque vous l'avez lancée et le nom d'utilisateur par défaut AMI que vous avez utilisé pour lancer votre instance. Car RHEL le nom d'utilisateur par défaut est `ec2-user` ou`root`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Pour plus d'informations sur la connexion à votre instance, consultez Connectez-vous à votre instance Linux à l'aide d'un SSH client.

2. Si vous utilisez un HTTPS proxy HTTP ou, vous devez définir les variables d'`https_proxy`environnement `http_proxy` or dans la session shell en cours.

   Si vous n'utilisez pas de proxy, vous pouvez ignorer cette étape.

   - Pour un serveur HTTP proxy, exécutez les commandes suivantes :

     ```
     $ export http_proxy=http://hostname:port
     $ export https_proxy=http://hostname:port
     ```

   - Pour un serveur HTTPS proxy, exécutez les commandes suivantes :

     ```
     $ export http_proxy=https://hostname:port
     $ export https_proxy=https://hostname:port
     ```

3. Installez le package EC2 Instance Connect sur votre instance en exécutant les commandes suivantes.

   Les fichiers de configuration d'EC2Instance Connect pour RHEL sont fournis dans un package Red Hat Package Manager (RPM), avec différents RPM packages pour RHEL 8 et RHEL 9 et pour les types d'instances qui s'exécutent sur Intel/ AMD (x86_64) ou (). ARM AArch64

Utilisez le bloc de commandes correspondant à votre système d'exploitation et à votre CPU architecture.

- RHEL8

  Intel/ AMD (x86_64)

  ```
  [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
  west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rhel8.rpm -o /
  tmp/ec2-instance-connect/ec2-instance-connect.rpm
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
  west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
  selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
  selinux.rpm
  [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
  connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
  ```

  ARM (AArch64)

  ```
  [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
  west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rhel8.rpm -o /
  tmp/ec2-instance-connect/ec2-instance-connect.rpm
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
  west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
  selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
  selinux.rpm
  [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
  connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
  ```

- RHEL9

  Intel/ AMD (x86_64)

  ```
  [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
  west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rpm -o /tmp/ec2-
  instance-connect/ec2-instance-connect.rpm
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
  west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
  ```

```
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rpm -o /tmp/ec2-
instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

Vous devriez voir ce nouveau script dans le dossier `/opt/aws/bin/` :

```
eic_run_authorized_keys
```

4. (Facultatif) Vérifiez qu'EC2Instance Connect a été correctement installé sur votre instance.

   - Pour RHEL 8 personnes :

     ```
     [ec2-user ~]$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-
     connect.conf
     ```

   - Pour RHEL 9 personnes :

     ```
     [ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
     ```

   EC2Instance Connect a été correctement installée si les `AuthorizedKeysCommandUser` lignes `AuthorizedKeysCommand` et contiennent les valeurs suivantes :

   ```
   AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
   AuthorizedKeysCommandUser ec2-instance-connect
   ```

- `AuthorizedKeysCommand` définit le script `eic_run_authorized_keys` pour rechercher les clés à partir des métadonnées de l'instance.
- `AuthorizedKeysCommandUser` définit l'utilisateur système comme `ec2-instance-connect`.

> **Note**
>
> Si vous avez déjà configuré `AuthorizedKeysCommand` et`AuthorizedKeysCommandUser`, l'installation d'EC2Instance Connect ne modifiera pas les valeurs et vous ne pourrez pas utiliser EC2 Instance Connect.

Ubuntu

Pour installer EC2 Instance Connect sur une instance lancée avec Ubuntu 16.04 ou version ultérieure

1. Connectez-vous à votre instance à l'aide deSSH.

   Remplacez les valeurs de l'exemple dans la commande suivante par vos propres valeurs. Utilisez la paire de SSH clés attribuée à votre instance lorsque vous l'avez lancée et utilisez le nom d'utilisateur par défaut AMI que vous avez utilisé pour lancer votre instance. Pour un UbuntuAMI, le nom d'utilisateur est`ubuntu`.

   ```
   $ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Pour plus d'informations sur la connexion à votre instance, consultez Connectez-vous à votre instance Linux à l'aide d'un SSH client.

2. (Facultatif) Assurez-vous que votre instance dispose de la dernière version d'UbuntuAMI.

   Exécutez les commandes suivantes pour mettre à jour tous les paquets sur votre instance.

   ```
   ubuntu:~$ sudo apt-get update
   ```

   ```
   ubuntu:~$ sudo apt-get upgrade
   ```

3. Installez le package EC2 Instance Connect sur votre instance.

```
ubuntu:~$ sudo apt-get install ec2-instance-connect
```

Trois nouveaux scripts doivent apparaître dans le dossier `/usr/share/ec2-instance-connect/` :

```
eic_curl_authorized_keys
eic_parse_authorized_keys
eic_run_authorized_keys
```

4. (Facultatif) Vérifiez qu'Instance Connect a été installé avec succès sur votre instance.

```
ubuntu:~$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
```

EC2Instance Connect a été correctement installée si les `AuthorizedKeysCommandUser` lignes `AuthorizedKeysCommand` et contiennent les valeurs suivantes :

```
AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized_keys %
%u %%f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` définit le script `eic_run_authorized_keys` pour rechercher les clés à partir des métadonnées de l'instance.
- `AuthorizedKeysCommandUser` définit l'utilisateur système comme `ec2-instance-connect`.

> **Note**
>
> Si vous avez déjà configuré `AuthorizedKeysCommand` et`AuthorizedKeysCommandUser`, l'installation d'EC2Instance Connect ne modifiera pas les valeurs et vous ne pourrez pas utiliser EC2 Instance Connect.

Connectez-vous à l'aide d'EC2Instance Connect

Les instructions suivantes expliquent comment vous connecter à votre instance Linux à l'aide d'EC2Instance Connect via la EC2 console Amazon AWS CLI, le ou un SSH client.

Prérequis

Avant de commencer, assurez-vous de passer en revue les prérequis.

Options de connexion

- Connect à l'aide de la EC2 console Amazon
- Connectez-vous à l'aide du AWS CLI
- Connectez-vous à l'aide de votre propre clé et de votre propre SSH client
- Dépannage

Connect à l'aide de la EC2 console Amazon

Vous pouvez vous connecter à une instance à l'aide d'EC2Instance Connect via la EC2 console Amazon. Instance Connect gère les autorisations.

Exigence

Pour se connecter à l'aide de EC2 la console Amazon, l'instance doit disposer d'une IPv4 adresse publique. Si l'instance n'a qu'une IPv6 adresse, vous pouvez vous connecter à l'aide des commandes AWS CLI ec2-instance-connect.

Pour vous connecter à votre instance à l'aide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance, puis choisissez Connect (Connexion).
4. Choisissez l'onglet EC2Instance Connect.
5. Pour le type de connexion, choisissez Connect using EC2 Instance Connect.
6. Pour Nom d'utilisateur, vérifiez le nom d'utilisateur.
7. Choisissez Connecter pour ouvrir une fenêtre de terminal.

Connectez-vous à l'aide du AWS CLI

Vous pouvez utiliser les AWS CLI commandes ec2-instance-connect pour vous connecter à votre instance à l'aide d'un client. SSH

Si vous ne spécifiez aucun type de connexion, EC2 Instance Connect essaie de se connecter à l'instance comme suit :

- Connectez-vous à l'aide de l'IPv4adresse publique.
- S'il n'y a pas d'IPv4adresse publique, connectez-vous à l'aide de l'IPv4adresse privée et d'un point de terminaison EC2 Instance Connect
- S'il n'existe aucune IPv4 adresse privée ou aucun point de terminaison EC2 Instance Connect, connectez-vous à l'aide de IPv6 cette adresse.

Prérequis

Vous devez vous préparer à utiliser la AWS CLI version 2. Pour plus d'informations, voir Installer ou mettre à jour vers la dernière version du AWS CLI.

Types de connexion

`auto` (default)

CLItente de se connecter en utilisant les adresses IP de l'instance dans l'ordre suivant et avec le type de connexion correspondant :

- Publique IPv4 : `direct`
- Privé IPv4 : `eice`
- IPv6: `direct`

`direct`

Il CLI essaie de se connecter en utilisant les adresses IP de l'instance dans l'ordre suivant (il ne se connecte pas via un point de terminaison EC2 Instance Connect) :

- Publique IPv4
- IPv6
- Privé IPv4

`eice`

Il utilise CLI toujours l'IPv4adresse privée de l'instance.

> **Note**
>
> Dans le futur, nous pourrions changer le comportement du type de connexion `auto`. Pour vous assurer que le type de connexion que vous souhaitez est utilisé, nous vous recommandons de définir explicitement `--connection-type` sur `direct` ou `eice`.

Lorsque vous vous connectez à une instance à l'aide d'EC2Instance Connect, EC2 Instance API Connect envoie une clé SSH publique aux métadonnées de l'instance, où elle reste pendant 60 secondes. Une IAM politique attachée à votre utilisateur autorise celui-ci à transmettre la clé publique aux métadonnées de l'instance.

Pour se connecter à une instance en utilisant l'ID de l'instance

Si vous ne connaissez que l'ID de l'instance et que vous souhaitez laisser EC2 Instance Connect déterminer le type de connexion à utiliser lors de la connexion à votre instance, utilisez la CLI commande ec2-instance-connect et spécifiez le `ssh` paramètre et l'ID d'instance.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example
```

> **Tip**
>
> Si une erreur s'affiche lors de l'utilisation de cette commande, assurez-vous que vous utilisez la AWS CLI version 2, car le `ssh` paramètre n'est disponible que dans cette version majeure. Nous vous recommandons également de passer régulièrement à la dernière version mineure de la AWS CLI version 2 pour accéder aux dernières fonctionnalités. Pour plus d'informations, consultez la section À propos de AWS CLI la version 2 dans le guide de AWS Command Line Interface l'utilisateur.

Pour vous connecter à une instance à l'aide de l'ID d'instance et d'un point de terminaison EC2 Instance Connect

Si vous souhaitez vous connecter à votre instance via un point de terminaison EC2 Instance Connect, utilisez la commande précédente et spécifiez également le `--connection-type` paramètre avec la `eice` valeur.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --connection-type eice
```

Pour vous connecter à une instance en utilisant l'ID de l'instance et votre propre fichier de clé privée

Si vous souhaitez vous connecter à votre instance via un point de terminaison EC2 Instance Connect à l'aide de votre propre clé privée, spécifiez l'ID de l'instance et le chemin d'accès au fichier de clé privée. Ne pas inclure *file://* dans le chemin ; l'exemple suivant échouera : *file:///path/to/key*.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --private-key-file /path/to/key.pem
```

Connectez-vous à l'aide de votre propre clé et de votre propre SSH client

Vous pouvez utiliser votre propre SSH clé et vous connecter à votre instance depuis le SSH client de votre choix lorsque vous utilisez EC2 Instance ConnectAPI. Cela vous permet de bénéficier de la capacité d'Instance Connect d'envoyer une clé publique en mode push à l'instance. Cette méthode de connexion fonctionne pour les instances avec des adresses IP publiques et privées.

Prérequis

- Exigences relatives aux paires de clés
  - Types pris en charge : RSA (ouvert SSH etSSH2) et ED25519
  - Longueurs prises en charge : 2048 et 4096
  - Pour de plus amples informations, veuillez consulter Créez une paire de clés à l'aide d'un outil tiers et importez la clé publique sur Amazon EC2.
- Lorsque vous vous connectez à une instance qui ne possède que des adresses IP privées, l'ordinateur local à partir duquel vous lancez la SSH session doit être connecté au point de terminaison du service EC2 Instance Connect (pour transmettre votre clé SSH publique à l'instance) ainsi qu'une connectivité réseau à l'adresse IP privée de l'instance pour établir la SSH session. Le point de terminaison du service EC2 Instance Connect est accessible via Internet ou via une interface virtuelle AWS Direct Connect publique. Pour vous connecter à l'adresse IP privée de l'instance, vous pouvez tirer parti de services tels que AWS Direct ConnectAWS Site-to-Site VPN, ou le VPCpeering.

Pour vous connecter à votre instance à l'aide de votre propre clé et de n'importe quel SSH client

1. (Facultatif) Générez de nouvelles clés SSH privées et publiques

   Vous pouvez générer de nouvelles clés SSH privées et publiques `my_key` et`my_key.pub`, à l'aide de la commande suivante :

   ```
   ssh-keygen -t rsa -f my_key
   ```

2. Transférez votre clé SSH publique à l'instance

   Utilisez la send-ssh-public-keycommande pour transmettre votre clé SSH publique à l'instance. Si vous avez lancé votre instance en utilisant AL2 023 ou Amazon Linux 2, le nom d'utilisateur par défaut AMI est`ec2-user`. Si vous avez lancé votre instance avec Ubuntu, le nom d'utilisateur par défaut AMI est`ubuntu`.

   L'exemple suivant pousse la clé publique vers l'instance spécifiée dans la zone de disponibilité spécifiée, afin d'authentifier `ec2-user`.

   ```
   aws ec2-instance-connect send-ssh-public-key \
       --region us-west-2 \
       --availability-zone us-west-2b \
       --instance-id i-001234a4bf70dec41EXAMPLE \
       --instance-os-user ec2-user \
       --ssh-public-key file://my_key.pub
   ```

3. Connexion à l'instance avec votre clé privée

   Utilisez la commande ssh pour vous connecter à l'instance à l'aide de la clé privée avant que la clé publique ne soit supprimée des métadonnées de l'instance (vous disposez de 60 secondes avant qu'elle ne soit supprimée). Spécifiez la clé privée qui correspond à la clé publique, le nom d'utilisateur par défaut utilisé pour lancer votre instance et le DNS nom public de l'instance (si vous vous connectez via un réseau privé, spécifiez le DNS nom privé ou l'adresse IP). AMI Ajoutez l'option `IdentitiesOnly=yes` pour vous assurer que seuls les fichiers de la configuration ssh et la clé spécifiée sont utilisés pour la connexion.

   ```
   ssh -o "IdentitiesOnly=yes" -i my_key ec2-
   user@ec2-198-51-100-1.compute-1.amazonaws.com
   ```

Dépannage

Si vous recevez une erreur lors d'une tentative de connexion à votre instance, consultez ce qui suit.

- Résoudre les problèmes de connexion à votre instance Amazon EC2 Linux
- Comment résoudre les problèmes de connexion à mon EC2 instance à l'aide d'EC2Instance Connect ?

Désinstallez EC2 Instance Connect

Pour désactiver EC2 Instance Connect, connectez-vous à votre instance Linux et désinstallez le `ec2-instance-connect` package installé sur le système d'exploitation. Si la `sshd` configuration correspond à celle définie lors de l'installation d'EC2Instance Connect, la désinstallation supprime `ec2-instance-connect` également la `sshd` configuration. Si vous avez modifié la `sshd` configuration après avoir installé EC2 Instance Connect, vous devez la mettre à jour manuellement.

Amazon Linux

Vous pouvez désinstaller EC2 Instance Connect sur AL2 023 et Amazon Linux 2 2.0.20190618 ou version ultérieure, où Instance Connect est préconfiguré. EC2

Pour désinstaller EC2 Instance Connect sur une instance lancée à l'aide d'Amazon Linux

1. Connectez-vous à votre instance à l'aide deSSH. Spécifiez la paire de SSH clés que vous avez utilisée pour votre instance lorsque vous l'avez lancée et le nom d'utilisateur par défaut pour le AL2 023 ou Amazon Linux 2AMI, qui est`ec2-user`.

   Par exemple, la ssh commande suivante permet de se connecter à l'instance avec le DNS nom public`ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, à l'aide de la paire de clés`my_ec2_private_key.pem`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

2. Désinstallez le package `ec2-instance-connect` à l'aide de la commande yum.

   ```
   [ec2-user ~]$ sudo yum remove ec2-instance-connect
   ```

Ubuntu

Pour désinstaller EC2 Instance Connect sur une instance lancée à l'aide d'un Ubuntu AMI

1. Connectez-vous à votre instance à l'aide deSSH. Spécifiez la paire de SSH clés que vous avez utilisée pour votre instance lorsque vous l'avez lancée et le nom d'utilisateur par défaut pour UbuntuAMI, qui estubuntu.

   Par exemple, la ssh commande suivante permet de se connecter à l'instance avec le DNS nom publicec2-a-b-c-d.us-west-2.compute.amazonaws.com, à l'aide de la paire de clésmy_ec2_private_key.pem.

   ```
   $ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

2. Désinstallez le package `ec2-instance-connect` à l'aide de la commande apt-get.

   ```
   ubuntu:~$ sudo apt-get remove ec2-instance-connect
   ```

Connectez-vous à vos instances à l'aide d'EC2Instance Connect Endpoint

EC2Instance Connect Endpoint vous permet de vous connecter en toute sécurité à une instance depuis Internet, sans utiliser d'hôte bastion ni exiger que votre cloud privé virtuel (VPC) dispose d'une connexion Internet directe.

Avantages

- Vous pouvez vous connecter à vos instances sans que celles-ci aient besoin d'une IPv4 adresse publique. AWS frais pour toutes les IPv4 adresses publiques, y compris les IPv4 adresses publiques associées aux instances en cours d'exécution et les adresses IP Elastic. Pour plus d'informations, consultez l'onglet IPv4Adresse publique sur la page de VPC tarification d'Amazon.
- Vous pouvez vous connecter à vos instances depuis Internet sans avoir besoin d'une connexion Internet directe via une passerelle Internet. VPC
- Vous pouvez contrôler l'accès à la création et à l'utilisation des points de terminaison EC2 Instance Connect pour vous connecter aux instances à l'aide de IAMpolitiques et d'autorisations.
- Toutes les tentatives de connexion à vos instances, qu'elles soient réussies ou non, sont enregistrées CloudTrail.

Tarification

L'utilisation des points de terminaison EC2 Instance Connect n'entraîne aucun coût supplémentaire. Si vous utilisez un point de terminaison EC2 Instance Connect pour vous connecter à une instance située dans une autre zone de disponibilité, des frais supplémentaires sont facturés pour le transfert de données entre les zones de disponibilité.

Table des matières

Comment ça marche

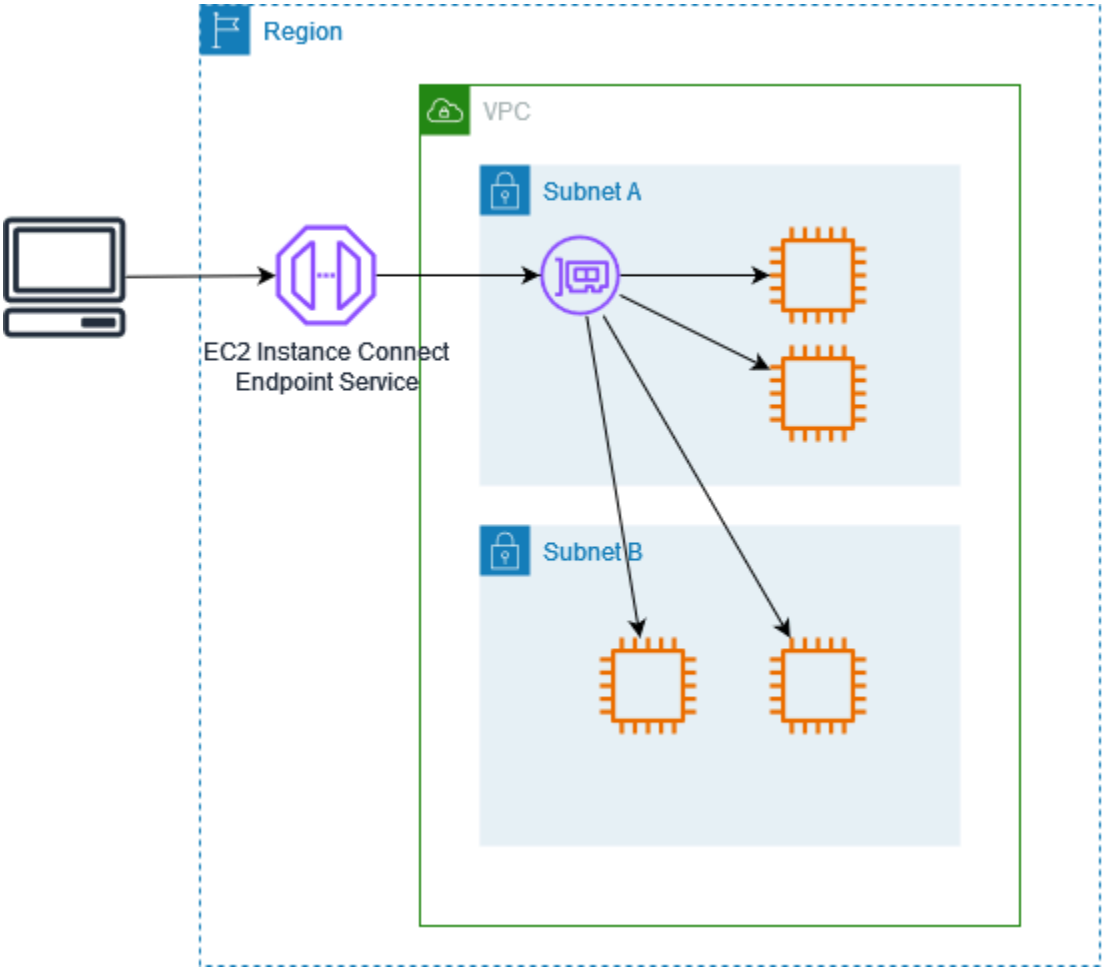
EC2Instance Connect Endpoint est un proxy sensible à l'identitéTCP. Le service EC2 Instance Connect Endpoint établit un tunnel privé entre votre ordinateur et le point de terminaison à l'aide des informations d'identification de votre IAM entité. Le trafic est authentifié et autorisé avant qu'il n'atteigne votreVPC.

Vous pouvez configurer des règles de groupe de sécurité supplémentaires pour limiter le trafic entrant vers vos instances. Par exemple, vous pouvez utiliser des règles entrantes pour autoriser le trafic sur les ports de gestion uniquement à partir du point de terminaison EC2 Instance Connect.

Vous pouvez configurer les règles de table de routage pour permettre au point de terminaison de se connecter à n'importe quelle instance de n'importe quel sous-réseau duVPC.

Le schéma suivant montre comment un utilisateur peut se connecter à ses instances depuis Internet à l'aide d'un point de terminaison EC2 Instance Connect. Créez d'abord un point de terminaison EC2 Instance Connect dans le sous-réseau A. Nous créons une interface réseau pour le point de

terminaison du sous-réseau, qui sert de point d'entrée pour le trafic destiné à vos instances dans le. VPC Si la table de routage du sous-réseau B autorise le trafic en provenance du sous-réseau A, vous pouvez utiliser le point de terminaison pour atteindre les instances du sous-réseau B.



Considérations

Avant de commencer, considérez les points suivants.

- EC2Instance Connect Endpoint est spécifiquement conçu pour les cas d'utilisation du trafic de gestion, et non pour les transferts de données à volume élevé. Les transferts de données à haut volume sont limités.
- Votre instance doit avoir une IPv4 adresse (privée ou publique). EC2Instance Connect Endpoint ne prend pas en charge la connexion aux instances à l'aide d'IPv6adresses.
- (Instances Linux) Si vous utilisez votre propre paire de clés, vous pouvez utiliser n'importe quel système LinuxAMI. Dans le cas contraire, Instance Connect doit être installé sur votre EC2 instance. Pour plus d'informations sur ce qui AMIs inclut EC2 Instance Connect et sur la façon de l'installer sur d'autres appareils pris en chargeAMIs, consultezInstallez EC2 Instance Connect.

- Vous pouvez attribuer un groupe de sécurité à un point de terminaison EC2 Instance Connect lorsque vous le créez. Dans le cas contraire, nous utilisons le groupe de sécurité par défaut pourVPC. Le groupe de sécurité d'un point de terminaison EC2 Instance Connect doit autoriser le trafic sortant vers les instances de destination. Pour de plus amples informations, veuillez consulter Groupes de sécurité pour EC2 Instance Connect Endpoint.
- Vous pouvez configurer un point de terminaison EC2 Instance Connect pour conserver les adresses IP sources des clients lors du routage des demandes vers les instances. Dans le cas contraire, l'adresse IP de l'interface réseau devient l'adresse IP du client pour tout le trafic entrant.
  - Si vous activez la préservation de l'adresse IP des clients, les groupes de sécurité des instances doivent autoriser le trafic provenant des clients. En outre, les instances doivent se trouver dans le même emplacement VPC que le point de terminaison EC2 Instance Connect.
  - Si vous désactivez la préservation de l'adresse IP du client, les groupes de sécurité des instances doivent autoriser le trafic en provenance duVPC. Il s'agit de l'option par défaut.
  - Les types d'instance suivants ne prennent pas en charge la préservation de l'adresse IP du client : C1 CG1CG2,,, G1HI1, M1, M2, M3 et T1. Si vous activez la préservation de l'adresse IP du client et que vous tentez de vous connecter à une instance avec l'un de ces types d'instance à l'aide d'EC2Instance Connect Endpoint, la connexion échoue.
  - La préservation de l'adresse IP du client n'est pas prise en charge lorsque le trafic est acheminé via une passerelle de transit.
- Lorsque vous créez un point de terminaison EC2 Instance Connect, un rôle lié à un service est automatiquement créé pour le EC2 service Amazon dans AWS Identity and Access Management ()IAM. Amazon EC2 utilise le rôle lié à un service pour fournir des interfaces réseau dans votre compte, qui sont requises lors de la création de points de terminaison EC2 Instance Connect. Pour de plus amples informations, veuillez consulter Rôle lié à un service pour Instance EC2 Connect Endpoint.
- Vous ne pouvez créer qu'un seul point de terminaison EC2 Instance Connect par sous-réseau. VPC Pour de plus amples informations, veuillez consulter Quotas pour EC2 Instance Connect Endpoint. Si vous devez créer un autre point de terminaison EC2 Instance Connect dans une autre zone de disponibilité au sein de la même zoneVPC, vous devez d'abord supprimer le point de terminaison EC2 Instance Connect existant. Dans le cas contraire, vous recevrez une erreur de quota.
- Chaque point de terminaison EC2 Instance Connect peut prendre en charge jusqu'à 20 connexions simultanées.
- La durée maximale d'une TCP connexion établie est de 1 heure (3 600 secondes). Vous pouvez spécifier la durée maximale autorisée dans une IAM politique, qui peut aller jusqu'à 3 600

secondes. Pour de plus amples informations, veuillez consulter Autorisations d'utilisation du point de terminaison EC2 Instance Connect pour se connecter aux instances.

Accorder des autorisations pour utiliser EC2 Instance Connect Endpoint

Par défaut, IAM les entités ne sont pas autorisées à créer, décrire ou modifier les points de terminaison EC2 Instance Connect. Un IAM administrateur peut créer des IAM politiques qui accordent les autorisations nécessaires pour effectuer des actions spécifiques sur les ressources dont il a besoin.

Pour plus d'informations sur la création de IAM politiques, voir Création de IAM politiques dans le Guide de IAM l'utilisateur.

Les exemples de politiques suivants montrent que vous pouvez contrôler les autorisations dont disposent les utilisateurs sur les points de terminaison EC2 Instance Connect.

Exemples

- Autorisations pour créer, décrire et supprimer des points de terminaison EC2 Instance Connect
- Autorisations d'utilisation du point de terminaison EC2 Instance Connect pour se connecter aux instances
- Autorisations de connexion uniquement à partir d'une plage d'adresses IP spécifique

Autorisations pour créer, décrire et supprimer des points de terminaison EC2 Instance Connect

Pour créer un point de terminaison EC2 Instance Connect, les utilisateurs ont besoin d'autorisations pour effectuer les actions suivantes :

- `ec2:CreateInstanceConnectEndpoint`
- `ec2:CreateNetworkInterface`
- `ec2:CreateTags`
- `iam:CreateServiceLinkedRole`

Pour décrire et supprimer les points de terminaison EC2 Instance Connect, les utilisateurs doivent disposer d'autorisations pour effectuer les actions suivantes :

- `ec2:DescribeInstanceConnectEndpoints`
- `ec2:DeleteInstanceConnectEndpoint`

Vous pouvez créer une politique qui autorise la création, la description et la suppression des points de terminaison EC2 Instance Connect dans tous les sous-réseaux. Vous pouvez également restreindre les actions pour des sous-réseaux spécifiques uniquement en spécifiant le sous-réseau ARNs comme étant autorisé `Resource` ou en utilisant la clé de `ec2:SubnetID` condition. Vous pouvez également utiliser la clé de condition `aws:ResourceTag` pour autoriser ou refuser explicitement la création de points de terminaison avec certaines balises. Pour plus d'informations, consultez la section Politiques et autorisations IAM dans le guide de IAM l'utilisateur.

Exemple IAM de politique

Dans l'exemple de IAM politique suivant, la `Resource` section autorise la création et la suppression de points de terminaison dans tous les sous-réseaux, spécifiés par l'astérisque (). * Les `ec2:Describe*` API actions ne prennent pas en charge les autorisations au niveau des ressources. Par conséquent, le caractère générique * est nécessaire dans l'élément `Resource`.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "GrantAllActionsInAllSubnets",
            "Action": [
                "ec2:CreateInstanceConnectEndpoint",
                "ec2:DeleteInstanceConnectEndpoint",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "iam:CreateServiceLinkedRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:region:account-id:subnet/*"
        },
        {
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:::security-group/*"
        },
        {
            "Sid": "DescribeInstanceConnectEndpoints",
            "Action": [
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
```

```
            "Resource": "*"
        }
    ]
}
```

Autorisations d'utilisation du point de terminaison EC2 Instance Connect pour se connecter aux instances

L'`ec2-instance-connect:OpenTunnel`action autorise l'établissement d'une TCP connexion à une instance afin de se connecter via le point de terminaison EC2 Instance Connect. Vous pouvez spécifier le point de terminaison EC2 Instance Connect à utiliser. Sinon, un `Resource` astérisque (*) permet aux utilisateurs d'utiliser n'importe quel point de terminaison EC2 Instance Connect disponible. Vous pouvez également limiter l'accès aux instances en fonction de la présence ou de l'absence de balises de ressources en tant que clés de condition.

Conditions

- `ec2-instance-connect:remotePort`— Le port de l'instance qui peut être utilisé pour établir une TCP connexion. Lorsque cette clé de condition est utilisée, toute tentative de connexion à une instance sur un port autre que celui spécifié dans la politique se solde par un échec.
- `ec2-instance-connect:privateIpAddress`— Adresse IP privée de destination associée à l'instance avec laquelle vous souhaitez établir une TCP connexion. Vous pouvez spécifier une adresse IP unique, telle que`10.0.0.1/32`, ou une plage de IPs pointsCIDRs, telle que`10.0.1.0/28`. Lorsque cette clé de condition est utilisée, toute tentative de connexion à une instance avec une adresse IP privée différente ou hors CIDR plage entraîne un échec.
- `ec2-instance-connect:maxTunnelDuration`— La durée maximale d'une TCP connexion établie. L'unité est la seconde et la durée va d'un minimum de 1 seconde à un maximum de 3 600 secondes (1 heure). Si la condition n'est pas spécifiée, la durée par défaut est fixée à 3 600 secondes (1 heure). Toute tentative de connexion à une instance pendant une durée supérieure à la durée spécifiée dans la IAM politique ou au-delà du maximum par défaut entraîne un échec. La connexion est interrompue après la durée spécifiée.

  Si cela `maxTunnelDuration` est spécifié dans la IAM politique et que la valeur spécifiée est inférieure à 3 600 secondes (valeur par défaut), vous devez le spécifier `--max-tunnel-duration` dans la commande lors de la connexion à une instance. Pour plus d'informations sur la manière de se connecter à une instance, consultez Connectez-vous à une EC2 instance Amazon à l'aide d'EC2Instance Connect Endpoint.

Vous pouvez également accorder à un utilisateur l'accès pour établir des connexions aux instances en fonction de la présence de balises de ressources sur le point de terminaison EC2 Instance Connect. Pour plus d'informations, consultez la section Politiques et autorisations IAM dans le guide de IAM l'utilisateur.

Pour les instances Linux, l'`ec2-instance-connect:SendSSHPublicKey`action autorise le transfert de la clé publique à une instance. La condition `ec2:osuser` spécifie le nom de l'utilisateur du système d'exploitation qui peut envoyer la clé publique en mode push à une instance. Utilisez le nom d'utilisateur par défaut pour celui AMI que vous avez utilisé pour lancer l'instance. Pour de plus amples informations, veuillez consulter Accorder IAM des autorisations pour EC2 Instance Connect.

Exemple IAM de politique

Les exemples de IAM politiques suivants permettent à un IAM principal de se connecter à une instance en utilisant uniquement le point de terminaison EC2 Instance Connect spécifié, identifié par l'ID de point de terminaison spécifié`eice-123456789abcdef`. La connexion n'est établie avec succès que si toutes les conditions sont remplies.

> **Note**
>
> Les `ec2:Describe*` API actions ne prennent pas en charge les autorisations au niveau des ressources. Par conséquent, le caractère générique `*` est nécessaire dans l'élément `Resource`.

Linux

Cet exemple évalue si la connexion à l'instance est établie sur —port 22 (SSH), si l'adresse IP privée de l'instance se situe dans la plage de `10.0.1.0/31` (entre `10.0.1.0` et`10.0.1.1`), et si elle `maxTunnelDuration` est inférieure ou égale à `3600` quelques secondes. La connexion est interrompue au bout de `3600` secondes (1 heure).

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EC2InstanceConnect",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:region:account-id:instance-connect-
endpoint/eice-123456789abcdef",
```

```
            "Condition": {
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "22"
                },
                "IpAddress": {
                    "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
                },
                "NumericLessThanEquals": {
                    "ec2-instance-connect:maxTunnelDuration": "3600"
                }
            }
        },
        {
            "Sid": "SSHPublicKey",
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Sid": "Describe",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Windows

Cet exemple évalue si la connexion à l'instance est établie sur le port 3389 (RDP), si l'adresse IP privée de l'instance se situe dans la plage de `10.0.1.0/31` (entre `10.0.1.0` et`10.0.1.1`) et si elle `maxTunnelDuration` est inférieure ou égale à `3600` quelques secondes. La connexion est interrompue au bout de `3600` secondes (1 heure).

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EC2InstanceConnect",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:region:account-id:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "3389"
                },
                "IpAddress": {
                    "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
                },
                "NumericLessThanEquals": {
                    "ec2-instance-connect:maxTunnelDuration": "3600"
                }
            }
        },
        {
            "Sid": "Describe",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Autorisations de connexion uniquement à partir d'une plage d'adresses IP spécifique

L'exemple de IAM stratégie suivant permet à un IAM principal de se connecter à une instance à condition qu'il se connecte à partir d'une adresse IP comprise dans la plage d'adresses IP spécifiée dans la stratégie. Si les appels IAM principaux `OpenTunnel` proviennent d'une adresse IP qui n'est pas comprise dans `192.0.2.0/24` (exemple de plage d'adresses IP dans cette politique), la réponse est`Access Denied`. Pour plus d'informations, consultez [`aws:SourceIp`](#)le guide de IAM l'utilisateur.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Resource": "arn:aws:ec2:region:account-id:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "192.0.2.0/24"
                },
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "22"
                }
            }
        },
        {
            "Sid": "SSHPublicKey",
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Resource": "*"
        }
    ]
}
```

Groupes de sécurité pour EC2 Instance Connect Endpoint

Un groupe de sécurité contrôle le trafic autorisé à atteindre et à quitter les ressources auxquelles il est associé. Par exemple, nous refusons le trafic à destination et en provenance d'une EC2 instance Amazon, sauf s'il est spécifiquement autorisé par les groupes de sécurité associés à l'instance.

Les exemples suivants vous montrent comment configurer les règles du groupe de sécurité pour le point de terminaison EC2 Instance Connect et les instances cibles.

Exemples

- EC2Règles du groupe de sécurité Instance Connect Endpoint
- Règles du groupe de sécurité de l'instance cible

EC2Règles du groupe de sécurité Instance Connect Endpoint

Les règles du groupe de sécurité pour un point de terminaison EC2 Instance Connect doivent autoriser le trafic sortant destiné aux instances cibles à quitter le point de terminaison. Vous pouvez spécifier le groupe de sécurité de l'instance ou la plage d'IPv4adresses de l'instance VPC comme destination.

Le trafic vers le point de terminaison provient du service EC2 Instance Connect Endpoint, et il est autorisé quelles que soient les règles de trafic entrant pour le groupe de sécurité du point de terminaison. Pour contrôler qui peut utiliser EC2 Instance Connect Endpoint pour se connecter à une instance, utilisez une IAM politique. Pour de plus amples informations, veuillez consulter Autorisations d'utilisation du point de terminaison EC2 Instance Connect pour se connecter aux instances.

Exemple de règle sortante : référencement de groupes de sécurité

L'exemple suivant utilise le référencement des groupes de sécurité, ce qui signifie que la destination est un groupe de sécurité associé aux instances cibles. Cette règle autorise le trafic sortant du point de terminaison vers toutes les instances qui utilisent ce groupe de sécurité.

Protocole	Destination	Plage de ports	Comment
TCP	*ID of instance security group*	22	Autorise le SSH trafic sortant vers toutes les instances associées au groupe de sécurité des instances

Exemple de règle sortante : plage d'IPv4adresses

L'exemple suivant autorise le trafic sortant vers la plage d'IPv4adresses spécifiée. Les IPv4 adresses d'une instance sont attribuées à partir de son sous-réseau. Vous pouvez donc utiliser la plage d'IPv4adresses duVPC.

Protocole	Destination	Plage de ports	Comment
TCP	*VPC IPv4 CIDR*	22	Autorise le SSH trafic sortant vers VPC

Règles du groupe de sécurité de l'instance cible

Les règles du groupe de sécurité pour les instances cibles doivent autoriser le trafic entrant depuis le point de terminaison EC2 Instance Connect. Vous pouvez spécifier le groupe de sécurité du point de terminaison ou une plage d'IPv4adresses comme source. Si vous spécifiez une plage d'IPv4adresses, la source varie selon que la préservation de l'adresse IP du client est activée ou désactivée. Pour de plus amples informations, veuillez consulter Considérations.

Les groupes de sécurité étant dynamiques, le trafic de réponse est autorisé à quitter le statut, VPC quelles que soient les règles de sortie applicables au groupe de sécurité d'instance.

Exemple de règle entrante : référencement de groupes de sécurité

L'exemple suivant utilise le référencement des groupes de sécurité, ce qui signifie que la source est le groupe de sécurité associé au point de terminaison. Cette règle autorise le SSH trafic entrant depuis le point de terminaison vers toutes les instances qui utilisent ce groupe de sécurité, que la préservation de l'adresse IP du client soit activée ou non. S'il n'existe aucune autre règle de groupe de sécurité entrant pourSSH, les instances n'acceptent que le SSH trafic provenant du point de terminaison.

Protocole	Source	Plage de ports	Comment
TCP	*ID of endpoint security group*	22	Autorise le SSH trafic entrant depuis les ressources associées au groupe de sécurité du point de terminaison

Exemple de règle entrante : conservation de l'adresse IP du client désactivée

L'exemple suivant autorise le SSH trafic entrant à partir de la plage d'IPv4adresses spécifiée. La préservation de l'adresse IP du client étant désactivée, l'IPv4adresse source est l'adresse de

l'interface réseau du point de terminaison. L'adresse de l'interface réseau du point de terminaison est attribuée à partir de son sous-réseau. Vous pouvez donc utiliser la plage d'IPv4adresses du VPC pour autoriser les connexions à toutes les instances duVPC.

Protocole	Source	Plage de ports	Comment
TCP	*VPC IPv4 CIDR*	22	Autorise le SSH trafic entrant en provenance du VPC

Exemple de règle entrante : préservation de l'adresse IP du client sur

L'exemple suivant autorise le SSH trafic entrant à partir de la plage d'IPv4adresses spécifiée. La préservation de l'adresse IP du client étant activée, l'IPv4adresse source est l'adresse du client.

Protocole	Source	Plage de ports	Comment
TCP	*Public IPv4 address range*	22	Autorise le trafic entrant à partir de la plage d'IPv4adresses client spécifiée

Création d'un point de terminaison EC2 Instance Connect

Vous pouvez créer un point de terminaison EC2 Instance Connect pour permettre une connexion sécurisée à vos instances.

Vous ne pouvez pas modifier un point de terminaison EC2 Instance Connect une fois que vous l'avez créé. Vous devez plutôt supprimer le point de terminaison EC2 Instance Connect et en créer un nouveau avec les paramètres dont vous avez besoin.

Prérequis

Vous devez disposer des IAM autorisations requises pour créer un point de terminaison EC2 Instance Connect. Pour de plus amples informations, veuillez consulter Autorisations pour créer, décrire et supprimer des points de terminaison EC2 Instance Connect.

Sous-réseaux partagés

Vous pouvez créer un point de terminaison EC2 Instance Connect dans un sous-réseau partagé avec vous. Vous ne pouvez pas utiliser un point de terminaison EC2 Instance Connect créé par le VPC propriétaire dans un sous-réseau partagé avec vous.

Créez le point de terminaison à l'aide de la console

Utilisez la procédure suivante pour créer un point de terminaison EC2 Instance Connect.

Pour créer un point de terminaison EC2 Instance Connect

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation de gauche, sélectionnez Points de terminaison.
3. Choisissez Créer un point de terminaison, puis spécifiez les paramètres du point de terminaison comme suit :
   a. (Facultatif) Pour Balise de nom, saisissez un nom pour le point de terminaison.
   b. Pour la catégorie Service, choisissez EC2Instance Connect Endpoint.
   c. Pour VPC, sélectionnez celui VPC qui possède les instances cibles.
   d. (Facultatif) Pour conserver les adresses IP des clients, développez les paramètres supplémentaires et cochez la case. Sinon, l'interface réseau du point de terminaison est utilisée par défaut comme adresse IP du client.
   e. (Facultatif) Pour Groupes de sécurité, sélectionnez le groupe de sécurité à associer au point de terminaison. Dans le cas contraire, le groupe de sécurité par défaut est utilisé pourVPC. Pour de plus amples informations, veuillez consulter Groupes de sécurité pour EC2 Instance Connect Endpoint.
   f. Pour Sous-réseau, sélectionnez le sous-réseau dans lequel créer le point de terminaison.
   g. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
4. Vérifiez vos paramètres, puis choisissez Create endpoint.

   Le statut initial du point de terminaison est En attente. Avant de pouvoir vous connecter à une instance à l'aide de ce point de terminaison, vous devez attendre que l'état du point de terminaison soit disponible. Cette opération peut prendre quelques minutes.
5. Pour vous connecter à une instance à l'aide de votre point de terminaison, consultezConnexion à une instance.

Créez le point de terminaison à l'aide du AWS CLI

Utilisez la create-instance-connect-endpointcommande pour créer un point de terminaison EC2 Instance Connect.

Prérequis

Installez AWS CLI la version 2 et configurez-la à l'aide de vos informations d'identification. Pour plus d'informations, voir Installer ou mettre à jour la dernière version du AWS CLI et Configurer le AWS CLI dans le guide de AWS Command Line Interface l'utilisateur. Vous pouvez également ouvrir AWS CloudShell et exécuter AWS CLI des commandes dans son shell pré-authentifié.

Pour créer le point de terminaison

Utilisez la commande suivante pour créer une interface réseau de point de terminaison pour votre point de terminaison EC2 Instance Connect dans le sous-réseau spécifié.

```
aws ec2 create-instance-connect-endpoint --subnet-id subnet-0123456789example
```

Voici un exemple de sortie.

```
 {
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "create-complete",
        "StateMessage": "",
        "DnsName": "eice-0123456789example.0123abcd.ec2-instance-connect-endpoint.us-
east-1.amazonaws.com",
        "FipsDnsName": "eice-0123456789example.0123abcd.fips.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com",
        "NetworkInterfaceIds": [
            "eni-0123abcd"
        ],
        "VpcId": "vpc-0123abcd",
        "AvailabilityZone": "us-east-1a",
        "CreatedAt": "2023-04-07T15:43:53.000Z",
        "SubnetId": "subnet-0123abcd",
        "PreserveClientIp": false,
        "SecurityGroupIds": [
            "sg-0123abcd"
```

```
        ],
        "Tags": []
}
```

Pour surveiller le statut de création

La valeur initiale du champ `State` est `create-in-progress`. Avant de pouvoir vous connecter à une instance à l'aide de ce point de terminaison, attendez que l'état soit `create-complete`. Utilisez la describe-instance-connect-endpointscommande pour surveiller l'état du point de terminaison EC2 Instance Connect. Le paramètre --query filtre les résultats dans le `State` champ.

```
aws ec2 describe-instance-connect-endpoints --instance-connect-endpoint-
ids eice-0123456789example --query InstanceConnectEndpoints[*].State --output text
```

Voici un exemple de sortie.

```
create-complete
```

Connectez-vous à une EC2 instance Amazon à l'aide d'EC2Instance Connect Endpoint

Vous pouvez utiliser EC2 Instance Connect Endpoint pour vous connecter à une EC2 instance Amazon qui prend en charge SSH ouRDP.

Table des matières

Prérequis

- Vous devez disposer de l'IAMautorisation requise pour vous connecter à un point de terminaison EC2 Instance Connect. Pour de plus amples informations, veuillez consulter Autorisations d'utilisation du point de terminaison EC2 Instance Connect pour se connecter aux instances.
- Le point de terminaison EC2 Instance Connect doit être à l'état Disponible (console) ou `create-complete` (AWS CLI). Si vous ne possédez pas de point de terminaison EC2 Instance Connect pour votre VPC compte, vous pouvez en créer un. Pour de plus amples informations, veuillez consulter Création d'un point de terminaison EC2 Instance Connect.
- Votre instance doit avoir une IPv4 adresse (privée ou publique). EC2Instance Connect Endpoint ne prend pas en charge la connexion aux instances à l'aide d'IPv6adresses.

- (Instances Linux) Pour utiliser la EC2 console pour vous connecter à votre instance, ou pour utiliser la pour vous CLI connecter et laisser EC2 Instance Connect gérer la clé éphémère, Instance EC2 Connect doit être installée sur votre instance. Pour de plus amples informations, veuillez consulter Installez EC2 Instance Connect.
- Assurez-vous que le groupe de sécurité de l'instance autorise le SSH trafic entrant depuis le point de terminaison EC2 Instance Connect. Pour de plus amples informations, veuillez consulter Règles du groupe de sécurité de l'instance cible.

Connectez-vous à votre instance Linux à l'aide de la EC2 console Amazon

Vous pouvez vous connecter à une instance à l'aide de la EC2 console Amazon comme suit.

Pour vous connecter à votre instance à l'aide du client basé sur un navigateur

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance, choisissez Connect.
4. Choisissez l'onglet EC2Instance Connect.
5. Pour le type de connexion, choisissez Connect using EC2 Instance Connect Endpoint.
6. Pour EC2Instance Connect Endpoint, choisissez l'ID du point de terminaison EC2 Instance Connect.
7. Pour Nom d'utilisateur, si celui AMI que vous avez utilisé pour lancer l'instance utilise un nom d'utilisateur autre que`ec2-user`, entrez le nom d'utilisateur correct.
8. Pour Durée maximale du tunnel (secondes), entrez la durée maximale autorisée pour la SSH connexion.

   La durée doit être conforme à toutes les `maxTunnelDuration` conditions spécifiées dans la IAM politique. Si vous n'avez pas accès à la IAM politique, contactez votre administrateur.
9. Choisissez Se connecter. Cela ouvre une fenêtre de terminal pour votre instance.

Connectez-vous à votre instance Linux à l'aide de SSH

Vous pouvez l'utiliser SSH pour vous connecter à votre instance Linux et utiliser la `open-tunnel` commande pour établir un tunnel privé. Vous pouvez utiliser `open-tunnel` en mode connexion unique ou multi-connexion.

Pour plus d'informations sur l'utilisation du AWS CLI pour vous connecter à votre instance à SSH l'aide deConnectez-vous à l'aide du AWS CLI.

Les exemples suivants utilisent Open SSH. Vous pouvez utiliser n'importe quel autre SSH client compatible avec le mode proxy.

Connexion simple

Pour n'autoriser qu'une seule connexion à une instance en utilisant SSH et la **`open-tunnel`** commande

Utilisez `ssh` et la open-tunnel AWS CLI commande comme suit. La commande proxy `-o` contient la commande `open-tunnel` qui crée le tunnel privé vers l'instance.

```
ssh -i my-key-pair.pem ec2-user@i-0123456789example \
    -o ProxyCommand='aws ec2-instance-connect open-tunnel --instance-
id i-0123456789example'
```

Pour :

- `-i` – Spécifie la paire de clés utilisée pour lancer l'instance.
- *`ec2-user`*`@`*`i-0123456789example`*— Spécifiez le nom d'utilisateur utilisé pour lancer l'instance, ainsi AMI que l'ID de l'instance.
- `--instance-id` – Spécifie l'ID de l'instance à laquelle se connecter. Vous pouvez également spécifier `%h`, qui extrait l'ID de l'instance de l'utilisateur.

Multi-connexion

Pour autoriser plusieurs connexions à une instance, exécutez d'abord la open-tunnel AWS CLI commande pour commencer à écouter TCP les nouvelles connexions, puis `ssh` utilisez-la pour créer une nouvelle TCP connexion et un tunnel privé vers votre instance.

Pour autoriser plusieurs connexions à votre instance à l'aide de SSH et de la **`open-tunnel`** commande

1. Exécutez la commande suivante pour commencer à écouter TCP les nouvelles connexions sur le port spécifié de votre machine locale.

   ```
   aws ec2-instance-connect open-tunnel \
       --instance-id i-0123456789example \
   ```

```
    --local-port 8888
```

Sortie attendue

```
Listening for connections on port 8888.
```

2. Dans une nouvelle fenêtre de terminal, exécutez la `ssh` commande suivante pour créer une nouvelle TCP connexion et un tunnel privé vers votre instance.

```
ssh -i my-key-pair.pem ec2-user@localhost -p 8888
```

Résultat attendu : dans la première fenêtre de terminal, vous verrez ce qui suit :

```
[1] Accepted new tcp connection, opening websocket tunnel.
```

Vous pouvez également voir ce qui suit :

```
[1] Closing tcp connection.
```

Connectez-vous à votre instance Linux à l'aide du AWS CLI

Si vous ne connaissez que l'ID de votre instance, vous pouvez utiliser la AWS CLI commande ec2-instance-connect pour vous connecter à votre instance via un client. SSH Pour plus d'informations sur l'utilisation de la commande ec2-instance-connect, consultez. Connectez-vous à l'aide du AWS CLI

Prérequis

Installez AWS CLI la version 2 et configurez-la à l'aide de vos informations d'identification. Pour plus d'informations, voir Installer ou mettre à jour la dernière version du AWS CLI et Configurer le AWS CLI dans le guide de AWS Command Line Interface l'utilisateur. Vous pouvez également ouvrir AWS CloudShell et exécuter AWS CLI des commandes dans son shell pré-authentifié.

Pour vous connecter à une instance à l'aide de l'ID d'instance et d'un point de terminaison EC2 Instance Connect

Si vous ne connaissez que l'ID d'instance, utilisez la CLI commande ec2-instance-connect et spécifiez la `ssh` commande, l'ID d'instance et le `--connection-type` paramètre avec la valeur. `eice`

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --connection-type eice
```

> **Tip**
>
> Si un message d'erreur s'affiche lors de l'utilisation de cette commande, assurez-vous que vous utilisez AWS CLI la version 2. Le `ssh` paramètre n'est disponible que dans AWS CLI la version 2. Pour plus d'informations, consultez la section À propos de AWS CLI la version 2 dans le guide de AWS Command Line Interface l'utilisateur.

Connectez-vous à votre instance Windows à l'aide d'EC2Instance Connect Endpoint

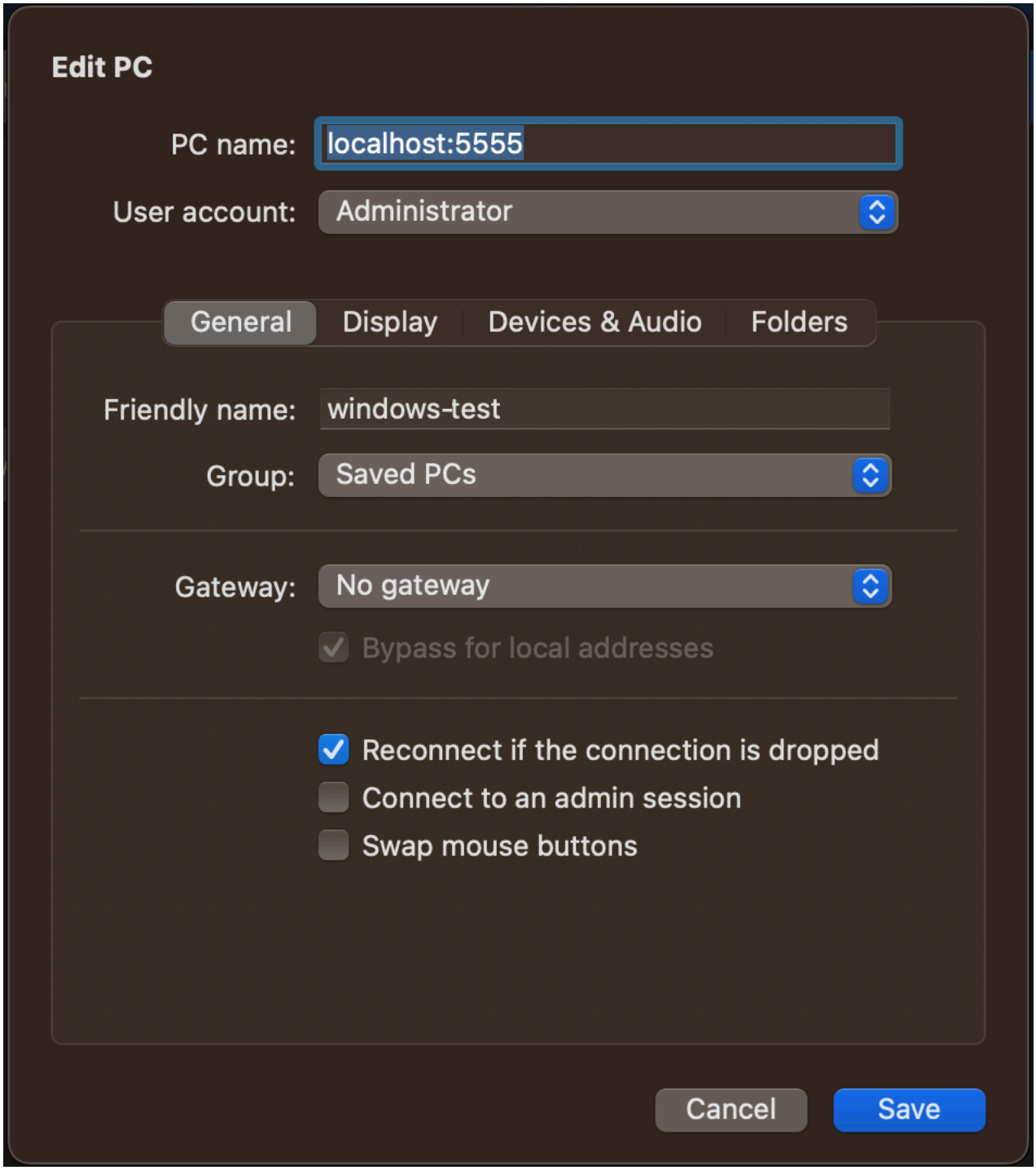
Vous pouvez utiliser le protocole Remote Desktop (RDP) sur EC2 Instance Connect Endpoint pour vous connecter à une instance Windows sans IPv4 adresse publique ni DNS nom public.

Pour vous connecter à votre instance Windows à l'aide d'un RDP client

1. Effectuez les étapes 1 à 8 de Connect to your Windows instance à l'aide deRDP. Après avoir téléchargé le fichier de RDP bureau à l'étape 8, vous recevrez un message Unable to connect, ce qui est normal car votre instance ne possède pas d'adresse IP publique.
2. Exécutez la commande suivante pour établir un tunnel privé vers celui VPC dans lequel se trouve l'instance. `--remote-port`doit être `3389` parce qu'il RDP utilise le port 3389 par défaut.

   ```
   aws ec2-instance-connect open-tunnel \
       --instance-id i-0123456789example \
       --remote-port 3389 \
       --local-port any-port
   ```
3. Dans votre dossier Téléchargements, recherchez le fichier RDP de bureau que vous avez téléchargé et faites-le glisser dans la fenêtre du RDP client.
4. Cliquez avec le bouton droit RDP sur le fichier de bureau et sélectionnez Modifier.
5. Dans la fenêtre Modifier le PC, pour le nom du PC (l'instance à laquelle se connecter), entrez`localhost:local-port`, where *`local-port`* utilise la même valeur que celle que vous avez spécifiée à l'étape 2, puis choisissez Enregistrer.

   Notez que la capture d'écran suivante de la fenêtre Modifier le PC provient de Microsoft Remote Desktop sur Mac. Si vous utilisez un client Windows, la fenêtre peut être différente.



6. Dans le RDP client, cliquez avec le bouton droit sur le PC (que vous venez de configurer) et choisissez Connect pour vous connecter à votre instance.
7. À l'invite, saisissez le mot de passe déchiffré du compte administrateur.

Dépannage

Utilisez les informations suivantes pour diagnostiquer et résoudre les problèmes que vous pourriez rencontrer lors de l'utilisation d'EC2Instance Connect Endpoint pour connecter une instance.

Impossible de se connecter à votre instance

Les raisons les plus courantes pour lesquelles vous ne pouvez pas vous connecter à votre instance sont les suivantes.

- Groupes de sécurité : vérifiez les groupes de sécurité attribués au point de terminaison EC2 Instance Connect et à votre instance. Pour plus d'informations sur les règles de groupe de sécurité requises, consultez Groupes de sécurité pour EC2 Instance Connect Endpoint.
- État de l'instance : vérifiez que l'état de votre instance est `running`.
- Paire de clés : si la commande que vous utilisez pour vous connecter nécessite une clé privée, vérifiez que votre instance possède une clé publique et que vous disposez de la clé privée correspondante.
- IAMautorisations — Vérifiez que vous disposez des IAM autorisations requises. Pour de plus amples informations, veuillez consulter Accorder des autorisations pour utiliser EC2 Instance Connect Endpoint.

Pour plus de conseils de résolution des problèmes relatifs aux instances Linux, consultezRésoudre les problèmes de connexion à votre instance Amazon EC2 Linux. Pour obtenir des conseils de résolution des problèmes relatifs aux instances Windows, consultezthe section called "RDPProblèmes liés aux instances Windows".

ErrorCode: AccessDeniedException

Si vous recevez une `AccessDeniedException` erreur et que la `maxTunnelDuration` condition est spécifiée dans la IAM politique, veillez à spécifier le `--max-tunnel-duration` paramètre lors de la connexion à une instance. Pour plus d'informations sur ce paramètre, consultez open-tunnel dans la Référence de la commande AWS CLI .

Journaliser les connexions établies via EC2 Instance Connect Endpoint

Vous pouvez enregistrer les opérations sur les ressources et auditer les connexions établies via le point de terminaison EC2 Instance Connect à l'aide de AWS CloudTrail journaux.

Pour plus d'informations sur l'utilisation AWS CloudTrail avec AmazonEC2, consultezEnregistrez les EC2 API appels Amazon en utilisant AWS CloudTrail.

Enregistrez les API appels du point de terminaison EC2 Instance Connect avec AWS CloudTrail

EC2Les opérations sur les ressources du point de terminaison Instance Connect sont enregistrées en CloudTrail tant qu'événements de gestion. Lorsque les API appels suivants sont effectués, l'activité est enregistrée en tant qu' CloudTrail événement dans l'historique des événements :

- `CreateInstanceConnectEndpoint`
- `DescribeInstanceConnectEndpoints`
- `DeleteInstanceConnectEndpoint`

Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements dans le Guide de AWS CloudTrail l'utilisateur.

AWS CloudTrail À utiliser pour auditer les utilisateurs qui se connectent à une instance à l'aide d'EC2Instance Connect Endpoint

Les tentatives de connexion aux instances via EC2 Instance Connect Endpoint sont enregistrées CloudTrail dans l'historique des événements. Lorsqu'une connexion à une instance est initiée via un point de terminaison EC2 Instance Connect, la connexion est enregistrée en tant qu'événement de CloudTrail gestion avec le nom `eventName` de`OpenTunnel`.

Vous pouvez créer des EventBridge règles Amazon qui acheminent l' CloudTrail événement vers une cible. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.

Voici un exemple d'événement de `OpenTunnel` gestion connecté CloudTrail.


```
{
     "eventVersion": "1.08",
     "userIdentity": {
         "type": "IAMUser",
         "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
         "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
         "accountId": "123456789012",
         "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
         "userName": "IAM-friendly-name"
```

```
    },
    "eventTime": "2023-04-11T23:50:40Z",
    "eventSource": "ec2-instance-connect.amazonaws.com",
    "eventName": "OpenTunnel",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "1.2.3.4",
    "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
    "requestParameters": {
        "instanceConnectEndpointId": "eici-0123456789EXAMPLE",
        "maxTunnelDuration": "3600",
        "remotePort": "22",
        "privateIpAddress": "10.0.1.1"
    },
    "responseElements": null,
    "requestID": "98deb2c6-3b3a-437c-a680-03c4207b6650",
    "eventID": "bbba272c-8777-43ad-91f6-c4ab1c7f96fd",
    "readOnly": false,
    "resources": [{
        "accountId": "123456789012",
        "type": "AWS::EC2::InstanceConnectEndpoint",
        "ARN": "arn:aws:ec2:us-east-1:123456789012:instance-connect-endpoint/
eici-0123456789EXAMPLE"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


Supprimer un point de terminaison EC2 Instance Connect

Lorsque vous avez terminé d'utiliser un point de terminaison EC2 Instance Connect, vous pouvez le supprimer.

Vous devez disposer des IAM autorisations requises pour créer un point de terminaison EC2 Instance Connect. Pour de plus amples informations, veuillez consulter Autorisations pour créer, décrire et supprimer des points de terminaison EC2 Instance Connect.

Lorsque vous supprimez un point de terminaison EC2 Instance Connect à l'aide de la console, il passe à l'état Suppression. Si la suppression est réussie, le point de terminaison supprimé n'apparaît plus. Si la suppression échoue, l'état est rétabli `delete-failed` et le message d'état indique la raison de l'échec.

Lorsque vous supprimez un point de terminaison EC2 Instance Connect à l'aide du AWS CLI, il passe à l'`delete-in-progress`état. Si la suppression est réussie, elle passe à l'`delete-complete`état. Si la suppression échoue, l'état est rétabli `delete-failed` et `StateMessage` indique la raison de l'échec.

Console

Pour supprimer un point de terminaison EC2 Instance Connect

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation de gauche, sélectionnez Points de terminaison.
3. Sélectionnez le point de terminaison.
4. Choisissez Actions, puis Supprimer les VPC points de terminaison.
5. À l'invite de confirmation, saisissez **`delete`**.
6. Sélectionnez Delete (Supprimer).

AWS CLI

Pour supprimer un point de terminaison EC2 Instance Connect

Utilisez la delete-instance-connect-endpoint AWS CLI commande et spécifiez l'ID du point de terminaison EC2 Instance Connect à supprimer.

```
aws ec2 delete-instance-connect-endpoint --instance-connect-endpoint-
id eice-03f5e49b83924bbc7
```

Voici un exemple de sortie.

```
{
    "InstanceConnectEndpoint": {
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "delete-in-progress",
        "StateMessage": "",
        "NetworkInterfaceIds": [],
        "VpcId": "vpc-0123abcd",
        "AvailabilityZone": "us-east-1d",
        "CreatedAt": "2023-02-07T12:05:37+00:00",
```

```
        "SubnetId": "subnet-0123abcd"
    }
}
```

Rôle lié à un service pour Instance EC2 Connect Endpoint

Amazon EC2 utilise AWS Identity and Access Management (IAM) des rôles liés à un service. Un rôle lié à un service est un type unique de IAM rôle directement lié à Amazon. EC2 Les rôles liés aux services sont prédéfinis par Amazon EC2 et incluent toutes les autorisations requises pour qu'Amazon EC2 puisse appeler d'autres personnes en votre services AWS nom. Pour plus d'informations, consultez la section Rôles liés aux services dans le Guide de l'IAMutilisateur.

Autorisations de rôle liées au service pour Instance EC2 Connect Endpoint

Amazon EC2 les utilise AWSServiceRoleForEC2InstanceConnectpour créer et gérer les interfaces réseau de votre compte qui sont requises par EC2 Instance Connect Endpoint.

Le rôle AWSServiceRoleForEC2InstanceConnectlié à un service fait confiance aux services suivants pour assumer le rôle :

- `ec2-instance-connect.amazonaws.com`

Le rôle AWSServiceRoleForEC2InstanceConnectlié à un service utilise la politique gérée Ec2. InstanceConnectEndpoint Pour consulter les autorisations associées à cette politique, consultez Ec2 InstanceConnectEndpoint dans le manuel AWS Managed Policy Reference.

Vous devez configurer les autorisations pour autoriser une IAM entité (telle qu'un utilisateur, un groupe ou un rôle) à créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez la section Autorisations relatives aux rôles liés à un service dans le Guide de l'IAMutilisateur.

Création d'un rôle lié à un service pour Instance EC2 Connect Endpoint

Vous n'avez pas besoin de créer manuellement un rôle lié au service . Lorsque vous créez un point de terminaison EC2 Instance Connect, Amazon EC2 crée le rôle lié au service pour vous.

Modifier un rôle lié à un service pour Instance EC2 Connect Endpoint

EC2Instance Connect Endpoint ne vous permet pas de modifier le rôle AWSServiceRoleForEC2InstanceConnectlié au service.

Supprimer un rôle lié à un service pour Instance EC2 Connect Endpoint

Si vous n'avez plus besoin d'utiliser EC2 Instance Connect Endpoint, nous vous recommandons de supprimer le rôle AWSServiceRoleForEC2InstanceConnectlié au service.

Vous devez supprimer toutes les ressources du point de terminaison EC2 Instance Connect avant de pouvoir supprimer le rôle lié à un service.

Pour supprimer le rôle lié à un service, voir Supprimer un rôle lié à un service dans le Guide de l'utilisateur. IAM

Quotas pour EC2 Instance Connect Endpoint

Vous Compte AWS disposez de quotas par défaut, anciennement appelés limites, pour chaque AWS service. Sauf indication contraire, chaque quota est spécifique à la région.

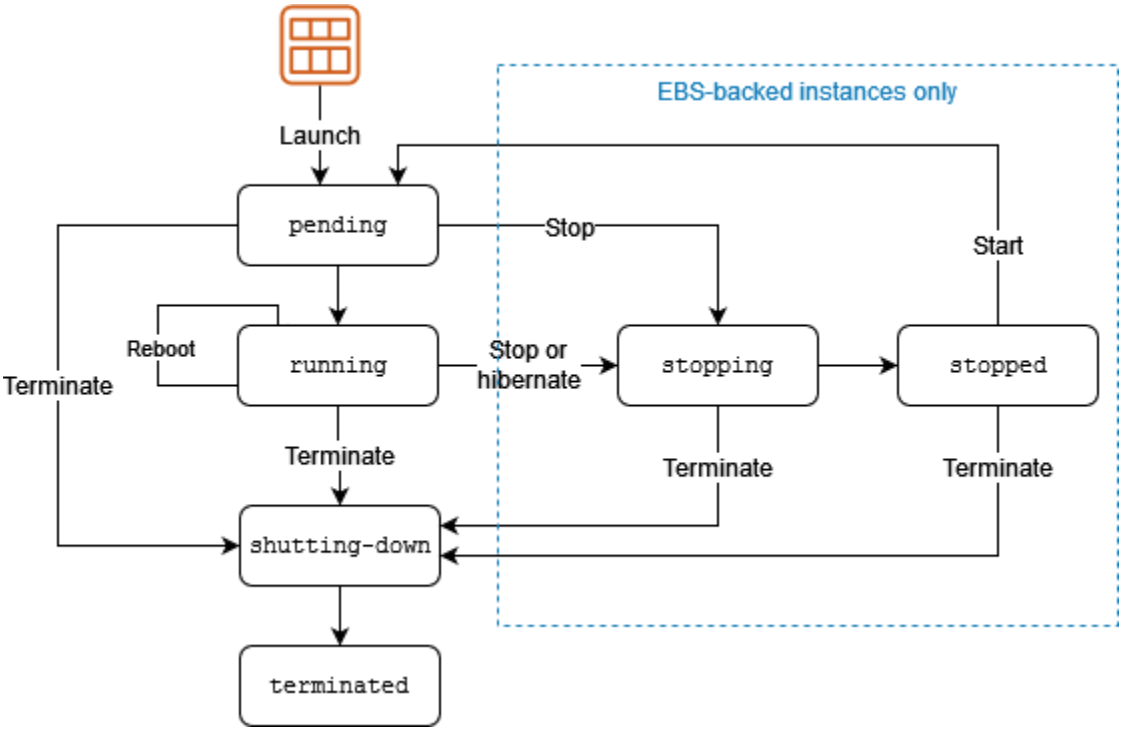
Vous Compte AWS disposez des quotas suivants relatifs à EC2 Instance Connect Endpoint.

Nom	Par défaut	Ajustable
Nombre maximal de points de terminaison EC2 Instance Connect par personne Compte AWS Région AWS	5	Non
Nombre maximal de points de terminaison EC2 Instance Connect par VPC	1	Non
Nombre maximal de points de terminaison EC2 Instance Connect par sous-réseau	1	Non
Nombre maximal de connexions simultanées par point de terminaison EC2 Instance Connect	20	Non

Modifications de l'état de l'EC2instance Amazon

Une EC2 instance Amazon passe par différents états entre le moment où vous la lancez et son arrêt.

L'illustration suivante représente les transitions entre les états de l'instance.



Vous pouvez recevoir des notifications lorsque vos instances changent d'état. Pour de plus amples informations, veuillez consulter the section called "Événements de changement d'état".

Facturation par état de l'instance

Le tableau suivant fournit une brève description de l'état de chaque instance et indique si l'utilisation de l'instance est facturée. Certaines AWS ressources, telles que les EBS volumes Amazon et les adresses IP Elastic, sont facturées quel que soit l'état de l'instance. Pour plus d'informations, consultez Éviter les frais inattendus dans le Guide de l'utilisateur AWS Billing .

État de l'instance	Description	Facturation de l'utilisation de l'instance
`pending`	L'instance se prépare à passer à l'état `running`. Une instance passe à l'état `pending` lorsqu'elle est lancée ou lorsqu'elle est démarrée après avoir été à l'état `stopped`.	Non facturé

État de l'instance	Description	Facturation de l'utilisation de l'instance
`running`	L'instance est en cours d'exécution et prête à être utilisée.	Facturé
`stopping`	L'instance se prépare à être arrêtée.	Non facturé **Note** Si vous mettez une instance en veille prolongée , vous êtes facturé tant que l'instance est dans l'état. `stopping`
`stopped`	L'instance est arrêtée et ne peut pas être utilisée. L'instance peut être démarrée à tout moment.	Non facturé
`shutting-down`	L'instance se prépare à être supprimée.	Non facturé
`terminated`	L'instance a été définitivement supprimée et ne peut pas être démarrée.	Non facturé **Note** Les instances réservées appliquées aux instances résiliées sont facturées jusqu'à la fin de leur période de validité, selon l'option de paiement. Pour plus d'informations, consultez EC2Présentation des instances réservées pour Amazon.

Instances en attente

Lorsque vous lancez une instance, elle entre dans l'état `pending`. Le type d'instance que vous avez spécifié au lancement détermine les capacités matérielles de l'ordinateur hôte de votre instance. Nous utilisons l'Amazon Machine Image (AMI) que vous avez spécifiée au lancement pour démarrer l'instance. Une fois que l'instance est prête, elle entre dans l'état `running`. Vous pouvez vous connecter à votre instance en cours d'exécution et l'utiliser comme vous le feriez d'un ordinateur devant lequel vous êtes assis.

Dès que votre instance passe à l'état `running`, vous êtes facturé pour chaque seconde d'exécution de l'instance, avec un minimum d'une minute, même si l'instance demeure inactive et que vous ne vous y connectez pas.

Instances arrêtées

Si votre instance échoue à une vérification de statut ou n'exécute pas vos applications comme prévu, et si le volume racine de votre instance est un EBS volume Amazon, vous pouvez arrêter et démarrer votre instance pour essayer de résoudre le problème.

Lorsque vous arrêtez votre instance, elle entre dans l'état `stopping`, puis dans l'état `stopped`. Aucuns frais d'utilisation ou de transfert de données ne vous sont facturés pour votre instance lorsqu'elle est `stopped`. Des frais sont facturés pour le stockage de tous les EBS volumes Amazon. Lorsque votre instance se trouve dans l'état `stopped`, vous pouvez modifier certains attributs de l'instance, y compris le type d'instance.

Lorsque vous démarrez votre instance, elle passe à l'état `pending` et elle est déplacée vers un nouvel ordinateur hôte (même si, dans la plupart des cas, elle reste sur l'hôte actuel). Lorsque vous arrêtez et démarrez votre instance, vous perdez toutes les données des volumes de stockage d'instances attachés à l'ordinateur hôte précédent.

Votre instance conserve son IPv4 adresse privée, ce qui signifie qu'une adresse IP élastique associée à l'IPv4adresse privée ou à l'interface réseau reste associée à votre instance. Si votre instance possède une IPv6 adresse, elle la IPv6 conserve.

Chaque fois que vous opérez la transition d'une instance de l'état `stopped` à l'état `running`, vous êtes facturé par seconde d'exécution de l'instance, avec un minimum d'une minute par instance démarrée.

Pour plus d'informations sur l'arrêt et le redémarrage d'une instance, consultez Arrêtez et démarrez les EC2 instances Amazon.

Instances mises en veille prolongée

Lorsque vous mettez une instance en veille prolongée, nous signalons au système d'exploitation d'exécuter hibernation (suspend-to-disk), qui enregistre le contenu de la mémoire de l'instance (RAM) sur votre volume racine AmazonEBS. Nous conservons le volume EBS racine Amazon de l'instance et tous les volumes de EBS données Amazon attachés. Lorsque vous démarrez votre instance, le volume EBS racine Amazon est restauré dans son état antérieur et son RAM contenu est rechargé. Les volumes de données précédemment attachés sont attachés à nouveau et l'instance conserve son ID d'instance.

Lorsque vous mettez votre instance en veille prolongée, elle entre dans l'état `stopping`, puis dans l'état `stopped`. Nous ne facturons pas l'utilisation d'une instance en veille prolongée à l'état `stopped`, mais nous la facturons quand elle est à l'état `stopping`, contrairement à ce qui se produit quand vous arrêtez une instance sans la mettre en veille prolongée. Nous ne facturons pas d'utilisation pour les frais de transfert de données, mais nous facturons le stockage de tous les EBS volumes Amazon, y compris le stockage des RAM données.

Lorsque vous démarrez votre instance mise en veille prolongée, elle passe à l'état `pending` et nous déplaçons l'instance vers un nouvel ordinateur hôte (même si, dans la plupart des cas, elle reste sur l'hôte actuel).

Votre instance conserve son IPv4 adresse privée, ce qui signifie qu'une adresse IP élastique associée à l'IPv4adresse privée ou à l'interface réseau est toujours associée à votre instance. Si votre instance possède une IPv6 adresse, elle la conserveIPv6.

Pour de plus amples informations, veuillez consulter Hibernez votre instance Amazon EC2.

Redémarrage d'instances

Vous pouvez redémarrer votre instance à l'aide de la EC2 console Amazon, d'un outil de ligne de commande et d'Amazon EC2API. Nous vous recommandons d'utiliser Amazon EC2 pour redémarrer votre instance au lieu d'exécuter la commande de redémarrage du système d'exploitation depuis votre instance.

Le redémarrage d'une instance est similaire à celui d'un système d'exploitation. L'instance reste sur le même ordinateur hôte et conserve son DNS nom public, son adresse IP privée et toutes les données présentes sur ses volumes de stockage d'instance. Le redémarrage nécessite généralement quelques minutes pour s'exécuter, mais le temps réel dépend de la configuration de l'instance.

Le redémarrage d'une instance ne déclenche pas de nouvelle période de facturation ; la facturation par seconde se poursuit, sans frais minimum d'une minute.

Pour de plus amples informations, veuillez consulter Redémarrer votre instance.

Instances résiliées

Si vous jugez que vous n'avez plus besoin d'une instance, vous pouvez la mettre hors service. Dès que l'état d'une instance passe à `shutting-down` ou `terminated`, l'instance ne vous est plus facturée.

Si vous activez la protection contre la résiliation, vous ne pouvez pas mettre fin à l'instance à l'aide de la consoleCLI, ouAPI.

Une fois que vous avez mis une instance hors service, elle demeure visible sur la console pendant un court instant, puis l'entrée est supprimée automatiquement. Vous pouvez également décrire une instance interrompue à l'aide du CLI etAPI. Les ressources (telles que les balises) sont progressivement dissociées de l'instance résiliées. Par conséquent, elles ne seront plus visibles dans l'instance terminée après un certain temps. Vous ne pouvez pas vous connecter à une instance terminée, ni la récupérer.

Chaque instance EBS soutenue par Amazon prend en charge l'`InstanceInitiatedShutdownBehavior`attribut, qui contrôle si l'instance s'arrête ou se termine lorsque vous lancez l'arrêt depuis l'instance elle-même (par exemple, en utilisant la shutdown commande sous Linux). Le comportement par défaut est celui de l'arrêt de l'instance. Vous pouvez modifier la valeur de cet attribut tandis que l'instance est en cours d'exécution ou arrêtée.

Chaque EBS volume Amazon prend en charge l'`DeleteOnTermination`attribut, qui détermine si le volume est supprimé ou préservé lorsque vous mettez fin à l'instance à laquelle il est attaché. Par défaut, le volume du périphérique racine est supprimé et les autres EBS volumes sont conservés.

Pour de plus amples informations, veuillez consulter Mettre fin aux EC2 instances Amazon.

Différences entre les états des instances

Le tableau suivant résume les principales différences entre le redémarrage, l'arrêt, la mise en veille prolongée et la résiliation d'une instance.

Caractéristiques	Redémarrer	Arrêter/démarrer (instances EBS soutenues par Amazon uniquement)	Hibernate (instances basées sur Amazon EBS uniquement)	Terminer
Ordinateur hôte	L'instance demeure sur le même ordinateur hôte.	Nous déplaçons l'instance vers un nouvel ordinateur hôte (même si, dans certains cas, elle reste sur l'hôte actuel).	Nous déplaçons l'instance vers un nouvel ordinateur hôte (même si, dans certains cas, elle reste sur l'hôte actuel).	Aucun
IPv4Adresses privées et publiques	Ces adresses demeurent identiques.	L'instance conserve son IPv4 adresse privée. L'instance obtient une nouvelle IPv4 adresse publique, sauf si elle possède une adresse IP élastique, qui ne change pas lors d'un arrêt/démarrage.	L'instance conserve son IPv4 adresse privée. L'instance obtient une nouvelle IPv4 adresse publique, sauf si elle possède une adresse IP élastique, qui ne change pas lors d'un arrêt/démarrage.	Aucun
Adresses IP élastiques (IPv4)	L'adresse IP Elastic reste associée à l'instance	L'adresse IP Elastic reste associée à l'instance	L'adresse IP Elastic reste associée à l'instance	L'adresse IP Elastic est dissociée de l'instance.
IPv6adresse	L'instance conserve son IPv6 adresse	L'instance conserve son IPv6 adresse	L'instance conserve son IPv6 adresse	Aucun

Caractéristiques	Redémarrer	Arrêter/démarrer (instances EBS soutenues par Amazon uniquement)	Hibernate (instances basées sur Amazon EBS uniquement)	Terminer
Volumes de stockage d'instances	Les données sont conservées.	Les données sont effacées.	Les données sont effacées.	Les données sont effacées.
volume du périphérique racine	Le volume est conservé	Le volume est conservé	Le volume est conservé	Le volume est supprimé par défaut.
RAM(contenu de la mémoire)	Le RAM est effacé	Le RAM est effacé	Le RAM est enregistré dans un fichier sur le volume racine	Le RAM est effacé

Caractéristiques	Redémarrer	Arrêter/démarrer (instances EBS soutenues par Amazon uniquement)	Hibernate (instances basées sur Amazon EBS uniquement)	Terminer
Facturation	L'heure de facturation de l'instance ne change pas	Vous cessez d'être facturé aussitôt que l'état d'une instance devient `stopping`. Chaque fois qu'une instance passe de l'état `stopped` à l'état `running`, nous commençons une nouvelle période de facturation, en facturant un minimum d'une minute à chaque démarrage de l'instance.	Des frais vous sont facturés lorsque l'instance est à l'état `stopping`, mais ne le sont plus lorsque l'instance passe à l'état `stopped`. Chaque fois qu'une instance passe de l'état `stopped` à l'état `running`, nous commençons une nouvelle période de facturation, en facturant un minimum d'une minute à chaque démarrage de l'instance.	Vous arrêtez de payer des frais pour une instance dès que son état passe à `shutting-down`

Les commandes d'arrêt du système d'exploitation terminent toujours une instance basée sur le stockage d'instances. Vous pouvez contrôler si les commandes d'arrêt du système d'exploitation arrêtent ou mettent fin à une instance EBS basée sur Amazon. Pour de plus amples informations, veuillez consulter Modifier le comportement d'arrêt lancé de l'instance.

Arrêtez et démarrez les EC2 instances Amazon

Vous pouvez arrêter et démarrer votre instance si elle possède un EBS volume Amazon comme périphérique racine. Lorsque vous arrêtez une instance, elle s'arrête. Lorsque vous démarrez une

instance, celle-ci est généralement migrée vers un nouvel ordinateur hôte sous-jacent et une nouvelle IPv4 adresse publique lui est attribuée.

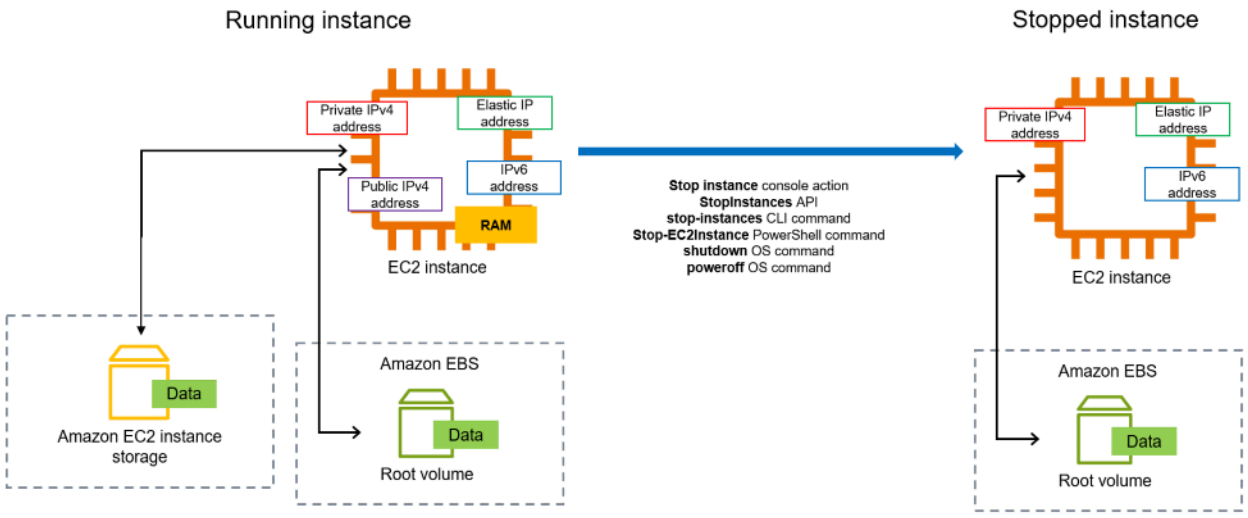
Lorsque vous arrêtez une instance, elle n'est pas supprimée. Si vous jugez que vous n'avez plus besoin d'une instance, vous pouvez y mettre fin. Pour de plus amples informations, veuillez consulter Mettre fin aux EC2 instances Amazon. Si vous souhaitez mettre une instance en veille prolongée pour enregistrer le contenu de la mémoire d'instance (RAM), consultez. Hibernez votre instance Amazon EC2 Pour connaître les différences entre les actions du cycle de vie des instances, consultez Différences entre les états des instances.

Table des matières

Fonctionnement de l'arrêt et du démarrage d'une EC2 instance

Lorsque vous arrêtez une instance, les modifications sont enregistrées au niveau du système d'exploitation de l'instance, certaines ressources sont perdues et certaines ressources persistent. Lorsque vous démarrez une instance, les modifications sont enregistrées au niveau de l'instance.

Le schéma suivant montre ce qui est perdu et ce qui persiste lorsqu'une EC2 instance Amazon est arrêtée. Lorsqu'une instance s'arrête, elle perd tous les volumes de stockage d'instance attachés et les données stockées sur ces volumes, les données stockées sur l'instance RAM et l'IPv4adresse publique attribuée si aucune adresse IP élastique n'est associée à l'instance. Une instance conserve les IPv4 adresses privées attribuées, les adresses IP élastiques associées à l'instance, toutes IPv6 les adresses, ainsi que tous les EBS volumes Amazon attachés et les données qu'ils contiennent.



Ce qui se passe lorsque vous arrêtez une instance

Modifications enregistrées au niveau du système d'exploitation

- La API demande envoie un événement d'appui sur un bouton à l'invité.
- Divers services système sont arrêtés à la suite de l'événement d'appui sur le bouton. L'arrêt progressif est déclenché par le fait que l'hyperviseur appuie sur le bouton d'ACPIarrêt.
- ACPIl'arrêt est lancé.
- L'instance s'arrête lorsque le processus d'arrêt normal se termine. L'heure d'arrêt du système d'exploitation n'est pas configurable.
- Si le système d'exploitation d'instance ne s'arrête pas proprement en quelques minutes, un arrêt dur est effectué.
- L'instance cesse de s'exécuter.
- L'état de l'instance devient `stopping`, puis `stopped`.
- [Auto Scaling] Si votre instance fait partie d'un groupe Auto Scaling, si elle se trouve dans un EC2 état Amazon autre que celui d'Amazon`running`, ou si son statut pour les vérifications de statut devient le cas`impaired`, Amazon EC2 Auto Scaling considère que l'instance n'est pas saine et la remplace. Pour plus d'informations, consultez la section Health checks for Auto Scaling instances dans le manuel Amazon EC2 Auto Scaling User Guide.
- [Instances Windows] Lorsque vous arrêtez et démarrez une instance Windows, l'agent de lancement exécute des tâches sur l'instance, telles que la modification des lettres du lecteur pour tous les EBS volumes Amazon attachés. Pour plus d'informations sur ces valeurs par défaut et sur la manière dont vous pouvez les modifier, consultezthe section called "EC2Launch v2".

Ressources perdues

- Données stockées sur leRAM.
- Les données stockées sur les volumes de stockage d'instances.
- IPv4Adresse publique qu'Amazon a EC2 automatiquement attribuée à l'instance lors du lancement ou du démarrage. Pour conserver une IPv4 adresse publique qui ne change jamais, vous pouvez associer une adresse IP élastique à votre instance.

Des ressources qui persistent

- Tous les EBS volumes Amazon joints.
- Données stockées sur les EBS volumes Amazon joints.
- IPv4Adresses privées.
- IPv6adresses.
- Les adresses IP élastiques associées à l'instance. Veuillez noter que lorsque l'instance est arrêtée, nous commençons à vous facturer les adresses IP Elastic associées.

Pour plus d'informations sur ce qui se passe lorsque vous arrêtez une instance Mac, consultezArrêtez ou mettez fin à votre instance Amazon EC2 Mac.

Ce qui se passe lorsque vous lancer une instance

Modifications enregistrées au niveau du système d'exploitation

- L'instance est généralement migrée vers un nouvel ordinateur hôte sous-jacent (même si, dans certains cas, comme lorsqu'une instance est allouée à un hôte dans une configuration Hôte dédié, elle reste sur l'hôte actuel).
- Amazon EC2 attribue une nouvelle IPv4 adresse publique à l'instance si celle-ci est configurée pour recevoir une IPv4 adresse publique. Pour conserver une IPv4 adresse publique qui ne change jamais, vous pouvez associer une adresse IP élastique à votre instance.

Tester la réponse de l'application pour l'arrêt et le démarrage

Vous pouvez l'utiliser AWS Fault Injection Service pour tester la façon dont votre application répond lorsque votre instance est arrêtée et démarrée. Pour plus d'informations, consultez le AWS Fault Injection Service Guide de l'utilisateur .

Coûts liés à l'arrêt et au démarrage de l'instance

Les coûts suivants sont associés à l'arrêt et au démarrage d'une instance.

Arrêt : dès que l'état d'une instance passe à `shutting-down` ou `terminated`, l'instance ne vous est plus facturée. Aucuns frais d'utilisation ou de transfert de données ne vous sont facturés pour une instance arrêtée. Des frais sont facturés pour stocker les volumes EBS de stockage Amazon.

Démarrage : chaque fois que vous démarrez une instance arrêtée, nous facturons au minimum une minute d'utilisation. Après une minute, seules les secondes que vous utilisez vous sont facturées. Si, par exemple, vous exécutez une instance pendant 20 secondes, puis que vous l'arrêtez, nous vous facturons une minute complète. Si vous exécutez une instance pendant 3 minutes et 40 secondes, nous vous facturons exactement 3 minutes et 40 secondes d'utilisation.

Arrêtez et démarrez manuellement vos instances

Vous pouvez arrêter et démarrer vos instances EBS soutenues par Amazon (instances dotées d'appareils EBS root). Vous ne pouvez pas arrêter et démarrer des instances avec le périphérique racine du stockage d'instance.

> **Warning**
>
> Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Avant d'arrêter une instance, vérifiez que vous avez copié toutes les données dont vous avez besoin depuis les volumes de stockage de l'instance vers un stockage persistant, tel qu'Amazon EBS ou Amazon S3.

Console

Pour arrêter et démarrer une instance basée sur Amazon EBS

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation de gauche, choisissez Instances, puis sélectionnez l'instance.
3. Dans l'onglet Stockage, vérifiez que le type de périphérique racine est EBS. Dans le cas contraire, vous ne pouvez pas arrêter l'instance.
4. Choisissez État de l'instance, Arrêter l'instance. Si cette option est désactivée, l'instance est déjà arrêtée ou son périphérique racine est un volume de stockage d'instances.

5. Lorsque vous êtes invité à confirmer l'opération, choisissez Arrêter. L'arrêt de l'instance peut prendre quelques minutes.
6. Pour démarrer une instance arrêtée, sélectionnez l'instance et choisissez État de l'instance, Démarrer l'instance.
7. Il peut s'écouler quelques minutes avant que l'instance ne passe à l'état `running`.
8. Si vous avez arrêté une instance EBS basée sur Amazon et qu'elle semble « bloquée » dans son `stopping` état, vous pouvez l'arrêter de force. Pour de plus amples informations, veuillez consulter Résoudre les problèmes d'arrêt des EC2 instances Amazon.

Command line

Prérequis

Vérifiez que le périphérique racine de l'instance est un EBS volume. Par exemple, exécutez la AWS CLI commande describe-instances et vérifiez que ce `RootDeviceType` n'est `ebs` pas le cas. `instance-store`

Pour arrêter et démarrer une instance basée sur Amazon EBS

Utilisez l'une des commandes suivantes :

- AWS CLI : stop-instances et start-instances.
- AWS Tools for PowerShell— Stop-EC2Instanceet Start-EC2Instance.
- Commandes du système d'exploitation : vous pouvez lancer un arrêt à l'aide des commandes shutdown ou poweroff. Lorsque vous utilisez une commande du système d'exploitation, l'instance s'arrête par défaut. Vous pouvez modifier ce comportement pour que l'instance prenne fin. Pour de plus amples informations, veuillez consulter Modifier le comportement d'arrêt lancé de l'instance.

[Instances Linux] L'utilisation de la halt commande du système d'exploitation depuis une instance ne déclenche pas d'arrêt. Si vous utilisez la halt commande, l'instance ne s'arrête pas ; au lieu de cela, elle place le CPU dans`HLT`, ce qui suspend le CPU fonctionnement. L'instance reste en cours d'exécution.

Arrêter et démarrer automatiquement vos instances

Vous pouvez automatiser l'arrêt et le démarrage de vos instances à l'aide des services suivants :

Planificateur d'instance activé AWS

Vous pouvez utiliser Instance Scheduler activé AWS pour automatiser le démarrage et l'arrêt des EC2 instances. Pour plus d'informations, consultez Comment utiliser le planificateur d'instances CloudFormation pour planifier EC2 des instances ? Notez que des frais supplémentaires sont facturés.

AWS Lambda et une EventBridge règle Amazon

Vous pouvez utiliser Lambda et une EventBridge règle pour arrêter et démarrer vos instances selon un calendrier. Pour plus d'informations, consultez Comment utiliser Lambda pour arrêter et démarrer des EC2 instances Amazon à intervalles réguliers ?

Amazon EC2 Auto Scaling

Pour vous assurer de disposer du nombre correct d'EC2instances Amazon disponibles pour gérer la charge d'une application, créez des groupes Auto Scaling. Amazon EC2 Auto Scaling garantit que votre application dispose toujours de la capacité nécessaire pour répondre à la demande de trafic et réduit les coûts en lançant des instances uniquement lorsqu'elles sont nécessaires. Veuillez noter que Amazon EC2 Auto Scaling résilie les instances inutiles plutôt que de les arrêter. Pour configurer des groupes Auto Scaling, consultez Get started with Amazon EC2 Auto Scaling.

Trouver toutes les instances en cours d'exécution et arrêtées

Vous pouvez trouver toutes vos instances en cours d'exécution et arrêtées Régions AWS sur une seule page à l'aide d'Amazon EC2 Global View. Cette capacité est particulièrement utile pour faire l'inventaire et rechercher les instances oubliées. Pour plus d'informations sur l'utilisation de Global View, consultez Afficher les ressources de différentes régions à l'aide d'Amazon EC2 Global View.

Activez la protection anti-arrêt pour vos EC2 instances

Pour éviter qu'une instance ne soit arrêtée accidentellement, vous pouvez activer la protection contre l'arrêt de l'instance. La protection contre l'arrêt protège également votre instance contre la résiliation accidentelle.

L'`DisableApiStop`attribut Amazon EC2 `ModifyInstanceAttribute`APIdétermine si l'instance peut être arrêtée à l'aide de la EC2 console Amazon AWS CLI, du ou de l'Amazon EC2API. Vous pouvez définir la valeur de cet attribut lorsque vous lancez l'instance, pendant l'exécution de l'instance ou une fois l'instance arrêtée.

Considérations

- L'activation de la protection contre les arrêts ne vous empêche pas d'arrêter accidentellement une instance en déclenchant un arrêt à partir de l'instance à l'aide d'une commande du système d'exploitation telle que shutdown ou poweroff.
- L'activation de la protection d'arrêt n' AWS empêche pas l'arrêt de l'instance lorsqu'un événement planifié est prévu pour arrêter l'instance.
- L'activation de la protection d'arrêt n'empêche pas Amazon EC2 Auto Scaling de mettre fin à une instance lorsque celle-ci est défectueuse ou lors d'événements de montée en puissance. Vous pouvez contrôler si un groupe Auto Scaling peut résilier une instance en particulier lors de la diminution de la taille en utilisant la protection contre la diminution de la taille d'instance.
- La protection anti-arrêt empêche non seulement l'arrêt accidentel de votre instance, mais également son arrêt accidentel lors de l'utilisation de la console AWS CLI, ouAPI. Cependant, cela ne définit pas automatiquement l'attribut `DisableApiTermination`. Notez que lorsque l'`DisableApiStop`attribut est défini sur`false`, le paramètre `DisableApiTermination` d'attribut détermine si l'instance peut être interrompue à l'aide de la console AWS CLI, ouAPI. Pour plus d'informations, voir Mettre fin aux EC2 instances Amazon.
- Vous ne pouvez pas activer la protection contre l'arrêt pour les instances basées sur le stockage d'instances.
- Vous ne pouvez pas activer la protection contre l'arrêt pour les instances Spot.
- Amazon EC2 API suit un modèle de cohérence final lorsque vous activez ou désactivez la protection anti-arrêt. Cela signifie que le résultat de l'exécution de commandes pour définir l'attribut de protection contre l'arrêt peut ne pas être immédiatement visible pour toutes les commandes suivantes que vous exécuterez. Pour plus d'informations, consultez la section Cohérence éventuelle dans le manuel Amazon EC2 Developer Guide.

Tâches de la protection contre l'arrêt

- Activer la protection contre l'arrêt d'une instance lors du lancement
- Activer la protection contre l'arrêt d'une instance en cours d'exécution ou arrêtée
- Désactivez la protection contre l'arrêt d'une instance en cours d'exécution ou arrêtée

Activer la protection contre l'arrêt d'une instance lors du lancement

Vous pouvez activer la protection contre l'arrêt d'une instance lors du lancement d'instance à l'aide d'une des méthodes suivantes.

Console

Pour activer la protection contre l'arrêt d'une instance lors du lancement

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Sur le tableau de bord, choisissez Lancer une instance.
3. Configurez votre instance dans le nouvel assistant de lancement d'instance.
4. Dans l'assistant, activez la protection contre l'arrêt en choisissant Activer pour Protection contre l'arrêt sous Détails avancés.

AWS CLI

Pour activer la protection contre l'arrêt d'une instance lors du lancement

Utilisez la AWS CLI commande run-instances pour lancer l'instance et spécifiez le `disable-api-stop` paramètre.

```
aws ec2 run-instances \
    --image-id ami-a1b2c3d4e5example \
    --instance-type t3.micro \
    --key-name MyKeyPair \
    --disable-api-stop \
    ...
```

Activer la protection contre l'arrêt d'une instance en cours d'exécution ou arrêtée

Vous pouvez activer la protection contre l'arrêt d'une instance lorsque l'instance est en cours d'exécution ou est arrêtée à l'aide d'une des méthodes suivantes.

Console

Pour activer la protection contre l'arrêt d'une instance en cours d'exécution ou arrêtée

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation de gauche, sélectionnez Instances.
3. Sélectionnez l'instance, puis cliquez sur Actions>Paramètres de l'instance>Modifier la protection contre l'arrêt.
4. Cochez la case Enable (Activer), puis choisissez Save (Enregistrer).

AWS CLI

Pour activer la protection contre l'arrêt d'une instance en cours d'exécution ou arrêtée

Utilisez la modify-instance-attribute AWS CLI commande et spécifiez le `disable-api-stop` paramètre.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --disable-api-stop
```

Désactivez la protection contre l'arrêt d'une instance en cours d'exécution ou arrêtée

Vous pouvez désactiver la protection contre l'arrêt d'une instance pour une instance en cours d'exécution ou arrêtée à l'aide d'une des méthodes suivantes.

Console

Pour désactiver la protection contre l'arrêt d'une instance en cours d'exécution ou arrêtée

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation de gauche, sélectionnez Instances.
3. Sélectionnez l'instance, puis cliquez sur Actions, Instance Settings (Paramètres de l'instance) et Change stop protection (Modifier la protection contre l'arrêt).
4. Décochez la case Enable (Activer), puis choisissez Save (Enregistrer).

AWS CLI

Pour désactiver la protection contre l'arrêt d'une instance en cours d'exécution ou arrêtée

Utilisez la modify-instance-attribute AWS CLI commande et spécifiez le `no-disable-api-stop` paramètre.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --no-disable-api-stop
```

Hibernez votre instance Amazon EC2

Lorsque vous mettez une instance en veille prolongée, Amazon EC2 indique au système d'exploitation de procéder à l'hibernation (). suspend-to-disk Hibernation enregistre le contenu de la mémoire d'instance (RAM) sur votre volume racine Amazon Elastic Block Store (AmazonEBS). Amazon EC2 conserve le volume EBS racine de l'instance et tous les volumes de EBS données associés. Lorsque votre instance est démarrée :

- Le volume EBS racine est restauré à son état précédent
- Le RAM contenu est rechargé
- Les processus qui s'exécutaient précédemment sur l'instance reprennent.
- Les volumes de données précédemment attachés sont attachés à nouveau et l'instance conserve son ID d'instance.

Vous pouvez mettre une instance en veille prolongée uniquement si celle-ci est activée pour la mise en veille prolongée et si elle répond aux prérequis de mise en veille prolongée.

Si les actions d'amorçage d'une instance ou d'une application et de création d'une empreinte mémoire afin de devenir complètement productive prennent du temps, vous pouvez utiliser la mise en veille prolongée pour préchauffer l'instance. Pour préchauffer l'instance, vous :

1. La lancez avec la mise en veille prolongée activée.
2. La placez dans l'état souhaité.
3. Mettez-la en veille prolongée afin qu'elle soit prête à reprendre à l'état désiré lorsque cela est nécessaire.

Vous n'êtes pas facturé pour l'utilisation d'une instance en veille prolongée lorsqu'elle est en `stopped` état ou pour le transfert de données lorsque le contenu de l'instance est transféré vers le volume EBS racine. RAM Le stockage de tous les EBS volumes, y compris le stockage du RAM contenu, vous est facturé.

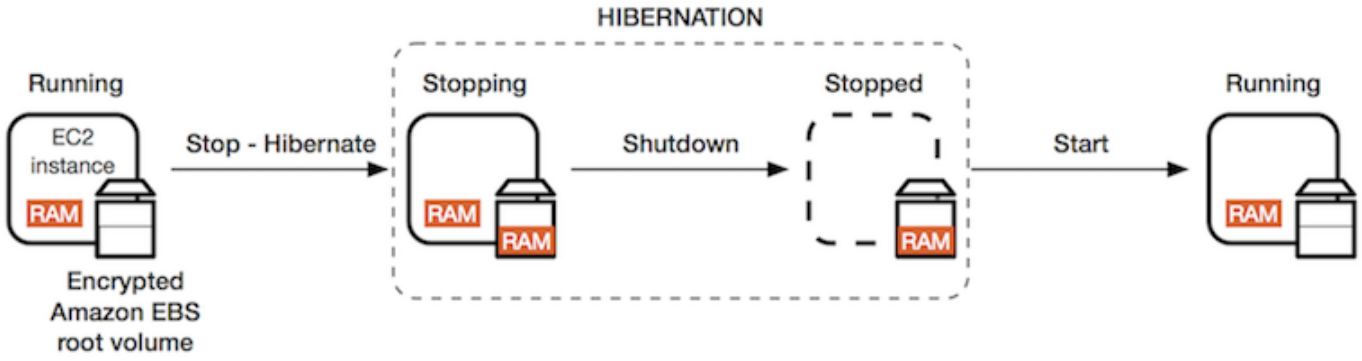
Si vous n'avez plus besoin d'une instance, vous pouvez la résilier à tout moment, y compris quand elle est à un état `stopped` (en veille prolongée). Pour de plus amples informations, veuillez consulter Mettre fin aux EC2 instances Amazon.

Table des matières

- Conditions préalables à l'hibernation des EC2 instances Amazon
- Configurer un système Linux AMI pour prendre en charge l'hibernation
- Activer l'hibernation pour une instance Amazon EC2
- Désactiver KASLR sur une instance (Ubuntu uniquement)
- Hiberner une instance Amazon EC2
- Démarrez une instance Amazon mise en veille prolongée EC2
- Résoudre les problèmes liés à l'hibernation des EC2 instances Amazon

Comment fonctionne l'hibernation des EC2 instances Amazon

Le schéma suivant présente un aperçu de base du processus d'hibernation pour les EC2 instances.



Que se passe-t-il lorsque vous mettez une instance en veille prolongée

Lorsque vous mettez une instance en veille prolongée, voici ce qui se produit :

- L'instance passe à l'état `stopping`. Amazon EC2 indique au système d'exploitation d'exécuter l'hibernation (suspend-to-disk). L'hibernation bloque tous les processus, enregistre le contenu du RAM volume EBS racine, puis effectue un arrêt régulier.
- Lorsque l'arrêt est terminé, l'instance passe à l'état `stopped`.
- Tous EBS les volumes restent attachés à l'instance et leurs données sont conservées, y compris le contenu enregistré duRAM.
- Tous les volumes de stockage d'EC2instance Amazon restent attachés à l'instance, mais les données sur les volumes de stockage d'instance sont perdues.
- Lorsque votre instance se trouve dans l'état `stopped`, vous pouvez modifier certains attributs de l'instance, y compris le type ou la taille d'instance.

- L'instance est généralement migrée vers un nouvel ordinateur hôte sous-jacent lorsqu'elle démarre. Cela se produit également lorsque vous arrêtez et démarrez une instance.
- Lorsque l'instance est démarrée, elle démarre et le système d'exploitation lit le contenu du volume RAM depuis la EBS racine, avant de dégeler les processus pour rétablir son état.
- L'instance conserve ses IPv4 adresses privées et toutes IPv6 les adresses. Lorsque l'instance est démarrée, elle continue de conserver ses IPv4 adresses privées et toutes IPv6 les adresses.
- Amazon EC2 publie l'IPv4adresse publique. Lorsque l'instance est démarrée, Amazon lui EC2 attribue une nouvelle IPv4 adresse publique.
- L'instance conserve les adresses IP Elastic qui lui sont associées. Les adresses IP Elastic qui sont associées à une instance mise en veille prolongée vous seront facturées.

Pour plus d'informations sur les différences entre la mise en veille prolongée, et le redémarrage, l'arrêt et la résiliation, consultez Différences entre les états des instances.

Limites

- Lorsque vous mettez en veille une instance, les données contenues sur les volumes de stockage d'instances sont perdues.
- (Instances Linux) Vous ne pouvez pas mettre en veille prolongée une instance Linux contenant plus de 150 Go de. RAM
- (Instances Windows) Vous ne pouvez pas mettre en veille prolongée une instance Windows contenant plus de 16 Go de. RAM
- Si vous créez un instantané ou AMI à partir d'une instance mise en veille prolongée ou dont l'hibernation est activée, il se peut que vous ne puissiez pas vous connecter à une nouvelle instance lancée depuis AMI ou depuis une AMI instance créée à partir de l'instantané.
- (Instances Spot uniquement) Si Amazon met EC2 en veille prolongée votre instance Spot, seul Amazon EC2 peut reprendre votre instance. Si vous mettez votre instance Spot en veille prolongée (mise en veille prolongée à l'initiative de l'utilisateur), vous pouvez la relancer. Une instance Spot mise en veille prolongée ne peut être relancée que si la capacité est disponible et si le prix Spot est inférieur ou égal au prix maximum spécifié.
- Vous ne pouvez pas mettre en veille prolongée une instance appartenant à un groupe Auto Scaling ou utilisée par Amazon. ECS Si votre instance fait partie d'un groupe Auto Scaling et que vous essayez de la mettre en veille prolongée, le service Amazon EC2 Auto Scaling indique que l'instance arrêtée est défectueuse et peut la mettre hors service et lancer une instance de

remplacement. Pour plus d'informations, consultez la section Contrôles de santé des instances d'un groupe Auto Scaling dans le manuel Amazon EC2 Auto Scaling User Guide.

- Vous ne pouvez pas mettre en veille prolongée une instance configurée pour démarrer en UEFI mode lorsque le démarrage UEFI sécurisé est activé.
- Si vous mettez en veille prolongée une instance qui a été lancée dans une Réservation de capacité, la Réservation de capacité ne garantit pas que l'instance mise en veille prolongée peut reprendre après avoir essayé de la démarrer.
- Vous ne pouvez pas mettre en veille prolongée une instance qui utilise un noyau inférieur à la version 5.10 si le mode Federal Information Processing Standard (FIPS) est activé.
- Nous ne prenons pas en charge la conservation d'une instance mise en veille prolongée au-delà de 60 jours. Pour conserver l'instance mise en veille prolongée au-delà de 60 jours, vous devez la démarrer, l'arrêter, puis la démarrer.
- Nous mettons à jour en permanence notre plateforme avec des mises à niveau et des correctifs de sécurité qui peuvent être en conflit avec des instances mises en veille prolongée existantes. Nous vous avertissons des mises à niveau critiques qui nécessitent un démarrage des instances mises en veille prolongée pour que nous puissions effectuer un arrêt ou un redémarrage afin d'appliquer les mises à niveau et les correctifs de sécurité requis.

Considérations relatives à la mise en veille prolongée d'une instance Spot

- Si vous mettez votre instance Spot en veille prolongée, vous pouvez la redémarrer à condition que la capacité soit disponible et que le prix Spot soit inférieur ou égal au prix maximum spécifié.
- Si Amazon met en EC2 veille prolongée votre instance Spot :
  - Seul Amazon EC2 peut reprendre votre instance.
  - Amazon EC2 reprend l'instance Spot mise en veille prolongée lorsque de la capacité devient disponible avec un prix au comptant inférieur ou égal au prix maximum que vous avez spécifié.
  - Avant qu'Amazon ne EC2 mette votre instance Spot en veille prolongée, vous recevrez un avis d'interruption deux minutes avant le début de l'hibernation.

  Pour de plus amples informations, veuillez consulter Interruptions d'instance Spot.

Conditions préalables à l'hibernation des EC2 instances Amazon

Vous pouvez activer la prise en charge de l'hibernation pour une instance à la demande ou une instance ponctuelle lorsque vous la lancez. Vous ne pouvez pas activer l'hibernation sur une instance

existante, qu'elle soit en cours d'exécution ou arrêtée. Pour de plus amples informations, veuillez consulter Activer l'hibernation de l'instance.

Exigences relatives à la mise en veille prolongée d'une instance

- Régions AWS
- AMIs
- Familles d'instances
- RAMTaille de l'instance
- Type de volume racine
- Taille du volume racine
- Chiffrement du volume racine
- EBStype de volume
- Demandes d'instance Spot

Régions AWS

Vous pouvez utiliser l'hibernation avec toutes Régions AWS les instances.

AMIs

Vous devez utiliser un système HVM AMI qui supporte l'hibernation. Les options suivantes AMIs prennent en charge l'hibernation :

Linux AMIs

AMIspour Intel et les types d'AMDinstances

- AL2023 AMI publié le 2023.09.20 ou version ultérieure
- Amazon Linux 2 AMI publié le 29/08/2019 ou version ultérieure
- Amazon Linux AMI 2018.03 publié le 16 novembre 2018 ou version ultérieure
- CentOS version 8 AMI [1] (une configuration supplémentaire est requise)
- Fedora version 34 ou ultérieure AMI [1] (une configuration supplémentaire est requise)
- Red Hat Enterprise Linux (RHEL) 9 AMI [1] (une configuration supplémentaire est requise)
- Red Hat Enterprise Linux (RHEL) 8 AMI [1] (une configuration supplémentaire est requise)
- Ubuntu 22.04.2 LTS (Jammy Jellyfish) AMI publié sous le numéro de série 20230303 ou version ultérieure[2]

- Ubuntu 20.04 LTS (Focal Fossa) AMI publié sous le numéro de série 20210820 ou version ultérieure[2]
- Ubuntu 18.04 LTS (Bionic Beaver) AMI publié sous le numéro de série 20190722.1 ou version ultérieure [2] [4]
- Ubuntu 16.04 LTS (Xenial Xerus) AMI [2] [3] [4] (une configuration supplémentaire est requise)

AMIspour les types d'instances Graviton

- AL2023 AMI (Arm 64 bits) publié le 2024.07.01 ou version ultérieure
- Amazon Linux 2 AMI (Arm 64 bits) publié le 2024.06.20 ou version ultérieure
- Ubuntu 22.04.2 LTS (Arm 64 bits) (Jammy Jellyfish) AMI publié sous le numéro de série 20240701 ou version ultérieure[2]
- Ubuntu 20.04 LTS (Arm 64 bits) (Focal Fossa) AMI publié sous le numéro de série 20240701 ou version ultérieure[2]

[1] Pour CentOS, Fedora et Red Hat Enterprise Linux, la mise en veille prolongée n'est prise en charge que sur les instances Nitro.

[2] Nous recommandons de désactiver KASLR les instances avec Ubuntu 22.04.2 LTS (Jammy Jellyfish), Ubuntu 20.04 (Focal Fossa), Ubuntu 18.04 LTS (Bionic Beaver) et Ubuntu 16.04 LTS (Xenial Xerus). LTS Pour de plus amples informations, veuillez consulter Désactiver KASLR sur une instance (Ubuntu uniquement).

[3] Pour Ubuntu 16.04 LTS (Xenial Xerus)AMI, l'hibernation n'est pas prise en charge sur les types d'instances. `t3.nano` Aucun correctif ne sera disponible, car Ubuntu (Xenial Xerus) a mis fin au support en avril 2021. Si vous souhaitez utiliser des types d'`t3.nano`instances, nous vous recommandons de passer à Ubuntu 22.04.2 LTS (Jammy Jellyfish), Ubuntu 20.04 (Focal Fossa) ou Ubuntu 18.04 LTS (Bionic AMI Beaver). LTS AMI

[4] Support pour Ubuntu 18.04 LTS (Bionic Beaver) et Ubuntu 16.04 LTS (Xenial Xerus) est arrivé à expiration.

Pour configurer le vôtre AMI afin de prendre en charge l'hibernation, consultezConfigurer un système Linux AMI pour prendre en charge l'hibernation.

La prise en charge d'autres versions d'Ubuntu et d'autres systèmes d'exploitation sera bientôt disponible.

Fenêtres AMIs

- Windows Server 2022 AMI publié le 2023.09.13 ou version ultérieure
- Windows Server 2019 AMI publié le 11 septembre 2019 ou version ultérieure
- Windows Server 2016 AMI publié le 11 septembre 2019 ou version ultérieure
- Windows Server 2012 R2 AMI publié en 2019.09.11 ou version ultérieure
- Windows Server 2012 AMI publié le 11 septembre 2019 ou version ultérieure

Familles d'instances

Vous devez utiliser une famille d'instances qui prend en charge l'hibernation.

- Usage général : M3, M4, M5, M5a, M5ad, M5d, M6g, M6gd, M6i, M6id, M7g, M7GD, M7i, M7i-Flex, T2, T3, T3a, T4g
- Optimisé pour le calcul : C3, C4, C5, C5d, C6g, C6gd, C6gn, C6i, C6id, C7a, C7g, C7gd, C7i, C7i-Flex
- Mémoire optimisée : R3, R4, R5, R5a, R5ad, R5d, R6g, R6gd, R7a, R7g, R7gd, R7i, R7iz
- Stockage optimisé : I3, i3EN

Instances Nitro : les instances bare metal ne sont pas prises en charge.

Pour consulter les types d'instance disponibles qui prennent en charge la mise en veille prolongée dans une région spécifique

Les types d'instance disponibles varient selon la région. Pour voir les types d'instances disponibles qui prennent en charge l'hibernation dans une région, utilisez la describe-instance-typescommande avec le `--region` paramètre. Incluez le paramètre `--filters` pour étendre les résultats aux types d'instance qui prennent en charge la mise en veille prolongée et le paramètre `--query` pour étendre la sortie à la valeur de `InstanceType`.

```
aws ec2 describe-instance-types --filters Name=hibernation-supported,Values=true --
query "InstanceTypes[*].[InstanceType]" --output text | sort
```

Exemple de sortie

```
c3.2xlarge
c3.4xlarge
c3.8xlarge
c3.large
c3.xlarge
c4.2xlarge
c4.4xlarge
c4.8xlarge
...
```

RAMTaille de l'instance

Instances Linux : leur taille doit être inférieure à 150 Go.

Instances Windows : jusqu'à 16 Go. Pour mettre en veille prolongée une instance Windows T3 ou T3a, nous recommandons au moins 1 Go de. RAM

Type de volume racine

Le volume racine doit être un EBS volume et non un volume de stockage d'instance.

Taille du volume racine

Le volume racine doit être suffisamment grand pour stocker le RAM contenu et s'adapter à votre utilisation prévue, par exemple, le système d'exploitation ou les applications. Si vous activez l'hibernation, de l'espace est alloué sur le volume racine au lancement pour stocker leRAM.

Chiffrement du volume racine

Le volume racine doit être chiffré pour garantir la protection du contenu sensible qui se trouve en mémoire au moment de l'hibernation. Lorsque RAM les données sont déplacées vers le volume EBS racine, elles sont toujours chiffrées. Le chiffrement du volume racine est appliqué au lancement de l'instance.

Utilisez l'une des trois options suivantes pour vous assurer que le volume racine est un EBS volume chiffré :

- EBSchiffrement par défaut : vous pouvez activer le EBS chiffrement par défaut pour vous assurer que tous les nouveaux EBS volumes créés dans votre AWS compte sont chiffrés. De cette façon, vous pouvez activer l'hibernation pour vos instances sans spécifier d'intention de chiffrement au moment du lancement de l'instance. Pour plus d'informations, voir Activer le chiffrement par défaut.

- EBSChiffrement « en une seule étape » : vous pouvez lancer des EC2 instances EBS cryptées à partir d'une instance non chiffrée AMI et activer l'hibernation en même temps. Pour de plus amples informations, veuillez consulter Utiliser le chiffrement avec des AMI basées sur EBS.
- Chiffré AMI : vous pouvez activer EBS le chiffrement en utilisant un système crypté AMI pour lancer votre instance. Si vous AMI ne disposez pas d'un instantané racine chiffré, vous pouvez le copier dans un nouveau AMI et demander le chiffrement. Pour plus d'informations, consultez Chiffrement d'une image non chiffrée pendant la copie et Copier une AMI.

EBStype de volume

Les EBS volumes doivent utiliser l'un des types de EBS volumes suivants :

- Usage général SSD (`gp2`et`gp3`)
- Provisionné IOPS SSD (`io1`et`io2`)

Si vous choisissez un type de IOPS SSD volume provisionné, vous devez le provisionner avec le EBS volume approprié IOPS afin d'obtenir des performances optimales pour l'hibernation. Pour plus d'informations, consultez les types de EBS volumes Amazon dans le guide de EBS l'utilisateur Amazon.

Demandes d'instance Spot

Pour les instances Spot, les exigences suivantes s'appliquent :

- Le type de la demande d'instance Spot doit être `persistent`.
- Vous ne pouvez pas spécifier de groupe de lancement dans la demande d'instance Spot.

Configurer un système Linux AMI pour prendre en charge l'hibernation

Les systèmes Linux suivants AMIs peuvent prendre en charge la mise en veille prolongée d'une EC2 instance Amazon, à condition que vous suiviez les étapes de configuration supplémentaires décrites dans cette section.

Une configuration supplémentaire est requise pour :

- Amazon Linux 2 version minimale AMI publiée le 29/08/2019 ou version ultérieure
- Amazon Linux 2 publiées avant le 29.08.2019

- Amazon Linux 2 publiées avant le 16.11.2018
- CentOS version 8 ou ultérieure
- Fedora version 34 ou ultérieure
- Red Hat Enterprise Linux version 8 ou 9
- Ubuntu 20.04 LTS (Focal Fossa) publié avant le numéro de série 20210820
- Ubuntu 18.04 (Bionic Beaver) publié avant le numéro de série 20190722.1
- Ubuntu 16.04 (Xenial Xenus)

Pour les systèmes Linux et Windows AMIs qui prennent en charge l'hibernation et pour lesquels aucune configuration supplémentaire n'est requise, consultezAMIs.

Pour plus d'informations, consultez Mettre à jour le logiciel de l'instance sur votre instance Amazon Linux 2.

Amazon Linux 2 version minimale AMI publiée le 29/08/2019 ou version ultérieure

Pour configurer une version minimale d'Amazon Linux 2 AMI publiée le 29/08/2019 ou une version ultérieure afin de prendre en charge l'hibernation

1. Installez le package `ec2-hibinit-agent` à partir des référentiels.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

2. Redémarrez le service .

```
[ec2-user ~]$ sudo systemctl start hibinit-agent
```

Amazon Linux 2 publiées avant le 29.08.2019

Pour configurer un Amazon Linux 2 AMI publié avant le 29/08/2019 afin de prendre en charge l'hibernation

1. Mettez à jour le noyau vers `4.14.138-114.102` ou version ultérieure.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installez le package `ec2-hibinit-agent` à partir des référentiels.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

4. Vérifiez que la version du noyau a été mise à jour vers `4.14.138-114.102` ou une version ultérieure.

```
[ec2-user ~]$ uname -a
```

5. Arrêtez l'instance et créez unAMI. Pour de plus amples informations, veuillez consulter Créez un compte soutenu EBS par Amazon AMI.

Amazon Linux 2 publiées avant le 16.11.2018

Pour configurer un Amazon Linux AMI publié avant le 2018.11.16 afin de prendre en charge l'hibernation

1. Mettez à jour le noyau vers `4.14.77-70.59` ou version ultérieure.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installez le package `ec2-hibinit-agent` à partir des référentiels.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

4. Vérifiez que la version du noyau est mise à jour vers `4.14.77-70.59` ou une version ultérieure.

```
[ec2-user ~]$ uname -a
```

5. Arrêtez l'instance et créez unAMI. Pour de plus amples informations, veuillez consulter Créez un compte soutenu EBS par Amazon AMI.

CentOS version 8 ou ultérieure

Pour configurer une version 8 ou ultérieure de CentOS AMI pour prendre en charge l'hibernation

1. Mettez à jour le noyau vers `4.18.0-305.7.1.el8_4.x86_64` ou version ultérieure.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installez le dépôt Fedora Extra Packages pour Enterprise Linux (EPEL).

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

3. Installez le package `ec2-hibinit-agent` à partir des référentiels.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Activez l'agent de mise en veille prolongée pour démarrer au démarrage.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

6. Vérifiez que la version du noyau a été mise à jour vers `4.18.0-305.7.1.el8_4.x86_64` ou une version ultérieure.

```
[ec2-user ~]$ uname -a
```

Fedora version 34 ou ultérieure

Pour configurer une version 3.4 ou ultérieure de Fedora pour prendre en charge AMI l'hibernation

1. Mettez à jour le noyau vers `5.12.10-300.fc34.x86_64` ou version ultérieure.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installez le package `ec2-hibinit-agent` à partir des référentiels.

```
[ec2-user ~]$ sudo dnf install ec2-hibinit-agent
```

3. Activez l'agent de mise en veille prolongée pour démarrer au démarrage.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

4. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

5. Vérifiez que la version du noyau a été mise à jour vers `5.12.10-300.fc34.x86_64` ou une version ultérieure.

```
[ec2-user ~]$ uname -a
```

Red Hat Enterprise Linux version 8 ou 9

Pour configurer un système Red Hat Enterprise Linux 8 ou 9 AMI afin de prendre en charge l'hibernation

1. Mettez à jour le noyau vers `4.18.0-305.7.1.el8_4.x86_64` ou version ultérieure.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installez le dépôt Fedora Extra Packages pour Enterprise Linux (EPEL).

   RHELversion 8 :

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   RHELversion 9 :

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

3. Installez le package `ec2-hibinit-agent` à partir des référentiels.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Activez l'agent de mise en veille prolongée pour démarrer au démarrage.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

6. Vérifiez que la version du noyau a été mise à jour vers `4.18.0-305.7.1.el8_4.x86_64` ou une version ultérieure.

```
[ec2-user ~]$ uname -a
```

Ubuntu 20.04 LTS (Focal Fossa) publié avant le numéro de série 20210820

Pour configurer un Ubuntu 20.04 LTS (Focal Fossa) AMI publié avant le numéro de série 20210820 pour prendre en charge l'hibernation

1. Mettez à jour le linux-aws-kernel vers `5.8.0-1038.40` ou une version ultérieure, et grub2 vers `2.04-1ubuntu26.13` ou une version ultérieure.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt dist-upgrade
```

2. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

3. Vérifiez que la version du noyau a été mise à jour vers `5.8.0-1038.40` ou une version ultérieure.

```
[ec2-user ~]$ uname -a
```

4. Vérifiez que la version de grub2 a été mise à jour vers `2.04-1ubuntu26.13` ou une version ultérieure.

```
[ec2-user ~]$ dpkg --list | grep grub2-common
```

Ubuntu 18.04 (Bionic Beaver) publié avant le numéro de série 20190722.1

Pour configurer un Ubuntu 18.04 LTS AMI publié avant le numéro de série 20190722.1 afin de prendre en charge l'hibernation

1. Mettez à jour le noyau vers `4.15.0-1044` ou version ultérieure.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt dist-upgrade
```

2. Installez le package `ec2-hibinit-agent` à partir des référentiels.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

4. Vérifiez que la version du noyau a été mise à jour vers `4.15.0-1044` ou une version ultérieure.

```
[ec2-user ~]$ uname -a
```

Ubuntu 16.04 (Xenial Xenus)

Pour configurer Ubuntu 16.04 afin de prendre LTS en charge l'hibernation, vous devez installer le package du linux-aws-hwe noyau version 4.15.0-1058-aws ou ultérieure et l'agent ec2-hibinit-agent.

> **Important**
>
> Le package noyau `linux-aws-hwe` est pris en charge par Canonical. Le support standard d'Ubuntu 16.04 LTS a pris fin en avril 2021 et le package ne reçoit plus de mises à jour régulières. Il recevra toutefois des mises à jour de sécurité supplémentaires jusqu'à ce que la prise en charge de la maintenance de sécurité étendue prenne fin en 2024. Pour plus d'informations, consultez Amazon EC2 Hibernation pour Ubuntu 16.04 LTS désormais disponible sur le blog Canonical Ubuntu.

Nous vous recommandons de passer à Ubuntu 20.04 LTS (Focal Fossa) AMI ou Ubuntu 18.04 LTS (Bionic Beaver). AMI

Pour configurer un Ubuntu 16.04 LTS AMI pour prendre en charge l'hibernation

1. Mettez à jour le noyau vers `4.15.0-1058-aws` ou version ultérieure.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt install linux-aws-hwe
```

2. Installez le package `ec2-hibinit-agent` à partir des référentiels.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

4. Vérifiez que la version du noyau a été mise à jour vers `4.15.0-1058-aws` ou une version ultérieure.

```
[ec2-user ~]$ uname -a
```

Activer l'hibernation pour une instance Amazon EC2

Pour mettre en veille prolongée une instance, vous devez d'abord l'activer pour la mise en veille prolongée lors du lancement de l'instance.

Important

Vous ne pouvez pas activer ou désactiver la mise en veille prolongée pour une instance après son lancement.

Rubriques

- Activer la mise en veille prolongée pour les instances à la demande
- Activer la mise en veille prolongée pour les instances Spot

- Voir si une instance est activée pour la mise en veille prolongée

Activer la mise en veille prolongée pour les instances à la demande

Utilisez l'une des méthodes suivantes pour activer la mise en veille prolongée pour vos instances à la demande.

Console

Pour activer la mise en veille prolongée pour une instance à la demande

1. Suivez la procédure pour lancer une instance, mais ne lancez l'instance qu'après avoir effectué les étapes suivantes pour activer l'hibernation.
2. Pour activer l'hibernation, configurez les champs suivants dans l'assistant de lancement de l'instance :

   a. Sous Images de l'application et du système d'exploitation (Amazon Machine Image), sélectionnez une image AMI qui prend en charge l'hibernation. Pour de plus amples informations, veuillez consulter AMIs.

   b. Pour Instance type (Type d'Instance), sélectionnez un type d'instance pris en charge. Pour de plus amples informations, veuillez consulter Familles d'instances.

   c. Sous Configure storage (Configurer le stockage), choisissez Advanced (Avancé) (à droite), et spécifiez les informations suivantes pour le volume racine :

      - Pour Taille (GiB), entrez la taille du volume EBS racine. Le volume doit être suffisamment grand pour stocker le RAM contenu et s'adapter à l'utilisation prévue.
      - Pour le type de volume, sélectionnez un type de EBS volume pris en charge : usage général SSD (`gp2`et`gp3`) ou provisionné IOPS SSD (`io1`et`io2`).
      - Pour Encrypted (Chiffré), choisissez Yes (Oui). Si vous avez activé le chiffrement par défaut dans cette AWS région, l'option Oui est sélectionnée.
      - Pour KMSclé, sélectionnez la clé de chiffrement pour le volume. Si vous avez activé le chiffrement par défaut dans cette AWS région, la clé de chiffrement par défaut est sélectionnée.

      Pour plus d'informations sur les prérequis relatifs au volume racine, consultez Conditions préalables à l'hibernation des EC2 instances Amazon.

d. Développez Advanced details (Détails avancés), et pour Stop - Hibernate behavior (Arrêt – Comportement de mise en veille prolongée), choisissez Enable (Activer).

3. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance). Pour de plus amples informations, veuillez consulter Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console.

AWS CLI

Pour activer la mise en veille prolongée pour une instance à la demande

Utilisez la commande run-instances pour lancer une instance. Spécifiez les paramètres du volume EBS racine à l'aide du `--block-device-mappings file://mapping.json` paramètre et activez l'hibernation à l'aide du `--hibernation-options Configured=true` paramètre.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type m5.large \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
    --key-name MyKeyPair
```

Spécifiez les éléments suivants dans `mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 30,
            "VolumeType": "gp2",
            "Encrypted": true
        }
    }
]
```

> **Note**
>
> La valeur de `DeviceName` doit correspondre au nom du périphérique racine associé auAMI. Pour trouver le nom du périphérique racine, utilisez la commande describe-images (décrire les images).
>
> ```
> aws ec2 describe-images --image-id ami-0abcdef1234567890
> ```
>
> Si vous avez activé le chiffrement par défaut dans cette AWS région, vous pouvez l'omettre`"Encrypted": true`.

PowerShell

Pour activer le mode hibernation pour une instance à la demande à l'aide du AWS Tools for Windows PowerShell

Utilisez la New-EC2Instancecommande pour lancer une instance. Spécifiez le volume EBS racine en définissant d'abord le mappage des périphériques en mode bloc, puis en l'ajoutant à la commande à l'aide du `-BlockDeviceMappings` paramètre. Activez la mise en veille prolongée à l'aide du paramètre `-HibernationOptions_Configured $true`.

```
PS C:\> $ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
PS C:\> $ebs_encrypt.DeviceName = "/dev/xvda"
PS C:\> $ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
PS C:\> $ebs_encrypt.Ebs.VolumeSize = 30
PS C:\> $ebs_encrypt.Ebs.VolumeType = "gp2"
PS C:\> $ebs_encrypt.Ebs.Encrypted = $true

PS C:\> New-EC2Instance `
            -ImageId ami-0abcdef1234567890 `
            -InstanceType m5.large `
            -BlockDeviceMappings $ebs_encrypt `
            -HibernationOptions_Configured $true `
            -MinCount 1 `
            -MaxCount 1 `
            -KeyName MyKeyPair
```

> **Note**
>
> La valeur de `DeviceName` doit correspondre au nom du périphérique racine associé auAMI. Pour trouver le nom du périphérique racine, utilisez la Get-EC2Imagecommande.
>
> ```
> Get-EC2Image -ImageId ami-0abcdef1234567890
> ```
>
> Si vous avez activé le chiffrement par défaut dans cette AWS région, vous pouvez omettre le mappage `Encrypted = $true` des périphériques par blocs.

Activer la mise en veille prolongée pour les instances Spot

Utilisez l'une des méthodes suivantes pour activer la mise en veille prolongée pour vos instances Spot. Pour plus d'informations sur la mise en veille prolongée des instances Spot en cas d'interruption, consultez la rubrique Interruptions d'instance Spot.

Console

Vous pouvez utiliser l'assistant de lancement d'instance dans la EC2 console Amazon pour activer l'hibernation d'une instance Spot.

Pour activer la mise en veille prolongée pour une instance Spot

1. Suivez la procédure pour demande une instance Spot à l'aide de l'assistant de lancement d'instance, mais ne lancez l'instance qu'après avoir effectué les étapes suivantes pour activer la mise en veille prolongée.
2. Pour activer l'hibernation, configurez les champs suivants dans l'assistant de lancement de l'instance :

   a. Sous Images de l'application et du système d'exploitation (Amazon Machine Image), sélectionnez une image AMI qui prend en charge l'hibernation. Pour de plus amples informations, veuillez consulter AMIs.

   b. Pour Instance type (Type d'Instance), sélectionnez un type d'instance pris en charge. Pour de plus amples informations, veuillez consulter Familles d'instances.

   c. Sous Configure storage (Configurer le stockage), choisissez Advanced (Avancé) (à droite), et spécifiez les informations suivantes pour le volume racine :

- Pour Taille (GiB), entrez la taille du volume EBS racine. Le volume doit être suffisamment grand pour stocker le RAM contenu et s'adapter à l'utilisation prévue.
- Pour le type de volume, sélectionnez un type de EBS volume pris en charge : usage général SSD (`gp2etgp3`) ou provisionné IOPS SSD (`io1etio2`).
- Pour Encrypted (Chiffré), choisissez Yes (Oui). Si vous avez activé le chiffrement par défaut dans cette AWS région, l'option Oui est sélectionnée.
- Pour KMSclé, sélectionnez la clé de chiffrement pour le volume. Si vous avez activé le chiffrement par défaut dans cette AWS région, la clé de chiffrement par défaut est sélectionnée.

Pour plus d'informations sur les prérequis relatifs au volume racine, consultez Conditions préalables à l'hibernation des EC2 instances Amazon.

d. Développez Détails avancés et, en plus des champs de configuration d'une instance Spot, procédez comme suit :

   i. Pour Type de demande, choisissez Persistente.

   ii. Pour Comportement d'interruption, choisissez Mise en veille prolongée. Sinon, pour Comportement d'arrêt - mise en veille prolongée, choisissez Activer. Les deux champs activent la mise en veille prolongée sur votre instance Spot. Vous devez uniquement configurer l'un de ces champs.

3. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance). Pour de plus amples informations, veuillez consulter Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console.

AWS CLI

Vous pouvez activer la mise en veille prolongée pour une instance Spot à l'aide de la commande de l' AWS CLI run-instances.

Pour activer la mise en veille prolongée pour une instance Spot à l'aide du paramètre **`hibernation-options`**

Utilisez la commande run-instances pour demander une instance Spot. Spécifiez les paramètres du volume EBS racine à l'aide du `--block-device-mappings file://mapping.json`

paramètre et activez l'hibernation à l'aide du `--hibernation-options Configured=true` paramètre. Le type de la demande Spot (`SpotInstanceType`) doit être `persistent`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c4.xlarge \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
    --key-name MyKeyPair
    --instance-market-options
        {
           "MarketType":"spot",
           "SpotOptions":{
              "MaxPrice":"1",
              "SpotInstanceType":"persistent"
            }
        }
```

Spécifiez les paramètres du volume EBS racine `mapping.json` comme suit.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 30,
            "VolumeType": "gp2",
            "Encrypted": true
        }
    }
]
```

> **Note**
>
> La valeur de `DeviceName` doit correspondre au nom du périphérique racine associé auAMI. Pour trouver le nom du périphérique racine, utilisez la commande describe-images (décrire les images).
>
> ```
> aws ec2 describe-images --image-id ami-0abcdef1234567890
> ```

Si vous avez activé le chiffrement par défaut dans cette AWS région, vous pouvez l'omettre`"Encrypted": true`.

PowerShell

Pour activer le mode hibernation pour une instance Spot à l'aide du AWS Tools for Windows PowerShell

Utilisez la New-EC2Instancecommande pour demander une instance Spot. Spécifiez le volume EBS racine en définissant d'abord le mappage des périphériques en mode bloc, puis en l'ajoutant à la commande à l'aide du `-BlockDeviceMappings` paramètre. Activez la mise en veille prolongée à l'aide du paramètre `-HibernationOptions_Configured $true`.

```
PS C:\> $ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
PS C:\> $ebs_encrypt.DeviceName = "/dev/xvda"
PS C:\> $ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
PS C:\> $ebs_encrypt.Ebs.VolumeSize = 30
PS C:\> $ebs_encrypt.Ebs.VolumeType = "gp2"
PS C:\> $ebs_encrypt.Ebs.Encrypted = $true

PS C:\> New-EC2Instance `
            -ImageId ami-0abcdef1234567890 `
            -InstanceType m5.large `
            -BlockDeviceMappings $ebs_encrypt `
            -HibernationOptions_Configured $true `
            -MinCount 1 `
            -MaxCount 1 `
            -KeyName MyKeyPair `
            -InstanceMarketOption @(
                  MarketType = spot;
                  SpotOptions @{
                  MaxPrice = 1;
                  SpotInstanceType = persistent}
               )
```

> **Note**
>
> La valeur de `DeviceName` doit correspondre au nom du périphérique racine associé auAMI. Pour trouver le nom du périphérique racine, utilisez la Get-EC2Imagecommande.

```
Get-EC2Image -ImageId ami-0abcdef1234567890
```

Si vous avez activé le chiffrement par défaut dans cette AWS région, vous pouvez omettre le mappage `Encrypted = $true` des périphériques par blocs.

Voir si une instance est activée pour la mise en veille prolongée

Utilisez les instructions suivantes pour voir si une instance est activée pour la mise en veille prolongée.

Console

Pour voir si une instance est activée pour la mise en veille prolongée

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance et, sous l'onglet Détails de la section Détails de l'instance, inspectez le comportement Stop-hibernate. La valeur Enabled (Activé) indique que l'instance est activée pour la mise en veille prolongée.

AWS CLI

Pour voir si une instance est activée pour la mise en veille prolongée

Utilisez la commande describe-instances et spécifiez le paramètre `--filters "Name=hibernation-options.configured,Values=true"` pour filtrer les instances qui sont activées pour la mise en veille prolongée.

```
aws ec2 describe-instances \
    --filters "Name=hibernation-options.configured,Values=true"
```

Le champ suivant dans le résultat indique que l'instance est activée pour la mise en veille prolongée.

```
"HibernationOptions": {
    "Configured": true
}
```

PowerShell

Pour voir si une instance est activée pour la mise en veille prolongée à l'aide d' AWS Tools for Windows PowerShell

Utilisez la Get-EC2Instancecommande et spécifiez le `-Filter @{ Name="hibernation-options.configured"; Value="true"}` paramètre pour filtrer les instances activées pour l'hibernation.

```
(Get-EC2Instance -Filter @{Name="hibernation-options.configured";
 Value="true"}).Instances
```

Le résultat répertorie les EC2 instances activées pour l'hibernation.

Désactiver KASLR sur une instance (Ubuntu uniquement)

Pour exécuter l'hibernation sur une instance récemment lancée avec Ubuntu 16.04 LTS (Xenial Xerus), Ubuntu 18.04 LTS (Bionic Beaver) publié avec le numéro de série 20190722.1 ou version ultérieure, ou Ubuntu 20.04 (Focal Fossa) publié avec le numéro de série 20210820 ou version ultérieure, nous vous recommandons de désactiver LTS (Kernel Address Space Layout Randomization). KASLR Sur Ubuntu 16.04LTS, Ubuntu 18.04 LTS ou Ubuntu 20.04 LTS KASLR est activé par défaut.

KASLRest une fonctionnalité de sécurité standard du noyau Linux qui permet d'atténuer l'exposition aux vulnérabilités d'accès à la mémoire non encore découvertes et les conséquences de ces vulnérabilités en répartissant de manière aléatoire la valeur de l'adresse de base du noyau. Lorsque cette option est KASLR activée, il est possible que l'instance ne reprenne pas après sa mise en veille prolongée.

Pour en savoir plusKASLR, consultez la section Fonctionnalités d'Ubuntu.

Pour désactiver KASLR une instance lancée avec Ubuntu

1. Connectez-vous à votre instance à l'aide deSSH. Pour de plus amples informations, veuillez consulter Connectez-vous à votre instance Linux à l'aide de SSH.
2. Ouvrez le fichier `/etc/default/grub.d/50-cloudimg-settings.cfg` dans l'éditeur de votre choix. Éditez la ligne `GRUB_CMDLINE_LINUX_DEFAULT` de sorte à ajouter l'option `nokaslr` à la fin de la ligne, comme illustré dans l'exemple suivant.

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
 nvme_core.io_timeout=4294967295 nokaslr"
```

3. Enregistrez le fichier et quittez votre éditeur.
4. Exécutez la commande suivante pour recréer la configuration Grub.

```
sudo update-grub
```

5. Redémarrez l'instance.

```
sudo reboot
```

6. Exécutez la commande suivante pour confirmer que `nokaslr` a été ajouté.

```
cat /proc/cmdline
```

Le résultat de la commande doit inclure l'option `nokaslr`.

Hiberner une instance Amazon EC2

Vous pouvez lancer l'hibernation sur une instance à la demande ou une instance ponctuelle si l'instance est une instance EBS sauvegardée, si elle est activée pour l'hibernation et si elle répond aux exigences d'hibernation. Si une instance ne peut pas être mise en veille prolongée, un arrêt normal a lieu.

Console

Pour mettre une instance en veille prolongée

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez une instance et choisissez État de l'instance, Mettre en veille prolongée les instances. Si Mettre l'instance en veille prolongée est désactivé, l'instance est déjà en veille prolongée ou arrêtée, ou elle ne peut pas être mise en veille prolongée. Pour plus d'informations, consultez Conditions préalables à l'hibernation des EC2 instances Amazon.
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Mettre en veille prolongée. La mise en veille prolongée de l'instance peut prendre quelques minutes. L'état de l'instance

passe d'abord à Stopping(En cours d'arrêt), puis passe à Stopped (Arrêté(e)) lorsque l'instance est mise en veille prolongée.

AWS CLI

Pour mettre en veille prolongée une instance sauvegardée EBS

Utilisez la commande stop-instances et spécifiez le paramètre `--hibernate`.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --hibernate
```

PowerShell

Pour mettre en veille prolongée une instance à l'aide du AWS Tools for Windows PowerShell

Utilisez la Stop-EC2Instancecommande et spécifiez le `-Hibernate $true` paramètre.

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Hibernate $true
```

Console

Pour voir si la mise en veille prolongée est initiée sur une instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance et, sous l'onglet Détails de la section Détails de l'instance, vérifiez la valeur du champ Message de transition d'état.

   Cliente. UserInitiatedHibernate: La mise en veille prolongée initiée par l'utilisateur indique que vous avez lancé l'hibernation sur l'instance à la demande ou sur l'instance ponctuelle.

AWS CLI

Pour voir si la mise en veille prolongée est initiée sur une instance

Utilisez la commande describe-instances et spécifiez le filtre `state-reason-code` pour afficher les instances sur lesquelles la mise en veille prolongée est initiée.

```
aws ec2 describe-instances \
    --filters "Name=state-reason-code,Values=Client.UserInitiatedHibernate"
```

Le champ suivant dans le résultat indique que la mise en veille prolongée a été initiée sur l'instance à la demande ou sur l'instance Spot.

```
"StateReason": {
    "Code": "Client.UserInitiatedHibernate"
}
```

PowerShell

Pour voir si la mise en veille prolongée est initiée sur une instance à l'aide d' AWS Tools for Windows PowerShell

Utilisez la Get-EC2Instancecommande et spécifiez le `state-reason-code` filtre pour voir les instances sur lesquelles l'hibernation a été initiée.

```
Get-EC2Instance `
    -Filter @{Name="state-reason-code";Value="Client.UserInitiatedHibernate"}
```

Le résultat répertorie les EC2 instances sur lesquelles l'hibernation a été initiée.

Démarrez une instance Amazon mise en veille prolongée EC2

Démarrez une instance mise en veille prolongée comme vous le feriez pour une instance arrêtée.

> **Note**
>
> Pour les instances Spot, si Amazon EC2 a mis l'instance en veille prolongée, seul Amazon EC2 peut la reprendre. Vous ne pouvez relancer une instance Spot mise en veille prolongée que si vous êtes à l'origine de la mise en veille prolongée. Les instances Spot ne peuvent être relancées que si la capacité est disponible et si le prix Spot est inférieur ou égal au prix maximum spécifié.

Console

Pour démarrer une instance mise en veille prolongée

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez une instance mise en veille prolongée et choisissez État de l'instance, Démarrer l'instance. Il peut s'écouler quelques minutes avant que l'instance ne passe à l'état `running`. Pendant ce temps, les contrôles de statut de l'instance montrent l'instance à un état d'échec jusqu'à ce que l'instance ait démarré.

AWS CLI

Pour démarrer une instance mise en veille prolongée

Utilisez la commande start-instances.

```
aws ec2 start-instances \
    --instance-ids i-1234567890abcdef0
```

PowerShell

Pour démarrer une instance mise en veille prolongée à l'aide du AWS Tools for Windows PowerShell

Utilisez la Start-EC2Instancecommande.

```
Start-EC2Instance `
    -InstanceId i-1234567890abcdef0
```

Résoudre les problèmes liés à l'hibernation des EC2 instances Amazon

Utilisez ces informations pour diagnostiquer et résoudre les problèmes courants que vous pourriez rencontrer lors de la mise en veille prolongée d'une instance.

Problèmes relatifs à la mise en veille prolongée

- Impossible d'effectuer une mise en veille prolongée immédiatement après le lancement
- Le passage de stopping à stopped prend du temps et l'état de la mémoire n'est pas restauré après le démarrage

- Instance « bloquée » à l'état stopping
- Impossible de démarrer l'instance Spot immédiatement après la mise en veille prolongée
- Échec de la reprise des instances Spot

Impossible d'effectuer une mise en veille prolongée immédiatement après le lancement

Si vous essayez de mettre en veille prolongée une instance trop rapidement après l'avoir lancée, vous obtiendrez une erreur.

Vous devez attendre environ deux minutes pour les instances Linux et environ cinq minutes pour les instances Windows après le lancement avant de passer en veille prolongée.

Le passage de stopping à stopped prend du temps et l'état de la mémoire n'est pas restauré après le démarrage

Si votre instance mise en veille prolongée prend du temps pour passer de l'état `stopping` à `stopped`, et si l'état de la mémoire n'est pas restauré après que vous avez démarré, cela peut indiquer que la mise en veille prolongée n'a pas été configurée correctement.

Instances Linux

Consultez le journal système de l'instance et recherchez les messages liés à la mise en veille prolongée. Pour accéder au journal système, connectez-vous à l'instance ou utilisez la get-console-outputcommande. Recherchez les lignes de journal de l'agent `hibinit-agent`. Si les lignes de journal indiquent un échec ou si les lignes de journal sont manquantes, il est probable qu'un échec de la configuration de la mise en veille prolongée au lancement ait eu lieu.

Par exemple, le message suivant indique que le volume racine de l'instance n'est pas suffisamment grand : `hibinit-agent: Insufficient disk space. Cannot create setup for hibernation. Please allocate a larger root device.`

Si la dernière ligne de journal de `hibinit-agent` est `hibinit-agent: Running: swapoff /swap`, la mise en veille prolongée a été configurée avec succès.

Si aucun journal de ces processus ne s'affiche, il est possible que vous ne AMI preniez pas en charge l'hibernation. Pour plus d'informations sur les AMIs pris en charge, veuillez consulter Conditions préalables à l'hibernation des EC2 instances Amazon. Si vous avez utilisé votre propre système LinuxAMI, assurez-vous d'avoir suivi les instructions deConfigurer un système Linux AMI pour prendre en charge l'hibernation.

Windows Server 2016 et versions ultérieures

Consultez le journal de EC2 lancement et recherchez les messages liés à l'hibernation. Pour accéder au journal de EC2 lancement, connectez-vous à l'instance et ouvrez le `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\Ec2Launch.log` fichier dans un éditeur de texte. Si vous utilisez la EC2Launch version 2, ouvrez`C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

> **Note**
>
> Par défaut, Windows masque les fichiers et les dossiers qui se trouvent sous `C:\ProgramData`. Pour afficher les répertoires et les fichiers de EC2 lancement, entrez le chemin dans l'Explorateur Windows ou modifiez les propriétés du dossier pour afficher les fichiers et dossiers cachés.

Recherchez les lignes de journal pour la mise en veille prolongée. Si les lignes de journal indiquent un échec ou si les lignes de journal sont manquantes, il est probable qu'un échec de la configuration de la mise en veille prolongée au lancement ait eu lieu.

Par exemple, le message suivant indique que l'hibernation n'a pas pu être configurée : `Message: Failed to enable hibernation.` si le message d'erreur inclut des ASCII valeurs décimales, vous pouvez convertir les ASCII valeurs en texte brut afin de lire le message d'erreur complet.

Si la ligne de journal contient `HibernationEnabled: true`, la mise en veille prolongée a été configurée avec succès.

Windows Server 2012 R2 et versions antérieures

Consultez le journal de EC2 configuration et recherchez les messages liés à l'hibernation. Pour accéder au journal de EC2 configuration, connectez-vous à l'instance et ouvrez le `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt` fichier dans un éditeur de texte. Recherchez les lignes de journal pour `SetHibernateOnSleep`. Si les lignes de journal indiquent un échec ou si les lignes de journal sont manquantes, il est probable qu'un échec de la configuration de la mise en veille prolongée au lancement ait eu lieu.

Par exemple, le message suivant indique que le volume racine de l'instance n'est pas suffisamment grand : `SetHibernateOnSleep: Failed to enable hibernation: Hibernation failed with the following error: There is not enough space on the disk.`

Si la ligne de journal est `SetHibernateOnSleep: HibernationEnabled: true`, la mise en veille prolongée a été configurée avec succès.

Taille de l'instance Windows

Si vous utilisez une instance Windows T3 ou T3a avec moins de 1 Go deRAM, essayez d'augmenter la taille de l'instance à une instance contenant au moins 1 Go de. RAM

Instance « bloquée » à l'état stopping

Si vous avez mis votre instance en veille prolongée que celle-ci semble « bloquée » à l'état `stopping`, vous pouvez forcer son arrêt. Pour de plus amples informations, veuillez consulter Résoudre les problèmes d'arrêt des EC2 instances Amazon.

Impossible de démarrer l'instance Spot immédiatement après la mise en veille prolongée

Si vous essayez de démarrer une instance Spot dans les deux minutes suivant sa mise en veille prolongée, le message d'erreur suivant peut s'afficher :

```
You failed to start the Spot Instance because the associated Spot Instance request is not in an appropriate state to support start.
```

Attendez environ deux minutes pour les instances Linux et environ cinq minutes pour les instances Windows, puis réessayez de démarrer l'instance.

Échec de la reprise des instances Spot

Si votre instance Spot a été mise en veille prolongée avec succès, mais qu'elle n'a pas pu reprendre, et qu'elle a été redémarrée (un nouveau redémarrage où l'état de mise en veille prolongée n'est pas conservé), cela peut être dû au fait que les données utilisateur contenaient le script suivant :

```
/usr/bin/enable-ec2-spot-hibernation
```

Supprimez ce script du champ Données utilisateur du modèle de lancement, puis demandez une nouvelle instance Spot.

Notez que même si l'instance n'a pas pu reprendre, si l'état de mise en veille prolongée n'est pas préservé, l'instance peut toujours être démarrée de la même manière qu'en partant de l'état `stopped`.

Redémarrer votre instance

Le redémarrage d'une instance est similaire à celui d'un système d'exploitation. Dans la plupart des cas, il suffit de quelques minutes pour redémarrer votre instance.

Lorsque vous redémarrez une instance, elle conserve les éléments suivants :

- DNSNom public (IPv4)
- IPv4Adresse privée
- IPv4Adresse publique
- IPv6adresse (le cas échéant)
- Toutes les données présentes sur ses volumes de stockage d'instance

Le redémarrage d'une instance ne déclenche pas de nouvelle période de facturation (avec un minimum d'une minute), contrairement à un arrêt et à un démarrage d'une instance.

Il peut nous arriver de planifier le redémarrage d'une instance pour effectuer des tâches de maintenance, par exemple pour appliquer des mises à jour qui requièrent un redémarrage. Le cas échéant, aucune action n'est requise de votre part. Nous vous recommandons d'attendre simplement le redémarrage dans le créneau horaire prévu. Pour plus d'informations, consultez Événements planifiés pour les EC2 instances Amazon.

Nous vous recommandons d'utiliser la EC2 console Amazon, un outil de ligne de commande ou Amazon EC2 API pour redémarrer votre instance au lieu d'exécuter la commande de redémarrage du système d'exploitation depuis votre instance. Si vous utilisez la EC2 console Amazon, un outil de ligne de commande ou Amazon EC2 API pour redémarrer votre instance, nous effectuons un redémarrage dur si l'instance ne s'arrête pas correctement au bout de quelques minutes. Si vous utilisez AWS CloudTrail, le fait d'utiliser Amazon EC2 pour redémarrer votre instance crée également un API enregistrement indiquant le moment où votre instance a été redémarrée.

instances Windows

Si Windows installe des mises à jour sur votre instance, nous vous recommandons de ne pas redémarrer ou arrêter votre instance à l'aide de la EC2 console Amazon ou de la ligne de commande tant que toutes les mises à jour ne sont pas installées. Lorsque vous utilisez la EC2 console Amazon ou la ligne de commande pour redémarrer ou arrêter votre instance, celle-ci risque d'être redémarrée de manière définitive. Un redémarrage matériel pendant l'installation de mises à jour peut entraîner l'instabilité de votre instance.

Console

Pour redémarrer une instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance et choisissez Instance state (État de l'instance), Reboot instance (Redémarrer l'instance).

   Vous pouvez également sélectionner l'instance, puis choisir Actions, Manage instance state (Gérer l'état de l'instance). Dans l'écran qui s'ouvre, choisissez Reboot (Redémarrer), puis Change state (Modifier l'état).
4. Lorsque vous êtes invité à confirmer l'opération, sélectionnez Redémarrer.

   L'instance reste dans l'état `running`.

Command line

Pour redémarrer une instance

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez Accédez à Amazon EC2.

- reboot-instances (AWS CLI)
- Restart-EC2Instance (AWS Tools for Windows PowerShell)

Pour exécuter une expérience d'injection de défauts contrôlés

Vous pouvez l'utiliser AWS Fault Injection Service pour tester la façon dont votre application répond lorsque votre instance est redémarrée. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS Fault Injection Service.

Mettre fin aux EC2 instances Amazon

Vous pouvez supprimer votre instance lorsque vous n'en avez plus besoin. Cette opération est appelée mise hors service (ou résiliation) de votre instance. Dès que l'état d'une instance passe à `shutting-down` ou `terminated`, l'instance ne vous est plus facturée.

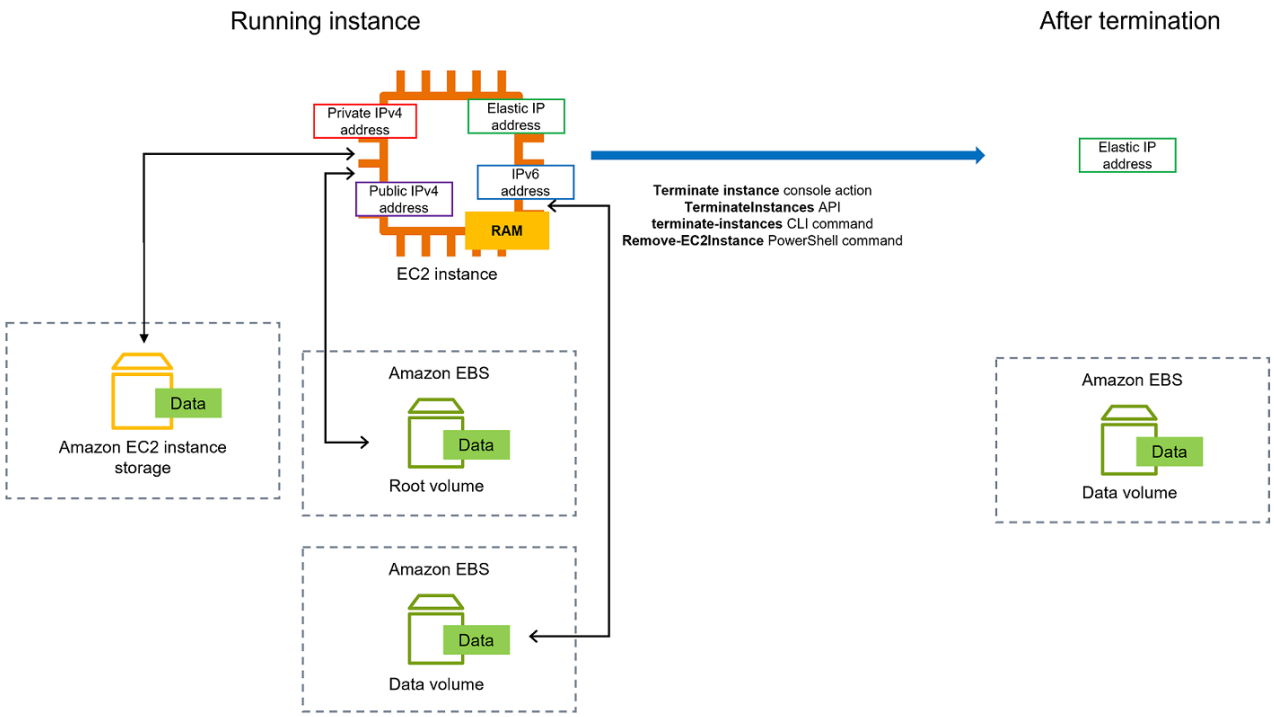
Vous ne pouvez pas vous connecter à une instance mise hors service, ni la démarrer. Toutefois, vous pouvez lancer des instances supplémentaires en utilisant le même outilAMI. Si vous préférez arrêter ou mettre en veille prolongée une instance, consultez Arrêtez et démarrez les EC2 instances Amazon ou. Hibernez votre instance Amazon EC2 Pour de plus amples informations, veuillez consulter Différences entre les états des instances.

Table des matières

Comment fonctionne la résiliation d'une instance

Lorsque vous mettez fin à une instance, les modifications sont enregistrées au niveau du système d'exploitation de l'instance, certaines ressources sont perdues et certaines ressources persistent.

Le schéma suivant montre ce qui est perdu et ce qui persiste lorsqu'une EC2 instance Amazon est résiliée. Lorsqu'une instance se termine, les données de tous les volumes de stockage d'instance et les données stockées sur l'instance RAM sont effacées. Toutes les adresses IP élastiques associées à l'instance sont détachées. Pour les EBS volumes Amazon et les données qu'ils contiennent, le résultat dépend du paramètre Supprimer en cas de résiliation du volume. Par défaut, le volume racine est supprimé et les volumes de données sont préservés.



Considérations

- Lorsqu'une instance est mise hors service, les données des volumes de stockage d'instances associées à cette instance sont supprimées.
- Par défaut, les volumes du périphérique EBS racine Amazon sont automatiquement supprimés lorsque l'instance se termine. Toutefois, tous les EBS volumes supplémentaires que vous attachez au lancement ou les EBS volumes que vous attachez à une instance existante sont conservés même après la fin de l'instance. Pour de plus amples informations, veuillez consulter Conservation des données lors de la résiliation d'une instance.

> **Note**
>
> Tous les volumes qui ne sont pas supprimés lors de la résiliation de l'instance continueront à entraîner des frais.

- Pour éviter qu'une instance ne soit accidentellement interrompue par quelqu'un, activez la protection contre la résiliation.
- Pour contrôler si une instance s'arrête ou se termine lorsque l'arrêt est initié à partir de l'instance, modifiez le comportement d'arrêt initié par l'instance.

- Si vous exécutez un script de la résiliation d'une instance, il est possible que cette dernière soit résiliée de façon anormale dans la mesure où nous ne pouvons pas garantir le bon fonctionnement des scripts d'arrêt. Amazon EC2 essaie d'arrêter correctement une instance et d'exécuter les scripts d'arrêt du système ; toutefois, certains événements (tels qu'une panne matérielle) peuvent empêcher l'exécution de ces scripts d'arrêt du système.
- Les instances bare metal x86 ne prennent pas en charge l'arrêt coopératif.

Ce qui se passe lorsque vous résiliez une instance

Modifications enregistrées au niveau du système d'exploitation

- La API demande envoie un événement d'appui sur un bouton à l'invité.
- Divers services système sont arrêtés à la suite de l'événement d'appui sur le bouton. L'arrêt progressif du système est assuré par systemd (Linux) ou le processus système (Windows). L'arrêt progressif est déclenché par le fait que l'hyperviseur appuie sur le bouton d'ACPIarrêt.
- ACPIl'arrêt est lancé.
- L'instance s'arrêtera une fois le processus d'arrêt progressif terminé. L'heure d'arrêt du système d'exploitation n'est pas configurable. L'instance reste visible dans la console pendant une courte période, puis l'entrée est automatiquement supprimée.

Ressources perdues

- Les données stockées sur un volume de stockage d'instances.
- Données stockées sur les volumes de l'appareil EBS racine Amazon si l'`DeleteOnTermination`attribut est défini sur true.

Des ressources qui persistent

- Données stockées sur des EBS volumes Amazon supplémentaires attachés au lancement ou après le lancement d'une instance.

Test de la réponse de l'application à la résiliation d'instance

Vous pouvez l'utiliser AWS Fault Injection Service pour tester la façon dont votre application réagit lorsque votre instance est arrêtée. Pour plus d'informations, consultez le AWS Fault Injection Service Guide de l'utilisateur .

Résilier une instance

Vous pouvez mettre fin à une instance à tout moment.

Console

Pour résilier une instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance, puis choisissez État de l'instance, Terminer (supprimer) l'instance.
4. Choisissez Terminate (supprimer) lorsque vous êtes invité à confirmer.
5. Une fois que vous avez mis fin à une instance, elle reste visible pendant un court instant, avec un état `determinated`.

   Si la résiliation échoue ou si une instance interrompue est visible pendant plus de quelques heures, consultezInstance terminée toujours affichée.

Command line

Pour résilier une instance à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez Accédez à Amazon EC2.

- terminate-instances (AWS CLI)
- Remove-EC2Instance (AWS Tools for Windows PowerShell)

Résoudre les problèmes de résiliation d'instance

Le demandeur doit être autorisé à appelerec2:TerminateInstances. Pour plus d'informations, consultez la section Exemples de politiques pour travailler avec les instances.

Si vous mettez fin à votre instance et qu'une autre instance démarre, vous avez probablement configuré le dimensionnement automatique via une fonctionnalité telle que EC2 Fleet ou Amazon EC2 Auto Scaling. Pour de plus amples informations, veuillez consulter instances lancées ou terminées automatiquement.

Vous ne pouvez pas mettre fin à une instance si la protection contre la résiliation est activée. Pour plus d'informations, consultez la section Protection contre le licenciement.

Si votre instance reste dans `shutting-down` cet état plus longtemps que d'habitude, elle doit être nettoyée (mise hors service) par des processus automatisés au sein du EC2 service Amazon. Pour de plus amples informations, veuillez consulter Mise à fin d'instance retardée.

Activer la protection de la résiliation

Pour éviter que votre instance ne soit résiliée accidentellement, vous pouvez activer la protection contre la résiliation pour l'instance. L'`DisableApiTermination`attribut contrôle si l'instance peut être interrompue à l'aide du AWS Management Console, AWS Command Line Interface (AWS CLI) ouAPI. Par défaut, la protection contre la résiliation est désactivée pour votre instance, ce qui signifie que celle-ci peut être résiliée à l'aide du AWS Management Console ouAPI. AWS CLI Vous pouvez définir la valeur de cet attribut lorsque vous lancez une instance, pendant que l'instance est en cours d'exécution ou lorsqu'elle est arrêtée (pour les instances EBS soutenues par Amazon).

L'attribut `DisableApiTermination` ne vous empêche pas de résilier une instance en déclenchant l'arrêt à partir de l'instance (à l'aide d'une commande du système d'exploitation pour l'arrêt système) lorsque l'attribut `InstanceInitiatedShutdownBehavior` est défini. Pour de plus amples informations, veuillez consulter Modifier le comportement d'arrêt lancé de l'instance.

Considérations

- L'activation de la protection contre la résiliation n' AWS empêche pas de mettre fin à l'instance lorsqu'un événement planifié est prévu pour mettre fin à l'instance.
- L'activation de la protection contre la résiliation n'empêche pas Amazon EC2 Auto Scaling de mettre fin à une instance lorsque celle-ci est défectueuse ou lors d'événements de montée en puissance. Vous pouvez contrôler si un groupe Auto Scaling peut résilier une instance en particulier lors de la mise à l'échelle en utilisant la protection contre la mise à l'échelle horizontale de l'instance. Vous pouvez contrôler si un groupe Auto Scaling peut résilier des instances défectueuses en suspendant le processus de mise à l'échelle ReplaceUnhealthy.
- Vous ne pouvez pas activer la protection de la résiliation pour les instances Spot.

Pour activer la protection contre la résiliation d'une instance lors du lancement

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

2. Dans le tableau de bord, sélectionnez Lancer une instance et suivez les instructions de l'assistant.
3. Sur la page Configurer les détails de l'instance, activez la case à cocher Activer la protection de la résiliation.

Pour activer la protection contre la résiliation d'une instance en cours d'exécution ou arrêtée

1. Sélectionnez l'instance, puis Actions, Instance Settings (Paramètres de l'instance) et Change Termination Protections (Changer la protection de la résiliation).
2. Choisissez Yes, Enable (Oui, Activer).

Pour désactiver la protection contre la résiliation d'une instance en cours d'exécution ou arrêtée

1. Sélectionnez l'instance, puis Actions, Instance Settings (Paramètres de l'instance) et Change Termination Protections (Changer la protection de la résiliation).
2. Choisissez Oui, désactiver.

Pour activer ou désactiver la protection contre la résiliation à l'aide de la ligne de commande.

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- modify-instance-attribute (AWS CLI)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Mettez fin à plusieurs instances grâce à une protection contre la résiliation

Si vous mettez fin à plusieurs instances dans plusieurs zones de disponibilité dans la même demande et qu'une ou plusieurs des instances spécifiées sont activées pour la protection contre la résiliation, la demande échoue avec les résultats suivants :

- Les instances spécifiées qui se trouvent dans la même zone de disponibilité que l'instance protégée ne sont pas résiliées.
- Les instances spécifiées qui se trouvent dans des zones de disponibilité différentes, où aucune autre instance spécifiée n'est protégée, sont résiliées avec succès.

Exemple

Supposons que vous disposiez des quatre instances suivantes réparties dans deux zones de disponibilité.

Instance	Zone de disponibilité	Protection contre la résiliation
Instance 1	EN TANT QUE	`Disabled`
Instance 2		`Disabled`
Instance 3	AZ B	`Enabled`
Instance 4		`Disabled`

Si vous tentez de résilier toutes ces instances dans la même demande, la demande signale un échec avec les résultats suivants :

- Les instances 1 et 2 sont mises hors service avec succès car aucune des deux instances n'est activée pour la protection contre les mises hors service.
- L'instance 3 et l'instance 4 ne parviennent pas à se terminer car l'instance 3 est activée pour la protection contre la résiliation.

Modifier le comportement d'arrêt lancé de l'instance

Par défaut, lorsque vous initiez un arrêt à partir d'une instance EBS sauvegardée par Amazon (à l'aide d'une commande telle que shutdown oupoweroff), l'instance s'arrête. Vous pouvez modifier ce comportement pour que l'instance soit résiliée à la place en modifiant l'attribut `InstanceInitiatedShutdownBehavior` de l'instance. Vous pouvez modifier cet attribut tandis que l'instance est en cours d'exécution ou arrêtée.

La commande halt ne déclenche pas un arrêt. Si elle est utilisée, l'instance ne s'arrête pas ; au lieu de cela, elle place le CPU dans `HLT` et l'instance continue de s'exécuter.

> **Note**
>
> L'attribut `InstanceInitiatedShutdownBehavior` n'est applicable que si vous procédez à l'arrêt du système d'exploitation ou de l'instance elle-même. Cela ne s'applique pas lorsque

vous arrêtez une instance à l'aide de la console `StopInstances` API ou de la EC2 console Amazon.

Vous pouvez modifier l'`InstanceInitiatedShutdownBehavior`attribut à l'aide de la EC2 console Amazon ou de la ligne de commande.

Console

Pour modifier le comportement d'arrêt lancé de l'instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance.
4. Choisissez Actions, Paramètres d'instance, Modifier le comportement d'arrêt.

   Comportement d'arrêt affiche le comportement actuel.
5. Pour modifier le comportement, pour Comportement d'arrêt, choisissez Arrêter ou Résilier.
6. Choisissez Save (Enregistrer).

Command line

Pour modifier le comportement d'arrêt lancé de l'instance

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- modify-instance-attribute (AWS CLI)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Conservation des données lors de la résiliation d'une instance

Selon votre cas d'utilisation, vous souhaiterez peut-être conserver les données relatives au volume de stockage de votre instance ou au EBS volume Amazon lorsque l'EC2instance Amazon est résiliée. Les données sur un volume de stockage d'instances ne persistent pas lorsqu'une instance est résiliée. Si vous devez conserver les données stockées sur un volume de stockage d'instance au-delà de la durée de vie de l'instance, vous devez les copier manuellement vers un stockage plus

persistant, tel qu'un EBS volume Amazon, un compartiment Amazon S3 ou un système de EFS fichiers Amazon. Pour de plus amples informations, veuillez consulter Options de stockage pour vos EC2 instances Amazon.

Pour les données relatives aux EBS volumes Amazon, Amazon EC2 utilise la valeur de l'`DeleteOnTermination`attribut de chaque EBS volume Amazon attaché afin de déterminer s'il convient de conserver ou de supprimer le volume.

La valeur par défaut de l' attribut `DeleteOnTermination` diffère selon que le volume est le volume racine de l'instance ou un volume non racine attaché à l'instance.

Volume racine

Par défaut, lorsque vous lancez une instance, l'`DeleteOnTermination`attribut du volume racine de l'instance est défini sur`true`. Par conséquent, l'action par défaut consiste à supprimer le volume racine de l'instance lorsque celle-ci est résiliée.

Volume non racine

Par défaut, lorsque vous attachez un EBS volume non root à une instance, son `DeleteOnTermination` attribut est défini sur. `false` L'action par défaut consiste donc à conserver ces volumes.

> **Note**
>
> Une fois l'instance mise hors service, vous pouvez prendre un instantané du volume conservé ou attacher celui-ci à une autre instance. Vous devez supprimer un volume pour éviter de générer des frais supplémentaires.

L'`DeleteOnTermination`attribut peut être défini par le créateur d'une instance AMI ainsi que par la personne qui lance une instance. Lorsque l'attribut est modifié par le créateur d'une instance AMI ou par la personne qui lance une instance, le nouveau paramètre remplace le paramètre AMI par défaut d'origine. Nous vous recommandons de vérifier le paramètre par défaut de l'`DeleteOnTermination`attribut après avoir lancé une instance avec unAMI.

Pour vérifier si un EBS volume Amazon sera supprimé lors de la résiliation de l'instance, consultez les détails du volume dans le volet de détails de l'instance. Dans l'onglet Storage (Stockage), sous Block devices (périphérique de stockage en mode bloc), faites défiler vers la droite pour afficher le paramètre Delete on termination (supprimer à la date de résiliation) pour le volume.

- Si la réponse est Oui, le volume sera supprimé lors de la résiliation de l'instance.
- Si la réponse est Non, le volume ne sera pas supprimé lors de la résiliation de l'instance. Tous les volumes qui ne sont pas supprimés lors de la résiliation de l'instance continueront à entraîner des frais.

Modifiez le volume racine pour qu'il persiste au lancement

À l'aide de la console, vous pouvez modifier l'attribut `DeleteOnTermination` lorsque vous lancez une instance. Pour modifier cet attribut lorsqu'il est associé à une instance en cours d'exécution, vous devez utiliser la ligne de commande.

Utilisez l'une des méthodes suivantes pour modifier le volume racine afin qu'il persiste lors du lancement.

Console

Pour modifier le volume racine d'une instance afin de le conserver lors du lancement à l'aide de la console

1. Suivez la procédure pour lancer une instance, mais ne la lancez qu'après avoir effectué les étapes suivantes pour modifier le volume racine afin qu'il persiste.
2. Sous Stockage (volumes), développez les informations sous le volume racine.
3. Pour Supprimer à la résiliation, choisissez Oui.
4. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance). Pour de plus amples informations, veuillez consulter Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console.

Command line

Modification du volume racine d'une instance pour qu'il persiste lors du lancement à l'aide de la ligne de commande

Lorsque vous lancez une instance EBS sauvegardée par -backed, vous pouvez utiliser l'une des commandes suivantes pour que le volume du périphérique racine soit persistant. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- run-instances (AWS CLI)
- New-EC2Instance (AWS Tools for Windows PowerShell)

Dans les mappages de périphérique de stockage en mode bloc pour les volumes que vous voulez conserver, incluez `--DeleteOnTermination`, et spécifiez `false`.

Par exemple, pour conserver un volume, ajoutez l'option suivante à votre commande `run-instances` :

```
--block-device-mappings file://mapping.json
```

Dans `mapping.json`, indiquez le nom du périphérique, par exemple `/dev/sda1` ou `/dev/xvda`, et pour `--DeleteOnTermination`, indiquez `false`.

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

Modifier le volume racine d'une instance en cours d'exécution pour qu'il persiste

Vous pouvez utiliser l'une des commandes suivantes pour faire en sorte que le volume du périphérique racine d'une instance EBS sauvegardée en cours d'exécution soit conservé. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- modify-instance-attribute (AWS CLI)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Par exemple, utilisez la commande suivante :

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-mappings file://mapping.json
```

Dans `mapping.json`, indiquez le nom du périphérique, par exemple `/dev/sda1` ou `/dev/xvda`, et pour `--DeleteOnTermination`, indiquez `false`.

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

Mise hors service d'instance

La mise hors service d'une instance est planifiée lorsqu'une défaillance irréparable du matériel sous-jacent hébergeant l'instance est AWS détectée. Le périphérique racine de l'instance détermine le comportement de la mise hors service de l'instance :

- Si le périphérique racine de votre instance est un EBS volume Amazon, l'instance est arrêtée et vous pouvez la redémarrer à tout moment. Le démarrage de l'instance arrêtée la migre vers un nouveau matériel.
- Si le périphérique racine de votre instance est un volume de stockage d'instance, l'instance est résiliée et ne peut pas être réutilisée.

Pour plus d'informations sur les types d'événements d'instance, consultez Événements planifiés pour les EC2 instances Amazon.

Sommaire

Identifier des instances prévues pour une mise hors service

Si votre instance est planifiée pour une mise hors service, vous recevez un courrier électronique préalable à l'événement avec l'ID d'instance et la date de mise hors service. Vous pouvez également

vérifier les instances dont la mise hors service est prévue à l'aide de la EC2 console Amazon ou de la ligne de commande.

> **Important**
>
> Si une instance est programmée pour une mise hors service, nous vous recommandons de prendre des mesures dès que possible car elle peut être inaccessible. (La notification par e-mail que vous recevez indique ce qui suit : « En raison de cette dégradation, votre instance pourrait déjà être inaccessible. ») Pour plus d'informations sur les mesures recommandées, consultez Check if your instance is reachable.

Comment identifier des instances prévues pour une mise hors service

- Notification par e-mail
- Identification par la console

Notification par e-mail

Si votre instance est planifiée pour une mise hors service, vous recevez un courrier électronique préalable à l'événement avec l'ID d'instance et la date de mise hors service.

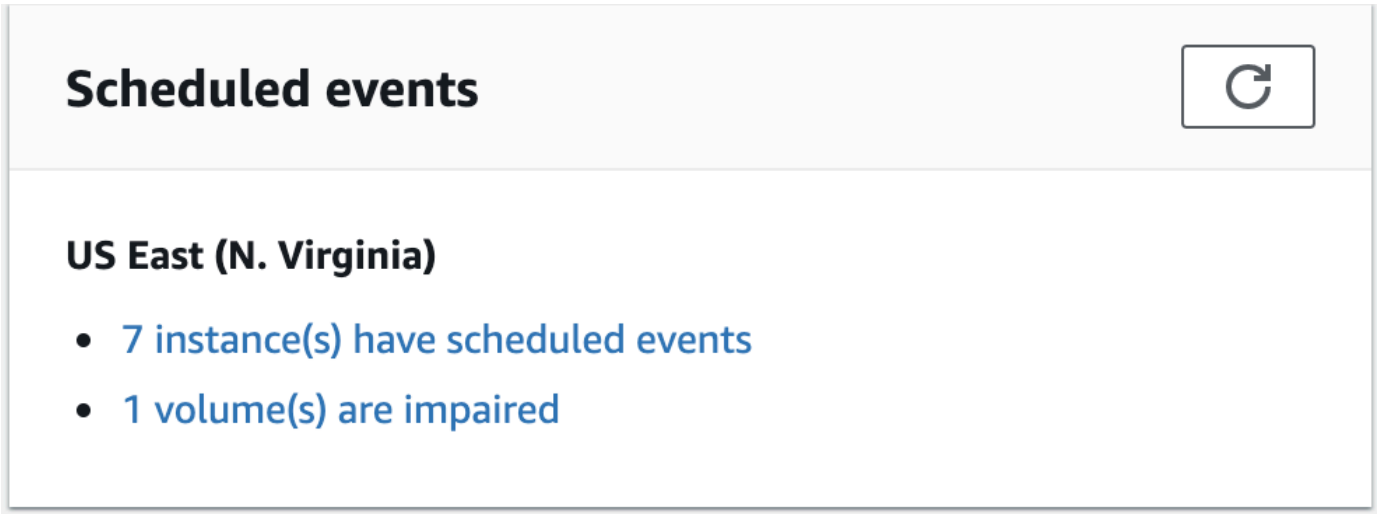
L'e-mail est envoyé au titulaire principal du compte et au contact des opérations. Pour plus d'informations sur la gestion des contacts de votre compte, voir Mettre à jour les coordonnées de votre AWS compte dans le Guide de AWS Account Managementréférence.

Identification par la console

Si vous utilisez un compte e-mail que vous ne consultez pas régulièrement, par exemple pour les notifications de mise hors service, vous pouvez utiliser la EC2 console Amazon ou la ligne de commande pour déterminer si le retrait de l'une de vos instances est prévu.

Pour identifier les instances planifiées pour une mise hors service à l'aide de la console

1. Ouvrez la EC2 console Amazon.
2. Dans le volet de navigation, choisissez EC2Dashboard. Sous Événements planifiés, vous pouvez voir les événements associés à vos EC2 instances et volumes Amazon, organisés par région.



3. Si vous avez une instance avec un événement planifié affiché, sélectionnez le lien sous le nom de la région pour accéder à la page Événements.
4. La page Events répertorie toutes les ressources qui ont des événements associés. Pour afficher les instances planifiées pour une mise hors service, sélectionnez Instance resources dans la première liste de filtres, puis Instance stop or retirement dans la deuxième liste de filtres.
5. Si les résultats du filtre affichent une instance planifiée pour une mise hors service, sélectionnez-la et notez les date et heure dans le champ Start time du volet des détails. Il s'agit de la date de mise hors service de votre instance.

Pour identifier les instances planifiées pour une mise hors service à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- describe-instance-status (AWS CLI)
- Get-EC2InstanceStatus (AWS Tools for Windows PowerShell)

Mesures à prendre pour les instances EBS sauvegardées dont la mise hors service est prévue

Pour conserver les données de votre instance mise hors service, vous pouvez effectuer l'une des actions suivantes. Il est important que vous preniez cette action avant la date de mise hors service de l'instance, afin de prévenir tout arrêt et perte de données imprévus.

Pour les instances Linux, si vous ne savez pas si votre instance est sauvegardée par EBS un magasin d'instances, consultezVolumes root pour vos EC2 instances Amazon.

Vérifier si votre instance est accessible

Lorsque vous êtes averti que votre instance est programmée pour une mise hors service, nous vous recommandons de prendre les mesures suivantes dès que possible :

- Vérifiez si votre instance est accessible en vous connectant ou en envoyant une demande ping à celle-ci.
- Si votre instance est accessible, vous devez prévoir de l'arrêter/la démarrer à un moment approprié avant la date de mise hors service prévue, lorsque l'impact est minime. Pour plus d'informations sur l'arrêt et le redémarrage de votre instance, et sur ce que vous devez escompter quand votre instance est arrêtée, comme les conséquences sur les adresses publiques, privées et IP Elastic associées à votre instance, consultez Arrêtez et démarrez les EC2 instances Amazon. Veuillez noter que les données sur les volumes de stockage d'instances sont perdues lorsque vous arrêtez et démarrez votre instance.
- Si votre instance est inaccessible, vous devez prendre des mesures immédiates et effectuer un arrêt/démarrage pour la récupérer.
- Sinon, si vous souhaitez mettre fin à votre instance, prévoyez de le faire dès que possible, afin de cesser d'engager des frais pour cette dernière.

Créez une sauvegarde de votre instance

Créez un EBS -backed AMI à partir de votre instance afin de disposer d'une sauvegarde. Pour garantir l'intégrité des données, arrêtez l'instance avant de créer leAMI. Vous pouvez attendre la date de mise hors service planifiée quand l'instance est arrêtée ou arrêtez l'instance vous-même avant la date de mise hors service. Vous pouvez redémarrer l'instance à tout moment. Pour de plus amples informations, veuillez consulter Créez un compte soutenu EBS par Amazon AMI.

Lancement d'une instance de remplacement

Après avoir créé une instance AMI à partir de votre instance, vous pouvez l'utiliser AMI pour lancer une instance de remplacement. Dans la EC2 console Amazon, sélectionnez votre nouvelle instance, AMI puis choisissez Launch instance from AMI. Configurez les paramètres de votre instance, puis choisissez Launch instance. Pour plus d'informations concernant chaque champ, consultez Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console.

Mesures à prendre pour les instances sauvegardées dans le stockage d'instances dont la mise hors service est prévue

Pour conserver les données de votre instance mise hors service, vous pouvez effectuer l'une des actions suivantes. Il est important que vous preniez cette action avant la date de mise hors service de l'instance, afin de prévenir tout arrêt et perte de données imprévus.

> **Warning**
>
> Si votre instance basée sur le stockage d'instances dépasse sa date de mise hors service, elle est terminée et vous ne pouvez pas récupérer l'instance ou les données qui y étaient stockées. Quel que soit le périphérique racine de votre instance, les données sur les volumes de stockage d'instance sont perdues lorsque l'instance est retirée, même si les volumes sont attachés à une instance EBS sauvegardée.

Vérifier si votre instance est accessible

Lorsque vous êtes averti que votre instance est programmée pour une mise hors service, nous vous recommandons de prendre les mesures suivantes dès que possible :

- Vérifiez si votre instance est accessible en vous connectant ou en envoyant une demande ping à celle-ci.
- Si votre instance est inaccessible, les chances de la récupérer sont vraiment très réduites. Pour plus d'informations, consultezRésoudre les problèmes liés à une instance Amazon inaccessible EC2. AWS mettra fin à votre instance à la date de mise hors service prévue. Ainsi, dans le cas d'une instance inaccessible, vous pouvez immédiatement mettre fin à l'instance vous-même.

Lancement d'une instance de remplacement

Créez une instance sauvegardée en magasin AMI à partir de votre instance à l'aide AMI des outils décrits dans. Création d'une instance sauvegardée en magasin AMI Dans la EC2 console Amazon, sélectionnez votre nouvelle instance, AMI puis choisissez Launch instance from AMI. Configurez les paramètres de votre instance, puis choisissez Launch instance. Pour plus d'informations concernant chaque champ, consultez Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console.

Convertissez votre instance en instance EBS sauvegardée

Transférez vos données vers un EBS volume, prenez un instantané du volume, puis créez AMI à partir de cet instantané. Vous pouvez lancer une instance de remplacement à partir de votre nouvelle instanceAMI. Pour de plus amples informations, veuillez consulter Convertissez votre instance sauvegardée par le stockage en une instance sauvegardée par -backed AMI EBS AMI.

Résilience des instances

> **Important**
>
> Les informations suivantes s'appliquent à la configuration des fonctionnalités liées à la restauration sur des instances saines. Si vous rencontrez actuellement des difficultés pour accéder à votre instance, consultez Résoudre les problèmes liés aux EC2 instances.

S'il s'avère qu' AWS une instance n'est pas disponible en raison d'un problème matériel sous-jacent, vous pouvez configurer deux mécanismes pour garantir la résilience de l'instance afin de rétablir la disponibilité : la restauration automatique simplifiée et la restauration basée sur CloudWatch l'action Amazon. Ce processus est appelé restauration d'instance.

Au moins un mécanisme doit être configuré ou activé à l'avance avec les ressources prises en charge pour que le processus de restauration de l'instance ait lieu. Par défaut, la restauration automatique simplifiée est activée pour les instances prises en charge lors de leur lancement.

Rubriques

- Présentation de la restauration d'instances
- Alternatives de restauration d'instance
- Configuration de la restauration basée sur l' CloudWatch action
- Configuration d'une restauration automatique simplifiée

Présentation de la restauration d'instances

Voici des exemples de problèmes matériels sous-jacents susceptibles de nécessiter une restauration d'instance :

- Perte de connectivité réseau
- Perte d'alimentation système
- Problèmes logiciels sur un hôte physique

- Problèmes matériels sur un hôte physique ayant un impact sur l'accessibilité du réseau

Une instance récupérée est identique à l'instance d'origine, notamment :

- ID d'instance
- Adresses IP publiques, privées et élastiques
- Métadonnées de l'instance
- Groupe de placement
- EBSVolumes joints
- Zone de disponibilité

Une restauration d'instance réussie apparaîtra à l'instance comme un redémarrage imprévu. En d'autres termes, le contenu stocké dans la mémoire volatile sera perdu, les données du stockage d'instance seront effacées et le temps de fonctionnement du système d'exploitation recommencera à zéro.

Pour vous protéger contre la perte de données, nous vous recommandons de créer régulièrement des sauvegardes de données importantes. Pour plus d'informations sur les meilleures pratiques de sauvegarde et de restauration pour les EC2 instances Amazon, consultez la section Meilleures pratiques pour Amazon EC2.

Alternatives de restauration d'instance

Les alternatives suivantes à la restauration d'instance peuvent être envisagées lorsqu'elles répondent au cas d'utilisation de vos instances.

Groupes Auto Scaling

Vous pouvez utiliser les groupes Auto Scaling pour regrouper un ensemble d'instances à des fins de dimensionnement et de disponibilité. Si une instance d'un groupe Auto Scaling devient indisponible, elle sera automatiquement remplacée (et non récupérée) par le groupe Auto Scaling. Pour plus d'informations, consultez Qu'est-ce qu'Amazon EC2 Auto Scaling ? dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.

Amazon EBS Multi-Attach

Vous pouvez configurer Amazon EBS Multi-Attach pour vos instances afin de permettre à plusieurs instances d'être connectées au même EBS volume. Combiné à un logiciel approprié,

cela permet d'activer le clustering à haute disponibilité. Pour un exemple de configuration avec des instances Linux, consultez la section Stockage en cluster simplifié : GFS2 sur les volumes compatibles avec Amazon EBS Multi-Attach sur le blog AWS de stockage.

Configuration de la restauration basée sur l' CloudWatch action

Important

- Les informations suivantes s'appliquent à la configuration des fonctionnalités liées à la restauration sur des instances saines. Si vous rencontrez actuellement des difficultés pour accéder à votre instance, consultez Résoudre les problèmes liés aux EC2 instances.
- Pour que votre charge de travail fonctionne correctement après une restauration d'instance réussie, celle-ci doit démarrer et accepter le trafic sans intervention manuelle.

Vous pouvez configurer la restauration basée sur CloudWatch l'action Amazon pour ajouter des actions de restauration aux CloudWatch alarmes Amazon. CloudWatch la restauration basée sur l'action fonctionne avec la `StatusCheckFailed_System` métrique. CloudWatch la restauration basée sur les actions fournit une to-the-minute granularité du temps de réponse et des notifications Amazon Simple Notification Service (AmazonSNS) concernant les actions de restauration et les résultats. Ces options de configuration permettent des tentatives de restauration plus rapides grâce à un contrôle plus précis de la réponse à l'échec de la vérification de l'état du système, par rapport à une restauration automatique simplifiée. Pour plus d'informations sur les CloudWatch options disponibles, consultez la section Contrôles de statut de vos instances.

La restauration basée sur CloudWatch l'action d'Amazon ne fonctionne pas lors d'événements de service dans le AWS Health Dashboard. Pour de plus amples informations, veuillez consulter the section called “Résolution des défaillances de restauration basées sur l' CloudWatchaction”.

Rubriques

- Exigences et limites de la restauration basée sur CloudWatch l'action
- Configuration de la restauration basée sur l' CloudWatchaction
- Résolution des défaillances de restauration basées sur l' CloudWatchaction

Exigences et limites de la restauration basée sur CloudWatch l'action

CloudWatch la restauration basée sur l'action peut tenter de récupérer une instance si elle :

- Est dans l'`running`État. Pour de plus amples informations, veuillez consulter the section called "Changements d'état de l'instance".
- Utilisations `default` (à la demande) ou location d'`dedicated`instance. Pour de plus amples informations, veuillez consulter the section called "Options de facturation et d'achat".
- Il s'agit d'un type d'instance pour lequel Amazon EC2 dispose de capacités disponibles. Dans certaines situations, telles que des pannes importantes, la capacité disponible sera insuffisante et certaines tentatives de restauration risquent d'échouer.
- N'utilise pas la location d'`dedicated`instance. Pour les hôtes Amazon EC2 Dedicated, vous pouvez utiliser Dedicated Host Auto Recovery pour récupérer automatiquement les instances défectueuses.
- N'utilise pas d'adaptateur Elastic Fabric.
- N'est pas membre d'un groupe Auto Scaling.
- Ne fait actuellement l'objet d'aucun événement de maintenance planifié.
- Utilise l'un des types d'instance suivants :
  - Usage général : A1 | M3 | M4 | M5 | M5a | M5n | M5zn | M6a | M6g | M6i | M6in | M7a | M7g | M7i | M7i-flex | T1 | T2 | T3 | T3a | T4g
  - Optimisé pour le calcul : C3 | C4 | C5 | C5a | C5n | C6a | C6g | C6gn | C6i | C6in | C7a | C7g | C7gn | C7i | C7i-Flex
  - Mémoire optimisée : R3 | R4 | R5 | R5a | R5b | R5n | R6a | R6g | R6i | R6in | R7a | R7g | R7i | R7iz | R8g | u-3tb1 | u-6tb1 | u-12tb1 | u-18tb1 | u-24tb1 | u7i-12tb | u7 en 16 To | U7 en 24 To | U7 en 32 To | X1 | X1e | X2ieZN
  - Calcul accéléré : G3 | G3s | G5g | Inf1 | P2 | P3 | VT1
  - Calcul haute performance : hPC6a | hPC7a | hPC7g
  - Instances métalliques : n'importe lequel des types ci-dessus avec la taille de l'instance métallique.
- Possède des volumes de stockage d'instance et utilise l'un des types d'instance suivants : M3 | C3 | R3 | X1 | X1e | X2idn | X2iEDN

⚠ Warning

- Les données relatives aux volumes de stockage de l'instance seront perdues si l'instance est arrêtée. Pour plus d'informations sur l'arrêt d'une instance, consultezthe section called "Instances arrêtées".
- En cas d'échec de la vérification de l'état du système, les données mappées du périphérique de stockage et de bloc de l'instance peuvent être perdues. Pour ces types d'instances, vous pouvez envisager d'utiliserthe section called "Activer la protection de la résiliation".

Nous vous recommandons de créer régulièrement des sauvegardes de données importantes. Pour plus d'informations sur les meilleures pratiques de sauvegarde et de restauration pour AmazonEC2, consultez la section Meilleures pratiques pour Amazon EC2.

Vous pouvez également utiliser le AWS Management Console ou le AWS CLI pour afficher les types d'instances qui prennent en charge la restauration basée sur CloudWatch l'action.

Console

Pour voir les types d'instances qui prennent en charge la restauration basée sur CloudWatch l'action d'Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation de gauche, choisissez Instance Types (Types d'instance).
3. Dans la barre de filtre, saisissez Auto Recovery support: true (Prise en charge de la restauration automatique : vrai). Sinon, lorsque vous saisissez les caractères et que le nom du filtre apparaît, vous pouvez le sélectionner.

   Le tableau des types d'instances affiche tous les types d'instances qui prennent en charge la restauration basée sur CloudWatch l'action Amazon.

AWS CLI

Pour voir les types d'instances qui prennent en charge la restauration basée sur CloudWatch l'action d'Amazon

Utilisez la describe-instance-typescommande.

```
aws ec2 describe-instance-types --filters Name=auto-recovery-supported,Values=true
--query "InstanceTypes[*].[InstanceType]" --output text | sort
```

Configuration de la restauration basée sur l' CloudWatchaction

CloudWatch la restauration basée sur l'action fonctionne avec la `StatusCheckFailed_System` métrique. CloudWatch la restauration basée sur l'action est configurée via la CloudWatch console. Pour configurer la restauration basée sur CloudWatch l'action, consultez la section Ajouter des actions de restauration aux CloudWatch alarmes dans le guide de CloudWatch l'utilisateur Amazon.

Résolution des défaillances de restauration basées sur l' CloudWatchaction

Les problèmes suivants peuvent entraîner l'échec de la restauration de votre instance avec une restauration basée sur l' CloudWatch action :

- CloudWatch la restauration basée sur l'action ne fonctionne pas lors d'événements de service dans le AWS Health Dashboard. Il se peut que vous ne receviez pas de notifications d'échec de récupération pour de tels événements. Pour obtenir les dernières informations sur la disponibilité du service, consultez la page État de santé du service.
- Capacité temporaire, insuffisante du matériel de remplacement.
- L'instance a atteint l'indemnité journalière maximale pour les tentatives de rétablissement. Votre instance pourrait ensuite être retirée si la récupération automatique échoue et si une dégradation matérielle est la cause première de l'échec du contrôle de statut du système d'origine.

Si l'échec de la vérification de l'état du système de l'instance persiste malgré plusieurs tentatives de restauration, consultez Résoudre les problèmes des instances dont les vérifications d'état ont échoué pour obtenir des instructions supplémentaires.

Configuration d'une restauration automatique simplifiée

> **Important**
>
> - Les informations suivantes s'appliquent à la configuration des fonctionnalités liées à la restauration sur des instances saines. Si vous rencontrez actuellement des difficultés pour accéder à votre instance, consultez Résoudre les problèmes liés aux EC2 instances.

- Pour que votre charge de travail fonctionne correctement après une restauration d'instance réussie, celle-ci doit démarrer et accepter le trafic sans intervention manuelle.

Par défaut, la restauration automatique simplifiée surveille toutes les instances en cours d'exécution prises en charge. En cas d'échec de la vérification de l'état du système, des tentatives de restauration automatique simplifiées visent à rétablir l'état sain de l'instance. La restauration automatique simplifiée ne fonctionne pas lors d'événements de service dans le AWS Health Dashboard. Pour de plus amples informations, veuillez consulter the section called "Résolution des défaillances de restauration automatique simplifiées".

Lorsqu'un événement de restauration automatique simplifié se produit, vous recevez un AWS Health Dashboard événement. Pour configurer les notifications relatives à ces événements, reportez-vous à la section Getting Started with Notifications des utilisateurs AWS du guide de Notifications des utilisateurs AWS l'utilisateur. Vous pouvez également utiliser EventBridge les règles Amazon pour surveiller les événements de restauration automatique simplifiés à l'aide des codes d'événement suivants :

- `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS` – événements réussis
- `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE` – événements échoués

Pour plus d'informations, consultez les EventBridge règles d'Amazon.

Rubriques

Exigences et limites pour une restauration automatique simplifiée

La restauration automatique simplifiée tentera de récupérer une instance si elle :

- Est dans l'`running`État. Pour de plus amples informations, veuillez consulter the section called "Changements d'état de l'instance".
- Utilisations `default` (à la demande) ou `dedicated` location. Pour de plus amples informations, veuillez consulter the section called "Options de facturation et d'achat".

- Il s'agit d'un type d'instance pour lequel Amazon EC2 dispose de capacités disponibles. Dans certaines situations, telles que des pannes importantes, la capacité disponible sera insuffisante et certaines tentatives de restauration risquent d'échouer.
- N'utilise pas la `host` location. Pour les hôtes Amazon EC2 Dedicated, vous pouvez utiliser Dedicated Host Auto Recovery pour récupérer automatiquement les instances défectueuses.
- N'utilise pas d'adaptateur Elastic Fabric.
- Il ne s'agit pas d'une taille d'`metal`instance.
- N'est pas membre d'un groupe Auto Scaling.
- Ne fait actuellement l'objet d'aucun événement de maintenance planifié.
- Ne possède pas de volumes de stockage d'instance.
- Utilise l'un des types d'instance suivants :
  - Usage général : A1 | M3 | M4 | M5 | M5a | M5n | M5zn | M6a | M6g | M6i | M6in | M7a | M7g | M7i | M7i-flex | T1 | T2 | T3 | T3a | T4g
  - Optimisé pour le calcul : C3 | C4 | C5 | C5a | C5n | C6a | C6g | C6gn | C6i | C6in | C7a | C7g | C7gn | C7i | C7i-Flex
  - Mémoire optimisée : R3 | R4 | R5 | R5a | R5b | R5n | R6a | R6g | R6i | R6in | R7a | R7g | R7i | R7iz | R8g | u-3tb1 | u-6tb1 | u-12tb1 | u-18tb1 | u-24tb1 | u7i-12tb | u7 en 16 To | U7 en 24 To | U7 en 32 To | X1 | X1e | X2ieZN
  - Calcul accéléré : G3 | G3s | G5g | Inf1 | P2 | P3 | VT1
  - Calcul haute performance : hPC6a | hPC7a | hPC7g

> **Warning**
>
> - Les données relatives aux volumes de stockage de l'instance seront perdues si l'instance est arrêtée. Pour plus d'informations sur l'arrêt d'une instance, consultezthe section called "Instances arrêtées".
> - En cas d'échec de la vérification de l'état du système, les données mappées du périphérique de stockage et de bloc de l'instance peuvent être perdues. Pour ces types d'instances, vous pouvez envisager d'utiliserthe section called "Activer la protection de la résiliation".

Nous vous recommandons de créer régulièrement des sauvegardes de données importantes. Pour plus d'informations sur les meilleures pratiques de sauvegarde et de restauration pour AmazonEC2, consultez la section Meilleures pratiques pour Amazon EC2.

Configuration d'une restauration automatique simplifiée

La restauration automatique simplifiée est activée par défaut lorsque vous lancez une instance prise en charge. Vous pouvez définir le comportement de restauration automatique `disabled` pendant ou après le lancement de l'instance. La `default` configuration n'active pas la restauration automatique simplifiée pour un type d'instance non pris en charge.

Console

Pour désactiver la récupération automatique simplifiée lors du lancement de l'instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances, puis Launch instance (Lancer une instance).
3. Dans la section Advanced details (Détails avancés), pour nstance auto-recovery (Récupération automatique de l'instance), sélectionnez Disabled (Désactivé).
4. Configurez les paramètres de lancement de l'instance restants selon les besoins, puis lancez l'instance.

Désactivation de la récupération automatique simplifiée d'une instance en cours d'exécution ou arrêtée

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance, puis choisissez Actions, Instance Settings (Paramètres de l'instance), Change auto-recovery Behavior (Changer le comportement de restauration automatique).
4. Choisissez Off (Désactiver), puis Save (Enregistrer).

Pour définir le comportement de récupération automatique sur **`default`** pour une instance en cours d'exécution ou arrêtée

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance, puis choisissez Actions, Instance Settings (Paramètres de l'instance), Change auto-recovery Behavior (Changer le comportement de restauration automatique).
4. Choisissez Par défaut (Activé), puis Enregistrer.

AWS CLI

Désactivation de la récupération automatique simplifiée au lancement

Utilisez la commande run-instances.

```
aws ec2 run-instances \
--image-id ami-1a2b3c4d \
--instance-type t2.micro \
--key-name MyKeyPair \
--maintenance-options AutoRecovery=Disabled \
  [...]
```

Désactivation de la récupération automatique simplifiée d'une instance en cours d'exécution ou arrêtée

Utilisez la modify-instance-maintenance-optionscommande.

```
aws ec2 modify-instance-maintenance-options \
--instance-id i-0abcdef1234567890 \
--auto-recovery disabled
```

Pour définir le comportement de récupération automatique sur **`default`** pour une instance en cours d'exécution ou arrêtée

Utilisez la modify-instance-maintenance-optionscommande.

```
aws ec2 modify-instance-maintenance-options \
--instance-id i-0abcdef1234567890 \
```

```
--auto-recovery default
```

Résolution des défaillances de restauration automatique simplifiées

Les problèmes suivants peuvent entraîner l'échec de la restauration de votre instance avec restauration automatique simplifiée :

- La restauration automatique simplifiée ne fonctionne pas lors d'événements de service dans le AWS Health Dashboard. Il se peut que vous ne receviez pas de notifications d'échec de récupération pour de tels événements. Pour obtenir les dernières informations sur la disponibilité du service, consultez la page État de santé du service.
- Capacité temporaire, insuffisante du matériel de remplacement.
- L'instance a atteint l'indemnité journalière maximale pour les tentatives de rétablissement. Votre instance pourrait ensuite être retirée si la récupération automatique échoue et si une dégradation matérielle est la cause première de l'échec du contrôle de statut du système d'origine.

Si l'échec de la vérification de l'état du système de l'instance persiste malgré plusieurs tentatives de restauration, consultez Résoudre les problèmes des instances dont les vérifications d'état ont échoué pour obtenir des instructions supplémentaires.

Utiliser les métadonnées de l'instance pour gérer votre EC2 instance

Les métadonnées d'instance sont des données portant sur votre instance que vous pouvez utiliser pour configurer ou gérer l'instance en cours d'exécution. Les métadonnées de l'instance incluent les éléments suivants :

Propriétés des métadonnées de l'instance

Les propriétés des métadonnées de l'instance sont divisées en catégories, par exemple le nom d'hôte, les événements et les groupes de sécurité.

Données dynamiques

Les données dynamiques sont des métadonnées générées lors du lancement de l'instance, telles qu'un document d'identité d'instance. Pour de plus amples informations, veuillez consulter Catégories de données dynamiques.

Données utilisateur

Vous pouvez également utiliser les métadonnées de l'instance pour accéder aux données utilisateur que vous avez spécifiées lors du lancement de votre instance. Par exemple, vous pouvez spécifier des paramètres pour la configuration de votre instance ou inclure un script simple. Vous pouvez également créer des fichiers génériques AMIs et utiliser les données utilisateur pour modifier les fichiers de configuration fournis au moment du lancement. Par exemple, si vous gérez des serveurs Web pour différentes petites entreprises, elles peuvent toutes utiliser le même générique AMI et récupérer leur contenu à partir d'un compartiment Amazon S3 que vous spécifiez dans les données utilisateur au lancement. Pour ajouter un nouveau client à tout moment, créez un compartiment pour le client, ajoutez son contenu et lancez-le AMI avec le nom de compartiment unique fourni dans votre code dans les données utilisateur. Si vous lancez plusieurs instances à l'aide du même `RunInstances` appel, les données utilisateur sont disponibles pour toutes les instances de cette réservation. Chaque instance faisant partie de la même réservation possède un `ami-launch-index` numéro unique, ce qui vous permet d'écrire du code qui contrôle ce que font les instances. Par exemple, le premier hôte peut s'élire comme nœud d'origine dans un cluster. Pour un exemple de AMI lancement détaillé, voirIdentifiez chaque instance lancée en une seule demande.

> **Important**
>
> Bien que les métadonnées d'instance et les données utilisateur ne soient accessibles qu'au sein de l'instance elle-même, elles ne sont pas protégées par des méthodes d'authentification ou de chiffrement. Toute personne ayant un accès direct à l'instance, et potentiellement tout logiciel s'exécutant sur l'instance, peut afficher ses métadonnées. Vous ne devez donc pas stocker de données sensibles, telles que des mots de passe ou des clés de chiffrement à longue durée, ou des données utilisateur.

Table des matières

- Identifiez chaque instance lancée en une seule demande

Catégories de métadonnées d'instance

Les propriétés des métadonnées de l'instance sont divisées en catégories. Pour récupérer les propriétés des métadonnées de l'instance, vous spécifiez la catégorie dans la demande, et les métadonnées sont renvoyées dans la réponse.

Lorsque de nouvelles catégories sont publiées, un nouveau build de métadonnées d'instance est créé avec un nouveau numéro de version. Dans le tableau suivant, la colonne Version when category was released (Version lors de la publication de la catégorie) indique la version du build lorsqu'une catégorie de métadonnées d'instance a été publiée. Pour éviter d'avoir à mettre à jour votre code chaque fois qu'Amazon EC2 publie une nouvelle version de métadonnées d'instance, utilisez `latest` plutôt le numéro de version dans vos demandes de métadonnées. Pour de plus amples informations, veuillez consulter Obtenir les versions disponibles des métadonnées d'instance.

Lorsqu'Amazon EC2 publie une nouvelle catégorie de métadonnées d'instance, les métadonnées d'instance de la nouvelle catégorie peuvent ne pas être disponibles pour les instances existantes. Avec une instance basée sur le système Nitro, vous ne pouvez récupérer les métadonnées de l'instance que pour les catégories qui étaient disponibles au lancement. Pour une instance avec l'hyperviseur Xen, vous pouvez l'arrêter puis la démarrer afin de mettre à jour les catégories disponibles pour cette instance.

Le tableau ci-après répertorie les catégories de métadonnées d'instance. Certains noms de catégorie incluent des espaces réservés pour les données, qui sont propres à votre instance. Par exemple, *`mac`* représente l'MACadresse de l'interface réseau. Quand vous récupérez les métadonnées de l'instance, vous devez remplacer les espaces réservés par des valeurs réelles.

Catégorie	Description	Version lors de la publication de la catégorie
`ami-id`	AMIID utilisé pour lancer l'instance.	1.0
`ami-launch-index`	Si vous lancez plusieurs instances à l'aide du même `RunInstances` appel, cette valeur indique l'ordre de lancement de chaque	1.0

Catégorie	Description	Version lors de la publication de la catégorie
	instance. La valeur 0 indique la première instance lancée. Si vous lancez des instances à l'aide d'Auto Scaling ou de EC2 fleet, cette valeur est toujours égale à 0.	
`ami-manifest-path`	Le chemin d'accès au fichier AMI manifeste dans Amazon S3. Si vous avez utilisé une instance EBS soutenue par Amazon AMI pour lancer l'instance, le résultat renvoyé est`unknown`.	1.0
`ancestor-ami-ids`	Le AMI IDs de toutes les instances qui ont été regroupées pour créer cela. AMI Cette valeur n'exister a que si le fichier AMI manifeste contient une `ancestor-amis` clé.	2007-10-10

Catégorie	Description	Version lors de la publication de la catégorie
`autoscaling/target-lifecycle-state`	Valeur indiquant l'état cible du cycle de vie Auto Scaling vers lequel une instance Auto Scaling est en train de passer. Présent lorsque l'instance passe à l'un des états de cycle de vie cibles après le 10 mars 2022. Valeurs possibles : `Detached | InService | Standby | Terminated | Warmed:Hibernated | Warmed:Running | Warmed:Stopped | Warmed:Terminated`. Consultez la section Récupérer l'état du cycle de vie cible via les métadonnées de l'instance dans le manuel Amazon EC2 Auto Scaling User Guide.	15/07/2021
`block-device-mapping/ami`	Le périphérique virtuel qui contient le système de fichiers racine/démarrage.	2007-12-15
`block-device-mapping/ebs` N	Les appareils virtuels associés à tous les EBS volumes Amazon. Les EBS volumes Amazon ne sont disponibles dans les métadonnées que s'ils étaient présents au moment du lancement ou lors du dernier démarrage de l'instance. Le N indique l'indice du EBS volume Amazon (tel que `ebs1` ou `ebs2`).	2007-12-15

Catégorie	Description	Version lors de la publication de la catégorie
`block-device-mapping/ephemeral` N	Les périphériques virtuels pour tous les volumes de stockage NVMe autres que les instances . Le N indique l'index de chaque volume. Le nombre de volumes de stockage d'instances dans le mappage d'appareils en bloc peut ne pas correspondre au nombre réel de volumes de stockage d'instances pour l'instance. Le type d'instance détermine le nombre de volumes de stockage d'instances disponibles pour une instance. Si le nombre de volumes de stockage d'instances dans un mappage d'appareils en bloc dépasse le nombre disponible pour une instance, les volumes de stockage d'instances supplémentaires sont ignorés.	2007-12-15
`block-device-mapping/root`	Les périphériques ou partitions virtuels associés aux périphéri ques ou partitions racines sur le périphérique virtuel où le système de fichiers racine (/ ou C:) est associé avec l'instance donnée.	2007-12-15
`block-device-mapping/swap`	Les périphériques virtuels associés avec `swap`. Pas toujours présents.	2007-12-15

Catégorie	Description	Version lors de la publication de la catégorie
`elastic-gpus/associations/ elastic-gpu-id`	Si un Elastic est GPU attaché à l'instance, il contient une JSON chaîne contenant des informations sur l'ElasticGPU, notamment son identifiant et ses informations de connexion.	2016-11-30
`elastic-inference/associations/ eia-id`	Si un accélérateur Elastic Inference est attaché à l'instance, il contient une JSON chaîne contenant des informations sur l'accélérateur Elastic Inference, notamment son ID et son type.	2018-11-29
`events/maintenance/history`	Si des événements de maintenance sont terminés ou annulés pour l'instance, contient une JSON chaîne contenant des informations sur les événements.	2018-08-17
`events/maintenance/scheduled`	S'il existe des événements de maintenance actifs pour l'instance, contient une JSON chaîne contenant des informations sur ces événements. Pour de plus amples informations, veuillez consulter Afficher les événements planifiés qui affectent vos EC2 instances Amazon.	2018-08-17

Catégorie	Description	Version lors de la publication de la catégorie
`events/recommendations/rebalance`	Heure approximative, enUTC, à laquelle la notification de recommandation de rééquilibrage d'EC2instance est émise pour l'instance. Voici un exemple de métadonnées pour cette catégorie : `{"noticeTime": "2020-11-05T08:22:00Z"}` . Cette catégorie n'est disponible qu'après l'émission de la notification. Pour de plus amples informations, veuillez consulter EC2recommandations de rééquilibrage des instances.	27/10/2020
`hostname`	Si l'EC2instance utilise un nommage basé sur l'adresse IP (IPBN), il s'agit du IPv4 DNS nom d'hôte privé de l'instance. Si l'EC2instance utilise le nommage basé sur les ressources (RBN), il s'agit du. RBN Dans le cas où plusieurs interfaces réseau sont présentes, cela fait référence au périphérique eth0 (le périphérique dont le numéro de périphérique est 0). Pour plus d'informations sur IPBN etRBN, voirTypes de noms EC2 d'hôte des instances Amazon.	1.0

Catégorie	Description	Version lors de la publication de la catégorie
`iam/info`	Si un IAM rôle est associé à l'instance, contient des informations sur la dernière mise à jour du profil de l'instance, y compris la LastUpdated date de l'instance InstanceProfileArn, etInstanceProfileId. Sinon, absent.	2012-01-12
`iam/security-credentials/role-name`	Si un IAM rôle est associé à l'instance, *`role-name`* est le nom du rôle, et *`role-name`* contient les informations d'identification de sécurité temporaires associées au rôle (pour plus d'informations, voirExtraire les informations d'identification de sécurité à partir des métadonnées d'instance). Sinon, absent.	2012-01-12
`identity-credentials/ec2/info`	Informations sur les informations d'identification dans `identity-credentials/ec2/security-credentials/ec2-instance` .	2018-05-23

Catégorie	Description	Version lors de la publication de la catégorie
`identity-credentials/ec2/security-credentials/ec2-instance`	Informations d'identification pour le rôle d'identité d'instance qui permettent au logiciel sur instance de s'identifier afin de AWS prendre en charge des fonctionnalités telles qu'EC2Instance Connect et la configuration de gestion d'hôte AWS Systems Manager par défaut. Aucune politique n'est attachée à ces informations d'identification. Elles ne disposent donc d'aucune AWS API autorisation supplémentaire au-delà de l'identification de l'instance par rapport à la AWS fonctionnalité. Pour de plus amples informations, veuillez consulter Rôles d'identité d'instance pour les EC2 instances Amazon.	2018-05-23
`instance-action`	Informe l'instance qu'elle devrait redémarrer en vue de la création d'un bundle. Valeurs valides : `none` | `shutdown` | `bundle-pending` .	2008-09-01
`instance-id`	L'ID de cette instance.	1.0
`instance-life-cycle`	Option d'achat de cette instance. Pour plus d'informations, consultez Options EC2 de facturation et d'achat Amazon.	01-10-2019

Catégorie	Description	Version lors de la publication de la catégorie
`instance-type`	Le type d'instance. Pour plus d'informations, consultez Types d'EC2instances Amazon.	2007-08-29
`ipv6`	IPv6Adresse de l'instance. Dans les cas où plusieurs interfaces réseau sont présentes, cela fait référence à l'interface réseau du périphérique eth0 (le périphérique dont le numéro de périphérique est 0) et à la première IPv6 adresse attribuée. Si aucune IPv6 adresse n'existe sur l'interface réseau [0], cet élément n'est pas défini et entraîne une réponse HTTP 404.	03/01/2021
`kernel-id`	L'ID du noyau lancé avec l'instanc e, le cas échéant.	2008-02-01

Catégorie	Description	Version lors de la publication de la catégorie
`local-hostname`	Dans le cas où plusieurs interfaces réseau sont présentes, cela fait référence au périphérique eth0 (le périphérique dont le numéro de périphérique est 0). Si l'EC2instance utilise un nommage basé sur l'adresse IP (IPBN), il s'agit du IPv4 DNS nom d'hôte privé de l'instance. Si l'EC2instance utilise le nommage basé sur les ressources (RBN), il s'agit du. RBN Pour plus d'informations sur IPBNRBN, et la dénomination des EC2 instances, consultezTypes de noms EC2 d'hôte des instances Amazon.	2007-01-19
`local-ipv4`	IPv4Adresse privée de l'instance. Dans le cas où plusieurs interfaces réseau sont présentes, cela fait référence au périphérique eth0 (le périphérique dont le numéro de périphérique est 0). S'il s'agit d'une instance IPv6 uniquement, cet élément n'est pas défini et entraîne une réponse HTTP 404.	1.0

Catégorie	Description	Version lors de la publication de la catégorie
`mac`	Adresse de contrôle d'accès au média (MAC) de l'instance. Dans le cas où plusieurs interfaces réseau sont présentes, cela fait référence au périphérique eth0 (le périphéri que dont le numéro de périphéri que est 0).	2011-01-01
`metrics/vhostmd`	Plus disponible.	2011-05-01
`network/interfaces/ macs/mac/device-number`	Le numéro de périphérique unique associé à cette interface. Le numéro de périphérique correspon d au nom du périphérique, par exemple un `device-number` de 2 est pour le périphérique eth2. Cette catégorie correspon d aux `device-index` champs `DeviceIndex` et utilisés par Amazon EC2 API et aux EC2 commandes pour le AWS CLI.	2011-01-01
`network/interfaces/ macs/mac/interface-id`	L'ID de l'interface réseau.	2011-01-01
`network/interfaces /macs/mac/ipv4-as sociations/public-ip`	Les IPv4 adresses privées associées à chaque adresse IP publique et attribuées à cette interface.	2011-01-01
`network/interfaces/ macs/mac/ipv6s`	Les IPv6 adresses attribuées à l'interface.	2016-06-30

Catégorie	Description	Version lors de la publication de la catégorie
`network/interfaces/macs/mac/ipv6-prefix`	Le IPv6 préfixe attribué à l'interface réseau.	
`network/interfaces/macs/mac/local-hostname`	Le IPv4 DNS nom d'hôte privé de l'instance. Dans le cas où plusieurs interfaces réseau sont présentes, cela fait référence au périphérique eth0 (le périphérique dont le numéro de périphérique est 0). S'il s'agit d'une instance IPv6 uniquement, il s'agit du nom basé sur les ressources. Pour plus d'informations sur IPBN etRBN, voirTypes de noms EC2 d'hôte des instances Amazon.	2007-01-19
`network/interfaces/macs/mac/local-ipv4s`	Les IPv4 adresses privées associées à l'interface. S'il s'agit d'une interface réseau IPv6 uniquement, cet élément n'est pas défini et entraîne une réponse HTTP 404.	2011-01-01
`network/interfaces/macs/mac/mac`	MACAdresse de l'instance.	2011-01-01
`network/interfaces/macs/`*`mac`*`/network-card`	L'index de la carte réseau. Certains types d'instance prennent en charge plusieurs cartes réseau.	2020-11-01

Catégorie	Description	Version lors de la publication de la catégorie
`network/interfaces/macs/mac/owner-id`	L'ID du propriétaire de l'interface réseau. Dans les environnements à interfaces multiples, une interface peut être attachée à un tiers, par exemple Elastic Load Balancing. Le trafic sur l'interface est toujours facturé au propriétaire de l'interface.	2011-01-01
`network/interfaces/macs/mac/public-hostname`	L'interface est publique DNS (IPv4). Cette catégorie n'est retournée que si l'attribut `enableDnsHostnames` est défini comme `true`. Pour plus d'informations, consultez DNSles attributs correspondants VPC dans le guide de VPC l'utilisateur Amazon. Si l'instance possède uniquement une IPv6 adresse publique et aucune IPv4 adresse publique, cet élément n'est pas défini et entraîne une réponse HTTP 404.	2011-01-01
`network/interfaces/macs/mac/public-ipv4s`	L'adresse IP publique ou les adresses IP Elastic associées à l'interface. Il peut y avoir plusieurs IPv4 adresses sur une instance.	2011-01-01
`network/interfaces/macs/mac/security-groups`	Les groupes de sécurité auxquels l'interface réseau appartient.	2011-01-01

Catégorie	Description	Version lors de la publication de la catégorie
`network/interfaces/macs/mac/security-group-ids`	Groupe IDs de sécurité auquel appartient l'interface réseau.	2011-01-01
`network/interfaces/macs/mac/subnet-id`	L'ID du sous-réseau (subnet) dans lequel l'interface réside.	2011-01-01
`network/interfaces/macs/mac/subnet-ipv4-cidr-block`	IPv4CIDRBloc du sous-réseau dans lequel réside l'interface.	2011-01-01
`network/interfaces/macs/mac/subnet-ipv6-cidr-blocks`	IPv6CIDRBloc du sous-réseau dans lequel réside l'interface.	2016-06-30
`network/interfaces/macs/mac/vpc-id`	L'ID du VPC dans lequel réside l'interface.	2011-01-01
`network/interfaces/macs/mac/vpc-ipv4-cidr-block`	Le IPv4 CIDR bloc principal duVPC.	2011-01-01
`network/interfaces/macs/mac/vpc-ipv4-cidr-blocks`	Les IPv4 CIDR blocs pour leVPC.	2016-06-30
`network/interfaces/macs/mac/vpc-ipv6-cidr-blocks`	Le IPv6 CIDR bloc VPC dans lequel réside l'interface.	2016-06-30
`placement/availability-zone`	La zone de disponibilité dans laquelle l'instance a été lancée.	2008-02-01

Catégorie	Description	Version lors de la publication de la catégorie
`placement/availability-zone-id`	ID de zone de disponibilité statique dans laquelle l'instance est lancée. L'ID de zone de disponibilité est cohérent entre les comptes. Toutefois, il peut être différent de la zone de disponibilité, qui peut varier selon le compte.	01-10-2019
`placement/group-name`	Nom du groupe de placement dans lequel l'instance est lancée.	2020-08-24
`placement/host-id`	ID de l'hôte sur lequel l'instance est lancée. Applicable uniquement aux Hôtes dédiés.	2020-08-24
`placement/partition-number`	Numéro de la partition dans laquelle l'instance est lancée.	2020-08-24
`placement/region`	AWS Région dans laquelle l'instance est lancée.	2020-08-24
`product-codes`	AWS Marketplace les codes de produit associés à l'instance, le cas échéant.	2007-03-01

Catégorie	Description	Version lors de la publication de la catégorie
`public-hostname`	L'instance est publique DNS (IPv4). Cette catégorie n'est retournée que si l'attribut `enableDnsHostnames` est défini comme `true`. Pour plus d'informations, consultez DNSles attributs correspondants VPC dans le guide de VPC l'utilisateur Amazon. Si l'instance possède uniquement une IPv6 adresse publique et aucune IPv4 adresse publique, cet élément n'est pas défini et entraîne une réponse HTTP 404.	2007-01-19
`public-ipv4`	L'IPv4adresse publique. Si une adresse IP Elastic est associée à l'instance, la valeur retournée est l'adresse IP Elastic.	2007-01-19
`public-keys/0/openssh-key`	Clé publique. Disponible uniquement si fournie au moment du lancement de l'instance.	1.0
`ramdisk-id`	ID du RAM disque spécifié au moment du lancement, le cas échéant.	2007-10-10
`reservation-id`	L'ID de la réservation.	1.0

Catégorie	Description	Version lors de la publication de la catégorie
`security-groups`	Les noms des groupes de sécurité appliqués à l'instance. Après le lancement, vous pouvez modifier les groupes de sécurité des instances. Ces changemen ts se reflètent ici et dans réseau/ interfaces/macs/ *`mac`*/groupes de sécurité.	1.0
`services/domain`	Le domaine des AWS ressources pour la région.	2014-02-25
`services/partition`	Partition dans laquelle se trouve la ressource. Pour les AWS régions standard, la partition est`aws`. Si vous avez des ressources dans d'autres partitions, la partition est `aws-`*`partitionname`* . Par exemple, la partition des ressource s de la région Chine (Beijing) est `aws-cn`.	2015-10-20
`spot/instance-action`	L'action (hibernation, arrêt ou fin) et l'heure approximative à laquelle UTC l'action aura lieu. Cet élément est présent uniquement si l'instanc e Spot a été balisée pour être mise en veille prolongée, arrêtée ou résiliée. Pour plus d'informations, consultez instance-action.	2016-11-15

Catégorie	Description	Version lors de la publication de la catégorie
`spot/termination-time`	Heure approximative, enUTC, pendant laquelle le système d'exploitation de votre instance Spot recevra le signal d'arrêt. Cet article est présent et contient une valeur temporelle (par exemple, 2015-01-05T 18:02:00 Z) uniquement si l'instance Spot a été marquée pour résiliation par Amazon. EC2 L'élément heure-arrêt n'est pas défini à une heure précise si vous avez mis fin vous-même à l'instance Spot. Pour plus d'informations, consultez terminati on-time.	2014-11-05
`tags/instance`	Identifications associées à l'instanc e. Disponible uniquement si vous autorisez explicitement l'accès aux identifications dans les métadonnées d'instance. Pour plus d'informations, consultez Autoriser l'accès aux identifications dans les métadonnées d'instance.	23/03/2021

Catégories de données dynamiques

Le tableau ci-après répertorie les catégories de données dynamiques.

Catégorie	Description	Version lors de la publication de la catégorie
`fws/instance-monitoring`	Valeur indiquant si le client a activé le suivi détaillé d'une minute dans CloudWatch. Valeurs valides : `enabled | disabled`	2009-04-04
`instance-identity/document`	JSONcontenant des attributs d'instance, tels que l'identifiant d'instance, l'adresse IP privée, etc. Consultez Documents d'identité d'instance pour les EC2 instances Amazon.	2009-04-04
`instance-identity/pkcs7`	Utilisé pour vérifier l'authenticité et le contenu du document par rapport à la signature. Consultez Documents d'identité d'instance pour les EC2 instances Amazon.	2009-04-04
`instance-identity/signature`	Les données pouvant être utilisées par d'autres pour vérifier leur origine et leur authenticité. Consultez Documents d'identité d'instance pour les EC2 instances Amazon.	2009-04-04

Accéder aux métadonnées d'une EC2 instance

Vous pouvez accéder aux métadonnées de l'EC2instance depuis l'instance elle-même ou depuis la EC2 consoleAPI,SDKs, ou le AWS CLI. Pour obtenir les paramètres actuels des métadonnées d'une instance à partir de la console ou de la ligne de commande, consultezInterroger les options de métadonnées d'instance pour les instances existantes.

Vous pouvez également modifier les données utilisateur pour les instances dotées d'un volume EBS racine. L'instance doit être à l'état arrêté. Pour obtenir des instructions de la console, consultez Mettre à jour les données utilisateur de l'instance. Pour un exemple de Linux utilisant le AWS CLI, voir modify-instance-attribute. Pour un exemple de Windows utilisant les outils pour Windows PowerShell, voirthe section called "Les données utilisateur et les outils pour Windows PowerShell".

Note

- Il existe une limite de 1024 paquets par seconde (PPS) pour les services qui utilisent des adresses lien-local. Cette limite inclut l'ensemble des requêtes Route 53 Resolver, des DNS requêtes Instance Meta Data Service (IMDS), des demandes Amazon Time Service Network Time Protocol (NTP) et des demandes du Windows Licensing Service (pour les instances basées sur Microsoft Windows).
- Les HTTP demandes utilisées pour récupérer les métadonnées de l'instance et les données utilisateur ne vous sont pas facturées.

Considérations concernant l'accès aux métadonnées des instances

Pour éviter les problèmes liés à la récupération des métadonnées d'instance, tenez compte des points suivants.

Format de commande

Le format de commande est différent selon que vous utilisez le service de métadonnées d'instance version 1 (IMDSv1) ou le service de métadonnées d'instance version 2IMDSv2. Par défaut, vous pouvez utiliser les deux versions du service de métadonnées d'instance. Pour demander l'utilisation deIMDSv2, voirUtiliser le service de métadonnées d'instance pour accéder aux métadonnées de l'instance.

(IMDSv2) Si IMDSv2 nécessaire, IMDSv1 ne fonctionne pas

Pour vérifier si IMDSv2 c'est nécessaire, sélectionnez l'instance pour en afficher les détails. La valeur pour IMDSv2est obligatoire (vous devez utiliserIMDSv2) ou facultative (vous pouvez utiliser l'une IMDSv2 ou l'autreIMDSv1).

(IMDSv2) /latest/api/token À utiliser pour récupérer le jeton

L'envoi de PUT requêtes vers un chemin spécifique à une version, par exemple`/2021-03-23/api/token`, entraîne le renvoi par le service de métadonnées 403 erreurs interdites. Ce comportement est prévu.

IPv6soutien

Pour récupérer les métadonnées de l'instance à l'aide de l'IPv6adresse, assurez-vous d'activer et d'utiliser à la `[fd00:ec2::254]` place de l'IPv4adresse. L'instance doit être construite sur le système AWS Nitro et lancée dans un sous-réseau compatible. IPv6

(Windows) Création d'une version personnalisée à AMIs l'aide de Windows Sysprep

Pour que cela IMDS fonctionne lorsque vous lancez une instance à partir d'un système Windows personnaliséAMI, AMI il doit s'agir d'une image standardisée créée avec Windows Sysprep. Sinon, cela IMDS ne fonctionnera pas. Pour plus d'informations, voirCréez un Amazon à EC2 AMI l'aide de Windows Sysprep.

Dans un environnement de conteneur, définissez la limite de sauts sur 2

L' AWS SDKsutilisateur IMDSv2 appelle par défaut. Si l'IMDSv2appel ne reçoit aucune réponse, il SDK tente à nouveau l'appel et, en cas d'échec, utiliseIMDSv1. Cela peut entraîner un retard, en particulier dans un environnement de conteneurs. Dans un environnement de conteneur, si la limite de sauts est de 1, la IMDSv2 réponse n'est pas renvoyée car l'accès au conteneur est considéré comme un saut réseau supplémentaire. Pour éviter le processus de repli IMDSv1 et le retard qui en résulte, dans un environnement de conteneur, nous vous recommandons de définir la limite de sauts à 2. Pour de plus amples informations, veuillez consulter Configuration des options du service de métadonnées d'instance.

Version des métadonnées

Pour éviter d'avoir à mettre à jour votre code chaque fois qu'Amazon EC2 publie une nouvelle version de métadonnées d'instance, nous vous recommandons d'utiliser `latest` le chemin et non le numéro de version.

Considérations supplémentaires relatives à l'accès aux données utilisateur

- Les données utilisateur sont traitées comme des données opaques : ce que vous spécifiez est ce que vous obtenez en retour lors de la récupération. C'est à l'instance d'interpréter et d'agir sur les données utilisateur.
- Les données utilisateur doivent être codées en base64. En fonction de l'outil ou de l'outil SDK que vous utilisez, le codage base64 peut être effectué pour vous. Par exemple :
  - La EC2 console Amazon peut effectuer le codage en base64 pour vous ou accepter les entrées codées en base64.
  - AWS CLI la version 2 effectue le codage en base64 des paramètres binaires pour vous par défaut. AWS CLI la version 1 effectue le codage en base64 du `--user-data` paramètre pour vous.
  - AWS SDK for Python (Boto3) Procède au codage base64 du `UserData` paramètre pour vous.

- Les données d'utilisateur sont limitées à 16 Ko en format brut, avant qu'elles soient encodées en base64. La taille d'une chaîne de longueur n après l'encodage base64 est ceil(n/3)*4.
- Les données utilisateur doivent être décodées en base64 lorsque vous les récupérez. Si vous les récupérez à l'aide des métadonnées d'instance ou de la console, les données sont décodées automatiquement.
- Si vous arrêtez une instance, modifiez ses données utilisateur et démarrez l'instance, les données utilisateur mises à jour ne sont pas exécutées automatiquement lorsque vous démarrez l'instance. Avec les instances Windows, vous pouvez configurer les paramètres de manière à ce que les scripts de données utilisateur mis à jour soient exécutés une fois lorsque vous démarrez l'instance ou chaque fois que vous redémarrez ou démarrez l'instance.
- Les données utilisateur sont un attribut d'instance. Si vous créez une AMI à partir d'une instance, les données utilisateur de l'instance ne sont pas incluses dans leAMI.

Accédez aux métadonnées de l'instance depuis une EC2 instance

Les métadonnées de votre instance étant disponibles depuis votre instance en cours d'exécution, vous n'avez pas besoin d'utiliser la EC2 console Amazon ou le AWS CLI. Cela peut être utile lorsque vous écrivez des scripts à exécuter depuis votre instance. Par exemple, vous pouvez accéder à l'adresse IP locale de votre instance à partir des métadonnées d'instance afin de gérer une connexion à une application externe.

Tous les éléments suivants sont considérés comme des métadonnées d'instance, mais ils sont accessibles de différentes manières. Sélectionnez l'onglet qui représente le type de métadonnées d'instance auquel vous souhaitez accéder pour obtenir plus d'informations.

Metadata

Les propriétés des métadonnées de l'instance sont divisées en catégories. Pour obtenir une description de chaque catégorie de métadonnées d'instance, consultez Catégories de métadonnées d'instance.

Pour accéder aux propriétés des métadonnées d'une instance à partir d'une instance en cours d'exécution, obtenez les données à partir de la page suivante IPv4 ou IPv6URIs. Ces adresses IP sont des adresses locales de lien et ne sont valides qu'à partir de l'instance. Pour de plus amples informations, veuillez consulter Adresses lien-local.

IPv4

```
http://169.254.169.254/latest/meta-data/
```

IPv6

```
http://[fd00:ec2::254]/latest/meta-data/
```

Dynamic data

Pour récupérer des données dynamiques depuis une instance en cours d'exécution, utilisez l'une des méthodes suivantesURIs.

IPv4

```
http://169.254.169.254/latest/dynamic/
```

IPv6

```
http://[fd00:ec2::254]/latest/dynamic/
```

Exemples : Accès avec c URL

Les exemples suivants permettent cURL de récupérer les catégories d'identité d'instance de haut niveau.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/
instance-identity/
rsa2048
pkcs7
document
signature
dsa2048
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/
rsa2048
```

```
pkcs7
document
signature
dsa2048
```

Exemples : Accès avec PowerShell

Les exemples suivants permettent PowerShell de récupérer les catégories d'identité d'instance de haut niveau.

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

Pour plus d'informations sur les données dynamiques et pour des exemples sur la façon de les récupérer, consultez Documents d'identité d'instance pour les EC2 instances Amazon.

User data

Pour récupérer les données utilisateur d'une instance, utilisez l'une des méthodes suivantesURIs. Pour récupérer les données utilisateur à l'aide de l'IPv6adresse, vous devez l'activer, et l'instance doit être une instance créée sur le système AWS Nitro dans un sous-réseau compatible. IPv6

IPv4

```
http://169.254.169.254/latest/user-data
```

IPv6

```
http://[fd00:ec2::254]/latest/user-data
```

Une demande de données utilisateur renvoie les données telles qu'elles sont (type de contenu `application/octet-stream`). Si l'instance ne possède aucune donnée utilisateur, la demande renvoie `404 - Not Found`.

Exemples : Accès avec c URL pour récupérer du texte séparé par des virgules

Les exemples suivants permettent de cURL récupérer des données utilisateur spécifiées sous forme de texte séparé par des virgules.

IMDSv2

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-
data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
curl http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

Exemples : Accès avec PowerShell pour récupérer du texte séparé par des virgules

Les exemples suivants permettent de PowerShell récupérer des données utilisateur spécifiées sous forme de texte séparé par des virgules.

IMDSv2

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri
 http://169.254.169.254/latest/user-data
```

```
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = Invoke-RestMethod -Headers
 @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
-Method PUT -Uri http://169.254.169.254/latest/api/token} -Method GET -uri
 http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

Exemples : Accès avec c URL pour récupérer un script

Les exemples suivants permettent cURL de récupérer les données utilisateur spécifiées sous forme de script.

IMDSv2

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-
data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

IMDSv1

```
curl http://169.254.169.254/latest/user-data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Exemples : Accès avec PowerShell pour récupérer un script

Les exemples suivants permettent PowerShell de récupérer les données utilisateur spécifiées sous forme de script.

IMDSv2

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri
 http://169.254.169.254/latest/user-data
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

IMDSv1

```
Invoke-RestMethod -uri http://169.254.169.254/latest/user-data
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Interroger les options de métadonnées d'instance pour les instances existantes

Vous pouvez interroger les options de métadonnées d'instance pour vos instances existantes en utilisant l'une des méthodes suivantes.

Console

Pour interroger les options de métadonnées d'instance pour une instance existante à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez votre instance.
4. Choisissez Actions, Paramètres de l'instance, puis Modifier les options des métadonnées d'instance.
5. Passez en revue les options de métadonnées d'instance actuelles dans la boîte de dialogue Modifier les options de métadonnées d'instance.

AWS CLI

Pour interroger les options de métadonnées d'instance pour une instance existante à l'aide du AWS CLI

Utilisez la commande describe-instancesCLI.

```
aws ec2 describe-instances \
    --instance-id i-1234567898abcdef0 \
    --query 'Reservations[].Instances[].MetadataOptions'
```

PowerShell

Pour interroger les options de métadonnées d'instance pour une instance existante à l'aide des outils de PowerShell

Utilisez l'Get-EC2Instanceapplet de commande.

```
(Get-EC2Instance `
    -InstanceId i-1234567898abcdef0).Instances.MetadataOptions
```

Réponses et messages d'erreur

Toutes les métadonnées de l'instance sont renvoyées sous forme de texte (type de HTTP contenu`text/plain`).

Une demande pour une ressource de métadonnées spécifique renvoie la valeur appropriée ou un code `404 - Not Found` HTTP d'erreur si la ressource n'est pas disponible.

Une demande de ressource de métadonnées générales (qui URI se termine par un/) renvoie une liste des ressources disponibles ou un code `404 - Not Found` HTTP d'erreur en l'absence d'une telle ressource. Les éléments de la liste se trouvent sur des lignes séparées, terminées par des fils de ligne (ASCII10).

Pour les demandes effectuées à l'aide de la version 2 du service de métadonnées d'instance, les codes HTTP d'erreur suivants peuvent être renvoyés :

- `400 - Missing or Invalid Parameters` – La demande PUT n'est pas valide.
- `401 - Unauthorized` – La demande GET utilise un jeton non valide. Il est recommandé dans ce cas de générer un nouveau jeton.

- `403 - Forbidden`— La demande n'est pas autorisée ou IMDS est désactivée.
- `503`— La demande n'a pas pu être traitée. Réitérez la requête .

Utiliser le service de métadonnées d'instance pour accéder aux métadonnées de l'instance

Vous pouvez accéder aux métadonnées d'instance à partir d'une instance en cours d'exécution en utilisant l'une des méthodes suivantes :

- Service de métadonnées d'instance version 2 (IMDSv2) : méthode orientée session

  Pour obtenir des exemples, consultez Exemples pour IMDSv2.
- Service de métadonnées d'instance version 1 (IMDSv1) : méthode de demande/réponse

  Pour obtenir des exemples, consultez Exemples pour IMDSv1.

Par défaut, vous pouvez utiliser l'un IMDSv1 ou IMDSv2 l'autre ou les deux.

Vous pouvez configurer le service de métadonnées d'instance (IMDS) sur chaque instance afin que le code local ou les utilisateurs puissent l'utiliserIMDSv2. Lorsque vous spécifiez que cela IMDSv2 doit être utilisé, cela IMDSv1 ne fonctionne plus. Pour plus d'informations sur la configuration de votre instance à utiliserIMDSv2, consultezConfiguration des options du service de métadonnées d'instance.

Les `GET` en-têtes `PUT` ou sont uniques à. IMDSv2 Si ces en-têtes sont présents dans la demande, la demande est destinée IMDSv2 à. Si aucun en-tête n'est présent, on suppose que la demande est destinée IMDSv1 à.

Pour un examen approfondi deIMDSv2, voir Ajouter une défense approfondie contre les pare-feux ouverts, les proxys inverses et les SSRF vulnérabilités grâce à des améliorations apportées au service de métadonnées d'EC2instance.

Rubriques

- Fonctionnement de Service des métadonnées d'instance Version 2
- Passer à l'utilisation de Service des métadonnées d'instance Version 2
- Utilisez un support AWS SDK
- Exemples pour IMDSv2
- Exemples pour IMDSv1

Fonctionnement de Service des métadonnées d'instance Version 2

IMDSv2 utilise des demandes orientées session. Lorsque vous utilisez des demandes orientées session, vous créez un jeton de session qui définit la durée de la session, qui doit être d'une seconde au minimum et de six heures au maximum. Durant la période spécifiée, vous pouvez utiliser le même jeton de session pour les demandes suivantes. Une fois la période spécifiée arrivée à expiration, vous devez créer un nouveau jeton de session à utiliser pour les futures demandes.

> **Note**
>
> Les exemples de cette section utilisent l'IPv4adresse du service de métadonnées d'instance (IMDS) :`169.254.169.254`. Si vous récupérez des métadonnées d'instance pour des EC2 instances via l'IPv6adresse, assurez-vous d'activer et d'utiliser l'IPv6adresse à la place :`[fd00:ec2::254]`. L'IPv6adresse du IMDS est compatible avec IMDSv2 les commandes. L'IPv6adresse n'est accessible que sur les instances créées sur le système AWS Nitro et dans un sous-réseau IPv6 compatible (double pile ou IPv6 uniquement).

Les exemples suivants utilisent un script shell IMDSv2 pour récupérer les éléments de métadonnées de l'instance de niveau supérieur. Chaque exemple :

- Crée un jeton de session d'une durée de six heures (21 600 secondes) en utilisant la demande PUT
- Stocke l'en-tête du jeton de session dans une variable nommée `TOKEN` (instances Linux) ou `token` (instances Windows)
- Demande les éléments de métadonnées de haut niveau à l'aide du jeton

Exemple Linux

Vous pouvez exécuter deux commandes distinctes ou les combiner.

Commandes distinctes

Tout d'abord, générez un jeton à l'aide de la commande suivante.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`
```

Utilisez ensuite le jeton pour générer des éléments de métadonnées de niveau supérieur à l'aide de la commande suivante.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/
```

Commandes combinées

Vous pouvez stocker le jeton et combiner les commandes. L'exemple suivant combine les deux commandes ci-dessus et stocke l'en-tête du jeton de session dans une variable nomméeTOKEN.

> **Note**
>
> En cas d'erreur lors de la création du jeton, un message d'erreur remplace le jeton valide dans la variable et la commande ne fonctionne pas.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
 && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
```

Une fois que vous avez créé un jeton, vous pouvez le réutiliser jusqu'à son expiration. Dans l'exemple de commande suivant, qui obtient l'ID AMI utilisé pour lancer l'instance, le jeton stocké `$TOKEN` dans l'exemple précédent est réutilisé.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/ami-id
```

Exemple Windows

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -
Uri http://169.254.169.254/latest/meta-data/
```

Une fois que vous avez créé un jeton, vous pouvez le réutiliser jusqu'à son expiration. Dans l'exemple de commande suivant, qui obtient l'ID AMI utilisé pour lancer l'instance, le jeton stocké `$token` dans l'exemple précédent est réutilisé.

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
 -Method GET -uri http://169.254.169.254/latest/meta-data/ami-id
```

Lorsque vous demandez IMDSv2 des métadonnées d'instance, la demande doit inclure les éléments suivants :

1. Utilisez une demande PUT pour lancer une session sur le service des métadonnées d'instance. La demande PUT renvoie un jeton qui doit être inclus dans les demandes GET suivantes envoyées au service des métadonnées d'instance. Le jeton est requis pour accéder aux métadonnées à l'aide deIMDSv2.
2. Incluez le jeton dans toutes les GET demandes adressées auIMDS. Lorsque l'utilisation des jetons est définie sur`required`, les demandes sans jeton valide ou dont le jeton a expiré reçoivent un code `401 - Unauthorized` HTTP d'erreur.
   - Le jeton est une clé propre à l'instance. Le jeton n'est pas valide sur EC2 les autres instances et sera rejeté si vous tentez de l'utiliser en dehors de l'instance sur laquelle il a été généré.
   - La PUT demande doit inclure un en-tête indiquant la durée de vie (TTL) du jeton, en secondes, jusqu'à un maximum de six heures (21 600 secondes). Le jeton représente une session logique. TTLSpécifie la durée de validité du jeton et, par conséquent, la durée de la session.
   - Une fois qu'un jeton est arrivé à expiration, pour pouvoir continuer à accéder aux métadonnées de l'instance, vous devez créer une nouvelle session en utilisant un autre PUT.
   - Vous pouvez choisir de réutiliser un jeton ou d'en créer un nouveau pour chaque demande. Pour un petit nombre de demandes, il peut être plus facile de générer et d'utiliser immédiatement un jeton chaque fois que vous devez accéder auIMDS. Cependant, pour une plus grande productivité, vous pouvez spécifier une durée plus longue pour le jeton et le réutiliser plutôt que de devoir écrire une demande PUT chaque fois que vous avez besoin de demander des métadonnées d'instance. Il n'existe pas de limite pratique au nombre de jetons simultanés, chacun représentant sa propre session. IMDSv2est toutefois toujours limité par les limites de IMDS connexion et de limitation normales. Pour de plus amples informations, veuillez consulter Limitation des demandes.

HTTPGETet HEAD les méthodes sont autorisées dans les demandes de métadonnées d'IMDSv2instance. PUTles demandes sont rejetées si elles contiennent un en-tête X-Forwarded-For.

Par défaut, la réponse aux demandes PUT possède une durée time-to-live (hop limit) de réponse de 1 au niveau du protocole IP. Si vous avez besoin d'une limite de sauts plus importante, vous pouvez l'ajuster à l'aide de la modify-instance-metadata-options AWS CLI commande. Par exemple,

vous pouvez avoir besoin d'une durée de vie plus élevée pour des raisons de compatibilité en amont avec les services de conteneur s'exécutant sur l'instance. Pour de plus amples informations, veuillez consulter Configurer les options de métadonnées d'instance pour les instances existantes.

Passer à l'utilisation de Service des métadonnées d'instance Version 2

Lors de la migration versIMDSv2, nous vous recommandons d'utiliser les outils et le chemin de transition suivants.

Rubriques

- Outils d'aide à la transition vers IMDSv2
- Chemin recommandé pour exiger IMDSv2

Outils d'aide à la transition vers IMDSv2

Si votre logiciel l'utiliseIMDSv1, utilisez les outils suivants pour vous aider à reconfigurer votre logiciel en vue de son utilisationIMDSv2.

AWS logiciel

Les dernières versions du AWS SDKs support AWS CLI etIMDSv2. Pour les utiliserIMDSv2, assurez-vous que vos EC2 instances disposent des dernières versions de CLI etSDKs. Pour plus d'informations sur la mise à jour duCLI, voir Installation, mise à jour et désinstallation du AWS CLI dans le guide de l'AWS Command Line Interface utilisateur.

Tous les packages logiciels Amazon Linux 2 et Amazon Linux 2023 sont pris en chargeIMDSv2. Dans Amazon Linux 2023, IMDSv1 il est désactivé par défaut.

Pour connaître les AWS SDK versions minimales prises en chargeIMDSv2, consultezUtilisez un support AWS SDK.

IMDSAnalyseur de paquets

L'analyseur de IMDS paquets est un outil open source qui identifie et enregistre les IMDSv1 appels depuis la phase de démarrage de votre instance. Cela peut vous aider à identifier le logiciel qui fait IMDSv1 appel aux EC2 instances, ce qui vous permet de déterminer exactement ce que vous devez mettre à jour pour que vos instances soient prêtes à être utilisées IMDSv2 uniquement. Vous pouvez exécuter IMDS Packet Analyzer à partir d'une ligne de commande ou l'installer en tant que service. Pour plus d'informations, consultez IMDSPacket Analyzer activé GitHub.

CloudWatch

IMDSv2utilise des sessions basées sur des jetons, alors que ce n'est IMDSv1 pas le cas. La `MetadataNoToken` CloudWatch métrique suit le nombre d'appels au service de métadonnées d'instance (IMDS) utilisésIMDSv1. En ramenant cette métrique à zéro, vous pouvez déterminer si et quand tous vos logiciels ont été mis à niveau pour être utilisésIMDSv2.

Une fois la désactivation terminéeIMDSv1, vous pouvez utiliser la `MetadataNoTokenRejected` CloudWatch métrique pour suivre le nombre de tentatives et de refus d'un IMDSv1 appel. En suivant cette métrique, vous pouvez déterminer si votre logiciel doit être mis à jour pour être utiliséIMDSv2.

Pour de plus amples informations, veuillez consulter Métriques des instances.

Mises à jour de EC2 APIs et CLIs

Pour les nouvelles instances, vous pouvez utiliser le RunInstancesAPIpour lancer de nouvelles instances nécessitant l'utilisation deIMDSv2. Pour de plus amples informations, veuillez consulter Configurer les options de métadonnées d'instance pour les nouvelles instances.

Pour les instances existantes, vous pouvez utiliser le ModifyInstanceMetadataOptionsAPIpour exiger l'utilisation deIMDSv2. Pour de plus amples informations, veuillez consulter Configurer les options de métadonnées d'instance pour les instances existantes.

Pour exiger l'utilisation de toutes IMDSv2 les nouvelles instances lancées par les groupes Auto Scaling, vos groupes Auto Scaling peuvent utiliser un modèle de lancement ou une configuration de lancement. Lorsque vous créez un modèle de lancement ou une configuration de lancement, vous devez configurer les `MetadataOptions` paramètres pour exiger l'utilisation deIMDSv2. Le groupe Auto Scaling lance de nouvelles instances à l'aide du nouveau modèle de lancement ou de la nouvelle configuration de lancement, mais les instances existantes ne sont pas affectées. Pour les instances existantes d'un groupe Auto Scaling, vous pouvez utiliser le ModifyInstanceMetadataOptionsAPIpour exiger l'utilisation IMDSv2 sur les instances existantes, ou mettre fin aux instances et le groupe Auto Scaling lancera de nouvelles instances de remplacement avec les paramètres des options de métadonnées d'instance définis dans le nouveau modèle de lancement ou dans la nouvelle configuration de lancement.

Utilisez un système AMI qui se configure IMDSv2 par défaut

Lorsque vous lancez une instance, vous pouvez automatiquement la configurer pour qu'elle soit utilisée IMDSv2 par défaut (le `HttpTokens` paramètre est défini sur`required`) en la lançant avec une AMI instance configurée avec le `ImdsSupport` paramètre défini sur`v2.0`. Vous pouvez

définir le `ImdsSupport` paramètre sur `v2.0` lorsque vous enregistrez le à l'AMIaide de la CLI commande register-image, ou vous pouvez modifier un existant à l'aide AMI de la modify-image-attributeCLIcommande. Pour de plus amples informations, veuillez consulter Configurez le AMI.

IAMpolitiques et SCPs

Vous pouvez utiliser une IAM stratégie ou une politique AWS Organizations de contrôle des services (SCP) pour contrôler les utilisateurs comme suit :

- Impossible de lancer une instance à l'aide de, RunInstancesAPIsauf si l'instance est configurée pour l'utiliserIMDSv2.
- Impossible de modifier une instance en cours d'exécution à l'aide du ModifyInstanceMetadataOptionsAPIpour la réactiverIMDSv1.

La IAM politique ou SCP doit contenir les clés de IAM condition suivantes :

- `ec2:MetadataHttpEndpoint`
- `ec2:MetadataHttpPutResponseHopLimit`
- `ec2:MetadataHttpTokens`

Si un paramètre de l'CLIappel API ou ne correspond pas à l'état spécifié dans la politique contenant la clé de condition, l'CLIappel API ou échoue avec une `UnauthorizedOperation` réponse.

En outre, vous pouvez choisir une couche de protection supplémentaire pour appliquer le passage de IMDSv1 àIMDSv2. Au niveau de la couche de gestion des accès, en ce qui concerne les informations d'identification APIs appelées via le EC2 rôle, vous pouvez utiliser une nouvelle clé de condition soit dans IAM les politiques, soit dans les politiques de contrôle des AWS Organizations services (SCPs). Plus précisément, en utilisant la clé de condition `ec2:RoleDelivery` avec une valeur de `2.0` dans vos IAM politiques, les API appels effectués avec les informations d'identification de EC2 rôle obtenues auprès de IMDSv1 recevront une `UnauthorizedOperation` réponse. La même chose peut être réalisée de manière plus générale avec cette condition requise par unSCP. Cela garantit que les informations d'identification fournies via IMDSv1 ne peuvent pas être réellement utilisées pour appeler, APIs car tout API appel ne correspondant pas à la condition spécifiée recevra une `UnauthorizedOperation` erreur.

Pour des exemples IAM de politiques, voirUtiliser des métadonnées d'instance. Pour plus d'informationsSCPs, voir les politiques de contrôle des services dans le guide de AWS Organizations l'utilisateur.

Chemin recommandé pour exiger IMDSv2

À l'aide des outils ci-dessus, nous vous recommandons de suivre cette voie pour effectuer la transition versIMDSv2.

Etape 1 : Au départ

Mettez à jour les SDKsCLIs, et vos logiciels qui utilisent les informations d'identification de rôle sur leurs EC2 instances vers des versions compatibles avecIMDSv2. Pour plus d'informations sur la mise à jour duCLI, reportez-vous à la section Mise à niveau vers la AWS CLI dernière version du Guide de AWS Command Line Interface l'utilisateur.

Modifiez ensuite votre logiciel qui accède directement aux métadonnées de l'instance (en d'autres termes, qui n'utilise pas deSDK) à l'aide des IMDSv2 requêtes. Vous pouvez utiliser l'analyseur de IMDS paquets pour identifier le logiciel que vous devez modifier pour utiliser les IMDSv2 demandes.

Étape 2 : suivre la progression de votre transition

Suivez la progression de votre transition à l'aide de la CloudWatch métrique`MetadataNoToken`. Cette métrique indique le nombre d'IMDSv1appels adressés IMDS à vos instances. Pour de plus amples informations, veuillez consulter Métriques des instances.

Étape 3 : Quand il n'y a aucune IMDSv1 utilisation

Lorsque la CloudWatch métrique `MetadataNoToken` enregistre une IMDSv1 utilisation nulle, vos instances sont prêtes à passer entièrement à l'utilisationIMDSv2. A ce stade, voici ce que vous pouvez faire :

- Compte par défaut

  Vous pouvez le IMDSv2 définir comme obligatoire comme compte par défaut. Lorsqu'une instance est lancée, la configuration de l'instance est automatiquement définie sur la valeur par défaut du compte.

  Pour définir le compte par défaut, procédez comme suit :

  - EC2Console Amazon : sur le EC2 tableau de bord, sous Attributs du compte, Protection des données et sécurité, pour les IMDSvaleurs par défaut, définissez le service de métadonnées de l'instance sur Activé et la version des métadonnées sur V2 uniquement (jeton requis). Pour de plus amples informations, veuillez consulter Définir IMDSv2 comme valeur par défaut pour le compte.

  - AWS CLI: utilisez la modify-instance-metadata-defaultsCLIcommande et spécifiez `--http-tokens required` et`--http-put-response-hop-limit 2`.
- Nouvelles instances

  Lors du lancement d'une nouvelle instance, vous pouvez effectuer les opérations suivantes :

  - EC2Console Amazon : dans l'assistant de lancement de l'instance, définissez les métadonnées accessibles sur Activé et la version des métadonnées sur V2 uniquement (jeton requis). Pour de plus amples informations, veuillez consulter Configurer l'instance au lancement.
  - AWS CLI: utilisez la CLI commande run-instances et spécifiez que IMDSv2 c'est obligatoire.
- Instances existantes

  Pour les instances existantes, vous pouvez exécuter les opérations suivantes :

  - EC2Console Amazon : sur la page Instances, sélectionnez votre instance, choisissez Actions, Paramètres de l'instance, Modifier les options de métadonnées de l'instance, et pour IMDSv2, choisissez Obligatoire. Pour de plus amples informations, veuillez consulter Exigence d'utilisation d'IMDSv2.
  - AWS CLI: Utilisez la modify-instance-metadata-optionsCLIcommande pour spécifier que seule cette IMDSv2 option doit être utilisée.

  Vous pouvez modifier les options des métadonnées d'instance sur les instances en cours d'exécution, et vous n'avez pas besoin de redémarrer les instances après avoir modifié ces options.

Étape 4 : Vérifiez si vos instances sont transférées vers IMDSv2

Vous pouvez vérifier si certaines instances ne sont pas encore configurées pour nécessiter l'utilisation deIMDSv2, en d'autres termes, si elles IMDSv2 sont toujours configurées comme`optional`. Si des instances sont toujours configurées en tant que`optional`, vous pouvez modifier les options de métadonnées de l'instance à effectuer IMDSv2 `required` en répétant l'étape 3 précédente.

Pour filtrer vos instances :

- EC2Console Amazon : sur la page Instances, filtrez vos instances à l'aide du filtre facultatif IMDSv2 =. Pour plus d'informations sur le filtrage, veuillez consulter la rubrique Filtrer des ressources à l'aide de la console. Vous pouvez également voir si IMDSv2 c'est obligatoire ou facultatif

pour chaque instance : dans la fenêtre Préférences, activez l'option IMDSv2pour ajouter la IMDSv2colonne au tableau Instances.

- AWS CLI: utilisez la CLI commande describe-instances et filtrez par`metadata-options.http-tokens = optional`, comme suit :

```
aws ec2 describe-instances --filters "Name=metadata-options.http-
tokens,Values=optional" --query "Reservations[*].Instances[*].[InstanceId]" --output
 text
```

Étape 5 : Lorsque toutes vos instances sont transférées vers IMDSv2

Les touches `ec2:MetadataHttpTokensec2:MetadataHttpPutResponseHopLimit`,, et de `ec2:MetadataHttpEndpoint` IAM condition peuvent être utilisées pour contrôler l'utilisation du RunInstancesModifyInstanceMetadataOptionsAPIset correspondantCLIs. Si une politique est créée et qu'un paramètre de l'APIappel ne correspond pas à l'état spécifié dans la politique à l'aide de la clé de condition, l'CLIappel API ou échoue avec une `Unauthorized0peration` réponse. Pour des exemples IAM de politiques, voirUtiliser des métadonnées d'instance.

En outre, après la désactivationIMDSv1, vous pouvez utiliser la `MetadataNoTokenRejected` CloudWatch métrique pour suivre le nombre de tentatives et de refus d'un IMDSv1 appel. Si, après la désactivationIMDSv1, vous avez un logiciel qui ne fonctionne pas correctement et que la `MetadataNoTokenRejected` métrique enregistre les IMDSv1 appels, il est probable que ce logiciel doive être mis à jour pour être utiliséIMDSv2.

Utilisez un support AWS SDK

Pour être utiliséesIMDSv2, vos EC2 instances doivent utiliser une AWS SDK version compatible avec l'utilisationIMDSv2. Les dernières versions de tous les AWS SDKs supports utilisantIMDSv2.

> **Important**
>
> Nous vous recommandons de vous tenir au courant des dernières SDK versions afin de vous tenir au courant des dernières fonctionnalités, des mises à jour de sécurité et des dépendances sous-jacentes. L'utilisation continue d'une SDK version non prise en charge n'est pas recommandée et se fait à votre discrétion. Pour plus d'informations, consultez la politique de maintenance de AWS SDKs and Tools dans le guide de référence AWS SDKs and Tools.

Les versions minimales prises en charge sont les suivantes IMDSv2 :

- AWS CLI : 1.16.289
- AWS Tools for Windows PowerShell – 4.0.1.0
- AWS SDK for .NET : 3.3.634.1
- AWS SDK for C++ : 1.7.229
- AWS SDK for Go : 1.25.38
- AWS SDKpour Go v2 — 0.19.0
- AWS SDK for Java : 1.11.678
- AWS SDK for Java 2.x : 2.10.21
- AWS SDKpour JavaScript dans Node.js — 2.722.0
- AWS SDK for PHP : 3.147.7
- AWS SDKpour Python (Botocore) — 1.13.25
- AWS SDK for Python (Boto3) : 1.12.6
- AWS SDK for Ruby : 3.79.0

Exemples pour IMDSv2

Exécutez les exemples suivants sur votre EC2 instance Amazon pour récupérer les métadonnées de l'instance pourIMDSv2.

Sur les instances Windows, vous pouvez utiliser Windows PowerShell ou installer c URL ou wget. Si vous installez un outil tiers sur une instance Windows, veillez à lire attentivement la documentation qui l'accompagne, car les appels et le résultat peuvent être différents de ceux décrits ici.

Exemples

- Obtenir les versions disponibles des métadonnées d'instance
- Obtenir les éléments de métadonnées de niveau supérieur
- Obtenir les valeurs des éléments de métadonnées
- Obtenir la liste des clés publiques disponibles
- Montrer les formats pour lesquels une clé publique 0 est disponible
- Obtenir la clé publique 0 (au format SSH clé ouverte)
- Obtenir l'ID de sous-réseau d'une instance
- Obtenir les identifications d'une instance

Obtenir les versions disponibles des métadonnées d'instance

Cet exemple permet d'obtenir les versions disponibles des métadonnées d'instance. Chaque version fait référence à un build de métadonnées d'instance lorsque de nouvelles catégories de métadonnées d'instance ont été publiées. Les versions de compilation des métadonnées de l'instance ne sont pas corrélées aux EC2 API versions d'Amazon. Les versions antérieures sont disponibles au cas où vous ayez des scripts reposant sur la structure et les informations présentes dans une version précédente.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/
1.0
2007-01-19
```

```
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

Obtenir les éléments de métadonnées de niveau supérieur

Cet exemple permet d'obtenir les éléments de métadonnées de niveau supérieur. Pour plus d'informations sur les éléments contenus dans la réponse, consultezCatégories de métadonnées d'instance.

Notez que les balises ne sont incluses dans cette sortie que si vous en avez autorisé l'accès. Pour de plus amples informations, veuillez consulter the section called "Autoriser l'accès aux identifications dans les métadonnées d'instance".

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
```

```
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
```

```
public-keys/
reservation-id
security-groups
services/
tags/
```

Obtenir les valeurs des éléments de métadonnées

Ces exemples obtiennent les valeurs de certains éléments de métadonnées de haut niveau obtenus dans l'exemple précédent. Ces demandes utilisent le jeton stocké créé à l'aide de la commande de l'exemple précédent. Le jeton ne doit pas avoir expiré.

cURL

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/reservation-id
r-0efghijk987654321
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

PowerShell

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Obtenir la liste des clés publiques disponibles

Cet exemple permet d'obtenir la liste des clés publiques disponibles.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/
0=my-public-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

Montrer les formats pour lesquels une clé publique 0 est disponible

Cet exemple montre les formats pour lesquels une clé publique 0 est disponible.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/
```

```
openssh-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
openssh-key
```

Obtenir la clé publique 0 (au format SSH clé ouverte)

Cet exemple obtient la clé publique 0 (au format Open SSH key).

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Obtenir l'ID de sous-réseau d'une instance

Cet exemple permet d'obtenir l'ID de sous-réseau pour une instance.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -
Method GET -Uri http://169.254.169.254/latest/meta-data/network/interfaces/
macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Obtenir les identifications d'une instance

Si l'accès aux balises d'instance dans les métadonnées de l'instance est activé, vous pouvez obtenir les balises d'une instance à partir des métadonnées de l'instance. Pour de plus amples informations, veuillez consulter Extraire les identifications à partir des métadonnées d'instance.

Exemples pour IMDSv1

Exécutez les exemples suivants sur votre EC2 instance Amazon pour récupérer les métadonnées de l'instance pourIMDSv1.

Sur les instances Windows, vous pouvez utiliser Windows PowerShell ou installer c URL ou wget. Si vous installez un outil tiers sur une instance Windows, veillez à lire attentivement la documentation qui l'accompagne, car les appels et le résultat peuvent être différents de ceux décrits ici.

Exemples

- Obtenir les versions disponibles des métadonnées d'instance
- Obtenir les éléments de métadonnées de niveau supérieur
- Obtenir les valeurs des éléments de métadonnées
- Obtenir la liste des clés publiques disponibles
- Montrer les formats pour lesquels une clé publique 0 est disponible
- Obtenir la clé publique 0 (au format SSH clé ouverte)
- Obtenir l'ID de sous-réseau d'une instance
- Obtenir les identifications d'une instance

Obtenir les versions disponibles des métadonnées d'instance

Cet exemple permet d'obtenir les versions disponibles des métadonnées d'instance. Chaque version fait référence à un build de métadonnées d'instance lorsque de nouvelles catégories de métadonnées d'instance ont été publiées. Les versions de compilation des métadonnées de l'instance ne sont pas corrélées aux EC2 API versions d'Amazon. Les versions antérieures sont disponibles au cas où vous ayez des scripts reposant sur la structure et les informations présentes dans une version précédente.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/
```

```
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

Obtenir les éléments de métadonnées de niveau supérieur

Cet exemple permet d'obtenir les éléments de métadonnées de niveau supérieur. Pour plus d'informations sur les éléments contenus dans la réponse, consultezCatégories de métadonnées d'instance.

Notez que les balises ne sont incluses dans cette sortie que si vous en avez autorisé l'accès. Pour de plus amples informations, veuillez consulter the section called "Autoriser l'accès aux identifications dans les métadonnées d'instance".

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
```

```
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

Obtenir les valeurs des éléments de métadonnées

Ces exemples obtiennent les valeurs de certains éléments de métadonnées de haut niveau obtenus dans l'exemple précédent.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Obtenir la liste des clés publiques disponibles

Cet exemple permet d'obtenir la liste des clés publiques disponibles.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-keys/ 0=my-public-key
```

Montrer les formats pour lesquels une clé publique 0 est disponible

Cet exemple montre les formats pour lesquels une clé publique 0 est disponible.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/
```

```
openssh-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
keys/0/openssh-key
openssh-key
```

Obtenir la clé publique 0 (au format SSH clé ouverte)

Cet exemple obtient la clé publique 0 (au format Open SSH key).

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
```

```
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Obtenir l'ID de sous-réseau d'une instance

Cet exemple permet d'obtenir l'ID de sous-réseau pour une instance.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/
macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/network/
interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Obtenir les identifications d'une instance

Si l'accès aux balises d'instance dans les métadonnées de l'instance est activé, vous pouvez obtenir les balises d'une instance à partir des métadonnées de l'instance. Pour de plus amples informations, veuillez consulter Extraire les identifications à partir des métadonnées d'instance.

Limitation des demandes

Nous limitons les requêtes IMDS au cas par cas, et nous limitons le nombre de connexions simultanées entre une instance et le. IMDS

Si vous utilisez le IMDS pour récupérer des informations d'identification de AWS sécurité, évitez de demander des informations d'identification lors de chaque transaction ou simultanément à partir d'un grand nombre de threads ou de processus, car cela pourrait entraîner un ralentissement. Nous vous conseillons plutôt de placer les informations d'identification en cache jusqu'à ce que leur date

d'expiration approche. Pour plus d'informations sur IAM le rôle et les informations d'identification de sécurité associées au rôle, consultezExtraire les informations d'identification de sécurité à partir des métadonnées d'instance.

Si vous êtes limité lors de l'accès auIMDS, réessayez votre requête avec une stratégie de réduction exponentielle.

Limiter l'accès au service de métadonnées d'instance

Vous pouvez envisager d'utiliser des règles de pare-feu locales pour désactiver l'accès de certains ou de tous les processus au service de métadonnées d'instance (IMDS).

Pour les instances basées sur le système AWS Nitro, elles sont IMDS accessibles depuis votre propre réseau lorsqu'un appareil réseau intégré au vôtreVPC, tel qu'un routeur virtuel, transmet des paquets à l'IMDSadresse et que le contrôle source/destination par défaut sur l'instance est désactivé. Pour éviter qu'une source extérieure à vous n'VPCatteigne leIMDS, nous vous recommandons de modifier la configuration de l'appliance réseau afin de supprimer les paquets contenant l'IPv4adresse de destination du IMDS `169.254.169.254` et, si vous avez activé le IPv6 point de terminaison, l'IPv6adresse du IMDS`[fd00:ec2::254]`.

Limiter IMDS l'accès pour les instances Linux

Utilisation d'éléments iptables pour limiter l'accès

L'exemple suivant utilise des éléments Linux iptables et le module `owner` associé pour empêcher le serveur web Apache (en fonction de son ID utilisateur d'installation par défaut `apache`) d'accéder à l'adresse 169.254.169.254. Il utilise une règle de refus pour rejeter toutes les demandes de métadonnées d'instance (qu'elles IMDSv1 proviennent ouIMDSv2) de tout processus exécuté sous le nom de cet utilisateur.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner
 --uid-owner apache --jump REJECT
```

Vous pouvez aussi envisager d'autoriser uniquement l'accès à des utilisateurs ou des groupes particuliers à l'aide de règles d'autorisation (allow). Les règles allow peuvent être plus faciles à gérer du point de vue de la sécurité, car elles nécessitent que vous déterminiez quels sont les logiciels ayant besoin d'accéder aux métadonnées d'instance. Si vous utilisez des règles allow, vous risquez moins d'autoriser accidentellement un logiciel à accéder au service des métadonnées en cas de modification ultérieure des logiciels ou de la configuration sur une instance. Vous pouvez également

combiner une utilisation de groupes avec des règles allow, afin de pouvoir ajouter et supprimer des utilisateurs dans un groupe autorisé sans avoir à modifier la règle du pare-feu.

L'exemple suivant empêche l'accès à tous IMDS les processus, à l'exception des processus exécutés dans le compte utilisateur`trustworthy-user`.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match
 owner ! --uid-owner trustworthy-user --jump REJECT
```

> **Note**
>
> - Pour utiliser des règles de pare-feu locales, vous devez adapter les commandes de l'exemple précédent à vos besoins.
> - Par défaut, les règles iptables ne sont pas persistantes après un redémarrage du système. Elles peuvent être rendues persistantes en utilisant des fonctionnalités du système d'exploitation qui ne sont pas décrites ici.
> - Le module iptables `owner` correspond uniquement à l'appartenance au groupe si le groupe est le groupe principal d'un utilisateur local donné. Les autres groupes n'ont pas de correspondance.

Utilisation de PF ou IPFW pour limiter l'accès

Si vous utilisez Free BSD ou OpenBSD, vous pouvez également envisager d'utiliser PF ouIPFW. Les exemples suivants limitent l'accès IMDS au seul utilisateur root.

PF

```
$ block out inet proto tcp from any to 169.254.169.254
```

```
$ pass out inet proto tcp from any to 169.254.169.254 user root
```

IPFW

```
$ allow tcp from any to 169.254.169.254 uid root
```

```
$ deny tcp from any to 169.254.169.254
```

> **Note**
>
> L'ordre du PF et des IPFW commandes est important. PF utilise par défaut la dernière règle de correspondance et la première règle de correspondance IPFW par défaut.

Limiter IMDS l'accès pour les instances Windows

Utilisation du pare-feu Windows pour limiter l'accès

L' PowerShell exemple suivant utilise le pare-feu Windows intégré pour empêcher le serveur Web Internet Information Server (sur la base de son ID utilisateur d'installation par défaut`NT AUTHORITY\IUSR`) d'accéder au 169.254.169.254. Il utilise une règle de refus pour rejeter toutes les demandes de métadonnées d'instance (qu'elles IMDSv1 proviennent ou`IMDSv2`) de tout processus exécuté sous le nom de cet utilisateur.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount ("NT
 AUTHORITY\IUSR")
PS C:\> $BlockPrincipalSID =
 $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $BlockPrincipalSDDL = "D:(A;;CC;;;$BlockPrincipalSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service from IIS" -Action
 block -Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $BlockPrincipalSDDL
```

Vous pouvez aussi envisager d'autoriser uniquement l'accès à des utilisateurs ou des groupes particuliers à l'aide de règles d'autorisation (allow). Les règles allow peuvent être plus faciles à gérer du point de vue de la sécurité, car elles nécessitent que vous déterminiez quels sont les logiciels ayant besoin d'accéder aux métadonnées d'instance. Si vous utilisez des règles allow, vous risquez moins d'autoriser accidentellement un logiciel à accéder au service des métadonnées en cas de modification ultérieure des logiciels ou de la configuration sur une instance. Vous pouvez également combiner une utilisation de groupes avec des règles allow, afin de pouvoir ajouter et supprimer des utilisateurs dans un groupe autorisé sans avoir à modifier la règle du pare-feu.

L'exemple suivant empêche tous les processus s'exécutant en tant que groupe OS spécifié dans la variable `blockPrincipal` (dans cet exemple, le groupe Windows `Everyone`) d'accéder aux métadonnées d'instance, à l'exception des processus spécifiés dans `exceptionPrincipal` (dans cet exemple, un groupe appelé `trustworthy-users`). Vous devez spécifier à la fois des principaux d'autorisation (allow) et de refus (deny), car le pare-feu Windows, contrairement à la règle `! --uid-`

`owner trustworthy-user` dans les éléments Linux iptables, ne fournit pas de mécanisme de raccourci permettant d'autoriser uniquement un principal particulier (utilisateur ou groupe) en refusant l'accès à tous les autres.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
 ("Everyone")
PS C:\> $BlockPrincipalSID =
 $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $exceptionPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
 ("trustworthy-users")
PS C:\> $ExceptionPrincipalSID =
 $exceptionPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $PrincipalSDDL = "O:LSD:(D;;CC;;;$ExceptionPrincipalSID)(A;;CC;;;
$BlockPrincipalSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service for
 $($blockPrincipal.Value), exception: $($exceptionPrincipal.Value)" -Action block -
Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $PrincipalSDDL
```

> **Note**
>
> Pour utiliser des règles de pare-feu locales, vous devez adapter les commandes de l'exemple précédent à vos besoins.

Utilisation de règles netsh pour limiter l'accès

Vous pouvez envisager de bloquer tous les logiciels à l'aide de règles `netsh`, mais ces règles sont beaucoup moins souples.

```
C:\> netsh advfirewall firewall add rule name="Block metadata service altogether"
 dir=out protocol=TCP remoteip=169.254.169.254 action=block
```

> **Note**
>
> - Pour utiliser des règles de pare-feu locales, vous devez adapter les commandes de l'exemple précédent à vos besoins.
> - `netsh`Les règles doivent être définies à partir d'une invite de commande élevée et ne peuvent pas être définies sur des principaux deny ou allow particuliers.

Configuration des options du service de métadonnées d'instance

Le service de métadonnées d'instance (IMDS) s'exécute localement sur chaque EC2 instance. Les options de métadonnées d'instance font référence à un ensemble de configurations qui contrôlent l'accessibilité et IMDS le comportement de l'EC2instance.

Vous pouvez configurer les options de métadonnées d'instance suivantes sur chaque instance :

Service de métadonnées d'instance (IMDS) : `enabled` | `disabled`

Vous pouvez activer ou désactiver le IMDS sur une instance. Lorsque cette option est désactivée, vous ou aucun code ne pourrez accéder aux métadonnées de l'instance.

IMDSII possède deux points de terminaison sur une instance : IPv4 (`169.254.169.254`) et IPv6 (`[fd00:ec2::254]`). Lorsque vous activez leIMDS, le IPv4 point de terminaison est automatiquement activé. Si vous souhaitez activer le IPv6 point de terminaison, vous devez le faire explicitement.

IMDSIPv6point de terminaison : `enabled` | `disabled`

Vous pouvez activer explicitement le IPv6 IMDS point de terminaison sur une instance. Lorsque le IPv6 point de terminaison est activé, il reste activé. IPv4 Le IPv6 point de terminaison n'est pris en charge que sur les instances créées sur le système AWS Nitro et dans un sous-réseau IPv6 compatible (double pile ou IPv6 uniquement).

Version des métadonnées : `IMDSv1 or IMDSv2 (token optional)` | `IMDSv2 only (token required)`

Lors de la demande de métadonnées d'instance, IMDSv2 les appels nécessitent un jeton. IMDSv1les appels ne nécessitent pas de jeton. Vous pouvez configurer une instance pour autoriser les IMDSv2 appels (lorsqu'un jeton est facultatif), ou pour autoriser uniquement les IMDSv2 appels (lorsqu'un jeton est requis). IMDSv1

Limite de sauts de réponse aux métadonnées : 1 — 64

La limite de sauts est le nombre de sauts réseau que la PUT réponse est autorisée à effectuer. Vous pouvez définir la limite de sauts sur un minimum 1 et un maximum de64. Dans un environnement de conteneurs, nous vous recommandons de définir la limite de sauts sur2. Pour de plus amples informations, veuillez consulter Considérations concernant l'accès aux métadonnées des instances.

Accès aux balises dans les métadonnées de l'instance : `enabled` | `disabled`

Vous pouvez activer ou désactiver l'accès aux balises de l'instance à partir des métadonnées d'une instance. Pour de plus amples informations, veuillez consulter Afficher les balises de vos EC2 instances à l'aide des métadonnées de l'instance.

Où configurer les options de métadonnées de l'instance

Les options de métadonnées d'instance peuvent être configurées à différents niveaux, comme suit :

- Compte : vous pouvez définir des valeurs par défaut pour les options de métadonnées de l'instance au niveau du compte pour chacune d'entre elles Région AWS. Lorsqu'une instance est lancée, les options de métadonnées de l'instance sont automatiquement définies sur les valeurs au niveau du compte. Vous pouvez modifier ces valeurs au lancement. Les valeurs par défaut au niveau du compte n'affectent pas les instances existantes.
- AMI— Vous pouvez définir le `imds-support` paramètre sur `v2.0` lorsque vous enregistrez ou modifiez unAMI. Lorsqu'une instance est lancée avec celaAMI, la version des métadonnées de l'instance est automatiquement définie sur 2 IMDSv2 et la limite de sauts est définie sur 2.
- Instance : vous pouvez modifier toutes les options de métadonnées d'une instance au lancement, en remplaçant les paramètres par défaut. Vous pouvez également modifier les options de métadonnées de l'instance après le lancement d'une instance en cours d'exécution ou arrêtée. Notez que les modifications peuvent être limitées par une SCP politique du IAM système d'exploitation.

Pour plus d'informations, consultez Configurer les options de métadonnées d'instance pour les nouvelles instances et Configurer les options de métadonnées d'instance pour les instances existantes.

Ordre de priorité pour les options de métadonnées des instances

La valeur de chaque option de métadonnées d'instance est déterminée au lancement de l'instance, selon un ordre de priorité hiérarchique. La hiérarchie, avec la priorité la plus élevée au sommet, est la suivante :

- Priorité 1 : Configuration de l'instance au lancement — Les valeurs peuvent être spécifiées dans le modèle de lancement ou dans la configuration de l'instance. Toutes les valeurs spécifiées ici remplacent les valeurs spécifiées au niveau du compte ou dans leAMI.

- Priorité 2 : paramètres du compte — Si aucune valeur n'est spécifiée au lancement de l'instance, elle est déterminée par les paramètres au niveau du compte (définis pour chacun). Région AWS Les paramètres au niveau du compte incluent une valeur pour chaque option de métadonnées ou n'indiquent aucune préférence.
- Priorité 3 : AMI configuration — Si aucune valeur n'est spécifiée au lancement de l'instance ou au niveau du compte, elle est déterminée par la AMI configuration. Cela s'applique uniquement à `HttpTokens` et `HttpPutResponseHopLimit`.

Chaque option de métadonnées est évaluée séparément. L'instance peut être configurée en combinant la configuration directe de l'instance, les paramètres par défaut au niveau du compte et la configuration du. AMI

Vous pouvez modifier la valeur de n'importe quelle option de métadonnées après le lancement sur une instance en cours d'exécution ou arrêtée, sauf si les modifications sont limitées par une SCP politique de IAM or.

Déterminer les valeurs des options de métadonnées — Exemple 1

Dans cet exemple, une EC2 instance est lancée dans une région où le paramètre `HttpPutResponseHopLimit` est défini 1 sur au niveau du compte. Le paramètre spécifié AMI est `ImdsSupport` défini sur`v2.0`. Aucune option de métadonnées n'est spécifiée directement sur l'instance au lancement. L'instance est lancée avec les options de métadonnées suivantes :

```
"MetadataOptions": {
    ...
    "HttpTokens": "required",
    "HttpPutResponseHopLimit": 1,
    ...
```

Ces valeurs ont été déterminées comme suit :

- Aucune option de métadonnées spécifiée au lancement : lors du lancement de l'instance, aucune valeur spécifique pour les options de métadonnées n'était fournie ni dans les paramètres de lancement de l'instance ni dans le modèle de lancement.
- Les paramètres du compte ont la priorité suivante : en l'absence de valeurs spécifiques spécifiées au lancement, les paramètres au niveau du compte dans la région sont prioritaires. Cela signifie que les valeurs par défaut configurées au niveau du compte sont appliquées. Dans ce cas, le `HttpPutResponseHopLimit` a été réglé sur`1`.

- AMIles paramètres ont la dernière priorité : en l'absence de valeur spécifique spécifiée au lancement ou au niveau du compte pour `HttpTokens` (la version des métadonnées de l'instance), le AMI paramètre est appliqué. Dans ce cas, le AMI paramètre a `ImdsSupport: v2.0` déterminé qu'il `HttpTokens` était défini sur`required`. Notez que bien que le AMI paramètre `ImdsSupport: v2.0` soit conçu pour être défini`HttpPutResponseHopLimit: 2`, il a été remplacé par le paramètre au niveau du compte`HttpPutResponseHopLimit: 1`, qui a une priorité plus élevée.

Déterminer les valeurs des options de métadonnées — Exemple 2

Dans cet exemple, l'EC2instance est lancée avec les mêmes paramètres que dans l'exemple 1 précédent, mais avec la `HttpTokens` valeur définie sur `optional` directement sur l'instance au lancement. L'instance est lancée avec les options de métadonnées suivantes :

```
"MetadataOptions": {
    ...
    "HttpTokens": "optional",
    "HttpPutResponseHopLimit": 1,
    ...
```

La valeur pour `HttpPutResponseHopLimit` est déterminée de la même manière que dans l'exemple 1. Toutefois, la valeur pour `HttpTokens` est déterminée comme suit : Les options de métadonnées configurées sur l'instance au lancement sont prioritaires. Même si le AMI a été configuré avec `ImdsSupport: v2.0` (en d'autres termes, `HttpTokens` est défini sur`required`), la valeur spécifiée sur l'instance au lancement (`HttpTokens`définie sur`optional`) était prioritaire.

Définissez la version des métadonnées de l'instance

Lorsqu'une instance est lancée, la valeur de la version des métadonnées de l'instance est `IMDSv1 or IMDSv2 (token optional)` ou`IMDSv2 only (token required)`.

Au lancement de l'instance, vous pouvez soit spécifier manuellement la valeur de la version des métadonnées, soit utiliser la valeur par défaut. Si vous spécifiez manuellement la valeur, elle remplace toutes les valeurs par défaut. Si vous choisissez de ne pas spécifier manuellement la valeur, elle sera déterminée par une combinaison de paramètres par défaut, comme indiqué dans le tableau suivant.

Le tableau montre comment la version des métadonnées d'une instance au lancement (indiquée par Configuration de l'instance résultante dans la colonne 4) est déterminée par les paramètres aux

différents niveaux de configuration. L'ordre de priorité est de gauche à droite, la première colonne ayant la priorité la plus élevée, comme suit :

- Colonne 1 : paramètre de lancement : représente le paramètre de l'instance que vous spécifiez manuellement au lancement.
- Colonne 2 : Niveau de compte par défaut — Représente le paramètre du compte.
- Colonne 3 : AMIpar défaut — Représente le paramètre duAMI.

Paramètre de lancement	Niveau de compte par défaut	AMIpar défaut	Configuration de l'instance résultante
V2 uniquement (jeton requis)	Aucune préférence	V2 uniquement	V2 uniquement
V2 uniquement (jeton requis)	V2 uniquement	V2 uniquement	V2 uniquement
V2 uniquement (jeton requis)	V1 ou V2	V2 uniquement	V2 uniquement
V1 ou V2 (jeton facultatif)	Aucune préférence	V2 uniquement	V1 ou V2
V1 ou V2 (jeton facultatif)	V2 uniquement	V2 uniquement	V1 ou V2
V1 ou V2 (jeton facultatif)	V1 ou V2	V2 uniquement	V1 ou V2
Non défini	Aucune préférence	V2 uniquement	V2 uniquement
Non défini	V2 uniquement	V2 uniquement	V2 uniquement
Non défini	V1 ou V2	V2 uniquement	V1 ou V2
V2 uniquement (jeton requis)	Aucune préférence	null	V2 uniquement

Paramètre de lancement	Niveau de compte par défaut	AMIpar défaut	Configuration de l'instance résultante
V2 uniquement (jeton requis)	V2 uniquement	null	V2 uniquement
V2 uniquement (jeton requis)	V1 ou V2	null	V2 uniquement
V1 ou V2 (jeton facultatif)	Aucune préférence	null	V1 ou V2
V1 ou V2 (jeton facultatif)	V2 uniquement	null	V1 ou V2
V1 ou V2 (jeton facultatif)	V1 ou V2	null	V1 ou V2
Non défini	Aucune préférence	null	V1 ou V2
Non défini	V2 uniquement	null	V2 uniquement
Non défini	V1 ou V2	null	V1 ou V2

Utiliser des clés de IAM condition pour restreindre les options de métadonnées de l'instance

Vous pouvez utiliser des clés de IAM condition dans une IAM politique ou SCP comme suit :

- Autoriser le lancement d'une instance uniquement si elle est configurée pour nécessiter l'utilisation de IMDSv2
- Restreindre le nombre de sauts autorisés
- Désactiver l'accès aux métadonnées d'instance

Tâches

- Configurer les options de métadonnées d'instance pour les nouvelles instances
- Configurer les options de métadonnées d'instance pour les instances existantes

> **Note**
>
> Vous devez procéder avec précautions et effectuer des tests méticuleux avant toute modification. Notez les informations suivantes :
>
> - Si vous en forcez l'utilisationIMDSv2, les applications ou les agents qui utilisent, par IMDSv1 exemple, l'accès aux métadonnées seront interrompus.
> - Si vous désactivez tous les accès aux métadonnées d'instance, les applications ou agents dont le fonctionnement repose sur l'accès aux métadonnées d'instance cesseront de fonctionner.
> - CarIMDSv2, vous devez l'utiliser `/latest/api/token` lors de la récupération du jeton.
> - (Windows uniquement) Si votre PowerShell version est antérieure à 4.0, vous devez effectuer la mise à jour vers Windows Management Framework 4.0 pour exiger l'utilisation deIMDSv2.

Configurer les options de métadonnées d'instance pour les nouvelles instances

Vous pouvez configurer les options de métadonnées d'instance suivantes pour les nouvelles instances.

Options

- Exigence d'utilisation d'IMDSv2
- Activez les points de IPv6 terminaison IMDS IPv4 et
- Désactiver l'accès aux métadonnées d'instance

Exigence d'utilisation d'IMDSv2

Vous pouvez utiliser les méthodes suivantes pour exiger l'utilisation de IMDSv2 sur vos nouvelles instances.

Pour exiger IMDSv2

- Définir IMDSv2 comme valeur par défaut pour le compte
- Configurer l'instance au lancement
- Configurez le AMI
- Utiliser une IAM politique

Définir IMDSv2 comme valeur par défaut pour le compte

Vous pouvez définir la version par défaut du service de métadonnées d'instance (IMDS) au niveau du compte pour chacun d'entre eux Région AWS. Cela signifie que lorsque vous lancez une nouvelle instance, la version des métadonnées de l'instance est automatiquement définie sur la valeur par défaut au niveau du compte. Toutefois, vous pouvez modifier manuellement la valeur au lancement ou après le lancement. Pour plus d'informations sur la manière dont les paramètres au niveau du compte et les remplacements manuels affectent une instance, consultez. Ordre de priorité pour les options de métadonnées des instances

> **Note**
>
> La définition de la valeur par défaut au niveau du compte ne réinitialise pas les instances existantes. Par exemple, si vous définissez la valeur par défaut au niveau du compte surIMDSv2, les instances existantes définies sur ne IMDSv1 sont pas affectées. Si vous souhaitez modifier la valeur des instances existantes, vous devez modifier manuellement la valeur des instances elles-mêmes.

Vous pouvez définir la valeur par défaut du compte pour la version des métadonnées de l'instance de IMDSv2 telle sorte que toutes les nouvelles instances du compte soient lancées comme IMDSv2 requises et IMDSv1 soient désactivées. Avec ce compte par défaut, lorsque vous lancez une instance, les valeurs par défaut de l'instance sont les suivantes :

- Console : la version des métadonnées est définie sur V2 uniquement (jeton requis) et la limite de sauts de réponse des métadonnées est définie sur 2.
- AWS CLI: `HttpTokens` est défini sur `required` et `HttpPutResponseHopLimit` est défini sur2.

> **Note**
>
> Avant de définir la valeur par défaut du compte surIMDSv2, assurez-vous que vos instances ne dépendent pas deIMDSv1. Pour de plus amples informations, veuillez consulter Chemin recommandé pour exiger IMDSv2.

Console

À définir IMDSv2 comme compte par défaut pour la région spécifiée

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le volet de navigation, choisissez EC2Dashboard.
4. Sous Attributs du compte, sélectionnez Protection et sécurité des données.
5. À côté des IMDSvaleurs par défaut, choisissez Gérer.
6. Sur la page Gérer les IMDS paramètres par défaut, procédez comme suit :

    a. Pour le service de métadonnées d'instance, choisissez Enabled.

    b. Pour Choisir une version des métadonnées, sélectionnez V2 (jeton obligatoire).

    c. Pour la limite de sauts de réponse aux métadonnées, spécifiez 2 si vos instances hébergeront des conteneurs. Sinon, sélectionnez Aucune préférence. Lorsqu'aucune préférence n'est spécifiée, au lancement, la valeur par défaut est 2 si AMI nécessaire IMDSv2 ; sinon, elle est définie par défaut sur 1.

    d. Choisissez Mettre à jour.

AWS CLI

À définir IMDSv2 comme compte par défaut pour la région spécifiée

Utilisez la modify-instance-metadata-defaultscommande et spécifiez la région dans laquelle vous souhaitez modifier les paramètres au niveau du IMDS compte. Incluez `--http-tokens` set to `required` et `--http-put-response-hop-limit` set to 2 si vos instances hébergeront des conteneurs. Dans le cas contraire, spécifiez `-1` pour n'indiquer aucune préférence. Lorsque `-1` (aucune préférence) est spécifiée, au lancement, la valeur par défaut est 2 si AMI nécessaire IMDSv2 ; dans le cas contraire, elle est définie par défaut sur. 1

```
aws ec2 modify-instance-metadata-defaults \
    --region us-east-1 \
    --http-tokens required \
    --http-put-response-hop-limit 2
```

Sortie attendue

```
{
    "Return": true
}
```

Pour afficher les paramètres de compte par défaut pour les options de métadonnées de l'instance pour la région spécifiée

Utilisez la get-instance-metadata-defaultscommande et spécifiez la région.

```
aws ec2 get-instance-metadata-defaults --region us-east-1
```

Exemple de sortie

```
{
    "AccountLevel": {
        "HttpTokens": "required",
        "HttpPutResponseHopLimit": 2
    }
}
```

À définir IMDSv2 comme compte par défaut pour toutes les régions

Utilisez la modify-instance-metadata-defaultscommande pour modifier les paramètres au niveau du IMDS compte pour toutes les régions. Incluez `--http-tokens` set to `required` et `--http-put-response-hop-limit` set to 2 si vos instances hébergeront des conteneurs. Dans le cas contraire, spécifiez `-1` pour n'indiquer aucune préférence. Lorsque `-1` (aucune préférence) est spécifiée, au lancement, la valeur par défaut est 2 si AMI nécessaire IMDSv2 ; dans le cas contraire, elle est définie par défaut sur. 1

```
echo -e "Region          \t Modified" ; \
echo -e "--------------  \t ---------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 modify-instance-metadata-defaults \
            --region $region \
```

```
            --http-tokens required \
            --http-put-response-hop-limit 2 \
            --output text)
        echo -e "$region        \t $output"
    );
done
```

Sortie attendue

```
Region                  Modified
--------------          ---------
ap-south-1              True
eu-north-1              True
eu-west-3               True
...
```

Pour afficher les paramètres de compte par défaut pour les options de métadonnées de l'instance pour toutes les régions

Utilisez la get-instance-metadata-defaultscommande.

```
echo -e "Region   \t Level          Hops    HttpTokens" ; \
echo -e "-------------- \t ------------   ----    ----------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 get-instance-metadata-defaults \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Sortie attendue

```
Region           Level          Hops    HttpTokens
--------------   ------------   ----    ----------
ap-south-1       ACCOUNTLEVEL   2       required
```

```
eu-north-1       ACCOUNTLEVEL   2       required
eu-west-3        ACCOUNTLEVEL   2       required
...
```

PowerShell

À définir IMDSv2 comme compte par défaut pour la région spécifiée

Utilisez la Edit-EC2InstanceMetadataDefaultcommande et spécifiez la région dans laquelle vous souhaitez modifier les paramètres au niveau du IMDS compte. Incluez `-HttpToken` set to `required` et `-HttpPutResponseHopLimit` set to 2 si vos instances hébergeront des conteneurs. Dans le cas contraire, spécifiez `-1` pour n'indiquer aucune préférence. Lorsque `-1` (aucune préférence) est spécifiée, au lancement, la valeur par défaut est 2 si AMI nécessaire IMDSv2 ; dans le cas contraire, elle est définie par défaut sur. 1

```
Edit-EC2InstanceMetadataDefault `
    -Region us-east-1 `
    -HttpToken required `
    -HttpPutResponseHopLimit 2
```

Sortie attendue

```
True
```

Pour afficher les paramètres de compte par défaut pour les options de métadonnées de l'instance pour la région spécifiée

Utilisez la Get-EC2InstanceMetadataDefaultcommande et spécifiez la région.

```
Get-EC2InstanceMetadataDefault -Region us-east-1 | Format-List
```

Exemple de sortie

```
HttpEndpoint            :
HttpPutResponseHopLimit : 2
HttpTokens              : required
InstanceMetadataTags    :
```

À définir IMDSv2 comme compte par défaut pour toutes les régions

Utilisez l'Edit-EC2InstanceMetadataDefaultapplet de commande pour modifier les paramètres au niveau du IMDS compte pour toutes les régions. Incluez `-HttpToken` set to `required` et `-HttpPutResponseHopLimit` set to 2 si vos instances hébergeront des conteneurs. Dans le cas contraire, spécifiez `-1` pour n'indiquer aucune préférence. Lorsque `-1` (aucune préférence) est spécifiée, au lancement, la valeur par défaut est 2 si AMI nécessaire IMDSv2 ; dans le cas contraire, elle est définie par défaut sur. 1

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region   = $_
        Modified = (Edit-EC2InstanceMetadataDefault `
                -Region $_ `
                -HttpToken required `
                -HttpPutResponseHopLimit 2)
    }
} | `
Format-Table Region, Modified -AutoSize
```

Sortie attendue

```
Region         Modified
------         --------
ap-south-1         True
eu-north-1         True
eu-west-3          True
...
```

Pour afficher les paramètres de compte par défaut pour les options de métadonnées de l'instance pour toutes les régions

Utilisez l'Get-EC2InstanceMetadataDefaultapplet de commande.

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region = $_
        HttpPutResponseHopLimit = (Get-EC2InstanceMetadataDefault -Region
 $_).HttpPutResponseHopLimit
        HttpTokens              = (Get-EC2InstanceMetadataDefault -Region
 $_).HttpTokens
    }
```

```
} | `
Format-Table -AutoSize
```

Exemple de sortie

```
Region         HttpPutResponseHopLimit HttpTokens
------         ----------------------- ----------
ap-south-1                           2 required
eu-north-1                           2 required
eu-west-3                            2 required
...
```

Configurer l'instance au lancement

Lorsque vous lancez une instance, vous pouvez configurer l'instance pour qu'elle nécessite son utilisation IMDSv2 en configurant les champs suivants :

- EC2Console Amazon : définissez la version des métadonnées sur V2 uniquement (jeton requis).
- AWS CLI : définissez `HttpTokens` sur `required`.

Lorsque vous spécifiez que cela IMDSv2 est obligatoire, vous devez également activer le point de terminaison du service de métadonnées d'instance (IMDS) en définissant les métadonnées accessibles sur Enabled (console) ou `HttpEndpoint` sur `enabled` (AWS CLI).

Dans un environnement de conteneurs, lorsque cela IMDSv2 est nécessaire, nous vous recommandons de définir la limite de sauts sur2. Pour de plus amples informations, veuillez consulter Considérations concernant l'accès aux métadonnées des instances.

Console

Pour exiger l'utilisation de IMDSv2 sur une nouvelle instance

- Lorsque vous lancez une nouvelle instance dans la EC2 console Amazon, développez les informations avancées et procédez comme suit :
  - PourAccéder aux métadonnées, choisissezActivé.
  - Pour Choisir une version des métadonnées, sélectionnez V2 (jeton obligatoire).
  - (Environnement de conteneur) Pour Limite de sauts de réponse aux métadonnées, choisissez 2.

Pour de plus amples informations, veuillez consulter Détails avancés.

AWS CLI

Pour exiger l'utilisation de IMDSv2 sur une nouvelle instance

L'exemple run-instances ci-dessous lance une instance `c6i.large` avec `--metadata-options` défini sur `HttpTokens=required`. Lorsque vous spécifiez une valeur pour `HttpTokens`, vous devez également définir `HttpEndpoint` sur `enabled`. Comme l'en-tête du jeton sécurisé est configuré `required` pour les demandes de récupération de métadonnées, cela nécessite que l'instance soit utilisée IMDSv2 lors de la demande de métadonnées d'instance.

Dans un environnement de conteneurs, lorsque cela IMDSv2 est nécessaire, nous vous recommandons de définir la limite de sauts sur 2 with`HttpPutResponseHopLimit=2`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
 ...
    --metadata-options
 "HttpEndpoint=enabled,HttpTokens=required,HttpPutResponseHopLimit=2"
```

PowerShell

Pour exiger l'utilisation de IMDSv2 sur une nouvelle instance

L'exemple d'New-EC2Instanceapplet de commande suivant lance une `c6i.large` instance dont le paramètre est `MetadataOptions_HttpEndpoint` défini sur `enabled` et le `MetadataOptions_HttpTokens` paramètre sur. `required` Lorsque vous spécifiez une valeur pour `HttpTokens`, vous devez également définir `HttpEndpoint` sur `enabled`. Comme l'en-tête du jeton sécurisé est configuré `required` pour les demandes de récupération de métadonnées, cela nécessite que l'instance soit utilisée IMDSv2 lors de la demande de métadonnées d'instance.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint enabled `
    -MetadataOptions_HttpTokens required
```

AWS CloudFormation

Pour spécifier les options de métadonnées pour une instance en utilisant AWS CloudFormation, consultez la LaunchTemplate MetadataOptions propriété AWS: : EC2 : : dans le guide de AWS CloudFormation l'utilisateur.

Configurez le AMI

Lorsque vous enregistrez un nouveau AMI ou modifiez un existantAMI, vous pouvez définir le `imds-support` paramètre sur`v2.0`. Les instances lancées à partir de cette option AMI auront la version des métadonnées définie sur V2 uniquement (jeton requis) (console) ou `HttpTokens` définie sur `required` (AWS CLI). Avec ces paramètres, l'instance exige que cela IMDSv2 soit utilisé lors de la demande de métadonnées d'instance.

Notez que lorsque vous définissez `imds-support` cette option`v2.0`, la limite de sauts de réponse des métadonnées (console) ou `http-put-response-hop-limit` (AWS CLI) AMI sera également définie sur 2 pour les instances lancées à partir de ce paramètre.

> **Important**
>
> N'utilisez pas ce paramètre à moins que votre AMI logiciel ne le prenne en chargeIMDSv2. Une fois que vous avez défini la valeur sur `v2.0`, vous ne pouvez pas revenir en arrière. La seule façon de « réinitialiser » votre image AMI est d'en créer une nouvelle à AMI partir de l'instantané sous-jacent.

Pour configurer un nouveau AMI pour IMDSv2

Utilisez l'une des méthodes suivantes pour configurer un nouveau AMI pourIMDSv2.

AWS CLI

L'exemple d'image de registre suivant enregistre une image AMI en utilisant l'instantané spécifié d'un volume EBS racine comme périphérique. `/dev/xvda` Spécifiez `v2.0` le `imds-support` paramètre afin que les instances lancées à partir de ce AMI paramètre nécessitent son utilisation lors de la demande de métadonnées d'instance. IMDSv2

```
aws ec2 register-image \
    --name my-image \
```

```
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/
xvda,Ebs={SnapshotId=snap-0123456789example} \
    --architecture x86_64 \
    --imds-support v2.0
```

PowerShell

L'exemple d'Register-EC2Imageapplet de commande suivant enregistre une AMI copie d'écran spécifiée d'un volume EBS racine en tant que périphérique. `/dev/xvda` Spécifiez `v2.0` le `ImdsSupport` paramètre afin que les instances lancées à partir de ce AMI paramètre nécessitent son utilisation lors de la demande de métadonnées d'instance. IMDSv2

```
Register-EC2Image `
    -Name 'my-image' `
    -RootDeviceName /dev/xvda `
    -BlockDeviceMapping  (
    New-Object `
        -TypeName Amazon.EC2.Model.BlockDeviceMapping `
        -Property @{
        DeviceName = '/dev/xvda';
        EBS        = (New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property
 @{
                SnapshotId = 'snap-0123456789example'
                VolumeType = 'gp3'
                } )
        }  ) `
    -Architecture X86_64 `
    -ImdsSupport v2.0
```

Pour configurer un objet existant AMI pour IMDSv2

Utilisez l'une des méthodes suivantes pour configurer un AMI pour existantIMDSv2.

AWS CLI

L'modify-image-attributeexemple suivant IMDSv2 ne modifie qu'un objet existant AMI pour. Spécifiez `v2.0` le `imds-support` paramètre afin que les instances lancées à partir de ce AMI paramètre nécessitent son utilisation lors de la demande de métadonnées d'instance. IMDSv2

```
aws ec2 modify-image-attribute \
```

```
    --image-id ami-0123456789example \
    --imds-support v2.0
```

PowerShell

L'exemple d'Edit-EC2ImageAttributeapplet de commande suivant modifie uniquement un objet existant AMI pour. IMDSv2 Spécifiez `v2.0` le `imds-support` paramètre afin que les instances lancées à partir de ce AMI paramètre nécessitent son utilisation lors de la demande de métadonnées d'instance. IMDSv2

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -ImdsSupport 'v2.0'
```

Utiliser une IAM politique

Vous pouvez créer une IAM politique qui empêche les utilisateurs de lancer de nouvelles instances à moins qu'ils n'IMDSv2en aient besoin.

Pour imposer l'utilisation de IMDSv2 sur toutes les nouvelles instances à l'aide d'une IAM politique

Pour garantir que les utilisateurs ne peuvent lancer que des instances dont l'utilisation est requise IMDSv2 lors de la demande de métadonnées d'instance, vous pouvez spécifier que la condition requise IMDSv2 doit être remplie avant qu'une instance puisse être lancée. Pour un exemple IAM de politique, voirUtiliser des métadonnées d'instance.

Activez les points de IPv6 terminaison IMDS IPv4 et

IMDSIl possède deux points de terminaison sur une instance : IPv4 (`169.254.169.254`) et IPv6 (`[fd00:ec2::254]`). Lorsque vous activez leIMDS, le IPv4 point de terminaison est automatiquement activé. Le IPv6 point de terminaison reste désactivé même si vous lancez une instance dans un IPv6 sous-réseau uniquement. Pour activer le IPv6 point de terminaison, vous devez le faire explicitement. Lorsque vous activez le IPv6 point de IPv4 terminaison, celui-ci reste activé.

Vous pouvez activer le IPv6 point de terminaison au lancement de l'instance ou après.

Conditions requises pour activer le IPv6 point de terminaison

- Le type d'instance sélectionné est basé sur le système AWS Nitro.

- Le sous-réseau sélectionné prend IPv6 en charge les sous-réseaux à double pile ou IPv6 uniquement.

Utilisez l'une des méthodes suivantes pour lancer une instance avec le IMDS IPv6 point de terminaison activé.

New console

Pour activer le IMDS IPv6 point de terminaison lors du lancement de l'instance

- Lancez l'instance dans la EC2 console Amazon avec les informations suivantes spécifiées dans la section Détails avancés :
  - Pour le IPv6point de terminaison des métadonnées, choisissez Enabled.

Pour de plus amples informations, veuillez consulter Détails avancés.

AWS CLI

Pour activer le IMDS IPv6 point de terminaison lors du lancement de l'instance

L'exemple d'exécution d'instances suivant lance une `c6i.large` instance avec le IPv6 point de terminaison activé pour. IMDS Pour activer le IPv6 point de terminaison, spécifiez le `--metadata-options` paramètre`HttpProtocolIpv6=enabled`. Lorsque vous spécifiez une valeur pour `HttpProtocolIpv6`, vous devez également définir `HttpEndpoint` sur `enabled`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
    ...
    --metadata-options "HttpEndpoint=enabled,HttpProtocolIpv6=enabled"
```

PowerShell

Pour activer le IMDS IPv6 point de terminaison lors du lancement de l'instance

L'exemple d'New-EC2Instanceapplet de commande suivant lance une `c6i.large` instance avec le IPv6 point de terminaison activé pour. IMDS Pour activer le IPv6 point de terminaison, spécifiez `MetadataOptions_HttpProtocolIpv6` commee`enabled`. Lorsque vous spécifiez une valeur pour `MetadataOptions_HttpProtocolIpv6`, vous devez également définir `MetadataOptions_HttpEndpoint` sur `enabled`.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint enabled `
    -MetadataOptions_HttpProtocolIpv6 enabled
```

Désactiver l'accès aux métadonnées d'instance

Vous pouvez désactiver l'accès aux métadonnées de l'instance en le désactivant IMDS lorsque vous lancez une instance. Vous pouvez activer l'accès ultérieurement en réactivant leIMDS. Pour de plus amples informations, veuillez consulter Activer l'accès aux métadonnées d'instance.

> **Important**
>
> Vous pouvez choisir de le désactiver IMDS au lancement ou après le lancement. Si vous désactivez le IMDS au lancement, les opérations suivantes risquent de ne pas fonctionner :
>
> - Il se peut que vous n'ayez pas SSH accès à votre instance. Le`public-keys/0/openssh-key`, qui est la SSH clé publique de votre instance, ne sera pas accessible car la clé est normalement fournie et accessible à partir des métadonnées de l'EC2instance.
> - EC2les données utilisateur ne seront pas disponibles et ne seront pas exécutées au démarrage de l'instance. EC2les données utilisateur sont hébergées sur leIMDS. Si vous le désactivezIMDS, vous désactivez effectivement l'accès aux données utilisateur.
>
> Pour accéder à cette fonctionnalité, vous pouvez la réactiver IMDS après le lancement.

Console

Pour désactiver l'accès aux métadonnées d'instance

- Lancez l'instance dans la EC2 console Amazon avec les informations suivantes spécifiées dans la section Détails avancés :
  - PourAccéder aux métadonnées, choisissez Activé.

Pour de plus amples informations, veuillez consulter Détails avancés.

AWS CLI

Pour désactiver l'accès aux métadonnées d'instance au lancement

Lancez l'instance avec `--metadata-options` défini sur `HttpEndpoint=disabled`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
    ...
    --metadata-options "HttpEndpoint=disabled"
```

PowerShell

Pour désactiver l'accès aux métadonnées d'instance au lancement

L'exemple d'[New-EC2Instance]applet de commande suivant lance une instance dont la valeur est `MetadataOptions_HttpEndpoint` définie sur. `disabled`

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint disabled
```

AWS CloudFormation

Pour spécifier les options de métadonnées pour une instance en utilisant AWS CloudFormation, consultez la LaunchTemplate MetadataOptions propriété [AWS: : EC2 : :] dans le guide de AWS CloudFormation l'utilisateur.

Configurer les options de métadonnées d'instance pour les instances existantes

Vous pouvez modifier les options des métadonnées d'instance pour les instances existantes.

Vous pouvez également créer une IAM politique qui empêche les utilisateurs de modifier les options de métadonnées des instances existantes. Pour contrôler quels utilisateurs peuvent modifier les options de métadonnées de l'instance, spécifiez une politique qui empêche tous les utilisateurs autres que les utilisateurs ayant un rôle spécifique d'utiliser le [ModifyInstanceMetadataOptions]API. Pour un exemple IAM de politique, voir[Utiliser des métadonnées d'instance].

Exigence d'utilisation d'IMDSv2

Utilisez l'une des méthodes suivantes pour modifier les options de métadonnées d'instance sur une instance existante afin d'exiger qu'elle IMDSv2 soit utilisée lors de la demande de métadonnées d'instance. Lorsque cela IMDSv2 est nécessaire, IMDSv1 ne peut pas être utilisé.

> **Note**
>
> Avant de demander que cela IMDSv2 soit utilisé, assurez-vous que l'instance ne passe pas d'IMDSv1appels. La `MetadataNoToken` CloudWatch métrique suit les IMDSv1 appels. Lorsqu'`MetadataNoToken`aucune IMDSv1 utilisation n'est enregistrée pour une instance, celle-ci est alors prête à être requiseIMDSv2.

Console

Pour exiger l'utilisation de IMDSv2 sur une instance existante

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez votre instance.
4. Choisissez Actions, Paramètres de l'instance, puis Modifier les options des métadonnées d'instance.
5. Dans la boîte de dialogue Modifier les options des métadonnées d'instance, procédez comme suit :
   a. Pour Service de métadonnées d'instance, sélectionnez Activer.
   b. Pour IMDSv2, choisissez Obligatoire.
   c. Choisissez Save (Enregistrer).

AWS CLI

Pour exiger l'utilisation de IMDSv2 sur une instance existante

Utilisez la modify-instance-metadata-optionsCLIcommande et définissez le `http-tokens` paramètre sur`required`. Lorsque vous spécifiez une valeur pour `http-tokens`, vous devez également définir `http-endpoint` sur `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-tokens required \
    --http-endpoint enabled
```

PowerShell

Pour exiger l'utilisation de IMDSv2 sur une instance existante

Utilisez l'Edit-EC2InstanceMetadataOptionapplet de commande et définissez le `HttpTokens` paramètre sur. `required` Lorsque vous spécifiez une valeur pour `HttpTokens`, vous devez également définir `HttpEndpoint` sur `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpTokens required `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Restaurez l'utilisation de IMDSv1

Lorsque cela IMDSv2 est nécessaire, IMDSv1 cela ne fonctionnera pas lors de la demande de métadonnées d'instance. Quand IMDSv2 c'est facultatif, alors IMDSv2 les deux IMDSv1 fonctionneront. Par conséquent, pour effectuer une restaurationIMDSv1, IMDSv2 rendez-la facultative en utilisant l'une des méthodes suivantes.

Console

Pour rétablir l'utilisation de IMDSv1 sur une instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez votre instance.
4. Choisissez Actions, Paramètres de l'instance, puis Modifier les options des métadonnées d'instance.
5. Dans la boîte de dialogue Modifier les options des métadonnées d'instance, procédez comme suit :

    a. Pour Service de métadonnées d'instance, assurez-vous que l'option Activer est sélectionnée.

b. Pour IMDSv2, choisissez Facultatif.

c. Choisissez Save (Enregistrer).

AWS CLI

Pour rétablir l'utilisation de IMDSv1 sur une instance

Vous pouvez utiliser la modify-instance-metadata-optionsCLIcommande avec `http-tokens` set `optional` to pour rétablir l'utilisation de IMDSv1 lorsque vous demandez des métadonnées d'instance.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-tokens optional \
    --http-endpoint enabled
```

PowerShell

Pour rétablir l'utilisation de IMDSv1 sur une instance

Vous pouvez utiliser l'Edit-EC2InstanceMetadataOptionapplet de commande avec `HttpTokens` set `optional` to pour rétablir l'utilisation de IMDSv1 lorsque vous demandez des métadonnées d'instance.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpTokens optional `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Modifier la limite de sauts de PUT réponse

Pour les instances existantes, vous pouvez modifier les paramètres de la durée de vie (hop limit) de la réponse PUT.

Actuellement, seuls les AWS CLI et AWS SDKs prennent en charge la modification de la limite de sauts de PUT réponse.

AWS CLI

Pour modifier la limite de sauts de PUT réponse

Utilisez la modify-instance-metadata-optionsCLIcommande et définissez le `http-put-response-hop-limit` paramètre sur le nombre de sauts requis. Dans l'exemple suivant, la durée de vie (hop limit) est définie `3`. Notez que lorsque vous spécifiez une valeur pour `http-put-response-hop-limit`, vous devez également définir `http-endpoint` sur `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-put-response-hop-limit 3 \
    --http-endpoint enabled
```

PowerShell

Pour modifier la limite de sauts de PUT réponse

Utilisez l'Edit-EC2InstanceMetadataOptionapplet de commande et définissez le `HttpPutResponseHopLimit` paramètre sur le nombre de sauts requis. Dans l'exemple suivant, la durée de vie (hop limit) est définie `3`. Notez que lorsque vous spécifiez une valeur pour `HttpPutResponseHopLimit`, vous devez également définir `HttpEndpoint` sur `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpPutResponseHopLimit 3 `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Activez les points de IPv6 terminaison IMDS IPv4 et

IMDSII possède deux points de terminaison sur une instance : IPv4 (`169.254.169.254`) et IPv6 (`[fd00:ec2::254]`). Lorsque vous activez leIMDS, le IPv4 point de terminaison est automatiquement activé. Le IPv6 point de terminaison reste désactivé même si vous lancez une instance dans un IPv6 sous-réseau uniquement. Pour activer le IPv6 point de terminaison, vous devez le faire explicitement. Lorsque vous activez le IPv6 point de IPv4 terminaison, celui-ci reste activé.

Vous pouvez activer le IPv6 point de terminaison au lancement de l'instance ou après.

Conditions requises pour activer le IPv6 point de terminaison

- Le type d'instance sélectionné est basé sur le système AWS Nitro.
- Le sous-réseau sélectionné prend IPv6 en charge les sous-réseaux à double pile ou IPv6 uniquement.

Actuellement, seul le AWS SDKs support AWS CLI et active le IMDS IPv6 point de terminaison après le lancement de l'instance.

AWS CLI

Pour activer le IMDS IPv6 point de terminaison pour votre instance

Utilisez la modify-instance-metadata-optionsCLIcommande et définissez le `http-protocol-ipv6` paramètre sur`enabled`. Notez que lorsque vous spécifiez une valeur pour `http-protocol-ipv6`, vous devez également définir `http-endpoint` sur `enabled`.

```
aws ec2 modify-instance-metadata-options \
 --instance-id i-1234567898abcdef0 \
 --http-protocol-ipv6 enabled \
 --http-endpoint enabled
```

PowerShell

Pour activer le IMDS IPv6 point de terminaison pour votre instance

Utilisez l'Edit-EC2InstanceMetadataOptionapplet de commande et définissez le `HttpProtocolIpv6` paramètre sur. `enabled` Notez que lorsque vous spécifiez une valeur pour `HttpProtocolIpv6`, vous devez également définir `HttpEndpoint` sur `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpProtocolIpv6 enabled `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Activer l'accès aux métadonnées d'instance

Vous pouvez activer l'accès aux métadonnées de l'instance en activant le HTTP point de terminaison IMDS sur votre instance, quelle que soit la version IMDS que vous utilisez. Vous pouvez annuler cette modification à tout moment en désactivant le HTTP terminal.

Pour activer l'accès aux métadonnées d'instance sur une instance, utilisez l'une des méthodes suivantes.

Console

Activation de l'accès aux métadonnées d'instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez votre instance.
4. Choisissez Actions, Paramètres de l'instance, puis Modifier les options des métadonnées d'instance.
5. Dans la boîte de dialogue Modifier les options des métadonnées d'instance, procédez comme suit :
   a. Pour Service de métadonnées d'instance, sélectionnez Activer.
   b. Choisissez Save (Enregistrer).

AWS CLI

Activation de l'accès aux métadonnées d'instance

Utilisez la modify-instance-metadata-optionsCLIcommande et définissez le `http-endpoint` paramètre sur`enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-endpoint enabled
```

PowerShell

Activation de l'accès aux métadonnées d'instance

Utilisez l'Edit-EC2InstanceMetadataOptionapplet de commande et définissez le `HttpEndpoint` paramètre sur. `enabled`

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Désactiver l'accès aux métadonnées d'instance

Vous pouvez désactiver l'accès aux métadonnées de l'instance en désactivant le HTTP point de terminaison de l'IMDSinstance, quelle que soit la version que IMDS vous utilisez. Vous pouvez annuler cette modification à tout moment en activant le HTTP point de terminaison.

Pour désactiver l'accès aux métadonnées d'instance sur une instance, utilisez l'une des méthodes suivantes.

Console

Désactivation de l'accès aux métadonnées d'instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez votre instance.
4. Choisissez Actions, Paramètres de l'instance, puis Modifier les options des métadonnées d'instance.
5. Dans la boîte de dialogue Modifier les options des métadonnées d'instance, procédez comme suit :
   a. Pour Service de métadonnées d'instance, désélectionnez Activer.
   b. Choisissez Save (Enregistrer).

AWS CLI

Désactivation de l'accès aux métadonnées d'instance

Utilisez la modify-instance-metadata-optionsCLIcommande et définissez le `http-endpoint` paramètre sur`disabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-endpoint disabled
```

PowerShell

Désactivation de l'accès aux métadonnées d'instance

Utilisez l'Edit-EC2InstanceMetadataOptionapplet de commande et définissez le `HttpEndpoint` paramètre sur. `disabled`

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpEndpoint disabled).InstanceMetadataOptions
```

Exécuter des commandes lorsque vous lancez une EC2 instance avec saisie de données utilisateur

Lorsque vous lancez une EC2 instance Amazon, vous pouvez transmettre les données utilisateur à l'instance qui est utilisée pour effectuer des tâches de configuration automatisées ou pour exécuter des scripts après le démarrage de l'instance.

Si vous êtes intéressé par des scénarios d'automatisation plus complexes, vous pouvez envisager AWS CloudFormation ou AWS OpsWorks. Pour plus d'informations, consultez les ressources suivantes :

- Déploiement d'applications sur Amazon EC2 AWS CloudFormation dans le guide de AWS CloudFormation l'utilisateur.
- AWS OpsWorks Guide de l'utilisateur.

Sur les instances Linux, vous pouvez transmettre deux types de données utilisateur à Amazon EC2 : les scripts shell et les directives cloud-init. Vous pouvez également transmettre ces données à l'assistant de lancement d'instance sous forme de texte brut, de fichier (utile pour lancer des instances à l'aide des outils de ligne de commande) ou de texte codé en base64 (pour les API appels).

Sur les instances Windows, les agents de lancement gèrent vos scripts de données utilisateur. Les sections suivantes présentent les différences dans la manière dont les données utilisateur sont traitées sur chaque système d'exploitation.

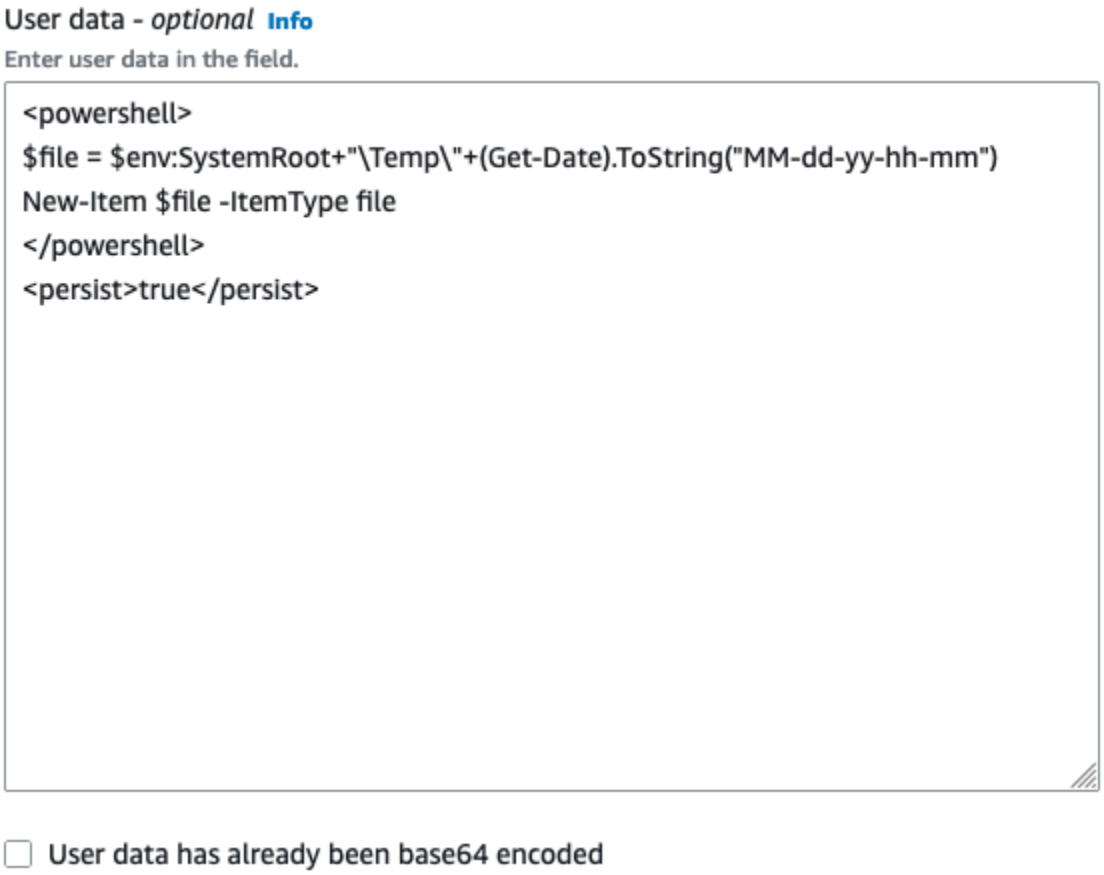
Données utilisateur dans le AWS Management Console

Vous pouvez spécifier des données utilisateur d'instance lorsque vous lancez l'instance. Si le volume racine de l'instance est un EBS volume, vous pouvez également arrêter l'instance et mettre à jour ses données utilisateur.

Spécifiez les données utilisateur de l'instance au lancement avec le Launch Wizard

Vous pouvez spécifier les données utilisateur lorsque vous lancez une instance à l'aide du Launch Wizard de la EC2 console. Pour spécifier les données utilisateur lors du lancement, suivez la procédure de lancement d'une instance. Le champ User data (Données utilisateur) se trouve dans la section Détails avancés de l'assistant de lancement d'instance. Entrez votre PowerShell script dans le champ Données utilisateur, puis terminez la procédure de lancement de l'instance.

Dans la capture d'écran suivante du champ Données utilisateur, l'exemple de script crée un fichier dans le dossier temporaire Windows, en utilisant la date et l'heure actuelles dans le nom de fichier. Lorsque vous incluez `<persist>true</persist>`, le script est exécuté chaque fois que vous redémarrez ou démarrez l'instance. Si vous laissez la case à cocher Les données utilisateur ont déjà été encodées en base64 vide, la EC2 console Amazon effectue le codage en base64 pour vous.



Pour de plus amples informations, veuillez consulter Spécifiez les données utilisateur de l'instance au lancement avec le Launch Wizard. Pour un exemple de Linux utilisant le AWS CLI, voirthe section called "Les données de l'utilisateur et le AWS CLI". Pour un exemple de Windows utilisant les outils pour Windows PowerShell, voirthe section called "Les données utilisateur et les outils pour Windows PowerShell".

Affichage et mise à jour des données utilisateur d'instance

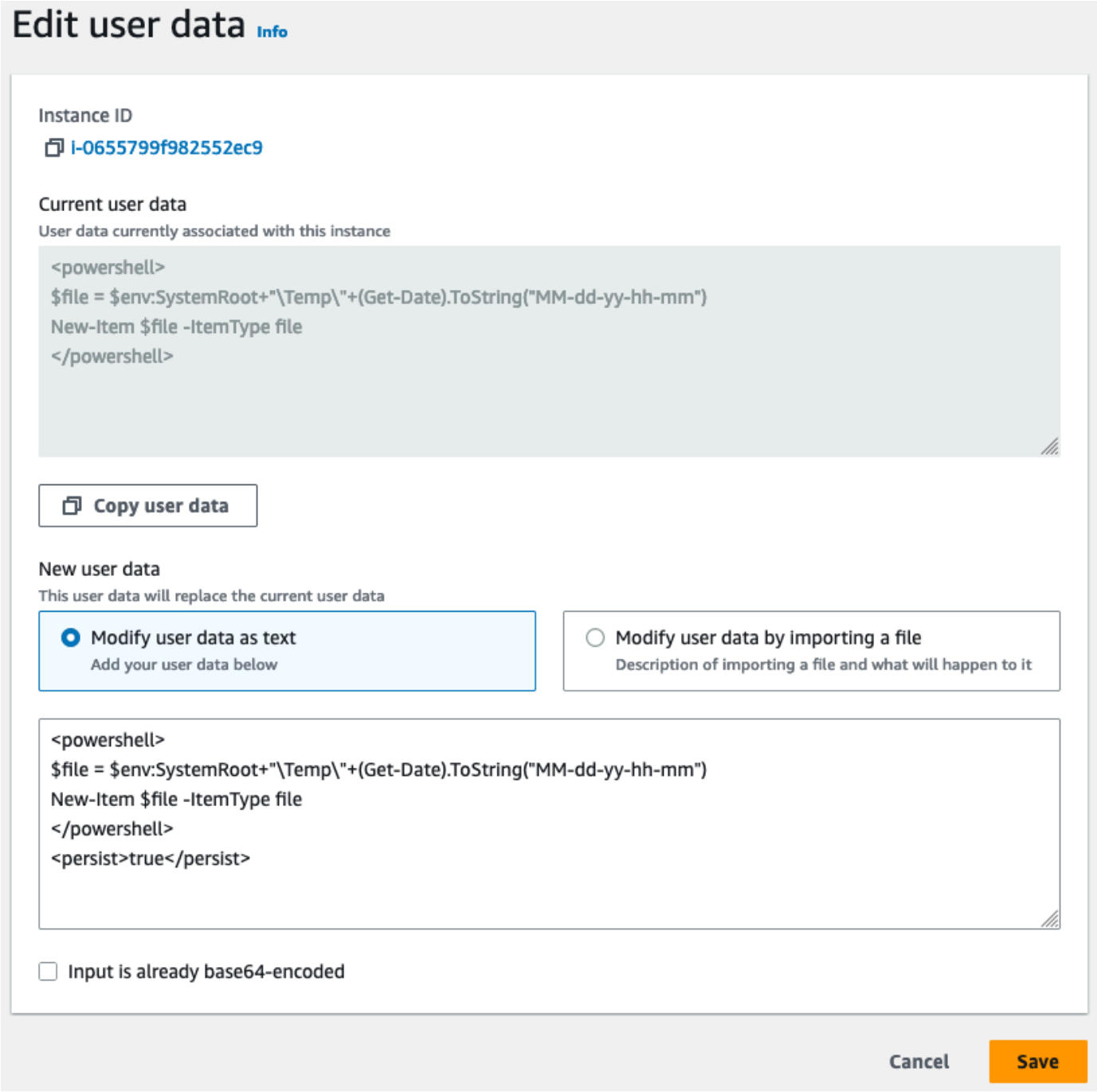
Vous pouvez afficher les données utilisateur d'instance pour n'importe quelle instance, et vous pouvez mettre à jour les données utilisateur d'instance pour une instance arrêtée.

Pour mettre à jour les données utilisateur pour une instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance et choisissez Actions, État de l'instance, Arrêter l'instance.

   > **Warning**
   >
   > Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

4. Lorsque vous êtes invité à confirmer l'opération, choisissez Arrêter. L'arrêt de l'instance peut prendre quelques minutes.
5. Alors que l'instance est toujours sélectionnée, choisissez Actions, Instance settings (Paramètres de l'instance), Edit user data (Modifier les données utilisateur). Vous ne pouvez changer les données utilisateur si l'instance est en cours d'exécution, mais vous pouvez les voir.
6. Dans la boîte de dialogue Modifier les données utilisateur, mettez à jour les données utilisateur, puis cliquez sur Enregistrer. Pour exécuter des scripts de données utilisateur chaque fois que vous redémarrez ou démarrez l'instance, ajoutez `<persist>true</persist>`, comme illustré dans l'exemple suivant.



7. Démarrez l'instance. Si vous avez activé l'exécution des données utilisateur pour les redémarrages ou démarrages suivants, les scripts de données utilisateur mis à jour sont exécutés dans le cadre du processus de démarrage de l'instance.

Comment Amazon EC2 gère les données utilisateur pour les instances Linux

Dans les exemples suivants, les commandes d'installation d'un LAMP serveur sur Amazon Linux 2 sont converties en un script shell et en un ensemble de directives cloud-init qui s'exécutent au lancement de l'instance. Dans chaque exemple, les tâches suivantes sont exécutées par les données de l'utilisateur :

- Les packages logiciels de distribution sont mis à jour.
- Le serveur web, les packages php et `mariadb` nécessaires sont installés.
- Le service `httpd` est lancé et activé via la commande systemctl.
- L'utilisateur `ec2-user` est ajouté au groupe Apache.
- La propriété et les autorisations sur les fichiers appropriées sont définies pour le répertoire web et les fichiers qu'il contient.
- Une page Web simple est créée pour tester le serveur Web et le PHP moteur.

Table des matières

Prérequis

Les exemples de cette rubrique supposent ce qui suit :

- Votre instance possède un DNS nom public accessible depuis Internet.
- Le groupe de sécurité associé à votre instance est configuré pour autoriser le trafic SSH (port 22) afin que vous puissiez vous connecter à l'instance pour consulter les fichiers journaux de sortie.
- Votre instance est lancée avec un Amazon Linux 2AMI. Ces instructions sont destinées à Amazon Linux 2, et il se peut que les commandes et les directives ne fonctionnent pas pour d'autres distributions Linux. Pour obtenir plus d'informations sur d'autres distributions, comme leur support pour cloud-init, consultez leur documentation spécifique.

Données utilisateur et scripts shell

Si vous connaissez le scripting de shell, il s'agit de la méthode la plus simple et la plus complète pour envoyer des instructions à une instance lors du lancement. L'ajout de ces tâches au moment du démarrage augmente le temps que cela prend pour démarrer l'instance. Vous devriez laisser s'écouler quelques minutes supplémentaires pour que les tâches s'effectuent avant de vérifier que le script utilisateur a fini avec succès.

> **Important**
>
> Par défaut, les scripts de données utilisateur et les directives cloud init s'exécutent uniquement pendant le cycle de démarrage lorsque vous lancez une instance pour la première fois. Vous pouvez mettre à jour votre configuration pour vous assurer que vos scripts de données utilisateur et vos directives cloud-init s'exécutent chaque fois que vous redémarrez votre instance. Pour plus d'informations, consultez Comment utiliser les données utilisateur pour exécuter automatiquement un script à chaque redémarrage de mon instance Amazon EC2 Linux ? dans le AWS Knowledge Center.

Les scripts shell de données utilisateur doivent commencer par les caractères `#!` et le chemin vers interpréteur que vous avez choisi pour la lecture du script (généralement /bin/bash)). Pour une introduction aux scripts shell, consultez le manuel de référence Bash sur le site Web du système GNU d'exploitation.

Les scripts entrés en tant que données utilisateur sont exécutés en tant qu'utilisateur root, donc n'utilisez pas la commande sudo dans le script. N'oubliez pas que tous les fichiers que vous créez seront la propriété de l'utilisateur root. Si vous avez besoin qu'un utilisateur non root ait accès aux fichiers, vous devez modifier les autorisations en conséquence dans le script. Par ailleurs, étant donné que le script n'est pas exécuté de façon interactive, vous ne pouvez pas inclure des commandes qui nécessitent les réactions de l'utilisateur (comme yum update sans l'indicateur `-y`).

Si vous utilisez un AWS API, y compris le AWS CLI, dans un script de données utilisateur, vous devez utiliser un profil d'instance lors du lancement de l'instance. Un profil d'instance fournit les AWS informations d'identification appropriées requises par le script de données utilisateur pour émettre l'APIappel. Pour plus d'informations, consultez la section Utilisation des profils d'instance dans le Guide de IAM l'utilisateur. Les autorisations que vous attribuez au IAM rôle dépendent des services que vous appelez avec leAPI. Pour de plus amples informations, veuillez consulter IAMrôles pour Amazon EC2.

Le fichier journal de sortie cloud-init () capture la sortie de la console, si bien que vous pouvez facilement déboguer vos scripts après un lancement si l'instance ne se comporte pas comme vous le vouliez. Pour afficher le fichier journal,connexion à l'instanceet ouvrez`/var/log/cloud-init-output.log`.

Lorsqu'un script de données utilisateur est traité, il est copié dans et exécuté à partir de l `/var/lib/cloud/instances/`*`instance-id`*`/`. Le script n'est pas supprimé après son exécution. Assurez-vous de supprimer les scripts de données utilisateur `/var/lib/cloud/instances/`*`instance-id`*`/` avant de créer un script AMI à partir de l'instance. Dans le cas contraire, le script existera dans ce répertoire sur n'importe quelle instance lancée depuis leAMI.

Mettre à jour les données utilisateur de l'instance

Pour mettre à jour les données de l'utilisateur de l'instance, vous devez d'abord arrêter l'instance. Si l'instance est en cours d'exécution, vous pouvez afficher les données utilisateur, mais vous ne pouvez pas les modifier.

> **Warning**
>
> Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

Pour modifier les données utilisateur d'instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance et choisissez État de l'instance, Arrêter l'instance. Si cette option est désactivée, l'instance est déjà arrêtée ou son périphérique racine est un volume de stockage d'instances.
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Arrêter. L'arrêt de l'instance peut prendre quelques minutes.
5. Alors que l'instance est toujours sélectionnée, choisissez Actions, Instance settings (Paramètres de l'instance), Edit user data (Modifier les données utilisateur).
6. Modifiez les données utilisateur selon vos besoins, puis choisissez Save (Enregistrer).
7. Démarrez l'instance. Les nouvelles données utilisateur sont visibles sur votre instance, après son démarrage. Par contre, les scripts des données utilisateur ne sont pas exécutés.

Directives sur les données utilisateur et Cloud-Init

Le package cloud-init configure les aspects spécifiques d'une nouvelle instance Amazon Linux lorsqu'elle est lancée. Il configure plus particulièrement le fichier `.ssh/authorized_keys` pour l'utilisateur ec2 afin que vous puissiez vous connecter avec votre clé privée. Pour plus d'informations sur les tâches de configuration effectuées par le package cloud-init pour les instances Amazon Linux, consultez la section Utilisation de cloud-init sur Amazon Linux 2 dans le guide de l'utilisateur Amazon Linux 2.

Les directives d'utilisateur cloud-init peuvent être transférées vers une instance au moment du lancement tout comme un script, même si la syntaxe est différente. Pour plus d'informations sur cloud-init, consultez http://cloudinit.readthedocs.org/en/latest/index.html.

> **Important**
>
> Par défaut, les scripts de données utilisateur et les directives cloud init s'exécutent uniquement pendant le cycle de démarrage lorsque vous lancez une instance pour la première fois. Vous pouvez mettre à jour votre configuration pour vous assurer que vos scripts de données utilisateur et vos directives cloud-init s'exécutent chaque fois que vous redémarrez votre instance. Pour plus d'informations, consultez Comment utiliser les données utilisateur pour exécuter automatiquement un script à chaque redémarrage de mon instance Amazon EC2 Linux ? dans le AWS Knowledge Center.

L'ajout de ces tâches au moment du démarrage augmente le temps que cela prend pour démarrer une instance. Vous devriez laisser s'écouler quelques minutes supplémentaires pour que les tâches s'effectuent avant de vérifier que vos directives sur les données utilisateur sont terminées.

Pour transférer les directives cloud-init vers une instance avec les données utilisateur

1. Suivez la procédure pour lancer une instance. Le champ User data (Données utilisateur) se trouve dans la section Détails avancés de l'assistant de lancement d'instance. Saisissez le texte de la directive cloud-init dans le champ User data (Données utilisateur), puis terminez la procédure de lancement de l'instance.

   Pour l'exemple ci-dessous, les directives créent et configurent un serveur Web sur Amazon Linux 2. La ligne `#cloud-config` en haut est requise pour identifier les commandes en tant que directives cloud-init.

```
#cloud-config
repo_update: true
repo_upgrade: all

packages:
- httpd
- mariadb-server

runcmd:
- [ sh, -c, "amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2" ]
- systemctl start httpd
- sudo systemctl enable httpd
- [ sh, -c, "usermod -a -G apache ec2-user" ]
- [ sh, -c, "chown -R ec2-user:apache /var/www" ]
- chmod 2775 /var/www
- [ find, /var/www, -type, d, -exec, chmod, 2775, {}, \; ]
- [ find, /var/www, -type, f, -exec, chmod, 0664, {}, \; ]
- [ sh, -c, 'echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php' ]
```

2. Laissez assez de temps à l'instance pour lancer et exécuter les directives dans vos données utilisateur, puis vérifiez que vos directives ont terminé les tâches que vous souhaitiez.

   Pour cet exemple, dans un navigateur Web, entrez le fichier URL de PHP test créé par les directives. Il URL s'agit de l'DNSadresse publique de votre instance suivie d'une barre oblique et du nom du fichier.

   ```
   http://my.public.dns.amazonaws.com/phpinfo.php
   ```

   Vous devriez voir la page PHP d'information. Si vous ne pouvez pas voir la page PHP d'informations, vérifiez que le groupe de sécurité que vous utilisez contient une règle autorisant le trafic HTTP (port 80). Pour de plus amples informations, veuillez consulter Configuration des règles du groupe de sécurité.

3. (Facultatif) Si vos directives n'ont pas accompli les tâches que vous attendiez ou si vous voulez uniquement vérifier que vos directives se sont terminées sans erreur, connectez-vous à l'instance, examinez le fichier journal de sortie (`/var/log/cloud-init-output.log`) et recherchez les messages erronés dans les résultats. Pour plus d'informations sur le débogage, vous pouvez ajouter la ligne suivante à vos directives :

   ```
   output : { all : '| tee -a /var/log/cloud-init-output.log' }
   ```

Cette directive envoie le résultat runcmd à `/var/log/cloud-init-output.log`.

Les données de l'utilisateur et le AWS CLI

Vous pouvez utiliser le AWS CLI pour spécifier, modifier et afficher les données utilisateur de votre instance. Pour plus d'informations sur l'affichage des données utilisateur de votre instance à l'aide des métadonnées d'instance, consultez Accéder aux métadonnées d'une EC2 instance.

Sous Windows, vous pouvez utiliser le AWS Tools for Windows PowerShell au lieu du AWS CLI. Pour plus d'informations, consultez Les données utilisateur et les outils pour Windows PowerShell.

Exemple : spécification des données utilisateur au moment du lancement

Pour spécifier les données utilisateur lorsque vous lancez l'instance, utilisez la commande run-instances avec le paramètre `--user-data`. Avecrun-instances, il AWS CLI effectue le codage base64 des données utilisateur pour vous.

L'exemple suivant montre comment définir un script en tant que chaîne sur la ligne de commande :

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
    --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234
 \
    --user-data echo user data
```

L'exemple suivant montre comment définir un script en utilisant un fichier texte. Assurez-vous d'utiliser le préfixe `file://` pour spécifier le fichier.

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
    --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234
 \
    --user-data file://my_script.txt
```

L'exemple suivant est celui d'un fichier texte avec un script shell.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Exemple : Modification des données utilisateur d'une instance arrêtée

Vous pouvez modifier les données utilisateur d'une instance arrêtée à l'aide de la modify-instance-attributecommande. Avecmodify-instance-attribute, le AWS CLI n'effectue pas le codage base64 des données utilisateur pour vous.

- Sur un ordinateur Linux utilisez la commande base64 pour encoder les données utilisateur.

```
base64 my_script.txt >my_script_base64.txt
```

- Sur un ordinateur Windows, utilisez la commande certutil pour encoder les données utilisateur. Avant de pouvoir utiliser ce fichier avec le AWS CLI, vous devez supprimer les première (BEGINCERTIFICATE) et dernière (ENDCERTIFICATE) lignes.

```
certutil -encode my_script.txt my_script_base64.txt
notepad my_script_base64.txt
```

Utilisez les paramètres `--attribute` et `--value` afin d'utiliser le fichier texte encodé pour spécifier les données utilisateur. Assurez-vous d'utiliser le préfixe `file://` pour spécifier le fichier.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --value file://my_script_base64.txt
```

Exemple : Effacer les données utilisateur d'une instance arrêtée

Pour supprimer les données utilisateur existantes, utilisez la modify-instance-attributecommande suivante :

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --user-data Value=
```

Exemple : Affichage des données utilisateur

Pour récupérer les données utilisateur d'une instance, utilisez la describe-instance-attributecommande. Avecdescribe-instance-attribute, le AWS CLI n'effectue pas de décodage base64 des données utilisateur pour vous.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData
```

Voici un exemple de sortie avec les données utilisateur base64 encodées.

```
{
    "UserData": {
        "Value":
 "IyEvYmluL2Jhc2gKeXVtIHVwZGF0ZSAteQpzZXJ2aWNlIGh0dHBkIHN0YXJ0CmNoa2NvbmZpZyBodHRwZCBvbg=="
    },
    "InstanceId": "i-1234567890abcdef0"
}
```

- Sur un ordinateur Linux, utilisez l'option `--query` pour obtenir les données utilisateur encodées et la commande base64 pour les décoder.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --output text --query "UserData.Value" | base64 --decode
```

- Sur un ordinateur Windows, utilisez l'option `--query` pour obtenir les données utilisateur codées et la commande certutil pour les décoder. Notez que la sortie encodée est stockée dans un fichier et que la sortie décodée est stockée dans un autre fichier.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --output text --query "UserData.Value" >my_output.txt
certutil -decode my_output.txt my_output_decoded.txt
type my_output_decoded.txt
```

Voici un exemple de sortie.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Combiner des scripts shell et des directives cloud-init

Par défaut, vous ne pouvez inclure qu'un seul type de contenu à la fois dans les données utilisateur. Toutefois, vous pouvez utiliser les types de contenu `text/cloud-config` et `text/x-shellscript` dans un fichier MIME en plusieurs parties pour inclure à la fois un script shell et des directives cloud-init dans vos données utilisateur.

Le format MIME en plusieurs parties est représenté ci-dessous.

```
Content-Type: multipart/mixed; boundary="//"
```

```
MIME-Version: 1.0

--//
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config
cloud-init directives

--//
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash
shell script commands
--//--
```

Par exemple, les données utilisateur suivantes incluent des directives cloud-init et un script shell bash. Les directives cloud-init créent un fichier (`/test-cloudinit/cloud-init.txt`) et y écrivent `Created by cloud-init`. Le script shell bash crée un fichier (`/test-userscript/userscript.txt`) et y écrit `Created by bash shell script`.

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0

--//
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config
runcmd:
- [ mkdir, /test-cloudinit ]
write_files:
- path: /test-cloudinit/cloud-init.txt
content: Created by cloud-init

--//
```

```
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash
mkdir test-userscript
touch /test-userscript/userscript.txt
echo "Created by bash shell script" >> /test-userscript/userscript.txt
--//--
```

Comment Amazon EC2 gère les données utilisateur pour les instances Windows

Sur les instances Windows, l'agent de lancement exécute les tâches liées aux données utilisateur. Pour plus d'informations, consultez les ressources suivantes :

- EC2Launch v2
- EC2Launch
- EC2Configservice

Pour des exemples d'assemblage d'une `UserData` propriété dans un AWS CloudFormation modèle, voir Propriété codée en Base64 et UserData Propriété codée en Base64 avec AccessKey et. UserData SecretKey

Pour un exemple d'exécution de commandes sur une instance au sein d'un groupe Auto Scaling qui fonctionne avec des hooks de cycle de vie, consultez Tutoriel : Configurer les données utilisateur pour récupérer l'état du cycle de vie cible via les métadonnées de l'instance dans le guide de l'utilisateur Amazon EC2 Auto Scaling.

Table des matières

Scripts de données utilisateur

Pour `EC2Config` ou `EC2Launch` pour exécuter des scripts, vous devez placer le script dans une balise spéciale lorsque vous l'ajoutez aux données utilisateur. La balise que vous utilisez varie selon

que les commandes sont exécutées dans une fenêtre d'invite de commandes (commandes par lots) ou qu'elles utilisent WindowsPowerShell.

Si vous spécifiez à la fois un script batch et un PowerShell script Windows, le script batch s'exécute en premier et le PowerShell script Windows s'exécute ensuite, quel que soit l'ordre dans lequel ils apparaissent dans les données utilisateur de l'instance.

Si vous utilisez un AWS API, y compris le AWS CLI, dans un script de données utilisateur, vous devez utiliser un profil d'instance lors du lancement de l'instance. Un profil d'instance fournit les AWS informations d'identification appropriées requises par le script de données utilisateur pour effectuer l'APIappel. Pour de plus amples informations, veuillez consulter Profils d'instance. Les autorisations que vous attribuez au IAM rôle dépendent des services que vous appelez avec leAPI. Pour de plus amples informations, veuillez consulter IAMrôles pour Amazon EC2.

Type de script

- Syntaxe des scripts par lots
- Syntaxe des PowerShell scripts Windows
- Syntaxe des scripts YAML de configuration
- Encodage Base64

Syntaxe des scripts par lots

Spécifiez un script par lots à l'aide de la balise `script`. Séparez les commandes à l'aide de sauts de ligne, comme indiqué dans l'exemple suivant.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
```

Par défaut, les scripts de données utilisateur s'exécutent une seule fois, lorsque vous lancez l'instance. Pour exécuter des scripts de données utilisateur chaque fois que vous redémarrez ou démarrez l'instance, ajoutez `<persist>true</persist>` aux données utilisateur.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
```

```
<persist>true</persist>
```

EC2Launchagent v2

Pour exécuter un script de données XML utilisateur en tant que processus détaché avec la executeScript tâche EC2Launch v2 dans l'`UserData`étape, ajoutez `<detach>true</detach>` les données utilisateur.

> **Note**
>
> La detach balise n'est pas prise en charge par les agents de lancement précédents.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
<detach>true</detach>
```

Syntaxe des PowerShell scripts Windows

AWS Windows AMIs inclut le AWS Tools for Windows PowerShell, afin que vous puissiez spécifier ces applets de commande dans les données utilisateur. Si vous associez un IAM rôle à votre instance, vous n'avez pas besoin de spécifier d'informations d'identification pour les applets de commande, car les applications qui s'exécutent sur l'instance utilisent les informations d'identification du rôle pour accéder aux AWS ressources (par exemple, les compartiments Amazon S3).

Spécifiez un PowerShell script Windows à l'aide de la `<powershell>` balise. Séparez les commandes à l'aide de sauts de ligne. La balise `<powershell>` est sensible à la casse.

Par exemple :

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
```

Par défaut, les scripts de données utilisateur s'exécutent une seule fois lorsque vous lancez l'instance. Pour exécuter des scripts de données utilisateur chaque fois que vous redémarrez ou démarrez l'instance, ajoutez `<persist>true</persist>` aux données utilisateur.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Vous pouvez spécifier un ou plusieurs PowerShell arguments à l'aide de la `<powershellArguments>` balise. Si aucun argument n'est passé, EC2Launch et que la EC2Launch v2 ajoute l'argument suivant par défaut :`-ExecutionPolicy Unrestricted`.

Exemple :

```
<powershell>
    $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

EC2Launchagent v2

Pour exécuter un script de données XML utilisateur en tant que processus détaché avec la executeScript tâche EC2Launch v2 dans l'`UserData`étape, ajoutez `<detach>true</detach>` les données utilisateur.

> **Note**
>
> La detach balise n'est pas prise en charge par les agents de lancement précédents.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<detach>true</detach>
```

Syntaxe des scripts YAML de configuration

Si vous utilisez la EC2Launch version 2 pour exécuter des scripts, vous pouvez utiliser le YAML format. Pour consulter les tâches de configuration, les détails et les exemples relatifs à la EC2Launch version 2, consultezEC2Launchconfiguration des tâches v2.

Spécifiez un YAML script avec la `executeScript` tâche.

Exemple de YAML syntaxe pour exécuter un PowerShell script

```
version: 1.0
    tasks:
    - task: executeScript
      inputs:
      - frequency: always
        type: powershell
        runAs: localSystem
        content: |-
          $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
          New-Item $file -ItemType file
```

Exemple de YAML syntaxe pour exécuter un script batch

```
version: 1.1
    tasks:
    - task: executeScript
      inputs:
      - frequency: always
        type: batch
        runAs: localSystem
        content: |-
          echo Current date and time >> %SystemRoot%\Temp\test.log
          echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
```

Encodage Base64

Si vous utilisez Amazon EC2 API ou un outil qui n'effectue pas de codage base64 des données utilisateur, vous devez les encoder vous-même. Si ce n'est pas le cas, une erreur indiquant qu'aucune balise `script` ou `powershell` à exécuter n'a été trouvée est consignée. Voici un exemple d'encodage à l'aide de Windows PowerShell.

```
$UserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Voici un exemple de décodage à l'aide PowerShell de.

```
$Script =
 [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData))
```

Pour plus d'informations sur l'encodage base64, consultez https://www.ietf.org/rfc/rfc4648.txt.

Exécution de données utilisateur

Par défaut, l'exécution AMIs des données utilisateur est activée sur tous les systèmes AWS Windows lors du lancement initial. Vous pouvez spécifier que les scripts de données utilisateur doivent être exécutés au prochain réamorçage ou redémarrage de l'instance. Vous pouvez également spécifier que les scripts de données utilisateur doivent être exécutés chaque fois que l'instance est réamorcée ou redémarre.

> **Note**
>
> Les données utilisateur ne sont pas activées pour être exécutées par défaut après le lancement initial. Pour activer l'exécution des données utilisateur lorsque vous redémarrez ou démarrez l'instance, consultez Exécuter des scripts lors des redémarrages ou démarrages suivants.

Les scripts de données utilisateur sont exécutés depuis le compte de l'administrateur local quand un mot de passe aléatoire est généré. Sinon, les scripts de données utilisateur sont exécutés depuis le compte système.

Scripts de lancement d'instance

Les scripts figurant dans les données utilisateur d'instance sont exécutés lors du lancement initial de l'instance. Si la balise `persist` est trouvée, l'exécution des données utilisateur est activée pour les réamorçages ou démarrages suivants. Les fichiers journaux pour les EC2Launch versions 2 et 2 EC2Config contiennent le résultat de la sortie standard et des flux d'erreurs standard. EC2Launch

EC2Launch v2

Le fichier journal de la EC2Launch v2 est`C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

> **Note**
>
> Le dossier `C:\ProgramData` peut être masqué. Pour afficher le dossier, vous devez afficher les fichiers et les dossiers masqués.

Les informations suivantes sont enregistrées lorsque les données utilisateur sont exécutées :

- `Info: Converting user-data to yaml format`— Si les données utilisateur ont été fournies au XML format
- `Info: Initialize user-data state` – Début de l'exécution des données utilisateur
- `Info: Frequency is: always` – Si la tâche de données utilisateur est en cours d'exécution à chaque démarrage
- `Info: Frequency is: once` – Si la tâche de données utilisateur est exécutée une seule fois
- `Stage: postReadyUserData execution completed` – Fin de l'exécution des données utilisateur

EC2Launch

Le fichier journal de EC2Launch est `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\UserdataExecution.log`.

Le dossier `C:\ProgramData` peut être masqué. Pour afficher le dossier, vous devez afficher les fichiers et les dossiers masqués.

Les informations suivantes sont enregistrées lorsque les données utilisateur sont exécutées :

- `Userdata execution begins` – Début de l'exécution des données utilisateur
- `<persist> tag was provided: true` – Si l'identification persist est trouvée
- `Running userdata on every boot` – Si l'identification persist est trouvée
- `<powershell> tag was provided.. running powershell content` – Si la balise powershell est trouvée
- `<script> tag was provided.. running script content` – Si l'identification script est trouvée

- `Message: The output from user scripts` – Si des scripts de données utilisateur sont exécutés, leur sortie est journalisée

EC2Config

Le fichier journal de EC2Config est `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2Config.log`. Les informations suivantes sont enregistrées lorsque les données utilisateur sont exécutées :

- `Ec2HandleUserData: Message: Start running user scripts` – Début de l'exécution des données utilisateur
- `Ec2HandleUserData: Message: Re-enabled userdata execution` – Si l'identification persist est trouvée
- `Ec2HandleUserData: Message: Could not find <persist> and </persist>` – Si la balise persist n'est pas trouvée
- `Ec2HandleUserData: Message: The output from user scripts` – Si des scripts de données utilisateur sont exécutés, leur sortie est journalisée

Exécuter des scripts lors des redémarrages ou démarrages suivants

Lorsque vous mettez à jour des données utilisateur d'instance, les scripts de données utilisateur sont exécutés automatiquement lorsque vous redémarrez ou démarrez l'instance. Toutefois, vous pouvez activer l'exécution des données utilisateur pour que les scripts de données utilisateur soient exécutés une seule fois lorsque vous redémarrez ou démarrez l'instance ou chaque fois que vous redémarrez ou démarrez l'instance.

Si vous choisissez l'option Arrêter avec Sysprep, les scripts de données utilisateur sont exécutés quand l'instance est redémarrée ou démarrée, même si vous n'avez pas activé l'exécution des données utilisateur pour les redémarrages ou démarrages suivants. Les scripts de données utilisateur ne seront pas exécutés lors des redémarrages ou démarrages ultérieurs.

Pour activer l'exécution des données utilisateur avec la EC2Launch version 2

- Pour exécuter une tâche dans les données utilisateur au premier démarrage, définissez `frequency` sur `once`.
- Pour exécuter une tâche dans les données utilisateur à chaque démarrage, définissez `frequency` sur `always`.

Pour activer l'exécution des données utilisateur avec EC2Launch

1. Connectez-vous à votre instance Windows.
2. Ouvrez une fenêtre de PowerShell commande et exécutez la commande suivante :

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
```

3. Déconnectez-vous de votre instance Windows. Pour exécuter les scripts mis à jour au démarrage suivant de l'instance, arrêtez l'instance et mettez à jour les données utilisateur.

Pour activer l'exécution des données utilisateur avec EC2Config

1. Connectez-vous à votre instance Windows.
2. Ouvrir `C:\Program Files\Amazon\Ec2ConfigService\Ec2ConfigServiceSetting.exe`.
3. Pour les données utilisateur, sélectionnez Activer UserData l'exécution pour le prochain démarrage du service.
4. Déconnectez-vous de votre instance Windows. Pour exécuter les scripts mis à jour au démarrage suivant de l'instance, arrêtez l'instance et mettez à jour les données utilisateur.

Les données utilisateur et les outils pour Windows PowerShell

Vous pouvez utiliser les Outils pour Windows PowerShell pour spécifier, modifier et afficher les données utilisateur de votre instance. Pour plus d'informations sur l'affichage des données utilisateur de votre instance à l'aide des métadonnées d'instance, consultez Accéder aux métadonnées d'une EC2 instance. Pour plus d'informations sur les données utilisateur et le AWS CLI, voirLes données de l'utilisateur et le AWS CLI.

Exemple : Spécification des données utilisateur d'instance au moment du lancement

Créez un fichier texte avec les données utilisateur d'instance. Pour exécuter des scripts de données utilisateur chaque fois que vous redémarrez ou démarrez l'instance, ajoutez `<persist>true</persist>`, comme illustré dans l'exemple suivant.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
```

```
<persist>true</persist>
```

Pour spécifier les données utilisateur de l'instance lorsque vous lancez votre instance, utilisez la New-EC2Instancecommande. Cette commande n'effectue pas l'encodage base64 des données utilisateur pour vous. Utilisez les commandes suivantes pour encoder les données utilisateur dans un fichier texte nommé `script.txt`.

```
PS C:\> $Script = Get-Content -Raw script.txt
PS C:\> $UserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Utilisez le paramètre `-UserData` pour transmettre les données utilisateur à la commande New-EC2Instance.

```
PS C:\> New-EC2Instance -ImageId ami-abcd1234 -MinCount 1 -MaxCount 1 -
InstanceType m3.medium \
    -KeyName my-key-pair -SubnetId subnet-12345678 -SecurityGroupIds sg-1a2b3c4d \
    -UserData $UserData
```

Exemple : Mise à jour des données utilisateur d'instance pour une instance arrêtée

Vous pouvez modifier les données utilisateur d'une instance arrêtée à l'aide de la Edit-EC2InstanceAttributecommande.

Créez un fichier texte contenant le nouveau script. Utilisez les commandes suivantes pour encoder les données utilisateur dans le fichier texte nommé `new-script.txt`.

```
PS C:\> $NewScript = Get-Content -Raw new-script.txt
PS C:\> $NewUserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($NewScript))
```

Utilisez les paramètres `-UserData` et `-Value` pour spécifier les données utilisateur.

```
PS C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute userData -
Value $NewUserData
```

Exemple : Affichage des données utilisateur d'instance

Pour récupérer les données utilisateur d'une instance, utilisez la Get-EC2InstanceAttributecommande.

```
PS C:\> (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute
 userData).UserData
```

Voici un exemple de sortie. Notez que les données utilisateur sont encodées.

```
PHBvd2Vyc2hlbGw
+DQpSZW5hbWUtQ29tcHV0ZXIgLU5ld05hbWUgdXNlci1kYXRhLXRlc3QNCjwvcG93ZXJzaGVsbD4=
```

Utilisez les commandes suivantes pour stocker les données utilisateur encodées dans une variable, puis les décoder.

```
PS C:\> $UserData_encoded = (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -
Attribute userData).UserData
PS C:
\> [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData_encoded)
```

Voici un exemple de sortie.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Exemple : Attribution d'un nouveau nom à l'instance pour correspondre à la valeur de la balise

Vous pouvez utiliser la Get-EC2Tagcommande pour lire la valeur de la balise, renommer l'instance au premier démarrage pour qu'elle corresponde à la valeur de la balise, puis redémarrer. Pour exécuter correctement cette commande, vous devez disposer d'un rôle doté d'`ec2:DescribeTags`autorisations associées à l'instance, car les informations de balise sont récupérées par l'APIappel. Pour plus d'informations sur les paramètres des autorisations à l'aide de IAM rôles, consultezAttacher un IAM rôle à une instance.

IMDSv2

```
<powershell>
    [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri 'http://169.254.169.254/latest/api/token' -
UseBasicParsing
```

```
    $instanceId = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" =
 $token} -Method GET -Uri 'http://169.254.169.254/latest/meta-data/instance-id' -
UseBasicParsing
 $nameValue = (Get-EC2Tag -Filter @{Name="resource-id";Value=
$instanceid},@{Name="key";Value="Name"}).Value
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

IMDSv1

```
<powershell>
 $instanceId = (Invoke-WebRequest http://169.254.169.254/latest/meta-data/instance-
id -UseBasicParsing).content
 $nameValue = (Get-EC2Tag -Filter @{Name="resource-id";Value=
$instanceid},@{Name="key";Value="Name"}).Value
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

Vous pouvez également renommer l'instance à l'aide d'identifications dans les métadonnées d'instance si votre instance est configurée pour accéder aux identifications à partir des métadonnées d'instance. Pour de plus amples informations, veuillez consulter Afficher les balises de vos EC2 instances à l'aide des métadonnées de l'instance.

IMDSv2

```
<powershell>
    [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri 'http://169.254.169.254/latest/api/token' -
UseBasicParsing
 $nameValue = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token}
 -Method GET -Uri 'http://169.254.169.254/latest/meta-data/tags/instance/Name' -
UseBasicParsing
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

IMDSv1

```
<powershell>
 $nameValue = Get-EC2InstanceMetadata -Path /tags/instance/Name
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

Identifiez chaque instance lancée en une seule demande

Cet exemple montre comment vous pouvez utiliser à la fois les données utilisateur et les métadonnées des instances pour configurer vos EC2 instances Amazon.

> **Note**
>
> Les exemples de cette section utilisent l'IPv4adresse du IMDS :`169.254.169.254`. Si vous récupérez des métadonnées d'instance pour EC2 des instances via l'IPv6adresse, assurez-vous d'activer et d'utiliser plutôt l'IPv6adresse :`[fd00:ec2::254]`. L'IPv6adresse du IMDS est compatible avec IMDSv2 les commandes. L'IPv6adresse n'est accessible que sur les instances créées sur le système AWS Nitro et dans un sous-réseau IPv6 compatible (double pile ou IPv6 uniquement).

Alice souhaite lancer quatre instances de sa base de données préféréeAMI, la première faisant office d'instance d'origine et les trois autres de répliques. Lorsqu'elle les lance, elle souhaite ajouter des données utilisateur portant sur la stratégie de réplication pour chaque réplica. Elle sait que ces données seront disponibles pour les quatre instances. Elle a donc besoin de structurer les données utilisateur de sorte que chaque instance reconnaisse quelles parties la concernent. Pour ce faire, elle peut utiliser la valeur de métadonnées d'instance `ami-launch-index` qui sera unique pour chaque instance. Si elle démarre plus d'une instance à la fois, la valeur `ami-launch-index` indique l'ordre dans lequel les instances ont été lancées. La valeur de la première instance lancée est `0`.

Voici les données utilisateur construites par Alice.

```
replicate-every=1min | replicate-every=5min | replicate-every=10min
```

La donnée `replicate-every=1min` définit la configuration du premier réplica, `replicate-every=5min` définit la configuration du deuxième réplica, et ainsi de suite. Alice décide de fournir ces données sous forme de ASCII chaîne avec un symbole en forme de tube (`|`) délimitant les données pour les différentes instances.

Alice lance quatre instances à l'aide de la commande run-instances, en spécifiant les données utilisateur.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
```

```
    --count 4 \
    --instance-type t2.micro \
    --user-data "replicate-every=1min | replicate-every=5min | replicate-every=10min"
```

Après leur lancement, toutes les instances ont une copie des données utilisateur et des métadonnées communes présentées ici :

- AMIIdentifiant : ami-0abcdef1234567890
- ID de réservation : r-1234567890abcabc0
- Clés publiques : aucune
- Nom du groupe de sécurité : par défaut
- Type d'instance : t2.micro

Cependant, chaque instance possède des métadonnées uniques, comme indiqué dans les tableaux suivants.

Metadonnées	Valeur
instance-id	i-1234567890abcdef0
ami-launch-index	0
public-hostname	ec2-203-0-113-25.compute-1.amazonaws.com
public-ipv4	67.202.51.223
local-hostname	ip-10-251-50-12.ec2.internal
local-ipv4	10.251.50.35

Metadonnées	Valeur
instance-id	i-0598c7d356eba48d7
ami-launch-index	1
public-hostname	ec2-67-202-51-224.compute-1.amazonaws.com

Metadonnées	Valeur
public-ipv4	67.202.51.224
local-hostname	ip-10-251-50-36.ec2.internal
local-ipv4	10.251.50.36

Metadonnées	Valeur
instance-id	i-0ee992212549ce0e7
ami-launch-index	2
public-hostname	ec2-67-202-51-225.compute-1.amazonaws.com
public-ipv4	67.202.51.225
local-hostname	ip-10-251-50-37.ec2.internal
local-ipv4	10.251.50.37

Metadonnées	Valeur
instance-id	i-1234567890abcdef0
ami-launch-index	3
public-hostname	ec2-67-202-51-226.compute-1.amazonaws.com
public-ipv4	67.202.51.226
local-hostname	ip-10-251-50-38.ec2.internal
local-ipv4	10.251.50.38

Alice peut utiliser la valeur `ami-launch-index` pour déterminer quelle portion des données utilisateur est applicable à une instance particulière.

1. Elle se connecte à l'une des instances et récupère `ami-launch-index` pour cette instance afin de s'assurer qu'il s'agit de l'un des réplicas :

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/meta-data/api/
   token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
   data/ami-launch-index
   2
   ```

   Pour les étapes suivantes, les IMDSv2 demandes utilisent le jeton stocké dans la IMDSv2 commande précédente, en supposant que le jeton n'a pas expiré.

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-launch-index
   2
   ```

2. Elle enregistre les données `ami-launch-index` sous forme de variable.

   IMDSv2

   ```
   [ec2-user ~]$ ami_launch_index=`curl -H "X-aws-ec2-metadata-token: $TOKEN"
    http://169.254.169.254/latest/meta-data/ami-launch-index`
   ```

   IMDSv1

   ```
   [ec2-user ~]$ ami_launch_index=`curl http://169.254.169.254/latest/meta-data/ami-
   launch-index`
   ```

3. Elle enregistre les données utilisateur sous forme de variable.

   IMDSv2

   ```
   [ec2-user ~]$ user_data=`curl -H "X-aws-ec2-metadata-token: $TOKEN"
    http://169.254.169.254/latest/user-data`
   ```

IMDSv1

```
[ec2-user ~]$ user_data=`curl http://169.254.169.254/latest/user-data`
```

4. Enfin, Alice utilise la commande cut pour extraire la portion de données utilisateur applicable à cette instance.

   IMDSv2

   ```
   [ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
   replicate-every=5min
   ```

   IMDSv1

   ```
   [ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
   replicate-every=5min
   ```

Détecter si un hôte est une EC2 instance

Vous devrez peut-être savoir si votre application ou votre site Web s'exécute sur une EC2 instance, en particulier si vous disposez d'un environnement informatique mixte. Vous pouvez utiliser l'une des options suivantes pour déterminer si l'hôte de votre application ou de votre site Web est une EC2 instance.

Options

- Inspecter le Documents d'identité d'instance
- Inspectez le système UUID
- Inspecter l'identificateur de génération de machine virtuelle du système

Inspecter le Documents d'identité d'instance

Chaque instance possède un document d'identité d'instance signé que vous pouvez vérifier de manière cryptographique. Vous pouvez trouver ces documents à l'aide du service de métadonnées d'instance (IMDS).

Pour de plus amples informations, veuillez consulter Documents d'identité d'instance.

Inspectez le système UUID

Vous pouvez obtenir le système UUID et regarder dans le premier octet du UUID for EC2 (sous Linux, cela peut être en minusculesec2). Cette méthode est rapide, mais potentiellement imprécise, car il est peu probable qu'un système qui n'est pas une EC2 instance UUID ait un nom commençant par ces caractères. De plus, certaines versions de SMBIOS utilisent le format little-endian, qui n'est pas inclus EC2 au début du. UUID Cela peut être le cas pour les EC2 instances qui utilisent la version SMBIOS 2.4 pour Windows ou pour les distributions Linux autres qu'Amazon Linux qui ont leur propre implémentation deSMBIOS.

Exemple Linux : obtenir le UUID depuis DMI (HVMAMIsuniquement)

Utilisez la commande suivante pour obtenir l'UUIDutilisation de l'interface de gestion de bureau (DMI) :

```
[ec2-user ~]$ sudo dmidecode --string system-uuid
```

Dans l'exemple de sortie suivant, le UUID message commence par EC2 « », ce qui indique que le système est probablement une EC2 instance.

```
EC2E1916-9099-7CAF-FD21-012345ABCDEF
```

Dans l'exemple de sortie suivant, le UUID est représenté au format little-endian.

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Sinon, pour les instances construites sur le système Nitro, vous pouvez utiliser la commande suivante :

```
[ec2-user ~]$ cat /sys/devices/virtual/dmi/id/board_asset_tag
```

Si le résultat est un ID d'instance, comme dans l'exemple de sortie suivant, le système est une EC2 instance :

```
i-0af01c0123456789a
```

Exemple Linux : obtenir le UUID depuis l'hyperviseur (PV AMIs uniquement)

Utilisez la commande suivante pour obtenir le UUID depuis l'hyperviseur :

```
[ec2-user ~]$ cat /sys/hypervisor/uuid
```

Dans l'exemple de sortie suivant, le fichier UUID commence par « ec2 », ce qui indique que le système est probablement une EC2 instance.

```
ec2e1916-9099-7caf-fd21-012345abcdef
```

Exemple Windows : Get the UUID using WMI ou Windows PowerShell

Utilisez la ligne de commande Windows Management Instrumentation (WMIC) comme suit :

```
wmic path win32_computersystemproduct get uuid
```

Si vous utilisez Windows PowerShell, vous pouvez également utiliser l'Get-WmiObjectapplet de commande comme suit :

```
PS C:\> Get-WmiObject -query "select uuid from Win32_ComputerSystemProduct" | Select
 UUID
```

Dans l'exemple de sortie suivant, le UUID message commence par EC2 « », ce qui indique que le système est probablement une EC2 instance.

```
EC2AE145-D1DC-13B2-94ED-012345ABCDEF
```

Dans les cas utilisant la SMBIOS version 2.4, UUID ils peuvent être représentés au format little-endian ; par exemple :

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Inspecter l'identificateur de génération de machine virtuelle du système

Un identificateur de génération de machine virtuelle consiste en un tampon unique de 128 bits interprété comme un entier unique aléatoire cryptographique. Vous pouvez récupérer l'identificateur de génération de machine virtuelle pour identifier votre instance Amazon Elastic Compute Cloud. L'identifiant de génération est exposé dans le système d'exploitation invité de l'instance par le biais d'une entrée de ACPI table. La valeur change si votre machine est clonée, copiée ou importée dans AWS, par exemple avec VM Import/Export.

Exemple : récupérer l'identifiant de génération de machine virtuelle depuis Linux

Vous pouvez utiliser les commandes suivantes pour récupérer l'identifiant de génération de machine virtuelle à partir de vos instances exécutant Linux.

Amazon Linux 2

1. Mettez à jour vos packages logiciels existants, le cas échéant, à l'aide de la commande suivante :

   ```
   sudo yum update
   ```

2. Si nécessaire, créez le package busybox à l'aide de la commande suivante :

   ```
   sudo curl https://www.rpmfind.net/linux/epel/next/8/Everything/x86_64/Packages/
   b/busybox-1.35.0-2.el8.next.x86_64.rpm --output busybox.rpm
   ```

3. Si nécessaire, installez les packages préalables à l'aide de la commande suivante :

   ```
   sudo yum install busybox.rpm iasl -y
   ```

4. Exécutez la `iasl` commande suivante pour générer une sortie à partir de la ACPI table :

   ```
   sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
   ```

5. Exécutez la commande suivante pour vérifier la sortie de la commande `iasl` :

   ```
   cat SSDT2.dsl
   ```

   La sortie doit fournir l'espace d'adressage requis pour récupérer l'identificateur de génération de machine virtuelle :

   ```
   Intel ACPI Component Architecture
   ASL+ Optimizing Compiler/Disassembler version 20190509
   Copyright (c) 2000 - 2019 Intel Corporation

   File appears to be binary: found 32 non-ASCII characters, disassembling
   Binary file appears to be a valid ACPI table, disassembling
   Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
   ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
    00000001)
   ```

```
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
*
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*     Signature        "SSDT"
*     Length           0x0000007B (123)
*     Revision         0x01
*     Checksum         0xB8
*     OEM ID           "AMAZON"
*     OEM Table ID     "AMZNSSDT"
*     OEM Revision     0x00000001 (1)
*     Compiler ID      "AMZN"
*     Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
Scope (\_SB)
{
    Device (VMGN)
    {
        Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
        Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
        Name (_HID, "AMZN0000")  // _HID: Hardware ID
        Name (ADDR, Package (0x02)
        {
            0xFED01000,
            Zero
        })
    }
}
```

```
}
```

6. (Facultatif) Augmentez les autorisations de votre terminal pour les étapes restantes à l'aide de la commande suivante :

```
sudo -s
```

7. Utilisez la commande suivante pour stocker l'espace d'adressage précédemment collecté :

```
VMGN_ADDR=0xFED01000
```

8. Utilisez la commande suivante pour parcourir l'espace d'adressage et créer l'identificateur de génération de machine virtuelle :

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

9. Récupérez l'identificateur de génération de machine virtuelle à partir du fichier de sortie à l'aide de la commande suivante :

```
cat vmgenid ; echo
```

Votre sortie doit ressembler à ce qui suit :

```
EC2F335D979132C4165896753E72BD1C
```

Ubuntu

1. Mettez à jour vos packages logiciels existants, le cas échéant, à l'aide de la commande suivante :

```
sudo apt update
```

2. Si nécessaire, installez les packages préalables à l'aide de la commande suivante :

```
sudo apt install busybox iasl -y
```

3. Exécutez la `iasl` commande suivante pour générer une sortie à partir de la ACPI table :

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

4. Exécutez la commande suivante pour vérifier la sortie de la commande `iasl` :

```
cat SSDT2.dsl
```

La sortie doit fournir l'espace d'adressage requis pour récupérer l'identificateur de génération de machine virtuelle :

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
*
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*     Signature        "SSDT"
*     Length           0x0000007B (123)
*     Revision         0x01
*     Checksum         0xB8
*     OEM ID           "AMAZON"
```

```
*     OEM Table ID     "AMZNSSDT"
*     OEM Revision     0x00000001 (1)
*     Compiler ID      "AMZN"
*     Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
Scope (\_SB)
{
    Device (VMGN)
    {
        Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
        Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
        Name (_HID, "AMZN0000")  // _HID: Hardware ID
        Name (ADDR, Package (0x02)
        {
            0xFED01000,
            Zero
        })
    }
}
}
```

5. (Facultatif) Augmentez les autorisations de votre terminal pour les étapes restantes à l'aide de la commande suivante :

```
sudo -s
```

6. Utilisez les commandes suivantes pour stocker l'espace d'adressage précédemment collecté :

```
VMGN_ADDR=0xFED01000
```

7. Utilisez la commande suivante pour parcourir l'espace d'adressage et créer l'identificateur de génération de machine virtuelle :

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

8. Récupérez l'identificateur de génération de machine virtuelle à partir du fichier de sortie à l'aide de la commande suivante :

```
cat vmgenid ; echo
```

Votre sortie doit ressembler à ce qui suit :

```
EC2F335D979132C4165896753E72BD1C
```

Exemple : récupérer l'identifiant de génération de machine virtuelle depuis Windows

Vous pouvez créer un exemple d'application pour récupérer l'identificateur de génération de machine virtuelle à partir de vos instances exécutant Windows. Pour plus d'informations, consultez Obtention de l'identificateur de génération de l'ordinateur virtuel dans la documentation Microsoft.

Documents d'identité d'instance pour les EC2 instances Amazon

Chaque instance que vous lancez a un Documents d'identité d'instance qui fournit des informations sur l'instance elle-même. Vous pouvez utiliser le Documents d'identité d'instance pour valider les attributs de l'instance.

Le document d'identité d'instance est généré lorsque l'instance est arrêtée et démarrée, redémarrée ou lancée. Vous pouvez accéder au document d'identité d'une instance via le service de métadonnées d'instance (IMDS). Pour obtenir des instructions, consultez Récupérez le document d'identité de l'instance.

Le document d'identité de l'instance utilise le JSON format texte brut. Il contient les informations suivantes.

non structurées	Description
`accountId`	L'ID du AWS compte qui a lancé l'instance.
`architecture`	Architecture AMI utilisée pour lancer l'instance (i386 | x86_64 | arm64).
`availabilityZone`	Zone de disponibilité dans laquelle l'instance est en cours d'exécution.
`billingProducts`	Produits de facturation de l'instance.

non structurées	Description
`devpayProductCodes`	Obsolète.
`imageId`	L'ID AMI utilisé pour lancer l'instance.
`instanceId`	ID de l'instance.
`instanceType`	Type de l'instance.
`kernelId`	ID du noyau associé à l'instance, le cas échéant.
`marketplaceProductCodes`	Le code AWS Marketplace produit AMI utilisé pour lancer l'instance.
`pendingTime`	Date et heure auxquelles l'instance a été lancée.
`privateIp`	IPv4Adresse privée de l'instance.
`ramdiskId`	ID du RAM disque associé à l'instance, le cas échéant.
`region`	Région dans laquelle l'instance est en cours d'exécution.
`version`	La version du format du Documents d'identité d'instance

Récupérez le document d'identité d'instance pour une EC2 instance Amazon

Le document d'identité d'instance pour une EC2 instance Amazon utilise un JSON format de texte brut. Pour une description du contenu d'un document d'identité d'instance, consultezthe section called "Documents d'identité d'instance".

les documents d'identité de l'instance sont stockés dans les métadonnées de l'instance, dans la catégorie des données `instance-identity/document` dynamiques. Vous accédez au document d'identité d'une instance en vous connectant à l'instance et en le récupérant à partir des métadonnées de l'instance.

Vous pouvez accéder aux métadonnées de l'instance à l'aide de l'IPv4adresse 169.254.169.254 ou de l'IPv6adressefd00:ec2::254. Il s'agit d'adresses locales de liens, ce qui signifie que vous ne pouvez y accéder qu'à partir de l'instance. Pour de plus amples informations, veuillez consulter Adresses lien-local. Les exemples de cette page utilisent l'IPv4adresse du IMDS :169.254.169.254. Pour récupérer les métadonnées d'instance pour EC2 les IPv6 instances, utilisez fd00:ec2::254 instead.

Pour vérifier l'authenticité du document d'identité d'une instance après l'avoir récupéré. Pour de plus amples informations, veuillez consulter Vérifier le document d'identité de l'instance.

Pour récupérer le document d'identité de l'instance

Connectez-vous à l'instance et exécutez la commande suivante pour accéder au document d'identité de l'instance à partir des métadonnées de l'instance.

cURL

IMDSv2

```
$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/
instance-identity/document
```

IMDSv1

```
$ curl http://169.254.169.254/latest/dynamic/instance-identity/document
```

PowerShell

IMDSv2

```
PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
token).Content
```

```
PS C:\> (Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $Token}
 http://169.254.169.254/latest/dynamic/instance-identity/document).Content
```

IMDSv1

```
PS C:\> (Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/
document).Content
```

Voici un exemple de sortie.

```
{
    "devpayProductCodes" : null,
    "marketplaceProductCodes" : [ "1abc2defghijklm3nopqrs4tu" ],
    "availabilityZone" : "us-west-2b",
    "privateIp" : "10.158.112.84",
    "version" : "2017-09-30",
    "instanceId" : "i-1234567890abcdef0",
    "billingProducts" : null,
    "instanceType" : "t2.micro",
    "accountId" : "123456789012",
    "imageId" : "ami-5fb8c835",
    "pendingTime" : "2016-11-19T16:32:11Z",
    "architecture" : "x86_64",
    "kernelId" : null,
    "ramdiskId" : null,
    "region" : "us-west-2"
}
```

Vérifier le document d'identité de l'instance pour une EC2 instance Amazon

Si vous avez l'intention d'utiliser le contenu du Documents d'identité d'instance à des fins importantes, vous devez vérifier son contenu et son authenticité avant de l'utiliser.

Le Documents d'identité d'instance en texte brut est accompagné de trois signatures hachées et chiffrées. Vous pouvez utiliser ces signatures pour vérifier l'origine et l'authenticité du Documents d'identité d'instance et les informations qu'il contient. Les signatures suivantes sont fournies :

- Signature codée en base64 : il s'agit d'un SHA256 hachage codé en base64 du document d'identité de l'instance chiffré à l'aide d'une paire de clés. RSA
- PKCS7Signature : il s'agit d'un SHA1 hachage du document d'identité de l'instance chiffré à l'aide d'une paire de clés. DSA
- RSASignature -2048 : il s'agit d'un SHA256 hachage du document d'identité de l'instance chiffré à l'aide d'une paire de clés -2048. RSA

Chaque signature est disponible à un point de terminaison différent dans les métadonnées de l'instance. Vous pouvez utiliser l'une de ces signatures en fonction de vos exigences de hachage et de chiffrement. Pour vérifier les signatures, vous devez utiliser le certificat AWS public correspondant.

Options

- Option 1 : vérifier le document d'identité de l'instance à l'aide de la PKCS7 signature
- Option 2 : vérifier le document d'identité de l'instance à l'aide de la signature codée en base64
- Option 3 : vérifier le document d'identité de l'instance à l'aide de la signature RSA -2048

Option 1 : vérifier le document d'identité de l'instance à l'aide de la PKCS7 signature

Cette rubrique explique comment vérifier le document d'identité de l'instance à l'aide de la PKCS7 signature et du certificat AWS DSA public.

Instances Linux

Pour vérifier le document d'identité de l'instance à l'aide de la PKCS7 signature et du certificat AWS DSA public

1. Connectez-vous à l'instance.
2. Récupérez la PKCS7 signature à partir des métadonnées de l'instance et ajoutez-la à un nouveau fichier nommé `pkcs7` avec l'en-tête et le pied de page requis. Utilisez l'une des commandes suivantes en fonction de la IMDS version utilisée par l'instance.

   IMDSv2

   ```
   $ echo "-----BEGIN PKCS7-----" >> pkcs7 \
    && TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/pkcs7 >> pkcs7 \
    && echo "" >> pkcs7 \
    && echo "-----END PKCS7-----" >> pkcs7
   ```

   IMDSv1

   ```
   $ echo "-----BEGIN PKCS7-----" >> pkcs7 \
    && curl -s http://169.254.169.254/latest/dynamic/instance-identity/pkcs7
    >> pkcs7 \
   ```

```
&& echo "" >> pkcs7 \
&& echo "-----END PKCS7-----" >> pkcs7
```

3. Trouvez le certificat DSApublic de votre région dans AWS des certificats publics, par exemple des signatures de documents d'identité et ajoutez-en le contenu dans un nouveau fichier nommé`certificate`.
4. Utilisez la commande Open SSL smime pour vérifier la signature. Incluez l'option `-verify` indiquant que la signature doit être vérifiée et l'option `-noverify` indiquant que le certificat n'a pas besoin d'être vérifié.

   ```
   $ openssl smime -verify -in pkcs7 -inform PEM -certfile certificate -noverify | tee
    document
   ```

   Si la signature est valide, le message `Verification successful` s'affiche.

   La commande écrit également le contenu du document d'identité d'instance dans un nouveau fichier nommé `document`. Vous pouvez comparer le contenu du document d'identité d'instance provenant des métadonnées d'instance avec le contenu de ce fichier à l'aide des commandes suivantes.

   ```
   $ openssl dgst -sha256 < document
   ```

   ```
   $ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/document | openssl dgst -sha256
   ```

   Si la signature ne peut pas être vérifiée, contactez AWS Support.

instances Windows

Prérequis

Cette procédure nécessite le `System.Security` Microsoft. NETClasse de base. Pour ajouter la classe à votre PowerShell session, exécutez la commande suivante.

```
PS C:\> Add-Type -AssemblyName System.Security
```

> **Note**
>
> La commande ajoute la classe à la PowerShell session en cours uniquement. Si vous démarrez une nouvelle séance, vous devez exécuter à nouveau la commande.

Pour vérifier le document d'identité de l'instance à l'aide de la PKCS7 signature et du certificat AWS DSA public

1. Connectez-vous à l'instance.
2. Récupérez la PKCS7 signature à partir des métadonnées de l'instance, convertissez-la en tableau d'octets et ajoutez-la à une variable nommée`$Signature`. Utilisez l'une des commandes suivantes en fonction de la IMDS version utilisée par l'instance.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
   ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/pkcs7).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/pkcs7).Content)
   ```

3. Récupérez le document d'identité d'instance en texte brut à partir des métadonnées d'instance, convertissez-le en un tableau d'octets et ajoutez-le à une variable nommée `$Document`. Utilisez l'une des commandes suivantes en fonction de la IMDS version utilisée par l'instance.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/document).Content)
   ```

IMDSv1

```
PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

4. Trouvez le certificat DSApublic de votre région dans AWS des certificats publics, par exemple des signatures de documents d'identité et ajoutez-en le contenu dans un nouveau fichier nommé`certificate.pem`.
5. Extrayez le certificat du fichier de certificat et stockez-le dans une variable nommée `$Store`.

```
PS C:\> $Store =
 [Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog
Path certificate.pem)))
```

6. Vérifiez la signature.

```
PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
```

```
PS C:\> $SignatureDocument.Decode($Signature)
```

```
PS C:\> $SignatureDocument.CheckSignature($Store, $true)
```

Si la signature est valide, la commande ne renvoie aucune sortie. Si la signature ne peut pas être vérifiée, la commande renvoie `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer`. Si votre signature ne peut pas être vérifiée, contactez AWS Support.

7. Validez le contenu du document d'identité d'instance.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

Si le contenu du document d'identité d'instance est valide, la commande renvoie `True`. Si le document d'identité de l'instance ne peut pas être validé, contactez AWS Support.

Option 2 : vérifier le document d'identité de l'instance à l'aide de la signature codée en base64

Cette rubrique explique comment vérifier le document d'identité de l'instance à l'aide de la signature codée en base64 et du certificat AWS RSA public.

Instances Linux

Pour valider le document d'identité de l'instance à l'aide de la signature codée en base64 et du certificat public AWS RSA

1. Connectez-vous à l'instance.
2. Récupérez la signature codée en base64 à partir des métadonnées d'instance, convertissez-la en binaire et ajoutez-la à un fichier nommé `signature`. Utilisez l'une des commandes suivantes en fonction de la IMDS version utilisée par l'instance.

   IMDSv2

   ```
   $ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/signature | base64 -d >> signature
   ```

   IMDSv1

   ```
   $ curl -s http://169.254.169.254/latest/dynamic/instance-identity/signature | base64 -d >> signature
   ```

3. Récupérez le Documents d'identité d'instance en texte brut à partir des métadonnées de l'instance et ajoutez-le à un fichier nommé `document`. Utilisez l'une des commandes suivantes en fonction de la IMDS version utilisée par l'instance.

   IMDSv2

   ```
   $ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/document >> document
   ```

IMDSv1

```
$ curl -s http://169.254.169.254/latest/dynamic/instance-identity/document
 >> document
```

4. Trouvez le certificat RSApublic de votre région dans AWS des certificats publics, par exemple des signatures de documents d'identité et ajoutez-en le contenu dans un nouveau fichier nommé`certificate`.
5. Extrayez la clé publique du certificat AWS RSA public et enregistrez-la dans un fichier nommé`key`.

```
$ openssl x509 -pubkey -noout -in certificate >> key
```

6. Utilisez la commande Open SSL dgst pour vérifier le document d'identité de l'instance.

```
$ openssl dgst -sha256 -verify key -signature signature document
```

Si la signature est valide, le message `Verification successful` s'affiche.

La commande écrit également le contenu du document d'identité d'instance dans un nouveau fichier nommé `document`. Vous pouvez comparer le contenu du document d'identité d'instance provenant des métadonnées d'instance avec le contenu de ce fichier à l'aide des commandes suivantes.

```
$ openssl dgst -sha256 < document
```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/document | openssl dgst -sha256
```

Si la signature ne peut pas être vérifiée, contactez AWS Support.

instances Windows

Pour valider le document d'identité de l'instance à l'aide de la signature codée en base64 et du certificat public AWS RSA

1. Connectez-vous à l'instance.

2. Récupérez la signature codée en base64 à partir des métadonnées d'instance, convertissez-la en un tableau d'octets et ajoutez-la à la variable nommée `$Signature`. Utilisez l'une des commandes suivantes en fonction de la IMDS version utilisée par l'instance.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
   ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/signature).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/signature).Content)
   ```

3. Récupérez le document d'identité d'instance en texte brut à partir des métadonnées d'instance, convertissez-le en un tableau d'octets et ajoutez-le à une variable nommée `$Document`. Utilisez l'une des commandes suivantes en fonction de la IMDS version utilisée par l'instance.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/document).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
   ```

4. Trouvez le certificat RSApublic de votre région dans AWS des certificats publics, par exemple des signatures de documents d'identité et ajoutez-en le contenu dans un nouveau fichier nommé`certificate.pem`.

5. Vérifier le document d'identité d'instance

```
PS C:\> [Security.Cryptography.X509Certificates.X509Certificate2]::new((Resolve-
Path certificate.pem)).PublicKey.Key.VerifyData($Document, 'SHA256', $Signature)
```

Si la signature est valide, la commande renvoie `True`. Si la signature ne peut pas être vérifiée, contactez AWS Support.

Option 3 : vérifier le document d'identité de l'instance à l'aide de la signature RSA -2048

Cette rubrique explique comment vérifier le document d'identité de l'instance à l'aide de la signature RSA -2048 et du certificat public AWS RSA -2048.

Instances Linux

Pour vérifier le document d'identité de l'instance à l'aide de la signature RSA -2048 et du certificat public AWS RSA -2048

1. Connectez-vous à l'instance.
2. Récupérez la signature RSA -2048 à partir des métadonnées de l'instance et ajoutez-la à un fichier nommé le `rsa2048` long de l'en-tête et du pied de page requis. Utilisez l'une des commandes suivantes en fonction de la IMDS version utilisée par l'instance.

   IMDSv2

   ```
   $ echo "-----BEGIN PKCS7-----" >> rsa2048 \
    && TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/rsa2048 >> rsa2048 \
    && echo "" >> rsa2048 \
    && echo "-----END PKCS7-----" >> rsa2048
   ```

   IMDSv1

   ```
   $ echo "-----BEGIN PKCS7-----" >> rsa2048 \
    && curl -s http://169.254.169.254/latest/dynamic/instance-identity/rsa2048
    >> rsa2048 \
    && echo "" >> rsa2048 \
   ```

```
 && echo "-----END PKCS7-----" >> rsa2048
```

3. Recherchez le certificat public RSA-2048 pour votre région AWS des certificats publics, par exemple des signatures de documents d'identité et ajoutez-en le contenu dans un nouveau fichier nommé. `certificate`
4. Utilisez la commande Open SSL smime pour vérifier la signature. Incluez l'option `-verify` indiquant que la signature doit être vérifiée et l'option `-noverify` indiquant que le certificat n'a pas besoin d'être vérifié.

   ```
   $ openssl smime -verify -in rsa2048 -inform PEM -certfile certificate -noverify |
    tee document
   ```

   Si la signature est valide, le message `Verification successful` s'affiche. Si la signature ne peut pas être vérifiée, contactez AWS Support.

instances Windows

Prérequis

Cette procédure nécessite le `System.Security` Microsoft. NETClasse de base. Pour ajouter la classe à votre PowerShell session, exécutez la commande suivante.

```
PS C:\> Add-Type -AssemblyName System.Security
```

> **Note**
>
> La commande ajoute la classe à la PowerShell session en cours uniquement. Si vous démarrez une nouvelle séance, vous devez exécuter à nouveau la commande.

Pour vérifier le document d'identité de l'instance à l'aide de la signature RSA -2048 et du certificat public AWS RSA -2048

1. Connectez-vous à l'instance.
2. Récupérez la signature RSA -2048 à partir des métadonnées de l'instance, convertissez-la en tableau d'octets et ajoutez-la à une variable nommée. `$Signature` Utilisez l'une des commandes suivantes en fonction de la IMDS version utilisée par l'instance.

IMDSv2

```
PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
token).Content
```

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
 @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
instance-identity/rsa2048).Content)
```

IMDSv1

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/rsa2048).Content)
```

3. Récupérez le document d'identité d'instance en texte brut à partir des métadonnées d'instance, convertissez-le en un tableau d'octets et ajoutez-le à une variable nommée `$Document`. Utilisez l'une des commandes suivantes en fonction de la IMDS version utilisée par l'instance.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/document).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
   ```

4. Recherchez le certificat public RSA-2048 pour votre région AWS des certificats publics, par exemple des signatures de documents d'identité et ajoutez-en le contenu dans un nouveau fichier nommé. `certificate.pem`

5. Extrayez le certificat du fichier de certificat et stockez-le dans une variable nommée `$Store`.

   ```
   PS C:\> $Store =
    [Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog
   Path certificate.pem)))
   ```

6. Vérifiez la signature.

```
PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
```

```
PS C:\> $SignatureDocument.Decode($Signature)
```

```
PS C:\> $SignatureDocument.CheckSignature($Store, $true)
```

   Si la signature est valide, la commande ne renvoie aucune sortie. Si la signature ne peut pas être vérifiée, la commande renvoie `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer`. Si votre signature ne peut pas être vérifiée, contactez AWS Support.

7. Validez le contenu du document d'identité d'instance.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

   Si le contenu du document d'identité d'instance est valide, la commande renvoie `True`. Si le document d'identité de l'instance ne peut pas être validé, contactez AWS Support.

AWS des certificats publics, par exemple des signatures de documents d'identité

Les certificats AWS publics suivants peuvent être utilisés pour vérifier le contenu du document d'identité d'une instance, comme décrit dansVérifier le document d'identité de l'instance.

Assurez-vous d'utiliser le bon certificat pour votre région et pour la procédure de vérification que vous utilisez. Si vous vérifiez la PKCS7 signature, utilisez le DSA certificat. Si vous vérifiez la signature codée en base6, utilisez le RSA certificat. Si vous vérifiez la signature RSA -2048, utilisez le certificat RSA -2048.

Développez chaque région ci-dessous pour afficher les certificats spécifiques à chaque région.

USA Est (Virginie du Nord) — us-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUE1y2NIKCU+Rg4uu4u32koG9QEYIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MzQwMVoXDTI5MDQyODE3MzQwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUE1y2NIKC
U+Rg4uu4u32koG9QEYIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAlxSmwcWnhT4uAeSinJuz+1BTcKhVSWb5jT8pYjQb8ZoZkXXRGb09mvYeU
NeqOBr27rvRAnaQ/9LUQf72+SahDFuS4CMI8nwowytqbmwquqFr4dxA/SDADyRiF
ea1UoMuNHTY49J/1vPomqsVn7mugTp+TbjqCfOJTpu0temHcFA==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALFpzEAVWaQZMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU5MTJaGA8yMTk1MDExNzA4NTkxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjS2vqZu9mEOhOq+0bRpAbCUiapbZMFNQqRg7kTlr7Cf+gDqXKpHPjsng
SfNz+JHQd8WPI+pmNs+q0Z2aTe23klmf2U52KH9/j1k8RlIbap/yFibFTSedmegX
E5r447GbJRsHUmuIIfZTZ/oRlpuIIO5/Vz7SOj22tdkdY2ADp7caZkNxhSP915fk
2jJMTBUOzyXUS2rBU/ulNHbTTeePjcEkvzVYPahD30TeQ+/A+uWUu89bHSQOJR8h
Um4cFApzZgN3aD5j2LrSMu2pctkQwf9CaWyVznqrsGYjYOY66LuFzSCXwqSnFBfv
fFBAFsjCgY24G2DoMyYkF3MyZlu+rwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUrynSPp4uqSECwy+PiO4qyJ8TWSkwgY4GA1UdIwSBhjCBg4AUrynS
Pp4uqSECwy+PiO4qyJ8TWSmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALFpzEAVWaQZMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADW/s8lXijwdP6NkEoH1m9XLrvK4YTqkNfR6
er/uRRgTx2QjFcMNrx+g87gAml11z+D0crAZ5LbEhDMs+JtZYR3ty0HkDk6SJM85
haoJNAFF7EQ/zCp1EJRIkLLsC7bcDL/Eriv1swt78/BB4RnC9W9kSp/sxd5svJMg
N9a6FAplpNRsWAnbP8JBlAP93oJzblX2LQXgykTghMkQO7NaY5hg/H5o4dMPclTK
lYGqlFUCH6A2vdrxmpKDLmTn5//5pujdD2MN0df6sZWtxwZ0osljV4rDjm9Q3VpA
NWIsDEcp3GUB4proOR+C7PNkY+VGODitBOw09qBGosCBstwyEqY=
-----END CERTIFICATE-----
```

USA Est (Ohio) – us-east-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUVJTc+hOU+8Gk3JlqsX438Dk5c58wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MTE0OVoXDTI5MDQyODE3MTE0OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUVJTc+hOU
+8Gk3JlqsX438Dk5c58wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAywJQaVNWJqW0R0T0xVOSoN1GLk9x9kKEuN67RN9CLin4dA97qa7Mr5W4P
FZ6vnh5CjOhQBRXV9xJUeYSdqVItNAUFK/fEzDdjf1nUfPlQ3OJ49u6CV01NoJ9m
usvY9kWcV46dqn2bk2MyfTTgvmeqP8fiMRPxxnVRkSzlldP5Fg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM07oeX4xevdMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA2MTAx
MjU4MThaGA8yMTk1MTExNDEyNTgxOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6v6kGMnRmFDLxBEqXzP4npnL65OO0kmQ7w8YXQygSdmNIoScGSU5wfh9
mZdcvCxCdxgALFsFqPvH8fqiE9ttI0fEfuZvHOs8wUsIdKr0Zz0MjSx3cik4tKET
```

```
ch0EKfMnzKOgDBavraCDeX1rUDU0Rg7HFqNAOry3uqDmnqtk00XC9GenS3z/7ebJ
fIBEPAam5oYMVFpX6M6St77WdNE8wEU8SuerQughiMVx9kMB07imeVHBiELbMQ0N
lwSWRL/61fA02keGSTfSp/0m3u+lesf2VwVFhqIJs+JbsEscPxOkIRlzy8mGd/JV
ONb/DQpTedzUKLgXbw7KtO3HTG9iXQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU2CTGYE5fTjx7gQXzdZSGPEWAJY4wgY4GA1UdIwSBhjCBg4AU2CTG
YE5fTjx7gQXzdZSGPEWAJY6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM07oeX4xevdMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANdqkIpVypr2PveqUsAKke1wKCOSuw1UmH9k
xX1/VRoHbrI/UznrXtPQOPMmHA2LKSTedwsJuorUn3cFH6qNs8ixBDrl8pZwfKOY
IBJcTFBbI1xBEFkZoO3wczzo5+8vPQ60RVqAaYb+iCa1HFJpccC3Ovajfa4GRdNb
n6FYnluIcDbmpcQePoVQwX7W3oOYLB1QLN7fE6H1j4TBIsFdO3OuKzmaifQlwLYt
DVxVCNDabpOr6Uozd5ASm4ihPPoEoKo7Ilp0fOT6fZ41U2xWA4+HF/89UoygZSo7
K+cQ90xGxJ+gmlYbLFR5rbJOLfjrgDAb2ogbFy8LzHo2ZtSe60M=
-----END CERTIFICATE-----
```

USA Ouest (Californie du Nord) – us-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIDITCCAoqgAwIBAgIUK2zmY9PUSTR7rc1k2OwPYu4+g7wwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MDI0M1oXDTI5MDQyODE3MDI0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUK2zmY9PU
STR7rc1k2OwPYu4+g7wwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQA1Ng4QmN4n7iPh5CnadSOc0ZfM7by0dBePwZJyGvOHdaw6P6E/vEk76KsC
Q8p+akuzVzVPkU4kBK/TRqLp19wEWoVwhhTaxHjQ1tTRHqXIVlrkw4JrtFbeNM21
GlkSLonuzmNZdivn9WuQYeGe7nUD4w3q9GgiF3CPorJe+UxtbA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJANNPkIpcyEtIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAzMDdaGA8yMTk1MDQwMzA5MDMwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApHQGvHvq3SVCzDrC7575BW7GWLzcj8CLqYcL3YY7Jffupz7OjcftO57Z
4fo5Pj0CaS8DtPzh8+8vdwUSMbiJ6cDd3ooio3MnCq6DwzmsY+pY7CiI3UVG7KcH
4TriDqr1Iii7nB5MiPJ8wTeAqX89T3SYaf6Vo+4GCb3LCDGvnkZ9TrGcz2CHkJsj
AIGwgopFpwhIjVYm7obmuIxSIUv+oNH0wXgDL029Zd98SnIYQd/njiqkzE+lvXgk
4h4Tu17xZIKBgFcTtWPky+POGu81DYFqiWVEyR2JKKm2/iR1dL1YsT39kbNg47xY
aR129sS4nB5Vw3TRQA2jL0ToTIxzhQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUgepyiONs8j+q67dmcWu+mKKDa+gwgY4GA1UdIwSBhjCBg4AUgepy
iONs8j+q67dmcWu+mKKDa+ihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJANNPkIpcyEtIMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGLFWyutf1u0xcAc+kmnMPqtc/Q6b79VIX0E
tNoKMI2KR8lcV8ZElXDb0NC6v8UeLpe1WBKjaWQtEjL1ifKg9hdY9RJj4RXIDSK7
33qCQ8juF4vep2U5TTBd6hfWxt1Izi88xudjixmbpUU4YKr8UPbmixldYR+BEx0u
B1KJi9l1lxvuc/Igy/xeHOAZEjAXzVvHp8Bne33VVwMiMxWECZCiJxE4I7+Y6fqJ
pLLSFFJKbNaFyXlDiJ3kXyePEZSc1xiWeyRB2ZbTi5eu7vMG4i3AYWuFVLthaBgu
```

```
lPfHafJpj/JDcqt2vKUKfur5edQ6j1CGdxqqjawhOTEqcN8m7us=
-----END CERTIFICATE-----
```

USA Ouest (Oregon) – us-west-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFx8PxCkbHwpD31bOyCtyz3GclbgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MjM1OVoXDTI5MDQyODE3MjM1OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFx8PxCkb
```

```
HwpD31bOyCtyz3GclbgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBzOl+9Xy1+UsbUBI95HO9mbbdnuX+aMJXgG9uFZNjgNEbMcvx+h8P9IMko
z7PzFdheQQ1NLjsHH9mSR1SyC4m9ja6BsejH5nLBWyCdjfdP3muZM4O5+r7vUa1O
dWU+hP/T7DUrPAIVMOE7mpYa+WPWJrN6BlRwQkKQ7twm9kDalA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALZL3lrQCSTMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAxMzJaGA8yMTk1MDExNzA5MDEzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA02Y59qtAA0a6uzo7nEQcnJ26OKF+LRPwZfixBH+EbEN/Fx0gYy1jpjCP
s5+VRNg6/WbfqAsV6X2VSjUKN59ZMnMY9ALA/Ipz0n00Huxj38EBZmX/NdNqKm7C
qWu1q5kmIvYjKGiadfboU8wLwLcHo8ywvfgI6FiGGsEO9VMC56E/hL6Cohko11LW
dizyvRcvg/IidazVkJQCN/4zC9PUOVyKdhW33jXy8BTg/QH927QuNk+ZzD7HH//y
tIYxDhR6TIZsSnRjz3bOcEHxt1nsidc65mY0ejQty4hy7ioSiapw316mdbtE+RTN
fcH9FPIFKQNBpiqfAW5Ebp3Lal3/+wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU7coQx8Qnd75qA9XotSWT3IhvJmowgY4GA1UdIwSBhjCBg4AU7coQ
x8Qnd75qA9XotSWT3IhvJmqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALZL3lrQCSTMMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFZ1e2MnzRaXCaLwEC1pW/f0oRG8nHrlPZ9W
OYZEWbh+QanRgaikBNDtVTwARQcZm3z+HWSkaIx3cyb6vM0DSkZuiwzm1LJ9rDPc
aBm03SEt5v8mcc7sXWvgFjCnUpzosmky6JheCD4O1Cf8k0olZ93FQnTrbg62OK0h
83mGCDeVKU3hLH97FYoUq+3N/IliWFDhvibAYYKFJydZLhIdlCiiB99AM6Sg53rm
oukS3csyUxZyTU2hQfdjyo1nqW9yhvFAKjnnggiwxNKTTPZzstKW8+cnYwiiTwJN
QpVoZdt0SfbuNnmwRUMi+QbuccXweav29QeQ3ADqjgB0CZdSRKk=
-----END CERTIFICATE-----
```

Afrique (Le Cap) – af-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7DCCAqwCCQCncbCtQbjuyzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA2MDQxMjQ4MDVaFw00
NTA2MDQxMjQ4MDVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
```

```
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQC12Nr1gMrHcFSZ7S/A
pQBSCMHWmn2qeoQTMVWqe50fnTd0zGFxDdIjKxUK58/8zjWG5uR4TXRzmZpGpmXB
bSufAR6BGqud2LnT/HIWGJAsnX2uOtSyNfCoJigqwhea5w+CqZ6I7iBDdnB4TtTw
qO6TlnExHFVj8LMkylZgiaE1CQIVAIhdobse4K0QnbAhCL6R2euQzloXAoGAV/21
WUuMz/79Ga0JvQcz1FNy1sT0pU9rU4TenqLQIt5iccn/7EIfNtvVO5TZKulIKq7J
gXZr0x/KIT8zsNweetLOaGehPIYRMPX0vunMMR7hN7qA7W17WZv/76adywIsnDKq
ekfe15jinaX8MsKUdyDK7Y+ifCG4PVhoM4+W2XwDgYQAAoGAIxOKbVgwLxbn6Pi2
6hBOihFv16jKxAQI0hHzXJLV0Vyv9QwnqjJJRfOCy3dB0zicLXiIxeIdYfvqJr+u
hlN8rGxEZYYJjEUKMGvsc0DW85jonXz0bNfcP0aaKH0lKKVjL+OZi5n2kn9wgdo5
F3CVnMl8BUra8A1Tr2yrrE6TVZ4wCQYHKoZIzjgEAwMvADAsAhQfa7MCJZ+/TEY5
AUr0J4wm8VzjoAIUSYZVu2NdRJ/ERPmDfhW5EsjHlCA=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAKumfZiRrNvHMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTExMjcw
NzE0MDVaGA8yMTk5MDUwMjA3MTQwNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDFd571nUzVtke3rPyRkYfvs3jh0C0EMzzG72boyUNjnfw1+m0TeFraTLKb9T6F
7TuB/ZEN+vmlYqr2+5Va8U8qLbPF0bRH+FdaKjhgWZdYXxGzQzU3ioy5W5ZM1VyB
7iUsxEAlxsybC3ziPYaHI42UiTkQNahmoroNeqVyHNnBpQIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAAJLylWyElEgOpW4B1XPyRVD4pAds8Guw2+krgqkY0HxLCdjosuH
RytGDGN+q75aAoXzW5a7SGpxLxk6Hfv0xp3RjDHsoeP0i1d8MD3hAC5ezxS4oukK
s5gbPOnokhKTMPXbTdRn5ZifCbWlx+bYN/mTYKvxho7b5SVg2o1La9aK
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAIFI+O5A6/ZIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA2MDQx
MjQ4MDRaGA8yMTk4MTEwNzEyNDgwNFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy7/WHBBHOrk+20aumT07g8rxrSM0UXgki3eYgKauPCG4Xx//vwQbuZwI
oeVmR9nqnhfij2wOcQdbLandh0EGtbxerete3IoXzd1KXJb11PVmzrzyu5SPBPuP
iCeV4qdjjkXo2YWM6t9YQ911hcG96YSp89TBXFYUh3KLxfqAdTVhuC0NRGhXpyii
```

```
j/czo9njofHhqhTr7UEyPun8NVS2QWctLQ86N5zWR3Q0GRoVqqMrJs0cowHTrVw2
9Qr7QBjjBOVbyYmtYxm/DtiKprYV/e6bCAVok015X1sZDd3oCOQNoGlv5XbHJe2o
JFD8GRRy2rkWO/lNwVFDcwec6zC3QwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCE
goqzjpCpmMgCpszFHwvRaSMbspKtK7wNImUjrSBOfBJsfFulyg1Zgn2nDCK7kQhx
jMJmNIvXbps3yMqQ2cHUkKcKf5t+WldfeT4Vk1Rz6HSA8sd0kgVcIesIaoy2aaXU
VEB/oQziRGyKdN1d4TGYVZXG44CkrzSDvlbmfiTq5tL+kAieznVF3bzHgPZW6hKP
EXC3G/IXrXicFEe6YyE1Rakl62VncYSXiGe/i2XvsiNH3Qlmnx5XS7W0SCN0oAxW
EH9twibauv82DVg1WOkQu8EwFw8hFde9X0Rkiu0qVcuU8lJgFEvPWMDFU5sGB6ZM
gkEKTzMvlZpPbBhg99Jl
-----END CERTIFICATE-----
```

Asie-Pacifique (Hong Kong) – ap-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq4CCQCO7MJe5Y3VLjAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDMwMjIxMjFaFw00
NTAyMDMwMjIxMjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDvQ9RzVvf4MAwGbqfX
blCvCoVb9957OkLGn/04CowHXJ+vTBR7eyIa6AoXltsQXBOmrJswToFKKxT4gbuw
jK7s9QQX4CmTRWcEgO2RXtZSVjOhsUQMh+yf7Ht4OVL97LWnNfGsX2cwjcRWHYgI
7lvnuBNBzLQHdSEwMNq0Bk76PwIVAMan6XIEEPnwr4e6u/RNnWBGKd9FAoGBAOCG
eSNmxpW4QFu4pIlAykm6EnTZKKHT87gdXkAkfoC5fAfOxxhnE2HezZHp9Ap2tMV5
8bWNvoPHvoKCQqwfm+OUBlAxC/3vqoVkKL2mG1KgUH9+hrtpMTkwO3RREnKe7I5O
x9qDimJpOihrL4I0dYvy9xUOoz+DzFAW8+ylWVYpA4GFAAKBgQDbnBAKSxWr9QHY
6Dt+EFdGz6lAZLedeBKpaP53Z1DTO34J0C55YbJTwBTFGqPtOLxnUVDlGiD6GbmC
80f3jvogPR1mSmGsydbNbZnbUEVWrRhe+y5zJ3g9qs/DWmDW0deEFvkhWVnLJkFJ
9pdOu/ibRPH1lE2nz6pK7GbOQtLyHTAJBgcqhkjOOAQDAzAAMC0CFQCoJlwGtJQC
cLoM4p/jtVFOj26xbgIUUS4pDKyHaG/eaygLTtFpFJqzWHc=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICSzCCAbQCCQDtQvkVxRvK9TANBgkqhkiG9w0BAQsFADBqMQswCQYDVQQGEwJV
UzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHU2VhdHRsZTEYMBYGA1UE
ChMPQW1hem9uLmNvbSBJbmMuMRowGAYDVQQDExFlYzIuYW1hem9uYXdzLmNvbTAe
Fw0xOTAyMDMwMzAwMDZaFw0yOTAyMDIwMzAwMDZaMGoxCzAJBgNVBAYTAlVTMRMw
EQYDVQQIEwpXYXNoaW5ndG9uMRAwDgYDVQQHEwdTZWF0dGxlMRgwFgYDVQQKEw9B
```

```
bWF6b24uY29tIEluYy4xGjAYBgNVBAMTEWVjMi5hbWF6b25hd3MuY29tMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1kkHXYTfc7gY5Q55JJhjTieHAgacaQkiR
Pity9QPDE3b+NXDh4UdP1xdIw73JcIIG3sG9RhWiXVCHh6KkuCTqJfPUknIKk8vs
M3RXflUpBe8Pf+P92pxqPMCz1Fr2NehS3JhhpkCZVGxxwLC5gaG0Lr4rFORubjYY
Rh84dK98VwIDAQABMA0GCSqGSIb3DQEBCwUAA4GBAA6xV9f0HMqXjPHuGILDyaNN
dKcvplNFwDTydVg32MNubAGnecoEBtUPtxBsLoVYXCOb+b5/ZMDubPF9tU/vSXuo
TpYM5Bq57gJzDRaBOntQbX9bgHiUxw6XZWaTS/6xjRJDT5p3S1E0mPI3lP/eJv4o
Ezk5zb3eIf10/sqt4756
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMoxixvs3YssMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA3MjAw
ODQ0NDRaGA8yMTk3MTIyMzA4NDQ0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA4T1PNsOg0FDrGlWePoHeOSmOJTA3HCRy5LSbYD33GFU2eBrOIxoU/+SM
rInKu3GghAMfH7WxPW3etIAZiyTDDU5RLcUq2Qwdr/ZpXAWpYocNc/CEmBFtfbxF
z4uwBIN3/drM0RSbe/wP9EcgmNUGQMMZWeAji8sMtwpOblNWAP9BniUG0Flcz6Dp
uPovwDTLdAYT3TyhzlohKL3f6O48TR5yTaV+3Ran2SGRhyJjfh3FRpP4VC+z5LnT
WPQHN74Kdq35UgrUxNhJraMGCzznolUuoR/tFMwR93401GsM9fVA7SW3jjCGF81z
PSzjy+ArKyQqIpLW1YGWDFk3sf08FQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDK
2/+C3nPMgtyOFX/I3Cyk+Pui44IgOwCsIdNGwuJysdqp5VIfnjegEu2zIMWJSKGO
lMZoQXjffkVZZ97J7RNDW06oB7kj3WVE8a7U4WEOfnO/CbMUf/x99CckNDwpjgW+
K8V8SzAsQDvYZs2KaE+18GFfLVF1TGUYK2rPSZMHyX+v/TIlc/qUceBycrIQ/kke
jDFsihUMLqgmOV2hXKUpIsmiWMGrFQV4AeV0iXP8L/ZhcepLf1t5SbsGdUA3AUY1
3If8s81uTheiQjwY5t9nM0SY/1Th/tL3+RaEI79VNEVfG1FQ8mgqCK0ar4m0oZJl
tmmEJM7xeURdpBBx36Di
-----END CERTIFICATE-----
```

Asie-Pacifique (Hyderabad) – ap-south-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCArCgAwIBAgIGAXjrQ4+XMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24g
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
```

```
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAJCKGBBoxIUxqBk94JHhwZZbgvbP0DAOoHENQWxp/98lI7/
YOfYJOVMJS22aCnHDurofmo5rvNIkgXi7Rztbhu
+lko9rK6DgpmpUwBU0WZtf34aZ2IWNBwHaVhHvWAQf9/46u18dMa2YucK1Wi+Vc+M
+KldrvgXmhym6ErNlzhJyMAkGByqGSM44BAMDLwAwLAIUaaPKxaOHoYvwz709xXpsQueIq+UCFFa/
GpzoDOSokl1057NU/2hnsiW4
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjwLj9CMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+sFcobrjvcAYm0PNRD8f4R1jAzvoLt2+qGeOTAyO1Httj6cmsYN3AP1hN5iYuppFiYsl2eNPa/
CD0Vg0BAfDFlV5rzjpA0j7TJabVh4kj7JvtD+xYMi6wEQA4x6SPONY4OeZ2+8o/
HS8nucpWDVdPRO6ciWUlMhjmDmwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAAy6sgTdRkTqELHBeWj69q60xHyUmsWqHAQ
TGGbYP0yP2qfMl0cCImzRI5W0gn8gogdervfeT7nH5ih0TWEy/QDWfkQ601L4erm4yh4YQq8vcqAPSkf04N
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAIVWfPw/X82fMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MDQx
NDMwMjhaGA8yMjAxMTIwODE0MzAyOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAg29QEFriG+qFEjYW/v62nN70lMJY/Hevx5TtmU/VIYBPQa3HUGTBAbbI
2Tmy8UMpa8kZeaYeI3RAfiQWt0Ws7wUrBuO2Pdp518WDPaJUH7RWEuu1BDDkyZRW
NAMNPCn3ph7Od243IFcLGku7HVekel5poqRpSfojrMasjlf+CvixUeAJbmFoxUHK
kh5unzG2sZyO4wHXcJPQkRf5a8zSTPe9YZP1kXPPEv4p/jTSggaYPxXyS6QVaTlV
zLeLFZ0fesLPMeil3KYQtV7IKLQiEA2F6dxWnxNWQlyMHtdq6PucfEmVx17i/Xza
yNBRo0azY8WUNVkEXrRhp/pU8Nh3GQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU9AO1aZk9RLXk2ZvRVoUxYvQy9uwwgY4GA1UdIwSBhjCBg4AU9AO1
aZk9RLXk2ZvRVoUxYvQy9uyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAIVWfPw/X82fMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADexluMRQRftqViahCnauEWGdMvLCBr8A+Yr
6hJq0guoxEk/lahxR137DnfMPuSbi1Rx5QKo7oBrWfG/zsgQUnF2IwHTzwD+i/2m
XCane6FiS5RpK3lGdILq8ZmlhQk+6iI8yoZLr0LCfTh+CLgIKHOknfR5lFzgzAiF
SI8/Q9mm+uvYtSTZECI6Zh57QZPoETAG/yl+9jiOy2lAelqa/k1i+Qo8gMfOc+Pm
```

```
dwY7o6fV+oucgRlsdey6VM45LeyILQqv0RXtVzjuowanzmCCFMjgqiO9oZAWu4Oh
+F3unijELo01vZJs8s2N3KGlo3/jtUFTX6RTKShZlAPLwBi5GMI=
-----END CERTIFICATE-----
```

Asie-Pacifique (Jakarta) – ap-southeast-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCArCgAwIBAgIGAXbVDEikMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24g
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAPjuiEx05N3JQ6cVwntJie67D8OuNo4jGRn
+crEtL7YO0jSVB9zGE1ga
+UgRPIaYETL293S8rTJTVgXAqdpBwfaHC6NUzre8U8iJ8FMNnlP9Gw1oUIlgQBjORyynVJexoB31TDZM
+/52g9O/bpq1QqNyKbeIgyBBlc1dAtr1QLnsMAkGByqGSM44BAMDLwAwLAIUK8E6RDIRtwK+9qnaTOBhvO/
njuQCFFocyT1OxK+UDR888oNsdgtif2Sf
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXbVDG2yMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
Vbt0gQ1ebWcur2hSO7PnJifE4OPxQ7RgSAlc4/spJp1sDP+ZrS0LO1ZJfKhXf1R9S3AUwLnsc7b
+IuVXdY5LK9RKqu64nyXP5dx170zoL8loEyCSuRR2fs+04i2QsWBVP+KFNAn7P5L1EHRjkgTO8kjNKviwRV
+OkP9ab5wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAI4WUy6+DKh0JDSzQEZNyBgNlSoSuC2owtMxCwGB6nBfzzfcekWvs
+87w/g9lNwUnUt0ZHYyh2tuBG6hVJuUEwDJ/z3wDd6wQviLOTF3MITawt9P8siR1hXqLJNxpjRQFZrgHqi
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMtdyRcH51j9MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MDgx
MjM5MTZaGA8yMjAxMDkxMjEyMzkxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
```

```
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvUsKCxoH6KXRYJLeYTWAQfaBQeCwhJaR56mfUeFHJE4g8aFjWkiN4uc1
TvOyYNnIZKTHWmzmulmdinWNbwP0GiROHb/i7ro0Hhvnptyyc Gt8ag8affiIbx5X
7ohdwSN2KJ6G0IKflIx7f2NEI0oAMM/9k+T1eVF+MVWzpZoiDp8frLNkqp8+RAgz
ScZsbRfwv3u/if5xJAvdg2nCkIWDMSHEVPoz0lJo7v0ZuDtWWsL1LHnL5ozvsKEk
+ZJyEi23r+U1hIT1NTBdp4yoigNQexedtwCSr7q36oOdDwvZpqYlkLi3uxZ4ta+a
01pzOSTwMLgQZSbKWQrpMvsIAPrxoQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU1GgnGdNpbnL3lLF30Jomg7Ji9hYwgY4GA1UdIwSBhjCBg4AU1Ggn
GdNpbnL3lLF30Jomg7Ji9hahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMtdyRcH51j9MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACVl00qQlatBKVeiWMrhpczsJroxDxlZTOba
6wTMZk7c3akb6XMOSZFbGaifkebPZqTHEhDlrClM2j9AIlYcCx6YCrTf4cuhn2mD
gcJN33143eOWSaeRY3ee4j+V9ne98y3kO2wLz95VrRgclPFR8po2iWGzGhwUi+FG
q8dXeCH3N0DZgQsSgQWwmdNQXZZej6RHLU/8In5trHKLY0ppnLBjn/UZQbeTyW5q
RJB3GaveXjfgFUWj2qOcDuRGaikdS+dYaLsi5z9cA3FolHzWxx9MOs8io8vKqQzV
XUrLTNWwuhZy88cOlqGPxnoRbw7TmifwPw/cunNrsjUUOgs6ZTk=
-----END CERTIFICATE-----
```

Asie-Pacifique (Malaisie) — ap-southeast-5

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq4CCQC5X6U+vgoLEDAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDAxMDMxMjU3NTRaGA8y
MDUwMDEwMzEyNTc1NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtjCCASsGByqGSM44BAEwggEeAoGBAIzEMPCIPFfOYCg4
BCjKGyl60wOfmwHPzSOXZ3Z2wS/LYNHUtHGwtVNePSTyCu/CuZF6gC9n/wBORtQp
+SSkn+weGc/BmUA1mp/vrN7v+aSCgKJoO+sgpa1PPOgNvUaMw6O5odsZWQCMSjkU
6RTo/PL2v/tMfiCocF4ghvyRC6hvAhUA0VoObKC2IXzXgVvRRupo4qHbcm8CgYAe
bbNuawh3rAxkFvUs9FPzW5E+xllG16Z//61PENKqonmk+zBiBdiIlS1F6ZqmTqkI
z5+qfSt1m3pb3j2W0NT7lEDFvy8Gr6Y2vohCHmL+T1u1Yy4PeqbgrFwcen7y7WoO
/KCV7Y9/ODQMMyuAzT3h5wJNweT7L5MUN8JYpZSi3QOBhAACgYBqaDuG2u6V91Qj
K2wEAElxaaRaNo/ewg/wWDmHYqoeHOR0HfuFCYgASE9f7ULqYtX1VURcgcjw9XN4
BDmPilXvfi04INPTnw4IxFJKDzzC0kVH7esVas982Po8v3megH32H9Rl87r7UG1c
ZEbkSkKVX6YKYg1PR3rfjXgdwVZv/zAJBgcqhkjOOAQDAzAAMC0CFFWeRe2fYW2i
6mMd26Wzbx87Y0DXAhUAoPCnF+5hGJw0jT9aL7QsgcfLi9Y=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAMuBl6rhZCJKMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDAxMDMx
MjU3NTRaGA8yMjAzMDYwOTEyNTc1NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDFuKydxZsordNH7bLwIluEGOkX7/CdLdpeqkDKEhQkFwzpRxaX4EAlkGh2/o7D
8qneC9cGQhqSG5WVVBrmZG7sfkFOM4m1AtY++kfv+MYto1VFgLk1xJbkpq1r4YeQ
Ul+ZsJYsZpyX/t+g8s7rW0OVcBsYx4L75bf34z38mwK8PQIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBADD9C4pWL8RUvF1CJW8kExj35xmozlFlmrKs8Zpi8+Eg6q+W9dgd
xMdH95tgZtmVMDqlvVR+DK0iO1BNpqPjrqWkk2tTLivpS+sGzCE/jCl18Q28Rk71
/A3gLD7Rtbq5TKNvuFCHwYMjrTDHI6aBjIaAlDm4e2/j/OxVtHyZGTre
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANC3xtbPhQ2GMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDAxMDMx
MjU3NTRaGA8yMjAzMDYwOTEyNTc1NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAt3aMy7Hsp4ySG3mlfi+pdTcZw6H6XNU1Y36fNdi4c+MzinQQbnqMPyt7
QLgU+XCWmcWsVo7GQF6n9N01Rh+UXXUZU4jcXlFocQPCWf9O+IIIPXkd67kFMUV
HAxCELjfxHbC+I8e7dwOJhmdF4Bfi52Ty8zz0HdE8JDypPkTDlXuGvTgDyW7NP56
I/vlQaXLoYSbcQe5pv2a9gyBaaCM1QoeqwAHAeCNXb9Nuj9ZX3GHGJb3TuqAeKCD
5i9TscCB9XjY6Fx+zfSAobjBZwgLEtLOwJhbZnKmx4gJMaaNFipAjVT2FSS3+yev
eTYBoa1dvhk0ivQyQIPpHmihrmkWuwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBC
fdgyI8GjmCqiHAlh+L1bj0LdNql9zl7RXmOEzsuRdtdMumkxYXX88UtROy3fdi1i
VaEwHdAK8ThzRkesgHza/cXzqCMewaYxujSI6p6G7x99FFeGif1x0FJdj8AoeTL7
4h9bmS/6l4/NL7DJI9G7ovES/hoUA9v9TDhv+vauxXlgfrp0MPecprxBYlrc+DH2
adGCdKCp2lQ2YDKOD9TCEjYIli8XSoyevoWHUjfDYrCrCp8l4s/p7HOgYr8fJBAs
EuVy8211LVz1/X4EMBRNtNjXK9sklsxAOX14NDfBFSS0toxl3K6Tf9t/PviBl95d
hncyDAcFgDCK4w8LLlVW
-----END CERTIFICATE-----
```

Asie-Pacifique (Melbourne) ap-southeast-4

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjWF7P2MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAPRXSsQP9E3dw8QXKlrgBgEVCprLHdK/bbrMas0XMu1EhOD
+q
+0PcTr8+iwbtoXlY5MCeatWIp1GrXQjVqsF8vQqxlEuRuYKbR3nq4mWwaeGlx9AG5EjQHRa3GQ44wWHOdof0M3NRI1MP
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjSh40SMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+qWTGAbGsPeMX4hBMjAJUKys2NIRcRZaLM/BCew2FIPVjNtlaj6Gwn9ipU4Mlz3zIwAMWi1AvGMSreppt
+wV6MRtfOjh0Dvj/veJe88aEZJMozNgkJFRS
+WFWsckQeL56tf6kY6QTlNo8V/0CsQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAF7vpPghH0FRo5gu49EArRNPrIvW1egM
wcgkqIwwuXYj+1rhlL+/
iMpQWjdVGEqIZSeXn5fLmdx50eegFCwND837r9e8XYTiQS143Sxt9+Yi6BZ7U7YD8kK9NBWoJxFqUeHdpRCs0O7COjT3
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAN4GTQ64zVs8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTMx
MzMzMDBaGA8yMjAxMTIxNzEzMzMwMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA2BYgeCr+Rk/jIAEDOHS7wJql62vc83QEwjuzk0qOFEReIZzlN1fBRNXK
g0T178Kd3gLYcE59wEFbTe/X5yOA1Lo95x1anSAo7R+Cisf9C2HQuJp+gVb+zx71
lniPF7gHziGpm0M8DdAU/IW+wkZwGbP4z7Hq9+bJ0P2ltvPJ5yxSgkFuDsI9VBHa
CLoprHsCHh2VdP8KcMgQQMmHe1NmBpyTk0ul/aLmQkCQEX6ZIRGOeq228fwlh/t+
Ho+jv87duihVKic6MrL32SlD+maX0LSDUydWdaOLLTGkh7oV7+bFuH6msrXUu+Ur
```

```
ZEP1r/MidCWMhfgrFzeTBzOHA97qxQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUcHMd1cHqzmsQ5hpUK3EMLhHdsi4wgY4GA1UdIwSBhjCBg4AUcHMd
1cHqzmsQ5hpUK3EMLhHdsi6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAN4GTQ64zVs8MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAI4PFyVN+7EGSObioiPnv0LL0f70SSzUZJ8p
XO90d4rWea7jIbgZ2AKb+ErynkU9xVg7XQQ5k6KDWgp/4jYFL2dqnt/YAY4PS0un
RSrYElawxLT0BcLn4rcSDC79vQe1xGC5//wDdV6b399COAHRAK6axWYy5w32u9PL
uw0cIp3Ch8JoNwcgTHKRRGzePmBeR4PNqhHTArG4/dJk6/aUO4OpX0WzI6L67CGY
6Nex3dau+gkLCK93dTEkrXtyXHu4wB0J9zd1w+iQ0SEa9eKc78/NjEsF/FZdGrWC
t57lIMOOXJhQ1kRgSwNeZdQWV1dRakvO6sfcvVYkfj1wAvZvvAw=
-----END CERTIFICATE-----
```

Asie-Pacifique (Mumbai) – ap-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUDLA+x6tTAP3LRTr0z6nOxfsozdMwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
```

```
MB4XDTI0MDQyOTE0MTMwMVoXDTI5MDQyODE0MTMwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUDLA+x6tT
AP3LRTr0z6nOxfsozdMwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAZ7rYKoAwwiiH1M5GJbrT/BEk3OO2VrEPw8ZxgpqQ/EKlzMlOs/0Cyrmp7
UYyUgYFQe5nq37Z94rOUSeMgv/WRxaMwrLlLqD78cuF9DSkXaZIX/kECtVaUnjk8
BZx0QhoIHOpQocJUSlm/dLeMuE0+0A3HNR6JVktGsUdv9ulmKw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPRYyD8TtmC0MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjAzMDcx
MDQ1MDFaGA8yMTk1MDgxMTEwNDUwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA0LSS5I/eCT2PM0+qusorBx67QL26BIWQHd/yF6ARtHBb/1DdFLRqE5Dj
07Xw7eENC+T79mOxOAbeWg91KaODOzw6i9I/2/HpK0+NDEdD6sPKDA1d45jRra+v
CqAjI+nV9Vw91wv7HjMk3RcjWGziM8/hw+3YNIutt7aQzZRwIWlBpcqx3/AFd8Eu
2UsRMSHgkGUW6UzUF+h/U8218XfrauKNGmNKDYUhtmyBrHT+k6J0hQ4pN7fe6h+Z
w9RVHm24BGhlLxLHLmsOIxvbrF277uX9Dxu1HfKfu5D2kimTY7xSZDNLR2dt+kNY
/+iWdIeEFpPT0PLSILt52wP6stF+3QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBI
E6w+WWC2gCfoJO6c9HMyGLMFEpqZmz1n5IcQt1h9iyO7Vkm1wkJiZsMhXpk73zXf
TPxuXEacTX3SOEa07OIMCFwkusO5f6leOyFTynHCzBgZ3U0UkRVZA3WcpbNB6Dwy
h7ysVlqyT9WZd7EOYm5j5oue2G2xdei+6etgn5UjyWm6liZGrcOF6WPTdmzqa6WG
ApEqanpkQd/HM+hUYex/ZS6zEhd4CCDLgYkIjlrFbFb3pJ1OVLztIfSN5J4Oolpu
JVCfIq5u1NkpzL7ys/Ub8eYipbzI6P+yxXiUSuF0v9b98ymczMYjrSQXIf1e8In3
OP2CclCHoZ8XDQcvvKAh
-----END CERTIFICATE-----
```

Asie-Pacifique (Osaka) – ap-northeast-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUHTRhxHhBZFOGvTFKxHoy9+f5Hl8wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2NTQwN1oXDTI5MDQyODE2NTQwN1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUHTRhxHhB
ZFOGvTFKxHoy9+f5Hl8wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAUZx7DcYbhWNTD4BNGhr5beruT2OUoGHH9J73UKxwdqeb9bH1LIWhIZO0X
/1mjn3bWBgCwfoS8gjZwsVB6fZbNBRy8urdBZJ87xF/4JPBjt7S9oGx/zthDUYrC
yK0Y0v4G0PgiS81CvYLg09LpmYhLSJbXENlkC04v5yxdKxZxyg==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMn1yPk22ditMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA3MTkx
MTEyNThaGA8yMTk2MTIyMjExMTI1OFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArznEYef8IjhrJoazI0QGZkmlmHm/4rEbyQbMNifxjsDE8YWtHNwaM91z
zmyK6Sk/tKlWxcnl3g31iq305ziyFPEewe5Qbwf1iz2cMsvfNBcTh/E6u+mBPH3J
gvGanqUJt6c4IbipdEouIjjnynyVWd4D6erLl/ENijeR1OxVpaqSW5SBK7jms49E
pw3wtbchEl3qsE42Ip4IYmWxqjgaxB7vps91n4kfyzAjUmklcqTfMfPCkzmJCRgp
Vh1C79vRQhmriVKD6BXwfZ8tG3a7mijeDn7kTsQzgO07Z2SAE63PIO48JK8HcObH
tXORUQ/XF1jzi/SIaUJZT7kq3kWl8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBj
ThtO9dLvU2QmKuXAhxXjsIdlQgGG3ZGh/Vke4If1ymgLx95v2Vj9Moxk+gJuUSRL
BzFte3TT6b3jPolbECgmAorjj8NxjC17N8QAAI1d0S0gI8kqkG7V8iRyPIFekv+M
pcai1+cIv5IV5qAz8QOMGYfGdYkcoBjsgiyvMJu/2N2UbZJNGWvcEGkdjGJUYYOO
NaspCAFm+6HA/K7BD9zXB1IKsprLgqhiIUgEaW3UFEbThJT+z8UfHG9fQjzzfN/J
nT6vuY/0RRu1xAZPyh2gr5okN/s6rnmh2zmBHU1n8cbCc64MVfXe2g3EZ9Glq/9n
izPrI09hMypJDP04ugQc
-----END CERTIFICATE-----
```

Asie-Pacifique (Séoul) – ap-northeast-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
```

```
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUbBSn2UIO6vYk4iNWV0RPxJJtHlgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTEzMzg0NloXDTI5MDQyODEzMzg0NlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUbBSn2UIO
6vYk4iNWV0RPxJJtHlgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAmjTjalG8MGLqWTC2uYqEM8nzI3px1eo0ArvFRsyqQ3fgmWcQpxExqUqRy
l3+2134Kv8dFab04Gut5wlfRtc2OwPKKicmv/IXGN+9bKFnQFjTqif08NIzrDZch
aFT/uvxrIiM+oN2YsHq66GUhO2+xVRXDXVxM/VObFgPERbJpyA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANuCgCcHtOJhMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTQx
NTU3NDRaGA8yMTk1MDIxNzE1NTc0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA66iNv6pJPmGM20W8HbVYJSlKcAg2vUGx8xeAbzZIQdpGfkabVcUHGB6m
Gy59VXDMDlrJckDDk6dxUOhmcX9z785TtVZURq1fua9QosdbTzX4kAgHGdp4xQEs
mO6QZqg5qKjBP6xr3+PshfQ1rB8Bmwg0gXEm22CC7o77+7N7Mu2sWzWbiUR7vil4
9FjWS8XmMNwFTlShp4l1TDTevDWW/uYmC30RThM9S4QPvTZ0rAS18hHVam8BCTxa
LHaVCH/Yy52rsz0hM/FlghnSnK105ZKj+b+KIp3adBL8OMCjgc/Pxi0+j3HQLdYE
32+FaXWU84D2iP2gDT28evnstzuYTQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQC1
```

```
mA4q+12pxy7By6g3nBk1s34PmWikNRJBwOqhF8ucGRv8aiNhRRye9lokcXomwo8r
KHbbqvtK85l0xUZp/Cx4sm4aTgcMvfJP29jGLclDzeqADIvkWEJ4+xncxSYVlS9x
+78TvF/+8h9U2LnSl64PXaKdxHy2IsHIVRN4GtoaP2Xhpa1S0M328Jykq/571nfN
1WRD1c/fQf1edgzRjhQ4whcAhv7WRRF+qTbfQJ/vDxy8lkiOsvU9XzUaZ0fZSfXX
wXxZamQbONvFcxVHY/0PSiM8nQoUmkkBQuKleDwRWvkoJKYKyr3jvXK7HIWtMrO4
jmXe0aMy3thyK6g5sJVg
-----END CERTIFICATE-----
```

Asie-Pacifique (Singapour) – ap-southeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUSqP6ih+++5KF07NXngrWf26mhSUwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE0MzAxNFoXDTI5MDQyODE0MzAxNFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
```

```
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUSqP6ih++
+5KF07NXngrWf26mhSUwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAw13BxW11U/JL58j//Fmk7qqtrZTqXmaz1qm2WlIpJpW750MOcP4ux1uPy
eM0RdVZ4jHSMv5gtLAv/PjExBfw9n6vNCk+5GZG4Xec5DoapBZHXmfMo93sjxBFP
4x9rWn0GuwAVO9ukjYPevq2Rerilrq5VvppHtbATVNY2qecXDA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAJVMGw5SHkcvMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
ODU3MTlaGA8yMTk1MDQwMzA4NTcxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAlaSSLfBl7OgmikjLReHuNhVuvM20dCsVzptUyRbut+KmIEEc24wd/xVy
2RMIrydGedkW4tUjkUyOyfET5OAyT43jTzDPHZTkRSVkYjBdcYbe9o/0Q4P7IVS3
XlvwrUu0qo9nSID0mxMnOoF1l8KAqnn10tQ0W+lNSTkasW7QVzcb+3okPEVhPAOq
MnlY3vkMQGI8zX4iOKbEcSVIzf6wuIffXMGHVC/JjwihJ2USQ8fq6oy686g54P4w
ROg415kLYcodjqThmGJPNUpAZ7MOc5Z4pymFuCHgNAZNvjhZDA842Ojecqm62zcm
Tzh/pNMNeGCRYq2EQX0aQtYOIj7bOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU6SSB+3qALorPMVNjToM1Bj3oJMswgY4GA1UdIwSBhjCBg4AU6SSB
+3qALorPMVNjToM1Bj3oJMuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAJVMGw5SHkcvMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAF/0dWqkIEZKg5rca8o0P0VS+tolJJE/FRZO
atHOeaQbWzyac6NEwjYeeV2kY63skJ+QPuYbSuIBLM8p/uTRIvYM4LZYImLGUvoO
IdtJ8mAzq8CZ3ipdMs1hRqF5GRp8lg4w2QpX+PfhnW47iIOBiqSAUkIr3Y3BDaDn
EjeXF6qS4iPIvBaQQ0cvdddNh/pE33/ceghbkZNTYkrwMyBkQlRTTVKXFN7pCRUV
+L9FuQ9y8mP0BYZa5e1sdkwebydU+eqVzsil98ntkhpjvRkaJ5+Drs8TjGaJWlRw
5WuOr8unKj7YxdL1bv7//RtVYVVi296ldoRUYv4SCvJF11z0OdQ=
-----END CERTIFICATE-----
```

Asie-Pacifique (Sydney) – ap-southeast-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFxWyAdk4oiXIOC9PxcgjYYh71mwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1MjE0M1oXDTI5MDQyODE1MjE0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFxWyAdk4
oiXIOC9PxcgjYYh71mwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQByjeQe6lr7fiIhoGdjBXYzDfkX0lGGvMIhRh57G1bbceQfaYdZd7Ptc0jl
bpycKGaTvhUdkpMOiV2Hi9dOOYawkdhyJDstmDNKu6P9+b6Kak8He5z3NU1tUR2Y
uTwcz7Ye8Nldx//ws3raErfTI7D6s9m63OX8cAJ/f8bNgikwpw==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL2bOgb+dq9rMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAwNTdaGA8yMTk1MDQwMzA5MDA1N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAmRcyLWraysQS8yDC1b5Abs3TUaJabjqWu7d5gHik5Icd6dKl8EYpQSeS
vz6pLhkgO4xBbCRGlgE8LS/OijcZ5HwdrxBiKbicR1YvIPaIyEQQvF5sX6UWkGYw
Ma5IRGj4YbRmJkBybw+AAV9Icb5LJNOMWPi34OWM+2tMh+8L234v/JA6ogpdPuDr
sM6YFHMZ0NWo58MQ0FnEj2D7H58Ti//vFPl0TaaPWaAIRF85zBiJtKcFJ6vPidqK
f2/SDuAvZmyHC8ZBHg1moX9bR5FsU3QazfbW+c+JzAQWHj2AaQrGSCITxCMlS9sJ
l51DeoZBjnx8cnRe+HCaC4YoRBiqIQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU/wHIo+r5U31VIsPoWoRVsNXGxowwgY4GA1UdIwSBhjCBg4AU/wHI
o+r5U31VIsPoWoRVsNXGxoyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL2bOgb+dq9rMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACobLvj8IxlQyORTz/9q7/VJL509/p4HAeve
92riHp6+Moi0/dSEYPeFTgdWB9W3YCNc34Ss9TJq2D7t/zLGGlbI4wYXU6VJjL0S
hCjWeIyBXUZOZKFCb0DSJeUElsTRSXSFuVrZ9EAwjLvHni3BaC9Ve34iP71ifr75
8Tpk6PEj0+JwiijFH8E4GhcV5chB0/iooU6ioQqJrMwFYnwo1cVZJD5v6D0mu9bS
TMIJLJKv4QQQqPsNdjiB7G9bfkB6trP8fUVYLHLsVlIy5lGx+tgwFEYkG1N8IOO/
2LCawwaWm8FYAFd3IZl04RImNs/IMG7VmH1bf4swHOBHgCN1uYo=
-----END CERTIFICATE-----
```

Asie-Pacifique (Tokyo) – ap-northeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIULgwDh7TiDrPPBJwscqDwiBHkEFQwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTEyMjMxMFoXDTI5MDQyODEyMjMxMFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IULgwDh7Ti
DrPPBJwscqDwiBHkEFQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBtjAglBde1t4F9EHCZOj4qnY6Gigy07Ou54i+lR77MhbpzE8V28Li9l+YT
QMIn6SzJqU3/fIycIro1OVY1lHmaKYgPGSEZxBenSBHfzwDLRmC9oRp4QMe0BjOC
gepj1lUoiN7OA6PtA+ycNlsP0oJvdBjhvayLiuM3tUfLTrgHbw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL9KIB7Fgvg/MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAwMjVaGA8yMTk1MDExNzA5MDAyNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAz0djWUcmRW85C5CiCKPFiTIvj6y2OuopFxNE5d3Wtab10bm06vnXVKXu
tz3AndG+Dg0zIL0gMlU+QmrSR0PH2PfV9iejfLak9iwdm1WbwRrCEAj5VxPe0Q+I
```

```
KeznOtxzqQ5Wo5NLE9bA61sziUAFNVsTFUzphEwRohcekYyd3bBC4v/RuAjCXHVx
40z6AIksnAOGN2VABMlTeMNvPItKOCIeRLlllSqXX1gbtL1gxSW40JWdF3WPB68E
e+/1U3F7OEr7XqmNODOL6yh92QqZ8fHjG+afOL9Y2Hc4g+P1nk4w4iohQOPABqzb
MPjK7B2Rze0f9OEc51GBQu13kxkWWQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU5DS5IFdU/QwYbikgtWvkU3fDwRgwgY4GA1UdIwSBhjCBg4AU5DS5
IFdU/QwYbikgtWvkU3fDwRihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL9KIB7Fgvg/MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAG/N7ua8IE9IMyno0n5T57erBvLTOQ79fIJN
Mf+mKRM7qRRsdg/eumFft0rLOKo54pJ+Kim2cngCWNhkzctRHBV567AJNt4+ZDG5
hDgV0IxWO1+eaLE4qzqWP/9VrO+p3reuumgFZLVpvVpwXBBeBFUf2drUR14aWfI2
L/6VGINXYs7uP8v/2VBS7r6XZRnPBUy/R4hv5efYXnjwA9gq8+a3stC2ur8m5ySl
faKSwE4H320yAyaZWH4gpwUdbUlYgPHtm/ohRtiWPrN7KEG5Wq/REzMIjZCnxOfS
6KR6PNjlhxBsImQhmBvz6j5PLQxOxBZIpDoiK278e/1Wqm9LrBc=
-----END CERTIFICATE-----
```

Canada (Centre) – ca-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIDITCCAoqgAwIBAgIUIrLgixJJB5C4G8z6pZ5rB0JU2aQwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1MzU0M1oXDTI5MDQyODE1MzU0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUIrLgixJJ
B5C4G8z6pZ5rB0JU2aQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBHiQJmzyFAaSYs8SpiRijIDZW2RIo7qBKb/pI3rqK6yOWDlPuMr6yNI81D
IrKGGftg4Z+2KETYU4x76HSf0s//vfH3QA57qFaAwddhKYy4BhteFQl/Wex3xTlX
LiwI07kwJvJy3mS6UfQ4HcvZy219tY+0iyOWrz/jVxwq7TOkCw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAJNKhJhaJOuMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA3Mjkx
MTM3MTdaGA8yMTk2MDEwMjExMzcxN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAhDUh6j1ACSt057nSxAcwMaGr8Ez87VA2RW2HyY8l9XoHndnxmP50Cqld
+26AJtltlqHpI1YdtnZ6OrVgVhXcVtbvte0lZ3ldEzC3PMvmISBhHs6A3SWHA9ln
InHbToLX/SWqBHLOX78HkPRaG2k0COHpRy+fG9gvz8HCiQaXCbWNFDHZev9OToNI
xhXBVzIa3AgUnGMalCYZuh5AfVRCEeALG60kxMMC8IoAN7+HG+pMdqAhJxGUcMO0
LBvmTGGeWhi04MUZWfOkwn9JjQZuyLg6B1OD4Y6s0LB2P1MovmSJKGY4JcF8Qu3z
xxUbl7Bh9pvzFR5gJN1pjM2n3gJEPwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAJ
UNKM+gIIHNk0G0tzv6vZBT+o/vt+tIp8lEoZwaPQh1121iw/I7ZvhMLAigx7eyvf
IxUt9/nf8pxWaeGzi98RbSmbap+uxYRynqe1p5rifTamOsguuPrhVpl12OgRWLcT
rjg/K60UMXRsmg2w/cxV45pUBcyVb5h6Op5uEVAVq+CVns13ExiQL6kk3guG4+Yq
LvP1p4DZfeC33a2Rfre2IHLsJH5D4SdWcYqBsfTpf3FQThH0l0KoacGrXtsedsxs
9aRd7OzuSEJ+mBxmzxSjSwM84Ooh78DjkdpQgv967p3d+8NiSLt3/n7MgnUy6WwB
KtDujDnB+ttEHwRRngX7
-----END CERTIFICATE-----
```

Canada Ouest (Calgary) – ca-ouest-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAYPouptUMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAMITzTJUa6cBsIfdHN69zW/
aHjUB4r1ZfKb1FMhIp9EZtEf5n+06oXjUG2+dKRSlFQeEK333ehNZsPd6uqey6TYKtHpFb5XRLS8BpqB
+7gnbAd0CBZM5o4NWesSQ1GLnTdQcGZkYG/
QESkbadoCXQTifCujJE682hTDLIVt1d4ewwCQYHKoZIzjgEAwMvADAsAhRJc4gRS/HWTkCR2MESaQEe/
jOMNQIUNoTwLvuPrmGPupPlGiHe0veZiO8=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAYPou9weMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
v4XBVH13ZCMgqlRHMqV8AWI5iO6gFn2A9sN3AZXTMqwtZeiDdebq3k6Wt7ieYvpXTg0qvgsjQIovRZWaBDBJy9x8C2hW
+w9lMQjFHkJ7Jy/
PHCJ69EzebQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAGe9Snkz1A6rHBH6/5kDtYvtPYwhx2sXNxztbhkXErFk40Nw5l4
gvDVtWG7qyb6fAqgoisyAbk8K9LzxSim2S1nmT9vD84B/t/VvwQBylc
+ej8kRxMH7fquZLp7IXfmtBzyUqu6Dpbne+chG2
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALyTn5IHrIZjMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMzEyMDcx
NTM3MDFaGA8yMjAzMDUxMzE1MzcwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA1GP5os424BJmGPCKOSgOclP7lzUiB85du03M4hfjzSOszsBpmBGFDLz1
owYHtIxlq3+Vi1Lt5Qlx3id/ov1QyaBPFWXVeklHVXy9vieCcI3TdjGjTl1W/8MM
m3X26QPcsnHM/Kk2wJ7s186MrqmdSsp3SCPpxv4vEG2Q9yR2bXY41hpc2rWlW8qU
D0JGXluvmmAdFnto20l1XWZ6xFen1h60DRugek/ufCbN+ljKy0xLqPoavH0Ybjsb
```

```
UpsAsBs7phaoN+X/5hIERfbp5LfVnqq54pNG5KNu4KynfW9+kA/WS4cJ6FTTN5t+
y0P1HvcL+BL2RuDy6T2bB21xw5WqtQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQURTvu/Dd4zDnmS5G5CfVLnmUBNOswgY4GA1UdIwSBhjCBg4AURTvu
/Dd4zDnmS5G5CfVLnmUBNOuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALyTn5IHrIZjMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFt523A3Aug6/F8xxyITgA8gkU0btFhlXNSP
U4U2OQ9n0tWI9WqnKNWH3KBxwY5EPitU6b3LM4xc9lDWpz7h2Pto+WhxP9LVKe6f
r8r7teTLCVZ7cfYZHzHg+flZjVpAgzE5BVfrRlj3QKpv0hYT3J1wMtI++Vorq5Nf
aPjzedehJLhmZVALwnfqfLrgv6/gmraP9Vmoa8U4D6AljNiQGYaLwyoPoRm3bUs2
v1Mh9GkEQ1b9+1pFXcqgzJJTGRuiPCyPbECI79FAnx5JM/CkGJV8HlOmjIW1qkK1
Y2qT7wzErrKLJyB53Pw15BdIM1onbDAQreZb0yZQLdoEl/tx7Uk=
-----END CERTIFICATE-----
```

Chine (Beijing) – cn-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIDCzCCAnSgAwIBAgIJALSOMbOoU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uhhUNlqAZdcWWB/OSDVDGk3OA99EFzOn/mJlmciQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+elKtJW/C0Sz/LYo60PUqd6iXF4h+upB9HkOOGuWHXsHBTsvgkgGA
1CGgel4U0Cdq+23eANr8N8m28UzljjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIGOBgNVHSME
gYYwgYOAFBkZu3wT27NnYgrfH+xJz4HJaNJooWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqmzll7e8Hgb
oADS0ph+YUz5P/bUCm61wFjlxaTfwKcuTR3ytj7bFLoW5Bm7Sa+TCl3lOGb2taon
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUeK+MRiWu+Oh5/lJGii3qw4YByx
SUDlRyNy1jJFstEZjOhs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAOtrM5XLDSjCMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQx
MDAxNDJaGA8yMTk1MDExNzEwMDE0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvVBz+WQNdPiM9S+aUULOQEriTmNDUrjLWLr7SfaOJScBzis5D5ju0jh1
+qJdkbuGKtFX5OTWTm8pWhInX+hIOoS3exC4BaANoa1A3o6quoG+Rsv72qQf8LLH
sgEi6+LMlCN9TwnRKOToEabmDKorss4zFl7VSsbQJwcBSfOcIwbdRRaW9Ab6uJHu
79L+mBR3Ea+G7vSDrVIA8goAPkae6jY9WGw9KxsOrcvNdQoEkqRVtHo4bs9fMRHU
Etphj2gh4ObXlFN92VtvzD6QBs3CcoFWgyWGvzg+dNG5VCbsiiuRdmii3kcijZ3H
Nv1wCcZoEAqH72etVhsuvNRC/xAP8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA8
ezx5LRjzUU9EYWYhyYIEShFlP1qDHs7F4L46/5lc4pL8FPoQm5CZuAF31DJhYi/b
fcV7i3n++/ymQbCLC6kAg8DUB7NrcROll5ag8d/JXGzcTCnlDXLXx1905fPNa+jI
0q5quTmdmiSi0taeaKZmyUdhrB+a7ohWdSdlokEIOtbH1P+g5yll3bI2leYE6Tm8
LKbyfK/532xJPqO9abx4Ddn89ZEC6vvWVNDgTsxERg992Wi+/xoSw3XxkgAryIv1
zQ4dQ6irFmXwCWJqc6kHg/M5W+z60S/94+wGTXmp+19U6Rkq5jVMLh16XJXrXwHe
4KcgIS/aQGVgjM6wivVA
-----END CERTIFICATE-----
```

Chine (Ningxia) – cn-northwest-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDCzCCAnSgAwIBAgIJALSOMbOoU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uhhUNlqAZdcWWB/OSDVDGk3OA99EFzOn/mJlmciQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+elKtJW/C0Sz/LYo60PUqd6iXF4h+upB9HkOOGuWHXsHBTsvgkgGA
1CGgel4U0Cdq+23eANr8N8m28UzljjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIGOBgNVHSME
gYYwgYOAFBkZu3wT27NnYgrfH+xJz4HJaNJooWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqmzll7e8Hgb
oADS0ph+YUz5P/bUCm61wFjlxaTfwKcuTR3ytj7bFLoW5Bm7Sa+TCl3lOGb2taon
```

```
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUeK+MRiWu+Oh5/lJGii3qw4YByx
SUDlRyNy1jJFstEZjOhs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPu4ssY3BlzcMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEyMDMy
MTI5MzJaGA8yMTk1MDUwODIxMjkzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAsOiGi4A6+YTLzCdIyP8b8SCT2M/6PGKwzKJ5XbSBoL3gsnSWiFYqPg9c
uJPNbiy9wSA9vlyfWMd90qvTfiNrT6vewP813QdJ3EENZOx4ERcf/Wd22tV72kxD
yw1Q3I1OMH4bOItGQAxU5OtXCjBZEEUZooOkU8RoUQOU2Pql4NTiUpzWacNutAn5
HHS7MDc4lUlsJqbN+5QW6fFrcNG/0Mrib3JbwdFUNhrQ5j+Yq5h78HarnUivnX/3
Ap+oPbentv1qd7wvPJu556LZuhfqI0TohiIT1Ah+yUdN5osoaMxTHKKtf/CsSJ1F
w3qXqFJQA0VWsqjFyHXFI32I/GOupwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCn
Um00QHvUsJSN6KATbghowLynHn3wZSQsuS8E0COpcFJFxP2SV0NYkERbXu0n/Vhi
yq5F8v4/bRA2/xpedLWmvFs7QWlomuXhSnYFkd33Z5gnXPb9vRkLwiMSw4uXls35
qQraczUJ9EXDhrv7VmngIk9H3YsxYrlDGEqh/oz4Ze4ULOgnfkauanHikk+BUEsg
/jsTD+7e+niEzJPihHdsvKFDlud5pakEzyxovHwNJ1GS2I//yxrJFIL91mehjqEk
RLPdNse7N6UvSnuXcOokwu6l6kfzigGkJBxkcq4gre3szZFdCQcUioj7Z4xtuTL8
YMqfiDtN5cbD8R8ojw9Y
-----END CERTIFICATE-----
```

Europe (Francfort) – eu-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
```

```
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFD5GsmkxRuecttwsCG763m3u63UwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1NTUyOVoXDTI5MDQyODE1NTUyOVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFD5Gsmkx
RuecttwsCG763m3u63UwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBBh0WaXlBsW56Hqk588MmJxsOrvcKfDjF57RgEDgnGnQaJcStCVWDO9UYO
JX2tdsPw+E7AjDqjsuxYaotLn3Mr3mK0sNOXq9BljBnWD4pARg89KZnZI8FN35HQ
O/LYOVHCknuPL123VmVRNs51qQA9hkPjvw21UzpDLxaUxt9Z/w==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAKD+v6LeR/WrMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTA4MTlaGA8yMTk1MDExNzA5MDgxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAka8FLhxs1cSJGK+Q+q/vTf8zVnDAPZ3U6oqppOW/cupCtpwMAQcky8DY
Yb62GF7+C6usniaq/9W6xPn/3o//wti0cNt6MLsiUeHqNl5H/4U/Q/fR+GA8pJ+L
npqZDG2tFi1WMvvGhGgIbScrjR4VO3TuKy+rZXMYvMRk1RXZ9gPhk6evFnviwHsE
jV5AEjxLz3duD+u/SjPp1vloxe2KuWnyC+EKInnka909sl4ZAUh+qIYfZK85DAjm
```

```
GJP4W036E9wTJQF2hZJrzsiB1MGyC1WI9veRISd30izZZL6VVXLXUtHwVHnVASrS
zZDVpzj+3yD5hRXsvFigGhY0FCVFnwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUxC2l6pvJaRflgu3MUdN6zTuP6YcwgY4GA1UdIwSBhjCBg4AUxC2l
6pvJaRflgu3MUdN6zTuP6YehYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAKD+v6LeR/WrMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAIK+DtbUPppJXFqQMv1f2Gky5/82ZwgbbfXa
HBeGSii55b3tsyC3ZW5ZlMJ7Dtnr3vUkiWbV1EUaZGOUlndUFtXUMABCb/coDndw
CAr53XTv7UwGVNe/AFO/6pQDdPxXn3xBhF0mTKPrOGdvYmjZUtQMSVb9lbMWCFfs
w+SwDLnm5NF4yZchIcTs2fdpoyZpOHDXy0xgxO1gWhKTnYbaZOxkJvEvcckxVAwJ
obF8NyJla0/pWdjhlHafEXEN8lyxyTTyOa0BGTuYOBD2cTYYynauVKY4fqHUkr3v
Z6fboaHEd4RFamShM8uvSu6eEFD+qRmvqlcodbpsSOhuGNLzhOQ=
-----END CERTIFICATE-----
```

Europe (Irlande) – eu-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUakDaQ1Zqy87Hy9ESXA1pFC116HkwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
```

```
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MTgxMFoXDTI5MDQyODE2MTgxMFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUakDaQ1Zq
y87Hy9ESXA1pFC116HkwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQADIkn/MqaLGPuK5+prZZ5Ox4bBZLPtreO2C7r0pqU2kPM2lVPyYYydkvP0
lgSmmsErGu/oL9JNztDe2oCA+kNy17ehcsf8cw0uP861czNFKCeU8b7FgBbL+sIm
qi33rAq6owWGi/5uEcfCR+JP7W+oSYVir5r/yDmWzx+BVH5S/g==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOrmqHuaUt0vMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTA2MTlaGA8yMTk1MDQwMzA5MDYxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjE7nVu+aHLtzp9FYV25Qs1mvJ1JXD7J0iQ1Gs/RirW9a5ZECCtc4ssnf
zQHq2JRVr0GRchvDrbm1HaP/avtFQR/Thvfltwu9AROVT22dUOTvERdkNzveoFCy
hf52Rqf0DMrLXG8ZmQPPXPDFAv+sVMWCDftcChxRYZ6mP9O+TpgYNT1krD5PdvJU
7HcXrkNHDYqbsg8A+Mu2hzl0QkvUET83Csg1ibeK54HP9w+FsD6F5W+6ZSHGJ88l
FI+qYKs7xsjJQYgXWfEt6bbckWs1kZIaIOyMzYdPF6ClYzEec/UhIe/uJyUUNfpT
VIsI5OltBbcPF4c7Y20jOIwwI2SgOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUF2DgPUZivKQR/Zl8mB/MxIkjZDUwgY4GA1UdIwSBhjCBg4AUF2Dg
PUZivKQR/Zl8mB/MxIkjZDWhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOrmqHuaUt0vMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGm6+57W5brzJ3+T8/XsIdLTuiBSe5ALgSqI
qnO5usUKAeQsa+kZIJPyEri5i8LEodh46DAF1RlXTMYgXXxl0YggX88XPmPtok17
l4hib/D9/lu4IaFIyLzYNSzsETYWKWoGVe7ZFz60MTRTwY2u8YgJ5dec7gQgPSGj
avB0vTIgoW41G58sfw5b+wjXCsh0nROon79RcQFFhGnvup0MZ+JbljyhZUYFzCli
31jPZiKzqWa87xh2DbAyvj2KZrZtTe2LQ48Z4G8wWytJzxEeZdREe4NoETf+Mu5G
4CqoaPR05KWkdNUdGNwXewydb3+agdCgfTs+uAjeXKNdSpbhMYg=
-----END CERTIFICATE-----
```

Europe (Londres) – eu-west-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUCgCV/DPxYNND/swDgEKGiC5I+EwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MjkxNFoXDTI5MDQyODE2MjkxNFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUCgCV/DPx
YNND/swDgEKGiC5I+EwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQATPu/sOE2esNa4+XPEGKlEJSgqzyBSQLQc+VWo6FAJhGG9fp7D97jhHeLC
5vwfmtTAfnGBxadfAOT3ASkxnOZhXtnRna460LtnNHm7ArCVgXKJo7uBn6ViXtFh
uEEw4y6p9YaLQna+VC8Xtgw6WKq2JXuKzuhuNKSFaGGw9vRcHg==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANBx0E2bOCEPMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA4MTEx
NDU2NDJaGA8yMTk2MDExNTE0NTY0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArYS3mJLGaMrh2DmiPLbqr4Z+xWXTzBWCjOwpsuHE9H6dWUUyl2Bgnu+Z
d8QvW306Yleec45M4F2RA3J4hWHtShzsMlOJVRt+YulGeTf9OCPr26QmIFfs5nD4
fgsJQEry2MBSGA9Fxq3Cw6qkWcrOPsCR+bHOU0XykdKl0MnIbpBf0kTfciAupQEA
dEHnM2J1L2iI0NTLBgKxy5PXLH9weX20BFauNmHH9/J07OpwL20SN5f8TxcM9+pj
Lbk8h1V4KdIwVQpdWkbDL9BCGlYjyadQJxSxz1J343NzrnDM0M4h4HtVaKOS7bQo
Bqt2ruopLRCYgcuFHck/1348iAmbRQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBG
wujwU1Otpi3iBgmhjMClgZyMMn0aQIxMigoFNqXMUNx1Mq/e/Tx+SNaOEAu0n2FF
aiYjvY0/hXOx75ewzZvM7/zJWIdLdsgewpUqOBH4DXFhbSk2TxggSPb0WRqTBxq5
Ed7F7+7GRIeBbRzdLqmISDnfqey8ufW0ks51XcQNomDIRG5s9XZ5KHviDCar8FgL
HngBCdFI04CMagM+pwTO9XN1Ivt+NzUj208ca3oP1IwEAd5KhIhPLcihBQA5/Lpi
h1s3170z1JQ1HZbDrH1pgp+8hSI0DwwDVb3IIH8kPR/J0Qn+hvOl2HOpaUg2Ly0E
pt1RCZe+W7/dF4zsbqwK
-----END CERTIFICATE-----
```

Europe (Milan) – eu-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAqwCCQCMElHPdwG37jAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA0MjkyMDM1MjJaFw00
NTA0MjkyMDM1MjJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQDAkoL4YfdMI/MrQ0oL
NPfeEk94eiCQA5xNOnU7+2eVQtEqjFbDADFENh1p3sh9Q9OoheLFH8qpSfNDWn/0
ktCS909ApTY6Esx1ExjGSeQq/U+SC2JSuuTT4WFMKJ63a/czMtFkEPPnVIjJJJmT
HJSKSsVUgpdDIRvJXuyB0zdB+wIVALQ3OLaVGdlPMNfS1nD/Yyn+32wnAoGAPBQ3
7XHg5NLOS4326eFRUT+4ornQFjJjP6dp3pOBEzpImNmZTtkCNNUKE4Go9hv5T4lh
R0pODvWv0CBupMAZVBP9ObplXPCyEIZtuDqVa7ukPOUpQNgQhLLAqkigTyXVOSmt
ECBj9tu5WNP/x3iTZTHJ+g0rhIqpgh012UwJpKADgYQAAoGAV1OEQPYQUg5/M3xf
```

```
6vE7jKTxxyFWEyjKfJK7PZCzOIGrE/swgACy4PYQW+AwcUweSlK/Hx2OaZVUKzWo
wDUbeu65DcRdw2rSwCbBTU342sitFo/iGCV/Gjf+BaiAJtxniZze7J1ob8vOBeLv
uaMQmgOYeZ5e0fl04GtqPl+lhcQwCQYHKoZIzjgEAwMwADAtAhQdoeWLrkm0K49+
AeBK+j6m2h9SKQIVAIBNhS2a8cQVABDCQXVXrc0tOmO8
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAOZ3GEIaDcugMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTEwMjQx
NTE5MDlaGA8yMTk5MDMyOTE1MTkwOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCjiPgW3vsXRj4JoA16WQDyoPc/eh3QBARaApJEc4nPIGoUolpAXcjFhWplo2O+
ivgfCsc4AU9OpYdAPha3spLey/bhHPRi1JZHRNqScKP0hzsCNmKhfnZTIEQCFvsp
DRp4zr91/WS06/flJFBYJ6JHhp0KwM81XQG59lV6kkoW7QIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAGLLrY3P+HH6C57dYgtJkuGZGT2+rMkk2n81/abzTJvsqRqGRrWv
XRKRXlKdM/dfiuYGokDGxiC0Mg6TYy6wvsR2qRhtXW1OtZkiHWcQCnOttz+8vpew
wx8JGMvowtuKB1iMsbwyRqZkFYLcvH+Opfb/Aayi20/ChQLdI6M2R5VU
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAO/+DgYF78KwMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA0Mjky
MDM1MjJaGA8yMTk4MTAwMjIwMzUyMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAv1ZLV+Z/P6INq+R1qLkzETBg7sFGKPiwHekbpuB6lrRxKHhj8V9vaReM
lnv1Ur5LAPpMPYDsuJ4WoUbPYAqVqyMAo7ikJHCCM1cXgZJefgN6z9bpS+uA3YVh
V/0ipHh/X2hc2S9wvxKWiSHu6Aq9GVpqL035tJQD+NJuqFd+nXrtcw4yGtmvA6wl
5Bjn8WdsP3xOTKjrByYY1BhXpP/f1ohU9jE9dstsRXLa+XTgTPWcWdCS2oRTWPGR
c5Aeh47nnDsyQfP9gLxHeYeQItV/BD9kU/2Hn6mnRg/B9/TYH8qzlRTzLapXp4/5
iNwusrTNexGl8BgvAPrfhjDpdgYuTwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB7
5ya11K/hKgvaRTvZwVV8GlVZt0CGPtNvOi4AR/UN6TMm51BzUB5nurB4z0R2MoYO
Uts9sLGvSFALJ4otoB77hyNpH3drttU1CVVwal/yK/RQLSon/IoUkaGEbqalu+mH
nYad5IG4tEbmepX456XXcO58MKmnczNbPyw3FRzUZQtI/sf94qBwJ1Xo6XbzPKMy
xjL57LHIZCssD+XPifXay69OFlsCIgLim11HgPkRIHEOXLSf3dsW9r+4CjoZqB/Z
jj/P4TLCxbYCLkvglwaMjgEWF40Img0fhx7yT2X92MiSrs3oncv/IqfdVTiN8OXq
```

```
jgnq1bf+EZEZKvb6UCQV
-----END CERTIFICATE-----
```

Europe (Paris) – eu-west-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUaC9fX57UDr6u1vBvsCsECKBZQyIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MzczOFoXDTI5MDQyODE2MzczOFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUaC9fX57U
```

```
Dr6u1vBvsCsECKBZQyIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCARv1bQEDaMEzYI0nPlu8GHcMXgmgA94HyrXhMMcaIlQwocGBs6VILGVhM
TXP2r3JFaPEpmXSQNQHvGA13clKwAZbni8wtzv6qXb4L4muF34iQRHF0nYrEDoK7
mMPR8+oXKKuPO/mv/XKo6XAV5DDERdSYHX5kkA2R9wtvyZjPnQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALWSfgHuT/ARMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA1MzEx
MTE4MTZaGA8yMTk2MTEwMzExMTgxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy5V7KDqnEvF3DrSProFcgu/oL+QYD62b1U+Naq8aPuljJe127Sm9WnWA
EBdOSASkOaQ9fzjCPoG5SGgWKxYoZjsevHpmzjVv9+Ci+F57bSuMbjgUbvbRIFUB
bxQojVoXQPHgK5v433ODxkQ4sjRyUbf4YV1AFdfU7zabC698YgPVOExGhXPlTvco
8mlc631ubw2g52j0lzaozUkHPSbknTomhQIvO6kUfX0e0TDMH4jLDG2ZIrUB1L4r
OWKG4KetduFrRZyDHF6ILZu+s6ywiMicUd+2UllDFC6oas+a8D11hmO/rpWU/ieV
jj4rWAFrsebpn+Nhgy96iiVUGS2LuQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDE
iYv6FQ6knXCg+svlcaQG9q59xUC5z8HvJZ1+SxzPKKC4PKQdKvIIfE8GxVXqlZG1
cl5WKTFDMapnzb9RV/DTaVzWx3cMYT77vm1Hl1XGjhx611CGcENH1egI3lOTILsa
+KfopuJEQQ9TDMAIkGjhA+KieU/U5Ctv9fdej6d0GC6OEuwKkTNzPWue6UMq8d4H
2xqJboWsE1t4nybEosvZfQJcZ8jyIYcYBnsG13vCLM+ixjuU5MVVQNMY/gBJzqJB
V+U0QiGiuT5cYgY/QihxdHt99zwGaE0ZBC7213NKrlNuLSrqhDI2NLu8NsExqOFy
OmY0v/xVmQUQl26jJXaM
-----END CERTIFICATE-----
```

Europe (Espagne) – eu-south-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAq
+gAwIBAgIGAXjwLk46MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAGG2m8EKmaf5qQqj3Z
```

```
+rzSaTaXE3B/R/4A2VuGqRYR7MljPtwdmU6/3CPjCACcZmTIcOAKbFiDHqadQgBZXfzGpzw8Zo
+eYmmk5fXycgnj57PYH1dIWU6I7mCbAah5MZMcmHaTmIsomGrhcnWB8d8qOU7oZ0UWK4lbiAQs1MihoUwCQYHKoZIzjg
WmbaU7YM5GwCFCvIJOesO5hZ8PHC52dAR8WWC6oe
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjwLkiaMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
VvR1+45Aey5zn3vPk6xBm5o9grSDL6D2iAuprQnfVXn8CIbSDbWFhA3fi5ippjKkh3sl8VyCvCOUXKdOaNrYBrPRkrdH
+3m/
rxIUZ2IK1fDlC6sWAjddf6sBrV2w2a78H0H8EwuwiSgttURBjwJ7KPPJCqaqrQIDAQABMA0GCSqGSIb3DQEBBQUAA4GB
+FzqQDzun/
iMMzcFucmLMl5BxEblrFXOz7IIuOeiGkndmrqUeDCykztLku45s7hxdNy4ltTuVAaE5aNBdw5J8U1mRvsKvHLy2ThH6h
+hBgiphYp84DUbWVYeP8YqLEJSqscKscWC
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALWSmO6DvSpQMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTgx
MzU4NDNaGA8yMjAxMTIyMjEzNTg0M1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAuAAhuSpsHC00/fD2zNlBDpNLRndi9qbHsNeuz3WqN7Samj2aSrM2hS+i
hUxx0BspZj0tZCOsbpPZ+i74NOEQtFeqQoEGvKhB1nJiF4y5I81HDhs5qHvoIivm
7rbbik3zgm1PqS/DmDjVQaXPcD31Rd9ILwBmWEwJqHigyNVlxYtCzTQcrlBrvNZM
dnNgCDAdX/HBEFxx9O12xeu0bSt0s+PJWZ1RTbYrNe7LIH6ntUqHxP/ziQ5trXEZ
uqy7aWk1L8uK4jmyNph0lbaqBa3Y6pYmU1nC27UE4i3fnPB0LSiAr+SrwVvX1g4z
ilo8kr+tbIF+JmcgYLBvO8Jwp+EUqQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUwvGzKJL9A5LReJ4Fxo5K6I20xcowgY4GA1UdIwSBhjCBg4AUwvGz
KJL9A5LReJ4Fxo5K6I20xcqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALWSmO6DvSpQMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAJAZd31jyoTGLawAD2+v/vQsaB9vZIx5EImi
G8YGkd61uFWeNhAmtrwyE/i6FDSIphDrMHBkvw/D3BsqK+Ev/JOK/VYuaYDx/8fp
H4cwp9jC57CXzdIDREWNf6M9PsHFg2WA9XNNtClOZL5WJiJwel8eDSg+sqJUxE0l
MW+QChq/20F6niyaRK4bXrZq14as7h+F9u3A9xHEOVP7Zk9C2ehrBXzCMLSDt3GV
fEuMea2RxMhozwz34Hkdb6j18qoCfygubulovRNQjKw/cEmgPR16KfZPP5caILVt
9qkYPvePmbiVswZDee73cDymJYxLqILpOZwyXvUH8StiH42FHZQ=
-----END CERTIFICATE-----
```

Europe (Stockholm) – eu-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUN1c9U6U/xiVDFgJcYKZB4NkH1QEwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MDYwM1oXDTI5MDQyODE2MDYwM1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUN1c9U6U/
xiVDFgJcYKZB4NkH1QEwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBTIQdoFSDRHkpqNPUbZ9WXR2O5v/9bpmHojMYZb3Hw46wsaRso7STiGGX/
tRqjIkPUIXsdhZ3+7S/RmhFznmZc8e0bjU4n5vi9CJtQSt+1u4E17+V2bF+D3h/7
wcfE0l3414Q8JaTDtfEf/aF3F0uyBvr4MDMd7mFvAMmDmBPSlA==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALc/uRxg++EnMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
NDAwMTFaGA8yMTk3MDkxMzE0MDAxMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzwCGJEJIxqtr2PD2a1mA6LhRzKhTBa1AZsg3eYfpETXIVlrpojMfvVoN
qHvGshWLgrGTT6os/3gsaADheSaJKavxwX3X6tJA8fvEGqr3a1C1MffH9hBWbQqC
LbfUTAbkwis4GdTUwOwPjT1Cm3u9R/VzilCNwkj7iQ65AFAI8Enmsw3UGldEsop4
yChKB3KW3WI0FTh0+gD0YtjrqqYJxpGOYBpJp5vwdd3fZ4t1vidmDMs7liv4f9Bx
p0oSmUobU4GUlFhBchK1DukICVQdnOVzdMonYm7s+HtpFbVHR8yf6QoixBKGdSal
mBf7+y0ixjCn0pnC0VLVooGo4mi17QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDG
4ONZiixgk2sjJctwbyD5WKLTH6+mxYcDw+3y/F0fWz561YORhP2FNnPOmEkf0Sl/
Jqk4svzJbCbQeMzRoyaya/46d7UioXMHRZam5IaGBhOdQbi97R4VsQjwQj0RmQsq
yDueDyuKTwWLK9KnvI+ZA6e6bRkdNGflK4N8GGKQ+fBhPwVELkbT9f16OJkezeeN
S+F/gDADGJgmPXfjogICb4Kvshq0H5Lm/xZlDULF2g/cYhyNY6EOI/eS5m1I7R8p
D/m6WoyZdpInxJfxW616OMkxQMRVsruLTNGtby3u1g6ScjmpFtvAMhYejBSdzKG4
FEyxIdEjoeO1jhTsck3R
-----END CERTIFICATE-----
```

Europe (Zurich) – eu-central-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXiKJnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAYNjaCNg/
cfgQOOl1BUj5ClUulqwZ9Q+SfDzPZh9D2C0VbiRANiZoxrV8RdgmzzC5T7VcriVwjwvta2Ch//
b+sZ86E5h0XWWr+BeEjD9cu3eDj12XB5sWEbNHNx49p5Tmtu5r2LDtlL8X/
Rpfalu2Z2OJgjFJWGf7hRwxe456n
+lowCQYHKoZIzjgEAwMvADAsAhRChsLcj4U5CVb2cp5M0RE1XbXmhAIUeGSnH+aiUQIWmPEFja+itWDufIk=
```

```
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjSGFGiMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
opKZAUusJx2hpgU3pUHhlp9ATh/VeVD582jTd9IY
+8t5MDa6Z3fGliByEiXz0LEHdi8MBacLREu1TwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAILlpoE3k9o7KdALAxsFJNit
+g3RMzdbiFM+7MA63Nv5fsf+0xgcjSNBElvPCDKFvTJl4QQhToy056llO5GvdS9RK
+H8xrP2mrqngApoKTApv93vHBixgFSn5KrczRO0YSm3OjkqbydU7DFlmkXXR7GYE+5jbHvQHYiT1J5sMu
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALvT012pxTxNMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTgx
NTEyMDdaGA8yMjAxMTIyMjE1MTIwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAyn+Lsnq1ykrfYlZkk6aAAYNReNd9Iw8AUwCBkgOr2eBiBBepYxHwU85N
++moQ+j0EV2VaahBeTLShGZZS1HsyK8+cYT2QzpghIoamcYhrPXyIxlWiRQlaqSg
OFiE9bsqL3rCF5Vz+tOiTe5W/7ojfOFls6++g7ZpobwJlpMbuJepqyeHMPyjvO5A
age81lJewc4bxo2ntaW0HCqNksqfYB78j6X6kn3PFpX7FaYAwZA+Xx6C7UCY7rNi
UdQzfAo8htfJi4chz7frpUdQ9kl3IOQrsLshBB5fFUjl09NiFipCGBwi+8ZMeSn1
5qwBI01BWXPfG7WX6Owyjhmh6JtE1wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU8HN4vvJrsZgPQeksMBgJb9xR1yYwgY4GA1UdIwSBhjCBg4AU8HN4
vvJrsZgPQeksMBgJb9xR1yahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALvT012pxTxNMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGlHYDtcHpfBvdHx9HeQE8HgNugJUPdEqxun
t9U33p8VFrs+uLPtrOd9HDJEGvvs5h84EUie/oGJxRt7V1Vlid1PvHf6cRmpjgqY
YdggAVkZtY/PnFVmzf2bMVlSQPrqCl7U0zaw2Kvnj4zgX0rZyCetgrRZSUSxotyp
978Wy9ccXwVSeYG/YAr5rJpS6ZH7eRQvUY0IzwFNeaOPgOTEVpcjWlV6+MQEvsEx
W85q+s6AVr49eppEx8SLJsl0C23yB+L+t32tAveQImRWtJMpzZ5cxh/sYgDVeoC0
85H1NK/7H9fAzT1cPu1oHSnB0xYzzHGOAmXmusMfwUk8fL1RQkE=
-----END CERTIFICATE-----
```

Israël (Tel Aviv) – il-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq+gAwIBAgIGAX0QPi
+9MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcMB1NlYX
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAbazCL5XXyPmcw3+oMYQUF5/9YogW6D0FZbYuyPgjOoUwWdl6fjlzWca
pq+l1ezuK2DFOzNTEyPEwwCQYHKoZIzjgEAwMvADAsAhRt1jkpXsvrS
+xTo2M9h2s2uLAhEQIUOZ2FcnTSrshF2EIdixZZwtNv66Q=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAX0QQGVLMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+S8vOy5hpLoRe4RkOrY0cM3bN07GdEMlin5mU0y1t8y3ct4YewvmkgT42kTyMM
+t1K4S0xsqjXxxS716uGYh7eWtkxrCihj8AbXN/6pa095h
+7TZyl2n83keiNUzM2KoqQVMwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBADwA6VVEIIZD2YL00F12po40xDLzIc9XvqFPS
FmU7H8s62/jD6cOR1A1cClIyZUe1yT1ZbPySCs43J+Thr8i8FSRxzDBSZZi5foW
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOVp1h2I9wW7MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTUx
MjQ0MTJaGA8yMjAxMTIxOTEyNDQxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA13PkyWvl61iV/SYfO1UFO76UpDfPm2SF/Rz/o33cm699X++EYPxTnoEc
vmWeS0I7eDXc4OCUiToG0sEx0klE0CX1Z1tK6qJ+zgWQLZ9SZEC9H0NsSA6LhrHu
Nq0dzeK3LjhdfcX46/4GqdiptpdTuM4m/hOQ5yx4JMQ/n1sdpv4M5VLRWwWW9Lem
ufb79Id7O9SispxgRsz1KXIjp7N9S4BY7itSXz97uSyzTqEjWZ6mDUhTu3t21GKC
6flALGTTrG2yghEhz53rkvLsvwzjPSSlT6LIf0mrRPzHaf+EdaKoasElE1SHh+ZH
9mI81HywpE+HZ+W+5hBCvjYp90Y1fwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
```

```
BgNVHQ4EFgQU58tN2JO+yEGq5JbIXxGi4vRVPyIwgY4GA1UdIwSBhjCBg4AU58tN
2JO+yEGq5JbIXxGi4vRVPyKhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOVp1h2I9wW7MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANBN0e1EqNy4+IU2yQzMJ+Wy5ZIOtTP6GSBR
7muVY1bDeAwtNTEOpwgrZVlC7/xq5Q0LC1y0Z70hHXEf8au7qStaAoUtxzvhTAZI
NC0lwoFU56UFw4N0vZII17iqEfoqRC4PpI3OxqEJHFy0VLlvAzJoKB4QLLqDAYVA
LXCiOLoVT+y9tRYsxw5MyO0Bi6fxQIIADl2bE9xkunTN1Jkkwqo3LxNy/ryz4QWR
8K7jHUItifv4h/hxBKpHEquN8CkdvM9oeGl7I8PFrSFEpGr1euDXY0euZzzYiDBV
m6GpTJgzpVsEuIX52dPcPemwQncoIfZyhWDW85MJUnby2WTEcFo=
-----END CERTIFICATE-----
```

Moyen-Orient (Bahreïn) – me-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7jCCAq4CCQCVWIgSmP8RhTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDUxMzA2MjFaFw00
NTAyMDUxMzA2MjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDcwojQfgWdV1QliO0B
8n6cLZ38VE7ZmrjZ9OQV//Gst6S1h7euhC23YppKXi1zovefSDwFU54zi3/oJ++q
PHlP1WGL8IZ34BUgRTtG4TVolvp0smjkMvyRu5hIdKtzjV93Ccx15gVgyk+o1IEG
fZ2Kbw/Dd8JfoPS7KaSCmJKxXQIVAIZbIaDFRGa2qcMkW2HWASyNDl7bAoGBANtz
IdhfMq+l2I5iofY2oj3HI21Kj3LtZrWEg3W+/4rVhL3lTm0Nne1rl9yGujrjQwy5
Zp9V4A/w9w2O10Lx4K6hj34Eefy/aQnZwNdNhv/FQP7Az0fju+Yl6L13OOHQrL0z
Q+9cF7zEosekEnBQx3v6psNknKgD3Shgx+GO/LpCA4GFAAKBgQCVS7m77nuNAlZ8
wvUqcooxXMPkxJFl54NxAsAul9KP9KN4svm0O3Zrb7t2FOtXRM8zU3TqMpryq1o5
mpMPsZDg6RXo9BF7Hn0DoZ6PJTamkFA6md+NyTJWJKvXC7iJ8fGDBJqTciUHuCKr
12AztQ8bFWsrTgTzPE3p6U5ckcgV1TAJBgcqhkjOOAQDAy8AMCwCFB2NZGWm5EDl
86ayV3c1PEDukgQIAhQow38rQkN/VwHVeSW9DqEshXHjuQ==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDPDCCAqWgAwIBAgIJAMl6uIV/zqJFMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0dGxlMSAw
HgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwRZWMyLmFt
YXpvbmF3cy5jb20wIBcNMTkwNDI2MTQzMjQ3WhgPMjE5ODA5MjkxNDMyNDdaMHIx
```

```
CzAJBgNVBAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0
dGxlMSAwHgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwR
ZWMyLmFtYXpvbmF3cy5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALVN
CDTZEnIeoX1SEYqq6k1BV0ZlpY5y3KnoOreCAE589TwS4MX5+8Fzd6AmACmugeBP
Qk7Hm6b2+g/d4tWycyxLaQlcq81DB1GmXehRkZRgGeRge1ePWd1TUA0I8P/QBT7S
gUePm/kANSFU+P7s7u1NNl+vynyi0wUUrw7/wIZTAgMBAAGjgdcwgdQwHQYDVR0O
BBYEFILtMd+T4YgH1cgc+hVsVOV+480FMIGkBgNVHSMEgZwwgZmAFILtMd+T4YgH
1cgc+hVsVOV+480FoXakdDByMQswCQYDVQQGEwJVUzETMBEGA1UECAwKV2FzaGlu
Z3RvbjEQMA4GA1UEBwwHU2VhdHRsZTEgMB4GA1UECgwXQW1hem9uIFdlYiBTZXJ2
aWNlcyBMTEMxGjAYBgNVBAMMEWVjMi5hbWF6b25hd3MuY29tggkAyXq4hX/OokUw
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOBgQBhkNTBIFgWFd+ZhC/LhRUY
4OjEiykmbEp6hlzQ79T0Tfbn5A4NYDI2icBP0+hmf6qSnIhwJF6typyd1yPK5Fqt
NTpxxcXmUKquX+pHmIkK1LKDO8rNE84jqxrxRsfDi6by82fjVYf2pgjJW8R1FAw+
mL5WQRFexbfB5aXhcMo0AA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANZkFlQR2rKqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTAyMDUx
MzA2MjBaGA8yMTk4MDcxMTEzMDYyMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy4Vnit2eBpEjKgOKBmyupJzJAiT4fr74tuGJNwwa+Is2vH12jMZn9Il1
UpvvEUYTIboIgISpf6SJ5LmV5rCv4jT4a1Wm0kjfNbiIlkUi8SxZrPypcw24m6ke
BVuxQZrZDs+xDUYIZifTmdgD50u5YE+TLg+YmXKnVgxBU6WZjbuK2INohi71aPBw
2zWUR7Gr/ggIpf635JLU3KIBLNEmrkXCVSnDFlsK4eeCrB7+UNak+4BwgpuykSGG
Op9+2vsuNqFeU1l9daQeG9roHR+4rIWSPa0opmMxv5nctgypOrE6zKXx2dNXQldd
VULv+WH7s6Vm4+yBeG8ctPYH5GOo+QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBs
ZcViiZdFdpcXESZP/KmZNDxB/kktlIEIhsQ+MNn29jayE5oLmtGjHj5dtA3XNKlr
f6PVygVTKbtQLQqunRT83e8+7iCZMKI5ev7pITUQVvTUwI+Fc01JkYZxRFlVBuFA
WGZO+98kxCS4n6tTwVt+nSuJr9BJRVC17apfHBgSS8c5OWna0VU/Cc9ka4eAfQR4
7pYSDU3wSRE01cs30q34lXZ629IyFirSJ5TTOIc0osNL7vwMQYj8HOn4OBYqxKy8
ZJyvfXsIPh0Na76PaBIs6ZlqAOflLrjGzxBPiwRM/XrGmF8ze4KzoUqJEnK13O6A
KHKgfiigQZ1+gv5FlyXH
-----END CERTIFICATE-----
```

Moyen-Orient (UAE) — me-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXhqnnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAW+csuHsWp/7/
pv8CTKFwxsYudxuR6rbWaHCykIeAydXL9AWnphK6yp1ODEMBFl68Xq8Hp23sOWyf8moOhqCom9+0+ovuUFdpvCie86bp
TOZU568Ty1ff3dDWbdRzeNQRHodRG+XEQSizMkAreeWt4kBa+PUwCQYHKoZIzjgEAwMvADAsAhQD3Z
+XGmzKmgaLgGcVX/Qf1+Tn4QIUH1cgksBSVKbWj81tovBMJeKgdYo=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjRrnDjMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
KyA6zyruJQrYy00a6wqLA7eeUzk3bMiTkLsTeDQfrkaZMfBAjGaaOymRo1C3qzE4rIenmahvUplu9ZmLwL1idWXMRX2R
+d2SeoKOKQWoc2UOFZMHYxDue7zkyk1CIRaBukTeY13/
RIrlc6X61zJ5BBtZXlHwayjQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBABTqTy3R6RXKPW45FA+cgo7YZEj/
Cnz5YaoUivRRdX2A83BHuBTvJE2+WX00FTEj4hRVjameE1nENoO8Z7fUVloAFDlDo69fhkJeSvn51D1WRrPnoWGgEfr1
B+Wqm3kVEz/QNcz6npmA6
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM4h7b1CVhqqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MTEx
MDE1MDNaGA8yMjAxMDkxNTEwMTUwM1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApybTWfMOhSoMpqPo72eqAmnn1dXGZM+G8EoZXzwHwT/+IHEXNB4q5N6k
tudYLre1bJxuzEw+iProSHjmb9bB9YscRTofjVhBlt35Fc+i8BaMeH94SR/eE8QO
mll8gnLNW3d62lyuhzuyv1e5wVlRqzYw+X2zRH4/wRDOCOpzjKoHIgyPKsMgwsw5
aTZhNMsGxZN9dbkf0iCGeQLDytwU/JTh/HqvSr3VfUOapTJJiyAxoCtZWgp1/7wC
RvOCSMRJobpUqxZgl/VsttwNkikSFz1wGkcYeSQvk+odbnYQckA8tdddoVI56eD4
```

```
qtREQvfpMAX5v7fcqLexl5d5vH8uZQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUOadrbTs+OhzwoAgUJ7RqQNdwufkwgY4GA1UdIwSBhjCBg4AUOadr
bTs+OhzwoAgUJ7RqQNdwufmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM4h7b1CVhqqMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAICTdAOGEOnII8HaGCpCB8us/hGFaLptJaAf
D5SJAyVy66/mdfjGzE1BKkKxnbxemEVUIzbRidOnyilB+pKwN3edAjTZtWdpVA0V
R/G/qQPmcVljtycBz4VC6SuOUYflGzLH1GZ6GJWbuDtFzw8r7HGdRN1wrEPe3UF2
sMpuVezqnRUdvVRoVQP4jFgNsE7kNvtn2NiPhb/CtrxpcwIQ7r6YeoHcBSheuV1Z
xZDHynC3KUprQGx1+Z9QqPrDf180MaoqAlTl4+W6Pr2NJYrVUFGS/ivYshMg574l
CPU6r4wWZSKwEUXq4BInYX6z6iclp/p/J5QnJp2mAwyi6M+I13Y=
-----END CERTIFICATE-----
```

Amérique du Sud (São Paulo) – sa-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUX4Bh4MQ86Roh37VDRRX1MNOB3TcwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
```

```
MB4XDTI0MDQyOTE2NDYwOVoXDTI5MDQyODE2NDYwOVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUX4Bh4MQ8
6Roh37VDRRX1MNOB3TcwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBnhocfH6ZIX6F5K9+Y9V4HFk8vSaaKL5ytw/P5td1h9ej94KF3xkZ5fyjN
URvGQv3kNmNJBoNarcP9I7JIMjsNPmVzqWawyCEGCZImoARxSS3Fc5EAs2PyBfcD
9nCtzMTaKO09Xyq0wqXVYn1xJsE5d5yBDsGrzaTHKjxo61+ezQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMcyoxx4U0xxMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU4MDJaGA8yMTk1MDExNzA4NTgwMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAw45IhGZVbQcy1fHBqzROhO8CsrDzxj/WP4cRbJo/2DAnimVrCCDs5O86
FA39Zo1xsDuJHDlwMKqeXYXkJXHYbcPWc6EYYAnR+PlLG+aNSOGUzsy202S03hT0
B20hWPCqpPp39itIRhG4id6nbNRJOzLm6evHuepMAHR4/OV7hyGOiGaV/v9zqiNA
pMCLhbh2xk0PO35HCVBuWt3HUjsgeks2eEsu9Ws6H3JXTCfiqp0TjyRWapM29OhA
cRJfJ/d/+wBTz1fkWOZ7TF+EWRIN5ITEadlDTPnF1r8kBRuDcS/lIGFwrOOHLo4C
cKoNgXkhTqDDBDu6oNBb2rS0K+sz3QIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUqBy7D847Ya/w321Dfr+rBJGsGTwwgY4GA1UdIwSBhjCBg4AUqBy7
D847Ya/w321Dfr+rBJGsGTyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMcyoxx4U0xxMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACOoWSBf7b9AlcNrl4lr3QWWSc7k90/tUZal
PlT0G3Obl2x9T/ZiBsQpbUvs0lfotG0XqGVVHcIxF38EbVwbw9KJGXbGSCJSEJkW
vGCtc/jYMHXfhx67Szmftm/MTYNvnzsyQQ3v8y3Rdah+xe1NPdpFrwmfL6xe3pFF
cY33KdHA/3PNLdn9CaEsHmcmj3ctaaXLFIzZhQyyjtsrgGfTLvXeXRokktvsLDS/
YgKedQ+jFjzVJqgr4NjfY/Wt7/8kbbdhzaqlB5pCPjLLzv0zp/XmO6k+JvOePOGh
JzGk5t1QrSju+MqNPFk3+1O7o910Vrhqw1QRB0gr1ExrviLbyfU=
-----END CERTIFICATE-----
```

AWS GovCloud (USA Est) — -1 us-gov-east

DSA

```
-----BEGIN CERTIFICATE-----
 MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
 FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
 VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
 ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
 IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
 cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
 ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
 VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
 hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
 k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
 hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
 lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
 MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
 MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
 vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
 7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
 -----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
 MIIDITCCAoqgAwIBAgIULVyrqjjwZ461qelPCiShB1KCCj4wDQYJKoZIhvcNAQEL
 BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
 BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
 MB4XDTI0MDUwNzE1MjIzNloXDTI5MDUwNjE1MjIzNlowXDELMAkGA1UEBhMCVVMx
 GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
 BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
 A4GNADCBiQKBgQCpohwYUVPH9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBRO9K80al
 esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
 vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
 o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHVlVjg7918V
 gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHVlVjg7918VgE+hYKReMFwxCzAJ
 BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
 ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IULVyrqjjw
 Z461qelPCiShB1KCCj4wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
 AAOBgQBfAL/YZv0y3zmVbXjyxQCsDloeDCJjFKIu3ameEckeIWJbST9LMto0zViZ
 puIAf05x6GQiEqfBMk+YMxJfcTmJB4Ebaj4egFlslJPSHyC2xuydHlr3B04INOH5
 Z2oCM68u6GGbj0jZjg7GJonkReG9N72kDva/ukwZKgq8zErQVQ==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALPB6hxFhay8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
MjMyNDlaGA8yMTk3MDkxMzEyMzI0OVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAva9xsI9237KYb/SPWmeCVzi7giKNron8hoRDwlwwMC9+uHPd53UxzKLb
pTgtJWAPkZVxEdl2Gdhwr3SULoKcKmkqE6ltVFrVuPT33La1UufguT9k8ZDDuO9C
hQNHUdSVEuVrK3bLjaSsMOS7Uxmnn7lYT990IReowvnBNBsBlcabfQTBV04xfUG0
/m0XUiUFjOxDBqbNzkEIblW7vK7ydSJtFMSljga54UAVXibQt9EAIF7B8k9l2iLa
mu9yEjyQy+ZQICTuAvPUEWe6va2CHVY9gYQLA31/zU0VBKZPTNExjaqK4j8bKs1/
7dOV1so39sIGBz21cUBec1o+yCS5SwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBt
hO2W/Lm+Nk0qsXW6mqQFsAou0cASc/vtGNCyBfoFNX6aKXsVCHxq2aq2TUKWENs+
mKmYu1lZVhBOmLshyllh3RRoL3Ohp3jCwXytkWQ7ElcGjDzNGc0FArzB8xFyQNdK
MNvXDi/ErzgrHGSpcvmGHiOhMf3UzChMWbIr6udoDlMbSIO7+8F+jUJkh4Xl1lKb
YeN5fsLZp7T/6YvbFSPpmbn1YoE2vKtuGKxObRrhU3h4JHdp1Zel1pZ6lh5iM0ec
SD11SximGIYCjfZpRqI3q50mbxCd7ckULz+UUPwLrfOds4VrVVSj+x0ZdY19Plv2
9shw5ez6Cn7E3IfzqNHO
-----END CERTIFICATE-----
```

AWS GovCloud (US-Ouest) — -1 us-gov-west

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
```

```
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUe5wGF3jfb7lUHzvDxmM/ktGCLwwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDUwNzE3MzAzMloXDTI5MDUwNjE3MzAzMlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCpohwYUVPH9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBRO9K80al
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHVlVjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHVlVjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUe5wGF3jf
b7lUHzvDxmM/ktGCLwwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCbTdpx1Iob9SwUReY4exMnlwQlmkTLyA8tYGWzchCJOJJEPfsW0ryy1A0H
YIuvyUty3rJdp9ib8h3GZR71BkZnNddHhy06kPs4p8ewF8+d8OWtOJQcI+ZnFfG4
KyM4rUsBrljpG2aOCm12iACEyrvgJJrS8VZwUDZS6mZEnn/lhA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANCOF0Q6ohnuMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTAx
OTQyNDdaGA8yMTk1MDIxMzE5NDI0N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzIcGTzNqie3f1olrrqcfzGfbymSM2QfbTzDIOG6xXXeFrCDAmOq0wUhi
3fRCuoeHlKOWAPu76B9os71+zgF22dIDEVkpqHCjBrGzDQZXXUwOzhm+PmBUI8Z1
qvbVD4ZYhjCujWWzrsX6Z4yEK7PEFjtf4M4W8euw0RmiNwjy+knIFa+VxK6aQv94
lW98URFP2fD84xedHp6ozZlr3+RZSIFZsOiyxYsgiwTbesRMI0Y7LnkKGCIHQ/XJ
OwSISWaCddbu59BZeADnyhl4f+pWaSQpQQ1DpXvZAVBYvCH97J1oAxLfH8xcwgSQ
/se3wtn095VBt5b7qTVjOvy6vKZazwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA/
```

```
S8+a9csfASkdtQUOLsBynAbsBCH9Gykq2m8JS7YE4TGvqlpnWehz78rFTzQwmz4D
fwq8byPkl6DjdF9utqZ0JUo/Fxelxom0h6oievtBlSkmZJNbgc2WYm1zi6ptViup
Y+4S2+vWZyg/X1PXD7wyRWuETmykk73uEyeWFBYKCHWsO9sI+62O4Vf8Jkuj/cie
1NSJX8fkervfLrZSHBYhxLbL+actVEo00tiyZz8GnhgWx5faCY38D/k4Y/j5Vz99
7lUX/+fWHT3+lTL8ZZK7fOQWh6NQpI0wTP9KtWqfOUwMIbgFQPoxkP00TWRmdmPz
WOwTObEf9ouTnjG9OZ20
-----END CERTIFICATE-----
```

Synchronisation précise de l'heure et de l'heure sur votre EC2 instance

Une référence temporelle cohérente et précise sur votre EC2 instance Amazon est essentielle pour de nombreuses tâches et processus liés au serveur. Les horodatages dans les journaux système jouent un rôle essentiel pour identifier le moment où les problèmes sont survenus et l'ordre chronologique des événements. Lorsque vous utilisez le AWS CLI ou an AWS SDK pour effectuer des demandes depuis votre instance, ces outils signent les demandes en votre nom. Si les paramètres de date et d'heure de votre instance sont inexacts, cela peut entraîner un écart entre la date figurant dans la signature et la date de la demande, ce qui peut entraîner le AWS rejet de vos demandes.

Pour répondre à cet aspect important, Amazon propose le service Amazon Time Sync, qui est accessible depuis toutes les EC2 instances et utilisé par de nombreuses personnes services AWS. Le service utilise une flotte d'horloges de référence atomiques et connectées par satellite Région AWS pour fournir des relevés temporels précis et actuels conformément à la norme mondiale du temps universel coordonné (UTC).

Pour de meilleures performances, nous vous recommandons d'utiliser le service Amazon Time Sync local sur vos EC2 instances. Pour effectuer une sauvegarde vers le service Amazon Time Sync local sur vos instances, ou pour connecter des ressources extérieures EC2 à Amazon Time Sync Service, vous pouvez utiliser le service public Amazon Time Sync situé à l'adresse `time.aws.com`. Le service public Amazon Time Sync, tout comme le service Amazon Time Sync local, imprime automatiquement les secondes intercalaires qui y sont ajoutéesUTC. Le service public Amazon Time Sync est pris en charge dans le monde entier par notre flotte d'horloges de référence atomiques et connectées par satellite dans chacun d'entre eux. Région AWS

Secondes intercalaires

Les secondes intercalaires, introduites en 1972, sont des ajustements occasionnels d'une seconde du UTC temps pour tenir compte des irrégularités de la rotation de la Terre afin de tenir compte des différences entre le temps atomique international (TAI) et l'heure solaire (Ut1). Pour gérer les secondes intercalaires pour le compte des clients, nous avons conçu la correction des secondes intercalaires au sein du Service de synchronisation temporelle d'Amazon. Pour plus d'informations, consultez le billet de blog Look Before You Leap – The Coming Leap Second and AWS.

Les secondes intercalaires sont en train de disparaître, et nous soutenons pleinement la décision prise lors de la 27e Conférence générale des poids et mesures d'abandonner les secondes intercalaires d'ici 2035.

Pour faciliter cette transition, nous prévoyons toujours de réduire le temps lors d'une seconde intercalaire lors de l'accès au service Amazon Time Sync via une NTP connexion locale ou via nos NTP pools publics (`time.aws.com`). L'horloge PTP matérielle ne propose toutefois pas d'option de temporisation différée. En cas de seconde intercalaire, l'horloge PTP matérielle ajoutera la seconde intercalaire UTC conformément aux normes. Les sources temporelles à seconde intercalaire corrigées et non corrigées sont généralement identiques. Toutefois, étant donné qu'elles diffèrent en cas d'ajout de seconde intercalaire, nous vous déconseillons d'utiliser à la fois des sources temporelles corrigées et non corrigées dans la configuration de votre client temporel lors de l'ajout d'une seconde intercalaire.

Rubriques

- Définissez la référence temporelle sur votre EC2 instance pour utiliser le service Amazon Time Sync local
- Définissez la référence temporelle sur votre EC2 instance ou sur tout appareil connecté à Internet pour utiliser le service public Amazon Time Sync
- Comparez les horodatages de vos instances Linux
- Modifier le fuseau horaire de votre instance

Ressources connexes

- AWS Blog informatique : Il était temps : des horloges précises à la microseconde sur les instances Amazon EC2
- AWS Blog sur les opérations et les migrations dans le cloud : Gérez la précision de l'horloge des EC2 instances Amazon à l'aide d'Amazon Time Sync Service et d'Amazon CloudWatch — Partie 1
- (Linux) https://chrony-project.org/

Définissez la référence temporelle sur votre EC2 instance pour utiliser le service Amazon Time Sync local

Le service Amazon Time Sync local utilise le Network Time Protocol (NTP) ou fournit une horloge matérielle locale Precision Time Protocol (PTP) sur les instances prises en charge. L'horloge PTP matérielle prend en charge soit une NTP connexion (instances Linux et Windows), soit une PTP connexion directe (instances Linux uniquement). Les NTP PTP connexions directes utilisent la même source de temps très précise, mais la PTP connexion directe est plus précise que la NTP connexion. La NTP connexion au service Amazon Time Sync prend en charge le décalage horaire, tandis que la PTP connexion à l'horloge PTP matérielle ne modifie pas l'heure. Pour de plus amples informations, veuillez consulter Secondes intercalaires.

Vos instances peuvent accéder au Service de synchronisation temporelle d'Amazon local comme suit :

- Par le biais NTP des points de terminaison d'adresses IP suivants :
  - IPv4: `169.254.169.123`
  - IPv6: `fd00:ec2::123` (Accessible uniquement par les instances créées sur le système AWS Nitro.)
- (Linux uniquement) Via une PTP connexion directe pour se connecter à une horloge PTP matérielle locale :
  - `PHC0`

Amazon Linux AMIsAMIs, Windows et la plupart de leurs partenaires AMIs configurent votre instance pour utiliser le NTP IPv4 point de terminaison par défaut. Il s'agit du paramètre recommandé pour la plupart des charges de travail des clients. Aucune autre configuration n'est requise pour les instances lancées à partir de ceux-ci, AMIs sauf si vous souhaitez utiliser le IPv6 point de terminaison ou vous connecter directement à l'horloge PTP matérielle.

NTPet PTP les connexions ne nécessitent aucune modification VPC de configuration, et votre instance n'a pas besoin d'accéder à Internet.

> **Note**
>
> - Il existe une limite de 1024 paquets par seconde (PPS) pour les services qui utilisent des adresses lien-local. Cette limite inclut l'ensemble des requêtes Route 53 Resolver, des DNS requêtes Instance Meta Data Service (IMDS), des demandes Amazon Time Service Network Time Protocol (NTP) et des demandes du Windows Licensing Service (pour les instances basées sur Microsoft Windows).
> - Seules les instances Linux peuvent utiliser une PTPconnexion directe pour se connecter à l'horloge PTP matérielle locale. Les instances Windows sont utilisées NTP pour se connecter à l'horloge PTP matérielle locale.

Rubriques

- Connectez-vous au IPv4 point de terminaison du service Amazon Time Sync
- Connectez-vous au IPv6 point de terminaison du service Amazon Time Sync
- Connect à l'horloge PTP matérielle

Connectez-vous au IPv4 point de terminaison du service Amazon Time Sync

Cette section décrit comment configurer votre instance pour utiliser le service Amazon Time Sync local via le IPv4 point de terminaison.

Utilisez les instructions fournies pour le système d'exploitation de votre instance.

Linux

AL2La version 023 et les dernières versions d'Amazon Linux 2 et d'Amazon Linux AMIs sont configurées pour utiliser le point de IPv4 terminaison Amazon Time Sync Service par défaut. Aucune autre configuration n'est requise pour les instances lancées à partir de celles-ci AMIs et vous pouvez ignorer la procédure suivante.

Si vous utilisez un serveur sur AMI lequel le service Amazon Time Sync n'est pas configuré par défaut, suivez l'une des procédures suivantes pour configurer le service Amazon Time Sync sur votre

instance à l'aide du `chrony` client. Cela nécessite d'ajouter une entrée de serveur pour le Service de synchronisation temporelle d'Amazon au fichier de configuration `chrony`.

Utilisez les instructions fournies pour le système d'exploitation de votre instance.

Amazon Linux

Pour vous connecter au IPv4 point de terminaison du service Amazon Time Sync sur Amazon Linux à l'aide de chrony

1. Connectez-vous à votre instance et désinstallez le NTP service.

```
[ec2-user ~]$ sudo yum erase 'ntp*'
```

2. Installez le package `chrony`.

```
[ec2-user ~]$ sudo yum install chrony
```

3. Ouvrez le fichier `/etc/chrony.conf` avec un éditeur de texte (tel que vim ou nano). Vérifiez que le fichier contienne la ligne suivante :

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

   Si la ligne est présente, le service Amazon Time Sync est déjà configuré pour utiliser le IPv4 point de terminaison du service Amazon Time Sync et vous pouvez passer à l'étape suivante. Si ce n'est pas le cas, ajoutez la ligne après toute autre instruction `server` ou `pool` déjà présente dans le fichier, puis enregistrer les changements.

4. Relancez le démon `chrony` (`chronyd`).

```
[ec2-user ~]$ sudo service chronyd restart
```

```
Starting chronyd:                                          [  OK  ]
```

> **Note**
>
> Sur RHEL et CentOS (jusqu'à la version 6), le nom du service est à la `chrony` place de. `chronyd`

5. Pour configurer `chronyd` afin de lancer ce service à chaque démarrage système, utilisez la commande `chkconfig`.

```
[ec2-user ~]$ sudo chkconfig chronyd on
```

6. Vérifiez qu'`chronyd`il utilise le `169.254.169.123` IPv4 point de terminaison pour synchroniser l'heure.

```
[ec2-user ~]$ chronyc sources -v
```

```
210 Number of sources = 7

  .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
 / .- Source state '*' = current synced, '+' = combined , '-' = not
combined,
| /   '?' = unreachable, 'x' = time may be in error, '~' = time too
variable.
||                                                 .- xxxx [ yyyy ] +/-
zzzz
||      Reachability register (octal) -.           |  xxxx = adjusted
offset,
||      Log2(Polling interval) --.      |          |  yyyy = measured
offset,
||                                \     |          |  zzzz = estimated
error.
||                                 |    |           \
MS Name/IP address         Stratum Poll Reach LastRx Last sample


===============================================================================
^* 169.254.169.123               3   6    17    43    -30us[ -226us] +/-
 287us
^- ec2-12-34-231-12.eu-west>     2   6    17    43   -388us[ -388us] +/-
  11ms
^- tshirt.heanet.ie              1   6    17    44   +178us[  +25us] +/-
1959us
^? tbag.heanet.ie                0   6     0     -     +0ns[   +0ns] +/-
   0ns
^? bray.walcz.net                0   6     0     -     +0ns[   +0ns] +/-
   0ns
^? 2a05:d018:c43:e312:ce77:>     0   6     0     -     +0ns[   +0ns] +/-
   0ns
```

```
        ^? 2a05:d018:dab:2701:b70:b>     0   6     0     -     +0ns[   +0ns] +/-
    0ns
```

Dans le résultat retourné, ^* indique la source de temps préférée.

7. Vérifiez les métriques de synchronisation du temps présentées par `chrony`.

```
[ec2-user ~]$ chronyc tracking
```

```
Reference ID    : A9FEA97B (169.254.169.123)
        Stratum         : 4
        Ref time (UTC)  : Wed Nov 22 13:18:34 2017
        System time     : 0.000000626 seconds slow of NTP time
        Last offset     : +0.002852759 seconds
        RMS offset      : 0.002852759 seconds
        Frequency       : 1.187 ppm fast
        Residual freq   : +0.020 ppm
        Skew            : 24.388 ppm
        Root delay      : 0.000504752 seconds
        Root dispersion : 0.001112565 seconds
        Update interval : 64.4 seconds
        Leap status     : Normal
```

Ubuntu

Pour vous connecter au IPv4 point de terminaison du service Amazon Time Sync sur Ubuntu à l'aide de chrony

1. Connectez-vous à votre instance et utilisez `apt` pour installer le package `chrony`.

```
ubuntu:~$ sudo apt install chrony
```

> **Note**
>
> Si nécessaire, mettez d'abord à jour votre instance en exécutant `sudo apt update`.

2. Ouvrez le fichier `/etc/chrony/chrony.conf` avec un éditeur de texte (tel que vim ou nano). Ajoutez la ligne suivante avant toute autre instruction `server` ou `pool` déjà présente dans le fichier, puis enregistrer les changements :

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

3. Redémarrez le service `chrony`.

```
ubuntu:~$ sudo /etc/init.d/chrony restart
```

```
Restarting chrony (via systemctl): chrony.service.
```

4. Vérifiez qu'`chrony`il utilise le `169.254.169.123` IPv4 point de terminaison pour synchroniser l'heure.

```
ubuntu:~$ chronyc sources -v
```

```
210 Number of sources = 7

             .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
            / .- Source state '*' = current synced, '+' = combined , '-' = not
 combined,
           | /   '?' = unreachable, 'x' = time may be in error, '~' = time too
 variable.
           ||                                                .- xxxx [ yyyy ]
 +/- zzzz
           ||      Reachability register (octal) -.          |  xxxx =
 adjusted offset,
           ||      Log2(Polling interval) --.      |         |  yyyy =
 measured offset,
           ||                                \     |         |  zzzz =
 estimated error.
           ||                                 |    |          \
           MS Name/IP address         Stratum Poll Reach LastRx Last sample

 ===============================================================================
           ^* 169.254.169.123               3   6    17    12    +15us[  +57us]
 +/-  320us
           ^- tbag.heanet.ie                1   6    17    13  -3488us[-3446us]
 +/- 1779us
           ^- ec2-12-34-231-12.eu-west-     2   6    17    13   +893us[ +935us]
 +/- 7710us
           ^? 2a05:d018:c43:e312:ce77:6     0   6     0   10y     +0ns[   +0ns]
 +/-    0ns
```

```
            ^? 2a05:d018:d34:9000:d8c6:5     0   6     0   10y     +0ns[   +0ns]
 +/-    0ns
            ^? tshirt.heanet.ie              0   6     0   10y     +0ns[   +0ns]
 +/-    0ns
            ^? bray.walcz.net                0   6     0   10y     +0ns[   +0ns]
 +/-    0ns
```

Dans le résultat retourné, sur la ligne commençant par `^*`, cela indique la source de temps préférée.

5. Vérifiez les métriques de synchronisation du temps présentées par `chrony`.

```
ubuntu:~$ chronyc tracking
```

```
Reference ID    : 169.254.169.123 (169.254.169.123)
            Stratum         : 4
            Ref time (UTC)  : Wed Nov 29 07:41:57 2017
            System time     : 0.000000011 seconds slow of NTP time
            Last offset     : +0.000041659 seconds
            RMS offset      : 0.000041659 seconds
            Frequency       : 10.141 ppm slow
            Residual freq   : +7.557 ppm
            Skew            : 2.329 ppm
            Root delay      : 0.000544 seconds
            Root dispersion : 0.000631 seconds
            Update interval : 2.0 seconds
            Leap status     : Normal
```

SUSE Linux

À partir de SUSE Linux Enterprise Server 15, `chrony` c'est l'implémentation par défaut deNTP.

Pour vous connecter au IPv4 point de terminaison du service Amazon Time Sync SUSE sous Linux à l'aide de Chrony

1. Ouvrez le fichier `/etc/chrony.conf` avec un éditeur de texte (tel que vim ou nano).
2. Vérifiez que le fichier contient la ligne suivante :

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

Si la ligne n'est pas présente, vous pouvez l'ajouter manuellement.

3. Placez en commentaire les autres lignes sur le serveur ou le groupe (pool).
4. Ouvrez yaST et activez le service chrony.

Windows

À partir de la version d'août 2018, Windows AMIs utilise le service Amazon Time Sync par défaut. Aucune autre configuration n'est requise pour les instances lancées à partir de celles-ci AMIs et vous pouvez ignorer les procédures suivantes.

Si vous utilisez un serveur sur AMI lequel le service Amazon Time Sync n'est pas configuré par défaut, vérifiez d'abord votre NTP configuration actuelle. Si votre instance utilise déjà le IPv4 point de terminaison du service Amazon Time Sync, aucune autre configuration n'est requise. Si votre instance n'utilise pas le service Amazon Time Sync, suivez la procédure pour modifier le NTP serveur afin qu'il utilise le service Amazon Time Sync.

Pour vérifier la NTP configuration

1. Depuis votre instance, ouvrez une fenêtre d'invite de commande.
2. Obtenez la NTP configuration actuelle en saisissant la commande suivante :

   ```
   w32tm /query /configuration
   ```

   Cette commande renvoie les paramètres de configuration actuels de l'instance Windows et indique si vous êtes connecté au Service de synchronisation temporelle d'Amazon.
3. (Facultatif) Obtenez l'état de la configuration actuelle en tapant la commande suivante :

   ```
   w32tm /query /status
   ```

   Cette commande renvoie des informations telles que la dernière synchronisation de l'instance avec le NTP serveur et l'intervalle entre les interrogations.

Pour modifier le NTP serveur afin d'utiliser le service Amazon Time Sync

1. A partir d'une fenêtre d'invite de commande, exécutez la commande suivante :

```
w32tm /config /manualpeerlist:169.254.169.123 /syncfromflags:manual /update
```

2. Vérifiez vos nouveaux paramètres en exécutant la commande suivante :

```
w32tm /query /configuration
```

Dans le résultat renvoyé, vérifiez que le point de `169.254.169.123` IPv4 terminaison est `NtpServer` affiché.

Paramètres du protocole horaire réseau par défaut (NTP) pour Amazon Windows AMIs

Amazon Machine Images (AMIs) respecte généralement les out-of-the-box valeurs par défaut, sauf dans les cas où des modifications sont nécessaires pour fonctionner sur EC2 l'infrastructure. Les paramètres suivants ont été déterminés comme étant efficaces dans un environnement virtuel et permettant de maintenir la dérive d'horloge dans une précision d'une seconde :

- Intervalle de mise à jour — Détermine la fréquence à laquelle le service horaire ajustera l'heure du système pour qu'elle soit précise. AWS configure l'intervalle de mise à jour pour qu'il se produise une fois toutes les deux minutes.
- NTPServeur : à partir de la version d'août 2018, AMIs utilisez le service Amazon Time Sync par défaut. Cette fois, le service est accessible depuis n'importe quel point de Région AWS terminaison 169.254.169.123IPv4. De plus, l'indicateur 0x9 indique que le service temporel agit en tant que client et qu'il convient d'utiliser `SpecialPollInterval` pour déterminer la fréquence à laquelle se signaler auprès du serveur horaire configuré.
- Type — « NTP » signifie que le service agit en tant que NTP client autonome au lieu d'agir dans le cadre d'un domaine.
- Activé et InputProvider — Le service horaire est activé et fournit du temps au système d'exploitation.
- Intervalle d'interrogation spécial : vérification par rapport au NTP serveur configuré toutes les 900 secondes (15 minutes).

Chemin de registre	Nom de la touche	Données
HKLM: \ System \ \ services CurrentControlSet \ w32time \ Config	UpdateInterval	120
HKLM: \ System \ CurrentCo ntrolSet \ services \ w32time \ Paramètres	NtpServer	169.254.169.123,0x9
HKLM: \ System \ CurrentCo ntrolSet \ services \ w32time \ Paramètres	Type	NTP
HKLM: \ Système \ CurrentCo ntrolSet \ services \ w32time \ \ TimeProviders NtpClient	Activées	1
HKLM: \ Système \ CurrentCo ntrolSet \ services \ w32time \ \ TimeProviders NtpClient	InputProvider	1
HKLM: \ Système \ CurrentCo ntrolSet \ services \ w32time \ \ TimeProviders NtpClient	SpecialPollInterval	900

Connectez-vous au IPv6 point de terminaison du service Amazon Time Sync

Cette section explique en quoi les étapes décrites dans la section Connectez-vous au IPv4 point de terminaison du service Amazon Time Sync diffèrent si vous configurez votre instance pour utiliser le service Amazon Time Sync local via le IPv6 point de terminaison. Il n'explique pas l'intégralité du processus de configuration Amazon Time Sync Service.

Le IPv6 point de terminaison n'est accessible que sur les instances créées sur le système AWS Nitro.

> **Note**
>
> Nous ne recommandons pas d'utiliser à la fois les entrées IPv4 et les entrées du point de IPv6 terminaison. Les IPv6 NTP paquets IPv4 et proviennent du même serveur local que celui de votre instance. La configuration à la fois IPv4 des IPv6 points de terminaison n'est pas nécessaire et n'améliorera pas la précision de l'heure sur votre instance.

Utilisez les instructions fournies pour le système d'exploitation de votre instance.

Linux

Selon la distribution Linux que vous utilisez, lorsque vous atteindrez l'étape de modification du fichier chrony.conf, vous utiliserez le IPv6 point de terminaison du service Amazon Time Sync (`fd00:ec2::123`) plutôt que le IPv4 point de terminaison (`169.254.169.123`) :

```
server fd00:ec2::123 prefer iburst minpoll 4 maxpoll 4
```

Enregistrez le fichier et vérifiez qu'`chrony`il utilise le `fd00:ec2::123` IPv6 point de terminaison pour synchroniser l'heure :

```
[ec2-user ~]$ chronyc sources -v
```

Dans la sortie, si vous voyez le `fd00:ec2::123` IPv6 point de terminaison, la configuration est terminée.

Windows

Lorsque vous atteindrez l'étape consistant à modifier le NTP serveur pour utiliser le service Amazon Time Sync, vous utiliserez le IPv6 point de terminaison du service Amazon Time Sync (`fd00:ec2::123`) plutôt que le IPv4 point de terminaison (`169.254.169.123`) :

```
w32tm /config /manualpeerlist:fd00:ec2::123 /syncfromflags:manual /update
```

Vérifiez que vos nouveaux paramètres utilisent le `fd00:ec2::123` IPv6 point de terminaison pour synchroniser l'heure :

```
w32tm /query /configuration
```

Dans le résultat, vérifiez que le point de `fd00:ec2::123` IPv6 terminaison est `NtpServer` affiché.

Connect à l'horloge PTP matérielle

L'horloge PTP matérielle fait partie du système AWS Nitro. Elle est donc directement accessible sur les EC2instances bare metal et virtualisées prises en charge sans utiliser les ressources du client.

Les NTP points de terminaison de l'horloge PTP matérielle sont les mêmes que ceux du service Amazon Time Sync standard. Si votre instance dispose d'une horloge PTP matérielle et que vous avez configuré la NTP connexion (vers le point de IPv6 terminaison IPv4 ou vers le point de terminaison), l'heure de votre instance est automatiquement calculée à partir de l'horloge PTP matérielleNTP.

Pour les instances Linux, vous pouvez configurer une PTP connexion directe, qui vous donnera une heure plus précise que la NTP connexion. Les instances Windows ne prennent en charge qu'une NTP connexion à l'horloge PTP matérielle.

Prérequis

L'horloge PTP matérielle est disponible sur une instance lorsque les conditions suivantes sont remplies :

- Soutenu Régions AWS : USA Est (Virginie du Nord) et Asie-Pacifique (Tokyo)
- Familles d'instances prises en charge
  - Usage général : M7a, M7g, M7gD, M7i
  - Optimisé pour le calcul : C7a, C7gd, C7i
  - Mémoire optimisée : R7a, R7g, R7gd, R7i
- (Linux uniquement) version 2.10.0 ou ultérieure du ENA pilote installée sur un système d'exploitation pris en charge. Pour plus d'informations sur les systèmes d'exploitation pris en charge, consultez les conditions requises pour les pilotes sur GitHub.

(Linux uniquement) Configurer une PTP connexion directe à l'horloge PTP matérielle

Cette section décrit comment configurer votre instance Linux pour utiliser le service Amazon Time Sync local via l'horloge PTP matérielle à l'aide d'une PTP connexion directe. Cela nécessite l'ajout d'une entrée serveur pour l'horloge PTP matérielle dans le fichier `chrony` de configuration.

Pour configurer une PTP connexion directe à l'horloge PTP matérielle (instances Linux uniquement)

1. Connectez-vous à votre instance Linux et procédez comme suit :

a. Installez le pilote du noyau Linux pour Elastic Network Adapter (ENA) version 2.10.0 ou ultérieure.

b. Activez l'horloge PTP matérielle.

Pour les instructions d'installation, consultez le pilote de noyau Linux pour la famille Elastic Network Adapter (ENA) sur GitHub.

2. Vérifiez que l'appareil `/dev/ptp0` apparaît sur votre instance.

```
[ec2-user ~]$ ls /dev/ptp0
```

La sortie attendue est la suivante : Si `/dev/ptp0` ce n'est pas le cas dans la sortie, cela signifie que le ENA pilote n'a pas été correctement installé. Passez en revue l'étape 1 de cette procédure pour installer le pilote.

```
/dev/ptp0
```

3. Modifiez `/etc/chrony.conf` à l'aide d'un éditeur de texte et ajoutez la ligne suivante n'importe où dans le fichier.

```
refclock PHC /dev/ptp0 poll 0 delay 0.000010 prefer
```

4. Redémarrez Chrony.

```
[ec2-user ~]$ sudo systemctl restart chronyd
```

5. Vérifiez que Chrony utilise l'horloge PTP matérielle pour synchroniser l'heure sur cette instance.

```
[ec2-user ~]$ chronyc sources
```

Sortie attendue

```
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
#* PHC0                          0   0    377    1   +2ns[ +1ns] +/-   5031ns
```

Dans la sortie renvoyée, * indique la source de temps préférée. PHC0correspond à l'horloge PTP matérielle. Vous devrez peut-être attendre quelques secondes après avoir redémarré chrony pour que l'astérisque apparaisse.

Définissez la référence temporelle sur votre EC2 instance ou sur tout appareil connecté à Internet pour utiliser le service public Amazon Time Sync

Vous pouvez configurer votre instance, ou tout appareil connecté à Internet tel que votre ordinateur local ou un serveur sur site, pour utiliser le Service de synchronisation temporelle d'Amazon public, accessible via Internet à l'adresse `time.aws.com`. Vous pouvez utiliser le service public Amazon Time Sync comme solution de sauvegarde pour le service Amazon Time Sync local et pour connecter des ressources extérieures AWS au service Amazon Time Sync.

> **Note**
>
> Pour de meilleures performances, nous vous recommandons d'utiliser le service Amazon Time Sync local sur vos instances et de n'utiliser que le service public Amazon Time Sync en tant que sauvegarde.

Suivez les instructions relatives au système d'exploitation de votre instance ou de votre appareil.

Linux

Pour configurer votre instance ou appareil Linux afin qu'il utilise le Service de synchronisation temporelle d'Amazon public à l'aide de chrony ou ntpd

1. Modifiez `/etc/chrony.conf` (si vous utilisez chrony) ou `/etc/ntp.conf` (si vous utilisez ntpd) à l'aide d'un éditeur de texte comme suit :

   a. Pour empêcher votre instance ou votre appareil d'essayer de mélanger des serveurs corrigés et non corrigés, supprimez ou commentez les lignes commençant par `server` sauf les connexions existantes au Service de synchronisation temporelle d'Amazon local.

> **Important**
>
> Si vous configurez votre EC2 instance pour qu'elle se connecte au service public Amazon Time Sync, ne supprimez pas la ligne suivante qui définit votre instance pour qu'elle se connecte au service Amazon Time Sync local. Le Service de synchronisation temporelle d'Amazon local fournit une connexion plus directe et une meilleure précision de l'horloge. Le Service de synchronisation temporelle d'Amazon public doit uniquement être utilisé comme sauvegarde.
>
> ```
> server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
> ```

b. Ajoutez la ligne suivante pour vous connecter au Service de synchronisation temporelle d'Amazon public.

```
pool time.aws.com iburst
```

2. Redémarrez le démon à l'aide de l'une des commandes suivantes.

   - chrony

     ```
     sudo service chronyd force-reload
     ```

   - ntpd

     ```
     sudo service ntp reload
     ```

macOS

Pour configurer votre instance ou appareil macOS afin qu'il utilise le Service de synchronisation temporelle d'Amazon public

1. Ouvrez System Preferences (Préférences système).
2. Choisissez Date & Time (Date et heure), puis choisissez l'onglet Date & Time (Date et heure).
3. Pour apporter des modifications, choisissez l'icône en forme de cadenas et saisissez votre mot de passe lorsque vous y êtes invité.

4. Pour Set date and timqe automatically (Définir automatiquement la date et l'heure), saisissez **`time.aws.com`**.

Windows

Pour configurer votre instance ou appareil Windows afin qu'il utilise le Service de synchronisation temporelle d'Amazon public

1. Ouvrez le Control Panel (Panneau de configuration).
2. Cliquez sur l'icône Date and Time (Date et heure).
3. Choisissez l'onglet Internet Time (Heure Internet). Cet onglet n'est pas disponible si votre PC fait partie d'un domaine. Dans ce cas, votre PC synchronise l'heure avec le contrôleur de domaine. Vous pouvez configurer le contrôleur pour qu'il utilise le Service de synchronisation temporelle d'Amazon public.
4. Choisissez Change qsettings (Modifier les paramètres).
5. Cochez la case Synchronize with an Internet time server (Synchroniser avec un serveur de temps Internet).
6. À côté de Server (Serveur), saisissez **`time.aws.com`**.

Pour configurer votre instance ou appareil Windows Server afin qu'il utilise le Service de synchronisation temporelle d'Amazon public

- Suivez les instructions de Microsoft (français non disponible) pour mettre à jour votre registre.

Comparez les horodatages de vos instances Linux

Si vous utilisez le service Amazon Time Sync, vous pouvez comparer les horodatages de vos instances Amazon EC2 Linux ClockBound pour déterminer l'heure réelle d'un événement. ClockBound mesure la précision de l'horloge de votre EC2 instance et vous permet de vérifier si un horodatage donné correspond au passé ou au futur par rapport à l'horloge actuelle de votre instance. Ces informations sont précieuses pour déterminer l'ordre et la cohérence des événements et des transactions entre les EC2 instances, indépendamment de l'emplacement géographique de chaque instance.

ClockBound est un daemon et une bibliothèque open source. Pour en savoir plus ClockBound, y compris les instructions d'installation, reportez-vous à ClockBoundla section GitHub.

ClockBound n'est pris en charge que pour les instances Linux.

Si vous utilisez une PTP connexion directe à l'horloge PTP matérielle, votre démon temporel, par exemple, sous-estimera chrony la limite d'erreur d'horloge. Cela est dû au fait qu'une horloge PTP matérielle ne transmet pas les informations correctes liées aux erreurschrony, comme elle le NTP fait. Par conséquent, votre démon de synchronisation d'horloge suppose que l'horloge est précise UTC et possède donc une limite d'`0`erreur égale à. Pour mesurer la limite d'erreur complète, le système Nitro calcule la borne d'erreur de l'horloge PTP matérielle et la met à la disposition de votre EC2 instance via le système de fichiers du ENA pilote`sysfs`. Vous pouvez le lire directement sous forme de valeur, en nanosecondes.

Pour récupérer la limite d'erreur de l'horloge PTP matérielle

1. Trouvez d'abord l'emplacement correct de l'horloge PTP matérielle à l'aide de l'une des commandes suivantes. Le chemin indiqué dans la commande est différent en fonction du chemin AMI utilisé pour lancer l'instance.

   - Dans Amazon Linux 2:

     ```
     cat /sys/class/net/eth0/device/uevent | grep PCI_SLOT_NAME
     ```

   - Pour Amazon Linux 2023 :

     ```
     cat /sys/class/net/ens5/device/uevent | grep PCI_SLOT_NAME
     ```

   La sortie est le nom du PCI slot, qui correspond à l'emplacement de l'horloge PTP matérielle. Dans cet exemple, l'emplacement est`0000:00:03.0`.

   ```
   PCI_SLOT_NAME=0000:00:03.0
   ```

2. Pour récupérer la limite d'erreur de l'horloge PTP matérielle, exécutez la commande suivante. Incluez le nom du PCI slot indiqué à l'étape précédente.

   ```
   cat /sys/bus/pci/devices/0000:00:03.0/phc_error_bound
   ```

   La sortie est la borne d'erreur d'horloge de l'horloge PTP matérielle, en nanosecondes.

Pour calculer la bonne erreur d'horloge liée à un moment précis lors de l'utilisation de la PTP connexion directe à l'horloge PTP matérielle, vous devez ajouter l'erreur d'horloge liée ClockBound à chrony ou à l'heure qui chrony interroge l'horloge PTP matérielle. Pour plus d'informations sur la mesure et le suivi de la précision de l'horloge, consultez Gérer la précision de l'horloge des EC2 instances Amazon à l'aide d'Amazon Time Sync Service et d'Amazon CloudWatch — Partie 1.

Modifier le fuseau horaire de votre instance

Les EC2 instances Amazon sont définies sur le fuseau horaire UTC (temps universel coordonné) par défaut. Vous pouvez modifier l'heure d'une instance au fuseau horaire local ou à un autre fuseau horaire de votre réseau.

Utilisez les instructions fournies pour le système d'exploitation de votre instance.

Linux

> **Important**
>
> Ces informations s'appliquent à Amazon Linux. Pour obtenir des informations sur d'autres distributions, consultez leur documentation spécifique.

Pour modifier le fuseau horaire sur une instance AL2 023 ou Amazon Linux 2

1. Affichez le paramètre de fuseau horaire actuel du système.

```
[ec2-user ~]$ timedatectl
```

2. Répertoriez les fuseaux horaires disponibles.

```
[ec2-user ~]$ timedatectl list-timezones
```

3. Définissez le fuseau horaire choisi.

```
[ec2-user ~]$ sudo timedatectl set-timezone America/Vancouver
```

4. (Facultatif) Vérifiez que le fuseau horaire actuel est mis à jour vers le nouveau fuseau horaire en ré-exécutant la commande timedatectl.

```
[ec2-user ~]$ timedatectl
```

Windows

Pour modifier le fuseau horaire sur une instance Windows

1. Depuis votre instance, ouvrez une fenêtre d'invite de commande.
2. Identifiez le fuseau horaire à utiliser sur l'instance. Pour obtenir une liste des fuseaux horaires, utilisez la commande suivante :

   ```
   tzutil /l
   ```

   Cette commande renvoie une liste de tous les fuseaux horaires disponibles, au format suivant :

   ```
   display name
   time zone ID
   ```
3. Recherchez l'ID du fuseau horaire à attribuer à l'instance.
4. Attribuez à un autre fuseau horaire à l'aide de la commande suivante :

   ```
   tzutil /s "Pacific Standard Time"
   ```

   Le nouveau fuseau horaire doit prendre effet immédiatement.

> **Note**
>
> Vous pouvez attribuer le UTC fuseau horaire à l'aide de la commande suivante :
>
> ```
> tzutil /s "UTC"
> ```

Pour empêcher que votre fuseau horaire ne change une fois que vous l'avez défini pour Windows Server

Lorsque vous modifiez le fuseau horaire d'une instance Windows, vous devez vérifier que le fuseau horaire persiste lors du redémarrage du système. Sinon, lorsque l'instance redémarre, elle revient à l'heure d'utilisationUTC. Vous pouvez conserver votre paramètre de fuseau horaire en ajoutant une clé de RealTimeIsUniversal registre. Cette clé est définie par défaut sur toutes les instances de

génération en cours. Pour vérifier si la clé de Registre RealTimeIsUniversal est définie, consultez l'étape 4 de la procédure suivante. Si la clé n'est pas définie, procédez comme suit depuis le début.

Pour définir la clé RealTimeIsUniversal de registre

1. Depuis l'instance, ouvrez une fenêtre d'invite de commande.
2. Cette commande vous permet d'ajouter la clé de registre :

```
reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation" /
v RealTimeIsUniversal /d 1 /t REG_DWORD /f
```

3. Si vous utilisez un Windows Server 2008 AMI (et non Windows Server 2008 R2) créé avant le 22 février 2013, nous vous recommandons de passer à la dernière version de AWS WindowsAMI. Si vous utilisez un Windows Server 2008 R2 en cours d'AMIexécution (et non Windows Server 2008), vous devez vérifier que le correctif Microsoft KB2922223est installé. Si ce correctif n'est pas installé, nous vous recommandons de passer à la dernière version de AWS WindowsAMI.
4. (Facultatif) Vérifiez que l'instance a enregistré la clé à l'aide de la commande suivante :

```
reg query "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control
\TimeZoneInformation" /s
```

Cette commande renvoie les sous-clés de la clé de registre TimeZoneInformation. La clé RealTimeIsUniversal doit s'afficher en bas de la liste, comme suit :

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation
    Bias                            REG_DWORD     0x1e0
    DaylightBias                    REG_DWORD     0xffffffc4
    DaylightName                    REG_SZ        @tzres.dll,-211
    DaylightStart                   REG_BINARY    00000300020002000000000000000000
    StandardBias                    REG_DWORD     0x0
    StandardName                    REG_SZ        @tzres.dll,-212
    StandardStart                   REG_BINARY    00000B0001000200000000000000000
    TimeZoneKeyName                 REG_SZ        Pacific Standard Time
    DynamicDaylightTimeDisabled     REG_DWORD     0x0
    ActiveTimeBias                  REG_DWORD     0x1a4
    RealTimeIsUniversal             REG_DWORD     0x1
```

Gérez les pilotes de périphériques pour votre EC2 instance

Les pilotes de périphériques sont des composants logiciels qui communiquent avec le matériel virtualisé de votre EC2 instance Amazon. Pour éviter les erreurs système, les problèmes de performances et autres comportements inattendus, il est important de conserver vos pilotes up-to-date. Cela est particulièrement vrai pour les pilotes qui peuvent avoir un impact important sur les performances du système en fonction de votre utilisation, tels que les pilotes réseau, graphiques et de périphériques de stockage. Les nouvelles versions de pilotes peuvent inclure des correctifs ou introduire des fonctionnalités étendues dont vous souhaiterez peut-être tirer parti pour les instances en cours d'exécution.

Pilotes réseau

Les distributions Linux peuvent intégrer des fonctionnalités réseau telles qu'Elastic Network Adapter (ENA) ou Elastic Fabric Adapter (EFA) dans le noyau. Cependant, le calendrier de mise en œuvre des fonctionnalités du pilote du noyau peut varier au sein des différentes distributions.

ENAet les pilotes du noyau EFA Linux sont disponibles dans le GitHub référentiel Amazon Drivers. Pour plus d'informations et des liens vers les pilotes disponibles, consultez Amazon Drivers sur GitHub.

Pour plus d'informations sur ENA les pilotes, consultezActivez une mise en réseau améliorée avec ENA vos EC2 instances. Pour plus d'informations sur EFA les pilotes, consultez les rubriques relatives à la mise en route dans la Adaptateur Elastic Fabric pour les charges de travail ML HPC et ML sur Amazon EC2 section de ce guide.

Pour installer ou mettre à jour les pilotes réseau sur les instances Windows, consultez les rubriques suivantes :

- Installez le ENA pilote sous Windows
- Installez les derniers pilotes AWS PV

  Pour de plus amples informations, veuillez consulter Pilotes de virtualisation paravirtuelle pour les instances Windows.

> **Note**
>
> EFAn'est pas pris en charge sur les instances Windows.

Pilotes graphiques

Pour installer ou mettre à jour les pilotes graphiques, consultez les rubriques suivantes :

- AMDpilotes pour votre EC2 instance
- NVIDIApilotes pour votre EC2 instance Amazon

Pilotes de périphériques de stockage

Pour installer ou mettre à jour les pilotes de stockage, consultez les rubriques suivantes :

- Pour les instances Linux, consultez la section Installer ou mettre à niveau le NVMe pilote dans le guide de EBS l'utilisateur Amazon.
- Pour les instances Windows, voirAWS NVMepilotes pour instances Windows.

AMDpilotes pour votre EC2 instance

Le AMD pilote approprié doit être installé sur une instance associée AMDGPU, telle qu'une instance G4ad. Selon vos besoins, vous pouvez soit utiliser un AMI avec le pilote préinstallé, soit télécharger un pilote depuis Amazon S3.

Pour installer des NVIDIA pilotes sur une instance associée NVIDIAGPU, telle qu'une instance G4dn, consultez NVIDIApilotes plutôt.

Table des matières

AMDLogiciel Radeon Pro pour pilote d'entreprise

Le pilote AMD Radeon Pro Software for Enterprise est conçu pour prendre en charge les cas d'utilisation de cartes graphiques de niveau professionnel. À l'aide du pilote, vous pouvez configurer vos instances avec deux écrans 4K par instanceGPU.

Soutenu APIs

- OpenGL, OpenCL
- Vulkan
- AMDFramework multimédia avancé
- Accélération vidéo API
- DirectX 9 et versions ultérieures
- Microsoft Hardware Media Foundation Transform

AMIsavec le AMD pilote installé

AWS propose différentes Amazon Machine Images (AMIs) fournies avec les AMD pilotes installés. Offres Open Marketplace avec AMD chauffeur.

AMDtéléchargement du pilote

Si vous n'utilisez pas AMI un AMD pilote installé, vous pouvez télécharger le AMD pilote et l'installer sur votre instance. Seules les versions de système d'exploitation suivantes prennent en charge AMD les pilotes :

- Amazon Linux 2 avec la version 4.14 du noyau

> **Note**
>
> AMDla version du pilote amdgpu-pro-20.20-1184451 et les versions plus récentes nécessitent la version 5.15 ou supérieure du noyau.

- Windows Server 2016
- Windows Server 2019

Ces téléchargements ne sont disponibles que pour AWS les clients. En téléchargeant, vous acceptez d'utiliser le logiciel téléchargé uniquement AMIs pour le développer et l'utiliser avec le matériel AMD Radeon Pro V520. Lors de l'installation du logiciel, vous êtes lié par les termes du contrat de licence utilisateur final du AMD logiciel.

Installez le AMD pilote sur votre instance Linux

1. Connectez-vous à votre instance Linux.

2. Installez-le AWS CLI sur votre instance Linux et configurez les informations d'identification par défaut. Pour plus d'informations, consultez Installation d' AWS CLI dans le Guide de l'utilisateur AWS Command Line Interface .

   > **Important**
   >
   > Votre utilisateur ou rôle doit disposer des autorisations accordées conformément à la politique d'AmazonS3 ReadOnlyAccess. Pour plus d'informations, consultez la politique AWS gérée : AmazonS3 ReadOnlyAccess dans le guide de l'utilisateur d'Amazon Simple Storage Service.

3. Installez gcc et make, si ce n'est pas déjà fait.

```
$ sudo yum install gcc make
```

4. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

   - Dans Amazon Linux 2:

```
$ sudo amazon-linux-extras install epel -y
$ sudo yum update -y
```

   - Pour Ubuntu 22.04 :

```
$ wget https://repo.radeon.com/.preview/a0e4ef1dffbc95b4abb54e891f265e61/amdgpu-install/5.5.02.05.2/ubuntu/jammy/amdgpu-install_5.5.02.05.50502-1_all.deb
$ sudo apt install ./amdgpu-install_5.5.02.05.50502-1_all.deb
$ sudo sed -i 's#repo.radeon.com#&/.preview/a0e4ef1dffbc95b4abb54e891f265e61#' /etc/apt/sources.list.d/{amdgpu.list,rocm.list,amdgpu-proprietary.list}
```

   - Pour les autres versions d'Ubuntu :

```
$ sudo dpkg --add-architecture i386
$ sudo apt-get update -y && sudo apt upgrade -y
```

   - Pour CentOS :

```
$ sudo yum install epel-release -y
$ sudo yum update -y
```

5. Redémarrez l'instance.

```
$ sudo reboot
```

6. Reconnectez-vous à l'instance après son redémarrage.
7. Téléchargez le dernier AMD pilote.

> **Note**
>
> Ignorez cette étape pour Ubuntu 22.04.

```
$ aws s3 cp --recursive s3://ec2-amd-linux-drivers/latest/ .
```

8. Extrayez le fichier.

   - Pour Amazon Linux 2 et CentOS :

   ```
   $ tar -xf amdgpu-pro-*rhel*.tar.xz
   ```

   - Pour Ubuntu :

   > **Note**
   >
   > Ignorez cette étape pour Ubuntu 22.04.

   ```
   $ tar -xf amdgpu-pro*ubuntu*.xz
   ```

9. Sélectionnez le dossier du pilote extrait.
10. Ajoutez les modules manquants pour l'installation du pilote.

    - Pour Amazon Linux 2 et CentOS :

      Ignorez cette étape.

    - Pour Ubuntu :

> **Note**
>
> Ignorez cette étape pour Ubuntu 22.04.

```
$ sudo apt install linux-modules-extra-$(uname -r) -y
```

11. Exécutez le script d'installation automatique pour installer la pile graphique complète.

    - Pour Ubuntu 22.04 :

      ```
      $ sudo amdgpu-install --usecase=workstation --vulkan=pro --opencl=rocr,legacy -y
      ```

    - Pour Amazon Linux 2, CentOS et les autres versions d'Ubuntu :

      ```
      $ ./amdgpu-pro-install -y --opencl=pal,legacy
      ```

12. Redémarrez l'instance.

    ```
    $ sudo reboot
    ```

13. Vérifiez que le pilote fonctionne.

    ```
    $ dmesg | grep amdgpu
    ```

    Les résultats doivent avoir l'aspect suivant :

    ```
    Initialized amdgpu
    ```

Installez le AMD pilote sur votre instance Windows

1. Connectez-vous à votre instance Windows et ouvrez une PowerShell fenêtre.
2. Configurez les informations d'identification par défaut pour votre instance Windows. AWS Tools for Windows PowerShell Pour plus d'informations, voir Démarrer avec les AWS Tools for Windows PowerShell dans le Guide de l'utilisateur AWS Tools for Windows PowerShell .

> **Important**
>
> Votre utilisateur ou rôle doit disposer des autorisations accordées conformément à la politique d'AmazonS3 ReadOnlyAccess. Pour plus d'informations, consultez la politique AWS gérée : AmazonS3 ReadOnlyAccess dans le guide de l'utilisateur d'Amazon Simple Storage Service.

3. Définissez le préfixe de clé en fonction de votre version de Windows :

   - Windows 10 et Windows 11

   ```
   $KeyPrefix = "latest/AMD_GPU_WINDOWS10"
   ```

   - Windows Server 2016

   ```
   $KeyPrefix = "archives"
   ```

   - Windows Server 2019

   ```
   $KeyPrefix = "latest/AMD_GPU_WINDOWS_2K19 # use "archives" for Windows Server
    2016"
   ```

   - Windows Server 2022

   ```
   $KeyPrefix = "latest/AMD_GPU_WINDOWS_2K22"
   ```

4. Téléchargez les pilotes depuis Amazon S3 sur votre bureau à l'aide des PowerShell commandes suivantes.

```
$Bucket = "ec2-amd-windows-drivers"
$LocalPath = "$home\Desktop\AMD"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
    $LocalFilePath = Join-Path $LocalPath $LocalFileName
    Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
    }
}
```

5. Décompressez le fichier de pilote téléchargé et exécutez le programme d'installation à l'aide des PowerShell commandes suivantes.

```
Expand-Archive $LocalFilePath -DestinationPath "$home\Desktop\AMD\$KeyPrefix" -
Verbose
```

Vérifiez maintenant le contenu du nouveau répertoire. Le nom du répertoire peut être récupéré à l'aide de la `Get-ChildItem` PowerShell commande.

```
Get-ChildItem "$home\Desktop\AMD\$KeyPrefix"
```

La sortie doit ressembler à ce qui suit :

```
Directory: C:\Users\Administrator\Desktop\AMD\latest

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----       10/13/2021  12:52 AM                210414a-365562C-Retail_End_User.2
```

Installez les pilotes :

```
pnputil /add-driver $home\Desktop\AMD\$KeyPrefix\*.inf /install /subdirs
```

6. Suivez les instructions pour installer le pilote et redémarrez votre instance le cas échéant.
7. Pour vérifier que le GPU fonctionne correctement, consultez le Gestionnaire de périphériques. La « AMD Radeon Pro V520 Mx GPU » devrait apparaître dans la liste des adaptateurs d'affichage.
8. Pour tirer parti des quatre écrans d'une résolution maximale de 4K, configurez le protocole d'affichage haute performance NICEDCV.

NVIDIApilotes pour votre EC2 instance Amazon

Le pilote approprié NVIDIA doit être installé sur une instance associée NVIDIAGPU, telle qu'une instance P3 ou G4dn. Selon le type d'instance, vous pouvez soit télécharger un NVIDIA pilote public, soit télécharger un pilote disponible uniquement pour les AWS clients depuis Amazon S3, soit en utiliser un AMI avec le pilote préinstallé.

Pour installer des AMD pilotes sur une instance associée AMDGPU, telle qu'une instance G4ad, consultez. AMDpilotes Pour installer NVIDIA les pilotes, voirNVIDIApilotes.

Table des matières

Types de NVIDIA conducteurs

Les principaux types de NVIDIA pilotes pouvant être utilisés avec les instances GPU basées sont les suivants.

Pilotes Tesla

Ces pilotes sont principalement destinés aux charges de travail informatiques, qui sont utilisées GPUs pour des tâches informatiques telles que les calculs à virgule flottante parallélisés pour l'apprentissage automatique et les transformations de Fourier rapides pour les applications informatiques hautes performances.

GRIDpilotes

Ces pilotes sont certifiés pour fournir des performances optimales pour les applications de visualisation professionnelles qui traitent des contenus tels que des modèles 3D ou des vidéos haute résolution. Vous pouvez configurer GRID les pilotes pour qu'ils prennent en charge deux modes. Les stations de travail virtuelles Quadro donnent accès à quatre écrans 4K par unité. GPU GRID vApps fournir des capacités d'hébergement d'RDSHapplications.

Pilotes de jeu

Ces pilotes contiennent des optimisations pour le jeu et sont fréquemment mis à jour pour améliorer les performances. Ils prennent en charge un seul écran 4K parGPU.

Mode configuré

Sous Windows, les pilotes Tesla sont configurés pour fonctionner en mode Tesla Compute Cluster (TCC). Les pilotes GRID et les pilotes de jeu sont configurés pour fonctionner en mode Windows Display Driver Model (WDDM). En TCC mode, la carte est dédiée au calcul des charges de travail. En WDDM mode, la carte prend en charge les charges de travail informatiques et graphiques.

NVIDIApanneau de commande

Le panneau NVIDIA de commande est compatible avec les pilotes GRID et Gaming. Il n'est pas pris en charge avec les pilotes Tesla.

Pris en charge APIs pour Tesla GRID et les pilotes de jeux

- OpenCL, OpenGL et Vulkan
- NVIDIACUDAet bibliothèques associées (par exemple, cuDNN, TensorRT, JPEG nv et cu) BLAS
- NVENCpour le codage vidéo et NVDEC pour le décodage vidéo
- Windows uniquement : DirectX, APIs Direct2D, accélération vidéo DirectX, Raytracing DirectX

Pilotes disponibles par type d'instance

Le tableau suivant récapitule les NVIDIA pilotes pris en charge pour chaque type d'GPUinstance.

Type d'instance	Pilote Tesla	GRIDchauffeur	Pilote de jeu
G3	Oui	Oui	Non
G4dn	Oui	Oui	Oui
G5	Oui	Oui	Oui
G5g	Oui [1]	Non	Non
G6	Oui	Oui	Non
G6e	Oui	Non	Non
Gr 6	Oui	Oui	Non
P2	Oui	Non	Non
P3	Oui	Non	Non

Type d'instance	Pilote Tesla	GRIDchauffeur	Pilote de jeu
P4d	Oui	Non	Non
P4de	Oui	Non	Non

[1] Ce pilote Tesla prend également en charge les applications graphiques optimisées spécifiques à la ARM64 plate-forme

[2] En utilisant Marketplace AMIs uniquement

Options d'installation

Utilisez l'une des options suivantes pour obtenir les NVIDIA pilotes requis pour votre GPU instance.

Options

- Option 1 : AMIs avec NVIDIA les pilotes installés
- Option 2 : NVIDIA Conducteurs publics
- Option 3 : GRID pilotes (instances G6, Gr6, G5, G4dn et G3)
- Option 4 : pilotes NVIDIA de jeu (instances G5 et G4dn)

Option 1 : AMIs avec NVIDIA les pilotes installés

AWS et NVIDIA proposent différentes Amazon Machine Images (AMIs) fournies avec les NVIDIA pilotes installés.

- Offres Marketplace avec le pilote Tesla
- Les offres Marketplace avec GRID chauffeur
- Offres Marketplace avec le pilote de jeu

Pour passer en revue les considérations qui dépendent de la plate-forme de votre système d'exploitation (OS), choisissez l'onglet qui s'applique à votreAMI.

Linux

Pour mettre à jour la version du pilote installée à l'aide de l'un d'entre euxAMIs, vous devez désinstaller les NVIDIA packages de votre instance afin d'éviter les conflits de versions. Utilisez cette commande pour désinstaller les NVIDIA packages :

```
[ec2-user ~]$ sudo yum erase nvidia cuda
```

Le package du CUDA kit d'outils dépend des NVIDIA pilotes. La désinstallation des NVIDIA packages efface le kit d'outils. CUDA Vous devez réinstaller le CUDA kit d'outils après avoir installé le NVIDIA pilote.

Windows

Si vous créez un Windows personnalisé à AMI l'aide de l'une des AWS Marketplace offres, AMI il doit s'agir d'une image standardisée créée avec Windows Sysprep pour garantir le fonctionnement du GRID pilote. Pour de plus amples informations, veuillez consulter Créez un Amazon à EC2 AMI l'aide de Windows Sysprep.

Option 2 : NVIDIA Conducteurs publics

Les options proposées AWS sont accompagnées du permis nécessaire pour le conducteur. Alternativement, vous pouvez installer les pilotes publics et apporter votre propre licence. Pour installer un pilote public, téléchargez-le depuis le NVIDIA site comme décrit ici.

Vous pouvez également utiliser les options proposées par les conducteurs publics à la AWS place. Pour utiliser un GRID pilote sur une instance P3, utilisez le AWS Marketplace AMIs comme décrit dans l'option 1. Pour utiliser un GRID pilote sur une instance G6, G6e, Gr6, G5, G4dn ou G3, utilisez le AWS Marketplace AMIs comme décrit dans l'option 1 ou installez les NVIDIA pilotes fournis par comme décrit dans. AWS Option 3 : GRID pilotes (instances G6, Gr6, G5, G4dn et G3)

Pour télécharger un NVIDIA pilote public

Connectez-vous à votre instance et téléchargez le NVIDIA pilote 64 bits correspondant au type d'instance depuis http://www.nvidia.com/Download/Find.aspx. Pour Type de produit, Série de produits et Produit, utilisez les options du tableau suivant.

Instance	Type de produit	Série de produits	Produit
G3	Tesla	M-Class	M60

Instance	Type de produit	Série de produits	Produit
G4dn	Tesla	T-Series	T4
G5 1	Tesla	Série A	A10
G5 g 2	Tesla	T-Series	NVIDIAT4G
G-6 (3)	Tesla	Série L	L4
G6E 4	Tesla	Série L	ANNÉES 40
Gr 6 3	Tesla	Série L	L4
P2	Tesla	Série K	K80
P3	Tesla	Série V	V100
P4d	Tesla	Série A	A100
P4de	Tesla	Série A	A100
P5 (5)	Tesla	Série H	H100

[1] Les instances G5 nécessitent la version 470.00 ou ultérieure du pilote.

[2] instances G5g nécessitent la version du pilote 470.82.01 ou ultérieure. Le système d'exploitation est Linux aarch64.

[3] Les instances G6 et Gr6 nécessitent la version du pilote 525.0 ou ultérieure.

[4] instances G6e nécessitent la version 535.0 ou ultérieure du pilote.

[5] instances P5 nécessitent la version 530 ou ultérieure du pilote.

Pour installer le NVIDIA pilote sur les systèmes d'exploitation Linux, consultez le Guide de démarrage rapide d'installation du NVIDIA pilote.

Pour installer le NVIDIA pilote sous Windows, procédez comme suit :

1. Ouvrez le dossier dans lequel vous avez téléchargé le pilote et lancez le fichier d'installation. Suivez les instructions pour installer le pilote et redémarrez votre instance le cas échéant.

2. Désactivez la carte vidéo nommée Microsoft Basic Display Adapter qui est marquée d'une icône d'avertissement à l'aide du Gestionnaire de périphériques. Installez les fonctionnalités Windows : Media Foundation et Quality Windows Audio Video Experience.

   > **Important**
   >
   > Ne désactivez pas la carte vidéo nommée Microsoft Remote Display Adapter. Si Microsoft Remote Display Adapter est désactivée, votre connexion peut s'interrompre et les tentatives de connexion à l'instance après son redémarrage peuvent échouer.

3. Vérifiez le Gestionnaire de périphériques pour vérifier qu'GPUil fonctionne correctement.
4. Pour optimiser vos performancesGPU, suivez les étapes d'optimisation décrites dansOptimisation GPU des paramètres sur les EC2 instances Amazon.

Option 3 : GRID pilotes (instances G6, Gr6, G5, G4dn et G3)

Ces téléchargements ne sont disponibles que pour AWS les clients. En téléchargeant, afin de respecter les exigences de la AWS solution mentionnées dans le contrat de licence utilisateur final du NVIDIA GRID cloud (EULA), vous acceptez d'utiliser le logiciel téléchargé uniquement AMIs pour le développer en vue de l'utiliser avec le matériel NVIDIA L4, NVIDIA A10G, NVIDIA Tesla T4 ou NVIDIA Tesla M60. Lors de l'installation du logiciel, vous êtes lié par les termes du contrat de licence utilisateur final du NVIDIA GRID Cloud. Pour plus d'informations sur la version du NVIDIA GRID pilote pour votre système d'exploitation, consultez la documentation du logiciel NVIDIA® Virtual GPU (vGPU) sur le NVIDIAsite Web.

Considérations

- Les instances G6 et Gr6 nécessitent la version GRID 17.1 ou une version ultérieure.
- Les instances G5 nécessitent la version GRID 13.1 ou une version ultérieure (ou la version GRID 12.4 ou une version ultérieure).
- Les instances G3 nécessitent une DNS résolution AWS fournie pour que la GRID licence fonctionne.
- IMDSv2n'est pris en charge qu'avec la version 14.0 ou supérieure du NVIDIA pilote.
- Pour les instances Windows, si vous lancez votre instance à partir d'un système Windows personnaliséAMI, AMI il doit s'agir d'une image standardisée créée avec Windows Sysprep pour garantir le fonctionnement du GRID pilote. Pour de plus amples informations, veuillez consulter Créez un Amazon à EC2 AMI l'aide de Windows Sysprep.

- GRIDLes versions 17.0 et ultérieures ne sont pas compatibles avec Windows Server 2019.
- GRIDLes versions 14.2 et ultérieures ne sont pas compatibles avec Windows Server 2016.
- GRIDLes versions 17.0 et ultérieures ne sont pas prises en charge avec les instances G3.

Amazon Linux et Amazon Linux 2

Pour installer le NVIDIA GRID pilote sur votre instance

1. Connectez-vous à votre instance Linux.
2. Installez-le AWS CLI sur votre instance Linux et configurez les informations d'identification par défaut. Pour plus d'informations, consultez Installation d' AWS CLI dans le Guide de l'utilisateur AWS Command Line Interface .

   > **Important**
   >
   > Votre utilisateur ou rôle doit disposer des autorisations accordées conformément à la politique d'AmazonS3 ReadOnlyAccess. Pour plus d'informations, consultez la politique AWS gérée : AmazonS3 ReadOnlyAccess dans le guide de l'utilisateur d'Amazon Simple Storage Service.

3. Installez gcc et make, si ce n'est pas déjà fait.

   ```
   [ec2-user ~]$ sudo yum install gcc make
   ```

4. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

   ```
   [ec2-user ~]$ sudo yum update -y
   ```

5. Redémarrez votre instance pour charger la dernière version du noyau.

   ```
   [ec2-user ~]$ sudo reboot
   ```

6. Reconnectez-vous à votre instance après son redémarrage.
7. Installez le compilateur gcc et le package d'en-têtes de noyau correspondant à la version du noyau que vous utilisez actuellement.

   ```
   [ec2-user ~]$ sudo yum install -y kernel-devel-$(uname -r)
   ```

8. Téléchargez l'utilitaire d'installation du GRID pilote à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Plusieurs versions du GRID pilote sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

9. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

10. Exécutez le script d'auto-installation comme suit pour installer le GRID pilote que vous avez téléchargé. Par exemple :

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

> **Note**
>
> Si vous utilisez Amazon Linux 2 avec la version 5.10 du noyau, utilisez la commande suivante pour installer le GRID pilote.
>
> ```
> [ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
> ```

Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

11. Vérifiez que le pilote fonctionne. La réponse à la commande suivante répertorie la version installée du NVIDIA pilote et des informations sur leGPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

12. Si vous utilisez le GPU logiciel NVIDIA v version 14.x ou supérieure sur les instances G4dn, G5 ou G5g, GSP désactivez-le à l'aide des commandes suivantes. Pour plus d'informations, pour savoir pourquoi cela est nécessaire, consultez NVIDIAla documentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

13. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

14. (Facultatif) Selon votre cas d'utilisation, vous pouvez effectuer les étapes facultatives suivantes. Si vous n'avez pas besoin de cette fonctionnalité, n'effectuez pas ces étapes.

    a. Pour tirer parti des quatre écrans d'une résolution maximale de 4K, configurez le protocole d'affichage haute performance NICEDCV.

    b. NVIDIALe mode Quadro Virtual Workstation est activé par défaut. Pour activer les applications GRID virtuelles pour les fonctionnalités d'hébergement d'RDSHapplications, suivez les étapes d'activation des applications GRID virtuelles décrites dansActivez des applications NVIDIA GRID virtuelles sur vos instances EC2 GPU basées sur Amazon.

CentOS 7 et Red Hat Enterprise Linux 7

Pour installer le NVIDIA GRID pilote sur votre instance

1. Connectez-vous à votre instance Linux. Installez gcc et make, si ce n'est pas déjà fait.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

2. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
[ec2-user ~]$ sudo yum update -y
```

3. Redémarrez votre instance pour charger la dernière version du noyau.

```
[ec2-user ~]$ sudo reboot
```

4. Reconnectez-vous à votre instance après son redémarrage.

5. Installez le package d'en-têtes du noyau correspondant à la version du noyau que vous utilisez actuellement.

```
[ec2-user ~]$ sudo yum install -y kernel-devel-$(uname -r)
```

6. Désactivez le pilote nouveau open source pour les cartes NVIDIA graphiques.

   a. Ajoutez nouveau au fichier de liste noire `/etc/modprobe.d/blacklist.conf`. Copiez le bloc de code suivant et collez-le dans un terminal.

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Modifiez le fichier `/etc/default/grub` et ajoutez la ligne suivante :

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. Générez à nouveau la configuration Grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Téléchargez l'utilitaire d'installation du GRID pilote à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   Plusieurs versions du GRID pilote sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

8. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

9. Exécutez le script d'auto-installation comme suit pour installer le GRID pilote que vous avez téléchargé. Par exemple :

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

   Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

10. Vérifiez que le pilote fonctionne. La réponse à la commande suivante répertorie la version installée du NVIDIA pilote et des informations sur leGPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

11. Si vous utilisez le GPU logiciel NVIDIA v version 14.x ou supérieure sur les instances G4dn, G5 ou G5g, GSP désactivez-le à l'aide des commandes suivantes. Pour plus d'informations, pour savoir pourquoi cela est nécessaire, consultez NVIDIAla documentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

12. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

13. (Facultatif) Selon votre cas d'utilisation, vous pouvez effectuer les étapes facultatives suivantes. Si vous n'avez pas besoin de cette fonctionnalité, n'effectuez pas ces étapes.

    a. Pour tirer parti des quatre écrans d'une résolution maximale de 4K, configurez le protocole d'affichage haute performance NICEDCV.

    b. NVIDIALe mode Quadro Virtual Workstation est activé par défaut. Pour activer les applications GRID virtuelles pour les fonctionnalités d'hébergement d'RDSHapplications, suivez les étapes d'activation des applications GRID virtuelles décrites dansActivez des applications NVIDIA GRID virtuelles sur vos instances EC2 GPU basées sur Amazon.

    c. Installez le package de GUI bureau/station de travail.

```
[ec2-user ~]$ sudo yum groupinstall -y "Server with GUI"
```

CentOS Stream 8 et Red Hat Enterprise Linux 8

Pour installer le NVIDIA GRID pilote sur votre instance

1. Connectez-vous à votre instance Linux. Installez gcc et make, si ce n'est pas déjà fait.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

2. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
[ec2-user ~]$ sudo yum update -y
```

3. Redémarrez votre instance pour charger la dernière version du noyau.

```
[ec2-user ~]$ sudo reboot
```

4. Reconnectez-vous à votre instance après son redémarrage.
5. Installez le package d'en-têtes du noyau correspondant à la version du noyau que vous utilisez actuellement.

```
[ec2-user ~]$ sudo dnf install -y elfutils-libelf-devel libglvnd-devel kernel-
devel-$(uname -r)
```

6. Téléchargez l'utilitaire d'installation du GRID pilote à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   Plusieurs versions du GRID pilote sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Exécutez le script d'auto-installation comme suit pour installer le GRID pilote que vous avez téléchargé. Par exemple :

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

9. Vérifiez que le pilote fonctionne. La réponse à la commande suivante répertorie la version installée du NVIDIA pilote et des informations sur leGPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Si vous utilisez le GPU logiciel NVIDIA v version 14.x ou supérieure sur les instances G4dn, G5 ou G5g, GSP désactivez-le à l'aide des commandes suivantes. Pour plus d'informations, pour savoir pourquoi cela est nécessaire, consultez NVIDIAla documentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

12. (Facultatif) Selon votre cas d'utilisation, vous pouvez effectuer les étapes facultatives suivantes. Si vous n'avez pas besoin de cette fonctionnalité, n'effectuez pas ces étapes.

    a. Pour tirer parti des quatre écrans d'une résolution maximale de 4K, configurez le protocole d'affichage haute performance NICEDCV.

    b. NVIDIALe mode Quadro Virtual Workstation est activé par défaut. Pour activer les applications GRID virtuelles pour les fonctionnalités d'hébergement d'RDSHapplications, suivez les étapes d'activation des applications GRID virtuelles décrites dansActivez des applications NVIDIA GRID virtuelles sur vos instances EC2 GPU basées sur Amazon.

    c. Installez le package du GUI poste de travail.

    ```
    [ec2-user ~]$ sudo dnf groupinstall -y workstation
    ```

Rocky Linux 8

Pour installer le NVIDIA GRID pilote sur votre instance Linux

1. Connectez-vous à votre instance Linux. Installez gcc et make, si ce n'est pas déjà fait.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

2. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
[ec2-user ~]$ sudo yum update -y
```

3. Redémarrez votre instance pour charger la dernière version du noyau.

```
[ec2-user ~]$ sudo reboot
```

4. Reconnectez-vous à votre instance après son redémarrage.
5. Installez le package d'en-têtes du noyau correspondant à la version du noyau que vous utilisez actuellement.

```
[ec2-user ~]$ sudo dnf install -y elfutils-libelf-devel libglvnd-devel kernel-
devel-$(uname -r)
```

6. Téléchargez l'utilitaire d'installation du GRID pilote à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   Plusieurs versions du GRID pilote sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Exécutez le script d'auto-installation comme suit pour installer le GRID pilote que vous avez téléchargé. Par exemple :

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

9. Vérifiez que le pilote fonctionne. La réponse à la commande suivante répertorie la version installée du NVIDIA pilote et des informations sur leGPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Si vous utilisez le GPU logiciel NVIDIA v version 14.x ou supérieure sur les instances G4dn, G5 ou G5g, GSP désactivez-le à l'aide des commandes suivantes. Pour plus d'informations, pour savoir pourquoi cela est nécessaire, consultez NVIDIAla documentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

12. (Facultatif) Selon votre cas d'utilisation, vous pouvez effectuer les étapes facultatives suivantes. Si vous n'avez pas besoin de cette fonctionnalité, n'effectuez pas ces étapes.

    a. Pour tirer parti des quatre écrans d'une résolution maximale de 4K, configurez le protocole d'affichage haute performance NICEDCV.

    b. NVIDIALe mode Quadro Virtual Workstation est activé par défaut. Pour activer les applications GRID virtuelles pour les fonctionnalités d'hébergement d'RDSHapplications, suivez les étapes d'activation des applications GRID virtuelles décrites dansActivez des applications NVIDIA GRID virtuelles sur vos instances EC2 GPU basées sur Amazon.

Ubuntu et Debian

Pour installer le NVIDIA GRID pilote sur votre instance

1. Connectez-vous à votre instance Linux. Installez gcc et make, si ce n'est pas déjà fait.

```
[ec2-user ~]$ sudo apt-get install -y gcc make
```

2. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
$ sudo apt-get update -y
```

3. (Ubuntu) Mettez à niveau le package `linux-aws` pour recevoir la version la plus récente.

```
$ sudo apt-get upgrade -y linux-aws
```

(Debian) Mettez à niveau le package pour recevoir la version la plus récente.

```
$ sudo apt-get upgrade -y
```

4. Redémarrez votre instance pour charger la dernière version du noyau.

```
$ sudo reboot
```

5. Reconnectez-vous à votre instance après son redémarrage.
6. Installez le compilateur gcc et le package d'en-têtes de noyau correspondant à la version du noyau que vous utilisez actuellement.

```
$ sudo apt-get install -y linux-headers-$(uname -r)
```

7. Désactivez le pilote `nouveau` open source pour les cartes NVIDIA graphiques.

   a. Ajoutez `nouveau` au fichier de liste noire `/etc/modprobe.d/blacklist.conf`. Copiez le bloc de code suivant et collez-le dans un terminal.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Modifiez le fichier `/etc/default/grub` et ajoutez la ligne suivante :

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

c. Générez à nouveau la configuration Grub.

```
$ sudo update-grub
```

8. Téléchargez l'utilitaire d'installation du GRID pilote à l'aide de la commande suivante :

```
$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Plusieurs versions du GRID pilote sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante.

```
$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

9. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante.

```
$ chmod +x NVIDIA-Linux-x86_64*.run
```

10. Exécutez le script d'auto-installation comme suit pour installer le GRID pilote que vous avez téléchargé. Par exemple :

```
$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

11. Vérifiez que le pilote fonctionne. La réponse à la commande suivante répertorie la version installée du NVIDIA pilote et des informations sur leGPUs.

```
$ nvidia-smi -q | head
```

12. Si vous utilisez le GPU logiciel NVIDIA v version 14.x ou supérieure sur les instances G4dn, G5 ou G5g, GSP désactivez-le à l'aide des commandes suivantes. Pour plus d'informations, pour savoir pourquoi cela est nécessaire, consultez NVIDIAla documentation.

```
$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/
modprobe.d/nvidia.conf
```

13. Redémarrez l'instance.

```
$ sudo reboot
```

14. (Facultatif) Selon votre cas d'utilisation, vous pouvez effectuer les étapes facultatives suivantes. Si vous n'avez pas besoin de cette fonctionnalité, n'effectuez pas ces étapes.

    a. Pour tirer parti des quatre écrans d'une résolution maximale de 4K, configurez le protocole d'affichage haute performance NICEDCV.

    b. NVIDIALe mode Quadro Virtual Workstation est activé par défaut. Pour activer les applications GRID virtuelles pour les fonctionnalités d'hébergement d'RDSHapplications, suivez les étapes d'activation des applications GRID virtuelles décrites dansActivez des applications NVIDIA GRID virtuelles sur vos instances EC2 GPU basées sur Amazon.

    c. Installez le package de GUI bureau/station de travail.

```
$ sudo apt-get install -y lightdm ubuntu-desktop
```

Systèmes d'exploitation Windows

Pour installer le NVIDIA GRID pilote sur votre instance Windows

1. Connectez-vous à votre instance Windows et ouvrez une PowerShell fenêtre.
2. Configurez les informations d'identification par défaut pour votre instance Windows. AWS Tools for Windows PowerShell Pour plus d'informations, voir Démarrer avec les AWS Tools for Windows PowerShell dans le Guide de l'utilisateur AWS Tools for Windows PowerShell .

> **Important**
>
> Votre utilisateur ou rôle doit disposer des autorisations accordées conformément à la politique d'AmazonS3 ReadOnlyAccess. Pour plus d'informations, consultez la politique AWS gérée : AmazonS3 ReadOnlyAccess dans le guide de l'utilisateur d'Amazon Simple Storage Service.

3. Téléchargez les pilotes et le contrat de licence utilisateur final du NVIDIA GRID cloud depuis Amazon S3 sur votre bureau à l'aide des PowerShell commandes suivantes.

```
$Bucket = "ec2-windows-nvidia-drivers"
$KeyPrefix = "latest"
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
    $LocalFilePath = Join-Path $LocalPath $LocalFileName
    Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

   Plusieurs versions du NVIDIA GRID pilote sont stockées dans ce compartiment. Vous pouvez télécharger toutes les versions Windows disponibles dans le compartiment en supprimant l'option `-KeyPrefix $KeyPrefix`. Pour plus d'informations sur la version du NVIDIA GRID pilote pour votre système d'exploitation, consultez la documentation du logiciel NVIDIA® Virtual GPU (vGPU) sur le NVIDIAsite Web.

   À partir de GRID la version 11.0, vous pouvez utiliser les pilotes ci-dessous `latest` pour les instances G3 et G4dn. Nous n'ajouterons pas les versions postérieures à 11.0 à `g4/latest`, mais nous conserverons la version 11.0 et les versions antérieures spécifiques à G4dn sous `g4/latest`.

   Les instances G5 nécessitent la version GRID 13.1 ou une version ultérieure (ou la version GRID 12.4 ou une version ultérieure).

4. Accédez au bureau et double-cliquez sur le fichier d'installation pour le lancer (choisissez la version du pilote qui correspond à la version du système d'exploitation de votre instance). Suivez les instructions pour installer le pilote et redémarrez votre instance le cas échéant. Pour vérifier que le GPU fonctionne correctement, consultez le Gestionnaire de périphériques.

5. (Facultatif) Utilisez la commande suivante pour désactiver la page de licence dans le panneau de configuration afin d'empêcher les utilisateurs de modifier accidentellement le type de produit (NVIDIAGRIDVirtual Workstation est activé par défaut). Pour plus d'informations, consultez le Guide de l'utilisateur des GRID licences.

   PowerShell

Exécutez les PowerShell commandes suivantes pour créer la valeur de registre afin de désactiver la page de licence dans le panneau de configuration. AWS Windows AMIs utilise par défaut la version 32 bits et cette commande échoue. AWS Tools for PowerShell Utilisez plutôt la version 64 bits PowerShell fournie avec le système d'exploitation.

```
New-Item -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name GridLicensing
New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" -
Name "NvCplDisableManageLicensePage" -PropertyType "DWord" -Value "1"
```

Invite de commande

Exécutez la commande de registre suivante pour créer la valeur de registre afin de désactiver la page des licences dans le panneau de configuration. Vous pouvez l'exécuter à l'aide de la fenêtre d'invite de commandes ou d'une version 64 bits dePowerShell.

```
reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" /v
 NvCplDisableManageLicensePage /t REG_DWORD /d 1
```

6. (Facultatif) Selon votre cas d'utilisation, vous pouvez effectuer les étapes facultatives suivantes. Si vous n'avez pas besoin de cette fonctionnalité, n'effectuez pas ces étapes.

   a. Pour tirer parti des quatre écrans d'une résolution maximale de 4K, configurez le protocole d'affichage haute performance NICEDCV.

   b. NVIDIALe mode Quadro Virtual Workstation est activé par défaut. Pour activer les applications GRID virtuelles pour les fonctionnalités d'hébergement d'RDSHapplications, suivez les étapes d'activation des applications GRID virtuelles décrites dansActivez des applications NVIDIA GRID virtuelles sur vos instances EC2 GPU basées sur Amazon.

Option 4 : pilotes NVIDIA de jeu (instances G5 et G4dn)

Ces pilotes ne sont disponibles que pour AWS les clients. En les téléchargeant, vous acceptez de n'utiliser le logiciel téléchargé que AMIs pour le développer en vue d'une utilisation avec le NVIDIA matériel A10G et NVIDIA Tesla T4. Lors de l'installation du logiciel, vous êtes lié par les termes du contrat de licence utilisateur final du NVIDIA GRID Cloud.

Considérations

- Les instances G3 nécessitent une DNS résolution AWS fournie pour que la GRID licence fonctionne.
- IMDSv2n'est pris en charge qu'avec la version 495.x ou supérieure du NVIDIA pilote.

Prérequis

Avant d'installer les pilotes NVIDIA de jeu, vérifiez qu'ils sont AWS CLI installés sur votre instance et que vous avez configuré les informations d'identification par défaut. Pour plus d'informations, consultez Installation d' AWS CLI dans le Guide de l'utilisateur AWS Command Line Interface .

> **Important**
>
> Votre utilisateur ou rôle doit disposer des autorisations accordées conformément à la politique d'AmazonS3 ReadOnlyAccess. Pour plus d'informations, consultez la politique AWS gérée : AmazonS3 ReadOnlyAccess dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Amazon Linux et Amazon Linux 2

Pour installer le pilote NVIDIA de jeu sur votre instance

1. Connectez-vous à votre instance Linux.
2. Installez gcc et make, si ce n'est pas déjà fait.

```
[ec2-user ~]$ sudo yum install gcc make
```

3. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
[ec2-user ~]$ sudo yum update -y
```

4. Redémarrez votre instance pour charger la dernière version du noyau.

```
[ec2-user ~]$ sudo reboot
```

5. Reconnectez-vous à votre instance après son redémarrage.

6. Installez le package d'en-têtes du noyau correspondant à la version du noyau que vous utilisez actuellement.

```
[ec2-user ~]$ sudo yum install -y kernel-devel-$(uname -r)
```

7. Téléchargez l'utilitaire d'installation du pilote de jeu à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   Plusieurs versions du pilote de jeu sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

8. Extrayez l'utilitaire d'installation du pilote de jeu de l'archive téléchargé `.zip`.

```
[ec2-user ~]$ unzip latest-driver-name.zip -d nvidia-drivers
```

9. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante :

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

10. Exécutez le programme d'installation à l'aide de la commande suivante :

```
[ec2-user ~]$ sudo ./nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

> **Note**
>
> Si vous utilisez Amazon Linux 2 avec la version 5.10 du noyau, utilisez la commande suivante pour installer les pilotes de NVIDIA jeu.
>
> ```
> [ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
> ```

   Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

11. Utilisez la commande suivante pour créer le fichier de configuration requis.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

12. Utilisez la commande suivante pour télécharger et renommer le fichier de certification.

    - Pour la version 460.39 ou ultérieure :

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
      ```

    - Pour les versions 440.68 à 445.48 :

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
      ```

    - Pour des versions antérieures :

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
      ```

13. Si vous utilisez la version 510.x ou supérieure du NVIDIA pilote sur les instances G4dn, G5 ou G5g, désactivez-la à l'aide des commandes suivantes. GSP Pour plus d'informations, pour savoir pourquoi cela est nécessaire, consultez NVIDIAla documentation.

    ```
    [ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
    ```

    ```
    [ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
    ```

14. Redémarrez l'instance.

    ```
    [ec2-user ~]$ sudo reboot
    ```

15. (Facultatif) Pour tirer parti d'un affichage unique d'une résolution maximale de 4K, configurez le protocole d'affichage haute performance NICEDCV.

CentOS 7 et Red Hat Enterprise Linux 7

Pour installer le pilote NVIDIA de jeu sur votre instance

1. Connectez-vous à votre instance Linux. Installez gcc et make, si ce n'est pas déjà fait.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

2. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
[ec2-user ~]$ sudo yum update -y
```

3. Redémarrez votre instance pour charger la dernière version du noyau.

```
[ec2-user ~]$ sudo reboot
```

4. Reconnectez-vous à votre instance après son redémarrage.
5. Installez le package d'en-têtes du noyau correspondant à la version du noyau que vous utilisez actuellement.

```
[ec2-user ~]$ sudo yum install -y unzip kernel-devel-$(uname -r)
```

6. Désactivez le pilote `nouveau` open source pour les cartes NVIDIA graphiques.

   a. Ajoutez `nouveau` au fichier de liste noire `/etc/modprobe.d/blacklist.conf`. Copiez le bloc de code suivant et collez-le dans un terminal.

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Modifiez le fichier `/etc/default/grub` et ajoutez la ligne suivante :

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. Générez à nouveau la configuration Grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Téléchargez l'utilitaire d'installation du pilote de jeu à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Plusieurs versions du pilote de jeu sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

8. Extrayez l'utilitaire d'installation du pilote de jeu de l'archive téléchargé `.zip`.

```
[ec2-user ~]$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

9. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante :

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

10. Exécutez le programme d'installation à l'aide de la commande suivante :

```
[ec2-user ~]$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

11. Utilisez la commande suivante pour créer le fichier de configuration requis.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

12. Utilisez la commande suivante pour télécharger et renommer le fichier de certification.
    - Pour la version 460.39 ou ultérieure :

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

    - Pour les versions 440.68 à 445.48 :

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Pour des versions antérieures :

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

13. Si vous utilisez la version 510.x ou supérieure du NVIDIA pilote sur les instances G4dn, G5 ou G5g, désactivez-la à l'aide des commandes suivantes. GSP Pour plus d'informations, pour savoir pourquoi cela est nécessaire, consultez NVIDIAla documentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

14. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

15. (Facultatif) Pour tirer parti d'un affichage unique d'une résolution maximale de 4K, configurez le protocole d'affichage haute performance NICEDCV. Si vous n'avez pas besoin de cette fonctionnalité, n'effectuez pas cette étape.

CentOS Stream 8 et Red Hat Enterprise Linux 8

Pour installer le pilote NVIDIA de jeu sur votre instance

1. Connectez-vous à votre instance Linux. Installez gcc et make, si ce n'est pas déjà fait.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

2. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
[ec2-user ~]$ sudo yum update -y
```

3. Redémarrez votre instance pour charger la dernière version du noyau.

```
[ec2-user ~]$ sudo reboot
```

4. Reconnectez-vous à votre instance après son redémarrage.
5. Installez le package d'en-têtes du noyau correspondant à la version du noyau que vous utilisez actuellement.

```
[ec2-user ~]$ sudo yum install -y unzip kernel-devel-$(uname -r)
```

6. Téléchargez l'utilitaire d'installation du pilote de jeu à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   Plusieurs versions du pilote de jeu sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Extrayez l'utilitaire d'installation du pilote de jeu de l'archive téléchargé `.zip`.

```
[ec2-user ~]$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante :

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

9. Exécutez le programme d'installation à l'aide de la commande suivante :

```
[ec2-user ~]$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

   Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

10. Utilisez la commande suivante pour créer le fichier de configuration requis.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Utilisez la commande suivante pour télécharger et renommer le fichier de certification.
    - Pour la version 460.39 ou ultérieure :

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
      ```

    - Pour les versions 440.68 à 445.48 :

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
      ```

    - Pour des versions antérieures :

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
      ```

12. Si vous utilisez la version 510.x ou supérieure du NVIDIA pilote sur les instances G4dn, G5 ou G5g, désactivez-la à l'aide des commandes suivantes. GSP Pour plus d'informations, pour savoir pourquoi cela est nécessaire, consultez NVIDIAla documentation.

    ```
    [ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
    ```

    ```
    [ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
    ```

13. Redémarrez l'instance.

    ```
    [ec2-user ~]$ sudo reboot
    ```

14. (Facultatif) Pour tirer parti d'un affichage unique d'une résolution maximale de 4K, configurez le protocole d'affichage haute performance NICEDCV.

Rocky Linux 8

Pour installer le pilote NVIDIA de jeu sur votre instance

1. Connectez-vous à votre instance Linux. Installez gcc et make, si ce n'est pas déjà fait.

   ```
   [ec2-user ~]$ sudo yum install -y gcc make
   ```

2. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
[ec2-user ~]$ sudo yum update -y
```

3. Redémarrez votre instance pour charger la dernière version du noyau.

```
[ec2-user ~]$ sudo reboot
```

4. Reconnectez-vous à votre instance après son redémarrage.
5. Installez le package d'en-têtes du noyau correspondant à la version du noyau que vous utilisez actuellement.

```
[ec2-user ~]$ sudo dnf install -y unzip elfutils-libelf-devel libglvnd-devel
 kernel-devel-$(uname -r)
```

6. Téléchargez l'utilitaire d'installation du pilote de jeu à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Plusieurs versions du pilote de jeu sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Extrayez l'utilitaire d'installation du pilote de jeu de l'archive téléchargé `.zip`.

```
[ec2-user ~]$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante :

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

9. Exécutez le programme d'installation à l'aide de la commande suivante :

```
[ec2-user ~]$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

10. Utilisez la commande suivante pour créer le fichier de configuration requis.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Utilisez la commande suivante pour télécharger et renommer le fichier de certification.

    - Pour la version 460.39 ou ultérieure :

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

    - Pour les versions 440.68 à 445.48 :

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

    - Pour des versions antérieures :

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Si vous utilisez la version 510.x ou supérieure du NVIDIA pilote sur les instances G4dn, G5 ou G5g, désactivez-la à l'aide des commandes suivantes. GSP Pour plus d'informations, pour savoir pourquoi cela est nécessaire, consultez NVIDIAla documentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

13. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

14. (Facultatif) Pour tirer parti d'un affichage unique d'une résolution maximale de 4K, configurez le protocole d'affichage haute performance NICEDCV.

Ubuntu et Debian

Pour installer le pilote NVIDIA de jeu sur votre instance

1. Connectez-vous à votre instance Linux. Installez gcc et make, si ce n'est pas déjà fait.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

2. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
$ sudo apt-get update -y
```

3. Mettez à niveau le package `linux-aws` pour recevoir la version la plus récente.

```
$ sudo apt-get upgrade -y linux-aws
```

4. Redémarrez votre instance pour charger la dernière version du noyau.

```
$ sudo reboot
```

5. Reconnectez-vous à votre instance après son redémarrage.
6. Installez le package d'en-têtes du noyau correspondant à la version du noyau que vous utilisez actuellement.

```
$ sudo apt-get install -y unzip linux-headers-$(uname -r)
```

7. Désactivez le pilote `nouveau` open source pour les cartes NVIDIA graphiques.

   a. Ajoutez `nouveau` au fichier de liste noire `/etc/modprobe.d/blacklist.conf`. Copiez le bloc de code suivant et collez-le dans un terminal.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Modifiez le fichier `/etc/default/grub` et ajoutez la ligne suivante :

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

c. Générez à nouveau la configuration Grub.

```
$ sudo update-grub
```

8. Téléchargez l'utilitaire d'installation du pilote de jeu à l'aide de la commande suivante :

```
$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Plusieurs versions du pilote de jeu sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante :

```
$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

9. Extrayez l'utilitaire d'installation du pilote de jeu de l'archive téléchargé `.zip`.

```
$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

10. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante :

```
$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

11. Exécutez le programme d'installation à l'aide de la commande suivante :

```
$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

12. Utilisez la commande suivante pour créer le fichier de configuration requis.

```
$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

13. Utilisez la commande suivante pour télécharger et renommer le fichier de certification.

- Pour la version 460.39 ou ultérieure :

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

- Pour les versions 440.68 à 445.48 :

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Pour des versions antérieures :

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

14. Si vous utilisez la version 510.x ou supérieure du NVIDIA pilote sur les instances G4dn, G5 ou G5g, désactivez-la à l'aide des commandes suivantes. GSP Pour plus d'informations, pour savoir pourquoi cela est nécessaire, consultez NVIDIAla documentation.

```
$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/
modprobe.d/nvidia.conf
```

15. Redémarrez l'instance.

```
$ sudo reboot
```

16. (Facultatif) Pour tirer parti d'un affichage unique d'une résolution maximale de 4K, configurez le protocole d'affichage haute performance NICEDCV. Si vous n'avez pas besoin de cette fonctionnalité, n'effectuez pas cette étape.

Systèmes d'exploitation Windows

Avant d'installer un pilote de NVIDIA jeu sur votre instance, vous devez vous assurer que les conditions préalables suivantes sont remplies, en plus des considérations mentionnées pour tous les pilotes de jeu.

- Si vous lancez votre instance Windows à l'aide d'un système Windows personnaliséAMI, AMI il doit s'agir d'une image standardisée créée avec Windows Sysprep pour garantir le bon fonctionnement

du pilote de jeu. Pour de plus amples informations, veuillez consulter Créez un Amazon à EC2 AMI l'aide de Windows Sysprep.

- Configurez les informations d'identification par défaut pour votre instance Windows. AWS Tools for Windows PowerShell Pour plus d'informations, voir Démarrer avec les AWS Tools for Windows PowerShell dans le Guide de l'utilisateur AWS Tools for Windows PowerShell .

Pour installer le pilote NVIDIA de jeu sur votre instance Windows

1. Connectez-vous à votre instance Windows et ouvrez une PowerShell fenêtre.
2. Téléchargez et installez le pilote de jeu à l'aide des PowerShell commandes suivantes.

```
$Bucket = "nvidia-gaming"
$KeyPrefix = "windows/latest"
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
    $LocalFilePath = Join-Path $LocalPath $LocalFileName
    Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

   Plusieurs versions du NVIDIA GRID pilote sont stockées dans ce compartiment S3. Vous pouvez télécharger toutes les versions disponibles dans le compartiment si vous modifiez la valeur de la `$KeyPrefix` variable de "windows/latest" à "windows".
3. Accédez au bureau et double-cliquez sur le fichier d'installation pour le lancer (choisissez la version du pilote qui correspond à la version du système d'exploitation de votre instance). Suivez les instructions pour installer le pilote et redémarrez votre instance le cas échéant. Pour vérifier que le GPU fonctionne correctement, consultez le Gestionnaire de périphériques.
4. Utilisez l'une des méthodes suivantes pour enregistrer le pilote.

   Version 527.27 or above

   Créez la clé de registre suivante à l'aide de la version 64 bits de PowerShell ou de la fenêtre d'invite de commande.

Clé : `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global`

nom : vGamingMarketplace

type : DWord

valeur : 2

PowerShell

Exécutez la PowerShell commande suivante pour créer cette valeur de registre. AWS Windows AMIs utilise par défaut la version 32 bits et cette commande échoue. AWS Tools for PowerShell Utilisez plutôt la version 64 bits PowerShell fournie avec le système d'exploitation.

```
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global"
 -Name "vGamingMarketplace" -PropertyType "DWord" -Value "2"
```

Invite de commande

Exécutez la commande de registre suivante pour créer cette valeur de registre. Vous pouvez l'exécuter à l'aide de la fenêtre d'invite de commandes ou d'une version 64 bits de PowerShell.

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global" /v
 vGamingMarketplace /t REG_DWORD /d 2
```

Earlier versions

Créez la clé de registre suivante à l'aide de la version 64 bits de PowerShell ou de la fenêtre d'invite de commande.

Clé : `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global`

nom : vGamingMarketplace

type : DWord

valeur : 2

PowerShell

Exécutez la PowerShell commande suivante pour créer cette valeur de registre. AWS Windows AMIs utilise par défaut la version 32 bits et cette commande échoue. AWS Tools for PowerShell Utilisez plutôt la version 64 bits PowerShell fournie avec le système d'exploitation.

```
New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name
 "vGamingMarketplace" -PropertyType "DWord" -Value "2"
```

Invite de commande

Exécutez la commande de registre suivante pour créer cette clé de registre avec la fenêtre d'invite de commandes. Vous pouvez également utiliser cette commande dans la version 64 bits dePowerShell.

```
reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global" /v vGamingMarketplace /t
 REG_DWORD /d 2
```

5. Exécutez la commande suivante dans PowerShell. Celle-ci télécharge le fichier de certification, le renomme en `GridSwCert.txt` et le déplace vers le dossier Public Documents (Documents publics) sur votre lecteur système. En général, le chemin du dossier est `C:\Users\Public\Documents`.

   - Pour la version 461.40 ou ultérieure :

     ```
     Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
     Archive/GridSwCertWindows_2023_9_22.cert" -OutFile "$Env:PUBLIC\Documents
     \GridSwCert.txt"
     ```

   - Pour la version 445.87 :

     ```
     Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
     Archive/GridSwCert-Windows_2020_04.cert" -OutFile "$Env:PUBLIC\Documents
     \GridSwCert.txt"
     ```

   - Pour des versions antérieures :

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
Archive/GridSwCert-Windows_2019_09.cert" -OutFile "$Env:PUBLIC\Documents
\GridSwCert.txt"
```

> **Note**
>
> Si un message d'erreur s'affiche lors du téléchargement du fichier et que vous utilisez Windows Server 2016 ou une version antérieure, il est possible que la version TLS 1.2 doive être activée sur votre PowerShell terminal. Vous pouvez activer la TLS version 1.2 pour la PowerShell session en cours à l'aide de la commande suivante, puis réessayer :
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

6. Redémarrez votre instance.
7. Vérifiez la licence NVIDIA de jeu à l'aide de la commande suivante.

   ```
   C:\Windows\System32\DriverStore\FileRepository\nvgridsw_aws.inf_*\nvidia-smi.exe -q
   ```

   La sortie doit ressembler à ce qui suit.

   ```
   vGPU Software Licensed Product
   Product Name              : NVIDIA Cloud Gaming
   License Status            : Licensed (Expiry: N/A)
   ```

8. (Facultatif) Pour tirer parti de l'affichage unique d'une résolution maximale de 4K, configurez le protocole d'affichage haute performance NICEDCV. Si vous n'avez pas besoin de cette fonctionnalité, n'effectuez pas cette étape.

Installez une version supplémentaire de CUDA

Après avoir installé un pilote NVIDIA graphique sur votre instance, vous pouvez installer une version CUDA autre que celle fournie avec le pilote graphique. La procédure suivante explique comment configurer plusieurs versions de CUDA sur l'instance.

Installez le CUDA kit d'outils sous Linux

Pour installer le kit d'CUDAoutils sous Linux, procédez comme suit :

1. Connectez-vous à votre instance Linux.
2. Ouvrez le NVIDIAsite Web et sélectionnez la version CUDA dont vous avez besoin.
3. Sélectionnez l'architecture, la distribution et la version du système d'exploitation de votre instance. Pour Installer Type (Type de programme d'installation), sélectionnez runfile (local).
4. Suivez les instructions pour télécharger le script d'installation.
5. Ajoutez les autorisations d'exécution au script d'installation que vous avez téléchargé à l'aide de la commande suivante.

```
[ec2-user ~]$ chmod +x downloaded_installer_file
```

6. Exécutez le script d'installation comme suit pour installer le CUDA kit d'outils et ajoutez le numéro de CUDA version au chemin du kit d'outils.

```
[ec2-user ~]$ sudo sh downloaded_installer_file --silent --override --toolkit --
samples --toolkitpath=/usr/local/cuda-version --samplespath=/usr/local/cuda --no-
opengl-libs
```

7. (Facultatif) Définissez la CUDA version par défaut comme suit.

```
[ec2-user ~]$ sudo ln -s /usr/local/cuda-version /usr/local/cuda
```

Installez le CUDA kit d'outils sous Windows

Pour installer le kit d'CUDAoutils sous Windows, procédez comme suit :

Pour installer le CUDA kit d'outils

1. Connectez-vous à votre instance Windows.
2. Ouvrez le NVIDIAsite Web et sélectionnez la version CUDA dont vous avez besoin.
3. Pour Installer Type (Type de programme d'installation, sélectionnez exe (local) puis choisissez Download (Télécharger).
4. À l'aide de votre navigateur, exécutez le fichier d'installation téléchargé. Suivez les instructions pour installer le CUDA kit d'outils. Vous devrez peut-être redémarrer l'instance.

Installation du ENA pilote sur les instances EC2 Windows

Si votre instance n'est pas basée sur l'une des dernières images Windows Amazon Machine (AMIs) fournies par Amazon, utilisez la procédure suivante pour installer le ENA pilote actuel sur votre instance. Vous devez effectuer cette mise à jour à un moment où il est possible de redémarrer votre instance. Si le script d'installation ne redémarre pas automatiquement votre instance, nous vous recommandons de redémarrer l'instance à la dernière étape.

Si vous utilisez un volume de stockage d'instances pour stocker des données pendant que l'instance fonctionne, ces données sont effacées lorsque vous arrêtez l'instance. Avant d'arrêter votre instance, vérifiez que vous avez copié toutes les données dont vous avez besoin depuis les volumes de stockage de votre instance vers un stockage persistant, tel qu'Amazon EBS ou Amazon S3.

Prérequis

Pour installer ou mettre à niveau le ENA pilote, votre instance Windows doit répondre aux conditions préalables suivantes :

- Avoir installé PowerShell la version 3.0 ou ultérieure

Étape 1 : sauvegarder vos données

Nous vous recommandons de créer une sauvegarde AMI au cas où vous ne parviendriez pas à annuler vos modifications via le Gestionnaire de périphériques. Pour créer une sauvegarde AMI avec le AWS Management Console, procédez comme suit :

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance qui nécessite la mise à niveau du pilote, puis choisissez Arrêter l'instance dans le menu État de l'instance.
4. Une fois l'instance arrêtée, sélectionnez-la à nouveau. Pour créer votre sauvegarde, choisissez Image et modèles dans le menu Actions, puis choisissez Créer une image.
5. Pour redémarrer votre instance, choisissez Démarrer l'instance dans le menu État de l'instance.

Étape 2 : Installation ou mise à niveau de votre ENA pilote

Vous pouvez installer ou mettre à niveau votre ENA pilote avec AWS Systems Manager Distributor ou avec des PowerShell applets de commande. Pour plus d'instructions, sélectionnez l'onglet correspondant à la méthode que vous voulez utiliser.

Systems Manager Distributor

Vous pouvez utiliser la fonctionnalité Systems Manager Distributor pour déployer des packages sur vos nœuds gérés par Systems Manager. Avec Systems Manager Distributor, vous pouvez installer le package de ENA pilotes une seule fois ou avec des mises à jour planifiées. Pour plus d'informations sur l'installation du package de ENA pilotes (`AwsEnaNetworkDriver`) avec Systems Manager Distributor, consultez la section Installer ou mettre à jour des packages dans le Guide de AWS Systems Manager l'utilisateur.

PowerShell

Cette section explique comment télécharger et installer des packages de ENA pilotes sur votre instance à l'aide d' PowerShell applets de commande.

Option 1 : télécharger et extraire la dernière version

1. Connectez-vous à votre instance en tant qu'administrateur local.
2. Utilisez la cmdlet invoke-webrequest pour télécharger le dernier package de pilotes :

```
PS C:\> invoke-webrequest https://ec2-windows-drivers-
downloads.s3.amazonaws.com/ENA/Latest/AwsEnaNetworkDriver.zip -
outfile $env:USERPROFILE\AwsEnaNetworkDriver.zip
```

> **Note**
>
> Si un message d'erreur s'affiche lors du téléchargement du fichier et que vous utilisez Windows Server 2016 ou une version antérieure, il est possible que la version TLS 1.2 doive être activée sur votre PowerShell terminal. Vous pouvez activer la TLS version 1.2 pour la PowerShell session en cours à l'aide de la commande suivante, puis réessayer :
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

Vous pouvez également télécharger le package de pilotes le plus récent à partir d'une fenêtre de navigateur sur votre instance.

3. Utilisez la cmdlet expand-archive pour extraire l'archive zip que vous avez téléchargée sur votre instance :

```
PS C:\> expand-archive $env:userprofile\AwsEnaNetworkDriver.zip -
DestinationPath $env:userprofile\AwsEnaNetworkDriver
```

Option 2 : télécharger et extraire une version spécifique

1. Connectez-vous à votre instance en tant qu'administrateur local.
2. Téléchargez le package de ENA pilotes pour la version spécifique que vous souhaitez à partir du lien de version figurant dans le ENAHistorique des versions du pilote Windows tableau.
3. Décompressez l'archive zip dans votre instance.

Installez le ENA pilote avec PowerShell

Les étapes d'installation sont les mêmes, que vous ayez téléchargé le dernier pilote ou une version spécifique. Pour installer le ENA pilote, procédez comme suit.

1. Pour installer le pilote, exécutez le `install.ps1` PowerShell script depuis le `AwsEnaNetworkDriver` répertoire de votre instance. Si un message d'erreur s'affiche, assurez-vous que vous utilisez la PowerShell version 3.0 ou une version ultérieure.
2. Si le programme d'installation ne redémarre pas automatiquement votre instance, exécutez l'Restart-Computer PowerShell applet de commande.

```
PS C:\> Restart-Computer
```

Étape 3 (optionnelle) : vérifier la version du ENA pilote après l'installation

Pour vous assurer que le package de ENA pilotes a été correctement installé sur votre instance, vous pouvez vérifier la nouvelle version comme suit :

1. Connectez-vous à votre instance en tant qu'administrateur local.

2. Pour ouvrir le Gestionnaire de périphériques Windows, saisissez `devmgmt.msc` la fenêtre Exécuter.
3. Choisissez OK. La fenêtre du Gestionnaire de périphériques s'ouvre.
4. Sélectionnez la flèche qui apparaît à gauche de Cartes réseau pour développer la liste.
5. Choisissez le nom ou ouvrez le menu contextuel pour Amazon Elastic Network Adapter, puis choisissez Propriétés. Cela ouvre la boîte de dialogue Propriétés d'Amazon Elastic Network Adapter.

> **Note**
>
> ENAles adaptateurs utilisent tous le même pilote. Si vous avez plusieurs ENA adaptateurs, vous pouvez sélectionner l'un d'entre eux pour mettre à jour le pilote de tous les ENA adaptateurs.

6. Pour vérifier la version actuelle installée, ouvrez l'onglet Pilote et vérifiez la version du pilote. Si la version actuelle ne correspond pas à votre version cible, consultez Résoudre les problèmes liés au pilote Windows d'Elastic Network Adapter.

Annulation et installation ENA du pilote

En cas de problème lors de l'installation, vous devrez peut-être restaurer le pilote. Procédez comme suit pour revenir à la version précédente du ENA pilote installé sur votre instance.

1. Connectez-vous à votre instance en tant qu'administrateur local.
2. Pour ouvrir le Gestionnaire de périphériques Windows, saisissez `devmgmt.msc` la fenêtre Exécuter.
3. Choisissez OK. La fenêtre du Gestionnaire de périphériques s'ouvre.
4. Sélectionnez la flèche qui apparaît à gauche de Cartes réseau pour développer la liste.
5. Choisissez le nom ou ouvrez le menu contextuel pour Amazon Elastic Network Adapter, puis choisissez Propriétés. Cela ouvre la boîte de dialogue Propriétés d'Amazon Elastic Network Adapter.

> **Note**
>
> ENAles adaptateurs utilisent tous le même pilote. Si vous avez plusieurs ENA adaptateurs, vous pouvez sélectionner l'un d'entre eux pour mettre à jour le pilote de tous les ENA adaptateurs.

6. Pour annuler le pilote, ouvrez l'onglet Pilote et choisissez Annuler le pilote. Cela ouvre la fenêtre Restauration du package de pilotes.

> **Note**
>
> Si l'onglet Pilote n'affiche pas l'action Annuler le pilote, ou si l'action n'est pas disponible, cela signifie que le magasin de pilotes de votre instance ne contient pas le package de pilotes précédemment installé. Pour résoudre ce problèmeScénarios de résolution des problèmes, consultez et développez la section Version du ENA pilote installée de manière inattendue. Pour plus d'informations sur le processus de sélection du package de pilotes de périphériques, consultez Comment Windows sélectionne un package de pilotes pour un périphérique sur le site Web de documentation de Microsoft.

Suivez ENA les versions des pilotes Windows

Windows AMIs inclut le pilote ENA Windows pour permettre une mise en réseau améliorée.

Le tableau suivant indique la version de ENA pilote correspondante à télécharger pour chaque version de Windows Server.

Version Windows Server	Version du pilote ENA
Windows Server 2022	2.4.0 et versions ultérieures
Windows Server 2019	dernières
Windows Server 2016	dernières
Windows Server 2012 R2	2.6.0 et versions antérieures
Windows Server 2012	2.6.0 et versions antérieures

Version Windows Server	Version du pilote ENA
Windows Server 2008 R2	2.2.3 et version antérieure

ENANotifications de publication de pilotes Windows avec Amazon SNS

Amazon SNS peut vous avertir lorsque de nouvelles versions de EC2 Windows Drivers sont publiées. Pour vous abonner à ces notifications, utilisez la procédure suivante.

S'abonner aux notifications EC2

1. Ouvrez la SNS console Amazon sur https://console.aws.amazon.com/sns/v3/home.
2. Dans la barre de navigation, changez la région en US Est (Virginie du Nord), si nécessaire. Vous devez sélectionner cette région car les SNS notifications auxquelles vous êtes abonné se trouvent dans cette région.
3. Dans le panneau de navigation, sélectionnez Abonnements.
4. Choisissez Créer un abonnement.
5. Dans la boîte de dialogue Créer un abonnement, exécutez l'une des actions suivantes :
   a. Pour le sujet ARN, copiez le nom de ressource Amazon suivant (ARN) :

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers
   b. Pour Protocole, choisissez `Email`.
   c. Pour Point de terminaison, entrez une adresse e-mail que vous pouvez utiliser pour recevoir les notifications.
   d. Choisissez Créer un abonnement.
6. Vous recevrez rapidement un e-mail de confirmation. Ouvrez l'e-mail et suivez les instructions pour terminer votre abonnement.

Chaque fois que de nouveaux pilotes EC2 Windows sont publiés, nous envoyons des notifications aux abonnés. Si vous ne souhaitez plus recevoir ces notifications, exécutez la procédure suivante pour annuler votre abonnement.

Se désabonner de la notification relative aux pilotes Amazon EC2 Windows

1. Ouvrez la SNS console Amazon sur https://console.aws.amazon.com/sns/v3/home.

2. Dans le panneau de navigation, choisissez Abonnements.
3. Cochez la case correspondant à l'abonnement, puis choisissez Actions, Supprimer des abonnements. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

ENAHistorique des versions du pilote Windows

Le tableau suivant résume les modifications pour chaque version.

Versions du pilote	Détails	Date de publication
2.7.0	Nouvelles fonctions • Suppression du support pour Windows Server 2012 (Windows 8) et Windows Server 2012 R2 (Windows 8.1). Le support de ces versions du système d'exploitation a atteint la fin du AWS. L'installation du pilote échouera sous Windows Server 2012 et versions antérieures. • Ajout de la prise en charge du transfert du calcul de la somme de contrôle IPv6 Tx vers l'appareil. • Ajout d'une large prise en charge de la file d'attente à faible latence (LLQ). Ceci est activé dynamiquement en fonction des recommandations de l'appareil. Vous pouvez remplacer ce paramètre par la nouvelle clé de registre « Wide LLQ ». • Ajout de rapports pour les pertes de paquets résultant d'un dépassement de Rx, ce qui indique un espace insuffisant dans l'anneau Rx pour les paquets entrants. • Ajout de la prise en charge des notifications de configuration sous-optimales provenant de l'appareil.	1er mai 2024

Versions du pilote	Détails	Date de publication
	Consultez l'ID de l'événement `59000` dans l'observateur d'événements Windows. Correctifs de bogue • Évitez toute réinitialisation inutile du périphérique provoquée par des paquets Tx dont les en-têtes dépassent la taille d'en-tête Low Latency Queuing (LLQ) maximale.	

Versions du pilote	Détails	Date de publication

2.6.0	Nouvelles fonctions
	• Ajoute les mesures de performance réseau suivantes pour les types d'instances compatibles avec ENA Express.
	  • `ena_srd_mode`
	  • `ena_srd_tx_pkts`
	  • `ena_srd_eligible_tx_pkts`
	  • `ena_srd_rx_pkts`
	  • `ena_srd_resource_utilization`
	• Ajoute la métrique de performance réseau `conntrack_allowance_available` pour les types d'instance basés sur Nitro.
	• Ajoute un nouveau motif de réinitialisation de l'adaptateur en raison de la détection d'une corruption des données RX.
	• Met à jour l'infrastructure de journalisation des pilotes.
	
	Correctifs de bogue
	• Empêche la réinitialisation de l'adaptateur en cas d'échec CPU de la mise à jour des indicateurs de performance du réseau en cas d'indisponibilité.
	•
		20 juin 2023

Versions du pilote	Détails	Date de publication
	Empêche la fausse détection d'une interruption de la pulsation de l'appareil. • Corrige le script d'installation du pilote pour prendre en charge l'opération de rétrogradation. • Corrige les statistiques relatives au nombre d'erreurs de réception.	
2.5.0	Annonce ENALa version 2.5.0 du pilote Windows a été annulée en raison d'un échec d'initialisation sur le contrôleur de domaine Windows. Windows Client et Windows Server ne sont pas affectés.	17 février 2023

Versions du pilote	Détails	Date de publication
2.4.0	Nouvelles fonctions • Ajout de la prise en charge de Windows Server 2022. • Supprime la prise en charge de Windows Server 2008 R2. • Définit Low Latency Queuing (LLQ) sur Toujours activé afin d'améliorer les performances des instances Amazon EC2 de sixième génération. Correctif de bogue. • Résout un échec de publication des mesures de performance réseau sur le système Performance Counters for Windows (PCW). • Corrige une fuite de mémoire lors de l'opération de lecture des clés de registre. • Empêche une boucle de réinitialisation infinie en cas d'erreur irrécupérable lors du processus de réinitialisation de dispositif.	28 avril 2022

Versions du pilote	Détails	Date de publication
2.2.4	Annonce ENALa version 2.2.4 du pilote Windows a été annulée en raison d'une éventuelle dégradation des performances sur les EC2 instances de sixième génération. Nous vous recommandons de revenir à une version plus ancienne du pilote à l'aide de l'une des méthodes suivantes : • Installer la version précédente 1. Téléchargez le package de la version précédente à partir du lien de ce tableau (version 2.2.3). 2. Exécutez le script install.ps1 PowerShell d'installation. Pour plus de détails sur les étapes pré-installation et post-installation, consultez Activer les réseaux améliorés sur Windows. Utiliser Amazon EC2 Systems Manager pour une mise à jour groupée • Effectuez une mise à jour SSM groupée via un document`AWS-ConfigureAWSPackage` , avec les paramètres suivants : • Nom : AwsEnaNetworkDriver • Version : 2.2.3	26 octobre 2021

Versions du pilote	Détails	Date de publication
2.2.3	Nouvelle fonction • Ajoute la prise en charge des nouvelles cartes Nitro avec la mise en réseau d'une instance jusqu'à 400 Gbit/s. Correctif de bogue. • Corrige les conditions de course entre le changement d'heure du système et la demande d'heure du système par le ENA pilote, ce qui entraîne une détection faussement positive de l'absence de réponse du matériel. La version 2.2.3 du ENA pilote Windows est la version finale compatible avec Windows Server 2008 R2. Les types d'instances actuellement disponibles qui sont utilisés ENA continueront d'être pris en charge sur Windows Server 2008 R2, et les pilotes sont disponibles par téléchargement. Aucun futur type d'instance ne supportera Windows Server 2008 R2, et vous ne pouvez pas lancer, importer ou migrer des images Windows Server 2008 R2 vers de futurs types d'instance.	25 mars 2021

Versions du pilote	Détails	Date de publication
2.2.2	Nouvelle fonction • Permet d'interroger les indicateurs de performance des adaptateurs réseau avec CloudWatch les compteurs de performance pour les utilisateurs de Windows. Correctif de bogue. • Résout les problèmes de performances sur les instances nues.	21 décembre 2020
2.2.1	Nouvelle fonction • Ajoute une méthode permettant à l'hôte d'interroger l'adaptateur réseau Elastic pour les métriques des performances réseau.	1er octobre 2020

Versions du pilote	Détails	Date de publication
2.2.0	Nouvelles fonctions • Ajoute la prise en charge des types de matériel de nouvelle génération. • Améliore le temps de démarrage de l'instance après la sortie de stop-hibernate et élimine les faux messages d'erreur positifs. ENA Optimisations des performances • Optimise le traitement du trafic entrant. • Améliore la gestion de la mémoire partagée dans un environnement avec peu de ressources. Correctif de bogue. • Évite le crash du système lors du retrait du ENA périphérique dans les rares cas où le pilote ne parvient pas à se réinitialiser.	12 août 2020
2.1.5	Correctif de bogue. • Résout les échecs occasionnels d'initialisation de la carte réseau sur les instances nues.	23 Juin 2020

Versions du pilote	Détails	Date de publication
2.1.4	Correctifs de bogue • Prévenez les problèmes de connectivité causés par des métadonnées de LSO paquets corrompues provenant de la pile réseau. • Empêche la panne du système provoquée par une condition de concurrence rare qui se traduit par l'accès d'une mémoire de paquets déjà libérée.	25 novembre 2019
2.1.2	Nouvelle fonction • Ajout de la prise en charge du rapport d'identification du fournisseur pour permettre au système d'exploitation de générer des MAC données basées sur UUIDs Correctifs de bogue • Performances de configuration DHCP réseau améliorées lors de l'initialisation. • Calculez correctement la somme de contrôle L4 sur le IPv6 trafic entrant lorsque l'unité de transmission maximale (MTU) dépasse 4K. • Améliorations générales de la stabilité du pilote et correctifs de bogues mineurs.	4 novembre 2019

Versions du pilote	Détails	Date de publication
2.1.1	Correctifs de bogue • Empêchez les pertes de TCP LSO paquets très fragmentés provenant du système d'exploitation. • Gérez correctement le protocole Encapsulating Security Payload (ESP) au sein des réseaux internesI PSec. IPv6	16 septembre 2019

Versions du pilote	Détails	Date de publication

2.1.0	ENALe pilote Windows v2.1 introduit de ENA nouvelles fonctionnalités, améliore les performances, ajoute de nouvelles fonctionnalités et inclut de nombreuses améliorations de stabilité.
	• Nouvelles fonctionnalités
	  • Utilisez la clé de registre Windows normalisée pour la configuration des trames Jumbo.
	  • Autoriser le réglage de l'VLANidentifiant via les propriétés du ENA piloteGUI.
	  • Flux de récupération améliorés
	  • Amélioration du mécanisme d'identification des défaillances.
	  • Ajout de la prise en charge pour les paramètres de récupération réglables.
	  • Support de 32 files d'attente d'E/S pour les nouvelles EC2 instances qui en comptent plus de 8. vCPUs
	  • ~90 % de réduction d'empreinte mémoire du pilote.
	• Optimisation des performances
	  • Réduction de la latence du chemin de transmission.
	  • Prise en charge de la réception du transfert du total de contrôle.
	  •
		1 juillet 2019

Versions du pilote	Détails	Date de publication
	Optimisation des performances pour un système extrêmement chargé (utilisation optimisée des mécanismes de verrouillage). • Améliorations supplémentaires pour réduire CPU l'utilisation et améliorer la réactivité du système sous charge. • Correctifs de bogue • Correction des incidents dus à une analyse non valide des en-têtes Tx non contigus. • Correction des incidents du pilote v1.5 pendant le détachement de l’interface réseau Elastic sur des instances de matériel nu. • Corrigez l'erreur de calcul de la somme de contrôle du LSO pseudo-en-tête. IPv6 • Correction de la fuite de ressources mémoire potentielles lors de l’échec d’initialisation. • Désactive le déchargementTCP/UDPchecksum pour les IPv4 fragments. • Correctif pour VLAN la configuration. VLANa été incorrectement désactivé alors que seule VLAN la priorité aurait dû être désactivée. • Activation de l’analyse correcte des messages de pilote personnalisés par la visionneuse d’événements. •	

Versions du pilote	Détails	Date de publication
	Correction de l'échec d'initialisation en raison d'un traitement non valide de l'horodatage. • Corrigez la course entre le traitement des données et la désactivation de ENA l'appareil.	
1.5.0	• Amélioration de la stabilité et des correctifs de performance. • Les tampons de réception peuvent désormais être configurés jusqu'à une valeur de 8192 dans les propriétés avancées du. ENA NIC • Tampons de réception par défaut de 1 000 octets.	4 octobre 2018
1.2.3	Inclut les correctifs de fiabilité et unifie la prise en charge de Windows Server 2008 R2 via Windows Server 2016.	13 février 2018
1.0.8	Version initiale. Inclus AMIs pour Windows Server 2008 R2, Windows Server 2012RTM, Windows Server 2012 R2 et Windows Server 2016.	juillet 2016

Pilotes de virtualisation paravirtuelle pour les instances Windows

Windows AMIs contient un ensemble de pilotes permettant d'accéder au matériel virtualisé. Ces pilotes sont utilisés par Amazon EC2 pour mapper le magasin d'instances et les EBS volumes Amazon à leurs appareils. Le tableau suivant présente les principales différences entre les différents pilotes.

	RedHat PV	Virtualisation paravirtuelle Citrix	AWS PV
Type d'instance	Non pris en charge pour tous les types d'instance. Si vous spécifiez un type d'instance non pris en charge, l'instance est dégradée.	Pris en charge pour les types d'instance Xen.	Pris en charge pour les types d'instance Xen.
Volumes attachés	Prend en charge jusqu'à 16 volumes attachés.	Prend en charge plus de 16 volumes attachés.	Prend en charge plus de 16 volumes attachés.
Réseau	Le pilote présente des problèmes connus liés à la réinitialisation de la connexion réseau sous des charges élevées, par exemple lors de transferts de FTP fichiers rapides.		Le pilote configure automatiquement des trames jumbo sur la carte réseau lorsqu'il se trouve sur un type d'instance compatible. Lorsque l'instance se trouve dans un groupe de placement de cluster, cela améliore les performan

	RedHat PV	Virtualisation paravirtuelle Citrix	AWS PV
			ces réseau entre les instances du groupe de placement de cluster. Pour de plus amples informations, veuillez consulter Groupes de placement pour vos EC2 instances Amazon.

Le tableau suivant indique les pilotes PV que vous devez exécuter sur chaque version de Windows Server sur AmazonEC2.

Version Windows Server	Version de pilote PV
Windows Server 2022	AWS Dernière version de PV
Windows Server 2019	AWS Dernière version de PV
Windows Server 2016	AWS Dernière version de PV
Windows Server 2012 R2	AWS Dernière version de PV
Windows Server 2012	AWS Dernière version de PV
Windows Server 2008 R2	AWS Version PC 8.3.5

Version Windows Server	Version de pilote PV
Windows Server 2008	PV Citrix 5.9
Windows Server 2003	PV Citrix 5.9

Table des matières

AWS Pilotes photovoltaïques

Les pilotes AWS PV sont stockés dans le `%ProgramFiles%\Amazon\Xentools` répertoire. Ce répertoire contient également des symboles publics et un outil de ligne de commande qui vous permet d'accéder aux entrées de XenStore. `xenstore_client.exe` Par exemple, la PowerShell commande suivante renvoie l'heure actuelle depuis l'hyperviseur :

```
PS C:\> [DateTime]::FromFileTimeUTC((gwmi -n root\wmi -cl
 AWSXenStoreBase).XenTime).ToString("hh:mm:ss")
11:17:00
```

Les composants du pilote AWS PV sont répertoriés dans le registre Windows sous`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`. Ces composants de pilote sont les suivants : xenbus, xeniface, xennet, xenvbd et xenvif.

AWS Les pilotes PV ont également un service Windows nommé LiteAgent, qui s'exécute en mode utilisateur. Il gère des tâches telles que les événements d'arrêt et de redémarrage à partir AWS APIs des instances de génération Xen. Vous pouvez accéder aux services et les gérer en exécutant `Services.msc` dans la ligne de commande. Lors de l'exécution sur des instances de génération Nitro, les pilotes AWS PV ne sont pas utilisés et le LiteAgent service s'arrête automatiquement à partir de la version 8.2.4 du pilote. La mise à jour vers le dernier pilote AWS PV permet également de mettre à jour LiteAgent et d'améliorer la fiabilité de toutes les générations d'instances.

Installez les derniers pilotes AWS PV

Amazon Windows AMIs contient un ensemble de pilotes permettant d'accéder au matériel virtualisé. Ces pilotes sont utilisés par Amazon EC2 pour mapper le magasin d'instances et les EBS volumes Amazon à leurs appareils. Nous vous recommandons d'installer les derniers pilotes pour améliorer la stabilité et les performances de vos instances EC2 Windows.

Options d'installation

- Vous pouvez l'utiliser AWS Systems Manager pour mettre à jour automatiquement les pilotes PV. Pour plus d'informations, voir Procédure pas à pas : mise à jour automatique des pilotes PV sur les instances EC2 Windows (console) dans le guide de l'AWS Systems Manager utilisateur.
- Vous pouvez télécharger le package de pilotes et exécuter le programme d'installation manuellement. Consultez le fichier `readme.txt` pour connaître la configuration système requise. Pour plus d'informations sur le téléchargement et l'installation des pilotes PV AWS , ou si vous mettez à niveau un contrôleur de domaine, consultez Mettre à niveau les instances Windows Server (mise à niveau AWS PV) manuellement.

AWS Historique du package de pilotes PV

Le tableau suivant indique les modifications apportées aux pilotes AWS PV pour chaque version du pilote.

Version du package	Détails	Date de publication
8.4.3	Correction de bogues dans le programme d'installation du package afin d'améliorer l'expérience de mise à niveau.	24 janvier 2023
8.4.2	Correctifs de stabilité pour répondre aux conditions de concurrence.	13 avril 2022
8.4.1	Package d'installation amélioré.	7 janvier 2022
8.4.0	• Correctifs de stabilité pour traiter de rares cas d'IO de disque bloqué. • Correctifs de stabilité pour résoudre les rares cas de pannes lors du détachement EBS du volume.	2 mars 2021

Version du package	Détails	Date de publication
	• Ajout d'une fonctionnalité permettant de répartir la charge sur plusieurs cœurs pour les charges de travail supérieures à 20 000 unités IOPS et dont la dégradation est due à des goulots d'étranglement. Pour activer cette fonctionnalité, consultez Les charges de travail qui exploitent plus de 20 000 disques IOPS subissent une dégradation due à des goulots d'étranglement CPU. • AWS L'installation de PV 8.4 sur Windows Server 2008 R2 échouera. AWS Les versions PV 8.3.5 et antérieures sont prises en charge sur Windows Server 2008 R2.	
8.3.5	Package d'installation amélioré.	7 janvier 2022
8.3.4	Amélioration de la fiabilité de la connexion des périphériques réseau.	4 août 2020
8.3.3	• Mise à jour du composant XenStore orienté vers -facing pour empêcher la vérification des bogues lors des chemins de gestion des erreurs. • Mettez à jour le composant de stockage pour éviter les pannes en cas de soumission d'un message non SRB valide. Pour mettre à jour ce pilote sur les instances Windows Server 2008 R2, vous devez d'abord vérifier que les correctifs appropriés sont installés de manière à répondre à l'avis de sécurité Microsoft suivant : Microsoft Security Advisory 3033929.	4 février 2020
8.3.2	Fiabilité améliorée des composants de mise en réseau.	30 juillet 2019
8.3.1	Améliorations des performances et robustesse du composant de stockage.	12 juin 2019
8.2.7	Efficacité renforcée pour la prise en charge de la migration vers les types d'instance de dernière génération.	20 mai 2019

Version du package	Détails	Date de publication
8.2.6	Amélioration de l'efficacité du chemin de vidage en cas de plantage.	15 janvier 2019
8.2.5	Améliorations de sécurité supplémentaires. PowerShell le programme d'installation est désormais disponible sous forme de package.	12 décembre 2018
8.2.4	Améliorations de la fiabilité.	2 octobre 2018
8.2.3	Correctifs de bogues et améliorations de performances. Indiquez l'ID EBS du volume sous forme de numéro de série du disque pour les EBS volumes. Ceci permet des scénarios de cluster tels que S2D.	29 mai 2018
8.2.1	Amélioration des performances réseau et stockage, et correctifs de robustesse. Pour vérifier que cette version a été installée, reportez-vous à la valeur de registre Windows suivant : `HKLM\Software\Amazon\PVDriver\Version 8.2.1` .	8 mars 2018
7.4.6	Correctifs de stabilité pour rendre les pilotes AWS photovoltaïques plus résilients.	26 avril 2017
7.4.3	Ajout de la prise en charge de Windows Server 2016. Correctifs de stabilité pour toutes les versions du système d'exploitation Windows prises en charge. * La signature du pilote AWS PV version 7.4.3 expire le 29 mars 2019. Nous vous recommandons de mettre à jour le pilote AWS PV le plus récent.	18 nov 2016

Version du package	Détails	Date de publication
7.4.2	Correctifs de stabilité pour la prise en charge du type d'instance X1.	2 août 2016
7.4.1	• Amélioration des performances du pilote de stockage AWS photovoltaïque. • Correctifs de stabilité dans le pilote AWS PV Storage : correction d'un problème à cause duquel les instances rencontraient un crash du système avec le code de vérification des bogues 0x0000DEAD. • Corrections de stabilité dans le pilote AWS PV Network. • Ajout de la prise en charge de Windows Server 2008 R2.	12 juillet 2016
7.3.2	• Amélioration de la journalisation et des diagnostics. • Correctif de stabilité dans le pilote de stockage AWS PV. Dans certains cas, les disques n'apparaissent pas sur Windows après les avoir réassociés à l'instance. • Ajout de la prise en charge de Windows Server 2012.	24 juin 2015
7.3.1	TRIMmise à jour : correction liée aux TRIM demandes. Ce correctif stabilise les instances et améliore les performances des instances lors de la gestion d'un grand nombre de TRIM demandes.	
7.3.0	TRIMsupport : le pilote AWS PV envoie désormais des TRIM demandes à l'hyperviseur. Les disques éphémères traiteront correctement les TRIM demandes compte tenu des supports de stockage sous-jacents TRIM ()SSD. Notez que le stockage EBS basé n'est TRIM plus pris en charge depuis mars 2015.	

Version du package	Détails	Date de publication
7.2.5	• Correction de stabilité dans les pilotes de stockage AWS photovoltaïque : dans certains cas, le pilote AWS photovolt aïque peut déréférencer une mémoire non valide et provoquer une défaillance du système. • Correctif de stabilité lors de la génération d'un crash dump : dans certains cas, le pilote AWS photovoltaïque peut se retrouver bloqué dans des conditions de course lorsqu'il rédige un crash dump. Avant cette version, le seul moyen de résoudre ce problème était de forcer l’arrêt, puis le redémarra ge du pilote afin de supprimer le fichier de vidage de mémoire.	
7.2.4	Persistance de l'identifiant du périphérique : ce correctif masque l'identifiant du PCI périphérique de la plate-forme et oblige le système à toujours afficher le même identifiant de périphéri que, même si l'instance est déplacée. De façon plus générale, ce correctif concerne la façon dont l’hyperviseur affiche les appareils virtuels. Le correctif inclut également des modifications apportées au co-installateur pour les pilotes AWS PV afin que le système conserve les périphériques virtuels mappés.	
7.2.2	• Chargez les pilotes AWS PV en mode restauration des services d'annuaire (DSRM) : le mode de restauration des services d'annuaire est une option de démarrage en mode sécurisé pour les contrôleurs de domaine Windows Server. • Persister l'ID du périphérique lorsque le périphérique adaptateur réseau virtuel est reconnecté : ce correctif oblige le système à vérifier le mappage des MAC adresses et à conserver l'ID du périphérique. Il garantit que les cartes réseau rattachées conservent leurs paramètres statiques.	

Version du package	Détails	Date de publication
7.2.1	• Exécution en mode sans échec : résolution du problème empêchant le chargement du pilote en mode sans échec. Auparavant, les pilotes AWS PV n'étaient instanciés que dans les systèmes fonctionnant normalement. • Ajout de disques aux groupes de stockage Microsoft Windows : précédemment, nous synthétisions les requêtes de page 83. Ce correctif a désactivé la prise en charge de page 83. Notez que cela ne concerne pas les groupes de stockage qui sont utilisés dans un environnement de cluster, car les disques PV ne sont pas des disques de cluster valides.	
7.2.0	Base : version de base AWS PV.	

Pilotes PV Citrix

Les pilotes PV Citrix sont stockés dans le répertoire `%ProgramFiles%\Citrix\XenTools` (instances 32 bits) ou `%ProgramFiles(x86)%\Citrix\XenTools` (instances 64 bits).

Les composants de pilote PV Citrix sont répertoriés dans le registre Windows sous `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services`. Ces composants de pilote sont les suivants : xenevtchn, xeniface, xennet, Xennet6, xensvc, xenvbd et xenvif.

Citrix possède également un composant pilote nommé XenGuestAgent, qui s'exécute en tant que service Windows. Il gère des tâches telles que les événements d'arrêt et de redémarrage à partir duAPI. Vous pouvez accéder aux services et les gérer en exécutant `Services.msc` dans la ligne de commande.

Si vous rencontrez des erreurs réseau lors de l'exécution de certaines charges de travail, vous devrez peut-être désactiver la fonctionnalité de TCP déchargement pour le pilote PV Citrix. Pour de plus amples informations, veuillez consulter TCPdéchargement.

RedHat Pilotes photovoltaïques

RedHat les pilotes sont pris en charge pour les anciennes instances, mais ne sont pas recommandés sur les nouvelles instances de plus de 12 Go RAM en raison des limitations liées aux pilotes. Les

instances comportant plus de 12 Go de RedHat pilotes RAM en cours d'exécution peuvent ne pas démarrer et devenir inaccessibles. Nous recommandons de mettre à niveau RedHat les pilotes vers des pilotes PV Citrix, puis de mettre à niveau les pilotes PV Citrix vers des pilotes AWS PV.

Les fichiers source des RedHat pilotes se trouvent dans le répertoire `%ProgramFiles%\RedHat` (instances 32 bits) ou `%ProgramFiles(x86)%\RedHat` (instances 64 bits). Les deux pilotes sont `rhelnet` le pilote réseau RedHat paravirtualisé et le pilote du `rhelscsi` RedHat SCSI miniport.

S'abonner aux notifications

Amazon SNS peut vous avertir lorsque de nouvelles versions de EC2 Windows Drivers sont publiées. Utilisez l'une des méthodes suivantes pour vous abonner à ces notifications.

> **Note**
>
> Vous devez spécifier la région pour le SNS sujet auquel vous vous abonnez.

S'abonner aux EC2 notifications depuis la console

1. Ouvrez la SNS console Amazon sur https://console.aws.amazon.com/sns/v3/home.
2. Dans la barre de navigation, changez la région en US Est (Virginie du Nord), si nécessaire. Vous devez sélectionner cette région car les SNS notifications auxquelles vous êtes abonné se trouvent dans cette région.
3. Dans le panneau de navigation, sélectionnez Abonnements.
4. Choisissez Créer un abonnement.
5. Dans la boîte de dialogue Créer un abonnement, exécutez l'une des actions suivantes :
   a. Pour le sujet ARN, copiez le nom de ressource Amazon suivant (ARN) :

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers
   b. Pour Protocole, choisissez `Email`.
   c. Pour Point de terminaison, tapez une adresse e-mail que vous pouvez utiliser pour recevoir les notifications.
   d. Choisissez Créer un abonnement.
6. Vous recevrez rapidement un e-mail de confirmation. Ouvrez l'e-mail et suivez les instructions pour terminer votre abonnement.

Abonnez-vous aux EC2 notifications à l'aide du AWS CLI

Pour vous abonner aux EC2 notifications avec le AWS CLI, utilisez la commande suivante.

```
aws sns subscribe --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-
windows-drivers --region us-east-1 --protocol email --notification-
endpoint YourUserName@YourDomainName.ext
```

Abonnez-vous aux EC2 notifications à l'aide du AWS Tools for PowerShell

Pour vous abonner aux EC2 notifications avec Tools for Windows PowerShell, utilisez la commande suivante.

```
Connect-SNSNotification -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-
drivers' -Region us-east-1 -Protocol email -Endpoint 'YourUserName@YourDomainName.ext'
```

Chaque fois que de nouveaux pilotes EC2 Windows sont publiés, nous envoyons des notifications aux abonnés. Si vous ne souhaitez plus recevoir ces notifications, exécutez la procédure suivante pour annuler votre abonnement.

Se désabonner de la notification relative aux pilotes Amazon EC2 Windows

1. Ouvrez la SNS console Amazon sur https://console.aws.amazon.com/sns/v3/home.
2. Dans le panneau de navigation, choisissez Abonnements.
3. Cochez la case correspondant à l'abonnement, puis choisissez Actions, Supprimer des abonnements. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Mettre à niveau les pilotes PV sur EC2 les instances Windows

Nous vous recommandons d'installer les derniers pilotes PV afin d'améliorer la stabilité et les performances de vos instances EC2 Windows. Les instructions sur cette page vous aident à télécharger le package de pilotes et à exécuter le programme d'installation.

Pour vérifier quel pilote votre instance Windows utilise

Ouvrez Connexions réseau dans le Panneau de configuration et affichez Connexion au réseau local. Vérifiez si le pilote est l'un des suivants :

- AWS Dispositif de réseau PV
- Carte Ethernet PV Citrix

- RedHat NICPilote PV

Sinon, vous pouvez vérifier la sortie de la commande `pnputil -e`.

Configuration système requise

Consultez le fichier `readme.txt` pour connaître la configuration système requise.

Table des matières

Mettre à niveau les instances Windows Server (mise à niveau AWS PV) avec Distributor

Vous pouvez utiliser Distributor, une fonctionnalité de AWS Systems Manager, pour installer ou mettre à niveau le package de pilotes AWS PV. L'installation ou la mise à niveau peut être effectuée une seule fois, ou vous pouvez l'installer ou la mettre à jour selon un calendrier. L'`In-place update`option Type d'installation n'est pas prise en charge pour ce package de distribution.

> **Important**
>
> Si votre instance est un contrôleur de domaine, consultez Mettre à niveau un contrôleur de domaine (mise à niveau AWS PV). Le processus de mise à niveau pour les instances de contrôleur de domaine est différent de celui des éditions standard de Windows.

1. Nous vous recommandons de créer une sauvegarde au cas où vous auriez besoin d'annuler vos modifications.

   > **Tip**
   >
   > Au lieu de le créer AMI depuis la EC2 console Amazon, vous pouvez utiliser Systems Manager Automation pour le créer à l'AMIaide du `AWS-CreateImage` runbook. Pour

plus d'informations, consultez le Guide AWS-CreateImagede l'utilisateur de référence du runbook AWS Systems Manager Automation.

a. Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Avant d'arrêter une instance, vérifiez que vous avez copié toutes les données dont vous avez besoin depuis les volumes de stockage de votre instance vers un stockage persistant, tel qu'Amazon EBS ou Amazon S3.

b. Dans le panneau de navigation, choisissez Instances.

c. Sélectionnez l'instance qui nécessite la mise à niveau du pilote, puis État de l'instance, Arrêter l'instance.

d. Une fois l'instance arrêtée, sélectionnez l'instance, puis Actions, Image et modèles, et enfin Créer une image.

e. Choisissez État de l'instance, Démarrer l'instance.

2. Se connecter à l'instance en utilisant le Bureau à distance. Pour de plus amples informations, veuillez consulter the section called "Connect à l'aide d'un RDP client".

3. Nous vous recommandons d'utiliser des disques non système hors ligne et de prendre en compte les drive mappages de lettres de lecteurs aux disques secondaires dans Gestion des disques avant d'exécuter cette mise à niveau. Cette étape n'est pas obligatoire si vous effectuez une mise à jour sur place des pilotes AWS PV. Nous vous recommandons également de définir les services non essentiels sur le start-up Manuel dans la console Services.

4. Pour les instructions relatives à l'installation ou à la mise à niveau du package de pilotes AWS PV à l'aide de Distributor, reportez-vous aux procédures décrites dans la section Installer ou mettre à jour des packages dans le guide de AWS Systems Manager l'utilisateur.

5. Dans Nom, choisissez AWSPVDriver.

6. Pour le type d'installation, sélectionnez Désinstaller et réinstallez.

7. Configurez les autres paramètres du package selon les besoins et exécutez l'installation ou la mise à niveau à l'aide de la procédure référencée dansStep 4.

   Après avoir exécuté le package Distributor, l'instance redémarre automatiquement puis met à niveau le pilote. L'instance ne sera pas disponible pendant 15 minutes.

8. Une fois la mise à niveau terminée et l'instance passée avec succès les deux tests de santé dans la EC2 console Amazon, vérifiez que le nouveau pilote a été installé en vous connectant à l'instance via Remote Desktop.

9. Une fois connecté, exécutez la PowerShell commande suivante :

```
Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
```

10. Vérifiez que la version du pilote est identique à la version la plus récente répertoriée dans l'historique des versions de pilote. Pour plus d'informations, consultez AWS Historique du package de pilotes PV Open Disk Management pour passer en revue les volumes secondaires hors ligne et les mettre en ligne conformément aux lettres de lecteur indiquées dansStep 3.

Si vous avez précédemment désactivé TCPdéchargement l'utilisation de Netsh pour les pilotes PV Citrix, nous vous recommandons de réactiver cette fonctionnalité après la mise à niveau vers les pilotes AWS PV. TCPLes problèmes de déchargement liés aux pilotes Citrix ne sont pas présents dans les pilotes AWS PV. Par conséquent, le TCP déchargement offre de meilleures performances avec les pilotes AWS photovoltaïques.

Si vous avez déjà appliqué une adresse IP statique ou une DNS configuration à l'interface réseau, vous devrez peut-être réappliquer l'adresse IP statique ou la DNS configuration après la mise à niveau des pilotes AWS PV.

Mettre à niveau les instances Windows Server (mise à niveau AWS PV) manuellement

Utilisez la procédure suivante pour effectuer une mise à niveau sur place des pilotes AWS PV ou pour passer des pilotes PV Citrix aux pilotes AWS PV sous Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 ou Windows Server 2022. Cette mise à niveau n'est pas disponible pour RedHat les pilotes, ni pour les autres versions de Windows Server.

Certaines anciennes versions de Windows Server ne peuvent pas utiliser les derniers pilotes. Pour vérifier la version du pilote à utiliser pour votre système d'exploitation, consultez le tableau des versions de pilotes de la page Pilotes de virtualisation paravirtuelle pour les instances Windows.

> **Important**
>
> Si votre instance est un contrôleur de domaine, consultez Mettre à niveau un contrôleur de domaine (mise à niveau AWS PV). Le processus de mise à niveau pour les instances de contrôleur de domaine est différent de celui des éditions standard de Windows.

Pour mettre à niveau les pilotes AWS PV manuellement

1. Nous vous recommandons de créer une sauvegarde au cas où vous auriez besoin d'annuler vos modifications.

   > **Tip**
   >
   > Au lieu de le créer AMI depuis la EC2 console Amazon, vous pouvez utiliser Systems Manager Automation pour le créer à l'AMIaide du `AWS-CreateImage` runbook. Pour plus d'informations, consultez le Guide AWS-CreateImagede l'utilisateur de référence du runbook AWS Systems Manager Automation.

   a. Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Avant d'arrêter une instance, vérifiez que vous avez copié toutes les données dont vous avez besoin depuis les volumes de stockage de votre instance vers un stockage persistant, tel qu'Amazon EBS ou Amazon S3.

   b. Dans le panneau de navigation, choisissez Instances.

   c. Sélectionnez l'instance qui nécessite la mise à niveau du pilote, puis État de l'instance, Arrêter l'instance.

   d. Une fois l'instance arrêtée, sélectionnez l'instance, puis Actions, Image et modèles, et enfin Créer une image.

   e. Choisissez État de l'instance, Démarrer l'instance.

2. Se connecter à l'instance en utilisant le Bureau à distance.

3. Nous vous recommandons d'utiliser des disques non système hors ligne et de prendre en compte les drive mappages de lettres de lecteurs aux disques secondaires dans Gestion des disques avant d'exécuter cette mise à niveau. Cette étape n'est pas obligatoire si vous effectuez une mise à jour sur place des pilotes AWS PV. Nous vous recommandons également de définir les services non essentiels sur le start-up Manuel dans la console Services.

4. Téléchargez le package de pilotes le plus récent sur l'instance.

   Vous pouvez également exécuter la PowerShell commande suivante :

   ```
   Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/
   Latest/AWSPVDriver.zip -outfile $env:USERPROFILE\pv_driver.zip
   ```

```
Expand-Archive $env:userprofile\pv_driver.zip -DestinationPath
 $env:userprofile\pv_drivers
```

> **Note**
>
> Si un message d'erreur s'affiche lors du téléchargement du fichier et que vous utilisez Windows Server 2016 ou une version antérieure, il est possible que la version TLS 1.2 doive être activée sur votre PowerShell terminal. Vous pouvez activer la TLS version 1.2 pour la PowerShell session en cours à l'aide de la commande suivante, puis réessayer :
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

5. Extrayez le contenu du dossier, puis exécutez `AWSPVDriverSetup.msi`.

Après avoir exécuté leMSI, l'instance redémarre automatiquement puis met à niveau le pilote. L'instance ne sera pas disponible pendant 15 minutes. Une fois la mise à niveau terminée et l'instance passée avec succès les deux tests de santé dans la EC2 console Amazon, vous pouvez vérifier que le nouveau pilote a été installé en vous connectant à l'instance via Remote Desktop, puis en exécutant la PowerShell commande suivante :

```
Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
```

Vérifiez que la version du pilote est identique à la version la plus récente répertoriée dans l'historique des versions de pilote. Pour plus d'informations, consultez AWS Historique du package de pilotes PV Open Disk Management pour passer en revue les volumes secondaires hors ligne et les mettre en ligne conformément aux lettres de lecteur indiquées dansStep 3.

Si vous avez précédemment désactivé TCPdéchargement l'utilisation de Netsh pour les pilotes PV Citrix, nous vous recommandons de réactiver cette fonctionnalité après la mise à niveau vers les pilotes AWS PV. TCPLes problèmes de déchargement liés aux pilotes Citrix ne sont pas présents dans les pilotes AWS PV. Par conséquent, le TCP déchargement offre de meilleures performances avec les pilotes AWS photovoltaïques.

Si vous avez déjà appliqué une adresse IP statique ou une DNS configuration à l'interface réseau, vous devrez peut-être réappliquer l'adresse IP statique ou la DNS configuration après la mise à niveau des pilotes AWS PV.

Mettre à niveau un contrôleur de domaine (mise à niveau AWS PV)

Utilisez la procédure suivante sur un contrôleur de domaine pour effectuer une mise à niveau sur place des pilotes AWS PV ou pour passer des pilotes PV Citrix aux pilotes AWS PV.

Pour mettre à niveau un contrôleur de domaine

1. Nous vous recommandons de créer une sauvegarde de votre contrôleur de domaine au cas où vous auriez besoin d'annuler vos modifications. L'utilisation d'un AMI comme sauvegarde n'est pas prise en charge. Pour plus d'informations, consultez Considérations de sauvegarde et de restauration pour les contrôleurs de domaine virtualisés dans la documentation Microsoft.
2. Exécutez la commande suivante pour configurer Windows afin qu'il démarre en mode restauration des services d'annuaire (DSRM).

   > **Warning**
   >
   > Avant d'exécuter cette commande, vérifiez que vous connaissez le DSRM mot de passe. Vous aurez besoin de ces informations pour vous connecter à votre instance une fois que la mise à niveau est terminée et que l'instance redémarre automatiquement.

   ```
   bcdedit /set {default} safeboot dsrepair
   ```

   PowerShell:

   ```
   PS C:\> bcdedit /set "{default}" safeboot dsrepair
   ```

   Le système doit démarrer DSRM car l'utilitaire de mise à niveau supprime les pilotes de stockage PV Citrix afin de pouvoir installer les pilotes AWS PV. Nous vous recommandons donc de noter les lettres de lecteur et mappages de dossiers aux disques secondaires dans Gestion des disques. En l'absence de pilote de stockage PV Citrix, les disques secondaires ne sont pas détectés. Les contrôleurs de domaine qui utilisent un NTDS dossier sur des disques secondaires ne démarrent pas car le disque secondaire n'est pas détecté.

> **Warning**
>
> Après avoir exécuté cette commande, ne redémarrez pas le système manuellement. Le système sera inaccessible car les pilotes PV Citrix ne sont pas pris en chargeDSRM.

3. Exécutez la commande suivante pour ajouter **`DisableDCCheck`** au registre :

```
reg add HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck /t
 REG_SZ /d true
```

4. Téléchargez le package de pilotes le plus récent sur l'instance.
5. Extrayez le contenu du dossier, puis exécutez `AWSPVDriverSetup.msi`.

   Après avoir exécuté leMSI, l'instance redémarre automatiquement puis met à niveau le pilote. L'instance ne sera pas disponible pendant 15 minutes.
6. Une fois la mise à niveau terminée et l'instance passée les deux tests de santé dans la EC2 console Amazon, connectez-vous à l'instance à l'aide de Remote Desktop. Ouvrez Gestion des disques pour vérifier la présence de volumes secondaires hors ligne et les mettre en ligne en les faisant correspondre aux lettres des lecteurs et aux mappages de dossiers notés précédemment.

   Vous devez vous connecter à l'instance en spécifiant le nom d'utilisateur au format suivant hostname \ administrator. Par exemple, Win2k12 \ administratorTestBox.
7. Exécutez la commande suivante pour supprimer la configuration de DSRM démarrage :

```
bcdedit /deletevalue safeboot
```

8. Redémarrez l'instance.
9. Pour exécuter le processus de mise à niveau, vérifiez que le nouveau pilote a été installé. Dans le Gestionnaire de périphériques, sous Contrôleurs de stockage, recherchez Carte hôte AWS PV Storage. Vérifiez que la version du pilote est identique à la version la plus récente répertoriée dans l'historique des versions de pilote. Pour plus d'informations, consultez AWS Historique du package de pilotes PV.
10. Exécutez la commande suivante pour supprimer **`DisableDCCheck`** du registre :

```
reg delete HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck
```

> **Note**
>
> Si vous avez précédemment désactivé TCPdéchargement l'utilisation de Netsh pour les pilotes PV Citrix, nous vous recommandons de réactiver cette fonctionnalité après la mise à niveau vers les pilotes AWS PV. TCPLes problèmes de déchargement liés aux pilotes Citrix ne sont pas présents dans les pilotes AWS PV. Par conséquent, le TCP déchargement offre de meilleures performances avec les pilotes AWS photovoltaïques.

Mise à niveau des instances Windows Server 2008 et 2008 R2 (Mise à niveau d'un PV Redhat vers Citrix)

Avant de commencer à mettre à niveau vos RedHat pilotes vers les pilotes PV Citrix, assurez-vous de suivre les étapes suivantes :

- Installez la dernière version du EC2Config service. Pour de plus amples informations, veuillez consulter Installez la dernière version de EC2Config.
- Vérifiez que Windows PowerShell 3.0 est installé. Pour vérifier la version que vous avez installée, exécutez la commande suivante dans une PowerShell fenêtre :

  ```
  PS C:\> $PSVersionTable.PSVersion
  ```

  Windows PowerShell 3.0 est fourni dans le package d'installation de Windows Management Framework (WMF) version 3.0. Si vous devez installer Windows PowerShell 3.0, consultez la section Windows Management Framework 3.0 dans le Microsoft Download Center.
- Sauvegardez vos informations importantes sur l'instance ou créez-en une AMI à partir de l'instance. Pour plus d'informations sur la création d'unAMI, consultezCréez un compte soutenu EBS par Amazon AMI.

  > **Tip**
  >
  > Au lieu de le créer AMI depuis la EC2 console Amazon, vous pouvez utiliser Systems Manager Automation pour le créer à l'AMIaide du `AWS-CreateImage` runbook. Pour plus d'informations, consultez le Guide AWS-CreateImagede l'utilisateur de référence du runbook AWS Systems Manager Automation.

Si vous créez unAMI, assurez-vous d'effectuer les opérations suivantes :

- Prenez note de votre mot de passe.
- N'exécutez pas l'outil Sysprep manuellement ou à l'aide du service. EC2Config
- Configurez votre adaptateur Ethernet pour obtenir automatiquement une adresse IP à l'aide deDHCP.

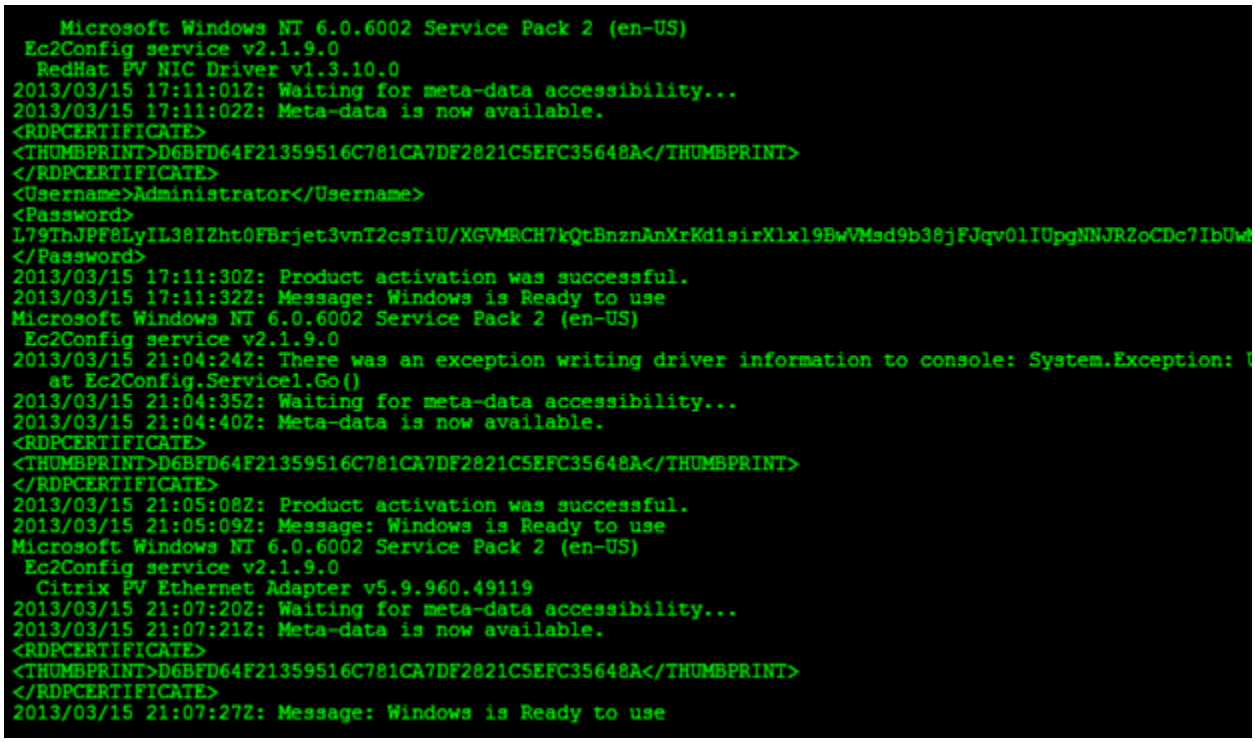
Pour mettre à niveau RedHat les pilotes

1. Connectez-vous à votre instance en tant qu'administrateur local. Pour plus d'informations sur la connexion à votre instance, consultez Connectez-vous à votre instance Windows à l'aide de RDP.
2. Dans votre instance, téléchargez le package de mise à niveau de PV Citrix.
3. Extrayez le contenu du package de mise à niveau à un emplacement de votre choix.
4. Double-cliquez sur le fichier Upgrade.bat. Si vous recevez un avertissement de sécurité, cliquez sur Run (Exécuter).
5. Dans la boîte de dialogue Upgrade Drivers (Mettre à niveau les pilotes), consultez les informations et cliquez sur Yes (Oui) si vous êtes prêt à démarrer la mise à niveau.
6. Dans la boîte de dialogue de désinstallation des pilotes Xen paravirtualisés Red Hat pour Windows, choisissez Oui pour supprimer le logiciel. RedHat Votre instance va être redémarrée.

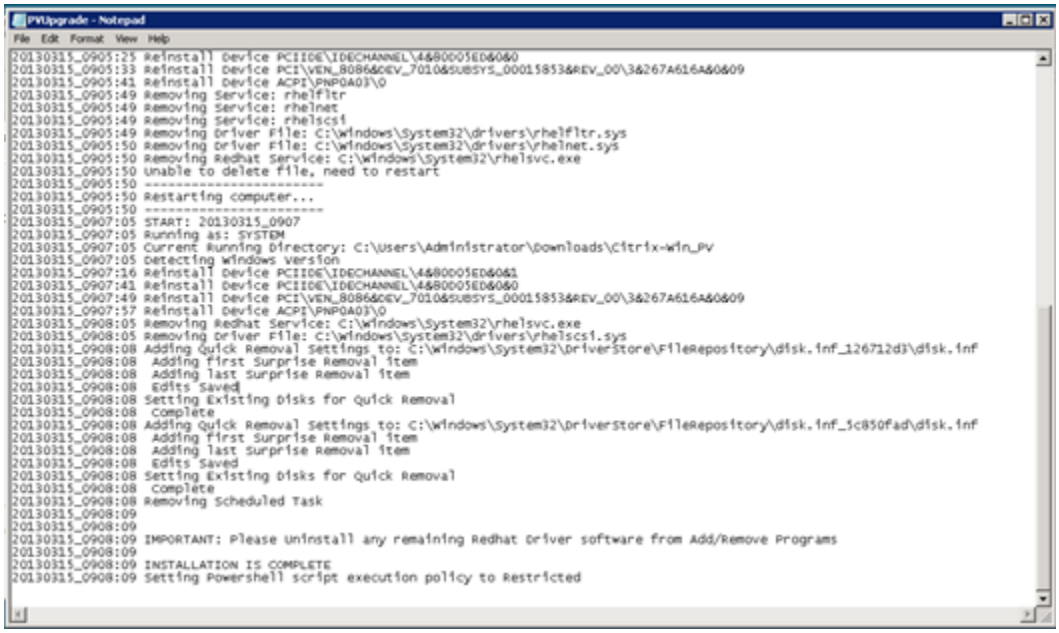
> **Note**
>
> Si la boîte de dialogue du programme de désinstallation ne s'affiche pas, cliquez sur Red Hat Paravirtualize... dans la barre des tâches de Windows.

7. Vérifiez que l'instance a été redémarrée et qu'elle est prête à être utilisée.
   a. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
   b. Sur la page Instances, sélectionnez Actions, Surveiller et dépanner, puis Obtenir le journal système.

c. Les opérations de mise à niveau doivent avoir redémarré le serveur 3 ou 4 fois. Vous pouvez vous en assurer dans le fichier journal avec le nombre de fois où `Windows is Ready to use` s'affiche.



8. Connectez-vous à votre instance en tant qu'administrateur local.
9. Fermez la boîte de dialogue Red Hat Paravirtualized Xen Drivers for Windows uninstaller (Programme de désinstallation des pilotes Xen Red Hat Paravirtualize pour Windows).
10. Confirmez que l'installation est terminée. Accédez au dossier `Citrix-WIN_PV` que vous avez extrait précédemment, ouvrez le fichier `PVUpgrade.log`, puis recherchez le texte `INSTALLATION IS COMPLETE`.



Mettre à niveau votre service d'agent invité Citrix Xen

Si vous utilisez des pilotes PV Citrix sur Windows Server, vous pouvez mettre à niveau le service d'agent invité Citrix Xen. Ce service Windows gère des tâches telles que les événements d'arrêt et de redémarrage à partir duAPI. Vous pouvez exécuter ce package de mise à niveau sur toute version de Windows Server dans la mesure où l'instance exécute des pilotes PV Citrix.

> **Important**
>
> Pour Windows Server 2008 R2 et versions ultérieures, nous vous recommandons de passer aux pilotes AWS PV qui incluent la mise à jour de l'agent invité.

Avant de commencer à mettre à niveau vos pilotes, assurez-vous de sauvegarder vos informations importantes sur l'instance ou d'en créer une AMI à partir de l'instance. Pour plus d'informations sur la création d'unAMI, consultezCréez un compte soutenu EBS par Amazon AMI.

> **Tip**
>
> Au lieu de le créer AMI depuis la EC2 console Amazon, vous pouvez utiliser Systems Manager Automation pour le créer à l'AMIaide du `AWS-CreateImage` runbook. Pour plus

d'informations, consultez le Guide AWS-CreateImagede l'utilisateur de référence du runbook AWS Systems Manager Automation.

Si vous créez unAMI, veillez à effectuer les opérations suivantes :

- N'activez pas l'outil Sysprep dans le service. EC2Config
- Prenez note de votre mot de passe.
- Réglez votre adaptateur Ethernet surDHCP.

Pour mettre à niveau votre service d'agent invité Citrix Xen

1. Connectez-vous à votre instance en tant qu'administrateur local. Pour plus d'informations sur la connexion à votre instance, consultez Connectez-vous à votre instance Windows à l'aide de RDP.
2. Dans votre instance, téléchargez le package de mise à niveau de Citrix.
3. Extrayez le contenu du package de mise à niveau à un emplacement de votre choix.
4. Double-cliquez sur le fichier Upgrade.bat. Si vous recevez un avertissement de sécurité, cliquez sur Run (Exécuter).
5. Dans la boîte de dialogue Upgrade Drivers (Mettre à niveau les pilotes), consultez les informations et cliquez sur Yes (Oui) si vous êtes prêt à démarrer la mise à niveau.
6. Une fois la mise à niveau terminée, le fichier `PVUpgrade.log` s'ouvre et affiche le texte `UPGRADE IS COMPLETE`.
7. Redémarrez votre instance.

Résoudre les problèmes liés aux pilotes PV sur les instances Windows

Vous trouverez ci-dessous des solutions aux problèmes que vous pourriez rencontrer avec les anciennes EC2 images Amazon et les anciens pilotes PV.

Table des matières

- Les charges de travail qui exploitent plus de 20 000 disques IOPS subissent une dégradation due à des goulots d'étranglement CPU

Windows Server 2012 R2 perd la connectivité au réseau ou à l'unité de stockage après le redémarrage d'une instance

> **Important**
>
> Ce problème se produit uniquement AMIs s'il est disponible avant septembre 2014.

Windows Server 2012 R2 Amazon Machine Images (AMIs) mises à disposition avant le 10 septembre 2014 peuvent perdre la connectivité réseau et de stockage après le redémarrage d'une instance. L'erreur dans le journal du AWS Management Console système indique : « Difficulté à détecter les détails du pilote PV pour la sortie de console ». La perte de connectivité est causée par la fonction de nettoyage Plug and Play. Cette fonction recherche et désactive les périphériques système inactifs tous les 30 jours. La fonctionnalité identifie incorrectement le périphérique EC2 réseau comme étant inactif et le supprime du système. Le cas échéant, l'instance perd la connectivité au réseau après un redémarrage.

Pour les systèmes que vous soupçonnez d'être vulnérables à ce problème, vous pouvez télécharger et exécuter une mise à niveau de pilote sur place. Si vous ne parvenez pas à effectuer la mise à jour du pilote sur place, vous pouvez exécuter un script d'assistant. Ce script détermine si le problème affecte votre instance. S'il est concerné et que le périphérique EC2 réseau Amazon n'a pas été retiré, le script désactive le scan Plug and Play Cleanup. Si le périphérique réseau a été supprimé, le script le répare, désactive l'analyse de la fonctionnalité de nettoyage Plug and Play et laisse l'instance redémarrer avec la connectivité réseau activée.

Sommaire

Choisir comment résoudre les problèmes

Deux méthodes vous permettent de restaurer la connectivité au réseau et au stockage d'une instance affectée par ce problème. Choisissez l'une des méthodes suivantes :

Méthode	Prérequis	Présentation de la procédure
Méthode 1 - Mise en réseau améliorée	La mise en réseau améliorée n'est disponible que dans un cloud privé virtuel (VPC) qui nécessite un type d'instanc e C3. Si le serveur n'utilise pas le type d'instance C3 actuellement, vous devez le modifier temporairement.	Vous modifiez le type d'instance du serveur pour une instance C3. La mise en réseau améliorée vous permet de vous connecter à l'instance affectée pour résoudre le problème. Une fois le problème résolu, vous modifiez à nouveau l'instance pour revenir au type d'instanc e original. Cette méthode est généralement plus rapide que la Méthode 2 et risque moins entraîner des erreurs d'utilisa teur. Des frais supplémen taires seront facturés tant que l'instance C3 sera en cours d'exécution.
Méthode 2 - Configuration du registre	Capacité à créer ou à accéder à un second serveur. Capacité à modifier les paramètres du registre.	Démontez et détachez le volume racine à partir de l'instance affectée, attachez-le à une autre instance et effectuez les modifications dans le registre. Des frais supplémentaires seront facturés tant que le serveur supplémentaire sera en cours d'exécution. Cette méthode est plus lente que

Méthode	Prérequis	Présentation de la procédure
		la Méthode 1, mais elle a fonctionné dans certaines situations dans lesquelles la Méthode 1 a échoué à résoudre le problème.

Méthode 1 - Mise en réseau améliorée

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Recherchez l'instance concernée. Sélectionnez l'instance, État de l'instance, puis Arrêter l'instance.

   > **Warning**
   >
   > Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

4. Une fois l'instance arrêtée, créez une sauvegarde. Sélectionnez l'instance, puis Actions, Image et modèles, et enfin Créer une image.
5. Modifiez le type d'instance avec un n'importe quel type d'instance C3.
6. Démarrez l'instance.
7. Connectez-vous à l'instance à l'aide de Remote Desktop, puis téléchargez le package AWS PV Drivers Upgrade sur l'instance.
8. Extrayez le contenu du dossier, puis exécutez `AWSPVDriverSetup.msi`.

   Après avoir exécuté leMSI, l'instance redémarre automatiquement puis met à niveau les pilotes. L'instance ne sera pas disponible pendant 15 minutes.
9. Une fois la mise à niveau terminée et l'instance passée les deux tests de santé dans la EC2 console Amazon, connectez-vous à l'instance à l'aide de Remote Desktop et vérifiez que les nouveaux pilotes ont été installés. Dans le Gestionnaire de périphériques, sous Contrôleurs de stockage, recherchez Carte hôte AWS PV Storage. Vérifiez que la version du pilote est

identique à la version la plus récente répertoriée dans l'historique des versions de pilote. Pour plus d'informations, consultez AWS Historique du package de pilotes PV.

10. Arrêtez l'instance et modifiez-la à nouveau pour revenir à son type d'instance original.
11. Démarrez l'instance et reprenez une utilisation normale.

Méthode 2 - Configuration du registre

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Recherchez l'instance concernée. Sélectionnez l'instance, État de l'instance, puis Arrêter l'instance.

> **Warning**
>
> Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

4. Sélectionnez Lancer des instances et créez une instance Windows Server 2008 ou Windows Server 2012 dans la même zone de disponibilité que l'instance affectée. Ne créez pas d'instance Windows Server 2012 R2.

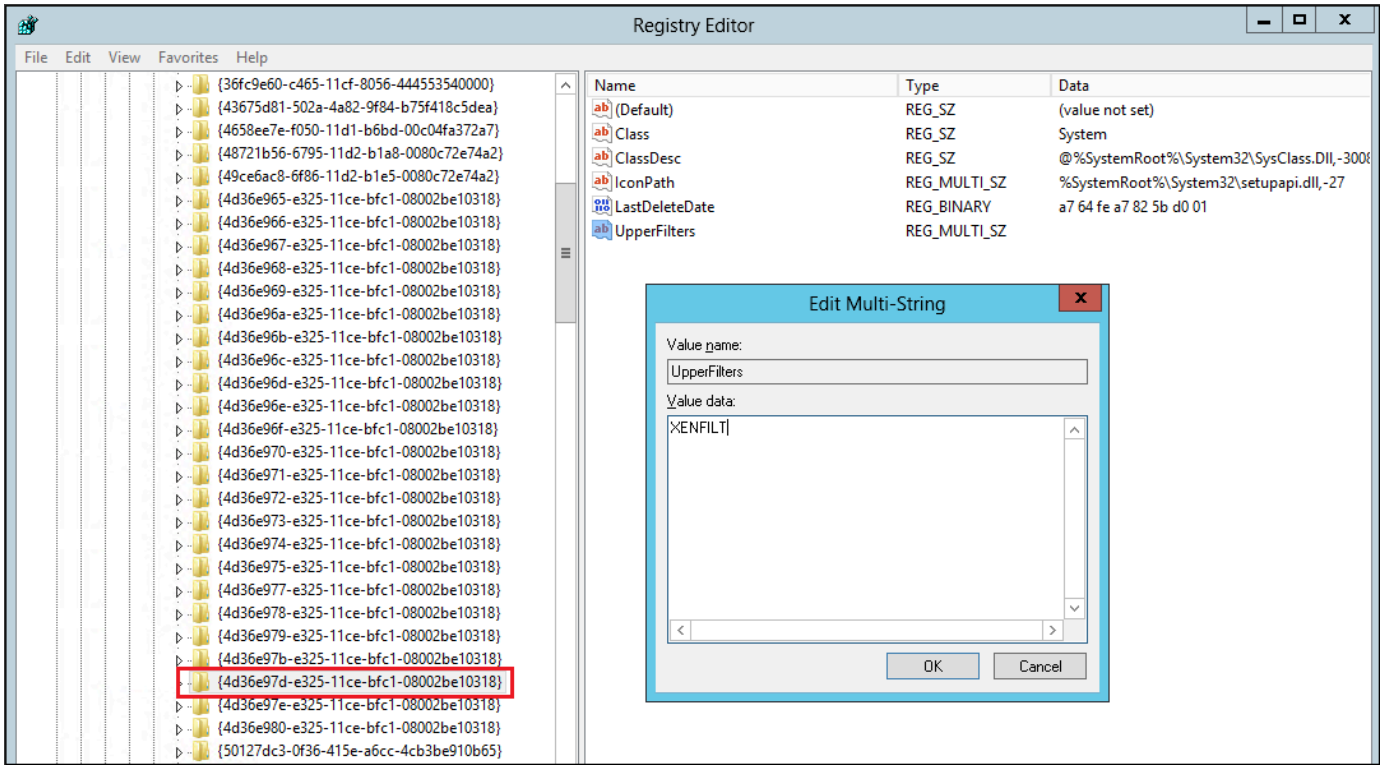
> **Important**
>
> Si vous ne créez pas l'instance dans la même zone de disponibilité que l'instance affectée, vous ne pourrez pas attacher le volume racine de celle-ci à la nouvelle instance.

5. Dans le panneau de navigation, choisissez Volumes.
6. Recherchez le volume racine de l'instance affectée. Détachez le volume et attachez-le à l'instance temporaire que vous avez créée précédemment. Attachez-le avec le nom du périphérique par défaut (xvdf).
7. Utilisez les services Bureau à distance pour vous connecter à l'instance temporaire, puis utilisez l'utilitaire Gestion des disques pour rendre le volume disponible.
8. Sur l'instance temporaire, ouvrez la boîte de dialogue Run (Exécuter), tapez **`regedit`** et appuyez sur Entrée.

9. Dans le volet de navigation de l'éditeur de registre, choisissez HKEY_Local_Machine, puis dans le menu Fichier, choisissez Load Hive.
10. Dans la boîte de dialogue Load Hive (Charger Hive), accédez à Affected Volume (Volume affecté)\Windows\System32\config\System et tapez un nom temporaire dans a boîte de dialogue Key Name (Nom de la clé). Par exemple, entrez OldSys.
11. Dans le volet de navigation de l'Editeur du registre, recherchez les clés suivantes :

    HKEY_LOCAL_MACHINE***your_temporary_key_name***\ ControlSet 001 \ Contrôle \ Classe \ 4d36e97d-e325-11ce-bfc1-08002be10318

    HKEY_LOCAL_MACHINE***your_temporary_key_name***\ ControlSet 001 \ Contrôle \ Classe \ 4d36e96a-e325-11ce-bfc1-08002be10318
12. Pour chaque touche, double-cliquez UpperFilters, entrez une valeur deXENFILT, puis choisissez OK.



13. Recherchez les clés suivantes :

    HKEY_LOCAL_MACHINE***your_temporary_key_name***\ ControlSet 001 \ Services \ XENBUS \ Paramètres
14. Créez une nouvelle chaîne (REG_SZ) avec le nom ActiveDevice et la valeur suivants :

PCI\ VEN _5853 & _0001 & _00015853 & DEV _01 SUBSYS REV

15. Recherchez les clés suivantes :

    HKEY_LOCAL_MACHINE***your_temporary_key_name**\ ControlSet 001 \ Services \ XENBUS

16. Remplacez la valeur Nombre de 0 à 1.
17. Recherchez et supprimez les clés suivantes :

    HKEY_LOCAL_MACHINE***your_temporary_key_name**\ ControlSet 001 \ Prestations \ xenvbd \ StartOverride

    HKEY_LOCAL_MACHINE ***your_temporary_key_name**\ ControlSet 001 \ Services \ xenfilt \ StartOverride

18. Dans le volet de navigation de l'Editeur du Registre, choisissez la clé temporaire que vous avez créée lorsque vous avez ouvert pour la première fois l'Editeur du Registre.
19. Dans le menu File (Fichier), choisissez Unload Hive (Décharger Hive).
20. Dans l'utilitaire Gestion des disques, choisissez le lecteur que vous avez attaché précédemment, ouvrez le menu contextuel (clic droit) et choisissez Hors connexion.
21. Dans la EC2 console Amazon, détachez le volume concerné de l'instance temporaire et attachez-le à nouveau à votre instance Windows Server 2012 R2 avec le nom de l'appareil /dev/sda1. Vous devez spécifier ce nom de périphérique pour désigner le volume en tant que volume racine.
22. Démarrez l'instance.
23. Connectez-vous à l'instance à l'aide de Remote Desktop, puis téléchargez le package AWS PV Drivers Upgrade sur l'instance.
24. Extrayez le contenu du dossier, puis exécutez `AWSPVDriverSetup.msi`.

    Après avoir exécuté leMSI, l'instance redémarre automatiquement puis met à niveau les pilotes. L'instance ne sera pas disponible pendant 15 minutes.

25. Une fois la mise à niveau terminée et l'instance passée les deux tests de santé dans la EC2 console Amazon, connectez-vous à l'instance à l'aide de Remote Desktop et vérifiez que les nouveaux pilotes ont été installés. Dans le Gestionnaire de périphériques, sous Contrôleurs de stockage, recherchez Carte hôte AWS PV Storage. Vérifiez que la version du pilote est identique à la version la plus récente répertoriée dans l'historique des versions de pilote. Pour plus d'informations, consultez AWS Historique du package de pilotes PV.

26. Supprimez ou arrêtez l'instance temporaire que vous avez créée au cours de cette procédure.

Exécuter le script de correction

Si vous ne pouvez pas exécuter une mise à niveau du pilote sur place ou migrer vers une instance plus récente, vous pouvez exécuter le script de correction pour corriger les problèmes causés par la tâche de nettoyage Plug and Play.

Pour exécuter le script de correction

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance pour laquelle vous souhaitez exécuter le script de correction. Sélectionnez État de l'instance, puis Arrêter l'instance.

   > **Warning**
   >
   > Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

4. Une fois l'instance arrêtée, créez une sauvegarde. Sélectionnez l'instance, puis Actions, Image et modèles et enfin Créer une image.
5. Sélectionnez État de l'instance, puis Démarrer l'instance.
6. Connectez-vous à l'instance à l'aide de Remote Desktop, puis téléchargez le dossier RemediateDriverIssue .zip sur l'instance.
7. Extrayez le contenu du dossier.
8. Exécutez le script de correction en fonction des instructions contenues dans le fichier Readme.txt. Le fichier se trouve dans le dossier dans lequel vous avez extrait le fichier RemediateDriverIssue .zip.

TCPdéchargement

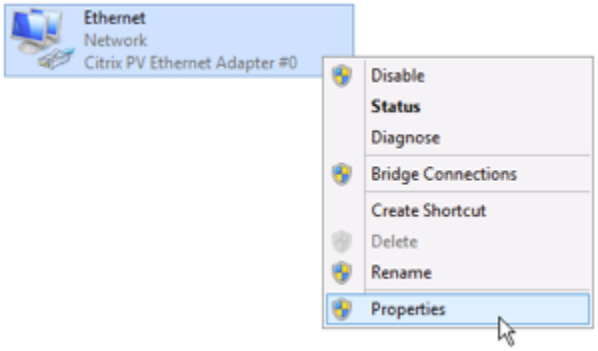
> **Important**
>
> Ce problème ne s'applique pas aux instances exécutant des pilotes réseau AWS PV ou Intel.

Par défaut, le TCP déchargement est activé pour les pilotes PV Citrix sous WindowsAMIs. Si vous rencontrez des erreurs au niveau du transport ou des erreurs de transmission de paquets (comme le montre l'Analyseur de performances Windows), par exemple lorsque vous exécutez certaines SQL charges de travail, vous devrez peut-être désactiver cette fonctionnalité.

> **Warning**
>
> La désactivation TCP du déchargement peut réduire les performances réseau de votre instance.

Pour désactiver le TCP déchargement pour Windows Server 2012 et 2008

1. Connectez-vous à votre instance en tant qu'administrateur local.
2. Si vous utilisez Windows Server 2012, appuyez sur Ctrl+Échap pour accéder à l'écran Démarrer, puis cliquez sur Panneau de configuration. Si vous utilisez Windows Server 2008, cliquez sur Démarrer et sélectionnez Panneau de configuration.
3. Choisissez Réseau et Internet, puis Centre Réseau et partage.
4. Cliquez sur Modifier les paramètres de la carte.
5. Cliquez avec le bouton droit sur Carte Ethernet PV Citrix #0, puis cliquez sur Propriétés.



6. Dans la boîte de dialogue Propriétés de la connexion au réseau local, cliquez sur Configurer pour ouvrir la boîte de dialogue Propriétés de la carte Ethernet PV Citrix #0.
7. Dans l'onglet Avancé, désactivez chacune des propriétés, à l'exception de CorrectTCP/UDPChecksum Value. Pour désactiver une propriété, sélectionnez-la dans Property (Propriété) et choisissez Disabled (Désactivé) dans Value (Valeur).
8. Choisissez OK.
9. A partir d'une fenêtre d'invite de commande, exécutez les commandes suivantes :

```
netsh int ip set global taskoffload=disabled
netsh int tcp set global chimney=disabled
netsh int tcp set global rss=disabled
netsh int tcp set global netdma=disabled
```

10. Redémarrez l'instance.

Synchronisation du temps

Avant la sortie de Windows 2013.02.13AMI, l'agent invité Citrix Xen pouvait définir l'heure système de manière incorrecte. Cela peut entraîner l'expiration de votre DHCP bail. En cas de problème pour vous connecter à votre instance, vous pouvez avoir besoin de mettre à niveau l'agent.

Pour déterminer si vous avez l'agent invité Citrix Xen mis à jour, vérifiez que le fichier `C:\Program Files\Citrix\XenGuestAgent.exe` date de mars 2013. Si la date sur le fichier est antérieure, mettez à jour le service d'agent invité Citrix Xen. Pour de plus amples informations, veuillez consulter Mettre à niveau votre service d'agent invité Citrix Xen.

Les charges de travail qui exploitent plus de 20 000 disques IOPS subissent une dégradation due à des goulots d'étranglement CPU

Vous pouvez être concerné par ce problème si vous utilisez des instances Windows exécutant des pilotes AWS PV qui exploitent plus de 20 000 IOPS pilotes et que vous rencontrez un code de vérification des bogues`0x9E: USER_MODE_HEALTH_MONITOR`.

Les lectures et écritures sur disque (IOs) dans les pilotes AWS PV se déroulent en deux phases : préparation des E/S et achèvement des E/S. Par défaut, la phase de préparation s'exécute sur un cœur arbitraire unique. La phase d'achèvement s'exécute sur le cœur `0`. La quantité de calcul requise pour traiter une opération d'IO varie en fonction de sa taille et d'autres propriétés. Certains IOs utilisent davantage de calculs dans la phase de préparation, d'autres dans la phase d'achèvement. Lorsqu'une instance en génère plus de 20 000IOPS, la phase de préparation ou d'achèvement peut créer un goulot d'étranglement, la capacité CPU sur laquelle elle s'exécute étant atteinte à 100 % de sa capacité. Le fait que la phase de préparation ou d'achèvement devienne un goulot d'étranglement dépend des propriétés du produit IOs utilisé par l'application.

À partir de la version 8.4.0 des pilotes AWS photovoltaïques, la charge de la phase de préparation et de la phase d'achèvement peut être répartie sur plusieurs cœurs, éliminant ainsi les goulots d'étranglement. Chaque application utilise des propriétés d'IO différentes. Par conséquent, l'application de l'une des configurations suivantes peut augmenter, diminuer ou ne pas affecter

les performances de votre application. Après avoir appliqué l'une de ces configurations, surveillez l'application pour vérifier qu'elle enregistre les performances souhaitées.

1. Prérequis

   Avant de commencer cette procédure de dépannage, vérifiez que les prérequis suivants sont respectés :

   - Votre instance utilise la version 8.4.0 ou ultérieure des pilotes AWS PV. Pour effectuer une mise à niveau, consultez Mettre à niveau les pilotes PV sur EC2 les instances Windows.
   - Vous avez RDP accès à l'instance. Pour savoir comment vous connecter à votre instance Windows à l'aide deRDP, consultezConnectez-vous à votre instance Windows à l'aide d'un RDP client.
   - Vous disposez d'un accès administrateur à l'instance.

2. Observez CPU la charge sur votre instance

   Vous pouvez utiliser le Gestionnaire des tâches de Windows pour visualiser la charge de chacun d'entre eux afin CPU de déterminer les obstacles potentiels aux E/S sur le disque.

   1. Vérifiez que votre application est en cours d'exécution et gère un trafic similaire à votre charge de travail de production.
   2. Connectez-vous à votre instance à l'aide deRDP.
   3. Accédez menu Start (Démarrer) de votre instance.
   4. Saisissez `Task Manager` dans le menu Start (Démarrer) pour ouvrir le Gestionnaire des tâches.
   5. Si le Gestionnaire des tâches affiche la vue récapitulative, choisissez More details (Plus de détails) pour développer la vue détaillée.
   6. Sélectionnez l'onglet Performance.
   7. Sélectionnez CPUdans le volet de gauche.
   8. Cliquez avec le bouton droit de la souris sur le graphique dans le volet principal et sélectionnez Change graph to>Logical processors (Changer le graphique en > processeurs logiques) pour afficher chaque cœur individuel.
   9. Selon le nombre de cœurs présents sur votre instance, vous pouvez voir des lignes indiquant la CPU charge au fil du temps, ou simplement un chiffre.
      - Si vous voyez des graphiques illustrant la charge au fil du temps, recherchez les CPUs endroits où le cadre est presque entièrement ombré.

- Si vous voyez un nombre sur chaque cœur, recherchez les cœurs qui affichent systématiquement 95 % ou plus.

10. Notez si le cœur `0` ou un autre cœur subit une charge lourde.

3. Choisir la configuration à appliquer

Nom de la configuration	Quand appliquer cette configuration	Remarques
Default configuration	La charge de travail en génère moins de 20 000IOPS, ou les autres configurations n'ont pas amélioré les performances ou la stabilité.	Pour cette configuration, les IO se produisent sur quelques cœurs, ce qui peut bénéficier à des charges de travail plus petites en augmentant la localité du cache et en réduisant le basculement de contexte.
Allow driver to choose whether to distribute completion	La charge de travail en entraîne plus de 20 000 IOPS et une charge modérée ou élevée est observée sur le noyau`0`.	Cette configuration est recommandée pour toutes les instances Xen utilisant PV 8.4.0 ou version ultérieur e et exploitant plus de 20 000 instancesIOPS, que des problèmes soient rencontrés ou non.
Distribute both preparation and completion	La charge de travail en entraîne plus de 20 000IOPS, et soit le fait de permettre au conducteur de choisir la distribution n'a pas amélioré les performan ces, soit un cœur autre que celui qui `0` est soumis à une charge élevée.	Cette configuration permet la distribution à la fois de la préparation et de l'achèvem ent des IO.

> **Note**
>
> Nous vous recommandons de ne pas distribuer la préparation des IO sans distribuer également l'achèvement des IO (ne pas définir `DpcRedirection` sans définir `NotifierDistributed`), car la phase d'achèvement est sensible à la surcharge par la phase de préparation lorsque la phase de préparation est exécutée en parallèle.

Valeurs clés de registre

- NotifierDistributed

  Valeur `0` ou aucune valeur — La phase d'achèvement se déroulera sur le cœur `0`.

  Valeur `1` — Le pilote choisit d'exécuter la phase d'achèvement sur le cœur `0` ou sur un cœur supplémentaire par disque connecté.

  Valeur `2` — Le pilote exécute la phase d'achèvement sur un cœur supplémentaire par disque connecté.
- DpcRedirection

  Valeur `0` ou aucune valeur — La phase de préparation se déroulera sur un cœur unique et arbitraire.

  Valeur `1` — La phase de préparation est répartie sur plusieurs cœurs.

Configuration par défaut

Appliquez la configuration par défaut avec les versions du pilote AWS PV antérieures à la version 8.4.0, ou si une dégradation des performances ou de la stabilité est observée après l'application de l'une des autres configurations de cette section.

1. Connectez-vous à votre instance à l'aide deRDP.
2. Ouvrez une nouvelle invite de PowerShell commande en tant qu'administrateur.

3. Exécutez les commandes suivantes pour supprimer les clés de registre `NotifierDistributed` et `DpcRedirection`.

```
Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Name NotifierDistributed
```

```
Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Name DpcRedirection
```

4. Redémarrez votre instance.

Autoriser le pilote à choisir s'il doit distribuer l'achèvement

Définissez la clé de registre `NotiferDistributed` pour permettre au pilote de stockage PV de choisir de distribuer ou non l'achèvement des IO.

1. Connectez-vous à votre instance à l'aide deRDP.
2. Ouvrez une nouvelle invite de PowerShell commande en tant qu'administrateur.
3. Exécutez la commande suivante pour ajouter la clé de registre `NotiferDistributed`.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name NotifierDistributed
```

4. Redémarrez votre instance.

Distribuer la préparation et l'achèvement

Définissez les clés de registre `NotifierDistributed` et `DpcRedirection` pour toujours distribuer les phases de préparation et d'achèvement.

1. Connectez-vous à votre instance à l'aide deRDP.
2. Ouvrez une nouvelle invite de PowerShell commande en tant qu'administrateur.
3. Exécutez les commandes suivantes pour définir les clés de registre `NotifierDistributed` et `DpcRedirection`.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000002 -Name NotifierDistributed
```

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name DpcRedirection
```

4. Redémarrez votre instance.

AWS NVMepilotes pour instances Windows

EBSLes volumes Amazon et les volumes de stockage d'instances sont exposés sous forme de NVMe blocs sur des instances basées sur le système AWS Nitro. Pour utiliser pleinement les performances et les fonctionnalités des EBS fonctionnalités d'Amazon pour les volumes exposés sous forme de périphériques en mode NVMe bloc, le AWS NVMe pilote doit être installé sur l'instance. Le AWS NVMe pilote est installé par défaut sur tous les systèmes AWS Windows AMIs de dernière génération.

Pour plus d'informations sur EBS etNVMe, consultez Amazon EBS et NVMe le guide de EBS l'utilisateur Amazon. Pour plus d'informations sur le stockage d'SSDinstances etNVMe, consultezSSDvolumes de stockage d'instance pour les EC2 instances.

Installez ou mettez à niveau AWS NVMe les pilotes à l'aide de PowerShell

Si vous n'utilisez pas la dernière version de AWS Windows AMIs fournie par Amazon, suivez la procédure ci-dessous pour installer le AWS NVMe pilote actuel. Vous devez effectuer cette mise à jour à un moment où il est possible de redémarrer votre instance. Soit le script d'installation redémarre votre instance, soit vous la redémarrez à l'étape finale.

Prérequis

PowerShell 3.0 ou version ultérieure

Pour télécharger et installer le dernier AWS NVMe pilote

1. Nous vous recommandons de créer une sauvegarde AMI comme suit, au cas où vous auriez besoin d'annuler vos modifications.

   a. Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Avant d'arrêter une instance, vérifiez que vous avez copié toutes

les données dont vous avez besoin depuis les volumes de stockage de votre instance vers un stockage persistant, tel qu'Amazon EBS ou Amazon S3.

b. Dans le panneau de navigation, choisissez Instances.

c. Sélectionnez l'instance qui nécessite la mise à niveau du pilote, puis État de l'instance, Arrêter l'instance.

d. Une fois l'instance arrêtée, sélectionnez l'instance, puis Actions, Image et modèles, et enfin Créer une image.

e. Choisissez État de l'instance, Démarrer l'instance.

2. Connectez-vous à votre instance en tant qu'administrateur local.

3. Téléchargez et extrayez les pilotes vers votre instance à l'aide de l'une des options suivantes :

   - Avec un navigateur :

     a. Téléchargez le package de pilotes le plus récent sur l'instance.

     b. Décompressez l'archive zip.

   - En utilisant PowerShell :

```
Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/NVMe/
Latest/AWSNVMe.zip -outfile $env:USERPROFILE\nvme_driver.zip
Expand-Archive $env:userprofile\nvme_driver.zip -DestinationPath
 $env:userprofile\nvme_driver
```

> **Note**
>
> Si un message d'erreur s'affiche lors du téléchargement du fichier et que vous utilisez Windows Server 2016 ou une version antérieure, il est possible que la version TLS 1.2 doive être activée sur votre PowerShell terminal. Vous pouvez activer la TLS version 1.2 pour la PowerShell session en cours à l'aide de la commande suivante, puis réessayer :
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

4. Installez le pilote sur votre instance en exécutant le `install.ps1` PowerShell script depuis le `nvme_driver` répertoire (`.\install.ps1`). Si un message d'erreur s'affiche, assurez-vous que vous utilisez la PowerShell version 3.0 ou une version ultérieure.

a. (Facultatif) À partir de AWS NVMe la version`1.5.0`, les réservations persistantes Small Computer System Interface (SCSI) sont prises en charge pour Windows Server 2016 et versions ultérieures. Cette fonctionnalité ajoute la prise en charge du clustering Windows Server Failover avec un stockage Amazon EBS partagé. Par défaut, cette fonctionnalité n'est pas activée lors de l'installation.

   Vous pouvez désactiver cette fonctionnalité lors de l'exécution du script `install.ps1` pour installer le pilote en spécifiant le paramètre `EnableSCSIPersistentReservations` avec une valeur de `$true`.

```
PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $true
```

   Vous pouvez désactiver cette fonctionnalité lors de l'exécution du script `install.ps1` pour installer le pilote en spécifiant le paramètre `EnableSCSIPersistentReservations` avec une valeur de `$false`.

```
PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $false
```

b. À partir de AWS NVMe `1.5.0` là, le `install.ps1` script installe toujours l'`ebsnvme-id`outil avec le pilote.

   (Facultatif) Pour les versions `1.4.0`, `1.4.1` et `1.4.2`, le script `install.ps1` vous permet de spécifier si l'outil `ebsnvme-id` doit être installé avec le pilote.

   i. Pour installer l'outil `ebsnvme-id`, spécifiez `InstallEBSNVMeIdTool 'Yes'`.

   ii. Si vous ne souhaitez pas installer l'outil, spécifiez `InstallEBSNVMeIdTool 'No'`.

   Si vous ne spécifiez pas `InstallEBSNVMeIdTool` et que l'outil est déjà présent sur `C:\ProgramData\Amazon\Tools`, le package met à niveau l'outil par défaut. Si l'outil n'est pas présent, `install.ps1` ne mettra pas à niveau l'outil par défaut.

   Si vous ne souhaitez pas installer l'outil dans le package, mais que vous souhaitez l'installer ultérieurement, vous trouverez la dernière version ou l'outil dans le package du pilote. Vous pouvez également télécharger la version `1.0.0` depuis Amazon S3 :

   Téléchargez l'outil `ebsnvme-id`.

5. Si le programme d'installation ne redémarre pas votre instance, procédez vous-même au redémarrage.

Installation ou mise à niveau des AWS NVMe pilotes avec le distributeur

Vous pouvez utiliser Distributor, une fonctionnalité de AWS Systems Manager, pour installer le package de NVMe pilotes une seule fois ou avec des mises à jour planifiées.

1. Pour obtenir les instructions relatives à l'installation du package de NVMe pilotes à l'aide de Distributor, consultez les procédures décrites dans la section Installer ou mettre à jour des packages dans le guide de l'utilisateur d'Amazon EC2 Systems Manager.
2. Pour le type d'installation, sélectionnez Désinstaller et réinstallez.
3. Dans Nom, choisissez AWSNVMe.
4. (Facultatif) Pour les arguments supplémentaires, vous pouvez personnaliser l'installation en spécifiant des valeurs. Les valeurs doivent être mises en forme à l'aide d'une JSON syntaxe valide. Pour des exemples de transmission d'arguments supplémentaires pour le `aws configure` package, consultez la documentation Amazon EC2 Systems Manager.

   a. À partir de AWS NVMe`1.5.0`, le pilote prend en charge les réservations SCSI persistantes pour Windows Server 2016 et versions ultérieures. Par défaut, cette fonctionnalité n'est pas activée lors de l'installation.

      - Pour activer cette fonctionnalité, spécifiez`{"SSM_EnableSCSIPersistentReservations": "true"}`.
      - Si vous ne souhaitez pas activer cette fonctionnalité, spécifiez`{"SSM_EnableSCSIPersistentReservations": "false"}`.

   b. À partir de AWS NVMe `1.5.0` là, le `install.ps1` script installera toujours l'`ebsnvme-id`outil.

      (Facultatif) Pour les versions `1.4.0`, `1.4.1` et `1.4.2`, le script `install.ps1` vous permet de spécifier si l'outil ebsnvme-id doit être installé avec le pilote.

      - Pour installer l'outil ebsnvme-id, spécifiez. `{"SSM_InstallEBSNVMeIdTool": "Yes"}`
      - Si vous ne souhaitez pas installer l'outil, spécifiez `{"SSM_InstallEBSNVMeIdTool": "No"}`.

        Si `SSM_InstallEBSNVMeIdTool` n'est pas spécifié pour Additional Arguments (Arguments supplémentaires) et que l'outil est déjà présent sur `C:\ProgramData\Amazon\Tools`, le package met à niveau l'outil par défaut. Si l'outil n'est pas présent, le package ne mettra pas à niveau l'outil par défaut.

Si vous ne souhaitez pas installer l'outil dans le package, mais que vous souhaitez l'installer ultérieurement, vous trouverez la dernière version ou l'outil dans le package du pilote. Vous pouvez également télécharger la version `1.0.0` depuis Amazon S3 :

Téléchargez l'outil `ebsnvme-id`.

5. Si le programme d'installation ne redémarre pas votre instance, procédez vous-même au redémarrage.

Configuration SCSI des réservations persistantes

Une fois la version du AWS NVMe pilote `1.5.0` ou une version ultérieure installée, vous pouvez activer ou désactiver les réservations SCSI persistantes à l'aide du registre Windows pour Windows Server 2016 et versions ultérieures. Vous devez redémarrer l'instance pour que les modifications du registre prennent effet.

Vous pouvez activer les réservations SCSI persistantes à l'aide de la commande suivante qui définit la valeur `EnableSCSIPersistentReservations` à`1`.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters
\Device"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 1
```

Vous pouvez désactiver les réservations SCSI persistantes à l'aide de la `EnableSCSIPersistentReservations` commande suivante qui définit la valeur de`0`.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters
\Device"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 0
```

AWS NVMeHistorique des versions du pilote Windows

Le tableau suivant indique quels AWS NVMe pilotes s'exécutent sur chaque version de Windows Server sur AmazonEC2.

Version Windows Server	Version du pilote AWS NVMe
Windows Server 2022	dernière version

Version Windows Server	Version du pilote AWS NVMe
Windows Server 2019	dernière version
Windows Server 2016	dernière version
Windows Server 2012 R2	dernière version
Windows Server 2012	dernière version
Windows Server 2008 R2	version 1.3.2 et antérieures
Windows Server 2008	version 1.3.2 et antérieures

Le tableau suivant décrit les versions publiées du AWS NVMe pilote.

Version du package	Versions du pilote	Détails	Date de publication
1.5.1	1.5.0	Correction du script d'installation permettant de créer un dossier pour l'outil ebsnvme-id s'il n'est pas présent.	17 novembre 2023
1.5.0	1.5.0	Ajout de la prise en charge des réservations persistantes Small Computer System Interface (SCSI) pour les instances exécutant Windows Server 2016 et versions ultérieures. L'outil ebsnvme-id (`ebsnvme-id.exe`) est désormais installé par défaut.	31 août 2023
1.4.2	1.4.2	Correction d'un bogue qui Pilote AWS NVMe empêchait les volumes de stockage d'instance sur les instances D3.	16 mars 2023
1.4.1	1.4.1	Signale Namespace Preferred Write Granularity (NPGW) pour les EBS volumes qui prennent en charge cette fonctionnalité facultativeNVMe. Pour plus d'informations, consultez la section 8.25, « Amélioration des performances grâce à la taille des E/S et à	20 mai 2022

Version du package	Versions du pilote	Détails	Date de publication
		l'adhérence à l'alignement », dans la spécification de NVMe base, version 1.4.	
1.4.0	1.4.0	• Ajout d'un support IOCTLs permettant aux applications d'interagir avec NVMe les appareils. Cette prise en charge permet aux applications d'obtenir `IdentifyController` et de `NameSpace` répertorier des applications à partir de l'NVMeapp areil. `IdentifyNamespace` Pour plus d'informations, consultez Requêtes spécifiques au protocole dans la documentation Microsoft. • AWSNVMeL'installation de la version 1.4.0 sur Windows Server 2008 R2 échouera. AWSNVMe les versions 1.3.2 et antérieures sont prises en charge sur Windows Server 2008 R2. • La version 1.4.0 du pilote et le dernier outil `ebsnvme-id` (`ebsnvme-id.exe`) sont combinés dans un seul package. Cette combinaison vous permet d'installer à la fois le pilote et l'outil à partir d'un seul package. Pour en savoir plus, consultez Installez ou mettez à niveau AWS NVMe les pilotes à l'aide de PowerShell. • Correctifs de bogues et améliorations de fiabilité.	23 novembre 2021
1.3.2	1.3.2	Correction d'un problème lié à la modification des EBS volumes traitant activement les E/S, qui pouvait entraîner une corruption des données. Les clients qui ne modifient pas les EBS volumes en ligne (par exemple, en les redimensionnant ou en changeant de type) ne sont pas concernés.	10 septembre 2019

Version du package	Versions du pilote	Détails	Date de publication
1.3.1	1.3.1	Améliorations de la fiabilité.	21 mai 2019
1.3.0	1.3.0	Améliorations de l'optimisation des appareils.	31 août 2018
1.2.0	1.2.0	Améliorations des performances et de la fiabilité des AWS NVMe appareils sur toutes les instances prises en charge, y compris les instances bare metal.	13 juin 2018
1.0.0	1.0.0	AWS NVMepilote pour les types d'instances pris en charge exécutant Windows Server.	12 février 2018

S'abonner aux notifications

Amazon SNS peut vous avertir lorsque de nouvelles versions de EC2 Windows Drivers sont publiées. Pour vous abonner à ces notifications, utilisez la procédure suivante.

Pour vous abonner aux EC2 notifications depuis la console

1. Ouvrez la SNS console Amazon sur https://console.aws.amazon.com/sns/v3/home.
2. Dans la barre de navigation, changez la région en US Est (Virginie du Nord), si nécessaire. Vous devez sélectionner cette région car les SNS notifications auxquelles vous êtes abonné se trouvent dans cette région.
3. Dans le panneau de navigation, sélectionnez Abonnements.
4. Choisissez Créer un abonnement.
5. Dans la boîte de dialogue Créer un abonnement, exécutez l'une des actions suivantes :
   a. Pour le sujet ARN, copiez le nom de ressource Amazon suivant (ARN) :

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers
   b. Pour Protocole, choisissez `Email`.
   c. Pour Point de terminaison, tapez une adresse e-mail que vous pouvez utiliser pour recevoir les notifications.

d. Choisissez Créer un abonnement.

6. Vous recevrez rapidement un e-mail de confirmation. Ouvrez l'e-mail et suivez les instructions pour terminer votre abonnement.

Chaque fois que de nouveaux pilotes EC2 Windows sont publiés, nous envoyons des notifications aux abonnés. Si vous ne souhaitez plus recevoir ces notifications, exécutez la procédure suivante pour annuler votre abonnement.

Pour vous désabonner de la notification relative aux pilotes Amazon EC2 Windows

1. Ouvrez la SNS console Amazon sur https://console.aws.amazon.com/sns/v3/home.
2. Dans le panneau de navigation, choisissez Abonnements.
3. Cochez la case correspondant à l'abonnement, puis choisissez Actions, Supprimer des abonnements. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Pour vous abonner aux EC2 notifications à l'aide du AWS CLI

Pour vous abonner aux EC2 notifications avec le AWS CLI, utilisez la commande suivante.

```
aws sns subscribe --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers --
protocol email --notification-endpoint YourUserName@YourDomainName.ext
```

Pour vous abonner aux EC2 notifications à l'aide de AWS Tools for Windows PowerShell

Pour vous abonner aux EC2 notifications avec AWS Tools for Windows PowerShell, utilisez la commande suivante.

```
Connect-SNSNotification -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-
drivers' -Protocol email -Region us-east-1 -Endpoint 'YourUserName@YourDomainName.ext'
```

Configuration de votre instance Amazon EC2 Windows

Après avoir lancé une instance Windows, vous pouvez vous connecter en tant qu'administrateur pour effectuer une configuration supplémentaire des fonctionnalités Windows et des paramètres système.

Vous pouvez configurer les agents de lancement Windows et les autres fonctionnalités spécifiques à Windows comme suit.

Agents de lancement Windows

Chaque AWS système Windows AMI (et de nombreux autres AMIs appareils disponibles sur le AWS Marketplace) inclut un agent de lancement Windows préconfiguré avec les paramètres par défaut. Les agents de lancement exécutent des tâches lors du démarrage de l'instance et s'exécutent si une instance est arrêtée puis redémarrée ultérieurement, ou redémarrée.

EC2Lancement rapide pour Windows

Chaque instance Amazon EC2 Windows doit suivre les étapes de lancement standard du système d'exploitation (OS) Windows, qui incluent plusieurs redémarrages, et prennent souvent 15 minutes ou plus. Amazon EC2 Windows Server sur AMIs lequel la fonctionnalité EC2 Fast Launch est activée effectue certaines de ces étapes et redémarre à l'avance afin de réduire le temps nécessaire au lancement d'une instance.

> **Note**
>
> Les instances Amazon Elastic Graphics pour Windows ont atteint leur fin de vie le 8 janvier 2024. Pour les charges de travail nécessitant une accélération graphique, nous vous recommandons d'utiliser un type d'instance accéléré. Pour plus d'informations, consultez les spécifications relatives aux types d'instance pour le calcul accéléré dans le Amazon EC2 Instance Types Guide.

Paramètres système spécifiques à Windows

La liste suivante inclut certains paramètres système qui s'appliquent uniquement aux systèmes d'exploitation Windows :

Modifier le mot de passe de l'administrateur Windows

Lorsque vous vous connectez à une instance Windows, vous devez indiquer un compte utilisateur et un mot de passe autorisés à accéder à l'instance. La première fois que vous vous connectez à une instance, vous devez utiliser le compte administrateur et fournir le mot de passe par défaut. Lorsque vous vous connectez à une instance pour la première fois, nous vous recommandons de modifier la valeur entrée par défaut pour le mot de passe administrateur.

Ajouter des composants du système Windows

Les systèmes d'exploitation Windows Server comprennent de nombreux composants facultatifs. AMIIl n'est pas pratique d'inclure tous les composants facultatifs dans chaque serveur AWS Windows. Nous fournissons plutôt des EBS instantanés du support d'installation contenant les fichiers nécessaires pour configurer ou installer des composants sur votre instance Windows.

Installer WSL sous Windows.

Windows Subsystem for Linux (WSL) est un téléchargement gratuit que vous pouvez installer sur votre instance Windows. En installantWSL, vous pouvez exécuter des outils de ligne de commande Linux natifs directement sur votre instance Windows et utiliser les outils Linux pour créer des scripts, en plus de votre bureau Windows traditionnel. Vous pouvez facilement passer de Linux à Windows sur une seule instance Windows, ce qui peut s'avérer utile dans un environnement de développement.

Agents de lancement Windows sur les instances Amazon EC2 Windows

Chaque AWS Windows AMI inclut un agent de lancement Windows préconfiguré avec les paramètres par défaut. Les agents de lancement exécutent des tâches lors du démarrage de l'instance et s'exécutent si une instance est arrêtée puis redémarrée ultérieurement, ou redémarrée. Pour plus d'informations sur un agent spécifique, consultez les pages détaillées de la liste suivante.

Pour plus d'informations sur AWS WindowsAMIs, consultez la AMIréférence AWS Windows.

- Utiliser l'agent EC2Launch v2 pour effectuer des tâches lors du lancement de l'instance EC2 Windows
- Utiliser l'agent EC2Launch v1 pour effectuer des tâches lors du lancement de l'instance EC2 Windows
- Utiliser le EC2Config service pour effectuer des tâches lors du lancement de EC2 l'ancienne instance du système d'exploitation Windows

Contenu

- Comparez les agents EC2 de lancement Amazon
- Configurer le DNS suffixe pour les agents de lancement EC2 Windows
- Abonnez-vous aux notifications de l'agent de lancement EC2 Windows

- Migrer vers la EC2Launch version v2 pour les instances Windows
- Administration des services Windows pour la EC2Launch version 2 et les EC2Config agents

Comparez les agents EC2 de lancement Amazon

Le tableau suivant montre les principales différences fonctionnelles entre EC2Config EC2Launch v1 et EC2Launch v2.

Fonctionnalité	EC2Config	EC2Launch v1	EC2Launch v2
Exécuter en tant que	Windows Service	PowerShell Scripts	Windows Service
Prend en charge	Système d'exploitation hérité uniquement	Windows 2016 Windows 2019 (LTSCetSAC)	Windows 2016 Windows 2019 (LTSCetSAC) Windows 2022
Fichier de configuration	XML	JSON	JSON/YAML
Définir le nom d'utilisateur de l'administrateur	Non	Non	Oui
Taille des données utilisateur	16 Ko	16 Ko	60 Ko (compressé)
Les données des utilisateurs locaux sont conservées AMI	Non	Non	Oui, configurable
Configuration de la tâche dans les données utilisateur	Non	Non	Oui
Fond d'écran configurable	Non	Non	Oui

Fonctionnalité	EC2Config	EC2Launch v1	EC2Launch v2
Personnaliser l'ordre d'exécution des tâches	Non	Non	Oui
Tâches configurables	15	9	20 au lancement
Prend en charge l'Observateur d'événements Windows	Oui	Non	Oui
Nombre de types d'événements de l'Observateur d'événements	2	0	30

> **Note**
>
> EC2Configla documentation est fournie à titre de référence historique uniquement. Les versions du système d'exploitation sur lesquelles il s'exécute ne sont plus prises en charge par Microsoft. Nous vous recommandons vivement de passer au dernier service de lancement.

Configurer le DNS suffixe pour les agents de lancement EC2 Windows

Avec les agents de EC2 lancement Amazon, vous pouvez configurer une liste de DNS suffixes utilisés par les instances Windows pour la résolution des noms de domaine. Les agents de lancement remplacent les paramètres Windows standard de la clé de `System\CurrentControlSet\Services\Tcpip\Parameters\SearchList` registre en ajoutant les valeurs suivantes à la liste de recherche de DNS suffixes :

- Le domaine de l'instance
- Les suffixes résultant de la dévolution du domaine d'instance
- Domaine NV

- Les domaines spécifiés par chaque carte d'interface réseau

Tous les agents de lancement prennent en charge la configuration des DNS suffixes. Pour plus d'informations, consultez la version de votre agent de lancement spécifique :

- Pour plus d'informations sur la `setDnsSuffix` tâche et sur la façon de configurer les DNS suffixes dans la EC2Launch version 2, consultez. setDnsSuffix
- Pour plus d'informations sur la configuration de la liste de DNS suffixes et sur la façon d'activer ou de désactiver le transfert pour la version EC2Launch 1, consultez. Configurer l'agent EC2Launch v1 sur votre instance Windows
- Pour plus d'informations sur la configuration des listes de DNS suffixes et sur la manière d'activer ou de désactiver le transfert pourEC2Config, consultez. EC2Configfichiers de paramètres

Dévolution des noms de domaine

La dévolution des noms de domaine est un comportement Active Directory qui permet aux ordinateurs d'un domaine enfant d'accéder aux ressources du domaine parent sans utiliser de nom de domaine complet. Par défaut, la dévolution des noms de domaine se poursuit jusqu'à ce qu'il ne reste que deux nœuds dans la progression des noms de domaine.

Les agents de lancement effectuent la dévolution du nom de domaine si l'instance est connectée à un domaine et ajoutent les résultats à la liste de recherche de DNS suffixes conservée dans la clé de **`System\CurrentControlSet\Services\Tcpip\Parameters\SearchList`**registre. Les agents utilisent les paramètres des clés de registre suivantes pour déterminer le comportement de dévolution.

- **`System\CurrentControlSet\Services\Tcpip\Parameters\UseDomainNameDevolution`**
  - Lorsqu'il n'est pas défini, désactive la dévolution
  - Lorsqu'il est défini sur`1`, active la dévolution (par défaut)
  - Lorsque ce paramètre est défini sur`0`, désactive la dévolution
- **`System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel`**
  - Lorsqu'il n'est pas défini, utilisez le niveau de 2 (par défaut)
  - Lorsque le paramètre est réglé sur 3 ou supérieur, utilisez la valeur pour définir le niveau

Lorsque vous désactivez la dévolution ou que vous modifiez vos paramètres de dévolution à un niveau supérieur, la clé de `System\CurrentControlSet\Services\Tcpip\Parameters\SearchList` registre contient toujours les suffixes ajoutés précédemment. Ils ne sont pas automatiquement supprimés. Vous pouvez mettre à jour la liste manuellement ou effacer la liste et laisser votre agent suivre le processus de configuration de la nouvelle liste.

> **Note**
>
> Pour effacer la liste des DNS suffixes du registre, vous pouvez exécuter la commande suivante.
>
> ```
> PS C:\> Invoke-CimMethod -ClassName Win32_NetworkAdapterConfiguration -
> MethodName "SetDNSSuffixSearchOrder" -Arguments @{ DNSDomainSuffixSearchOrder =
>  $null } | Out-Null
> ```

Exemples de dévolution

Les exemples suivants montrent la progression des noms de domaine tout au long du processus de dévolution.

`corp.example.com`

- Procède à `example.com`

`locale.region.corp.example.com`

1. Procède à `region.corp.example.com`
2. Procède à `corp.example.com`
3. Procède à `example.com`

`locale.region.corp.example.com`avec un réglage de `DomainNameDevolutionLevel=3`

1. Procède à `region.corp.example.com`
2. Progresse vers`corp.example.com`. La progression s'arrête là, en raison du réglage du niveau.

Abonnez-vous aux notifications de l'agent de lancement EC2 Windows

Amazon SNS peut vous avertir lorsque de nouvelles versions des agents de EC2 lancement sont publiées. Pour vous abonner à ces notifications, utilisez la procédure suivante.

S'abonner aux notifications EC2Config

1. Ouvrez la SNS console Amazon sur https://console.aws.amazon.com/sns/v3/home.
2. Dans la barre de navigation, changez la région en US Est (Virginie du Nord), si nécessaire. Vous devez sélectionner cette région car les SNS notifications auxquelles vous êtes abonné ont été créées dans cette région.
3. Dans le panneau de navigation, sélectionnez Abonnements.
4. Choisissez Créer un abonnement.
5. Dans la boîte de dialogue Créer un abonnement, exécutez l'une des actions suivantes :

    a. Pour Topic ARN, utilisez le nom de ressource Amazon (ARN) suivant qui correspond à l'agent pour lequel vous souhaitez recevoir des notifications :

    - EC2Launchversion 2 :

    ```
    arn:aws:sns:us-east-1:309726204594:amazon-ec2launch-v2
    ```

    - EC2Launchou EC2Config :

    ```
    arn:aws:sns:us-east-1:801119661308:ec2-windows-ec2config
    ```

    b. Pour Protocol (Protocole), choisissez `Email`.

    c. Pour Endpoint, entrez l'adresse e-mail à laquelle vous souhaitez recevoir les notifications.

    d. Choisissez Créer un abonnement.
6. Vous recevrez un e-mail vous demandant de confirmer votre abonnement. Ouvrez l'e-mail et suivez les instructions pour terminer votre abonnement.

Chaque fois qu'une nouvelle version de l'agent de lancement est publiée, nous envoyons des notifications aux abonnés. Si vous ne souhaitez plus recevoir ces notifications, exécutez la procédure suivante pour annuler votre abonnement.

Se désabonner des notifications de l'agent de lancement

1. Ouvrez la SNS console Amazon.
2. Dans le panneau de navigation, sélectionnez Abonnements.
3. Sélectionnez l'abonnement, puis sous Actions, sélectionnez Supprimer des abonnements. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Migrer vers la EC2Launch version v2 pour les instances Windows

L'outil de EC2Launch migration met à niveau l'agent de lancement installé (EC2Configet la EC2Launch version EC2Launch 1) en le désinstallant et en installant la version 2. Les configurations applicables des services de lancement précédents sont automatiquement migrées vers le nouveau service. L'outil de migration ne détecte aucune tâche planifiée liée aux scripts EC2Launch v1 ; par conséquent, il ne configure pas automatiquement ces tâches dans la EC2Launch version v2. Pour configurer ces tâches, modifiez le `agent-config.yml`fichier ou utilisez la boîte de dialogue des EC2Launch paramètres de la version 2. Par exemple, si une tâche planifiée est exécutée sur une instance`InitializeDisks.ps1`, après avoir exécuté l'outil de migration, vous devez spécifier les volumes que vous souhaitez initialiser dans la boîte de dialogue des paramètres de EC2Launch la version 2. Voir l'étape 6 de la procédure pour Modifier les paramètres à l'aide de la boîte de EC2Launch dialogue des paramètres de la version 2.

Vous pouvez télécharger l'outil de migration ou l'installer avec un SSM RunCommand document.

Vous pouvez télécharger l'outil à partir des emplacements suivants :

> **Note**
>
> Le lien vers l'outil de migration 32 bits sera obsolète. Nous vous recommandons d'utiliser le lien 64 bits pour migrer vers la EC2Launch version v2. Si vous avez besoin d'un agent de lancement 32 bits, utilisez EC2Config.

- 64 bits — https://s3.amazonaws.com/amazon-ec2launch-v2-utils/MigrationTool/windows/amd64/latest/ .zip EC2LaunchMigrationTool
- 32 bits — https://s3.amazonaws.com/amazon-ec2launch-v2-utils/ MigrationTool /windows/386/latest/ .zip EC2LaunchMigrationTool

> **Note**
>
> Vous devez exécuter l'outil de migration EC2Launch v2 en tant qu'administrateur. EC2LaunchLa v2 est installée en tant que service après l'exécution de l'outil de migration. Il ne s'exécute pas immédiatement. Par défaut, il s'exécute au démarrage de l'instance et si une instance est arrêtée puis démarrée ultérieurement ou redémarrée.

Utilisez le `AWSEC2Launch-RunMigration`SSMdocument pour migrer vers la dernière version EC2Launch v2 avec SSM Run Command. Le document ne nécessite aucun paramètre. Pour plus d'informations sur l'utilisation de SSM Run Command, consultez AWS Systems Manager Run Command.

L'outil de migration applique les configurations suivantes de la EC2Launch version 2 EC2Config à la version 2.

- S'il `Ec2DynamicBootVolumeSize` est défini sur`false`, supprime le `boot` stade EC2Launch v2
- S'il `Ec2SetPassword` est défini sur`Enabled`, définit le type de mot de passe EC2Launch v2 sur `random`
- S'il `Ec2SetPassword` est défini sur`Disabled`, définit le type de mot de passe EC2Launch v2 sur `donothing`
- S'il `SetDnsSuffixList` est défini sur`false`, supprime la `setDnsSuffix` tâche EC2Launch v2
- S'il `EC2SetComputerName` est défini sur true, ajoute la `setHostName` tâche EC2Launch v2 à la `yaml` configuration

L'outil de migration applique les configurations suivantes de la EC2Launch v1 à la EC2Launch v2.

- S'il `ExtendBootVolumeSize` est défini sur`false`, supprime le `boot` stade EC2Launch v2
- S'il `AdminPasswordType` est défini sur`Random`, définit le type de mot de passe EC2Launch v2 sur `random`
- Si la valeur `AdminPasswordType` est définie sur`Specify`, définit le type EC2Launch v2password `static` et les données du mot de passe sur le mot de passe spécifié dans `AdminPassword`
- S'il `SetWallpaper` est défini sur`false`, supprime la `setWallpaper` tâche EC2Launch v2
- S'il `AddDnsSuffixList` est défini sur`false`, supprime la `setDnsSuffix` tâche EC2Launch v2
- S'il `SetComputerName` est défini sur`true`, ajoute une `setHostName` tâche EC2Launch v2

Administration des services Windows pour la EC2Launch version 2 et les EC2Config agents

Si vous vous êtes connecté à votre instance en tant qu'utilisateur disposant de droits d'administration, vous pouvez gérer la EC2Launch version 2 et EC2Config lancer les agents comme vous le feriez pour n'importe quel autre service Windows. EC2Launchv1 est un ensemble de PowerShell scripts gérés par défaut via une tâche planifiée. Cette section couvre l'administration des services pour les EC2Launch versions 2 etEC2Config.

Pour appliquer les paramètres mis à jour à votre instance, vous pouvez arrêter et redémarrer l'agent EC2Launch v2 ou l'agent de lancement de EC2Config service depuis l'interface Microsoft Management Console (MMC) pour Services. De même, lorsque vous installez une nouvelle version de l'agent de lancement, vous devez d'abord arrêter l'agent, puis le redémarrer une fois l'installation terminée.

> **Note**
>
> Vous devez ouvrir l'interface MMC des services en tant qu'administrateur pour sélectionner ces actions. Pour ce faire, vous pouvez sélectionner Exécuter en tant qu'administrateur dans le menu contextuel. Sinon, pour ouvrir l'interface à l'aide de votre clavier, procédez comme suit :
>
> 1. À l'aide des `Tab` touches ou des flèches, sélectionnez l'élément de menu Services dans le menu Outils d'administration.
> 2. Utilisez la combinaison de touches suivante pour ouvrir en tant qu'administrateur : `Ctrl + Shift +Enter`.

Les procédures suivantes répertorient les étapes permettant d'arrêter et de démarrer l'agent de lancement sur votre instance.

Arrêtez l'agent de lancement

1. Lancez et connectez-vous à votre instance Windows.
2. Sélectionnez Outils d'administration dans le menu Démarrer de Windows.
3. Ouvrez la console Services en tant qu'administrateur, comme décrit au début de cette section.

4. Dans la liste des services, sélectionnez l'agent qui s'exécute sur votre instance (EC2Launchou EC2Config), puis choisissez Stop dans le menu Action. Vous pouvez également utiliser le menu contextuel pour arrêter l'agent.

Redémarrer l'agent de lancement

1. Lancez et connectez-vous à votre instance Windows.
2. Sélectionnez Outils d'administration dans le menu Démarrer de Windows.
3. Ouvrez la console Services en tant qu'administrateur, comme décrit au début de cette section.
4. Dans la liste des services, sélectionnez l'agent qui s'exécute sur votre instance (EC2Launchou EC2Config), puis choisissez Démarrer ou Redémarrer dans le menu Action. Vous pouvez également utiliser le menu contextuel pour redémarrer l'agent.

Si vous n'avez pas besoin de mettre à jour les paramètres de configuration, de créer les vôtres AMI ou d'utiliser AWS Systems Manager, vous pouvez supprimer ou désinstaller l'agent de lancement.

Suppression

La suppression d'un service entraîne celle de sa sous-clé du registre.

Désinstaller

La désinstallation d'un service entraîne la suppression des fichiers, de la sous-clé du registre et de tous les raccourcis vers le service.

Supprimer l'agent de lancement

1. Lancez et connectez-vous à votre instance Windows.
2. Ouvrez une fenêtre d'invite de commandes Windows.
3. Exécutez l'une des commandes suivantes pour supprimer l'agent de lancement.
   - Exécutez la commande suivante pour supprimer le EC2Launch ou EC2Launch v2 :

     ```
     sc delete ec2launch
     ```

   - Exécutez la commande suivante pour supprimer le EC2Config service :

     ```
     sc delete ec2config
     ```

Désinstallez l'agent de lancement

1. Lancez et connectez-vous à votre instance Windows.
2. Choisissez Système Windows, puis Panneau de configuration dans le menu Démarrer de Windows.
3. Choisissez Programmes et fonctionnalités pour ouvrir la liste des programmes installés sur votre instance.
4. Sélectionnez votre agent de lancement dans la liste (Amazon EC2Launch ou EC2ConfigService), puis choisissez Désinstaller dans le menu Fichier. Vous pouvez également utiliser le menu contextuel.

> **Note**
>
> Vous pouvez voir quelle version de l'agent de lancement est installée dans la colonne Version.

Utiliser l'agent EC2Launch v2 pour effectuer des tâches lors du lancement de l'instance EC2 Windows

Toutes les instances d'Amazon prises en charge EC2 qui sont lancées à partir de AWS Windows Server 2022 AMIs incluent l'agent de lancement EC2Launch v2 (`EC2Launch.exe`) par défaut. Nous fournissons également Windows Server 2016 et 2019 AMIs avec la EC2Launch version v2 installée comme agent de lancement par défaut. Ils AMIs sont fournis en plus des versions Windows Server 2016 et 2019 AMIs qui incluent la version EC2Launch 1. Vous pouvez rechercher des Windows AMIs qui incluent la EC2Launch v2 par défaut en saisissant le préfixe suivant dans votre recherche AMIssur la page de la EC2 console Amazon :`EC2LaunchV2-Windows_Server-*`.

Pour comparer les fonctionnalités des versions de l'agent de lancement, voirComparez les agents EC2 de lancement Amazon.

EC2LaunchLa v2 exécute des tâches lors du démarrage de l'instance et s'exécute si une instance est arrêtée puis redémarrée ultérieurement, ou redémarrée. EC2LaunchLa v2 peut également effectuer des tâches à la demande. Certaines de ces tâches sont automatiquement activées, alors que d'autres doivent être activées manuellement. Le service EC2Launch v2 prend en charge toutes EC2Config les EC2Launch fonctionnalités.

Ce service utilise un fichier de configuration pour contrôler son fonctionnement. Vous pouvez mettre à jour le fichier de configuration à l'aide d'un outil graphique ou en le modifiant directement en tant que fichier .yml unique (`agent-config.yml`). Les binaires de service se trouvent dans le répertoire `%ProgramFiles%\Amazon\EC2Launch`.

EC2LaunchLa v2 publie des journaux d'événements Windows pour vous aider à résoudre les erreurs et à définir des déclencheurs. Pour de plus amples informations, veuillez consulter Journaux d'événements Windows.

L'agent EC2Launch v2 prend en charge les versions suivantes du système d'exploitation Windows Server :

Versions d'OS prises en charge

- Windows Server 2022
- Windows Server 2019 (canal de maintenance à long terme et canal semestriel)
- Windows Server 2016

EC2Launchconcepts de la version 2

Les concepts suivants sont utiles à comprendre lorsque l'on envisage la EC2Launch version 2.

Tâche

Vous pouvez invoquer une tâche pour effectuer une action sur une instance. Vous pouvez configurer les tâches dans le fichier `agent-config.yml` ou via les données utilisateur. Pour une liste des tâches disponibles pour la EC2Launch version 2, consultez la section tâches de la EC2Launch version 2. Pour le schéma de configuration des tâches et les détails, consultez EC2Launchconfiguration des tâches v2.

Étape

Une étape est un regroupement logique de tâches exécutées par l'agent EC2Launch v2. Certaines tâches ne peuvent s'exécuter qu'à un stade spécifique. D'autres peuvent fonctionner en plusieurs étapes. Lors de l'utilisation de `agent-config.yml`, vous devez spécifier une liste d'étapes et une liste de tâches à exécuter au sein de chaque étape.

Le service exécute les étapes dans l'ordre suivant :

Étape 1 : Démarrage

Étape 2 : Réseau

Étape 3 : PreReady

Windows est prêt

Une fois l' PreReady étape terminée, le service envoie le `Windows is ready` message à la EC2 console Amazon.

Étape 4 : PostReady

Les données utilisateur sont exécutées pendant la PostReadyphase. Certaines versions de script s'exécutent avant le PostReadystade du `agent-config.yml` fichier, tandis que d'autres s'exécutent après, comme suit :

Avant `agent-config.yml`

- YAMLversion 1.1 des données utilisateur
- XMLdonnées utilisateur

Après `agent-config.yml`

- YAMLdonnées utilisateur version 1.0 (ancienne version pour la rétrocompatibilité)

Pour des exemples d'étapes et de tâches, consultez Exemple : `agent-config.yml`.

Lorsque vous utilisez des données utilisateur, vous devez spécifier une liste de tâches que l'agent de lancement doit exécuter. L'étape est implicite. Pour des exemples de tâches, consultez Exemple : données utilisateur.

EC2LaunchLa v2 exécute la liste des tâches dans l'ordre que vous spécifiez dans `agent-config.yml` et dans les données utilisateur. Les étapes s'exécutent de manière séquentielle. L'étape suivante commence lorsque l'étape précédente est terminée. Les tâches sont également exécutées de manière séquentielle.

Fréquence

La fréquence des tâches détermine le moment où les tâches doivent être exécutées, en fonction du contexte de démarrage. La plupart des tâches n'ont qu'une seule fréquence autorisée. Vous pouvez spécifier une fréquence pour les tâches `executeScript`.

Vous verrez les fréquences suivantes dans la EC2Launchconfiguration des tâches v2.

- Une fois — La tâche s'exécute une fois, lors du AMI premier démarrage (fin de Sysprep).
- Toujours : la tâche s'exécute chaque fois que l'agent de lancement s'exécute. L'agent de lancement s'exécute lorsque :
  - une instance démarre ou redémarre
  - le EC2Launch service fonctionne
  - `EC2Launch.exe run` est invoqué

agent-config

`agent-config`est un fichier qui se trouve dans le dossier de configuration de la EC2Launch v2. Il inclut la configuration du démarrage PreReady, du réseau et des PostReady stages. Ce fichier est utilisé pour spécifier la configuration de l'instance pour les AMI tâches qui doivent être exécutées lors du premier démarrage ou ultérieurement.

Par défaut, l'installation EC2Launch v2 installe un `agent-config` fichier qui inclut les configurations recommandées utilisées dans Amazon Windows AMIs standard. Vous pouvez mettre à jour le fichier de configuration afin de modifier l'expérience de démarrage par défaut AMI spécifiée par la EC2Launch v2.

Données utilisateur

Les données utilisateur sont des données configurables lorsque vous lancez une instance. Vous pouvez mettre à jour les données utilisateur pour modifier de manière dynamique le mode de configuration personnalisé AMIs ou de démarrage rapideAMIs. EC2LaunchLa v2 prend en charge une longueur de saisie de données utilisateur de 60 kB. Les données utilisateur incluent uniquement l' UserData étape et s'exécutent donc après le `agent-config` fichier. Vous pouvez saisir des données utilisateur lorsque vous lancez une instance à l'aide de l'assistant de lancement d'instance, ou vous pouvez modifier les données utilisateur depuis la EC2 console. Pour plus d'informations sur l'utilisation des données d'utlisateur, consultez Comment Amazon EC2 gère les données utilisateur pour les instances Windows.

EC2Launchvue d'ensemble des tâches v2

EC2LaunchLa v2 peut effectuer les tâches suivantes à chaque démarrage :

- Configurez un nouveau fond d'écran personnalisé qui rend des informations sur l'instance.
- Définissez les attributs du compte d'administrateur créé sur la machine locale.

- Ajoutez des DNS suffixes à la liste des suffixes de recherche. Seuls les suffixes qui n'existent pas déjà sont ajoutés à la liste.
- Définissez les lettres de lecteur pour les volumes supplémentaires et étendez-les pour utiliser l'espace disponible.
- Écrivez les fichiers de la configuration sur le disque.
- Exécutez les scripts spécifiés dans le fichier de configuration EC2Launch v2 ou à partir de`user-data`. Les scripts de `user-data` peuvent être en texte brut ou compressés et fournis au format base64.
- Exécutez un programme avec des arguments donnés.
- Définir le nom d'ordinateur
- Envoyez les informations de l'instance à la EC2 console Amazon.
- Envoyez l'empreinte RDP numérique du certificat à la console AmazonEC2.
- Etendez de manière dynamique la partition du système d'exploitation pour inclure l'espace non partitionné.
- Exécutez des données utilisateur. Pour plus d'informations sur la spécification de données utilisateur, consultez EC2Launchconfiguration des tâches v2.
- Définissez des routes non statiques permanentes pour atteindre le service de métadonnées et les serveurs AWS KMS .
- Définissez les partitions autres que le démarrage sur `mbr` ou`gpt`.
- Démarrez le service Systems Manager après Sysprep.
- Optimisez ENA les paramètres.
- Activez Ouvrir SSH pour les versions ultérieures de Windows.
- Activez les trames Jumbo.
- Configurez Sysprep pour qu'il s'exécute avec la version v2. EC2Launch
- Publiez les journaux des événements Windows.

EC2Launchstructure du répertoire v2

EC2LaunchLa v2 doit être installée dans les répertoires suivants :

- Binaires de service : `%ProgramFiles%\Amazon\EC2Launch`
- Données de service (paramètres, fichiers journaux et fichiers d'état) : `%ProgramData%\Amazon\EC2Launch`

> **Note**
>
> Par défaut, Windows masque les fichiers et les dossiers qui se trouvent sous `C:\ProgramData`. Pour afficher les EC2Launch répertoires et les fichiers de la version 2, vous devez soit entrer le chemin dans l'Explorateur Windows, soit modifier les propriétés du dossier pour afficher les fichiers et dossiers cachés.

Le répertoire `%ProgramFiles%\Amazon\EC2Launch` contient des binaires et des bibliothèques de support. Il comprend les sous-répertoires suivants :

- `settings`
  - `EC2LaunchSettingsUI.exe` — Interface utilisateur pour modifier le fichier `agent-config.yml`
  - `YamlDotNet.dll`— DLL pour prendre en charge certaines opérations dans l'interface utilisateur
- `tools`
  - `ebsnvme-id.exe`— outil pour examiner les métadonnées des EBS volumes de l'instance
  - `AWSAcpiSpcrReader.exe`— outil pour déterminer le COM port correct à utiliser
  - `EC2LaunchEventMessage.dll`— DLL pour prendre en charge la journalisation des événements Windows pourEC2Launch.
- `service`
  - `EC2LaunchService.exe` — Exécutable de service Windows qui est lancé lorsque l'agent de lancement s'exécute en tant que service.
- `EC2Launch.exe`— EC2Launch exécutable principal
- `EC2LaunchAgentAttribution.txt`— attribution du code utilisé dans EC2 Launch

Le répertoire `%ProgramData%\Amazon\EC2Launch` contient les sous-répertoires suivants. Toutes les données produites par le service, y compris les journaux, la configuration et l'état, sont stockées dans ce répertoire.

- `config`— Configuration

  Le fichier de configuration du service est stocké dans ce répertoire sous la forme de `agent-config.yml`. Ce fichier peut être mis à jour pour modifier, ajouter ou supprimer des tâches

exécutées par le service par défaut. L'autorisation de créer des fichiers dans ce répertoire est limitée au compte administrateur pour empêcher l'escalade des privilèges.

- `log`— Journaux d'instance

  Les journaux relatifs au service (`agent.log`), à la console (`console.log`), aux performances (`bench.log`), aux erreurs (`err.log`) et à la télémétrie () `telemetry.log` sont stockés dans ce répertoire. Les fichiers journaux sont ajoutés lors des exécutions ultérieures du service.

- `state`— Données sur l'état du service

  L'état utilisé par le service pour déterminer les tâches à exécuter est stocké ici. Il existe un fichier `.run-once` qui indique si le service a déjà été exécuté après Sysprep (donc les tâches avec une fréquence d'une fois seront ignorées lors de la prochaine exécution). Ce sous-répertoire inclut un `state.json` et `previous-state.json` pour suivre l'état de chaque tâche.

- `sysprep`— Sysprep

  Ce répertoire contient les fichiers utilisés pour déterminer les opérations à effectuer par Sysprep lorsqu'il crée un Windows personnalisé AMI qui peut être réutilisé.

- `wallpaper`— Papier peint

  Ces images de fond d'écran sont stockées dans ce répertoire.

Télémétrie

La télémétrie est une information supplémentaire qui permet de mieux AWS comprendre vos besoins, de diagnostiquer les problèmes et de fournir des fonctionnalités pour améliorer votre expérience avec. services AWS

EC2LaunchLes versions v2 `2.0.592` et ultérieures collectent des données télémétriques, telles que les métriques d'utilisation et les erreurs. Ces données sont collectées à partir de l'EC2instance Amazon sur laquelle s'exécute la EC2Launch v2. Cela inclut tous les appareils Windows AMIs détenus par AWS.

Les types de télémétrie suivants sont collectés par EC2Launch la v2 :

- Usage information (Informations d'utilisation) : commandes de l'agent, méthode d'installation et fréquence d'exécution planifiée.
- Erreurs et informations de diagnostic : codes d'erreur d'installation de l'agent, codes d'erreur d'exécution et piles d'appels d'erreur.

Exemples de données collectées :

```
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsUserDataScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandCode=1
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandErrorCode=5
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallCode=2
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallErrorCode=0
```

La télémétrie est activée par défaut. Vous pouvez désactiver la collecte de données de télémétrie à tout moment. Si la télémétrie est activée, la EC2Launch version 2 envoie des données de télémétrie sans notification supplémentaire au client.

Visibilité de la télémétrie

Lorsque la télémétrie est activée, elle apparaît dans la sortie de EC2 la console Amazon comme suit.

```
2021/07/15 21:44:12Z: Telemetry: <Data>
```

Désactiver la télémétrie sur une instance

Pour désactiver la télémétrie pour une seule instance, vous pouvez définir une variable d'environnement système ou utiliser le MSI pour modifier l'installation.

Pour désactiver la télémétrie en paramétrant une variable d'environnement système, exécutez la commande suivante en tant qu'administrateur.

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Pour désactiver la télémétrie à l'aide duMSI, exécutez la commande suivante après avoir téléchargé le. MSI

```
msiexec /i ".\AmazonEC2Launch.msi" Remove="Telemetry" /q
```

Autres sujets pour la EC2Launch version 2

- Installez la dernière version de EC2Launch v2
- Configurer les paramètres EC2Launch v2 pour les instances Windows
- Définitions de tâches pour les tâches de EC2Launch démarrage de la version 2
- Résoudre les problèmes liés à l'agent EC2Launch v2

- EC2Launchhistorique des versions de la v2

Installez la dernière version de EC2Launch v2

Vous pouvez utiliser l'une des méthodes suivantes pour installer l'agent EC2Launch v2 sur votre EC2 instance :

- Téléchargez l'agent depuis Amazon S3 et installez-le avec Windows PowerShell. Pour le téléchargementURLs, voirEC2Launchtéléchargements de la version 2 sur Amazon S3.
- Installation avec le SSM distributeur.
- Installez à partir d'un composant EC2 Image Builder lorsque vous créez une image personnalisée.
- Lancez votre instance à partir d'une instance sur AMI laquelle la EC2Launch version v2 est préinstallée.

> **Warning**
>
> Amazon EC2Launch .msi désinstalle les versions précédentes des services de EC2 lancement, telles que EC2Launch (v1) et. EC2Config

Pour les étapes d'installation, sélectionnez l'onglet correspondant à votre méthode préférée.

Windows PowerShell

Pour installer la dernière version de l'agent EC2Launch v2 sous Windows PowerShell, procédez comme suit.

1. Créez votre répertoire local.

```
New-Item -Path "$env:USERPROFILE\Desktop\EC2Launchv2" -ItemType Directory
```

2. Définissez l'emplacement URL de votre téléchargement. Exécutez la commande suivante avec l'Amazon S3 URL que vous allez utiliser. Pour le téléchargementURLs, voir EC2Launchtéléchargements de la version 2 sur Amazon S3

```
$Url = "Amazon S3 URL/AmazonEC2Launch.msi"
```

3. Utilisation de la commande combinée suivante pour télécharger et installer l'agent

```
$DownloadFile = "$env:USERPROFILE\Desktop\EC2Launchv2\" + $(Split-Path -Path
 $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadFile
msiexec /i "$DownloadFile"
```

> **Note**
>
> Si un message d'erreur s'affiche lors du téléchargement du fichier et que vous utilisez Windows Server 2016 ou une version antérieure, il est possible que la version TLS 1.2 doive être activée sur votre PowerShell terminal. Vous pouvez activer la TLS version 1.2 pour la PowerShell session en cours à l'aide de la commande suivante, puis réessayer :
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

4. Pour vérifier l'installation, vérifiez que le fichier msi existe dans le répertoire EC2Launch v2 de votre instance (`C:\ProgramData\Amazon\EC2Launch`).

AWS Systems Manager Distributor

Pour configurer les mises à jour automatiques pour la EC2Launch version 2 avec AWS Systems Manager Quick Setup, voirInstallation et mise à jour automatiques avec le programme de configuration rapide du distributeur.

Vous pouvez également effectuer une installation unique du `AWSEC2Launch-Agent` package depuis le AWS Systems Manager distributeur. Pour obtenir des instructions sur l'installation d'un package à partir d'un distributeur Systems Manager, veuillez consulter la rubrique Installer ou mettre à jour des packages dans le Guide de l'utilisateur AWS Systems Manager .

EC2 Image Builder component

Vous pouvez installer le `ec2launch-v2-windows` composant lorsque vous créez une image personnalisée avec EC2 Image Builder. Pour obtenir des instructions sur la création d'une image personnalisée avec EC2 Image Builder, voir Création d'un pipeline d'images à l'aide de l'assistant de console EC2 Image Builder dans le guide de l'utilisateur d'EC2Image Builder.

AMI

EC2LaunchLa v2 est préinstallée par défaut sur les systèmes Windows Server 2022 suivants et UEFI AMIs :

- Windows_Server-2022-English-Full-Base
- Windows_Server-2022-English-Core-Base
- Windows Server 2022 AMIs avec toutes les autres langues
- Windows Server 2022 AMIs avec SQL installation
- Windows_Server-2_English-Core- _Optimisé EKS

EC2LaunchLa v2 est également préinstallée sur le serveur AMIs Windows suivant. Vous pouvez les trouver sur AMIs la EC2 console Amazon ou en utilisant le préfixe de recherche suivant : `EC2LaunchV2-` dans le AWS CLI.

- EC2LaunchV2-Windows_Server-2019-Anglais-Core-Base
- EC2LaunchV2-Windows_Server-2019-Anglais-Base complète
- EC2LaunchV2-Windows_Server-2016-Anglais-Core-Base
- EC2LaunchV2-Windows_Server-2016-Anglais-Base complète
- EC2LaunchV2-Windows_Server-2012_R2_ -Anglais-Base complète RTM
- EC2LaunchV2-Windows_Server-2012_ -Anglais-Base complète RTM

Installation et mise à jour automatiques de la EC2Launch v2 avec le programme de configuration rapide du AWS Systems Manager distributeur

Avec AWS Systems Manager Distributor Quick Setup, vous pouvez configurer des mises à jour automatiques pour la EC2Launch version 2. Le processus suivant permet de configurer une association Systems Manager sur votre instance qui met automatiquement à jour l'agent EC2Launch v2 à une fréquence que vous spécifiez. L'association créée par le programme de configuration rapide du distributeur peut inclure des instances au sein d'une région Compte AWS et, ou des instances au sein d'une AWS organisation. Pour plus d'informations sur la configuration d'une organisation, voir Tutoriel : Création et configuration d'une organisation dans le Guide de AWS Organizations l'utilisateur.

Avant de commencer, assurez-vous que vos instances répondent à tous les prérequis.

Prérequis

Pour configurer les mises à jour automatiques avec Distributor Quick Setup, vos instances doivent répondre aux conditions préalables suivantes.

- Vous avez au moins une instance en cours d'exécution qui prend en charge la EC2Launch version 2. Consultez les systèmes d'exploitation pris en charge pourEC2Launch v2.
- Vous avez effectué les tâches de configuration de Systems Manager sur vos instances. Pour plus d'informations, consultez la section Configuration de Systems Manager dans le guide de AWS Systems Manager l'utilisateur.
- EC2Launchv2 doit être le seul agent de lancement installé sur votre instance. Si plusieurs agents de lancement sont installés, la configuration de configuration rapide de votre distributeur échouera. Avant de configurer la EC2Launch v2 à l'aide d'un distributeur Quick Setup, désinstallez EC2Config ou lancez les agents EC2Launch v1, s'ils existent.

Configurer la configuration rapide du distributeur pour la EC2Launch version 2

Pour créer une configuration pour la EC2Launch version 2 à l'aide de la configuration rapide du distributeur, utilisez les paramètres suivants lorsque vous terminez les étapes du déploiement du package du distributeur :

- Packages logiciels : agent Amazon EC2Launch v2.
- Fréquence de mise à jour : sélectionnez une fréquence dans la liste.
- Cibles : choisissez parmi les options de déploiement disponibles.

Pour vérifier l'état de votre configuration, accédez à l'onglet Configurations de configuration rapide de Systems Manager dans le AWS Management Console.

1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.
2. Dans le panneau de navigation, choisissez Configuration rapide.
3. Dans l'onglet Configurations, sélectionnez la ligne associée à la configuration que vous avez créée. L'onglet Configurations répertorie vos configurations et inclut un résumé des principaux détails, tels que la région, le statut du déploiement et le statut de l'association.

> **Note**
>
> Le nom de l'association pour chaque configuration de distributeur EC2Launch v2 commence par le préfixe suivant :`AWS-QuickSetup-Distributor-EC2Launch-Agent-`.

4. Pour afficher les détails, sélectionnez la configuration et choisissez Afficher les détails.

Pour plus d'informations et pour connaître les étapes de résolution des problèmes, consultez la section Résolution des problèmes liés à la configuration rapide dans le Guide de AWS Systems Manager l'utilisateur.

EC2Launchtéléchargements de la version 2 sur Amazon S3

Pour installer la dernière version de EC2Launch v2, téléchargez le programme d'installation depuis l'un des emplacements suivants :

> **Note**
>
> Le lien d'installation 32 bits sera obsolète. Nous vous recommandons d'utiliser le lien d'installation 64 bits pour installer la EC2Launch version 2. Si vous avez besoin d'un agent de lancement 32 bits, utilisez EC2Config.

- 64 bits — https://s3.amazonaws.com/amazon-ec2launch-v2/EC2LaunchWindows/AMD64/latest/Amazon .msi
- 32 bits — https://s3.amazonaws.com/amazon-ec2launch-v2/EC2LaunchWindows/386/latest/Amazon .msi

Configuration des options d'installation

Lorsque vous installez ou mettez à niveau la version EC2Launch v2, vous pouvez configurer les options d'installation à l'aide de la boîte de dialogue d'installation de la EC2Launch version 2 ou à l'aide de la msiexec commande dans un interpréteur de ligne de commande.

La première fois que le programme d'EC2Launchinstallation de la version 2 s'exécute sur une instance, il initialise les paramètres de l'agent de lancement sur votre instance comme suit :

- Il crée le chemin local et y écrit le fichier de l'agent de lancement. C'est ce que l'on appelle parfois l'installation propre.
- Il crée la variable d'environnement `EC2LAUNCH_TELEMETRY` si elle n'existe pas déjà, et la définit en fonction de votre configuration.

Pour les détails de configuration, sélectionnez l'onglet correspondant à la méthode de configuration que vous allez utiliser.

Amazon EC2Launch Setup dialog

Lorsque vous installez ou mettez à niveau la version EC2Launch v2, vous pouvez configurer les options d'installation suivantes via la boîte de dialogue d'installation de la EC2Launch v2.

Options d'installation de base

Envoyer des données de télémétrie

Lorsque vous incluez cette fonctionnalité dans la boîte de dialogue de configuration, le programme d'installation définit la variable d'environnement `EC2LAUNCH_TELEMETRY` sur une valeur de `1`. Si vous désactivez Envoyer des données de télémétrie, le programme d'installation définit la valeur de la variable d'environnement sur `0`.

Lorsque l'agent EC2Launch v2 s'exécute, il lit la variable d'`EC2LAUNCH_TELEMETRY`environnement pour déterminer s'il convient de télécharger des données de télémétrie. Si la valeur est égale à `1`, il charge les données. Dans le cas contraire, il ne les charge pas.

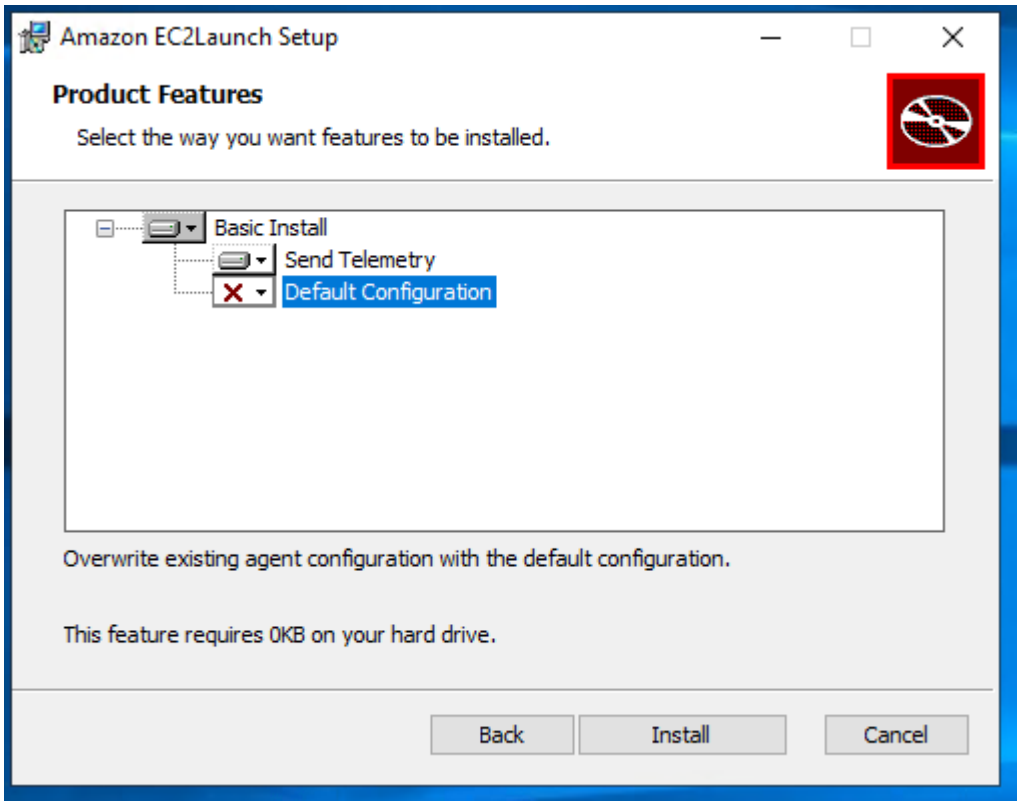
Configuration par défaut

La configuration par défaut pour la EC2Launch v2 consiste à remplacer l'agent de lancement local s'il existe déjà. La première fois que vous exécutez une installation sur une instance, la configuration par défaut effectue une installation propre. Si vous désactivez la configuration par défaut lors de l'installation initiale, l'installation échoue.

Si vous réexécutez l'installation sur l'instance, vous pouvez désactiver la configuration par défaut afin d'effectuer une mise à niveau qui ne remplace pas le fichier `%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`.

Exemple : mise à niveau de la EC2Launch v2 avec la télémétrie

L'exemple suivant montre la boîte de dialogue EC2Launch de configuration de la version 2 configurée pour mettre à niveau l'installation actuelle et activer la télémétrie. Cette configuration effectue une installation sans remplacer le fichier de configuration de l'agent et définit la valeur de la variable d'environnement `EC2LAUNCH_TELEMETRY` sur 1.



Command line

Lorsque vous installez ou mettez à niveau la version EC2Launch v2, vous pouvez configurer les options d'installation suivantes à l'aide de la msiexec commande dans un shell de ligne de commande.

Valeurs de paramètres **`ADDLOCAL`**

De base (obligatoire)

Installez l'agent de lancement. Si cette valeur n'est pas présente dans le paramètre `ADDLOCAL`, l'installation se termine.

Propre

Lorsque vous incluez la valeur `Clean` dans le paramètre `ADDLOCAL`, le programme d'installation écrit le fichier de configuration de l'agent à l'emplacement suivant :

`%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`. Si le fichier de configuration de l'agent existe déjà, il le remplace.

Lorsque vous enlevez la valeur `Clean` du paramètre `ADDLOCAL`, le programme d'installation effectue une mise à niveau qui ne remplace pas le fichier de configuration de l'agent.

Télémétrie

Lorsque vous incluez la valeur `Telemetry` dans le paramètre `ADDLOCAL`, le programme d'installation définit la valeur de la variable d'environnement `EC2LAUNCH_TELEMETRY` sur `1`.

Lorsque vous enlevez la valeur `Telemetry` du paramètre `ADDLOCAL`, le programme d'installation définit la valeur de la variable d'environnement sur `0`.

Lorsque l'agent EC2Launch v2 s'exécute, il lit la variable d'`EC2LAUNCH_TELEMETRY`environnement pour déterminer s'il convient de télécharger des données de télémétrie. Si la valeur est égale à `1`, il charge les données. Dans le cas contraire, il ne les charge pas.

Exemple : installation de la EC2Launch v2 avec télémétrie

```
& msiexec /i "C:\Users\Administrator\Desktop\EC2Launchv2\AmazonEC2Launch.msi"
 ADDLOCAL="Basic,Clean,Telemetry" /q
```

Vérifiez la version EC2Launch v2

Utilisez l'une des procédures suivantes pour vérifier la version de EC2Launch v2 installée sur vos instances.

Windows PowerShell

Vérifiez la version installée de EC2Launch v2 avec Windows PowerShell, comme suit.

1. Lancez une instance depuis votre AMI ordinateur et connectez-vous à celle-ci.
2. Exécutez la commande suivante PowerShell pour vérifier la version installée de la EC2Launch v2 :

```
& "C:\Program Files\Amazon\EC2Launch\EC2Launch.exe" version
```

Windows Control Panel

Vérifiez la version installée de EC2Launch v2 dans le panneau de configuration Windows, comme suit.

1. Lancez une instance depuis votre AMI ordinateur et connectez-vous à celle-ci.
2. Ouvrez le panneau de configuration Windows, puis choisissez Programmes et fonctionnalités.
3. Recherchez `Amazon EC2Launch` dans la liste des programmes installés. Son numéro de version s'affiche dans la colonne Version.

Pour consulter les dernières mises à jour de AWS WindowsAMIs, consultez l'historique des AMI versions de Windows dans le Guide de AMIréférence AWS Windows.

Pour la dernière version de la EC2Launch v2, voirEC2Launchhistorique des versions v2.

Pour obtenir la dernière version de l'outil de migration EC2Launch v2, consultezEC2Launchhistorique des versions de l'outil de migration v2.

Vous pouvez recevoir des notifications lorsque de nouvelles versions du service EC2Launch v2 sont publiées. Pour de plus amples informations, veuillez consulter Abonnez-vous aux notifications de l'agent de lancement EC2 Windows.

Configurer les paramètres EC2Launch v2 pour les instances Windows

Cette section contient des informations sur la configuration des paramètres pour la EC2Launch version 2.

Les sujets suivants sont notamment abordés :

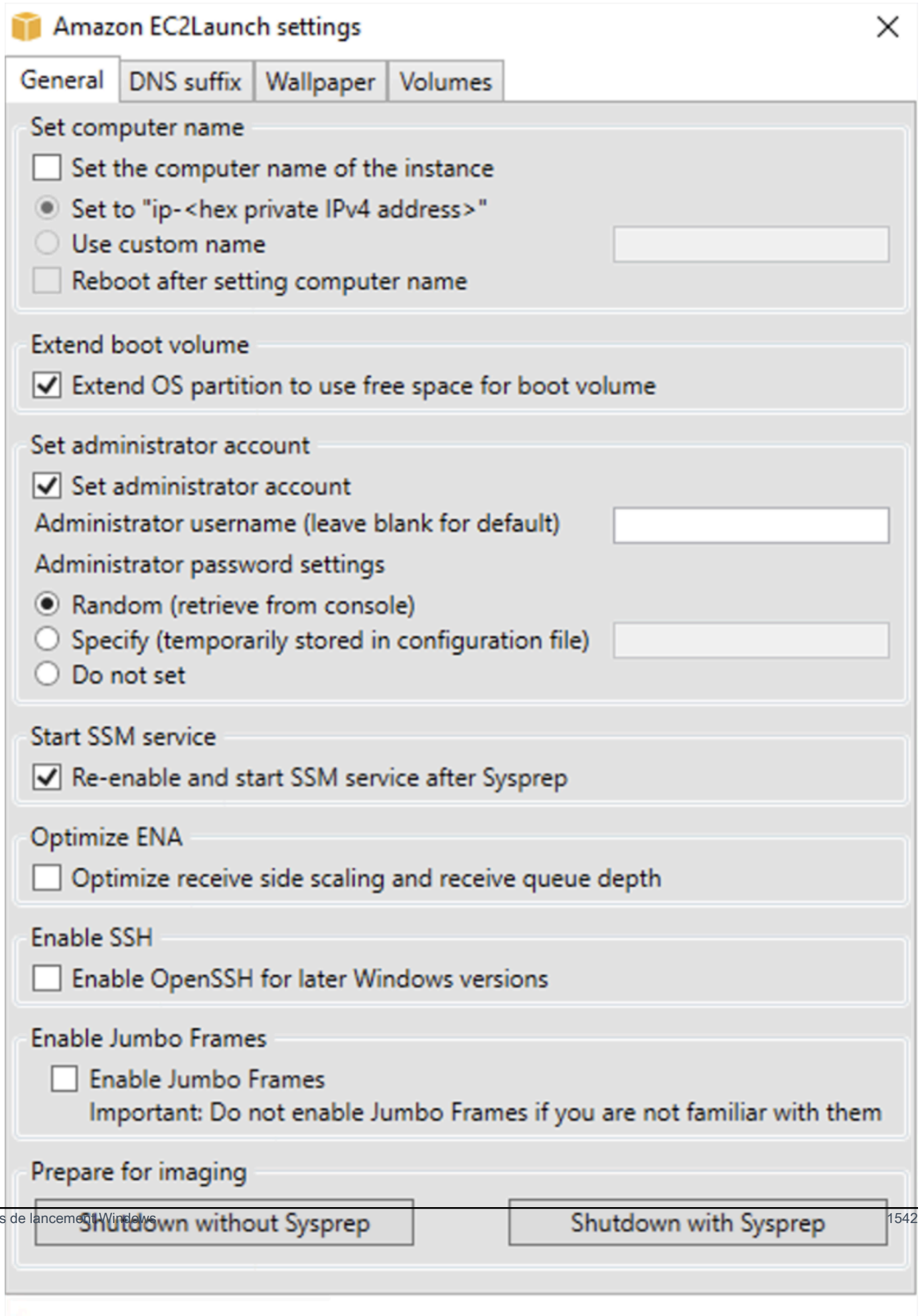
- Modifier les paramètres à l'aide de la boîte de EC2Launch dialogue des paramètres de la version 2
- Configurez la EC2Launch v2 à l'aide du CLI
- EC2Launchconfiguration des tâches v2
- EC2LaunchCodes de sortie et redémarrages de la v2
- EC2Launchv2 et Sysprep

Modifier les paramètres à l'aide de la boîte de EC2Launch dialogue des paramètres de la version 2

La procédure suivante décrit comment utiliser la boîte de dialogue EC2Launch des paramètres de la version 2 pour activer ou désactiver les paramètres.

> **Note**
>
> Si vous configurez de manière incorrecte les tâches personnalisées dans le fichier agent-config.yml et que vous essayez d'ouvrir la boîte de dialogue des EC2Launch paramètres Amazon, vous recevrez un message d'erreur. Pour un exemple de schéma, consultez Exemple : `agent-config.yml`.

1. Lancez et connectez-vous à votre instance Windows.
2. Dans le menu Démarrer, choisissez Tous les programmes, puis accédez aux EC2Launchparamètres.


Amazon EC2Launch settings
General
DNS suffix
Wallpaper
Volumes
Set computer name
Set the computer name of the instance
Set to "ip-<hex private IPv4 address>"
Use custom name
Reboot after setting computer name
Extend boot volume
Extend OS partition to use free space for boot volume
Set administrator account
Set administrator account
Administrator username (leave blank for default)
Administrator password settings
Random (retrieve from console)
Specify (temporarily stored in configuration file)
Do not set
Start SSM service
Re-enable and start SSM service after Sysprep
Optimize ENA
Optimize receive side scaling and receive queue depth
Enable SSH
Enable OpenSSH for later Windows versions
Enable Jumbo Frames
Enable Jumbo Frames
Important: Do not enable Jumbo Frames if you are not familiar with them
Prepare for imaging
Shutdown without Sysprep
Shutdown with Sysprep

3. Dans l'onglet Général de la boîte de dialogue des EC2Launchparamètres, vous pouvez activer ou désactiver les paramètres suivants.

   a. Set Computer Name (Définir le nom de l'ordinateur)

      Si ce paramètre est activé (il est désactivé par défaut), le nom d'hôte actuel est comparé au nom d'hôte souhaité à chaque démarrage. Si les noms d'hôte ne correspondent pas, le nom d'hôte est réinitialisé et le système redémarre éventuellement pour récupérer le nouveau nom d'hôte. Si aucun nom d'hôte personnalisé n'est spécifié, il est généré à l'aide de l'IPv4adresse privée au format hexadécimal, par exemple,. `ip-AC1F4E6` Pour empêcher que votre nom d'hôte existant ne soit modifié, n'activez pas ce paramètre.

   b. Étendre le volume de démarrage

      Ce paramètre étend de manière dynamique `Disk 0`/`Volume 0` pour inclure l'espace non partitionné. Cela peut être utile lorsque l'instance est démarrée à partir d'un volume du périphérique racine doté d'une taille personnalisée.

   c. Définir le compte administrateur

      Lorsque cette option est activée, vous pouvez définir les attributs de nom d'utilisateur et de mot de passe pour le compte d'administrateur créé sur votre ordinateur local. Si cette fonctionnalité n'est pas activée, un compte d'administrateur n'est pas créé sur le système après Sysprep. Indiquez un mot de passe dans `adminPassword` uniquement si `adminPasswordtype` est `Specify`.

      Les types de mots de passe sont définis comme suit :

      i. `Random`

         EC2Launchgénère un mot de passe et le chiffre à l'aide de la clé de l'utilisateur. Le système désactive ce paramètre après le lancement de l'instance afin que ce mot de passe persiste si l'instance est redémarrée, arrêtée ou démarrée.

      ii. `Specify`

         EC2Launchutilise le mot de passe que vous spécifiez dans`adminPassword`. Si le mot de passe ne répond pas aux exigences du système, EC2Launch génère un mot de passe aléatoire à la place. Le mot de passe est stocké dans le fichier `agent-config.yml` sous forme de texte clair et est supprimé une fois que le mot de passe est défini par Sysprep. EC2Launchchiffre le mot de passe à l'aide de la clé de l'utilisateur.

iii. `Do not set`

EC2Launchutilise le mot de passe que vous spécifiez dans le fichier unattend.xml. Si vous ne spécifiez pas de mot de passe dans unattend.xml, le compte d'administrateur est désactivé.

d. Démarrer le SSM service

Lorsque cette option est sélectionnée, le service Systems Manager est activé pour démarrer à la suite de Sysprep. EC2LaunchLa v2 exécute toutes les tâches décrites précédemment, et l'SSMagent traite les demandes relatives aux fonctionnalités de Systems Manager, telles que Run Command et State Manager.

Vous pouvez utiliser Run Command pour mettre à niveau vos instances existantes afin d'utiliser la dernière version du service et de l'SSMagent EC2Launch v2. Pour plus d'informations, consultez la section Update SSM Agent en utilisant Run Command dans le Guide de l'utilisateur de AWS Systems Manager.

e. Optimisez ENA

Lorsque cette option est sélectionnée, ENA les paramètres sont configurés pour garantir que les paramètres de mise à l'échelle côté ENA réception et de profondeur de la file d'attente de réception sont optimisés AWS. Pour de plus amples informations, veuillez consulter Configurer l'CPUaffinité de dimensionnement côté réception.

f. Activer SSH

Ce paramètre active Open SSH pour les versions ultérieures de Windows afin de permettre l'administration du système à distance.

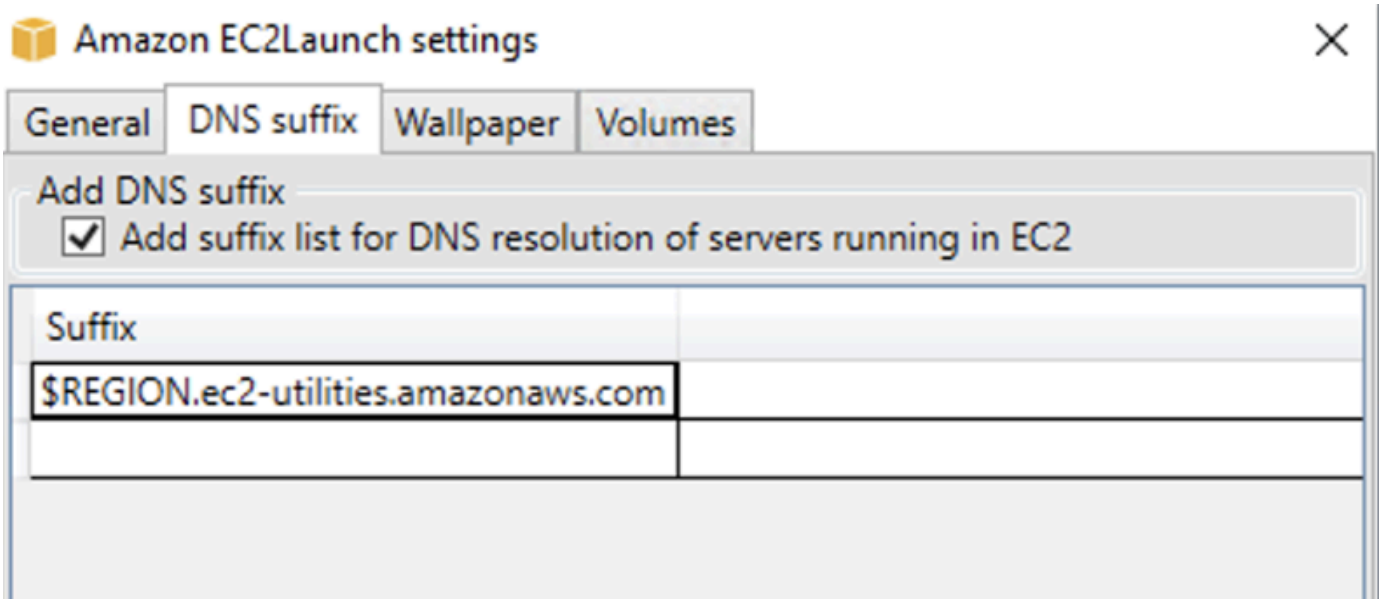
g. Activer les trames Jumbo

Sélectionnez cette option pour activer les trames Jumbo. Les trames Jumbo peuvent avoir des effets inattendus sur vos communications réseau. Assurez-vous donc de comprendre comment les trames Jumbo auront un impact sur votre système avant de les activer. Pour plus d'informations sur les trames jumbo, consultez Cadres Jumbo (9001MTU).

h. Préparer l'imagerie

Indiquez si vous souhaitez que votre EC2 instance s'arrête avec ou sans Sysprep. Lorsque vous souhaitez exécuter Sysprep avec la version EC2Launch v2, choisissez Shutdown with Sysprep.

4. Dans l'onglet DNSSuffixe, vous pouvez indiquer si vous souhaitez ajouter une liste de DNS suffixes pour la DNS résolution des serveurs en cours d'exécutionEC2, sans fournir le nom de domaine complet. DNSles suffixes peuvent contenir les variables `$REGION` et. `$AZ` Seuls les suffixes qui n'existent pas déjà seront ajoutés à la liste.



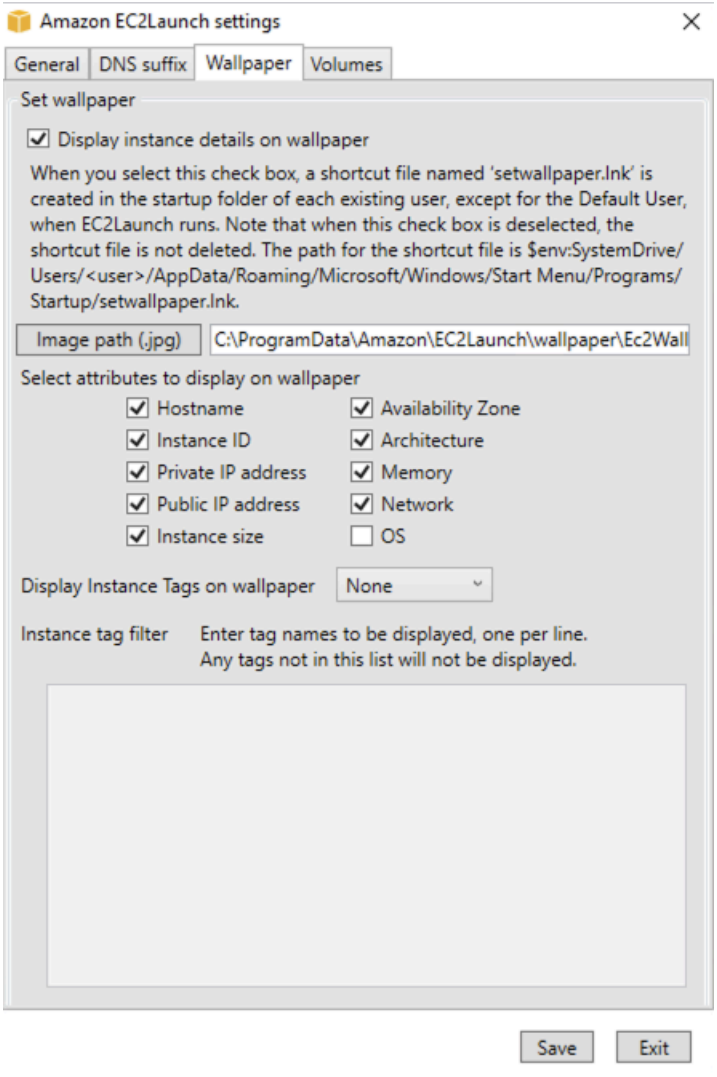
5. Dans l'onglet Fond d'écran, vous pouvez configurer le fond d'écran de votre instance avec une image d'arrière-plan et spécifier les détails de l'instance à afficher dans le fond d'écran. Amazon EC2 génère les informations à chaque fois que vous vous connectez.

   Vous pouvez configurer votre fond d'écran à l'aide des commandes suivantes.

   - Afficher les détails de l'instance sur le fond d'écran – Cette case à cocher active ou désactive l'affichage des détails de l'instance sur le fond d'écran.
   - Chemin de l'image (.jpg) – Spécifiez le chemin d'accès à l'image à utiliser comme fond d'écran.
   - Sélectionner les attributs à afficher sur le fond d'écran – Cochez les cases correspondant aux détails de l'instance que vous voulez voir apparaître sur le fond d'écran. Décochez les cases des détails d'instance précédemment sélectionnés que vous voulez supprimer du fond d'écran.
   - Afficher les balises d'instance sur le fond d'écran – Sélectionnez l'un des paramètres suivants pour afficher les balises d'instance sur le fond d'écran :
     - Aucun : n'affichez aucune balise d'instance sur le fond d'écran.
     - Afficher tout : affiche toutes les balises d'instance sur le fond d'écran.

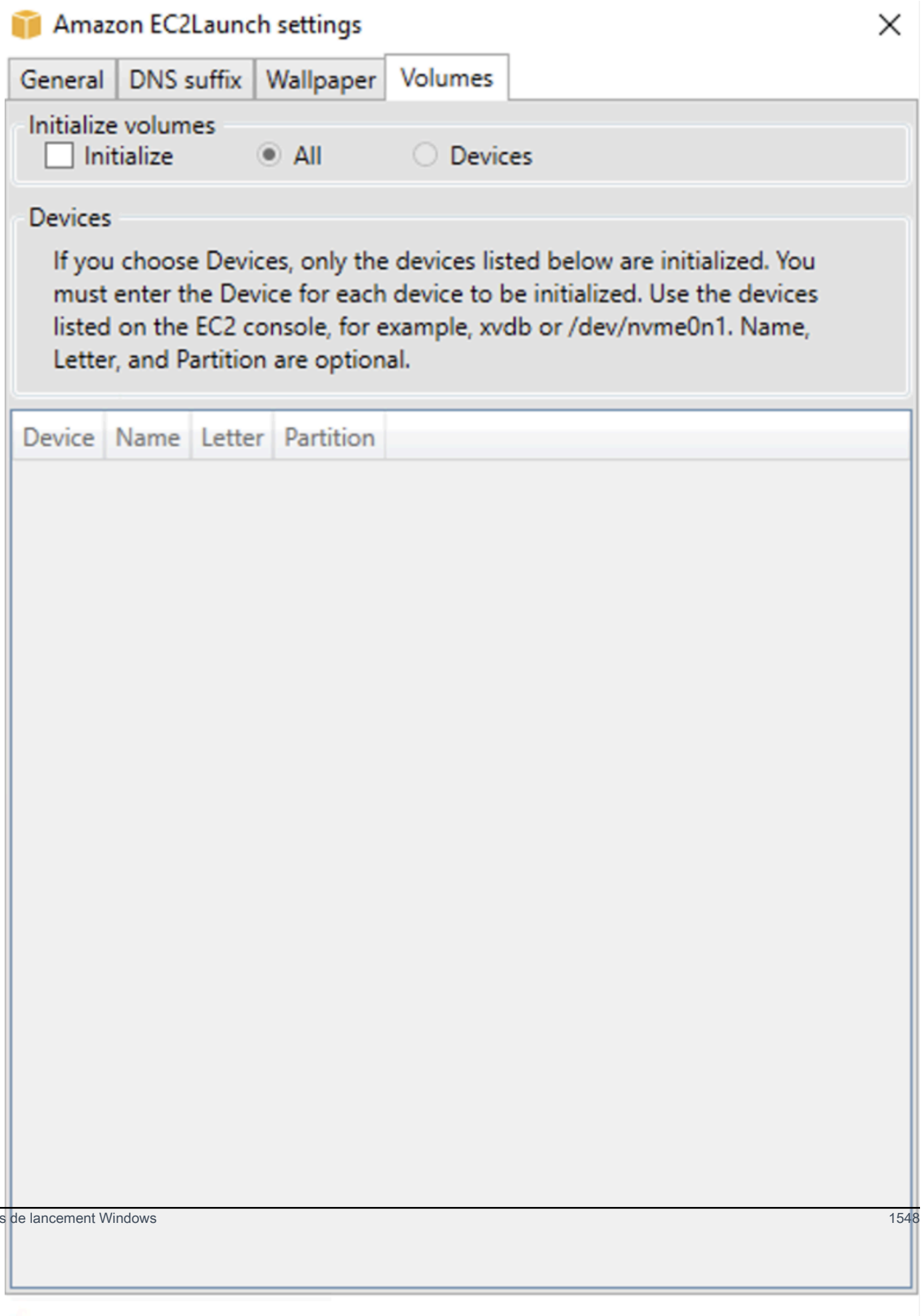
- Afficher avec filtre : affiche les balises d'instance spécifiées sur le fond d'écran. Lorsque vous sélectionnez ce paramètre, vous pouvez ajouter les balises d'instance que vous souhaitez voir s'afficher sur votre fond d'écran dans la zone Filtre de balise d'instance.

> **Note**
>
> Vous devez activer les balises dans les métadonnées pour afficher les balises sur le fond d'écran. Pour plus d'informations sur les balises et métadonnées d'instance, consultez Afficher les balises de vos EC2 instances à l'aide des métadonnées de l'instance.



6. Sous l'onglet Volumes, indiquez si vous souhaitez initialiser les volumes attachés à l'instance. L'activation définit les lettres de lecteur pour tous les volumes supplémentaires et les étend pour utiliser l'espace disponible. Si vous sélectionnez Tous, tous les volumes de stockage sont initialisés. Si vous sélectionnez Appareils, seuls les appareils spécifiés dans la liste sont initialisés. Vous devez entrer l'appareil pour chaque appareil à initialiser. Utilisez les appareils répertoriés sur la EC2 console, par exemple, `xvdb` ou`/dev/nvme0n1`. La liste déroulante affiche les volumes de stockage attachés à l'instance. Pour entrer un appareil qui n'est pas attaché à l'instance, saisissez-le dans le champ de texte.

   Nom, Lettre et Partition sont des champs facultatifs. Si aucune valeur n'est spécifiée pour Partition, les volumes de stockage supérieurs à 2 To sont initialisés avec le type de `gpt` partition, et ceux inférieurs à 2 To sont initialisés avec le type de `mbr` partition. Si des périphériques sont configurés et qu'un NTFS appareil autre qu'un périphérique contient une table de partition ou que les 4 premiers Ko du disque contiennent des données, le disque est ignoré et l'action est consignée.


Amazon EC2Launch settings
General
DNS suffix
Wallpaper
Volumes
Initialize volumes
Initialize
All
Devices
Devices
If you choose Devices, only the devices listed below are initialized. You must enter the Device for each device to be initialized. Use the devices listed on the EC2 console, for example, xvdb or /dev/nvme0n1. Name, Letter, and Partition are optional.
Device
Name
Letter
Partition

Voici un exemple de YAML fichier de configuration créé à partir des paramètres saisis dans la EC2Launch boîte de dialogue.

```
version: 1.0
config:
  - stage: boot
 tasks:
      - task: extendRootPartition
  - stage: preReady
    tasks:
      - task: activateWindows
        inputs:
          activation:
            type: amazon
      - task: setDnsSuffix
        inputs:
          suffixes:
            - $REGION.ec2-utilities.amazonaws.com
      - task: setAdminAccount
        inputs:
          password:
            type: random
      - task: setWallpaper
        inputs:
          path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
          attributes:
            - hostName
            - instanceId
            - privateIpAddress
            - publicIpAddress
            - instanceSize
            - availabilityZone
            - architecture
            - memory
            - network
  - stage: postReady
    tasks:
      - task: startSsm
```

Configurez la EC2Launch v2 à l'aide du CLI

Vous pouvez utiliser l'interface de ligne de commande (CLI) pour configurer vos EC2Launch paramètres et gérer le service. La section suivante contient des descriptions et des informations d'utilisation pour les CLI commandes que vous pouvez utiliser pour gérer la EC2Launch version 2.

Commandes

collect-logs

Collecte les fichiers journauxEC2Launch, les compresse et les place dans un répertoire spécifié.

Exemple

```
ec2launch collect-logs -o C:\Mylogs.zip
```

Utilisation

`ec2launch collect-logs [flags]`

Indicateurs

`-h`, `--help`

aide pour `collect-logs`

`-o, --output string`

chemin d'accès aux fichiers journaux de sortie compressés

get-agent-config

Imprime `agent-config.yml` dans le format spécifié (JSONouYAML). Si aucun format n'est spécifié, `agent-config.yml` est imprimé dans le format précédemment spécifié.

Exemple

```
ec2launch get-agent-config -f json
```

Exemple 2

Les PowerShell commandes suivantes indiquent comment modifier et enregistrer le `agent-config` fichier au JSON format.

```
$config = & "$env:ProgramFiles/Amazon/EC2Launch/EC2Launch.exe" --format json |
 ConvertFrom-Json
$jumboFrame =@"
{
   "task": "enableJumboFrames"
}
"@
$config.config | %{if($_.stage -eq 'postReady'){$_.tasks += (ConvertFrom-Json -
InputObject $jumboFrame)}}
$config | ConvertTo-Json -Depth 6 | Out-File -encoding UTF8
$env:ProgramData/Amazon/EC2Launch/config/agent-config.yml
```

Utilisation

`ec2launch get-agent-config [flags]`

Indicateurs

`-h, --help`

aide pour `get-agent-config`

`-f, --format string`

format de sortie du fichier `agent-config` : `json`, `yaml`

list-volumes

Répertorie tous les volumes de stockage attachés à l'instance, y compris les volumes éphémères et les EBS volumes.

Exemple

```
ec2launch list-volumes
```

Utilisation

`ec2launch list-volumes`

Indicateurs

`-h`, `--help`

aide pour `list-volumes`

reset

L'objectif principal de cette tâche est de réinitialiser l'agent pour sa prochaine exécution. Pour ce faire, la reset commande supprime toutes les données d'état de l'agent pour la EC2Launch v2 du `EC2Launch` répertoire local (voirEC2Launchstructure du répertoire v2). Reset supprime éventuellement le service et les journaux Sysprep.

Le comportement des scripts dépend du mode dans lequel l'agent exécute les scripts : en ligne ou détaché.

En ligne (par défaut)

L'agent EC2Launch v2 exécute les scripts un par un (`detach: false`). Il s'agit du paramètre par défaut.

> **Note**
>
> Lorsque votre script en ligne émet une commande reset ou sysprep, il s'exécute immédiatement et réinitialise l'agent. La tâche en cours se termine, puis l'agent s'arrête sans exécuter d'autres tâches.

Par exemple, si la tâche qui émet la commande aurait été suivie d'une tâche `startSsm` (incluse par défaut après l'exécution des données utilisateur), la tâche ne s'exécute pas et le service Systems Manager ne démarre jamais.

Detached

L'agent EC2Launch v2 exécute des scripts simultanément avec d'autres tâches (`detach: true`).

> **Note**
>
> Lorsque votre script détaché émet une commande reset ou sysprep, ces commandes attendent que l'agent ait terminé leur exécution avant de s'exécuter. Les tâches suivantes executeScript seront toujours exécutées.

Exemple

```
ec2launch reset -c
```

Utilisation

`ec2launch reset [flags]`

Indicateurs

`-c`, `--clean`

nettoie les journaux d'instance avant la `reset`

`-h`, `--help`

aide pour `reset`

run

Exécute la EC2Launch v2.

Exemple

```
ec2launch run
```

Utilisation

`ec2launch run [flags]`

Indicateurs

`-h, --help`

aide pour `run`

status

Obtient le statut de l'agent EC2Launch v2. Il est possible de bloquer le processus jusqu'à ce que l'agent soit terminé. Le code de sortie du processus détermine l'état de l'agent :

- `0` : l'agent a été exécuté avec succès.
- `1` : l'agent a été exécuté et a échoué.
- `2` : l'agent est toujours en cours d'exécution.
- `3` : l'agent est dans un état inconnu. L'état de l'agent n'est pas en cours d'exécution ou arrêté.
- `4` : une erreur s'est produite lors de la tentative de récupération de l'état de l'agent.
- `5` : l'agent n'est pas en cours d'exécution et l'état de la dernière exécution connue est inconnu. Cela peut signifier :
  - qu'à la fois `state.json` et `previous-state.json` sont supprimés.
  - que `previous-state.json` est corrompu.

  Il s'agit de l'état de l'agent après l'exécution de la commande `reset`.

Exemple :

```
ec2launch status -b
```

Utilisation

`ec2launch status [flags]`

Indicateurs

`-b,--block`

bloque le processus jusqu'à la fin de l'exécution de l'agent

`-h,--help`

aide pour `status`

sysprep

L'objectif principal de cette tâche est de réinitialiser l'agent pour sa prochaine exécution. Pour ce faire, la sysprep commande réinitialise l'état de l'agent, met à jour le `unattend.xml` fichier, désactive et exécute RDP Sysprep.

Le comportement des scripts dépend du mode dans lequel l'agent exécute les scripts : en ligne ou détaché.

En ligne (par défaut)

L'agent EC2Launch v2 exécute les scripts un par un (`detach: false`). Il s'agit du paramètre par défaut.

> **Note**
>
> Lorsque votre script en ligne émet une commande reset ou sysprep, il s'exécute immédiatement et réinitialise l'agent. La tâche en cours se termine, puis l'agent s'arrête sans exécuter d'autres tâches.
> Par exemple, si la tâche qui émet la commande aurait été suivie d'une tâche `startSsm` (incluse par défaut après l'exécution des données utilisateur), la tâche ne s'exécute pas et le service Systems Manager ne démarre jamais.

Detached

L'agent EC2Launch v2 exécute des scripts simultanément avec d'autres tâches (`detach: true`).

> **Note**
>
> Lorsque votre script détaché émet une commande reset ou sysprep, ces commandes attendent que l'agent ait terminé leur exécution avant de s'exécuter. Les tâches suivantes executeScript seront toujours exécutées.

Exemple :

```
ec2launch sysprep
```

Utilisation

`ec2launch sysprep [flags]`

Indicateurs

`-c,--clean`

nettoie les journaux d'instance avant la `sysprep`

`-h,--help`

aide pour Sysprep

`-s,--shutdown`

arrête l'instance après l'exécution de `sysprep`

valider

Valide le fichier `agent-config` `C:\ProgramData\Amazon\EC2Launch\config\agent-config.yml`.

Exemple

```
ec2launch validate
```

Utilisation

`ec2launch validate [flags]`

Indicateurs

-h , `--help`

aide pour `validate`

version

Obtient la version exécutable.

Exemple

```
ec2launch version
```

Utilisation

`ec2launch version [flags]`

Indicateurs

`-h`, `--help`

aide pour `version`

fond d'écran

Définit le nouveau fond d'écran sur le chemin d'écran fourni (fichier .jpg) et affiche les détails de l'instance sélectionnée.

Syntaxe

```
ec2launch wallpaper ^
--path="C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg" ^
--all-tags ^
--
attributes=hostName,instanceId,privateIpAddress,publicIpAddress,instanceSize,availabilityZone,a
```

Inputs

Paramètres

--balises autorisées [***tag-name-1***, ***tag-name-n***]

(Facultatif) JSON Tableau codé en Base64 de noms de balises d'instance à afficher sur le fond d'écran. Vous pouvez utiliser cette balise ou l'option `--all-tags`, mais pas les deux.

--attributs ***attribute-string-1***, ***attribute-string-n***

(Facultatif) Une liste de chaînes d'attributs `wallpaper` séparées par des virgules pour appliquer des paramètres au fond d'écran.

[--chemin | -p] ***path-string***

(Obligatoire) Spécifie le chemin du fichier image d'arrière-plan `wallpaper`.

Indicateurs

--all-tags

(Facultatif) Affiche toutes les balises d'instance sur le fond d'écran. Vous pouvez utiliser cette balise ou l'option `--allowed-tags`, mais pas les deux.

[--help | -h]

Affiche l'aide concernant la commande wallpaper.

EC2Launchconfiguration des tâches v2

Cette section inclut les schémas de configuration, les tâches, les détails et les exemples pour `agent-config.yml` et les données utilisateur.

Tâches et exemples

- Schéma : agent-config.yml
- Configurer les scripts de données utilisateur EC2Launch v2 qui s'exécutent lors du lancement ou du redémarrage

Schéma : **`agent-config.yml`**

La structure du fichier `agent-config.yml` est illustrée ci-dessous. Notez qu'une tâche ne peut pas être répétée dans la même étape. Pour connaître les propriétés des tâches, consultez les descriptions de tâches suivantes.

Structure du document : agent-config.yml

JSON

```
{
 "version": "1.0",
 "config": [
  {
   "stage": "string",
   "tasks": [
```

```
    {
     "task": "string",
     "inputs": {
      ...
     }
    },
    ...
   ]
  },
  ...
 ]
}
```

YAML

```
version: 1.0
config:
- stage: string
  tasks:
  - task: string
 inputs:
   ...
  ...
...
```

Exemple : **`agent-config.yml`**

L'exemple suivant montre les paramètres du fichier de configuration `agent-config.yml`.

```
version: 1.0
config:
- stage: boot
  tasks:
  - task: extendRootPartition
- stage: preReady
  tasks:
  - task: activateWindows
    inputs:
      activation:
        type: amazon
  - task: setDnsSuffix
    inputs:
      suffixes:
```

```
      - $REGION.ec2-utilities.amazonaws.com
  - task: setAdminAccount
    inputs:
      password:
        type: random
  - task: setWallpaper
    inputs:
      path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
      attributes:
      - hostName
      - instanceId
      - privateIpAddress
      - publicIpAddress
      - instanceSize
      - availabilityZone
      - architecture
      - memory
      - network
- stage: postReady
  tasks:
  - task: startSsm
```

Configurer les scripts de données utilisateur EC2Launch v2 qui s'exécutent lors du lancement ou du redémarrage

Les YAML exemples suivants JSON montrent la structure du document pour les données utilisateur. Amazon EC2 analyse chaque tâche nommée dans le `tasks` tableau que vous spécifiez dans le document. Chaque tâche possède son propre ensemble de propriétés et d'exigences. Pour obtenir des détails, veuillez consulter le Définitions de tâches pour les tâches de EC2Launch démarrage de la version 2.

> **Note**
>
> Une tâche ne doit apparaître qu'une seule fois dans le tableau des tâches relatives aux données utilisateur.

Structure du document : données utilisateur

JSON

```
{
```

```
 "version": "1.1",
 "tasks": [
  {
   "task": "string",
   "inputs": {
    ...
   },
  },
  ...
 ]
}
```

YAML

```
version: 1.1
tasks:
- task: string
  inputs:
    ...
...
```

Exemple : données utilisateur

Pour plus d'informations sur les rôles d'utilisateur, consultez Comment Amazon EC2 gère les données utilisateur pour les instances Windows.

L'exemple de YAML document suivant montre un PowerShell script que la EC2Launch version 2 exécute en tant que données utilisateur pour créer un fichier.

```
version: 1.1
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: powershell
    runAs: localSystem
    content: |-
      New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
```

Vous pouvez utiliser un XML format pour les données utilisateur compatible avec les versions précédentes de l'agent de lancement. EC2LaunchLa v2 exécute le script en tant que

`executeScript` tâche dans la `UserData` phase. Pour se conformer à la EC2Launch v1 et au EC2Config comportement, le script de données utilisateur s'exécute par défaut en tant que processus attaché/en ligne.

Vous pouvez ajouter des balises facultatives pour personnaliser l'exécution de votre script. Par exemple, pour exécuter le script de données utilisateur lors du redémarrage de l'instance et lors du lancement de l'instance, vous pouvez utiliser la balise suivante :

`<persist>true</persist>`

Exemple :

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Vous pouvez spécifier un ou plusieurs PowerShell arguments à l'aide de la `<powershellArguments>` balise. Si aucun argument n'est transmis, la EC2Launch v2 ajoute l'argument suivant par défaut : `-ExecutionPolicy Unrestricted`

Exemple :

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

Pour exécuter un script de données XML utilisateur en tant que processus détaché, ajoutez la balise suivante à vos données utilisateur.

`<detach>true</detach>`

Exemple :

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
```

```
</powershell>
<detach>true</detach>
```

> **Note**
>
> La balise detach n'est pas prise en charge sur les agents de lancement précédents.

Journal des modifications : données utilisateur

Le tableau suivant répertorie les modifications apportées aux données utilisateur et les référence à la version de l'agent EC2Launch v2 applicable.

Version des données utilisateur	Détails	Présenté dans
1.1	• Les tâches relatives aux données utilisateur s'exécutent avant l'étape `PostReady` dans le fichier de configuration de l'agent. • Exécute les données utilisateur avant de démarrer l'agent Systems Manager (même comportement que les versions EC2Launch 1 et 1EC2Config) . *	EC2Launch Version v2 2.0.1245
1.0	• Deviendra obsolète. • Les tâches relatives aux données utilisateur s'exécutent après l'étape `PostReady` dans le fichier de configuration de l'agent. Ce n'est pas rétrocompatible avec la EC2Launch v1. • Affecté par une condition de concurrence entre les tâches de démarrage et de données utilisateur de l'agent Systems Manager.	EC2Launch v2 version 2.0.0

* Lorsqu'il est utilisé avec le fichier `agent-config.yml` par défaut.

EC2LaunchCodes de sortie et redémarrages de la v2

Vous pouvez utiliser la EC2Launch version 2 pour définir la manière dont les codes de sortie sont gérés par vos scripts. Par défaut, le code de sortie de la dernière commande exécutée dans un script est signalé comme le code de sortie pour l'ensemble du script. Par exemple, si un script inclut trois commandes et que la première commande échoue mais que les suivantes réussissent, le statut d'exécution est signalé comme `success` étant donné que la commande finale a réussi.

Si vous souhaitez qu'un script redémarre une instance, vous devez le spécifier `exit 3010` dans votre script, même si le redémarrage est la dernière étape de votre script. `exit 3010`demande à EC2Launch v2 de redémarrer l'instance et d'appeler à nouveau le script jusqu'à ce qu'il renvoie un code de sortie qui ne l'est pas`3010`, ou jusqu'à ce que le nombre maximal de redémarrages soit atteint. EC2LaunchLa version v2 autorise un maximum de 5 redémarrages par tâche. Si vous tentez de redémarrer une instance à partir d'un script à l'aide d'un mécanisme différent, tel que `Restart-Computer`, le statut d'exécution du script sera incohérent. Par exemple, il peut être bloqué dans une boucle de redémarrage ou ne pas effectuer le redémarrage.

Si vous utilisez un format de données XML utilisateur compatible avec les anciens agents, les données utilisateur risquent de s'exécuter plus souvent que prévu. Pour plus d'informations, consultez Le service exécute les données utilisateur plus d'une fois dans la section de résolution des problèmes.

EC2Launchv2 et Sysprep

Le service EC2Launch v2 exécute Sysprep, un outil Microsoft qui vous permet de créer un Windows personnalisé AMI qui peut être réutilisé. Lorsque la EC2Launch v2 appelle Sysprep, elle utilise les fichiers `%ProgramData%\Amazon\EC2Launch` pour déterminer les opérations à effectuer. Vous pouvez modifier ces fichiers indirectement à l'aide de la boîte de dialogue des EC2Launchparamètres ou directement à l'aide d'un YAML éditeur ou d'un éditeur de texte. Cependant, certains paramètres avancés ne sont pas disponibles dans la boîte de dialogue des EC2Launchparamètres. Vous devez donc modifier ces entrées directement.

Si vous créez une instance AMI à partir d'une instance après avoir mis à jour ses paramètres, les nouveaux paramètres sont appliqués à toute instance lancée à partir de la nouvelle instanceAMI. Pour plus d'informations sur la création d'unAMI, consultezCréez un compte soutenu EBS par Amazon AMI.

Définitions de tâches pour les tâches de EC2Launch démarrage de la version 2

Chaque tâche exécutée par la EC2Launch v2 lors du lancement ou du démarrage possède son propre ensemble de propriétés et d'exigences. Les détails des tâches incluent les paramètres relatifs à la fréquence d'exécution d'une tâche (une fois ou toujours), l'étape du processus de démarrage de l'agent à laquelle elle s'exécute, la syntaxe et des exemples de YAML documents. Pour plus d'informations, consultez les détails des tâches présentés dans cette référence.

EC2LaunchTâches v2

- activateWindows
- enableJumboFrames
- enableOpenSsh
- executeProgram
- executeScript
- extendRootPartition
- initializeVolume
- optimizeEna
- setAdminAccount
- setDnsSuffix
- setHostName
- setWallpaper
- startSsm
- sysprep
- writeFile

activateWindows

Active Windows sur un ensemble de AWS KMS serveurs. L'activation est ignorée si l'instance est détectée comme Bring-Your-Own-License (). BYOL

Fréquence — Une fois

AllowedStages — `[PreReady]`

Entrées —

`activation` : (carte)

`type` : type d'activation (string) à utiliser, défini sur `amazon`

Exemple

```
task: activateWindows
  inputs:
    activation:
    type: amazon
```

enableJumboFrames

Active les jumbo Frames, qui augmentent l'unité de transmission maximale (MTU) de l'adaptateur réseau. Pour de plus amples informations, veuillez consulter Cadres Jumbo (9001MTU).

Fréquence — Toujours

AllowedStages — `[PostReady, UserData]`

Entrées — Aucune

Exemple

```
task: enableJumboFrames
```

enableOpenSsh

Active Windows Open SSH et ajoute la clé publique de l'instance dans le dossier des clés autorisées.

Fréquence — Une fois

AllowedStages — `[PreReady, UserData]`

Entrées — Aucune

Exemple

L'exemple suivant montre comment activer Ouvrir SSH sur une instance et ajouter la clé publique de l'instance dans le dossier des clés autorisées. Cette configuration fonctionne uniquement sur les instances exécutant Windows Server 2019 et versions ultérieures.

```
task: enableOpenSsh
```

executeProgram

Exécute un programme avec des arguments facultatifs et une fréquence spécifiée.

Étapes : vous pouvez exécuter la tâche `executeProgram` pendant les étapes `PreReady`, `PostReady` et `UserData`.

Fréquence : configurable, voir Entrées.

Inputs

Cette section contient un ou plusieurs programmes pour la executeProgram tâche à exécuter (entrées). Chaque entrée peut inclure les paramètres configurables suivants :

fréquence (chaîne)

(Obligatoire) Spécifiez exactement l'une des valeurs suivantes :

- `once`
- `always`

chemin (chaîne)

(Obligatoire) Le chemin d'accès au fichier de l'exécutable à exécuter.

arguments (liste de chaînes)

(Facultatif) Liste d'arguments séparés par des virgules à fournir au programme en entrée.

runAs (chaîne)

(Obligatoire) Doit être défini sur `localSystem`

Sortie

Toutes les tâches écrivent des entrées du fichier journal dans le fichier `agent.log`. Les résultats supplémentaires de la tâche `executeProgram` sont stockés séparément dans un dossier nommé dynamiquement, comme suit :

`%LocalAppData%\Temp\`*`EC2Launch#########\outputfilename.tmp`*

Le chemin exact vers les fichiers de sortie est inclus dans le fichier `agent.log`, par exemple :

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\ExecuteProgramInputs.tmp
```

```
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

Fichiers de sortie pour la tâche **executeProgram**

ExecuteProgramInputs.tmp

Contient le chemin de l'exécutable et tous les paramètres d'entrée que la tâche `executeProgram` lui transmet lors de son exécution.

Output.tmp

Contient la sortie d'exécution du programme exécuté par la tâche `executeProgram`.

Err.tmp

Contient les messages d'erreur d'exécution du programme exécuté par la tâche `executeProgram`.

Exemples

Les exemples suivants montrent comment exécuter un fichier exécutable à partir d'un répertoire local sur une instance avec la tâche `executeProgram`.

Exemple 1 : configuration d'un exécutable avec un seul argument

Cet exemple montre une tâche `executeProgram` qui exécute un exécutable d'installation en mode silencieux.

```
task: executeProgram
  inputs:
    - frequency: always
      path: C:\Users\Administrator\Desktop\setup.exe
      arguments: ['-quiet']
```

Exemple 2 : VLC exécutable avec deux arguments

Cet exemple montre une `executeProgram` tâche qui exécute un fichier VLC exécutable avec deux arguments transmis en tant que paramètres d'entrée.

```
task: executeProgram
  inputs:
```

```
    - frequency: always
      path: C:\vlc-3.0.11-win64.exe
      arguments: ['/L=1033','/S']
      runAs: localSystem
```

executeScript

Exécute un script avec des arguments facultatifs et une fréquence spécifiée. Le comportement des scripts dépend du mode dans lequel l'agent exécute les scripts : en ligne ou détaché.

En ligne (par défaut)

L'agent EC2Launch v2 exécute les scripts un par un (`detach: false`). Il s'agit du paramètre par défaut.

> **Note**
>
> Lorsque votre script en ligne émet une commande reset ou sysprep, il s'exécute immédiatement et réinitialise l'agent. La tâche en cours se termine, puis l'agent s'arrête sans exécuter d'autres tâches.
> Par exemple, si la tâche qui émet la commande aurait été suivie d'une tâche `startSsm` (incluse par défaut après l'exécution des données utilisateur), la tâche ne s'exécute pas et le service Systems Manager ne démarre jamais.

Detached

L'agent EC2Launch v2 exécute des scripts simultanément avec d'autres tâches (`detach: true`).

> **Note**
>
> Lorsque votre script détaché émet une commande reset ou sysprep, ces commandes attendent que l'agent ait terminé leur exécution avant de s'exécuter. Les tâches suivantes executeScript seront toujours exécutées.

Étapes : vous pouvez exécuter la tâche `executeScript` pendant les étapes `PreReady`, `PostReady` et `UserData`.

Fréquence : configurable, voir Entrées.

Inputs

Cette section contient un ou plusieurs scripts pour la executeScript tâche à exécuter (entrées). Chaque entrée peut inclure les paramètres configurables suivants :

fréquence (chaîne)

(Obligatoire) Spécifiez exactement l'une des valeurs suivantes :

- `once`
- `always`

type (chaîne)

(Obligatoire) Spécifiez exactement l'une des valeurs suivantes :

- `batch`
- `powershell`

arguments (liste de chaînes)

(Facultatif) Une liste d'arguments de chaîne à passer au shell. Ce paramètre n'est pas pris en charge pour `type: batch`. Si aucun argument n'est transmis, la EC2Launch v2 ajoute l'argument suivant par défaut : `-ExecutionPolicy Unrestricted`

contenu (chaîne)

(Obligatoire) Contenu du script.

runAs (chaîne)

(Obligatoire) Spécifiez exactement l'une des valeurs suivantes :

- `admin`
- `localSystem`

detach (booléen)

(Facultatif) L'agent EC2Launch v2 exécute par défaut les scripts un par un (`detach: false`). Pour exécuter le script en même temps que d'autres tâches, définissez la valeur sur `true` (`detach: true`).

> **Note**
>
> Codes de sortie de script (y compris `3010`) n'ont aucun effet lorsque `detach` a la valeur `true`.

Sortie

Toutes les tâches écrivent des entrées du fichier journal dans le fichier `agent.log`. Les résultats supplémentaires du script exécuté par la tâche `executeScript` sont stockés séparément dans un dossier nommé dynamiquement, comme suit :

`%LocalAppData%\Temp\`*`EC2Launch#########`*`\`*`outputfilename.ext`*

Le chemin exact vers les fichiers de sortie est inclus dans le fichier `agent.log`, par exemple :

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\UserScript.ps1
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

Fichiers de sortie pour la tâche **`executeScript`**

`UserScript.`*`ext`*

Contient le script exécuté par la tâche `executeScript`. L'extension de fichier dépend du type de script que vous avez spécifié dans le paramètre `type` de la tâche `executeScript`, comme suit :

- Si le type est `batch`, l'extension du fichier est `.bat`.
- Si le type est `powershell`, l'extension du fichier est `.ps1`.

`Output.tmp`

Contient la sortie d'exécution du script exécuté par la tâche `executeScript`.

`Err.tmp`

Contient les messages d'erreur d'exécution du script exécuté par la tâche `executeScript`.

Exemples

Les exemples suivants montrent comment exécuter un script en ligne avec la tâche `executeScript`.

Exemple 1 : fichier texte de sortie Hello World

Cet exemple montre une `executeScript` tâche qui exécute un PowerShell script pour créer un fichier texte « Hello world » sur le `C:` lecteur.

```
task: executeScript
  inputs:
    - frequency: always
      type: powershell
      runAs: admin
      content: |-
        New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
        Set-Content 'C:\PowerShellTest.txt' "Hello world"
```

Exemple 2 : exécuter deux scripts

Cet exemple montre que la tâche `executeScript` peut exécuter plusieurs scripts et que le type de script ne doit pas nécessairement correspondre.

Le premier script (`type: powershell`) écrit un résumé des processus en cours d'exécution sur l'instance dans un fichier texte situé sur le lecteur `C:`.

Le second script (`batch`) écrit les informations système dans le fichier `Output.tmp`.

```
task: executeScript
  inputs:
    - frequency: always
      type: powershell
      content: |
        Get-Process | Out-File -FilePath C:\Process.txt
      runAs: localSystem
    - frequency: always
      type: batch
        content: |
        systeminfo
```

Exemple 3 : configuration d'un système idempotent avec redémarrages

Cet exemple montre une tâche `executeScript` qui exécute un script idempotent pour effectuer la configuration système suivante avec un redémarrage entre chaque étape :

- Renommer l'ordinateur.
- Joindre l'ordinateur au domaine.
- Activer Telnet.

Le script garantit que chaque opération ne s'exécute qu'une seule fois. Cela empêche une boucle de redémarrage et rend le script idempotent.

```
task: executeScript
  inputs:
    - frequency: always
      type: powershell
      runAs: localSystem
      content: |-
        $name = $env:ComputerName
        if ($name -ne $desiredName) {
          Rename-Computer -NewName $desiredName
          exit 3010
        }
        $domain = Get-ADDomain
        if ($domain -ne $desiredDomain)
        {
          Add-Computer -DomainName $desiredDomain
          exit 3010
        }
        $telnet = Get-WindowsFeature -Name Telnet-Client
        if (-not $telnet.Installed)
        {
          Install-WindowsFeature -Name "Telnet-Client"
          exit 3010
        }
```

extendRootPartition

Étend le volume racine pour utiliser tout l'espace disponible sur le disque.

Fréquence — Une fois

AllowedStages — `[Boot]`

Entrées — Aucune

Exemple

```
task: extendRootPartition
```

initializeVolume

Initialise les volumes vides attachés à l'instance afin qu'ils soient activés et partitionnés. L'agent de lancement ignore l'initialisation s'il détecte que le volume n'est pas vide. Un volume est considéré comme vide si les 4 premiers Kio d'un volume sont vides ou si un volume n'a pas de disposition de lecteur reconnaissable par Windows.

Le paramètre d'entrée `letter` est toujours appliqué lors de l'exécution de cette tâche, que le lecteur soit déjà initialisé ou non.

La tâche `initializeVolume` effectue ensuite les actions suivantes.

- Définissez les attributs de disque `offline` et `readonly` sur False.
- Créez une partition. Si aucun type de partition n'est spécifié dans le paramètre d'entrée `partition`, les valeurs par défaut suivantes s'appliquent :
  - Si la taille de disque est inférieure à 2 To, définissez le type de partition sur `mbr`.
  - Si la taille de disque est supérieure ou égale à 2 To, définissez le type de partition sur `gpt`.
- Formatez le volume en tant queNTFS.
- Définissez l'étiquette du volume comme suit :
  - Utilisez la valeur du paramètre d'entrée `name`, le cas échéant.
  - Si le volume est éphémère et qu'aucun nom n'a été spécifié, définissez l'étiquette du volume sur `Temporary Storage Z`.
- Si le volume est éphémère (SSDou HDD s'il ne s'agit pas d'AmazonEBS), créez un `Important.txt` fichier à la racine du volume avec le contenu suivant :

```
This is an 'Instance Store' disk and is provided at no additional charge.

*This disk offers increased performance since it is local to the host
*The number of Instance Store disks available to an instance vary by instance type
*DATA ON THIS DRIVE WILL BE LOST IN CASES OF IMPAIRMENT OR STOPPING THE INSTANCE.
 PLEASE ENSURE THAT ANY IMPORTANT DATA IS BACKED UP FREQUENTLY
```

```
For more information, please refer to: Stockage d'instances Stockage par blocs
 temporaire pour les EC2 instances.
```

- Réglez la lettre de lecteur sur la valeur spécifiée dans le paramètre d'entrée `letter`.

Étapes : vous pouvez exécuter la tâche `initializeVolume` pendant les étapes `PostReady` et `UserData`.

Fréquence : toujours.

Inputs

Vous pouvez configurer les paramètres d'exécution comme suit :

appareils (liste de cartes)

(Condition) Configuration pour chaque appareil initialisé par l'agent de lancement. Ceci est obligatoire si le paramètre d'entrée `initialize` est défini sur `devices`.

- appareil (chaîne, obligatoire) : identifie l'appareil lors de la création de l'instance. Par exemple, `xvdb`, `xvdf` ou `\dev\nvme0n1`.
- lettre (chaîne, facultatif) : un caractère. La lettre de lecteur à attribuer.
- nom (chaîne, facultatif) : le nom de volume à attribuer.
- partition (chaîne, facultatif) : spécifiez l'une des valeurs suivantes pour le type de partition à créer, ou laissez l'agent de lancement par défaut en fonction de la taille du volume :
  - mbr
  - tpt

initialiser (chaîne)

(Obligatoire) Spécifiez exactement l'une des valeurs suivantes :

- `all`
- `devices`

Exemples

Voici des exemples de configurations d'entrée pour la tâche `initializeVolume`.

Exemple 1 : Initialiser deux volumes sur une instance

Cet exemple montre une tâche `initializeVolume` qui initialise deux volumes secondaires sur une instance. L'appareil nommé `DataVolume2` dans l'exemple est éphémère.

```
task: initializeVolume
inputs:
  initialize: devices
  devices:
  - device: xvdb
    name: DataVolume1
    letter: D
    partition: mbr
  - device: /dev/nvme0n1
    name: DataVolume2
    letter: E
    partition: gpt
```

Exemple 2 : Initialisation EBS des volumes attachés à une instance

Cet exemple montre une `initializeVolume` tâche qui initialise tous les EBS volumes vides attachés à l'instance.

```
task: initializeVolume
inputs:
  initialize: all
```

optimizeEna

Optimise ENA les paramètres en fonction du type d'instance actuel ; peut redémarrer l'instance.

Fréquence — Toujours

AllowedStages — `[PostReady, UserData]`

Entrées — Aucune

Exemple

```
task: optimizeEna
```

setAdminAccount

Définit les attributs du compte d'administrateur par défaut créé sur la machine locale.

Fréquence — Une fois

AllowedStages — `[PreReady]`

Entrées —

`name` : nom (chaîne) du compte administrateur

`password` : (carte)

`type` : stratégie (chaîne) pour définir le mot de passe, comme `static`, `random` ou `doNothing`

`data` : (chaîne) stocke les données si le champ `type` est statique

Exemple

```
task: setAdminAccount
inputs:
  name: Administrator
  password:
  type: random
```

setDnsSuffix

Ajoute des DNS suffixes à la liste des suffixes de recherche. Seuls les suffixes qui n'existent pas déjà sont ajoutés à la liste. Pour plus d'informations sur la façon dont les agents de lancement définissent les DNS suffixes, consultez. Configurer le DNS suffixe pour les agents de lancement EC2 Windows

Fréquence — Toujours

AllowedStages — `[PreReady]`

Entrées —

`suffixes`: (liste de chaînes) liste d'un ou plusieurs DNS suffixes valides ; les variables de substitution valides sont et `$REGION` `$AZ`

Exemple

```
task: setDnsSuffix
inputs:
```

```
  suffixes:
  - $REGION.ec2-utilities.amazonaws.com
```

setHostName

Définit le nom d'hôte de l'ordinateur sur une chaîne personnalisée ou, si elle n'`hostName`est pas spécifiée, sur l'IPv4adresse privée.

Fréquence — Toujours

AllowedStages — `[PostReady, UserData]`

Entrées —

`hostName` : (chaîne) nom d'hôte facultatif, qui doit être formaté comme suit.

- Doit contenir 15 caractères ou moins
- Doit contenir uniquement des caractères alphanumériques (a-z, A-Z, 0-9) et tiret (-).
- Ne doit pas être entièrement composé de caractères numériques.

`reboot` : (booléen) indique si un redémarrage est autorisé lorsque le nom d'hôte est modifié

Exemple

```
task: setHostName
inputs:
  reboot: true
```

setWallpaper

Crée le fichier de raccourci `setwallpaper.lnk` dans le dossier de démarrage de chaque utilisateur existant, sauf pour `Default User`. Ce fichier de raccourci s'exécute lorsque l'utilisateur se connecte pour la première fois après le démarrage de l'instance. Il configure l'instance avec un fond d'écran personnalisé qui affiche les attributs de l'instance.

Le chemin du fichier de raccourci est le suivant :

```
$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/
Startup/setwallpaper.lnk
```

> **Note**
>
> Lorsque vous supprimez la tâche `setWallpaper`, ce fichier de raccourci n'est pas supprimé. Pour de plus amples informations, veuillez consulter La tâche `setWallpaper` n'est pas activée, mais le fond d'écran se réinitialise au redémarrage.

Étapes : vous pouvez configurer le fond d'écran au cours des étapes `PreReady` et `UserData`.

Fréquence : `always`

Configuration du fond d'écran

Vous pouvez utiliser les paramètres suivants pour configurer votre fond d'écran.

Inputs

Paramètres d'entrée que vous fournissez et attributs que vous pouvez définir pour configurer votre fond d'écran :

attributs (liste de chaînes)

(Facultatif) Vous pouvez ajouter un ou plusieurs des attributs suivants à votre fond d'écran :

- `architecture`
- `availabilityZone`
- `hostName`
- `instanceId`
- `instanceSize`
- `memory`
- `network`
- `privateIpAddress`
- `publicIpAddress`

instanceTags

(Facultatif) Vous pouvez utiliser exactement l'une des options suivantes pour ce paramètre.

- AllTags(string) — Ajoutez toutes les balises d'instance à votre fond d'écran.

```
instanceTags: AllTags
```

- instanceTags(liste de chaînes) — Spécifiez une liste de noms de balises d'instance à ajouter à votre fond d'écran. Par exemple :

```
instanceTags:
  - Tag 1
  - Tag 2
```

chemin (chaîne)

(Obligatoire) Le chemin du nom du fichier image au format .jpg local à utiliser pour votre image de fond d'écran.

Exemple

L'exemple suivant montre les entrées de configuration du fond d'écran qui définissent le chemin du fichier pour l'image d'arrière-plan du fond d'écran, ainsi que les balises d'instance nommées `Tag 1` et `Tag 2`, ainsi que les attributs qui incluent le nom d'hôte, l'ID d'instance et les adresses IP privées et publiques de l'instance.

```
task: setWallpaper
inputs:
  path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
  attributes:
  - hostName
  - instanceId
  - privateIpAddress
  - publicIpAddress
instanceTags:
  - Tag 1
  - Tag 2
```

> **Note**
>
> Vous devez activer les balises dans les métadonnées pour afficher les balises sur le fond d'écran. Pour plus d'informations sur les balises et métadonnées d'instance, consultez Afficher les balises de vos EC2 instances à l'aide des métadonnées de l'instance.

startSsm

Démarre le service Systems Manager (SSM) après Sysprep.

Fréquence — Toujours

AllowedStages — `[PostReady, UserData]`

Entrées — Aucune

Exemple

```
task: startSsm
```

sysprep

Réinitialise l'état du service, met à jour`unattend.xml`, désactive et exécute RDP Sysprep. Cette tâche s'exécute uniquement une fois que toutes les autres tâches sont terminées.

Fréquence — Une fois

AllowedStages — `[UserData]`

Entrées —

`clean` : (booléen) nettoie les journaux d'instance avant d'exécuter Sysprep

`shutdown` : (booléen) arrête l'instance après avoir exécuté Sysprep

Exemple

```
task: sysprep
inputs:
clean: true
shutdown: true
```

writeFile

Écrit un fichier vers une destination.

Fréquence — voir Entrées

AllowedStages — `[PostReady, UserData]`

Entrées —

`frequency` : (chaîne) `once` ou `always`

`destination` : (chaîne) chemin vers lequel écrire le contenu

`content` : (chaîne) texte à écrire dans la destination

Exemple

```
task: writeFile
inputs:
  - frequency: once
  destination: C:\Users\Administrator\Desktop\booted.txt
  content: Windows Has Booted
```

Résoudre les problèmes liés à l'agent EC2Launch v2

Cette section présente les scénarios de résolution des problèmes courants pour la EC2Launch version 2, des informations sur l'affichage des journaux d'événements Windows, ainsi que les résultats et les messages des journaux de console.

Résolution des problèmes liés aux rubriques

- Scénarios courants de résolution des problèmes
- Journaux d'événements Windows
- EC2Launchsortie du journal de la console v2

Scénarios courants de résolution des problèmes

Cette section présente les scénarios de dépannage courants et les étapes de résolution.

Scénarios

- Le service ne parvient pas à définir le fond d'écran
- Le service ne parvient pas à exécuter les données utilisateur
- Le service exécute une tâche une seule fois
- Le service ne parvient pas à exécuter une tâche
- Le service exécute les données utilisateur plus d'une fois
- Les tâches planifiées de la EC2Launch version 1 ne s'exécutent pas après la migration vers la EC2Launch version 2
- Le service initialise un EBS volume qui n'est pas vide

- La tâche setWallpaper n'est pas activée, mais le fond d'écran se réinitialise au redémarrage
- Service bloqué en mode d'exécution
- Non valide agent-config.yml empêche l'ouverture de la boîte de dialogue des paramètres de la EC2Launch v2
- task:executeScript should be unique and only invoked once

Le service ne parvient pas à définir le fond d'écran

Résolution

1. Vérifiez si `%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\setwallpaper.lnk` existe.
2. Vérifiez dans `%ProgramData%\Amazon\EC2Launch\log\agent.log` pour voir si des erreurs se sont produites.

Le service ne parvient pas à exécuter les données utilisateur

Cause possible : le service peut avoir échoué avant l'exécution des données utilisateur.

Résolution

1. Vérifiez `%ProgramData%\Amazon\EC2Launch\state\previous-state.json`.
2. Voyez si `boot`, `network`, `preReady` et `postReadyLocalData` ont tous été marqués comme une réussite.
3. Si l'une des étapes a échoué, vérifiez si `%ProgramData%\Amazon\EC2Launch\log\agent.log` contient des erreurs spécifiques.

Le service exécute une tâche une seule fois

Résolution

1. Vérifiez la fréquence de la tâche.
2. Si le service a déjà été exécuté après Sysprep et que la fréquence de la tâche est définie sur `once`, la tâche ne s'exécutera plus.
3. Définissez la fréquence de la tâche sur `always` si vous souhaitez qu'elle l'exécute à chaque exécution de la EC2Launch v2.

Le service ne parvient pas à exécuter une tâche

Résolution

1. Vérifiez les dernières entrées dans `%ProgramData%\Amazon\EC2Launch\log\agent.log`.
2. Si aucune erreur n'est survenue, essayez d'exécuter le service manuellement à partir de `"%ProgramFiles%\Amazon\EC2Launch\EC2Launch.exe" run` pour voir si les tâches réussissent.

Le service exécute les données utilisateur plus d'une fois

Résolution

Les données utilisateur sont traitées différemment entre la EC2Launch v1 et la EC2Launch v2. EC2Launchv1 exécute les données utilisateur sous forme de tâche planifiée sur l'instance lorsqu'elle `persist` est définie sur`true`. Si `persist` est défini sur `false`, la tâche n'est pas planifiée même lorsqu'elle se termine avec un redémarrage ou est interrompue pendant son exécution.

EC2LaunchLa v2 exécute les données utilisateur en tant que tâche d'agent et suit leur état d'exécution. Si les données utilisateur entraînent un redémarrage de l'ordinateur ou si leur exécution est interrompue, l'état d'exécution `pending` persiste et les données utilisateur seront réexécutées au démarrage suivant de l'instance. Si vous souhaitez empêcher le script de données utilisateur de s'exécuter plusieurs fois, rendez le script idempotent.

L'exemple suivant de script idempotent définit le nom de l'ordinateur et joint un domaine.

```
<powershell>
  $name = $env:computername
  if ($name -ne $desiredName) {
 Rename-Computer -NewName $desiredName
  }
  $domain = Get-ADDomain
  if ($domain -ne $desiredDomain)
  {
 Add-Computer -DomainName $desiredDomain
  }
  $telnet = Get-WindowsFeature -Name Telnet-Client
  if (-not $telnet.Installed)
  {
 Install-WindowsFeature -Name "Telnet-Client"
  }
```

```
</powershell>
<persist>false</persist>
```

Les tâches planifiées de la EC2Launch version 1 ne s'exécutent pas après la migration vers la EC2Launch version 2

Résolution

L'outil de migration ne détecte aucune tâche planifiée liée aux scripts EC2Launch v1 ; par conséquent, il ne configure pas automatiquement ces tâches dans la EC2Launch version v2. Pour configurer ces tâches, modifiez le `agent-config.yml`fichier ou utilisez la boîte de dialogue des EC2Launch paramètres de la version 2. Par exemple, si une tâche planifiée est exécutée sur une instance`InitializeDisks.ps1`, après avoir exécuté l'outil de migration, vous devez spécifier les volumes que vous souhaitez initialiser dans la boîte de dialogue des paramètres de EC2Launch la version 2. Voir l'étape 6 de la procédure pour Modifier les paramètres à l'aide de la boîte de EC2Launch dialogue des paramètres de la version 2.

Le service initialise un EBS volume qui n'est pas vide

Résolution

Avant d'initialiser un volume, la EC2Launch v2 tente de détecter s'il est vide. Si un volume n'est pas vide, il ignore l'initialisation. Les volumes détectés comme non vides ne sont pas initialisés. Un volume est considéré comme vide si les 4 premiers Ko d'un volume sont vides ou si un volume n'a pas de disposition de lecteur reconnaissable par Windows. Un volume initialisé et formaté sur un système Linux ne possède pas de disposition de lecteur reconnaissable par Windows, par exemple ou. MBR GPT Par conséquent, il sera considéré comme vide et initialisé. Si vous souhaitez conserver ces données, ne vous fiez pas à la détection des disques vides dans la EC2Launch version v2. Spécifiez plutôt les volumes que vous souhaitez initialiser dans la boîte de dialogue des EC2Launch paramètres de la version 2 (voir étape 6) ou dans le `agent-config.yml`.

La tâche **`setWallpaper`** n'est pas activée, mais le fond d'écran se réinitialise au redémarrage

La tâche `setWallpaper` crée le fichier de raccourci `setwallpaper.lnk` dans le dossier de démarrage de chaque utilisateur existant, sauf pour `Default User`. Ce fichier de raccourci s'exécute lorsque l'utilisateur se connecte pour la première fois après le démarrage de l'instance. Il configure l'instance avec un fond d'écran personnalisé qui affiche les attributs de l'instance. La suppression de la tâche `setWallpaper` ne supprime pas ce fichier de raccourci. Vous devez supprimer manuellement ce fichier ou le supprimer à l'aide d'un script.

Le chemin du raccourci est le suivant :

`$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/setwallpaper.lnk`

Résolution

Supprimez manuellement ce fichier ou supprimez-le à l'aide d'un script.

Exemple de PowerShell script pour supprimer un fichier de raccourci

```
foreach ($userDir in (Get-ChildItem "C:\Users" -Force -Directory).FullName)
{
 $startupPath = Join-Path $userDir -ChildPath "AppData\Roaming\Microsoft\Windows\Start
 Menu\Programs\Startup"
 if (Test-Path $startupPath)
 {
  $wallpaperSetupPath = Join-Path $startupPath -ChildPath "setwallpaper.lnk"
  if (Test-Path $wallpaperSetupPath)
  {
   Remove-Item $wallpaperSetupPath -Force -Confirm:$false
  }
 }
}
```

Service bloqué en mode d'exécution

Description

EC2LaunchLa v2 est bloquée, avec des messages de journal (`agent.log`) similaires aux suivants :

```
2022-02-24 08:08:58 Info:
 ********************************************************************************
2022-02-24 08:08:58 Info: EC2Launch Service starting
2022-02-24 08:08:58 Info: Windows event custom log exists: Amazon EC2Launch
2022-02-24 08:08:58 Info: ACPI SPCR table not supported. Bailing Out
2022-02-24 08:08:58 Info: Serial port is in use. Waiting for Serial Port...
2022-02-24 08:09:00 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:02 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:04 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:06 Info: ACPI SPCR table not supported. Use default console port.
```

Cause possible

SACest activé et utilise le port série. Pour plus d'informations, consultez la section Utiliser SAC pour dépanner votre instance Windows.

Résolution

Essayez les étapes suivantes pour résoudre ce problème :

- Désactivez le service qui utilise le port série.
- Si vous voulez que le service continue à utiliser le port série, écrivez des scripts personnalisés pour exécuter les tâches de l'agent de lancement et invoquez-les en tant que tâches planifiées.

Non valide **`agent-config.yml`** empêche l'ouverture de la boîte de dialogue des paramètres de la EC2Launch v2

Description

EC2Launchv2 settings tente d'analyser le `agent-config.yml` fichier avant qu'il n'ouvre la boîte de dialogue. Si le fichier YAML de configuration ne suit pas le schéma pris en charge, la boîte de dialogue affiche le message d'erreur suivant :

```
Unable to parse configuration file agent-config.yml. Review configuration file. Exiting application.
```

Résolution

1. Vérifiez que le fichier de configuration est conforme au schéma pris en charge.
2. Si vous souhaitez commencer à zéro, copiez le fichier de configuration par défaut dans `agent-config.yml`. Vous pouvez utiliser l'exemple `agent-config.yml` fourni dans la section Configuration des tâches.
3. Vous pouvez également recommencer en supprimant `agent-config.yml`. EC2Launchv2 settings génère un fichier de configuration vide.

`task:executeScript should be unique and only invoked once`

Description

Une tâche ne peut pas être répétée dans la même étape.

Résolution

Certaines tâches doivent être saisies sous forme de tableau, telles que executeScriptet executeProgram. Pour un exemple de la façon d'écrire le script sous forme de tableau, consultez executeScript.

Journaux d'événements Windows

EC2LaunchLa v2 publie des journaux d'événements Windows pour les événements importants, tels que le démarrage du service, le fait que Windows est prêt, ainsi que la réussite ou l'échec des tâches. Les identificateurs d'événement identifient de manière unique un événement particulier. Chaque événement contient des informations sur l'étape, la tâche et le niveau, ainsi qu'une description. Vous pouvez définir des déclencheurs pour des événements spécifiques à l'aide de l'identificateur d'événement.

Événement : IDs fournissez des informations sur un événement et identifiez certains événements de manière unique. Le chiffre le moins significatif d'un ID d'événement indique la gravité d'un événement.

Événement	Chiffre le moins significatif
Success	. . .0
Informational	. . .1
Warning	. . .2
Error	. . .3

Les événements liés au service qui sont générés au démarrage ou à l'arrêt du service incluent un identifiant d'événement à un seul chiffre.

Événement	Identifiant à un chiffre
Success	0
Informational	1
Warning	2
Error	3

Les messages d'événement pour les événements `EC2LaunchService.exe` commencent par `Service:`. Les messages d'événement pour les événements `EC2Launch.exe` ne commencent pas par `Service:`.

Un événement à quatre chiffres IDs inclut des informations sur le stade, la tâche et la gravité d'un événement.

Rubriques

Format de l'ID d'événement

Le tableau suivant indique le format d'un identifiant d'événement EC2Launch v2.

3	2 1	0
S	T	L

Les lettres et les chiffres du tableau représentent le type d'événement et les définitions suivants.

Type d'événement	Définition
S (Stage)	0 - Message de niveau de service 1 - Démarrer 2 - Réseau 3 - PreReady 5 - Windows est prêt 6 - PostReady 7 - Données utilisateur

Type d'événement	Définition
T (Tâche)	Les tâches représentées par les deux valeurs correspondantes sont différentes pour chaque étape. Pour afficher la liste complète des événements, consultez Schéma du journal des événements Windows.
L (Niveau de l'événement)	0 - Réussite 1 - Informationnel 2 - Avertissement 3 - Erreur

Exemples d'ID d'événement

Voici un exemple d'événementIDs.

- `5000` - Windows est prêt à l'emploi
- `3010`- La tâche d'activation de Windows en cours d' PreReady étape a été réussie
- `6013`- La tâche de définition du fond d'écran dans le stage PostReady Local Data a rencontré une erreur

Schéma du journal des événements Windows

MessageId/Identifiant de l'événement	Message d'événement
`. . .0`	`Success`
`. . .1`	`Informational`
`. . .2`	`Warning`
`. . .3`	`Error`

MessageId/Identifiant de l'événement	Message d'événement
x	EC2Launch service-level logs
0	EC2Launch service exited successfully
1	EC2Launch service informational logs
2	EC2Launch service warning logs
3	EC2Launch service error logs
10	Replace state.json with previous-state.json
100	Serial Port
200	Sysprep
300	PrimaryNic
400	Metadata
x000	Stage (1 digit), Task (2 digits), Status (1 digit)
1000	Boot
1010	Boot - extend_root_partition
2000	Network
2010	Network - add_routes
3000	PreReady
3010	PreReady - activate_windows
3020	PreReady - install_egpu_manager

MessageId/Identifiant de l'événement	Message d'événement
3030	PreReady - set_monitor_on
3040	PreReady - set_hibernation
3050	PreReady - set_admin_account
3060	PreReady - set_dns_suffix
3070	PreReady - set_wallpaper
3080	PreReady - set_update_schedule
3090	PreReady - output_log
3100	PreReady - enable_open_ssh
5000	Windows is Ready to use
6000	PostReadyLocalData
7000	PostReadyUserData
6010/7010	PostReadyLocal/UserData - set_wallpaper
6020/7020	PostReadyLocal/UserData - set_update_schedule
6030/7030	PostReadyLocal/UserData - set_hostname
6040/7040	PostReadyLocal/UserData - execute_program
6050/7050	PostReadyLocal/UserData - execute_script
6060/7060	PostReadyLocal/UserData - manage_package

MessageId/Identifiant de l'événement	Message d'événement
6070/7070	PostReadyLocal/UserData - initialize_volume
6080/7080	PostReadyLocal/UserData - write_file
6090/7090	PostReadyLocal/UserData - start_ssm
7100	PostReadyUserData - enable_open_ssh
6110/7110	PostReadyLocal/UserData - enable_jumbo_frames

EC2Launchsortie du journal de la console v2

Cette section contient des exemples de sortie du journal de console pour la EC2Launch version v2 et répertorie tous les messages d'erreur du journal de console EC2Launch v2 pour vous aider à résoudre les problèmes. Pour plus d'informations sur la sortie de la console d'instance et sur la manière d'y accéder, consultezthe section called "Sortie de la console de l'instance".

Outputs

- EC2Launchsortie du journal de la console v2
- EC2Launchmessages de journal de la console v2

EC2Launchsortie du journal de la console v2

Voici un exemple de sortie du journal de console pour la EC2Launch version 2.

```
2023/11/30 20:18:53Z: Windows sysprep configuration complete.
2023/11/30 20:18:57Z: Message: Waiting for access to metadata...
2023/11/30 20:18:57Z: Message: Meta-data is now available.
2023/11/30 20:18:57Z: AMI Origin Version: 2023.11.15
2023/11/30 20:18:57Z: AMI Origin Name: Windows_Server-2022-English-Full-Base
2023/11/30 20:18:58Z: OS: Microsoft Windows NT 10.0.20348
2023/11/30 20:18:58Z: OsVersion: 10.0
```

```
2023/11/30 20:18:58Z: OsProductName: Windows Server 2022 Datacenter
2023/11/30 20:18:58Z: OsBuildLabEx: 20348.1.amd64fre.fe_release.210507-1500
2023/11/30 20:18:58Z: OsCurrentBuild: 20348
2023/11/30 20:18:58Z: OsReleaseId: 2009
2023/11/30 20:18:58Z: Language: en-US
2023/11/30 20:18:58Z: TimeZone: UTC
2023/11/30 20:18:58Z: Offset: UTC +0000
2023/11/30 20:18:58Z: Launch: EC2 Launch v2.0.1643
2023/11/30 20:18:58Z: AMI-ID: ami-1234567890abcdef1
2023/11/30 20:18:58Z: Instance-ID: i-1234567890abcdef0
2023/11/30 20:18:58Z: Instance Type: c5.large
2023/11/30 20:19:00Z: Driver: AWS NVMe Driver v1.5.0.33
2023/11/30 20:19:00Z: SubComponent: AWS NVMe Driver v1.5.0.33;
 EnableSCSIPersistentReservations: 0
2023/11/30 20:19:00Z: Driver: AWS PV Driver Package v8.4.3
2023/11/30 20:19:01Z: Driver: Amazon Elastic Network Adapter v2.6.0.0
2023/11/30 20:19:01Z: RDPCERTIFICATE-SUBJECTNAME: EC2AMAZ-SO1T009
2023/11/30 20:19:01Z: RDPCERTIFICATE-THUMBPRINT:
 1234567890ABCDEF1234567890ABCDEF1234567890
2023/11/30 20:19:09Z: SSM: Amazon SSM Agent v3.2.1705.0
2023/11/30 20:19:13Z: Username: Administrator
2023/11/30 20:19:13Z: Password: <Password>
1234567890abcdef1EXAMPLEPASSWORD
</Password>
2023/11/30 20:19:14Z: User data format: no_user_data
2023/11/30 20:19:14Z: EC2LaunchTelemetry: IsTelemetryEnabled=true
2023/11/30 20:19:14Z: EC2LaunchTelemetry: AgentOsArch=windows_amd64
2023/11/30 20:19:14Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2023/11/30 20:19:14Z: EC2LaunchTelemetry: AgentCommandErrorCode=0
2023/11/30 20:19:14Z: Message: Windows is Ready to use
```

EC2Launchmessages de journal de la console v2

Vous trouverez ci-dessous une liste de tous les messages du journal de la console EC2Launch v2.

```
Message: Error EC2Launch service is stopping. {error message}
 Error setting up EC2Launch agent folders
 See instance logs for detail
 Error stopping service
 Error initializing service
Message: Windows sysprep configuration complete
Message: Invalid administrator username: {invalid username}
Message: Invalid administrator password
Username: {username}
```

```
Password: <Password>{encrypted password}</Password>
AMI Origin Version: {amiVersion}
AMI Origin Name: {amiName}
Microsoft Windows NT {currentVersion}.{currentBuildNumber}
OsVersion: {currentVersion}
OsProductName: {productName}
OsBuildLabEx: {buildLabEx}
OsCurrentBuild: {currentBuild}
OsReleaseId: {releaseId}
Language: {language}
TimeZone: {timeZone}
Offset: UTC {offset}
Launch agent: EC2Launch {BuildVersion}
AMI-ID: {amiId}
Instance-ID: {instanceId}
Instance Type: {instanceType}
RDPCERTIFICATE-SUBJECTNAME: {certificate subject name}
RDPCERTIFICATE-THUMBPRINT: {thumbprint hash}
SqlServerBilling: {sql billing}
SqlServerInstall: {sql patch leve, edition type}
Driver: AWS NVMe Driver {version}
Driver: Inbox NVMe Driver {version}
Driver: AWS PV Driver Package {version}
Microsoft-Hyper-V is installed.
Unable to get service status for vmms
Microsoft-Hyper-V is {status}
SSM: Amazon SSM Agent {version}
AWS VSS Version: {version}
Message: Windows sysprep configuration complete
Message: Windows is being configured. SysprepState is {state}
Windows is still being configured. SysprepState is {state}
Message: Windows is Ready to use
Message: Waiting for meta-data accessibility...
Message: Meta-data is now available.
Message: Still waiting for meta-data accessibility...
Message: Failed to find primary network interface...retrying...
User data format: {format}
```

EC2Launchhistorique des versions de la v2

Historique des versions

- EC2Launchhistorique des versions v2
- EC2Launchhistorique des versions de l'outil de migration v2

EC2Launchhistorique des versions v2

Le tableau suivant décrit les versions publiées de la EC2Launch v2.

Version	Détails	Date de publication
2,0,1981	• Messages d'erreur de `EC2Launch.exe` CLI commande mis à jour pour les utilisateurs non administrateurs.	6 juillet 2024
2,0,1948	• Ajout de la télémétrie pour surveiller l'utilisation des options de mot de passe d'administrateur. • EC2LaunchPermissions modifiées.	1er juillet 2024
2,0,1924	• Mise à jour de l'interface utilisateur des EC2Launch paramètre s. • Mise à jour de la CLI commande de fond d'écran. • Mise à jour du EC2Launch programme d'installation.	10 juin 2024
2,0,114	• Ajoutez des itinéraires avec des adresses de passerelle non spécifiées (`0.0.0.0`pour IPv4 ou `::` pourIPv6). • Ajoutez toujours les deux IPv4 et IPv6 les itinéraires. • Correction d'un problème en raison duquel le `Administr ator` nom d'utilisateur était ajouté au `agent-config.yml` fichier alors qu'il n'était pas spécifié. • Permissions EC2Launch v2 modifiées.	5 juin 2024
2,0,1881	• Ajout d'une option de mot de passe crypté à `setAdminA ccount` la tâche. •	8 mai 2024

Version	Détails	Date de publication
	Ajout d'une CLI commande pour chiffrer le mot de passe statique dans agent-config.yml. • Correction d'un problème en raison duquel les données XML utilisateur n'ajoutaient pas d' PowerShell arguments lorsqu'el les étaient exécutées avec des autorisations d'administrateur. Pour en savoir plus, consultez Comment Amazon EC2 gère les données utilisateur pour les instances Windows. • PowerShell Arguments ajustés pour les scripts de `executeScript` tâche et de données utilisateur lorsqu'ils sont exécutés avec `LocalSystem` des autorisations. Lorsque les arguments sont vides, l'agent utilise la valeur par défaut suivante : `-ExecutionPolicy Unrestricted` • Impossible d'imprimer des versions de pilotes dupliquées dans le journal de la console.	
2,0,1815	• Gestion des erreurs ajustée pour échouer en cas de problèmes de configuration critiques avant Sysprep. • Correction d'un problème en raison duquel les tâches de fond d'écran et de nom d'hôte pouvaient utiliser une adresse IP incorrecte sur les instances où plusieurs adresses IP étaient attribuées à l'interface réseau principale. • Les tâches de fond d'écran et de nom d'hôte ont d'IMDSabord été modifiées pour obtenir une adresse IP privée, puis elles sont retournées à la WMI case IMDS désactivée. • Correction d'un problème lié à la `initializeVolume` tâche qui `sc1` empêchait l'initialisation des volumes en raison d'une erreur transitoire.	6 mars 2024

Version	Détails	Date de publication
2,0,1739	• Correction d'un problème qui empêchait les codes de sortie d'être capturés par `executeScript` des tâches exécutées en tant qu'administrateur Windows.	17 janvier 2024
2,0.1702	• Autorisations `Telemetry.log` limitées de `read-execute` uniquement pour les utilisateurs standard. • Configuré le service EC2Launch Windows pour qu'il redémarre en cas d'échec du démarrage. • Défaillances `add-routes` rendues exploitables en enregistr ant les résultats `route.exe stderr`. • Correction d'un problème qui se produisait lorsque les métriques d'itinéraire se situaient en dehors de la plage [1-9999]. • Ajout de la prise en charge du fond d'écran à plusieurs nouveaux types d'instance. • Correction d'un problème causé par les scripts de données utilisateur qui s'exécutaient en tant qu'utilisateur administr ateur Windows et envoyaient des résultats à `stderr`.	4 janvier 2024

Version	Détails	Date de publication
2,0,1643	• Mise à jour de l'outil `ebsnvme-id.exe` vers la version 1.1.0.7. • Correction d'un problème lié aux paramètres de dimension nement côté réception (RSS) et de profondeur de file d'attente de réception sur les types d'instances métalliques commençan t par « metal-* », tels que metal-48x1. • Evénement de télémétrie qui signalait les commandes XML userdata bloquant l'agent a été supprimé. • Mise à jour de la tâche `setDnsSuffix` pour limiter la dévolution des noms de domaine en fonction de l'entrée dans le registre :`HKEY_LOCAL_MACHINE\System\C urrentControlSet\Services\Dnscache\P arameters\DomainNameDevolutionLevel` . • Ajout d'une tâche publique CLI qui ajoute des routes réseau. • Remarque : cette version est officiellement la dernière à être compatible avec Windows Server 2012. • Remarque : cette version est officiellement la dernière à être compatible avec les systèmes d'exploitation 32 bits.	4 octobre 2023
2,0.1580	• Modification de la façon dont l'agent de lancement gère les erreurs lorsque vous modifiez les autorisations du fichier journal. • Ajout d'un délai d'attente pour la connexion au port série. Le délai d'attente permet à l'agent de lancement de continuer à fonctionner si le port série est utilisé.	5 septembre 2023

Version	Détails	Date de publication

2,0,1521	• L'indicateur –`block` des commandes `EC2Launch.exe` , reset et sysprep est devenu obsolète.
	• Mise à jour de `EC2Launch.exe` pour détecter et gérer les commandes reset et sysprep utilisées dans les tâches `executeScript` en ligne. Ces commandes interrompent l'exécution de l'agent une fois la tâche `executeScript` exécutée.
	• Scripts de XML données utilisateur mis à jour pour qu'ils s'exécutent en ligne par défaut.
	• Activez XML les scripts userdata pour qu'ils s'exécutent indépendamment avec la nouvelle `detach` balise. Pour en savoir plus, consultez Scripts de données utilisateur.
	• A apporté les modifications suivantes au journal de l'agent.
	  • Messages du journal de l'agent mis à jour.
	  • Contenu `executeScript` et sortie supprimés du journal de l'agent.
	  • Arguments `executeProgram` et sortie supprimés du journal de l'agent.
	• A apporté les modifications suivantes au journal de la console.
	  • Valeur `EnableSCSIPersistentReservations` ajoutée au journal de la console.
		3 juillet 2023

Version	Détails	Date de publication
2,0.1303	• Ajout d'une gestion des erreurs et de lignes de journal supplémentaires lors de l'ajout d'itinéraires réseau. • `executeScript` Autorisés et `executeProgram` tâches en cours de PreReady stage. • `executeProgram` Tâche mise à jour pour générer des fichiers de sortie similaires à ceux de la executeScript tâche. Pour de plus amples informations, veuillez consulter executeProgram. • Ajout de la télémétrie pour surveiller l'utilisation des commandes de l'agent de blocage dans les données XML utilisateur.	3 mai 2023
2,0.1245	• Visibilité améliorée des incidents en enregistrant les piles d'appels d'incidents en texte clair. • Le EventLog service a été ajouté en tant que dépendance au démarrage pour corriger un crash lorsque le EC2Launch service Amazon démarre plus rapidement que le EventLog service. • A fait exécuter les données XML utilisateur avant l' PostReady étape à partir du fichier de configuration de l'agent (comme EC2Launch v1 etEC2Config). • Ajout de la version 1.1 des données YAML utilisateur pour que les données utilisateur soient exécutées avant l' PostReady étape à partir du fichier de configuration de l'agent (la version 1.0 des données YAML utilisateur s'exécute après l' PostReady étape à partir du fichier de configuration de l'agent).	8 mars 2023

Version	Détails	Date de publication
2,0.1173	• Ajoute une fonction facultative pour afficher les balises d'instance sur le fond d'écran. Pour de plus amples informations, veuillez consulter setWallpaper . • Ajoute la gestion des erreurs lorsque le groupe de sécurité pour Elastic Graphics n'est pas correctement configuré. • Corrige un délai d'expiration lorsque le service de métadonnées d'instance n'est pas activé.	6 février 2023
2,0.1121	• Résout un problème selon lequel une erreur 404 est imprimée sur le fond d'écran lorsqu'aucune IPv4 adresse publique n'est attribuée. • Corrige un problème où le système de fichiers du volume est formaté en `RAW` au lieu de `NTFS` lorsque la lettre de lecteur de son périphérique est définie sur `D`. • Résout un problème d'identification incorrecte des NVMe SSD volumes en tant que EBS volumes. • Corrige une erreur lors de l'activation de Windows lorsqu'IMDSil est désactivé.	4 janvier 2023

Version	Détails	Date de publication
2,0.1082	• Résout un problème selon lequel le `privateIpAddress` champ `setWallpaper` : est vide lorsqu'il IMDS est désactivé. • Résout un problème lié à la définition du nom d'hôte sur l'IPv4adresse privée lorsque cette option IMDS est désactivée. • Corrige un problème lié à l'initialisation des volumes sous Windows Server 2012. • Corrige un problème lié à la définition des trames Jumbo. • Corrige une erreur lorsqu'aucune SSH clé n'est spécifiée au lancement de l'instance. • Corrige une erreur sur Windows Server 2012 lorsque Windows ne possède pas de clé de registre ReleaseId « ».	7 décembre 2022
2,0.1011	• Corrige la logique de recherche de l'adaptateur réseau lorsque le P nPDevice ID est vide.	11 novembre 2022
2,0.1009	• Utilise les informations du PCI segment pour sélectionner le port de console.	8 novembre 2022

Version	Détails	Date de publication
2,0.982	• Ajoute une logique de nouvelle tentative pour obtenir des RDP informations. • Corrige les erreurs lors de l'initialisation du volume sur les instances `d2.8xlarge` . • Corrige les problèmes liés à la sélection d'une carte réseau incorrecte après un redémarrage. • Supprime le message d'erreur de fausse alarme lorsqu'il ACPI SPCR n'est pas disponible.	31 octobre 2022
2,0.863	• Met à jour la logique d'IMDSattente pour ne faire que IMDSv2 des demandes. • Ajoute une logique pour attribuer une lettre de lecteurs aux volumes déjà initialisés, mais non montés. • Affiche un message d'erreur plus spécifique lorsque le type de paire de clés n'est pas pris en charge. • Corrige le bogue de code de redémarrage 3010. • Ajoute la vérification de la validité des données utilisateur encodées en base64.	6 juillet 2022
2,0,698	• Corrige la faute d'orthographe dans la sortie du journal lors de l'exécution de scripts.	30 janvier 2022

Version	Détails	Date de publication
2,0,674	• La télémétrie charge le contrôle de confidentialité activé/dé sactivé. • Corrige le bogue `index out of bounds`. • Supprime les raccourcis de fond d'écran pendant `sysprep`.	15 novembre 2021
2,0,651	• Ajoute une logique pour désinstaller les anciens agents lors de l'installation EC2Launch de la version 2. • Résout le `list-volume` CLI problème lorsque le volume racine n'est pas répertorié comme volume 0.	7 octobre 2021
2,0,592	• Corrige un bug pour signaler correctement l'état de l'étape. • Supprime les faux messages d'alarme lorsque les fichiers journaux sont fermés. • Ajoute la télémétrie.	31 août 2021
2,0.548	• Ajout de zéros de début pour le nom d'hôte IP hexadécimal • Correction des autorisations de fichier pour la tâche `enableOpenSsh` . • Correction du plantage de la commande sysprep.	4 août 2021

Version	Détails	Date de publication
2,0,470	• Corrige un bogue au niveau du réseau DHCP qui empêchait d'attribuer une adresse IP à l'instance. • Correction d'un bug avec `setDnsSuffix` lorsque la clé de registre `SearchList` n'existe pas. • Corrige un bogue dans DNS la logique de dévolution dans. `setDnsSuffix` • Ajout des itinéraires réseau après les redémarrages intermédiaires. • Autorise `initializeVolume` à réécrire les volumes existants. • Supprime les informations supplémentaires de la sous-commande de version.	20 juillet 2021
2.0.285	• Ajoute une option pour exécuter des scripts utilisateur dans un processus détaché. • Les anciennes données utilisateur (XMLuserdata) s'exécutent désormais dans le cadre d'un processus détaché, dont le comportement est similaire à celui de l'agent de lancement précédent. • Ajoute un CLI indicateur aux `reset` commandes `sysprep` et, ce qui leur permet de bloquer jusqu'à ce que le service s'arrête. • Restreint les autorisations du dossier de configuration.	8 mars 2021

Version	Détails	Date de publication
2.0.207	• Ajoute un champ `hostName` facultatif à la tâche `setHostName` . • Correction du bogue de redémarrage. Les tâches de redémarrage `executeScript` et `executeProgram` seront marquées comme étant en cours d'exécution. • Ajoute d'autres codes de retour à la commande d'état. • Ajoute un service d'amorçage pour résoudre le problème de démarrage lors de l'exécution sur le type d'instance `t2.nano`. • Corrige le mode d'installation propre pour supprimer les fichiers non suivis par le programme d'installation.	2 février 2021
2.0.160	• Corrige la commande `validate` pour qu'elle détecte les noms d'étape non valides. • Ajoute la commande `w32tm resync` dans la tâche `addroutes` . • Résout le problème lié à la modification de l'ordre de recherche des DNS suffixes. • Ajoute des conditions de vérification pour mieux signaler les données utilisateur invalides.	4 décembre 2020
2.0.153	Ajoute la fonctionnalité Sysprep dans. UserData	3 novembre 2020

Version	Détails	Date de publication
2.0.146	• Résout un problème lié à une langue RootExtend autre que l'anglaisAMIs. • Donne aux utilisateurs l'autorisation d'écriture de groupe pour les fichiers journaux. • Crée une partition MS Reserved pour les GPT volumes. • Ajoute la commande list-volumes et la liste déroulante des volumes dans les paramètres Amazon. EC2Launch • Ajoute une get-agent-config commande pour imprimer le fichier agent-config.yml au format yaml ou json. • Efface le mot de passe statique si aucune clé publique n'a été détectée.	6 octobre 2020
2.0.124	• Ajoute l'option pour afficher la version du système d'exploit ation sur le fond d'écran. • Initialise les EBS volumes chiffrés. • Ajoute des itinéraires pour VPCs les personnes sans DNS nom local.	10 septembre 2020
2.0.104	• Crée une liste de recherche de DNS suffixes si elle n'existe pas. • Ignore la mise en veille prolongée si elle n'est pas demandée.	12 août 2020
2.0.0	Première version.	30 juin 2020

EC2Launchhistorique des versions de l'outil de migration v2

Le tableau suivant décrit les versions publiées de l'outil de migration EC2Launch v2.

Vous pouvez recevoir des notifications lorsque de nouvelles versions de l'agent EC2Launch v2 sont publiées. Pour de plus amples informations, veuillez consulter Abonnez-vous aux notifications de l'agent de lancement EC2 Windows.

Version	Détails	Date de publication
1,0413	• Mettre à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1981.	9 août 2024
1,0412	• Mettez à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1948.	7 août 2024
1,0,396	• Mettez à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1924.	11 juin 2024
1,0,394	• Mettez à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1914.	6 juin 2024
1,0,384	• Mettez à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1881.	8 mai 2024
1,0,358	• Mettez à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1815.	8 mars 2024
1,0,345	• Mettez à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1739.	18 janvier 2024
1,0,342	• Mettez à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1702.	5 janvier 2024

Version	Détails	Date de publication
1,0,331	• Mettre à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1643 • Correction d'une erreur qui se produit lors de l'exécution de `.Install.ps1 -DryRun` . • Correction d'un problème en raison duquel la configuration du mot de passe n'est pas correctement définie `random` pendant la migration depuisEC2Config. • Corrigez une erreur qui se produit s'`setWallpaper` il est défini sur `False` lors de la migration depuisEC2Launch.	3 novembre 2023
1,0,303	Mettez à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1580.	14 septembre 2023
1,0,286	Mettez à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1521.	14 juillet 2023
1,0,272	Mettez à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1303.	3 mai 2023
1,0,262	Mettez à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1245.	9 mars 2023
1,0,241	Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.1011.	7 décembre 2022
1,0,218	• Valide la valeur de région extraite des métadonnées de l'instance. • Corrige un bogue d'échec de migration dans les modules linguistiques. • Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.863.	3 septembre 2022

Version	Détails	Date de publication
100,162	• Déplace la logique de suppression des anciens agents vers la EC2Launch v2MSI. • Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.698.	18 mars 2022
100,136	Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.651.	13 octobre 2021
100,130	Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.548.	5 août 2021
100,113	Utilisations IMDSv2 à la place deIMDSv1.	4 juin 2021
1.0.101	Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.285.	12 mars 2021
1.0.86	Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.207.	3 février 2021
1.0.76	Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.160.	4 décembre 2020
1.0.69	Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.153.	5 novembre 2020
1.0.65	Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.146.	9 octobre 2020
1.0.60	Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.124.	10 septembre 2020

Version	Détails	Date de publication
1.0.54	• Installe la EC2Launch version 2 si aucun agent n'est installé. • Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.104. • Découple l'agent. SSM	12 août 2020
1.0.50	Supprime NuGet la dépendance.	10 août 2020
1.0.0	Première version.	30 juin 2020

Utiliser l'agent EC2Launch v1 pour effectuer des tâches lors du lancement de l'instance EC2 Windows

EC2Launchest un ensemble de PowerShell scripts Windows qui a remplacé le EC2Config service sur Windows Server 2016 et 2019AMIs. Beaucoup d'entre eux AMIs sont toujours disponibles. EC2Launchv2 est le dernier agent de lancement pour toutes les versions de Windows prises en charge, qui remplace à la fois EC2Config etEC2Launch. Pour de plus amples informations, veuillez consulter Utiliser l'agent EC2Launch v2 pour effectuer des tâches lors du lancement de l'instance EC2 Windows.

> **Note**
>
> Pour être utilisée EC2Launch avecIMDSv2, la version doit être 1.3.2002730 ou ultérieure.

Vous pouvez utiliser la PowerShell commande Windows suivante pour vérifier la version installée deEC2Launch.

```
Test-ModuleManifest -Path "C:\ProgramData\Amazon\EC2-Windows\Launch\Module
\Ec2Launch.psd1" | Select Version
```

EC2Launchtâches

EC2Launchexécute les tâches suivantes par défaut lors du démarrage initial de l'instance :

- Configure un nouveau fond d'écran qui présente les informations relatives à l'instance.
- Définit le nom de l'ordinateur comme étant l'IPv4adresse privée de l'instance.
- Envoie les informations de l'instance à la EC2 console Amazon.
- Envoie l'empreinte numérique du RDP certificat à la EC2 console.
- Définit un mot de passe aléatoire pour le compte d'administrateur.
- Ajoute des DNS suffixes.
- Etend de manière dynamique la partition du système d'exploitation pour inclure l'espace non partitionné.
- Exécute les données utilisateur (si spécifié). Pour plus d'informations sur la spécification de données utilisateur, consultez Exécuter des commandes lorsque vous lancez une EC2 instance avec saisie de données utilisateur.
- Définit des itinéraires statiques persistants pour atteindre le service de métadonnées et AWS KMS les serveurs.

> **Important**
>
> Si une configuration personnalisée AMI est créée à partir de cette instance, ces routes sont capturées dans le cadre de la configuration du système d'exploitation et toutes les nouvelles instances lancées à partir de cette instance AMI conserveront les mêmes routes, quel que soit l'emplacement du sous-réseau. Pour mettre à jour les routes, consultez Mettre à jour les KMS métadonnées/routes pour Server 2016 et versions ultérieures lors du lancement d'une version personnalisée AMI.

Les tâches suivantes permettent de maintenir la rétrocompatibilité avec le EC2Config service. Vous pouvez également configurer EC2Launch pour effectuer les tâches suivantes au démarrage :

- Initialisez les EBS volumes secondaires.
- Envoyez les journaux d'événements Windows aux journaux de la EC2 console.
- Envoyez le message Windows est prêt à être utilisé à la EC2 console.

Pour plus d'informations concernant Windows Server 2019, consultez la page relative à la comparaison des fonctions dans les versions de Windows Server sur Microsoft.com.

Structure de répertoire EC2Launch

EC2Launchest installé par défaut sur Windows Server 2016 et versions ultérieures AMIs dans le répertoire racine`C:\ProgramData\Amazon\EC2-Windows\Launch`.

> **Note**
>
> Par défaut, Windows masque les fichiers et les dossiers qui se trouvent sous `C:\ProgramData`. Pour afficher les EC2Launch répertoires et les fichiers, vous devez saisir le chemin dans l'Explorateur Windows ou modifier les propriétés du dossier pour afficher les fichiers et dossiers cachés.

Le répertoire `Launch` contient les sous-répertoires suivants.

- `Scripts`— Contient les PowerShell scripts qui le composentEC2Launch.
- `Module`— Contient le module permettant de créer des scripts liés à AmazonEC2.
- `Config` — Contient les fichiers de configuration de script que vous pouvez personnaliser.
- `Sysprep` — Contient les ressources Sysprep.
- `Settings` — Contient une application pour l'interface utilisateur graphique de Sysprep.
- `Library`— Contient des bibliothèques partagées pour les agents de EC2 lancement.
- `Logs` — Contient les fichiers journaux générés par des scripts.

Télémétrie

La télémétrie est une information supplémentaire qui permet de mieux AWS comprendre vos besoins, de diagnostiquer les problèmes et de fournir des fonctionnalités pour améliorer votre expérience avec AWS les services.

EC2Launchversion `1.3.2003498` et versions ultérieures collectent des données télémétriques, telles que les métriques d'utilisation et les erreurs. Ces données sont collectées à partir de l'EC2instance Amazon sur laquelle EC2Launch s'exécute. Cela inclut tous les appareils Windows AMIs détenus par AWS.

Les types de télémétrie suivants sont collectés par : EC2Launch

- Usage information (Informations d'utilisation) : commandes de l'agent, méthode d'installation et fréquence d'exécution planifiée.

- Errors and diagnostic information (Erreurs et informations de diagnostic) : installation de l'agent et exécution des codes d'erreur.

Exemples de données collectées :

```
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsUserDataScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandCode=1
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandErrorCode=5
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallCode=2
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallErrorCode=0
```

La télémétrie est activée par défaut. Vous pouvez désactiver la collecte de données de télémétrie à tout moment. Si la télémétrie est activée, EC2Launch envoie les données de télémétrie sans notification supplémentaire au client.

Le choix d'activer ou de désactiver la télémétrie est collecté.

Vous pouvez choisir de vous inscrire ou de vous désinscrire de la collecte de télémétrie. Votre choix est collecté afin de nous assurer que nous le respectons.

Visibilité de la télémétrie

Lorsque la télémétrie est activée, elle apparaît dans la sortie de EC2 la console Amazon comme suit :

```
2021/07/15 21:44:12Z: Telemetry: <Data>
```

Désactiver la télémétrie sur une instance

Pour désactiver la télémétrie en paramétrant une variable d'environnement système, exécutez la commande suivante en tant qu'administrateur :

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Pour désactiver la télémétrie pendant l'installation, exécutez `install.ps1` comme suit :

```
. .\install.ps1 -EnableTelemetry:$false
```

Plus de sujets pour EC2Launch

- Installez la dernière version de EC2Launch

- Configurer l'agent EC2Launch v1 sur votre instance Windows
- Historique des versions EC2Launch

Installez la dernière version de EC2Launch

Suivez la procédure ci-dessous pour télécharger et installer la dernière version de EC2Launch sur vos instances.

Pour télécharger et installer la dernière version de EC2Launch

1. Si vous avez déjà installé et configuré EC2Launch une instance, effectuez une sauvegarde du fichier de EC2Launch configuration. Le processus d'installation ne conserve pas les modifications de ce fichier. Par défaut, le fichier se trouve dans le répertoire `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. Téléchargez le EC2fichier -Windows-Launch.zip dans un répertoire de l'instance.
3. Téléchargez install.ps1 dans le répertoire dans lequel vous avez téléchargé `EC2-Windows-Launch.zip`.
4. Exécutez `install.ps1`
5. Si vous avez effectué une sauvegarde du fichier de EC2Launch configuration, copiez-le `C:\ProgramData\Amazon\EC2-Windows\Launch\Config` dans le répertoire.

Pour télécharger et installer la dernière version d'EC2Launchutilisation PowerShell

Si vous avez déjà installé et configuré EC2Launch une instance, effectuez une sauvegarde du fichier de EC2Launch configuration. Le processus d'installation ne conserve pas les modifications de ce fichier. Par défaut, le fichier se trouve dans le répertoire `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Pour installer la dernière version de EC2Launch using PowerShell, exécutez les commandes suivantes depuis une PowerShell fenêtre

```
mkdir $env:USERPROFILE\Desktop\EC2Launch
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/EC2-Windows-Launch.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/install.ps1"
```

```
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $Url -
Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
& $env:USERPROFILE\Desktop\EC2Launch\install.ps1
```

> **Note**
>
> Si un message d'erreur s'affiche lors du téléchargement du fichier et que vous utilisez Windows Server 2016, il est possible que vous deviez activer la version TLS 1.2 sur votre PowerShell terminal. Vous pouvez activer la TLS version 1.2 pour la PowerShell session en cours à l'aide de la commande suivante, puis réessayer :
>
> ```
> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
> ```

Vérifiez l'installation en vérifiant l'agent de lancement comme suit.

```
Import-Module C:\ProgramData\Amazon\EC2-Windows\Launch\Module\Ec2Launch.psm1
Import-LocalizedData -BaseDirectory C:\ProgramData\Amazon\EC2-Windows\Launch\Module\ -
FileName 'Ec2Launch.psd1' -BindingVariable moduleManifest
$moduleManifest.Get_Item('ModuleVersion')
```

Configurer l'agent EC2Launch v1 sur votre instance Windows

Une fois que votre instance a été initialisée pour la première fois, vous pouvez la configurer EC2Launch pour qu'elle soit réexécutée et effectuer différentes tâches de démarrage.

Tâches

- Configuration des tâches d'initialisation
- Programmez EC2Launch pour une exécution à chaque démarrage
- Initialisation des disques et mappage des lettres de lecteur
- Envoyer les journaux d'événements Windows à la EC2 console
- Envoi du message « Windows Is Ready » après un démarrage réussi

Configuration des tâches d'initialisation

Spécifiez les paramètres dans le fichier `LaunchConfig.json` pour activer ou désactiver les tâches d'initialisation suivantes :

- Définissez le nom de l'ordinateur sur l'IPv4adresse privée de l'instance.
- Réglez le moniteur pour qu'il reste toujours en fonction.
- Configurer un nouveau fond d'écran
- Ajoutez une liste de DNS suffixes.

> **Note**
>
> Cela ajoute une recherche de DNS suffixe pour le domaine suivant et configure d'autres suffixes standard. Pour plus d'informations sur la façon dont les agents de lancement définissent les DNS suffixes, consultez. Configurer le DNS suffixe pour les agents de lancement EC2 Windows
>
> ```
> region.ec2-utilities.amazonaws.com
> ```

- Elargir la taille de volume de démarrage
- Définir le mot de passe de l'administrateur

Pour configurer les paramètres d'initialisation

1. Dans l'instance à configurer, ouvrez le fichier suivant `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\LaunchConfig.json` dans un éditeur de texte.
2. Mettez à jour les paramètres suivants au besoin et enregistrez vos modifications. Indiquez un mot de passe dans `adminPassword` uniquement si `adminPasswordtype` est `Specify`.

```
{
 "setComputerName": false,
 "setMonitorAlwaysOn": true,
 "setWallpaper": true,
 "addDnsSuffixList": true,
 "extendBootVolumeSize": true,
 "handleUserData": true,
 "adminPasswordType": "Random | Specify | DoNothing",
 "adminPassword": "password that adheres to your security policy (optional)"
}
```

Les types de mots de passe sont définis comme suit :

`Random`

EC2Launchgénère un mot de passe et le chiffre à l'aide de la clé de l'utilisateur. Le système désactive ce paramètre après le lancement de l'instance afin que ce mot de passe persiste si l'instance est redémarrée, arrêtée ou démarrée.

`Specify`

EC2Launchutilise le mot de passe que vous spécifiez dans`adminPassword`. Si le mot de passe ne répond pas aux exigences du système, EC2Launch génère un mot de passe aléatoire à la place. Le mot de passe est stocké dans le fichier `LaunchConfig.json` sous forme de texte clair et est supprimé une fois que le mot de passe est défini par Sysprep. EC2Launchchiffre le mot de passe à l'aide de la clé de l'utilisateur.

`DoNothing`

EC2Launchutilise le mot de passe que vous avez indiqué dans le `unattend.xml` fichier. Si vous ne spécifiez pas de mot de passe dans `unattend.xml`, le compte d'administrateur est désactivé.

3. Dans Windows PowerShell, exécutez la commande suivante pour planifier l'exécution du script en tant que tâche planifiée Windows. Le script s'exécute une seule fois lors du prochain démarrage, puis désactive toute nouvelle exécution de ces tâches.

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
```

Programmez EC2Launch pour une exécution à chaque démarrage

Vous pouvez planifier EC2Launch l'exécution à chaque démarrage au lieu de vous limiter au démarrage initial.

Pour activer EC2Launch l'exécution à chaque démarrage :

1. Ouvrez Windows PowerShell et exécutez la commande suivante :

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
SchedulePerBoot
```

2. Ou exécutez le fichier exécutable avec la commande suivante :

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Settings\Ec2LaunchSettings.exe
```

Ensuite, sélectionnez `Run EC2Launch on every boot`. Vous pouvez spécifier que votre EC2 instance `Shutdown without Sysprep` ou`Shutdown with Sysprep`.

> **Note**
>
> Lorsque vous activez EC2Launch l'option d'exécution à chaque démarrage, les événements suivants se produisent lors de la prochaine EC2Launch exécution :
>
> - S'il `AdminPasswordType` est toujours défini sur`Random`, un nouveau mot de passe EC2Launch sera généré au prochain démarrage. Après ce démarrage, `AdminPasswordType` il est automatiquement configuré sur `DoNothing` pour empêcher la génération EC2Launch de nouveaux mots de passe lors des démarrages suivants. Pour éviter EC2Launch de générer un nouveau mot de passe lors du premier démarrage, `AdminPasswordType` réglez-le manuellement `DoNothing` avant le redémarrage.
> - `HandleUserData` sera redéfini sur `false` sauf si `persist` est défini sur `true` pour les données utilisateur. Pour de plus amples informations, veuillez consulter the section called "Scripts de données utilisateur".

Initialisation des disques et mappage des lettres de lecteur

Spécifiez les paramètres du `DriveLetterMappingConfig.json` fichier pour associer les lettres du lecteur aux volumes de votre EC2 instance. Le script initialise les lecteurs qui ne sont pas encore initialisés et partitionnés. Pour plus d'informations sur l'obtention de détails sur les volumes sous Windows, veuillez consulter Get-Volume (français non garanti) dans la documentation Microsoft.

Pour mapper les lettres de lecteur avec les volumes

1. Ouvrez le fichier `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` dans un éditeur de texte.
2. Spécifiez les paramètres de volume suivants et enregistrez vos modifications :

```
{
 "driveLetterMapping": [
  {
```

```
    "volumeName": "sample volume",
    "driveLetter": "H"
   }
  ]
}
```

3. Ouvrez Windows PowerShell et utilisez la commande suivante pour exécuter le EC2Launch script qui initialise les disques :

   ```
   C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
   ```

   Pour initialiser les disques chaque fois que l'instance démarre, ajoutez l'indicateur `-Schedule` comme suit :

   ```
   C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -Schedule
   ```

Envoyer les journaux d'événements Windows à la EC2 console

Spécifiez les paramètres du `EventLogConfig.json` fichier pour envoyer les journaux d'événements Windows aux journaux de EC2 console.

Pour configurer les paramètres permettant d'envoyer les journaux d'événements Windows

1. Sur l'instance, ouvrez le fichier `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\EventLogConfig.json` dans un éditeur de texte.
2. Configurez les paramètres de journaux suivants au besoin et enregistrez vos modifications.

   ```
   {
    "events": [
     {
      "logName": "System",
      "source": "An event source (optional)",
      "level": "Error | Warning | Information",
      "numEntries": 3
     }
    ]
   }
   ```

3. Sous Windows PowerShell, exécutez la commande suivante afin que le système planifie l'exécution du script en tant que tâche planifiée Windows à chaque démarrage de l'instance.

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendEventLogs.ps1 -Schedule
```

Les journaux peuvent prendre trois minutes ou plus pour apparaître dans les journaux de la EC2 console.

Envoi du message « Windows Is Ready » après un démarrage réussi

Le EC2Config service a envoyé le message « Windows est prêt » à la EC2 console après chaque démarrage. EC2Launchenvoie ce message uniquement après le démarrage initial. Pour des raisons de rétrocompatibilité avec le EC2Config service, vous pouvez planifier EC2Launch l'envoi de ce message après chaque démarrage. Sur l'instance, ouvrez Windows PowerShell et exécutez la commande suivante. Le système programme le script pour s'exécuter en tant que tâche planifiée Windows.

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendWindowsIsReady.ps1 -Schedule
```

Historique des versions EC2Launch

AMIsÀ partir de Windows Server 2016, Windows inclut un ensemble de scripts Windows Powershell appelésEC2Launch. EC2Launchexécute des tâches lors du démarrage initial de l'instance. Pour plus d'informations sur les EC2Launch versions incluses dans AWS WindowsAMIs, consultez l'historique des AMI versions de AWS Windows.

Pour télécharger et installer la dernière version deEC2Launch, voirInstallez la dernière version de EC2Launch.

Vous pouvez recevoir des notifications lorsque de nouvelles versions de l'EC2Launchagent sont publiées. Pour de plus amples informations, veuillez consulter Abonnez-vous aux notifications de l'agent de lancement EC2 Windows.

Le tableau suivant décrit les versions publiées deEC2Launch. Notez que le format de version a changé après la version 1.3.610.

Version	Détails	Date de publication
1,3.2005008	•	6 août 2024

Version	Détails	Date de publication
	Mis `Set-Wallpaper` à jour pour revenir à un arrière-plan de couleur unie si l'image de fond d'écran par défaut n'est pas trouvée.	
1,3.2004959	• Logique d'installation mise à jour pour empêcher toute installation non prise en charge sur Windows Server 2025 ou version ultérieure.	2 juillet 2024
1,3.2004891	• Correction d'un problème en raison duquel le paramètre n'`HandleUserData` était pas réglé `false` comme prévu. • Ajout d'une option `Encrypted` de mot de passe à`LaunchConfig.json` . • `Settings UI`Comportement modifié pour chiffrer le mot de passe spécifié par l'utilisateur par défaut. • Ajouté `SetAdminPasswordConfig.ps1` pour convertir l'option de `Specify` mot de passe en option de `Encrypted` mot de passe dans le fichier de configuration de l'agent.	31 mai 2024
1,3.2004617	• Correction d'une erreur lors du réglage du fond d'écran.	15 janvier 2024

Version	Détails	Date de publication
1,3.2004592	• Autorisations d'accès mises à jour définies par install.ps1 pour `%ProgramData%\Amazon\EC2-Windows\Launch` . • Accès restreint aux EC2Launch dossiers/fichiers en lecture et en exécution uniquement pour les comptes utilisateur standard. • Modification de l'agent pour arrêter d'attendre que le service de métadonnées d'instance (IMDS) s'initialise s'il n'IMDSest pas activé pour l'instance. • Ajout d'un délai d'attente de cinq minutes en attendant l'IMDSinitialisation. • Modification de l'agent pour qu'il enregistre la télémétrie dans le journal de la console de l'instance avant le message `Windows is Ready` plutôt qu'après. • Ajout de la prise en charge du fond d'écran à plusieurs nouveaux types d'instance. Pour plus d'informations sur les autorisations d'accès et les autorisations de compte utilisateur pour EC2Launch les annuaires, consultezthe section called "Structure de répertoire EC2Launch".	2 janvier 2024
1,3.2004491	• Ajout d'une télémétrie pour surveiller l'utilisation de l'option Spécifier le mot de passe administrateur.	9 novembre 2023
1,3.2004462	• Ajout d'un vidage après chaque écriture sur la console série.	18 octobre 2023

Version	Détails	Date de publication
1,3.2004438	• Limite la dévolution des noms de domaine en fonction de l'entrée dans le registre : `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Autorisations `UserdataExecution.log` limitées à `Administrators` uniquement. • Des messages d'erreur ont été ajoutés dans le journal des événements Windows en cas d'échec de l'initialisation du journal.	4 octobre 2023
1,3.2004256	• Valeur `EnableSCSIPersistentReservations` ajoutée au journal de la console. • Capacité de nouvelle tentative ajoutée pour Get-ConsolePort.	7 juillet 2023
1,3.2004052	• Correction d'une erreur qui se produisait lorsqu'aucune SSH clé n'était spécifiée au lancement de l'instance. • Mise à jour pour réessayer de démarrer le service mazonSSMAgent Windows A en cas d'échec. • Mis à jour pour échouer SysprepInstance .ps1 si BeforeSysprep .cmd échoue avec un code de sortie différent de zéro.	8 mars 2023
1,3.2003975	• Correction d'un problème affectant les AMI versions de Packer qui `SysprepInstance.ps1` renvoyaient une valeur `$LastErrorCode` de 1.	24 décembre 2022

Version	Détails	Date de publication
1,3.2003961	• Correction d'un problème selon lequel les mots de passe administrateur spécifiés de manière explicite étaient remplacés par un mot de passe aléatoire sur les instances à lancement rapide. • Problème résolu : l'SSMagent ne démarrait pas sur des types d'instances plus petits. • Correction d'un problème en raison duquel le journal de la console de l'instance contient `RDPCERTIFICATE-THUMBPRINT: 0000000000000000000000` au lieu d'une valeur d'empreinte numérique valide le RDP certificat.	6 décembre 2022
1,3.2003923	• Corrige la logique de recherche de l'adaptateur réseau lorsque le P nPDevice ID est vide.	9 novembre 2022
1,3.2003919	• Informations sur les PCI segments « ConsolePort Get-to-use » mises à jour. • Correction d'un problème selon lequel la sélection d'une carte réseau est incorrecte après un redémarrage. • Logique de temporisation de démarrage fixe de SSM l'agent. • Correction de la rétrocompatibilité pour l'alias de AdminCredentials la fonction d'envoi.	8 novembre 2022
1,3.2003857	• Hiérarchise les cartes dotées d'une passerelle par défaut lorsque la carte réseau principale est sélectionnée. • Chiffrement des mots de passe en mémoire étendu.	3 octobre 2022

Version	Détails	Date de publication
1,3.2003824	• Correction d'une erreur pendant `setComputerName` . • Ajout d'une logique permettant d'ignorer l'activation de Windows lorsqu'un code BYOL de facturation est détecté. • Ajout du chiffrement des mots de passe en mémoire. • Correction d'une erreur pendant l'initialisation du volume sur `m6id.4xlarge` .	30 août 2022
1,3.2003691	• Logique IMDS d'attente mise à jour pour ne faire que IMDSv2 des demandes. • Correction d'un bug impactant l'GPUinstallation.	21 juin 2022
1,3.2003639	• Ajout d'une logique d'attente de la carte réseau pour empêcher l'utilisation avant l'initialisation. • Des problèmes mineurs ont été résolus.	10 mai 2022
1,3.2003498	• Ajout de la télémétrie. • Ajout du raccourci vers l'interface utilisateur des paramètres. • PowerShell Scripts formatés. • Le problème d'arrêt survenant avant la fin du BeforeSysprep fichier .cmd a été résolu.	31 janvier 2022
1,3.2003411	Modification de la logique de génération de mot de passe pour exclure les mots de passe de faible complexité.	4 août 2021
1,3.2003364	Installation mise à jour EgpuManager avec IMDSv2 support.	7 juin 2021

Version	Détails	Date de publication
1,3.2003312	• Ajout de lignes de journal avant et après le paramètre `setMonitorAlwaysOn` . • La version du package AWS Nitro Enclaves a été ajoutée au journal de la console.	04 mai 2021
1.3.2003284	Modèle d'autorisation amélioré grâce à la mise à jour de l'emplacement pour stocker les données utilisateur vers `LocalAppData` .	23 mars 2021
1.3.2003236	• Méthode mise à jour pour définir le mot de passe utilisateur dans `Set-AdminAccount` et `Randomize-LocalAdminPassword` . • Correction de `InitializeDisks` pour vérifier si le disque est configuré en lecture seule avant de le définir en écriture.	11 février 2021
1.3.2003210	Correction de localisation pour `install.ps1` .	7 janvier 2021
1.3.2003205	Correction de sécurité pour `install.ps1` pour mettre à jour les autorisations sur le répertoire `%ProgramData%AmazonEC2-WindowsLaunchModuleScripts` .	28 décembre 2020
1.3.2003189	`w32tm resync` ajouté après l'ajout des routes.	4 décembre 2020
1.3.2003155	Informations du type d'instance mises à jour.	25 août 2020
1.3.2003150	Ajout de `OsCurrentBuild` et `OsReleaseId` à la sortie de la console.	22 avril 2020
1.3.2003040	Logique de repli de la IMDS version 1 corrigée.	7 avril 2020
1.3.2002730	Ajout du support pour la IMDS V2.	3 mars 2020
1.3.2002240	Des problèmes mineurs ont été résolus.	31 octobre 2019

Version	Détails	Date de publication
1.3.2001660	Problème de connexion automatique résolu pour les utilisateurs sans mot de passe après la première exécution de SysPrep.	2 juillet 2019
1.3.2001360	Des problèmes mineurs ont été résolus.	27 mars 2019
1.3.2001220	Tous les PowerShell scripts sont signés.	28 février 2019
1.3.2001200	Résolution d'un problème lié au InitializeDisks fichier .ps1 selon lequel l'exécution du script sur un nœud d'un cluster Windows Server Failover formatait les lecteurs situés sur des nœuds distants dont la lettre du lecteur correspondait à la lettre du lecteur local.	27 février 2019
1.3.2001160	Correction du problème de papier peint manquant dans Windows 2019.	22 février 2019
1.3.2001040	• Ajout d'un plugin pour configurer le moniteur pour qu'il ne s'éteigne jamais pour résoudre ACPI les problèmes. • SQLÉdition du serveur et version écrites sur la console.	21 janvier 2019
1.3.2000930	Correctif pour ajouter des routes aux métadonnées sur IPv6 activéENIs.	2 janvier 2019
1.3.2000760	• Ajout de la configuration par défaut RSS et des paramètres de file d'attente de réception pour ENA les appareils. • Désactivation de la mise en veille prolongée lors de Sysprep	5 décembre 2018
1.3.2000630	• Ajout de la route 169.254.169.253/32 pour le serveur. DNS • Ajout d'un filtre pour le paramétrage de l'utilisateur Admin • Améliorations apportées à la mise en veille prolongée d'instances. • Ajout d'une option EC2Launch pour planifier l'exécution à chaque démarrage.	9 novembre 2018

Version	Détails	Date de publication
1.3.2000430.0	• Ajout de la route 169.254.169.123/32 au service horaire. AMZN • Ajout de la route 169.254.169.249/32 au service de licence. GRID • Ajout d'un délai d'attente de 25 secondes lors de la tentative de démarrage de Systems Manager.	19 septembre 2018
1.3.200039.0	• Correction d'un lettrage incorrect des disques pour les EBS NVME volumes. • Ajout d'une journalisation supplémentaire pour les versions NVME du pilote.	15 août 2018
1.3.2000080	Des problèmes mineurs ont été résolus.	
1.3.610	Correction d'un problème lié à la redirection des sorties et des erreurs vers des fichiers à partir de données utilisateur.	
1.3.590	• Ajout de types d'instance manquant dans le papier peint. • Résolution d'un problème de mappage de lettre de lecteur et d'installation de disque.	
1.3.580	• `Get-Metadata` corrigé afin d'utiliser les paramètres de proxy système par défaut pour les demandes web. • Ajout d'un cas spécial pour NVMe l'initialisation du disque. • Des problèmes mineurs ont été résolus.	
1.3.550	Ajout d'une option `-NoShutdown` pour activer Sysprep sans arrêt.	
1.3.540	Des problèmes mineurs ont été résolus.	
1.3.530	Des problèmes mineurs ont été résolus.	
1.3.521	Des problèmes mineurs ont été résolus.	

Version	Détails	Date de publication
1.3.0	• Un problème de longueur hexadécimale a été résolu pour le changement de nom d'ordinateur. • Une éventuelle boucle de redémarrage a été corrigée pour le changement de nom d'ordinateur. • Un problème de configuration du papier peint a été résolu.	
1.2.0	• Mise à jour pour afficher des informations sur le système d'exploitation (OS) installé dans EC2 le journal système. • Mise à jour pour afficher EC2Launch la version de SSM l'agent dans EC2 le journal système. • Des problèmes mineurs ont été résolus.	

Version	Détails	Date de publication
1.1.2	• Mise à jour pour afficher les informations du ENA pilote dans EC2 le journal système. • Mise à jour pour exclure Hyper-V de la logique du NIC filtre principal. • AWS KMS Serveur et port ajoutés dans la clé de registre pour KMS l'activation. • La configuration du papier peint pour plusieurs utilisateurs a été améliorée. • Mise à jour permettant d'effacer les routes du magasin persistant. • Mettez à jour pour supprimer le z de la zone de disponibilité dans la liste des DNS suffixes. • Mise à jour pour résoudre un problème lié à la balise < runAsLocal System> dans les données utilisateur.	
1.1.1	Première version.	

Utiliser le EC2Config service pour effectuer des tâches lors du lancement de EC2 l'ancienne instance du système d'exploitation Windows

> **Note**
>
> EC2Configla documentation est fournie à titre de référence historique uniquement. Les versions du système d'exploitation sur lesquelles il s'exécute ne sont plus prises en charge par Microsoft. Nous vous recommandons vivement de passer à la dernière version de l'agent de lancement.

> Le dernier agent de lancement pour Windows Server 2022 est la EC2Launchversion v2, qui remplace les deux EC2Launch versions EC2Config et est préinstallée sur AWS Windows Server 2022AMIs. Vous pouvez également Migrer vers la EC2Launch version v2 utiliser l'outil de migration ou installer et configurer manuellement l'agent sur Windows Server 2016 et 2019.

Les versions de Windows AMIs pour Windows Server antérieures à Windows Server 2016 incluent un service optionnel, le EC2Config service (`EC2Config.exe`). EC2Configdémarre lorsque l'instance démarre et exécute des tâches pendant le démarrage et chaque fois que vous arrêtez ou démarrez l'instance. EC2Configpeut également effectuer des tâches à la demande. Certaines de ces tâches sont automatiquement activées, alors que d'autres doivent être activées manuellement. Bien que facultatif, ce service offre l'accès à des fonctions avancées indisponibles dans d'autres cas. Ce service s'exécute dans le LocalSystem compte.

Le EC2Config service exécute Sysprep, un outil Microsoft qui permet de créer un Windows personnalisé AMI qui peut être réutilisé. Lorsqu'il EC2Config appelle Sysprep, il utilise les fichiers qu'il contient `%ProgramFiles%\Amazon\EC2ConfigService\Settings` pour déterminer les opérations à effectuer. Vous pouvez modifier ces fichiers indirectement à l'aide de la boîte de dialogue système Propriétés du EC2 service ou directement à l'aide d'un XML éditeur ou d'un éditeur de texte. Cependant, certains paramètres avancés ne sont pas disponibles dans la boîte de dialogue système Ec2 Service Properties, vous devez donc modifier ces entrées directement.

Si vous créez une instance AMI à partir d'une instance après avoir mis à jour ses paramètres, les nouveaux paramètres sont appliqués à toute instance lancée à partir de la nouvelle instanceAMI. Pour plus d'informations sur la création d'unAMI, consultezCréez un compte soutenu EBS par Amazon AMI.

EC2Configutilise des fichiers de paramètres pour contrôler son fonctionnement. Vous pouvez mettre à jour ces fichiers de paramètres à l'aide d'un outil graphique ou en modifiant directement XML les fichiers. Les fichiers binaires et les fichiers supplémentaires du service sont stockés dans le répertoire `%ProgramFiles%\Amazon\EC2ConfigService`.

Table des matières

- Installez la dernière version de EC2Config
- Configurez. NETparamètres de proxy pour le EC2Config service
- Définissez les propriétés du EC2Config service à partir de la boîte de dialogue système de votre instance EC2 Windows
- Résoudre les problèmes liés à l'agent de EC2Config lancement
- Historique des versions EC2Config

EC2Configet AWS Systems Manager

Le EC2Config service traite les demandes de Systems Manager sur les instances créées AMIs à partir de versions de Windows Server antérieures à Windows Server 2016 publiées avant novembre 2016.

Les instances créées AMIs à partir de versions de Windows Server antérieures à Windows Server 2016 publiées après novembre 2016 incluent le EC2Config service et l'SSMagent. EC2Configexécute toutes les tâches décrites précédemment, et l'SSMagent traite les demandes relatives aux fonctionnalités de Systems Manager telles que Run Command et State Manager.

Vous pouvez utiliser Run Command pour mettre à niveau vos instances existantes afin de les utiliser vers la dernière version du EC2Config service et de l'SSMagent. Pour plus d'informations, consultez la section Mettre à jour SSM l'agent à l'aide de la commande Exécuter dans le guide de AWS Systems Manager l'utilisateur.

EC2Configtâches

EC2Configexécute les tâches de démarrage initiales lors du premier démarrage de l'instance, puis les désactive. Pour les réexécuter, vous devez les activer explicitement avant d'arrêter l'instance ou en exécutant Sysprep manuellement. Ces tâches se présentent comme suit :

- Définissez un mot de passe chiffré aléatoire pour le nouveau compte d'administrateur.
- Générez et installez le certificat d'hôte utilisé pour la connexion au Bureau à distance.
- Etendez de manière dynamique la partition du système d'exploitation pour inclure l'espace non partitionné.
- Exécutez les données utilisateur spécifiées (et Cloud-Init, s'il est installé). Pour plus d'informations sur la spécification de données utilisateur, consultez Exécuter des commandes lorsque vous lancez une EC2 instance avec saisie de données utilisateur.

EC2Configexécute les tâches suivantes à chaque démarrage de l'instance :

- Modifiez le nom d'hôte pour que celui-ci corresponde à l'adresse IP privée dans la notation hexadécimale (cette tâche est désactivée par défaut et doit être activée pour s'exécuter au démarrage de l'instance).
- Configurez le serveur gestionnaire de clés (AWS KMS), vérifiez l'état de l'activation Windows et activez Windows au besoin.
- Montez tous les EBS volumes Amazon et les volumes de stockage d'instance, et associez les noms des volumes aux lettres du lecteur.
- Ecrivez les entrées du journal d'événements sur la console pour faciliter le dépannage (cette tâche est désactivée par défaut et doit être activée pour s'exécuter au démarrage de l'instance).
- Ecrivez sur la console que Windows est prêt.
- Ajoutez un itinéraire personnalisé à l'adaptateur réseau principal pour activer les adresses IP suivantes lorsqu'une NIC ou plusieurs adresses NICs sont connectées : `169.254.169.250169.254.169.251`, et`169.254.169.254`. Ces adresses sont utilisées par l'activation de Windows et lorsque vous accédez aux métadonnées de l'instance.

> **Note**
>
> Si le système d'exploitation Windows est configuré pour être utiliséIPv4, ces adresses IPv4 locales de liens peuvent être utilisées. Si le système d'exploitation Windows a désactivé la pile de protocoles IPv4 réseau et l'utilise à la IPv6 place, ajoutez `[fd00:ec2::240]` à la place de `169.254.169.250` et`169.254.169.251`. Ensuite, ajoutez `[fd00:ec2::254]` à la place de `169.254.169.254`.

EC2Configexécute la tâche suivante chaque fois qu'un utilisateur se connecte :

- Affiche les informations du papier peint sur l'arrière-plan du bureau.

Pendant que l'instance est en cours d'exécution, vous pouvez demander qu'EC2Configelle exécute la tâche suivante à la demande :

- Exécutez Sysprep et arrêtez l'instance afin de pouvoir en créer une AMI à partir de celle-ci. Pour de plus amples informations, veuillez consulter Créez un Amazon à EC2 AMI l'aide de Windows Sysprep.

EC2Configfichiers de paramètres

Les fichiers de paramètres contrôlent le fonctionnement du EC2Config service. Ces fichiers se trouvent dans le répertoire `C:\Program Files\Amazon\Ec2ConfigService\Settings` :

- `ActivationSettings.xml`—Contrôle l'activation du produit à l'aide d'un serveur gestionnaire de clés (AWS KMS).
- `AWS.EC2.Windows.CloudWatch.json`—Contrôle les compteurs de performance auxquels envoyer CloudWatch et les journaux à envoyer à CloudWatch Logs.
- `BundleConfig.xml`: contrôle le mode de EC2Config préparation d'une instance sauvegardée par le stockage en vue de sa création. AMI
- `Config.xml` — Contrôle les paramètres principaux.
- `DriveLetterConfig.xml` — Contrôle les mappages de lettres de lecteurs.
- `EventLogConfig.xml` — Contrôle les informations de journaux d'événements affichés sur la console au démarrage de l'instance.
- `WallpaperSettings.xml` — Contrôle les informations affichées sur l'arrière-plan du bureau.

ActivationSettings.xml

Ce fichier contient les paramètres qui contrôlent l'activation du produit. Au démarrage de Windows, le EC2Config service vérifie si Windows est déjà activé. Si Windows n'est pas le cas, il tente de l'activer en recherchant le serveur AWS KMS spécifié.

- `SetAutodiscover`—Indique si un AWS KMS doit être détecté automatiquement.
- `TargetKMSServer`—Enregistre l'adresse IP privée d'un AWS KMS. Le AWS KMS doit être situé dans la même région que votre instance.
- `DiscoverFromZone`—Découvre le AWS KMS serveur depuis la DNS zone spécifiée.
- `ReadFromUserData`—Récupère le AWS KMS serveur depuis. UserData
- `LegacySearchZones`—Découvre le AWS KMS serveur depuis la DNS zone spécifiée.
- `DoActivate` — Fait des tentatives d'activation à l'aide des paramètres spécifiés dans la section. Cette valeur peut être `true` ou `false`.
- `LogResultToConsole` — Affiche le résultat sur la console.

BundleConfig.xml

Ce fichier contient des paramètres qui contrôlent le mode de EC2Config préparation d'une instance en vue de AMI sa création.

- `AutoSysprep` — Indique si Sysprep doit être utilisé automatiquement. Modifiez la valeur à `Yes` pour utiliser Sysprep.
- `SetRDPCertificate` — Définit un certificat autosigné sur le serveur des services Bureau à distance. Cela vous permet d'accéder aux instances RDP en toute sécurité. Modifiez la valeur à `Yes` si les nouvelles instances doivent avoir le certificat.

  Ce paramètre n'est pas utilisé pour les instances dont les versions du système d'exploitation sont antérieures à Windows Server 2016, car elles peuvent générer leurs propres certificats.
- `SetPasswordAfterSysprep` — Définit un mot de passe aléatoire sur une instance lancée récemment, chiffre celui-ci avec la clé de lancement de l'utilisateur et sort le mot de passe chiffré sur la console. Modifiez la valeur de ce paramètre à `No` si les nouvelles instances ne doivent pas être définies sur un mot de passe chiffré aléatoire.

Config.xml

Plug-ins (Compléments)

- `Ec2SetPassword` — Génère un mot de passe chiffré chaque fois que vous lancez une instance. Par défaut cette fonction est désactivée après le premier lancement afin que les redémarrages de cette instance ne modifient pas un mot de passe défini par l'utilisateur. Modifiez ce paramètre à `Enabled` pour continuer de générer des mots de passe chaque fois que vous lancez une instance.

  Ce paramètre est important si vous envisagez de créer un à AMI partir de votre instance.
- `Ec2SetComputerName` — Définit le nom d'hôte de l'instance sur un nom unique basé sur l'adresse IP de l'instance et redémarre l'instance. Pour définir votre propre nom d'hôte ou pour empêcher que votre nom d'hôte existant soit modifié, désactivez ce paramètre.
- `Ec2InitializeDrives` — Initialise et formate tous les volumes au démarrage. Cette caractéristique est activée par défaut.
- `Ec2EventLog` — Affiche les entrées du journal des événements sur la console. Par défaut, les trois entrées d'erreurs les plus récentes du journal d'événements du système sont affichées. Pour spécifier les entrées du journal des événements à afficher, modifiez le fichier `EventLogConfig.xml` situé dans le répertoire `EC2ConfigService\Settings`. Pour

plus d'informations sur les paramètres de ce fichier, consultez Eventlog Key dans la MSDN bibliothèque.

- `Ec2ConfigureRDP` — Configure un certificat autosigné sur l'instance, afin que les utilisateurs puissent accéder en toute sécurité à l'instance à l'aide des services Bureau à distance. Ce paramètre n'est pas utilisé pour les instances dont les versions du système d'exploitation sont antérieures à Windows Server 2016, car elles peuvent générer leurs propres certificats.
- `Ec2OutputRDPCert` — Affiche les informations du certificat des services Bureau à distance sur la console afin que les utilisateurs puissent les vérifier auprès de l'empreinte numérique.
- `Ec2SetDriveLetter` — Définit les lettres de lecteurs des volumes montés, sur la base des paramètres définis par l'utilisateur. Par défaut, lorsqu'un EBS volume Amazon est attaché à une instance, il peut être monté à l'aide de la lettre du lecteur figurant sur l'instance. Pour spécifier vos mappages de lettres de lecteurs, modifiez le fichier `DriveLetterConfig.xml` situé dans le répertoire `EC2ConfigService\Settings`.
- `Ec2WindowsActivate` — Le plug-in gère l'activation de Windows. Il vérifie si Windows est activé. Dans le cas contraire, il met à jour les paramètres du AWS KMS client, puis active Windows.

  Pour modifier les AWS KMS paramètres, modifiez le `ActivationSettings.xml` fichier situé dans le `EC2ConfigService\Settings` répertoire.
- `Ec2DynamicBootVolumeSize` — Étend le disque 0/volume 0 pour inclure l'espace non partitionné.
- `Ec2HandleUserData` — Crée et exécute les scripts créés par l'utilisateur au premier lancement d'une instance une fois Sysprep exécuté. Les commandes encapsulées dans des balises de script sont enregistrées dans un fichier batch, et les commandes encapsulées dans des PowerShell balises sont enregistrées dans un fichier .ps1 (correspond à la case à cocher Données utilisateur dans la boîte de dialogue système Ec2 Service Properties).
- `Ec2ElasticGpuSetup`—Installe le package GPU logiciel Elastic si l'instance est associée à un Elastic. GPU
- `Ec2FeatureLogging` — Envoie à la console l'état d'installation de la fonction Windows et du service correspondant. Pris en charge uniquement pour la fonction Microsoft Hyper-V et le service correspondant vmms.

Paramètres globaux

- `ManageShutdown`—Garantit que les instances lancées à partir d'instances sauvegardées dans le stockage ne s'arrêtent AMIs pas pendant l'exécution de Sysprep.

- `SetDnsSuffixList`—Définit le DNS suffixe de l'adaptateur réseau pour Amazon. EC2 Cela permet de DNS résoudre les serveurs exécutés sur Amazon EC2 sans fournir le nom de domaine complet.

  > **Note**
  >
  > Cela ajoute une recherche de DNS suffixe pour le domaine suivant et configure d'autres suffixes standard. Pour plus d'informations sur la façon dont les agents de lancement définissent les DNS suffixes, consultez. Configurer le DNS suffixe pour les agents de lancement EC2 Windows
  >
  > ```
  > region.ec2-utilities.amazonaws.com
  > ```

- `WaitForMetaDataAvailable`—Garantit que le EC2Config service attendra que les métadonnées soient accessibles et que le réseau soit disponible avant de poursuivre le démarrage. Cette vérification garantit que EC2Config vous pouvez obtenir des informations à partir des métadonnées pour l'activation et d'autres plug-ins.
- `ShouldAddRoutes`—Ajoute un itinéraire personnalisé à l'adaptateur réseau principal pour activer les adresses IP suivantes lorsque plusieurs adresses NICs sont connectées : 169.254.169.250, 169.254.169.251 et 169.254.169.254. Ces adresses sont utilisées par l'activation de Windows et lorsque vous accédez aux métadonnées de l'instance.
- `RemoveCredentialsfromSyspreponStartup` — Supprime le mot de passe administrateur du fichier `Sysprep.xml` au démarrage suivant du service. Pour vous assurer que le mot de passe persiste, modifiez le paramètre.

DriveLetterConfig.xml

Ce fichier contient les paramètres qui contrôlent les mappages de lettres de lecteurs. Par défaut, un volume peut être mappé à n'importe quelle lettre de lecteur disponible. Vous pouvez monter un volume sur une lettre de lecteur spécifique comme indiqué ci-après.

```
<?xml version="1.0" standalone="yes"?>
<DriveLetterMapping>
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
  . . .
```

```
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
</DriveLetterMapping>
```

- `VolumeName` — Étiquette du volume. Par exemple, *`My Volume`*. Pour spécifier un mappage pour un volume de stockage d'instance, utilisez l'étiquette `Temporary Storage X`, où `X` est un chiffre de 0 à 25.
- `DriveLetter` — Lettre du lecteur. Par exemple, *`M:`*. Le mappage de la lettre du lecteur échoue si celle-ci est déjà utilisée.

EventLogConfig.xml

Ce fichier contient les paramètres qui contrôlent les informations de journaux d'événements affichés sur la console au démarrage de l'instance. Par défaut, les trois entrées d'erreurs les plus récentes du journal d'événements du système sont affichées.

- `Category` — Clé du journal des événements à surveiller.
- `ErrorType` — Type d'événement (par exemple, `Error`, `Warning`, `Information`.)
- `NumEntries` — Nombre d'événements stockés pour cette catégorie.
- `LastMessageTime` — Pour empêcher que le même message soit envoyé de manière répétée, le service met à jour cette valeur chaque fois qu'il envoie un message.
- `AppName` — Source de l'événement ou application ayant enregistré l'événement.

WallpaperSettings.xml

Ce fichier contient les paramètres qui contrôlent les informations affichées sur l'arrière-plan du bureau. Les informations suivantes sont affichées par défaut.

- `Hostname` — Affiche le nom de l'ordinateur.
- `Instance ID` — Affiche l'ID de l'instance.
- `Public IP Address` — Affiche l'adresse IP publique de l'instance.
- `Private IP Address` — Affiche l'adresse IP privée de l'instance.
- `Availability Zone` — Affiche la zone de disponibilité dans laquelle l'instance s'exécute.
- `Instance Size` — Affiche le type de l'instance.

- `Architecture` — Affiche le paramètre de la variable d'environnement `PROCESSOR_ARCHITECTURE`.

Vous pouvez supprimer toutes les informations affichées par défaut en supprimant leurs entrées. Vous pouvez ajouter les métadonnées de l'instance à afficher comme suit.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>metadata</source>
  <identifier>meta-data/path</identifier>
</WallpaperInformation>
```

Vous pouvez ajouter les variables d'environnement du système à afficher comme suit.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>EnvironmentVariable</source>
  <identifier>variable-name</identifier>
</WallpaperInformation>
```

InitializeDrivesSettings.xml

Ce fichier contient les paramètres qui contrôlent le mode d'EC2Configinitialisation des lecteurs.

Par défaut, EC2Config initialisez les lecteurs qui n'ont pas été mis en ligne avec le système d'exploitation. Vous pouvez personnaliser le plugin comme suit.

```
<InitializeDrivesSettings>
    <SettingsGroup>setting</SettingsGroup>
</InitializeDrivesSettings>
```

Utilisez un groupe de paramètres pour spécifier comment vous souhaitez initialiser les disques:

FormatWithTRIM

Active la TRIM commande lors du formatage des lecteurs. Après le formatage et l'initialisation d'un lecteur, le système rétablit TRIM la configuration.

À partir de EC2Config la version 3.18, la TRIM commande est désactivée par défaut lors de l'opération de formatage du disque. Cela améliore les délais de formatage. Utilisez ce paramètre

pour l'activer TRIM lors de l'opération de formatage du disque pour les EC2Config versions 3.18 et ultérieures.

FormatWithoutTRIM

Désactive la TRIM commande lors du formatage des disques et améliore les temps de formatage sous Windows. Après le formatage et l'initialisation d'un lecteur, le système rétablit TRIM la configuration.

DisableInitializeDrives

Désactive le formatage des nouveaux disques. Utilisez-le pour initialiser les disques manuellement.

Installez la dernière version de EC2Config

Par défaut, le EC2Config service est inclus dans les AMIs versions antérieures à Windows Server 2016. Lorsque le EC2Config service est mis à jour, les nouvelles versions AMIs de Windows AWS incluent la dernière version du service. Toutefois, vous devez mettre à jour votre propre Windows AMIs et vos instances avec la dernière version deEC2Config.

> **Note**
>
> EC2Launchremplace EC2Config sur Windows Server 2016 et 2019. Pour de plus amples informations, veuillez consulter Utiliser l'agent EC2Launch v1 pour effectuer des tâches lors du lancement de l'instance EC2 Windows. Le dernier service de lancement pour toutes les versions de Windows Server prises en charge est la EC2Launchv2, qui remplace à la fois EC2Config etEC2Launch.

Pour plus d'informations sur la façon de recevoir des notifications pour les EC2Config mises à jour, consultezAbonnez-vous aux notifications de l'agent de lancement EC2 Windows. Pour plus d'informations sur les modifications apportées à chaque version, consultez le document Historique des versions EC2Config.

Avant de commencer

- Vérifiez que vous l'avez fait. NETframework 3.5 SP1 ou supérieur.
- Par défaut, le programme d'installation remplace vos fichiers de paramètres par des fichiers de paramètres par défaut lors de l'installation et redémarre le EC2Config service une fois l'installation

terminée. Si vous avez modifié les paramètres du EC2Config service, copiez le `config.xml` fichier depuis le `%Program Files%\Amazon\Ec2ConfigService\Settings` répertoire. Après avoir mis à jour le EC2Config service, vous pouvez restaurer ce fichier pour conserver vos modifications de configuration.

- Si votre version de EC2Config est antérieure à la version 2.1.19 et que vous installez la version 2.2.12 ou antérieure, vous devez d'abord installer la version 2.1.19. Pour installer la version 2.1.19, téléchargez EC2Install_2.1.19.zip, décompressez le fichier, puis exécutez-le. `EC2Install.exe`

> **Note**
>
> Si votre version de EC2Config est antérieure à la version 2.1.19 et que vous installez la version 2.3.313 ou ultérieure, vous pouvez l'installer directement sans installer la version 2.1.19 au préalable.

Vérifier la version EC2Config

Utilisez la procédure suivante pour vérifier EC2Config que la version de celui-ci est installée sur vos instances.

Pour vérifier la version installée de EC2Config

1. Lancez une instance depuis votre AMI ordinateur et connectez-vous à celle-ci.
2. Dans le Panneau de configuration, sélectionnez Programmes et fonctionnalités.
3. Dans la liste des programmes installés, recherchez `Ec2ConfigService`. Son numéro de version s'affiche dans la colonne Version.

Mettre à jour EC2Config

Suivez la procédure ci-dessous pour télécharger et installer la dernière version de EC2Config sur vos instances.

Pour télécharger et installer la dernière version de EC2Config

1. Téléchargez et décompressez le EC2Configprogramme d'installation.
2. Exécutez `EC2Install.exe`. Pour obtenir une liste complète des options, exécutez `EC2Install` avec l'option `/?`. Par défaut, la configuration affiche les invites. Pour exécuter la commande sans invites, utilisez l'option `/quiet`.

> **Important**
>
> Pour conserver les paramètres personnalisés du `config.xml` fichier que vous avez enregistré, exécutez `EC2Install` l'`/norestart`option, restaurez vos paramètres, puis redémarrez le EC2Config service manuellement.

3. Si vous exécutez EC2Config la version 4.0 ou ultérieure, vous devez redémarrer l'SSMagent sur l'instance à partir du composant logiciel enfichable Microsoft Services.

> **Note**
>
> Les informations de EC2Config version mises à jour n'apparaîtront pas dans le journal système de l'instance ou dans la vérification de Trusted Advisor tant que vous n'aurez pas redémarré ou arrêté et démarré votre instance.

Pour télécharger et installer la dernière version EC2Config de PowerShell

Pour télécharger, décompresser et installer la dernière version d'EC2ConfigUsing PowerShell, exécutez les commandes suivantes depuis une PowerShell fenêtre :

```
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Config/EC2Install.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\" + $(Split-Path -Path $Url -Leaf)
$ExtractPath = "$env:USERPROFILE\Desktop\"
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$ExtractShell = New-Object -ComObject Shell.Application
$ExtractFiles = $ExtractShell.Namespace($DownloadZipFile).Items()
$ExtractShell.NameSpace($ExtractPath).CopyHere($ExtractFiles)
Start-Process $ExtractPath
Start-Process `
    -FilePath $env:USERPROFILE\Desktop\EC2Install.exe `
    -ArgumentList "/S"
```

> **Note**
>
> Si un message d'erreur s'affiche lors du téléchargement du fichier et que vous utilisez Windows Server 2016 ou une version antérieure, il est possible que la version TLS 1.2 doive être activée sur votre PowerShell terminal. Vous pouvez activer la TLS version 1.2 pour la PowerShell session en cours à l'aide de la commande suivante, puis réessayer :

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

Vérifiez l'installation en vérifiant que le répertoire `C:\Program Files\Amazon\` contient le répertoire `Ec2ConfigService`.

Configurez. NETparamètres de proxy pour le EC2Config service

Vous pouvez configurer le EC2Config service pour qu'il communique via un proxy en utilisant l'une des méthodes suivantes : le AWS SDK for. NET, l'`system.net`élément, ou Microsoft Group Policy et Internet Explorer. En utilisant le AWS SDK formulaire. NETest la méthode préférée car vous pouvez spécifier des informations de connexion.

Méthodes

- Configurez les paramètres du proxy à l'aide du AWS SDK for .NET (préféré)
- Configurer les paramètres de proxy à l'aide de l'élément system.net
- Configurer les paramètres de proxy à l'aide de la politique de groupe Microsoft et de Microsoft Internet Explorer

Configurez les paramètres du proxy à l'aide du AWS SDK for .NET (préféré)

Vous pouvez configurer les paramètres du proxy pour le EC2Config service en spécifiant l'`proxy`élément dans le `Ec2Config.exe.config` fichier. Pour plus d'informations, consultez la section Référence des fichiers de configuration AWS SDK pour. NET.

Pour spécifier l'élément proxy dans le fichier Ec2Config.exe.config

1. Modifiez le `Ec2Config.exe.config` fichier sur une instance sur laquelle vous souhaitez que le EC2Config service communique via un proxy. Par défaut, le fichier se trouve dans le répertoire suivant : `%ProgramFiles%\Amazon\Ec2ConfigService`.
2. Ajoutez l'élément `aws` suivant aux `configSections`. Ne l'ajoutez pas à des `sectionGroups` existants.

   Pour EC2Config les versions 3.17 ou antérieures

   ```
   <configSections>
      <section name="aws" type="Amazon.AWSSection, AWSSDK"/>
   ```

```
</configSections>
```

Pour EC2Config les versions 3.18 ou ultérieures

```
<configSections>
     <section name="aws" type="Amazon.AWSSection, AWSSDK.Core"/>
</configSections>
```

3. Ajoutez l'élément `aws` suivant au fichier `Ec2Config.exe.config`.

```
<aws>
   <proxy
     host="string value"
     port="string value"
     username="string value"
     password="string value" />
</aws>
```

4. Enregistrez vos modifications.

Configurer les paramètres de proxy à l'aide de l'élément system.net

Vous pouvez spécifier les paramètres proxy dans un élément `system.net` dans le fichier `Ec2Config.exe.config`. Pour plus d'informations, voir defaultProxyElement (paramètres réseau) activéMSDN.

Pour spécifier l'élément system.net dans le fichier Ec2Config.exe.config

1. Modifiez le `Ec2Config.exe.config` fichier sur une instance sur laquelle vous souhaitez que le EC2Config service communique via un proxy. Par défaut, le fichier se trouve dans le répertoire suivant : `%ProgramFiles%\Amazon\Ec2ConfigService`.
2. Ajoutez une entrée `defaultProxy` à `system.net`. Pour plus d'informations, voir defaultProxy Element (paramètres réseau) activéMSDN.

   Par exemple, la configuration suivante achemine tout le trafic pour utiliser le proxy qui est actuellement configuré pour Internet Explorer, à l'exception des métadonnées et du trafic de licence qui contournent le proxy.

```
<defaultProxy>
    <proxy usesystemdefault="true" />
```

```
    <bypasslist>
        <add address="169.254.169.250" />
        <add address="169.254.169.251" />
        <add address="169.254.169.254" />
        <add address="[fd00:ec2::250]" />
        <add address="[fd00:ec2::254]" />
    </bypasslist>
</defaultProxy>
```

3. Enregistrez vos modifications.

Configurer les paramètres de proxy à l'aide de la politique de groupe Microsoft et de Microsoft Internet Explorer

Le EC2Config service s'exécute sous le compte utilisateur du système local. Vous pouvez spécifier des paramètres proxy à l'échelle de l'instance pour ce compte dans Internet Explorer après avoir modifié les paramètres de la politique de groupe sur l'instance.

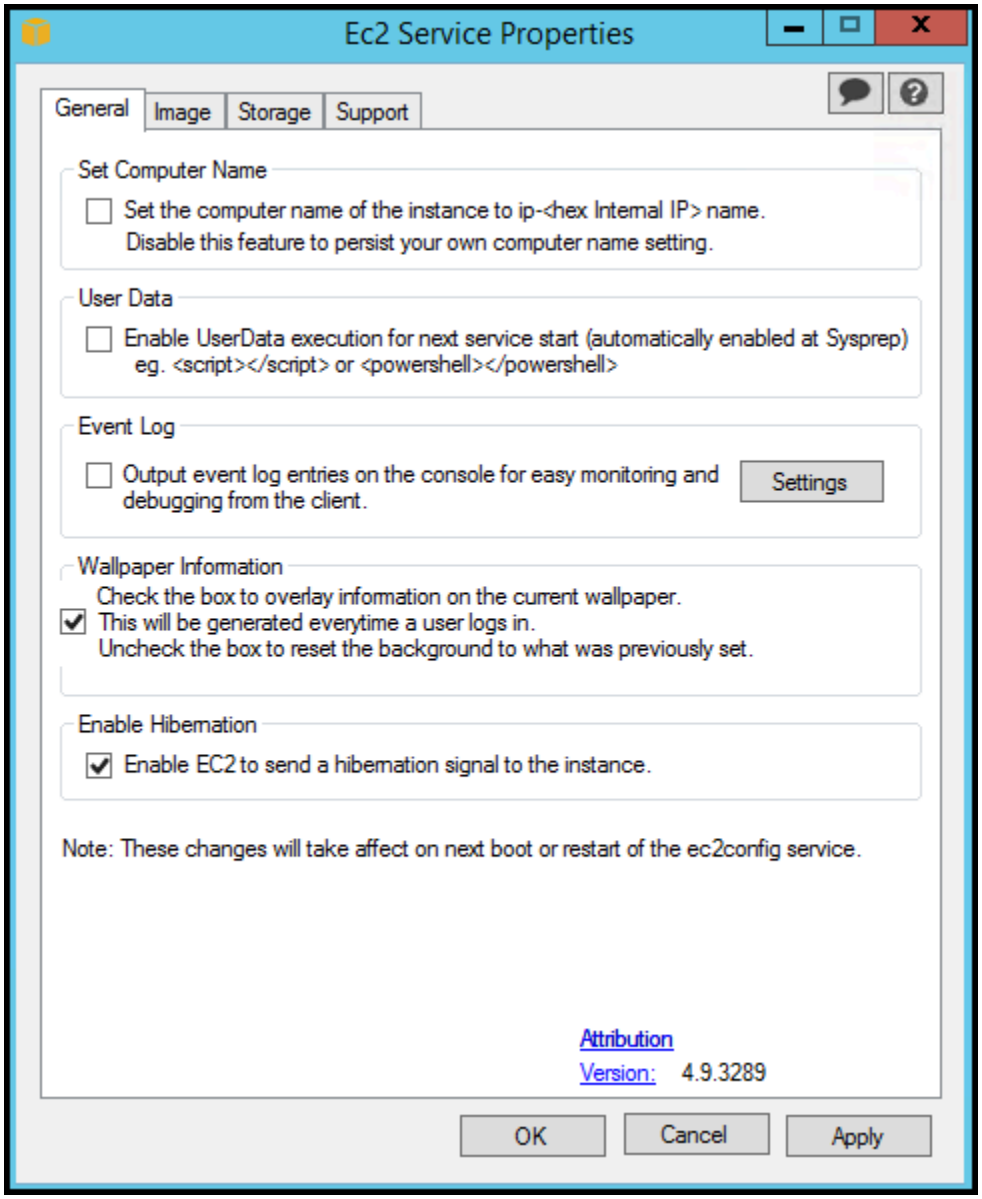
Pour configurer les paramètres proxy à l'aide de la politique de groupe et d'Internet Explorer

1. Sur une instance où vous souhaitez que le EC2Config service communique via un proxy, ouvrez une invite de commande en tant qu'administrateur**`gpedit.msc`**, tapez et appuyez sur Entrée.
2. Dans l'Editeur de stratégie de groupe locale, sous Stratégie Ordinateur local, choisissez Configuration ordinateur, Modèles d'administration, Composants Windows, Internet Explorer.
3. Dans le volet droit, choisissez Paramètres machine du serveur proxy (plutôt que les paramètres individualisés), puis Modifier les paramètres de la stratégie.
4. Choisissez Activée, puis Appliquer.
5. Ouvrez Internet Explorer, puis cliquez sur le bouton Outils.
6. Choisissez Options Internet, puis choisissez l'onglet Connexions.
7. Choisissez LANles paramètres.
8. Sous Serveur proxy, choisissez l'option Utiliser un serveur proxy pour votre LAN option.
9. Spécifiez l'adresse et les informations sur le port, puis choisissez OK.

Définissez les propriétés du EC2Config service à partir de la boîte de dialogue système de votre instance EC2 Windows

La procédure suivante décrit comment utiliser la boîte de dialogue système Propriétés du EC2 service pour activer ou désactiver les paramètres.

1. Lancez et connectez-vous à votre instance Windows.
2. Dans le menu Démarrer, cliquez sur Tous les programmes, puis sur EC2ConfigServiceParamètres.



3. Dans l'onglet Général de la boîte de dialogue système Propriétés du EC2 service, vous pouvez activer ou désactiver les paramètres suivants.

Set Computer Name (Définir le nom de l'ordinateur)

Si ce paramètre est activé (il est désactivé par défaut), le nom d'hôte est comparé à l'adresse IP interne actuelle à chaque démarrage. Si le nom d'hôte et l'adresse IP interne ne correspondent pas, le nom d'hôte est réinitialisé pour contenir l'adresse IP interne, puis le système redémarre pour récupérer le nouveau nom d'hôte. Pour définir votre propre nom d'hôte ou pour empêcher que votre nom d'hôte existant soit modifié, n'activez pas ce paramètre.

User Data (Données utilisateur)

L'exécution des données utilisateur vous permet de spécifier des scripts dans les métadonnées de l'instance. Par défaut, ces scripts sont exécutés lors du lancement initial. Vous pouvez également les configurer pour les exécuter la prochaine fois que vous réamorcez ou démarrez l'instance, ou chaque fois que vous réamorcez ou démarrez l'instance.

Si vous avez un script volumineux, nous vous recommandons d'utiliser les données utilisateur pour télécharger le script, puis de l'exécuter.

Pour plus d'informations, consultez Exécution de données utilisateur.

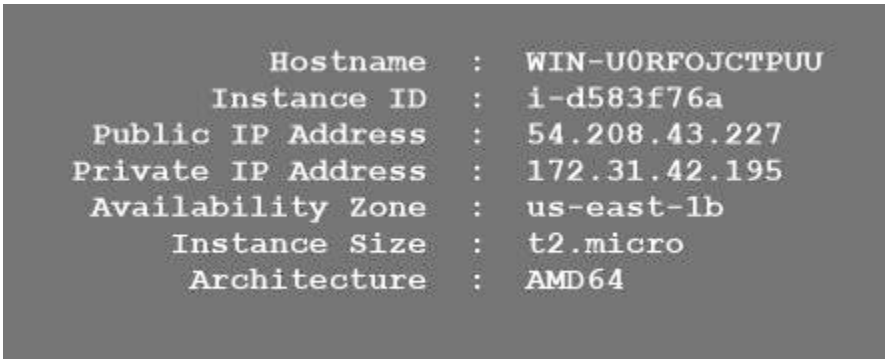
Event Log

Utilisez ce paramètre pour afficher les entrées du journal d'événements sur la console pendant le démarrage afin de simplifier la surveillance et le débogage.

Cliquez sur Settings (Paramètres) pour spécifier des filtres pour les entrées du journal envoyées à la console. Le filtre par défaut envoie les trois entrées d'erreurs les plus récentes du journal d'événements du système vers la console.

Wallpaper Information (Informations sur le papier peint)

Utilisez ce paramètre pour afficher les informations système sur l'arrière-plan du bureau. L'exemple suivant présente les informations affichées sur l'arrière-plan du bureau.

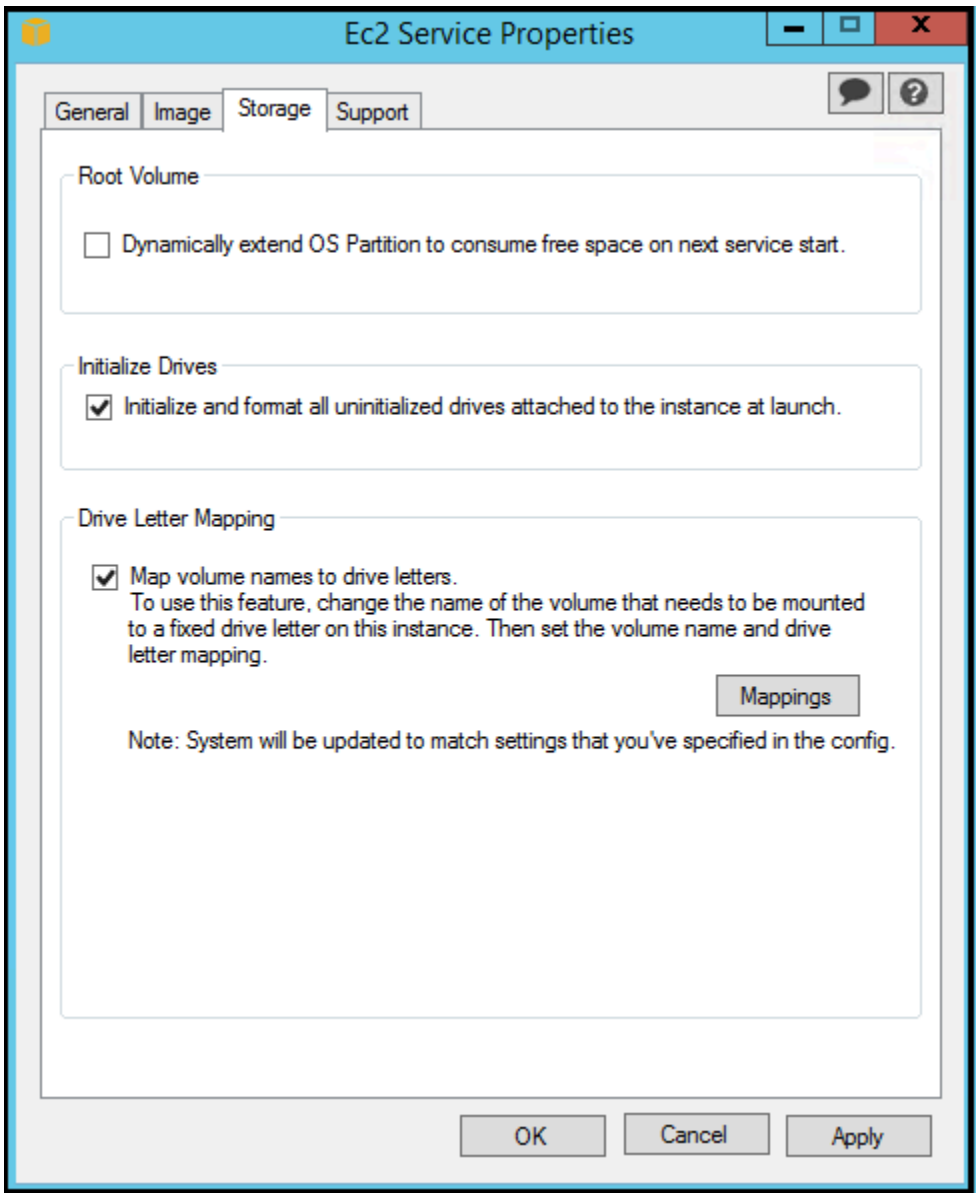


Les informations affichées à l'arrière-plan du bureau sont contrôlées par le fichier de paramètres `EC2ConfigService\Settings\WallpaperSettings.xml`.

Enable Hibernation (Activer la mise en veille prolongée)

Utilisez ce paramètre pour EC2 autoriser le système d'exploitation à effectuer l'hibernation.

4. Cliquez sur l'onglet Storage (Stockage). Vous pouvez activer ou désactiver les paramètres suivants.



Root Volume (Volume racine)

Ce paramètre étend de manière dynamique le disque 0/volume 0 pour inclure l'espace non partitionné. Cela peut être utile lorsque l'instance est démarrée à partir d'un volume du périphérique racine doté d'une taille personnalisée.

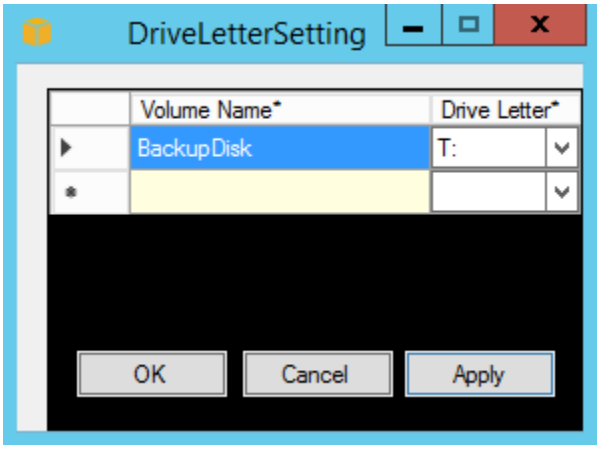
Initialize Drives (Initialiser les lecteurs)

Ce paramètre formate et monte tous les volumes attachés à l'instance au démarrage.

Drive Letter Mapping (Mappage de lettres de lecteur)

Le système mappe les volumes attachés à une instance aux lettres des lecteurs. Pour les EBS volumes Amazon, la valeur par défaut est d'attribuer des lettres de lecteur allant de D : à Z :. Par exemple, les volumes de stockage, la valeur par défaut dépend du pilote. AWS Les pilotes PV et Citrix PV attribuent aux volumes de stockage des instances des lettres de lecteur allant de Z : à A :. Les pilotes Red Hat attribuent les lettres de lecteurs de volumes de stockage d'instances allant de D: à A:.

Pour choisir les lettres de lecteurs de vos volumes, cliquez sur Mappings (Mappages). Dans la DriveLetterSettingboîte de dialogue, spécifiez les valeurs du nom du volume et de la lettre du lecteur pour chaque volume, cliquez sur Appliquer, puis sur OK. Nous vous recommandons de sélectionner les lettres de lecteurs qui permettent d'éviter les conflits avec es lettres de lecteurs susceptibles d'être utilisées, comme celles du milieu de l'alphabet.



Après avoir défini un mappage de lettres de lecteur et attaché un volume portant la même étiquette que l'un des noms de volume que vous avez spécifiés, assigne EC2Config automatiquement la lettre de lecteur spécifiée à ce volume. En revanche, le mappage de lettre de lecteur échoue si celle-ci est déjà utilisée. Notez que EC2Config cela ne modifie pas les lettres de lecteur des volumes déjà montés lorsque vous avez spécifié le mappage des lettres de lecteur.

5. Pour enregistrer vos paramètres et continuer à les modifier ultérieurement, cliquez sur OK pour fermer la boîte de dialogue système des propriétés du EC2 service. Si vous avez terminé de personnaliser votre instance et que vous souhaitez en créer une à AMI partir de cette instance, consultezCréez un Amazon à EC2 AMI l'aide de Windows Sysprep.

Résoudre les problèmes liés à l'agent de EC2Config lancement

Les informations suivantes peuvent vous aider à résoudre les problèmes liés au EC2Config service.

Mise à jour EC2Config sur une instance inaccessible

Utilisez la procédure suivante pour mettre à jour le EC2Config service sur une instance Windows Server inaccessible via Remote Desktop.

Pour effectuer une mise à jour EC2Config sur une instance EBS Windows basée sur Amazon à laquelle vous ne pouvez pas vous connecter

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Recherchez l'instance concernée. Sélectionnez l'instance, État de l'instance, puis Arrêter l'instance.

   > **Warning**
   >
   > Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

4. Sélectionnez Lancer des instances et créez une instance `t2.micro` temporaire dans la même zone de disponibilité que l'instance affectée. Utilisez une instance différente AMI de celle que vous avez utilisée pour lancer l'instance concernée.

   > **Important**
   >
   > Si vous ne créez pas l'instance dans la même zone de disponibilité que l'instance affectée, vous ne pourrez pas attacher le volume racine de celle-ci à la nouvelle instance.

5. Dans la EC2 console, sélectionnez Volumes.
6. Recherchez le volume racine de l'instance affectée. Détachez le volume et attachez-le à l'instance temporaire que vous avez créée précédemment. Attachez-le avec le nom du périphérique par défaut (xvdf).
7. Utilisez les services Bureau à distance pour vous connecter à l'instance temporaire, puis utilisez l'utilitaire Gestion des disques pour rendre le volume disponible.

8. Téléchargez la dernière version du EC2Config service. Extrayez les fichiers du fichier `.zip` dans le répertoire `Temp` du lecteur que vous avez attaché.
9. Sur l'instance temporaire, ouvrez la boîte de dialogue Run (Exécuter), tapez **`regedit`** et appuyez sur Entrée.
10. Sélectionnez `HKEY_LOCAL_MACHINE`. Dans le menu File (Fichier), choisissez Load Hive (Charger Hive). Choisissez le lecteur, puis accédez au fichier `Windows\System32\config\SOFTWARE` et ouvrez-le. Quand vous y êtes invité, spécifiez un nom de clé.
11. Sélectionnez la clé que vous venez de charger et naviguez jusqu'à `Microsoft\Windows\CurrentVersion`. Choisissez la clé `RunOnce`. Si elle n'existe pas, choisissez `CurrentVersion` dans le menu contextuel (clic droit), choisissez Nouveau, puis Clé. Nommez la clé `RunOnce`.
12. Dans le menu contextuel (clic droit), choisissez la clé `RunOnce`, Nouveau, puis Valeur de chaîne. Entrez le nom `Ec2Install` et les données `C:\Temp\Ec2Install.exe /quiet`.
13. Choisissez la clé `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon`. Dans le menu contextuel (clic droit), choisissez Nouveau, puis Valeur de chaîne. Entrez le nom **`AutoAdminLogon`** et les données **`1`**.
14. Choisissez la clé `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon>`. Dans le menu contextuel (clic droit), choisissez Nouveau, puis Valeur de chaîne. Entrez le nom **`DefaultUserName`** et les données **`Administrator`**.
15. Choisissez la clé `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon`. Dans le menu contextuel (clic droit), choisissez Nouveau, puis Valeur de chaîne. Entrez le nom **`DefaultPassword`** ainsi qu'un mot de passe dans les données de la valeur.
16. Dans le volet de navigation de l'Éditeur du Registre, choisissez la clé temporaire que vous avez créée lorsque vous avez ouvert pour la première fois l'Éditeur du Registre.
17. Dans le menu File (Fichier), choisissez Unload Hive (Décharger Hive).
18. Dans l'utilitaire Gestion des disques, choisissez le lecteur que vous avez attaché précédemment, ouvrez le menu contextuel (clic droit) et choisissez Hors connexion.
19. Dans la EC2 console Amazon, détachez le volume concerné de l'instance temporaire et attachez-le à nouveau à votre instance avec le nom de l'appareil. `/dev/sda1` Vous devez spécifier ce nom de périphérique pour désigner le volume en tant que volume racine.
20. Arrêtez et démarrez les EC2 instances Amazon l'instance.
21. Une fois l'instance démarrée, consultez le journal système et vérifiez que le message Windows is ready to use est affiché.

22. Ouvrez l'Éditeur du Registre et choisissez `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`. Supprimez les clés String Value que vous avez créées précédemment : AutoAdminLogonDefaultUserName, et DefaultPassword.
23. Supprimez ou arrêtez l'instance temporaire que vous avez créée au cours de cette procédure.

Historique des versions EC2Config

Les AMIs versions antérieures à Windows Server 2016 incluent un service optionnel appelé EC2Config service (`EC2Config.exe`). EC2Configdémarre lorsque l'instance démarre et exécute des tâches pendant le démarrage et chaque fois que vous arrêtez ou démarrez l'instance.

Vous pouvez recevoir des notifications lorsque de nouvelles versions du EC2Config service sont publiées. Pour de plus amples informations, veuillez consulter Abonnez-vous aux notifications de l'agent de lancement EC2 Windows.

Le tableau suivant décrit les versions publiées deEC2Config. Pour plus d'informations sur les mises à jour de SSM l'agent, consultez les notes de version de SSM l'agent Systems Manager.

Version	Détails	Date de publication
4,9,5777	• Correction d'un problème RSS de configuration incorrecte pour certains types d'instances. • Nouvelle version d'SSMAgent`3.3.484.0` .	17 juin 2024
4,9,5554	• Limite la dévolution des noms de domaine en fonction de l'entrée dans le registre : `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Nouvelle version d'SSMAgent`3.2.1630.0` .	4 octobre 2023
4,9,5467	• Ajout d'une fonctionnalité de nouvelle tentative pour découvrir le port de console. •	1er août 2023

Version	Détails	Date de publication
	Nouvelle version de l'SSMagent`3.1.2282.0` .	
4,9,5288	• Mise à jour AWS du noyau SDK vers la version`3.7.103.23` . • Problème résolu : le `AWS-UpdateEC2Config` SSM document ne se met pas à jour `EC2Config` sur les instances activées uniquement avecIMDSv2. • Nouvelle version de l'SSMagent`3.1.2144.0` .	8 mars 2023
4,9,5231	• Nouvelle version de l'SSMAgent 3.1.1927.0.	14 février 2023
4,9,5103	• Correction d'un problème d'identification incorrecte des volumes éphémères sur les familles d'instances r5d et i4i. • Nouvelle version de l'SSMAgent 3.1.1856.0.	5 décembre 2022
4,9,5064	• Mis à jour pour utiliser les informations du PCI segment pour sélectionner le port de console. • PowerShell Scripts signés et en-têtes de copyright ajoutés. • Correction de la logique de sélection de l'adaptateur réseau principal. • Nouvelle version de l'SSMAgent 3.1.1732.0.	16 novembre 2022

Version	Détails	Date de publication
4,9,4588	• Logique IMDS d'attente mise à jour pour ne faire que IMDSv2 des demandes. • Ajout de la bibliothèque partagée de l'agent de lancement libec2launch.dll. • Nouvelle version de l'SSMAgent 3.1.1188.0.	31 mai 2022
4,9,4556	• Ajout d'une logique d'attente pour garantir l'initialisation complète de NIC avant utilisation. • La nouvelle version de Log4Net 2.0.14.0 reprend le correctif de sécurité. • La nouvelle version de l'SSMAgent 3.1.1045.0 intègre le correctif de sécurité.	1 mars 2022
4,9,4536	• Correction d'un incident des données utilisateur lorsque le dossier Temp est manquant. • Nouvelle version de l'SSMAgent 3.1.804.0.	31 janvier 2022
4,9.4508	• Correction du problème pour calculer correctement le chemin du script diskpart. • Nouvelle version de l'SSMAgent 3.1.338.0.	6 octobre 2021
4,9,4500	• Mis à jour `Install-EgpuManagerConfig` avec le support IMDS de la version 2. • Mise à jour des liens Web pour utiliser https. • Nouvelle version de l'SSMAgent 3.1.282.0	7 septembre 2021

Version	Détails	Date de publication
4,9,4419	• Logique de repli de la IMDS version 1 corrigée • Mise à jour de toutes les utilisations du répertoire temporaire Windows vers le répertoire EC2Config temporaire • Nouvelle version de l'SSMAgent 3.0.1124.0	2 juin 2021
4.9.4381	• Ajout du support pour la version 2.2 du schéma de SSM document dans EC2ConfigUpdater • Ajout de la version du package AWS Nitro Enclaves au journal de la console • Nouvelle version de l'SSMAgent 3.0.529.0	4 mai 2021
4.9.4326	• Suppression de tous les liens dans l'interface utilisateur des paramètres • Il s'agit de la dernière EC2Config version compatible avec Windows Server 2008.	3 mars 2021
4.9.4279	• Correction d'un problème de sécurité lié à la tâche `Ec2ConfigMonitor` planifiée • Correction du problème de mappage des lettres de lecteur et du nombre de disques éphémères incorrect • Ajout de `OsCurrentBuild` et `OsReleaseId` à la sortie de la console • Nouvelle version de l'SSMAgent 2.3.871.0	11 décembre 2020
4.9.4222	• Logique de repli de la IMDS version 1 corrigée • Nouvelle version de l'SSMAgent 2.3.842.0	7 avril 2020
4.9.4122	• Ajout du support pour la IMDS version 2 • Nouvelle version de l'SSMAgent 2.3.814.0	4 mars 2020

Version	Détails	Date de publication
4.9.3865	• Correction d'un problème de détection du COM port pour Windows Server 2008 R2 sur les instances métalliques • Nouvelle version de l'SSMAgent 2.3.722.0	31 octobre 2019
4.9.3519	• Nouvelle version de l'SSMAgent 2.3.634.0	18 juin 2019
4.9.3429	• Nouvelle version de l'SSMAgent 2.3.542.0	25 avril 2019
4.9.3289	• Nouvelle version de l'SSMAgent 2.3.444.0	11 février 2019
4.9.3270	• Ajout d'un plugin pour configurer le moniteur pour qu'il ne s'éteigne jamais pour résoudre les ACPI problèmes • SQLÉdition du serveur et version écrites sur la console • Nouvelle version de l'SSMAgent 2.3.415.0	22 janvier 2019
4.9.3230	• Mise à jour de la description du mappage de lettres de lecteur pour mieux correspondre à la fonctionnalité. • Nouvelle version de l'SSMAgent 2.3.372.0	10 janvier 2019
4.9.3160	• Temps d'attente accru pour le primaire NIC • Ajout de la configuration par défaut RSS et des paramètres de file d'attente de réception pour les ENA appareils • Désactivation de la mise en veille prolongée lors de Sysprep • Nouvelle version de l'SSMAgent 2.3.344.0 • Mise à niveau AWS SDK vers la version 3.3.29.13	15 décembre 2018
4.9.3067	• Améliorations apportées à la mise en veille prolongée d'instances • Nouvelle version de l'SSMAgent 2.3.235.0	8 novembre 2018
4.9.3034	• Ajout de la route 169.254.169.253/32 pour le serveur DNS • Nouvelle version de l'SSMAgent 2.3.193.0	24 octobre 2018

Version	Détails	Date de publication
4.9.2986	• Signature ajoutée pour tous les fichiers binaires EC2Config associés • Nouvelle version de l'SSMAgent 2.3.136.0	11 octobre 2018
4.9.2953	Nouvelle version de l'SSMagent (2.3.117.0)	2 octobre 2018
4.9.2926	Nouvelle version de l'SSMagent (2.3.68.0)	18 septembre 2018
4.9.2905	• Nouvelle version de l'SSMagent (2.3.50.0) • Ajout de la route 169.254.169.123/32 au service Time AMZN • Ajout de la route 169.254.169.249/32 au service de licence GRID • Correction d'un problème à cause EBS NVMe duquel les volumes étaient marqués comme éphémères	17 septembre 2018
4.9.2854	Nouvelle version de l'SSMagent (2.3.13.0)	17 août 2018
4.9.2831	Nouvelle version de l'SSMagent (2.2.916.0)	7 août 2018
4.9.2818	Nouvelle version de l'SSMagent (2.2.902.0)	31 juillet 2018
4.9.2756	Nouvelle version de l'SSMagent (2.2.800.0)	27 juin 2018
4.9.2688	Nouvelle version de l'SSMagent (2.2.607.0)	25 mai 2018
4.9.2660	Nouvelle version de l'SSMagent (2.2.546.0)	11 mai 2018
4.9.2644	Nouvelle version de l'SSMagent (2.2.493.0)	26 avril 2018
4.9.2586	Nouvelle version de l'SSMagent (2.2.392.0)	28 mars 2018

Version	Détails	Date de publication
4.9.2565	• Nouvelle version de l'SSMagent (2.2.355.0) • Problème sur les instances M5 et C5 (pilotes PV introuvables) • Ajoutez la journalisation de la console pour le type d'instance, les pilotes PV les plus récents et NVMe les pilotes	13 mars 2018
4.9.2549	Nouvelle version de l'SSMagent (2.2.325.0)	8 mars 2018
4.9.2461	Nouvelle version de l'SSMagent (2.2.257.0)	15 février 2018
4.9.2439	Nouvelle version de l'SSMagent (2.2.191.0)	6 février 2018
4.9.2400	Nouvelle version de l'SSMagent (2.2.160.0)	16 janvier 2018
4.9.2327	• Nouvelle version de l'SSMagent (2.2.120.0) • Ajout de la découverte de COM ports sur les instances EC2 Bare Metal d'Amazon • Ajout de la journalisation de l'état Hyper-V sur les instances Amazon EC2 Bare Metal	2 janvier 2018
4.9.2294	Nouvelle version de l'SSMagent (2.2.103.0)	4 décembre 2017
4.9.2262	Nouvelle version de l'SSMagent (2.2.93.0)	15 novembre 2017
4.9.2246	Nouvelle version de l'SSMagent (2.2.82.0)	11 novembre 2017
4.9.2218	Nouvelle version de l'SSMagent (2.2.64.0)	29 octobre 2017
4.9.2212	Nouvelle version de l'SSMagent (2.2.58.0)	23 octobre 2017
4.9.2203	Nouvelle version de l'SSMagent (2.2.45.0)	19 octobre 2017

Version	Détails	Date de publication
4.9.2188	Nouvelle version de l'SSMagent (2.2.30.0)	10 octobre 2017
4.9.2180	• Nouvelle version de l'SSMagent (2.2.24.0) • Ajout du GPU plugin Elastic pour les GPU instances	5 octobre 2017
4.9.2143	Nouvelle version de l'SSMagent (2.2.16.0)	1 octobre 2017
4.9.2140	Nouvelle version de l'SSMagent (2.1.10.0)	
4.9.2130	Nouvelle version de l'SSMagent (2.1.4.0)	
4.9.2106	Nouvelle version de l'SSMagent (2.0.952.0)	
4.9.2061	Nouvelle version de l'SSMagent (2.0.922.0)	
4.9.2047	Nouvelle version de l'SSMagent (2.0.913.0)	
4.9.2031	Nouvelle version de l'SSMagent (2.0.902.0)	
4.9.2016	• Nouvelle version de l'SSMagent (2.0.879.0) • Correction du chemin du répertoire des CloudWatch journaux pour Windows Server 2003	
4.9.1981	• Nouvelle version de l'SSMagent (2.0.847.0) • Le problème lié à la génération `important.txt` en EBS volumes a été résolu.	
4.9.1964	Nouvelle version de l'SSMagent (2.0.842.0)	

Version	Détails	Date de publication
4.9.1951	• Nouvelle version de l'SSMagent (2.0.834.0) • Correction du problème lié à l'absence de mappage de la lettre du lecteur à partir de Z: pour les disques éphémères.	
4.9.1925	• Nouvelle version de l'SSMagent (2.0.822.0) • [Bug] Cette version n'est pas une cible de mise à jour valide depuis l'SSMAgent v4.9.1775.	
4.9.1900	Nouvelle version de l'SSMagent (2.0.805.0)	
4.9.1876	• Nouvelle version de l'SSMagent (2.0.796.0) • Correction d'un problème lié à la redirection des sorties/erreurs pour l'exécution userdata administrateur.	
4.9.1863	• Nouvelle version de l'SSMagent (2.0.790.0) • Correction de problèmes liés à l'attachement de plusieurs EBS volumes à une EC2 instance Amazon. • CloudWatch Amélioré pour suivre un chemin de configuration, en conservant la rétrocompatibilité.	
4.9.1791	Nouvelle version de l'SSMagent (2.0.767.0)	
4.9.1775	Nouvelle version de l'SSMagent (2.0.761.0)	
4.9.1752	Nouvelle version de l'SSMagent (2.0.755.0)	
4.9.1711	Nouvelle version de l'SSMagent (2.0.730.0)	
4.8.1676	Nouvelle version de l'SSMagent (2.0.716.0)	

Version	Détails	Date de publication
4.7.1631	Nouvelle version de l'SSMagent (2.0.682.0)	
4.6.1579	• Nouvelle version de l'SSMagent (2.0.672.0) • Le problème de mise à jour de l'agent a été résolu dans v4.3, v4.4 et v4.5	
4.5.1534	Nouvelle version de l'SSMagent (2.0.645.1)	
4.4.1503	Nouvelle version de l'SSMagent (2.0.633.0)	
4.3.1472	Nouvelle version de l'SSMagent (2.0.617.1)	
4.2.1442	Nouvelle version de l'SSMagent (2.0.599.0)	
4.1.1378	Nouvelle version de l'SSMagent (2.0.558.0)	

Version	Détails	Date de publication
4.0.1343	• Run Command, State Manager, l' CloudWatch agent et le support de jointure de domaine ont été transférés vers un autre agent appelé SSM Agent. SSML'agent sera installé dans le cadre de la EC2Config mise à niveau. Pour de plus amples informations, veuillez consulter EC2Configet AWS Systems Manager. • Si un proxy est configuré dansEC2Config, vous devez mettre à jour vos paramètres de proxy pour l'SSMAgent avant de procéder à la mise à niveau. Si vous ne mettez pas à jour les paramètres de proxy, vous ne pourrez pas utiliser la fonctionn alité Exécuter la commande pour gérer vos instances. Pour éviter cela, consultez les informations suivantes avant de passer à la version la plus récente : Installation et configura tion de SSM l'agent sur les instances Windows dans le guide de AWS Systems Manager l'utilisateur. • Si vous avez précédemment activé CloudWatch l'intégration sur vos instances à l'aide d'un fichier de configuration local (`AWS.EC2.Windows.CloudWatch.json`), vous devez configurer le fichier pour qu'il fonctionne avec SSM l'Agent.	
3.19.1153	• Plug-in d'activation réactivé pour les instances avec une ancienne AWS KMS configuration. Ignorez l'activation pour BYOL les utilisateurs. • Modifiez le TRIM comportement par défaut pour qu'il soit désactivé pendant le formatage du disque et ajouté FormatWit h TRIM pour remplacer le InitializeDisks plugin par userdata.	

Version	Détails	Date de publication
3.18.1118	• Correctif permettant d'ajouter des routages à la carte réseau principale de manière fiable. • Mises à jour pour améliorer le support AWS des services.	
3.17.1032	• Correctif qui résout le problème de duplication des journaux système lorsque les filtres étaient définis sur la même catégorie. • Correctifs empêchant toute suspension pendant l'initialisation du disque.	
3.16.930	Prise en charge de la consignation de l'événement « Window is Ready to use » dans le journal d'événements Windows au démarrage.	
3.15.880	Correctif permettant de charger la sortie générée par la fonctionnalité Exécuter la commande de Systems Manager dans les compartiments S3 dont le nom inclut le caractère « . ».	
3.14.786	Ajout du support pour remplacer les paramètres InitializeDisks du plugin. Par exemple : pour accélérer l'initialisation SSD du disque, vous pouvez la désactiver temporairement TRIM en spécifiant ceci dans userdata : <InitializeDrivesSettings><SettingsGroup>FormatWithoutTRIM</SettingsGroup></InitializeDrivesSettings	
3.13.727	Fonctionnalité Exécuter la commande de Systems Manager : correctifs permettant de traiter les commandes en toute sécurité après le redémarrage de Windows.	

Version	Détails	Date de publication
3.12.649	• Correctif permettant de traiter correctement le redémarrage lors de l'exécution de commandes/scripts. • Correctif permettant d'annuler en toute sécurité les commandes en cours d'exécution. • Ajoutez la prise en charge du téléchargement (facultatif) de MSI journaux vers S3 lors de l'installation d'applications via la commande Run Command de Systems Manager.	
3.11.521	• Correctifs pour activer la RDP génération d'empreintes digitales pour Windows Server 2003. • Corrections visant à inclure le fuseau horaire et le UTC décalage dans les lignes de EC2Config journal. • Prise en charge de Systems Manager pour l'exécution des commandes Exécuter la commande en parallèle. • Restauration d'une modification précédente pour mettre en ligne les disques partitionnés.	
3.10.442	• Corrigez les défaillances de configuration de Systems Manager lors de l'installation d'MSIapplications. • Correctif permettant de mettre en ligne les disques de stockage en toute sécurité. • Mises à jour pour améliorer le support AWS des services.	

Version	Détails	Date de publication
3.9.359	• Correctif du script Post-Sysprep afin de laisser la configuration de la mise à jour Windows dans un état par défaut. • Corrigez le plugin de génération de mots de passe pour améliorer la fiabilité de l'obtention des paramètres GPO de politique de mot de passe. • Limitez les autorisations du dossierEC2Config/SSMlog au groupe d'administrateurs local. • Mises à jour pour améliorer le support AWS des services.	
3.8.294	• Correction d'un problème CloudWatch qui empêchait le téléchargement des journaux lorsqu'ils ne se trouvaient pas sur le disque principal. • Amélioration du processus d'initialisation de disque en ajoutant une logique de nouvelle tentative. • Ajout d'une meilleure gestion des erreurs lorsque le SetPassword plugin échouait parfois lors de AMI la création. • Mises à jour pour améliorer le support AWS des services.	

Version	Détails	Date de publication
3.7.308	• Amélioration de l'utilitaire ec2config-cli pour les tests de configuration et le dépannage au sein de l'instance. • Évitez d'ajouter des routes statiques AWS KMS et un service de métadonnées sur un adaptateur OpenVPN. • Correction d'un problème où l'exécution des données utilisate ur ne tenait pas compte de la balise « persist ». • Amélioration de la gestion des erreurs lorsque la connexion à la EC2 console n'est pas disponible. • Mises à jour pour améliorer le support AWS des services.	
3.6.269	• Correctif de fiabilité de l'activation Windows afin d'utiliser l'adresse locale de lien 169.254.0.250/251 pour l'activation de Windows via AWS KMS • Amélioration de la gestion du proxy pour les scénarios Systems Manager, d'activation de Windows et de jonction de domaine • Correction d'un problème où les lignes dupliquées des comptes d'utilisateur étaient ajoutées au fichier de réponse Sysprep	
3.5.228	• Résolution d'un scénario selon lequel le CloudWatch plug-in pouvait consommer trop de mémoire CPU et lire les journaux d'événements Windows • Ajout d'un lien vers la documentation CloudWatch de configuration dans l'interface utilisateur des EC2Config paramètres	

Version	Détails	Date de publication
3.4.212	• Corrige le problème EC2Config lorsqu'il est utilisé en combinaison avec VM-Import. • Correction du problème de nom des services dans le programme d’installation WiX.	
3.3.174	• Amélioration de la gestion des exceptions en cas d’échec au niveau de Systems Manager et de la jonction de domaine. • Modification visant à prendre en charge la gestion des versions SSM du schéma Systems Manager. • Correctif apporté au formatage des disques éphémères sur Win2K3. • Modification prenant en charge une taille de disque configura tion supérieure à 2 To. • Réduction de l’utilisation de la mémoire virtuelle en affectant le mode GC par défaut. • Support pour le téléchargement d'artefacts depuis le UNC chemin d'accès `aws:psModule` et `aws:application` le plugin. • Amélioration de la journalisation pour le plugin d’activation Windows.	

Version	Détails	Date de publication
3.2.97	• Améliorations des performances en retardant le chargement des SSM assemblages Systems Manager. • Amélioration de la gestion des exceptions pour les fichiers sysprep2008.xml mal formés. • Prise en charge de la ligne de commande pour la configura tion de « Apply » dans Systems Manager. • Modification prenant en charge la jonction de domaine lorsque le changement de nom d'un ordinateur est en attente. • Prise en charge des paramètres facultatifs dans le plugin `aws:applications` . • Prise en charge du tableau de commande dans le plugin `aws:psModule` .	
3.0.54	• Activer la prise en charge de Systems Manager. • Joignez automatiquement des instances EC2 Windows à un AWS répertoire par le biais de Systems Manager. • Configurez et téléchargez les CloudWatch logs/métriques via Systems Manager. • Installez PowerShell les modules via Systems Manager. • Installez MSI les applications via Systems Manager.	

Version	Détails	Date de publication
2.4.233	• Ajout d'une tâche planifiée pour effectuer une restauration en cas EC2Config d'échec du démarrage du service. • Améliorations apportées aux messages d'erreur des journaux de la console. • Mises à jour pour améliorer le support AWS des services.	
2.3.313	• Correction d'un problème lié à une consommation de mémoire importante dans certains cas lorsque la fonction CloudWatch Logs est activée. • Correction d'un bug de mise à niveau afin de permettre aux versions ec2config inférieures à 2.1.19 de passer à la dernière version. • Exception d'ouverture de COM port mise à jour pour qu'elle soit plus conviviale et utile dans les journaux. • L'configServiceSettings interface utilisateur Ec2 a désactivé le redimensionnement et corrigé l'attribution et le placement de l'affichage des versions dans l'interface utilisateur.	
2.2.12	• Géré NullPointerException lors de la requête d'une clé de registre pour déterminer l'état de Windows Sysprep qui renvoyait parfois null. • Libération des ressources non gérées dans un bloc final.	
2.2.11	Correction d'un problème lié à la gestion des lignes de journal vides dans le CloudWatch plugin.	

Version	Détails	Date de publication
2.2.10	• Suppression de la configuration CloudWatch des paramètres des journaux via l'interface utilisateur. • Permettez aux utilisateurs de définir CloudWatch les paramètres des journaux dans `%ProgramFiles%\Amazon\Ec2ConfigService\Settings\AWS.EC2.Windows.CloudWatch.json` le fichier afin de permettre de futures améliorations.	
2.2.9	Correctif de l'exception non gérée et ajout de la journalisation.	
2.2.8	• Corrige l'enregistrement de la version du système d'exploit ation Windows dans le EC2Config programme d'installation pour qu'il soit compatible avec Windows Server 2003 SP1 et versions ultérieures. • Correctifs apportés à la gestion des valeurs null lors de la lecture des clés de registre liées à la mise à jour des fichiers de configuration Sysprep.	
2.2.7	• Ajout de la prise en charge EC2Config de l'exécution pendant l'exécution de Sysprep pour Windows 2008 et versions ultérieures. • Amélioration de la gestion des exceptions et de la journalis ation pour des diagnostics plus précis	
2.2.6	• Réduction de la charge sur l'instance et sur les CloudWatch journaux lors du téléchargement des événements du journal. • Résolution d'un problème de mise à niveau en raison duquel le plug-in CloudWatch Logs ne restait pas toujours activé	

Version	Détails	Date de publication
2.2.5	• Ajout de la prise en charge du téléchargement des journaux vers CloudWatch Log Service. • Correction d'un problème de conditions de course dans le plug-in Ec2O utputRDPCert • Modification EC2Config de l'option de restauration du service à partir de laquelle il faut redémarrer TakeNoAction • Ajout d'informations supplémentaires sur les exceptions en cas EC2Config de crash	
2.2.4	• Correction d'une faute de frappe dans PostSysprep le fichier .cmd • Correction du bogue qui EC2Config ne s'épinglait pas dans le menu de démarrage pour les versions 012 et OS2 ultérieures	

Version	Détails	Date de publication
2.2.3	• Ajout d'une option d'installation EC2Config sans démarrage du service immédiatement après l'installation. Pour l’utilise r, exécutez ’Ec2Install.exe start=false’ à partir de l’invite de commande • Paramètre ajouté dans le plugin de fond d’écran pour contrôler l’ajout ou la suppression du fond d’écran. Pour l'utiliser, exécutez « Ec2 WallpaperInfo .exe set » ou « Ec2 WallpaperInfo .exe revert » à partir de l'invite de commande • Ajout de la vérification de RealTimeIsUniversal la clé, affichage des paramètres incorrects de la clé de RealTimeI sUniveral registre sur la console • EC2ConfigDépendance supprimée sur le dossier temporaire de Windows • Suppression de la dépendance UserData d'exécution sur .Net 3.5	
2.2.2	• Vérification supplémentaire du comportement d’arrêt du service afin de s’assurer que les ressources sont libérées • Correction d’un problème de lenteur d’exécution lors de la jonction à un domaine	

Version	Détails	Date de publication
2.2.1	• Mise à jour du programme d'installation pour permettre les mises à niveau à partir des versions antérieures • Correction d'un WallpaperInfo bogue Ec2 dans l'environ nement .Net4.5 uniquement • Correction du bug intermittent de détection des pilotes • Ajout de l'option d'installation en mode silencieux. Exécuter Ec2Install.exe avec l'option '-q' (par exemple, 'Ec2Install.exe -q')	
2.2.0	• Ajout de la prise en charge des environnements .Net4 et .Net4.5 • Mise à jour du programme d'installation	
2.1.19	• Ajout de la prise en charge de l'étiquetage des disques éphémères en cas d'utilisation du pilote réseau Intel (par exemple, type d'instance C3). Pour de plus amples informati ons, veuillez consulter Mise en réseau améliorée sur les EC2 instances Amazon. • Ajout AMI de la prise en charge de la version AMI d'origine et du nom d'origine à la sortie de la console • Modifications apportées à la sortie de la console pour une analyse et une mise en forme cohérentes • Mise à jour du fichier d'aide	

Version	Détails	Date de publication
2.1.18	• EC2ConfigWMIObjet ajouté pour la notification d'achèvement (-Namespace root \ Amazon EC2 -Class _) ConfigService • Amélioration des performances de la WMI requête de démarrage avec des journaux d'événements volumineux ; risque de provoquer un pic prolongé CPU lors de l'exécution initiale	
2.1.17	• Correction UserData d'un problème d'exécution avec le remplissage de la mémoire tampon en sortie standard et en erreur standard • Correction d'une RDP empreinte numérique incorrecte apparaissant parfois dans la sortie de console pour le système d'exploitation >= w2k8 • La sortie console contient désormais « RDPCERTIFICATE - SubjectName : » pour Windows 2008+, qui contient la valeur du nom de la machine • Ajout de D:\ dans le menu déroulant de mappage de lettres de lecteur • Déplacement du bouton d'aide en haut à droite et modification de l'aspect de l'interface • Ajout d'un lien renvoyant vers une enquête utilisateur en haut à droite	

Version	Détails	Date de publication
2.1.16	• L'onglet Général inclut un lien vers EC2Config la page de téléchargement des nouvelles versions • La superposition de papier peint du bureau est désormais stockée dans le dossier Appdata local des utilisateurs au lieu de Mes documents pour permettre la redirection MyDoc • MSSQLServernom synchronisé avec le système dans le script Post-Sysprep (2008+) • Réorganisation du dossier d'application (transfert des fichiers vers le répertoire Plugin et suppression des fichiers dupliqués) • Modification de la sortie du journal système (console) : • *Activation d'un format de date, de nom ou de valeur pour faciliter l'analyse (veuillez commencer la migration des dépendances vers le nouveau format) • * Ajout du statut du plugin « Ec2 SetPassword » • * Ajouté des heures de début et de fin Sysprep • Correction d'un problème empêchant l'étiquetage des disques éphémères en tant que « stockage temporaire » pour les systèmes d'exploitation non anglophones • Correction d'un échec de EC2Config désinstallation après l'exécution de Sysprep	

Version	Détails	Date de publication
2.1.15	• Requêtes optimisées pour le service de métadonnées • Les métadonnées contournent maintenant les paramètres de proxy • Placement des disques éphémères étiquetés en tant que « stockage temporaire » et Important.txt sur volume le lorsqu'il s sont détectés (pilotes PV Citrix uniquement). Pour plus d'informations, consultez Mettre à niveau les pilotes PV sur EC2 les instances Windows. • Attribution des lettres de lecteurs Z à A aux disques éphémères (pilotes PV Citrix uniquement) : cette attributi on peut être remplacée à l'aide du plugin de mappage de lettres de lecteur avec les volumes dont l'étiquette indique « Stockage temporaire X », où x est un nombre compris entre 0 et 25 • UserData s'exécute désormais immédiatement après « Windows est prêt »	
2.1.14	Correctifs apportés au fond d'écran du Bureau	
2.1.13	• Le fond d'écran du Bureau affiche le nom d'hôte par défaut • Suppression de la dépendance au service d'horloge Windows • Route ajoutée dans les cas où plusieurs IPs sont assignés à une seule interface	

Version	Détails	Date de publication
2.1.11	• Modifications apportées au plugin Ec2Activation • - Vérifie l'état d'activation tous les 30 jours • - S'il reste 90 jours (sur 180) pour la période de grâce, tente une nouvelle activation	
2.1.10	• La superposition du fond d'écran sur le Bureau ne persiste plus avec Sysprep ou en cas de fermeture sans Sysprep • Exécution de l'option UserData à chaque démarrage du service avec <persist>true</persist> • Emplacement et nom modifiés de/DisableWinUpdate.cmd en / Scripts/ .cmd PostSysprep • Le mot de passe administrateur est configuré pour ne pas expirer par défaut dans PostSysprep /Scripts/ .cmd • La désinstallation supprimera EC2Config PostSysprep le script de c:\windows\setup\script \ CommandComplete .cmd • L'ajout du routage prend en charge les métriques d'interface personnalisées	
2.1.9	UserData L'exécution n'est plus limitée à 3851 caractères	

Version	Détails	Date de publication
2.1.7	• Écriture de l'identifiant de langue et de version du système d'exploitation dans la console • EC2Configversion écrite sur console • Écriture de la version du pilote PV dans la console • Détection de la vérification des bugs et, le cas échéant, envoi à la console lors du démarrage suivant • Ajout d'une option à config.xml afin de rendre persistantes les informations d'identification Sysprep • Ajouter la logique Route Retry en cas ENI d'indisponibilité au démarrage • Exécution des données utilisateur PID écrites sur la console • Longueur minimale du mot de passe généré extrait de GPO • Définition de 3 tentatives de démarrage du service • Ajout d'exemples de fichiers S3_ DownloadFile .ps1 et S3_Upload .ps1 dans le dossier /Scripts	

Version	Détails	Date de publication
2.1.6	• Ajout des informations de version dans l'onglet General • Remplacement du nom de l'onglet Bundle par Image • Simplification du processus de spécification des mots de passe et transfert de l'interface utilisateur liée aux mots de passe dans l'onglet Image au lieu de l'onglet General • Remplacement du nom de l'onglet Disk Settings par Storage • Ajout d'un onglet Support offrant des outils communs permettant de résoudre les problèmes • Configuration de Windows Server 2003 `sysprep.ini` pour étendre par défaut la partition du système d'exploitation • Ajout de l'adresse IP privée au fond d'écran • Affichage de l'adresse IP privée sur le fond d'écran • Ajout d'une logique de nouvelle tentative pour la sortie de la console • Exception de port COM fixe pour l'accessibilité des métadonnées : elle devait EC2Config s'arrêter avant que la sortie de la console ne soit affichée • Vérification de l'état d'activation à chaque démarrage (activati on si nécessaire) • Correction du problème lié aux chemins d'accès relatifs, qui survenait lors de l'exécution manuelle d'un raccourci de fond d'écran à partir du dossier de démarrage, renvoyant vers Administrator/logs	

Version	Détails	Date de publication
	• Correction de la couleur d'arrière-plan par défaut pour les utilisateurs Windows Server 2003 (autre qu'administrateurs)	

Version	Détails	Date de publication
2.1.2	• Horodatage de la console en UTC (zoulou) • Suppression de l'affichage du lien hypertexte dans l'onglet Sysprep • Ajout d'une fonctionnalité afin d'étendre dynamiquement le volume racine lors du premier démarrage de Windows 2008 ou version ultérieure • Lorsque Set-Password est activé, il permet désormais de définir automatiquement le mot EC2Config de passe • EC2Configvérifie l'état d'activation avant d'exécuter Sysprep (affiche un avertissement s'il n'est pas activé) • Windows Server 2003 utilise `Sysprep.xml` désormais le UTC fuseau horaire par défaut au lieu du Pacifique • Serveurs d'activation aléatoires • Remplacement du nom de l'onglet Drive Mapping par Disk Settings • Transfert des éléments d'interface d'initialisation des disques dans l'onglet Disk Settings à partir de l'onglet General • Le bouton d'aide pointe désormais vers le fichier HTML d'aide • Fichier d'HTMLaide mis à jour avec modifications • Mise à jour du texte « Note » pour les mappages de lettres de lecteur •	

Version	Détails	Date de publication
	Ajout du InstallUpdates fichier .ps1 au dossier /Scripts pour automatiser les correctifs et le nettoyage avant Sysprep	
2.1.0	• Le fond d'écran du Bureau affiche les informations d'instanc e par défaut dès la première connexion (pas en cas de déconnexion et de reconnexion) • PowerShell peut être exécuté à partir des données utilisateur en entourant le code avec<powershell></powershell>	

Utilisez EC2 Fast Launch pour vos instances Windows

Lorsque vous configurez un serveur Windows AMI pour un lancement EC2 rapide, Amazon EC2 crée un ensemble de snapshots préconfigurés à utiliser pour un lancement plus rapide, comme suit.

1. Amazon EC2 lance un ensemble d'instances t3 temporaires, en fonction de vos paramètres.
2. Au fur et à mesure que chaque instance temporaire termine les étapes de lancement standard, Amazon EC2 crée un instantané préprovisionné de l'instance. Il stocke l'instantané dans votre compartiment Amazon S3.
3. Lorsque le snapshot est prêt, Amazon EC2 met fin à l'instance t3 associée afin de réduire au maximum les coûts des ressources.
4. La prochaine fois qu'Amazon EC2 lancera une instance alors que le lancement EC2 rapide est activéAMI, il utilisera l'un des instantanés pour réduire considérablement le temps de lancement.

Amazon réapprovisionne EC2 automatiquement les instantanés que vous avez sous la main lorsqu'il les utilise pour lancer des instances à partir du lancement EC2 rapide activé. AMI

Tout compte AMI ayant accès à un compte dont le lancement EC2 rapide est activé peut bénéficier de délais de lancement réduits. Lorsque le AMI propriétaire vous autorise à lancer des instances, les instantanés préprovisionnés proviennent du compte du AMI propriétaire.

Si un fichier AMI compatible avec EC2 Fast Launch est partagé avec vous, vous pouvez activer ou désactiver AMI vous-même le lancement plus rapide sur le site partagé. Si vous activez un partage

AMI pour EC2 Fast Launch, Amazon EC2 crée les instantanés préconfigurés directement dans votre compte. Si vous supprimez les instantanés de votre compte, vous pouvez toujours utiliser les instantanés du compte du AMI propriétaire.

> **Note**
>
> EC2Fast Launch supprime les instantanés préprovisionnés dès qu'ils sont consommés par un lancement afin de minimiser les coûts de stockage et d'empêcher leur réutilisation. Toutefois, si les instantanés supprimés répondent à une règle de conservation, la Corbeille les conserve automatiquement. Nous vous recommandons de revoir le champ d'application de vos règles de conservation de la corbeille afin d'éviter que cela ne se produise. Pour plus d'informations, consultez la section Corbeille dans le guide de EBS l'utilisateur Amazon.
> Cette fonctionnalité est différente de la restauration EBS rapide des instantanés. Vous devez explicitement activer la restauration EBS rapide des instantanés par instantané, et cela a ses propres coûts associés.

La vidéo suivante explique comment configurer votre Windows AMI pour un lancement plus rapide avec un bref aperçu des termes clés associés et de leurs définitions : Lancer des instances EC2 Windows jusqu'à 65 % plus rapidement AWS.

Coûts des ressources

La configuration de Windows AMIs pour EC2 Fast Launch est gratuite. Toutefois, la tarification standard s'applique à toutes les AWS ressources sous-jacentes EC2 utilisées par Amazon. Pour en savoir plus sur les coûts de ressources associés et sur la façon de les gérer, consultez Gérez les coûts des ressources sous-jacentes de EC2 Fast Launch.

Table des matières

Termes clés

La fonction de lancement EC2 rapide utilise les termes clés suivants :

Instantané pré-approvisionné

Un instantané d'une instance qui a été lancée à partir d'un système Windows sur AMI lequel EC2 Fast Launch est activé et qui a effectué les étapes de lancement de Windows suivantes, en redémarrant selon les besoins.

- Sysprep specialize
- Expérience Windows prête à l'emploi (OOBE)

Lorsque ces étapes sont terminées, EC2 Fast Launch arrête l'instance et crée un instantané qui est ensuite utilisé pour un lancement plus rapide depuis leAMI, en fonction de votre configuration.

Fréquence de lancement

Contrôle le nombre de snapshots préprovisionnés qu'Amazon EC2 peut lancer dans le délai spécifié. Lorsque vous activez EC2 Fast Launch pour votreAMI, Amazon EC2 crée l'ensemble initial de snapshots préconfigurés en arrière-plan. Par exemple, si la fréquence de lancement est définie sur cinq lancements par heure, ce qui est la valeur par défaut, EC2 Fast Launch crée un ensemble initial de cinq instantanés préprovisionnés.

Lorsqu'Amazon EC2 lance une instance à partir d'une instance AMI dont le lancement EC2 rapide est activé, il utilise l'un des snapshots préconfigurés pour réduire le temps de lancement. Au fur et à mesure que les instantanés sont utilisés, ils sont automatiquement réapprovisionnés, jusqu’au nombre spécifié par la fréquence de lancement.

Si vous vous attendez à une augmentation du nombre d'instances lancées par votre AMI intermédiaire, par exemple lors d'un événement spécial, vous pouvez augmenter la fréquence de lancement à l'avance pour couvrir les instances supplémentaires dont vous aurez besoin. Lorsque votre cadence de lancement revient à la normale, vous pouvez réajuster la fréquence à la baisse.

Lorsque le nombre de lancements est plus élevé que prévu, vous risquez d’épuiser tous les instantanés pré-approvisionnés dont vous disposez. Cela ne provoque pas d’échec des lancements. Cependant, il peut arriver que certaines instances passent par le processus de lancement standard, jusqu’à ce que les instantanés puissent être réapprovisionnés.

Nombre de ressources cible

Le nombre de snapshots préprovisionnés à conserver à portée de main pour un serveur Amazon EC2 Windows AMI avec EC2 Fast Launch activé.

Nombre maximal de lancements parallèles

Contrôle le nombre d'instances qu'Amazon EC2 peut lancer en même temps afin de créer les instantanés préconfigurés pour EC2 Fast Launch. Si le nombre de ressources que vous ciblez est supérieur au nombre maximal de lancements parallèles que vous avez configuré, Amazon EC2 lance le nombre d'instances spécifié par Max parallel launchements pour commencer à créer les instantanés. Au fur et à mesure que ces instances terminent le processus, Amazon EC2 prend le snapshot et arrête l'instance. Il continue ensuite à lancer d'autres instances jusqu'à ce que le nombre total d'instantanés disponibles atteigne le nombre de ressources cible. La valeur pour Nombre maximal de lancements parallèles doit être supérieur ou égal à 6.

EC2Conditions requises pour le lancement rapide pour Windows

Avant de configurer EC2 Fast Launch, vérifiez que vous remplissez les conditions préalables suivantes qui sont requises pour créer des instantanés AMIs dans votre : Compte AWS

- Si vous n'utilisez pas de modèle de lancement pour configurer vos paramètres, assurez-vous qu'un modèle par défaut VPC est configuré pour la région dans laquelle vous utilisez EC2 Fast Launch.

  > **Note**
  >
  > Si vous supprimez accidentellement votre valeur par défaut VPC dans la région dans laquelle vous prévoyez de configurer EC2 Fast Launch, vous pouvez créer une nouvelle valeur par défaut VPC dans cette région. Pour en savoir plus, consultez la section Créer une valeur par défaut VPC dans le guide de VPC l'utilisateur Amazon.

- Pour spécifier une valeur autre que celle par défautVPC, vous devez utiliser un modèle de lancement lorsque vous configurez le lancement rapide de Windows. Pour plus d'informations, consultez Utilisez un modèle de lancement lorsque vous configurez EC2 Fast Launch.
- Si votre compte inclut une politique qui s'applique IMDSv2 aux EC2 instances Amazon, vous devez créer un modèle de lancement qui spécifie la configuration des métadonnées à appliquerIMDSv2.
- Private EC2 Fast Launch AMIs doit prendre en charge l'exécution de scripts de données utilisateur.
- Pour configurer EC2 Fast Launch pour unAMI, vous devez créer l'AMIutilisation Sysprep avec l'option d'arrêt. La fonctionnalité de lancement EC2 rapide ne prend actuellement pas en charge AMIs les fichiers créés à partir d'une instance en cours d'exécution.

  Pour créer un AMI usageSysprep, voirCréez un Amazon à EC2 AMI l'aide de Windows Sysprep.

- Le quota par défaut pour le nombre maximum de lancements parallèles sur AMIs l'ensemble de l' Compte AWS année est de 40 par région. Vous pouvez demander une augmentation des Service Quotas pour votre compte, comme suit.

  1. Connectez-vous à la console Service Quotas AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/servicequotas/.
  2. Dans le panneau de navigation, sélectionnez services AWS.
  3. Dans la barre de recherche, saisissez `EC2 Fast Launch`, puis sélectionnez le résultat.
  4. Sélectionnez le lien pour `Parallel instance launches`. Cela vous dirige vers la page détaillée Service Quotas du Lancement d'instances parallèles.
  5. Choisissez Request quota increase (Demander une augmentation de quota).

  Pour de plus amples informations, veuillez consulter Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas.

Configurer les paramètres EC2 Fast Launch pour votre Amazon EC2 Windows Server AMI

Vous pouvez configurer EC2 Fast Launch pour Windows AMIs qui vous appartient ou AMIs qui est partagé avec vous depuis AWS Management Console API,SDKs, CloudFormation, ou AWS Command Line Interface (AWS CLI). Avant de configurer EC2 Fast Launch, vérifiez que vous AMI répondez à toutes les conditions requises pour créer les instantanés préprovisionnés. Pour plus d'informations, consultez EC2Conditions requises pour le lancement rapide pour Windows.

Lorsque vous activez un lancement plus rapide pour les instances Windows, Amazon EC2 vérifie que vous disposez des autorisations requises pour lancer des instances à partir du modèle spécifié AMI et du modèle de lancement (le cas échéant), y compris les autorisations pour le chiffrementAMIs. Pour éviter les erreurs lors du processus de lancement de l'instance, le service valide vos autorisations avant que EC2 Fast Launch ne soit activé. Si vous ne disposez pas des autorisations requises, le service renvoie un message d'erreur et n'active pas le lancement EC2 rapide.

EC2Fast Launch s'intègre à EC2 Image Builder pour vous aider à créer des images personnalisées avec EC2 Fast Launch activé. Pour plus d'informations, voir Créer des paramètres de distribution pour un Windows AMI avec EC2 Fast Launch activé (AWS CLI) dans le guide de l'utilisateur d'EC2Image Builder.

Les sections suivantes décrivent les étapes de configuration de la EC2 console Amazon et AWS CLI.

Activer le lancement EC2 rapide

Pour activer le lancement EC2 rapide, choisissez l'onglet correspondant à votre environnement, puis suivez les étapes.

> **Note**
>
> Avant de modifier ces paramètres, assurez-vous que votre AMI région et celle dans laquelle vous vous trouvez répondent à tous les critèresEC2Conditions requises pour le lancement rapide pour Windows.

Console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sous Images, sélectionnez AMIs.
3. Choisissez le AMI à mettre à jour en cochant la case à côté du nom.
4. Dans le menu Actions situé au-dessus de la liste desAMIs, choisissez Configurer le lancement rapide. Cela ouvre la page Configurer le lancement rapide, dans laquelle vous configurez les paramètres du lancement EC2 rapide.
5. Pour commencer à utiliser des instantanés préprovisionnés afin de lancer des instances AMI plus rapidement depuis votre Windows, cochez la case Activer le lancement rapide pour Windows.
6. Depuis la liste déroulante Set anticipated launch frequency (Définir une fréquence de lancement prévue), choisissez une valeur afin de spécifier le nombre d'instantanés créés et gérés pour couvrir le volume de lancement d'instances attendu.
7. Une fois les modifications terminées, choisissez Save changes (Enregistrer les modifications).

> **Note**
>
> Si vous devez utiliser un modèle de lancement pour spécifier une valeur autre que celle par défautVPC, ou pour configurer des paramètres de métadonnées pourIMDSv2, consultezUtilisez un modèle de lancement lorsque vous configurez EC2 Fast Launch.

AWS CLI

La enable-fast-launch commande appelle l'EC2EnableFastLaunchAPIopération Amazon.

Syntaxe :

```
aws ec2 enable-fast-launch \
  --image-id <value> \
  --resource-type <value> \ (optional)
  --snapshot-configuration <value> \ (optional)
  --launch-template <value> \ (optional)
  --max-parallel-launches <value> \ (optional)
  --dry-run | --no-dry-run \  (optional)
  --cli-input-json <value> \ (optional)
  --generate-cli-skeleton <value> \ (optional)
```

Exemple :

L'enable-fast-launchexemple suivant active EC2 Fast Launch pour le paramètre spécifiéAMI, en lançant six instances parallèles pour le pré-provisionnement. `ResourceType` est défini sur `snapshot`, qui est la valeur par défaut.

```
aws ec2 enable-fast-launch \
         --image-id ami-01234567890abcedf  \
         --max-parallel-launches 6 \
         --resource-type snapshot
```

Sortie :

```
{
     "ImageId": "ami-01234567890abcedf",
     "ResourceType": "snapshot",
     "SnapshotConfiguration": {
         "TargetResourceCount": 10
     },
     "LaunchTemplate": {},
     "MaxParallelLaunches": 6,
     "OwnerId": "0123456789123",
     "State": "enabling",
     "StateTransitionReason": "Client.UserInitiated",
     "StateTransitionTime": "2022-01-27T22:16:03.199000+00:00"
```

```
}
```

PowerShell

L'Enable-EC2FastLaunchapplet de commande appelle l'EC2EnableFastLaunchAPIopération Amazon pour activer EC2 Fast Launch sur votre Windows. AMI

Syntaxe :

```
Enable-EC2FastLaunch
      -ImageId <String>
      -LaunchTemplate_LaunchTemplateId <String>
      -LaunchTemplate_LaunchTemplateName <String>
      -MaxParallelLaunch <Int32>
      -ResourceType <String>
      -SnapshotConfiguration_TargetResourceCount <Int32>
      -LaunchTemplate_Version <String>
      -Select <String>
      -PassThru <SwitchParameter>
      -Force <SwitchParameter>
```

Exemple :

L'Enable-EC2FastLaunchexemple suivant active EC2 Fast Launch pour le paramètre spécifiéAMI, en lançant six instances parallèles pour le pré-provisionnement. `ResourceType` est défini sur `snapshot`, qui est la valeur par défaut.

```
Enable-EC2FastLaunch `
 -ImageId ami-01234567890abcedf `
 -MaxParallelLaunch 6 `
 -Region us-west-2 `
 -ResourceType snapshot
```

Sortie :

```
 ImageId               : ami-01234567890abcedf
 LaunchTemplate        :
 MaxParallelLaunches   : 6
 OwnerId               : 0123456789123
 ResourceType          : snapshot
```

```
SnapshotConfiguration : Amazon.EC2.Model.FastLaunchSnapshotConfigurationResponse
State                 : enabling
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 12:24:11 PM
```

Désactiver le lancement EC2 rapide

Pour désactiver le lancement EC2 rapide, choisissez l'onglet correspondant à votre environnement, puis suivez les étapes.

> **Note**
>
> Avant de modifier ces paramètres, assurez-vous que votre AMI région et celle dans laquelle vous vous trouvez répondent à tous les critèresEC2Conditions requises pour le lancement rapide pour Windows.

Console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sous Images, sélectionnez AMIs.
3. Choisissez le AMI à mettre à jour en cochant la case à côté du nom.
4. Dans le menu Actions situé au-dessus de la liste desAMIs, choisissez Configurer le lancement rapide. Cela ouvre la page Configurer le lancement rapide, dans laquelle vous configurez les paramètres du lancement EC2 rapide.
5. Décochez la case Activer le lancement rapide pour Windows pour désactiver le lancement EC2 rapide et supprimer les instantanés préprovisionnés. Cela se traduit par l'AMIutilisation du processus de lancement standard pour chaque instance à l'avenir.

   > **Note**
   >
   > Lorsque vous désactivez l'optimisation des images Windows, tous les instantanés pré-approvisionnés existants sont automatiquement supprimés. Vous devez terminre cette étape pour recommencer à utiliser la fonction.

6. Une fois les modifications terminées, choisissez Save changes (Enregistrer les modifications).

AWS CLI

La disable-fast-launch commande appelle l'EC2DisableFastLaunchAPIopération Amazon.

Syntaxe :

```
aws ec2 disable-fast-launch \
  --image-id <value> \
  --force | --no-force \ (optional)
  --dry-run | --no-dry-run \ (optional)
  --cli-input-json <value> \ (optional)
  --generate-cli-skeleton <value> \ (optional)
```

Exemple :

L'disable-fast-launchexemple suivant désactive le lancement EC2 rapide sur le paramètre spécifié AMI et nettoie les instantanés préprovisionnés existants.

```
aws ec2 disable-fast-launch \
         --image-id ami-01234567890abcedf
```

Sortie :

```
{
     "ImageId": "ami-01234567890abcedf",
     "ResourceType": "snapshot",
     "SnapshotConfiguration": {},
     "LaunchTemplate": {
         "LaunchTemplateId": "lt-01234567890abcedf",
         "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
         "Version": "1"
     },
     "MaxParallelLaunches": 6,
     "OwnerId": "0123456789123",
     "State": "disabling",
     "StateTransitionReason": "Client.UserInitiated",
     "StateTransitionTime": "2022-01-27T22:47:29.265000+00:00"
 }
```

PowerShell

L'Disable-EC2FastLaunchapplet de commande appelle l'opération Amazon EC2 DisableFastLaunchAPI.

Syntaxe :

```
Disable-EC2FastLaunch
      -ImageId <String>
      -ForceStop <Boolean>
      -Select <String>
      -PassThru <SwitchParameter>
      -Force <SwitchParameter>
```

Exemple :

L'Disable-EC2FastLaunchexemple suivant désactive le lancement EC2 rapide sur le paramètre spécifié AMI et nettoie les instantanés préprovisionnés existants.

```
Disable-EC2FastLaunch -ImageId ami-01234567890abcedf
```

Sortie :

```
ImageId               : ami-01234567890abcedf
LaunchTemplate        :
Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
MaxParallelLaunches   : 6
OwnerId               : 0123456789123
ResourceType          : snapshot
SnapshotConfiguration :
State                 : disabling
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 1:10:08 PM
```

Utilisez un modèle de lancement lorsque vous configurez EC2 Fast Launch

Avec un modèle de lancement, vous pouvez configurer un ensemble de paramètres de lancement qu'Amazon EC2 utilise chaque fois qu'il lance une instance à partir de ce modèle. Vous pouvez spécifier des éléments tels que et AMI à utiliser pour votre image de base, les types d'instances, le stockage, les paramètres réseau, etc.

Les modèles de lancement sont facultatifs, sauf dans les cas spécifiques suivants, où vous devez utiliser un modèle de lancement pour votre Windows AMI lorsque vous configurez un lancement plus rapide :

- Vous devez utiliser un modèle de lancement pour spécifier une valeur autre que celle par défaut VPC pour votre WindowsAMI.
- Si votre compte inclut une politique qui s'applique IMDSv2 aux EC2 instances Amazon, vous devez créer un modèle de lancement qui spécifie la configuration des métadonnées à appliquerIMDSv2.

  Utilisez le modèle de lancement qui inclut votre configuration de métadonnées depuis la EC2 console, ou lorsque vous exécutez la enable-fast-launchcommande dans le AWS CLI, ou lorsque vous appelez l'EnableFastLaunchAPIaction.

Amazon EC2 EC2 Fast Launch ne prend pas en charge la configuration suivante lorsque vous utilisez un modèle de lancement. Si vous utilisez un modèle de lancement pour EC2 Fast Launch, vous ne devez spécifier aucune des options suivantes :

- Scripts de données utilisateur
- Protection de la résiliation
- Métadonnées désactivées
- Option spot
- Comportement d'arrêt qui met fin à l'instance
- Balises de ressources pour les demandes d'interface réseau, d'Elastic Graphic ou d'instance ponctuelle

Spécifiez une valeur autre que celle par défaut VPC

Étape 1 : créer un modèle de lancement

Créez un modèle de lancement qui spécifie les informations suivantes pour vos instances Windows :

- Le VPC sous-réseau.
- Un type d'instance de `t3.xlarge`.

Pour plus d'informations, consultez Création d'un modèle de EC2 lancement Amazon.

Étape 2 : Spécifiez le modèle de lancement pour votre EC2 Fast Launch AMI

Choisissez l'onglet qui correspond à votre processus :

Console

Pour définir le modèle de lancement pour EC2 Fast Launch à partir du AWS Management Console, procédez comme suit :

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sous Images, sélectionnez AMIs.
3. Choisissez le AMI à mettre à jour en cochant la case à côté du nom.
4. Dans le menu Actions situé au-dessus de la liste desAMIs, choisissez Configurer le lancement rapide. Cela ouvre la page Configurer le lancement rapide, dans laquelle vous configurez les paramètres du lancement EC2 rapide.
5. La case Launch template (Modèle de lancement) permet d'effectuer une recherche filtrée des modèles de lancement de votre compte dans la région actuelle qui correspondent au texte que vous avez saisi. Spécifiez la totalité ou une partie du nom ou de l'ID du modèle de lancement dans la case pour afficher la liste des modèles de lancement correspondants. Par exemple, si vous saisissez `fast` ce champ, Amazon EC2 trouve tous les modèles de lancement de votre compte dans la région actuelle dont le nom contient « rapide ».

   Pour créer votre modèle de lancement, vous pouvez choisir Create launch template (Créer un modèle de lancement).
6. Lorsque vous sélectionnez un modèle de lancement, Amazon EC2 affiche la version par défaut de ce modèle dans la zone Version du modèle source. Pour spécifier une version différente, mettez en évidence la version par défaut pour la remplacer et saisissez le numéro de version souhaité dans la case.
7. Une fois les modifications terminées, choisissez Save changes (Enregistrer les modifications).

AWS CLI, API

Pour spécifier le modèle de lancement pour EC2 Fast Launch à partir du AWS CLI, spécifiez le nom ou l'ID du modèle de lancement dans le `--launch-template` paramètre lorsque vous exécutez la enable-fast-launchcommande dans le AWS CLI.

Pour spécifier le modèle de lancement pour EC2 Fast Launch dans une API demande, spécifiez le nom ou l'ID du modèle de lancement dans le `LaunchTemplate` paramètre lorsque vous appelez l'EnableFastLaunchAPIaction.

Pour plus d'informations sur les modèles de EC2 lancement, consultezStockez les paramètres de lancement de l'instance dans les modèles de EC2 lancement Amazon.

Afficher AMIs avec lancement EC2 rapide activé

Vous pouvez utiliser la describe-fast-launch-imagescommande dans le ou les AWS CLIGet-EC2FastLaunchImageoutils de l' PowerShell applet de commande pour obtenir des informations sur les applications pour AMIs lesquelles le lancement EC2 rapide est activé.

Amazon EC2 fournit les informations suivantes pour chaque Windows AMI renvoyé dans les résultats :

- L'ID de l'image pour une image AMI dont le lancement EC2 rapide est activé.
- Type de ressource utilisé pour le pré-provisionnement du système Windows associé. AMI Valeur prise en charge : `snapshot`.
- La configuration des instantanés, qui est un groupe de paramètres qui configurent le préprovisionnement pour les systèmes Windows associés à l'AMIaide de snapshots.
- Informations sur le modèle de lancement, notamment l'ID, le nom et la version du modèle de lancement que l'associé AMI utilise lorsqu'il lance des instances Windows à partir de snapshots préprovisionnés.
- Le nombre maximum d'instances qui peuvent être lancées en même temps pour créer des ressources.
- ID du propriétaire de l'objet associéAMI. Ce champ n'est pas renseigné AMIs car ils sont partagés avec vous.
- État actuel de EC2 Fast Launch pour le périphérique associéAMI. Les valeurs prises en charge incluent : `enabling | enabling-failed | enabled | enabled-failed | disabling | disabling-failed`.

> **Note**
>
> Vous pouvez également voir l'état actuel affiché sur la page Gérer l'optimisation des images de la EC2 console, sous la forme État d'optimisation des images.

- La raison pour laquelle EC2 Fast Launch pour le produit associé est AMI passé à l'état actuel.
- Heure à laquelle EC2 Fast Launch pour le produit associé est AMI passée à l'état actuel.

Choisissez l'onglet qui correspond à votre environnement de ligne de commande :

AWS CLI

La describe-fast-launch-images commande appelle l'EC2DescribeFastLaunchImagesAPIopération Amazon.

Syntaxe :

```
aws ec2 describe-fast-launch-images \
 --image-ids <value> \ (optional)
 --filters <value> \ (optional)
 --dry-run | --no-dry-run \ (optional)
 --cli-input-json <value> \ (optional)
 --starting-token <value> \ (optional)
 --page-size <value> \ (optional)
 --max-items <value> \ (optional)
 --generate-cli-skeleton <value> \ (optional)
```

Exemple :

L'describe-fast-launch-imagesexemple suivant décrit les détails de chacun AMIs des éléments du compte configurés pour le lancement EC2 rapide. Dans cet exemple, un seul AMI élément du compte est configuré pour le lancement EC2 rapide.

```
aws ec2 describe-fast-launch-images
```

Sortie :

```
{
    "FastLaunchImages": [
        {
            "ImageId": "ami-01234567890abcedf",
            "ResourceType": "snapshot",
            "SnapshotConfiguration": {},
            "LaunchTemplate": {
                "LaunchTemplateId": "lt-01234567890abcedf",
```

```
                "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
                "Version": "1"
            },
            "MaxParallelLaunches": 6,
            "OwnerId": "0123456789123",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated",
            "StateTransitionTime": "2022-01-27T22:20:06.552000+00:00"
        }
    ]
}
```

Tools for PowerShell

L'Get-EC2FastLaunchImageapplet de commande appelle l'opération Amazon EC2 DescribeFastLaunchImagesAPI.

Syntaxe :

```
Get-EC2FastLaunchImage
-Filter <Filter[]>
-ImageId <String[]>
-MaxResult <Int32>
-NextToken <String>
-Select <String>
-NoAutoIteration <SwitchParameter>
```

Exemple :

L'Get-EC2FastLaunchImageexemple suivant décrit les détails de chacun AMIs des éléments du compte configurés pour le lancement EC2 rapide. Dans cet exemple, un seul AMI élément du compte est configuré pour le lancement EC2 rapide.

```
Get-EC2FastLaunchImage -ImageId ami-01234567890abcedf
```

Sortie :

```
ImageId               : ami-01234567890abcedf
LaunchTemplate        :
 Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
```

```
MaxParallelLaunches   : 6
OwnerId               : 0123456789123
ResourceType          : snapshot
SnapshotConfiguration :
State                 : enabled
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 12:54:43 PM
```

Gérez les coûts des ressources sous-jacentes de EC2 Fast Launch

La configuration de Windows AMIs pour EC2 Fast Launch est gratuite. Toutefois, lorsque vous activez EC2 Fast Launch pour Amazon EC2 WindowsAMI, la tarification standard s'applique aux AWS ressources sous-jacentes utilisées par Amazon EC2 pour préparer et stocker les instantanés préprovisionnés. Vous pouvez configurer des balises de répartition des coûts pour vous aider à suivre et à gérer les coûts associés aux ressources EC2 Fast Launch. Pour plus d'informations sur la configuration des balises de répartition des coûts, consultez Suivez les coûts de lancement EC2 rapide sur votre facture.

L'exemple suivant montre comment les coûts associés aux coûts des instantanés EC2 Fast Launch peuvent être répartis.

Exemple de scénario : La société AtoZ Example possède un système Windows AMI avec un volume racine de 50 EBS GiB. Ils EC2 activent le lancement rapide pour eux AMI et fixent le nombre de ressources cible à cinq. Au cours d'un mois, l'utilisation de EC2 Fast Launch leur AMI coûte environ 5$, et la répartition des coûts est la suivante :

1. Lorsqu'AtoZ Example active EC2 Fast Launch, Amazon EC2 lance cinq petites instances. Chaque instance exécute les étapes de lancement de Sysprep et de OOBE Windows et redémarre selon les besoins. Cela prend plusieurs minutes pour chaque instance (le temps peut varier en fonction de l'affluence de cette région ou de cette zone de disponibilité (AZ) et de la taille de laAMI).

   Coûts

   - Coûts d'exécution des instances (ou durée d'exécution minimale, le cas échéant) : cinq instances
   - Coûts de volume : cinq volumes EBS racines
2. Lorsque le processus de pré-provisionnement est terminé, Amazon EC2 prend un instantané de l'instance, qu'il stocke dans Amazon S3. Les instantanés sont généralement stockés pendant 4

à 8 heures avant d'être consommés par un lancement. Dans ce cas, le coût est d'environ 0,02 à 0,05 USD par instantané.

Coûts

- Stockage d'instantanés (Amazon S3) : cinq instantanés

3. Une fois EC2 qu'Amazon a pris le snapshot, il arrête l'instance. À ce stade, l'instance ne génère plus de coûts. Cependant, les coûts de EBS volume continuent de s'accumuler.

   Coûts

   - EBSvolumes : les coûts se poursuivent pour les volumes EBS racines associés.

> **Note**
>
> Les coûts présentés ici sont uniquement à des fins de démonstration. Vos coûts varient en fonction de votre AMI configuration et de votre plan tarifaire.

Suivez les coûts de lancement EC2 rapide sur votre facture

Les étiquettes de répartition des coûts peuvent vous aider à organiser votre AWS facture afin de refléter les coûts associés à EC2 Fast Launch. Vous pouvez utiliser la balise suivante qu'Amazon EC2 ajoute aux ressources qu'il crée lorsqu'il prépare et stocke des instantanés préprovisionnés pour EC2 Fast Launch :

Clé de balise : `CreatedBy`, Valeur : `EC2 Fast Launch`

Après avoir activé la balise dans la console de Billing and Cost Management et configuré votre rapport de facturation détaillé, la colonne `user:CreatedBy` apparaît sur le rapport. La colonne inclut les valeurs de tous les services. Toutefois, si vous téléchargez le CSV fichier, vous pouvez importer les données dans une feuille de calcul et filtrer `EC2 Fast Launch` la valeur. Ces informations apparaissent également AWS Cost and Usage Report lorsque le tag est activé.

Étape 1 : Activer les balises de répartition des coûts définies par l'utilisateur

Pour inclure les balises de ressources dans vos rapports sur les coûts, vous devez tout d'abord activer la balise dans la console Billing and Cost Management. Pour plus d'informations, consultez Activation des balises de répartition des coûts définies par l'utilisateur dans le Guide de l'utilisateur AWS Billing and Cost Management .

> **Note**
>
> L'activation peut prendre jusqu'à 24 heures.

Étape 2 : Définition d'un rapport sur les coûts

Si vous avez déjà configuré un rapport sur les coûts, une colonne correspondant à votre balise s'affichera lors de la prochaine exécution du rapport, une fois l'activation terminée. Pour configurer les rapports sur les coûts pour la première fois, sélectionnez l'une des options suivantes.

- Veuillez consulter la rubrique Setting up a monthly cost allocation report (Configuration du rapport de répartition des coûts mensuel) dans le Guide de l'utilisateur AWS Billing and Cost Management .
- Veuillez consulter la rubrique Creating Cost and Usage Reports (Créer des rapports de coûts et d'utilisation) dans le Guide de l'utilisateur AWS Cost and Usage Report .

> **Note**
>
> Cela peut prendre jusqu'à 24 heures pour commencer AWS à envoyer des rapports à votre compartiment S3.

Vous pouvez configurer EC2 Fast Launch pour Windows AMIs que vous possédez ou AMIs qui sont partagés avec vous à partir de la EC2 console AmazonAPI,SDKs, CloudFormation, ou des ec2 commandes du AWS CLI. Les sections suivantes décrivent les étapes de configuration de la EC2 console Amazon et AWS CLI.

Vous pouvez également créer des fenêtres personnalisées AMIs configurées pour EC2 Fast Launch avec EC2 Image Builder. Pour plus d'informations, voir Créer des paramètres de distribution pour un système Windows sur AMI lequel EC2 Fast Launch est activé (AWS CLI).

Lancement EC2 rapide du moniteur

Cette section explique comment surveiller le serveur AMIs Amazon EC2 Windows de votre compte sur lequel EC2 Fast Launch est activé.

Surveillez les changements d'état de EC2 Fast Launch avec EventBridge

Lorsque l'état change pour un Windows AMI avec EC2 Fast Launch activé, Amazon EC2 génère un `EC2 Fast Launch State-change Notification` événement. Amazon EC2 envoie ensuite l'événement de changement d'état à Amazon EventBridge (anciennement Amazon CloudWatch Events).

Vous pouvez créer des EventBridge règles qui déclenchent une ou plusieurs actions en réponse à l'événement de changement d'état. Par exemple, vous pouvez créer une EventBridge règle qui détecte l'activation de EC2 Fast Launch et effectue les actions suivantes :

- Envoie un message à un SNS sujet Amazon pour informer ses abonnés.
- Appelle une fonction Lambda qui effectue une action.
- Envoie les données de changement d'état à Amazon Data Firehose à des fins d'analyse.

Pour plus d'informations, consultez la section Création de EventBridge règles Amazon qui réagissent aux événements dans le guide de EventBridge l'utilisateur Amazon.

Événements de changement d'état

La fonction EC2 Fast Launch émet JSON au mieux des événements de changement d'état formatés. Amazon EC2 envoie les événements EventBridge en temps quasi réel. Cette section décrit les champs d'événement et présente un exemple de format d'événement.

`EC2 Fast Launch State-change Notification`

imageId

Identifie le AMI avec le changement d'état de lancement EC2 rapide.

resourceType

Type de ressource à utiliser pour l'allocation préalable. Valeur prise en charge : `snapshot`. La valeur par défaut est `snapshot`.

state

État actuel de la fonctionnalité de lancement EC2 rapide pour le paramètre spécifiéAMI. Les valeurs valides sont notamment les suivantes :

- activation : vous avez activé la fonctionnalité de lancement EC2 rapide pour leAMI, et Amazon EC2 a commencé à créer des instantanés pour le processus de pré-approvisionnement.

- enabling-failed — Un problème s'est produit qui a entraîné l'échec du processus de préprovisionnement la première fois que vous avez activé le EC2 lancement rapide pour un. AMI Cela peut se produire à tout moment pendant le processus d'allocation préalable.
- activé — La fonction de lancement EC2 rapide est activée. L'état change `enabled` dès qu'Amazon EC2 crée le premier instantané préprovisionné pour un lancement EC2 rapide récemment activé. AMI Si le AMI était déjà activé et fait l'objet d'un nouveau préprovisionnement, le changement d'état se produit immédiatement.
- enabled-failed : cet état ne s'applique que si ce n'est pas la première fois que votre EC2 Fast Launch AMI passe par le processus de préprovisionnement. Cela peut se produire si la fonctionnalité de lancement EC2 rapide est désactivée puis réactivée ultérieurement, ou en cas de modification de configuration ou d'une autre erreur une fois le préprovisionnement terminé pour la première fois.
- désactivation — Le AMI propriétaire a désactivé la fonction de lancement EC2 rapide pour leAMI, et Amazon EC2 a lancé le processus de nettoyage.
- désactivé — La fonction de lancement EC2 rapide est désactivée. L'état change `disabled` dès qu'Amazon EC2 termine le processus de nettoyage.
- disabling-failed : un problème est survenu et a entraîné l'échec du processus de nettoyage. Cela signifie que certains instantanés préalloués peuvent encore être conservés dans le compte.

stateTransitionReason

La raison pour laquelle l'état a changé pour le lancement EC2 rapideAMI.

> **Note**
>
> Tous les champs de ce message d'événement sont requis.

L'exemple suivant montre un lancement EC2 rapide récemment activé AMI qui a lancé la première instance pour démarrer le processus de préprovisionnement. À ce stade, l'état est `enabling`. Une fois qu'Amazon a EC2 créé le premier instantané préconfiguré, l'état passe à. `enabled`

```
{
 "version": "0",
 "id": "01234567-0123-0123-0123-012345678901",
 "detail-type": "EC2 Fast Launch State-change Notification",
```

```
 "source": "aws.ec2",
 "account": "123456789012",
 "time": "2022-08-31T20:30:12Z",
 "region": "us-east-1",
 "resources": [
  "arn:aws:ec2:us-east-1:123456789012:image/ami-123456789012"
 ],
 "detail": {
  "imageId": "ami-123456789012",
  "resourceType": "snapshot",
  "state": "enabling",
  "stateTransitionReason": "Client.UserInitiated"
 }
}
```

Surveillez les statistiques de lancement EC2 rapide avec CloudWatch

Amazon EC2 AMIs avec EC2 Fast Launch a activé l'envoi de métriques vers Amazon CloudWatch. Vous pouvez utiliser le AWS Management Console AWS CLI, le ou un API pour répertorier les métriques auxquelles EC2 Fast Launch envoie CloudWatch. L'`AWS/EC2`espace de noms inclut les métriques EC2 Fast Launch suivantes :

Métrique	Description
NumberOfAvailableFastLaunchSnapshots	Le nombre de snapshots préprovisionnés disponibles par lancement EC2 rapide activé. AMI
NumberOfInstancesFastLaunched	Nombre d'instances lancées à partir de snapshots préprovisionnés par EC2 Fast Launch activéAMI.
NumberOfInstancesNotFastLaunched	Le nombre d'instances par lancement EC2 rapide activé AMI qui a entraîné un démarrage à froid en raison de l'absence de snapshots préprovisionnés disponibles au moment du lancement.
FastLaunchSnapshotUsedToRefillStartTime	L'horodatage auquel Amazon EC2 a lancé une nouvelle image à partir d'un lancement EC2

Métrique	Description
	rapide a permis de AMI créer un autre instantan é après l'utilisation d'un instantané existant.
FastLaunchSnapshotCreationTime	Mesure le temps nécessaire EC2 à Amazon pour lancer une instance et créer un instantané pour un lancement EC2 rapide activéAMI.

Rôle lié au service pour EC2 Fast Launch

Amazon EC2 utilise des rôles liés à un service pour obtenir les autorisations nécessaires pour appeler d'autres personnes en votre services AWS nom. Un rôle lié à un service est un type unique de IAM rôle directement lié à un. service AWS Les rôles liés à un service constituent un moyen sécurisé de déléguer des autorisations, services AWS car seul le service lié peut assumer un rôle lié au service. Pour plus d'informations sur la manière dont Amazon EC2 utilise IAM les rôles, y compris les rôles liés à un service, consultez. IAMrôles pour Amazon EC2

Amazon EC2 utilise le rôle lié au service nommé `AWSServiceRoleForEC2FastLaunch` pour créer et gérer un ensemble de snapshots préconfigurés qui réduisent le temps nécessaire au lancement des instances depuis votre Windows. AMI

Vous n'avez pas besoin de créer manuellement ce rôle lié à un service. Lorsque vous commencez à utiliser EC2 Fast Launch pour votre compteAMI, Amazon EC2 crée le rôle lié au service pour vous, s'il n'existe pas déjà.

> **Note**
>
> Si le rôle lié au service est supprimé de votre compte, vous pouvez activer EC2 Fast Launch pour un autre Windows afin de AMI recréer le rôle dans votre compte. Vous pouvez également désactiver EC2 Fast Launch pour votre version actuelleAMI, puis le réactiver. Cependant, la désactivation de cette fonctionnalité vous oblige à AMI utiliser le processus de lancement standard pour toutes les nouvelles instances, tandis qu'Amazon EC2 supprime tous vos instantanés préprovisionnés. Une fois que tous les instantanés préprovisionnés ont disparu, vous pouvez réactiver l'utilisation de EC2 Fast Launch pour votre. AMI

Amazon EC2 ne vous autorise pas à modifier le rôle `AWSServiceRoleForEC2FastLaunch` lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Toutefois, vous pouvez modifier la description du rôle en utilisantIAM. Pour plus d'informations, consultez la section Modification d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de toutes les ressources connexes. Cela protège les EC2 ressources Amazon associées à votre serveur AMI Amazon EC2 Windows lorsque EC2 Fast Launch est activé, car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Amazon EC2 prend en charge le rôle lié au service EC2 Fast Launch dans toutes les régions où le EC2 service Amazon est disponible. Pour de plus amples informations, veuillez consulter Régions.

Autorisations octroyées par **`AWSServiceRoleForEC2FastLaunch`**

Amazon EC2 utilise la politique `EC2FastLaunchServiceRolePolicy` gérée pour effectuer les actions suivantes :

- `cloudwatch:PutMetricData`— Publiez les données métriques associées à EC2 Fast Launch dans l'espace de EC2 noms Amazon.
- `ec2:CreateLaunchTemplate`— Créez un modèle de lancement pour votre serveur Amazon EC2 Windows AMI avec EC2 Fast Launch activé.
- `ec2:CreateSnapshot`— Créez des instantanés préconfigurés pour votre serveur Amazon EC2 Windows AMI avec EC2 Fast Launch activé.
- `ec2:CreateTags`— Créez des balises pour les ressources associées au lancement et au préprovisionnement d'instances Windows pour votre Amazon EC2 Windows Server AMI avec EC2 Fast Launch activé.
- `ec2:DeleteSnapshots`— Supprimez tous les instantanés préprovisionnés associés si EC2 Fast Launch est désactivé pour une version précédemment activée. AMI
- `ec2:DescribeImages` : décrire les images de toutes les ressources.
- `ec2:DescribeInstanceAttribute` : décrire les attributs d'instance de toutes les ressources.
- `ec2:DescribeInstanceStatus` : décrire l'état de l'instance de toutes les ressources.
- `ec2:DescribeInstances` : décrire les instances de toutes les ressources.
- `ec2:DescribeInstanceTypeOfferings` : décrire les offres de type d'instance de toutes les ressources.

- `ec2:DescribeLaunchTemplates` : décrire les modèles de lancement de toutes les ressources.
- `ec2:DescribeLaunchTemplateVersions` : décrire les versions du modèle de lancement de toutes les ressources.
- `ec2:DescribeSnapshots` : décrire les ressources des instantanés de toutes les ressources.
- `ec2:DescribeSubnets` : décrire les sous-réseaux de toutes les ressources.
- `ec2:RunInstances`— Lancez des instances depuis un serveur Amazon EC2 Windows AMI avec EC2 Fast Launch activé, afin d'effectuer les étapes de provisionnement.
- `ec2:StopInstances`— Arrêtez les instances lancées depuis un serveur Amazon EC2 Windows AMI avec EC2 Fast Launch activé, afin de créer des instantanés préprovisionnés.
- `ec2:TerminateInstances`— Mettez fin à une instance qui a été lancée depuis un serveur Amazon EC2 Windows AMI avec EC2 Fast Launch activé, après avoir créé le snapshot préprovisionné à partir de celle-ci.
- `iam:PassRole` : autorise le rôle lié à un service `AWSServiceRoleForEC2FastLaunch` à lancer des instances en votre nom à l'aide du profil d'instance de votre modèle de lancement.

Pour plus d'informations sur l'utilisation des politiques gérées pour AmazonEC2, consultezAWS politiques gérées pour Amazon EC2.

Accès aux clés gérées par le client à utiliser avec des données chiffrées AMIs et des EBS instantanés

Prérequis

- Pour permettre à Amazon d'accéder EC2 à un fichier chiffré AMI en votre nom, vous devez être autorisé à effectuer cette `createGrant` action dans la clé gérée par le client.

Lorsque vous activez EC2 Fast Launch pour un fichier chiffréAMI, Amazon EC2 s'assure que le `AWSServiceRoleForEC2FastLaunch` rôle est autorisé à utiliser la clé gérée par le client pour accéder à votreAMI. Cette autorisation est nécessaire pour lancer des instances et créer des instantanés approvisionnés préalablement en votre nom.

Modifier le mot de passe d'administrateur Windows pour votre EC2 instance Amazon

Si vous lancez votre instance depuis un AWS système WindowsAMI, les agents de lancement préinstallés définissent le mot de passe par défaut comme suit :

- Pour Windows Server 2022 et versions ultérieures, EC2Launch v2 génère le mot de passe par défaut.
- Pour Windows Server 2016 et 2019, l'EC2Launchagent génère le mot de passe par défaut.
- Pour Windows Server 2012 R2 et versions antérieures, EC2Configservice génère le mot de passe par défaut.

> **Note**
>
> Pour Windows Server 2016 et versions ultérieuresAMIs, `Password never expires` est désactivé pour l'administrateur local. Pour AMI les versions antérieures à Windows Server 2016, `Password never expires` est activé pour l'administrateur local.

Modifier le mot de passe de l'administrateur après la connexion

Lorsque vous vous connectez à une instance pour la première fois, nous vous recommandons de modifier la valeur entrée par défaut pour le mot de passe administrateur. Procédez comme suit pour modifier le mot de passe Administrateur d'une instance Windows.

> **Important**
>
> Conservez le nouveau mot de passe en lieu sûr. Vous ne pourrez pas récupérer le nouveau mot de passe à l'aide de la EC2 console Amazon. La console ne peut récupérer que le mot de passe par défaut. Si vous tentez de vous connecter à l'instance à l'aide du mot de passe par défaut après l'avoir modifié, vous recevrez l'erreur suivante : « Your credentials did not work » (Vos informations d'identification sont incorrectes).

Pour modifier le mot de passe d'administrateur local

1. Connectez-vous à l'instance et ouvrez une invite de commande.
2. Exécutez la commande suivante. Si votre nouveau mot de passe comporte des caractères spéciaux, vérifiez que vous placez le mot de passe entre guillemets doubles.

```
net user Administrator "new_password"
```

3. Conservez le nouveau mot de passe en lieu sûr.

Modifier un mot de passe perdu ou expiré

Si vous oubliez votre mot de passe ou qu'il expire, vous pouvez générer un nouveau mot de passe. Pour les procédures de réinitialisation de mot de passe, consultez Réinitialisation du mot de passe administrateur Windows pour une instance Amazon EC2 Windows.

Ajouter des composants Windows Server facultatifs aux instances Amazon EC2 Windows

Pour accéder aux composants facultatifs et les installer, vous devez trouver le EBS snapshot correspondant à votre version de Windows Server, créer un volume à partir de cet instantané et attacher le volume à votre instance.

Avant de commencer

Utilisez l'outil AWS Management Console ou un outil de ligne de commande pour obtenir l'ID d'instance et la zone de disponibilité de votre instance. Vous devez créer votre EBS volume dans la même zone de disponibilité que votre instance.

Utilisez l'une des procédures suivantes pour ajouter des composants Windows Server à votre instance.

Console

Pour ajouter des composants Windows à une instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Dans la barre Filter (Filtre), choisissez Public snapshots (Instantanés publics).
4. Ajoutez le filtre Owner Alias (Alias de propriétaire), puis choisissez amazon.
5. Ajoutez le filtre Description et entrez **`Windows`**.
6. Appuyez sur Entrée
7. Sélectionnez l'instantané qui correspond à votre architecture système et votre préférence de langue. Par exemple, sélectionnez Windows 2019 English Installation Media si votre instance exécute Windows Server 2019.
8. Choisissez Actions, Create volume from snapshot (Créer un volume à partir d'un instantané).
9. Pour Availability Zone (Zone de disponibilité), sélectionnez la zone de disponibilité correspondant à votre instance Windows. Choisissez Add Tag (Ajouter une identification)

et saisissez **`Name`** pour la clé d'identification et un nom descriptif pour la valeur de la balise. Choisissez Créer un volume.

10. Dans le message Successfully created volume (Volume créé avec succès) (bannière verte), choisissez le volume que vous venez de créer.
11. Sélectionnez Actions, puis Attach volume (Attacher un volume).
12. Depuis Instance, sélectionnez l'ID d'instance.
13. Pour Device name (Nom de périphérique), saisissez le nom du périphérique pour l'attachement. Si vous avez besoin d'aide pour le nom du périphérique, consultez Noms des appareils pour les volumes sur les EC2 instances Amazon.
14. Choisissez Attacher un volume.
15. Connectez-vous à votre instance et rendez le volume disponible. Pour plus d'informations, consultez la section Rendre un EBS volume Amazon disponible pour utilisation dans le guide de EBS l'utilisateur Amazon.

> **Important**
>
> Ne pas initialiser le volume.

16. Ouvrez le Panneau de configuration, puis Programmes et fonctionnalités. Choisissez Activer ou désactiver des fonctionnalités Windows. Si vous êtes invité à saisir le support d'installation, spécifiez le EBS volume contenant le support d'installation.
17. (Facultatif) Lorsque vous avez terminé avec le support d'installation, vous pouvez détacher le volume. Après avoir détaché le volume, vous pouvez le supprimer.

AWS CLI

Pour ajouter des composants Windows à votre instance à l'aide du AWS CLI

1. Utilisez la commande describe-snapshots avec le paramètre `owner-ids` et le filtre `description` pour obtenir la liste des instantanés de support d'installation disponibles.

```
aws ec2 describe-snapshots --owner-ids amazon --filters
 Name=description,Values=Windows*
```

2. Dans la sortie, notez l'ID de l'instantané qui correspond à votre architecture système et à vos préférences linguistiques. Exemples :

```
{
    "Snapshots": [
    ...
        {
            "OwnerAlias": "amazon",
            "Description": "Windows 2019 English Installation Media",
            "Encrypted": false,
            "VolumeId": "vol-be5eafcb",
            "State": "completed",
            "VolumeSize": 6,
            "Progress": "100%",
            "StartTime": "2019-10-25T20:00:47.000Z",
            "SnapshotId": "snap-22da283e",
            "OwnerId": "123456789012"
        },
    ...
   ]
}
```

3. Utilisez la commande create-volume pour créer un volume à partir de l'instantané. Spécifiez la même zone de disponibilité que votre instance.

```
aws ec2 create-volume --snapshot-id snap-22da283e --volume-type gp2 --
availability-zone us-east-1a
```

4. Dans la sortie, notez l'ID du volume.

```
{
    "AvailabilityZone": "us-east-1a",
    "Encrypted": false,
    "VolumeType": "gp2",
    "VolumeId": "vol-0c98b37f30bcbc290",
    "State": "creating",
    "Iops": 100,
    "SnapshotId": "snap-22da283e",
    "CreateTime": "2017-04-18T10:33:10.940Z",
    "Size": 6
}
```

5. Utilisez la commande attach-volume pour attacher le volume à votre instance.

```
aws ec2 attach-volume --volume-id vol-0c98b37f30bcbc290 --instance-
id i-01474ef662b89480 --device xvdg
```

6. Connectez-vous à votre instance et rendez le volume disponible. Pour plus d'informations, consultez la section Rendre un EBS volume Amazon disponible pour utilisation dans le guide de EBS l'utilisateur Amazon.

> **Important**
>
> Ne pas initialiser le volume.

7. Ouvrez le Panneau de configuration, puis Programmes et fonctionnalités. Choisissez Activer ou désactiver des fonctionnalités Windows. Si vous êtes invité à saisir le support d'installation, spécifiez le EBS volume contenant le support d'installation.
8. (Facultatif) Lorsque vous avez terminé avec le support d'installation, utilisez la commande detach-volume pour détacher le volume de votre instance. Après avoir détaché le volume, vous pouvez utiliser la commande delete-volume pour supprimer le volume.

Tools for Windows PowerShell

Ajoutez des composants Windows à votre instance à l'aide des outils pour Windows PowerShell

1. Utilisez l'Get-EC2Snapshotapplet de commande avec les `description` filtres `Owner` et pour obtenir la liste des instantanés du support d'installation disponibles.

```
PS C:\> Get-EC2Snapshot -Owner amazon -Filter @{ Name="description";
 Values="Windows*" }
```

2. Dans la sortie, notez l'ID de l'instantané qui correspond à votre architecture système et à vos préférences linguistiques. Par exemple :

```
...
DataEncryptionKeyId :
Description         : Windows 2019 English Installation Media
Encrypted           : False
KmsKeyId            :
OwnerAlias          : amazon
OwnerId             : 123456789012
Progress            : 100%
```

```
SnapshotId          : snap-22da283e
StartTime           : 10/25/2019 8:00:47 PM
State               : completed
StateMessage        :
Tags                : {}
VolumeId            : vol-be5eafcb
VolumeSize          : 6
...
```

3. Utilisez l'New-EC2Volumeapplet de commande pour créer un volume à partir de l'instantané. Spécifiez la même zone de disponibilité que votre instance.

```
PS C:\> New-EC2Volume -AvailabilityZone us-east-1a -VolumeType gp2 -
SnapshotId snap-22da283e
```

4. Dans la sortie, notez l'ID du volume.

```
Attachments      : {}
AvailabilityZone : us-east-1a
CreateTime       : 4/18/2017 10:50:25 AM
Encrypted        : False
Iops             : 100
KmsKeyId         :
Size             : 6
SnapshotId       : snap-22da283e
State            : creating
Tags             : {}
VolumeId         : vol-06aa9e1fbf8b82ed1
VolumeType       : gp2
```

5. Utilisez l'Add-EC2Volumeapplet de commande pour attacher le volume à votre instance.

```
PS C:\> Add-EC2Volume -InstanceId i-087711ddaf98f9489 -
VolumeId vol-06aa9e1fbf8b82ed1 -Device xvdh
```

6. Connectez-vous à votre instance et rendez le volume disponible. Pour plus d'informations, consultez la section Rendre un EBS volume Amazon disponible pour utilisation dans le guide de EBS l'utilisateur Amazon.

> **Important**
>
> Ne pas initialiser le volume.

7. Ouvrez le Panneau de configuration, puis Programmes et fonctionnalités. Choisissez Activer ou désactiver des fonctionnalités Windows. Si vous êtes invité à saisir le support d'installation, spécifiez le EBS volume contenant le support d'installation.
8. (Facultatif) Lorsque vous avez terminé d'utiliser le support d'installation, utilisez l'Dismount-EC2Volumeapplet de commande pour détacher le volume de votre instance. Après avoir détaché le volume, vous pouvez utiliser l'Remove-EC2Volumeapplet de commande pour le supprimer.

Installez le sous-système Windows pour Linux sur votre instance EC2 Windows

Il existe deux versions du sous-système Windows pour Linux (WSL) que vous pouvez installer en fonction du type d'instance et du système d'exploitation de l'instance : WSL 1 et WSL 2. Pour les types d'`.metal`instance, vous pouvez installer WSL 1 ou WSL 2. Pour tous les autres types d'instances, les exigences suivantes s'appliquent :

- Pour les EC2 instances virtualisées, vous devez en installer WSL 1.
- Pour les instances qui exécutent Windows Server, la version du système d'exploitation doit être l'une des suivantes pour être installée WSL :
  - Windows Server 2019
  - Windows Server 2022

Pour plus d'informationsWSL, consultez la documentation du sous-système Windows pour Linux sur le site Web de Microsoft Build.

Installer WSL

Les instructions suivantes s'installent WSL sur une EC2 instance exécutant Windows Server 2022. Pour obtenir les instructions d'installation WSL sur une EC2 instance exécutant Windows Server 2019, voir Installer WSL sur les versions précédentes de Windows Server sur le site Web de

Microsoft. Après avoir suivi ces instructions, vous pouvez utiliser l'étape 3 des instructions ci-dessous WSL pour configurer l'utilisation de WSL 1.

Installation WSL 1

1. Pour l'installerWSL, exécutez la commande d'installation standard suivante sur votre EC2 instance, mais assurez-vous d'activer WSL 1 en incluant`--enable-wsl1`. Par défaut, WSL 2 est installé. Si votre instance a été lancée à l'aide d'un type d'instance virtualisée, vous devez effectuer l'étape 3 de cette procédure pour définir la version sur WSL 1.

   ```
   wsl --install --enable-wsl1 --no-launch
   ```

2. Redémarrez votre EC2 instance.

   ```
   shutdown -r -t 20
   ```

3. Pour configurer WSL pour utiliser WSL 1, exécutez la commande suivante sur votre instance. Pour plus d'informations sur le réglage de la WSL version, consultez la section Étapes d'installation manuelle pour les anciennes versions de WSL sur le site Web de Microsoft Build.

   ```
   wsl --set-default-version 1
   ```

4. Installez la distribution par défaut.

   ```
   wsl --install
   ```

Installation WSL 2

- Pour procéder à l'installationWSL, exécutez la commande d'installation standard suivante sur votre EC2 instance. Par défaut, WSL 2 est installé. Si vous effectuez l'installation WSL sur une `.metal` instance, il s'agit de la seule étape à effectuer.

  ```
  wsl --install
  ```

  Pour plus d'informations, voir Installer Linux sous Windows avec WSL sur le site Web de Microsoft Build.

Mettre à niveau une instance EC2 Windows vers une version plus récente de Windows Server

S'il est temps de mettre à niveau le système d'exploitation Windows Server de votre instance EC2 Windows à partir d'une version antérieure, vous pouvez utiliser l'une des méthodes suivantes.

Mise à niveau sur place

Une mise à niveau sur place fonctionne sur une instance existante. Seuls les fichiers du système d'exploitation sont affectés au cours de ce processus, tandis que vos paramètres, vos rôles de serveur et vos données restent intacts.

Migration (également appelée side-by-side mise à niveau)

Une migration implique de capturer des paramètres, des configurations et des données, puis de les porter vers un système d'exploitation plus récent sur une nouvelle instance EC2 Windows. Vous pouvez lancer votre instance depuis un Windows public ou privé AMI auquel vous êtes abonné depuis le AWS Marketplace, ou depuis un AMI système partagé avec vous. Vous pouvez également créer une personnalisation AMI avec EC2 Image Builder. Consultez le guide de l'utilisateur d'Image Builder pour plus d'informations.

> **Note**
>
> AWS fournit un ensemble d'Amazon Machine Images (AMIs) accessibles au public pour les versions de Windows Server exécutées sur EC2 des instances. Ils AMIs sont mis à jour tous les mois. Pour plus d'informations sur la dernière version de WindowsAMIs, consultez le Guide de AMIréférence AWS Windows.

Microsoft a toujours recommandé de migrer vers une version plus récente de Windows Server plutôt que de procéder à une mise à niveau sur place. La migration peut entraîner moins d'erreurs ou de problèmes de mise à niveau, mais peut prendre plus de temps qu'une mise à niveau sur place en raison de la nécessité de fournir une nouvelle instance, de planifier et de porter des applications, et d'ajuster les paramètres de configuration de la nouvelle instance. Une mise à niveau sur place peut être plus rapide, mais les incompatibilités logicielles peuvent entraîner des erreurs.

Table des matières

- Utiliser des runbooks d'automatisation pour mettre à niveau une instance EC2 Windows
- Migrer une instance EC2 Windows vers un type d'instance de génération actuelle
- Résoudre les problèmes liés à une mise à niveau du système d'exploitation sur une instance EC2 Windows

Effectuez une mise à niveau sur place sur votre instance EC2 Windows

Avant d'effectuer une mise à niveau sur place, vous devez déterminer quels pilotes réseau sont exécutés par l'instance. Les pilotes réseau PV vous permettent d'accéder à votre instance à l'aide des services Bureau à distance. Les instances utilisent des pilotes AWS PV, Intel Network Adapter ou Enhanced Networking. Pour de plus amples informations, veuillez consulter Pilotes de virtualisation paravirtuelle pour les instances Windows.

Avant de commencer une mise à niveau sur place

Exécutez les tâches suivantes et prenez note des renseignements importants suivants avant de démarrer la mise à niveau sur place.

- Lisez la documentation Microsoft pour comprendre la configuration requise de la mise à niveau, les problèmes connus et les restrictions. Consultez également les instructions officielles de la mise à niveau.
  - Upgrade Options for Windows Server 2012
  - Upgrade Options for Windows Server 2012 R2
  - Upgrade and conversion options for Windows Server 2016
  - Upgrade and conversion options for Windows Server 2019
  - Upgrade and conversion options for Windows Server 2022
  - Upgrade Center Windows Server
- Nous vous recommandons d'effectuer une mise à niveau du système d'exploitation sur les instances d'au moins 2 vCPUs ou 4 Go deRAM. Si nécessaire, vous pouvez changer l'instance à une taille plus grande du même type (t2.small à t2.large, par exemple), effectuer la mise à niveau, puis la redimensionner à la taille originale. Si vous devez conserver la taille de l'instance, vous pouvez suivre la progression à l'aide deCapture d'écran de console d'instance. Pour plus d'informations, consultez Changements de type d'EC2instance Amazon.
- Vérifiez que le volume racine de votre instance Windows dispose d'un espace disque suffisant. Le processus de l'installation Windows peut ne pas vous avertir en cas d'espace disque insuffisant.

Pour obtenir plus d'informations sur l'espace disque requis pour mettre à niveau un système d'exploitation spécifique, consultez la documentation Microsoft. Si le volume ne dispose pas d'un espace suffisant, celui-ci peut être étendu. Pour plus d'informations, consultez Amazon EBS Elastic Volumes dans le guide de EBS l'utilisateur Amazon.

- Déterminez le chemin de votre mise à niveau. Vous devez mettre à niveau le système d'exploitation sur la même architecture. Par exemple, vous devez mettre à niveau un système 32 bits vers un système 32 bits. Windows Server 2008 R2 et les versions ultérieures sont compatibles avec des systèmes 64 bits uniquement.
- Désactivez les logiciels anti-virus et anti-espion, ainsi que les pare-feu. Ces types de logiciels peuvent créer des conflits avec le processus de mise à niveau. Une fois la mise à niveau terminée, réactivez les logiciels anti-virus et anti-espion, ainsi que les pare-feu.
- Mettre à jour les derniers pilotes comme décrit dans Migrer une instance EC2 Windows vers un type d'instance de génération actuelle.
- Le service UpgradeHelperService prend uniquement en charge les instances exécutant des pilotes PV Citrix. Si l'instance exécute des pilotes Red Hat, vous devez d'abord les mettre à niveau manuellement.

Mettez à niveau une instance sur place avec le AWS PV, l'adaptateur réseau Intel ou les pilotes réseau améliorés

Utilisez la procédure suivante pour mettre à niveau une instance Windows Server utilisant des pilotes PV AWS , de carte réseau Intel ou de la mise en réseau améliorée.

Pour exécuter une mise à niveau sur place

1. Créez l'un AMI des systèmes que vous prévoyez de mettre à niveau à des fins de sauvegarde ou de test. Vous pouvez ensuite exécuter la mise à niveau sur la copie pour simuler un environnement de test. Si la mise à niveau réussit, vous pouvez basculer le trafic vers cette instance avec une interruption courte. Si la mise à niveau échoue, vous pouvez restaurer la sauvegarde. Pour de plus amples informations, veuillez consulter Créez un compte soutenu EBS par Amazon AMI.
2. Assurez-vous que votre instance Windows Server utilise les derniers pilotes réseau.

    a. Pour mettre à jour votre pilote AWS PV, voirMettre à niveau les pilotes PV sur EC2 les instances Windows.

b. Pour mettre à jour votre ENA pilote, consultezInstallation du ENA pilote sur les instances EC2 Windows.

c. Pour mettre à jour vos pilotes Intel, voir Mise en réseau améliorée avec l'interface Intel 82599 VF

3. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

4. Dans le panneau de navigation, choisissez Instances. Recherchez l'instance. Notez l'ID et la zone de disponibilité de l'instance. Vous aurez besoin de ces informations ultérieurement lors de cette procédure.

5. Si vous effectuez la mise à niveau depuis Windows Server 2012 ou 2012 R2 vers Windows Server 2016, 2019 ou 2022, procédez comme suit sur votre instance avant de continuer :

   a. Désinstallez le EC2Config service. Pour de plus amples informations, veuillez consulter Administration des services Windows pour la EC2Launch version 2 et les EC2Config agents.

   b. Installez l'agent EC2Launch v1 ou EC2Launch v2. Pour plus d'informations, consultez Utiliser l'agent EC2Launch v1 pour effectuer des tâches lors du lancement de l'instance EC2 Windows et Utiliser l'agent EC2Launch v2 pour effectuer des tâches lors du lancement de l'instance EC2 Windows.

   c. Installez l' AWS Systems Manager SSMagent. Pour plus d'informations, consultez la section Utilisation de SSM l'agent dans le guide de AWS Systems Manager l'utilisateur.

6. Créez un volume à partir d'un instantané du média d'installation de Windows Server.

   a. Dans le panneau de navigation, sous Elastic Block Store, sélectionnez Instantanés.

   b. Dans la barre Filtre, choisissez Instantanés publics.

   c. Dans la barre de recherche, spécifiez les filtres suivants :

      - Choisissez Alias du propriétaire, puis =, puis Amazon.
      - Choisissez Description, puis commencez à taper **`Windows`**. Sélectionnez le filtre Windows qui correspond à l'architecture système et la préférence de langue vers lesquelles vous effectuez la mise à niveau. Par exemple, sélectionnez Windows 2019 English Installation Media pour mettre à niveau vers Windows Server 2019.

   d. Cochez la case à côté de l'instantané correspondant à l'architecture du système et la langue préférée vers laquelle vous souhaitez effectuer la mise à niveau, puis sélectionnez Actions, Create volume from snapshot (Créer un volume à partir d'un instantané).

e. Dans la boîte de dialogue Create volume (Créer un volume), sélectionnez la zone de disponibilité correspondant à votre instance Windows, puis choisissez Create volume (Créer un volume).

7. Dans le volume créé avec succès vol-***1234567890example***bandeau en haut de page, choisissez l'identifiant du volume que vous venez de créer.
8. Sélectionnez Actions, puis Attach volume (Attacher un volume).
9. Sur la page Attach volume (Attacher un volume), pour l'Instance, sélectionnez l'ID d'instance de votre instance Windows, puis choisissez Attach volume (Attacher un volume).
10. Rendez le nouveau volume disponible pour utilisation en suivant les étapes décrites dans la section Mettre un EBS volume Amazon à disposition pour utilisation.

> **Important**
>
> Ne pas initialiser le disque car cela supprimerait les données existantes.

11. Sous Windows PowerShell, passez au nouveau lecteur de volume. Commencez la mise à niveau en ouvrant le volume du média d'installation que vous avez attaché à l'instance.

    a. Si vous mettez à niveau vers Windows Server 2016 ou ultérieur, procédez comme suit :

```
.\setup.exe /auto upgrade /dynamicupdate disable
```

> **Note**
>
> L'exécution du setup.exe avec l'option `/dynamicupdate` définie sur désactivée empêche Windows d'installer des mises à jour pendant le processus de mise à niveau de Windows Server, car l'installation de mises à jour pendant la mise à niveau peut provoquer des échecs. Vous pouvez installer les mises à jour avec Windows Update une fois la mise à niveau terminée.

Si vous mettez à niveau vers une version précédente de Windows Server, procédez comme suit :

```
Sources\setup.exe
```

b. Pour Sélectionnez le système d'exploitation que vous souhaitez installer, sélectionnez l'installation complète SKU pour votre instance Windows Server, puis choisissez Next.

c. Pour Quel type d'installation voulez-vous effectuer ?, choisissez Mise à niveau.

d. Exécutez l'assistant.

La configuration de Windows Server copie et traite les fichiers. Quelques minutes plus tard, votre session des services Bureau à distance se ferme. Le délai de la mise à niveau dépend du nombre d'applications et de rôles de serveurs s'exécutant sur votre instance Windows Server. Le processus de mise à niveau peut prendre de 40 minutes à plusieurs heures. L'instance échoue au contrôle de statut 1 sur 2 pendant le processus de mise à niveau. Une fois la mise à niveau terminée, les deux contrôles de statut réussissent. Vous pouvez consulter le journal système pour voir les résultats de la console ou utiliser CloudWatch les métriques Amazon relatives au disque et à CPU l'activité pour déterminer si la mise à niveau progresse.

> **Note**
>
> Si vous mettez à niveau vers Windows Server 2019, une fois la mise à niveau terminée, vous pouvez modifier manuellement l'arrière-plan du bureau pour supprimer le nom du système d'exploitation précédent si vous le souhaitez.

Si l'instance n'a pas validé les deux contrôles des statuts au bout de plusieurs heures, consultez Résoudre les problèmes liés à une mise à niveau du système d'exploitation sur une instance EC2 Windows.

Tâches post-mise à niveau

1. Connectez-vous à l'instance pour lancer une mise à niveau du. NETFramework et redémarrez le système lorsque vous y êtes invité.
2. Si vous ne l'avez pas déjà fait lors d'une étape précédente, installez l'agent EC2Launch v1 ou EC2Launch v2. Pour plus d'informations, consultez Utiliser l'agent EC2Launch v1 pour effectuer des tâches lors du lancement de l'instance EC2 Windows et Utiliser l'agent EC2Launch v2 pour effectuer des tâches lors du lancement de l'instance EC2 Windows.
3. Si vous avez effectué la mise à niveau vers Windows Server 2012 R2, nous vous recommandons de mettre à niveau les pilotes PV vers des pilotes AWS PV. Si vous avez effectué la mise à niveau sur une instance basée sur Nitro, nous vous recommandons

d'installer ou de mettre à jour les ENA pilotes NVME et. Pour plus d'informations, consultez Windows Server 2012 R2, Installez ou mettez à niveau AWS NVMe les pilotes à l'aide de PowerShell ou Activer les réseaux améliorés sur Windows.

4. Réactivez les logiciels anti-virus et anti-espion, ainsi que les pare-feu.

Utiliser des runbooks d'automatisation pour mettre à niveau une instance EC2 Windows

Vous pouvez effectuer une mise à niveau automatique de vos instances Windows et SQL Server à l' AWS aide des runbooks AWS Systems Manager Automation.

Table des matières

Services connexes

Les AWS services suivants sont utilisés dans le processus de mise à niveau automatique :

- AWS Systems Manager. AWS Systems Manager est une interface puissante et unifiée permettant de gérer vos AWS ressources de manière centralisée. Pour plus d'informations, consultez le Guide de l'utilisateur AWS Systems Manager.
- AWS Systems Manager L'agent (SSMagent) est un logiciel Amazon qui peut être installé et configuré sur une EC2 instance Amazon, un serveur sur site ou une machine virtuelle (VM). SSML'agent permet à Systems Manager de mettre à jour, de gérer et de configurer ces ressources. L'agent traite les demandes du service Systems Manager dans le Cloud AWS , puis les exécute comme spécifié dans la demande. Pour plus d'informations, consultez la section Utilisation de SSM l'agent dans le guide de AWS Systems Manager l'utilisateur.
- AWS Systems Manager SSMrunbooks. Un SSM runbook définit les actions que Systems Manager exécute sur vos instances gérées. SSMles runbooks utilisent JavaScript Object Notation (JSON) ouYAML, et ils incluent des étapes et des paramètres que vous spécifiez. Cette rubrique utilise deux SSM runbooks de Systems Manager pour l'automatisation. Pour plus d'informations,

consultez AWS Systems Manager Automation runbook reference dans le Guide de l'utilisateur AWS Systems Manager .

Options d'exécution

Lorsque vous sélectionnez Automation (Automatisation) sur la console Systems Manager, choisissez Execute (Exécuter). Après avoir sélectionné un document d'automatisation, vous êtes invité à choisir une option d'exécution de l'automatisation. Choisissez parmi les options suivantes. Dans les étapes des chemins fournis dans cette rubrique, nous utilisons l'option d'exécution simple.

Exécution simple

Choisissez cette option si vous souhaitez mettre à jour une seule instance mais que vous ne voulez pas passer par chaque étape d'automatisation pour auditer les résultats. Cette option est décrite plus en détails dans les étapes de mise à niveau qui suivent.

Contrôle du débit

Choisissez cette option si vous souhaitez appliquer la mise à niveau à plusieurs instances. Définissez les paramètres suivants.

- Paramètre

  Ce paramètre qui est également défini dans les paramètres Plusieurs comptes et plusieurs régions spécifie comment votre automatisation se ramifie.
- Cibles

  Sélectionnez la cible à laquelle appliquer l'automatisation. Ce paramètre est également défini dans les paramètres Plusieurs comptes et plusieurs régions.
- Valeurs de paramètres

  Utilisez les valeurs définies dans les paramètres du document d'automatisation.
- Groupe de ressources

  Dans AWS, une ressource est une entité avec laquelle vous pouvez travailler. Les exemples incluent les EC2 instances Amazon, les AWS CloudFormation stacks ou les buckets Amazon S3. Si vous travaillez avec plusieurs ressources, il peut être utile de les gérer en groupe plutôt que de passer d'un AWS service à l'autre pour chaque tâche. Dans certains cas, vous souhaiterez peut-être gérer un grand nombre de ressources connexes, telles que EC2 les instances qui constituent

une couche d'application. Dans ce cas, vous aurez probablement besoin d'exécuter des actions par lots simultanément sur ces ressources.

- Balises

  Les balises vous permettent de classer vos AWS ressources de différentes manières, par exemple par objectif, propriétaire ou environnement. Cette catégorisation est utile lorsque vous avez de nombreuses ressources du même type. Vous pouvez identifier rapidement une ressource spécifique à l'aide des balises attribuées.

- Contrôle du débit

  Le contrôle du débit est également défini dans les paramètres Plusieurs comptes et plusieurs régions. Lorsque vous définissez des paramètres de contrôle du débit, vous spécifiez la part de votre flotte à laquelle appliquer l'automatisation, par nombre de cibles ou selon un pourcentage du flotte.

Plusieurs comptes et plusieurs régions

Il existe deux paramètres en plus des paramètres spécifiés sous Contrôle du débit qui sont également utilisés dans les paramètres Plusieurs comptes et plusieurs régions :

- Comptes et unités organisationnelles (OUs)

  Spécifiez plusieurs comptes sur lesquels exécuter l'automatisation.

- Régions AWS

  Spécifiez plusieurs Régions AWS endroits où vous souhaitez exécuter l'automatisation.

Exécution manuelle

Cette option est similaire à Exécution simple, mais elle vous permet d'exécuter l'automatisation étape par étape et d'auditer les résultats.

Mettre à niveau Windows Server

Le `AWSEC2-CloneInstanceAndUpgradeWindows` runbook crée une Amazon Machine Image (AMI) à partir d'une instance Windows Server de votre compte et la met à niveau AMI vers une version compatible de votre choix. Ce processus en plusieurs étapes peut prendre jusqu'à deux heures.

Deux d'entre eux sont AMIs inclus dans le processus de mise à niveau automatique :

- Instance en cours d'exécution actuelle. La première AMI est l'instance en cours d'exécution, qui n'est pas mise à niveau. Ceci AMI est utilisé pour lancer une autre instance afin d'exécuter la mise à niveau sur place. Lorsque le processus est terminé, elle AMI est supprimée de votre compte, sauf si vous demandez spécifiquement de conserver l'instance d'origine. Ce paramètre est géré par le paramètre `KeepPreUpgradeImageBackUp` (la valeur par défaut est`false`, ce qui signifie qu'AMIil est supprimé par défaut).
- Amélioré AMI. C'AMIest le résultat du processus d'automatisation.

Le résultat final est unAMI, qui est l'instance mise à niveau duAMI.

Une fois la mise à niveau terminée, vous pouvez tester les fonctionnalités de votre application en lançant la nouvelle AMI application sur votre AmazonVPC. Après le test et avant de procéder à une autre mise à niveau, planifiez les temps d'arrêt de l'application avant de passer complètement à l'instance mise à niveau.

Prérequis

Afin d'automatiser votre mise à niveau de Windows Server avec le document AWS Systems Manager Automation, vous devez effectuer les tâches suivantes :

- Créez un IAM rôle avec les IAM politiques spécifiées pour permettre à Systems Manager d'effectuer des tâches d'automatisation sur vos EC2 instances Amazon et vérifiez que vous remplissez les conditions requises pour utiliser Systems Manager. Pour plus d'informations, consultez la section Création d'un rôle pour déléguer des autorisations à un AWS service dans le Guide de AWS Identity and Access Management l'utilisateur.
- Sélectionnez l'option souhaitée pour l'exécution de l'automatisation. Les options d'exécution sont Exécution simple, Contrôle du débit, Plusieurs comptes et plusieurs régions et Exécution manuelle. Pour plus d'informations sur ces options, consultez Options d'exécution.
- Vérifiez que SSM l'agent est installé sur votre instance. Pour plus d'informations, consultez Installation et configuration de SSM l'agent sur EC2 les instances Amazon pour Windows Server.
- Windows PowerShell 3.0 ou version ultérieure doit être installé sur votre instance.
- Pour les instances qui sont jointes à un domaine Microsoft Active Directory, nous vous recommandons de spécifier un `SubnetId` qui n'a pas de connectivité à vos contrôleurs de domaine afin d'éviter les conflits de noms d'hôte.

- Le sous-réseau de l'instance doit disposer d'une connectivité sortante à Internet, qui permet d'accéder services AWS à Amazon S3 et de télécharger des correctifs depuis Microsoft. Cette exigence est remplie soit si le sous-réseau est un sous-réseau public et que l'instance possède une adresse IP publique, soit si le sous-réseau est un sous-réseau privé avec une route qui envoie le trafic Internet vers un appareil public. NAT
- Cette automatisation fonctionne avec des instances exécutant Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016 et Windows Server 2019.
- Vérifiez que l'instance a 20 Go d'espace disque libre dans le disque de démarrage.
- Si l'instance n'utilise pas de licence Windows fournie par AWS, spécifiez un identifiant de EBS capture Amazon qui inclut le support d'installation de Windows Server 2012 R2. Pour cela :
  1. Vérifiez que l'EC2instance Amazon exécute Windows Server 2012 ou version ultérieure.
  2. Créez un EBS volume Amazon de 6 Go dans la même zone de disponibilité où l'instance est exécutée. Attachez le volume à l'instance. Montez-la, par exemple, en tant que lecteur D.
  3. Cliquez avec le bouton droit sur le ISO et montez-le sur une instance telle que, par exemple, le lecteur E.
  4. Copiez le contenu ISO du lecteur E : \ vers le lecteur D : \
  5. Créez un EBS instantané Amazon du volume de 6 Go créé à l'étape 2 ci-dessus.

Limitations de mise à niveau Windows Server

Cette procédure d'automatisation ne prend pas en charge la mise à niveau des contrôleurs de domaine Windows, des clusters ni des système d'exploitation de bureau Windows. En outre, cette automatisation ne prend pas en charge les EC2 instances Amazon pour Windows Server avec les rôles suivants installés :

- Hôte de session de bureau à distance (RDSH)
- Broker de connexion au bureau à distance (RDCB)
- Hôte de virtualisation de postes de travail à distance (RDVH)
- Accès Web aux postes de travail à distance (RDWA)

Étapes à suivre pour effectuer une mise à niveau automatisée de Windows Server

Suivez ces étapes pour mettre à niveau votre instance Windows Server à l'aide du runbook AWSEC2- CloneInstanceAndUpgradeWindows automation.

1. Ouvrez Systems Manager depuis la Console de gestion AWS .
2. Dans le panneau de navigation de gauche, sous Change Management (Gestion des modifications), choisissez Automation (Automatisation).
3. Choisissez Execute automation (Exécuter l'automatisation).
4. Recherchez le document d'automatisation appelé `AWSEC2-CloneInstanceAndUpgradeWindows`.
5. Lorsque le nom du document apparaît, sélectionnez-le. Les détails du document apparaissent alors.
6. Choisissez Execute automation (Exécuter l'automatisation) afin de saisir les paramètres pour ce document. Laissez l'option Exécution simple sélectionnée en haut de la page.
7. Entrez les paramètres demandés en suivant les indications suivantes.

   - `InstanceID`

     Type : chaîne

     (Obligatoire) L'instance exécutant Windows Server 2008 R2, 2012 R2, 2016 ou 2019 avec l'SSMagent installé.

   - `InstanceProfile`.

     Type : chaîne

     (Obligatoire) Le profil de l'IAMinstance. Il s'agit du IAM rôle utilisé pour effectuer l'automatisation de Systems Manager par rapport à l'EC2instance Amazon et AWS AMIs. Pour plus d'informations, consultez la section Créer un profil d'IAMinstance pour Systems Manager dans le guide de AWS Systems Manager l'utilisateur.

   - `TargetWindowsVersion`

     Type : chaîne

     (Obligatoire) Sélectionnez la version cible de Windows.

   - `SubnetId`

     Type : chaîne

     (Obligatoire) Il s'agit du sous-réseau pour le processus de mise à niveau et de l'emplacement de votre EC2 instance source. Vérifiez que le sous-réseau dispose d'une connectivité sortante

aux AWS services, notamment Amazon S3, ainsi qu'à Microsoft (afin de télécharger des correctifs).

- `KeepPreUpgradedBackUp`

  Type : chaîne

  (Facultatif) Si ce paramètre est défini sur `true`, l'automatisation conserve l'image créée depuis l'instance. Le paramètre par défaut est `false`.

- `RebootInstanceBeforeTakingImage`

  Type : chaîne

  (Facultatif) La valeur par défaut est `false` (pas de redémarrage). Si ce paramètre est défini sur`true`, Systems Manager redémarre l'instance avant de créer une instance AMI pour la mise à niveau.

8. Une fois que vous avez entré les paramètres, sélectionnez Execute (Exécuter). Lorsque l'automatisation commence, vous pouvez surveiller la progression de l'exécution.
9. Lorsque l'automatisation sera terminée, vous verrez l'AMIID. Vous pouvez lancer le AMI pour vérifier que le système d'exploitation Windows est mis à niveau.

> **Note**
>
> Il n'est nécessaire que l'automatisation exécute toutes les étapes. Les étapes sont conditionnelles en fonction du comportement de l'automatisation et de l'instance. Systems Manager peut ignorer certaines étapes qui ne sont pas requises.
> En outre, certaines étapes peuvent expirer. Systems Manager tente d'effectuer la mise à niveau et d'installer tous les derniers correctifs. Cependant, parfois, des correctifs expirent en fonction d'un paramètre de délai d'attente définissable pour l'étape donnée. Lorsque cela se produit, l'automatisation Systems Manager passe à l'étape suivante pour s'assurer que le système d'exploitation interne est mis à niveau vers la version de Windows Server cible.

10. Une fois l'automatisation terminée, vous pouvez lancer une EC2 instance Amazon à l'aide de l'AMIID pour vérifier votre mise à niveau. Pour plus d'informations sur la création d'une EC2 instance Amazon à partir d'un AWS AMI, consultez Comment lancer une EC2 instance depuis une instance personnalisée AMI ?

SQLServeur de mise à niveau

Le CloneInstanceAndUpgrade SQLServer script AWSEC2- crée une AMI EC2 instance Amazon exécutant SQL Server dans votre compte, puis la met à niveau AMI vers une version ultérieure de SQL Server. Ce processus en plusieurs étapes peut prendre jusqu'à deux heures.

Dans ce flux de travail, l'automatisation crée une AMI instance, puis lance la nouvelle AMI dans le sous-réseau que vous fournissez. L'automatisation effectue ensuite une mise à niveau sur place du SQL serveur. Une fois la mise à niveau terminée, l'automatisation en crée une nouvelle AMI avant de mettre fin à l'instance mise à niveau.

Deux d'entre eux sont AMIs inclus dans le processus de mise à niveau automatique :

- Instance en cours d'exécution actuelle. La première AMI est l'instance en cours d'exécution, qui n'est pas mise à niveau. Ceci AMI est utilisé pour lancer une autre instance afin d'exécuter la mise à niveau sur place. Lorsque le processus est terminé, elle AMI est supprimée de votre compte, sauf si vous demandez spécifiquement de conserver l'instance d'origine. Ce paramètre est géré par le paramètre `KeepPreUpgradeImageBackUp` (la valeur par défaut est`false`, ce qui signifie qu'AMIil est supprimé par défaut).
- Amélioré AMI. C'AMIest le résultat du processus d'automatisation.

Le résultat final est unAMI, qui est l'instance mise à niveau duAMI.

Une fois la mise à niveau terminée, vous pouvez tester les fonctionnalités de votre application en lançant la nouvelle AMI application sur votre AmazonVPC. Après le test et avant de procéder à une autre mise à niveau, planifiez les temps d'arrêt de l'application avant de passer complètement à l'instance mise à niveau.

Prérequis

Afin d'automatiser la mise à niveau de votre SQL serveur avec le document AWS Systems Manager Automation, vous devez effectuer les tâches suivantes :

- Créez un IAM rôle avec les IAM politiques spécifiées pour permettre à Systems Manager d'effectuer des tâches d'automatisation sur vos EC2 instances Amazon et vérifiez que vous remplissez les conditions requises pour utiliser Systems Manager. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un service AWS dans le Guide de l'utilisateur AWS Identity and Access Management .

- Sélectionnez l'option souhaitée pour l'exécution de l'automatisation. Les options d'exécution sont Exécution simple, Contrôle du débit, Plusieurs comptes et plusieurs régions et Exécution manuelle. Pour plus d'informations sur ces options, consultez Options d'exécution.
- L'EC2instance Amazon doit utiliser Windows Server 2008 R2 ou version ultérieure et SQL Server 2008 ou version ultérieure.
- Vérifiez que SSM l'agent est installé sur votre instance. Pour plus d'informations, consultez Travailler avec SSM l'agent sur EC2 les instances Amazon pour Windows Server.
- Vérifiez que l'instance dispose d'un espace disque suffisant :
  - Si vous effectuez une mise à niveau de Windows Server 2008 R2 vers 2012 R2, ou de Windows Server 2012 R2 vers un système d'exploitation plus récent, vérifiez que vous disposez de 20 Go d'espace disque libre sur le disque de démarrage de l'instance.
  - Si vous effectuez une mise à niveau de Windows Server 2008 R2 vers 2016 ou version ultérieure, vérifiez que l'instance dispose de 40 Go d'espace disque libre sur le disque de démarrage de l'instance.
- Pour les instances qui utilisent une version SQL du serveur Bring Your Own License (BYOL), les conditions supplémentaires suivantes s'appliquent :
  - Fournissez un identifiant de EBS capture Amazon qui inclut le support d'installation SQL du serveur cible. Pour cela :
    1. Vérifiez que l'EC2instance Amazon exécute Windows Server 2008 R2 ou version ultérieure.
    2. Créez un EBS volume Amazon de 6 Go dans la même zone de disponibilité où l'instance est exécutée. Attachez le volume à l'instance. Montez-la, par exemple, en tant que lecteur D.
    3. Cliquez avec le bouton droit sur le ISO et montez-le sur une instance telle que, par exemple, le lecteur E.
    4. Copiez le contenu ISO du lecteur E : \ vers le lecteur D : \
    5. Créez un EBS instantané Amazon du volume de 6 Go créé à l'étape 2.

SQLLimites de mise à niveau automatique du serveur

Les limitations suivantes s'appliquent lorsque vous utilisez le AWSEC2- CloneInstanceAndUpgrade SQLServer runbook pour effectuer une mise à niveau automatique :

- La mise à niveau ne peut être effectuée que sur un SQL serveur utilisant l'authentification Windows.

- Vérifiez qu'il n'y a pas de correctifs et mises à jour de sécurité en attente sur les instances. Ouvrez le Panneau de configuration, puis choisissez Rechercher les mises à jour.
- SQLLes déploiements de serveurs en mode HA et en mode miroir ne sont pas pris en charge.

Étapes pour effectuer une mise à niveau automatique du SQL serveur

Suivez ces étapes pour mettre à niveau votre SQL serveur à l'aide du runbook AWSEC2-CloneInstanceAndUpgrade SQLServer automation.

1. Si ce n'est pas déjà fait, téléchargez le fichier .iso SQL Server 2016 et montez-le sur le serveur source.
2. Une fois le fichier .iso monté, copiez tous les le fichiers de composant et placez-les sur un volume de votre choix.
3. Prenez un EBS instantané Amazon du volume et copiez l'identifiant de l'instantané dans un presse-papiers pour une utilisation ultérieure. Pour plus d'informations, consultez la section Créer des EBS instantanés Amazon dans le guide de l'EBSutilisateur Amazon.
4. Attachez le profil d'instance à l'instance EC2 source Amazon. Cela permet à Systems Manager de communiquer avec l'EC2instance et d'exécuter des commandes sur celle-ci après son ajout au AWS Systems Manager service. Pour cet exemple, nous avons nommé le rôle `SSM-EC2-Profile-Role` avec la stratégie `AmazonSSMManagedInstanceCore` attachée au rôle. Consultez la section Création d'un profil d'IAMinstance pour Systems Manager dans le guide de AWS Systems Manager l'utilisateur.
5. Dans le volet de navigation de gauche de la AWS Systems Manager console, sélectionnez Managed Instances. Vérifiez que votre EC2 instance figure dans la liste des instances gérées. Si vous ne voyez votre instance après quelques minutes, consultez Où sont mes instances ? dans le Guide de l'utilisateur AWS Systems Manager .
6. Dans le panneau de navigation de gauche, sous Change Management (Gestion des modifications), choisissez Automation (Automatisation).
7. Choisissez Execute automation (Exécuter l'automatisation).
8. Recherchez le document d'automatisation appelé `AWSEC2-CloneInstanceAndUpgradeSQLServer`.
9. Choisissez le `AWSEC2-CloneInstanceAndUpgradeSQLServer` SSM document, puis cliquez sur Suivant.
10. Assurez-vous que l'option Simple execution (Exécution simple) est sélectionnée.
11. Entrez les paramètres demandés en suivant les indications suivantes.

- `InstanceId`

  Type : chaîne

  (Obligatoire) L'instance exécutant SQL Server 2008 R2 (ou version ultérieure).

- `IamInstanceProfile`

  Type : chaîne

  (Obligatoire) Le profil de l'IAMinstance.

- `SQLServerSnapshotId`

  Type : chaîne

  (Obligatoire) L'ID du snapshot pour le support d'installation SQL du serveur cible. Ce paramètre n'est pas obligatoire pour les instances incluses dans une licence de SQL serveur.

- `SubnetId`

  Type : chaîne

  (Obligatoire) Il s'agit du sous-réseau pour le processus de mise à niveau et de l'emplacement de votre EC2 instance source. Vérifiez que le sous-réseau dispose d'une connectivité sortante aux AWS services, notamment Amazon S3, ainsi qu'à Microsoft (afin de télécharger des correctifs).

- `KeepPreUpgradedBackUp`

  Type : chaîne

  (Facultatif) Si ce paramètre est défini sur `true`, l'automatisation conserve l'image créée depuis l'instance. Le paramètre par défaut est `false`.

- `RebootInstanceBeforeTakingImage`

  Type : chaîne

  (Facultatif) La valeur par défaut est `false` (pas de redémarrage). Si ce paramètre est défini sur`true`, Systems Manager redémarre l'instance avant de créer une instance AMI pour la mise à niveau.

- `TargetSQLVersion`

Type : chaîne

(Facultatif) Version SQL du serveur cible. L'argument par défaut est `2016`.

12. Une fois que vous avez entré les paramètres, sélectionnez Execute (Exécuter). Lorsque l'automatisation commence, vous pouvez surveiller la progression de l'exécution.
13. Lorsque le statut d'exécution indique Succès, développez Sorties pour afficher les AMI informations. Vous pouvez utiliser l'AMIID pour lancer votre instance de SQL serveur pour celle VPC de votre choix.
14. Ouvrez la EC2 console Amazon. Dans le volet de navigation de gauche, choisissez AMIs. Tu devrais voir le nouveauAMI.
15. Pour vérifier que la nouvelle version SQL du serveur a été correctement installée, choisissez la nouvelle, AMI puis choisissez Launch.
16. Choisissez le type d'instance que vous souhaitez pour leAMI, le VPC sous-réseau sur lequel vous souhaitez déployer et le stockage que vous souhaitez utiliser. Comme vous lancez la nouvelle instance à partir d'unAMI, les volumes vous sont présentés sous forme d'option à inclure dans la nouvelle EC2 instance que vous lancez. Vous pouvez supprimer tout volume ou ajouter des volumes.
17. Ajoutez une balise pour vous aider à identifier votre instance.
18. Ajoutez le ou les groupes de sécurité à l'instance.
19. Choisissez Launch Instances.
20. Choisissez le nom de la balise pour l'instance et sélectionnez Connexion sous la liste déroulante Actions.
21. Vérifiez que la nouvelle version SQL du serveur est le moteur de base de données de la nouvelle instance.

Migrer une instance EC2 Windows vers un type d'instance de génération actuelle

Les AWS fenêtres AMIs sont configurées avec les paramètres par défaut utilisés par le support d'installation Microsoft, avec quelques personnalisations. Les personnalisations incluent des pilotes et des configurations qui prennent en charge les types d'instances de dernière génération, qui sont des instances basées sur le système AWS Nitro, telles qu'une M5 ou une C5.

Lors de la migration vers des instances basées sur Nitro, y compris des instances nues, nous vous recommandons de suivre les étapes décrites dans cette rubrique dans les cas suivants :

- Si vous lancez des instances à partir de Windows personnalisé AMIs
- Si vous lancez des instances depuis Windows AMIs fournies par Amazon qui ont été créées avant août 2018

Pour plus d'informations, consultez Amazon EC2 Update : types d'instances supplémentaires, système Nitro et CPU options.

> **Note**
>
> Les procédures de migration suivantes peuvent être effectuées sur Windows Server version 2008 R2 et les versions ultérieures. Pour migrer des instances Linux vers les types d'instances de dernière génération, consultezthe section called "Changements de type d'instance".

Table des matières

> **Note**
>
> Vous pouvez également utiliser le document d'automatisation `AWSSupport-UpgradeWindowsAWSDrivers` pour automatiser les procédures décrites dans la première, la deuxième et la troisième étape. Si vous choisissez d'utiliser la procédure automatisée,

consultez (Alternative) Améliorez le AWS PV et ENA les NVMe pilotes en utilisant AWS Systems Manager, puis continuez avec la quatrième et la cinquième étape.

Avant de commencer

Cette procédure suppose que vous exécutez actuellement un type d'instance Xen de génération précédente, tel qu'un M4 ou un C4, et que vous migrez vers une instance basée sur le système Nitro. AWS

Vous devez utiliser PowerShell la version 3.0 ou ultérieure pour effectuer correctement la mise à niveau.

> **Note**
>
> Lors de la migration vers les instances de dernière génération, l'adresse IP statique ou les paramètres DNS réseau personnalisés des instances existantes ENI peuvent être perdus car l'instance utilisera par défaut un nouveau périphérique Enhanced Networking Adapter.

Avant de commencer à suivre les étapes de cette procédure, nous vous conseillons de créer une sauvegarde de l'instance. Dans la EC2console, choisissez l'instance qui nécessite la migration, ouvrez le menu contextuel (clic droit), puis choisissez Instance State, Stop.

> **Warning**
>
> Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Pour préserver les données qui se trouvent sur les volumes de stockage d'instances, assurez-vous de les sauvegarder dans un stockage permanent.

Ouvrez le menu contextuel (clic droit) de l'instance dans la EC2console, choisissez Image, puis Create Image.

> **Note**
>
> Les parties 4 et 5 de ces instructions peuvent être terminées après avoir migré ou modifié le type d'instance vers la dernière génération. Toutefois, nous vous recommandons de

les terminer avant de procéder à la migration si vous migrez spécifiquement vers un type d'instance bare metal.

Partie 1 : Installation et mise à niveau des pilotes AWS PV

Bien que les pilotes AWS PV ne soient pas utilisés dans le système Nitro, vous devez tout de même les mettre à niveau si vous utilisez des versions précédentes de Citrix PV ou AWS PV. Les pilotes PV AWS permettent de corriger des bogues présents dans des versions précédentes de pilotes, susceptibles de se manifester sur un système Nitro, ou si vous devez revenir à une instance Xen. À titre de bonne pratique, nous vous recommandons de toujours mettre à jour les derniers pilotes pour les instances Windows activées AWS.

Utilisez la procédure suivante pour effectuer une mise à niveau sur place des pilotes AWS PV ou pour passer des pilotes PV Citrix aux pilotes AWS PV sous Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 ou Windows Server 2019. Pour de plus amples informations, veuillez consulter Mettre à niveau les pilotes PV sur EC2 les instances Windows.

Pour mettre à niveau un contrôleur de domaine, consultez Mettre à niveau un contrôleur de domaine (mise à niveau AWS PV).

Pour effectuer une mise à niveau ou vers des pilotes AWS PV

1. Connectez-vous à l'instance à l'aide des services Bureau à distance et préparez l'instance à la mise à niveau. Mettez tous les disques non système hors ligne avant d'exécuter la mise à niveau. Si vous effectuez une mise à jour sur place des pilotes AWS PV, cette étape n'est pas obligatoire. Définissez les services non essentiels sur le start-up Manual (Manuel) dans la console Services.
2. Téléchargez le package de pilotes le plus récent sur l'instance.
3. Extrayez le contenu du dossier, puis exécutez `AWSPVDriverSetup.msi`.

Après avoir exécuté leMSI, l'instance redémarre et met automatiquement à niveau le pilote. L'instance ne sera peut-être pas disponible pendant 15 minutes.

Une fois la mise à niveau terminée et l'instance passée les deux tests de santé dans la EC2 console Amazon, connectez-vous à l'instance à l'aide de Remote Desktop et vérifiez que le nouveau pilote a été installé. Dans le Gestionnaire de périphériques, sous Contrôleurs de stockage, recherchez Carte

hôte AWS PV Storage. Vérifiez que la version du pilote est identique à la version la plus récente répertoriée dans l'historique des versions de pilote. Pour de plus amples informations, veuillez consulter AWS Historique du package de pilotes PV.

Partie 2 : Installation et mise à niveau ENA

Effectuez une mise à niveau vers le pilote Elastic Network Adapter (ENA) le plus récent afin de garantir la prise en charge de toutes les fonctions du réseau. Si vous avez lancé votre instance et qu'elle n'a pas encore la mise en réseau améliorée activée, vous devez télécharger et installer le pilote de la carte réseau requis sur votre instance, Définissez ensuite l'attribut d' enaSupport instance pour activer la mise en réseau améliorée. Vous ne pouvez activer cet attribut que sur les types d'instances pris en charge et uniquement si le ENA pilote est installé. Pour de plus amples informations, veuillez consulter Activez une mise en réseau améliorée avec ENA vos EC2 instances.

1. Téléchargez le pilote le plus récent sur l'instance. Si vous avez besoin d'une version précédente du pilote, consultezENAHistorique des versions du pilote Windows.
2. Décompressez l'archive zip.
3. Installez le pilote en exécutant le `install.ps1` PowerShell script à partir du dossier extrait.

   > **Note**
   >
   > Afin d'éviter les erreurs d'installation, exécutez le script `install.ps1` en tant qu'administrateur.

4. Vérifiez si vous AMI l'avez enaSupport activé. Si ce n'est pas le cas, poursuivez à l'aide de la documentation disponible dans Activez une mise en réseau améliorée avec ENA vos EC2 instances.

Partie 3 : Mise à niveau des AWS NVMe pilotes

AWS NVMeles pilotes sont utilisés pour interagir avec Amazon EBS et les volumes de stockage d'SSDinstance exposés sous forme de NVMe blocs dans le système Nitro pour de meilleures performances.

> **Important**
>
> Les instructions suivantes sont modifiées spécifiquement pour l'installation ou la mise à niveau AWS NVMe d'une instance de génération précédente dans le but de migrer l'instance vers le type d'instance de dernière génération.

1. Téléchargez le package de pilotes le plus récent sur l'instance.

   Si vous avez besoin d'une version précédente du pilote, consultez NVMeVersions de pilotes Windows les versions prises en charge.
2. Décompressez l'archive zip.
3. Installez le pilote en exécutant `dpinst.exe`.
4. Ouvrez une PowerShellsession et exécutez la commande suivante :

   ```
   PS C:\> start rundll32.exe sppnp.dll,Sysprep_Generalize_Pnp -wait
   ```

   > **Note**
   >
   > Pour appliquer la commande, vous devez exécuter la PowerShell session en tant qu'administrateur. PowerShell les versions (x86) provoqueront une erreur.
   > Cette commande exécute uniquement Sysprep sur les pilotes de périphérique. Elle n'exécute pas la préparation Sysprep complète.
5. Pour Windows Server 2008 R2 et Windows Server 2012, arrêtez l'instance, remplacez le type d'instance par une instance de nouvelle génération et lancez-la. Passez ensuite à l'étape 4. Si vous redémarrez à nouveau l'instance sur un type d'instance de la génération précédente avant de migrer vers un type d'instance de nouvelle génération, elle ne démarrera pas. Pour les autres systèmes Windows pris en chargeAMIs, vous pouvez modifier le type d'instance à tout moment après le sysprep de l'appareil.

Partie 4 : Mise à jour EC2Config et EC2Launch

Pour les instances Windows, les versions les plus récentes EC2Config et les EC2Launch utilitaires fournissent des fonctionnalités et des informations supplémentaires lors de l'exécution sur le système Nitro, y compris sur EC2 Bare Metal. Par défaut, le EC2Config service est inclus dans les AMIs

versions antérieures à Windows Server 2016. EC2Launchremplace EC2Config sur Windows Server 2016 et versions ultérieuresAMIs.

Lorsque les EC2Launch services EC2Config et sont mis à jour, les nouvelles versions AMIs de Windows AWS incluent la dernière version du service. Toutefois, vous devez mettre à jour votre propre Windows AMIs et vos instances avec la dernière version de EC2Config etEC2Launch.

Pour installer ou mettre à jour EC2Config

1. Téléchargez et décompressez le EC2Configprogramme d'installation.
2. Exécutez `EC2Install.exe`. Pour obtenir une liste complète des options, exécutez `EC2Install` avec l'option `/?`. Par défaut, la configuration affiche les invites. Pour exécuter la commande sans invites, utilisez l'option `/quiet`.

Pour de plus amples informations, veuillez consulter Installez la dernière version de EC2Config.

Pour installer ou mettre à jour EC2Launch

1. Si vous avez déjà installé et configuré EC2Launch une instance, effectuez une sauvegarde du fichier de EC2Launch configuration. Le processus d'installation ne conserve pas les modifications de ce fichier. Par défaut, le fichier se trouve dans le répertoire `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. Téléchargez le EC2fichier -Windows-Launch.zip dans un répertoire de l'instance.
3. Téléchargez install.ps1 dans le répertoire dans lequel vous avez téléchargé `EC2-Windows-Launch.zip`.
4. Exécutez `install.ps1`.

> **Note**
>
> Afin d'éviter les erreurs d'installation, exécutez le script `install.ps1` en tant qu'administrateur.

5. Si vous avez effectué une sauvegarde du fichier de EC2Launch configuration, copiez-le `C:\ProgramData\Amazon\EC2-Windows\Launch\Config` dans le répertoire.

Pour de plus amples informations, veuillez consulter Utiliser l'agent EC2Launch v1 pour effectuer des tâches lors du lancement de l'instance EC2 Windows.

Étape 5 : Installer le pilote du port série pour les instances nues

Le type d'`i3.metal`instance utilise un périphérique série PCI basé sur un port d'E/S plutôt qu'un périphérique série basé sur un port d'E/S. La dernière version de Windows utilise AMIs automatiquement le périphérique série PCI basé et le pilote du port série est installé. Si vous n'utilisez pas d'instance lancée à partir d'un système Windows fourni par Amazon AMI daté du 11 avril 2018 ou version ultérieure, vous devez installer le pilote de port série pour activer le périphérique série pour des EC2 fonctionnalités telles que la génération de mots de passe et la sortie de console. Les derniers EC2Config EC2Launch utilitaires supportent également i3.metal et fournissent des fonctionnalités supplémentaires. Suivez les instructions de l'étape 4 si vous ne l'avez pas déjà fait.

Pour installer le pilote du port série

1. Téléchargez le package de pilotes série le plus récent sur l'instance.
2. Extrayez le contenu du dossier, ouvrez le menu contextuel (clic droit) pour `aws_ser.INF` et choisissez install (installer).
3. Choisissez OK.

Étape 6 : Mettre à jour les paramètres de gestion de l'alimentation

La mise à jour suivante des paramètres de gestion de l'alimentation fait en sorte que les écrans ne s'éteignent jamais, ce qui permet d'arrêter normalement le système d'exploitation sur le système Nitro. Tous les systèmes Windows AMIs fournis par Amazon au 28 novembre 2018 disposent déjà de cette configuration par défaut.

1. Ouvrez une invite de commande ou une PowerShell session.
2. Exécutez les commandes suivantes :

```
powercfg /setacvalueindex 381b4222-f694-41f0-9685-ff5bb260df2e 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex a1841308-3541-4fab-bc81-f71556f20b4a 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
```

Étape 7 : Mettre à jour les pilotes de puce Intel pour des nouveaux types d'instance

Les types d'`u-12tb1.metal`instance `u-6tb1.metal`u-9tb1.metal, et utilisent du matériel qui nécessite des pilotes de chipset qui n'étaient pas précédemment installés sous WindowsAMIs. Si vous n'utilisez pas d'instance lancée à partir d'un système Windows fourni par Amazon AMI daté du 19 novembre 2018 ou version ultérieure, vous devez installer les pilotes à l'aide de l'utilitaire Intel Chipset. INF

Pour installer les pilotes de puce

1. Téléchargez l'utilitaire de puce sur l'instance.
2. Extrayez les fichiers.
3. Exécutez `SetupChipset.exe`.
4. Acceptez le contrat de licence logicielle Intel et installez les pilotes de puce.
5. Redémarrez l'instance.

(Alternative) Améliorez le AWS PV et ENA les NVMe pilotes en utilisant AWS Systems Manager

Le document d'automatisation `AWSSupport-UpgradeWindowsAWSDrivers` automatise les étapes décrites dans la première, la deuxième et la troisième étape. Cette méthode peut également réparer une instance pour laquelle les mises à niveau du pilote ont échoué.

Le document `AWSSupport-UpgradeWindowsAWSDrivers` d'automatisation met à niveau ou répare le stockage et AWS les pilotes réseau sur l'EC2instance spécifiée. Le document tente d'installer les dernières versions des AWS pilotes en ligne en appelant l' AWS Systems Manager agent (SSMagent). Si SSM l'agent n'est pas joignable, le document peut effectuer une installation hors ligne des AWS pilotes si cela est explicitement demandé.

> **Note**
>
> Cette procédure échouera sur un contrôleur de domaine. Pour mettre à jour les pilotes sur un contrôleur de domaine, consultez Mettre à niveau un contrôleur de domaine (mise à niveau AWS PV).

Pour mettre à niveau automatiquement le AWS PV et ENA les NVMe pilotes à l'aide de AWS Systems Manager

1. Ouvrez la console Systems Manager à l'adresse https://console.aws.amazon.com/systems-manager.
2. Choisissez Automatisation, puis Execute automation (Exécuter l'automatisation).
3. Recherchez puis sélectionnez le document AWSSupport- UpgradeWindows AWSDrivers automatisation, puis choisissez Exécuter l'automatisation.
4. Dans la section Paramètres d'entrée, configurez les options suivantes :

   ID d'instance

   Saisissez l'ID unique de l'instance à mettre à niveau.

   AllowOffline

   (Facultatif) Choisissez l'une des options suivantes :

   - `True` : choisissez cette option pour effectuer une installation hors ligne. L'instance est arrêtée et redémarrée pendant le processus de mise à niveau.

     > **Warning**
     >
     > Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Pour préserver les données qui se trouvent sur les volumes de stockage d'instances, assurez-vous de les sauvegarder dans un stockage permanent.

   - `False` : (par défaut) pour effectuer une installation en ligne, laissez cette option sélectionnée. L'instance est redémarrée pendant le processus de mise à niveau.

     > **Important**
     >
     > Les mises à niveau en ligne et hors ligne créent un AMI avant de tenter les opérations de mise à niveau. Le AMI persiste une fois l'automatisation terminée. Sécurisez votre accès au AMI ou supprimez-le s'il n'est plus nécessaire.

SubnetId

(Facultatif) Entrez l'une des valeurs suivantes :

- `SelectedInstanceSubnet` : (par défaut) le processus de mise à niveau lance l'instance d'assistant dans le même sous-réseau que l'instance à mettre à niveau. Le sous-réseau doit autoriser la communication avec les points de terminaison Systems Manager (`ssm.*`).
- `CreateNewVPC`— Le processus de mise à niveau lance l'instance d'assistance dans une nouvelle VPC instance. Utilisez cette option si vous ne savez pas si le sous-réseau de l'instance cible autorise la communication avec les points de terminaison `ssm.*`. Votre utilisateur doit être autorisé à créer unVPC.
- Un ID de sous-réseau spécifique : spécifiez l'ID d'un sous-réseau spécifique dans lequel lancer l'instance d'assistant. Le sous-réseau doit appartenir à la même zone de disponibilité que l'instance à mettre à niveau, et il doit autoriser la communication avec les points de terminaison `ssm.*`.

5. Sélectionnez Execute (Exécuter).
6. Laissez la mise à niveau s'effectuer. Une mise à niveau en ligne peut prendre 10 minutes, et une mise à niveau en ligne jusqu'à 25 minutes.

Résoudre les problèmes liés à une mise à niveau du système d'exploitation sur une instance EC2 Windows

AWS fournit un support de mise à niveau pour les problèmes liés au service Upgrade Helper, un AWS utilitaire qui vous aide à effectuer des mises à niveau sur place impliquant des pilotes PV Citrix.

Après la mise à niveau, l'instance peut temporairement connaître une CPU utilisation supérieure à la moyenne pendant que le. NETLe service d'optimisation du temps d'exécution optimise le. NETcadre. Ce comportement est normal.

Si l'instance n'a pas validé les deux contrôles des statuts au bout de plusieurs heures, effectuez les vérifications suivantes.

- Si vous avez mis à niveau vers Windows Server 2008 et que les deux contrôles de statut échouent au bout de plusieurs heures, la mise à niveau peut avoir échoué et présenter l'invite Cliquez sur OK pour confirmer la restauration. Du fait que la console n'est pas accessible dans cet état, il n'est pas possible de cliquer sur le bouton. Pour contourner ce problème, effectuez un redémarrage via la

EC2 console Amazon ouAPI. Le redémarrage prend au moins dix minutes pour s'initier. L'instance peut devenir disponible au bout de 25 minutes.

- Supprimez les applications ou les rôles de serveur du serveur et réessayez.

Si l'instance ne valide pas les deux contrôles de statut après la suppression des applications ou des rôles de serveur du serveur, procédez comme suit.

- Arrêtez l'instance et attachez le volume racine à une autre instance. Pour plus d'informations, consultez la description de la méthode pour arrêter et attacher le volume racine à une autre instance dans « En attente du service de métadonnées ».
- Analysez les fichiers journaux et d'événements de l'installation Windows pour rechercher les échecs.

Pour tous les autres problèmes liés à la mise à niveau ou à la migration d'un système d'exploitation, nous vous recommandons de consulter les articles répertoriés dans Avant de commencer une mise à niveau sur place.

Tutoriel : Connecter une EC2 instance Amazon à une RDS base de données Amazon

Objectif du tutoriel

L'objectif de ce didacticiel est d'apprendre à configurer une connexion sécurisée entre une EC2 instance Amazon et une RDS base de données Amazon à l'aide du AWS Management Console.

Il existe différentes options pour configurer la connexion. Dans ce tutoriel, nous explorons les trois options suivantes :

- Option 1 : connecter automatiquement une instance à une RDS base de données à l'aide de la EC2 console

  Utilisez la fonctionnalité de connexion automatique de la EC2 console pour configurer automatiquement la connexion entre votre EC2 instance et votre RDS base de données afin d'autoriser le trafic entre l'EC2instance et la RDS base de données.
- Option 2 : connecter automatiquement une instance à une RDS base de données à l'aide de la RDS console

Utilisez la fonctionnalité de connexion automatique de la RDS console pour configurer automatiquement la connexion entre votre EC2 instance et votre RDS base de données afin d'autoriser le trafic entre l'EC2instance et la RDS base de données.

- Option 3 : connecter manuellement une instance à une RDS base de données en créant des groupes de sécurité

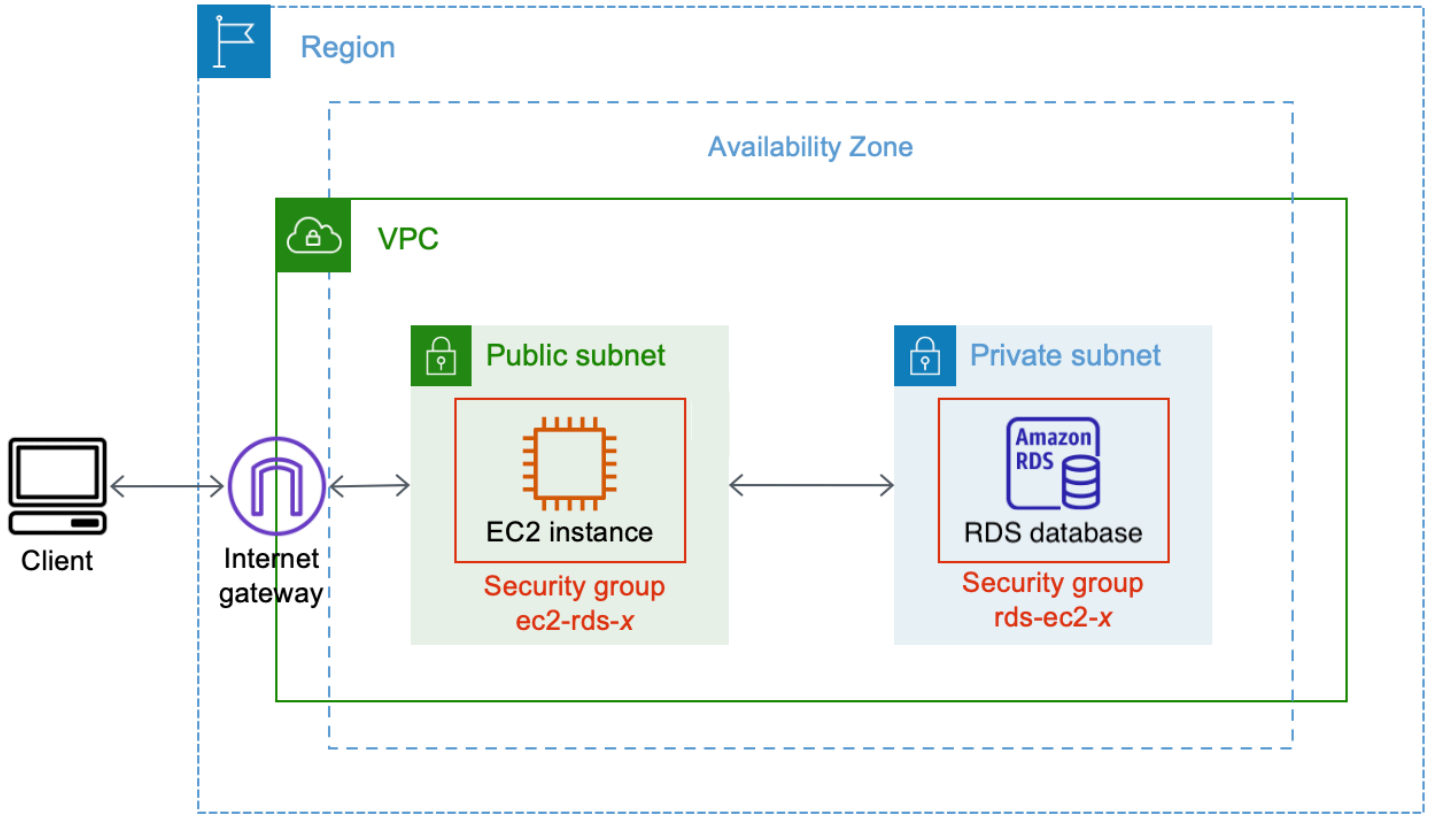
  Configurez la connexion entre votre EC2 instance et votre RDS base de données en configurant et en attribuant manuellement les groupes de sécurité afin de reproduire la configuration créée automatiquement par la fonctionnalité de connexion automatique dans les options 1 et 2.

Contexte

Pour expliquer pourquoi vous souhaitez configurer une connexion entre votre EC2 instance et une RDS base de données, considérons le scénario suivant : votre site Web présente un formulaire à remplir par vos utilisateurs. Vous devez capturer les données du formulaire dans une base de données. Vous pouvez héberger votre site Web sur une EC2 instance configurée en tant que serveur Web et vous pouvez capturer les données du formulaire dans une RDS base de données. L'EC2instance et la RDS base de données doivent être connectées l'une à l'autre pour que les données du formulaire puissent passer de l'EC2instance à la RDS base de données. Ce tutoriel explique comment configurer cette connexion. Notez qu'il ne s'agit que d'un exemple de cas d'utilisation pour connecter une EC2 instance et une RDS base de données.

Architecture

Le diagramme suivant montre les ressources créées et la configuration architecturale qui résulte de l'exécution de toutes les étapes de ce tutoriel.



Le diagramme illustre les ressources suivantes que vous allez créer :

- Vous allez créer une EC2 instance et une RDS base de données dans Région AWS la VPC même zone de disponibilité.
- Vous allez créer l'EC2instance dans un sous-réseau public.
- Vous allez créer la RDS base de données dans un sous-réseau privé.

  Lorsque vous utilisez la RDS console pour créer la RDS base de données et connecter automatiquement l'EC2instanceVPC, les paramètres de groupe de sous-réseaux de base de données et d'accès public pour la base de données sont automatiquement sélectionnés. La RDS base de données est automatiquement créée dans un sous-réseau privé au sein du même sous-réseau VPC que l'EC2instance.
- Les internautes peuvent se connecter à l'EC2instance en utilisant SSH ouHTTP/HTTPSvia une passerelle Internet.
- Les utilisateurs d'Internet ne peuvent pas se connecter directement à la RDS base de données ; seule l'EC2instance est connectée à la RDS base de données.

- Lorsque vous utilisez la fonctionnalité de connexion automatique pour autoriser le trafic entre l'EC2instance et la RDS base de données, les groupes de sécurité suivants sont automatiquement créés et ajoutés :
  - Groupe de sécurité ec2-rds-*x*est créé et ajouté à l'EC2instance. Il possède une règle sortante qui fait référence au rds-ec2-*x*groupe de sécurité comme destination. Cela permet au trafic provenant de l'EC2instance d'atteindre la RDS base de données avec le rds-ec2-*x*groupe de sécurité.
  - Groupe de sécurité rds-ec2-*x*est créé et ajouté à la RDS base de données. Il possède une règle entrante qui fait référence au ec2-rds-*x*groupe de sécurité comme source. Cela autorise le trafic depuis l'EC2instance avec le code ec2-rds-*x*groupe de sécurité pour accéder à la RDS base de données.

  En utilisant des groupes de sécurité distincts (un pour l'EC2instance et un pour la RDS base de données), vous pouvez mieux contrôler la sécurité de l'instance et de la base de données. Si vous deviez utiliser le même groupe de sécurité sur l'instance et la base de données, puis le modifier pour qu'il convienne, par exemple, uniquement à la base de données, la modification affecterait à la fois l'instance et la base de données. En d'autres termes, si vous deviez utiliser un groupe de sécurité, vous pourriez modifier involontairement la sécurité d'une ressource (soit l'instance, soit la base de données) parce que vous auriez oublié que le groupe de sécurité y est attaché.

  Les groupes de sécurité créés automatiquement respectent également le principe du moindre privilège car ils n'autorisent que la connexion mutuelle pour cette charge de travail sur le port de la base de données en créant une paire de groupes de sécurité spécifique à la charge de travail.

Considérations

Tenez compte des éléments suivants lorsque vous effectuez les tâches de ce tutoriel :

- Deux consoles : vous utiliserez les deux consoles suivantes pour ce tutoriel :
  - EC2Console Amazon : vous utiliserez la EC2 console pour lancer des instances, pour connecter automatiquement une EC2 instance à une RDS base de données et pour l'option manuelle permettant de configurer la connexion en créant les groupes de sécurité.
  - RDSConsole Amazon — Vous allez utiliser la RDS console pour créer une RDS base de données et pour connecter automatiquement une EC2 instance à une RDS base de données.
- Un VPC — Pour utiliser la fonctionnalité de connexion automatique, votre EC2 instance et votre RDS base de données doivent se trouver dans la même zoneVPC.

Si vous deviez configurer manuellement la connexion entre votre EC2 instance et votre RDS base de données, vous pourriez lancer votre EC2 instance dans l'une VPC et votre RDS base de données dans une autre VPC ; toutefois, vous devrez configurer un routage et une VPC configuration supplémentaires. Ce scénario n'est pas décrit dans ce tutoriel.

- Un Région AWS — L'EC2instance et la RDS base de données doivent être situées dans la même région.
- Deux groupes de sécurité : la connectivité entre l'EC2instance et la RDS base de données est configurée par deux groupes de sécurité : un groupe de sécurité pour votre EC2 instance et un groupe de sécurité pour votre RDS base de données.

  Lorsque vous utilisez la fonctionnalité de connexion automatique de la EC2 console ou de la RDS console pour configurer la connectivité (option 1 et option 2 de ce didacticiel), les groupes de sécurité sont automatiquement créés et attribués à l'EC2instance et à la RDS base de données.

  Si vous n'utilisez pas la fonction de connexion automatique, vous devrez créer et affecter manuellement les groupes de sécurité. Vous le faites dans l'option 3 de ce tutoriel.

Durée du didacticiel

30 minutes

Vous pouvez suivre l'intégralité de ce tutoriel en une seule séance ou effectuer une tâche à la fois.

Coûts

En suivant ce didacticiel, les AWS ressources que vous créez peuvent vous coûter cher.

Vous pouvez utiliser Amazon EC2 dans le cadre du niveau gratuit à condition que votre AWS compte date de moins de 12 mois et que vous configuriez vos ressources conformément aux exigences du niveau gratuit.

Si votre EC2 instance et votre RDS base de données se trouvent dans des zones de disponibilité différentes, des frais de transfert de données vous seront facturés. Pour éviter ces frais, l'EC2instance et la RDS base de données doivent se trouver dans la même zone de disponibilité. Pour plus d'informations sur les frais de transfert de données, consultez la section Transfert de données sur la page de tarification d'EC2Amazon On-Demand.

Pour éviter d'encourir des frais après avoir terminé le tutoriel, assurez-vous de supprimer les ressources si elles ne sont plus nécessaires. Pour connaître la marche à suivre pour supprimer les ressources, consultez Tâche 4 (facultatif) : Nettoyer.

Option 1 : connecter automatiquement une instance à une RDS base de données à l'aide de la EC2 console

L'objectif de l'option 1 est d'explorer la fonctionnalité de connexion automatique de la EC2 console qui configure automatiquement la connexion entre votre EC2 instance et la RDS base de données pour autoriser le trafic entre l'EC2instance et la RDS base de données. L'option 3 vous permet d'apprendre à configurer manuellement la connexion.

Tâches

Avant de commencer

Vous aurez besoin des éléments suivants pour compléter ce tutoriel :

- Une RDS base de données qui se trouve dans la même instance VPC que l'EC2instance. Vous pouvez utiliser une RDS base de données existante ou suivre les étapes de la tâche 1 pour créer une nouvelle RDS base de données.
- EC2Instance identique à la RDS base VPC de données. Vous pouvez utiliser une EC2 instance existante ou suivre les étapes de la tâche 2 pour créer une nouvelle EC2 instance.
- Des autorisations pour appeler les opérations suivantes :
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`

- `ec2:CreateSubnet`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:RevokeSecurityGroupEgress`

Tâche 1 (facultatif) : créer une RDS base de données

> **Note**
>
> La création d'une RDS base de données Amazon n'est pas l'objet de ce didacticiel. Si vous possédez déjà une RDS base de données et que vous souhaitez l'utiliser dans ce didacticiel, vous pouvez ignorer cette tâche.
> Si vous utilisez une RDS base de données existante, assurez-vous qu'elle se trouve dans la même instance VPC que votre EC2 instance afin de pouvoir utiliser la fonctionnalité de connexion automatique.

L'objectif de cette tâche est de créer une RDS base de données afin que vous puissiez terminer la tâche 3 dans laquelle vous configurez la connexion entre votre EC2 instance et votre RDS base de données. Les étapes de cette tâche configurent la RDS base de données comme suit :

- Type de moteur : My SQL
- Modèle : offre gratuite
- Identifiant d'instance de base de données : **`tutorial-database-1`**
- Classe d'instance de base de données : `db.t3.micro`

> **Important**
>
> Dans un environnement de production, vous devez configurer votre base de données pour répondre à vos besoins spécifiques.

Pour créer une base de SQL RDS données My

1. Ouvrez la RDS console Amazon à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le sélecteur de région (en haut à droite), sélectionnez une Région AWS. La base de données et l'EC2instance doivent se trouver dans la même région pour pouvoir utiliser la fonctionnalité de connexion automatique de la EC2 console.
3. Dans le tableau de bord, choisissez Create database (Créer une base de données).
4. Sous Choose a database creation method (Choisir une méthode de création de base de données), vérifiez que l'option Standard create (Création standard) est sélectionnée. Si vous choisissez Création facile, le VPC sélecteur n'est pas disponible. Vous devez vous assurer que votre base de données est VPC identique à celle de votre EC2 instance afin d'utiliser la fonctionnalité de connexion automatique de la EC2 console.
5. Sous Options du moteur, pour Type de moteur, sélectionnez Mon SQL.
6. Sous Templates (Modèles), choisissez un exemple de modèle pour répondre à vos besoins. Pour ce didacticiel, choisissez le niveau gratuit pour créer une RDS base de données gratuitement. Toutefois, notez que l'offre gratuite n'est disponible que si votre compte a moins de 12 mois. D'autres restrictions s'appliquent. Vous pouvez en savoir plus en cliquant sur le lien Info dans la case Free tier (Offre gratuite).
7. Sous Paramètres, effectuez l'une des actions suivantes :

   a. Pour DB instance identifier (Identifiant d'instance de base de données), saisissez un nom pour la base de données. Dans le cadre de ce didacticiel, entrez **`tutorial-database-1`**.

   b. Pour Master username (Nom d'utilisateur principal), laissez le nom par défaut, qui est **`admin`**.

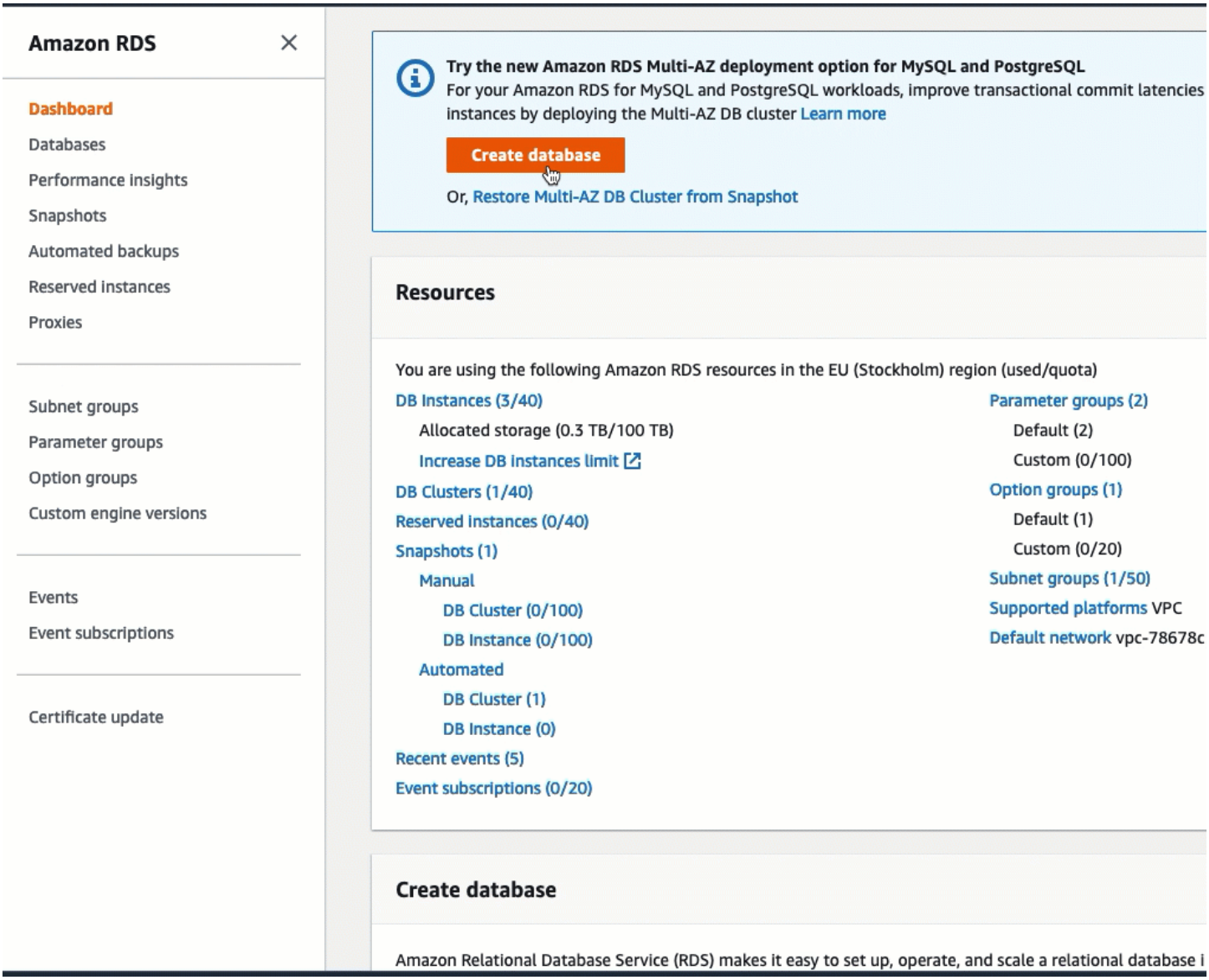
   c. Pour Master password (Mot de passe principal), saisissez un mot de passe dont vous pouvez vous souvenir pour ce tutoriel, puis, pour Confirm password (Confirmer le mot de passe), saisissez à nouveau le mot de passe.
8. Sous Configuration de l'instance, pour la classe d'instance de base de données, laissez la valeur par défaut, à savoir db.t3.micro. Si votre compte dure moins de 12 mois, vous pouvez utiliser cette classe de base de données gratuitement. D'autres restrictions s'appliquent. Pour de plus amples informations, veuillez consulter Niveau gratuit d'AWS.
9. Sous Connectivité, pour ressource de calcul, choisissez Ne pas vous connecter à une ressource de EC2 calcul, car vous connecterez l'EC2instance et la RDS base de données plus tard dans la tâche 3.

(Plus tard, dans l'option 2 de ce didacticiel, vous testerez la fonctionnalité de connexion automatique dans la RDS console en choisissant Se connecter à une ressource de EC2 calcul.)

10. Pour Virtual Private Cloud (VPC), choisissez unVPC. VPCIl doit avoir un groupe de sous-réseaux de base de données. Pour utiliser la fonctionnalité de connexion automatique, votre EC2 instance et votre RDS base de données doivent être identiquesVPC.
11. Conservez toutes les valeurs par défaut pour les autres champs de cette page.
12. Choisissez Créer une base de données.

    Sur l’écran Databases (Bases de données), le Status (Statut) de la nouvelle base de données est Creating (Création) jusqu’à ce que la base de données soit prête à être utilisée. Lorsque le statut passe à Available (Disponible), vous pouvez vous connecter à la base de données. En fonction de la classe de base de données et de la quantité de stockage, la mise à disposition de la nouvelle base de données peut prendre jusqu’à 20 minutes.

Afficher une animation : créer une RDS base de données



Tâche 2 (facultatif) : Lancer une EC2 instance

> **Note**
>
> Le lancement d'une instance n'est pas l'objet de ce tutoriel. Si vous possédez déjà une EC2 instance Amazon et que vous souhaitez l'utiliser dans ce didacticiel, vous pouvez ignorer cette tâche.
>
> Si vous utilisez une EC2 instance existante, assurez-vous qu'elle se trouve dans la même VPC que votre RDS base de données afin de pouvoir utiliser la fonctionnalité de connexion automatique.

L'objectif de cette tâche est de lancer une EC2 instance afin que vous puissiez terminer la tâche 3 dans laquelle vous configurez la connexion entre votre EC2 instance et votre RDS base de données Amazon. Les étapes de cette tâche configurent l'EC2instance comme suit :

- Nom de l'instance : **`tutorial-instance-1`**
- AMI: Amazon Linux 2
- Type d'instance : `t2.micro`
- Attribuer automatiquement l'adresse IP publique : Activé
- Groupe de sécurité avec les trois règles suivantes :
  - Autoriser SSH depuis votre adresse IP
  - Autorisez HTTPS le trafic depuis n'importe où
  - Autorisez HTTP le trafic depuis n'importe où

> **Important**
>
> Dans un environnement de production, vous devez configurer votre instance pour répondre à vos besoins spécifiques.

Pour lancer une instance EC2

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le sélecteur de région (en haut à droite), sélectionnez une Région AWS. L'instance et la RDS base de données doivent se trouver dans la même région pour pouvoir utiliser la fonctionnalité de connexion automatique de la EC2 console.
3. Sur le EC2tableau de bord, choisissez Launch instance.
4. Sous Name and tags (Noms et balises), pour Name (Nom), saisissez un nom pour identifier votre instance. Pour ce tutoriel, nommez l'instance **`tutorial-instance-1`**. Bien que le nom de l'instance ne soit pas obligatoire, lorsque vous sélectionnez votre instance dans la EC2 console, le nom vous aidera à l'identifier facilement.
5. Sous Images de l'application et du système d'exploitation, choisissez AMI celle qui répond aux besoins de votre serveur Web. Ce tutoriel utilise Amazon Linux 2.
6. Sous Instance type (Type d'instance), pour Instance type (Type d'instance), sélectionnez un type d'instance qui répond aux besoins de votre serveur Web. Ce tutoriel utilise `t2.micro`.

> **Note**
>
> Vous pouvez utiliser Amazon EC2 dans le cadre du niveau gratuit à condition que votre AWS compte date de moins de 12 mois et que vous choisissiez un type d'`t2.micro`instance, ou `t3.micro` dans les régions où ce type d'instance n'`t2.micro`est pas disponible. Sachez que lorsque vous lancez une instance t3.micro, elle passe par défaut en mode illimité, ce qui peut entraîner des frais supplémentaires en fonction de l'utilisation. CPU

7. Sous Key pair (login) (Paire de clés (connexion)), pour Key pair name (Nom de la paire de clés), choisissez votre paire de clés.
8. Sous Network settings (Paramètres réseau), effectuez les opérations suivantes :

   a. Pour le réseau et le sous-réseau, si vous n'avez pas modifié votre VPC ou vos sous-réseaux par défaut, vous pouvez conserver les paramètres par défaut.

      Si vous avez modifié vos sous-réseaux VPC ou sous-réseaux par défaut, vérifiez les points suivants :

      i. L'instance doit se trouver dans le même emplacement VPC que la RDS base de données pour utiliser la fonctionnalité de connexion automatique. Par défaut, vous n'en avez qu'unVPC.

      ii. L'instance dans VPC laquelle vous lancez votre instance doit être connectée à une passerelle Internet afin que vous puissiez accéder à votre serveur Web depuis Internet. Votre configuration par défaut VPC est automatiquement configurée avec une passerelle Internet.

      iii. Pour vous assurer que votre instance reçoit une adresse IP publique, pour Auto-assign public IP (Attribuer automatiquement une adresse IP publique), vérifiez que Enable (Activer) est sélectionné. Si l'option Disable (Désactiver) est sélectionnée, choisissez Edit (Modifier) (à droite de Network Settings (Paramètres réseau)), puis, pour Auto-assign public IP (Attribuer automatiquement une adresse IP publique), choisissez Enable (Activer).

   b. Pour vous connecter à votre instance en utilisantSSH, vous avez besoin d'une règle de groupe de sécurité qui autorise le trafic SSH (Linux) ou RDP (Windows) à partir de l'IPv4adresse publique de votre ordinateur. Par défaut, lorsque vous lancez une instance,

un nouveau groupe de sécurité est créé avec une règle qui autorise le SSH trafic entrant en provenance de n'importe où.

Pour vous assurer que seule votre adresse IP peut se connecter à votre instance, sous Pare-feu (groupes de sécurité), dans la liste déroulante située à côté de la case à cocher Autoriser le SSH trafic depuis, sélectionnez Mon adresse IP.

c. Pour autoriser le trafic depuis Internet vers votre instance, cochez les cases suivantes :

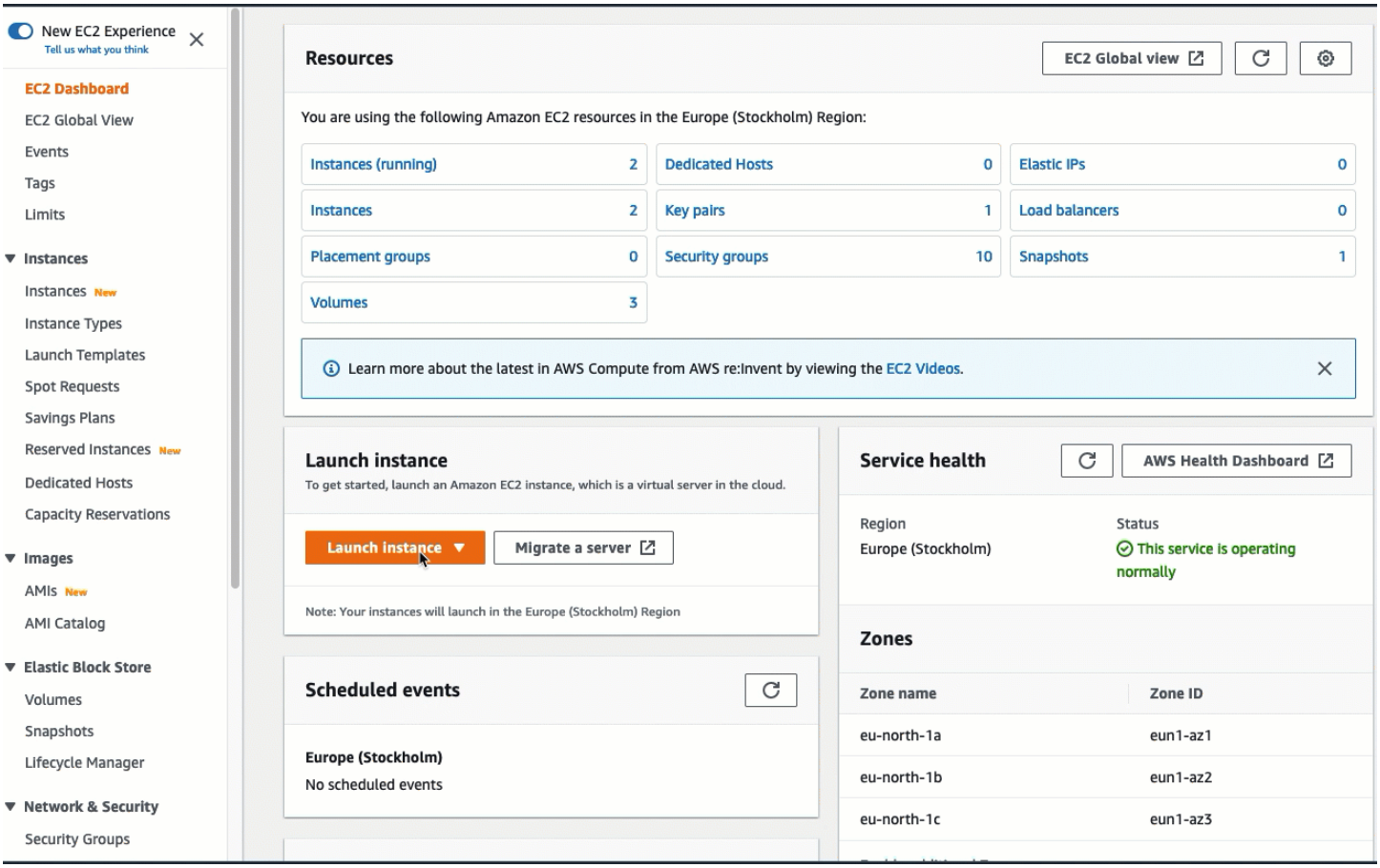
- Autoriser HTTPs le trafic en provenance d'Internet
- Autoriser HTTP le trafic en provenance d'Internet

9. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance).
10. Gardez la page de confirmation ouverte. Vous en aurez besoin pour la tâche suivante lorsque vous connecterez automatiquement votre instance à votre base de données.

    Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez Résoudre les problèmes de lancement des EC2 instances Amazon.

Pour plus d'informations sur le lancement d'une instance, consultez Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console.

Afficher une animation : lancer une EC2 instance



Tâche 3 : connecter automatiquement votre EC2 instance à votre RDS base de données

L'objectif de cette tâche est d'utiliser la fonctionnalité de connexion automatique de la EC2 console pour configurer automatiquement la connexion entre votre EC2 instance et votre RDS base de données.

Pour connecter automatiquement une EC2 instance à une RDS base de données à l'aide de la EC2 console

1. Sur la page de confirmation du lancement de l'instance (elle doit être ouverte depuis la tâche précédente), choisissez Connect an RDS database.

   Si vous avez fermé la page de confirmation, suivez ces étapes :

   a. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

   b. Dans le panneau de navigation, choisissez Instances.

c. Sélectionnez l'EC2instance que vous venez de créer, puis choisissez Actions, Networking, Connect RDS database.

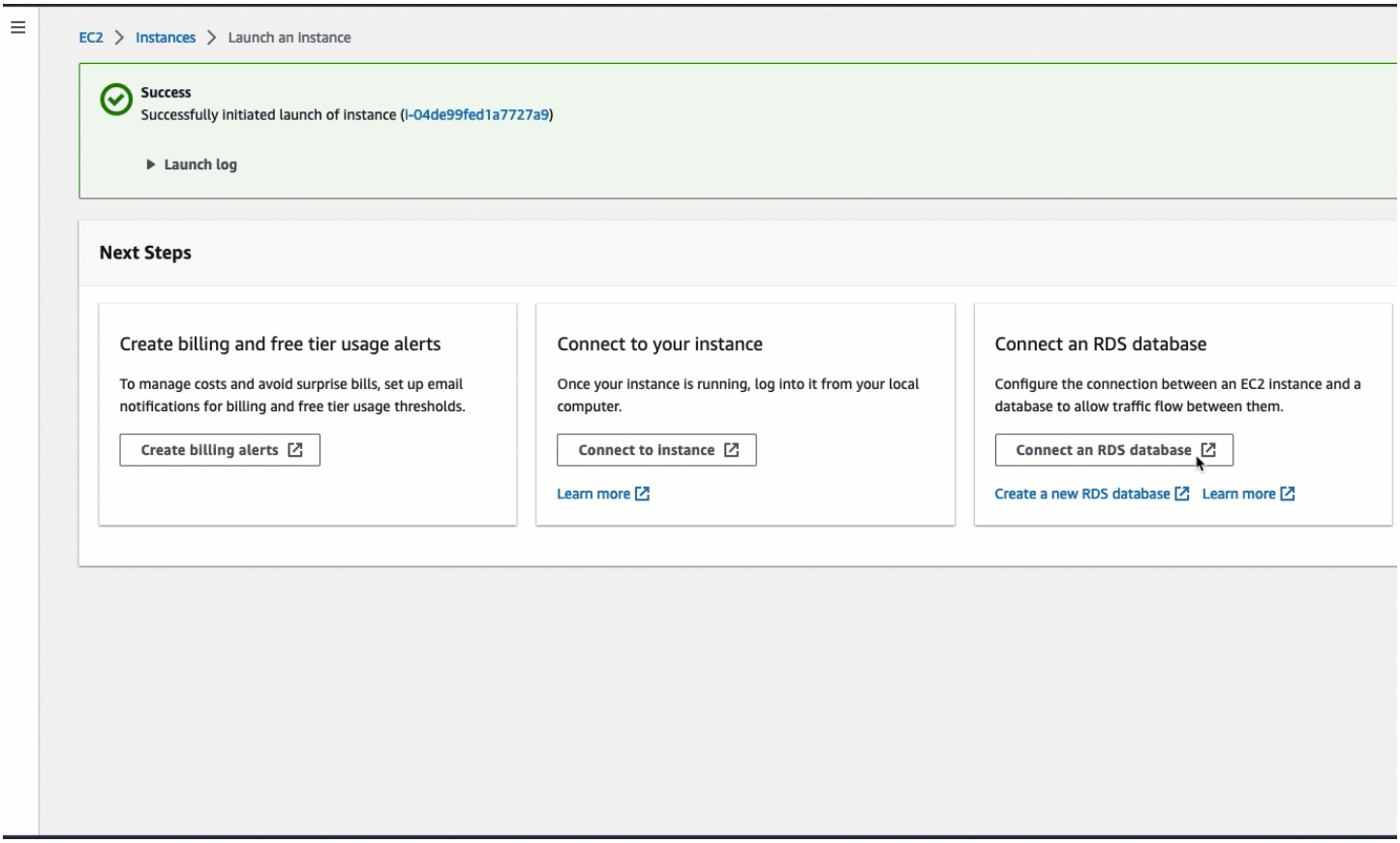
   Si la RDSbase de données Connect n'est pas disponible, vérifiez que l'EC2instance est en cours d'exécution.

2. Pour Database role (Rôle de la base de données), choisissez Instance. Dans ce cas, Instance fait référence à l'instance de la base de données.
3. Pour la RDSbase de données, choisissez la RDS base de données que vous avez créée dans la tâche 1.

> **Note**
>
> L'EC2instance et la RDS base de données doivent être identiques pour pouvoir VPC se connecter l'une à l'autre.

4. Choisissez Se connecter.

Afficher une animation : connecter automatiquement une EC2 instance nouvellement lancée à une base de données RDS



Tâche 4 : vérification de la configuration de la connexion

L'objectif de cette tâche est de vérifier que les deux groupes de sécurité ont été créés et affectés à l'instance et à la base de données.

Lorsque vous utilisez la fonctionnalité de connexion automatique de la console pour configurer la connectivité, les groupes de sécurité sont automatiquement créés et affectés à l'instance et à la base de données, comme suit :

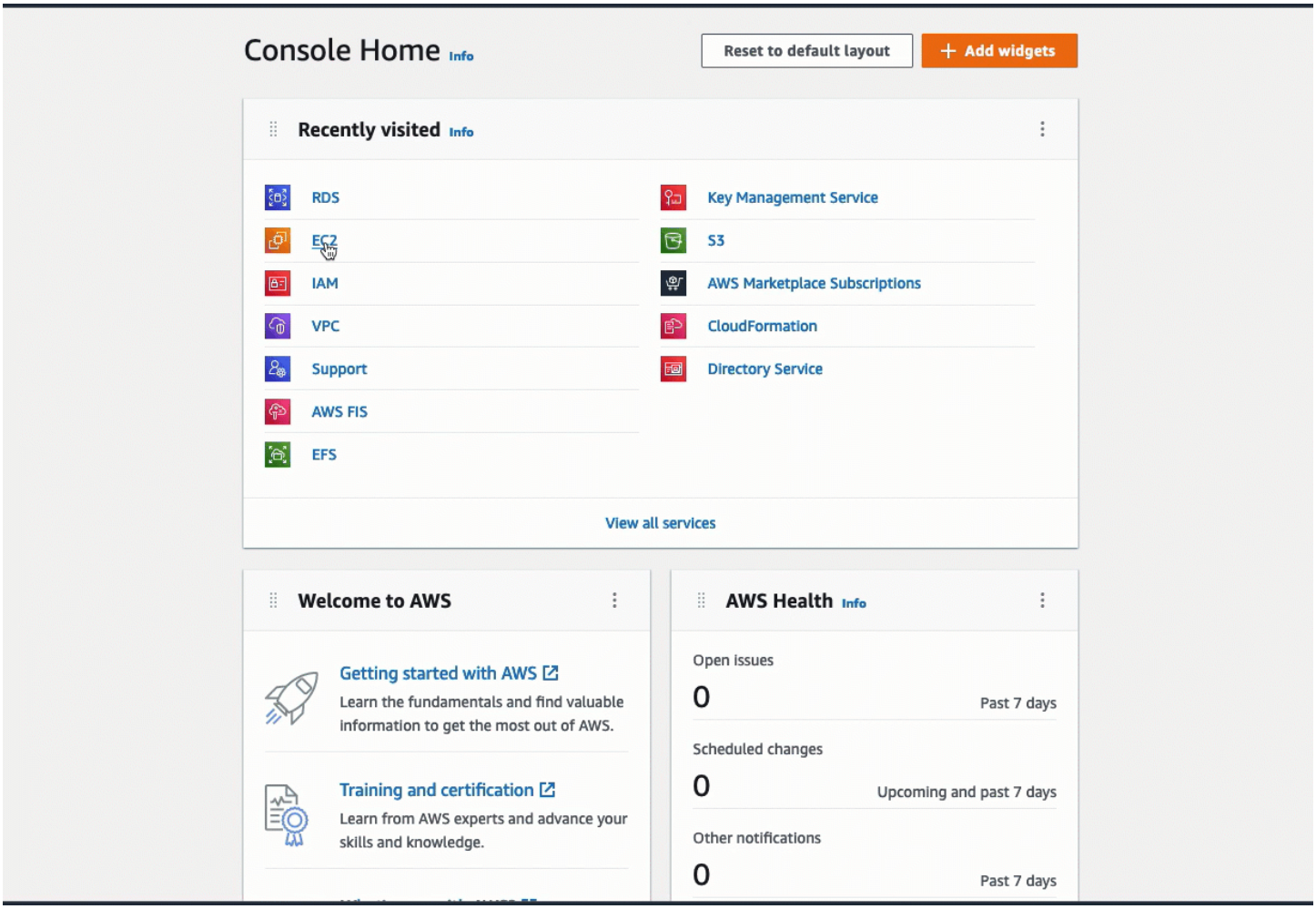
- Groupe de sécurité rds-ec2-***x***est créé et ajouté à la RDS base de données. Il possède une règle entrante qui fait référence au ec2-rds-***x***groupe de sécurité comme source. Cela autorise le trafic depuis l'EC2instance avec le code ec2-rds-***x***groupe de sécurité pour accéder à la RDS base de données.
- Groupe de sécurité ec2-rds-***x***est créé et ajouté à l'EC2instance. Il possède une règle sortante qui fait référence au rds-ec2-***x***groupe de sécurité comme destination. Cela permet au trafic provenant de l'EC2instance d'atteindre la RDS base de données avec le rds-ec2-***x***groupe de sécurité.

Pour vérifier la configuration de la connexion à l'aide de la console

1. Ouvrez la RDS console Amazon à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la page de navigation, choisissez Databases (Bases de données).
3. Choisissez la RDS base de données que vous avez créée pour ce didacticiel.
4. Dans l'onglet Connectivité et sécurité, sous Sécurité, groupes VPC de sécurité, vérifiez qu'un groupe de sécurité appelé rds-ec2-*x*s'affiche.
5. Choisissez le rds-ec2-*x*groupe de sécurité. L'écran Security Groups de la EC2 console s'ouvre.
6. Choisissez le rds-ec2-*x*groupe de sécurité pour l'ouvrir.
7. Choisissez l'onglet Inbound rules (Règles entrantes).
8. Vérifiez que la règle de groupe de sécurité suivante existe :
   - Type : MYSQL/Aurore
   - Plage de ports : 3306
   - Source : ***sg-0987654321example*** /ec2-rds-***x***— Il s'agit du groupe de sécurité attribué à l'EC2instance que vous avez vérifiée dans les étapes précédentes.
   - Description : Règle permettant d'autoriser les connexions depuis EC2 des instances avec ***sg-1234567890example*** attaché
9. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
10. Dans le panneau de navigation, choisissez Instances.
11. Choisissez l'EC2instance que vous avez sélectionnée pour vous connecter à la RDS base de données lors de la tâche précédente, puis cliquez sur l'onglet Sécurité.
12. Sous Détails de sécurité, Groupes de sécurité, vérifiez qu'un groupe de sécurité appelé ec2-rds-***x***est dans la liste. *x* est un chiffre.
13. Choisissez le ec2-rds-***x***groupe de sécurité pour l'ouvrir.
14. Choisissez l'onglet Outbound rules (Règles sortantes).
15. Vérifiez que la règle de groupe de sécurité suivante existe :
    - Type : MYSQL/Aurore
    - Plage de ports : 3306
    - Destination : ***sg-1234567890example*** /rds-ec2-***x***
    - Description : Règle pour autoriser les connexions à **`database-tutorial`** à partir de n'importe quelle instance à laquelle ce groupe de sécurité est attaché

En vérifiant que ces groupes de sécurité et ces règles de groupe de sécurité existent et qu'ils sont affectés à la RDS base de données et à l'EC2instance comme décrit dans cette procédure, vous pouvez vérifier que la connexion a été automatiquement configurée à l'aide de la fonctionnalité de connexion automatique.

Voir une animation : vérification de la configuration de la connexion



Vous avez terminé l'option 1 de ce tutoriel. Vous pouvez désormais soit terminer l'option 2, qui vous apprend à utiliser la RDS console pour connecter automatiquement une EC2 instance à une RDS base de données, soit suivre l'option 3, qui vous apprend à configurer manuellement les groupes de sécurité créés automatiquement dans l'option 1.

Tâche 5 (facultatif) : Nettoyage

Maintenant que vous avez terminé le tutoriel, il est recommandé de nettoyer (supprimer) toutes les ressources que vous ne voulez plus utiliser. Le nettoyage AWS des ressources évite à votre compte d'encourir des frais supplémentaires.

Si vous avez lancé une EC2 instance spécifiquement pour ce didacticiel, vous pouvez y mettre fin pour ne plus avoir à encourir de frais associés.

Pour résilier une instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance que vous avez créée pour ce tutoriel, puis choisissez Instance state (État de l'instance), Terminate instance (Résilier l'instance).
4. Choisissez Résilier lorsque vous êtes invité à confirmer.

Si vous avez créé une RDS base de données spécialement pour ce didacticiel, vous pouvez la supprimer pour ne plus être facturée.

Pour supprimer une RDS base de données à l'aide de la console

1. Ouvrez la RDS console Amazon à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Databases (Bases de données).
3. Sélectionnez la RDS base de données que vous avez créée pour ce didacticiel, puis choisissez Actions, Supprimer.
4. Saisissez **`delete me`** dans la case, puis choisissez Delete (Supprimer).

Option 2 : connecter automatiquement une instance à une RDS base de données à l'aide de la RDS console

L'objectif de l'option 2 est d'explorer la fonctionnalité de connexion automatique de la RDS console qui configure automatiquement la connexion entre votre EC2 instance et la RDS base de données pour autoriser le trafic entre l'EC2instance et la RDS base de données. L'option 3 vous permet d'apprendre à configurer manuellement la connexion.

Tâches

- Avant de commencer
- Tâche 1 (facultatif) : Lancer une EC2 instance
- Tâche 2 : créer une RDS base de données et la connecter automatiquement à votre EC2 instance
- Tâche 3 : vérification de la configuration de la connexion

- Tâche 4 (facultatif) : Nettoyer

Avant de commencer

Vous aurez besoin des éléments suivants pour compléter ce tutoriel :

- EC2Instance identique à la RDS base VPC de données. Vous pouvez utiliser une EC2 instance existante ou suivre les étapes de la tâche 1 pour créer une nouvelle instance.
- Des autorisations pour appeler les opérations suivantes :
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Tâche 1 (facultatif) : Lancer une EC2 instance

> **Note**
>
> Le lancement d'une instance n'est pas l'objet de ce tutoriel. Si vous possédez déjà une EC2 instance Amazon et que vous souhaitez l'utiliser dans ce didacticiel, vous pouvez ignorer cette tâche.

L'objectif de cette tâche est de lancer une EC2 instance afin que vous puissiez terminer la tâche 2 dans laquelle vous configurez la connexion entre votre EC2 instance et votre RDS base de données Amazon. Les étapes de cette tâche configurent l'EC2instance comme suit :

- Nom de l'instance : **`tutorial-instance-2`**
- AMI: Amazon Linux 2
- Type d'instance : `t2.micro`
- Attribuer automatiquement l'adresse IP publique : Activé
- Groupe de sécurité avec les trois règles suivantes :
  - Autoriser SSH depuis votre adresse IP
  - Autorisez HTTPS le trafic depuis n'importe où
  - Autorisez HTTP le trafic depuis n'importe où

> **Important**
>
> Dans un environnement de production, vous devez configurer votre instance pour répondre à vos besoins spécifiques.

Pour lancer une instance EC2

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Sur le EC2tableau de bord, choisissez Launch instance.
3. Sous Name and tags (Noms et balises), pour Name (Nom), saisissez un nom pour identifier votre instance. Pour ce tutoriel, nommez l'instance **`tutorial-instance-2`**. Bien que le nom de l'instance ne soit pas obligatoire, lorsque vous sélectionnez votre instance dans la RDS console, le nom vous aidera à l'identifier facilement.
4. Sous Images de l'application et du système d'exploitation, choisissez AMI celle qui répond aux besoins de votre serveur Web. Ce tutoriel utilise Amazon Linux.
5. Sous Instance type (Type d'instance), pour Instance type (Type d'instance), sélectionnez un type d'instance qui répond aux besoins de votre serveur Web. Ce tutoriel utilise `t2.micro`.

   > **Note**
   >
   > Vous pouvez utiliser Amazon EC2 dans le cadre du niveau gratuit à condition que votre AWS compte date de moins de 12 mois et que vous choisissiez un type d'`t2.micro`instance, ou `t3.micro` dans les régions où ce type d'instance n'`t2.micro`est pas disponible. Sachez que lorsque vous lancez une instance t3.micro,

elle passe par défaut en mode illimité, ce qui peut entraîner des frais supplémentaires en fonction de l'utilisation. CPU

6. Sous Key pair (login) (Paire de clés (connexion)), pour Key pair name (Nom de la paire de clés), choisissez votre paire de clés.
7. Sous Network settings (Paramètres réseau), effectuez les opérations suivantes :

   a. Pour le réseau et le sous-réseau, si vous n'avez pas modifié votre VPC ou vos sous-réseaux par défaut, vous pouvez conserver les paramètres par défaut.

      Si vous avez modifié vos sous-réseaux VPC ou sous-réseaux par défaut, vérifiez les points suivants :

      i. L'instance doit se trouver dans le même emplacement VPC que la RDS base de données pour utiliser la configuration de connexion automatique. Par défaut, vous n'en avez qu'unVPC.

      ii. L'instance dans VPC laquelle vous lancez votre instance doit être connectée à une passerelle Internet afin que vous puissiez accéder à votre serveur Web depuis Internet. Votre configuration par défaut VPC est automatiquement configurée avec une passerelle Internet.

      iii. Pour vous assurer que votre instance reçoit une adresse IP publique, pour Auto-assign public IP (Attribuer automatiquement une adresse IP publique), vérifiez que Enable (Activer) est sélectionné. Si l'option Disable (Désactiver) est sélectionnée, choisissez Edit (Modifier) (à droite de Network Settings (Paramètres réseau)), puis, pour Auto-assign public IP (Attribuer automatiquement une adresse IP publique), choisissez Enable (Activer).

   b. Pour vous connecter à votre instance en utilisantSSH, vous avez besoin d'une règle de groupe de sécurité qui autorise le trafic SSH (Linux) ou RDP (Windows) à partir de l'IPv4adresse publique de votre ordinateur. Par défaut, lorsque vous lancez une instance, un nouveau groupe de sécurité est créé avec une règle qui autorise le SSH trafic entrant en provenance de n'importe où.

      Pour vous assurer que seule votre adresse IP peut se connecter à votre instance, sous Pare-feu (groupes de sécurité), dans la liste déroulante située à côté de la case à cocher Autoriser le SSH trafic depuis, sélectionnez Mon adresse IP.

   c. Pour autoriser le trafic depuis Internet vers votre instance, cochez les cases suivantes :

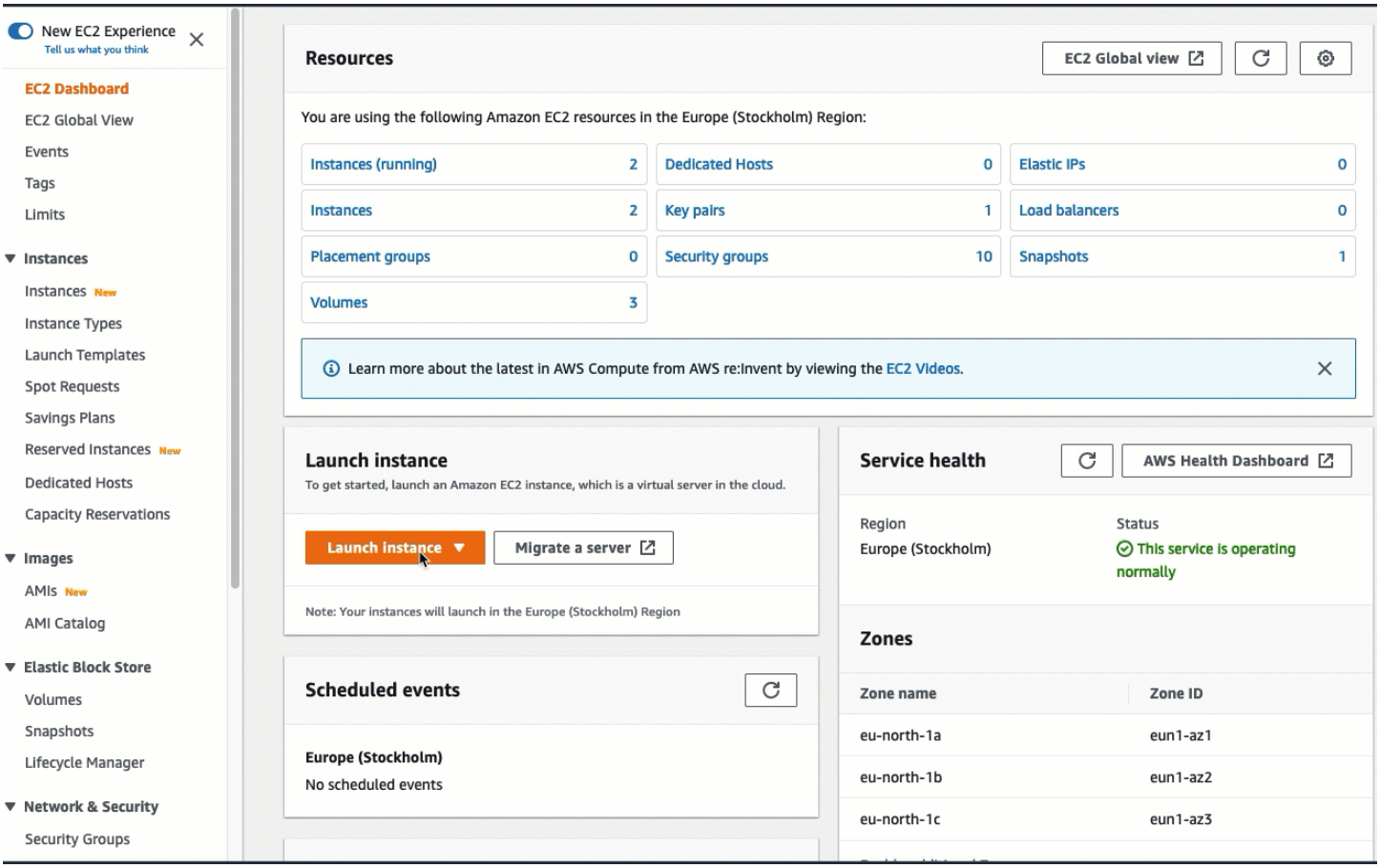
- Autoriser HTTPs le trafic en provenance d'Internet
- Autoriser HTTP le trafic en provenance d'Internet

8. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance).
9. Sélectionnez View all instances (Afficher toutes les instances) pour fermer la page de confirmation et revenir à la console. Votre instance sera d'abord dans un état `pending`, puis passera à l'état `running`.

   Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez Résoudre les problèmes de lancement des EC2 instances Amazon.

Pour plus d'informations sur le lancement d'une instance, consultez Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console.

Afficher une animation : lancer une EC2 instance



Tâche 2 : créer une RDS base de données et la connecter automatiquement à votre EC2 instance

L'objectif de cette tâche est de créer une RDS base de données et d'utiliser la fonctionnalité de connexion automatique de la RDS console pour configurer automatiquement la connexion entre votre EC2 instance et votre RDS base de données. Les étapes de cette tâche configurent l'instance de base de données comme suit :

- Type de moteur : My SQL
- Modèle : offre gratuite
- Identifiant d'instance de base de données : **`tutorial-database`**
- Classe d'instance de base de données : `db.t3.micro`

> **Important**
>
> Dans un environnement de production, vous devez configurer votre instance pour répondre à vos besoins spécifiques.

Pour créer une RDS base de données et la connecter automatiquement à une EC2 instance

1. Ouvrez la RDS console Amazon à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le sélecteur de région (en haut à droite), choisissez l'instance Région AWS dans laquelle vous avez créé l'EC2instance. L'EC2instance et la RDS base de données doivent se trouver dans la même région.
3. Dans le tableau de bord, choisissez Create database (Créer une base de données).
4. Sous Choose a database creation method (Choisir une méthode de création de base de données), vérifiez que l'option Standard create (Création standard) est sélectionnée. Si vous choisissez Easy create (Création facile), la fonction de connexion automatique n'est pas disponible.
5. Sous Options du moteur, pour Type de moteur, sélectionnez Mon SQL.
6. Sous Templates (Modèles), choisissez un exemple de modèle pour répondre à vos besoins. Pour ce didacticiel, choisissez le niveau gratuit pour créer une RDS base de données gratuitement. Toutefois, notez que l'offre gratuite n'est disponible que si votre compte a moins de

12 mois. D'autres restrictions s'appliquent. Vous pouvez en savoir plus en cliquant sur le lien Info dans la case Free tier (Offre gratuite).

7. Sous Paramètres, effectuez l'une des actions suivantes :

   a. Pour DB instance identifier (Identifiant d'instance de base de données), saisissez un nom pour la base de données. Dans le cadre de ce didacticiel, entrez **`tutorial-database`**.

   b. Pour Master username (Nom d'utilisateur principal), laissez le nom par défaut, qui est **`admin`**.

   c. Pour Master password (Mot de passe principal), saisissez un mot de passe dont vous pouvez vous souvenir pour ce tutoriel, puis, pour Confirm password (Confirmer le mot de passe), saisissez à nouveau le mot de passe.

8. Sous Configuration de l'instance, pour la classe d'instance de base de données, laissez la valeur par défaut, à savoir db.t3.micro. Si votre compte a moins de 12 mois, vous pouvez utiliser cette instance gratuitement. D'autres restrictions s'appliquent. Pour de plus amples informations, veuillez consulter Niveau gratuit d'AWS.

9. Sous Connectivité, pour Ressource de calcul, choisissez Se connecter à une ressource de EC2 calcul. Il s'agit de la fonction de connexion automatique de la RDS console.

10. Par EC2exemple, choisissez l'EC2instance à laquelle vous souhaitez vous connecter. Pour les besoins de ce tutoriel, vous pouvez choisir l'instance que vous avez créée dans la tâche précédente, que vous avez nommée **`tutorial-instance`**, ou choisir une autre instance existante. Si vous ne voyez pas votre instance dans la liste, choisissez l'icône d'actualisation à droite de Connectivity (Connectivité).

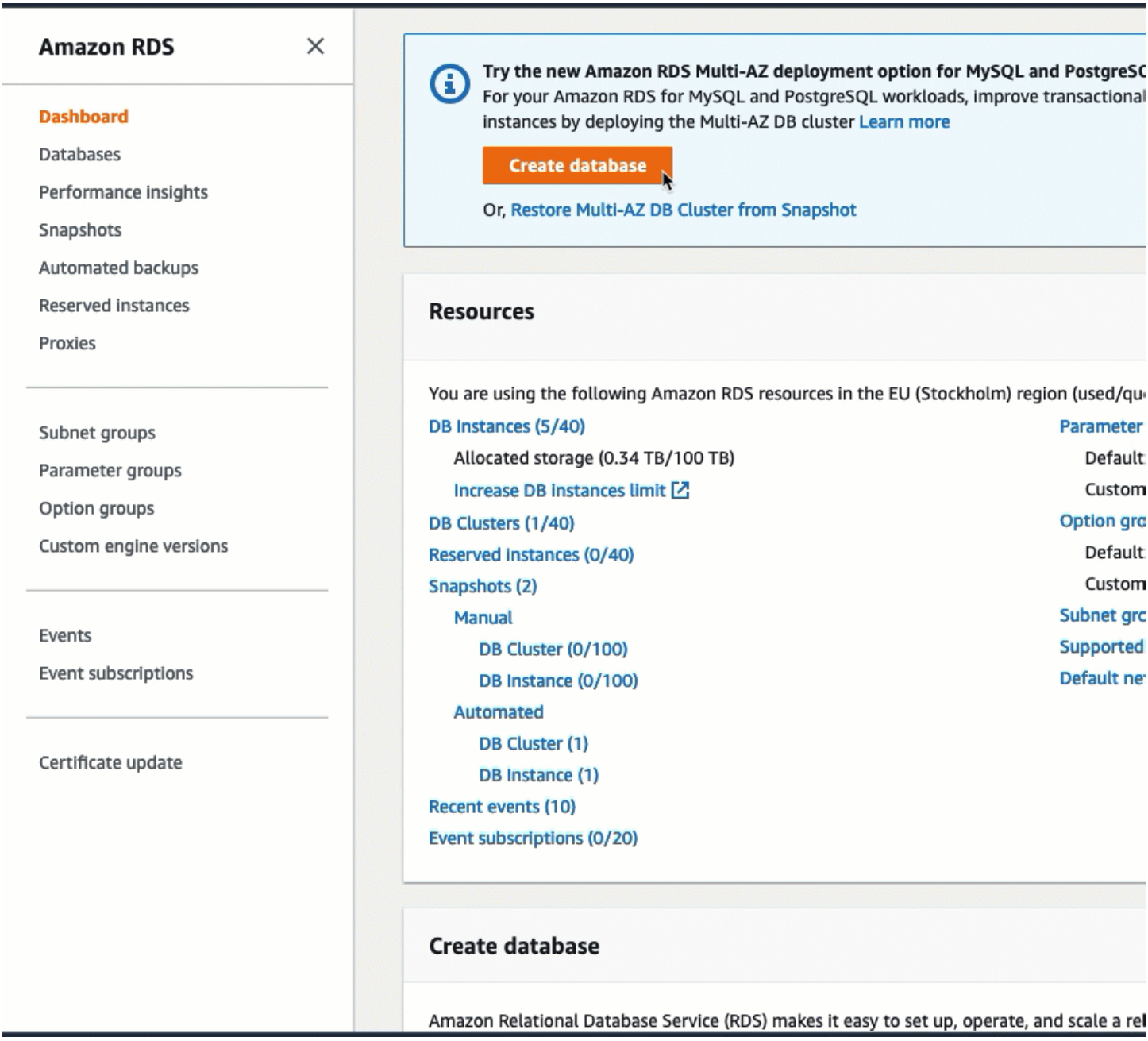
    Lorsque vous utilisez la fonctionnalité de connexion automatique, un groupe de sécurité est ajouté à cette EC2 instance et un autre groupe de sécurité est ajouté à la RDS base de données. Les groupes de sécurité sont automatiquement configurés pour autoriser le trafic entre l'EC2instance et la RDS base de données. Dans la tâche suivante, vous allez vérifier que les groupes de sécurité ont été créés et attribués à l'EC2instance et à la RDS base de données.

11. Choisissez Créer une base de données.

    Sur l'écran Databases (Bases de données), le Status (Statut) de la nouvelle base de données est Creating (Création) jusqu'à ce que la base de données soit prête à être utilisée. Lorsque le statut passe à Available (Disponible), vous pouvez vous connecter à la base de données. En fonction de la classe de base de données et de la quantité de stockage, la mise à disposition de la nouvelle base de données peut prendre jusqu'à 20 minutes.

Pour en savoir plus, consultez Configurer la connectivité réseau automatique avec une EC2 instance dans le guide de RDS l'utilisateur Amazon.

Afficher une animation : créer une RDS base de données et la connecter automatiquement à une EC2 instance



Tâche 3 : vérification de la configuration de la connexion

L'objectif de cette tâche est de vérifier que les deux groupes de sécurité ont été créés et affectés à l'instance et à la base de données.

Lorsque vous utilisez la fonctionnalité de connexion automatique de la console pour configurer la connectivité, les groupes de sécurité sont automatiquement créés et affectés à l'instance et à la base de données, comme suit :

- Groupe de sécurité rds-ec2-***x***est créé et ajouté à la RDS base de données. Il possède une règle entrante qui fait référence au ec2-rds-***x***groupe de sécurité comme source. Cela autorise le trafic depuis l'EC2instance avec le code ec2-rds-***x***groupe de sécurité pour accéder à la RDS base de données.
- Groupe de sécurité ec2-rds-***x***est créé et ajouté à l'EC2instance. Il possède une règle sortante qui fait référence au rds-ec2-***x***groupe de sécurité comme destination. Cela permet au trafic provenant de l'EC2instance d'atteindre la RDS base de données avec le rds-ec2-***x***groupe de sécurité.

Pour vérifier la configuration de la connexion à l'aide de la console

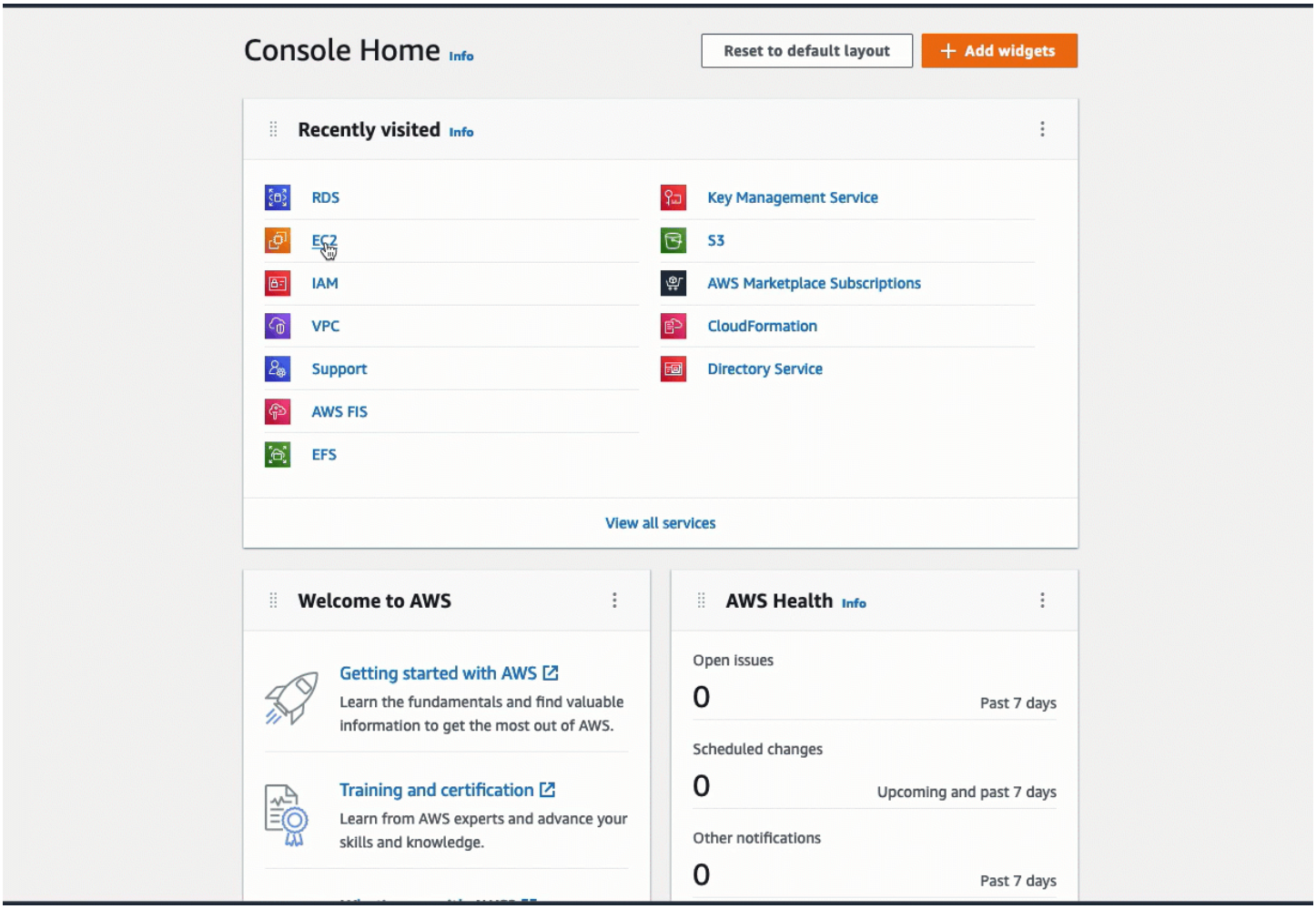
1. Ouvrez la RDS console Amazon à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la page de navigation, choisissez Databases (Bases de données).
3. Choisissez la RDS base de données que vous avez créée pour ce didacticiel.
4. Dans l'onglet Connectivité et sécurité, sous Sécurité, groupes VPC de sécurité, vérifiez qu'un groupe de sécurité appelé rds-ec2-***x***s'affiche.
5. Choisissez le rds-ec2-***x***groupe de sécurité. L'écran Security Groups de la EC2 console s'ouvre.
6. Choisissez le rds-ec2-***x***groupe de sécurité pour l'ouvrir.
7. Choisissez l'onglet Inbound rules (Règles entrantes).
8. Vérifiez que la règle de groupe de sécurité suivante existe :
    - Type : MYSQL/Aurore
    - Plage de ports : 3306
    - Source : ***sg-0987654321example*** /ec2-rds-***x***— Il s'agit du groupe de sécurité attribué à l'EC2instance que vous avez vérifiée dans les étapes précédentes.
    - Description : Règle permettant d'autoriser les connexions depuis EC2 des instances avec ***sg-1234567890example*** attaché
9. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
10. Dans le panneau de navigation, choisissez Instances.
11. Choisissez l'EC2instance que vous avez sélectionnée pour vous connecter à la RDS base de données lors de la tâche précédente, puis cliquez sur l'onglet Sécurité.

12. Sous Détails de sécurité, Groupes de sécurité, vérifiez qu'un groupe de sécurité appelé ec2-rds-*x*est dans la liste. *x* est un chiffre.
13. Choisissez le ec2-rds-*x*groupe de sécurité pour l'ouvrir.
14. Choisissez l'onglet Outbound rules (Règles sortantes).
15. Vérifiez que la règle de groupe de sécurité suivante existe :

    - Type : MYSQL/Aurore
    - Plage de ports : 3306
    - Destination : ***sg-1234567890example*** /rds-ec2-***x***
    - Description : Règle pour autoriser les connexions à **`database-tutorial`** à partir de n'importe quelle instance à laquelle ce groupe de sécurité est attaché

En vérifiant que ces groupes de sécurité et ces règles de groupe de sécurité existent et qu'ils sont affectés à la RDS base de données et à l'EC2instance comme décrit dans cette procédure, vous pouvez vérifier que la connexion a été automatiquement configurée à l'aide de la fonctionnalité de connexion automatique.

Voir une animation : vérification de la configuration de la connexion



Vous avez terminé l'option 2 de ce tutoriel. Vous pouvez maintenant terminer l'option 3, qui vous apprend à configurer manuellement les groupes de sécurité qui ont été créés automatiquement dans l'option 2.

Tâche 4 (facultatif) : Nettoyer

Maintenant que vous avez terminé le tutoriel, il est recommandé de nettoyer (supprimer) toutes les ressources que vous ne voulez plus utiliser. Le nettoyage AWS des ressources évite à votre compte d'encourir des frais supplémentaires.

Si vous avez lancé une EC2 instance spécifiquement pour ce didacticiel, vous pouvez y mettre fin pour ne plus avoir à encourir de frais associés.

Pour résilier une instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance que vous avez créée pour ce tutoriel, puis choisissez Instance state (État de l'instance), Terminate instance (Résilier l'instance).
4. Choisissez Résilier lorsque vous êtes invité à confirmer.

Si vous avez créé une RDS base de données spécialement pour ce didacticiel, vous pouvez la supprimer pour ne plus être facturée.

Pour supprimer une RDS base de données à l'aide de la console

1. Ouvrez la RDS console Amazon à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Databases (Bases de données).
3. Sélectionnez la RDS base de données que vous avez créée pour ce didacticiel, puis choisissez Actions, Supprimer.
4. Saisissez **`delete me`** dans la case, puis choisissez Delete (Supprimer).

Option 3 : connecter manuellement une instance à une RDS base de données en créant des groupes de sécurité

L'objectif de l'option 3 est d'apprendre à configurer manuellement la connexion entre une EC2 instance et une RDS base de données en reproduisant manuellement la configuration de la fonctionnalité de connexion automatique.

Tâches

- Avant de commencer
- Tâche 1 (facultatif) : Lancer une EC2 instance
- Tâche 2 (facultatif) : créer une RDS base de données
- Tâche 3 : connecter manuellement votre EC2 instance à votre RDS base de données en créant des groupes de sécurité et en les affectant aux instances
- Tâche 4 (facultatif) : Nettoyer

Avant de commencer

Vous aurez besoin des éléments suivants pour compléter ce tutoriel :

- EC2Instance identique à la RDS base VPC de données. Vous pouvez utiliser une EC2 instance existante ou suivre les étapes de la tâche 1 pour créer une nouvelle instance.
- Une RDS base de données qui se trouve dans la même instance VPC que l'EC2instance. Vous pouvez utiliser une RDS base de données existante ou suivre les étapes de la tâche 2 pour créer une nouvelle base de données.
- Des autorisations pour appeler les opérations suivantes :
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Tâche 1 (facultatif) : Lancer une EC2 instance

> **Note**
>
> Le lancement d'une instance n'est pas l'objet de ce tutoriel. Si vous possédez déjà une EC2 instance Amazon et que vous souhaitez l'utiliser dans ce didacticiel, vous pouvez ignorer cette tâche.

L'objectif de cette tâche est de lancer une EC2 instance afin que vous puissiez terminer la tâche 3 dans laquelle vous configurez la connexion entre votre EC2 instance et votre RDS base de données Amazon. Les étapes de cette tâche configurent l'EC2instance comme suit :

- Nom de l'instance : **`tutorial-instance`**
- AMI: Amazon Linux 2

- Type d'instance : `t2.micro`
- Attribuer automatiquement l'adresse IP publique : Activé
- Groupe de sécurité avec les trois règles suivantes :
  - Autoriser SSH depuis votre adresse IP
  - Autorisez HTTPS le trafic depuis n'importe où
  - Autorisez HTTP le trafic depuis n'importe où

> **Important**
>
> Dans un environnement de production, vous devez configurer votre instance pour répondre à vos besoins spécifiques.

Pour lancer une instance EC2

1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Sur le EC2tableau de bord, choisissez Launch instance.
3. Sous Name and tags (Noms et balises), pour Name (Nom), saisissez un nom pour identifier votre instance. Pour ce tutoriel, nommez l'instance **`tutorial-instance-manual-1`**. Bien que le nom de l'instance ne soit pas obligatoire, il vous aidera à l'identifier facilement.
4. Sous Images de l'application et du système d'exploitation, choisissez AMI celle qui répond aux besoins de votre serveur Web. Ce tutoriel utilise Amazon Linux.
5. Sous Instance type (Type d'instance), pour Instance type (Type d'instance), sélectionnez un type d'instance qui répond aux besoins de votre serveur Web. Ce tutoriel utilise `t2.micro`.

   > **Note**
   >
   > Vous pouvez utiliser Amazon EC2 dans le cadre du niveau gratuit à condition que votre AWS compte date de moins de 12 mois et que vous choisissiez un type d'`t2.micro`instance, ou `t3.micro` dans les régions où ce type d'instance n'`t2.micro`est pas disponible. Sachez que lorsque vous lancez une instance t3.micro, elle passe par défaut en mode illimité, ce qui peut entraîner des frais supplémentaires en fonction de l'utilisation. CPU

6. Sous Key pair (login) (Paire de clés (connexion)), pour Key pair name (Nom de la paire de clés), choisissez votre paire de clés.
7. Sous Network settings (Paramètres réseau), effectuez les opérations suivantes :

   a. Pour le réseau et le sous-réseau, si vous n'avez pas modifié votre VPC ou vos sous-réseaux par défaut, vous pouvez conserver les paramètres par défaut.

      Si vous avez modifié vos sous-réseaux VPC ou sous-réseaux par défaut, vérifiez les points suivants :

      i. L'instance doit être VPC identique à la RDS base de données. Par défaut, vous n'en avez qu'unVPC.

      ii. L'instance dans VPC laquelle vous lancez votre instance doit être connectée à une passerelle Internet afin que vous puissiez accéder à votre serveur Web depuis Internet. Votre configuration par défaut VPC est automatiquement configurée avec une passerelle Internet.

      iii. Pour vous assurer que votre instance reçoit une adresse IP publique, pour Auto-assign public IP (Attribuer automatiquement une adresse IP publique), vérifiez que Enable (Activer) est sélectionné. Si l'option Disable (Désactiver) est sélectionnée, choisissez Edit (Modifier) (à droite de Network Settings (Paramètres réseau)), puis, pour Auto-assign public IP (Attribuer automatiquement une adresse IP publique), choisissez Enable (Activer).

   b. Pour vous connecter à votre instance en utilisantSSH, vous avez besoin d'une règle de groupe de sécurité qui autorise le trafic SSH (Linux) ou RDP (Windows) à partir de l'IPv4adresse publique de votre ordinateur. Par défaut, lorsque vous lancez une instance, un nouveau groupe de sécurité est créé avec une règle qui autorise le SSH trafic entrant en provenance de n'importe où.

      Pour vous assurer que seule votre adresse IP peut se connecter à votre instance, sous Pare-feu (groupes de sécurité), dans la liste déroulante située à côté de la case à cocher Autoriser le SSH trafic depuis, sélectionnez Mon adresse IP.

   c. Pour autoriser le trafic depuis Internet vers votre instance, cochez les cases suivantes :

      - Autoriser HTTPs le trafic en provenance d'Internet
      - Autoriser HTTP le trafic en provenance d'Internet

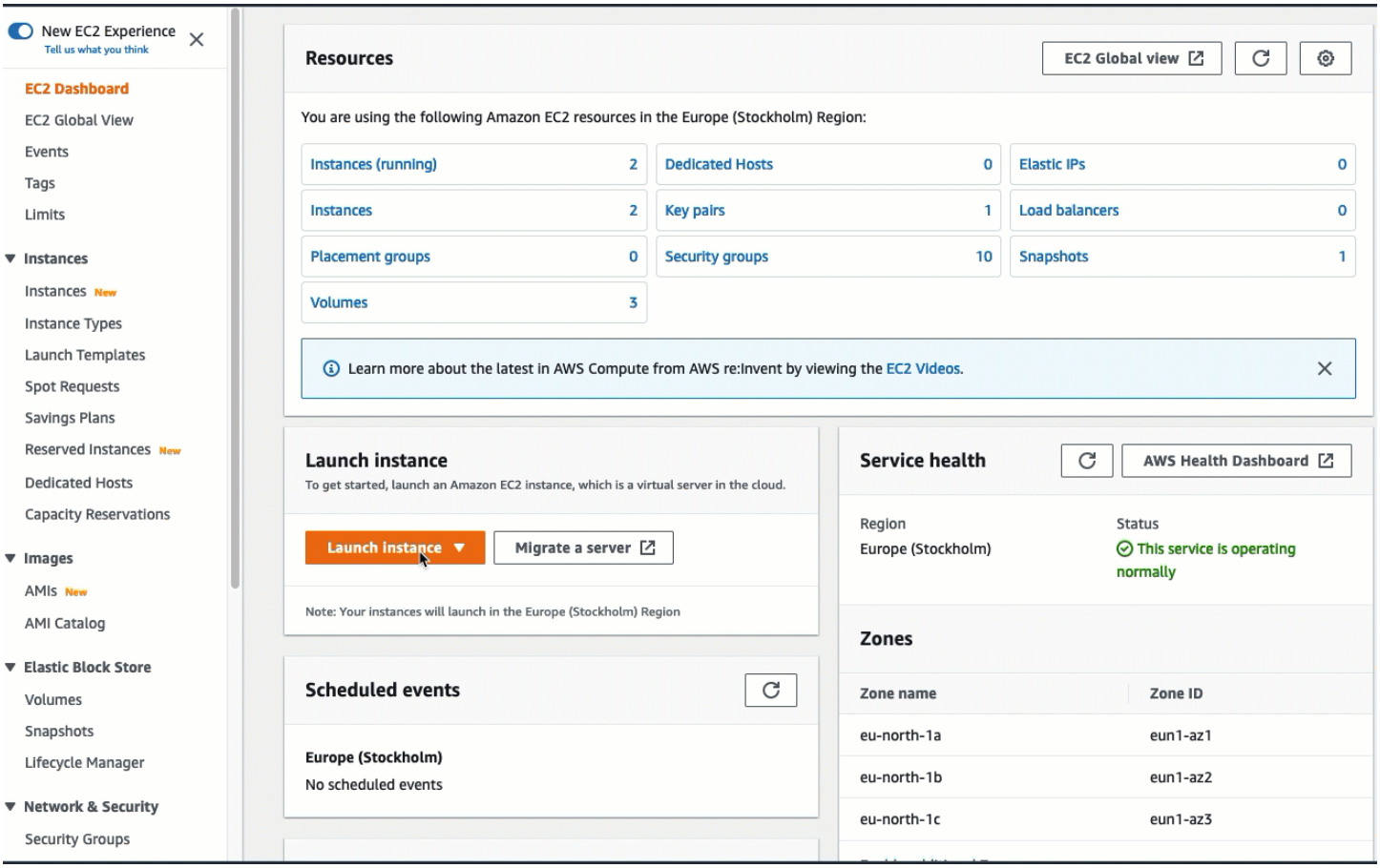
8. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance).

9. Sélectionnez View all instances (Afficher toutes les instances) pour fermer la page de confirmation et revenir à la console. Votre instance sera d'abord dans un état `pending`, puis passera à l'état `running`.

   Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez Résoudre les problèmes de lancement des EC2 instances Amazon.

Pour plus d'informations sur le lancement d'une instance, consultez Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console.

Afficher une animation : lancer une EC2 instance



Tâche 2 (facultatif) : créer une RDS base de données

> **Note**
>
> La création d'une RDS base de données n'est pas l'objet de cette partie du didacticiel. Si vous possédez déjà une RDS base de données et que vous souhaitez l'utiliser pour ce didacticiel, vous pouvez ignorer cette tâche.

L'objectif de cette tâche est de créer une RDS base de données. Vous utiliserez cette instance dans la tâche 3 lorsque vous la connecterez à votre EC2 instance. Les étapes de cette tâche configurent la RDS base de données comme suit :

- Type de moteur : My SQL
- Modèle : offre gratuite
- Identifiant d'instance de base de données : **`tutorial-database-manual`**
- Classe d'instance de base de données : `db.t3.micro`

> **Important**
>
> Dans un environnement de production, vous devez configurer votre instance pour répondre à vos besoins spécifiques.

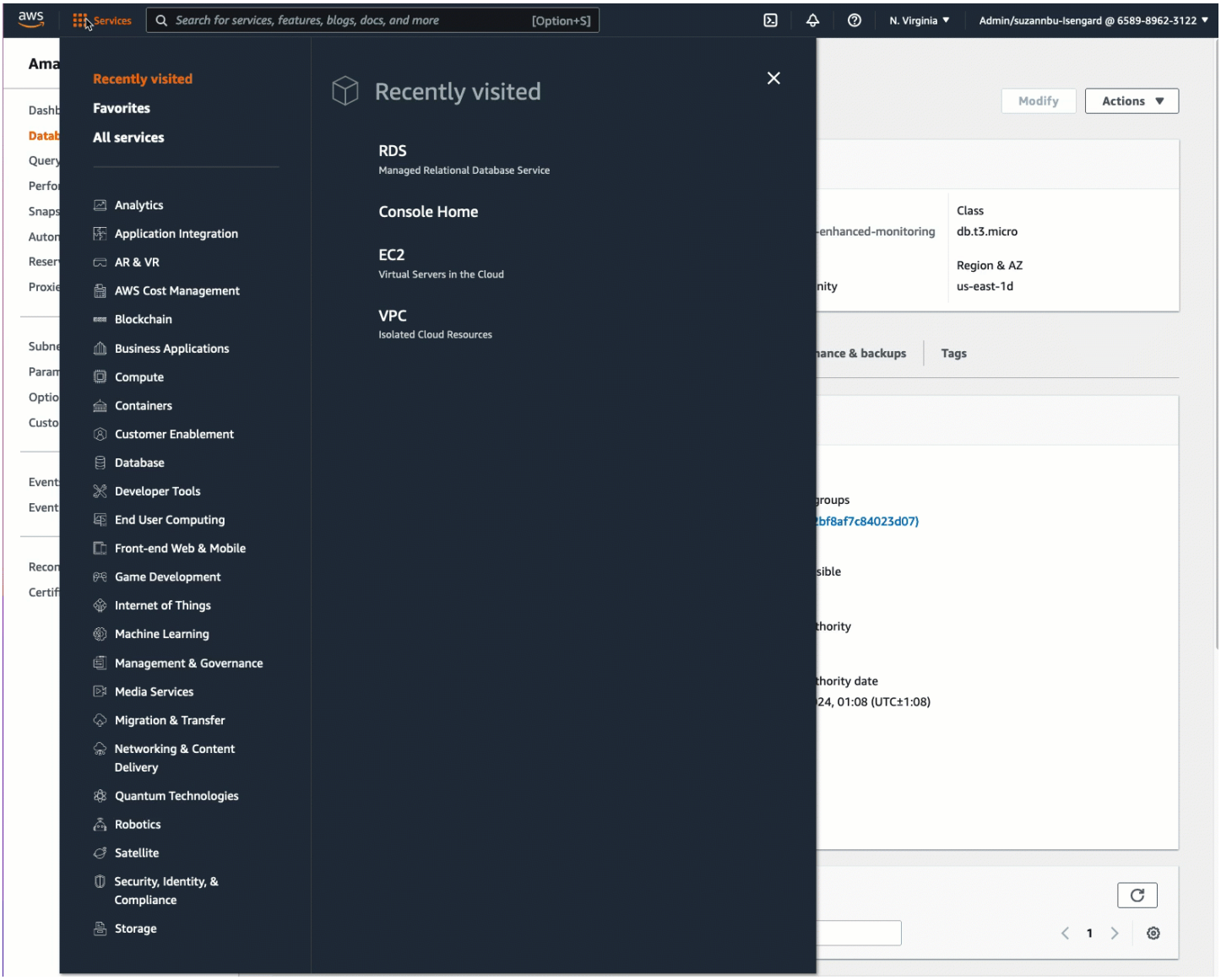
Pour créer une instance My SQL DB

1. Ouvrez la RDS console Amazon à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le sélecteur de région (en haut à droite), choisissez l'instance Région AWS dans laquelle vous avez créé l'EC2instance. L'EC2instance et l'instance de base de données doivent se trouver dans la même région.
3. Dans le tableau de bord, choisissez Create database (Créer une base de données).
4. Sous Choose a database creation method (Choisir une méthode de création de base de données), choisissez Easy create (Création facile). Lorsque vous choisissez cette option, la fonction de connexion automatique permettant de configurer automatiquement la connexion n'est pas disponible.

5. Sous Options du moteur, pour Type de moteur, sélectionnez Mon SQL.
6. Pour DB instance size (Taille de l'instance de base de données), choisissez Free tier (Offre gratuite).
7. Pour l'identifiant de l'instance de base de données, entrez le nom de la RDS base de données. Dans le cadre de ce didacticiel, entrez **`tutorial-database-manual`**.
8. Pour Master username (Nom d'utilisateur principal), laissez le nom par défaut, qui est **`admin`**.
9. Pour Master password (Mot de passe principal), saisissez un mot de passe dont vous pouvez vous souvenir pour ce tutoriel, puis, pour Confirm password (Confirmer le mot de passe), saisissez à nouveau le mot de passe.
10. Choisissez Créer une base de données.

    Sur l'écran Databases (Bases de données), le Status (Statut) de la nouvelle instance de base de données est Creating (Création) jusqu'à ce que l'instance de base de données soit prête à être utilisée. Lorsque l'état passe à Available (Disponible), vous pouvez vous connecter à l'instance de base de données. En fonction de la quantité de stockage et de la classe d'instance de base de données, la mise à disposition de la nouvelle instance peut prendre jusqu'à 20 minutes.

Voir une animation : création d'une instance de base de données



Tâche 3 : connecter manuellement votre EC2 instance à votre RDS base de données en créant des groupes de sécurité et en les affectant aux instances

L'objectif de cette tâche est de reproduire la configuration de connexion de la fonctionnalité de connexion automatique en effectuant manuellement les opérations suivantes : vous créez deux nouveaux groupes de sécurité, puis vous ajoutez un groupe de sécurité à l'EC2instance et à la RDS base de données.

Pour créer deux nouveaux groupes de sécurité et en attribuer un à l'EC2instance et à la RDS base de données

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Créez d'abord le groupe de sécurité à ajouter à l'EC2instance, comme suit :
   a. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité).
   b. Sélectionnez Create security group (Créer un groupe de sécurité).
   c. Pour Security group name (Nom du groupe de sécurité), saisissez un nom descriptif pour le groupe de sécurité. Dans le cadre de ce didacticiel, entrez **`ec2-rds-manual-configuration`**.
   d. Pour Description, saisissez une brève description. Dans le cadre de ce didacticiel, entrez **`EC2 instance security group to allow EC2 instance to securely connect to RDS database`**.
   e. Sélectionnez Create security group (Créer un groupe de sécurité). Vous reviendrez dans ce groupe de sécurité pour ajouter une règle sortante après avoir créé le groupe de sécurité de RDS base de données.
3. Créez maintenant le groupe de sécurité à ajouter à la RDS base de données, comme suit :
   a. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité).
   b. Sélectionnez Create security group (Créer un groupe de sécurité).
   c. Pour Security group name (Nom du groupe de sécurité), saisissez un nom descriptif pour le groupe de sécurité. Dans le cadre de ce didacticiel, entrez **`rds-ec2-manual-configuration`**.
   d. Pour Description, saisissez une brève description. Dans le cadre de ce didacticiel, entrez **`RDS database security group to allow EC2 instance to securely connect to RDS database`**.
   e. Sous Inbound rules (Règles entrantes), choisissez Add rule (Ajouter une règle), puis effectuez les opérations suivantes :
      i. Pour Type, choisissez MYSQL/Aurora.
      ii. Pour Source, choisissez le groupe de sécurité d'EC2instance ec2- rds-manual-configuration que vous avez créé à l'étape 2 de cette procédure.
   f. Sélectionnez Create security group (Créer un groupe de sécurité).
4. Modifiez le groupe de sécurité de l'EC2instance pour ajouter une règle sortante, comme suit :

a. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité).

b. Sélectionnez le groupe de sécurité de l'EC2instance (vous l'avez nommé**`ec2-rds-manual-configuration`**), puis cliquez sur l'onglet Règles sortantes.

c. Choisissez Edit outbound rules (Modifier les règles sortantes).

d. Choisissez Add rule (Ajouter une règle) et effectuez les opérations suivantes :

   i. Pour Type, choisissez MYSQL/Aurora.

   ii. Pour Source, choisissez le groupe de sécurité RDS de base de données rds-ec2-manual-configuration que vous avez créé à l'étape 3 de cette procédure.

   iii. Sélectionnez Enregistrer les règles.

5. Ajoutez le groupe de sécurité de l'EC2instance à l'EC2instance comme suit :

   a. Dans le panneau de navigation, choisissez Instances.

   b. Sélectionnez votre EC2 instance, puis choisissez Actions, Sécurité, Modifier les groupes de sécurité.

   c. Sous Groupes de sécurité associés, choisissez le champ Sélectionner les groupes de sécurité, choisissez ec2- rds-manual-configuration que vous avez créé précédemment, puis choisissez Ajouter un groupe de sécurité.

   d. Choisissez Save (Enregistrer).

6. Ajoutez le groupe RDS de sécurité de base de données à la RDS base de données comme suit :

   a. Ouvrez la RDS console Amazon à l'adresse https://console.aws.amazon.com/rds/.

   b. Dans le panneau de navigation, choisissez Databases (Bases de données) et sélectionnez votre base de données.

   c. Sélectionnez Modifier.

   d. Sous Connectivity (Connectivité), pour Security group (Groupe de sécurité), choisissez rds-ec2-manual-configuration que vous avez créé précédemment, puis cliquez sur Continue (Continuer).

   e. Sous Scheduling of Modifications (Planification des modifications), sélectionnez Apply immediately (Appliquer immédiatement).

   f. Choisissez Modifier l'instance de base de données.

Vous avez maintenant terminé les étapes manuelles qui imitent les étapes automatiques qui se produisent lorsque vous utilisez la fonction de connexion automatique.

Vous avez terminé l'option 3 de ce tutoriel. Si vous avez terminé les options 1, 2 et 3, et que vous n'avez plus besoin des ressources créées dans ce tutoriel, vous devriez les supprimer pour éviter d'encourir des coûts inutiles. Pour de plus amples informations, veuillez consulter Tâche 4 (facultatif) : Nettoyer.

Tâche 4 (facultatif) : Nettoyer

Maintenant que vous avez terminé le tutoriel, il est recommandé de nettoyer (supprimer) toutes les ressources que vous ne voulez plus utiliser. Le nettoyage AWS des ressources évite à votre compte d'encourir des frais supplémentaires.

Si vous avez lancé une EC2 instance spécifiquement pour ce didacticiel, vous pouvez y mettre fin pour ne plus avoir à encourir de frais associés.

Pour résilier une instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance que vous avez créée pour ce tutoriel, puis choisissez Instance state (État de l'instance), Terminate instance (Résilier l'instance).
4. Choisissez Résilier lorsque vous êtes invité à confirmer.

Si vous avez créé une RDS base de données spécialement pour ce didacticiel, vous pouvez la supprimer pour ne plus être facturée.

Pour supprimer une RDS base de données à l'aide de la console

1. Ouvrez la RDS console Amazon à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Databases (Bases de données).
3. Sélectionnez la RDS base de données que vous avez créée pour ce didacticiel, puis choisissez Actions, Supprimer.
4. Saisissez **`delete me`** dans la case, puis choisissez Delete (Supprimer).

EC2Fleet et Spot Fleet

EC2Fleet et Spot Fleet sont conçus pour être un moyen utile de lancer une flotte de dizaines, centaines ou milliers d'EC2instances Amazon en une seule opération. Chaque instance d'un parc est configurée soit par un modèle de lancement, soit par un ensemble de paramètres de lancement que vous configurez manuellement lors du lancement.

Rubriques

Fonctionnalités et avantages

Les flottes offrent les fonctionnalités et avantages suivants, qui vous permettent de maximiser les économies et d'optimiser la disponibilité et les performances lorsque vous exécutez des applications sur plusieurs EC2 instances.

Plusieurs types d'instances

Une flotte peut lancer plusieurs types d'instances, ce qui garantit qu'elle ne dépend pas de la disponibilité d'un seul type d'instance. Cela augmente la disponibilité globale des instances de votre flotte.

Répartition des instances dans les zones de disponibilité

Une flotte d'instances tente automatiquement de répartir uniformément les instances sur plusieurs zones de disponibilité pour une haute disponibilité. Cela garantit la résilience en cas d'indisponibilité d'une zone de disponibilité.

Plusieurs options d'achat

Une flotte peut lancer plusieurs options d'achat (instances ponctuelles et à la demande), ce qui vous permet d'optimiser les coûts grâce à l'utilisation d'instances ponctuelles. Vous pouvez également profiter des remises sur les instances réservées et le Savings Plan en les utilisant conjointement avec les instances à la demande au sein de la flotte.

Remplacement automatique des instances Spot

Si votre parc comprend des instances Spot, il peut automatiquement demander une capacité Spot de remplacement en cas d'interruption de vos instances Spot. Grâce au rééquilibrage des capacités, une flotte peut également surveiller et remplacer de manière proactive vos instances Spot qui présentent un risque élevé d'interruption.

Capacité de réserve à la demande

Une flotte peut utiliser une réservation de capacité à la demande pour réserver une capacité à la demande. Un parc peut également inclure des blocs de capacité pour le machine learning, ce qui vous permet de réserver des GPU instances à une date future afin de prendre en charge vos charges de travail d'apprentissage automatique (ML) de courte durée.

Quelle est la meilleure méthode de gestion de flotte à utiliser ?

En règle générale, nous vous recommandons de lancer des flottes d'instances ponctuelles et à la demande avec Amazon EC2 Auto Scaling, car cela fournit des fonctionnalités supplémentaires que vous pouvez utiliser pour gérer votre flotte. La liste des fonctionnalités supplémentaires inclut le remplacement automatique des surveillances de l'état pour les instances Spot et à la demande, les surveillances de l'état basées sur les applications et une intégration avec Elastic Load Balancing pour garantir une répartition uniforme du trafic applicatif vers vos instances saines. Vous pouvez également utiliser les groupes Auto Scaling lorsque vous utilisez AWS des services tels qu'AmazonECS, Amazon EKS (groupes de nœuds autogérés) et Amazon VPC Lattice. Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon EC2 Auto Scaling.

Si vous ne pouvez pas utiliser Amazon EC2 Auto Scaling, vous pouvez envisager d'utiliser EC2 Fleet ou Spot Fleet. EC2Fleet et Spot Fleet offrent les mêmes fonctionnalités de base. Cependant, EC2 Fleet n'est disponible qu'à l'aide d'une ligne de commande et ne fournit pas de support de console. Spot Fleet fournit un support pour console, mais est basé sur API un héritage sans investissement planifié.

Utilisez le tableau suivant pour déterminer la méthode de flotte à utiliser.

Méthode de gestion de flotte	Quand l'utiliser ?	Cas d'utilisation
Amazon EC2 Auto Scaling	• Vous avez besoin de plusieurs instances avec une configuration unique ou une configuration mixte. • Vous souhaitez automatiser la gestion du cycle de vie de vos instances.	Créez un groupe Auto Scaling qui gère le cycle de vie de vos instances tout en gardant le nombre d'instances souhaité. Prend en charge la mise à l'échelle horizontale (ajout d'instances supplémentaires) entre les limites minimale et maximale spécifiées.
EC2Flotte	• Vous avez besoin de plusieurs instances avec une configuration unique ou une configuration mixte. • Vous voulez gérer vous-même le cycle de vie de vos instances. • Si vous n'avez pas besoin de mise à l'échelle automatique, nous vous recommandons d'utiliser un `instant` type EC2 Fleet.	Créez un `instant` parc d'instances à la demande et d'instances ponctuelles en une seule opération, avec plusieurs spécifications de lancement qui varient en fonction du type d'instanceAMI, de la zone de disponibilité ou du sous-réseau. La stratégie d'allocation des instances Spot est définie par défaut `lowest-price` par unité, mais nous vous recommandons de la remplacer `price-capacity-optimized` par.
Parc d'instances Spot	• Nous vous déconseillons vivement d'utiliser Spot Fleet car il repose sur un héritage API sans investissement planifié. • Si vous souhaitez gérer le cycle de vie de votre	Utilisez Spot Fleet uniquement si vous avez besoin d'une assistance sur console pour un cas d'utilisation dans lequel vous utiliseriez EC2 Fleet.

Méthode de gestion de flotte	Quand l'utiliser ?	Cas d'utilisation
	instance, utilisez plutôt EC2 Fleet. • Si vous ne souhaitez pas gérer le cycle de vie de votre instance, utilisez plutôt un groupe Auto Scaling.	

Options de configuration pour votre EC2 flotte ou votre flotte ponctuelle

Lors de la planification de votre EC2 flotte ou de votre flotte ponctuelle, nous vous recommandons de prendre en compte les options suivantes pour décider comment configurer votre flotte.

Option de configuration	Question	Documentation
Type de demande de flotte	Voulez-vous une flotte qui soumet une demande unique pour la capacité cible souhaitée, ou une flotte qui maintient la capacité cible au fil du temps ?	EC2Types de demandes relatives aux flottes et aux flottes ponctuelles
Spot instances	Prévoyez-vous d'inclure des instances Spot dans votre flotte ? Passez en revue les meilleures pratiques de Spot et utilisez-les lorsque vous planifiez votre flotte afin de pouvoir fournir les instances au prix le plus bas possible.	Bonnes pratiques pour Amazon EC2 Spot
Limite de dépenses pour votre flotte	Voulez-vous limiter le montant que vous paierez pour votre flotte par heure ?	Fixez une limite de dépenses pour votre EC2 flotte ou votre flotte ponctuelle

Option de configuration	Question	Documentation
Types d'instances et sélection du type d'instance basée sur les attributs	Voulez-vous spécifier les types d'instances de votre parc ou laisser Amazon EC2 sélectionner les types d'instances qui répondent aux exigences de votre application ?	Spécifiez les attributs pour la sélection du type d'instance pour EC2 Fleet ou Spot Fleet
Pondération d'instance	Souhaitez-vous attribuer des pondérations à chaque type d'instance pour représenter sa capacité de calcul et ses performances, afin qu'Amazon EC2 puisse sélectionner n'importe quelle combinaison de types d'instances disponibles pour atteindre la capacité cible souhaitée ?	Utilisez la pondération des instances pour gérer les coûts et les performances de votre EC2 flotte ou de votre flotte ponctuelle
Stratégies d'allocation	Voulez-vous décider d'optimiser la capacité disponible, le prix ou les types d'instances à utiliser pour les instances ponctuelles et les instances à la demande de votre flotte ?	Utilisez des stratégies d'allocation pour déterminer comment EC2 Fleet ou Spot Fleet exploite les capacités sur place et à la demande
Rééquilibrage de la capacité	Voulez-vous que votre flotte remplace automatiquement les instances Spot à risque ?	Utilisez le rééquilibrage des capacités dans le EC2 parc et le parc ponctuel pour remplacer les instances ponctuelles à risque
Réservation de capacité à la demande	Voulez-vous réserver de la capacité pour les instances à la demande de votre flotte ?	Utilisez les réservations de capacité pour réserver de la capacité à la demande dans EC2 Fleet

EC2Types de demandes relatives aux flottes et aux flottes ponctuelles

Le type de demande pour une EC2 flotte ou un parc ponctuel détermine si la demande est synchrone ou asynchrone, et s'il s'agit d'une demande ponctuelle pour la capacité cible souhaitée ou d'un effort continu pour maintenir la capacité au fil du temps. Lors de la configuration de votre flotte, vous devez spécifier le type de demande.

EC2Fleet et Spot Fleet proposent deux types de demandes : `request` et`maintain`. En outre, EC2 Fleet propose un troisième type de demande appelé`instant`.

Types de demandes de flotte

`instant`(EC2Flotte uniquement)

Si vous configurez le type de demande comme `instant` suit, EC2 Fleet place une demande unique synchrone pour la capacité souhaitée. Dans la API réponse, il renvoie les instances qui ont été lancées et fournit des erreurs pour les instances qui n'ont pas pu être lancées. Pour de plus amples informations, veuillez consulter Configurer un type de EC2 flotte instant.

`request`

Si vous configurez le type de demande comme `request` suit, le parc envoie une demande unique asynchrone pour la capacité souhaitée. Si la capacité diminue en raison d'interruptions ponctuelles, le parc ne tente pas de réapprovisionner les instances ponctuelles et ne soumet pas de demandes dans d'autres pools de capacité ponctuels si la capacité n'est pas disponible. Lorsque vous créez un parc d'emplacements de type Spot `request` à l'aide de la console, désactivez la case à cocher Maintenir la capacité cible.

`maintain` (default)

Si vous configurez le type de demande comme `maintain` suit, le parc place une demande asynchrone pour la capacité souhaitée et la maintient en réapprovisionnant automatiquement toutes les instances Spot interrompues. Lorsque vous créez un parc d'emplacements de type Spot `maintain` à l'aide de la console, cochez la case Maintenir la capacité cible

Configurer un type de EC2 flotte instant

La EC2 flotte de type instantané est une demande unique synchrone qui ne fait qu'une seule tentative pour lancer la capacité souhaitée. La API réponse répertorie les instances qui ont été lancées, ainsi que les erreurs relatives aux instances qui n'ont pas pu être lancées. L'utilisation d'une EC2

flotte de type instantané présente plusieurs avantages, décrits dans cet article. Des exemples de configurations sont fournis à la fin de l'article.

Pour les charges de travail qui nécessitent un lancement uniquement API pour lancer des EC2 instances, vous pouvez utiliser le. RunInstances API Toutefois, avec RunInstances, vous ne pouvez lancer que des instances à la demande ou des instances ponctuelles, mais pas les deux dans la même demande. En outre, lorsque vous lancez RunInstances des instances Spot, votre demande d'instance Spot est limitée à un type d'instance et à une zone de disponibilité. Ceci cible un seul groupe de capacité Spot (ensemble d'instances inutilisées ayant le même type d'instance et la même zone de disponibilité). Si le pool de capacité Spot ne dispose pas d'une capacité d'instance Spot suffisante pour votre demande, l' RunInstances appel échoue.

Au lieu de l'utiliser RunInstances pour lancer des instances Spot, nous vous recommandons d'utiliser le CreateFleet API avec le `type` paramètre défini sur `instant` pour bénéficier des avantages suivants :

- Launch On-Demand instances and Spot instances in one request. (Lancez des instances à la demande et des instances Spot en une seule demande.) Une EC2 flotte peut lancer des instances à la demande, des instances ponctuelles ou les deux. La demande des instances Spot est satisfaite si la capacité disponible et le prix maximum par heure que vous avez spécifié pour la demande dépassent le prix spot actuel.
- Increase the availability of Spot instances. (Augmentez la disponibilité des instances Spot.). En utilisant une EC2 flotte de types`instant`, vous pouvez lancer des instances Spot en suivant les meilleures pratiques Spot avec les avantages qui en découlent :
  - Bonnes pratiques en matière d'instances Spot : Soyez flexible en ce qui concerne les types d'instance et les zones de disponibilité.

    Bénéfices : en spécifiant plusieurs types d'instance et zones de disponibilité, vous augmentez le nombre de groupes de capacités Spot. Cela donne au service Spot une meilleure chance de trouver et d'allouer la capacité de calcul Spot souhaitée. En règle générale, faites preuve de flexibilité sur au moins 10 types d'instances pour chaque charge de travail et assurez-vous que toutes les zones de disponibilité sont configurées pour être utilisées dans votreVPC.
  - Repérez les meilleures pratiques : utilisez la stratégie price-capacity-optimized d'allocation.

    Avantage : la stratégie `price-capacity-optimized` d'allocation identifie les instances parmi les pools de capacité ponctuels les plus disponibles, puis provisionne automatiquement les instances à partir des pools les moins chers de ces pools. Comme la capacité de vos instances

Spot provient de pools dotés d'une capacité optimale, cela réduit le risque que vos instances Spot soient interrompues lorsqu'Amazon aura EC2 besoin de récupérer la capacité.

- Get access to a wider set of capabilities. (Accédez à un ensemble plus large de fonctionnalités). Pour les charges de travail nécessitant uniquement un lancement et API pour lesquelles vous préférez gérer le cycle de vie de votre instance plutôt que de laisser EC2 Fleet le gérer à votre place, utilisez le type EC2 Fleet `instant` au lieu de. RunInstancesAPI EC2Fleet fournit un ensemble de capacités plus RunInstances large que ce que montrent les exemples suivants. Pour toutes les autres charges de travail, vous devez utiliser Amazon EC2 Auto Scaling car il fournit un ensemble de fonctionnalités plus complet pour une grande variété de charges de travail, telles que les applications ELB sauvegardées, les charges de travail conteneurisées et les tâches de traitement de files d'attente.

Vous pouvez utiliser EC2 Fleet de type instantané pour lancer des instances dans des blocs de capacité. Pour de plus amples informations, veuillez consulter Tutoriel : configurez votre EC2 flotte pour lancer des instances dans des blocs de capacité.

AWS des services tels qu'Amazon EC2 Auto Scaling et Amazon EMR utilisent EC2 Fleet of type instant pour lancer EC2 des instances.

Prérequis pour une EC2 flotte de type instantané

Pour connaître les conditions préalables à la création d'une EC2 flotte, consultezEC2Prérequis relatifs à la flotte.

Comment fonctionne Instant EC2 Fleet

Lorsque vous travaillez avec un type de EC2 flotte`instant`, la séquence des événements est la suivante :

1. Configurez le type de CreateFleetdemande comme`instant`. Pour de plus amples informations, veuillez consulter Création d'une EC2 flotte. Notez qu'une fois l'APIappel passé, vous ne pouvez pas le modifier.
2. Lorsque vous passez l'APIappel, EC2 Fleet fait une demande unique synchrone pour la capacité souhaitée.
3. La API réponse répertorie les instances qui ont été lancées, ainsi que les erreurs relatives aux instances qui n'ont pas pu être lancées.
4. Vous pouvez décrire votre EC2 flotte, répertorier les instances associées à votre EC2 flotte et consulter l'historique de votre EC2 flotte.

5. Après le lancement de vos instances, vous pouvez supprimer la demande de flotte. Lorsque vous supprimez la demande de flotte, vous pouvez également choisir de résilier les instances associées ou de les laisser en cours d'exécution.
6. Vous pouvez résilier les instances à tout moment.

Exemples

Les exemples suivants montrent comment utiliser EC2 Fleet of type `instant` pour différents cas d'utilisation. Pour plus d'informations sur l'utilisation EC2 CreateFleet API des paramètres, consultez CreateFleetla EC2APIréférence Amazon.

Exemples

- Exemple 1 : Lancer des instances Spot avec la stratégie d'allocation optimisée pour la capacité
- Exemple 2 : Lancer une unique instance Spot avec la stratégie d'allocation optimisée pour la capacité
- Exemple 3 : Lancer des instances Spot en utilisant la pondération d'instance
- Exemple 4 : Lancer des instances ponctuelles dans une seule zone de disponibilité
- Exemple 5 : Lancer des instances Spot de type d'instance unique dans une seule zone de disponibilité
- Exemple 6 : Lancer des instances Spot uniquement si une capacité cible minimale peut être lancée
- Exemple 7 : Lancer des instances Spot uniquement si une capacité cible minimale du même type d'instance et dans une seule zone de disponibilité peut être lancée
- Exemple 8 : Lancer des instances avec plusieurs modèles de lancement
- Exemple 9 : Lancer des instances Spot avec une base d'instances à la demande
- Exemple 10 : Lancer des instances Spot à l'aide d'une stratégie d'allocation optimisée pour la capacité avec une base d'instances à la demande en utilisant des réservations de capacité et la stratégie d'allocation prioritaire
- Exemple 11 : Lancer des instances ponctuelles à l'aide d' capacity-optimized-prioritized une stratégie d'allocation
- Exemple 12 : Spécifier un paramètre de Systems Manager au lieu d'un AMI ID

Exemple 1 : Lancer des instances Spot avec la stratégie d'allocation optimisée pour la capacité

L'exemple suivant spécifie les paramètres requis dans un type de EC2 flotte `instant` : un modèle de lancement, une capacité cible, une option d'achat par défaut et des remplacements de modèles de lancement.

- Le modèle de lancement est identifié par son nom de modèle de lancement et son numéro de version.
- Les 12 remplacements de modèle de lancement spécifient 4 types d'instance différents et 3 sous-réseaux différents, chacun dans une zone de disponibilité distincte. Chaque combinaison de type d'instance et de sous-réseau définit un groupe de capacités Spot, ce qui donne un total de 12 groupes de capacités Spot.
- La capacité cible pour la flotte est de 20 instances.
- L'option d'achat par défaut est `spot`, ce qui fait que la flotte tente de lancer 20 instances Spot dans le groupe de capacités Spot avec une capacité optimale pour le nombre d'instances qui sont lancées.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
            },
```

```
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
   ],
   "TargetCapacitySpecification": {
       "TotalTargetCapacity": 20,
       "DefaultTargetCapacityType": "spot"
   },
   "Type": "instant"
```

```
}
```

Exemple 2 : Lancer une unique instance Spot avec la stratégie d'allocation optimisée pour la capacité

Vous pouvez lancer de manière optimale une instance Spot à la fois en effectuant plusieurs API appels EC2 Fleet de type `instant` 1. TotalTargetCapacity

L'exemple suivant spécifie les paramètres requis dans une EC2 flotte de type instantané : un modèle de lancement, une capacité cible, une option d'achat par défaut et des remplacements de modèles de lancement. Le modèle de lancement est identifié par son nom de modèle de lancement et son numéro de version. Les 12 remplacements de modèle de lancement ont 4 types d'instance différents et 3 sous-réseaux différents, chacun dans une zone de disponibilité distincte. La capacité cible de la flotte est de 1 instance, et l'option d'achat par défaut est Spot, ce qui fait que la flotte tente de lancer une instance Spot à partir de l'un des 12 groupes de capacités Spot en fonction de la stratégie d'allocation optimisée pour la capacité, pour lancer une instance Spot à partir du groupe de capacités le plus disponible.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.large",
```

```
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"c5d.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"c5d.large",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemple 3 : Lancer des instances Spot en utilisant la pondération d'instance

Les exemples suivants utilisent la pondération d'instance, ce qui signifie que le prix est déterminé par heure d'unité, et non par heure d'instance. Chaque configuration de lancement répertorie un type d'instance différent et un poids différent en fonction du nombre d'unités de charge de travail pouvant être exécutées sur l'instance en supposant qu'une unité de charge de travail nécessite 15 Go de mémoire et 4 GovCPUs. Par exemple, un m5.xlarge (4 vCPUs et 16 Go de mémoire) peut exécuter une unité et est pondéré 1, un m5.2xlarge (8 vCPUs et 32 Go de mémoire) peut exécuter 2 unités et est pondéré 2, etc. La capacité cible totale est définie sur 40 unités. L'option d'achat par défaut est Spot et la stratégie d'allocation est optimisée pour la capacité, ce qui se traduit par 40 m5.xlarge (40 divisé par 1), 20 m5.2xlarge (40 divisé par 2), 10 m5.4xlarge (40 divisé par 4), 5 m5.8xlarge (40 divisé par 8) ou un mélange de types d'instances avec des pondérations totalisant la capacité désirée, sur la base de la stratégie d'allocation optimisée pour les capacités.

Pour de plus amples informations, veuillez consulter Utilisez la pondération des instances pour gérer les coûts et les performances de votre EC2 flotte ou de votre flotte ponctuelle.

```
{
   "SpotOptions":{
      "AllocationStrategy":"capacity-optimized"
   },
   "LaunchTemplateConfigs":[
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":1
```

```
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":2
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":2
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":2
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":4
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":4
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":4
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":8
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":8
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-49e41922",
```

```
               "WeightedCapacity":8
            }
         ]
      }
   ],
   "TargetCapacitySpecification":{
      "TotalTargetCapacity":40,
      "DefaultTargetCapacityType":"spot"
   },
   "Type":"instant"
}
```

Exemple 4 : Lancer des instances ponctuelles dans une seule zone de disponibilité

Vous pouvez configurer un parc pour lancer toutes les instances dans une seule zone de disponibilité en définissant les options Spot SingleAvailabilityZone sur true.

Les 12 remplacements de modèle de lancement ont des types d'instance et des sous-réseaux différents (chacun dans une zone de disponibilité distincte), mais la même capacité pondérée. La capacité cible totale est de 20 instances, l'option d'achat par défaut est Spot et la stratégie d'allocation Spot est optimisée pour la capacité. La EC2 flotte lance 20 instances Spot toutes dans une seule AZ, à partir du ou des pools de capacités Spot avec une capacité optimale conformément aux spécifications de lancement.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
```

```
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
   ],
```

```
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemple 5 : Lancer des instances Spot de type d'instance unique dans une seule zone de disponibilité

Vous pouvez configurer un parc pour lancer toutes les instances du même type et dans une seule zone de disponibilité en définissant SpotOptions SingleInstanceType les valeurs true et SingleAvailabilityZone true.

Les 12 remplacements de modèle de lancement ont des types d'instance et des sous-réseaux différents (chacun dans une zone de disponibilité distincte), mais la même capacité pondérée. La capacité cible totale est de 20 instances, l'option d'achat par défaut est Spot et la stratégie d'allocation Spot est optimisée pour la capacité. La EC2 flotte lance 20 instances Spot du même type d'instance, toutes regroupées dans une seule AZ à partir du pool d'instances Spot avec une capacité optimale conformément aux spécifications de lancement.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
```

```
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
   ],
   "TargetCapacitySpecification": {
```

```
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemple 6 : Lancer des instances Spot uniquement si une capacité cible minimale peut être lancée

Vous pouvez configurer une flotte pour lancer des instances uniquement si la capacité cible minimale peut être lancée en définissant les options MinTargetCapacity Spot sur la capacité cible minimale que vous souhaitez lancer ensemble.

Les 12 remplacements de modèle de lancement ont des types d'instance et des sous-réseaux différents (chacun dans une zone de disponibilité distincte), mais la même capacité pondérée. La capacité cible totale et la capacité cible minimum sont toutes deux de 20 instances, l'option d'achat par défaut est Spot et la stratégie d'allocation Spot est optimisée pour la capacité. La EC2 flotte lance 20 instances ponctuelles à partir du pool de capacités ponctuelles avec une capacité optimale en utilisant les remplacements du modèle de lancement, uniquement si elle peut lancer les 20 instances en même temps.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
```

```
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"c5d.4xlarge",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"c5d.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"c5d.4xlarge",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5d.4xlarge",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5d.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5d.4xlarge",
            "SubnetId":"subnet-49e41922"
         }
      ]
   }
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "DefaultTargetCapacityType": "spot"
```

```
    },
    "Type": "instant"
}
```

Exemple 7 : Lancer des instances Spot uniquement si une capacité cible minimale du même type d'instance et dans une seule zone de disponibilité peut être lancée

Vous pouvez configurer un parc pour lancer des instances uniquement si la capacité cible minimale peut être lancée avec un seul type d'instance dans une seule zone de disponibilité en définissant les options MinTargetCapacity Spot sur la capacité cible minimale que vous souhaitez lancer en même temps que SingleInstanceType les SingleAvailabilityZone options.

Les 12 spécifications de lancement, qui remplacent le modèle de lancement, ont des types et des sous-réseaux d'instances différents (chacun dans une AZ différentes), mais la même capacité pondérée. La capacité cible totale et la capacité cible minimale sont toutes deux fixées à 20 instances, l'option d'achat par défaut est au comptant, la stratégie d'allocation au comptant est optimisée en termes de capacité, SingleInstanceType c'est vrai et SingleAvailabilityZone vrai. La EC2 flotte lance 20 instances ponctuelles du même type, toutes regroupées dans une seule AZ à partir du pool de capacités ponctuelles avec une capacité optimale conformément aux spécifications de lancement, uniquement si elle peut lancer les 20 instances en même temps.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
```

```
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
   ],
```

```
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemple 8 : Lancer des instances avec plusieurs modèles de lancement

Vous pouvez configurer une flotte pour lancer des instances avec des spécifications de lancement différentes pour différents types d'instance ou un groupe de types d'instance, en spécifiant plusieurs modèles de lancement. Dans cet exemple, nous voulons avoir des tailles de EBS volume différentes pour différents types d'instances et cela est configuré dans les modèles de lancement ec2-fleet-lt-4xl, ec2-fleet-lt-9xl et ec2-fleet-lt-18xl.

Dans cet exemple, nous utilisons 3 modèles de lancement différents pour les 3 types d'instance en fonction de leur taille. Les remplacements de spécifications de lancement sur tous les modèles de lancement utilisent des pondérations d'instance basées vCPUs sur le type d'instance. La capacité cible totale est de 144 unités, l'option d'achat par défaut est Spot et la stratégie d'allocation Spot est optimisée pour la capacité. La EC2 flotte peut soit lancer 9 c5n.4xlarge (144 divisés par 16) en utilisant le modèle de lancement ec2-fleet-4xl, soit 4 c5n.9xlarge (144 divisés par 36) en utilisant le modèle de lancement ec2-fleet-9xl, soit 2 c5n.18xlarge (144 divisés par 72) en utilisant le modèle de lancement ec2-fleet-18xl, ou une combinaison de types d'instances avec des poids s'ajoutant à la capacité souhaitée en fonction du stratégie d'allocation optimisée en termes de capacité.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-18xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":72
            },
```

```
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":72
            },
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":72
            }
         ]
      },
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-9xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":36
            },
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":36
            },
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":36
            }
         ]
      },
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-4xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-fae8c380",
```

```
                "WeightedCapacity":16
            },
            {
                "InstanceType":"c5n.4xlarge",
                "SubnetId":"subnet-e7188bab",
                "WeightedCapacity":16
            },
            {
                "InstanceType":"c5n.4xlarge",
                "SubnetId":"subnet-49e41922",
                "WeightedCapacity":16
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 144,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemple 9 : Lancer des instances Spot avec une base d'instances à la demande

L'exemple suivant spécifie la capacité cible totale de 20 instances pour la flotte et une capacité cible de 5 instances à la demande. L'option d'achat par défaut est Spot. La flotte d'instances lance 5 instances à la demande comme spécifié, mais a besoin de lancer 15 instances supplémentaires pour assurer la capacité cible totale. L'option d'achat correspondant à la différence est calculée sous la forme TotalTargetCapacity — OnDemandTargetCapacity = DefaultTargetCapacityType, ce qui permet à la flotte de lancer 15 instances ponctuelles qui constituent l'un des 12 pools de capacités ponctuelles sur la base de la stratégie d'allocation optimisée pour les capacités.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
```

```
        "Overrides":[
           {
              "InstanceType":"c5.large",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"c5.large",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"c5.large",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"c5d.large",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"c5d.large",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"c5d.large",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"m5.large",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"m5.large",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"m5.large",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"m5d.large",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"m5d.large",
              "SubnetId":"subnet-e7188bab"
```

```
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemple 10 : Lancer des instances Spot à l'aide d'une stratégie d'allocation optimisée pour la capacité avec une base d'instances à la demande en utilisant des réservations de capacité et la stratégie d'allocation prioritaire

Vous pouvez configurer un parc pour utiliser les réservations de capacité à la demande d'abord lorsque vous lancez une base d'instances à la demande avec le type de capacité cible par défaut comme emplacement en définissant la stratégie d'utilisation pour les réservations de capacité sur use-capacity-reservations-first. Et si plusieurs groupes d'instances n'utilisent pas réservations de capacité, la stratégie d'allocation à la demande choisie est appliquée. Dans cet exemple, la stratégie d'allocation à la demande est prioritaire..

Dans cet exemple, il y a 6 réservations de capacité inutilisées disponibles. Cette capacité est inférieure à la capacité cible à la demande de la flotte de 10 instances à la demande.

Le compte dispose des 6 réservations de capacité suivantes inutilisées dans 2 groupes différents. Le nombre de réservations de capacité dans chaque pool est indiqué par AvailableInstanceCount.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

```
{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

La configuration de flotte suivante affiche uniquement les configurations pertinentes pour cet exemple. La stratégie d'allocation à la demande est priorisée, et la stratégie d'utilisation des réservations de capacité l'est use-capacity-reservations-first. La stratégie d'allocation Spot utilisée est optimisé au niveau de la capacité La capacité cible totale est 20, la capacité cible à la demande est 10 et le type de capacité cible par défaut est spot.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "OnDemandOptions":{
       "CapacityReservationOptions": {
         "UsageStrategy": "use-capacity-reservations-first"
       },
       "AllocationStrategy":"prioritized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 2.0
```

```
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 3.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 4.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 5.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 6.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 7.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 8.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 9.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 10.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab",
```

```
                "Priority": 11.0
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-49e41922",
                "Priority": 12.0
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity": 10,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Après avoir créé la flotte instantanée à l'aide de la configuration précédente, les 20 instances suivantes sont lancées pour atteindre la capacité cible :

- 7 instances à la demande c5.large dans us-east-1a ; c5.large dans us-east-1a est priorisé en premier et il y a 3 réservations de capacité c5.large inutilisées disponibles. Les réservations de capacité sont d'abord utilisées pour lancer 3 instances à la demande, puis 4 instances à la demande supplémentaires sont lancées selon la stratégie d'allocation à la demande, qui est prioritized dans cet exemple.
- 3 instances à la demande m5.large dans us-east-1a – m5.large dans us-east-1a est priorisé en second, et il y a 3 réservations de capacité c3.large inutilisées disponibles.
- 10 instances Spot issues de l'un des 12 groupes de capacités Spot ayant la capacité optimale selon la stratégie d'allocation optimisée pour cette capacité.

Une fois la flotte lancée, vous pouvez courir describe-capacity-reservationspour voir combien de réservations de capacité inutilisées restent. Dans cet exemple, vous devriez obtenir la réponse suivante, qui montre que toutes les réservations de capacité c5.large et m5.large ont été utilisées.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}
```

```
{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "AvailableInstanceCount": 0
}
```

Exemple 11 : Lancer des instances ponctuelles à l'aide d' capacity-optimized-prioritized une stratégie d'allocation

L'exemple suivant spécifie les paramètres requis dans une EC2 flotte de type instantané : un modèle de lancement, une capacité cible, une option d'achat par défaut et des remplacements de modèles de lancement. Le modèle de lancement est identifié par son nom de modèle de lancement et son numéro de version. Les 12 spécifications de lancement qui remplacent le modèle de lancement ont 4 types d'instance différents avec une priorité assigned, et 3 sous-réseaux différents, chacun dans une zone de disponibilité distincte. La capacité cible du parc est de 20 instances, et l'option d'achat par défaut est le spot, ce qui amène le parc à tenter de lancer 20 instances ponctuelles à partir de l'un des 12 pools de capacités ponctuelles sur la base de la stratégie d' capacity-optimized-prioritized allocation, qui met en œuvre les priorités au mieux, mais optimise d'abord la capacité.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 1.0
            },
            {
```

```
            "InstanceType":"c5.large",
            "SubnetId":"subnet-49e41922",
            "Priority": 1.0
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-fae8c380",
            "Priority": 2.0
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-e7188bab",
            "Priority": 2.0
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-49e41922",
            "Priority": 2.0
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-fae8c380",
            "Priority": 3.0
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-e7188bab",
            "Priority": 3.0
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-49e41922",
            "Priority": 3.0
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-fae8c380",
            "Priority": 4.0
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-e7188bab",
            "Priority": 4.0
         },
```

```
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 4.0
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemple 12 : Spécifier un paramètre de Systems Manager au lieu d'un AMI ID

L'exemple suivant utilise un modèle de lancement pour spécifier la configuration des instances de la flotte. Dans cet exemple`ImageId`, au lieu de spécifier un AMI identifiant, le AMI est référencé par un paramètre System Manager. Au lancement de l'instance, le paramètre Systems Manager devient un AMI ID.

Dans cet exemple, le paramètre Systems Manager est spécifié dans un format valide :`resolve:ssm:golden-ami`. Il existe d'autres formats valides pour le paramètre Systems Manager. Pour de plus amples informations, veuillez consulter Utiliser un paramètre Systems Manager au lieu d'un AMI ID.

> **Note**
>
> Le type de flotte doit être `instant`. Les autres types de flotte ne permettent pas de spécifier un paramètre System Manager au lieu d'un AMI ID.

```
{
    "LaunchTemplateData": {
        "ImageId": "resolve:ssm:golden-ami",
        "InstanceType": "m5.4xlarge",
        "TagSpecifications": [{
            "ResourceType": "instance",
            "Tags": [{
                "Key": "Name",
```

```
                "Value": "webserver"
            }]
        }]
    }
}
```

Fixez une limite de dépenses pour votre EC2 flotte ou votre flotte ponctuelle

Vous pouvez fixer une limite au montant que vous êtes prêt à dépenser par heure pour votre EC2 flotte ou votre flotte ponctuelle. Lorsque votre limite de dépenses est atteinte, la flotte arrête de lancer des instances, même si la capacité cible n'est pas atteinte.

Il existe des limites de dépenses distinctes pour les instances à la demande et les instances ponctuelles.

Pour configurer une limite de dépenses pour les instances à la demande et les instances ponctuelles de votre EC2 flotte

Utilisez la commande create-fleet (AWS CLI) et les paramètres suivants :

- Pour les instances à la demande : dans la `OnDemandOptions` structure, spécifiez votre limite de dépenses dans le `MaxTotalPrice` champ.
- Pour les instances ponctuelles : dans la `SpotOptions` structure, spécifiez votre limite de dépenses dans le `MaxTotalPrice` champ.

Pour configurer une limite de dépenses pour les instances à la demande et les instances ponctuelles de votre parc d'instances ponctuelles

Vous pouvez utiliser la EC2 console Amazon ou le AWS CLI pour configurer votre limite de dépenses.

(Console) Lorsque vous créez le parc Spot, cochez la case Définir le coût maximum pour les instances Spot, puis entrez une valeur pour Définir votre coût maximum (par heure). Pour plus d'informations, reportez-vous à l'étape 6.e. inCréation d'une demande de parc d'instances Spot à l'aide des paramètres définis (console).

(AWS CLI) Utilisez la request-spot-fleetcommande et les paramètres suivants :

- Pour les instances à la demande : Spécifiez votre limite de dépenses dans le `OnDemandMaxTotalPrice` champ.

- Pour les instances ponctuelles : Spécifiez votre limite de dépenses dans le `SpotMaxTotalPrice` champ.

Exemples

Les exemples suivants montrent deux manières de le faire. Dans le premier exemple, le parc arrête de lancer des instances à la demande lorsqu'il a atteint la capacité cible définie pour les instances à la demande (`OnDemandTargetCapacity`). Dans le deuxième exemple, le parc arrête de lancer des instances à la demande lorsqu'il a atteint le montant maximum que vous êtes prêt à payer par heure pour les instances à la demande (`MaxTotalPrice`).

Exemple : arrêter de lancer des instances à la demande lorsque la capacité cible est atteinte

Prenons l'exemple d'une demande pour `m4.large` Instances à la demande, avec :

- Prix à la demande : 0,10 USD par heure
- `OnDemandTargetCapacity` : 10
- `MaxTotalPrice` : 1,50 USD

La flotte lance 10 instances à la demande car le total de 1,00$ (10 instances x 0,10$) ne dépasse pas le montant `MaxTotalPrice` de 1,50 dollar pour les instances à la demande.

Exemple : arrêter de lancer des instances à la demande lorsque le prix total maximum est atteint

Prenons l'exemple d'une demande pour `m4.large` Instances à la demande, avec :

- Prix à la demande : 0,10 USD par heure
- `OnDemandTargetCapacity` : 10
- `MaxTotalPrice` : 0,80 USD

Si le parc utilise la capacité cible à la demande (10 instances à la demande), le coût total par heure serait de 1,00$. Ce montant est supérieur à celui (0,80 USD) spécifié pour `MaxTotalPrice` pour Instances à la demande. Pour éviter de dépenser plus que ce que vous êtes prêt à payer, la flotte ne lance que 8 instances à la demande (en deçà de la capacité cible), car le lancement d'un plus grand nombre d'instances dépasserait celui des instances à la `MaxTotalPrice` demande.

Instances de performance à capacité extensible

Si vous lancez vos instances Spot à l'aide d'un type d'instance à performances évolutives, et si vous prévoyez d'utiliser vos instances Spot à performances évolutives immédiatement et pendant une courte durée, sans aucune période d'inactivité pour accumuler des CPU crédits, nous vous recommandons de les lancer en mode Standard pour éviter de payer des coûts plus élevés. Si vous lancez des instances Spot aux performances exceptionnelles en mode illimité et que vous les explosez CPU immédiatement, vous dépenserez des crédits excédentaires pour le bursting. Si vous utilisez l'instance pendant une courte période, l'instance n'a pas le temps d'accumuler des CPU crédits pour rembourser les crédits excédentaires, et les crédits excédentaires vous sont facturés lorsque vous mettez fin à l'instance.

Le mode illimité convient aux instances Spot aux performances élevées uniquement si l'instance fonctionne suffisamment longtemps pour accumuler des CPU crédits en cas d'éclatement. Sinon, payer des crédits excédentaires rend les instances Spot de performance à capacité extensible plus coûteuses que les autres instances. Pour plus d'informations, consultez Quand utiliser le mode illimité plutôt que le mode fixe CPU.

Les crédits de lancement visent à optimiser la productivité du lancement initial des instances T2 en leur fournissant suffisamment de ressources de calcul pour pouvoir configurer l'instance. Il est interdit de procéder à des lancements répétés d'instances T2 pour bénéficier de nouveaux crédits de lancement. Si vous avez besoin d'une instance prolongéeCPU, vous pouvez gagner des crédits (en restant inactifs pendant un certain temps), utiliser le mode illimité pour les instances ponctuelles T2 ou utiliser un type d'instance dédiéeCPU.

Spécifiez les attributs pour la sélection du type d'instance pour EC2 Fleet ou Spot Fleet

Lorsque vous créez un EC2 parc ou un parc ponctuel, vous devez spécifier un ou plusieurs types d'instances pour configurer les instances à la demande et les instances ponctuelles du parc. Au lieu de spécifier manuellement les types d'instances, vous pouvez spécifier les attributs qu'une instance doit avoir, et Amazon EC2 identifiera tous les types d'instances avec ces attributs. C'est ce qu'on appelle la sélection de type d'instance basée sur des attributs. Par exemple, vous pouvez spécifier le nombre minimum et maximum d'instances vCPUs requises pour vos instances, et le parc lancera les instances en utilisant tous les types d'instances disponibles qui répondent à ces CPU exigences.

La sélection de type d'instance basée sur des attributs est idéale pour les charges de travail et les cadres qui peuvent être flexibles quant aux types d'instances qu'ils utilisent, par exemple lors de

l'exécution de conteneurs ou de flottes web, du traitement de big data et de la mise en œuvre d'outils de CI/CD (intégration et déploiement continus).

Avantages

La sélection de type d'instance basée sur des attributs présente les avantages suivants :

- Utilisez facilement les bons types d'instances : compte tenu du grand nombre de types d'instances disponibles, la recherche des types d'instances adaptés à votre charge de travail peut prendre beaucoup de temps. Lorsque vous spécifiez des attributs d'instance, les types d'instance auront automatiquement les attributs requis pour votre charge de travail.
- Configuration simplifiée — Pour spécifier manuellement plusieurs types d'instances pour un parc, vous devez créer un modèle de lancement distinct pour chaque type d'instance. Toutefois, avec la sélection de type d'instance basée sur des attributs, pour fournir plusieurs types d'instance, il suffit de spécifier les attributs d'instance dans le modèle de lancement ou dans un remplacement de modèle de lancement.
- Utilisation automatique de nouveaux types d'instances : lorsque vous spécifiez des attributs d'instance plutôt que des types d'instances, votre parc peut utiliser des types d'instances de nouvelle génération au fur et à mesure de leur publication, afin de « pérenniser » la configuration du parc.
- Flexibilité des types d'instances : lorsque vous spécifiez des attributs d'instance plutôt que des types d'instances, le parc peut choisir parmi un large éventail de types d'instances pour lancer des instances Spot, conformément aux meilleures pratiques Spot en matière de flexibilité des types d'instances.

Rubriques

Fonctionnement de la sélection de type d'instance basée sur des attributs

Pour utiliser la sélection de type d'instance basée sur des attributs dans la configuration de votre flotte, vous remplacez la liste des types d'instance par une liste d'attributs d'instance dont vos instances ont besoin. EC2Fleet ou Spot Fleet lancera des instances sur tous les types d'instances disponibles possédant les attributs d'instance spécifiés.

Rubriques

Types d'attributs d'instance

Il existe plusieurs attributs d'instance que vous pouvez spécifier pour exprimer vos besoins en matière de calcul, tels que :

- v CPU count — Le nombre minimum et maximum de vCPUs par instance.
- Mémoire : mémoire minimale et maximale GiBs par instance.
- Stockage local : s'il faut utiliser EBS ou instancier des volumes de stockage pour le stockage local.
- Performances éclatantes : s'il faut utiliser la famille d'instances T, y compris les types T4g, T3a, T3 et T2.

Pour une description de chaque attribut et des valeurs par défaut, consultez InstanceRequirementsle Amazon EC2 API Reference.

Où configurer la sélection de type d'instance basée sur des attributs

Selon que vous utilisez la console ou le AWS CLI, vous pouvez spécifier les attributs d'instance pour la sélection du type d'instance basée sur les attributs comme suit :

Dans la console, vous pouvez spécifier les attributs d'instance dans les composants de configuration de flotte suivants :

- Dans un modèle de lancement, puis référencez le modèle de lancement dans la demande de flotte
- (Spot Fleet uniquement) Dans la demande de flotte

Dans le AWS CLI, vous pouvez spécifier les attributs d'instance dans l'un ou l'ensemble des composants de configuration de flotte suivants :

- Dans un modèle de lancement, puis référencez le modèle de lancement dans la demande de flotte
- Dans un remplacement de modèle de lancement

  Si vous souhaitez une combinaison d'instances utilisant différentes optionsAMIs, vous pouvez spécifier des attributs d'instance dans le cadre de plusieurs remplacements de modèles de lancement. Par exemple, différents types d'instance peuvent utiliser des processeurs x86 et Arm.
- (Spot Fleet uniquement) Dans une spécification de lancement

Comment EC2 Fleet ou Spot Fleet utilise la sélection du type d'instance basée sur les attributs lors du provisionnement d'une flotte

EC2Fleet ou Spot Fleet approvisionne une flotte de la manière suivante :

- Il identifie les types d'instances dotés des attributs spécifiés.
- Il utilise la protection des prix pour déterminer les types d'instances à exclure.
- Il détermine les pools de capacité à partir desquels il envisagera de lancer les instances en fonction des AWS régions ou des zones de disponibilité ayant les types d'instances correspondants.
- Il applique la stratégie d'allocation spécifiée pour déterminer à partir de quels pools de capacités lancer les instances.

  Notez que la sélection du type d'instance basée sur les attributs ne permet pas de sélectionner les pools de capacités à partir desquels approvisionner le parc ; c'est le travail des stratégies d'allocation.

  Si vous spécifiez une stratégie d'allocation, la flotte lancera des instances conformément à la stratégie d'allocation spécifiée.

  - Pour les instances Spot, la sélection du type d'instance basée sur les attributs prend en charge les stratégies d'optimisation de la capacité en termes de prix, d'optimisation de la capacité et d'allocation du prix le plus bas. Notez que nous ne recommandons pas la stratégie d'allocation ponctuelle au prix le plus bas, car c'est elle qui présente le risque d'interruption le plus élevé pour vos instances ponctuelles.
  - Pour les instances à la demande, la sélection du type d'instance basée sur les attributs prend en charge la stratégie d'allocation du prix le plus bas.

- S'il n'y a pas de capacité pour les types d'instance avec des attributs d'instance spécifiés, aucune instance ne peut être lancée et la flotte renvoie une erreur.

Protection des prix

La protection des prix est une fonctionnalité qui empêche votre EC2 flotte ou votre flotte ponctuelle d'utiliser des types d'instances que vous jugeriez trop coûteux, même s'ils correspondent aux attributs que vous avez spécifiés. Pour utiliser la protection des prix, vous devez définir un seuil de prix. Ensuite, lorsqu'Amazon EC2 sélectionne des types d'instances avec vos attributs, il exclut les types d'instances dont le prix est supérieur à votre seuil.

Amazon EC2 calcule le seuil de prix de la manière suivante :

- Amazon identifie EC2 d'abord le type d'instance le moins cher parmi ceux qui correspondent à vos attributs.
- Amazon prend EC2 ensuite la valeur (exprimée en pourcentage) que vous avez spécifiée pour le paramètre de protection des prix et la multiplie par le prix du type d'instance identifié. Le résultat est le prix qui est utilisé comme seuil de prix.

Il existe des seuils de prix distincts pour les instances à la demande et les instances ponctuelles.

Lorsque vous créez un parc avec sélection du type d'instance basée sur les attributs, la protection des prix est activée par défaut. Vous pouvez conserver les valeurs par défaut ou définir les vôtres.

Vous pouvez également désactiver la protection des prix. Pour n'indiquer aucun seuil de protection des prix, spécifiez une valeur en pourcentage élevée, telle que`999999`.

Rubriques

- Comment est identifié le type d'instance le moins cher
- Protection du prix des instances à la demande
- Protection des prix des instances Spot
- Spécifiez le seuil de protection des prix

Comment est identifié le type d'instance le moins cher

Amazon EC2 détermine le prix sur lequel baser le seuil de prix en identifiant le type d'instance dont le prix est le plus bas parmi celles qui correspondent aux attributs que vous avez spécifiés. Pour ce faire, il procède de la manière suivante :

- Il examine d'abord les types d'instances C, M ou R de la génération actuelle qui correspondent à vos attributs. S'il trouve des correspondances, il identifie le type d'instance le moins cher.
- S'il n'y a pas de correspondance, il examine ensuite tous les types d'instances de la génération actuelle qui correspondent à vos attributs. S'il trouve des correspondances, il identifie le type d'instance le moins cher.
- S'il n'y a pas de correspondance, il examine ensuite tous les types d'instances de la génération précédente qui correspondent à vos attributs et identifie le type d'instance le moins cher.

Protection du prix des instances à la demande

Le seuil de protection des prix pour les types d'instances à la demande est calculé sous la forme d'un pourcentage supérieur au type d'instance à la demande le moins cher identifié (`OnDemandMaxPricePercentageOverLowestPrice`). Vous spécifiez le pourcentage supérieur que vous êtes prêt à payer. Si vous ne spécifiez pas ce paramètre, la valeur par défaut de `20` est utilisée pour calculer un seuil de protection des prix supérieur de 20 % au prix identifié.

Par exemple, si le prix de l'instance On-Demand identifié est`0.4271`, et que vous le spécifiez`25`, le seuil de prix est supérieur de 25 % à`0.4271`. Il est calculé comme suit :`0.4271 * 1.25 = 0.533875`. Le prix calculé est le montant maximum que vous êtes prêt à payer pour les instances à la demande et, dans cet exemple, Amazon EC2 exclura tous les types d'instances à la demande dont le coût est supérieur à`0.533875`.

Protection des prix des instances Spot

Par défaut, Amazon EC2 appliquera automatiquement une protection tarifaire optimale des instances Spot afin de sélectionner de manière cohérente un large éventail de types d'instances. Vous pouvez également définir vous-même la protection des prix manuellement. Toutefois, le fait de laisser Amazon EC2 s'en occuper à votre place peut améliorer les chances que votre capacité Spot soit atteinte.

Vous pouvez définir manuellement la protection des prix à l'aide de l'une des options suivantes. Si vous définissez manuellement la protection des prix, nous vous recommandons d'utiliser la première option.

- Pourcentage du type d'instance à la demande le moins cher identifié [`MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`]

  Par exemple, si le prix du type d'instance On-Demand identifié est`0.4271`, et que vous le spécifiez`60`, le seuil de prix est de 60 %`0.4271`. Il est calculé comme suit :`0.4271 * 0.60 = 0.25626`. Le prix calculé est le montant maximum que vous êtes prêt à payer pour les instances Spot et, dans cet exemple, Amazon EC2 exclura tous les types d'instances Spot dont le coût est supérieur à`0.25626`.

- Un pourcentage supérieur au type d'instance Spot le moins cher identifié [`SpotMaxPricePercentageOverLowestPrice`]

  Par exemple, si le prix du type d'instance Spot identifié est`0.1808`, et que vous le spécifiez`25`, le seuil de prix est supérieur de 25 % à`0.1808`. Il est calculé comme suit :`0.1808 * 1.25 = 0.226`. Le prix calculé est le montant maximum que vous êtes prêt à payer pour les instances Spot et, dans cet exemple, Amazon EC2 exclura tous les types d'instances Spot dont le coût est supérieur à`0.266`. Nous vous déconseillons d'utiliser ce paramètre car les prix au comptant peuvent fluctuer et, par conséquent, votre seuil de protection contre les prix peut également fluctuer.

Spécifiez le seuil de protection des prix

Pour définir le seuil de protection des prix à l'aide du AWS CLI

Lors de la création d'un EC2 parc ou d'un parc ponctuel à l'aide du AWS CLI, configurez le parc pour la sélection du type d'instance basé sur les attributs, puis procédez comme suit :

- Pour spécifier le seuil de protection des prix des instances à la demande, dans le fichier de JSON configuration, dans la `InstanceRequirements` structure, pour`OnDemandMaxPricePercentageOverLowestPrice`, entrez le seuil de protection des prix sous forme de pourcentage.
- Pour spécifier le seuil de protection des prix des instances Spot, dans le fichier de JSON configuration, dans la `InstanceRequirements` structure, spécifiez l'un des paramètres suivants :
  - Pour`MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`, entrez le seuil de protection des prix sous forme de pourcentage.
  - Pour`SpotMaxPricePercentageOverLowestPrice`, entrez le seuil de protection des prix sous forme de pourcentage.

Pour plus d'informations, consultez Création d'une EC2 flotte avec sélection du type d'instance basée sur les attributs ou Créer un parc d'instances Spot avec une sélection de type d'instance basée sur des attributs.

(Spot Fleet uniquement) Pour spécifier le seuil de protection des prix à l'aide de la console

Lors de la création d'un parc de spots dans la console, configurez le parc pour la sélection du type d'instance basé sur les attributs, puis procédez comme suit :

- Pour spécifier le seuil de protection des prix des instances à la demande, sous Attribut d'instance supplémentaire, choisissez Protection des prix à la demande, choisissez Ajouter un attribut, puis entrez le seuil de protection des prix sous forme de pourcentage.
- Pour spécifier le seuil de protection des prix des instances Spot, attribut d'instance supplémentaire, choisissez Protection des prix ponctuels, choisissez Ajouter un attribut, choisissez une valeur de base sur laquelle baser votre prix, puis entrez le seuil de protection des prix sous forme de pourcentage.

> **Note**
>
> Lors de la création du parc, si vous définissez `TargetCapacityUnitType` `vcpu` ou`memory-mib`, le seuil de protection des prix est appliqué en fonction du prix par v CPU ou par mémoire plutôt que du prix par instance.

Considérations

- Vous pouvez spécifier des types d'instances ou des attributs d'instance dans un EC2 parc ou un parc ponctuel, mais pas les deux en même temps.

  Lorsque vous utilisez leCLI, les remplacements du modèle de lancement remplaceront le modèle de lancement. Par exemple, si le modèle de lancement contient un type d'instance et que le remplacement du modèle de lancement contient des attributs d'instance, les instances identifiées par les attributs d'instance remplaceront le type d'instance dans le modèle de lancement.
- Lorsque vous utilisez leCLI, lorsque vous spécifiez des attributs d'instance en tant que remplacements, vous ne pouvez pas également spécifier de poids ou de priorités.
- Vous pouvez spécifier un maximum de quatre structures `InstanceRequirements` dans une configuration de demande.

Création d'une EC2 flotte avec sélection du type d'instance basée sur les attributs

Vous pouvez configurer un EC2 parc pour utiliser la sélection du type d'instance basée sur les attributs à l'aide du. AWS CLI

Pour créer une EC2 flotte avec une sélection de type d'instance basée sur les attributs ()AWS CLI

Utilisez la commande create-fleet (AWS CLI) pour créer une EC2 flotte. Spécifiez la configuration du parc dans un JSON fichier.

```
aws ec2 create-fleet \
    --region us-east-1 \
    --cli-input-json file://file_name.json
```

Exemple de fichier *file_name*.json

L'exemple suivant contient les paramètres qui configurent une EC2 flotte pour utiliser la sélection du type d'instance basée sur les attributs, et est suivi d'une explication textuelle.

```
{
 "SpotOptions": {
  "AllocationStrategy": "price-capacity-optimized"
 },
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }],
 "TargetCapacitySpecification": {
  "TotalTargetCapacity": 20,
  "DefaultTargetCapacityType": "spot"
```

```
  },
  "Type": "instant"
}
```

Les attributs de sélection du type d'instance basé sur des attributs sont spécifiés dans la structure `InstanceRequirements`. Dans cet exemple, deux attributs sont spécifiés :

- `VCpuCount`— Un minimum de 2 vCPUs est spécifié. Comme aucun maximum n'est spécifié, il n'y a pas de limite maximale.
- `MemoryMiB` : au moins 4 Mio de mémoire sont spécifiés. Comme aucun maximum n'est spécifié, il n'y a pas de limite maximale.

Tous les types d'instance dotés de 2 ou plus vCPUs et de 4 Mo de mémoire ou plus seront identifiés. Cependant, la protection des prix et la stratégie d'allocation peuvent exclure certains types d'instances lorsque EC2Fleet approvisionne la flotte.

Pour obtenir une liste et une description de tous les attributs possibles que vous pouvez spécifier, consultez InstanceRequirementsla EC2APIréférence Amazon.

> **Note**
>
> Lorsque `InstanceRequirements` est inclus dans la configuration de la flotte, `InstanceType` et `WeightedCapacity` doivent être exclus. Ils ne peuvent pas déterminer la configuration de la flotte en même temps que les attributs d'instance.

JSONIl contient également la configuration de flotte suivante :

- `"AllocationStrategy": "price-capacity-optimized"` : la stratégie d'allocation des instances Spot de la flotte.
- `"LaunchTemplateName": "my-launch-template", "Version": "1"` : le modèle de lancement contient certaines informations de configuration d'instance, mais si des types d'instance sont spécifiés, ils seront remplacés par les attributs spécifiés dans `InstanceRequirements`.
- `"TotalTargetCapacity": 20` : la capacité cible est de 20 instances Spot.
- `"DefaultTargetCapacityType": "spot"` : la capacité par défaut est celle des instances Spot.
- `"Type": "instant"` : le type de demande pour la flotte est `instant`.

Créer un parc d'instances Spot avec une sélection de type d'instance basée sur des attributs

Vous pouvez configurer un parc pour utiliser la sélection du type d'instance basée sur les attributs à l'aide de EC2 la console Amazon ou du. AWS CLI

Rubriques

- Créer un parc d'instances Spot à l'aide de la console
- Créez un parc d'instances Spot à l'aide de AWS CLI

Créer un parc d'instances Spot à l'aide de la console

Pour configurer un parc d'instances Spot pour la sélection de type d'instance basée sur des attributs (console)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Spot Requests (Demandes Spot) et sélectionnez Request Spot Instances (Demander des instances Spot).
3. Suivez les étapes permettant de créer un parc d'instances Spot. Pour de plus amples informations, veuillez consulter Création d'une demande de parc d'instances Spot à l'aide des paramètres définis (console).

   Lors de la création du parc d'instances Spot, configurez la flotte pour la sélection du type d'instance basée sur des attributs comme suit :

   a. Pour Instance type requirements (Exigences de type d'instance), choisissez Specify instance attributes that match your compute requirements (Spécifiez les attributs d'instance qui correspondent à vos exigences de calcul).

   b. Pour vCPUs, entrez le nombre minimum et maximum souhaités devCPUs. Pour ne spécifier aucune limite, sélectionnez No minimum (Pas de minimum), No maximum (Pas de maximum), ou les deux.

   c. Pour Memory (GiB) (Mémoire (Gio)), saisissez la quantité minimale et maximale de mémoire souhaitée. Pour ne spécifier aucune limite, sélectionnez No minimum (Pas de minimum), No maximum (Pas de maximum), ou les deux.

   d. (Facultatif) Pour Additional instance attributes (Attributs d'instance supplémentaires), vous pouvez éventuellement spécifier un ou plusieurs attributs pour exprimer vos exigences de

calcul plus en détail. Chaque attribut supplémentaire ajoute des contraintes supplémentaires à votre demande.

e. (Facultatif) Pour afficher les types d'instance avec vos attributs spécifiés, développez Preview matching instance types (Aperçu des types d'instance correspondants).

Créez un parc d'instances Spot à l'aide de AWS CLI

Pour configurer un parc d'instances Spot pour la sélection de type d'instance basée sur des attributs (AWS CLI)

Utilisez la commande request-spot-fleet(AWS CLI) pour créer un parc de spots. Spécifiez la configuration du parc dans un JSON fichier.

```
aws ec2 request-spot-fleet \
    --region us-east-1 \
    --spot-fleet-request-config file://file_name.json
```

Exemple de fichier *file_name*.json

L'exemple suivant contient les paramètres qui configurent un parc d'instances Spot afin qu'il utilise la sélection de type d'instance basée sur des attributs et est suivi d'une explication textuelle.

```
{
 "AllocationStrategy": "priceCapacityOptimized",
 "TargetCapacity": 20,
 "Type": "request",
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
```

```
 }]
}
```

Les attributs de sélection du type d'instance basé sur des attributs sont spécifiés dans la structure `InstanceRequirements`. Dans cet exemple, deux attributs sont spécifiés :

- `VCpuCount`— Un minimum de 2 vCPUs est spécifié. Comme aucun maximum n'est spécifié, il n'y a pas de limite maximale.
- `MemoryMiB` : au moins 4 Mio de mémoire sont spécifiés. Comme aucun maximum n'est spécifié, il n'y a pas de limite maximale.

Tous les types d'instance dotés de 2 ou plus vCPUs et de 4 Mo de mémoire ou plus seront identifiés. Toutefois, la protection des prix et la stratégie d'allocation peuvent exclure certains types d'instances lorsque le parc d'instances Spot alloue la flotte.

Pour obtenir une liste et une description de tous les attributs possibles que vous pouvez spécifier, consultez InstanceRequirementsla EC2APIréférence Amazon.

> **Note**
>
> Lorsque `InstanceRequirements` est inclus dans la configuration de la flotte, `InstanceType` et `WeightedCapacity` doivent être exclus. Ils ne peuvent pas déterminer la configuration de la flotte en même temps que les attributs d'instance.

JSONIl contient également la configuration de flotte suivante :

- `"AllocationStrategy": "priceCapacityOptimized"` : la stratégie d'allocation des instances Spot de la flotte.
- `"LaunchTemplateName": "my-launch-template", "Version": "1"` : le modèle de lancement contient certaines informations de configuration d'instance, mais si des types d'instance sont spécifiés, ils seront remplacés par les attributs spécifiés dans `InstanceRequirements`.
- `"TargetCapacity": 20` : la capacité cible est de 20 instances Spot.
- `"Type": "request"` : le type de demande pour la flotte est `request`.

Exemples de configurations de EC2 flotte valides et non valides

Si vous utilisez le AWS CLI pour créer une EC2 flotte, vous devez vous assurer que la configuration de votre flotte est valide. Les exemples suivants illustrent les configurations valides et non valides.

Les configurations sont considérées comme non valides lorsqu'elles contiennent les éléments suivants :

- Une seule structure `Overrides` avec `InstanceRequirements` et `InstanceType`
- Deux structures `Overrides`, l'une avec `InstanceRequirements` et l'autre avec `InstanceType`
- Deux structures `InstanceRequirements` avec des valeurs d'attributs qui se chevauchent au sein du même `LaunchTemplateSpecification`

Exemples de configuration

- Configuration valide : modèle de lancement unique avec remplacements
- Configuration valide : modèle de lancement unique avec plusieurs InstanceRequirements
- Configuration valide : deux modèles de lancement, chacun avec des remplacements
- Configuration valide : uniquement InstanceRequirements est spécifié, les valeurs d'attribut ne se chevauchent pas
- Configuration non valide : les Overrides contiennent InstanceRequirements et InstanceType
- Configuration non valide : deux Overrides contiennent InstanceRequirements et InstanceType
- Configuration non valide : chevauchement des valeurs d'attribut

Configuration valide : modèle de lancement unique avec remplacements

La configuration suivante est valide. Elle contient un modèle de lancement et une structure `Overrides` contenant une structure `InstanceRequirements`. Vous trouverez ci-dessous une explication textuelle de l'exemple de configuration.

```
{
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
```

```
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
                            "Max": 10000
                        },
                        "RequireHibernateSupport": true
                    }
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5000,
        "DefaultTargetCapacityType": "spot",
        "TargetCapacityUnitType": "vcpu"
        }
    }
}
```

`InstanceRequirements`

Pour utiliser la sélection d'instance basée sur les attributs, vous devez inclure la structure `InstanceRequirements` dans votre configuration de flotte et spécifier les attributs souhaités pour les instances de la flotte.

Dans l'exemple précédent, les attributs d'instance suivants sont spécifiés :

- `VCpuCount`— Les types d'instances doivent en avoir un minimum de 2 et un maximum de 8vCPUs.
- `MemoryMiB` : les types d'instance doivent disposer d'un maximum de 10 240 Mio de mémoire. Un minimum de 0 indique qu'il n'y a pas de limite minimale.
- `MemoryGiBPerVCpu`— Les types d'instance doivent disposer d'un maximum de 10 000 GiB de mémoire par v. CPU Le paramètre `Min` est facultatif. En l'omettant, vous n'indiquez aucune limite minimale.

`TargetCapacityUnitType`

Le paramètre `TargetCapacityUnitType` spécifie l'unité de la capacité cible. Dans l'exemple, la capacité cible est `5000` et le type d'unité de capacité cible est`vcpu`, ce qui définit ensemble une capacité cible souhaitée de 5 000vCPUs. EC2Fleet lancera suffisamment d'instances pour que le nombre total d'instances vCPUs de la flotte soit de 5 000vCPUs.

Configuration valide : modèle de lancement unique avec plusieurs InstanceRequirements

La configuration suivante est valide. Elle contient un modèle de lancement et une structure `0verrides` contenant deux structures `InstanceRequirements`. Les attributs spécifiés dans `InstanceRequirements` sont valides car les valeurs ne se chevauchent pas : la première `InstanceRequirements` structure indique une `VCpuCount` valeur comprise entre 0 et 2vCPUs, tandis que la seconde `InstanceRequirements` indique 4 à 8. vCPUs

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
```

```
                    }
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configuration valide : deux modèles de lancement, chacun avec des remplacements

La configuration suivante est valide. Elle contient deux modèles de lancement, chacun contenant une structure `Overrides` contenant une structure `InstanceRequirements`. Cette configuration est utile pour la prise en charge des architectures `arm` et `x86` au sein de la même flotte.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
```

```
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configuration valide : uniquement **`InstanceRequirements`** est spécifié, les valeurs d'attribut ne se chevauchent pas

La configuration suivante est valide. Elle contient deux structures `LaunchTemplateSpecification`, chacune avec un modèle de lancement et une structure `Overrides` contenant une structure `InstanceRequirements`. Les attributs spécifiés dans `InstanceRequirements` sont valides car les valeurs ne se chevauchent pas : la première `InstanceRequirements` structure indique une `VCpuCount` valeur comprise entre 0 et 2vCPUs, tandis que la seconde `InstanceRequirements` indique 4 à 8. vCPUs

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
```

```
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configuration non valide : les **`Overrides`** contiennent **`InstanceRequirements`** et **`InstanceType`**

La configuration suivante n'est pas valide. La structure `Overrides` contient à la fois `InstanceRequirements` et `InstanceType`. Pour les `Overrides`, vous pouvez spécifier `InstanceRequirements` ou `InstanceType`, mais pas les deux.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configuration non valide : deux **`Overrides`** contiennent **`InstanceRequirements`** et **`InstanceType`**

La configuration suivante n'est pas valide. Les structures `Overrides` contiennent à la fois `InstanceRequirements` et `InstanceType`. Vous pouvez spécifier `InstanceRequirements` ou `InstanceType`, mais pas les deux, même s'ils se trouvent dans différentes structures `Overrides`.

```
{
        "LaunchTemplateConfigs": [
            {
```

```
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configuration non valide : chevauchement des valeurs d'attribut

La configuration suivante n'est pas valide. Les deux structures `InstanceRequirements` contiennent chacune `"VCpuCount": {"Min": 0, "Max": 2}`. Les valeurs de ces attributs se chevauchent, ce qui entraîne des groupes de capacités en double.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
                    {
                      "InstanceRequirements": {
                          "VCpuCount": {
                              "Min": 0,
                              "Max": 2
                          },
                          "MemoryMiB": {
                              "Min": 0
                          }
                      }
                  }
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Exemples de configurations de parc Spot valides et non valides

Si vous utilisez le AWS CLI pour créer une flotte ponctuelle, vous devez vous assurer que la configuration de votre flotte est valide. Les exemples suivants illustrent les configurations valides et non valides.

Les configurations sont considérées comme non valides lorsqu'elles contiennent les éléments suivants :

- Une seule structure `Overrides` avec `InstanceRequirements` et `InstanceType`
- Deux structures `Overrides`, l'une avec `InstanceRequirements` et l'autre avec `InstanceType`
- Deux structures `InstanceRequirements` avec des valeurs d'attributs qui se chevauchent au sein du même `LaunchTemplateSpecification`

Exemples de configuration

- Configuration valide : modèle de lancement unique avec remplacements
- Configuration valide : modèle de lancement unique avec plusieurs InstanceRequirements
- Configuration valide : deux modèles de lancement, chacun avec des remplacements
- Configuration valide : uniquement InstanceRequirements est spécifié, les valeurs d'attribut ne se chevauchent pas
- Configuration non valide : les Overrides contiennent InstanceRequirements et InstanceType
- Configuration non valide : deux Overrides contiennent InstanceRequirements et InstanceType
- Configuration non valide : chevauchement des valeurs d'attribut

Configuration valide : modèle de lancement unique avec remplacements

La configuration suivante est valide. Elle contient un modèle de lancement et une structure `Overrides` contenant une structure `InstanceRequirements`. Vous trouverez ci-dessous une explication textuelle de l'exemple de configuration.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
```

```
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
                            "Max": 10000
                        },
                        "RequireHibernateSupport": true
                    }
                }
            ]
        }
    ],
        "TargetCapacity": 5000,
            "OnDemandTargetCapacity": 0,
            "TargetCapacityUnitType": "vcpu"
    }
}
```

`InstanceRequirements`

Pour utiliser la sélection d'instance basée sur les attributs, vous devez inclure la structure `InstanceRequirements` dans votre configuration de flotte et spécifier les attributs souhaités pour les instances de la flotte.

Dans l'exemple précédent, les attributs d'instance suivants sont spécifiés :

- `VCpuCount`— Les types d'instances doivent en avoir un minimum de 2 et un maximum de 8vCPUs.
- `MemoryMiB` : les types d'instance doivent disposer d'un maximum de 10 240 Mio de mémoire. Un minimum de 0 indique qu'il n'y a pas de limite minimale.

- `MemoryGiBPerVCpu`— Les types d'instance doivent disposer d'un maximum de 10 000 GiB de mémoire par v. CPU Le paramètre `Min` est facultatif. En l'omettant, vous n'indiquez aucune limite minimale.

`TargetCapacityUnitType`

Le paramètre `TargetCapacityUnitType` spécifie l'unité de la capacité cible. Dans l'exemple, la capacité cible est `5000` et le type d'unité de capacité cible est`vcpu`, ce qui définit ensemble une capacité cible souhaitée de 5 000vCPUs. Spot Fleet lancera suffisamment d'instances pour que le nombre total d'instances vCPUs de la flotte soit de 5 000vCPUs.

Configuration valide : modèle de lancement unique avec plusieurs InstanceRequirements

La configuration suivante est valide. Elle contient un modèle de lancement et une structure `0verrides` contenant deux structures `InstanceRequirements`. Les attributs spécifiés dans `InstanceRequirements` sont valides car les valeurs ne se chevauchent pas : la première `InstanceRequirements` structure indique une `VCpuCount` valeur comprise entre 0 et 2vCPUs, tandis que la seconde `InstanceRequirements` indique 4 à 8. vCPUs

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
```

```
                    }
                },
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configuration valide : deux modèles de lancement, chacun avec des remplacements

La configuration suivante est valide. Elle contient deux modèles de lancement, chacun contenant une structure `Overrides` contenant une structure `InstanceRequirements`. Cette configuration est utile pour la prise en charge des architectures `arm` et `x86` au sein de la même flotte.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
```

```
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configuration valide : uniquement **`InstanceRequirements`** est spécifié, les valeurs d'attribut ne se chevauchent pas

La configuration suivante est valide. Elle contient deux structures `LaunchTemplateSpecification`, chacune avec un modèle de lancement et une structure `Overrides` contenant une structure `InstanceRequirements`. Les attributs spécifiés dans `InstanceRequirements` sont valides car les valeurs ne se chevauchent pas : la première

`InstanceRequirements` structure indique une `VCpuCount` valeur comprise entre 0 et 2vCPUs, tandis que la seconde `InstanceRequirements` indique 4 à 8. vCPUs

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
```

```
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configuration non valide : les **`Overrides`** contiennent **`InstanceRequirements`** et **`InstanceType`**

La configuration suivante n'est pas valide. La structure `Overrides` contient à la fois `InstanceRequirements` et `InstanceType`. Pour les `Overrides`, vous pouvez spécifier `InstanceRequirements` ou `InstanceType`, mais pas les deux.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
```

```
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configuration non valide : deux **`Overrides`** contiennent **`InstanceRequirements`** et **`InstanceType`**

La configuration suivante n'est pas valide. Les structures `Overrides` contiennent à la fois `InstanceRequirements` et `InstanceType`. Vous pouvez spécifier `InstanceRequirements` ou `InstanceType`, mais pas les deux, même s'ils se trouvent dans différentes structures `Overrides`.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
```

```
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configuration non valide : chevauchement des valeurs d'attribut

La configuration suivante n'est pas valide. Les deux structures `InstanceRequirements` contiennent chacune `"VCpuCount": {"Min": 0, "Max": 2}`. Les valeurs de ces attributs se chevauchent, ce qui entraîne des groupes de capacités en double.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
```

```
                    },
                    "MemoryMiB": {
                        "Min": 0
                    }
                },
                {
                  "InstanceRequirements": {
                      "VCpuCount": {
                          "Min": 0,
                          "Max": 2
                      },
                      "MemoryMiB": {
                          "Min": 0
                      }
                  }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Aperçu des types d'instances avec des attributs spécifiés

Vous pouvez utiliser la AWS CLI commande get-instance-types-from-instance-requirements pour prévisualiser les types d'instances qui correspondent aux attributs que vous spécifiez. Cela est particulièrement utile pour déterminer les attributs à spécifier dans la configuration de votre demande sans lancer d'instance. Notez que la commande ne prend pas en compte la capacité disponible.

Pour prévisualiser une liste de types d'instance en spécifiant des attributs à l'aide de la AWS CLI

1. (Facultatif) Pour générer tous les attributs possibles pouvant être spécifiés, utilisez la commande get-instance-types-from-instance-requirements et le paramètre. `--generate-cli-skeleton` Vous pouvez éventuellement rediriger la sortie vers un fichier pour l'enregistrer à l'aide de `input > attributes.json`.

   ```
   aws ec2 get-instance-types-from-instance-requirements \
       --region us-east-1 \
   ```

```
    --generate-cli-skeleton input > attributes.json
```

Sortie attendue

```
{
    "DryRun": true,
    "ArchitectureTypes": [
        "i386"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 0,
            "Max": 0
        },
        "MemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "CpuManufacturers": [
            "intel"
        ],
        "MemoryGiBPerVCpu": {
            "Min": 0.0,
            "Max": 0.0
        },
        "ExcludedInstanceTypes": [
            ""
        ],
        "InstanceGenerations": [
            "current"
        ],
        "SpotMaxPricePercentageOverLowestPrice": 0,
        "OnDemandMaxPricePercentageOverLowestPrice": 0,
        "BareMetal": "included",
        "BurstablePerformance": "included",
        "RequireHibernateSupport": true,
        "NetworkInterfaceCount": {
            "Min": 0,
            "Max": 0
        },
```

```
        "LocalStorage": "included",
        "LocalStorageTypes": [
            "hdd"
        ],
        "TotalLocalStorageGB": {
            "Min": 0.0,
            "Max": 0.0
        },
        "BaselineEbsBandwidthMbps": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorTypes": [
            "gpu"
        ],
        "AcceleratorCount": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorManufacturers": [
            "nvidia"
        ],
        "AcceleratorNames": [
            "a100"
        ],
        "AcceleratorTotalMemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "NetworkBandwidthGbps": {
            "Min": 0.0,
            "Max": 0.0
        },
        "AllowedInstanceTypes": [
            ""
        ]
    },
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Créez un fichier JSON de configuration en utilisant le résultat de l'étape précédente et configurez-le comme suit :

> **Note**
>
> Vous devez fournir des valeurs pour `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` et `MemoryMiB`. Vous pouvez omettre les autres attributs. Lorsqu'ils sont omis, les valeurs par défaut sont utilisées.
> Pour une description de chaque attribut et de leurs valeurs par défaut, consultez get-instance-types-from-instance-requirements.

a. Pour `ArchitectureTypes`, spécifiez un ou plusieurs types d'architecture de processeur.

b. Pour `VirtualizationTypes`, spécifiez un ou plusieurs types de virtualisation.

c. Pour`VCpuCount`, spécifiez le nombre minimum et maximum devCPUs. Pour ne spécifier aucune limite minimale, pour `Min`, spécifiez `0`. Pour ne spécifier aucune limite maximale, omettez le paramètre `Max`.

d. Pour `MemoryMiB`, spécifiez la quantité minimale et maximale de mémoire en Mio. Pour ne spécifier aucune limite minimale, pour `Min`, spécifiez `0`. Pour ne spécifier aucune limite maximale, omettez le paramètre `Max`.

e. Vous pouvez éventuellement spécifier un ou plusieurs autres attributs pour limiter davantage la liste des types d'instance renvoyés.

3. Pour prévisualiser les types d'instances dotés des attributs que vous avez spécifiés dans le JSON fichier, utilisez la commande get-instance-types-from-instance-requirements et spécifiez le nom et le chemin d'accès à votre JSON fichier à l'aide du paramètre. `--cli-input-json` Vous pouvez éventuellement formater la sortie pour qu'elle apparaisse dans un format de tableau.

```
aws ec2 get-instance-types-from-instance-requirements \
    --cli-input-json file://attributes.json \
    --output table
```

Exemple *`attributes.json`* dans le fichier

Dans cet exemple, les attributs requis sont inclus dans le JSON fichier. Ils sont `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` et `MemoryMiB`. En outre, l'attribut facultatif `InstanceGenerations` est également inclus. Notez que pour `MemoryMiB`, la valeur `Max` peut être omise pour indiquer qu'aucune limite n'est applicable.

```
{
```

```
    "ArchitectureTypes": [
        "x86_64"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 4,
            "Max": 6
        },
        "MemoryMiB": {
            "Min": 2048
        },
        "InstanceGenerations": [
            "current"
        ]
    }
}
```

Exemple de sortie

```
-----------------------------------------
|GetInstanceTypesFromInstanceRequirements|
+---------------------------------------+
||             InstanceTypes            ||
|+-------------------------------------+|
||             InstanceType             ||
|+-------------------------------------+|
||  c4.xlarge                          ||
||  c5.xlarge                          ||
||  c5a.xlarge                         ||
||  c5ad.xlarge                        ||
||  c5d.xlarge                         ||
||  c5n.xlarge                         ||
||  d2.xlarge                          ||
...
```

4. Après avoir identifié les types d'instance qui répondent à vos besoins, prenez note des attributs d'instance que vous avez utilisés afin que vous puissiez les utiliser lors de la configuration de votre demande de flotte.

Utilisez la pondération des instances pour gérer les coûts et les performances de votre EC2 flotte ou de votre flotte ponctuelle

Avec la pondération des instances, vous attribuez une pondération à chaque type d'instance de votre EC2 flotte ou de votre flotte ponctuelle pour représenter leur capacité de calcul et leurs performances les unes par rapport aux autres. Sur la base des pondérations, le parc peut utiliser n'importe quelle combinaison des types d'instances spécifiés, à condition qu'il puisse atteindre la capacité cible souhaitée. Cela peut vous aider à gérer les coûts et les performances de votre flotte.

Le poids représente les unités de capacité qu'un type d'instance contribue à la capacité cible totale.

Exemple : utiliser la pondération des instances pour la gestion des performances

Supposons que votre parc comporte deux types d'instances et que vous attribuez une pondération différente à chaque type d'instance pour refléter le nombre dont vous avez besoin pour atteindre les mêmes performances, comme suit :

- `m5.large`— poids : 1
- `m5.2xlarge`— poids : 4

En attribuant ces pondérations, vous dites qu'il vous faudrait 4 `m5.large` instances pour obtenir les mêmes performances qu'une seule. `m5.2xlarge`

Pour calculer le nombre d'instances de chaque type d'instance nécessaires pour une capacité cible donnée, utilisez la formule suivante :

```
target capacity / weight = number of instances
```

Si votre capacité cible est de 8 unités, la flotte peut atteindre la capacité cible avec l'une `m5.large` ou l'autre des deux`m5.2xlarge`, ou une combinaison des deux, comme suit :

- 8 `m5.large` instances (capacité de 8/ poids de 1 = 8 instances)
- 2 `m5.2xlarge` instances (capacité de 8/ poids de 4 = 2 instances)
- 4 `m5.large` et 1 `m5.2xlarge`

Exemple : utiliser la pondération des instances pour la gestion des coûts

Par défaut, le prix que vous spécifiez représente le prix par heure d'instance. Lorsque vous utilisez la fonction de pondération d'instance, le prix que vous spécifiez correspond au prix par heure

d'unité. Vous pouvez calculer le prix par heure d'unité en divisant le prix pour un type d'instance par le nombre d'unités qu'il représente. Le parc calcule le nombre d'instances à lancer en divisant la capacité cible par le poids des instances. Si le résultat n'est pas un entier, la flotte d'instances l'arrondit à l'entier suivant afin que la taille de votre flotte ne soit pas inférieure à sa capacité cible. Le flotte d'instances peut sélectionner n'importe quel groupe indiqué dans votre spécification de lancement, même si la capacité des instances lancées dépasse la capacité cible demandée.

Le tableau suivant contient des exemples de calculs permettant de déterminer le prix par unité pour un parc d'une capacité cible de 10 personnes.

Type d'instance	Pondération de l'instance	Capacité cible	Nombre d'instances lancées	Prix par heure d'instance	Prix par heure d'unité
`r3.xlarge`	2	10	5 (10 divisé par 2)	0,05 USD	0,025 USD (0,05 divisé par 2)
`r3.8xlarge`	8	10	2 (10 divisé par 8, résultat arrondi)	0,10 USD	0,0125 USD (0,10 divisé par 8)

Utilisez la pondération des instances de flotte comme suit pour fournir la capacité cible que vous souhaitez dans les pools avec le prix unitaire le plus bas au moment de l'expédition :

1. Définissez la capacité cible de votre flotte en instances (par défaut) ou en unités de votre choix, telles que vCPU, mémoire, stockage ou débit.
2. Définissez le prix par unité.
3. Pour chaque spécification de lancement, spécifiez la pondération, à savoir le nombre d'unités que représente ce type d'instance par rapport à la capacité cible.

Exemple de pondération d'instance

Envisagez une demande de flotte avec la configuration suivante :

- Capacité cible de 24
- Spécification de lancement avec le type d'instance `r3.2xlarge` et une pondération de 6
- Spécification de lancement avec le type d'instance `c3.xlarge` et une pondération de 5

La pondération correspond au nombre d'unités du type d'instance par rapport à la capacité cible. Si la première spécification de lancement prévoit le prix unitaire le plus bas (prix `r3.2xlarge` par heure d'instance divisé par 6), le parc lancera quatre de ces instances (24 divisés par 6).

Si la deuxième spécification de lancement prévoit le prix unitaire le plus bas (prix `c3.xlarge` par heure d'instance divisé par 5), le parc lancera cinq de ces instances (24 divisées par 5, résultat arrondi au chiffre supérieur).

Pondération d'instance et stratégie d'allocation

Envisagez une demande de flotte avec la configuration suivante :

- Capacité cible de 30 instances Spot
- Spécification de lancement avec le type d'instance `c3.2xlarge` et une pondération de 8
- Spécification de lancement avec le type d'instance `m3.xlarge` et une pondération de 8
- Spécification de lancement avec le type d'instance `r3.xlarge` et une pondération de 8

La flotte lancerait quatre instances (30 divisées par 8, résultat arrondi vers le haut). Avec la stratégie `diversified`, le parc d'instances lance une instance dans chacun des trois groupes, et la quatrième instance dans l'un des trois groupes fournit le prix par unité le plus bas.

Utilisez des stratégies d'allocation pour déterminer comment EC2 Fleet ou Spot Fleet exploite les capacités sur place et à la demande

Lorsque vous utilisez plusieurs pools de capacités (chacun comprenant un type d'instance et une zone de disponibilité) dans un EC2 parc ou un parc d'emplacements, vous pouvez utiliser une stratégie d'allocation pour gérer la manière dont Amazon EC2 utilise vos capacités ponctuelles et à la demande à partir de ces pools. Les stratégies d'allocation peuvent optimiser la capacité disponible, le prix et les types d'instances à utiliser. Il existe différentes stratégies d'allocation pour les instances ponctuelles et les instances à la demande.

Rubriques

Stratégies d'allocation pour instances Spot

Votre configuration de lancement détermine tous les pools de capacité Spot possibles (types d'instances et zones de disponibilité) à partir desquels EC2 Fleet ou Spot Fleet peut lancer des instances Spot. Toutefois, lors du lancement d'instances, le parc utilise la stratégie d'allocation que vous spécifiez pour sélectionner les pools spécifiques parmi tous les pools possibles.

> **Note**
>
> (Instances Linux uniquement) Si vous configurez votre instance Spot pour qu'elle soit lancée avec AMDSEV- SNP activé, des frais d'utilisation supplémentaires vous sont facturés, équivalant à 10 % du tarif horaire à la demande pour le type d'instance sélectionné. Si la stratégie d'allocation utilise le prix comme entrée, la flotte n'inclut pas ces frais supplémentaires ; seul le prix spot est utilisé.

Vous pouvez spécifier l'une des stratégies d'allocation suivantes pour les instances Spot :

Capacité de prix optimisée (recommandé)

La flotte identifie les pools présentant la disponibilité de capacité la plus élevée compte tenu du nombre d'instances lancées. Cela signifie que nous demanderons des instances Spot auprès des groupes qui, selon nous, présentent le moins de risques d'interruption à court terme. La flotte demande ensuite des instances Spot auprès du pool le moins cher.

La stratégie d'allocation optimisée en termes de prix/capacité est le meilleur choix pour la plupart des charges de travail ponctuelles, telles que les applications conteneurisées sans état, les microservices, les applications Web, les tâches de données et d'analyse et le traitement par lots.

Si vous utilisez le AWS CLI, le nom du paramètre est `price-capacity-optimized` pour EC2 Fleet et `priceCapacityOptimized` pour Spot Fleet.

Capacité optimisée

La flotte identifie les pools présentant la disponibilité de capacité la plus élevée compte tenu du nombre d'instances lancées. Cela signifie que nous demanderons des instances Spot auprès des groupes qui, selon nous, présentent le moins de risques d'interruption à court terme. Vous pouvez éventuellement définir une priorité pour chaque type d'instance de votre parc, le parc étant d'abord optimisé en termes de capacité, mais respectant les priorités relatives aux types d'instance dans la mesure du possible.

Avec les instances Spot, la tarification change lentement au fil du temps en fonction des tendances à long terme en matière d'offre et de demande, mais la capacité fluctue en temps réel. La stratégie d'optimisation des capacités lance automatiquement les instances Spot dans les pools les plus disponibles en examinant les données de capacité en temps réel et en prédisant lesquelles sont les plus disponibles. Cela fonctionne bien pour les charges de travail dont le coût d'interruption lié au redémarrage du travail peut être plus élevé, telles que les longues charges de travail liées à l'intégration continue (CI), au rendu d'images et de médias, à l'apprentissage profond et au calcul haute performance (HPC) qui peuvent entraîner un coût d'interruption plus élevé associé au redémarrage du travail. En offrant la possibilité de réduire les interruptions, la stratégie d'optimisation des capacités peut réduire le coût global de votre charge de travail.

Vous pouvez également utiliser la stratégie d'allocation priorisée optimisée en termes de capacité avec un paramètre de priorité pour classer les types d'instances de la priorité la plus élevée à la plus faible. Vous pouvez définir la même priorité pour différents types d'instance. La flotte optimisera d'abord la capacité, mais respectera les priorités relatives aux types d'instances dans la mesure du possible (par exemple, si le respect des priorités n'affecte pas de manière significative la capacité de la flotte à fournir une capacité optimale). C'est une bonne option pour les charges de travail pour lesquelles la possibilité de perturbation doit être minimisée, mais la priorité de certains types d'instances est également importante. Notez que lorsque vous définissez la priorité des types d'instances pour votre capacité Spot, la même priorité est également appliquée à vos instances à la demande si la stratégie d'allocation à la demande est définie sur Priorisée. Pour Spot Fleet, l'utilisation de priorités n'est prise en charge que si votre flotte utilise un modèle de lancement.

Si vous utilisez le AWS CLI, les noms des paramètres sont `capacity-optimized` et `capacity-optimized-prioritized` pour EC2 Fleet `capacityOptimized` et `capacityOptimizedPrioritized` pour Spot Fleet.

Diversifié

Les instances Spot sont réparties sur tous les groupes de capacité Spot. Si vous utilisez le AWS CLI, le nom du paramètre correspond à la fois `diversified` à EC2 Fleet et à Spot Fleet.

Prix le plus bas (non recommandé)

> **Warning**
>
> Nous ne recommandons pas la stratégie d'allocation du prix le plus bas, car c'est elle qui présente le risque d'interruption le plus élevé pour vos instances Spot.

Les instances Spot proviennent du groupe dont le tarif est le plus bas et qui dispose d'une capacité disponible. Lorsque vous utilisez le AWS CLI, il s'agit de la stratégie par défaut. Cependant, nous vous recommandons de remplacer la valeur par défaut en spécifiant la stratégie d'allocation optimisée par le prix et la capacité.

Dans le cadre de la stratégie de prix le plus bas, si le pool le moins cher ne dispose pas de capacité disponible, les instances Spot proviennent du pool le moins cher qui dispose de la capacité disponible. Si un pool est à court de capacité avant d'atteindre la capacité souhaitée, la flotte continuera de répondre à votre demande en puisant dans le pool le moins cher suivant. Pour garantir que la capacité souhaitée est atteinte, vous pouvez recevoir des instances Spot de plusieurs groupes.

Cette stratégie prenant uniquement en compte que le prix des instances et non la capacité disponible, elle peut entraîner des taux d'interruption élevés.

La stratégie d'allocation du prix le plus bas n'est disponible que lorsque vous utilisez le AWS CLI. Le nom du paramètre est `lowest-price` pour EC2 Fleet et `lowestPrice` pour Spot Fleet.

Nombre de piscines à utiliser

Nombre de groupes d'instances Spot auxquels allouer votre capacité Spot cible. Valable uniquement lorsque la stratégie d'allocation est définie sur le prix le plus bas. La flotte sélectionne les pools de Spot les moins chers et répartit uniformément votre capacité de Spot cible entre le nombre de pools de Spot que vous spécifiez.

Notez que le parc essaie de tirer des instances Spot à partir du nombre de pools que vous spécifiez dans la mesure du possible. Si un pool est à court de capacité ponctuelle avant

d'atteindre votre capacité cible, la flotte continuera de répondre à votre demande en puisant dans le pool le moins cher suivant. Pour garantir l'atteinte de votre capacité cible, il se peut que vous receviez des instances Spot provenant d'un nombre de groupes supérieur à celui que vous avez spécifié. De même, si la plupart des pools n'ont pas de capacité Spot, il se peut que vous receviez votre capacité cible complète à partir d'un nombre de groupes inférieur à celui que vous avez spécifié.

Ce paramètre n'est disponible que lorsque vous spécifiez la stratégie d'allocation du prix le plus bas et uniquement lorsque vous utilisez le AWS CLI. Le nom du paramètre concerne `InstancePoolsToUseCount` à la fois EC2 Fleet et Spot Fleet.

Stratégies d'allocation pour les instances à la demande

Votre configuration de lancement détermine tous les pools de capacités possibles (types d'instances et zones de disponibilité) à partir desquels EC2 Fleet ou Spot Fleet peut lancer des instances à la demande. Toutefois, lors du lancement d'instances, le parc utilise la stratégie d'allocation que vous spécifiez pour sélectionner les pools spécifiques parmi tous les pools possibles.

Vous pouvez définir l'une des stratégies d'allocation suivantes pour les instances à la demande :

Prix le plus bas

Les instances à la demande proviennent du pool le moins cher disposant de la capacité disponible. Il s'agit de la stratégie par défaut.

Si le pool le moins cher ne dispose pas de capacité disponible, les instances à la demande proviennent du pool le moins cher qui dispose de la capacité disponible.

Si un pool est à court de capacité avant d'atteindre la capacité souhaitée, la flotte continuera de répondre à votre demande en puisant dans le pool le moins cher suivant. Pour garantir que la capacité souhaitée est atteinte, vous pouvez recevoir des instances à la demande provenant de plusieurs pools.

Priorisé

La flotte utilise la priorité que vous avez attribuée à chaque remplacement de modèle de lancement, en lançant les types d'instances par ordre de priorité la plus élevée en premier. Cette stratégie ne peut pas être utilisée avec la sélection du type d'instance basée sur les attributs. Pour un exemple d'utilisation de cette stratégie d'allocation, voirHiérarchiser les types d'instance pour la capacité à la demande.

Choisissez la stratégie d'allocation au comptant appropriée

Vous pouvez optimiser votre flotte en fonction de votre cas d'utilisation en choisissant la stratégie d'allocation de points appropriée.

Trouver un équilibre entre le prix le plus bas et la capacité disponible

Pour équilibrer les compromis entre les pools de capacité spot les moins chers et les pools de capacité spot offrant la plus grande disponibilité de capacité, nous vous recommandons d'utiliser la stratégie d'allocation optimisée en termes de prix/capacité. Cette stratégie prend des décisions concernant les groupes auprès desquels il convient de demander des instances Spot en fonction à la fois du prix des groupes et de la capacité disponible des instances Spot dans ces groupes. Cela signifie que nous demanderons des instances Spot auprès des groupes qui, selon nous, présentent le moins de risques d'interruption à court terme, tout en tenant compte du prix.

Si votre flotte exécute des charges de travail résilientes et apatrides, notamment des applications conteneurisées, des microservices, des applications Web, des tâches de données et d'analyse, ainsi que le traitement par lots, utilisez la stratégie d'allocation optimisée des capacités en termes de prix pour des économies de coûts et une disponibilité des capacités optimales.

Si votre flotte exécute des charges de travail dont l'interruption entraîne des coûts plus élevés associés au travail de redémarrage, vous devez implémenter des points de contrôle afin que les applications puissent redémarrer à partir de ce point, si elles sont interrompues. En utilisant le point de contrôle, vous adaptez la stratégie d'allocation optimisée en termes de prix/capacité à ces charges de travail, car elle alloue de la capacité à partir des pools les moins chers qui offrent également un faible taux d'interruption des instances ponctuelles.

Pour des exemples de JSON configurations qui utilisent la stratégie d'allocation optimisée par le prix et la capacité, consultez ce qui suit :

- EC2Flotte — Exemple 10 : Lancer des instances ponctuelles dans une price-capacity-optimized flotte
- Flotte Spot — Exemple 11 : Lancer des instances ponctuelles dans une priceCapacityOptimized flotte

Lorsque les charges de travail ont un coût d'interruption élevé

Vous pouvez éventuellement utiliser la stratégie d'optimisation des capacités si vous exécutez des charges de travail qui utilisent des types d'instances à prix similaires ou lorsque le coût des

interruptions est si important que toute économie de coûts est insuffisante par rapport à une augmentation marginale des interruptions. Cette stratégie alloue la capacité à partir des groupes de capacité Spot les plus disponibles qui offrent la possibilité de moins d'interruptions, ce qui peut réduire le coût global de votre charge de travail.

Lorsque les risques d'interruptions doivent être minimisés mais que la préférence pour certains types d'instances est importante, vous pouvez exprimer les priorités de votre pool en utilisant la stratégie d'allocation priorisée optimisée en termes de capacité, puis en définissant l'ordre des types d'instances à utiliser, de la priorité la plus élevée à la plus faible.

Notez que lorsque vous définissez des priorités pour l'optimisation des capacités, les mêmes priorités sont également appliquées à vos instances à la demande si la stratégie d'allocation à la demande est définie sur Priorisée. Notez également que, pour Spot Fleet, l'utilisation de priorités n'est prise en charge que si votre flotte utilise un modèle de lancement.

Pour des exemples de JSON configurations qui utilisent la stratégie d'allocation optimisée en termes de capacité, consultez les rubriques suivantes :

- EC2Flotte — Exemple 8 : Lancer des instances ponctuelles dans un parc à capacité optimisée
- Flotte Spot — Exemple 9 : lancer des instances Spot dans une flotte optimisée pour la capacité

Pour des exemples de JSON configurations qui utilisent la stratégie d'allocation priorisée optimisée en termes de capacité, consultez ce qui suit :

- EC2Flotte — Exemple 9 : Lancer des instances ponctuelles dans un parc à capacité optimisée avec des priorités
- Flotte Spot — Exemple 10 : lancer des instances Spot dans une flotte optimisée pour la capacité avec des priorités

Lorsque votre charge de travail est flexible dans le temps et que la capacité disponible n'est pas un facteur

Si votre flotte est petite ou fonctionne pendant une courte période, vous pouvez utiliser la capacité tarifaire optimisée pour maximiser les économies tout en tenant compte de la disponibilité des capacités.

Lorsque votre flotte est importante ou s'exécute pendant une longue période

Si votre flotte est importante ou fonctionne depuis longtemps, vous pouvez améliorer la disponibilité de votre flotte en répartissant les instances ponctuelles sur plusieurs pools en utilisant la stratégie diversifiée. Par exemple, si votre parc indique 10 pools et une capacité cible de 100 instances, le parc lance 10 instances ponctuelles dans chaque pool. Si le prix Spot d'un pool dépasse le prix maximum de ce pool, seul 10 % de votre flotte est touché. Avec cette stratégie, votre flotte est également moins affecté par les augmentations du prix Spot dans un pool au fil du temps. Dans le cadre de cette stratégie diversifiée, la flotte ne lance pas d'instances ponctuelles dans des pools dont le prix au comptant est égal ou supérieur au prix à la demande.

Maintien de la capacité cible pour les instances Spot

Une fois les instances Spot résiliées en raison d'une modification du prix Spot ou de la capacité disponible d'un pool de capacités Spot, un parc de ce type `maintain` lance des instances Spot de remplacement. La stratégie d'allocation détermine les groupes à partir desquels les instances de remplacement sont lancées, comme suit :

- Si la stratégie d'allocation est optimisée en termes de prix/capacité, le parc lance des instances de remplacement dans les pools présentant la plus grande disponibilité de capacité d'instances ponctuelles, tout en tenant compte du prix et en identifiant les pools les moins chers présentant une disponibilité de capacité élevée.
- Si la stratégie d'allocation est optimisée en termes de capacité, le parc lance des instances de remplacement dans les pools présentant la plus grande disponibilité de capacité d'instances ponctuelles.
- Si la stratégie d'allocation est diversifiée, le parc distribue les instances Spot de remplacement dans les pools restants.

Hiérarchiser les types d'instance pour la capacité à la demande

Lorsqu'une EC2 flotte ou une flotte ponctuelle tente d'atteindre votre capacité à la demande, elle lance par défaut le type d'instance le moins cher en premier. Si la stratégie d'allocation à la demande est définie sur Priorisée, le parc utilise la priorité pour déterminer le type d'instance à utiliser en premier lors de l'exploitation de la capacité à la demande. La priorité est affectée au remplacement du modèle de lancement, et la priorité la plus élevée est lancée en premier.

Exemple : donner la priorité aux types d'instance

Dans cet exemple, vous configurez trois dérogations au modèle de lancement, chacune avec un type d'instance différent.

Le prix à la demande des types d'instance varie. Voici les types d'instance utilisés dans cet exemple, classés par ordre de prix, en commençant par le type d'instance le moins cher :

- `m4.large` : le moins cher
- `m5.large`
- `m5a.large`

Si vous n'utilisez pas la priorité pour déterminer l'ordre, la flotte remplit la capacité à la demande en commençant par le type d'instance le moins cher.

Toutefois, supposons que vous avez des instances réservées `m5.large` inutilisées que vous voulez utiliser en premier. Vous pouvez définir la priorité de remplacement du modèle de lancement afin que les types d'instance soient utilisés dans l'ordre de priorité, comme suit :

- `m5.large` : priorité 1
- `m4.large` : priorité 2
- `m5a.large` : priorité 3

Utilisez le rééquilibrage des capacités dans le EC2 parc et le parc ponctuel pour remplacer les instances ponctuelles à risque

Grâce au rééquilibrage des capacités, votre EC2 flotte ou votre flotte ponctuelle peut maintenir la capacité ponctuelle souhaitée en remplaçant de manière proactive les instances ponctuelles risquant d'être interrompues. Lorsqu'une instance Spot présente un risque élevé d'interruption, Amazon EC2 envoie une recommandation de rééquilibrage. Si le rééquilibrage de capacité est activé, la recommandation de rééquilibrage déclenche le lancement d'une nouvelle instance ponctuelle avant que l'instance à risque ne soit interrompue.

Le rééquilibrage des capacités vous aide à maintenir la disponibilité de la charge de travail en augmentant de manière proactive votre flotte avec de nouvelles instances Spot avant que les instances en cours ne soient interrompues par Amazon. EC2

Pour configurer EC2 Fleet afin d'utiliser le rééquilibrage de capacité afin de lancer une instance Spot de remplacement

Utilisez la commande create-fleet (AWS CLI) et les paramètres appropriés dans la `MaintenanceStrategies` structure. Pour un exemple JSON de configuration, voirExemple 7 : configurer le rééquilibrage de capacité pour lancer des instances Spot de remplacement.

Pour configurer Spot Fleet afin d'utiliser le rééquilibrage de capacité afin de lancer une instance Spot de remplacement

Vous pouvez utiliser la EC2 console Amazon ou le AWS CLI pour configurer le rééquilibrage des capacités.

(Console) Lors de la création du parc Spot, cochez la case Rééquilibrage des capacités. Pour plus d'informations, consultez l'étape 6.d dans Création d'une demande de parc d'instances Spot à l'aide des paramètres définis (console).

(AWS CLI) Utilisez la request-spot-fleetcommande et les paramètres appropriés dans la `SpotMaintenanceStrategies` structure. Pour un exemple JSON de configuration, voirExemple 8 : Configurer le rééquilibrage de capacité pour lancer les instances Spot de remplacement.

Rubriques

- Limites
- Options de configuration
- Considérations

Limites

- Le rééquilibrage de capacité est disponible uniquement pour les flottes de type `maintain`.
- Lorsque la flotte est en cours d'exécution, vous ne pouvez pas modifier le paramètre Rééquilibrage de capacité. Pour modifier le paramètre Rééquilibrage de capacité, vous devez supprimer la flotte et en créer un nouveau.

Options de configuration

Les modèles `ReplacementStrategy` for EC2 Fleet et Spot Fleet prennent en charge les deux valeurs suivantes :

`launch-before-terminate`

Amazon EC2 met fin aux instances ponctuelles qui reçoivent une notification de rééquilibrage après le lancement de nouvelles instances ponctuelles de remplacement. Quand vous spécifiez `launch-before-terminate`, vous devez également spécifier une valeur pour `termination-delay`. Une fois les nouvelles instances de remplacement lancées, Amazon EC2 attend la durée de l`termination-delay`, puis met fin aux anciennes instances. Pour `termination-delay`, le minimum est de 120 secondes (2 minutes) et le maximum est de 7 200 secondes (2 heures).

Nous vous recommandons d'utiliser `launch-before-terminate` uniquement si vous pouvez prédire la durée de la procédure d'arrêt de votre instance. Cela garantit que les anciennes instances ne sont résiliées qu'une fois les procédures d'arrêt terminées. Notez qu'Amazon EC2 peut interrompre les anciennes instances avec un avertissement de deux minutes avant l`termination-delay`.

Nous vous déconseillons vivement d'utiliser la stratégie d'allocation `lowest-price` `lowestPrice` (EC2flotte) ou (flotte ponctuelle) en combinaison avec `launch-before-terminate` celle-ci afin d'éviter d'avoir des instances ponctuelles de remplacement présentant également un risque élevé d'interruption.

`launch`

Amazon EC2 lance des instances Spot de remplacement lorsqu'une notification de rééquilibrage est émise pour les instances Spot existantes. Amazon EC2 ne met pas fin aux instances qui reçoivent une notification de rééquilibrage. Vous pouvez résilier les anciennes instances ou les laisser en cours d'exécution. Toutes les instances en cours d'exécution vous sont facturées.

Considérations

Si vous configurez une EC2 flotte ou une flotte ponctuelle pour le rééquilibrage des capacités, tenez compte des points suivants :

Fournissez autant de groupes de capacité Spot que possible dans la demande

Configurez votre flotte pour utiliser plusieurs types d'instances et zones de disponibilité. Cela permet de lancer des instances Spot dans divers groupes dz capacité Spot. Pour de plus amples informations, veuillez consulter Soyez flexible en ce qui concerne les types d'instance et les zones de disponibilité.

Éviter un risque élevé d'interruption des instances Spot de remplacement

Pour éviter un risque élevé d'interruption, nous recommandons la stratégie `capacity-optimized-prioritized` d'allocation `capacity-optimized` or. Ces stratégies garantissent que les instances Spot de remplacement sont lancées dans les groupes de capacité Spot optimaux et sont donc moins susceptibles d'être interrompues dans un proche avenir. Pour de plus amples informations, veuillez consulter Utiliser la stratégie d'allocation optimisée pour le prix et la capacité.

Si vous utilisez la stratégie `lowest-price` d'allocation, vos instances Spot de remplacement peuvent présenter un risque élevé d'interruption. En effet, Amazon EC2 lancera toujours des instances dans le pool le moins cher dont la capacité est disponible à ce moment-là, même si vos instances Spot de remplacement sont susceptibles d'être interrompues peu de temps après leur lancement.

Amazon EC2 ne lancera une nouvelle instance que si la disponibilité est identique ou supérieure

L'un des objectifs du rééquilibrage de capacité est d'améliorer la disponibilité d'une instance Spot. Si une instance Spot existante reçoit une recommandation de rééquilibrage, Amazon EC2 ne lancera une nouvelle instance que si la nouvelle instance fournit une disponibilité identique ou supérieure à celle de l'instance existante. Si le risque d'interruption d'une nouvelle instance est plus élevé que celui de l'instance existante, Amazon ne EC2 lancera pas de nouvelle instance. Amazon EC2 continuera toutefois à évaluer les pools de capacité Spot et lancera une nouvelle instance si la disponibilité s'améliore.

Il est possible que votre instance existante soit interrompue si Amazon n'en lance pas une nouvelle de EC2 manière proactive. Dans ce cas, Amazon EC2 tentera de lancer une nouvelle instance, que celle-ci présente ou non un risque élevé d'interruption.

Le rééquilibrage de capacité n'augmente pas le taux d'interruption de votre instance Spot

Lorsque vous activez le rééquilibrage des capacités, cela n'augmente pas le taux d'interruption de votre instance Spot (le nombre d'instances ponctuelles récupérées lorsqu'Amazon a EC2 besoin de récupérer la capacité). Toutefois, si Capacity Rebalancing détecte qu'une instance risque d'être interrompue, Amazon EC2 tentera immédiatement de lancer une nouvelle instance. Il se peut donc que davantage d'instances soient remplacées que si vous aviez attendu qu'Amazon EC2 lance une nouvelle instance après l'interruption de l'instance à risque.

Bien que vous puissiez remplacer davantage d'instances lorsque le rééquilibrage de la capacité est activé, vous gagnerez à faire preuve de proactivité que de réactivité en disposant de plus

de temps d'action avant l'interruption de vos instances. En général, après un Avis d'interruption d'instance Spot., vous ne disposez que deux minutes pour arrêter correctement votre instance. Etant donné que le rééquilibrage de la capacité lance une nouvelle instance à l'avance, vous donnez aux processus existants de meilleures chances de se terminer sur votre instance à risque. Vous pouvez démarrer les procédures d'arrêt de votre instance et empêcher la planification de nouveaux travaux sur votre instance à risque. Vous pouvez également commencer à préparer l'instance nouvellement lancée afin de prendre le contrôle de l'application. Grâce au remplacement proactif de Capacity Rebalancing, vous bénéficiez d'une continuité.

À titre d'exemple théorique pour démontrer les risques et les avantages liés au rééquilibrage des capacités, considérez le scénario suivant :

- 14 h 00 — Une recommandation de rééquilibrage est reçue pour l'instance A, et Amazon commence EC2 immédiatement à tenter de lancer une instance B de remplacement, ce qui vous laisse le temps de démarrer vos procédures d'arrêt. *
- 14 h 30 — Une recommandation de rééquilibrage est reçue pour l'instance-B, remplacée par Instance-C, ce qui vous donne le temps de démarrer vos procédures d'arrêt. *
- 14 h 32 — Si le rééquilibrage de la capacité n'était pas activé, et si un avis d'interruption d'instance Spot avait été reçu à 14h32 pour l'instance-A, vous n'auriez disposé que de deux minutes pour agir. Cependant, l'instance-A aurait été en cours d'exécution jusqu'à ce moment.

* Si cela `launch-before-terminate` est spécifié, Amazon EC2 mettra fin à l'instance à risque une fois que l'instance de remplacement sera mise en ligne.

Amazon EC2 peut lancer de nouvelles instances Spot de remplacement jusqu'à ce que la capacité atteinte soit le double de la capacité cible

Lorsqu'un parc est configuré pour le rééquilibrage de capacité, le parc tente de lancer une nouvelle instance ponctuelle de remplacement pour chaque instance ponctuelle qui reçoit une recommandation de rééquilibrage. Une fois qu'une instance Spot reçoit une recommandation de rééquilibrage, elle n'est plus comptabilisée dans la capacité exécutée. Selon la stratégie de remplacement, Amazon EC2 met fin à l'instance après un délai d'arrêt préconfiguré ou la laisse fonctionner. Cela vous donne la possibilité d'effectuer des actions de rééquilibrage sur l'instance.

Si votre flotte atteint le double de sa capacité cible, il cesse de lancer de nouvelles instances de remplacement même si les instances de remplacement elles-mêmes reçoivent une recommandation de rééquilibrage.

Par exemple, vous créez un parc avec une capacité cible de 100 instances Spot. Toutes les instances Spot reçoivent une recommandation de rééquilibrage, ce qui oblige Amazon EC2

à lancer 100 instances Spot de remplacement. Cela augmente le nombre d'instances Spot exécutées à 200, soit le double de la capacité cible. Certaines instances de remplacement reçoivent une recommandation de rééquilibrage, mais aucune autre instance de remplacement n'est lancée car le parc ne peut pas dépasser le double de sa capacité cible.

Notez que vous êtes facturé pour toutes les instances pendant qu'elles sont en cours d'exécution.

Nous vous recommandons de configurer votre flotte de manière à mettre fin aux instances Spot qui reçoivent une recommandation de rééquilibrage

Si vous configurez votre parc pour le rééquilibrage des capacités, nous vous recommandons de choisir `launch-before-terminate` un délai de résiliation approprié uniquement si vous pouvez prévoir le temps que prendront les procédures d'arrêt de votre instance. Cela garantit que les anciennes instances ne sont résiliées qu'une fois les procédures d'arrêt terminées.

Si vous choisissez de résilier vous-même les instances recommandées pour le rééquilibrage, nous vous recommandons de surveiller le signal de recommandation de rééquilibrage reçu par les instances Spot de la flotte. En surveillant le signal, vous pouvez rapidement effectuer des actions de rééquilibrage sur les instances concernées avant qu'Amazon ne les EC2 interrompe, puis vous pouvez les résilier manuellement. Si vous ne résiliez pas les instances, vous continuez à les payer pendant qu'elles sont en cours d'exécution. Amazon EC2 ne met pas automatiquement fin aux instances qui reçoivent une recommandation de rééquilibrage.

Vous pouvez configurer des notifications à l'aide d'Amazon EventBridge ou des métadonnées d'instance. Pour de plus amples informations, veuillez consulter Surveiller les signaux de recommandation de rééquilibrage.

La flotte ne prend pas en compte les instances qui reçoivent une recommandation de rééquilibrage lors du calcul de la capacité remplie lors de l'introduction ou de la sortie d'échelle

Si votre flotte est configurée pour le rééquilibrage des capacités et que vous modifiez la capacité cible pour augmenter ou diminuer la capacité, la flotte ne compte pas les instances marquées pour le rééquilibrage dans le cadre de la capacité remplie, comme suit :

- Mise à l'échelle : si vous diminuez la capacité cible souhaitée, Amazon EC2 met fin aux instances qui ne sont pas destinées à être rééquilibrées tant que la capacité souhaitée n'est pas atteinte. Les instances marquées pour rééquilibrage ne sont pas prises en compte dans la capacité exécutée.

  Par exemple, vous créez un parc avec une capacité cible de 100 instances ponctuelles. 10 instances reçoivent une recommandation de rééquilibrage. Amazon EC2 lance donc 10

nouvelles instances de remplacement, soit une capacité totale de 110 instances. Vous réduisez ensuite la capacité cible à 50 (mise à l'échelle), mais la capacité remplie est en fait de 60 instances, car les 10 instances marquées pour le rééquilibrage ne sont pas résiliées par AmazonEC2. Vous devez résilier manuellement ces instances, ou vous pouvez les laisser en cours d’exécution.

- Extensification : si vous augmentez la capacité cible souhaitée, Amazon EC2 lance de nouvelles instances jusqu'à ce que la capacité souhaitée soit atteinte. Les instances marquées pour rééquilibrage ne sont pas prises en compte dans la capacité exécutée.

  Par exemple, vous créez un parc avec une capacité cible de 100 instances ponctuelles. 10 instances reçoivent une recommandation de rééquilibrage. Le parc lance donc 10 nouvelles instances de remplacement, soit une capacité totale de 110 instances. Vous augmentez ensuite la capacité cible à 200 (augmentation), mais la capacité exécutée est en fait de 210 instances car les 10 instances marquées pour rééquilibrage ne sont pas comptabilisées par la flotte comme faisant partie de la capacité cible. Vous devez résilier manuellement ces instances, ou vous pouvez les laisser en cours d’exécution.

Utilisez les réservations de capacité pour réserver de la capacité à la demande dans EC2 Fleet

Les réservations de capacité à la demande vous permet de réserver de la capacité de calcul pour vos instances à la demande dans une zone de disponibilité spécifique, quelle que soit la durée. Vous pouvez configurer une EC2 flotte pour qu'elle utilise d'abord les réservations de capacité lors du lancement d'instances à la demande.

Les réservations de capacité à la demande ne sont disponibles que pour les EC2 flottes dont le type de demande est défini sur`instant`.

Les réserves de capacité sont configurées comme `open` ou `targeted`. EC2Fleet peut lancer des instances à la demande dans le cadre de réservations `open` ou `targeted` de réservations de capacité, comme suit :

- Si une Réservation de capacité est `open`, les instances à la demande dont les attributs correspondent s’exécutent automatiquement dans la capacité réservée.
- Si la réservation de capacité est `targeted`, les instances doivent la cibler spécifiquement pour s’exécuter dans la capacité réservée. Cela est utile pour utiliser des réservations de capacité spécifiques ou pour contrôler quand utiliser des réservations de capacité spécifiques.

Si vous utilisez les réservations de `targeted` capacité dans votre EC2 flotte, il doit y avoir suffisamment de réservations de capacité pour atteindre la capacité à la demande cible, sinon le lancement échoue. Afin éviter un échec de lancement, ajoutez plutôt les réserves de capacité `targeted` à un groupe de ressources, puis cibler le groupe de ressources. Le groupe de ressources n'a pas besoin d'avoir suffisamment de réservations de capacité ; s'il manque de réservations de capacité avant l'exécution de la capacité à la demande cible, la flotte peut lancer la capacité cible restante dans une capacité à la demande régulière.

Pour utiliser les réservations de capacité avec EC2 Fleet

1. Configurer la flotte en tant que type `instant`. Vous ne pouvez pas utiliser les réservations de capacité pour les flottes d'autres types.
2. Configurer la stratégie d'utilisation des réservations de capacité en tant que`use-capacity-reservations-first`.
3. Dans le modèle de lancement, pourCapacity reservation (Réservation de capacité), choisissez entre Open (Ouvrir) et Target by group (Cible par groupe). Si vous choisissez Target by group (Cible par groupe(, spécifiez l'ID du groupe de ressources réservations de capacité.

Lorsque la flotte tente de remplir la capacité à la demande, si elle constate que plusieurs groupes d'instances ont des réservations de capacité correspondantes inutilisées, etlle détermine les groupes dans lesquels lancer les instances à la demande en fonction de la stratégie d'allocation à la demande (`lowest-price` ou `prioritized`).

Ressources connexes

- Pour des CLI exemples de configuration d'une flotte afin d'utiliser les réservations de capacité pour répondre aux besoins de capacité à la demandeExemples de CLI configurations pour EC2 Fleet, voir en particulier les exemples 5 à 7.
- Pour un didacticiel expliquant les étapes à suivre pour créer des réservations de capacité, les utiliser dans votre flotte et voir le nombre de réservations de capacité restantes, voir Tutoriel : configurer EC2 Fleet pour lancer des instances à la demande à l'aide de réservations de capacité ciblées
- Pour plus d'informations sur la configuration des réservations de capacité, consultez la section Réservez de la capacité de calcul grâce aux réservations de capacité à la demande et la réservation de capacité à la demande FAQs.

Collaborez avec EC2 Fleet

Pour commencer à utiliser une EC2 flotte, créez une demande qui inclut la capacité cible totale, la capacité à la demande, la capacité ponctuelle et un modèle de lancement spécifiant la configuration des instances de la flotte. Vous pouvez éventuellement spécifier des paramètres supplémentaires ou laisser le parc utiliser les valeurs par défaut. Vous pouvez également étiqueter la demande de flotte, ainsi que ses instances et volumes, lorsque vous créez la flotte.

La flotte lance des instances à la demande lorsque de la capacité est disponible, et lance des instances ponctuelles lorsque votre prix maximum dépasse le prix ponctuel et que la capacité est disponible.

Une fois votre flotte lancée, vous pouvez décrire la demande de flotte, les instances de la flotte et tout événement lié à la flotte. Vous pouvez également attribuer des balises supplémentaires selon vos besoins.

Si vous devez modifier les paramètres du parc, tels que la capacité cible totale, vous pouvez modifier le parc, à condition qu'il ait été configuré pour maintenir la capacité. Vous ne pouvez pas modifier la capacité d'une demande unique une fois qu'elle a été soumise.

La demande de flotte reste active jusqu'à son expiration ou jusqu'à ce que vous la supprimiez. Lorsque vous supprimez la demande de flotte, vous pouvez soit mettre fin aux instances, soit les laisser fonctionner. Si vous choisissez de les laisser en cours d'exécution, les instances à la demande s'exécutent jusqu'à ce que vous les résiliiez, et les instances ponctuelles s'exécutent jusqu'à ce qu'elles soient interrompues ou que vous les résiliiez.

Rubriques

EC2États des demandes de flotte

Une demande de EC2 flotte peut comporter plusieurs états, chaque état indiquant une étape différente du cycle de vie de la demande et de la gestion des instances.

Une demande EC2 de flotte peut se présenter dans l'un des états suivants :

`submitted`

La demande EC2 Fleet est en cours d'évaluation et Amazon EC2 se prépare à lancer le nombre cible d'instances. Si une requête dépasse les limites de votre flotte, elle est immédiatement supprimée.

`active`

La demande EC2 Fleet a été validée et Amazon EC2 essaie de maintenir le nombre cible d'instances en cours d'exécution. La demande conserve cet état jusqu'à ce qu'elle soit modifiée ou supprimée.

`modifying`

La demande EC2 de flotte est en cours de modification. La demande conserve cet état jusqu'à ce que la modification soit totalement traitée ou que la demande soit supprimée. Seul une flotte de type `maintain` peut être modifié. Cet état ne s'applique pas aux autres types de demandes.

`deleted_running`

La demande EC2 de flotte est supprimée et ne lance pas d'instances Spot supplémentaires. Ses instances existantes continuent de s'exécuter jusqu'à ce qu'elles soient interrompues ou résiliées manuellement. La demande conserve cet état jusqu'à ce que toutes les instances soient interrompues ou mises hors service. Seule une EC2 flotte de type `maintain` ou `request` peut avoir des instances en cours d'exécution après la suppression de la demande de EC2 flotte. Une flotte `instant` supprimé avec des instances en cours d'exécution n'est pas pris en charge. Cet état ne s'applique pas aux flottes`instant`.

`deleted_terminating`

La demande EC2 Fleet est supprimée et ses instances sont résiliées. La demande conserve cet état jusqu'à ce que toutes les instances soient mises hors service.

`deleted`

La EC2 flotte est supprimée et aucune instance n'est en cours d'exécution. La demande est supprimée deux jours après la mise hors service de ses instances.

Création d'une EC2 flotte

Pour créer une EC2 flotte, définissez la configuration de la flotte dans un JSON fichier et référencez le fichier à l'aide de la commande create-fleet AWS CLI . Dans le JSON fichier, vous devez spécifier la capacité cible totale du parc, des capacités cibles distinctes pour les instances ponctuelles et les instances à la demande, ainsi qu'un modèle de lancement qui définit la configuration des instances du parc, telles qu'un type d'instanceAMI, un sous-réseau ou une zone de disponibilité, et un ou plusieurs groupes de sécurité. Vous pouvez éventuellement spécifier des configurations supplémentaires, telles que des paramètres pour remplacer la configuration du modèle de lancement, des stratégies d'allocation pour sélectionner des instances ponctuelles et des instances à la demande dans les pools de EC2 capacités, et le montant maximum que vous êtes prêt à payer pour le parc. Pour de plus amples informations, veuillez consulter Options de configuration pour votre EC2 flotte ou votre flotte ponctuelle.

La EC2 flotte lance des instances à la demande lorsque la capacité est disponible, et lance des instances ponctuelles lorsque votre prix maximum dépasse le prix au comptant et que la capacité est disponible.

Si votre flotte inclut des instances Spot et qu'elle est de type`maintain`, Amazon EC2 essaiera de maintenir la capacité cible de votre flotte lorsque vos instances Spot sont interrompues.

EC2Limites de la flotte

Les restrictions suivantes s'appliquent à EC2 Fleet :

- La création d'une EC2 flotte est disponible uniquement via Amazon EC2 API AWS CLI, AWS SDKs, et AWS CloudFormation.
- Une demande EC2 de flotte ne peut pas couvrir plusieurs AWS régions. Vous devez créer une EC2 flotte distincte pour chaque région.
- Une demande EC2 de flotte ne peut pas couvrir différents sous-réseaux de la même zone de disponibilité.

EC2Prérequis relatifs à la flotte

Pour créer une EC2 flotte, les conditions préalables suivantes doivent être réunies :

- Modèle de lancement
- Rôle lié au service pour Fleet EC2

- Accordez l'accès aux clés gérées par le client pour les utiliser avec des données chiffrées AMIs et des EBS instantanés
- Autorisations pour les utilisateurs EC2 de la flotte

Modèle de lancement

Un modèle de lancement spécifie les informations de configuration relatives aux instances à lancer, telles que le type d'instance et la zone de disponibilité. Pour plus d'informations sur les modèles de lancement, consultezStockez les paramètres de lancement de l'instance dans les modèles de EC2 lancement Amazon.

Rôle lié au service pour Fleet EC2

Le `AWSServiceRoleForEC2Fleet` rôle accorde à la EC2 flotte l'autorisation de demander, de lancer, de résilier et d'étiqueter des instances en votre nom. Amazon EC2 utilise ce rôle lié au service pour effectuer les actions suivantes :

- `ec2:RunInstances` – Lancer des instances
- `ec2:RequestSpotInstances` – Demander des Instances Spot.
- `ec2:TerminateInstances` – Résilier des instances
- `ec2:DescribeImages`— Décrivez Amazon Machine Images (AMIs) pour les instances.
- `ec2:DescribeInstanceStatus`— Décrivez le statut des instances.
- `ec2:DescribeSubnets`— Décrivez les sous-réseaux des instances.
- `ec2:CreateTags`— Ajoutez des balises à la EC2 flotte, aux instances et aux volumes.

Assurez-vous que ce rôle existe avant d'utiliser le AWS CLI ou an API pour créer une EC2 flotte.

> **Note**
>
> Une `instant` EC2 flotte n'a pas besoin de ce rôle.

Pour créer le rôle, utilisez la IAM console comme suit.

Pour créer le AWSServiceRoleForEC2Fleet rôle pour EC2 Fleet

1. Ouvrez la IAM console à l'adresse https://console.aws.amazon.com/iam/.

2. Dans le panneau de navigation, choisissez Roles (Rôles).
3. Sélectionnez Create role (Créer un rôle).
4. Sur la page Select trusted entity (Sélectionner une entité de confiance), procédez comme suit :
   a. Pour Type d'entité de confiance, choisissez Service AWS .
   b. Sous Cas d'utilisation, pour Service ou cas d'utilisation, choisissez EC2- Fleet.

      > **Tip**
      >
      > Assurez-vous de choisir EC2- Fleet. Si vous le souhaitez EC2, le cas d'utilisation EC2- Fleet n'apparaît pas dans la liste des cas d'utilisation. Le EC2 cas d'utilisation de la flotte créera automatiquement une politique avec les IAM autorisations requises et suggérera le AWSServiceRoleForEC2Fleetnom du rôle.

   c. Choisissez Suivant.
5. Sur la page Ajouter des autorisations, sélectionnez Suivant.
6. Sur la page Nommer, vérifier et créer, choisissez Créer un rôle.

Si vous n'avez plus besoin d'utiliser EC2 Fleet, nous vous recommandons de supprimer le AWSServiceRoleForEC2Fleetrôle. Après la suppression de ce rôle de votre compte, vous pouvez créer de nouveau le rôle si vous créez une autre flotte

Pour plus d'informations, consultez la section Rôles liés aux services dans le Guide de l'IAMutilisateur.

Accordez l'accès aux clés gérées par le client pour les utiliser avec des données chiffrées AMIs et des EBS instantanés

Si vous spécifiez un EBS instantané Amazon chiffré AMI ou chiffré dans votre EC2 flotte et que vous utilisez une AWS KMS clé pour le chiffrement, vous devez autoriser le AWSServiceRoleForEC2Fleetrôle à utiliser la clé gérée par le client afin qu'Amazon EC2 puisse lancer des instances en votre nom. Pour cela, vous devez ajouter une autorisation à la clé gérée par le client, comme indiqué dans la procédure suivante.

Lorsque vous définissez les autorisations, les octrois constituent une alternative aux politiques de clé. Pour plus d'informations, consultez les rubriques Utilisation des octrois et Utilisation des politiques de clé dans AWS KMS dans le Guide du développeur AWS Key Management Service .

Pour accorder au AWSServiceRoleForEC2Fleet rôle l'autorisation d'utiliser la clé gérée par le client

- Utilisez la commande create-grant pour ajouter une autorisation à la clé gérée par le client et pour spécifier le principal (le rôle AWSServiceRoleForEC2Fleetlié au service) autorisé à effectuer les opérations autorisées par l'autorisation. La clé gérée par le client est spécifiée par le `key-id` paramètre et le ARN de la clé gérée par le client. Le principal est spécifié par le `grantee-principal` paramètre et le ARN rôle AWSServiceRoleForEC2Fleetlié au service.

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2Fleet \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Autorisations pour les utilisateurs EC2 de la flotte

Si vos utilisateurs veulent créer ou gérer une EC2 flotte, assurez-vous de leur accorder les autorisations requises.

Pour créer une politique pour EC2 Fleet

1. Ouvrez la IAM console à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Politiques.
3. Sélectionnez Create policy (Créer une politique).
4. Sur la page Créer une politique, choisissez l'JSONonglet, remplacez le texte par le texte suivant, puis sélectionnez Réviser la politique.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
              "iam:ListRoles",
              "iam:PassRole",
              "iam:ListInstanceProfiles"
            ],
            "Resource":"arn:aws:iam::123456789012:role/DevTeam*"
        }
    ]
}
```

`ec2:*`accorde à l'utilisateur l'autorisation d'appeler toutes les EC2 API actions Amazon. Pour limiter l'utilisateur à des EC2 API actions Amazon spécifiques, spécifiez plutôt ces actions.

L'utilisateur doit être autorisé à lancer l'`iam:ListRoles`action pour énumérer les IAM rôles existants, l'`iam:PassRole`action pour spécifier le rôle EC2 Fleet et l'`iam:ListInstanceProfiles`action pour énumérer les profils d'instance existants.

(Facultatif) Pour permettre à un utilisateur de créer des rôles ou des profils d'instance à l'aide de la IAM console, vous devez également ajouter les actions suivantes à la politique :

- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

5. Sur la page Review Policy (Vérifier la stratégie), saisissez un nom et une description pour la stratégie, puis choisissez Create policy (Créer une stratégie).
6. Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

   - Utilisateurs et groupes dans AWS IAM Identity Center :

     Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .

   - Utilisateurs gérés IAM par le biais d'un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Suivez les instructions de la section Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le guide de IAM l'utilisateur.

- IAMutilisateurs :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la section Création d'un rôle pour un IAM utilisateur dans le Guide de IAM l'utilisateur.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la section Ajouter des autorisations à un utilisateur (console) dans le guide de IAM l'utilisateur.

Création d'une EC2 flotte

Pour lancer une flotte d'instances à l'aide de EC2 Fleet, il vous suffit de spécifier les paramètres suivants dans votre demande de flotte, et la flotte utilisera les valeurs par défaut pour les autres paramètres :

- `LaunchTemplateId`ou `LaunchTemplateName` — Spécifie le modèle de lancement à utiliser (qui contient les paramètres des instances à lancer, tels que le type d'instance et la zone de disponibilité)
- `TotalTargetCapacity` : spécifie la capacité cible totale de la flotte
- `DefaultTargetCapacityType` : indique si l'option d'achat par défaut est à la demande ou Spot

Pour remplacer les paramètres spécifiés dans le modèle de lancement, vous pouvez spécifier un ou plusieurs remplacements. Chaque dérogation peut varier en fonction du type d'instance, de la zone de disponibilité, du sous-réseau et du prix maximum, et peut inclure une capacité pondérée différente. Au lieu de spécifier un type d'instance, vous pouvez spécifier les attributs qu'une instance doit avoir, et Amazon EC2 identifiera tous les types d'instances dotés de ces attributs. Pour de plus amples informations, veuillez consulter Spécifiez les attributs pour la sélection du type d'instance pour EC2 Fleet ou Spot Fleet.

Pour les EC2 flottes de type`instant`, vous pouvez spécifier un paramètre Systems Manager au lieu de l'AMIID. Vous pouvez spécifier le paramètre Systems Manager dans l'override ou dans le modèle de lancement. Pour de plus amples informations, veuillez consulter Utiliser un paramètre Systems Manager au lieu d'un AMI ID.

Vous pouvez définir les paramètres du parc dans un JSON fichier. Pour plus d'informations sur tous les paramètres possibles que vous pouvez spécifier, consultezAfficher toutes les options de configuration de la EC2 flotte.

Pour des exemples de configuration de flotte, voirExemples de CLI configurations pour EC2 Fleet.

La création d'une EC2 flotte n'est actuellement pas prise en charge par console.

Pour créer une EC2 flotte

- Utilisez la commande create-fleet (AWS CLI) pour créer la flotte et spécifiez le JSON fichier contenant les paramètres de configuration de la flotte.

```
aws ec2 create-fleet --cli-input-json file://file_name.json
```

Voici un exemple de sortie d'un parc d'instances du type `request` ou `maintain`.

```
{
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"
}
```

Voici un exemple de sortie d'un parc d'instances du type `instant` qui a lancé la capacité cible.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
```

```
        "i-9876543210abcdef9"
      ],
      "InstanceType": "c5.large",
      "Platform": null
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-5678901234abcdef0",
        "i-5432109876abcdef9"
      ]
  ]
}
```

Voici un exemple de sortie d'un parc d'instances du type `instant` qui a lancé une partie de la capacité cible avec les erreurs liées aux instances qui n'ont pas été lancées.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientInstanceCapacity",
```

```
      "ErrorMessage": ""
    },
  ],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ]
  ]
}
```

Voici un exemple de sortie d'un parc d'instances du type `instant` qui n'a lancé aucune instance.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
```

```
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
  ],
  "Instances": []
}
```

Créez une EC2 flotte qui remplace les instances Spot insalubres

EC2Fleet vérifie l'état de santé des instances de la flotte toutes les deux minutes. Le statut de l'état d'une instance est `healthy` ou `unhealthy`.

EC2Fleet détermine l'état de santé d'une instance à l'aide des contrôles de statut fournis par AmazonEC2. Une instance est déterminée comme `unhealthy` lorsque le contrôle du statut de l'instance ou de celui du système est `impaired` pendant trois vérifications consécutives de l'état d'intégrité. Pour de plus amples informations, veuillez consulter Contrôles de statut pour les EC2 instances Amazon.

Vous pouvez configurer votre flotte pour qu'il remplace les instances Spot non saine. Après avoir paramétré `ReplaceUnhealthyInstances` sur `true`, une instance Spot est remplacée lorsqu'elle est signalée comme `unhealthy`. Notez que la taille de la flotte peut être inférieure à sa capacité cible pendant quelques minutes pendant le remplacement d'une instance Spot non saine.

Prérequis

- Le remplacement du bilan de santé n'est pris en charge que pour EC2 les flottes qui maintiennent une capacité cible (flottes de type`maintain`), et non pour les flottes de type ou. `request` `instant`

- Le remplacement de la vérification de l'état n'est pris en charge que pour instances Spot. Cette fonctionnalité n'est pas prise en charge pour instances à la demande.
- Vous pouvez configurer votre EC2 flotte pour remplacer les instances défectueuses uniquement lorsque vous la créez.
- Les utilisateurs peuvent utiliser le remplacement lié à la surveillance de l'état seulement s'ils sont autorisés à appeler l'action `ec2:DescribeInstanceStatus`.

Pour configurer un EC2 parc afin de remplacer des instances Spot défectueuses

1. Utilisez les informations pour créer une EC2 flotte dansCréation d'une EC2 flotte.
2. Pour configurer le parc afin de remplacer les instances Spot défectueuses, dans le JSON fichier, pour`ReplaceUnhealthyInstances`, spécifie`true`.

Afficher toutes les options de configuration de la EC2 flotte

Pour consulter la liste complète des paramètres de configuration de la EC2 flotte, vous pouvez générer un JSON fichier. Pour obtenir une description de chaque paramètre, veuillez consulter create-fleet dans la référence des commandes AWS CLI .

Pour générer un JSON fichier avec tous les paramètres EC2 de flotte possibles

Utilisez la commande create-fleet (AWS CLI) et le `--generate-cli-skeleton` paramètre pour générer un JSON fichier EC2 Fleet, puis dirigez la sortie vers un fichier pour l'enregistrer.

```
aws ec2 create-fleet \
    --generate-cli-skeleton input > ec2createfleet.json
```

Exemple de sortie

```
{
    "DryRun": true,
    "ClientToken": "",
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch"
            }
        },
```

```
        "InstanceInterruptionBehavior": "hibernate",
        "InstancePoolsToUseCount": 0,
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
        "MaxTotalPrice": ""
    },
    "OnDemandOptions": {
        "AllocationStrategy": "prioritized",
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        },
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
        "MaxTotalPrice": ""
    },
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "",
                "LaunchTemplateName": "",
                "Version": ""
            },
            "Overrides": [
                {
                    "InstanceType": "r5.metal",
                    "MaxPrice": "",
                    "SubnetId": "",
                    "AvailabilityZone": "",
                    "WeightedCapacity": 0.0,
                    "Priority": 0.0,
                    "Placement": {
                        "AvailabilityZone": "",
                        "Affinity": "",
                        "GroupName": "",
                        "PartitionNumber": 0,
                        "HostId": "",
                        "Tenancy": "dedicated",
                        "SpreadDomain": "",
                        "HostResourceGroupArn": ""
                    },
                    "InstanceRequirements": {
```

```
                    "VCpuCount": {
                        "Min": 0,
                        "Max": 0
                    },
                    "MemoryMiB": {
                        "Min": 0,
                        "Max": 0
                    },
                    "CpuManufacturers": [
                        "amd"
                    ],
                    "MemoryGiBPerVCpu": {
                        "Min": 0.0,
                        "Max": 0.0
                    },
                    "ExcludedInstanceTypes": [
                        ""
                    ],
                    "InstanceGenerations": [
                        "previous"
                    ],
                    "SpotMaxPricePercentageOverLowestPrice": 0,
                    "OnDemandMaxPricePercentageOverLowestPrice": 0,
                    "BareMetal": "included",
                    "BurstablePerformance": "required",
                    "RequireHibernateSupport": true,
                    "NetworkInterfaceCount": {
                        "Min": 0,
                        "Max": 0
                    },
                    "LocalStorage": "excluded",
                    "LocalStorageTypes": [
                        "ssd"
                    ],
                    "TotalLocalStorageGB": {
                        "Min": 0.0,
                        "Max": 0.0
                    },
                    "BaselineEbsBandwidthMbps": {
                        "Min": 0,
                        "Max": 0
                    },
                    "AcceleratorTypes": [
                        "inference"
```

```
                    ],
                    "AcceleratorCount": {
                        "Min": 0,
                        "Max": 0
                    },
                    "AcceleratorManufacturers": [
                        "amd"
                    ],
                    "AcceleratorNames": [
                        "a100"
                    ],
                    "AcceleratorTotalMemoryMiB": {
                        "Min": 0,
                        "Max": 0
                    }
                }
            }
        ]
    }
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 0,
    "OnDemandTargetCapacity": 0,
    "SpotTargetCapacity": 0,
    "DefaultTargetCapacityType": "on-demand",
    "TargetCapacityUnitType": "memory-mib"
},
"TerminateInstancesWithExpiration": true,
"Type": "instant",
"ValidFrom": "1970-01-01T00:00:00",
"ValidUntil": "1970-01-01T00:00:00",
"ReplaceUnhealthyInstances": true,
"TagSpecifications": [
    {
        "ResourceType": "fleet",
        "Tags": [
            {
                "Key": "",
                "Value": ""
            }
        ]
    }
],
"Context": ""
```

```
}
```

Marquez une demande de EC2 flotte nouvelle ou existante ainsi que les instances et volumes qu'elle lance

Pour vous aider à classer et à gérer vos demandes de EC2 flotte ainsi que les instances et volumes qu'elle lance, vous pouvez les étiqueter à l'aide de métadonnées personnalisées. Vous pouvez attribuer un tag à une demande de EC2 flotte lorsque vous la créez ou ultérieurement. De même, vous pouvez attribuer une étiquette aux instances et aux volumes lorsqu'ils sont lancés par le parc ou ultérieurement.

Lorsque vous balisez une demande de flotte, les instances et les volumes lancés par la flotte ne sont pas balisés automatiquement. Vous devez baliser explicitement les instances et les volumes lancés par la flotte. Vous pouvez choisir d'attribuer des balises uniquement à la demande de flotte, ou uniquement aux instances lancées par la flotte, ou uniquement aux volumes attachés aux instances lancées par la flotte, ou à l'ensemble d'entre elles.

> **Note**
>
> Pour les types de parc `instant`, vous pouvez baliser les volumes attachés à Instances à la demande et Instances Spot. Pour les types de parc `request` ou `maintain`, vous pouvez uniquement baliser les volumes attachés à Instances à la demande.

Pour plus d'informations sur le fonctionnement des balises, consultez Marquez vos EC2 ressources Amazon.

Prérequis

Octroyez à l'utilisateur l'autorisation de baliser les ressources. Pour de plus amples informations, veuillez consulter Exemple : Baliser des ressources.

Pour accorder à un utilisateur l'autorisation de baliser les ressources

Créez une IAM politique qui inclut les éléments suivants :

- L'action `ec2:CreateTags`. Celle-ci accorde à l'utilisateur l'autorisation de créer des balises.
- L'action `ec2:CreateFleet`. Cela donne à l'utilisateur l'autorisation de créer une demande EC2 de flotte.

- Pour `Resource`, nous vous recommandons de spécifier `"*"`. Cela permet aux utilisateurs de baliser tous les types de ressources.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagEC2FleetRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:CreateFleet"
            ],
            "Resource": "*"
}
```

Important

Actuellement, nous ne prenons pas en charge les autorisations de niveau ressource pour la ressource `create-fleet`. Si vous spécifiez `create-fleet` en tant que ressource, vous recevrez une exception de non-autorisation lorsque vous tenterez de baliser le parc. L'exemple suivant illustre comment ne pas définir la stratégie.

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:CreateFleet"
    ],
    "Resource": "arn:aws:ec2:us-east-1:111122223333:create-fleet/*"
}
```

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés IAM par le biais d'un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Suivez les instructions de la section Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le guide de IAM l'utilisateur.

- IAMutilisateurs :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la section Création d'un rôle pour un IAM utilisateur dans le Guide de IAM l'utilisateur.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la section Ajouter des autorisations à un utilisateur (console) dans le guide de IAM l'utilisateur.

Pour étiqueter une nouvelle demande EC2 de flotte

Pour étiqueter une demande de EC2 flotte lorsque vous la créez, spécifiez la paire clé-valeur dans le JSONfichier utilisé pour créer la flotte. La valeur pour `ResourceType` doit être `fleet`. Si vous spécifiez une autre valeur, la demande de flotte d'instances échoue.

Pour étiqueter les instances et les volumes lancés par une EC2 flotte

Pour étiqueter les instances et les volumes lorsqu'ils sont lancés par la flotte, spécifiez les balises dans le modèle de lancement référencé dans la demande de EC2 flotte.

> **Note**
>
> Vous ne pouvez pas baliser les volumes attachés à Instances Spot qui sont lancés par un type de parc `request` ou `maintain`.

Pour étiqueter une demande, une instance et un volume de EC2 flotte existants

Utilisez la commande create-tags pour baliser les ressources existantes.

```
aws ec2 create-tags \
    --resources fleet-12a34b55-67cd-8ef9-
ba9b-9208dEXAMPLE i-1234567890abcdef0 vol-1234567890EXAMPLE \
    --tags Key=purpose,Value=test
```

Décrire la configuration, les instances et l'historique des événements de EC2 Fleet

Vous pouvez décrire la configuration de votre EC2 flotte, les instances de votre EC2 flotte et l'historique des événements de votre EC2 flotte.

Rubriques

Décrivez toutes vos EC2 flottes

Utilisez la commande describe-fleets pour décrire toutes vos flottes. EC2

```
aws ec2 describe-fleets
```

Important

Si une flotte est de type `instant`, vous devez spécifier son ID, sinon il n'apparaît pas dans la réponse. Inclure `--fleet-ids` comme suit :

```
aws ec2 describe-fleets --fleet-ids fleet-8a22eee4-f489-ab02-06b8-832a7EXAMPLE
```

Exemple de sortie

```
{
    "Fleets": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2022-02-09T03:35:52+00:00",
            "FleetId": "fleet-364457cd-3a7a-4ed9-83d0-7b63e51bb1b7",
            "FleetState": "active",
            "ExcessCapacityTerminationPolicy": "termination",
            "FulfilledCapacity": 2.0,
            "FulfilledOnDemandCapacity": 0.0,
            "LaunchTemplateConfigs": [
```

```
                {
                    "LaunchTemplateSpecification": {
                        "LaunchTemplateName": "my-launch-template",
                        "Version": "$Latest"
                    }
                }
            ],
            "TargetCapacitySpecification": {
                "TotalTargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "SpotTargetCapacity": 2,
                "DefaultTargetCapacityType": "spot"
            },
            "TerminateInstancesWithExpiration": false,
            "Type": "maintain",
            "ReplaceUnhealthyInstances": false,
            "SpotOptions": {
                "AllocationStrategy": "capacity-optimized",
                "InstanceInterruptionBehavior": "terminate"
            },
            "OnDemandOptions": {
                "AllocationStrategy": "lowestPrice"
            }
        }
    ]
}
```

Décrire toutes les instances de la EC2 flotte spécifiée

Utilisez la describe-fleet-instancescommande pour décrire les instances de la EC2 flotte spécifiée. La liste renvoyée des instances en cours d'exécution est actualisée périodiquement et peut ne pas être à jour.

```
aws ec2 describe-fleet-instances  --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Exemple de sortie

```
{
    "ActiveInstances": [
        {
            "InstanceId": "i-09cd595998cb3765e",
            "InstanceHealth": "healthy",
```

```
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-86k84j6p"
        },
        {
            "InstanceId": "i-09cf95167ca219f17",
            "InstanceHealth": "healthy",
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-dvxi7fsm"
        }
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

Décrivez l'historique des événements de votre EC2 flotte

Utilisez la describe-fleet-historycommande pour décrire les événements de la EC2 flotte spécifiée pour la durée spécifiée. Pour plus d'informations sur les événements renvoyés dans la sortie, consultezEC2Types d'événements liés à la flotte.

```
aws ec2 describe-fleet-history \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --start-time 2018-04-10T00:00:00Z
```

Exemple de sortie

```
{
    "HistoryRecords": [
        {
            "EventInformation": {
                "EventSubType": "submitted"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:05.000Z"
        },
        {
            "EventInformation": {
                "EventSubType": "active"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:15.000Z"
        },
        {
```

```
            "EventInformation": {
                "EventDescription": "t2.small, ami-07c8bc5c1ce9598c3, ...",
                "EventSubType": "progress"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-083a1c446e66085d2"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-090db02406cc3c2d6"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        }
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
    "LastEvaluatedTime": "1970-01-01T00:00:00.000Z",
    "StartTime": "2018-04-09T23:53:20.000Z"
}
```

Modifier une EC2 flotte

Vous pouvez modifier la capacité cible totale, la capacité ponctuelle et la capacité à la demande d'une EC2 flotte. Vous pouvez également modifier si les instances en cours d'exécution doivent être résiliées si la nouvelle capacité cible totale est réduite en dessous de la taille actuelle du parc.

Considérations

Tenez compte des points suivants lorsque vous modifiez une EC2 flotte :

- Type de flotte : vous ne pouvez modifier qu'un type de EC2 flotte`maintain`. Vous ne pouvez pas modifier une EC2 flotte de type `request` ou`instant`.

- Paramètres de flotte : vous pouvez modifier les paramètres suivants d'une EC2 flotte :
  - `target-capacity-specification`— Augmenter ou diminuer la capacité cible pour :
    - `TotalTargetCapacity`
    - `OnDemandTargetCapacity`
    - `SpotTargetCapacity`
  - `excess-capacity-termination-policy`— Si les instances en cours d'exécution doivent être interrompues si la capacité cible totale de la EC2 flotte est réduite en dessous de la taille actuelle de la flotte. Les valeurs valides sont :
    - `no-termination`
    - `termination`
- Comportement du parc lors de l'augmentation de la capacité cible totale : lorsque vous augmentez la capacité cible totale, le EC2 parc lance les instances supplémentaires conformément à l'option d'achat d'instance spécifiée`DefaultTargetCapacityType`, à savoir les instances à la demande ou les instances ponctuelles, et conformément à la stratégie d'allocation spécifiée.
- Comportement de la flotte lors de la diminution de la capacité cible du spot : lorsque vous diminuez la capacité cible du spot, le EC2 parc supprime toutes les demandes ouvertes qui dépassent la nouvelle capacité cible. Vous pouvez demander à la flotte de mettre fin aux instances Spot jusqu'à ce que la taille de la flotte atteigne la nouvelle capacité cible. Si la stratégie d'allocation est `lowest-price`, le parc d'instances met hors service les instances ayant le prix par unité le plus élevé. En revanche, si la stratégie d'allocation est `diversified`, le parc d'instances met hors service les instances des divers pools. Vous pouvez également demander à EC2 Fleet de conserver sa taille actuelle, mais pas de remplacer les instances ponctuelles interrompues ou les instances que vous résiliez manuellement.

  Lorsqu'une EC2 flotte met fin à une instance Spot parce que la capacité cible a été réduite, l'instance reçoit un avis d'interruption de l'instance Spot.
- État de la flotte : vous pouvez modifier une EC2 flotte qui est dans l'`active`état `submitted` ou. Lorsque vous modifiez un parc d'instances, il prend l'état `modifying`.

Commandes pour modifier une EC2 flotte

Vous pouvez utiliser la AWS CLI commande modify-fleet pour modifier une flotte. EC2

Pour modifier la capacité cible totale d'une EC2 flotte

Utilisez la commande modify-fleet pour mettre à jour la capacité cible de la flotte spécifiée. EC2

```
aws ec2 modify-fleet \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=20
```

Pour spécifier que les instances en cours d'exécution excédentaires ne doivent pas être supprimées lors de la diminution de la capacité cible totale d'une flotte EC2

Si vous diminuez la capacité cible, mais que vous souhaitez conserver la taille actuelle de la flotte, vous pouvez modifier la commande précédente comme suit :

```
aws ec2 modify-fleet \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=10 \
    --excess-capacity-termination-policy no-termination
```

Supprimer une demande de EC2 flotte et les instances de la flotte

Si vous n'avez plus besoin d'une demande de EC2 flotte, vous pouvez la supprimer. Une fois que vous avez supprimé une demande de flotte, toutes les demandes Spot associées à la flotte sont annulées, de sorte qu'aucune nouvelle instance Spot n'est lancée.

Lorsque vous supprimez une demande de EC2 flotte, vous devez également indiquer si vous souhaitez mettre fin à toutes ses instances. Cette action inclut les instances à la demande et les instances Spot. Pour les `instant` flottes, EC2 Fleet doit mettre fin aux instances lorsque la flotte est supprimée. Une flotte `instant` supprimé avec des instances en cours d'exécution n'est pas pris en charge.

Si vous spécifiez que les instances doivent être résiliées lorsque la demande de flotte est supprimée, la demande de flotte entre dans l'`deleted_terminating`état. Sinon, il passe à l'état `deleted_running` et les instances continuent à s'exécuter jusqu'à ce qu'elles soient interrompues ou jusqu'à ce que vous les mettiez hors service manuellement.

Restrictions

- Vous pouvez supprimer jusqu'à 25 flottes de types `instant` en une seule opération.
- Vous pouvez supprimer jusqu'à 100 flottes de types `maintain` ou `request` en une seule opération.
- Vous pouvez supprimer jusqu'à 125 flottes en une seule opération, à condition de ne pas dépasser le quota pour chaque type de flotte, comme indiqué ci-dessus.

- Si vous dépassez le nombre spécifié de flottes à supprimer, aucune flotte n'est supprimée.
- Jusqu'à 1 000 instances peuvent être résiliées en une seule opération pour supprimer `instant` des flottes.

Pour supprimer une EC2 flotte et mettre fin à ses instances

Utilisez la commande delete-fleets et le `--terminate-instances` paramètre pour supprimer le EC2 parc spécifié et mettre fin à ses instances associées.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

Exemple de sortie

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_terminating",
            "PreviousFleetState": "active",
            "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
        }
    ]
}
```

Pour supprimer une EC2 flotte sans mettre fin à ses instances

Vous pouvez modifier la commande précédente à l'aide du `--no-terminate-instances` paramètre pour supprimer le EC2 parc spécifié sans mettre fin aux instances associées.

> **Note**
>
> `--no-terminate-instances` n'est pas pris en charge pour les parcs `instant`.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

Exemple de sortie

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_running",
            "PreviousFleetState": "active",
            "FleetId": "fleet-4b8aaae8-dfb5-436d-a4c6-3dafa4c6b7dcEXAMPLE"
        }
    ]
}
```

Dépannage lorsqu'une flotte ne peut pas être supprimé

Si une EC2 flotte ne parvient pas à être `UnsuccessfulFleetDeletions` supprimée, la sortie renvoie l'ID de la EC2 flotte, un code d'erreur et un message d'erreur.

Les codes d'erreur sont :

- `ExceededInstantFleetNumForDeletion`
- `fleetIdDoesNotExist`
- `fleetIdMalformed`
- `fleetNotInDeletableState`
- `NoTerminateInstancesNotSupported`
- `UnauthorizedOperation`
- `unexpectedError`

Résoudre les problèmes liés à **`ExceededInstantFleetNumForDeletion`**

Si vous essayez de supprimer plus de 25 parcs `instant` en une seule demande, l'erreur `ExceededInstantFleetNumForDeletion` est renvoyée. Voici un exemple de sortie pour cette erreur.

```
{
    "UnsuccessfulFleetDeletions": [
     {
          "FleetId": " fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
```

```
          "Error": {
                 "Message": "Can't delete more than 25 instant fleets in a single
 request.",
                 "Code": "ExceededInstantFleetNumForDeletion"
           }
     },
     {
           "FleetId": "fleet-9a941b23-0286-5bf4-2430-03a029a07e31",
           "Error": {
                 "Message": "Can't delete more than 25 instant fleets in a single
 request.",
                 "Code": "ExceededInstantFleetNumForDeletion"
            }
     }
     .
     .
     .
     ],
     "SuccessfulFleetDeletions": []
}
```

Résoudre les problèmes liés à **`NoTerminateInstancesNotSupported`**

Si vous spécifiez que les instances d'un parc `instant` ne doivent pas être résiliées lorsque vous supprimez le parc, l'erreur `NoTerminateInstancesNotSupported` est renvoyée. `--no-terminate-instances` n'est pas pris en charge pour les parcs `instant`. Voici un exemple de sortie pour cette erreur.

```
{
      "UnsuccessfulFleetDeletions": [
            {
                 "FleetId": "fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
                 "Error": {
                        "Message": "NoTerminateInstances option is not supported for
 instant fleet",
                        "Code": "NoTerminateInstancesNotSupported"
                  }
            }
       ],
       "SuccessfulFleetDeletions": []
```

Résoudre les problèmes liés à **`UnauthorizedOperation`**

Si vous n'avez pas l'autorisation de résilier des instances, vous obtenez l'erreur `UnauthorizedOperation` lors de la suppression d'un parc qui doit résilier ses instances. Voici le message d'erreur.

```
<Response><Errors><Error><Code>UnauthorizedOperation</Code><Message>You are not
 authorized to perform this
operation. Encoded authorization failure message: VvuncIxj7Z_CPGNYXWqnuFV-
YjByeAU66Q9752NtQ-I3-qnDLWs6JLFd
KnSMMiq5s6cGqjjPtEDpsnGHzzyHasFHOaRYJpaDVravoW25azn6KNkUQQlFwhJyujt2dtNCdduJfrqcFYAjlEiRMkfDHt7
BHturzDK6A560Y2nDSUiMmAB1y9UNtqaZJ9SNe5sNxKMqZaqKtjRbk02RZu5V2vn9VMk6fm2aMVHbY9JhLvGypLcMUjtJ76
VPiU5v2s-
UgZ7h0p2yth6ysUdhlONg6dBYu8_y_HtEI54invCj4CoK0qawqzMNe6rcmCQHvtCxtXsbkgyaEbcwmrm2m01-
EMhekLFZeJLr
DtYOpYcEl4_nWFX1wtQDCnNNCmxnJZAoJvb3VMDYpDTsxjQv1PxODZuqWHs23YXWVywzgnLtHeRf2o4lUhGBw17mXsS07k7
PT9vrHtQiILor5VVTsjSPWg7edj__1rsnXhwPSu8gI48ZLRGrPQqFq0RmKO_QIE8N8s6NWzCK4yoX-9gDcheurOGpkprPIC
</Message></Error></Errors><RequestID>89b1215c-7814-40ae-a8db-41761f43f2b0</
RequestID></Response>
```

Pour résoudre l'erreur, vous devez ajouter l'`ec2:TerminateInstances`action à la IAM politique, comme indiqué dans l'exemple suivant.

```
{
       "Version": "2012-10-17",
       "Statement": [
            {
                "Sid": "DeleteFleetsAndTerminateInstances",
                "Effect": "Allow",
                "Action": [
                       "ec2:DeleteFleets"
                       "ec2:TerminateInstances"
                ],
                "Resource": "*"
            }
       ]
   }
```

Collaborez avec Spot Fleet

Pour commencer à utiliser un parc Spot, créez une demande qui inclut la capacité cible totale pour les instances Spot, une partie facultative à la demande, et spécifiez manuellement une paire de clés AMI et une paire de clés, ou spécifiez un modèle de lancement incluant la configuration des instances

du parc. Vous pouvez éventuellement spécifier des paramètres supplémentaires ou laisser le parc utiliser les valeurs par défaut. Vous pouvez également étiqueter la demande de flotte, ainsi que ses instances et volumes, lorsque vous créez la flotte.

La flotte lance des instances à la demande lorsque de la capacité est disponible, et lance des instances ponctuelles lorsque votre prix maximum dépasse le prix ponctuel et que la capacité est disponible.

Une fois votre flotte lancée, vous pouvez décrire la demande de flotte, les instances de la flotte et tout événement lié à la flotte. Vous pouvez également attribuer des balises supplémentaires selon vos besoins.

Si vous devez modifier les paramètres du parc, tels que la capacité cible totale, vous pouvez modifier le parc, à condition qu'il ait été configuré pour maintenir la capacité. Vous ne pouvez pas modifier la capacité d'une demande unique une fois qu'elle a été soumise.

La demande de flotte reste active jusqu'à son expiration ou jusqu'à ce que vous l'annuliez (supprimiez). Lorsque vous annulez la demande de flotte, vous pouvez soit mettre fin aux instances, soit les laisser fonctionner. Si vous choisissez de les laisser en cours d'exécution, les instances à la demande s'exécutent jusqu'à ce que vous les résiliiez, et les instances ponctuelles s'exécutent jusqu'à ce qu'elles soient interrompues ou que vous les résiliiez.

Rubriques

État des demandes de parc d'instances Spot

Une demande Spot Fleet peut comporter plusieurs états, chaque état indiquant une étape différente du cycle de vie de la demande et de la gestion des instances.

Une demande de parc d'instances Spot peut avoir l'un des états suivants :

`submitted`

La demande Spot Fleet est en cours d'évaluation et Amazon EC2 se prépare à lancer le nombre cible d'instances. Si une demande dépasse vos quotas de flotte Spot, elle est immédiatement annulée.

`active`

Le parc Spot a été validé et Amazon EC2 essaie de maintenir le nombre cible d'instances Spot en cours d'exécution. La demande conserve cet état jusqu'à ce qu'elle soit modifiée ou annulée.

`modifying`

La demande de parc d'instances Spot est en cours de modification. La demande reste dans cet état jusqu'à ce que la modification soit complètement traitée ou que la demande soit annulée. Seul une flotte de type `maintain` peut être modifié. Cet état ne s'applique pas à un type de `request` flotte ponctuel.

`cancelled_running`

Le parc Spot est annulé (supprimé) et ne lance pas d'instances Spot supplémentaires. Ses instances existantes continuent de s'exécuter jusqu'à ce qu'elles soient interrompues ou résiliées manuellement. La demande conserve cet état jusqu'à ce que toutes les instances soient interrompues ou mises hors service.

`cancelled_terminating`

Le Spot Fleet est annulé (supprimé) et ses instances sont en cours de résiliation. La demande conserve cet état jusqu'à ce que toutes les instances soient mises hors service.

`cancelled`

Le Spot Fleet est annulé (supprimé) et aucune instance n'est en cours d'exécution. La demande est supprimée deux jours après la mise hors service de ses instances.

Créer une flotte Spot

À l'aide du AWS Management Console, créez rapidement une demande de flotte ponctuelle en choisissant uniquement une capacité cible totale AMI et la capacité cible totale que vous souhaitez. Amazon EC2 configurera une flotte qui répond le mieux à vos besoins et suit les meilleures pratiques de Spot. Pour de plus amples informations, veuillez consulter Création rapide d'une demande de parc d'instances Spot (console). Sinon, vous pouvez modifier l'un des paramètres par défaut. Pour plus

d'informations, consultez Création d'une demande de parc d'instances Spot à l'aide des paramètres définis (console) et Créez une flotte de spots à l'aide du AWS CLI.

Si vous souhaitez inclure des instances à la demande dans votre flotte, vous devez spécifier un modèle de lancement dans votre demande et spécifier la capacité à la demande souhaitée.

La flotte lance des instances à la demande lorsque la capacité est disponible, et lance des instances ponctuelles lorsque votre prix maximum dépasse le prix au comptant et que la capacité est disponible.

Si votre flotte inclut des instances Spot et qu'elle est de type`maintain`, Amazon EC2 essaiera de maintenir la capacité cible de votre flotte lorsque vos instances Spot sont interrompues.

Rubriques

- Autorisations du parc d'instances Spot
- Création rapide d'une demande de parc d'instances Spot (console)
- Création d'une demande de parc d'instances Spot à l'aide des paramètres définis (console)
- Créez une flotte de spots à l'aide du AWS CLI
- Créez un parc Spot qui remplace les instances Spot insalubres

Autorisations du parc d'instances Spot

Si vos utilisateurs sont appelés à créer ou à gérer un parc d'instances Spot, veillez à leur accorder les autorisations nécessaires.

Si vous utilisez la EC2 console Amazon pour créer une flotte de spots, elle crée deux rôles liés à des services nommés `AWSServiceRoleForEC2SpotFleet` et`AWSServiceRoleForEC2Spot`, et un rôle nommé `aws-ec2-spot-fleet-tagging-role` qui octroie au parc de spots les autorisations de demander, de lancer, de résilier et d'étiqueter des ressources en votre nom. Si vous utilisez le AWS CLI ou unAPI, vous devez vous assurer que ces rôles existent.

Suivez les instructions ci-dessous pour accorder les autorisations requises et créer les rôles.

Autorisations et rôles

- Accorder des autorisations aux utilisateurs pour un parc instances Spot
- Rôle lié à un service pour un parc d'instances Spot
- Rôle lié à un service pour les instances Spot
- IAMrôle pour le balisage d'une flotte de spots

Accorder des autorisations aux utilisateurs pour un parc instances Spot

Si vos utilisateurs sont appelés à créer ou à gérer un parc d'instances Spot, veillez à leur accorder les autorisations nécessaires.

Pour créer une politique pour un parc d'instances Spot

1. Ouvrez la IAM console à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Policies (Politiques), puis Create policy (Créer une politique).
3. Sur la page Créer une politique JSON, choisissez et remplacez le texte par le texte suivant.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances",
                "ec2:CreateTags",
                "ec2:RequestSpotFleet",
                "ec2:ModifySpotFleetRequest",
                "ec2:CancelSpotFleetRequests",
                "ec2:DescribeSpotFleetRequests",
                "ec2:DescribeSpotFleetInstances",
                "ec2:DescribeSpotFleetRequestHistory"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole",
                "iam:ListRoles",
                "iam:ListInstanceProfiles"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

L'exemple de politique précédent accorde à un utilisateur les autorisations requises pour la plupart des cas d'utilisation de parc d'instances Spot. Pour limiter l'utilisateur à des API actions spécifiques, spécifiez uniquement ces API actions.

Obligatoire EC2 et IAM APIs

Les éléments suivants APIs doivent être inclus dans la politique :

- `ec2:RunInstances` : requis pour lancer des instances dans un parc d'instances Spot
- `ec2:CreateTags` : requis pour étiqueter la demande de parc d'instances Spot, les instances ou les volumes
- `iam:PassRole` : requis pour spécifier le rôle du parc d'instances Spot
- `iam:CreateServiceLinkedRole` : requis pour créer le rôle lié au service
- `iam:ListRoles`— Nécessaire pour énumérer les rôles existants IAM
- `iam:ListInstanceProfiles` : requis pour énumérer les profils d'instance existants

> **Important**
>
> Si vous spécifiez un rôle pour le profil d'IAMinstance dans la spécification de lancement ou le modèle de lancement, vous devez accorder à l'utilisateur l'autorisation de transmettre le rôle au service. Pour ce faire, incluez dans la IAM politique `"arn:aws:iam::*:role/IamInstanceProfile-role"` en tant que ressource pour l'`iam:PassRole`action. Pour plus d'informations, consultez la section Octroi à un utilisateur des autorisations lui permettant de transférer un rôle à un AWS service dans le Guide de IAM l'utilisateur.

Flotte Spot APIs

Ajoutez les API actions Spot Fleet suivantes à votre politique, selon vos besoins :

- `ec2:RequestSpotFleet`
- `ec2:ModifySpotFleetRequest`

- `ec2:CancelSpotFleetRequests`
- `ec2:DescribeSpotFleetRequests`
- `ec2:DescribeSpotFleetInstances`
- `ec2:DescribeSpotFleetRequestHistory`

Facultatif IAM APIs

(Facultatif) Pour permettre à un utilisateur de créer des rôles ou des profils d'instance à l'aide de la IAM console, vous devez ajouter les actions suivantes à la politique :

- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

4. Choisissez Examiner une stratégie.
5. Sur la page Review Policy (Vérifier la stratégie), saisissez un nom et une description pour la stratégie, puis choisissez Create policy (Créer une stratégie).
6. Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

   - Utilisateurs et groupes dans AWS IAM Identity Center :

     Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .
   - Utilisateurs gérés IAM via un fournisseur d'identité :

     Créez un rôle pour la fédération d'identité. Suivez les instructions de la section Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le guide de IAM l'utilisateur.
   - IAMutilisateurs :
     - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la section Création d'un rôle pour un IAM utilisateur dans le Guide de IAM l'utilisateur.
     - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la section Ajouter des autorisations à un utilisateur (console) dans le guide de IAM l'utilisateur.

Rôle lié à un service pour un parc d'instances Spot

Amazon EC2 utilise des rôles liés à un service pour obtenir les autorisations dont il a besoin pour appeler d'autres AWS services en votre nom. Un rôle lié à un service est un type unique de IAM rôle directement lié à un AWS service. Les rôles liés à un service constituent un moyen sécurisé de déléguer des autorisations aux AWS services, car seul le service lié peut assumer un rôle lié au service. Pour plus d'informations, consultez la section Rôles liés aux services dans le Guide de l'IAMutilisateur.

Amazon EC2 utilise le rôle lié au service nommé AWSServiceRoleForEC2SpotFleetpour lancer et gérer des instances en votre nom.

> **Important**
>
> Si vous spécifiez un EBS instantané Amazon chiffré AMI ou chiffré dans votre parc de spots, vous devez accorder au AWSServiceRoleForEC2SpotFleetrôle l'autorisation de l'utiliser CMK afin qu'Amazon EC2 puisse lancer des instances en votre nom. Pour de plus amples informations, veuillez consulter Autoriser l'accès à des CMKs fins d'utilisation avec des données chiffrées AMIs et des EBS instantanés.

Autorisations accordées par AWSServiceRoleForEC2SpotFleet

Le AWSServiceRoleForEC2SpotFleetrôle accorde à Spot Fleet l'autorisation de demander, de lancer, de résilier et d'étiqueter des instances en votre nom. Amazon EC2 utilise ce rôle lié au service pour effectuer les actions suivantes :

- `ec2:RequestSpotInstances` - Demander des Instances Spot
- `ec2:RunInstances` - Lancer des instances
- `ec2:TerminateInstances` - Résilier des instances
- `ec2:DescribeImages`- Décrivez Amazon Machine Images (AMIs) pour les instances
- `ec2:DescribeInstanceStatus` - Décrire le statut des instances.
- `ec2:DescribeSubnets` - Décrire les sous-réseaux des instances
- `ec2:CreateTags` : ajouter des identifications à la demande de parc d'instances Spot, aux instances et aux volumes
- `elasticloadbalancing:RegisterInstancesWithLoadBalancer` - Ajouter les instances spécifiées à l'équilibreur de charge indiqué.

- `elasticloadbalancing:RegisterTargets` - Enregistrer les cibles spécifiées auprès du groupe cible indiqué.

Création du rôle lié à un service

Dans la plupart des cas, vous n'avez pas besoin de créer manuellement un rôle lié à un service. Amazon EC2 crée le rôle AWSServiceRoleForEC2SpotFleetlié au service la première fois que vous créez un parc de spots à l'aide de la console.

Si vous avez reçu une demande Spot Fleet active avant octobre 2017, date à laquelle Amazon EC2 a commencé à prendre en charge ce rôle lié à un service, Amazon EC2 a créé le AWSServiceRoleForEC2SpotFleetrôle dans votre AWS compte. Pour plus d'informations, consultez la section Un nouveau rôle est apparu dans mon AWS compte dans le guide de IAM l'utilisateur.

Si vous utilisez le AWS CLI ou an API pour créer une flotte de spots, vous devez d'abord vous assurer que ce rôle existe.

Pour créer le AWSServiceRoleForEC2SpotFleet rôle pour Spot Fleet à l'aide de la console

1. Ouvrez la IAM console à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Roles (Rôles).
3. Sélectionnez Create role (Créer un rôle).
4. Sur la page Select trusted entity (Sélectionner une entité de confiance), procédez comme suit :
   a. Pour Type d'entité de confiance, choisissez Service AWS .
   b. Sous Cas d'utilisation, pour Service ou cas d'utilisation, sélectionnez EC2.
   c. Pour Cas d'utilisation, choisissez EC2- Spot Fleet.

      > **Note**
      >
      > Le cas d'utilisation de EC2- Spot Fleet créera automatiquement une politique avec les IAM autorisations requises et suggérera le AWSEC2SpotFleetServiceRolePolicynom du rôle.

   d. Choisissez Suivant.
5. Sur la page Ajouter des autorisations, sélectionnez Suivant.
6. Sur la page Nommer, vérifier et créer, choisissez Créer un rôle.

Pour créer le AWSServiceRoleForEC2SpotFleet rôle de Spot Fleet à l'aide du AWS CLI

Utilisez la commande create-service-linked-role comme suit.

```
aws iam create-service-linked-role --aws-service-name spotfleet.amazonaws.com
```

Si vous n'avez plus besoin d'utiliser Spot Fleet, nous vous recommandons de supprimer le AWSServiceRoleForEC2SpotFleetrôle. Une fois ce rôle supprimé de votre compte, Amazon le EC2 créera à nouveau si vous demandez un parc de spots à l'aide de la console. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Autoriser l'accès à des CMKs fins d'utilisation avec des données chiffrées AMIs et des EBS instantanés

Si vous spécifiez un EBS instantané Amazon chiffré AMI ou chiffré dans votre demande Spot Fleet et que vous utilisez une clé gérée par le client pour le chiffrement, vous devez accorder au AWSServiceRoleForEC2SpotFleetrôle l'autorisation d'utiliser le CMK afin qu'Amazon EC2 puisse lancer des instances en votre nom. Pour ce faire, vous devez ajouter une subvention auCMK, comme indiqué dans la procédure suivante.

Lorsque vous définissez les autorisations, les octrois constituent une alternative aux politiques de clé. Pour plus d'informations, consultez Utilisation des octrois et Utilisation des stratégies de clé dans AWS KMS dans le Guide du développeur AWS Key Management Service .

Pour accorder au AWSServiceRoleForEC2SpotFleet rôle l'autorisation d'utiliser le CMK

- Utilisez la commande create-grant pour ajouter une autorisation à CMK et pour spécifier le principal (le rôle AWSServiceRoleForEC2SpotFleetlié au service) autorisé à effectuer les opérations autorisées par l'autorisation. Le CMK est spécifié par le `key-id` paramètre et ARN leCMK. Le principal est spécifié par le `grantee-principal` paramètre et le ARN rôle AWSServiceRoleForEC2SpotFleetlié au service.

  ```
  aws kms create-grant \
      --region us-east-1 \
      --key-id arn:aws:kms:us-
  east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
      --grantee-principal arn:aws:iam::111122223333:role/
  AWSServiceRoleForEC2SpotFleet \
  ```

```
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
"GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
"ReEncryptTo"
```

Rôle lié à un service pour les instances Spot

Amazon EC2 utilise le rôle lié au service nommé AWSServiceRoleForEC2Spotpour lancer et gérer les instances Spot en votre nom. Pour de plus amples informations, veuillez consulter Rôle lié à un service pour les demandes d'instance Spot.

IAMrôle pour le balisage d'une flotte de spots

Le `aws-ec2-spot-fleet-tagging-role` IAM rôle accorde au Spot Fleet l'autorisation d'étiqueter la demande, les instances et les volumes du Spot Fleet. Pour de plus amples informations, veuillez consulter Marquez une demande Spot Fleet nouvelle ou existante ainsi que les instances et volumes qu'elle lance.

> **Important**
>
> Si vous choisissez d'étiqueter des instances dans la flotte et que vous choisissez également de maintenir la capacité cible (la demande de parc d'instances Spot est de type `maintain`), les différences dans les autorisations qui sont définies pour l'utilisateur et le rôle `IamFleetRole` peuvent entraîner un comportement d'étiquetage incohérent pour les instances de la flotte. Si le rôle `IamFleetRole` n'inclut pas l'autorisation `CreateTags`, il se peut que certaines instances lancées par le parc ne soient pas balisées. En attendant que cette incohérence soit corrigée, pour vous assurer que toutes les instances lancées par le parc sont marquées, nous vous recommandons d'utiliser le rôle `aws-ec2-spot-fleet-tagging-role` pour `IamFleetRole`. Sinon, pour utiliser un rôle existant, associez la politique `AmazonEC2SpotFleetTaggingRole` AWS gérée au rôle existant. Sinon, vous devrez ajouter manuellement l'autorisation `CreateTags` à votre stratégie.

Pour créer le IAM rôle permettant de baliser un parc de spots

1. Ouvrez la IAM console à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Roles (Rôles).
3. Sélectionnez Create role (Créer un rôle).

4. Sur la page Select trusted entity (Sélectionner entité de confiance), sous Trusted entity type (Type d'entité de service) choisissez AWS service.
5. Sous Cas d'utilisation, dans Cas d'utilisation pour d'autres AWS services, choisissez EC2, puis choisissez EC2- Spot Fleet Tagging.
6. Choisissez Suivant.
7. Sur la page Add permissions (Ajouter des autorisations), sélectionnez Next (Suivant).
8. Sur la page Name, review, and create (Nommer, réviser et créer) pour le Role name (nom de rôle), saisissez un nom de rôle (par exemple **`aws-ec2-spot-fleet-tagging-role`**).
9. Vérifiez les informations sur la page, puis choisissez Create role(Créer un rôle).

Prévention du cas de figure de l'adjoint désorienté entre services

Le problème de l'adjoint confus est un problème de sécurité dans lequel une entité qui n'a pas l'autorisation d'effectuer une action peut contraindre une entité plus privilégiée à effectuer cette action. Nous vous recommandons d'utiliser les clés de contexte de condition globale `aws:SourceArn` et `aws:SourceAccount` dans la politique d'approbation `aws-ec2-spot-fleet-tagging-role` pour limiter les autorisations que le parc d'instances Spot octroie à un autre service pour la ressource.

Pour ajouter les clés de SourceAccount condition aws : SourceArn et aws : à la politique de **`aws-ec2-spot-fleet-tagging-role`** confiance

1. Ouvrez la IAM console à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Roles (Rôles).
3. Recherchez la valeur`aws-ec2-spot-fleet-tagging-role`que vous avez créé précédemment et sélectionnez le lien (et non la case à cocher).
4. Sous Summary Summary (Résumé), sélectionnez l'onglet Trust relationships (Relations d'approbation), puis Edit trust policy (Modifier la politique d'approbation).
5. Dans la JSON déclaration, ajoutez un `Condition` élément contenant vos clés de contexte de condition `aws:SourceAccount` et celles de votre condition `aws:SourceArn` globale pour éviter le problème de confusion des adjoints, comme suit :

```
"Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:account_id:spot-fleet-request/sfr-
*"
```

```
      },
      "StringEquals": {
        "aws:SourceAccount": "account_id"
      }
```

> **Note**
>
> Si vous utilisez les deux clés de contexte de condition globale et que la valeur de `aws:SourceArn` contient l'ID de compte, la valeur de `aws:SourceAccount` et le compte indiqué dans la valeur de `aws:SourceArn` doivent utiliser le même ID de compte lorsqu'il est utilisé dans la même déclaration de politique.

La stratégie d'approbation finale sera la suivante :

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "spotfleet.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:account_id:spot-fleet-request/sfr-
*"
      },
      "StringEquals": {
        "aws:SourceAccount": "account_id"
      }
    }
  }
}
```

6. Choisissez Mettre à jour une politique.

Le tableau suivant fournit les valeurs potentielles pour`aws:SourceArn`pour limiter la portée de votre`aws-ec2-spot-fleet-tagging-role`à divers degrés de spécificité.

APIopération	Service appelé	Portée	**aws:SourceArn**
RequestSpotFleet	AWS STS (AssumeRole)	Limitez la AssumeRole aws-ec2-spot-fleet-tagging-role capacité spot-fleet-requests au compte spécifié.	arn:aws:ec2:*: *123456789012* :spot-fleet-request/sfr-*
RequestSpotFleet	AWS STS (AssumeRole)	Limitez la AssumeRole capacité aws-ec2-spot-fleet-tagging-role spot-fleet-requests au compte et à la région spécifiés. Notez que ce rôle ne sera pas utilisable dans d'autres régions.	arn:aws:ec2: *us-east-1* :*123456789012* :spot-fleet-request/sfr-*
RequestSpotFleet	AWS STS (AssumeRole)	Limitez laAssumeRole capacité suraws-ec2-spot-fleet-tagging-role uniquement aux actions affectant la flotte sfr-11111111-1111-1111-1111-111111111111. Notez que ce rôle peut ne pas être utilisable pour d'autres f Spot Fleets. De plus, ce rôle ne peut pas être utilisé pour lancer de nouvelles flottes	arn:aws:ec2: *us-east-1* :*123456789012* :spot-fleet-request/sfr-*11111111-1111-1111-1111-111111111111*

APIopération	Service appelé	Portée	`aws:SourceArn`
		ponctuelles. request-spot-fleet	

Création rapide d'une demande de parc d'instances Spot (console)

Pour créer rapidement une demande de parc d'instances Spot , procédez comme suit.

Pour créer une demande de parc d'instances Spot à l'aide des paramètres recommandés (console)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Si vous utilisez les instances Spot pour la première fois, sélectionnez Mise en route. Sinon, sélectionnez Demander des Instances Spot.
4. Sous Launch parameters (Paramètres de lancement), choisissez Manually configure launch parameters (Configuration manuelle des paramètres de lancement).
5. Pour AMI, choisissez unAMI.
6. Sous Target capacity (Capacité cible), pour Total target capacity (Capacité cible totale), indiquez le nombre d'unités à demander. Pour le type d'unité, vous pouvez choisir Instances ou Mémoire (GiB). vCPUs
7. Pour Your fleet request at a glance (Votre demande de flotte en un coup d'œil), passez en revue la configuration de votre flotte et choisissez Launch (Lancer).

Création d'une demande de parc d'instances Spot à l'aide des paramètres définis (console)

Vous pouvez créer un parc d'instances Spot à l'aide des paramètres que vous définissez.

Pour créer une demande de parc d'instances Spot à l'aide des paramètres définis (console)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Si vous utilisez les instances Spot pour la première fois, sélectionnez Mise en route. Sinon, sélectionnez Demander des Instances Spot.

4. Pour les paramètres de lancement, vous pouvez soit configurer manuellement les paramètres de lancement, soit utiliser un modèle de lancement, comme suit :

   a. [Configuration manuelle] Pour définir les paramètres de lancement dans la EC2 console Amazon, choisissez Configurer manuellement les paramètres de lancement, puis procédez comme suit :

      i. Pour AMI, choisissez l'une des options de base AMIs fournies par AWS, ou choisissez Rechercher AMI pour utiliser un membre AMI de notre communauté d'utilisateurs AWS Marketplace, le ou l'un des vôtres.

      > **Note**
      >
      > Si une instance AMI spécifiée dans les paramètres de lancement est désenregistrée ou désactivée, aucune nouvelle instance ne peut être lancée depuis le. AMI Pour les flottes conçues pour maintenir la capacité cible, la capacité cible ne sera pas maintenue.

      ii. (Facultatif) Pour Nom de la paire de clés, choisissez une paire de clés existante ou créez-en une.

      [Paire de clés existante] Choisissez la paire de clés.

      [Nouvelle paire de clés] Choisissez Créer une nouvelle paire de clés pour accéder à la page des paires de clés. Lorsque vous avez terminé, revenez à la page Spot Requests (Demandes Spot) puis actualisez la liste.

      iii. (Facultatif) Développez Additional launch parameters (Paramètres de lancement supplémentaires) et procédez comme suit.

         A. (Facultatif) Pour activer EBS l'optimisation d'Amazon, pour EBS-optimized, sélectionnez Launch EBS -optimized instances.

         B. (Facultatif) Pour ajouter de l'espace de stockage temporaire de niveau bloc pour vos instances, choisissez Attach at launch (Attacher au lancement) pour Stockage d'instance.

         C. (Facultatif) Pour ajouter du stockage, choisissez Ajouter un nouveau volume et spécifiez des volumes de stockage d'instance ou des EBS volumes Amazon supplémentaires, en fonction du type d'instance.

D. (Facultatif) Par défaut, la surveillance basique est activée pour vos instances. Pour activer la surveillance détaillée, pour Surveillance, sélectionnez Activer la surveillance CloudWatch détaillée.

E. (Facultatif) Pour exécuter une instance Spot dédiée, pour Location, choisissez Dédié : exécuter une instance dédiée.

F. (Facultatif) Pour Groupes de sécurité, choisissez un ou plusieurs groupes de sécurité ou créez-en un.

   [Groupe de sécurité existant] Choisissez un ou plusieurs groupes de sécurité.

   [Nouveau groupe de sécurité] Choisissez Create new security group (Créer un nouveau groupe de sécurité) pour accéder à la page Security Groups (Groupes de sécurité). Lorsque vous avez terminé, revenez à Spot Requests (Demandes Spot), puis actualisez la liste.

G. (Facultatif) Pour rendre vos instances accessibles depuis Internet, dans Attribuer automatiquement une adresse IP IPv4 publique, sélectionnez Activer.

H. (Facultatif) Pour lancer vos instances Spot avec un IAM rôle, par exemple un profil d'IAMinstance, choisissez le rôle.

I. (Facultatif) Pour exécuter un script de démarrage, copiez-le dans Données utilisateur.

J. (Facultatif) Pour ajouter une identification, choisissez Create tag (Créer une identification) et saisissez la clé et la valeur de l'identification, puis sélectionnez Create (Créer). Répétez l'opération pour chaque étiquette.

   Pour chaque identification, pour étiqueter les instances et la demande de parc d'instances Spot avec la même identification, assurez-vous que Instances et Fleet (Flotte) sont sélectionnées. Pour étiqueter uniquement les instances lancées par la flotte, supprimer Fleet (Flotte). Pour étiqueter uniquement la demande de parc d'instances Spot, supprimez Instances.

b. [Modèle de lancement] Pour utiliser une configuration que vous avez créée dans un modèle de lancement, choisissez Utiliser un modèle de lancement, et pour Modèle de lancement, choisissez un modèle de lancement.

> **Note**
>
> Si vous souhaitez intégrer une capacité à la demande dans votre parc de spots, vous devez spécifier un modèle de lancement.

5. Pour Additional request details (Détails de la demande supplémentaire), procédez comme suit :

   a. Vérifiez les détails de la demande supplémentaire. Pour effectuer des modifications, décochez la case Apply defaults (Appliquer les valeurs par défaut).

   b. (Facultatif) Pour le rôle de IAM flotte, vous pouvez utiliser le rôle par défaut ou choisir un autre rôle. Choisissez Use default role (Utiliser le rôle par défaut) pour utiliser le rôle par défaut après avoir changé de rôle.

   c. (Facultatif) Pour créer une demande valide uniquement pendant une période spécifique, modifiez les valeurs des champs Demande valide du et Demande valide jusqu'au.

   d. (Facultatif) Par défaut, Amazon EC2 met fin à vos instances Spot lorsque la demande de flotte Spot expire. Si vous souhaitez qu'elles continuent de s'exécuter après l'expiration de votre demande, décochez la case Terminate the instances when the request expires (Résilier les instances lorsque la demande expire).

   e. (Facultatif) Pour enregistrer vos Instances Spot auprès d'un équilibreur de charge, choisissez Receive traffic from one or more load balancers (Recevoir le trafic d'un ou plusieurs équilibreurs de charge) et choisissez un ou plusieurs Equilibreurs de charge classiques ou groupes cibles.

6. Dans Target capacity (Capacité cible), effectuez les opérations suivantes :

   a. Pour Total target capacity (Capacité cible totale), indiquez le nombre d'unités à demander. Pour le type d'unité, vous pouvez choisir Instances ou Mémoire (MiB). vCPUs Pour spécifier une capacité cible de 0 afin de pouvoir ajouter de la capacité ultérieurement, vous devez d'abord sélectionner Conserver la capacité cible.

   b. (Facultatif) Pour Include On-Demand base capacity (Inclure la capacité de base à la demande), indiquez le nombre d'unités à la demande à demander. Ce nombre doit être inférieur à la valeur du champ Capacité cible totale. Amazon EC2 calcule la différence et l'affecte aux unités Spot à demander.

> **Important**
>
> Pour spécifier une capacité à la demande facultative, vous devez commencer par choisir un modèle de lancement.

c. (Facultatif) Par défaut, Amazon EC2 met fin aux instances Spot lorsqu'elles sont interrompues. Pour maintenir la capacité cible, sélectionnez Maintain target capacity (Maintenir la capacité cible). Vous pouvez ensuite spécifier qu'Amazon EC2 met fin, arrête ou met en veille prolongée les instances Spot lorsqu'elles sont interrompues. Pour ce faire, choisissez l'option correspondante à partir de Interruption behavior (Comportement d'interruption).

> **Note**
>
> Si une instance AMI spécifiée dans les paramètres de lancement est désenregistrée ou désactivée, aucune nouvelle instance ne peut être lancée depuis le. AMI Dans ce cas, pour les flottes conçues pour maintenir la capacité cible, la capacité cible ne sera pas maintenue.

d. (Facultatif) Pour autoriser le parc d'instances Spot à lancer une instance Spot de remplacement lorsqu'une notification de rééquilibrage d'instance est émise pour une instance Spot existante dans la flotte, sélectionnez Capacity rebalance (Rééquilibrage de capacité), puis sélectionnez une stratégie de remplacement d'instance. Si vous choisissez Launch before terminate, spécifiez le délai (en secondes) avant qu'Amazon ne mette EC2 fin aux anciennes instances. Pour de plus amples informations, veuillez consulter Utilisez le rééquilibrage des capacités dans le EC2 parc et le parc ponctuel pour remplacer les instances ponctuelles à risque.

e. (Facultatif) Pour contrôler le montant que vous payez par heure pour l'ensemble des instances Spot de votre flotte, sélectionnez Set maximum cost for Spot instances (Définir le coût maximum pour les instances Spot), puis saisissez le montant total maximal que vous êtes prêt à payer par heure. Une fois le prix total maximum atteint, le parc d'instances Spot arrête de lancer des instances Spot même si la capacité cible n'a pas été atteinte. Pour de plus amples informations, veuillez consulter Fixez une limite de dépenses pour votre EC2 flotte ou votre flotte ponctuelle.

7. Pour Network (Réseau), procédez comme suit :

a. Pour Réseau, choisissez-en un existant VPC ou créez-en un nouveau.

   [ExistantVPC] Choisissez leVPC.

   [NouveauVPC] Choisissez Create new VPC pour accéder à la VPC console Amazon. Lorsque vous avez terminé, revenez à cet écran et actualisez la liste.

b. (Facultatif) Pour la zone de disponibilité, laissez Amazon EC2 choisir les zones de disponibilité pour vos instances Spot, ou spécifiez une ou plusieurs zones de disponibilité.

   Si vous avez plusieurs sous-réseaux dans une zone de disponibilité, choisissez le sous-réseau approprié dans Sous-réseau. Pour ajouter des sous-réseaux, choisissez Create new subnet pour accéder à la console AmazonVPC. Lorsque vous avez terminé, revenez à cet écran et actualisez la liste.

8. Pour les exigences relatives aux types d'instances, vous pouvez soit spécifier les attributs d'instance et laisser Amazon EC2 identifier les types d'instance optimaux avec ces attributs, soit spécifier une liste d'instances. Pour de plus amples informations, veuillez consulter Spécifiez les attributs pour la sélection du type d'instance pour EC2 Fleet ou Spot Fleet.

   a. Si vous choisissez Specify instance attributes that match your compute requirements (Spécifier les attributs d'instance qui correspondent à vos exigences de calcul), spécifiez les attributs de votre instance comme suit :

      i. Pour vCPUs, entrez le nombre minimum et maximum souhaités devCPUs. Pour ne définir aucune limite, sélectionnez Aucun minimum ou Aucun maximum, ou les deux.

      ii. Pour Memory (GiB) (Mémoire (Gio)), saisissez la quantité minimale et maximale de mémoire souhaitée. Pour ne définir aucune limite, sélectionnez Aucun minimum ou Aucun maximum, ou les deux.

      iii. (Facultatif) Pour l'attribut d'instance supplémentaire, vous pouvez éventuellement spécifier un ou plusieurs attributs pour exprimer vos besoins de calcul de manière plus détaillée. Chaque attribut supplémentaire ajoute une contrainte supplémentaire à votre demande. Vous pouvez omettre les attributs supplémentaires. Lorsque ces attributs sont omis, les valeurs par défaut sont utilisées. Pour une description de chaque attribut et de leurs valeurs par défaut, consultez le get-spot-placement-scoresmanuel Amazon EC2 Command Line Reference.

      iv. (Facultatif) Pour afficher les types d'instance avec vos attributs spécifiés, développez Preview matching instance types (Aperçu des types d'instance correspondants). Pour

empêcher des types d'instances d'être utilisés dans votre demande, sélectionnez les instances, puis choisissez Exclude selected instance types (Exclure les types d'instances sélectionnés).

b. Si vous choisissez Manually select instance types (Sélection manuelle des types d'instances), le parc d'instances Spot fournit une liste par défaut des types d'instances. Pour sélectionner d'autres types d'instances, choisissez Add instance types (Ajouter des types d'instances), sélectionnez les types d'instances à utiliser dans votre demande, puis choisissez Select (Sélectionner). Pour supprimer des types d'instance, sélectionnez les types d'instance et choisissez Delete (Supprimer).

9. Pour la stratégie d'allocation, choisissez une stratégie d'allocation au comptant et une stratégie d'allocation à la demande qui répondent à vos besoins. Pour de plus amples informations, veuillez consulter Utilisez des stratégies d'allocation pour déterminer comment EC2 Fleet ou Spot Fleet exploite les capacités sur place et à la demande.
10. Pour Your fleet request at a glance (Votre demande de flotte en un coup d'œil), passez en revue la configuration de votre flotte et effectuez les ajustements nécessaires.
11. (Facultatif) Pour télécharger une copie de la configuration de lancement à utiliser avec AWS CLI, choisissez JSONconfig.
12. Lorsque vous êtes prêt à lancer votre flotte de spots, choisissez Launch.

    Le type de demande de parc d'instances Spot est `fleet`. Une fois la demande exécutée, les demandes de type `instance` sont ajoutées, avec l'état `active` et le statut `fulfilled`.

Créez une flotte de spots à l'aide du AWS CLI

Pour créer une demande Spot Fleet à l'aide du AWS CLI

Utilisez la request-spot-fleetcommande pour créer une demande Spot Fleet.

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Pour accéder à des exemples de fichiers de configuration, consultez Exemples de CLI configurations Spot Fleet.

Voici un exemple de sortie :

```
{
```

```
    "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

Créez un parc Spot qui remplace les instances Spot insalubres

Le parc d'instances Spot vérifie l'intégrité des instances Spot de la flotte toutes les deux minutes. Le statut de l'état d'une instance est `healthy` ou `unhealthy`.

Spot Fleet détermine l'état de santé d'une instance à l'aide des contrôles de statut fournis par AmazonEC2. Une instance est déterminée comme `unhealthy` lorsque le contrôle du statut de l'instance ou de celui du système est `impaired` pendant trois surveillances consécutives de l'état. Pour de plus amples informations, veuillez consulter Contrôles de statut pour les EC2 instances Amazon.

Vous pouvez configurer votre flotte pour qu'il remplace les instances Spot non saine. Après avoir activé le remplacement de la vérification de l'état, une instance Spot est remplacée lorsqu'elle est signalée comme `unhealthy`. Notez que la taille de la flotte peut être inférieure à sa capacité cible pendant quelques minutes pendant le remplacement d'une instance Spot non saine.

Prérequis

- Le remplacement de la vérification de l'état est pris en charge uniquement pour les Parcs d'instances Spot qui maintiennent une capacité cible (parcs de type `maintain`), pas pour les Parcs d'instances Spot uniques (parcs de type `request`).
- Le remplacement de la vérification de l'état n'est pris en charge que pour instances Spot. Cette fonctionnalité n'est pas prise en charge pour instances à la demande.
- Vous pouvez configurer votre parc d'instances Spot pour qu'il remplace les instances non saines au moment de sa création uniquement.
- Les utilisateurs peuvent utiliser le remplacement lié à la surveillance de l'état seulement s'ils sont autorisés à appeler l'action `ec2:DescribeInstanceStatus`.

Console

Pour configurer un parc d'instances Spot pour remplacer des instances Spot non saines en utilisant la console

1. Suivez les étapes de création d'un parc de spots dansCréation d'une demande de parc d'instances Spot à l'aide des paramètres définis (console).

2. Pour configurer le parc afin de remplacer les instances Spot défectueuses, développez les paramètres de lancement supplémentaires et, sous Health check, sélectionnez Remplacer les instances malsaines. Pour activer cette option, vous devez d'abord choisir Maintain target capacity (Maintenir la capacité cible).

AWS CLI

Pour configurer un parc d'instances Spot pour remplacer des instances Spot non saines en utilisant la AWS CLI

1. Suivez les étapes de création d'un parc de spots dansCréez une flotte de spots à l'aide du AWS CLI.
2. Pour configurer le parc de manière à remplacer les Instances Spot non saines, pour `ReplaceUnhealthyInstances`, entrez `true`.

Marquez une demande Spot Fleet nouvelle ou existante ainsi que les instances et volumes qu'elle lance

Pour vous aider à classer et à gérer vos demandes de parc Spot ainsi que les instances et volumes qu'il lance, vous pouvez les étiqueter à l'aide de métadonnées personnalisées. Vous pouvez affecter une étiquette à une demande de parc d'instances Spot lorsque vous la créez, ou après. De même, vous pouvez attribuer une étiquette aux instances et aux volumes lorsqu'ils sont lancés par le parc ou ultérieurement.

Lorsque vous balisez une demande de flotte, les instances et les volumes lancés par la flotte ne sont pas balisés automatiquement. Vous devez baliser explicitement les instances et les volumes lancés par la flotte. Vous pouvez choisir d'attribuer des balises uniquement à la demande de flotte, ou uniquement aux instances lancées par la flotte, ou uniquement aux volumes attachés aux instances lancées par la flotte, ou à l'ensemble d'entre elles.

> **Note**
>
> Vous ne pouvez baliser que les volumes attachés à des instances à la demande. Vous ne pouvez pas baliser les volumes attachés à instances Spot.

Vous pouvez attribuer des balises à l'aide de la EC2 console Amazon ou d'un outil de ligne de commande.

Pour plus d'informations sur le fonctionnement des balises, consultez Marquez vos EC2 ressources Amazon.

Table des matières

Prérequis

Octroyez à l'utilisateur l'autorisation de baliser les ressources. Pour de plus amples informations, veuillez consulter Exemple : Baliser des ressources.

Pour accorder à un utilisateur l'autorisation de baliser les ressources

Créez une IAM politique qui inclut les éléments suivants :

- L'action `ec2:CreateTags`. Celle-ci accorde à l'utilisateur l'autorisation de créer des balises.
- L'action `ec2:RequestSpotFleet`. Celle-ci accorde à l'utilisateur l'autorisation de créer une demande de parc d'instances Spot.
- Pour `Resource`, vous devez spécifier `"*"`. Cela permet aux utilisateurs de baliser tous les types de ressources.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotFleetRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:RequestSpotFleet"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

Important

Actuellement, nous ne prenons pas en charge les autorisations de niveau ressource pour la ressource `spot-fleet-request`. Si vous spécifiez `spot-fleet-request` en tant que ressource, vous recevrez une exception de non-autorisation lorsque vous tenterez de baliser le parc. L'exemple suivant illustre comment ne pas définir la stratégie.

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:RequestSpotFleet"
    ],
    "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-request/*"
}
```

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés IAM via un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Suivez les instructions de la section Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le guide de IAM l'utilisateur.

- IAMutilisateurs :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la section Création d'un rôle pour un IAM utilisateur dans le Guide de IAM l'utilisateur.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la section Ajouter des autorisations à un utilisateur (console) dans le guide de IAM l'utilisateur.

Étiqueter un nouveau parc d'instances Spot et les instances et volumes qu'il lance

Pour étiqueter une nouvelle demande Spot Fleet ainsi que les instances et volumes qu'elle lance à l'aide de la console

1. Suivez la procédure Création d'une demande de parc d'instances Spot à l'aide des paramètres définis (console).
2. La façon dont vous ajoutez un tag varie selon que vous avez configuré manuellement la flotte ou que vous avez utilisé un modèle de lancement.

   - Si vous avez configuré le parc manuellement, procédez comme suit :

     Pour ajouter un tag, développez les paramètres de lancement supplémentaires, choisissez Create tag, puis entrez la clé et la valeur du tag. Répétez l'opération pour chaque balise.

     Pour chaque étiquette, vous pouvez étiqueter la demande de parc d'instances Spot et les instances avec la même étiquette. Pour baliser les deux, assurez-vous que les options Instances et Fleet sont sélectionnées. Pour étiqueter uniquement la demande de parc d'instances Spot, supprimez Instances. Pour étiqueter uniquement les instances lancées par la flotte, supprimer Fleet (Flotte).

     > **Note**
     >
     > Lorsque vous configurez manuellement un parc, il n'est pas possible de baliser les volumes. Les balises de volume ne sont prises en charge que pour les volumes attachés à instances à la demande. Lorsque vous configurez manuellement un parc, vous ne pouvez pas spécifier d'instances à la demande.

   - Si vous avez utilisé un modèle de lancement, procédez comme suit :

     Pour ajouter un tag à la demande de flotte, sous Tags, choisissez Create Tag, puis entrez la clé et la valeur du tag. Répétez l'opération pour chaque étiquette.

     Pour étiqueter les ressources de votre flotte, vous devez spécifier des balises dans le modèle de lancement.

Pour étiqueter une nouvelle demande Spot Fleet ainsi que les instances et volumes qu'elle lance à l'aide du AWS CLI

Pour étiqueter une demande de parc d'instances Spot lors de sa création et pour étiqueter les instances et les volumes lorsqu'ils sont lancés par la flotte, configurez la demande de parc d'instances Spot comme suit :

Étiquettes de demande de parc d'instances Spot

- Spécifiez les étiquettes pour la demande de parc d'instances Spot dans `SpotFleetRequestConfig`.
- Pour `ResourceType`, spécifiez `spot-fleet-request`. Si vous indiquez une autre valeur, la demande de flotte échouera.
- Pour `Tags`, spécifiez la paire clé-valeur. Vous pouvez définir plusieurs paires clé-valeur.

Balises d'instance :

- Spécifiez les balises des instances dans `LaunchSpecifications`.
- Pour `ResourceType`, spécifiez `instance`. Si vous indiquez une autre valeur, la demande de flotte échouera.
- Pour `Tags`, spécifiez la paire clé-valeur. Vous pouvez définir plusieurs paires clé-valeur.

  Vous pouvez également spécifier les étiquettes de l'instance dans le modèle de lancement référencé dans la demande de parc d'instances Spot.

Balises de volume :

- Spécifiez les étiquettes des volumes dans le modèle de lancement référencé dans la demande de parc d'instances Spot. Le balisage de volume dans `LaunchSpecifications` n'est pas pris en charge.

Dans l'exemple suivant, la demande de parc d'instances Spot est étiquetée par deux étiquettes : Key=Environment et Value=Production, ainsi que Key=Cost-Center et Value=123. Les instances qui sont lancées par la flotte sont identifiées avec une étiquette (qui est la même que l'une des étiquettes de la demande de parc d'instances Spot) : Key=Cost-Center et Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
```

```
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1,
        "TagSpecifications": [
            {
                "ResourceType": "spot-fleet-request",
                "Tags": [
                    {
                        "Key": "Environment",
                        "Value":"Production"
                    },
                    {
                        "Key": "Cost-Center",
                        "Value":"123"
                    }
                ]
            }
        ]
    }
}
```

Pour étiqueter les instances lancées par un parc de spots à l'aide du AWS CLI

Pour étiqueter les instances lorsqu'elles sont lancées par la flotte, vous pouvez spécifier les étiquettes dans le modèle de lancement référencé dans la demande de parc d'instances Spot ou dans la configuration de la demande de parc d'instances Spot comme suit :

- Spécifiez les balises des instances dans `LaunchSpecifications`.
- Pour `ResourceType`, spécifiez `instance`. Si vous indiquez une autre valeur, la demande de flotte échouera.
- Pour `Tags`, spécifiez la paire clé-valeur. Vous pouvez définir plusieurs paires clé-valeur.

Dans l'exemple suivant, les instances lancées par la flotte sont marquées avec une balise : Key=Cost-Center et Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
```

```
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1
    }
}
```

Pour étiqueter les volumes attachés aux instances à la demande lancées par un parc de spots à l'aide du AWS CLI

Pour étiqueter des volumes lorsqu'ils sont créés par la flotte, spécifiez les étiquettes dans le modèle de lancement référencé dans la demande de parc d'instances Spot.

> **Note**
>
> Les balises de volume ne sont prises en charge que pour les volumes attachés à instances à la demande. Vous ne pouvez pas baliser les volumes attachés à instances Spot.
> Le balisage de volume dans `LaunchSpecifications` n'est pas pris en charge.

Étiqueter un parc d'instances Spot existant

Pour étiqueter une demande de parc d'instances Spot existante à l'aide de la console

Après avoir créé une demande Spot Fleet, vous pouvez ajouter des tags à la demande de flotte à l'aide de la console.

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot.
4. Choisissez l'onglet Tags (Balises), puis Create Tag (Créer une balise).

Pour étiqueter une demande Spot Fleet existante à l'aide du AWS CLI

Utilisez la commande create-tags pour baliser les ressources existantes. Dans l'exemple suivant, la demande de parc d'instances Spot existante est étiquetée avec Key=purpose et Value=test.

```
aws ec2 create-tags \
    --resources sfr-11112222-3333-4444-5555-66666EXAMPLE \
    --tags Key=purpose,Value=test
```

Affichez les étiquettes de demande de parc d'instances Spot

Pour afficher les étiquettes d'une demande de parc d'instances Spot à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot et sélectionnez l'onglet Étiquette.

Pour décrire les étiquettes de demande de parc d'instances Spot

Utilisez la commande describe-tags pour afficher les balises de la ressource spécifiée. Dans l'exemple suivant, vous décrivez les étiquettes de la demande de parc d'instances Spot spécifiée.

```
aws ec2 describe-tags \
    --filters "Name=resource-id,Values=sfr-11112222-3333-4444-5555-66666EXAMPLE"
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Production"
        },
        {
            "Key": "Another key",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Another value"
        }
    ]
}
```

Vous pouvez également afficher les étiquettes d'une demande de parc d'instances Spot en décrivant la demande de parc d'instances Spot .

Utilisez la describe-spot-fleet-requestscommande pour afficher la configuration de la demande Spot Fleet spécifiée, qui inclut toutes les balises spécifiées pour la demande de flotte.

```
aws ec2 describe-spot-fleet-requests \
```

```
    --spot-fleet-request-ids sfr-11112222-3333-4444-5555-66666EXAMPLE
```


```
{
    "SpotFleetRequestConfigs": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2020-02-13T02:49:19.709Z",
            "SpotFleetRequestConfig": {
                "AllocationStrategy": "capacityOptimized",
                "OnDemandAllocationStrategy": "lowestPrice",
                "ExcessCapacityTerminationPolicy": "Default",
                "FulfilledCapacity": 2.0,
                "OnDemandFulfilledCapacity": 0.0,
                "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-
tagging-role",
                "LaunchSpecifications": [
                    {
                        "ImageId": "ami-0123456789EXAMPLE",
                        "InstanceType": "c4.large"
                    }
                ],
                "TargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "Type": "maintain",
                "ReplaceUnhealthyInstances": false,
                "InstanceInterruptionBehavior": "terminate"
            },
            "SpotFleetRequestId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "SpotFleetRequestState": "active",
            "Tags": [
                {
                    "Key": "Environment",
                    "Value": "Production"
                },
                {
                    "Key": "Another key",
                    "Value": "Another value"
                }
            ]
        }
    ]
}
```

Décrire la configuration d'une flotte Spot, ses instances et l'historique des événements

Vous pouvez décrire la configuration de votre parc de spots, les instances de votre parc de spots et l'historique des événements de votre parc de spots.

Pour décrire votre parc d'instances Spot (console)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot. L'identifiant commence par sfr-. Pour afficher les détails de la configuration, choisissez Description.
4. Pour répertorier les instances Spot du parc d'instances Spot, choisissezInstances.
5. Pour afficher l'historique du parc d'instances Spot, choisissez Historique.

Pour décrire votre parc d'instances Spot (AWS CLI)

Utilisez la describe-spot-fleet-requestscommande pour décrire vos demandes de parc Spot.

```
aws ec2 describe-spot-fleet-requests
```

Utilisez la describe-spot-fleet-instancescommande pour décrire les instances Spot pour le parc Spot spécifié.

```
aws ec2 describe-spot-fleet-instances \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Utilisez la commande describe-spot-fleet-request-history pour décrire l'historique des événements pour la demande Spot Fleet spécifiée.

```
aws ec2 describe-spot-fleet-request-history \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --start-time 2015-05-18T00:00:00Z
```

Modifier une demande de parc d'instances Spot

Vous pouvez modifier une demande de parc d'instances Spot active pour effectuer les tâches suivantes :

- Augmenter la capacité cible totale et la portion à la demande
- Diminuer la capacité cible totale et la portion à la demande

> **Note**
>
> Vous ne pouvez pas modifier une demande unique de parc d'instances Spot . Vous pouvez uniquement modifier une demande de parc d'instances Spot si vous avez sélectionné Maintenir la capacité cible au moment de la création de la demande de parc d'instances Spot.

Lorsque vous augmentez la capacité cible totale, le parc Spot lance des instances Spot supplémentaires. Lorsque vous augmentez la part à la demande, le parc d'instances Spot lance des instances à la demande supplémentaires.

Lorsque vous augmentez la capacité cible totale, le parc d'instances ponctuelles lance les instances ponctuelles supplémentaires conformément à la stratégie d'allocation pour sa demande de parc d'instances ponctuelles.

Lorsque vous diminuez la capacité cible totale, le Spot Fleet annule toutes les demandes ouvertes qui dépassent la nouvelle capacité cible. Vous pouvez demander à ce que le parc d'instances Spot résilie les instances Spot jusqu'à ce que la taille de la flotte atteigne la nouvelle capacité cible. Si la politique d'allocation sélectionnée est `diversified`, le parc d'instances Spot résilie les instances dans les groupes. Vous pouvez aussi demander à ce que le parc d'instances Spot conserve la taille actuelle de la flotte, mais sans remplacer les instances Spot interrompues ni les instances que vous résiliez manuellement.

Lorsqu'un parc d'instances Spot résilie une instance du fait de la diminution de la capacité cible, l'instance reçoit un avis d'interruption d'instance Spot.

Pour modifier une demande de parc d'instances Spot (console)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot.
4. Choisissez Actions, Modify target capacity (Modifier la capacité cible).
5. Dans Modify target capacity (Modifier la capacité cible), effectuez les opérations suivantes :

    a. Entrez la nouvelle capacité cible et la partie à la demande.

b. (Facultatif) Si vous diminuez la capacité cible, mais que vous souhaitez conserver la taille actuelle du parc, décochez la case Terminate instances (Résilier les instances).

c. Choisissez Submit.

Pour modifier une demande de parc Spot à l'aide du AWS CLI

Utilisez la modify-spot-fleet-requestcommande pour mettre à jour la capacité cible de la demande Spot Fleet spécifiée.

```
aws ec2 modify-spot-fleet-request \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 20
```

Vous pouvez modifier la commande précédente comme suit de façon à diminuer la capacité cible de la flotte Spot spécifié sans que cela n'ait pour effet de résilier les instances Spot.

```
aws ec2 modify-spot-fleet-request \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 10 \
    --excess-capacity-termination-policy NoTermination
```

Annuler (supprimer) une demande de Spot Fleet

Si vous n'avez plus besoin d'un parc de spots, vous pouvez annuler la demande de parc de spots, ce qui la supprime. Après l'annulation d'une demande de flotte, toutes les demandes Spot associées à la flotte sont également annulées, de sorte qu'aucune nouvelle instance Spot n'est lancée.

Lorsque vous annulez une demande de parc d'instances Spot, vous devez également spécifier si vous voulez résilier toutes ses instances. Cette action inclut les instances à la demande et les instances Spot.

Si vous spécifiez que les instances doivent être résiliées lorsque la demande de flotte est annulée, celle-ci entre dans l'état `cancelled_terminating`. Sinon, il passe à l'état `cancelled_running` et les instances continuent à s'exécuter jusqu'à ce qu'elles soient interrompues ou jusqu'à ce que vous les mettiez hors service manuellement.

Restrictions

- Vous pouvez annuler jusqu'à 100 flottes en une seule demande. Si vous dépassez le nombre spécifié, aucune flotte n'est annulée.

Pour annuler (supprimer) une demande Spot Fleet (console)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot.
4. Choisissez Actions, Annuler la demande.
5. Dans la boîte de dialogue Annuler la demande de flotte, procédez comme suit :

    a. Pour résilier les instances associées en même temps que vous annulez la demande de parc d'instances Spot, ne décochez pas la case Résilier les instances. Pour annuler la demande de parc d'instances Spot sans résilier les instances associées, décochez la case Résilier les instances.

    b. Choisissez Confirmer.

Pour annuler (supprimer) une demande Spot Fleet et mettre fin à ses instances à l'aide du AWS CLI

Utilisez la cancel-spot-fleet-requestscommande pour annuler la demande de parc Spot spécifiée et mettre fin à ses instances à la demande et à ses instances ponctuelles.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

Exemple de sortie

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_terminating",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
```

```
    "UnsuccessfulFleetRequests": []
}
```

Pour annuler (supprimer) une demande Spot Fleet sans mettre fin à ses instances à l'aide du AWS CLI

Vous pouvez modifier la commande précédente en utilisant le paramètre `--no-terminate-instances` pour annuler la demande de parc d'instances Spot spécifiée sans résilier ses instances à la demande et ses instances Spot.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

Exemple de sortie

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_running",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

Découvrez le dimensionnement automatique pour Spot Fleet

La mise à l'échelle automatique permet à votre flotte Spot d'augmenter ou de diminuer sa capacité cible en fonction de la demande. Grâce au dimensionnement automatique, un parc de spots peut soit lancer des instances (scalage externe), soit mettre fin à des instances (scaling in) dans une plage spécifiée, en réponse à une ou plusieurs politiques de dimensionnement.

Le dimensionnement automatique pour Spot Fleet est rendu possible grâce à la combinaison d'AmazonEC2, d'Amazon CloudWatch et d'Application Auto ScalingAPIs. Les demandes Spot Fleet sont créées avec AmazonEC2, les alarmes sont créées avec CloudWatch Application Auto Scaling et les politiques de dimensionnement sont créées avec Application Auto Scaling.

Types de mise à l'échelle automatique

Le parc d'instances Spot prend en charge les types de scalabilité automatique suivants :

- Mise à l'échelle du suivi des cibles : augmentation ou diminution la capacité actuelle de la flotte en ciblant une valeur pour une métrique spécifique. Cela ressemble à la façon dont votre thermostat maintient la température de votre maison : vous sélectionnez la température souhaitée et le thermostat fait le reste.
- Mise à l'échelle d'étape : augmente ou réduit la capacité actuelle de la flotte en fonction d'un ensemble d'ajustements de la mise à l'échelle, appelés ajustements d'étape, qui varient en fonction de la valeur d'utilisation hors limites de l'alarme.
- Mise à l'échelle planifiée : augmente ou réduit la capacité actuelle de la flotte en fonction de la date et de l'heure.

Considérations

Lorsque vous utilisez le dimensionnement automatique pour votre parc de spots, tenez compte des points suivants :

- Pondération des instances : si vous utilisez la pondération des instances, gardez à l'esprit que Spot Fleet peut dépasser la capacité cible selon les besoins. La capacité fournie peut correspondre à un nombre à virgule flottante, mais la capacité cible doit être un nombre entier pour que le parc d'instances Spot puisse l'arrondir au nombre entier suivant. Vous devez prendre ces comportements en compte lorsque vous examinez les résultats d'une politique de dimensionnement lorsqu'une alarme se déclenche. Par exemple, supposons que la capacité cible est 30, que la capacité fournie est 30,1 et que la politique de dimensionnement soustrait 1. Lorsque l'alarme se déclenche, le processus de scalabilité automatique soustrait 1 de 30,1 pour obtenir 29,1, puis arrondit la valeur à 30. Aucune action de mise à l'échelle n'est alors effectuée. Pour prendre un autre exemple, supposons que vous avez sélectionné des pondérations d'instance de 2, 4 et 8, et une capacité cible de 10, mais qu'aucune instance de pondération 2 n'était disponible, si bien que le parc d'instances Spot a provisionné des instances de pondération 4 et 8 pour une capacité fournie de 12. Si la politique de mise à l'échelle réduit la capacité cible de 20 % et qu'une alarme se déclenche, le processus de scalabilité automatique soustrait 12 x 0,2 de 12 pour obtenir 9,6, puis arrondit la valeur à 10. Aucune action de mise à l'échelle n'est alors effectuée.
- Période de recharge : les politiques de dimensionnement que vous créez pour Spot Fleet prévoient une période de recharge. C'est le nombre de secondes après la fin d'une activité de dimensionnement au cours desquelles les activités de dimensionnement précédentes liées à un déclencheur peuvent influer sur les événements de dimensionnement futurs. Pour les politiques

de montée en charge (scale-out), pendant la durée du temps de stabilisation, la capacité qui a été ajoutée par l'événement de montée en charge précédent qui a lancé la stabilisation est calculée dans le cadre de la capacité souhaitée pour la montée en charge suivante. L'objectif est d'effectuer une montée en charge continue (mais pas excessive). Pour les politiques de diminution de charge, la période de récupération est utilisée pour bloquer les demandes de montée en charge suivantes jusqu'à leur expiration. L'objectif est de diminuer la charge avec prudence afin de protéger la disponibilité de votre application. Toutefois, si une autre alarme déclenche une politique de montée en charge pendant le temps de stabilisation après une diminution en charge (scale-in), la scalabilité automatique monte immédiatement en charge votre cible scalable.

- Utilisez une surveillance détaillée : nous vous recommandons d'effectuer une mise à l'échelle en fonction des métriques de l'instance avec une fréquence d'une minute, car cela garantit une réponse plus rapide aux changements d'utilisation. Un dimensionnement sur des métriques à une fréquence de 5 minutes peut entraîner des temps de réponse plus lents et un dimensionnement sur des données de métrique obsolètes. Pour envoyer des données métriques pour vos instances par périodes d' CloudWatchune minute, vous devez spécifiquement activer la surveillance détaillée. Pour plus d'informations, consultez Gérez la surveillance détaillée de vos EC2 instances et Création d'une demande de parc d'instances Spot à l'aide des paramètres définis (console).
- AWS CLI— Si vous utilisez le AWS CLI pour configurer le dimensionnement pour Spot Fleet, vous utiliserez l'CLIapplication-autoscaling. Pour plus d'informations, consultez les ressources suivantes :
  - Section application-autoscaling du document Référence des commandes AWS CLI
  - APIRéférence d'Application Auto Scaling
  - Guide de l'utilisateur Application Auto Scaling

IAMautorisations requises pour le dimensionnement automatique de Spot Fleet

Le dimensionnement automatique pour Spot Fleet est rendu possible grâce à la combinaison d'AmazonEC2, d'Amazon CloudWatch et d'Application Auto ScalingAPIs. Les demandes Spot Fleet sont créées avec AmazonEC2, les alarmes sont créées avec CloudWatch Application Auto Scaling et les politiques de dimensionnement sont créées avec Application Auto Scaling. Outre les IAMautorisations requises pour utiliser Spot Fleet et AmazonEC2, l'utilisateur qui accède aux paramètres de dimensionnement du parc doit disposer des autorisations appropriées pour les services qui prennent en charge le dimensionnement automatique.

Pour utiliser le dimensionnement automatique pour Spot Fleet, les utilisateurs doivent être autorisés à utiliser les actions illustrées dans l'exemple de politique suivant.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:*",
                "ec2:DescribeSpotFleetRequests",
                "ec2:ModifySpotFleetRequest",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarmHistory",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeAlarmsForMetric",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DisableAlarmActions",
                "cloudwatch:EnableAlarmActions",
                "iam:CreateServiceLinkedRole",
                "sns:CreateTopic",
                "sns:Subscribe",
                "sns:Get*",
                "sns:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Vous pouvez également créer vos propres IAM politiques qui autorisent des autorisations plus précises pour les appels à Application Auto Scaling. API Pour plus d'informations, consultez Identity and Access Management for Application Auto Scaling dans le Guide de l'utilisateur d'Application Auto Scaling.

Le service Application Auto Scaling a également besoin d'une autorisation pour décrire votre parc de spots et vos CloudWatch alarmes, ainsi que d'autorisations pour modifier la capacité cible de votre parc de spots en votre nom. Si vous activez la scalabilité automatique pour votre parc d'instances Spot, il crée un rôle lié à un service nommé `AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest`. Le rôle lié à un service donne à Application Auto Scaling l'autorisation de décrire les alarmes de vos politiques, de surveiller la capacité actuelle du flotte et éventuellement de la modifier. Le rôle de parc d'instances

Spot géré original pour Application Auto Scaling était `aws-ec2-spot-fleet-autoscale-role`, mais il n'est plus nécessaire. Le rôle lié à un service est le rôle par défaut pour Application Auto Scaling. Pour plus d'informations, consultez Rôles liés aux services pour Application Auto Scaling dans le Guide de l'utilisateur Application Auto Scaling.

Mise à l'échelle du suivi des cibles : dimensionnez le parc de spots en ciblant une valeur pour une métrique spécifique

Avec le dimensionnement du suivi des cibles, vous créez une politique de dimensionnement du suivi des cibles en sélectionnant une métrique et en définissant une valeur cible. Spot Fleet crée et gère ensuite les CloudWatch alarmes qui déclenchent la politique de dimensionnement, puis calcule l'ajustement de dimensionnement en fonction de la métrique choisie et de la valeur cible. La politique de dimensionnement ajuste la capacité en ajoutant ou en supprimant des instances selon les besoins pour maintenir la métrique à la valeur cible spécifiée ou proche de celle-ci. Une politique de suivi des cibles permet non seulement de maintenir la métrique proche de la valeur cible, mais aussi de s'adapter aux fluctuations de la métrique dues à un schéma de charge fluctuant et de minimiser les fluctuations rapides de capacité.

Vous pouvez créer plusieurs politiques de dimensionnement du suivi des cibles pour un parc de spots, à condition que chaque politique utilise une métrique différente. Le parc évolue en fonction de la politique qui définit la plus grande capacité du parc. Cela vous permet de couvrir plusieurs scénarios afin de garantir une capacité suffisante pour les charges de travail de vos applications.

Pour garantir la disponibilité de l'application, la flotte augmente proportionnellement aux métriques aussi rapidement que possible, mais diminue plus progressivement.

Lorsqu'un parc Spot met fin à une instance Spot parce que la capacité cible a été réduite, l'instance reçoit un avis d'interruption de l'instance Spot.

> **Note**
>
> Ne modifiez ni ne supprimez les CloudWatch alarmes gérées par Spot Fleet dans le cadre d'une politique de dimensionnement du suivi des cibles. Le parc d'instances Spot supprime les alarmes automatiquement lorsque vous supprimez la politique de suivi des objectifs et d'échelonnement.

Prérequis

- La demande de parc d'instances Spot doit être de type `maintain`. La scalabilité automatique n'est pas prise en charge pour les demandes de type `request`.
- Configurez le IAMautorisations requises pour le dimensionnement automatique de Spot Fleet.
- Prenez connaissance des Considérations.

Pour configurer une politique de suivi de cible (console)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot.
4. Choisissez l'onglet Auto Scaling en bas de l'écran. Si vous avez sélectionné le lien pour votre Spot Fleet, il n'y a pas d'onglet ; faites défiler la page vers le bas jusqu'à la section Auto Scaling.
5. Si la mise à l'échelle automatique n'est pas configurée, sélectionnez Configurer.
6. Utilisez le champ Scale capacity between (Mettre à l'échelle la capacité entre) pour définir les capacités minimale et maximale de votre parc. Avec le dimensionnement automatique, votre flotte n'aura jamais une capacité inférieure ou supérieure aux limites fixées.
7. Pour Policy name (Nom de la stratégie), attribuez un nom à cette stratégie.
8. Choisissez une valeur Target Metric (Métrique cible).
9. Spécifiez une valeur Target Value (Valeur cible) pour la métrique.
10. Pour le Temps de stabilisation, spécifiez une nouvelle valeur (en secondes) ou conservez la valeur par défaut.
11. (Facultatif) Pour ne pas créer de politique de scale-in basée sur la configuration actuelle, sélectionnez Désactiver le scale-in. Vous pouvez créer une politique d'ajustement à la baisse à l'aide d'une autre configuration.
12. Choisissez Save (Enregistrer).

Pour configurer une politique de suivi des cibles à l'aide du AWS CLI

1. Enregistrez la demande Spot Fleet en tant que cible évolutive à l'aide de la register-scalable-targetcommande.
2. Créez une politique de dimensionnement à l'aide de la put-scaling-policycommande.

Étalage par étapes : dimensionnez le parc de spots à l'aide de politiques de dimensionnement par étapes

Avec les politiques de dimensionnement par étapes, vous spécifiez CloudWatch des alarmes pour déclencher le processus de dimensionnement. Par exemple, si vous souhaitez augmenter votre capacité lorsque CPU l'utilisation atteint un certain niveau, créez une alarme à l'aide de la `CPUUtilization` métrique fournie par AmazonEC2.

Lorsque vous créez une politique de dimensionnement d'étape, vous devez indiquer l'un des types d'ajustement suivants :

- Ajouter : augmentez la capacité cible de la flotte selon un nombre donné d'unités de capacité ou un pourcentage de la capacité actuelle spécifié.
- Supprimer : réduisez la capacité cible de la flotte selon un nombre donné d'unités de capacité ou un pourcentage de la capacité actuelle spécifié.
- Définir sur : définissez la capacité cible de la flotte selon un nombre précis d'unités de capacité spécifié.

Lorsqu'une alarme se déclenche, le processus de scalabilité automatique calcule la nouvelle capacité cible d'après la capacité fournie et la politique de mise à l'échelle, puis met à jour la capacité cible en conséquence. Par exemple, supposons que la capacité cible et la capacité fournie sont égales à 10 et que la politique de dimensionnement ajoute 1. Lorsque l'alarme se déclenche, le processus de scalabilité automatique ajoute 1 à 10 pour obtenir 11, pour que le parc d'instances Spot lance 1 instance.

Lorsqu'un parc Spot met fin à une instance Spot parce que la capacité cible a été réduite, l'instance reçoit un avis d'interruption de l'instance Spot.

Prérequis

- La demande de parc d'instances Spot doit être de type `maintain`. La scalabilité automatique n'est pas prise en charge pour les demandes de type `request`.
- Configurez le IAMautorisations requises pour le dimensionnement automatique de Spot Fleet.
- Déterminez quels CloudWatch indicateurs sont importants pour votre application. Vous pouvez créer des CloudWatch alarmes en fonction des métriques fournies par AWS ou de vos propres métriques personnalisées.

- Pour les AWS métriques que vous utiliserez dans vos politiques de dimensionnement, activez la collecte de CloudWatch métriques si le service qui fournit les métriques ne l'active pas par défaut.
- Prenez connaissance des Considérations.

Pour créer une CloudWatch alarme

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le volet de navigation, développez Alarmes et choisissez Toutes les alarmes.
3. Choisissez Create alarm (Créer une alarme).
4. Sur la page Specify metric and conditions (Spécifier une métrique et des conditions), sélectionnez Select metric (Sélectionner une métrique).
5. Choisissez EC2Spot, puis Fleet Request Metrics, puis sélectionnez une métrique (par exemple, TargetCapacity), puis sélectionnez Select metric.

   La page Specify metric and conditions (Spécifier les métriques et les conditions) apparaît, présentant un graphique et d'autres informations sur la métrique sélectionnée.
6. Dans Période, choisissez la période d'évaluation de l'alarme, par exemple 1 minute. Lors de l'évaluation de l'alarme, chaque période est regroupée en un point de données.

   > **Note**
   >
   > Une période plus courte crée une alarme plus sensible.

7. Sous Conditions, définissez l'alarme en définissant la condition de seuil. Par exemple, vous pouvez définir un seuil pour déclencher l'alarme lorsque la valeur de la métrique est supérieure ou égale à 80 %.
8. Sous Configuration supplémentaire, pour que les points de données génèrent une alarme, spécifiez le nombre de points de données (périodes d'évaluation) qui doivent être dans l'ALARMétat pour déclencher l'alarme, par exemple, 1 période d'évaluation ou 2 périodes d'évaluation sur 3. Cela crée une alarme qui se déclenche ALARM en cas de violation de ces nombreuses périodes consécutives. Pour plus d'informations, consultez la section Évaluation d'une alarme dans le guide de CloudWatch l'utilisateur Amazon.
9. Pour Missing data treatment (Traitement des données manquantes), choisissez l'une des options (ou conservez la valeur par défaut Treat missing data as missing (Traiter les données manquantes comme manquantes)). Pour plus d'informations, consultez la section Configuration

de la façon dont les CloudWatch alarmes traitent les données manquantes dans le guide de CloudWatch l'utilisateur Amazon.

10. Choisissez Suivant.
11. (Facultatif) Pour recevoir une notification concernant un événement de dimensionnement, dans Notification, vous pouvez choisir ou créer le SNS sujet Amazon que vous souhaitez utiliser pour recevoir des notifications. Sinon, vous pouvez supprimer la notification maintenant et en ajouter une plus tard si nécessaire.
12. Choisissez Suivant.
13. Sous Ajouter un nom et une description, entrez le nom et la description de l'alarme, puis choisissez Next.
14. Sélectionnez Créer une alarme.

Pour configurer une politique de mise à l'échelle d'étapes pour votre parc d'instances Spot (console)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot.
4. Choisissez l'onglet Auto Scaling en bas de l'écran. Si vous avez sélectionné le lien pour votre Spot Fleet, il n'y a pas d'onglet ; faites défiler la page vers le bas jusqu'à la section Auto Scaling.
5. Si la mise à l'échelle automatique n'est pas configurée, sélectionnez Configurer.
6. Utilisez le champ Scale capacity between (Mettre à l'échelle la capacité entre) pour définir les capacités minimale et maximale de votre parc. Avec les politiques de mise à l'échelle, votre flotte n'aura jamais une capacité inférieure ou supérieure aux limites fixées.
7. Sous Politiques de dimensionnement, pour Type de stratégie, choisissez Step Scaling policy.
8. À l'origine, la section Politiques de mise à l'échelle contient des politiques de mise à l'échelle nommées ScaleUp et ScaleDown. Vous pouvez compléter ces stratégies ou cliquer sur Remove policy (Supprimer la stratégie) pour les supprimer. Vous pouvez également choisir Add policy (Ajouter une stratégie).
9. Pour définir une politique, procédez comme suit :

    a. Pour Policy name (Nom de la stratégie), attribuez un nom à cette stratégie.

    b. Pour Policy Trigger, sélectionnez une alarme existante ou choisissez Create alarm pour ouvrir la CloudWatch console Amazon et créer une alarme.

c. Pour Modifier la capacité, définissez le nombre par lequel mettre à l'échelle ainsi que les limites inférieure et supérieure de l'ajustement par étapes. Vous pouvez ajouter ou supprimer un nombre spécifique d'instances ou un pourcentage de la taille de flotte existante, ou définir la flotte sur une taille exacte.

   Par exemple, pour créer une politique d'échelonnement qui augmente la capacité de la flotte de 30 %, choisissez Ajouter, entrez 30 dans le champ suivant, puis choisissez Pourcentage. Par défaut, la limite inférieure pour l'ajout d'une politique est le seuil de l'alarme et la limite supérieure est l'infini positif (+). Par défaut, la limite supérieure pour la suppression d'une politique est le seuil de l'alarme et la limite inférieure est l'infini négatif (-).

d. (Facultatif) Pour ajouter une autre étape, cliquez sur Ajouter une étape.

e. Pour le Temps de stabilisation, spécifiez une nouvelle valeur (en secondes) ou conservez la valeur par défaut.

10. Choisissez Save (Enregistrer).

Pour configurer des politiques de dimensionnement par étapes pour votre parc de spots à l'aide du AWS CLI

1. Enregistrez la demande Spot Fleet en tant que cible évolutive à l'aide de la register-scalable-targetcommande.
2. Créez une politique de dimensionnement à l'aide de la put-scaling-policycommande.
3. Créez une alarme qui déclenche la politique de dimensionnement à l'aide de la put-metric-alarmcommande.

Mise à l'échelle planifiée : adaptez votre flotte Spot selon un calendrier

La mise à l'échelle de votre parc selon un calendrier vous permet de faire évoluer votre application en fonction de l'évolution prévisible de la demande. En créant des actions planifiées, vous pouvez demander à Spot Fleet d'effectuer des activités de dimensionnement à des moments précis. Pour créer une action planifiée, vous devez spécifier un parc de spots existant, l'heure à laquelle l'activité de dimensionnement doit avoir lieu et les capacités minimale et maximale souhaitées. Les actions planifiées peuvent être configurées pour être mises à l'échelle une fois ou selon un calendrier récurrent. Si vous avez besoin de modifications, vous pouvez modifier ou supprimer des actions planifiées.

Prérequis

- Les actions planifiées ne peuvent être créées que pour les flottes de spots existantes. Vous ne pouvez pas créer d'action planifiée lorsque vous créez un parc de spots.
- La demande de parc d'instances Spot doit être de type `maintain`. La scalabilité automatique n'est pas prise en charge pour les demandes de type `request`.
- Configurez le IAMautorisations requises pour le dimensionnement automatique de Spot Fleet.
- Prenez connaissance des Considérations.

Pour créer une action planifiée unique

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot.
4. Choisissez l'onglet Scheduled Scaling en bas de l'écran. Si vous avez sélectionné le lien pour votre parc de spots, il n'y a pas d'onglet ; faites plutôt défiler la page vers le bas jusqu'à la section Scheduled Scaling.
5. Choisissez Créer une action planifiée.
6. Pour Nom, spécifiez un nouveau nom pour l'action planifiée.
7. Saisissez une valeur pour Minimum capacity (Capacité minimum), Maximum capacity (Capacité maximum), ou les deux.
8. Pour Recurrence (Récurrence), choisissez Once (Une fois).
9. (Facultatif) Choisissez la date et l'heure pour Heure de début, Heure de fin, ou les deux.
10. Sélectionnez Create (Créer).

Pour créer une action planifiée récurrente

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot.
4. Choisissez l'onglet Scheduled Scaling en bas de l'écran. Si vous avez sélectionné le lien pour votre parc de spots, il n'y a pas d'onglet ; faites plutôt défiler la page vers le bas jusqu'à la section Scheduled Scaling.
5. Pour Nom, spécifiez un nouveau nom pour l'action planifiée.

6. Saisissez une valeur pour Minimum capacity (Capacité minimum), Maximum capacity (Capacité maximum), ou les deux.
7. Pour Recurrence (Récurrence), choisissez un des calendriers prédéfinis (par exemple, Every day (Chaque jour)), ou choisissez Custom (Personnalisé) et saisissez une expression CRON. Pour plus d'informations sur les expressions cron prises en charge par le dimensionnement planifié, consultez la section Expressions cron dans le guide de EventBridge l'utilisateur Amazon.
8. (Facultatif) Choisissez la date et l'heure pour Heure de début, Heure de fin, ou les deux.
9. Choisissez Submit.

Pour modifier une action planifiée

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot.
4. Choisissez l'onglet Scheduled Scaling en bas de l'écran. Si vous avez sélectionné le lien pour votre parc de spots, il n'y a pas d'onglet ; faites plutôt défiler la page vers le bas jusqu'à la section Scheduled Scaling.
5. Sélectionnez l'action planifiée et choisissez Actions, Modifier.
6. Apportez les modifications nécessaires et choisissez Soumettre.

Pour supprimer une action planifiée

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot.
4. Choisissez l'onglet Scheduled Scaling en bas de l'écran. Si vous avez sélectionné le lien pour votre parc de spots, il n'y a pas d'onglet ; faites plutôt défiler la page vers le bas jusqu'à la section Scheduled Scaling.
5. Sélectionnez l'action planifiée et choisissez Actions, Supprimer.
6. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Pour gérer le dimensionnement planifié à l'aide du AWS CLI

Utilisez les commandes suivantes :

- put-scheduled-action
- describe-scheduled-actions
- delete-scheduled-action

Surveillez votre EC2 flotte ou repérez votre flotte

Une surveillance efficace de votre EC2 flotte ou de votre flotte ponctuelle est essentielle pour maintenir des performances optimales et garantir la fiabilité. Il existe différents outils pour vous aider à y parvenir, notamment Amazon CloudWatch et Amazon EventBridge, qui sont abordés dans cette rubrique.

Vous pouvez ainsi collecter et suivre les indicateurs, définir des alarmes et réagir automatiquement aux modifications de l'état de votre flotte. CloudWatch

Avec EventBridge, vous pouvez surveiller et répondre de manière programmatique aux événements émis par votre flotte. En définissant des règles dans EventBridge, vous pouvez automatiser les réponses à des événements spécifiques du parc, tels que la résiliation d'une instance ou les modifications de l'état du parc, améliorant ainsi votre efficacité opérationnelle.

Rubriques

- Surveillez votre EC2 flotte ou repérez votre flotte en utilisant CloudWatch
- Surveillez et répondez de manière programmatique aux événements émis par votre EC2 flotte ou Spot Fleet à l'aide d'Amazon EventBridge

Surveillez votre EC2 flotte ou repérez votre flotte en utilisant CloudWatch

Vous pouvez surveiller votre EC2 flotte ou votre flotte ponctuelle à l'aide CloudWatch des statistiques Amazon décrites dans cette section.

> **Important**
>
> Pour garantir la précision des informations, nous vous recommandons d'activer la surveillance détaillée lorsque vous utilisez ces métriques. Pour de plus amples informations, veuillez consulter Gérez la surveillance détaillée de vos EC2 instances.

Pour plus d'informations sur l'utilisation CloudWatch, consultezSurveillez vos instances à l'aide de CloudWatch.

EC2Statistiques relatives à la flotte et à la flotte ponctuelle

L'`AWS/EC2Spot`espace de noms inclut les métriques suivantes pour votre flotte, ainsi que les CloudWatch métriques pour les instances Spot de votre flotte. Pour de plus amples informations, veuillez consulter Métriques des instances.

Métrique	Description
`AvailableInstancePoolsCount`	Les pools de capacité Spot spécifiés dans la demande de flotte. Unités : nombre
`BidsSubmittedForCapacity`	Capacité pour laquelle Amazon EC2 a soumis des demandes de flotte. Unités : nombre
`EligibleInstancePoolCount`	Les pools de capacité ponctuels spécifiés dans la demande de flotte dans lesquels Amazon EC2 peut traiter les demandes. Amazon EC2 ne répond pas aux demandes dans les pools où le prix maximum que vous êtes prêt à payer pour les instances Spot est inférieur au prix Spot ou le prix Spot est supérieur au prix des instances à la demande. Unités : nombre
`FulfilledCapacity`	La capacité qu'Amazon EC2 a atteinte. Unités : nombre
`MaxPercentCapacityAllocation`	La valeur maximale de `PercentCapacityAllocation` tous les pools de flotte spécifiés dans la demande de flotte. Unités : pourcentage
`PendingCapacity`	Différence entre `TargetCapacity` et `FulfilledCapacity` .

Métrique	Description
	Unités : nombre
`PercentCapacityAllocation`	Capacité allouée pour le groupe de capacités Spot pour les dimensions spécifiées. Pour obtenir la valeur maximale enregistrée sur tous les groupes de capacités Spot, utilisez `MaxPercentCapacityAllocation` . Unités : pourcentage
`TargetCapacity`	Capacité cible de la demande de flotte. Unités : nombre
`TerminatingCapacity`	Capacité résiliée car la capacité allouée est supérieure à la capacité cible. Unités : nombre

Si l'unité de mesure d'une métrique est `Count`, la statistique la plus utile est`Average`.

EC2Dimensions de la flotte et de la flotte Spot

Pour filtrer les données de votre flotte, utilisez les dimensions suivantes.

Dimensions	Description
`AvailabilityZone`	Filtrer les données par Zone de disponibilité.
`FleetRequestId`	Filtrez les données par demande de flotte.
`InstanceType`	Filtrer les données par type d'instance.

Consultez les CloudWatch statistiques de votre EC2 flotte ou de votre flotte ponctuelle

Vous pouvez consulter les CloudWatch statistiques de votre flotte à l'aide de la CloudWatch console Amazon. Ces métriques s'affichent sous forme de graphiques de surveillance. Ces graphiques montrent les points de données si la flotte est active.

Les métriques sont d'abord regroupées par espace de noms, puis par les différentes combinaisons de dimensions au sein de chaque espace de noms. Par exemple, vous pouvez consulter toutes les mesures de flotte ou tous les groupes de métriques de flotte par ID de demande de flotte, type d'instance ou zone de disponibilité.

Pour consulter les statistiques de la flotte

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le volet de navigation, développez Metrics, puis sélectionnez All metrics.
3. Choisissez l'espace de noms EC2Spot.

> **Note**
>
> Si l'espace de noms EC2Spot n'est pas affiché, cela s'explique par deux raisons. Vous n'avez jamais utilisé EC2 Fleet ou Spot Fleet dans la région. Seuls les AWS services que vous utilisez envoient des statistiques à Amazon. CloudWatch Ou, si vous avez utilisé EC2 Fleet ou Spot Fleet dans la région, mais pas ces deux dernières semaines, l'espace de noms n'apparaît pas.

4. Pour filtrer les mesures par dimension, choisissez l'une des options suivantes :
   - Métriques des demandes de flotte — Regrouper par demande de flotte
   - Par zone de disponibilité — Regroupez par demande de flotte et zone de disponibilité
   - Par type d'instance — Regroupez par demande de flotte et type d'instance
   - Par zone de disponibilité ou type d'instance : groupez par demande de flotte, zone de disponibilité et type d'instance
5. Pour afficher les données d'une métrique, cochez la case en regard de la métrique.

Surveillez et répondez de manière programmatique aux événements émis par votre EC2 flotte ou Spot Fleet à l'aide d'Amazon EventBridge

Lorsque l'état d'une EC2 flotte ou d'une flotte ponctuelle change, une notification est émise. La notification est mise à disposition sous la forme d'un événement envoyé à Amazon EventBridge (anciennement Amazon CloudWatch Events). Les événements sont générés dans la mesure du possible.

Vous pouvez utiliser Amazon EventBridge pour créer des règles qui déclenchent des actions programmatiques en réponse à un événement. Par exemple, vous pouvez créer deux EventBridge règles : l'une déclenchée lorsqu'un état de flotte change, et l'autre déclenchée lorsqu'une instance du parc est résiliée. Dans cet exemple, vous pouvez configurer la première règle de telle sorte que, si l'état de la flotte change, la règle invoque un SNS sujet et vous envoie une notification par e-mail. Vous pouvez configurer la deuxième règle de telle sorte que, si une instance du parc est résiliée, la règle invoque une fonction Lambda pour lancer une nouvelle instance.

> **Note**
>
> Seuls les parcs de type `maintain` et `request` émettent des événements. Les parcs de type `instant` n'émettent pas d'événements car elles envoient des demandes uniques synchrones et l'état du parc est connu immédiatement dans la réponse. Pour utiliser Amazon EventBridge afin de surveiller les événements liés à la flotte, le type de demande doit être `maintain` ou`request`.

Pour obtenir des instructions sur la façon de décrire l'historique des événements d'une flotte, voirDécrivez l'historique des événements de votre EC2 flotte.

Rubriques

- Créez des EventBridge règles Amazon pour surveiller les événements EC2 de Fleet ou Spot Fleet
- EC2Types d'événements liés à la flotte
- Types d'événements de parc d'instances Spot

Créez des EventBridge règles Amazon pour surveiller les événements EC2 de Fleet ou Spot Fleet

Lorsqu'une notification de changement d'état est émise pour une EC2 flotte ou une flotte ponctuelle, elle est envoyée sous forme d'événement à Amazon EventBridge sous forme de JSON fichier. S'il EventBridge détecte un modèle d'événement correspondant à un modèle défini dans une règle, EventBridge invoque la ou les cibles spécifiées dans la règle.

Vous pouvez écrire EventBridge des règles pour automatiser les actions en fonction de modèles d'événements correspondants.

Les champs suivants de l'événement constituent le modèle d'événement défini dans la règle :

`"source": "aws.ec2fleet"`

Indique que l'événement provient de EC2 Fleet.

`"detail-type": "EC2 Fleet State Change"`

Identifie le type d'événement.

`"detail": { "sub-type": "submitted" }`

Identifie le sous-type d'événement.

Pour obtenir la liste des événements de EC2 Fleet et de Spot Fleet ainsi que des exemples de données d'événements, voir EC2Types d'événements liés à la flotte etTypes d'événements de parc d'instances Spot .

Exemples

- Création d'une EventBridge règle pour envoyer une notification
- Création d'une EventBridge règle pour déclencher une fonction Lambda

Création d'une EventBridge règle pour envoyer une notification

L'exemple suivant crée une EventBridge règle pour envoyer un e-mail, un SMS ou une notification push mobile chaque fois qu'Amazon EC2 émet une notification de modification de l'état de la EC2 flotte. Le signal de cet exemple est émis en tant qu'événement de `EC2 Fleet State Change`, ce qui déclenche l'action définie par la règle.

Prérequis

Avant de créer la EventBridge règle, vous devez créer le SNS sujet Amazon pour l'e-mail, le message texte ou la notification push mobile.

Pour créer une EventBridge règle permettant d'envoyer une notification lorsqu'un état EC2 de flotte change

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Choisissez Créer une règle.
3. Pour Define rule detail (Définir les détails de la règle), procédez comme suit :

    a. Entrez un nom et éventuellement une description pour la règle.

Une règle ne peut pas avoir le même nom qu'une autre règle de la même région et sur le même bus d'événement.

b. Pour Event bus (Bus d'événement), choisissez default (défaut). Lorsqu'un AWS service de votre compte génère un événement, celui-ci est toujours redirigé vers le bus d'événements par défaut de votre compte.

c. Pour Type de règle, choisissez Règle avec un modèle d'événement.

d. Choisissez Suivant.

4. Pour Build event pattern (Créer un modèle d'événement), procédez comme suit :

a. Dans Source de l'événement, choisissez AWS des événements ou des événements EventBridge partenaires.

b. Pour le Event pattern (Modèle d'événement), dans cet exemple, vous spécifierez le modèle d'événement suivant pour correspondre à l'événement `EC2 Fleet Instance Change`.

```
{
 "source": ["aws.ec2fleet"],
 "detail-type": ["EC2 Fleet Instance Change"]
}
```

Pour ajouter le modèle d'événement, vous pouvez soit utiliser un modèle en choisissant Formulaire de modèle d'événement, soit spécifier votre propre modèle en choisissant Modèle personnalisé (JSONéditeur), comme suit :

i. Pour utiliser un modèle pour créer le modèle d'événement, procédez comme suit :

A. Sélectionnez Event pattern form (Formulaire de modèle d'événement).

B. Pour Event source (Origine de l'événement), choisissez AWS services (Services).

C. Pour AWS Service, choisissez EC2Fleet.

D. Pour Type d'événement, choisissez EC2Fleet Instance Change.

E. Pour personnaliser le modèle, choisissez Edit pattern (Modifier le modèle) et apportez vos modifications pour correspondre à l'exemple de modèle d'événement.

ii. (Alternative) Pour spécifier un modèle d'événement personnalisé, procédez comme suit :

A. Choisissez Motif personnalisé (JSONéditeur).

B. Dans la boîte de dialogue Event pattern (Modèle d'événement), ajoutez le modèle d'événement pour cet exemple.

c. Choisissez Next (Suivant).

5. Pour Select target(s) (Sélectionner la ou les cibles), procédez comme suit :

   a. Pour Types de cibles, choisissez service AWS .

   b. Pour Sélectionner une cible, choisissez le SNSsujet pour envoyer un e-mail, un SMS ou une notification push mobile lorsque l'événement se produit.

   c. Pour Topic (Rubrique), sélectionnez une rubrique existante. Vous devez d'abord créer un SNS sujet Amazon à l'aide de la SNS console Amazon. Pour plus d'informations, consultez la section Utilisation d'Amazon SNS pour la messagerie application-to-person (A2P) dans le manuel du développeur Amazon Simple Notification Service.

   d. (Facultatif) Sous Additional settings (Paramètres supplémentaires), vous pouvez configurer des paramètres supplémentaires. Pour plus d'informations, consultez la section Création de EventBridge règles Amazon réagissant aux événements (étape 16) dans le guide de EventBridge l'utilisateur Amazon.

   e. Choisissez Suivant.

6. (Facultatif) Pour Tags (Identifications), vous pouvez également attribuer une ou plusieurs identifications à votre règle, puis choisir Next (Suivant).

7. Pour Review and create (Vérifier et créer), procédez comme suit :

   a. Consultez les détails de la règle et modifiez-les si nécessaire.

   b. Choisissez Créer une règle.

Pour plus d'informations, consultez les EventBridge règles Amazon et les modèles d' EventBridge événements Amazon dans le guide de EventBridge l'utilisateur Amazon

Création d'une EventBridge règle pour déclencher une fonction Lambda

L'exemple suivant crée une EventBridge règle pour déclencher une fonction Lambda chaque fois qu'Amazon EC2 émet une notification de modification d'instance EC2 Fleet lors du lancement d'une instance. Le signal de cet exemple est émis en tant qu'événement `EC2 Fleet Instance Change`, de sous-type `launched`, ce qui déclenche l'action définie par la règle.

Avant de créer la EventBridge règle, vous devez créer la fonction Lambda.

Pour créer la fonction Lambda à utiliser dans la règle EventBridge

1. Ouvrez la AWS Lambda console à l'adresse https://console.aws.amazon.com/lambda/.
2. Sélectionnez Créer une fonction.
3. Saisissez un nom pour votre fonction, configurez le code, puis sélectionnez Create function (Créer une fonction).

   Pour plus d'informations sur l'utilisation de Lambda, consultez Créer une fonction Lambda avec la console dans le AWS Lambda Guide du développeur.

Pour créer une EventBridge règle permettant de déclencher une fonction Lambda lorsqu'une instance d'un EC2 Fleet change d'état

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Choisissez Créer une règle.
3. Pour Define rule detail (Définir les détails de la règle), procédez comme suit :

   a. Entrez un nom et éventuellement une description pour la règle.

      Une règle ne peut pas avoir le même nom qu'une autre règle de la même région et sur le même bus d'événement.

   b. Pour Event bus (Bus d'événement), choisissez default (défaut). Lorsqu'un AWS service de votre compte génère un événement, celui-ci est toujours redirigé vers le bus d'événements par défaut de votre compte.

   c. Pour Type de règle, choisissez Règle avec un modèle d'événement.

   d. Choisissez Suivant.
4. Pour Build event pattern (Créer un modèle d'événement), procédez comme suit :

   a. Dans Source de l'événement, choisissez AWS des événements ou des événements EventBridge partenaires.

   b. Pour Event pattern (Modèle d'événement), pour cet exemple, vous allez spécifier le modèle d'événement suivant pour correspondre à l'événement `EC2 Fleet Instance Change` et au sous-type `launched`.

```
{
 "source": ["aws.ec2fleet"],
 "detail-type": ["EC2 Fleet Instance Change"],
```

```
 "detail": {
   "sub-type": ["launched"]
}
```

Pour ajouter le modèle d'événement, vous pouvez soit utiliser un modèle en choisissant Formulaire de modèle d'événement, soit spécifier votre propre modèle en choisissant Modèle personnalisé (JSONéditeur), comme suit :

i. Pour utiliser un modèle pour créer le modèle d'événement, procédez comme suit :

A. Sélectionnez Event pattern form (Formulaire de modèle d'événement).

B. Pour Event source (Origine de l'événement), choisissez AWS services (Services).

C. Pour AWS Service, choisissez EC2Fleet.

D. Pour Type d'événement, choisissez EC2Fleet Instance Change.

E. Choisissez Edit pattern (Modifier le modèle), et ajoutez `"detail": {"sub-type": ["launched"]` pour correspondre à l'exemple de modèle d'événement. Pour un JSON format correct, insérez une virgule (`,`) après le crochet précédent (`]`).

ii. (Alternative) Pour spécifier un modèle d'événement personnalisé, procédez comme suit :

A. Choisissez Motif personnalisé (JSONéditeur).

B. Dans la boîte de dialogue Event pattern (Modèle d'événement), ajoutez le modèle d'événement pour cet exemple.

c. Choisissez Next (Suivant).

5. Pour Select target(s) (Sélectionner la ou les cibles), procédez comme suit :

a. Pour Types de cibles, choisissez service AWS .

b. Pour Sélectionner une cible, choisissez le SNSsujet pour envoyer un e-mail, un SMS ou une notification push mobile lorsque l'événement se produit.

c. Pour Topic (Rubrique), sélectionnez Lambda function (Fonction Lambda) et, pour Function (Fonction), sélectionnez la fonction que vous avez créée pour répondre lorsque l'événement se produit.

d. (Facultatif) Sous Additional settings (Paramètres supplémentaires), vous pouvez configurer des paramètres supplémentaires. Pour plus d'informations, consultez la section Création

de EventBridge règles Amazon réagissant aux événements (étape 16) dans le guide de EventBridge l'utilisateur Amazon.

e. Choisissez Suivant.

6. (Facultatif) Pour Tags (Identifications), vous pouvez également attribuer une ou plusieurs identifications à votre règle, puis choisir Next (Suivant).
7. Pour Review and create (Vérifier et créer), procédez comme suit :

   a. Consultez les détails de la règle et modifiez-les si nécessaire.

   b. Choisissez Créer une règle.

Pour un didacticiel sur la création d'une fonction Lambda et d'une EventBridge règle qui exécute la fonction Lambda, voir Tutoriel : enregistrer l'état d'une EC2 instance Amazon EventBridge à l'aide du manuel du développeur.AWS Lambda

EC2Types d'événements liés à la flotte

Il existe cinq types d'événements EC2 liés à la flotte. Pour chaque type d'événement, il existe plusieurs sous-types.

Types d'événements

- EC2Modification de l'état de la flotte
- EC2Demande de modification de l'instance Fleet Spot
- EC2Changement d'instance de flotte
- EC2Informations sur le parc
- EC2Erreur de flotte

EC2Modification de l'état de la flotte

EC2Fleet envoie un `EC2 Fleet State Change` événement à Amazon EventBridge lorsqu'une EC2 flotte change d'état.

Voici un exemple de données pour cet événement.

```
{
    "version": "0",
    "id": "715ed6b3-b8fc-27fe-fad6-528c7b8bf8a2",
```

```
    "detail-type": "EC2 Fleet State Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:20Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
        "sub-type": "active"
    }
}
```

Les valeurs possibles pour `sub-type` sont :

`active`

La demande EC2 Fleet a été validée et Amazon EC2 essaie de maintenir le nombre cible d'instances en cours d'exécution.

`deleted`

La demande EC2 Fleet est supprimée et aucune instance n'est en cours d'exécution. La EC2 flotte sera supprimée deux jours après la résiliation de ses instances.

`deleted_running`

La demande EC2 Fleet est supprimée et ne lance pas d'instances supplémentaires. Ses instances existantes continuent de s'exécuter jusqu'à ce qu'elles soient interrompues ou mises hors service. La demande conserve cet état jusqu'à ce que toutes les instances soient interrompues ou mises hors service.

`deleted_terminating`

La demande EC2 Fleet est supprimée et ses instances sont résiliées. La demande conserve cet état jusqu'à ce que toutes les instances soient mises hors service.

`expired`

La demande EC2 de flotte a expiré. Si la demande a été créée avec un ensemble `TerminateInstancesWithExpiration`, un événement `terminated` ultérieur indique que les instances sont résiliées.

`modify_in_progress`

La demande EC2 de flotte est en cours de modification. La demande conserve cet état jusqu'à ce que la modification soit totalement traitée.

`modify_succeeded`

La demande EC2 de flotte a été modifiée.

`submitted`

La demande EC2 Fleet est en cours d'évaluation et Amazon EC2 se prépare à lancer le nombre cible d'instances.

`progress`

La demande de EC2 flotte est en cours de traitement.

EC2Demande de modification de l'instance Fleet Spot

EC2Fleet envoie un `EC2 Fleet Spot Instance Request Change` événement à Amazon EventBridge lorsqu'une demande d'instance Spot change d'état dans la flotte.

Voici un exemple de données pour cet événement.

```
{
    "version": "0",
    "id": "19331f74-bf4b-a3dd-0f1b-ddb1422032b9",
    "detail-type": "EC2 Fleet Spot Instance Request Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:05Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/
fleet-83fd4e48-552a-40ef-9532-82a3acca5f10"
    ],
    "detail": {
        "spot-instance-request-id": "sir-rmqske6h",
        "description": "SpotInstanceRequestId sir-rmqske6h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
```

```
}
```

Les valeurs possibles pour `sub-type` sont :

`active`

La demande d'instance Spot a été exécutée et est associée à une instance Spot.

`cancelled`

Vous avez annulé la demande d'instance Spot ou la demande d'instance Spot a expiré.

`disabled`

Vous avez arrêté l'instance Spot.

`submitted`

La demande d'Instance Spot est soumise.

EC2Changement d'instance de flotte

EC2Fleet envoie un `EC2 Fleet Instance Change` événement à Amazon EventBridge lorsqu'une instance de la flotte change d'état.

Voici un exemple de données pour cet événement.

```
{
    "version": "0",
    "id": "542ce428-c8f1-0608-c015-e8ed6522c5bc",
    "detail-type": "EC2 Fleet Instance Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:23Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
        "instance-id": "i-0c594155dd5ff1829",
        "description": "{\"instanceType\":\"c5.large\",\"image\":\"ami-6057e21a\",
\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":\"us-east-1d\"}",
        "sub-type": "launched"
```

```
    }
}
```

Les valeurs possibles pour `sub-type` sont :

`launched`

Une nouvelle instance a été lancée.

`terminated`

L'instance a été résiliée.

`termination_notified`

Une notification de résiliation d'instance a été envoyée lorsqu'une instance Spot a été résiliée par Amazon EC2 pendant la réduction, lorsque la capacité cible du parc a été modifiée à la baisse, par exemple, d'une capacité cible de 4 à une capacité cible de 3.

EC2Informations sur le parc

EC2Fleet envoie un `EC2 Fleet Information` événement à Amazon EventBridge en cas d'erreur lors de l'expédition. L'événement d'information n'empêche pas la flotte de tenter d'atteindre sa capacité cible.

Voici un exemple de données pour cet événement.

```
{
    "version": "0",
    "id": "76529817-d605-4571-7224-d36cc1b2c0c4",
    "detail-type": "EC2 Fleet Information",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T08:17:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-8becf5fe-
bb9e-415d-8f54-3fa5a8628b91"
    ],
    "detail": {
        "description": "c4.xlarge, ami-0947d2ba12ee1ff75, Linux/UNIX, us-east-1a,
 Spot price in either SpotFleetRequestConfigData or SpotFleetLaunchSpecification or
 LaunchTemplate or LaunchTemplateOverrides is less than Spot market price $0.0619",
```

```
        "sub-type": "launchSpecUnusable"
    }
}
```

Les valeurs possibles pour `sub-type` sont :

`fleetProgressHalted`

Le prix dans chaque spécification de lancement n'est pas valide car il est inférieur au prix Spot (toutes les spécifications de lancement ont produit des événements `launchSpecUnusable`). Une spécification de lancement peut devenir valide si le prix Spot change.

`launchSpecTemporarilyBlacklisted`

La configuration n'est pas valide et plusieurs tentatives de lancement d'instances ont échoué. Pour en savoir plus, consultez la description de l'événement.

`launchSpecUnusable`

Le prix d'une spécification de lancement n'est pas valide car il est inférieur au prix Spot.

`registerWithLoadBalancersFailed`

Une tentative d'enregistrement des instances avec des équilibreurs de charge a échoué. Pour en savoir plus, consultez la description de l'événement.

EC2Erreur de flotte

EC2Fleet envoie un `EC2 Fleet Error` événement à Amazon EventBridge en cas d'erreur lors de l'expédition. L'événement d'erreur empêche la flotte de tenter d'atteindre sa capacité cible.

Voici un exemple de données pour cet événement.

```
{
    "version": "0",
    "id": "69849a22-6d0f-d4ce-602b-b47c1c98240e",
    "detail-type": "EC2 Fleet Error",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-10-07T01:44:24Z",
    "region": "us-east-1",
    "resources": [
```

```
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-9bb19bc6-60d3-4fd2-ae47-
d33e68eafa08"
    ],
    "detail": {
        "description": "m3.large, ami-00068cd7555f543d5, Linux/UNIX: IPv6 is not
 supported for the instance type 'm3.large'. ",
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

Les valeurs possibles pour `sub-type` sont :

`iamFleetRoleInvalid`

La EC2 flotte ne dispose pas des autorisations requises pour lancer ou mettre fin à une instance.

`allLaunchSpecsTemporarilyBlacklisted`

Aucune des configurations n'est valide et plusieurs tentatives de lancement d'instances ont échoué. Pour en savoir plus, consultez la description de l'événement.

`spotInstanceCountLimitExceeded`

Vous avez atteint la limite du nombre d'instances Spot que vous pouvez lancer.

`spotFleetRequestConfigurationInvalid`

La configuration n'est pas valide. Pour en savoir plus, consultez la description de l'événement.

Types d'événements de parc d'instances Spot

Il existe cinq types d'événements de parc d'instances Spot . Pour chaque type d'événement, il existe plusieurs sous-types.

Types d'événements

- EC2Changement d'état du parc de véhicules Spot
- EC2Modification de la demande d'instance Spot Fleet Spot
- EC2Changement d'instance de Spot Fleet
- EC2Informations sur la flotte Spot
- EC2Repérez une erreur de flotte

EC2Changement d'état du parc de véhicules Spot

Spot Fleet envoie un `EC2 Spot Fleet State Change` événement à Amazon EventBridge lorsqu'un Spot Fleet change d'état.

Voici un exemple de données pour cet événement.

```
{
    "version": "0",
    "id": "d1af1091-6cc3-2e24-203a-3b870e455d5b",
    "detail-type": "EC2 Spot Fleet State Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:57:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-4b6d274d-0cea-4b2c-
b3be-9dc627ad1f55"
    ],
    "detail": {
        "sub-type": "submitted"
    }
}
```

Les valeurs possibles pour `sub-type` sont :

`active`

La demande Spot Fleet a été validée et Amazon EC2 essaie de maintenir le nombre cible d'instances en cours d'exécution.

`cancelled`

La demande de parc d'instances Spot est annulée et n'a aucune instance en cours d'exécution. Le parc d'instances sera supprimé deux jours après la résiliation de ses instances.

`cancelled_running`

La demande de parc d'instances Spot est annulée et ne lance pas d'instances supplémentaires. Ses instances existantes continuent de s'exécuter jusqu'à ce qu'elles soient interrompues ou mises hors service. La demande conserve cet état jusqu'à ce que toutes les instances soient interrompues ou mises hors service.

`cancelled_terminating`

La demande de parc d'instances Spot est annulée et ses instances sont résiliées. La demande conserve cet état jusqu'à ce que toutes les instances soient mises hors service.

`expired`

La demande de parc d'instances Spot a expiré. Si la demande a été créée avec un ensemble `TerminateInstancesWithExpiration`, un événement `terminated` ultérieur indique que les instances sont résiliées.

`modify_in_progress`

La demande de parc d'instances Spot est en cours de modification. La demande conserve cet état jusqu'à ce que la modification soit totalement traitée.

`modify_succeeded`

La demande de parc d'instances Spot a été modifiée.

`submitted`

La demande Spot Fleet est en cours d'évaluation et Amazon EC2 se prépare à lancer le nombre cible d'instances.

`progress`

La demande de parc d'instances Spot est en cours d'exécution.

EC2Modification de la demande d'instance Spot Fleet Spot

Spot Fleet envoie un `EC2 Spot Fleet Spot Instance Request Change` événement à Amazon EventBridge lorsqu'une demande d'instance Spot change d'état dans le parc.

Voici un exemple de données pour cet événement.

```
{
    "version": "0",
    "id": "cd141ef0-14af-d670-a71d-fe46e9971bd2",
    "detail-type": "EC2 Spot Fleet Spot Instance Request Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:53:21Z",
    "region": "us-east-1",
    "resources": [
```

```
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-
a98d2133-941a-47dc-8b03-0f94c6852ad1"
    ],
    "detail": {
        "spot-instance-request-id": "sir-a2w9gc5h",
        "description": "SpotInstanceRequestId sir-a2w9gc5h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

Les valeurs possibles pour `sub-type` sont :

`active`

La demande d'instance Spot a été exécutée et est associée à une instance Spot.

`cancelled`

Vous avez annulé la demande d'instance Spot ou la demande d'instance Spot a expiré.

`disabled`

Vous avez arrêté l'instance Spot.

`submitted`

La demande d'Instance Spot est soumise.

EC2Changement d'instance de Spot Fleet

Spot Fleet envoie un `EC2 Spot Fleet Instance Change` événement à Amazon EventBridge lorsqu'une instance du parc change d'état.

Voici un exemple de données pour cet événement.

```
{
    "version": "0",
    "id": "11591686-5bd7-bbaa-eb40-d46529c2710f",
    "detail-type": "EC2 Spot Fleet Instance Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T07:25:02Z",
    "region": "us-east-1",
    "resources": [
```

```
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-c8a764a4-bedc-4b62-
af9c-0095e6e3ba61"
    ],
    "detail": {
        "instance-id": "i-08b90df1e09c30c9b",
        "description": "{\"instanceType\":\"r4.2xlarge\",\"image\":
\"ami-032930428bf1abbff\",\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":
\"us-east-1a\"}",
        "sub-type": "launched"
    }
}
```

Les valeurs possibles pour `sub-type` sont :

`launched`

Une nouvelle instance a été lancée.

`terminated`

L'instance a été résiliée.

`termination_notified`

Une notification de résiliation d'instance a été envoyée lorsqu'une instance Spot a été résiliée par Amazon EC2 pendant la réduction, lorsque la capacité cible du parc a été modifiée à la baisse, par exemple, d'une capacité cible de 4 à une capacité cible de 3.

EC2Informations sur la flotte Spot

Spot Fleet envoie un `EC2 Spot Fleet Information` événement à Amazon EventBridge en cas d'erreur lors de l'expédition. L'événement d'information n'empêche pas la flotte de tenter d'atteindre sa capacité cible.

Voici un exemple de données pour cet événement.

```
{
    "version": "0",
    "id": "73a60f70-3409-a66c-635c-7f66c5f5b669",
    "detail-type": "EC2 Spot Fleet Information",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-08T20:56:12Z",
```

```
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-2531ea06-
af18-4647-8757-7d69c94971b1"
    ],
    "detail": {
        "description": "r3.8xlarge, ami-032930428bf1abbff, Linux/UNIX, us-east-1a, Spot
 bid price is less than Spot market price $0.5291",
        "sub-type": "launchSpecUnusable"
    }
}
```

Les valeurs possibles pour `sub-type` sont :

`fleetProgressHalted`

Le prix dans chaque spécification de lancement n'est pas valide car il est inférieur au prix Spot (toutes les spécifications de lancement ont produit des événements `launchSpecUnusable`). Une spécification de lancement peut devenir valide si le prix Spot change.

`launchSpecTemporarilyBlacklisted`

La configuration n'est pas valide et plusieurs tentatives de lancement d'instances ont échoué. Pour en savoir plus, consultez la description de l'événement.

`launchSpecUnusable`

Le prix d'une spécification de lancement n'est pas valide car il est inférieur au prix Spot.

`registerWithLoadBalancersFailed`

Une tentative d'enregistrement des instances avec des équilibreurs de charge a échoué. Pour en savoir plus, consultez la description de l'événement.

EC2Repérez une erreur de flotte

Spot Fleet envoie un `EC2 Spot Fleet Error` événement à Amazon EventBridge en cas d'erreur lors de l'expédition. L'événement d'erreur empêche la flotte de tenter d'atteindre sa capacité cible.

Voici un exemple de données pour cet événement.

```
{
    "version": "0",
    "id": "10adc4e7-675c-643e-125c-5bfa1b1ba5d2",
```

```
    "detail-type": "EC2 Spot Fleet Error",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T06:56:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/
sfr-38725d30-25f1-4f30-83ce-2907c56dba17"
    ],
    "detail": {
        "description": "r4.2xlarge, ami-032930428bf1abbff, Linux/UNIX: The
 associatePublicIPAddress parameter can only be specified for the network interface
 with DeviceIndex 0. ",
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

Les valeurs possibles pour `sub-type` sont :

`iamFleetRoleInvalid`

Le parc d'instances Spot ne dispose pas des autorisations requises pour lancer ou résilier une instance.

`allLaunchSpecsTemporarilyBlacklisted`

Aucune des configurations n'est valide et plusieurs tentatives de lancement d'instances ont échoué. Pour en savoir plus, consultez la description de l'événement.

`spotInstanceCountLimitExceeded`

Vous avez atteint la limite du nombre d'instances Spot que vous pouvez lancer.

`spotFleetRequestConfigurationInvalid`

La configuration n'est pas valide. Pour en savoir plus, consultez la description de l'événement.

Tutoriels pour EC2 Fleet

Il existe différentes manières de configurer une EC2 flotte. La configuration que vous choisissez dépend de votre cas d'utilisation spécifique.

Les didacticiels suivants couvrent certains des cas d'utilisation possibles et fournissent les tâches nécessaires à leur mise en œuvre.

Cas d'utilisation	Lien vers le didacticiel
Utilisez la pondération des instances pour gérer la disponibilité et les performances de votre EC2 flotte. Avec la pondération des instances, vous attribuez une pondération à chaque type d'instance de votre EC2 flotte pour représenter leur capacité de calcul et leurs performances les unes par rapport aux autres. Sur la base des pondérations, le parc peut utiliser n'importe quelle combinaison des types d'instances spécifiés, à condition qu'il puisse atteindre la capacité cible souhaitée.	Tutoriel : Configurer EC2 Fleet pour utiliser la pondération des instances
Utilisez la capacité à la demande pour garantir la disponibilité pendant les périodes de pointe, tout en bénéficiant d'une capacité ponctuelle supplémentaire à moindre coût. Configurez votre EC2 flotte pour utiliser les instances à la demande comme capacité principale afin de garantir la disponibilité de la capacité pendant les périodes de pointe. En outre, allouez une partie de la capacité aux instances Spot pour bénéficier de tarifs réduits, tout en gardant à l'esprit que les instances Spot peuvent être interrompues si Amazon EC2 a besoin de récupérer la capacité.	Tutoriel : configurer EC2 Fleet pour utiliser les instances à la demande comme capacité principale
Utilisez les réservations de capacité pour réserver de la capacité de calcul pour vos instances à la demande. Configurez votre EC2 flotte pour utiliser les réservations `targeted` de capacité en premier lors du lancement d'instances à la demande. Si	Tutoriel : configurer EC2 Fleet pour lancer des instances à la demande à l'aide de réservations de capacité ciblées

Cas d'utilisation	Lien vers le didacticiel
vous avez des exigences de capacité strictes et que vous exécutez des charges de travail critiques qui nécessitent un certain niveau de garantie de capacité à long ou à court terme, nous vous recommandons de créer une réservation de capacité afin de vous assurer de toujours avoir accès aux EC2 capacités Amazon quand vous en avez besoin, aussi longtemps que vous en avez besoin.	
Utilisez les blocs de capacité pour réserver des GPU instances très recherchées pour vos charges de travail ML. Configurez votre EC2 flotte pour lancer des instances dans des blocs de capacité.	Tutoriel : configurez votre EC2 flotte pour lancer des instances dans des blocs de capacité

Tutoriel : Configurer EC2 Fleet pour utiliser la pondération des instances

Ce didacticiel utilise une société fictive appelée Example Corp pour illustrer le processus de demande d'une EC2 flotte à l'aide de la pondération des instances.

Objectif

Example Corp, une société pharmaceutique, souhaite utiliser la puissance de calcul d'Amazon EC2 pour sélectionner des composés chimiques susceptibles d'être utilisés pour lutter contre le cancer.

Planification

Example Corp commence par examiner les bonnes pratiques en matière d'instances Spot. Example Corp détermine ensuite les besoins de sa EC2 flotte.

Types d'instances

Example Corp possède une application gourmande en calcul et en mémoire qui fonctionne le mieux avec au moins 60 Go de mémoire et huit unités virtuelles CPUs ()vCPUs. L'entreprise souhaite

optimiser ces ressources pour l'application au prix le plus bas possible. Example Corp décide que l'un des types d'EC2instances suivants répondrait à ses besoins :

Type d'instance	Mémoire (Gio)	vCPUs
r3.2xlarge	61	8
r3.4xlarge	122	16
r3.8xlarge	244	32

Capacité cible en unités

Avec la pondération des instances, la capacité cible peut être égale à un nombre d'instances (valeur par défaut) ou à une combinaison de facteurs tels que les cœurs (vCPUs), la mémoire (GiBs) et le stockage (GBs). En considérant la base de son application (60 Go RAM et huitvCPUs) comme une seule unité, Example Corp décide que 20 fois cette quantité répondrait à ses besoins. L'entreprise fixe donc la capacité cible de sa demande de EC2 flotte à 20 unités.

Pondérations d'instance

Après avoir déterminé sa capacité cible, Example Corp calcule ses pondérations d'instance. Pour calculer la pondération de chaque type d'instance, l'entreprise détermine les unités de chaque type d'instance nécessaires pour atteindre la capacité cible de la façon suivante :

- r3.2xlarge (61,0 Go, 8vCPUs) = 1 unité de 20
- r3.4xlarge (122,0 Go, 16vCPUs) = 2 unités de 20
- r3.8xlarge (244,0 Go, 32vCPUs) = 4 unités de 20

Par conséquent, Example Corp attribue des poids d'instance de 1, 2 et 4 aux configurations de lancement respectives dans sa demande de EC2 flotte.

Prix par heure d'unité

Example Corp utilise le prix à la Demande par heure d'instance comme point de départ de son prix. Elle peut également utiliser les prix Spot récents ou une combinaison des deux. Pour calculer le

prix par heure d'unité, elle divise le prix de départ basé sur l'heure d'instance par la pondération. Exemples :

Type d'instance	Prix à la Demande	Pondération de l'instance	Prix par heure d'unité
r3,2 xLarge	0,7 USD	1	0,7 USD
r3,4 xLarge	1,4 USD	2	0,7 USD
r3,8 xLarge	2.8 USD	4	0,7 USD

Example Corp peut utiliser un prix global par heure d'unité s'élevant à 0,7 USD et rester concurrentielle pour les trois types d'instance. Elle peut également utiliser un prix global par heure d'unité s'élevant à 0,7 USD et un prix spécifique par heure d'unité de 0,9 USD dans la spécification de lancement du type d'instance `r3.8xlarge`.

Vérifier les autorisations

Avant de créer une EC2 flotte, Example Corp vérifie qu'elle possède un IAM rôle doté des autorisations requises. Pour de plus amples informations, veuillez consulter EC2Prérequis relatifs à la flotte.

Créer un modèle de lancement

Ensuite, Example Corp crée un modèle de lancement. L'ID de modèle de lancement est utilisé à l'étape suivante. Pour de plus amples informations, veuillez consulter Création d'un modèle de EC2 lancement Amazon.

Créez la EC2 flotte

Example Corp crée un fichier avec la configuration suivante pour sa EC2 flotte. `config.json` Dans l'exemple suivant, remplacez les identificateurs de ressources par vos propres identificateurs de ressources.

```
{
```

```
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "r3.2xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 1
                },
                {
                    "InstanceType": "r3.4xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 2
                },
                {
                    "InstanceType": "r3.8xlarge",
                    "MaxPrice": "0.90",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 4
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Example Corp crée la EC2 flotte à l'aide de la commande create-fleet suivante.

```
aws ec2 create-fleet --cli-input-json file://config.json
```

Pour de plus amples informations, veuillez consulter Création d'une EC2 flotte.

Exécution

La stratégie d'allocation détermine de quels groupes de capacités Spot sont issues vos instances Spot.

Avec la stratégie `lowest-price` (qui est la stratégie par défaut), les Instances Spot sont issues du groupe ayant le prix par unité le plus bas au moment de l'exécution. Pour fournir 20 unités de capacité, la EC2 flotte lance 20 `r3.2xlarge` instances (20 divisées par 1), 10 `r3.4xlarge` instances (20 divisées par 2) ou 5 `r3.8xlarge` instances (20 divisées par 4).

Si Example Corp avait utilisé la stratégie `diversified`, les Instances Spot auraient été issues des trois groupes. La EC2 flotte lancerait 6 `r3.2xlarge` instances (qui fournissent 6 unités), 3 `r3.4xlarge` instances (qui fournissent 6 unités) et 2 `r3.8xlarge` instances (qui fournissent 8 unités), pour un total de 20 unités.

Tutoriel : configurer EC2 Fleet pour utiliser les instances à la demande comme capacité principale

Ce didacticiel utilise une société fictive appelée ABC Online pour illustrer le processus de demande d'une EC2 flotte avec la capacité principale à la demande et une capacité ponctuelle si elle est disponible.

Objectif

ABCOnline, une société de livraison de restaurants, vise à fournir la EC2 capacité Amazon à différents types d'EC2instances et options d'achat afin d'atteindre l'échelle, les performances et les coûts souhaités.

Plan

ABCOnline nécessite une capacité fixe pour gérer les périodes de pointe, mais souhaite bénéficier d'une capacité supplémentaire à moindre coût. L'entreprise détermine les exigences suivantes pour sa EC2 flotte :

- Capacité d'instance à la demande — ABC Online nécessite 15 instances à la demande pour garantir leur capacité à gérer le trafic en période de pointe.
- Capacité des instances ponctuelles : pour améliorer les performances, mais à un prix inférieur, ABC Online prévoit de fournir 5 instances ponctuelles.

Vérifier les autorisations

Avant de créer une EC2 flotte, ABC Online vérifie qu'elle possède un IAM rôle doté des autorisations requises. Pour de plus amples informations, veuillez consulter EC2Prérequis relatifs à la flotte.

Créer un modèle de lancement

ABCOnline crée ensuite un modèle de lancement. L'ID de modèle de lancement est utilisé à l'étape suivante. Pour de plus amples informations, veuillez consulter Création d'un modèle de EC2 lancement Amazon.

Créez la EC2 flotte

ABCOnline crée un fichier`config.json`, avec la configuration suivante pour sa EC2 flotte. Dans l'exemple suivant, remplacez les identificateurs de ressources par vos propres identificateurs de ressources.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "2"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity":15,
        "DefaultTargetCapacityType": "spot"
    }
}
```

ABCOnline crée la EC2 flotte à l'aide de la commande create-fleet suivante.

```
aws ec2 create-fleet --cli-input-json file://config.json
```

Pour de plus amples informations, veuillez consulter Création d'une EC2 flotte.

Exécution

La stratégie d'allocation détermine que la capacité à la demande est toujours atteinte, tandis que le solde de la capacité cible est atteint au comptant si de la capacité est disponible.

Tutoriel : configurer EC2 Fleet pour lancer des instances à la demande à l'aide de réservations de capacité ciblées

Ce didacticiel vous explique toutes les étapes que vous devez effectuer pour que votre EC2 flotte lance des instances à la demande dans les réservations `targeted` de capacité.

Vous verrez qu'il est possible de configurer une flotte EC2 pour qu'elle utilise d'abord la réservations de capacité `targeted` lors du lancement d'instances à la demande. Vous apprendrez également à configurer la flotte de sorte que, lorsque la capacité cible totale à la demande dépasse le nombre de réservations de capacité inutilisées disponibles, la flotte utilise la stratégie d'allocation spécifiée pour sélectionner les groupes d'instances dans lesquels lancer la capacité cible restante.

EC2Configuration de la flotte

Dans ce didacticiel, la flotte est configurée comme suit :

- Capacité cible : 10 instances à la demande
- Total de réservations de capacité `targeted` non utilisé : 6 (inférieur à la capacité cible à la demande de la flotte de 10 instances à la demande)
- Nombre de groupes de réservations de capacité : 2 (`us-east-1a` et `us-east-1b`)
- Nombre de réservations de capacité par groupe : 3
- Stratégie d'allocation à la demande :`lowest-price`(Lorsque le nombre de réservations de capacité inutilisées est inférieur à la capacité cible à la demande, la flotte détermine les groupes dans lesquels lancer la capacité à la demande restante en fonction de la stratégie d'allocation à la demande.)

  Notez que vous pouvez également utiliser la stratégie d'allocation `prioritized` au lieu de la stratégie d'allocation `lowest-price`.

Pour lancer des instances à la demande dans les réservations de capacité targeted, vous devez effectuer un certain nombre d'étapes, comme suit :

- Étape 1 : Créer des réservations de capacité
- Étape 2 : Création d'un groupe de ressources de Réservation de capacité
- Étape 3 : Ajouter les réservations de capacité au groupe de ressources de Réservation de capacité
- (Facultatif) Étape 4 : Afficher les réservations de capacité dans le groupe de ressources

- Étape 5 : Créer un modèle de lancement qui spécifie que la réservation de capacité cible un groupe de ressources spécifique
- (Facultatif) Étape 6 : Décrire le modèle de lancement
- Étape 7 : Création d'une EC2 flotte
- (Facultatif) Étape 8 : Afficher le nombre de réservations de capacité non utilisées restantes

Étape 1 : Créer des réservations de capacité

Utilisez la create-capacity-reservationcommande pour créer les réservations de capacité, trois pour `us-east-1a` et trois autres pour`us-east-1b`. À l'exception de la zone de disponibilité, les autres attributs des réservations de capacité sont identiques.

3 Capacity Reservations in **`us-east-1a`** (3 réservations de capacité sur).

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1a \
    --instance-type c5.xlarge \
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

Exemple d'ID de réservation de capacité en résultant

```
cr-1234567890abcdef1
```

3 Capacity Reservations in **`us-east-1b`** (3 réservations de capacité sur).

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1b \
    --instance-type c5.xlarge \
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

Exemple d'ID de réservation de capacité en résultant

```
cr-54321abcdef567890
```

Étape 2 : Création d'un groupe de ressources de Réservation de capacité

Utilisation de `resource-groups` et du service create-group (créer un groupe) pour créer un groupe de ressources de Réservation de capacité. Dans cet exemple, le groupe de ressources est nommé `my-cr-group`. Pour plus d'informations sur les raisons pour lesquelles vous devez créer un groupe de ressources, veuillez consulter Utilisez les réservations de capacité pour réserver de la capacité à la demande dans EC2 Fleet.

```
aws resource-groups create-group \
    --name my-cr-group \
    --configuration '{"Type":"AWS::EC2::CapacityReservationPool"}'
 '{"Type":"AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-resource-
types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

Étape 3 : Ajouter les réservations de capacité au groupe de ressources de Réservation de capacité

Utilisation de `resource-groups` et du service group-resources (groupement de ressources) pour ajouter les réservations de capacité créées à l'étape 1 au groupe de ressources de réservations de capacité. Notez que vous devez référencer les réservations de capacité à la demande par leur nomARNs.

```
aws resource-groups group-resources \
    --group my-cr-group \
    --resource-arns \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Exemple de sortie

```
{
   "Failed": [],
   "Succeeded": [
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
   ]
}
```

(Facultatif) Étape 4 : Afficher les réservations de capacité dans le groupe de ressources

Utilisez le `resource-groups` service et la list-group-resourcescommande pour éventuellement décrire le groupe de ressources afin d'afficher ses réservations de capacité.

```
aws resource-groups list-group-resources --group my-cr-group
```

Exemple de sortie

```
{
    "ResourceIdentifiers": [
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-1234567890abcdef1"
        },
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-54321abcdef567890"
        }
    ]
}
```

Étape 5 : Créer un modèle de lancement qui spécifie que la réservation de capacité cible un groupe de ressources spécifique

Utilisez la create-launch-templatecommande pour créer un modèle de lancement dans lequel vous pourrez spécifier les réservations de capacité à utiliser. Dans cet exemple, la flotte utilisera les réservations de capacité `targeted`, qui ont été ajoutées à un groupe de ressources. Par conséquent, les données du modèle de lancement spécifient que la réservation de capacité cible un groupe de ressources spécifique. Dans cet exemple, le modèle de lancement est nommé `my-launch-template`.

```
aws ec2 create-launch-template \
    --launch-template-name my-launch-template \
    --launch-template-data \
        '{"ImageId": "ami-0123456789example",
          "CapacityReservationSpecification":
            {"CapacityReservationTarget":
```

```
                { "CapacityReservationResourceGroupArn": "arn:aws:resource-groups:us-
east-1:123456789012:group/my-cr-group" }
            }
        }'
```

(Facultatif) Étape 6 : Décrire le modèle de lancement

Utilisez la describe-launch-template-versionscommande pour éventuellement décrire le modèle de lancement afin de visualiser sa configuration.

```
aws ec2 describe-launch-template-versions --launch-template-name my-launch-template
```

Exemple de sortie

```
{
    "LaunchTemplateVersions": [
        {
            "LaunchTemplateId": "lt-01234567890example",
            "LaunchTemplateName": "my-launch-template",
            "VersionNumber": 1,
            "CreateTime": "2021-01-19T20:50:19.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Admin",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0947d2ba12ee1ff75",
                "CapacityReservationSpecification": {
                    "CapacityReservationTarget": {
                        "CapacityReservationResourceGroupArn": "arn:aws:resource-
groups:us-east-1:123456789012:group/my-cr-group"
                    }
                }
            }
        }
    ]
}
```

Étape 7 : Création d'une EC2 flotte

Créez une EC2 flotte qui spécifie les informations de configuration pour les instances qu'elle lancera. La configuration EC2 de flotte suivante montre uniquement les configurations pertinentes pour cet exemple. Le modèle de lancement `my-launch-template` est le modèle de lancement que vous avez créé à l'étape 5. Il existe deux groupes d'instances, chacun ayant le même type d'instance

(`c5.xlarge`), mais avec des zones de disponibilité différentes (`us-east-1a` et `us-east-1b`). Le prix des groupes d'instances est le même car la tarification est définie pour la Région et non pour la zone de disponibilité. La capacité cible totale est 10 et le type de capacité cible par défaut est `on-demand`. La stratégie d'allocation à la demande est `lowest-price`. La stratégie d'utilisation des réservations de capacité est `use-capacity-reservations-first`.

> **Note**
>
> Le type de flotte doit être `instant`. Les autres types de flotte ne prennent pas en charge `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
               }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
```

```
}
```

Après avoir créé la flotte `instant` à l'aide de la configuration précédente, les 10 instances suivantes sont lancées pour atteindre la capacité cible :

- Les réservations de capacité sont utilisées en premier lieu pour lancer 6 instances à la demande comme suit :
  - 3 instances à la demande sont lancées dans les 3 réservations de capacité `c5.xlarge targeted` dans `us-east-1a`
  - 3 instances à la demande sont lancées dans les 3 réservations de capacité `c5.xlarge targeted` dans `us-east-1b`
- Pour atteindre la capacité cible, 4 instances à la demande supplémentaires sont lancées dans la capacité à la demande régulière selon la stratégie d'allocation à la demande, qui est `lowest-price` dans cet exemple. Toutefois, étant donné que les groupes ont le même prix (car le prix est défini par Région et non par zone de disponibilité), la flotte lance les 4 instances à la demande restantes dans l'un ou l'autre des groupes.

(Facultatif) Étape 8 : Afficher le nombre de réservations de capacité non utilisées restantes

Une fois la flotte lancée, vous pouvez éventuellement courir describe-capacity-reservationspour voir combien de réservations de capacité non utilisées restent. Dans cet exemple, vous devriez voir la réponse suivante, qui montre que tous les réservations de capacité de tous les groupes ont été utilisés.

```
{ "CapacityReservationId":  "cr-111",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}

 { "CapacityReservationId":  "cr-222",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}
```

Tutoriel : configurez votre EC2 flotte pour lancer des instances dans des blocs de capacité

Ce didacticiel vous explique les étapes à suivre pour que votre EC2 flotte lance des instances dans des blocs de capacité.

Dans la plupart des cas, la capacité cible de la demande de EC2 flotte doit être inférieure ou égale à la capacité disponible de la réservation du bloc de capacité que vous ciblez. Les demandes de capacité cible qui dépassent les limites de la réservation du bloc de capacité ne seront pas satisfaites. Si la demande de capacité cible dépasse les limites de votre réservation de bloc de capacité, vous recevrez un signal `Insufficient Capacity Exception` pour la capacité qui dépasse les limites de votre réservation de bloc de capacité.

> **Note**
>
> Pour les blocs de capacité, EC2 Fleet ne se contentera pas de lancer des instances à la demande pour le reste de la capacité cible souhaitée.

Si EC2 Fleet n'est pas en mesure d'atteindre la capacité cible demandée dans une réservation de bloc de capacité disponible, EC2 Fleet atteindra la capacité maximale et retournera les instances qu'elle a pu lancer. Vous pouvez répéter l'appel à EC2 Fleet jusqu'à ce que toutes les instances soient approvisionnées.

Après avoir configuré la demande de EC2 flotte, vous devez attendre la date de début de votre réservation Capacity Block. Si vous demandez à EC2 Fleet de se lancer dans un bloc de capacité qui n'a pas encore démarré, vous recevrez un`Insufficient Capacity Error`.

Une fois que votre réservation de bloc de capacité est active, vous pouvez passer des API appels à EC2 Fleet et approvisionner les instances dans votre bloc de capacité en fonction des paramètres que vous avez sélectionnés. Les instances exécutées dans le bloc de capacité continuent de fonctionner jusqu'à ce que vous les arrêtiez ou les résiliiez manuellement ou jusqu'à ce qu'Amazon mette EC2 fin aux instances lorsque la réservation du bloc de capacité prend fin.

Pour plus d'informations sur les blocs de capacité, consultezBlocs de capacité pour ML.

Considérations

- Seules les demandes de type EC2 Fleet `instant` sont prises en charge pour le lancement d'instances dans des blocs de capacité. Pour de plus amples informations, veuillez consulter Configurer un type de EC2 flotte instant.
- Les blocs de capacité multiples dans la même demande EC2 de flotte ne sont pas pris en charge.
- L'utilisation de `OnDemandTargetCapacity` ou `SpotTargetCapacity` lors de la configuration de `capacity-block` en tant que `DefaultTargetCapacity` n'est pas prise en charge.
- Si `DefaultTargetCapacityType` est défini sur `capacity-block`, vous ne pouvez pas mettre en service `OnDemandOptions::CapacityReservationOptions`. Une exception se produit.

Pour configurer une EC2 flotte afin de lancer des instances dans des blocs de capacité

1. Créez un modèle de lancement.

   Dans le modèle de lancement, procédez comme suit :

   - Pour`InstanceMarketOptionsRequest`, réglez `MarketType` sur`capacity-block`.
   - Pour cibler la réservation du bloc de capacité, pour`CapacityReservationID`, spécifiez l'ID de réservation du bloc de capacité.

   Notez le nom et la version du modèle de lancement. Vous utiliserez ces informations à l'étape suivante.

   Pour plus d'informations sur la création d'un modèle de lancement, consultezCréation d'un modèle de EC2 lancement Amazon.
2. Configurez la EC2 flotte.

   Créez un fichier avec la configuration suivante pour votre EC2 flotte. `config.json` Dans l'exemple suivant, remplacez les identificateurs de ressources par vos propres identificateurs de ressources.

   Pour plus d'informations sur la configuration d'une EC2 flotte, consultezCréation d'une EC2 flotte.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
```

```
                "LaunchTemplateName": "CBR-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "p5.48xlarge",
                    "AvailabilityZone": "us-east-1a"
                },
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "capacity-block"
    },
    "Type": "instant"
}
```

3. Lancez la flotte.

   Utilisez la commande create-fleet suivante.

   ```
   aws ec2 create-fleet --cli-input-json file://config.json
   ```

   Pour de plus amples informations, veuillez consulter Création d'une EC2 flotte.

Exemples de CLI configurations pour EC2 Fleet

Vous pouvez définir la configuration de votre EC2 flotte dans un JSON fichier, puis référencer ce fichier à l'aide de la AWS CLI commande create-fleet pour créer votre flotte, comme suit :

```
aws ec2 create-fleet --cli-input-json file://file_name.json
```

Les exemples suivants illustrent les configurations de lancement pour différents cas d'utilisation de EC2 Fleet. Pour plus d'informations sur les paramètres de configuration, voir create-fleet dans le manuel AWS CLI Command Reference.

Exemples

- Exemple 1 : Lancer instances Spot en tant qu'option d'achat par défaut
- Exemple 2 : Lancer instances à la demande en tant qu'option d'achat par défaut

- Exemple 3 : Lancer instances à la demande en tant que capacité principale
- Exemple 4 : Lancer des instances à la demande à l'aide de plusieurs réservations de capacité
- Exemple 5 : Lancer des instances à la demande à l'aide de réservations de capacité lorsque la capacité cible totale dépasse le nombre de réservations de capacité non utilisées
- Exemple 6 : Lancer des instances à la demande à l'aide de réservations de capacité ciblées
- Exemple 7 : configurer le rééquilibrage de capacité pour lancer des instances Spot de remplacement
- Exemple 8 : Lancer des instances ponctuelles dans un parc à capacité optimisée
- Exemple 9 : Lancer des instances ponctuelles dans un parc à capacité optimisée avec des priorités
- Exemple 10 : Lancer des instances ponctuelles dans une price-capacity-optimized flotte
- Exemple 11 : Configuration de la sélection du type d'instance basée sur les attributs

Pour plus d'CLIexemples de flottes de types`instant`, voirConfigurer un type de EC2 flotte instant.

Exemple 1 : Lancer instances Spot en tant qu'option d'achat par défaut

L'exemple suivant indique les paramètres minimaux requis dans une EC2 flotte : un modèle de lancement, une capacité cible et une option d'achat par défaut. Le modèle de lancement est identifié par son ID de modèle de lancement et son numéro de version. La capacité cible du parc d'instances est de 2 instances et l'option d'achat par défaut est `spot`, ce qui entraîne le lancement par le parc d'instances de 2 Instances Spot.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Exemple 2 : Lancer instances à la demande en tant qu'option d'achat par défaut

L'exemple suivant indique les paramètres minimaux requis dans une EC2 flotte : un modèle de lancement, une capacité cible et une option d'achat par défaut. Le modèle de lancement est identifié par son ID de modèle de lancement et son numéro de version. La capacité cible du parc d'instances est de 2 instances et l'option d'achat par défaut est `on-demand`, ce qui entraîne le lancement par le parc d'instances de 2 Instances à la demande.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "on-demand"
    }
}
```

Exemple 3 : Lancer instances à la demande en tant que capacité principale

L'exemple suivant spécifie la capacité cible totale de 2 instances pour la flotte d'instances et une capacité cible de 1 instance à la demande. L'option d'achat par défaut est `spot`. Le flotte d'instances lance 1 instance à la demande comme spécifié, mais a besoin de lancer une instance supplémentaire pour assurer la capacité cible totale. L'option d'achat pour la différence est calculée comme `TotalTargetCapacity` - `OnDemandTargetCapacity` = `DefaultTargetCapacityType`, ce qui entraîne le lancement d'1 instance Spot par la flotte.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
```

```
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "OnDemandTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Exemple 4 : Lancer des instances à la demande à l'aide de plusieurs réservations de capacité

Vous pouvez configurer une flotte pour qu'elle utilise d'abord Réservations de capacité à la demande lors du lancement d'Instances à la demande en définissant la stratégie d'utilisation des réservations de capacité sur `use-capacity-reservations-first`. Cet exemple montre comment la flotte sélectionne les réservations de capacité à utiliser lorsqu'il y a plus de réservations de capacité que nécessaire pour atteindre la capacité cible.

Dans cet exemple, la configuration de la flotte est la suivante :

- Capacité cible : 12 instances à la demande
- Total de réservations de capacité non utilisé : 15 (supérieur à la capacité cible à la demande de la flotte de 12 instances à la demande)
- Nombre de groupes de réservations de capacité : 3 (`m5.large`, `m4.xlarge`, et `m4.2xlarge`)
- Nombre de réservations de capacité par groupe : 5
- Stratégie d'allocation à la demande : `lowest-price` (Lorsqu'il y a plusieurs réservations de capacité inutilisées dans plusieurs groupes d'instances, la flotte détermine les groupes dans lesquels lancer les instances à la demande en fonction de la stratégie d'allocation à la demande.)

  Notez que vous pouvez également utiliser la stratégie d'allocation `prioritized` au lieu de la stratégie d'allocation `lowest-price`.

Réserve de capacité

Le compte a les 15 réservations de capacité suivants inutilisés dans 3 groupes différents. Le nombre de Réservations de capacité dans chaque pool est indiqué par `AvailableInstanceCount`.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Fleet configuration (Configuration de la flotte)

La configuration de flotte suivante affiche uniquement les configurations pertinentes pour cet exemple. La capacité totale cible est 12 et le type de capacité cible par défaut est `on-demand`. La stratégie d'allocation à la demande est `lowest-price`. La stratégie d'utilisation des réservations de capacité est `use-capacity-reservations-first`.

Dans cet exemple, le prix des instance à la demande est :

- `m5.large` – 0,096 dollars par heure
- `m4.xlarge` – 0,20 dollars par heure
- `m4.2xlarge` – 0,40 dollars par heure

> **Note**
>
> Le type de flotte doit être `instant`. Les autres types de flotte ne prennent pas en charge `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-abc1234567example",
                "Version": "1"
            }
            "Overrides": [
                {
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
              ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 12,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
```

```
    },
    "Type": "instant",
}
```

Après avoir créé la flotte `instant` à l'aide de la configuration précédente, les 12 instances suivantes sont lancées pour atteindre la capacité cible :

- 5 instances à la demande `m5.large` dans `us-east-1a` – `m5.large` dans `us-east-1a` est le prix le plus bas, et il y a 5 réservations de capacité `m5.large` disponibles inutilisés
- 5 instances à la demande `m4.xlarge` dans us-east-1a – `m4.xlarge` dans `us-east-1a` est le prix suivant le plus bas, et il y a 5 réservations de capacité `m4.xlarge` disponibles inutilisés
- 2 instances à la demande `m4.2xlarge` dans us-est-1a – `m4.2xlarge` dans `us-east-1a` est le troisième prix le plus bas, et il y a 5 réservations de capacité `m4.2xlarge` disponibles inutilisés dont seulement 2 sont nécessaires pour atteindre la capacité cible

Une fois la flotte lancée, vous pouvez courir describe-capacity-reservationspour voir combien de réservations de capacité inutilisées restent. Dans cet exemple, vous devriez voir la réponse suivante, qui montre que tous les réservations de capacité `m5.large` et `m4.xlarge` ont été utilisés, avec 3 réservations de capacité `m4.2xlarge` restants inutilisés.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 3
}
```

Exemple 5 : Lancer des instances à la demande à l'aide de réservations de capacité lorsque la capacité cible totale dépasse le nombre de réservations de capacité non utilisées

Vous pouvez configurer une flotte pour qu'elle utilise d'abord Réservations de capacité à la demande lors du lancement d'Instances à la demande en définissant la stratégie d'utilisation des réservations de capacité sur `use-capacity-reservations-first`. Cet exemple illustre comment la flotte sélectionne les grouesp d'instances dans lesquels lancer des instances à la demande lorsque la capacité cible totale dépasse le nombre de réservations de capacité non utilisées disponibles.

Dans cet exemple, la configuration de la flotte est la suivante :

- Capacité cible : 16 instances à la demande
- Total de réservations de capacité non utilisé : 15 (inférieur à la capacité cible à la demande de la flotte de 16 instances à la demande)
- Nombre de groupes de réservations de capacité : 3 (`m5.large`, `m4.xlarge`, et `m4.2xlarge`)
- Nombre de réservations de capacité par groupe : 5
- Stratégie d'allocation à la demande :`lowest-price`(Lorsque le nombre de réservations de capacité inutilisées est inférieur à la capacité cible à la demande, la flotte détermine les groupes dans lesquels lancer la capacité à la demande restante en fonction de la stratégie d'allocation à la demande.)

  Notez que vous pouvez également utiliser la stratégie d'allocation `prioritized` au lieu de la stratégie d'allocation `lowest-price`.

Réserve de capacité

Le compte a les 15 réservations de capacité suivants inutilisés dans 3 groupes différents. Le nombre de Réservations de capacité dans chaque pool est indiqué par `AvailableInstanceCount`.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
```

```
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Fleet configuration (Configuration de la flotte)

La configuration de flotte suivante affiche uniquement les configurations pertinentes pour cet exemple. La capacité cible totale est 16 et le type de capacité cible par défaut est `on-demand`. La stratégie d'allocation à la demande est `lowest-price`. La stratégie d'utilisation des réservations de capacité est `use-capacity-reservations-first`.

Dans cet exemple, le prix des instance à la demande est :

- m5.large – 0,096 USD par heure
- m4.xlarge – 0,20 USD par heure
- m4.2xlarge – 0,40 USD par heure

> **Note**
>
> Le type de flotte doit être `instant`. Les autres types de flotte ne prennent pas en charge `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }
            "Overrides": [
                {
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
              ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 16,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant",
}
```

Après avoir créé la flotte `instant` à l'aide de la configuration précédente, les 16 instances suivantes sont lancées pour atteindre la capacité cible :

- 6 instances à la demande `m5.large` dans `us-east-1a` – `m5.large` dans `us-east-1a` est le prix le plus bas, et il y a 5 réservations de capacité `m5.large` disponibles inutilisés Les réservations de capacité sont utilisées en premier afin de lancer 5 instances à la demande. Après l'utilisation des réservations de capacité `m4.xlarge` and `m4.2xlarge` restantes, une instance à la demande supplémentaire est lancée pour atteindre la capacité cible, conformément à la stratégie d'allocation à la demande, qui est `lowest-price` dans cet exemple.
- 5 instances à la demande `m4.xlarge` dans `us-east-1a` – `m4.xlarge` dans `us-east-1a` est le prix suivant le plus bas, et il y a 5 réservations de capacité `m4.xlarge` disponibles inutilisés
- 5 instances à la demande `m4.2xlarge` dans `us-east-1a` – `m4.2xlarge` dans `us-east-1a` est le troisième prix le plus bas, et il y a 5 réservations de capacité `m4.2xlarge` disponibles inutilisés

Une fois la flotte lancée, vous pouvez courir describe-capacity-reservationspour voir combien de réservations de capacité inutilisées restent. Dans cet exemple, vous devriez voir la réponse suivante, qui montre que tous les réservations de capacité de tous les groupes ont été utilisés.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 0
}
```

Exemple 6 : Lancer des instances à la demande à l'aide de réservations de capacité ciblées

Vous pouvez configurer une flotte pour qu'elle utilise `targeted` d'abord les réservations de capacité à la demande lors du lancement d'instances à la demande en paramétrant la stratégie d'utilisation

des réservations de capacité sur `use-capacity-reservations-first`. Cet exemple illustre comment lancer des instances à la demande dans réservations de capacité `targeted`, où les attributs des réservations de capacité sont les mêmes, à l'exception de leurs zones de disponibilité (`us-east-1a` et `us-east-1b`). Il illustre également comment la flotte sélectionne les groupes d'instances dans lesquels lancer des instances à la demande lorsque la capacité cible totale dépasse le nombre de réservations de capacité non utilisées disponibles.

Dans cet exemple, la configuration de la flotte est la suivante :

- Capacité cible : 10 instances à la demande
- Total de réservations de capacité `targeted` non utilisé : 6 (inférieur à la capacité cible à la demande de la flotte de 10 instances à la demande)
- Nombre de groupes de réservations de capacité : 2 (`us-east-1a` et `us-east-1b`)
- Nombre de réservations de capacité par groupe : 3
- Stratégie d'allocation à la demande :`lowest-price`(Lorsque le nombre de réservations de capacité inutilisées est inférieur à la capacité cible à la demande, la flotte détermine les groupes dans lesquels lancer la capacité à la demande restante en fonction de la stratégie d'allocation à la demande.)

  Notez que vous pouvez également utiliser la stratégie d'allocation `prioritized` au lieu de la stratégie d'allocation `lowest-price`.

Pour obtenir une démonstration pas à pas des procédures que vous devez effectuer pour exécuter cet exemple, veuillez consulter Tutoriel : configurer EC2 Fleet pour lancer des instances à la demande à l'aide de réservations de capacité ciblées.

Réserve de capacité

Le compte a les 6 réservations de capacité suivants inutilisés dans 2 groupes différents. Dans cet exemple, les groupes diffèrent selon leurs zones de disponibilité. Le nombre de Réservations de capacité dans chaque pool est indiqué par `AvailableInstanceCount`.


```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
```

```
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1b",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Fleet configuration (Configuration de la flotte)

La configuration de flotte suivante affiche uniquement les configurations pertinentes pour cet exemple. La capacité cible totale est 10 et le type de capacité cible par défaut est `on-demand`. La stratégie d'allocation à la demande est `lowest-price`. La stratégie d'utilisation des réservations de capacité est `use-capacity-reservations-first`.

Dans cet exemple, le prix des instance à la demande pour `c5.xlarge` dans `us-east-1` est 0,17 dollars par heure.

> **Note**
>
> Le type de flotte doit être `instant`. Les autres types de flotte ne prennent pas en charge `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
```

```
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
}
```

Après avoir créé la flotte `instant` à l'aide de la configuration précédente, les 10 instances suivantes sont lancées pour atteindre la capacité cible :

- Les réservations de capacité sont utilisées en premier lieu pour lancer 6 instances à la demande comme suit :
  - 3 instances à la demande sont lancées dans les 3 réservations de capacité `c5.xlarge targeted` dans `us-east-1a`
  - 3 instances à la demande sont lancées dans les 3 réservations de capacité `c5.xlarge targeted` dans `us-east-1b`
- Pour atteindre la capacité cible, 4 instances à la demande supplémentaires sont lancées dans la capacité à la demande régulière selon la stratégie d'allocation à la demande, qui est `lowest-price` dans cet exemple. Toutefois, étant donné que les groupes ont le même prix (car le prix est défini par Région et non par zone de disponibilité), la flotte lance les 4 instances à la demande restantes dans l'un ou l'autre des groupes.

Une fois la flotte lancée, vous pouvez courir describe-capacity-reservationspour voir combien de réservations de capacité inutilisées restent. Dans cet exemple, vous devriez voir la réponse suivante, qui montre que tous les réservations de capacité de tous les groupes ont été utilisés.

```
{
```

```
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}
```

Exemple 7 : configurer le rééquilibrage de capacité pour lancer des instances Spot de remplacement

L'exemple suivant configure le EC2 parc pour lancer une instance ponctuelle de remplacement lorsqu'Amazon EC2 émet une recommandation de rééquilibrage pour une instance ponctuelle du parc. Pour configurer le remplacement automatique de Instances Spot, pour `ReplacementStrategy`, spécifiez `launch-before-terminate`. Pour configurer le délai entre le lancement des nouvelles instances Spot de remplacement et le moment où les anciennes instances Spot sont automatiquement supprimées, pour `termination-delay`, spécifiez une valeur en secondes. Pour de plus amples informations, veuillez consulter Options de configuration.

> **Note**
>
> Nous vous recommandons d'utiliser `launch-before-terminate` uniquement si vous pouvez prédire en combien de temps les procédures d'arrêt de vos instances seront terminées, de sorte que les anciennes instances ne soient terminées qu'une fois ces procédures terminées. Toutes les instances en cours d'exécution vous sont facturées.

L'efficacité de la stratégie de rééquilibrage des capacités dépend du nombre de pools de capacités ponctuels spécifiés dans la demande de EC2 flotte. Nous vous recommandons de configurer le parc avec un ensemble diversifié de types d'instance et de zones de disponibilité, et pour `AllocationStrategy`, spécifiez `capacity-optimized`. Pour plus d'informations sur les éléments à prendre en compte lors de la configuration d'un EC2 parc pour le rééquilibrage des capacités, consultezUtilisez le rééquilibrage des capacités dans le EC2 parc et le parc ponctuel pour remplacer les instances ponctuelles à risque.

```
{
```

```
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "LaunchTemplate",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "c3.large",
                           "WeightedCapacity": 1,
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c4.large",
                           "WeightedCapacity": 1,
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c5.large",
                           "WeightedCapacity": 1,
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       }
                ]
          }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
```

```
    }
}
```

Exemple 8 : Lancer des instances ponctuelles dans un parc à capacité optimisée

L'exemple suivant montre comment configurer une EC2 flotte avec une stratégie d'allocation ponctuelle qui optimise la capacité. Pour optimiser la capacité, vous devez définir `AllocationStrategy` sur `capacity-optimized`.

Dans l'exemple suivant, les trois spécifications de lancement spécifient trois groupes de capacités Spot. La capacité cible est de 50 instances Spot. La EC2 flotte tente de lancer 50 instances ponctuelles dans le pool de capacités ponctuelles avec une capacité optimale compte tenu du nombre d'instances lancées.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           },
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
```

```
                        }
                    }
                ]
            }
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"

    }
}
```

Exemple 9 : Lancer des instances ponctuelles dans un parc à capacité optimisée avec des priorités

L'exemple suivant montre comment configurer une EC2 flotte avec une stratégie d'allocation ponctuelle qui optimise la capacité tout en utilisant la priorité au mieux.

Lors de l'utilisation de la stratégie d'allocation `capacity-optimized-prioritized`, vous pouvez utiliser le paramètre `Priority` pour spécifier les priorités des groupes de capacités Spot, où plus le nombre est faible, plus la priorité est élevée. Vous pouvez également définir la même priorité pour plusieurs groupes de capacités Spot si vous les privilégiez également. Si vous ne définissez pas de priorité pour un groupe, le groupe sera considéré comme le dernier en termes de priorité.

Pour hiérarchiser les groupes de capacités Spot, vous devez définir `AllocationStrategy` sur `capacity-optimized-prioritized`. EC2La flotte optimisera d'abord la capacité, mais respectera les priorités dans la mesure du possible (par exemple, si le respect des priorités n'affecte pas de manière significative la capacité de la EC2 flotte à fournir une capacité optimale). C'est une bonne option pour les charges de travail pour lesquelles la possibilité de perturbation doit être minimisée, mais la priorité de certains types d'instances est également importante.

Dans l'exemple suivant, les trois spécifications de lancement spécifient trois groupes de capacités Spot. Chaque groupe est classé par ordre de priorité, où plus le nombre est faible, plus la priorité est élevée. La capacité cible est de 50 instances Spot. La EC2 flotte tente de lancer 50 instances ponctuelles dans le pool de capacités ponctuelles avec la priorité la plus élevée, dans la mesure du possible, mais optimise d'abord la capacité.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
```

```
        },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                        {
                           "InstanceType": "r4.2xlarge",
                           "Priority": 1,
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
                       },
                        {
                           "InstanceType": "m4.2xlarge",
                           "Priority": 2,
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           },
                        },
                        {
                           "InstanceType": "c5.2xlarge",
                           "Priority": 3,
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           }
                        }
                    ]
             }
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"
}
```

Exemple 10 : Lancer des instances ponctuelles dans une price-capacity-optimized flotte

L'exemple suivant montre comment configurer une EC2 flotte avec une stratégie d'allocation ponctuelle qui optimise à la fois la capacité et le prix le plus bas. Pour optimiser la capacité tout en

tenant compte du prix, vous devez définir le Spot `AllocationStrategy` sur `price-capacity-optimized`.

Dans l'exemple suivant, les trois spécifications de lancement spécifient trois groupes de capacités Spot. La capacité cible est de 50 instances Spot. La EC2 flotte tente de lancer 50 instances ponctuelles dans le pool de capacités ponctuelles avec une capacité optimale compte tenu du nombre d'instances lancées, tout en choisissant le pool le moins cher.

```
{
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized",
        "MinTargetCapacity": 2,
        "SingleInstanceType": true
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           },
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           }
                       }
                ]
```

```
            }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 50,
        "OnDemandTargetCapacity":0,
        "SpotTargetCapacity":50,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemple 11 : Configuration de la sélection du type d'instance basée sur les attributs

L'exemple suivant montre comment configurer un EC2 parc de manière à utiliser la sélection de type d'instance basée sur les attributs pour identifier les types d'instance. Pour spécifier les attributs d'instance requis, vous devez les spécifier dans la structure `InstanceRequirements`.

Dans l'exemple suivant, deux attributs d'instance sont spécifiés :

- `VCpuCount`— Un minimum de 2 vCPUs est spécifié. Comme aucun maximum n'est spécifié, il n'y a pas de limite maximale.
- `MemoryMiB` : au moins 4 Mio de mémoire sont spécifiés. Comme aucun maximum n'est spécifié, il n'y a pas de limite maximale.

Tous les types d'instance dotés de 2 ou plus vCPUs et de 4 Mo de mémoire ou plus seront identifiés. Cependant, la protection des prix et la stratégie d'allocation peuvent exclure certains types d'instances lorsque EC2Fleet approvisionne la flotte.

Pour obtenir une liste et une description de tous les attributs possibles que vous pouvez spécifier, consultez InstanceRequirementsla EC2APIréférence Amazon.

```
{
 "SpotOptions": {
  "AllocationStrategy": "price-capacity-optimized"
 },
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
```

```
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }],
 "TargetCapacitySpecification": {
  "TotalTargetCapacity": 20,
  "DefaultTargetCapacityType": "spot"
 },
 "Type": "instant"
}
```

Exemples de CLI configurations Spot Fleet

Vous pouvez définir la configuration de votre parc Spot dans un JSON fichier, puis référencer ce fichier à l'aide de la request-spot-fleet AWS CLI commande pour créer votre parc, comme suit :

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://file_name.json
```

Les exemples suivants illustrent les configurations de lancement pour différents cas d'utilisation de Spot Fleet. Pour plus d'informations sur les paramètres de configuration, consultez request-spot-fleetla référence des AWS CLI commandes. Pour plus d'informations sur la création d'un parc de spots, consultezCréer une flotte Spot.

> **Note**
>
> Pour le parc d'instances Spot, vous ne pouvez pas spécifier d'ID d'interface réseau dans un modèle ou une spécification de lancement. Veillez à omettre le paramètre `NetworkInterfaceID` dans votre modèle ou spécification de lancement.

Exemples

Exemple 1 : Lancement d'instances Spot en utilisant la zone de disponibilité ou le sous-réseau offrant le prix le moins élevé de la région

L'exemple suivant spécifie une seule spécification de lancement sans Zone de disponibilité ou sous-réseau. Le parc d'instances Spot lance les instances dans la zone de disponibilité ayant le prix le moins élevé qui a un sous-réseau par défaut. Le prix que vous payez ne dépasse pas le prix à la demande.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
```

```
                {
                    "GroupId": "sg-1a2b3c4d"
                }
            ],
            "InstanceType": "m3.medium",
            "IamInstanceProfile": {
                "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
            }
        }
    ]
}
```

Exemple 2 : Lancement d'instances Spot en utilisant la zone de disponibilité ou le sous-réseau offrant le prix le moins élevé dans une liste spécifiée

Les exemples suivants spécifient deux spécifications de lancement avec des zones de disponibilité ou des sous-réseaux différents, mais avec le même type d'instance etAMI.

Zones de disponibilité

Le parc d'instances Spot lance les instances dans le sous-réseau par défaut de la zone de disponibilité ayant le prix le moins élevé que vous avez spécifié.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "Placement": {
              "AvailabilityZone": "us-west-2a, us-west-2b"
          },
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
```

```
        }
    ]
}
```

Sous-réseaux

Vous pouvez spécifier des sous-réseaux par défaut ou des sous-réseaux autres que ceux par défaut, et les sous-réseaux autres que ceux par défaut peuvent provenir d'un sous-réseau par défaut ou d'un sous-réseau autre que celui par défaut. VPC VPC Le service d'instances Spot lance les instances sur n'importe quel réseau se trouvant dans la zone de disponibilité ayant le prix le moins élevé.

Vous ne pouvez pas spécifier plusieurs sous-réseaux d'une même zone de disponibilité dans une demande de parc d'instances Spot.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "SubnetId": "subnet-a61dafcf, subnet-65ea5f08",
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Si les instances sont lancées par défautVPC, elles reçoivent une IPv4 adresse publique par défaut. Si les instances ne sont pas lancées par défautVPC, elles ne reçoivent pas d'IPv4adresse publique par défaut. Utilisez une interface réseau dans la spécification de lancement pour attribuer une IPv4 adresse publique aux instances lancées selon une méthode autre que celle par défautVPC. Lorsque vous spécifiez une interface réseau, vous devez inclure l'ID de sous-réseau et l'ID du groupe de sécurité à l'aide de l'interface réseau.

```
  ...
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "InstanceType": "m3.medium",
          "NetworkInterfaces": [
              {
                  "DeviceIndex": 0,
                  "SubnetId": "subnet-1a2b3c4d",
                  "Groups": [ "sg-1a2b3c4d" ],
                  "AssociatePublicIpAddress": true
              }
          ],
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::880185128111:instance-profile/my-iam-role"
          }
      }
  ...
```

Exemple 3 : Lancement d'instances Spot en utilisant le type d'instance offrant le prix le plus bas dans une liste spécifiée

Les exemples suivants spécifient deux configurations de lancement avec des types d'instance différents, mais identiques, AMI ainsi qu'une zone de disponibilité ou un sous-réseau. Le parc d'instances Spot lance les instances en utilisant le type d'instance spécifié offrant le prix le plus bas.

Zone de disponibilité

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "c5.4xlarge",
          "Placement": {
            "AvailabilityZone": "us-west-2b"
```

```
            }
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "SecurityGroups": [
                {
                    "GroupId": "sg-1a2b3c4d"
                }
            ],
            "InstanceType": "r3.8xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        }
    ]
}
```

Sous-réseau

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "c5.4xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "r3.8xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      }
```

```
  ]
}
```

Exemple 4 : Remplacement du prix pour la demande

Nous vous avons recommandé d'utiliser le prix maximum par défaut, qui correspond au prix à la demande. Si vous préférez, vous pouvez indiquer un prix maximum pour la demande du flotte, et les prix maximum des spécifications de lancement individuelles.

Les exemples suivants indiquent le prix maximum pour la demande du flotte, et les prix maximum pour deux des trois spécifications de lancement. Le prix maximum de la demande de flotte est utilisé pour toutes les spécifications de lancement qui ne spécifient aucun prix maximum. Le parc d'instances Spot lance les instances en utilisant le type d'instance offrant le prix le plus bas.

Zone de disponibilité

```
{
  "SpotPrice": "1.00",
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "SpotPrice": "0.10"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.4xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "SpotPrice": "0.20"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.8xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
```

```
            }
        }
    ]
}
```

Sous-réseau

```
{
  "SpotPrice": "1.00",
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.2xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "SpotPrice": "0.10"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.4xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "SpotPrice": "0.20"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.8xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      }
  ]
}
```

Exemple 5 : lancement d'un parc d'instances Spot en utilisant la stratégie d'allocation diversifiée

L'exemple suivant utilise la stratégie d'allocation `diversified`. Les spécifications de lancement ont des types d'instances différents mais identiques, qu'il s'agisse AMI d'une zone de disponibilité ou d'un sous-réseau. Le parc d'instances Spot répartit les 30 instances entre les trois spécifications de lancement de sorte qu'il existe 10 instances de chaque type. Pour de plus amples informations, veuillez consulter Utilisez des stratégies d'allocation pour déterminer comment EC2 Fleet ou Spot Fleet exploite les capacités sur place et à la demande.

Zone de disponibilité

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c4.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "m3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
  ]
}
```

Sous-réseau

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
```

```
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

Une bonne pratique pour augmenter les chances qu'une demande ponctuelle puisse être satisfaite en EC2 fonction de la capacité en cas de panne dans l'une des zones de disponibilité consiste à diversifier les zones. Pour ce scénario, incluez chaque zone disponibilité à votre disposition dans les spécifications de lancement. Et, au lieu d'utiliser le même sous-réseau à chaque fois, utilisez trois sous-réseaux uniques (chacun correspondant à une zone différente).

Zone de disponibilité

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c4.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2a"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "m3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
```

```
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2c"
          }
      }
  ]
}
```

Sous-réseau

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-2a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-3a2b3c4d"
        }
    ]
}
```

Exemple 6 : lancement d'un parc d'instances Spot en utilisant la pondération d'instance

Les exemples suivants utilisent la pondération d'instance, ce qui signifie que le prix est déterminé par heure d'unité, et non par heure d'instance. Chaque configuration de lancement répertorie un type d'instance différent et une pondération différente. Le parc d'instances Spot sélectionne le type

d'instance ayant le prix par heure d'unité le plus bas. Le parc d'instances Spot calcule le nombre d'instances Spot à lancer en divisant la capacité cible par la pondération d'instance. Si le résultat n'est pas un nombre entier, le parc d'instances Spot l'arrondit à l'entier suivant afin que la taille de votre flotte ne soit pas inférieure à sa capacité cible.

Si la demande `r3.2xlarge` est satisfaite, le parc d'instances Spot met en service 4 de ces instances. Divisez 20 par 6 pour un total de 3,33 instances, puis arrondissez à 4 instances.

Si la demande `c3.xlarge` est satisfaite, le parc d'instances Spot met en service 7 de ces instances. Divisez 20 par 3 pour un total de 6,66 instances, puis arrondissez à 7 instances.

Pour de plus amples informations, veuillez consulter Utilisez la pondération des instances pour gérer les coûts et les performances de votre EC2 flotte ou de votre flotte ponctuelle.

Zone de disponibilité

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "WeightedCapacity": 6
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "WeightedCapacity": 3
      }
    ]
}
```

Sous-réseau

```
{
```

```
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "WeightedCapacity": 6
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "WeightedCapacity": 3
      }
  ]
}
```

Exemple 7 : lancement d'un parc d'instances Spot avec une capacité à la demande

Pour garantir que vous avez toujours la capacité d'instance, vous pouvez inclure une demande de capacité à la demande dans votre demande de parc d'instances Spot . S'il y a la capacité nécessaire, la demande à la demande est toujours satisfaite. Le solde de la capacité cible est assuré en tant que Spot s'il existe une capacité et une disponibilité.

L'exemple suivant spécifie la capacité cible souhaitée de 10 instances, dont 5 correspondent à une capacité à la demande. La capacité Spot n'est pas spécifiée : elle est impliquée dans le solde de la capacité cible moins la capacité à la demande. Amazon EC2 lance 5 unités de capacité à la demande et 5 unités de capacité (10-5=5) sous forme de Spot si la EC2 capacité et la disponibilité d'Amazon sont disponibles.

```
{
  "IamFleetRole": "arn:aws:iam::781603563322:role/aws-ec2-spot-fleet-tagging-role",
  "AllocationStrategy": "lowestPrice",
  "TargetCapacity": 10,
  "SpotPrice": null,
  "ValidFrom": "2018-04-04T15:58:13Z",
  "ValidUntil": "2019-04-04T15:58:13Z",
  "TerminateInstancesWithExpiration": true,
```

```
  "LaunchSpecifications": [],
  "Type": "maintain",
  "OnDemandTargetCapacity": 5,
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-0dbb04d4a6cca5ad1",
        "Version": "2"
      },
      "Overrides": [
        {
          "InstanceType": "t2.medium",
          "WeightedCapacity": 1,
          "SubnetId": "subnet-d0dc51fb"
        }
      ]
    }
  ]
}
```

Exemple 8 : Configurer le rééquilibrage de capacité pour lancer les instances Spot de remplacement

L'exemple suivant configure le parc Spot pour lancer une instance Spot de remplacement lorsqu'Amazon EC2 émet une recommandation de rééquilibrage pour une instance Spot du parc. Pour configurer le remplacement automatique de Instances Spot, pour `ReplacementStrategy`, spécifiez `launch-before-terminate`. Pour configurer le délai entre le lancement des nouvelles instances Spot de remplacement et le moment où les anciennes instances Spot sont automatiquement supprimées, pour `termination-delay`, spécifiez une valeur en secondes. Pour de plus amples informations, veuillez consulter Options de configuration.

> **Note**
>
> Nous vous recommandons d'utiliser `launch-before-terminate` uniquement si vous pouvez prédire la durée de la procédure d'arrêt de votre instance. Cela garantit que les anciennes instances ne sont résiliées qu'une fois les procédures d'arrêt terminées. Toutes les instances en cours d'exécution vous sont facturées.

L'efficacité de la stratégie de rééquilibrage de capacité dépend du nombre de groupes de capacités Spot spécifiés dans la demande de parc d'instances Spot. Nous vous recommandons de configurer le parc avec un ensemble diversifié de types d'instance et de zones de disponibilité, et pour `AllocationStrategy`, spécifiez `capacityOptimized`. Pour plus d'informations sur ce que vous devez prendre en compte lors de la configuration d'un parc d'instances Spot pour le rééquilibrage de capacité, consultez la rubrique Utilisez le rééquilibrage des capacités dans le EC2 parc et le parc ponctuel pour remplacer les instances ponctuelles à risque.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "LaunchTemplate",
                    "Version": "1"
                },
                 "Overrides": [
                       {
                           "InstanceType": "c3.large",
                           "WeightedCapacity": 1,
                           "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c4.large",
                           "WeightedCapacity": 1,
                           "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c5.large",
                           "WeightedCapacity": 1,
                           "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       }
                ]
```

```
          }
    ],
        "TargetCapacity": 5,
        "SpotMaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
    }
}
```

Exemple 9 : lancer des instances Spot dans une flotte optimisée pour la capacité

L'exemple suivant montre comment configurer un parc d'instances Spot avec une stratégie d'allocation Spot qui optimise la capacité. Pour optimiser la capacité, vous devez définir `AllocationStrategy` sur `capacityOptimized`.

Dans l'exemple suivant, les trois spécifications de lancement spécifient trois groupes de capacités Spot. La capacité cible est de 50 instances Spot. Le parc d'instances Spot tente de lancer 50 instances Spot dans le groupe de capacités Spot avec une capacité optimale pour le nombre d'instances qui sont lancées.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "AvailabilityZone": "us-west-2a"
                      },
                       {
```

```
                        "InstanceType": "m4.2xlarge",
                        "AvailabilityZone": "us-west-2b"
                    },
                    {
                        "InstanceType": "c5.2xlarge",
                        "AvailabilityZone": "us-west-2b"
                    }
                ]
            }
        ]
}
```

Exemple 10 : lancer des instances Spot dans une flotte optimisée pour la capacité avec des priorités

L'exemple suivant montre comment configurer un parc d'instances Spot avec une stratégie d'allocation Spot qui optimise la capacité tout en utilisant la priorité sur la base du meilleur effort.

Lors de l'utilisation de la stratégie d'allocation `capacityOptimizedPrioritized`, vous pouvez utiliser le paramètre `Priority` pour spécifier les priorités des groupes de capacités Spot, où plus le nombre est faible, plus la priorité est élevée. Vous pouvez également définir la même priorité pour plusieurs groupes de capacités Spot si vous les privilégiez également. Si vous ne définissez pas de priorité pour un groupe, le groupe sera considéré comme le dernier en termes de priorité.

Pour hiérarchiser les groupes de capacités Spot, vous devez définir `AllocationStrategy` sur `capacityOptimizedPrioritized`. Le parc d'instances Spot optimisera la capacité d'abord, mais respectera les priorités sur la base du meilleur effort (par exemple, si le respect des priorités n'affecte pas de manière significative la capacité du parc d'instances Spot à fournir une capacité optimale). C'est une bonne option pour les charges de travail pour lesquelles la possibilité de perturbation doit être minimisée, mais la priorité de certains types d'instances est également importante.

Dans l'exemple suivant, les trois spécifications de lancement spécifient trois groupes de capacités Spot. Chaque groupe est classé par ordre de priorité, où plus le nombre est faible, plus la priorité est élevée. La capacité cible est de 50 instances Spot. Le parc d'instances Spot tente de lancer 50 instances Spot dans le groupe de capacités Spot avec la priorité la plus élevée sur la base du meilleur effort, mais optimise d'abord la capacité.

```
{
    "TargetCapacity": "50",
```

```
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimizedPrioritized"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                        {
                            "InstanceType": "r4.2xlarge",
                            "Priority": 1,
                            "AvailabilityZone": "us-west-2a"
                        },
                        {
                            "InstanceType": "m4.2xlarge",
                            "Priority": 2,
                            "AvailabilityZone": "us-west-2b"
                        },
                        {
                            "InstanceType": "c5.2xlarge",
                            "Priority": 3,
                            "AvailabilityZone": "us-west-2b"
                        }
                    ]
             }
       ]
}
```

Exemple 11 : Lancer des instances ponctuelles dans une priceCapacityOptimized flotte

L'exemple suivant montre comment configurer un parc d'instances Spot avec une stratégie d'allocation Spot qui optimise la capacité et le prix le plus bas. Pour optimiser la capacité tout en tenant compte du prix, vous devez définir le Spot `AllocationStrategy` sur `priceCapacityOptimized`.

Dans l'exemple suivant, les trois spécifications de lancement spécifient trois groupes de capacités Spot. La capacité cible est de 50 instances Spot. Le parc d'instances Spot tente de lancer 50 instances Spot dans le groupe de capacités Spot avec une capacité optimale pour le nombre d'instances qui sont lancées, tout en choisissant également le groupe le moins cher.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "OnDemandAllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111111111111:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "lt-0123456789example",
                    "Version": "1"
                },
                "Overrides": [
                     {
                           "InstanceType": "r4.2xlarge",
                           "AvailabilityZone": "us-west-2a"
                      },
                      {
                           "InstanceType": "m4.2xlarge",
                           "AvailabilityZone": "us-west-2b"
                      },
                      {
                           "InstanceType": "c5.2xlarge",
                           "AvailabilityZone": "us-west-2b"
                      }
                ]
            }
        ],
        "TargetCapacity": 50,
        "Type": "request"
    }
}
```

Exemple 12 : configurer la sélection de type d'instance basée sur des attributs

L'exemple suivant montre comment configurer un parc d'instances Spot pour qu'il utilise la sélection de type d'instance basée sur des attributs pour identifier les types d'instance. Pour spécifier les attributs d'instance requis, vous devez les spécifier dans la structure `InstanceRequirements`.

Dans l'exemple suivant, deux attributs d'instance sont spécifiés :

- `VCpuCount`— Un minimum de 2 vCPUs est spécifié. Comme aucun maximum n'est spécifié, il n'y a pas de limite maximale.
- `MemoryMiB` : au moins 4 Mio de mémoire sont spécifiés. Comme aucun maximum n'est spécifié, il n'y a pas de limite maximale.

Tous les types d'instance dotés de 2 ou plus vCPUs et de 4 Mo de mémoire ou plus seront identifiés. Toutefois, la protection des prix et la stratégie d'allocation peuvent exclure certains types d'instances lorsque le parc d'instances Spot alloue la flotte.

Pour obtenir une liste et une description de tous les attributs possibles que vous pouvez spécifier, consultez InstanceRequirementsla EC2APIréférence Amazon.

```
{
 "AllocationStrategy": "priceCapacityOptimized",
 "TargetCapacity": 20,
 "Type": "request",
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }]
}
```

Quotas pour EC2 la flotte et la flotte ponctuelle

Vous Compte AWS disposez de quotas par défaut, anciennement appelés limites, pour chaque AWS service. Sauf indication contraire, chaque quota est spécifique à la région.

Les EC2 quotas Amazon habituels s'appliquent aux instances lancées par une EC2 flotte ou une flotte ponctuelle, tels que les limites d'instances ponctuelles et les limites de volume.

En outre, vous disposez Compte AWS des quotas suivants relatifs à EC2 Fleet et Spot Fleet :

Description du quota	Quota
Le nombre de EC2 flottes et de flottes ponctuelles par type de région `maintain` et `request` dans `active` `deleted_running` les États `cancelled_running`	1 000 [1] [2] [3]
Le nombre de EC2 flottes de type `instant`	Illimité
Le nombre de pools de capacité Spot (combinaison unique de type d'instance et de sous-réseau) pour les EC2 flottes et les flottes ponctuelles de type et `maintain` `request`	300 [1]
Le nombre de pools de capacité Spot (combinaison unique de type d'instance et de sous-réseau) pour les EC2 flottes de type `instant`	Illimité
Taille des données utilisateur dans une spécification de lancement	16 Ko [2]
La capacité cible par EC2 flotte ou flotte ponctuelle	10 000
La capacité cible pour toutes les EC2 flottes et les flottes ponctuelles d'une région	100 000 [1]
Une demande EC2 de flotte ou une demande de flotte ponctuelle ne peut pas couvrir plusieurs régions.	
Une demande de EC2 flotte ou une demande de flotte ponctuelle ne peut pas couvrir différent	

Description du quota	Quota
s sous-réseaux d'une même zone de disponibi lité.	

[1] Ces quotas s'appliquent à la fois à vos EC2 flottes et à vos flottes ponctuelles.

[2] Ces quotas sont finis. Vous ne pouvez pas demander une augmentation de ces quotas.

[3] Après avoir supprimé une EC2 flotte ou annulé une demande de flotte ponctuelle, et si vous avez spécifié que la flotte ne devait pas résilier ses instances ponctuelles lorsque vous supprimez ou annulez la demande, la demande de flotte passe à l'état `deleted_running` (EC2flotte) ou `cancelled_running` (flotte ponctuelle) et les instances continuent de fonctionner jusqu'à ce qu'elles soient interrompues ou que vous les résiliiez manuellement. Si vous mettez fin aux instances, la demande de flotte passe à l'état `deleted_terminating` (EC2flotte) ou `cancelled_terminating` (flotte ponctuelle) et n'est pas prise en compte dans ce quota. Pour plus d'informations, consultez Supprimer une demande de EC2 flotte et les instances de la flotte et Annuler (supprimer) une demande de Spot Fleet.

Demander une augmentation de quota pour la capacité cible

S'il vous faut un quota par défaut supérieur à la capacité cible, demandez une augmentation de quota.

Demander une augmentation de quota pour la capacité cible

1. Ouvrez le formulaire AWS Support Center Create Case.
2. Sélectionnez Service Limit increase (Augmentation des limites de service).
3. Pour Type de limite, choisissez EC2Fleet.
4. Pour Région, choisissez la AWS région dans laquelle vous souhaitez demander l'augmentation du quota.
5. Pour Limit (Limite), choisissez Target Fleet Capacity per Fleet (in units) (Capacité cible de la flotte par flotte [en unités]) ou Target Fleet Capacity per Region (in units) (Capacité de flotte cible par région [en unités]), selon le quota que vous souhaitez augmenter.
6. Pour New limit value (Nouvelle valeur de la limite), saisissez la nouvelle valeur.
7. Pour demander l'augmentation d'un autre quota, choisissez Add another request (Ajouter une demande supplémentaire), et répétez les étapes 4 à 6.

8. Pour Use case description (Description du cas d’utilisation), indiquez la raison pour laquelle vous demandez une augmentation de quota.
9. Sous Contact options (Options de contact), spécifiez la langue de contact et la méthode de contact que vous préférez.
10. Sélectionnez Envoyer.

Réseautage sur Amazon EC2

Amazon vous VPC permet de lancer AWS des ressources, telles que des EC2 instances Amazon, dans un réseau virtuel dédié à votre AWS compte, connu sous le nom de cloud privé virtuel (VPC). Lorsque vous lancez une instance, vous pouvez sélectionner un sous-réseau dans leVPC. L'instance est configurée avec une interface réseau principale, qui est une carte réseau virtuelle logique. L'instance reçoit une adresse IP privée principale à partir de l'IPv4adresse du sous-réseau, et elle est attribuée à l'interface réseau principale.

Vous pouvez contrôler si l'instance reçoit une adresse IP publique du pool d'adresses IP publiques d'Amazon. L'adresse IP publique d'une instance est associée à votre instance uniquement jusqu'à ce qu'elle soit arrêtée ou résiliée. Si vous avez besoin d'une adresse IP publique persistante, vous pouvez attribuer une adresse IP élastique à votre AWS compte et l'associer à une instance ou à une interface réseau. Une adresse IP élastique reste associée à votre AWS compte jusqu'à ce que vous la publiiez, et vous pouvez la déplacer d'une instance à l'autre selon vos besoins. Vous pouvez apporter votre propre plage d'adresses IP à votre compte AWS , où elle apparaît sous la forme d'un pool d'adresses, puis allouer des adresses IP Elastic à partir de votre pool d'adresses.

Pour augmenter les performances réseau et réduire la latence, vous pouvez lancer des instances dans un groupe de placement. Vous pouvez obtenir des performances de paquets par seconde (PPS) nettement supérieures grâce à une mise en réseau améliorée. Vous pouvez accélérer les applications de calcul haute performance et d'apprentissage automatique à l'aide d'un adaptateur Elastic Fabric (EFA), qui est un périphérique réseau que vous pouvez associer à un type d'instance pris en charge.

Fonctionnalités

- Régions et zones
- Adressage IP de l'EC2instance Amazon
- Types de noms EC2 d'hôte des instances Amazon
- Apportez vos propres adresses IP (BYOIP) à Amazon EC2
- Adresses IP Elastic
- Interfaces réseau Elastic
- Bande passante réseau des EC2 instances Amazon
- Mise en réseau améliorée sur les EC2 instances Amazon

- Adaptateur Elastic Fabric pour les charges de travail ML HPC et ML sur Amazon EC2
- Topologie des EC2 instances Amazon
- Groupes de placement pour vos EC2 instances Amazon
- Unité de transmission maximale du réseau (MTU) pour votre EC2 instance
- Clouds privés virtuels pour vos EC2 instances

Régions et zones

Amazon EC2 est hébergé sur plusieurs sites dans le monde entier. Ces emplacements sont composés de zones de disponibilité Régions AWS, de zones locales et de zones de longueur d'onde. AWS Outposts

- Chaque région constitue une zone géographique séparée.
- Les zones de disponibilité sont des emplacements multiples isolés dans chaque région.
- Les Local Zones vous permettent de placer des ressources, telles que le calcul et le stockage, dans plusieurs emplacements plus proches de vos utilisateurs finaux.
- AWS Outposts apporte AWS des services, une infrastructure et des modèles d'exploitation natifs à pratiquement tous les centres de données, espaces de colocation ou installations sur site.
- Les zones Wavelength permettent aux développeurs de créer des applications qui offrent des latences ultra-faibles aux appareils 5G et aux utilisateurs finaux. Wavelength déploie des services de AWS calcul et de stockage standard à la périphérie des réseaux 5G des opérateurs de télécommunications.

AWS exploite state-of-the-art des centres de données à haute disponibilité. Bien qu'elles soient rares, des pannes touchant la disponibilité des instances se trouvant au même emplacement peuvent se produire. Si vous hébergez toutes vos instances dans un seul emplacement touché par une panne, aucune de vos instances ne sera disponible.

Table des matières

Régions

Chaque région est conçue pour être complètement isolée des autres régions . Cela permet d'atteindre la plus grande tolérance aux pannes possible et une stabilité optimale.

Lorsque vous consultez vos ressources, vous voyez uniquement celles liées à la région que vous avez spécifiée. Cela est dû au fait que les régions sont éloignées les unes des autres et que nous ne répliquons pas automatiquement les ressources entre régions .

Lorsque vous lancez une instance, vous devez en sélectionner une AMI qui se trouve dans la même région. S'il se AMI trouve dans une autre région, vous pouvez le AMI copier dans la région que vous utilisez. Pour de plus amples informations, veuillez consulter Copier un Amazon EC2 AMI.

Notez qu'il n'y a pas de frais pour le transfert de données entre régions. Pour plus d'informations, consultez Amazon EC2 Pricing - Data Transfer.

Régions disponibles

Votre compte détermine les régions qui vous sont disponibles.

- An Compte AWS fournit plusieurs régions afin que vous puissiez lancer des EC2 instances Amazon dans des endroits qui répondent à vos besoins. Par exemple, vous pouvez souhaiter

lancer des instances en Europe afin d'être plus proche de vos clients européens ou pour satisfaire à des exigences légales.

- Un compte AWS GovCloud (US-West) donne accès à la région AWS GovCloud (US-Ouest) et à la région AWS GovCloud (US-Est). Pour de plus amples informations, veuillez consulter AWS GovCloud (US).
- Un compte Amazon AWS (Chine) permet d'accéder uniquement aux régions de Pékin et de Ningxia. Pour plus d'informations, veuillez consulter Amazon Web Services en Chine.

Le tableau suivant répertorie les régions fournies par un Compte AWS. Vous ne pouvez pas décrire ou accéder à des régions supplémentaires à partir d'une région Compte AWS, telle que la AWS GovCloud (US) Regions ou les régions de Chine. Pour utiliser une région introduite après le 20 mars 2019, vous devez l'activer. Pour plus d'informations, voir Spécifier les AWS régions que votre compte peut utiliser dans le Guide de AWS Account Management référence.

Code	Nom	Statut d'inscription
us-east-1	USA Est (Virginie du Nord)	Facultatif
us-east-2	USA Est (Ohio)	Facultatif
us-west-1	USA Ouest (Californie du Nord)	Facultatif
us-west-2	USA Ouest (Oregon)	Facultatif
af-south-1	Afrique (Le Cap)	Obligatoire
ap-east-1	Asie-Pacifique (Hong Kong)	Obligatoire
ap-south-2	Asie-Pacifique (Hyderabad)	Obligatoire
ap-southeast-3	Asie-Pacifique (Jakarta)	Obligatoire
ap-southeast-5	Asie-Pacifique (Malaisie)	Obligatoire
ap-southeast-4	Asie-Pacifique (Melbourne)	Obligatoire
ap-south-1	Asie-Pacifique (Mumbai)	Facultatif
ap-northeast-3	Asie-Pacifique (Osaka)	Facultatif

Code	Nom	Statut d'inscription
ap-northeast-2	Asie-Pacifique (Séoul)	Facultatif
ap-southeast-1	Asie-Pacifique (Singapour)	Facultatif
ap-southeast-2	Asie-Pacifique (Sydney)	Facultatif
ap-northeast-1	Asie-Pacifique (Tokyo)	Facultatif
ca-central-1	Canada (Centre)	Facultatif
ca-west-1	Canada Ouest (Calgary)	Obligatoire
cn-north-1	Chine (Beijing)	Facultatif
cn-northwest-1	Chine (Ningxia)	Facultatif
eu-central-1	Europe (Francfort)	Facultatif
eu-west-1	Europe (Irlande)	Facultatif
eu-west-2	Europe (Londres)	Facultatif
eu-south-1	Europe (Milan)	Obligatoire
eu-west-3	Europe (Paris)	Facultatif
eu-south-2	Europe (Espagne)	Obligatoire
eu-north-1	Europe (Stockholm)	Facultatif
eu-central-2	Europe (Zurich)	Obligatoire
il-central-1	Israël (Tel Aviv)	Obligatoire
me-south-1	Moyen-Orient (Bahreïn)	Obligatoire
me-central-1	Moyen-Orient (UAE)	Obligatoire
sa-east-1	Amérique du Sud (São Paulo)	Facultatif

Pour plus d'informations, consultez Infrastructure mondiale AWS.

Points de terminaison régionaux

Lorsque vous travaillez avec une instance à l'aide de l'interface de ligne de commande ou d'APIactions, vous devez spécifier son point de terminaison régional. Pour plus d'informations sur les régions et les points de terminaison d'AmazonEC2, consultez la section Points de terminaison des EC2 services Amazon dans le guide du EC2développeur Amazon.

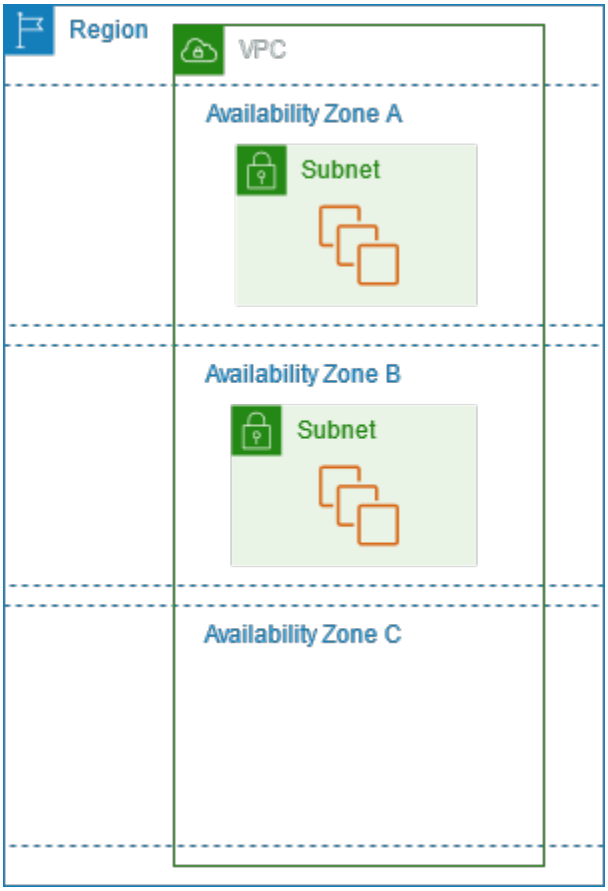
Pour plus d'informations sur les points de terminaison et les protocoles en AWS GovCloud (ouest des États-Unis), consultez la section Points de terminaison de service dans le guide de l'AWS GovCloud (US) utilisateur.

Zones de disponibilité

Chaque région se compose de plusieurs emplacements isolés appelés zones de disponibilité. Le code de la zone de disponibilité est son code de Région suivi d'un identifiant à lettre. Par exemple, `us-east-1a`.

Lorsque vous lancez une instance, vous sélectionnez une région et un cloud privé virtuel (VPC), puis vous pouvez soit sélectionner un sous-réseau dans l'une des zones de disponibilité, soit nous laisser le soin d'en choisir un pour vous. Si vous distribuez vos instances dans plusieurs zones de disponibilité et si une instance connaît une défaillance, vous pouvez concevoir votre application afin qu'une instance dans une autre zone de disponibilité puisse gérer les requêtes. Vous pouvez également utiliser les adresses IP Elastic pour masquer la défaillance d'une instance dans une zone de disponibilité en remappant rapidement l'adresse à une instance dans une autre zone de disponibilité.

Le schéma suivant illustre plusieurs zones de disponibilité dans une AWS région. La zone de disponibilité A et la zone de disponibilité B ont chacune un sous-réseau, et chaque sous-réseau possède des instances. La zone de disponibilité C n'a pas de sous-réseaux. Par conséquent, vous ne pouvez pas lancer d'instances dans cette zone de disponibilité.



Alors que les zones de disponibilité augmentent avec le temps, notre capacité à les développer peut devenir limitée. Dans ce cas, nous pouvons vous empêcher de lancer une instance dans une zone de disponibilité limitée, à moins que vous n'ayez déjà une instance dans cette zone de disponibilité. Finalement, nous pouvons également retirer la zone de disponibilité limitée de la liste des zones de disponibilité pour les nouveaux comptes. Par conséquent, votre compte peut avoir un nombre différent de zones de disponibilité disponibles dans une région qu'un autre compte.

AZ IDs

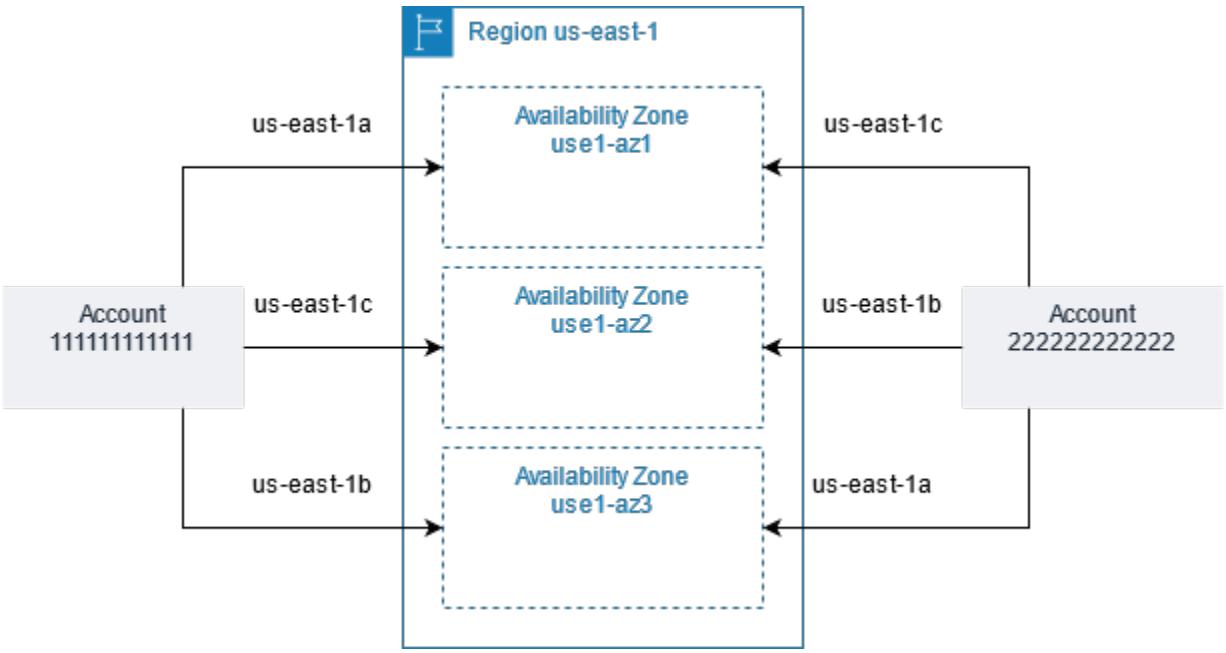
Pour garantir que les ressources sont réparties entre les zones de disponibilité d'une région, nous mappons indépendamment les zones de disponibilité aux codes de chacune Compte AWS de nos régions les plus anciennes. Par exemple, il se `us-east-1a` Compte AWS peut que votre emplacement physique ne soit pas le même que celui `us-east-1a` d'un autre Compte AWS.

Pour coordonner les zones de disponibilité entre les comptes de toutes les régions, même celles qui cartographient les zones de disponibilité, utilisez l'AZ IDs, qui sont des identifiants uniques et cohérents pour une zone de disponibilité. Par exemple, `use1-az1` il s'agit d'un identifiant AZ pour la `us-east-1` région, et il a le même emplacement physique dans chaque région Compte AWS.

Vous pouvez consulter l'AZ IDs de votre compte afin de déterminer l'emplacement physique de vos ressources par rapport aux ressources d'un autre compte. Par exemple, si vous partagez avec un autre compte un sous-réseau dans la zone de disponibilité portant l'ID `use1-az2`, ce sous-réseau est accessible par cet autre compte dans la zone de disponibilité portant également l'ID `use1-az2`.

Pour consulter l'AZ IDs de votre compte, consultez le panneau d'état du service sur le EC2tableau de bord ou utilisez la describe-availability-zones AWS CLI commande.

Le diagramme suivant illustre deux comptes avec des mappages différents entre le code de zone de disponibilité et l'ID de zone de disponibilité.



Zones de disponibilité disponibles

Chaque région possède plusieurs zones de disponibilité, comme indiqué dans la liste suivante.

- Est des États-Unis (Virginie du Nord) — `use1-az1` `use1-az2` | `use1-az3` | `use1-az4` | `use1-az5` | `use1-az6`
- Est des États-Unis (Ohio) — `use2-az1` | `use2-az2` | `use2-az3`
- Ouest des États-Unis (Californie du Nord) — `usw1-az1` | `usw1-az2` | `usw1-az3` †
- Ouest des États-Unis (Oregon) — `usw2-az1` | `usw2-az2` | `usw2-az3` | `usw2-az4`
- Afrique (Le Cap) — `afs1-az1` | `afs1-az2` | `afs1-az3`
- Asie-Pacifique (Hong Kong) — `ape1-az1` | `ape1-az2` | `ape1-az3`
- Asie-Pacifique (Hyderabad) — | | `aps2-az1` `aps2-az2` `aps2-az3`

- Asie-Pacifique (Jakarta) — apse3-az1 | apse3-az2 | apse3-az3
- Asie-Pacifique (Malaisie) — apse5-az1 | apse5-az2 | apse5-az3
- Asie-Pacifique (Melbourne) — apse4-az1 | apse4-az2 | apse4-az3
- Asie-Pacifique (Mumbai) — aps1-az1 | aps1-az2 | aps1-az3
- Asie-Pacifique (Osaka) — apne3-az1 | apne3-az2 | apne3-az3
- Asie-Pacifique (Séoul) — apne2-az1 | apne2-az2 | apne2-az3 | apne2-az4
- Asie-Pacifique (Singapour) — apse1-az1 | apse1-az2 | apse1-az3
- Asie-Pacifique (Sydney) — apse2-az1 | apse2-az2 | apse2-az3
- Asie-Pacifique (Tokyo) — apne1-az1 | apne1-az2 | apne1-az3 | apne1-az4
- Canada (Centre) — cac1-az1 | cac1-az2 | cac1-az4
- Canada-Ouest (Calgary) — caw1-az1 | caw1-az2 | caw1-az3
- Europe (Francfort) — euc1-az1 | euc1-az2 | euc1-az3
- Europe (Irlande) — euw1-az1 | euw1-az2 | euw1-az3
- Europe (Londres) — euw2-az1 | euw2-az2 | euw2-az3
- Europe (Milan) — eus1-az1 | eus1-az2 | eus1-az3
- Europe (Paris) — euw3-az1 | euw3-az2 | euw3-az3
- Europe (Espagne) — eus2-az1 | eus2-az2 | eus2-az3
- Europe (Stockholm) — eun1-az1 | eun1-az2 | eun1-az3
- Europe (Zurich) — euc2-az1 | euc2-az2 | euc2-az3
- Israël (Tel Aviv) — ilc1-az1 | ilc1-az2 | ilc1-az3
- Moyen-Orient (Bahreïn) — mes1-az1 | mes1-az2 | mes1-az3
- Moyen-Orient (UAE) — mec1-az1 | mec1-az2 | mec1-az3
- Amérique du Sud (São Paulo) — sae1-az1 | sae1-az2 | sae1-az3
- AWS GovCloud (USA Est) — usge1-az1 | | usge1-az2 usge1-az3
- AWS GovCloud (US-Ouest) — usgw1-az1 | | usgw1-az2 usgw1-az3

† Les nouveaux comptes peuvent accéder à deux zones de disponibilité dans l'ouest des États-Unis (Californie du Nord).

Instances situées dans des zones de disponibilité

Lorsque vous lancez une instance, sélectionnez une région qui rapproche vos instances de clients spécifiques, ou qui satisfait à vos exigences légales ou autres. En lançant vos instances dans des zones de disponibilité distinctes, vous pouvez protéger vos applications contre la défaillance d'un seul site de la région.

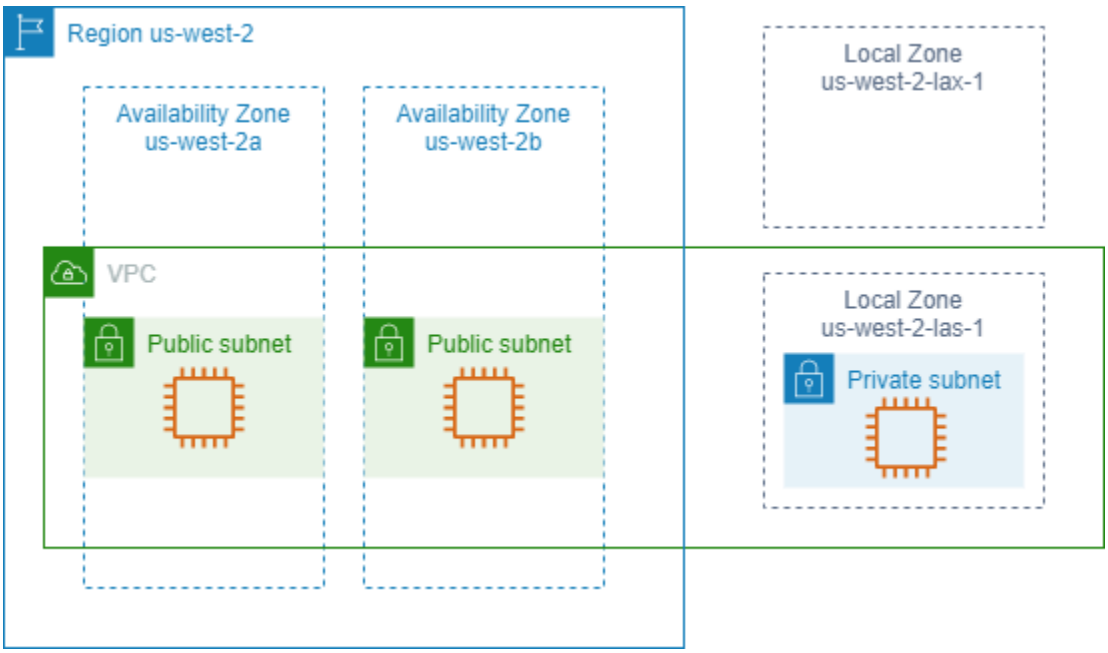
Lorsque vous lancez une instance, vous pouvez éventuellement spécifier une zone de disponibilité dans la région que vous utilisez. Si vous ne spécifiez pas de zone de disponibilité, nous sélectionnons une zone de disponibilité pour vous. Lorsque vous lancez vos instances initiales, nous vous recommandons d'accepter la zone de disponibilité par défaut, car cela nous permet de sélectionner la meilleure zone de disponibilité pour vous, en fonction de l'état de santé du système et de la capacité disponible. Si vous lancez des instances additionnelles, ne spécifiez une zone de disponibilité que si vos nouvelles instances doivent être proches ou séparées de vos instances en cours d'exécution.

Zones locales

Une zone locale est une extension d'une AWS région située à proximité géographique de vos utilisateurs. Les zones locales disposent de leurs propres connexions à Internet et de leur propre support AWS Direct Connect, de sorte que les ressources créées dans une zone locale peuvent servir les utilisateurs locaux avec des communications à faible latence. Pour plus d'informations, voir Qu'est-ce que AWS les zones locales ? dans le Guide de l'utilisateur des Zones AWS Locales.

Le code d'une zone locale est son code de Région suivi par un identifiant qui indique son emplacement physique. Par exemple, `us-west-2-lax-1` à Los Angeles.

Le schéma suivant illustre la AWS région`us-west-2`, deux de ses zones de disponibilité et deux de ses zones locales. Elle VPC couvre les zones de disponibilité et l'une des zones locales. Chaque zone du VPC possède un sous-réseau et chaque sous-réseau possède une instance.



Local Zones disponibles

Pour obtenir la liste des zones locales disponibles, consultez la section Zones locales disponibles dans le guide de l'utilisateur des zones AWS locales. Pour la liste des zones locales annoncées, consultez la section Emplacements AWS des zones locales.

Instances dans les Zones Locales

Pour utiliser une zone locale, vous devez d'abord l'activer. Créez ensuite un sous-réseau dans la zone locale. Vous pouvez spécifier le sous-réseau de zone locale lorsque vous lancez des instances, ce qui le place dans le sous-réseau de zone locale de la zone locale.

Lorsque vous lancez une instance dans une zone locale, vous allouez également une adresse IP à partir d'un groupe frontalier du réseau. Un groupe frontalier du réseau est un ensemble unique de zones de disponibilité, de zones locales ou de zones de longueur d'onde à partir AWS duquel les adresses IP sont publiées, par exemple,`us-west-2-lax-1a`. Vous pouvez allouer les adresses IP suivantes à partir d'un groupe de frontières réseau :

- Adresses Elastic fournies par Amazon IPv4
- IPv6VPCAdresses fournies par Amazon (disponibles uniquement dans les zones de Los Angeles)

Pour plus d'informations sur le lancement d'une instance dans une zone locale, consultez Getting started with AWS Local Zones dans le guide de l'utilisateur des zones AWS locales.

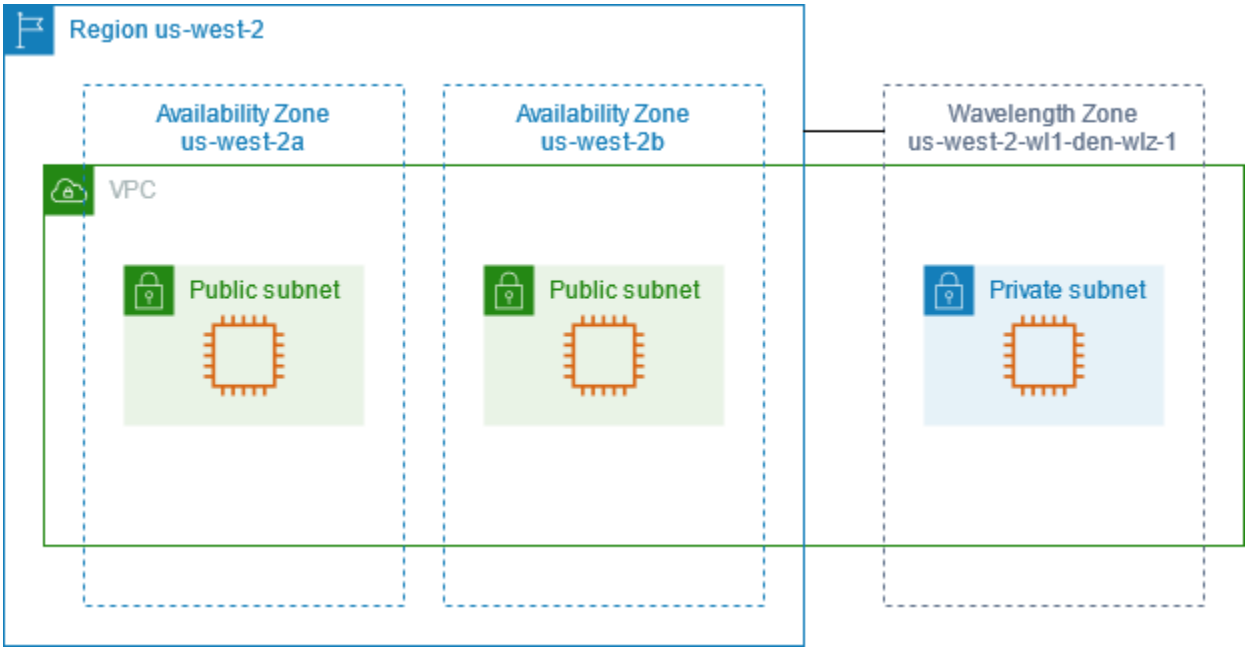
Zones Wavelength

AWS Wavelength permet aux développeurs de créer des applications offrant des latences extrêmement faibles aux appareils mobiles et aux utilisateurs finaux. Wavelength déploie des services de AWS calcul et de stockage standard à la périphérie des réseaux 5G des opérateurs de télécommunications. Les développeurs peuvent étendre un cloud privé virtuel (VPC) à une ou plusieurs zones de Wavelength, puis utiliser AWS des ressources telles que des EC2 instances Amazon pour exécuter des applications nécessitant une latence très faible et une connexion aux AWS services de la région.

Une zone Wavelength est une zone isolée située à l'emplacement du transporteur où l'infrastructure Wavelength est déployée. Les zones Wavelength sont liées à une région. Une zone Wavelength est une extension logique d'une région et est gérée par le plan de contrôle de la région.

Le code d'une zone Wavelength est son code de Région suivi par un identifiant qui indique son emplacement physique. Par exemple, `us-east-1-wl1-bos-wlz-1` à Boston.

Le schéma suivant illustre la AWS régionus-west-2, deux de ses zones de disponibilité et une zone Wavelength. Elle VPC couvre les zones de disponibilité et la zone Wavelength. Chaque zone du VPC possède un sous-réseau et chaque sous-réseau possède une instance.



Les zones Wavelength ne sont pas disponibles dans toutes les régions. Pour plus d'informations sur les régions qui prennent en charge les zones Wavelength, consultez Zones Wavelength disponibles dans le Guide du développeur AWS Wavelength .

Zones de longueur d'onde disponibles

Pour consulter la liste des zones de longueur d'onde disponibles, consultez la section « Zones de longueur d'onde disponibles » dans le AWS Wavelength guide.

Instances dans des zones Wavelength

Pour utiliser une zone Wavelength, vous devez d'abord vous inscrire à la zone. Créez ensuite un sous-réseau dans la Wavelength Zone. Vous pouvez spécifier le sous-réseau Wavelength lorsque vous lancez des instances. Vous allouez également une adresse IP de transporteur à partir d'un groupe de frontières réseau, qui est un ensemble unique de zones de disponibilité, de Local Zones ou de zones Wavelength à partir desquelles AWS annonce des adresses IP, par exemple `us-east-1-wl1-bos-wlz-1`.

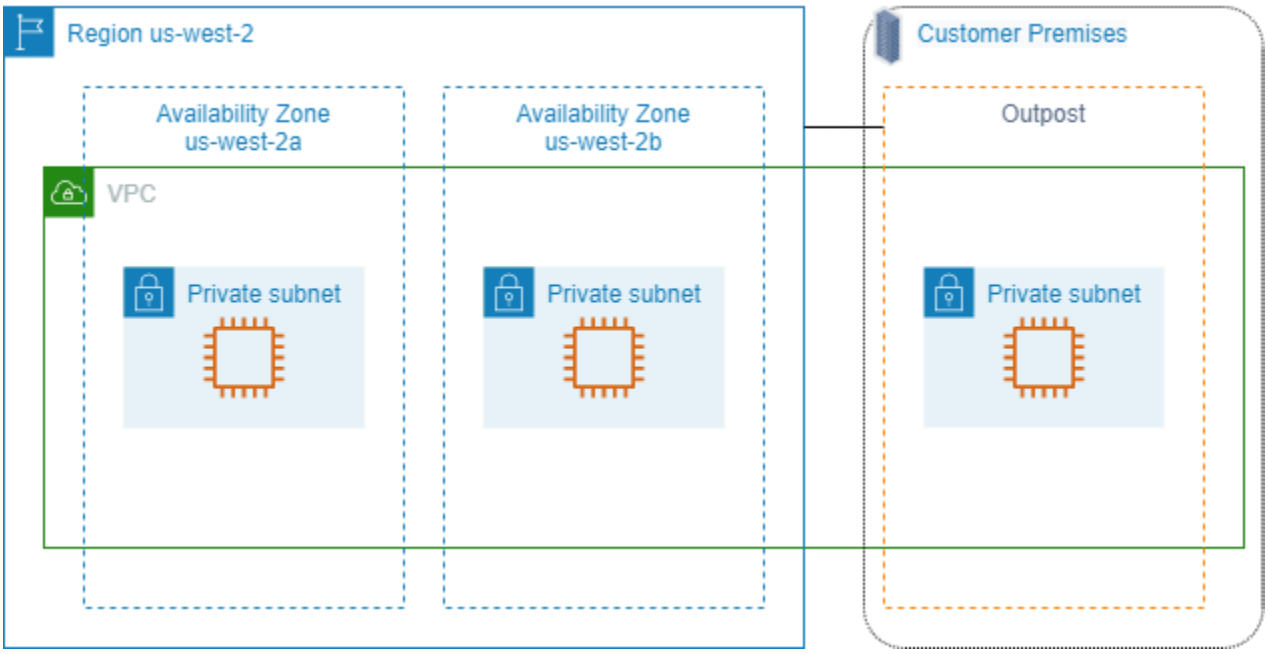
Pour step-by-step savoir comment lancer une instance dans une zone Wavelength, voir Get started with AWS Wavelength dans le Guide du AWS Wavelength développeur.

AWS Outposts

AWS Outposts est un service entièrement géré qui étend AWS l'infrastructureAPIs, les services et les outils aux locaux du client. En fournissant un accès local à l'infrastructure AWS gérée, il AWS Outposts permet aux clients de créer et d'exécuter des applications sur site en utilisant les mêmes interfaces de programmation que dans AWS les régions, tout en utilisant les ressources de calcul et de stockage locales pour réduire la latence et les besoins de traitement des données locaux.

Un avant-poste est un pool de capacités de AWS calcul et de stockage déployé sur le site d'un client. AWS exploite, surveille et gère cette capacité dans le cadre d'une AWS région. Vous pouvez créer des sous-réseaux sur votre Outpost et les spécifier lorsque vous créez des AWS ressources. Les instances des sous-réseaux Outpost communiquent avec d'autres instances de la AWS région à l'aide d'adresses IP privées, toutes au même endroit. VPC

Le schéma suivant illustre la AWS région`us-west-2`, deux de ses zones de disponibilité et un avant-poste. Elle VPC couvre les zones de disponibilité et l'avant-poste. L'Outpost se trouve dans un centre de données client sur site. Chaque zone du VPC possède un sous-réseau et chaque sous-réseau possède une instance.



Instances sur un avant-poste

Pour commencer à l'utiliser AWS Outposts, vous devez créer un avant-poste et commander une capacité d'avant-poste. AWS Outposts propose deux formats, les racks Outposts et les serveurs Outposts. Pour plus d'informations sur les configurations d'Outposts, consultez AWS Outposts Family. Une fois votre équipement Outpost installé, la capacité de calcul et de stockage est disponible lorsque vous lancez des EC2 instances sur votre Outpost.

Pour lancer EC2 des instances, vous devez créer un sous-réseau Outpost. Les groupes de sécurité contrôlent le trafic entrant et sortant pour les instances d'un sous-réseau Outpost, comme ils le font pour les instances d'un sous-réseau de zone de disponibilité. Pour vous connecter à une EC2 instance dans un sous-réseau Outpost, vous pouvez spécifier une paire de clés lorsque vous lancez l'instance, comme vous le faites pour les instances d'un sous-réseau de zone de disponibilité afin d'autoriser les connexions à utiliser. SSH

Pour plus d'informations, voir Commencer avec les racks Outposts ou Commencer avec les serveurs Outposts.

Volumes sur un rack Outposts

Si la capacité de calcul de vos Outposts se trouve sur un rack Outpost, vous pouvez créer des EBS volumes dans le sous-réseau Outpost que vous avez créé. Lorsque vous créez le volume, spécifiez le nom de la ressource Amazon (ARN) de l'Outpost.

La commande create-volume suivante crée un volume vide de 50 Go sur l'outpost spécifié.

```
aws ec2 create-volume --availability-zone us-east-2a --outpost-arn arn:aws:outposts:us-east-2:123456789012:outpost/op-03e6fecad652a6138 --size 50
```

Vous pouvez modifier dynamiquement la taille de vos volumes Amazon EBS gp2 sans les détacher. Pour plus d'informations sur la modification d'un volume sans le détacher, consultez la section Demander des modifications à vos EBS volumes dans le guide de l'EBSutilisateur Amazon.

Nous vous recommandons de limiter le volume racine d'une instance sur un rack Outpost à 30 GiB ou moins. Vous pouvez spécifier des volumes de données dans le mappage de périphériques par blocs de l'instance AMI ou de l'instance afin de fournir un stockage supplémentaire. Pour supprimer les blocs inutilisés du volume de démarrage, consultez la section Comment créer des EBS volumes épars sur le blog du réseau de AWS partenaires.

Nous vous recommandons d'augmenter le NVMe délai d'expiration du volume racine. Pour plus d'informations, consultez la section Délai d'expiration des opérations d'E/S dans le guide de EBSl'utilisateur Amazon.

Volumes sur un serveur Outposts

Les instances des serveurs Outposts fournissent des volumes de stockage d'instance mais ne les prennent pas en chargeEBS. Choisissez un produit EBS soutenu par Amazon AMI avec un seul EBS instantané. Choisissez une taille d'instance offrant suffisamment de stockage pour répondre aux besoins de votre application. Pour de plus amples informations, veuillez consulter Limites du stockage d'instances.

Adressage IP de l'EC2instance Amazon

Amazon EC2 et Amazon VPC prennent en charge à la fois les protocoles d'IPv6adressage IPv4 et d'adressage. Par défaut, Amazon VPC utilise le protocole d'IPv4adressage ; vous ne pouvez pas désactiver ce comportement. Lorsque vous créez unVPC, vous devez spécifier un IPv4 CIDR bloc (une plage d'IPv4adresses privées). Vous pouvez éventuellement attribuer un IPv6 CIDR bloc à votre VPC et attribuer IPv6 des adresses de ce bloc à des instances de vos sous-réseaux.

Table des matières

- IPv6adresses
- EC2noms d'hôte des instances
- Adresses lien-local
- Gérez les IPv4 adresses de vos EC2 instances
- Gérez les IPv6 adresses de vos EC2 instances
- Plusieurs adresses IP pour vos EC2 instances
- Configuration des IPv4 adresses privées secondaires pour les instances Windows

IPv4Adresses privées

Une IPv4 adresse privée est une adresse IP qui n'est pas accessible via Internet. Vous pouvez utiliser des IPv4 adresses privées pour communiquer entre les instances d'une même instanceVPC. Pour plus d'informations sur les normes et les spécifications relatives IPv4 aux adresses privées, voir RFC1918. Nous attribuons IPv4 des adresses privées aux instances qui utilisentDHCP.

> **Note**
>
> Vous pouvez créer un VPC avec un CIDR bloc routable publiquement qui se situe en dehors des plages d'IPv4adresses privées spécifiées en RFC 1918. Toutefois, dans le cadre de cette documentation, nous appelons IPv4 adresses privées (ou « adresses IP privées ») les adresses IP qui se trouvent à votre IPv4 CIDR portée. VPC

VPCles sous-réseaux peuvent être de l'un des types suivants :

- IPv4sous-réseaux -only : vous ne pouvez créer des ressources dans ces sous-réseaux qu'avec des IPv4 adresses qui leur sont attribuées.
- IPv6sous-réseaux -only : vous ne pouvez créer des ressources dans ces sous-réseaux qu'avec des IPv6 adresses qui leur sont attribuées.
- IPv4et IPv6 sous-réseaux : vous pouvez créer des ressources dans ces sous-réseaux en leur attribuant l'une IPv4 ou l'autre IPv6 des adresses.

Lorsque vous lancez une EC2 instance dans un sous-réseau IPv4 uniquement ou à double pile (IPv4etIPv6), l'instance reçoit une adresse IP privée principale provenant de la plage d'IPv4adresses du sous-réseau. Pour plus d'informations, consultez la section Adressage IP dans le guide de

VPC l'utilisateur Amazon. Si vous ne spécifiez pas d'adresse IP privée principale lorsque vous lancez l'instance, nous sélectionnons pour vous une adresse IP disponible dans la IPv4 plage du sous-réseau. Chaque instance possède une interface réseau par défaut (eth0) à laquelle est attribuée l'IPv4adresse privée principale. Vous pouvez également spécifier des IPv4 adresses privées supplémentaires, appelées IPv4adresses privées secondaires. Contrairement aux adresses IP privées principales, les adresses IP privées secondaires peuvent être réaffectées d'une instance à une autre. Pour de plus amples informations, veuillez consulter Plusieurs adresses IP pour vos EC2 instances.

Une IPv4 adresse privée, qu'il s'agisse d'une adresse principale ou secondaire, reste associée à l'interface réseau lorsque l'instance est arrêtée et démarrée, ou mise en veille prolongée et est libérée lorsque l'instance est arrêtée.

IPv4Adresses publiques

Une adresse IP publique est une IPv4 adresse accessible depuis Internet. Vous pouvez utiliser des adresses publiques pour les communications entre vos instances et Internet.

Lorsque vous lancez une instance dans une instance par défautVPC, nous lui attribuons une adresse IP publique par défaut. Lorsque vous lancez une instance dans une instance autre que celle par défautVPC, le sous-réseau possède un attribut qui détermine si les instances lancées dans ce sous-réseau reçoivent une adresse IP publique du pool d'adresses publiquesIPv4. Par défaut, nous n'attribuons aucune adresse IP publique aux instances lancées dans un sous-réseau autre que celui défini par défaut.

Vous pouvez contrôler si votre instance reçoit une adresse IP publique en procédant comme suit :

- Modifier l'attribut d'adressage IP public de votre sous-réseau. Pour plus d'informations, consultez Modifier l'attribut d'IPv4adressage public de votre sous-réseau dans le guide de l'VPCutilisateur Amazon.
- Activer ou désactiver la fonction d'adressage IP public pendant le lancement, ce qui remplace l'attribut d'adressage IP public du sous-réseau. Pour de plus amples informations, veuillez consulter Attribuer une IPv4 adresse publique lors du lancement de l'instance.
- Vous pouvez annuler l'attribution d'une adresse IP publique à votre instance après le lancement en gérant les adresses IP associées à une interface réseau.

Une adresse IP publique est attribuée à votre instance à partir du pool d'IPv4adresses publiques d'Amazon et n'est pas associée à votre AWS compte. Lorsqu'une adresse IP publique est dissociée

de votre instance, elle est réintégrée dans le pool d'IPv4adresses publiques et vous ne pouvez pas la réutiliser.

Dans certains cas, nous publions l'adresse IP publique de votre instance ou nous lui en attribuons une nouvelle :

- Nous libérons l'adresse IP publique de votre instance lorsqu'elle est arrêtée, mise en veille ou mise hors service. Toute instance arrêtée ou mise en veille de manière prolongée reçoit une nouvelle adresse IP publique au démarrage.
- L'adresse IP publique de votre instance est libérée lorsque vous lui associez une adresse IP Elastic. Lorsque vous dissociez l'adresse IP Elastic de votre instance, cette dernière reçoit une nouvelle adresse IP publique.
- Si l'adresse IP publique de votre instance VPC a été publiée, elle n'en recevra pas de nouvelle si plusieurs interfaces réseau sont associées à votre instance.
- Si l'adresse IP publique de votre instance est libérée alors qu'elle a une adresse IP privée secondaire associée à une adresse IP Elastic, l'instance ne reçoit pas de nouvelle adresse IP publique.

Si vous avez besoin d'une adresse IP publique permanente qui peut être associée aux instances et en être dissociée comme vous le souhaitez, utilisez plutôt une adresse IP Elastic.

Si vous utilisez Dynamic DNS pour associer un DNS nom existant à l'adresse IP publique d'une nouvelle instance, la propagation de l'adresse IP sur Internet peut prendre jusqu'à 24 heures. De ce fait, de nouvelles instances peuvent ne pas recevoir le trafic alors que des instances terminées continuent de recevoir des demandes. Pour résoudre ce problème, utilisez une adresse IP Elastic. Vous pouvez allouer votre propre adresse IP Elastic, puis l'associer à votre instance. Pour de plus amples informations, veuillez consulter Adresses IP Elastic.

Si vous utilisez Amazon VPC IP Address Manager (IPAM), vous pouvez obtenir un bloc contigu d'IPv4adresses publiques AWS et l'utiliser pour allouer des adresses IP élastiques aux AWS ressources. L'utilisation de blocs d'IPv4adresses contigus permet de réduire considérablement les frais de gestion des listes de contrôle d'accès de sécurité et de simplifier l'allocation et le suivi des adresses IP pour les entreprises qui se développent. AWS Pour plus d'informations, consultez la section Allocation d'adresses IP élastiques séquentielles à partir d'un IPAM pool dans le guide de VPC IPAM l'utilisateur Amazon.

Note

- AWS frais pour toutes les IPv4 adresses publiques, y compris les IPv4 adresses publiques associées aux instances en cours d'exécution et les adresses IP Elastic. Pour plus d'informations, consultez l'onglet IPv4Adresse publique sur la page de VPC tarification d'Amazon.
- Les instances qui accèdent à d'autres instances via leur adresse NAT IP publique sont facturées pour le transfert de données régional ou Internet, selon que les instances se trouvent ou non dans la même région.

Optimisation des IPv4 adresses publiques

AWS frais pour toutes les IPv4 adresses publiques, y compris les IPv4 adresses publiques associées aux instances en cours d'exécution et les adresses IP Elastic. Pour plus d'informations, consultez l'onglet IPv4Adresse publique sur la page de VPC tarification d'Amazon.

La liste suivante contient les mesures que vous pouvez prendre pour optimiser le nombre d'IPv4adresses publiques que vous utilisez :

- Utilisez un équilibreur de charge élastique pour équilibrer la charge du trafic vers vos EC2 instances et désactivez l'attribution automatique d'une adresse IP publique sur le serveur principal ENI attribué aux instances. Les équilibreurs de charge utilisent une IPv4 adresse publique unique, ce qui réduit le nombre d'IPv4adresses publiques. Vous souhaiterez peut-être également consolider les équilibreurs de charge existants afin de réduire davantage le nombre d'IPv4adresses publiques.
- Si la seule raison d'utiliser une NAT passerelle est d'accéder à une EC2 instance SSH d'un sous-réseau privé pour des raisons de maintenance ou d'urgence, envisagez plutôt d'utiliser EC2Instance Connect Endpoint. Avec EC2 Instance Connect Endpoint, vous pouvez vous connecter à une instance depuis Internet sans que celle-ci ait besoin d'une IPv4 adresse publique.
- Si vos EC2 instances se trouvent dans un sous-réseau public auquel des adresses IP publiques leur sont attribuées, envisagez de les déplacer vers un sous-réseau privé, de supprimer les adresses IP publiques et d'utiliser une NATpasserelle publique pour autoriser l'accès à vos EC2 instances et en provenance de celles-ci. L'utilisation des NAT passerelles comporte des considérations financières. Utilisez cette méthode de calcul pour déterminer si les NAT passerelles

sont rentables. Vous pouvez obtenir les informations `Number of public IPv4 addresses` nécessaires à ce calcul en créant un rapport sur les coûts AWS de facturation et l'utilisation.

```
NAT gateway per hour + NAT gateway public IPs + NAT gateway transfer / Existing
 public IP cost
```

Où :

- `NAT gateway per hour = $0.045 * 730 hours in a month * Number of Availability Zones the NAT gateways are in`
- `NAT gateway public IPs = $0.005 * 730 hours in a month * Number of IPs associated with your NAT gateways`
- `NAT gateway transfer = $0.045 * Number of GBs that will go through the NAT gateway in a month`
- `Existing public IP cost = $0.005 * 730 hours in a month * Number of public IPv4 addresses`

Si le total est inférieur à 1, les NAT passerelles sont moins chères que les IPv4 adresses publiques.

- Utilisez-le AWS PrivateLinkpour vous connecter en privé à AWS des services ou à des services hébergés par d'autres AWS comptes plutôt que d'utiliser IPv4 des adresses publiques et des passerelles Internet.
- Apportez votre propre plage d'adresses IP (BYOIP) AWS et utilisez-la pour les IPv4 adresses publiques plutôt que d'utiliser des adresses publiques IPv4 appartenant à Amazon.
- Désactivez l'attribution automatique d'une IPv4 adresse publique pour les instances lancées dans des sous-réseaux. Cette option est généralement désactivée par défaut VPCs lorsque vous créez un sous-réseau, mais vous devez vérifier vos sous-réseaux existants pour vous assurer qu'elle est désactivée.
- Si certaines de vos EC2 instances n'ont pas besoin d'IPv4adresses publiques, vérifiez que l'attribution automatique d'une adresse IP publique est désactivée sur les interfaces réseau associées à vos instances.
- Configurez les points de terminaison de l'accélérateur AWS Global Accelerator pour les EC2 instances situées dans des sous-réseaux privés afin de permettre au trafic Internet de circuler directement vers les points de terminaison de votre réseau VPCs sans avoir besoin d'adresses IP publiques. Vous pouvez également apporter vos propres adresses AWS Global Accelerator et utiliser vos propres IPv4 adresses pour les adresses IP statiques de votre accélérateur.

IPv6adresses

IPv6les adresses sont uniques au monde et peuvent être configurées pour rester privées ou accessibles via Internet. L'IPv6adressage public et privé est disponible en AWS :

- Privé IPv6 : AWS considère les IPv6 adresses privées comme celles qui ne sont pas annoncées et à partir desquelles il n'est pas possible de faire de la publicité sur Internet. AWS
- Public IPv6 : AWS prend en compte IPv6 les adresses publiques à partir AWS desquelles la publicité est faite sur Internet.

Pour plus d'informations sur les IPv6 adresses publiques et privées, consultez les IPv6adresses dans le guide de VPC l'utilisateur Amazon.

Vos EC2 instances reçoivent une IPv6 adresse si un IPv6 CIDR bloc est associé à votre sous-réseau VPC and, et si l'une des conditions suivantes est vraie :

- Votre sous-réseau est configuré pour attribuer automatiquement une IPv6 adresse à une instance lors du lancement. Pour plus d'informations, consultez Modifier les attributs d'adressage IP de votre sous-réseau.
- Vous attribuez une IPv6 adresse à votre instance lors du lancement.
- Vous attribuez une IPv6 adresse à l'interface réseau principale de votre instance après le lancement.
- Vous attribuez une IPv6 adresse à une interface réseau dans le même sous-réseau et vous attachez l'interface réseau à votre instance après le lancement.

Lorsque votre instance reçoit une IPv6 adresse lors du lancement, celle-ci est associée à l'interface réseau principale (eth0) de l'instance. Vous pouvez gérer les IPv6 adresses de l'interface réseau principale (eth0) de vos instances de la manière suivante :

- Attribuez et annulez IPv6 des adresses depuis l'interface réseau. Le nombre d'IPv6adresses que vous pouvez attribuer à une interface réseau et le nombre d'interfaces réseau que vous pouvez associer à une instance varient en fonction du type d'instance. Pour de plus amples informations, veuillez consulter Nombre maximum d'adresses IP par interface réseau.
- Activez une IPv6 adresse principale. Une IPv6 adresse principale vous permet d'éviter de perturber le trafic vers les instances ouENIs. Pour plus d'informations, consultez Créez une interface réseau pour votre EC2 instance ou Gérez les adresses IP de votre interface réseau.

Une IPv6 adresse persiste lorsque vous arrêtez et démarrez votre instance, ou lorsque vous la mettez en veille prolongée et que vous la redémarrez, et elle est publiée lorsque vous mettez fin à votre instance. Vous ne pouvez pas réattribuer une IPv6 adresse alors qu'elle est assignée à une autre interface réseau. Vous devez d'abord annuler son attribution.

Vous pouvez contrôler si les instances sont accessibles via leurs IPv6 adresses en contrôlant le routage de votre sous-réseau ou en utilisant les ACL règles du groupe de sécurité et du réseau. Pour plus d'informations, consultez la section Confidentialité du trafic interréseau dans le guide de l'VPCutilisateur Amazon.

Pour plus d'informations sur les plages d'IPv6adresses réservées, consultez les sections Registre d'adresses IANA IPv6 à usage spécial et. RFC4291

EC2noms d'hôte des instances

Lorsque vous créez une EC2 instance, AWS crée un nom d'hôte pour cette instance. Pour plus d'informations sur les types de noms d'hôtes et sur la manière dont ils sont fournis AWS, consultez. Types de noms EC2 d'hôte des instances Amazon Amazon fournit un DNS serveur qui résout les noms d'hôte et les adresses fournis par Amazon. IPv4 IPv6 Le DNS serveur Amazon est situé à la base de la portée de votre VPC réseau, plus deux. Pour plus d'informations, consultez DNSles attributs correspondants VPC dans le guide de VPC l'utilisateur Amazon.

Adresses lien-local

Les adresses lien-local sont des adresses IP connues et non routables. Amazon EC2 utilise les adresses issues de l'espace d'adressage lien-local pour fournir des services accessibles uniquement depuis une EC2 instance. Ces services ne s'exécutent pas sur l'instance, ils s'exécutent sur l'hôte sous-jacent. Lorsque vous accédez aux adresses lien-local pour ces services, vous communiquez soit avec l'hyperviseur Xen, soit avec le contrôleur Nitro.

Plage d'adresses lien-local

- IPv4— 169.254.0.0/16 (169.254.0.0 à 169.254.255.255)
- IPv6— fe80 : :/10

Services auxquels vous accédez à l'aide d'adresses lien-local

- Service des métadonnées d'instance

- Amazon Route 53 Resolver(également connu sous le nom de DNS serveur Amazon)
- Service de synchronisation temporelle d'Amazon
- AWS KMSserveurs

Gérez les IPv4 adresses de vos EC2 instances

Vous pouvez attribuer une IPv4 adresse publique à votre instance lorsque vous la lancez. Vous pouvez consulter les IPv4 adresses de votre instance dans la console via la page Instances ou la page Interfaces réseau.

Table des matières

Afficher les IPv4 adresses

Vous pouvez utiliser la EC2 console Amazon pour consulter les IPv4 adresses publiques et privées de vos instances. Vous pouvez également déterminer les IPv4 adresses publiques IPv4 et privées de votre instance à partir de celle-ci en utilisant les métadonnées de l'instance. Pour de plus amples informations, veuillez consulter Utiliser les métadonnées de l'instance pour gérer votre EC2 instance.

L'IPv4adresse publique est affichée en tant que propriété de l'interface réseau dans la console, mais elle est mappée à l'IPv4adresse privée principale viaNAT. Par conséquent, si vous inspectez les propriétés de votre interface réseau sur votre instance, par exemple via `ifconfig` (Linux) ou `ipconfig` (Windows), l'IPv4adresse publique n'est pas affichée. Pour déterminer l'IPv4adresse publique de votre instance à partir d'une instance, utilisez les métadonnées de l'instance.

Pour afficher les IPv4 adresses d'une instance à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell).

Pour déterminer les IPv4 adresses de votre instance à l'aide des métadonnées de l'instance

1. Connectez-vous à votre instance. Pour de plus amples informations, veuillez consulter Connect à votre EC2 instance.
2. Utilisez la commande suivante pour accéder à l'adresse IP privée.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/local-ipv4
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4
   ```

   Tools for Windows PowerShell

   ```
   PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/local-ipv4
   ```

3. Utilisez la commande suivante pour accéder à l'adresse IP publique. Notez que si une adresse IP Elastic est associée à l'instance, la valeur renvoyée est celle de l'adresse IP Elastic.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/public-ipv4
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-ipv4
   ```

   Tools for Windows PowerShell

   ```
   PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/public-ipv4
   ```

Attribuer une IPv4 adresse publique lors du lancement de l'instance

Chaque sous-réseau a un attribut qui détermine si une adresse IP publique est attribuée aux instances lancées dans ce sous-réseau. Par défaut, cet attribut est configuré sur false pour les sous-réseaux personnalisés et sur true pour les sous-réseaux par défaut. Lorsque vous lancez une instance, une fonctionnalité d'IPv4adressage public est également disponible pour vous permettre de contrôler si une IPv4 adresse publique est attribuée à votre instance ; vous pouvez remplacer le comportement par défaut de l'attribut d'adressage IP du sous-réseau. L'IPv4adresse publique est attribuée à partir du pool d'IPv4adresses publiques d'Amazon et est attribuée à l'interface réseau avec l'index de périphérique eth0. Cette fonction dépend de certaines conditions au moment du lancement de votre instance.

Considérations

- Vous pouvez annuler l'attribution de l'adresse IP publique à votre instance après le lancement en gérant les adresses IP associées à une interface réseau. Pour plus d'informations sur les IPv4 adresses publiques, consultezIPv4Adresses publiques.
- Vous ne pouvez pas attribuer automatiquement une adresse IP publique si vous spécifiez plusieurs interfaces réseau. En outre, vous ne pouvez pas remplacer le paramètre de sous-réseau à l'aide de la fonction « auto-assign IP public », si vous spécifiez une interface réseau existante pour eth0.
- Que vous attribuiez une adresse IP publique à votre instance lors du lancement ou non, vous pouvez associer une adresse IP élastique à votre instance après son lancement. Pour de plus amples informations, veuillez consulter Adresses IP Elastic. Vous pouvez également modifier le comportement d'IPv4adressage public de votre sous-réseau. Pour plus d'informations, consultez Modifier l'attribut d'IPv4adressage public de votre sous-réseau.

Pour attribuer une IPv4 adresse publique lors du lancement de l'instance à l'aide de la console

Suivez la procédure décrite pour lancer une instance, et lorsque vous configurez les Paramètres réseau, choisissez l'option Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique).

Pour activer ou désactiver la fonctionnalité d'adressage IP publique à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez Accédez à Amazon EC2.

- Utilisez l'option `--associate-public-ip-address` ou `--no-associate-public-ip-address` avec la commande run-instances (AWS CLI)

- Utilisez le `-AssociatePublicIp` paramètre avec la New-EC2Instancecommande (AWS Tools for Windows PowerShell)

Gérez les IPv6 adresses de vos EC2 instances

Vous pouvez consulter les IPv6 adresses attribuées à votre instance, attribuer une IPv6 adresse publique à votre instance ou annuler l'attribution d'une IPv6 adresse à votre instance. Vous pouvez afficher ces adresses dans la console via la page Instances ou la page Interfaces réseau.

Table des matières

Attribuer une IPv6 adresse à une instance

Si des IPv6 CIDR blocs sont associés à votre sous-réseau VPC et à votre sous-réseau, vous pouvez attribuer une IPv6 adresse à votre instance pendant ou après le lancement. L'IPv6adresse est attribuée à partir de la plage d'IPv6adresses du sous-réseau et est attribuée à l'interface réseau avec l'indice de périphérique eth0.

Pour attribuer une IPv6 adresse lors du lancement de l'instance

Suivez la procédure pour lancer une instance, puis lorsque vous configurez les paramètres réseau, choisissez l'option Attribuer automatiquement une IPv6 adresse IP.

Pour attribuer une IPv6 adresse après le lancement

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez votre instance et choisissez Actions, Mise en réseau, puis Gérer les adresses IP privées.
4. Sélectionnez l'interface réseau. Sous IPv6adresses, sélectionnez Attribuer une nouvelle adresse IP. Entrez une IPv6 adresse dans la plage du sous-réseau ou laissez le champ vide pour permettre à Amazon de choisir une IPv6 adresse pour vous.
5. Choisissez Save (Enregistrer).

Pour attribuer une IPv6 adresse à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez Accédez à Amazon EC2.

- Utilisez l'option `--ipv6-addresses` avec la commande run-instances (AWS CLI)
- Utilisez la `Ipv6Addresses` propriété for `-NetworkInterface` dans la New-EC2Instancecommande (AWS Tools for Windows PowerShell)
- assign-ipv6-addresses (AWS CLI)
- Register-EC2IpvAddressList(6AWS Tools for Windows PowerShell)

Afficher les IPv6 adresses

Vous pouvez utiliser la EC2 console Amazon et AWS CLI les métadonnées des instances pour consulter les IPv6 adresses de vos instances.

Pour afficher les IPv6 adresses d'une instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance.
4. Dans l'onglet Réseau, localisez IPv6les adresses.

Pour afficher les IPv6 adresses d'une instance à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell).

Pour afficher les IPv6 adresses d'une instance à l'aide des métadonnées de l'instance

1. Connectez-vous à votre instance. Pour de plus amples informations, veuillez consulter Connect à votre EC2 instance.
2. Obtenez l'MACadresse de l'instance auprès de`http://169.254.169.254/latest/meta-data/network/interfaces/macs/`.

3. Utilisez la commande suivante pour afficher l'IPv6adresse.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/network/interfaces/macs/mac-address/ipv6s
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/
   macs/mac-address/ipv6s
   ```

   Tools for Windows PowerShell

   ```
   PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/network/
   interfaces/macs/mac-address/ipv6s
   ```

Annuler l'attribution d'une IPv6 adresse à une instance

Vous pouvez annuler l'attribution d'une IPv6 adresse à une instance à tout moment.

Pour annuler l'attribution d'une IPv6 adresse à une instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez votre instance et choisissez Actions, Mise en réseau, puis Gérer les adresses IP privées.
4. Sélectionnez l'interface réseau. Sous IPv6adresses, choisissez Annuler l'attribution à côté de l'IPv6adresse.
5. Choisissez Save (Enregistrer).

Pour annuler l'attribution d'une IPv6 adresse à une instance à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez Accédez à Amazon EC2.

- unassign-ipv6-addresses (AWS CLI)
- Unregister-EC2IpvAddressList(6AWS Tools for Windows PowerShell).

Plusieurs adresses IP pour vos EC2 instances

Vous pouvez spécifier plusieurs adresses privées IPv4 et IPv6 adresses pour vos instances. Le nombre d'interfaces réseau, d'adresses privées IPv4 et d'IPv6adresses que vous pouvez spécifier pour une instance dépend du type d'instance. Pour de plus amples informations, veuillez consulter Nombre maximum d'adresses IP par interface réseau.

Il peut être utile d'attribuer plusieurs adresses IP à une instance de votre ordinateur VPC pour effectuer les opérations suivantes :

- Hébergez plusieurs sites Web sur un seul serveur en utilisant plusieurs SSL certificats sur un même serveur et en associant chaque certificat à une adresse IP spécifique.
- Faire fonctionner les composants des réseaux tels que les pare-feu ou les équilibreurs de charge qui ont plusieurs adresses IP pour chaque interface réseau.
- Rediriger le trafic interne vers une instance de secours en cas d'échec de votre instance, en réattribuant l'adresse IP secondaire à l'instance de secours.

Sommaire

Utilisation de plusieurs adresses IP

La liste suivante explique le fonctionnement de plusieurs adresses IP avec les interfaces réseau :

- Vous pouvez attribuer une IPv4 adresse privée secondaire à n'importe quelle interface réseau.
- Vous pouvez attribuer plusieurs IPv6 adresses à une interface réseau située dans un sous-réseau auquel est associé un IPv6 CIDR bloc.
- Vous devez choisir une IPv4 adresse secondaire dans la plage de IPv4 CIDR blocs du sous-réseau pour l'interface réseau.

- Vous devez choisir IPv6 des adresses dans la plage de IPv6 CIDR blocs du sous-réseau pour l'interface réseau.
- Vous associez des groupes de sécurité aux interfaces réseau, pas d'adresses IP individuelles. Par conséquent, chaque adresse IP que vous spécifiez dans une interface réseau est soumise au groupe de sécurité de son interface réseau.
- Plusieurs adresses IP peuvent être attribuées aux interfaces réseau liées aux instances en cours d'exécution ou arrêtées, ou leur attribution à ces interfaces peut être annulée.
- Les IPv4 adresses privées secondaires attribuées à une interface réseau peuvent être réattribuées à une autre si vous l'autorisez explicitement.
- Une IPv6 adresse ne peut pas être réattribuée à une autre interface réseau ; vous devez d'abord annuler l'attribution de l'IPv6adresse de l'interface réseau existante.
- Lorsque vous attribuez plusieurs adresses IP à une interface réseau à l'aide des outils de ligne de commandeAPI, l'opération entière échoue si l'une des adresses IP ne peut pas être attribuée.
- Les IPv4 adresses privées principales, les IPv4 adresses privées secondaires, les adresses IP élastiques et IPv6 les adresses restent associées à une interface réseau secondaire lorsqu'elle est détachée d'une instance ou attachée à une instance.
- Bien que vous ne puissiez pas détacher l'interface réseau principale d'une instance, vous pouvez réattribuer l'IPv4adresse privée secondaire de l'interface réseau principale à une autre interface réseau.

La liste suivante explique comment plusieurs adresses IP fonctionnent avec les adresses IP Elastic (IPv4uniquement) :

- Chaque IPv4 adresse privée peut être associée à une seule adresse IP élastique, et vice versa.
- Lorsqu'une IPv4 adresse privée secondaire est réaffectée à une autre interface, l'IPv4adresse privée secondaire conserve son association avec une adresse IP élastique.
- Lorsqu'une IPv4 adresse privée secondaire n'est pas attribuée depuis une interface, une adresse IP élastique associée est automatiquement dissociée de l'adresse privée IPv4 secondaire.

Travaillez avec plusieurs IPv4 adresses

Vous pouvez attribuer une IPv4 adresse privée secondaire à une instance, associer une IPv4 adresse élastique à une IPv4 adresse privée secondaire et annuler l'attribution d'une IPv4 adresse privée secondaire.

Tâches

- Attribuer une IPv4 adresse privée secondaire
- Configurer le système d'exploitation pour reconnaître les IPv4 adresses privées secondaires
- Associer une adresse IP élastique à l'IPv4adresse privée secondaire
- Afficher vos IPv4 adresses privées secondaires
- Annuler l'attribution d'une adresse privée IPv4 secondaire

Attribuer une IPv4 adresse privée secondaire

Vous pouvez attribuer l'IPv4adresse privée secondaire à l'interface réseau d'une instance lorsque vous lancez l'instance ou une fois que l'instance est en cours d'exécution.

Pour attribuer une IPv4 adresse privée secondaire lors du lancement d'une instance

1. Suivez la procédure pour lancer une instance. Sous Paramètres réseau, choisissez Modifier.
2. Sélectionnez un VPC et un sous-réseau.
3. Développez Configuration réseau avancée.
4. Pour l'adresse IP secondaire, choisissez Attribuer automatiquement et entrez le nombre d'adresses IP (Amazon attribue automatiquement les IPv4 adresses secondaires) ou choisissez Attribuer manuellement et entrez les IPv4 adresses.
5. Complétez les étapes suivantes pour lancer les instances.

Pour attribuer une IPv4 adresse secondaire lors du lancement à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez Accédez à Amazon EC2.

- L'option `--secondary-private-ip-addresses` avec la commande run-instances (AWS CLI)
- Définissez `-NetworkInterface` et spécifiez le `PrivateIpAddresses` paramètre à l'aide de la New-EC2Instancecommande (AWS Tools for Windows PowerShell).

Pour attribuer une IPv4 adresse privée secondaire à une interface réseau

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces, puis sélectionnez l'interface réseau pour l'instance.

3. Choisissez Actions, Gérer les adresses IP.
4. Sélectionnez l'interface réseau. Sous IPv4adresses, sélectionnez Attribuer une nouvelle adresse IP.
5. Entrez une IPv4 adresse spécifique comprise dans la plage de sous-réseau de l'instance, ou laissez le champ vide pour permettre à Amazon de sélectionner une IPv4 adresse pour vous.
6. (Facultatif) Sélectionnez Autoriser pour autoriser la réattribution de l'adresse IP privée secondaire si elle est déjà attribuée à une autre interface réseau.
7. Choisissez Save (Enregistrer).

Vous pouvez également attribuer une IPv4 adresse privée secondaire à une instance. Choisissez Instances dans le panneau de navigation, sélectionnez l'instance et choisissez Actions, sélectionnez Mise en réseau, puis Gérer les adresses IP. Vous pouvez configurer les mêmes informations que précédemment. L'adresse IP est attribuée à l'interface réseau principale (eth0) pour l'instance.

Pour attribuer une IPv4 adresse privée secondaire à une instance existante à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- assign-private-ip-addresses (AWS CLI)
- Register-EC2PrivateIpAddress (AWS Tools for Windows PowerShell)

Configurer le système d'exploitation pour reconnaître les IPv4 adresses privées secondaires

Après avoir attribué une IPv4 adresse privée secondaire à votre instance, vous devez configurer le système d'exploitation de votre instance pour qu'il reconnaisse l'adresse IP privée secondaire.

Instances Linux

- Si vous utilisez Amazon Linux, le package ec2-net-utils peut effectuer cette opération. Il configure les interfaces réseau supplémentaires que vous attachez pendant que l'instance est en cours d'exécution, actualise les IPv4 adresses secondaires lors du renouvellement du DHCP bail et met à jour les règles de routage associées. Vous pouvez actualiser immédiatement la liste des interfaces à l'aide de la commande, `sudo service network restart` puis afficher la up-to-date liste à l'aide `deip addr li`. Si vous avez besoin d'un contrôle manuel sur votre configuration réseau,

vous pouvez supprimer le package ec2-net-utils. Pour plus d'informations, consultez Configurer votre interface réseau à l'aide d'ec2-net-utils.

- Si vous utilisez une autre distribution Linux, consultez la documentation correspondante. Recherchez des informations sur la configuration d'interfaces réseau et d'IPv4adresses secondaires supplémentaires. Si l'instance a deux ou plusieurs interfaces sur le même sous-réseau, recherchez des informations sur l'utilisation des règles de routage pour contourner le routage asymétrique.

instances Windows

Pour de plus amples informations, veuillez consulter Configuration des IPv4 adresses privées secondaires pour les instances Windows.

Associer une adresse IP élastique à l'IPv4adresse privée secondaire

Pour associer une adresse IP élastique à une IPv4 adresse privée secondaire

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Elastic IPs.
3. Cochez la case correspondant à l'adresse IP élastique
4. Choisissez Actions, puis Associer une adresse IP élastique.
5. Pour Type de ressource, choisissez Interface réseau. Sélectionnez l'interface réseau, puis sélectionnez l'adresse IP secondaire dans la liste des adresses IP privées.
6. Pour Interface réseau, sélectionnez l'interface réseau. Sélectionnez l'adresse IP secondaire dans la liste des adresses IP privées.
7. Pour Adresse IP privée, sélectionnez l'adresse IP secondaire.
8. Choisissez Associer.

Pour associer une adresse IP élastique à une IPv4 adresse privée secondaire à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez Accédez à Amazon EC2.

- associate-address (AWS CLI)
- Register-EC2Address (AWS Tools for Windows PowerShell)

Afficher vos IPv4 adresses privées secondaires

Pour afficher les IPv4 adresses privées attribuées à une interface réseau

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).
3. Cochez la case correspondant à l'interface réseau.
4. Dans l'onglet Détails, sous Adresses IP, recherchez IPv4Adresse privée et IPv4Adresses privées secondaires.

Pour afficher les IPv4 adresses privées attribuées à une instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Cochez la case correspondant à l'instance.
4. Dans l'onglet Mise en réseau, sous Détails du réseau, recherchez IPv4les adresses privées et les IPv4adresses privées secondaires.

Annuler l'attribution d'une adresse privée IPv4 secondaire

Si vous n'avez plus besoin d'IPv4adresse privée secondaire, vous pouvez annuler son attribution à l'instance ou à l'interface réseau. Lorsqu'une IPv4 adresse privée secondaire n'est pas attribuée depuis une interface réseau, l'adresse IP élastique (si elle existe) est également dissociée.

Pour annuler l'attribution d'une IPv4 adresse privée secondaire à une instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez une instance, puis choisissez Actions, Mise en réseau, Gérer les adresses IP.
4. Sélectionnez l'interface réseau. Pour les IPv4adresses, choisissez Annuler l'attribution pour l'IPv4adresse à annuler.
5. Choisissez Save (Enregistrer).

Pour annuler l'attribution d'une IPv4 adresse privée secondaire depuis une interface réseau

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

2. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).
3. Sélectionnez l'interface réseau, choisissez Actions, Gérer les adresses IP.
4. Sélectionnez l'interface réseau. Pour les IPv4adresses, choisissez Annuler l'attribution pour l'IPv4adresse à annuler.
5. Choisissez Save (Enregistrer).

Pour annuler l'attribution d'une IPv4 adresse privée secondaire à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- unassign-private-ip-addresses (AWS CLI)
- Unregister-EC2PrivateIpAddress (AWS Tools for Windows PowerShell)

Travaillez avec plusieurs IPv6 adresses

Vous pouvez attribuer plusieurs IPv6 adresses à votre instance, consulter les IPv6 adresses attribuées à votre instance et annuler l'attribution d'IPv6adresses à votre instance.

Table des matières

Attribuer plusieurs IPv6 adresses

Vous pouvez attribuer une ou plusieurs IPv6 adresses à votre instance lors du lancement ou après le lancement. Pour attribuer une IPv6 adresse à une instance, le sous-réseau VPC and dans lequel vous lancez l'instance doit être associé à un IPv6 CIDR bloc.

Pour attribuer plusieurs IPv6 adresses lors du lancement

1. Suivez la procédure pour lancer une instance. Sous Paramètres réseau, choisissez Modifier.
2. Sélectionnez un VPC et un sous-réseau.
3. Développez Configuration réseau avancée.

4. Pour IPv6IPscela, choisissez Attribuer automatiquement et nombre d'adresses IP (Amazon attribue automatiquement les IPv6 adresses) ou choisissez Attribuer manuellement et entrez les IPv6 adresses.
5. Complétez les étapes suivantes pour lancer les instances.

Vous pouvez utiliser l'écran Instances de EC2 la console Amazon pour attribuer plusieurs IPv6 adresses à une instance existante. Cela affecte les IPv6 adresses à l'interface réseau principale (eth0) pour l'instance. Pour attribuer une IPv6 adresse spécifique à l'instance, assurez-vous qu'elle IPv6 n'est pas déjà attribuée à une autre instance ou interface réseau.

Pour attribuer plusieurs IPv6 adresses à une instance existante

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez votre instance, choisissez Actions, Mise en réseau, Gérer les adresses IP.
4. Sélectionnez l'interface réseau. Pour les IPv6adresses, choisissez Attribuer une nouvelle adresse IP pour chaque IPv6 adresse à ajouter. Vous pouvez spécifier une IPv6 adresse dans la plage du sous-réseau ou laisser le champ vide pour permettre à Amazon de choisir une IPv6 adresse pour vous.
5. Choisissez Save (Enregistrer).

Vous pouvez également attribuer plusieurs IPv6 adresses à une interface réseau existante. L'interface réseau doit avoir été créée dans un sous-réseau auquel est associé un IPv6 CIDR bloc. Pour attribuer une IPv6 adresse spécifique à l'interface réseau, assurez-vous qu'elle n'est pas déjà attribuée à une autre interface réseau. IPv6

Pour attribuer plusieurs IPv6 adresses à une interface réseau

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).
3. Sélectionnez votre interface réseau, choisissez Actions, Gérer les adresses IP.
4. Sélectionnez l'interface réseau. Pour les IPv6adresses, choisissez Attribuer une nouvelle adresse IP pour chaque IPv6 adresse à ajouter. Vous pouvez spécifier une IPv6 adresse dans la plage du sous-réseau ou laisser le champ vide pour permettre à Amazon de choisir une IPv6 adresse pour vous.

5. Choisissez Save (Enregistrer).

CLIvue d'ensemble

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- Attribuez une IPv6 adresse lors du lancement :
  - Utilisez les options `--ipv6-addresses` ou `--ipv6-address-count` avec la commande run-instances (AWS CLI)
  - Définissez `-NetworkInterface` et spécifiez les `Ipv6AddressCount` paramètres `Ipv6Addresses` or à l'aide de la New-EC2Instancecommande (AWS Tools for Windows PowerShell).
- Attribuez une IPv6 adresse à une interface réseau :
  - assign-ipv6-addresses (AWS CLI)
  - Register-EC2IpvAddressList(6AWS Tools for Windows PowerShell)

Afficher vos IPv6 adresses

Vous pouvez consulter les IPv6 adresses d'une instance ou d'une interface réseau.

Pour afficher les IPv6 adresses attribuées à une instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Cochez la case correspondant à votre instance.
4. Dans l'onglet Réseau, localisez le champ IPv6des adresses.

Pour afficher les IPv6 adresses attribuées à une interface réseau

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).
3. Cochez la case correspondant à votre interface réseau.
4. Dans l'onglet Détails, sous Adresses IP, recherchez le champ IPv6des adresses.

CLIvue d'ensemble

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- Consultez les IPv6 adresses d'une instance :
  - describe-instances (AWS CLI)
  - Get-EC2Instance (AWS Tools for Windows PowerShell).
- Consultez les IPv6 adresses d'une interface réseau :
  - describe-network-interfaces (AWS CLI)
  - Get-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Annuler l'attribution d'une adresse IPv6

Vous pouvez annuler l'attribution d'une IPv6 adresse depuis l'interface réseau principale d'une instance, ou vous pouvez annuler l'attribution d'une IPv6 adresse depuis une interface réseau.

Pour annuler l'attribution d'une IPv6 adresse à une instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Cochez la case correspondant à votre instance, puis choisissez Actions, Mise en réseau, Gérer les adresses IP.
4. Sélectionnez l'interface réseau. Sous IPv6adresses, choisissez Annuler l'attribution à côté de l'IPv6adresse.
5. Choisissez Save (Enregistrer).

Pour annuler l'attribution d'une IPv6 adresse depuis une interface réseau

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).
3. Cochez la case correspondant à votre interface réseau, puis choisissez Actions, Gérer les adresses IP.
4. Sélectionnez l'interface réseau. Sous IPv6adresses, choisissez Annuler l'attribution à côté de l'IPv6adresse.

5. Choisissez Save (Enregistrer).

CLIvue d'ensemble

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez Accédez à Amazon EC2.

- unassign-ipv6-addresses (AWS CLI)
- Unregister-EC2IpvAddressList(6AWS Tools for Windows PowerShell)

Configuration des IPv4 adresses privées secondaires pour les instances Windows

Vous pouvez spécifier plusieurs IPv4 adresses privées pour vos instances. Après avoir attribué une IPv4 adresse privée secondaire à une instance, vous devez configurer le système d'exploitation de l'instance pour qu'il reconnaisse l'IPv4adresse privée secondaire.

> **Note**
>
> Ces instructions sont basées sur Windows Server 2022. La mise en œuvre de ces étapes peut varier en fonction du système d'exploitation de l'instance Windows.

Tâches

- Prérequis
- Étape 1 : configurer l'adressage IP statique dans votre instance
- Étape 2 : Configurer une adresse IP privée secondaire pour votre instance
- Étape 3 : Configurer les applications pour qu'elles utilisent l'adresse IP privée secondaire

Prérequis

1. Attribuez l'IPv4adresse privée secondaire à l'interface réseau de l'instance. Vous pouvez attribuer l'IPv4adresse privée secondaire lorsque vous lancez l'instance ou après son exécution. Pour de plus amples informations, veuillez consulter Attribuer une IPv4 adresse privée secondaire.

2. Allouez une adresse IP élastique et associez-la à l'IPv4adresse privée secondaire. Pour plus d'informations, consultez allouer une adresse IP Elastic ; et Associer une adresse IP élastique à l'IPv4adresse privée secondaire.

Étape 1 : configurer l'adressage IP statique dans votre instance

Pour permettre à votre instance Windows d'utiliser plusieurs adresses IP, vous devez configurer votre instance pour qu'elle utilise un adressage IP statique plutôt qu'un DHCP serveur.

> **Important**
>
> Lorsque vous configurez l'adressage IP statique dans votre instance, l'adresse IP doit correspondre exactement à ce qui est affiché dans la consoleCLI, ouAPI. Si vous entrez ces adresses IP de manière incorrecte, l'instance peut devenir inaccessible.

Pour configurer l'adressage IP statique sur une instance Windows

1. Connectez-vous à votre instance.
2. Recherchez l'adresse IP, le masque de sous-réseau et les adresses de passerelle par défaut pour l'instance en exécutant les étapes suivantes :
   - Exécutez la commande suivante dans PowerShell :

     ```
     ipconfig /all
     ```

     Passez en revue le résultat et notez les valeurs d'IPv4adresse, de masque de sous-réseau, de passerelle par défaut et de DNSserveurs pour l'interface réseau. Votre sortie doit ressembler à l'exemple suivant :

     ```
     ...

     Ethernet adapter Ethernet 4:

        Connection-specific DNS Suffix  . : us-west-2.compute.internal
        Description . . . . . . . . . . . : Amazon Elastic Network Adapter #2
        Physical Address. . . . . . . . . : 02-9C-3B-FC-8E-67
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
     ```

```
   Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.200.0.128(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, April 8, 2024 12:19:29 PM
   Lease Expires . . . . . . . . . . : Monday, April 8, 2024 4:49:30 PM
   Default Gateway . . . . . . . . . : 10.200.0.1
   DHCP Server . . . . . . . . . . . : 10.200.0.1
   DHCPv6 IAID . . . . . . . . . . . : 151166011
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-
E7
   DNS Servers . . . . . . . . . . . : 10.200.0.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

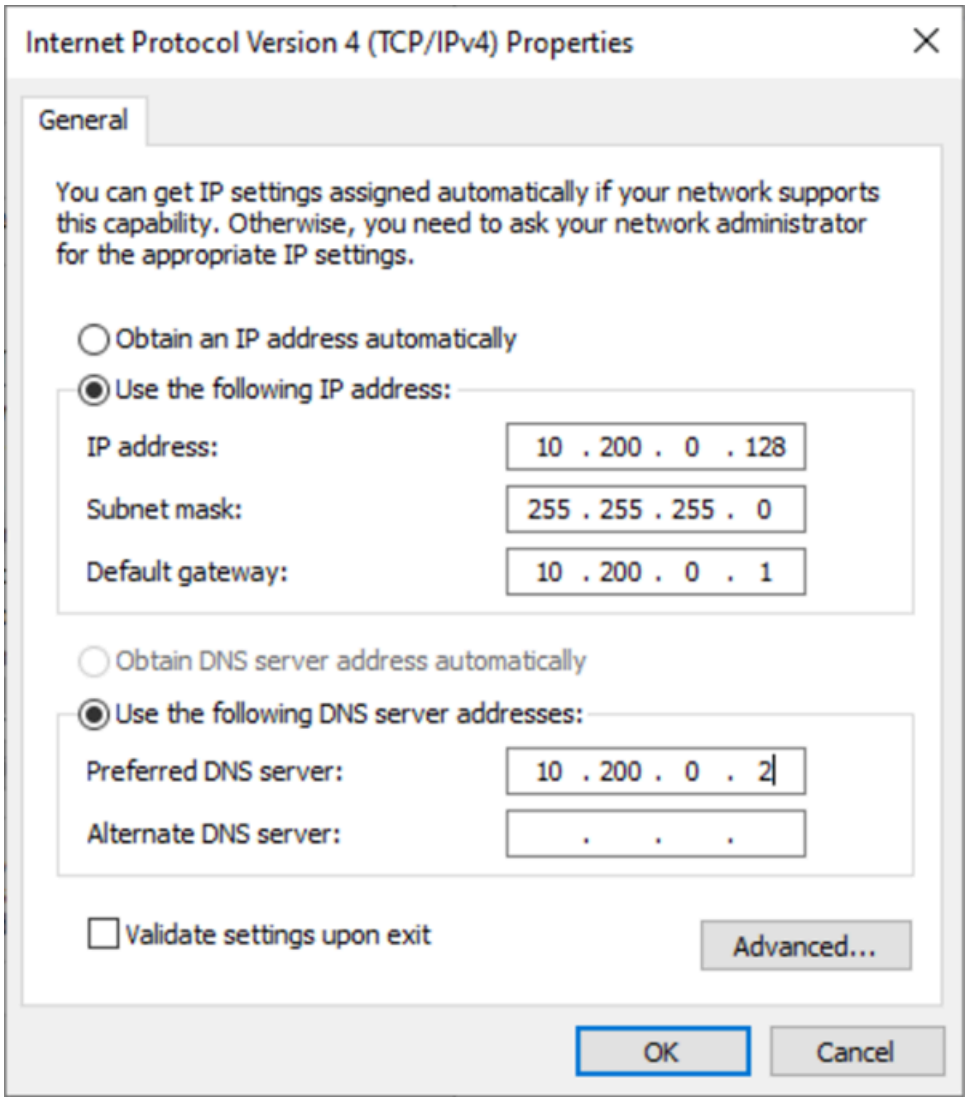
3. Ouvrez le Centre de réseau et de partage en exécutant la commande suivante dans PowerShell :

```
& $env:SystemRoot\system32\control.exe ncpa.cpl
```

4. Ouvrez le menu contextuel (clic droit) de l'interface réseau (connexion au réseau local ou Ethernet) et choisissez Propriétés.
5. Choisissez Internet Protocol Version 4 (TCP/IPv4), Propriétés.
6. Dans la boîte de dialogue Propriétés du protocole Internet version 4 (TCP/IPv4), choisissez Utiliser l'adresse IP suivante, entrez les valeurs suivantes, puis cliquez sur OK.

Champ	Value
Adresse IP	IPv4Adresse obtenue à l'étape 2 ci-dessus.
Masque de sous-réseau	Masque de sous-réseau obtenu à l'étape 2 ci-dessus.
Passerelle par défaut	Passerelle par défaut obtenue à l'étape 2 ci-dessus.
DNSServeur préféré	Le DNS serveur obtenu à l'étape 2 ci-dessus.
DNSServeur alternatif	Le DNS serveur alternatif obtenu à l'étape 2 ci-dessus. Si aucun autre DNS serveur n'est répertorié, laissez ce champ vide.

> **Important**
>
> Si vous définissez l'adresse IP sur n'importe quelle valeur autre que l'adresse IP actuelle, vous perdrez la connectivité à l'instance.



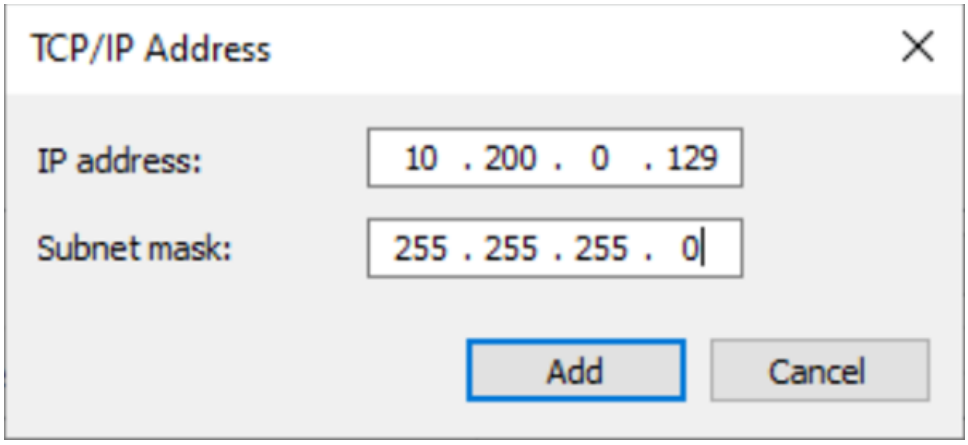
Vous perdrez la RDP connectivité à l'instance Windows pendant quelques secondes pendant que l'instance passe de l'adressage standard DHCP à l'adressage statique. L'instance conserve les mêmes informations d'adresse IP qu'auparavant, mais ces informations sont désormais statiques et ne sont pas gérées parDHCP.

Étape 2 : Configurer une adresse IP privée secondaire pour votre instance

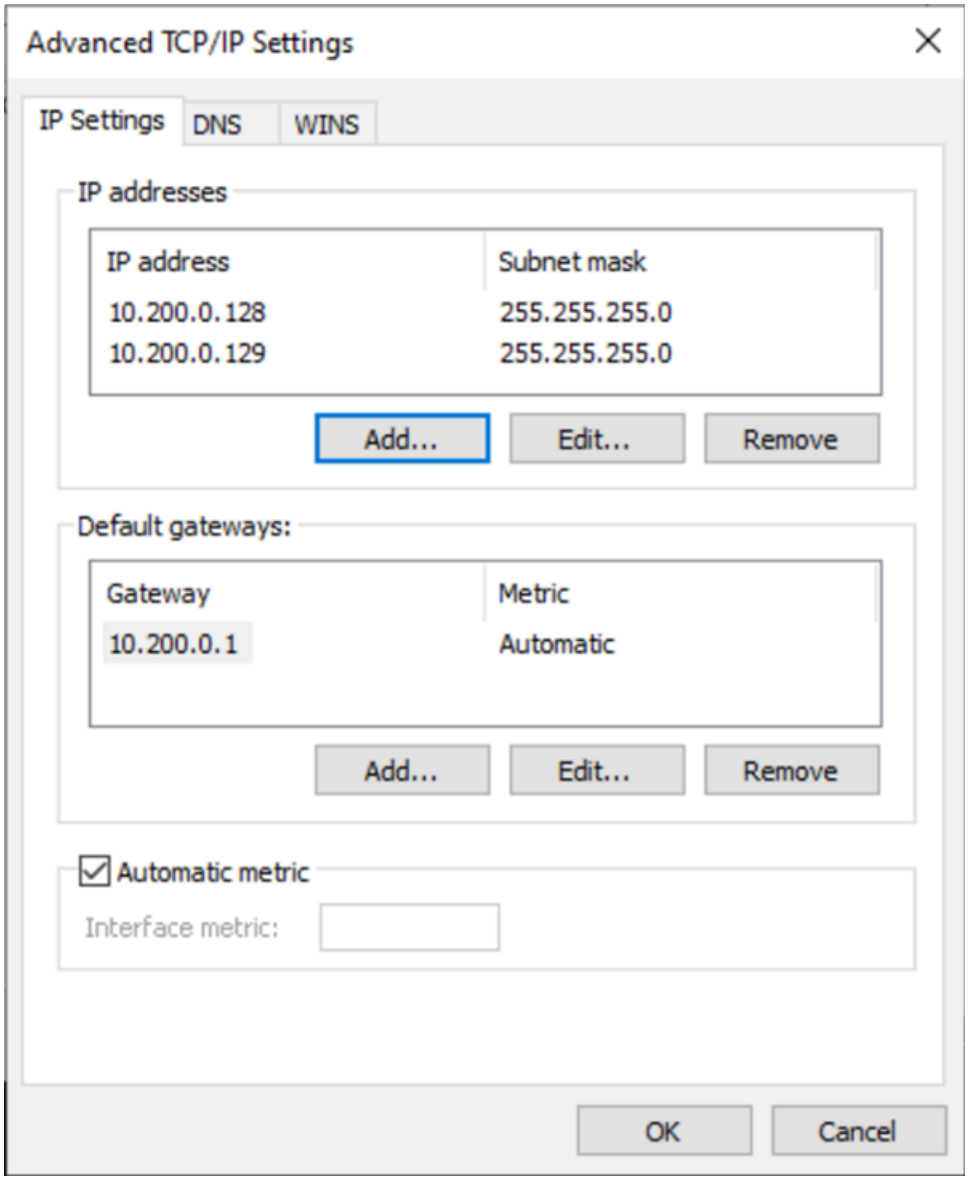
Après avoir configuré l'adressage IP statique sur votre instance Windows, vous pouvez préparer une seconde adresse IP privée.

Pour configurer une adresse IP secondaire

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Instances, puis choisissez votre instance.
3. Notez l'adresse IP secondaire que vous trouverez sur la page Mise en réseau.
4. Connectez-vous à votre instance.
5. Sur votre instance Windows, choisissez Démarrer, Panneau de configuration.
6. Choisissez Réseau et Internet, Centre Réseau et partage.
7. Sélectionnez l'interface réseau (connexion au réseau local ou Ethernet) et choisissez Propriétés.
8. Sur la page Propriétés de la connexion au réseau local, sélectionnez Internet Protocol version 4 (TCP/IPv4), Propriétés, Avancé.
9. Choisissez Ajouter.
10. Dans la boîte de dialogue TCP/IP Address, tapez l'adresse IP privée secondaire pour l'adresse IP. Dans Masque de sous-réseau, saisissez le même masque de sous-réseau que celui que vous avez entré pour l'adresse IP privée principale dans Étape 1 : configurer l'adressage IP statique dans votre instance, puis choisissez Ajouter.



11. Vérifiez les paramètres de l'adresse IP et choisissez OK.



12. Choisissez OK, Fermer.
13. Pour vérifier que l'adresse IP secondaire a été ajoutée au système d'exploitation, exécutez la `ipconfig /all` commande dans PowerShell. Votre sortie doit ressembler à ce qui suit :

```
Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Amazon Elastic Network Adapter #2
   Physical Address. . . . . . . . . : 02-9C-3B-FC-8E-67
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.200.0.128(Preferred)
```

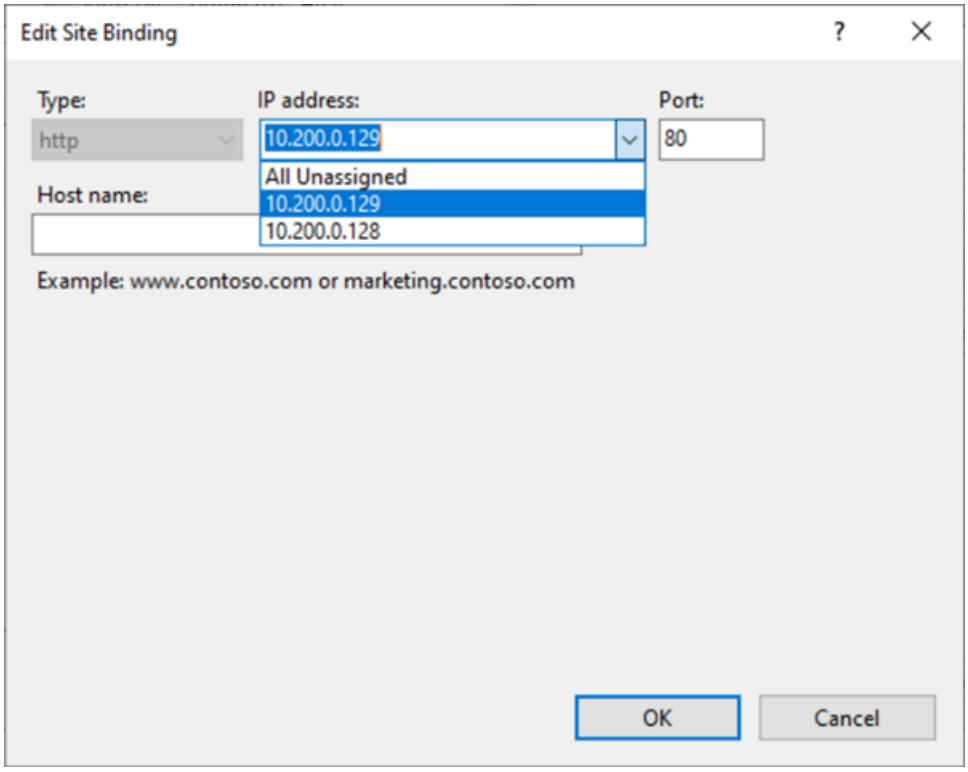
```
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IPv4 Address. . . . . . . . . . . : 10.200.0.129(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.200.0.1
   DHCPv6 IAID . . . . . . . . . . . : 151166011
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-E7
   DNS Servers . . . . . . . . . . . : 10.200.0.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Étape 3 : Configurer les applications pour qu'elles utilisent l'adresse IP privée secondaire

Vous pouvez configurer toutes les applications pour qu'elles utilisent l'adresse IP privée secondaire. Par exemple, si votre instance exécute un site WebIIS, vous pouvez configurer IIS pour utiliser l'adresse IP privée secondaire.

Pour configurer IIS l'utilisation de l'adresse IP privée secondaire

1. Connectez-vous à votre instance.
2. Ouvrez Internet Information Services (IIS) Manager.
3. Dans le volet Connexions, développez Sites.
4. Ouvrez le menu contextuel (clic droit) de votre site web et choisissez Modifier les liaisons.
5. Dans la boîte de dialogue Liaisons de site, pour Type, choisissez http, Modifier.
6. Dans la boîte de dialogue Modifier une liaison de site, pour Adresse IP, sélectionnez l'adresse IP privée secondaire. (Par défaut, chaque site Web accepte les HTTP demandes provenant de toutes les adresses IP.)



7. Choisissez OK, Fermer.

Types de noms EC2 d'hôte des instances Amazon

Cette section décrit les types de noms d'hôte du système d'exploitation invité Amazon EC2 disponibles lorsque vous lancez des instances dans vos VPC sous-réseaux.

Le nom d'hôte distingue les EC2 instances de votre réseau. Vous pouvez utiliser le nom d'hôte d'une instance si, par exemple, vous souhaitez exécuter des scripts pour communiquer avec toutes ou certaines instances de votre réseau.

Table des matières

Types de noms d'EC2hôtes

Il existe deux types de nom d'hôte pour le nom d'hôte du système d'exploitation invité lorsque les EC2 instances sont lancées dans un : VPC

- Nom IP : schéma de dénomination existant dans lequel, lorsque vous lancez une instance, l'IPv4adresse privée de l'instance est incluse dans le nom d'hôte de l'instance. Le nom IP existe pendant toute la durée de vie de l'EC2instance. Lorsqu'il est utilisé comme DNS nom d'hôte privé, il renvoie uniquement l'IPv4adresse privée (enregistrement A).
- Nom de la ressource : lorsque vous lancez une instance, l'ID de l'EC2instance est inclus dans le nom d'hôte de l'instance. Le nom de la ressource existe pendant toute la durée de vie de l'EC2instance. Lorsqu'il est utilisé comme DNS nom d'hôte privé, il peut renvoyer à la fois l'IPv4adresse privée (enregistrement A) et/ou l'adresse unicast IPv6 globale (AAAAenregistrement).

Le type de nom d'hôte du système d'exploitation invité de l'EC2instance dépend des paramètres du sous-réseau :

- Si l'instance est lancée dans un sous-réseau IPv4 réservé, vous pouvez sélectionner le nom IP ou le nom de la ressource.
- Si l'instance est lancée dans un sous-réseau à double pile (IPv4+IPv6), vous pouvez sélectionner le nom IP ou le nom de la ressource.
- Si l'instance est lancée dans un sous-réseau IPv6 uniquement, le nom de la ressource est utilisé automatiquement.

Table des matières

Nom d'adresse IP

Lorsque vous lancez une EC2 instance avec le type d'adresse IP Hostname, le nom d'hôte du système d'exploitation invité est configuré pour utiliser l'adresse privéeIPv4.

- Format d'une instance dans us-east-1 : `private-ipv4-address.ec2.internal`

- Exemple : *ip-10-24-34-0*.ec2.internal
- Format pour une instance dans n'importe quelle autre AWS région : *private-ipv4-address.region*.compute.internal
- Exemple : *ip-10-24-34-0.us-west-2*.compute.internal

Nom de la ressource

Lorsque vous lancez EC2 des instances dans des sous-réseaux IPv6 uniquement, le type de nom d'hôte du nom de ressource est sélectionné par défaut. Lorsque vous lancez une instance dans des sous-réseaux IPv4 -only ou à double pile (IPv4+IPv6), le nom de la ressource est une option que vous pouvez sélectionner. Après avoir lancé une instance, vous pouvez gérer la configuration du nom d'hôte. Pour de plus amples informations, veuillez consulter Modifier les options de dénomination basées sur les ressources pour Amazon EC2.

Lorsque vous lancez une EC2 instance avec un nom de ressource de type Hostname, le nom d'hôte du système d'exploitation invité est configuré pour utiliser l'ID de l'EC2instance.

- Format d'une instance dans us-east-1 : *ec2-instance-id*.ec2.internal
- Exemple : *i-0123456789abcdef*.ec2.internal
- Format pour une instance dans n'importe quelle autre AWS région : *ec2-instance-id.region*.compute.internal
- Exemple : *i-0123456789abcdef.us-west-2*.compute.internal

La différence entre le nom d'adresse IP et le nom de la ressource

DNSles requêtes relatives aux noms IP et aux noms de ressources coexistent pour garantir la rétrocompatibilité et vous permettre de passer d'une dénomination basée sur l'adresse IP pour les noms d'hôtes à une dénomination basée sur les ressources. Pour les DNS noms d'hôtes privés basés sur des noms IP, vous ne pouvez pas configurer si DNS une requête d'enregistrement A pour l'instance reçoit une réponse ou non. DNSLes requêtes d'enregistrement reçoivent toujours une réponse, quels que soient les paramètres du nom d'hôte du système d'exploitation invité.
En revanche, pour les DNS noms d'hôtes privés basés sur le nom de la ressource, vous pouvez configurer si DNS A et/ou les DNS AAAA requêtes relatives à l'instance reçoivent une réponse ou non. Vous configurez le comportement de réponse lorsque vous lancez une instance ou modifiez un sous-réseau. Pour de plus amples informations, veuillez consulter Modifier les options de dénomination basées sur les ressources pour Amazon EC2.

Où trouver les noms de ressources et les adresses IP

Vous pouvez voir les types de nom d'hôte, le nom de la ressource et le nom IP dans la EC2 console Amazon.

Table des matières

Lors de la création d'une EC2 instance

Lorsque vous créez une EC2 instance, selon le type de sous-réseau que vous sélectionnez, le type de nom d'hôte du nom de ressource peut être disponible ou il peut être sélectionné et ne pas être modifiable. Cette section décrit les scénarios dans lesquels vous pouvez consulter les types de nom d'hôte, nom de ressource et d'adresse IP.

Scénario 1

Vous créez une EC2 instance dans l'assistant (voirLancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console) et, lorsque vous configurez les détails, vous choisissez un sous-réseau que vous avez configuré pour être réservé aux utilisateurs uniquementIPv6.

Dans ce cas, le champ Hostname type (Type de nom d'hôte) de Resource name (Nom de la ressource) est sélectionné automatiquement et n'est pas modifiable. DNSLes options de nom d'hôte des requêtes Activer le nom IP IPv4 (enregistrement A) et Activer les DNS demandes basées sur les ressources IPv4 (enregistrement A) DNS sont désélectionnées automatiquement et ne sont pas modifiables. L'option Activer les DNS demandes basées sur les ressources IPv6 (AAAAenregistrement) est sélectionnée par défaut mais elle est modifiable. Si cette option est sélectionnée, les DNS demandes adressées au nom de la ressource seront résolues à l'IPv6adresse (AAAAenregistrement) de cette EC2 instance.

Scénario 2

Vous créez une EC2 instance dans l'assistant (voirLancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console) et, lorsque vous configurez les détails, vous choisissez un sous-réseau configuré avec un IPv4 CIDR bloc ou les deux IPv4 et un IPv6 CIDR bloc and (« dual stack »).

Dans ce cas, les DNSdemandes Activer le nom IP IPv4 (enregistrement A) sont sélectionnées automatiquement et ne peuvent pas être modifiées. Cela signifie que les demandes adressées au nom IP seront résolues vers l'IPv4adresse (enregistrement A) de cette EC2 instance.

Les options correspondent par défaut aux configurations du sous-réseau, mais vous pouvez modifier les options de cette instance en fonction des paramètres du sous-réseau :

- Type de nom d'hôte : détermine si vous souhaitez que le nom d'hôte du système d'exploitation invité de l'EC2instance soit le nom de la ressource ou le nom IP. La valeur par défaut est IP name (Nom d'adresse IP).
- Activer les DNS demandes basées sur les ressources IPv4 (enregistrement A) : détermine si les demandes adressées au nom de votre ressource sont résolues vers l'IPv4adresse privée (enregistrement A) de cette EC2 instance. Cette option n'est pas sélectionnée par défaut.
- Activer les DNS demandes basées sur les ressources IPv6 (AAAAenregistrement) : détermine si les demandes adressées au nom de votre ressource sont résolues à l'IPv6GUAadresse (AAAAenregistrement) de cette EC2 instance. Cette option n'est pas sélectionnée par défaut.

Lorsque vous consultez les détails d'une EC2 instance existante

Vous pouvez voir les valeurs du nom d'hôte d'une EC2 instance existante dans l'onglet Détails de l'EC2instance :

- Hostname type (Type de nom d'hôte) : nom d'hôte au format nom IP ou nom de ressource.
- DNSNom IP privé (IPv4uniquement) : nom IP qui sera toujours résolu en IPv4 adresse privée de l'instance.
- DNSNom de la ressource privée : nom de la ressource qui correspond aux DNS enregistrements sélectionnés pour cette instance.
- Répondez au DNS nom de la ressource privée : le nom de la ressource correspond aux DNS enregistrements IPv4 IPv6 (AAAAA), IPv6 () ou IPv4 (A etAAAA).

En outre, si vous vous connectez directement à votre EC2 instance SSH et que vous entrez la `hostname` commande, vous verrez le nom d'hôte au format du nom IP ou du nom de ressource.

Choix entre les noms de ressources et les noms IP

Lorsque vous lancez une EC2 instance (voirLancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console), si vous choisissez un type de nom d'hôte dans Nom de

ressource, l'EC2instance est lancée avec un nom d'hôte au format du nom de ressource. Dans ce cas, l'DNSenregistrement de cette EC2 instance peut également pointer vers le nom de la ressource. Cela vous donne la possibilité de choisir si ce nom d'hôte correspond à l'IPv4adresse, à l'IPv6adresse ou aux deux à l'IPv6adresse IPv4 et de l'instance. Si vous envisagez de les utiliser IPv6 à l'avenir ou si vous utilisez des sous-réseaux à double pile aujourd'hui, il est préférable d'utiliser un nom de ressource de type Nom d'hôte afin de modifier la DNS résolution des noms d'hôtes de vos instances sans apporter de modifications aux enregistrements eux-mêmes. DNS Le nom de la ressource vous permet d'ajouter, de supprimer IPv4 et de IPv6 DNS résoudre une EC2 instance.

Si vous choisissez plutôt un type de nom d'hôte comme nom d'hôte et que vous l'utilisez comme DNS nom d'hôte, il ne peut être résolu que par l'IPv4adresse de l'instance. Il ne sera pas résolu à l'IPv6adresse de l'instance même si l'instance possède à la fois une IPv4 IPv6 adresse et une adresse associées.

Modifier les options de dénomination basées sur les ressources pour Amazon EC2

Vous pouvez modifier le type de nom d'DNShôte et les configurations de nom d'hôte pour les sous-réseaux, ce qui affecte tous les lancements d'instance ultérieurs dans ce domaine, ou vous pouvez les modifier pour une EC2 instance après son lancement.

Sous-réseaux

Modifiez les configurations d'un sous-réseau en sélectionnant un sous-réseau dans la VPC console Amazon, puis en choisissant Actions, Modifier les paramètres du sous-réseau.

> **Note**
>
> La modification des paramètres du sous-réseau ne modifie pas la configuration des EC2 instances déjà lancées dans le sous-réseau.

- Type de nom d'hôte : détermine si vous souhaitez que le paramètre par défaut du nom d'hôte du système d'exploitation invité de l'EC2instance lancée dans le sous-réseau soit le nom de la ressource ou le nom IP.
- Activer les demandes de DNS nom d'hôte IPv4 (enregistrement A) : détermine si les DNS requêtes/requêtes adressées au nom de votre ressource sont résolues vers l'IPv4adresse privée (enregistrement A) de cette instance. EC2

- Activer les demandes de DNS nom d'hôte IPv6 (AAAAenregistrement) : détermine si les DNS requêtes/requêtes adressées au nom de votre ressource sont résolues à l'IPv6adresse (AAAAenregistrement) de cette instance. EC2

Instances EC2

Suivez les étapes décrites dans cette section pour modifier le type de nom d'hôte et les configurations DNS du nom d'hôte d'une EC2 instance.

Considérations

- Pour modifier le paramètre Use resource based naming as guest OS hostname (Utiliser la dénomination basée sur les ressources comme nom d'hôte du système d'exploitation invité), vous devez d'abord arrêter l'instance. Pour modifier les paramètres de demande de DNSnom d'hôte Answer IPv4 (enregistrement A) ou de demande de DNS nom d'hôte Answer IPv6 (AAAAenregistrement), il n'est pas nécessaire d'arrêter l'instance.
- Pour modifier les paramètres des types d'EC2instance non EBS sauvegardés, vous ne pouvez pas arrêter l'instance. Vous devez mettre fin à l'instance et en lancer une nouvelle avec le type de nom d'hôte et les configurations de nom d'DNShôte souhaités.

Pour modifier le type de nom d'hôte et les configurations de DNS nom d'hôte d'une instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Si vous souhaitez modifier le paramètre Utiliser un nom basé sur les ressources comme nom d'hôte du système d'exploitation invité, arrêtez d'abord l'EC2instance. Sinon, Ignorez cette étape.

   Pour arrêter l'instance, sélectionnez l'instance et choisissez Instance state (État de l'instance), Stop instance (Arrêter l'instance).
3. Sélectionnez l'instance, puis choisissez Actions, Instance settings (Paramètres des instances), Change resource based naming options (Modifier les options de dénomination basées sur les ressources).

   - Utiliser une dénomination basée sur les ressources comme nom d'hôte du système d'exploitation invité : détermine si vous souhaitez que le nom d'hôte du système d'exploitation invité de l'EC2instance soit le nom de la ressource ou le nom IP.

- Répondre aux demandes de DNS nom d'hôte IPv4 (enregistrement A) : détermine si les DNS requêtes/requêtes adressées au nom de votre ressource sont résolues vers l'IPv4adresse privée de cette instance. EC2
- Répondre aux demandes de DNS nom d'hôte IPv6 (AAAAenregistrement) : détermine si les DNS requêtes/requêtes adressées au nom de votre ressource sont résolues à l'IPv6adresse (AAAAenregistrement) de cette instance. EC2

4. Choisissez Save (Enregistrer).
5. Si vous aviez arrêté l'instance, redémarrez-la.

Apportez vos propres adresses IP (BYOIP) à Amazon EC2

Vous pouvez transférer une partie ou la totalité de votre réseau public IPv4 ou de votre plage d'IPv6adresses de votre réseau local vers votre. Compte AWS Vous continuez à contrôler la plage d'adresses et vous pouvez en faire la publicité sur Internet via AWS. Une fois que vous avez transféré la plage d'adresses à AmazonEC2, elle apparaît dans votre Compte AWS pool d'adresses.

> **Note**
>
> Cette documentation explique comment apporter votre propre plage d'adresses IP pour une utilisation sur Amazon EC2 uniquement. Pour apporter votre propre plage d'adresses IP à utiliser AWS Global Accelerator, voir Apporter vos propres adresses IP (BYOIP) dans le guide du AWS Global Accelerator développeur. Pour utiliser votre propre plage d'adresses IP Amazon VPC IP Address Manager, consultez le didacticiel « Importer vos adresses IP » IPAM dans le guide de VPC IPAM l'utilisateur Amazon.

Lorsque vous apportez une plage d'adresses IP à AWS, AWS confirme que vous contrôlez la plage d'adresses IP. Vous pouvez utiliser deux méthodes pour montrer que vous contrôlez la plage :

- Si votre plage d'adresses IP est enregistrée auprès d'un registre Internet compatible RDAP (tel queARIN, RIPE etAPNIC), vous pouvez vérifier le contrôle de votre domaine à l'aide d'un certificat X.509 en suivant le processus décrit sur cette page.
- Que votre registre Internet soit compatible ou nonRDAP, vous pouvez utiliser Amazon VPC IPAM pour vérifier le contrôle de votre domaine à l'aide d'un DNS TXT enregistrement. Ce processus est décrit dans Tutorial : Bring your IP addresses to IPAM in the Amazon VPC IPAM User Guide.

Pour plus d'informations, consultez le débat technique AWS en ligne sur le thème « Bring Your Own IP ».

Table des matières

BYOIPdéfinitions

- Certificat auto-signé X.509 : norme de certificat la plus couramment utilisée pour chiffrer et authentifier les données au sein d'un réseau. Il s'agit d'un certificat utilisé AWS pour valider le contrôle de l'espace IP à partir d'un RDAP enregistrement. Pour plus d'informations sur les certificats X.509, consultez RFC3280.
- Numéro de système autonome (ASN) : identifiant unique au monde qui définit un groupe de préfixes IP gérés par un ou plusieurs opérateurs de réseau qui appliquent une politique de routage unique et clairement définie.
- Registre Internet régional (RIR) : organisation qui gère l'attribution et l'enregistrement des adresses IP ASNs au sein d'une région du monde.
- Protocole d'accès aux données de registre (RDAP) — Protocole en lecture seule permettant d'interroger les données d'enregistrement actuelles dans un. RIR Les entrées de la base de RIR données interrogée sont appelées « RDAP enregistrements ». Certains types d'enregistrements doivent être mis à jour par les clients via un mécanisme RIR fourni. Ces enregistrements sont interrogés AWS pour vérifier le contrôle d'un espace d'adressage dans le. RIR
- Autorisation d'origine de la route (ROA) — Objet créé par RIRs les clients pour authentifier la publicité IP dans des systèmes autonomes particuliers. Pour un aperçu, consultez Route Origin Authorizations (ROAs) sur le ARIN site Web.
- Registre Internet local (LIR) — Organisations telles que les fournisseurs de services Internet qui allouent un bloc d'adresses IP à leurs clients et RIR à ceux-ci.

Exigences et quotas

- La plage d'adresses doit être enregistrée dans votre registre Internet régional (RIR). Consultez votre RIR pour connaître les politiques relatives aux régions géographiques. BYOIPprend actuellement en charge l'enregistrement auprès du registre américain des numéros Internet (ARIN), du centre de coordination du réseau Réseaux IP Européens (RIPE) ou du centre d'information du réseau Asie-Pacifique (APNIC). Elle doit être enregistrée pour une entreprise ou une entité institutionnelle et ne peut pas être enregistrée pour une personne individuelle.
- La plage d'IPv4adresses la plus précise que vous pouvez apporter est /24.
- La plage d'IPv6adresses la plus précise que vous pouvez apporter est /48 pour celles CIDRs qui sont publiables et /56 pour celles CIDRs qui ne le sont pas.
- ROAsne sont pas obligatoires pour les CIDR gammes qui ne sont pas accessibles au public, mais les RDAP enregistrements doivent tout de même être mis à jour.
- Vous pouvez attribuer chaque plage d'adresses à une AWS région à la fois.
- Vous pouvez ajouter un total de cinq plages BYOIP IPv4 d'IPv6adresses par AWS région à votre AWS compte. Vous ne pouvez pas ajuster les quotas pour BYOIP CIDRs utiliser la console Service Quotas, mais vous pouvez demander une augmentation des quotas en contactant le AWS Support Center comme indiqué dans la section Quotas de AWS service du Références générales AWS.
- Vous ne pouvez pas partager votre plage d'adresses IP avec d'autres comptes AWS RAM à moins d'utiliser Amazon VPC IP Address Manager (IPAM) et de l'intégrer IPAM à AWS Organizations. Pour plus d'informations, consultez Integrate IPAM with AWS Organizations dans le guide de VPC IPAM l'utilisateur Amazon.
- L'historique des adresses de la plage d'adresses IP doit être propre. Nous pouvons enquêter sur la réputation de la plage d'adresses IP et nous réserver le droit de rejeter une plage d'adresses IP si elle contient une adresse IP qui a une mauvaise réputation ou qui est associée à un comportement malveillant.
- L'espace d'adressage existant, l'IPv4espace d'adressage distribué par le registre central de l'Internet Assigned Numbers Authority (IANA) avant la création du système Regional Internet Registry (RIR), nécessite toujours un ROA objet correspondant.
- En LIRs effet, il est courant qu'ils utilisent un processus manuel pour mettre à jour leurs dossiers. Le déploiement peut prendre plusieurs jours en fonction duLIR.
- Un seul ROA objet et un seul RDAP enregistrement sont nécessaires pour un gros CIDR bloc. Vous pouvez transférer plusieurs petits CIDR blocs de cette plage AWS, même dans plusieurs AWS régions, en utilisant un seul objet et un seul enregistrement.

- BYOIPn'est pas compatible avec Wavelength Zones ou sur Wavelength AWS Outposts.
- N'apportez aucune modification manuelle à BYOIP in RADb ou à une autreIRR. BYOIPsera automatiquement mis à jourRADb. Toute modification manuelle incluant le BYOIP ASN entraînera l'échec de l'opération de BYOIP provisionnement.
- Une fois que vous avez transféré une plage d'IPv4adresses AWS, vous pouvez utiliser toutes les adresses IP de la plage, y compris la première adresse (adresse réseau) et la dernière adresse (adresse de diffusion).

Disponibilité par région

La BYOIP fonctionnalité est actuellement disponible dans toutes les AWS régions commerciales, à l'exception des régions chinoises.

Disponibilité de la zone locale

Une zone locale est une extension d'une AWS région située à proximité géographique de vos utilisateurs. Les Zones Locales sont regroupées en « groupes de frontières réseau ». Dans AWS, un groupe frontalier réseau est un ensemble de zones de disponibilité (AZs), de zones locales ou de zones de longueur d'onde à partir duquel AWS une adresse IP publique est annoncée. Les zones locales peuvent avoir des groupes de bordure de réseau différents de AZs ceux d'une AWS région afin de garantir une latence minimale ou une distance physique minimale entre le AWS réseau et les clients accédant aux ressources de ces zones.

Vous pouvez fournir des plages d'BYOIPv4adresses et les publier dans les groupes frontaliers du réseau de zones locales suivants à l'aide de l'`--network-border-group`option :

- us-east-1-dfw-2
- us-west-2-lax-1
- us-west-2-phx-2

Si les zones locales sont activées (voir Activer une zone locale), vous pouvez choisir un groupe de frontières réseau pour les zones locales lorsque vous approvisionnez et annoncez un BYOIPv4CIDR. Choisissez le groupe de bordure du réseau avec soin, car la EIP AWS ressource à laquelle il est associé doit résider dans le même groupe de bordure du réseau.

> **Note**
>
> Vous ne pouvez pas fournir ou publier des plages d'BYOIPv6adresses dans les Zones Locales pour le moment.

Conditions préalables pour BYOIP Amazon EC2

Le processus d'intégration BYOIP comporte deux phases, au cours desquelles vous devez effectuer trois étapes. Ces étapes correspondent aux étapes décrites dans le diagramme suivant. Nous incluons des étapes manuelles dans cette documentation, mais vous RIR pouvez proposer des services gérés pour vous aider dans ces étapes.

> **Tip**
>
> Les tâches de cette section nécessitent un terminal Linux et peuvent être effectuées à l'aide de Linux, du AWS CloudShell ou du sous-système Windows pour Linux.

Table des matières

Présentation

Phase de préparation

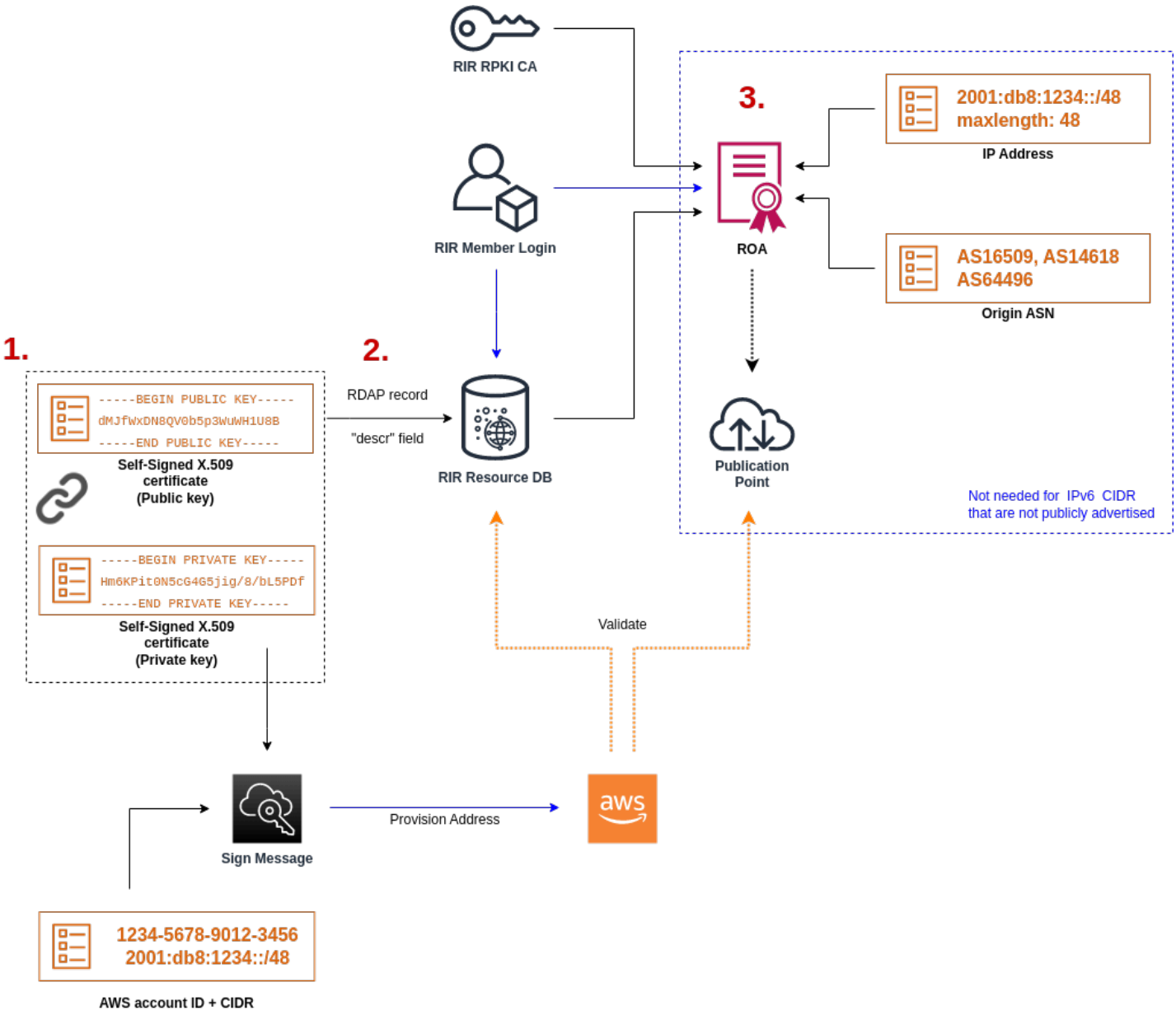
[1] Créez une clé privée et utilisez-la pour générer un certificat X.509 auto-signé à des fins d'authentification. Ce certificat n'est utilisé que pendant la phase d'allocation.

RIRphase de configuration

[2] Téléchargez le certificat autosigné dans les commentaires de votre RDAP dossier.

[3] Créez un ROA objet dans votreRIR. ROADéfinit la plage d'adresses souhaitée, les numéros de système autonomes (ASNs) autorisés à publier la plage d'adresses et une date d'expiration pour l'enregistrement auprès de l'infrastructure à clé publique de ressources (RPKI) de votreRIR.

> **Note**
>
> A n'ROAest pas obligatoire pour les espaces d'IPv6adressage non publicisés.



Pour ajouter plusieurs plages d'adresses non-contiguës, vous devez répéter ce processus avec chacune d'elles. Toutefois, il n'est pas nécessaire de répéter les étapes de préparation et de RIR configuration si vous divisez un bloc contigu sur plusieurs régions différentes. AWS

L'ajout d'une plage d'adresses n'a aucun effet sur les plages d'adresses que vous avez ajoutées précédemment.

Création d'une clé privée et génération d'un certificat X.509

Utilisez la procédure suivante pour créer un certificat X.509 auto-signé et l'ajouter à l'RDAPenregistrement de votre. RIR Cette paire de clés est utilisée pour authentifier la plage d'adresses avec leRIR. Les openssl commandes nécessitent la SSL version 1.0.2 ou ultérieure d'Open.

Copiez les commandes suivantes et remplacez uniquement les valeurs d'espace réservé (en italique et en couleur).

Cette procédure suit les meilleures pratiques qui consistent à chiffrer votre RSA clé privée et à exiger un mot de passe pour y accéder.

1. Générez une clé privée de RSA 2048 bits comme indiqué ci-dessous.

   ```
   $ openssl genpkey -aes256 -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out
    private-key.pem
   ```

   Le paramètre `-aes256` spécifie l'algorithme utilisé pour chiffrer la clé privée. La commande renvoie la sortie suivante, y compris les invites pour définir une phrase secrète :

   ```
   ......+++
   .+++
   Enter PEM pass phrase: xxxxxxx
   Verifying - Enter PEM pass phrase: xxxxxxx
   ```

   Vous pouvez inspecter la clé publique à l'aide de la commande suivante :

   ```
   $ openssl pkey -in private-key.pem -text
   ```

   Cela renvoie une invite de phrase secrète et le contenu de la clé, qui devrait être similaire à ce qui suit :

```
Enter pass phrase for private-key.pem: xxxxxxx
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDFBXHRI4HVKAhh
3seiciooizCRTbJe1+YsxNTja4XyKypVGIFWDGhZs44FCHlPOOSVJ+NqP74w96oM
7DPS3xo9kaQyZBFn2YEp2EBq5vf307KHNRmZZUmkn0zHOSEpNmY2fMxISBxewlxR
FAniwmSd/8TDvHJMY9FvAIvWuTsv5l0tJKk+a91K4+tO3UdDR7Sno5WXExfsBrW3
g1ydo3TBsx8i5/YiVOcNApy7ge2/FiwY3aCXJB6r6nuF6H8mRgI4r4vkMRsOlAhJ
DnZPNeweboo+K3Q3lwbgbmOKD/z9svk8N/+hUTBtIX0fRtbG+PLIw3xWRHGrMSn2
BzsPVuDLAgMBAAECggEACiJUj2hfJkKv47Dc3es3Zex67A5uDVjXmxfox2Xhdupn
fAcNqAptV6fXt0SPUNbhUxbBKNbshoJGufFwXPli1SXnpzvkdU4Hyco4zgbhXFsE
RNYjYfOGzTPwdBLpNMB6k3Tp4RHse6dNrlH0jDhpioL8cQEBdBJyVF5X0wymEbmV
mC0jgH/MxsBAPWW6ZKicg9ULMlWiAZ3MRAZPjHHgpYkAAsUWKAbCBwVQcVjGO59W
jfZjzTX5pQtVVH68ruciH88DTZCwjCkjBhxg+OIkJBLE5wkh82jIHSivZ63flwLw
z+E0+HhELSZJrn2MY6Jxmik3qNNUOF/Z+3msdj2luQKBgQDjwlC/3jxp8zJy6P8o
JQKv7TdvMwUj4VSWOHZBHLv4evJaaia0uQjIo1UDa8AYitqhX1NmCCehGH8yuXj/
v6V3CzMKDkmRr1NrONnSz5QsndQ04Z6ihAQlPmJ96g4wKtgoC7AYpyP0g1a+4/sj
b1+o3YQI4pD/F71c+qaztH7PRwKBgQDdc23yNmT3+Jyptf0fKjEvONK+xwUKzi9c
L/OzBq5yOIC1Pz2T85gOe1i8kwZws+xlpG6uBT6lmIJELd0k59FyupNu4dPvX5SD
6GGqdx4jk9KvI74usGeOBohmF0phTHkrWKBxXiyT0oS8zjnJlEn8ysIpGgO28jjr
LpaHNZ/MXQKBgQDfLNcnS0LzpsS2aK0tzyZU8SMyqVHOGMxj7quhneBq2T6FbiLD
T9TVlYaGNZ0j71vQaLI19qOubWymbautH0Op5KV8owdf4+bf1/NJaPIOzhDUSIjD
Qo01WW31Z9XDSRhKFTnWzmCjBdeIcajyzf10YKsycaAW9lItu8aBrMndnQKBgQDb
nNp/JyRwqjOrNljk7DHEs+SD39kHQzzCfqd+dnTPv2sc06+cpym3yulQcbokULpy
fmRo3bin/pvJQ3aZX/Bdh9woTXqhXDdrrSwWInVYMQPyPk8f/D9mIOJp5FUWMwHD
U+whIZSxsEeE+jtixlWtheKRYkQmzQZXbWdIhYyI3QKBgD+F/6wcZ85QW8nAUykA
3WrSIx/3cwDGdm4NRGct8ZOZjTHjiy9ojMOD1L7iMhRQ/3k3hUsin5LDMp/ryWGG
x4uIaLat40kiC7T4I66DM7P59euqdz3w0PD+VU+h7GSivvsFDdySUt7bNK0AUVLh
dMJfWxDN8QV0b5p3WuWH1U8B
-----END PRIVATE KEY-----
Private-Key: (2048 bit)
modulus:
    00:c5:05:71:d1:23:81:d5:28:08:61:de:c7:a2:72:
    2a:28:8b:30:91:4d:b2:5e:d7:e6:2c:c4:d4:e3:6b:
    85:f2:2b:2a:55:18:81:56:0c:68:59:b3:8e:05:08:
    79:4f:38:e4:95:27:e3:6a:3f:be:30:f7:aa:0c:ec:
    33:d2:df:1a:3d:91:a4:32:64:11:67:d9:81:29:d8:
    40:6a:e6:f7:f7:d3:b2:87:35:19:99:65:49:a4:9f:
    4c:c7:39:21:29:36:66:36:7c:cc:48:48:1c:5e:c2:
    5c:51:14:09:e2:c2:64:9d:ff:c4:c3:bc:72:4c:63:
    d1:6f:00:8b:d6:b9:3b:2f:e6:5d:2d:24:a9:3e:6b:
    dd:4a:e3:eb:4e:dd:47:43:47:b4:a7:a3:95:97:13:
    17:ec:06:b5:b7:83:5c:9d:a3:74:c1:b3:1f:22:e7:
    f6:22:54:e7:0d:02:9c:bb:81:ed:bf:16:2c:18:dd:
```

```
    a0:97:24:1e:ab:ea:7b:85:e8:7f:26:46:02:38:af:
    8b:e4:31:1b:0e:94:08:49:0e:76:4f:35:ec:1e:6e:
    8a:3e:2b:74:37:97:06:e0:6e:63:8a:0f:fc:fd:b2:
    f9:3c:37:ff:a1:51:30:6d:21:7d:1f:46:d6:c6:f8:
    f2:c8:c3:7c:56:44:71:ab:31:29:f6:07:3b:0f:56:
    e0:cb
publicExponent: 65537 (0x10001)
privateExponent:
    0a:22:54:8f:68:5f:26:42:af:e3:b0:dc:dd:eb:37:
    65:ec:7a:ec:0e:6e:0d:58:d7:9b:17:e8:c7:65:e1:
    76:ea:67:7c:07:0d:a8:0a:6d:57:a7:d7:b7:44:8f:
    50:d6:e1:53:16:c1:28:d6:ec:86:82:46:b9:f1:70:
    5c:f9:62:d5:25:e7:a7:3b:e4:75:4e:07:c9:ca:38:
    ce:06:e1:5c:5b:04:44:d6:23:61:f3:86:cd:33:f0:
    74:12:e9:34:c0:7a:93:74:e9:e1:11:ec:7b:a7:4d:
    ae:51:f4:8c:38:69:8a:82:fc:71:01:01:74:12:72:
    54:5e:57:d3:0c:a6:11:b9:95:98:2d:23:80:7f:cc:
    c6:c0:40:3d:65:ba:64:a8:9c:83:d5:0b:32:55:a2:
    01:9d:cc:44:06:4f:8c:71:e0:a5:89:00:02:c5:16:
    28:06:c2:07:05:50:71:58:c6:3b:9f:56:8d:f6:63:
    cd:35:f9:a5:0b:55:54:7e:bc:ae:e7:22:1f:cf:03:
    4d:90:b0:8c:29:23:06:1c:60:f8:e2:24:24:12:c4:
    e7:09:21:f3:68:c8:1d:28:af:67:ad:df:97:02:f0:
    cf:e1:34:f8:78:44:2d:26:49:ae:7d:8c:63:a2:71:
    9a:29:37:a8:d3:54:38:5f:d9:fb:79:ac:76:3d:a5:
    b9
prime1:
    00:e3:c2:50:bf:de:3c:69:f3:32:72:e8:ff:28:25:
    02:af:ed:37:6f:33:05:23:e1:54:96:38:76:41:1c:
    bb:f8:7a:f2:5a:6a:26:b4:b9:08:c8:a3:55:03:6b:
    c0:18:8a:da:a1:5f:53:66:08:27:a1:18:7f:32:b9:
    78:ff:bf:a5:77:0b:33:0a:0e:49:91:af:53:6b:38:
    d9:d2:cf:94:2c:9d:d4:34:e1:9e:a2:84:04:25:3e:
    62:7d:ea:0e:30:2a:d8:28:0b:b0:18:a7:23:f4:83:
    56:be:e3:fb:23:6f:5f:a8:dd:84:08:e2:90:ff:17:
    bd:5c:fa:a6:b3:b4:7e:cf:47
prime2:
    00:dd:73:6d:f2:36:64:f7:f8:9c:a9:b5:fd:1f:2a:
    31:2f:38:d2:be:c7:05:0a:ce:2f:5c:2f:f3:b3:06:
    ae:72:38:80:b5:3f:3d:93:f3:98:0e:7b:58:bc:93:
    06:70:b3:ec:65:a4:6e:ae:05:3e:a5:98:82:44:2d:
    dd:24:e7:d1:72:ba:93:6e:e1:d3:ef:5f:94:83:e8:
    61:aa:77:1e:23:93:d2:af:23:be:2e:b0:67:8e:06:
    88:66:17:4a:61:4c:79:2b:58:a0:71:5e:2c:93:d2:
```

```
    84:bc:ce:39:c9:94:49:fc:ca:c2:29:1a:03:b6:f2:
    38:eb:2e:96:87:35:9f:cc:5d
exponent1:
    00:df:2c:d7:27:4b:42:f3:a6:c4:b6:68:ad:2d:cf:
    26:54:f1:23:32:a9:51:ce:18:cc:63:ee:ab:a1:9d:
    e0:6a:d9:3e:85:6e:22:c3:4f:d4:d5:95:86:86:35:
    9d:23:ef:5b:d0:68:b2:35:f6:a3:ae:6d:6c:a6:6d:
    ab:ad:1f:43:a9:e4:a5:7c:a3:07:5f:e3:e6:df:d7:
    f3:49:68:f2:0e:ce:10:d4:48:88:c3:42:8d:35:59:
    6d:f5:67:d5:c3:49:18:4a:15:39:d6:ce:60:a3:05:
    d7:88:71:a8:f2:cd:fd:74:60:ab:32:71:a0:16:f6:
    52:2d:bb:c6:81:ac:c9:dd:9d
exponent2:
    00:db:9c:da:7f:27:24:70:aa:33:ab:36:58:e4:ec:
    31:c4:b3:e4:83:df:d9:07:43:3c:c2:7e:a7:7e:76:
    74:cf:bf:6b:1c:d3:af:9c:a7:29:b7:ca:e9:50:71:
    ba:24:50:ba:72:7e:64:68:dd:b8:a7:fe:9b:c9:43:
    76:99:5f:f0:5d:87:dc:28:4d:7a:a1:5c:37:6b:ad:
    2c:16:22:75:58:31:03:f2:3e:4f:1f:fc:3f:66:20:
    e2:69:e4:55:16:33:01:c3:53:ec:21:21:94:b1:b0:
    47:84:fa:3b:62:c6:55:ad:85:e2:91:62:44:26:cd:
    06:57:6d:67:48:85:8c:88:dd
coefficient:
    3f:85:ff:ac:1c:67:ce:50:5b:c9:c0:53:29:00:dd:
    6a:d2:23:1f:f7:73:00:c6:76:6e:0d:44:67:2d:f1:
    93:99:8d:31:e3:8b:2f:68:8c:c3:83:d4:be:e2:32:
    14:50:ff:79:37:85:4b:22:9f:92:c3:32:9f:eb:c9:
    61:86:c7:8b:88:68:b6:ad:e3:49:22:0b:b4:f8:23:
    ae:83:33:b3:f9:f5:eb:aa:77:3d:f0:d0:f0:fe:55:
    4f:a1:ec:64:a2:be:fb:05:0d:dc:92:52:de:db:34:
    ad:00:51:52:e1:74:c2:5f:5b:10:cd:f1:05:74:6f:
    9a:77:5a:e5:87:d5:4f:01
```

Conservez votre clé privée dans un endroit sécurisé lorsqu'elle n'est pas utilisée.

2. Générez un certificat X.509 à l'aide de la paire de clés créée à l'étape précédente. Dans cet exemple, le certificat expire dans 365 jours, après quoi il n'est plus fiable. Veillez donc à définir l'expiration de façon appropriée. Le certificat ne doit être valide que pendant la durée du processus de provisionnement. Vous pouvez supprimer le certificat RIR de votre dossier une fois le provisionnement terminé. La commande `tr -d "\n"` supprime les caractères de nouvelle ligne (sauts de ligne) de la sortie. Vous devez fournir un nom commun lorsque vous y êtes invité, mais les autres champs peuvent être laissés vides.

```
$ openssl req -new -x509 -key private-key.pem -days 365 | tr -d "\n" >
 certificate.pem
```

Cela génère une sortie semblable à ce qui suit :

```
Enter pass phrase for private-key.pem: xxxxxxx
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, fully qualified host name) []:example.com
Email Address []:
```

> **Note**
>
> Le nom commun n'est pas nécessaire pour le AWS provisionnement. Il peut s'agir de n'importe quel nom de domaine interne ou public.

Vous pouvez inspecter le certificat à l'aide de la commande suivante :

```
$ cat certificate.pem
```

La sortie doit être une longue chaîne PEM codée sans sauts de ligne, préfacée `-----BEGIN CERTIFICATE-----` et suivie de. `-----END CERTIFICATE-----`

Téléchargez le certificat X.509 dans l'RDAPenregistrement de votre RIR

Ajoutez le certificat que vous avez créé précédemment à l'RDAPenregistrement de votreRIR. Veillez à inclure le `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` avant et

après la partie encodée. Tout ce contenu doit se trouver sur une seule et longue ligne. La procédure de mise à jour RDAP dépend de RIR :

- En ARIN outre, utilisez le portail Account Manager pour ajouter le certificat dans la section « Commentaires publics » pour l'objet « Informations réseau » représentant votre plage d'adresses. Ne l'ajoutez pas à la section des commentaires de votre organisation.
- Pour celaRIPE, ajoutez le certificat sous la forme d'un nouveau champ « descr » à l'objet « inetnum » ou « inet6num » représentant votre plage d'adresses. Elles se trouvent généralement dans la section « Mes ressources » du portail de RIPE base de données. Ne l'ajoutez pas dans la section des commentaires de votre organisation ni dans le champ « remarques » des objets ci-dessus.
- Pour celaAPNIC, envoyez le certificat par e-mail à helpdesk@apnic.net pour l'ajouter manuellement dans le champ « remarques » de votre plage d'adresses. Envoyez l'e-mail en utilisant le contact APNIC autorisé pour les adresses IP.

Vous pouvez supprimer le certificat RIR de votre dossier une fois l'étape de provisionnement ci-dessous terminée.

Créez un ROA objet dans votre RIR

Créez un ROA objet pour autoriser les Amazon ASNs 16509 et 14618 à faire de la publicité pour votre plage d'adresses, ainsi que pour ceux ASNs qui sont actuellement autorisés à faire de la publicité pour la plage d'adresses. Pour le AWS GovCloud (US) Regions, autorisez ASN 8987 au lieu de 16509 et 14618. Vous devez définir la longueur maximale en fonction de la taille du produit CIDR que vous apportez. Le IPv4 préfixe le plus spécifique que vous pouvez apporter est /24. La plage d'IPv6adresses la plus précise que vous pouvez apporter est /48 pour celles CIDRs qui sont publiables et /56 pour celles CIDRs qui ne le sont pas.

> **Important**
>
> Si vous créez un ROA objet pour Amazon VPC IP Address Manager (IPAM), IPv4 CIDRs vous devez définir la ROAs longueur maximale d'un préfixe d'adresse IP sur`/24`. En IPv6 CIDRs effet, si vous les ajoutez à un pool publicitaire, la longueur maximale d'un préfixe d'adresse IP doit être de. `/48` Cela vous garantit une flexibilité totale pour répartir votre adresse IP publique entre AWS les régions. IPAMapplique la longueur maximale que vous avez définie. Pour plus d'informations sur BYOIP les adresses àIPAM, consultez Tutoriel : BYOIP address CIDRs to IPAM dans le guide de VPC IPAM l'utilisateur Amazon.

La mise à disposition d'Amazon peut prendre jusqu'à 24 heures. ROA Pour plus d'informations, consultez votre RIR :

- ARIN— ROADemandes
- RIPE— Gérer ROAs
- APNIC— Gestion des itinéraires

Lorsque vous migrez des publicités d'une charge de travail sur site vers AWS, vous devez en créer une ROA pour votre charge de travail existante ASN avant de créer une ROAs pour Amazon. ASNs Sinon, vous risquez de voir un impact sur votre routage et vos annonces existantes.

> **Important**
>
> Pour qu'Amazon puisse faire de la publicité et continuer à faire de la publicité pour votre plage ROAs d'adresses IP, vous ASNs devez respecter les directives ci-dessus sur Amazon. Si vous n'ROAsêtes pas valide ou si vous ne respectez pas les directives ci-dessus, Amazon se réserve le droit de cesser de faire de la publicité pour votre plage d'adresses IP.

> **Note**
>
> Cette étape n'est pas obligatoire pour les espaces d'IPv6adressage ne faisant pas l'objet d'une publicité publique.

Intégrez votre plage d'adresses pour une utilisation sur Amazon EC2

Le processus d'intégration BYOIP inclut les tâches suivantes, en fonction de vos besoins.

Tâches

- Fournir une plage d'adresses pouvant faire l'objet d'une publicité publique en AWS
- Fournir une plage d'IPv6adresses qui ne fait pas l'objet d'une publicité publique
- Faites connaître la plage d'adresses via AWS
- Mise hors service de la plage d'adresses
- Validez votre BYOIP

Fournir une plage d'adresses pouvant faire l'objet d'une publicité publique en AWS

Lorsque vous configurez une plage d'adresses à utiliser avec AWS, vous confirmez que vous contrôlez la plage d'adresses et que vous autorisez Amazon à en faire la publicité. Nous vérifions également que vous contrôlez la plage d'adresses via un message d'autorisation signé. Ce message est signé avec la paire de clés X.509 auto-signée que vous avez utilisée lors de la mise à jour de l'RDAPenregistrement avec le certificat X.509. AWS nécessite un message d'autorisation signé cryptographiquement qu'il présente auRIR. RIRAuthentifie la signature par rapport au certificat que vous avez ajouté et vérifie RDAP les détails de l'autorisation par rapport auROA.

Pour allouer la plage d'adresses

1. Composer un message

   Composez le message d'autorisation en texte brut. Le format du message est le suivant, où la date est la date d'expiration du message :

   ```
   1|aws|account|cidr|YYYYMMDD|SHA256|RSAPSS
   ```

   Remplacez le numéro de compte, la plage d'adresses et la date d'expiration par vos propres valeurs pour créer un message semblable au suivant :

   ```
   text_message="1|aws|0123456789AB|198.51.100.0/24|20211231|SHA256|RSAPSS"
   ```

   Il ne faut pas le confondre avec un ROA message qui a une apparence similaire.

2. Signer un message

   Signez le message en texte brut à l'aide de la clé privée que vous avez créée précédemment. La signature renvoyée par cette commande est une longue chaîne que vous devrez utiliser à l'étape suivante.

   > **Important**
   >
   > Nous vous recommandons de copier et de coller cette commande. À l'exception du contenu du message, ne modifiez ni ne remplacez aucune des valeurs.

```
signed_message=$( echo -n $text_message | openssl dgst -sha256 -sigopt
 rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private-key.pem -keyform PEM
 | openssl base64 | tr -- '+=/' '-_~' | tr -d "\n")
```

3. Approvisionner une adresse

   Utilisez la AWS CLI provision-byoip-cidrcommande pour configurer la plage d'adresses. La commande `--cidr-authorization-context` utilise les chaînes de message et de signature que vous avez créées précédemment.

   > **Important**
   >
   > Vous devez spécifier la AWS région dans laquelle la BYOIP plage doit être provisionnée si elle est différente de votre configuration du AWS CLI`Default region name`.

   ```
   aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
    Message="$text_message",Signature="$signed_message" --region us-east-1
   ```

   La mise en service d'une plage d'adresses est une opération asynchrone : l'appel est immédiatement renvoyé, mais la plage d'adresses ne peut pas être utilisée tant que son statut ne bascule pas de `pending-provision` à `provisioned`.

4. Surveiller la progression

   Bien que la plupart des approvisionnements soient effectués dans les deux heures, le processus d'approvisionnement pour les gammes pouvant faire l'objet d'une publicité publique peut prendre jusqu'à une semaine. Utilisez la describe-byoip-cidrscommande pour suivre les progrès, comme dans cet exemple :

   ```
   aws ec2 describe-byoip-cidrs --max-results 5 --region us-east-1
   ```

   S'il y a des problèmes pendant la mise en service et que l'état passe à `failed-provision`, vous devez exécuter à nouveau la commande `provision-byoip-cidr` une fois que les problèmes ont été résolus.

Fournir une plage d'IPv6adresses qui ne fait pas l'objet d'une publicité publique

Par défaut, une plage d'adresses est allouée pour être publiquement publiée sur Internet. Vous pouvez fournir une plage d'IPv6adresses qui ne fera pas l'objet d'une publicité publique. Pour les acheminements qui ne sont pas publiquement annoncés, le processus d'approvisionnement se termine généralement en quelques minutes. Lorsque vous associez un IPv6 CIDR bloc d'une plage d'adresses non publique à unVPC, celui-ci n'est IPv6 CIDR accessible que par le biais d'options de connectivité hybrides prenant en charge IPv6 AWS Direct Connect, telles que les passerelles de AWS site à site VPN ou Amazon VPC Transit Gateway.

A n'ROAest pas obligatoire pour fournir une plage d'adresses non publiques.

> **Important**
>
> - Vous ne pouvez spécifier si une plage d'adresses est publiquement publiée que pendant l'allocation. Vous ne pouvez pas modifier l'état annoncé ultérieurement.
> - Amazon VPC ne prend pas en charge les adresses locales uniques (ULA)CIDRs. Tous VPCs doivent être uniques IPv6CIDRs. Deux ne VPCs peuvent pas avoir la même IPv6 CIDR portée.

Pour fournir une plage d'IPv6adresses qui ne fera pas l'objet d'une publicité publique, utilisez la provision-byoip-cidrcommande suivante.

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
 Message="$text_message",Signature="$signed_message" --no-publicly-advertisable --
region us-east-1
```

Faites connaître la plage d'adresses via AWS

Une fois que la plage d'adresses est mise en service, elle est prête à être publiée. Vous devez publier la plage d'adresses exacte que vous avez mise en service. Vous ne pouvez pas publier seulement une portion de la plage d'adresses mise en service.

Si vous avez fourni une plage d'IPv6adresses qui ne sera pas publiée publiquement, vous n'avez pas besoin de suivre cette étape.

Nous vous recommandons de cesser de faire de la publicité pour la plage d'adresses ou toute partie de cette plage depuis d'autres sites avant de la diffuser AWS. Si vous continuez à faire de la publicité

pour votre plage d'adresses IP, en tout ou en partie, à partir d'autres sites, nous ne serons pas en mesure de fournir une assistance fiable ou de résoudre les problèmes. Plus précisément, nous ne pouvons pas garantir que le trafic vers la plage d'adresses ou une partie de cette plage entrera dans notre réseau.

Pour minimiser les temps d'arrêt, vous pouvez configurer vos AWS ressources pour utiliser une adresse de votre pool d'adresses avant qu'elle ne soit publiée, puis arrêter de la publier depuis son emplacement actuel et commencer à en faire la publicité par le biais AWS de cette adresse. Pour plus d'informations sur l'allocation d'une adresse IP Elastic à partir de votre groupe d'adresses, consultez allouer une adresse IP Elastic ;.

Limites

- Vous pouvez exécuter la commande advertise-byoip-cidr au moins une fois tous les 10 secondes, même si vous spécifiez des plages d'adresses différentes à chaque fois.
- Vous pouvez exécuter la commande withdraw-byoip-cidr au moins une fois tous les 10 secondes, même si vous spécifiez des plages d'adresses différentes à chaque fois.

Pour publier la plage d'adresses, utilisez la advertise-byoip-cidrcommande suivante.

```
aws ec2 advertise-byoip-cidr --cidr address-range --region us-east-1
```

Pour arrêter de publier la plage d'adresses, utilisez la withdraw-byoip-cidrcommande suivante.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Mise hors service de la plage d'adresses

Pour arrêter d'utiliser votre plage d'adresses AWS, libérez d'abord toutes les adresses IP élastiques et dissociez les IPv6 CIDR blocs encore alloués du pool d'adresses. Ensuite, arrêtez la publicité de la plage d'adresses et enfin, mettez hors service la plage d'adresses.

Vous ne pouvez pas mettre hors service une partie de la plage d'adresses. Si vous souhaitez utiliser une plage d'adresses plus spécifique avec AWS, déprovisionnez l'ensemble de la plage d'adresses et configurez une plage d'adresses plus spécifique.

(IPv4) Pour libérer chaque adresse IP élastique, utilisez la commande release-address suivante.

```
aws ec2 release-address --allocation-id eipalloc-12345678abcabcabc --region us-east-1
```

(IPv6) Pour dissocier un IPv6 CIDR bloc, utilisez la disassociate-vpc-cidr-blockcommande suivante.

```
aws ec2 disassociate-vpc-cidr-block --association-id vpc-cidr-assoc-12345abcd1234abc1
 --region us-east-1
```

Pour arrêter de publier la plage d'adresses, utilisez la withdraw-byoip-cidrcommande suivante.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Pour déprovisionner la plage d'adresses, utilisez la deprovision-byoip-cidrcommande suivante.

```
aws ec2 deprovision-byoip-cidr --cidr address-range --region us-east-1
```

La mise hors service d'une plage d'adresses peut prendre jusqu'à un jour.

Validez votre BYOIP

1. Valider la paire de clés x.509 auto-signée

   Vérifiez que le certificat a été chargé et est valide via la commande whois.

   PourARIN, utilisez `whois -h whois.arin.net r + 2001:0DB8:6172::/48` pour rechercher l'RDAPenregistrement correspondant à votre plage d'adresses. Recherchez la `NetRange` (plage réseau) dans la section `Public Comments` dans la sortie de commande. Le certificat doit être ajouté dans la section `Public Comments` pour la plage d'adresses.

   Vous pouvez inspecter le `Public Comments` contenant le certificat à l'aide de la commande suivante :

   ```
   whois -h whois.arin.net r + 2001:0DB8:6172::/48 | grep Comments | grep BEGIN
   ```

   Cela renvoie une sortie avec le contenu de la clé, qui devrait être similaire à ce qui suit :

   ```
   Public Comments:
   -----BEGIN CERTIFICATE-----
   MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
   LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
   hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
   wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
   NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
   ```

```
rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

PourRIPE, utilisez `whois -r -h whois.ripe.net` *`2001:0DB8:7269::/48`* pour rechercher l'RDAPenregistrement correspondant à votre plage d'adresses. Recherchez l'object `inetnum` (plage réseau) dans la section `descr` dans la sortie de commande. Le certificat doit être ajouté en tant que nouveau champ `descr` pour la plage d'adresses.

Vous pouvez inspecter le `descr` contenant le certificat à l'aide de la commande suivante :

```
whois -r -h whois.ripe.net 2001:0DB8:7269::/48 | grep descr | grep BEGIN
```

Cela renvoie une sortie avec le contenu de la clé, qui devrait être similaire à ce qui suit :

```
descr:
-----BEGIN CERTIFICATE-----MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8
RDAHSP+I1TowDQYJKoZIhvcNAQELBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAg
MCEF1Y2tsYW5kMREwDwYDVQQHDAhBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIF
dlYiBTZXJ2aWNlczETMBEGA1UECwwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPS
VAgRGVtbzAeFw0yMTEyMDcyMDI0NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNV
BAYTAk5aMREwDwYDVQQIDAhBdWNrbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDA
aBgNVBAoME0FtYXpvbiBXZWIgU2VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW
8xEzARBgNVBAMMCkJZT0lQIERlbW8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwg
gEKAoIBAQCfmacvDp0wZ0ceiXXcR/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanA
EskgAseyFypwEEQr4CJijI/5hp9prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3
stsI5QesHVRwOaXUdprAnndaTugmDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq
35wU/x+wXlAqBXg4MZK2KoUu27kYt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp
```

```
1ZnVIc7NqnhdeIW48QaYjhMlUEfxdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2r
GlHWkJsbhr0VEUyAGu1bwkgcdww3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBS
tFyujN6SYBr2glHpGt0XGF7GbGTAfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0
XGF7GbGTAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6Y
Lhz521lfyVfxY0t6o3410bQAeAF08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyL
xngwMYN0XY5tVhDQqk4/gmDNEKSZy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9
wySL507XQz76Uk5cFypBOzbnk35UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8
mBGqVpPpey+dXpzzzv1iBKN/VY4ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGC
vRDl/qdO/GIDJi77dmZWkh/ic90MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoN
PyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

PourAPNIC, utilisez `whois -h whois.apnic.net` *`2001:0DB8:6170::/48`* pour rechercher l'RDAPenregistrement correspondant à votre plage d'BYOIPadresses. Recherchez l'object `inetnum` (plage réseau) dans la section `remarks` dans la sortie de commande. Le certificat doit être ajouté en tant que nouveau champ `remarks` pour la plage d'adresses.

Vous pouvez inspecter le `remarks` contenant le certificat à l'aide de la commande suivante :

```
whois -h whois.apnic.net 2001:0DB8:6170::/48 | grep remarks | grep BEGIN
```

Cela renvoie une sortie avec le contenu de la clé, qui devrait être similaire à ce qui suit :

```
remarks:
-----BEGIN CERTIFICATE-----
MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
```

```
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

2. Valider la création d'un ROA objet

   Validez la création réussie des ROA objets à l'aide RIPEstat des donnéesAPI. Assurez-vous de tester votre plage d'adresses par rapport aux adresses Amazon ASNs 16509 et 14618, ainsi qu'à celles ASNs qui sont actuellement autorisées à faire de la publicité pour la plage d'adresses.

   Vous pouvez inspecter les ROA objets provenant de différents Amazon ASNs avec votre plage d'adresses à l'aide de la commande suivante :

   ```
   curl --location --request GET "https://stat.ripe.net/data/rpki-validation/data.json?
   resource=ASN&prefix=CIDR
   ```

   Dans cet exemple de sortie, le résultat de la réponse est `"status": "valid"` pour Amazon ASN 16509. Cela indique que l'ROAobjet de la plage d'adresses a été créé avec succès :

   ```
   {
       "messages": [],
       "see_also": [],
       "version": "0.3",
       "data_call_name": "rpki-validation",
       "data_call_status": "supported",
       "cached": false,
       "data": {
           "validating_roas": [
               {
                   "origin": "16509",
                   "prefix": "2001:0DB8::/32",
                   "max_length": 48,
                   "validity": "valid"
               },
               {
                   "origin": "14618",
                   "prefix": "2001:0DB8::/32",
                   "max_length": 48,
                   "validity": "invalid_asn"
               },
   ```

```
            {
                "origin": "64496",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "invalid_asn"
            }
        ],
        "status": "valid",
        "validator": "routinator",
        "resource": "16509",
        "prefix": "2001:0DB8::/32"
    },
    "query_id": "20230224152430-81e6384e-21ba-4a86-852a-31850787105f",
    "process_time": 58,
    "server_id": "app116",
    "build_version": "live.2023.2.1.142",
    "status": "ok",
    "status_code": 200,
    "time": "2023-02-24T15:24:30.773654"
}
```


Le statut "`unknown`" indique que l'ROAobjet de la plage d'adresses n'a pas été créé. Un statut de "`invalid_asn`" indique que l'ROAobjet de la plage d'adresses n'a pas été créé correctement.

Utilisez votre plage d'BYOIPadresses sur Amazon EC2

Vous pouvez consulter et utiliser les plages d'IPv6adresses IPv4 et d'adresses que vous avez configurées dans votre compte. Pour de plus amples informations, veuillez consulter the section called "Intégrez votre plage d'adresses".

IPv4plages d'adresses

Vous pouvez créer une adresse IP élastique à partir de votre pool d'IPv4adresses et l'utiliser avec vos AWS ressources, telles que les EC2 instances, les NAT passerelles et les équilibreurs de charge réseau.

Pour afficher des informations sur les pools d'IPv4adresses que vous avez configurés dans votre compte, utilisez la commande describe-public-ipv4-pools suivante.

```
aws ec2 describe-public-ipv4-pools --region us-east-1
```

Pour créer une adresse IP élastique à partir de votre pool d'IPv4adresses, utilisez la commande allocate-address. Vous pouvez utiliser l'option `--public-ipv4-pool` pour spécifier l'ID du groupe d'adresses renvoyé par `describe-byoip-cidrs`. Vous pouvez aussi utiliser l'option `--address` pour spécifier une adresse de la plage d'adresses que vous avez allouée.

IPv6plages d'adresses

Pour afficher des informations sur les pools d'IPv6adresses que vous avez configurés dans votre compte, utilisez la commande describe-ipv6-pools suivante.

```
aws ec2 describe-ipv6-pools --region us-east-1
```

Pour créer un VPC et en spécifier un IPv6 CIDR à partir de votre pool d'IPv6adresses, utilisez la commande create-vpc suivante. Pour permettre à Amazon IPv6 CIDR de choisir l'IPv6adresse dans votre pool d'adresses, omettez `--ipv6-cidr-block` cette option.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --ipv6-cidr-block ipv6-cidr --ipv6-
pool pool-id --region us-east-1
```

Pour associer un IPv6 CIDR bloc de votre pool d'IPv6adresses à unVPC, utilisez la associate-vpc-cidr-blockcommande suivante. Pour permettre à Amazon IPv6 CIDR de choisir l'IPv6adresse dans votre pool d'adresses, omettez `--ipv6-cidr-block` cette option.

```
aws ec2 associate-vpc-cidr-block --vpc-id vpc-123456789abc123ab --ipv6-cidr-block ipv6-
cidr --ipv6-pool pool-id --region us-east-1
```

Pour consulter les informations relatives à votre pool d'IPv6adresses VPCs et à celles associées, utilisez la commande describe-vpcs. Pour afficher des informations sur les IPv6 CIDR blocs associés à partir d'un pool d'IPv6adresses spécifique, utilisez la commande get-associated-ipv6-pool-cidrs suivante.

```
aws ec2 get-associated-ipv6-pool-cidrs --pool-id pool-id --region us-east-1
```

Si vous dissociez le IPv6 CIDR bloc de votreVPC, il est réintégré dans votre pool d'IPv6adresses.

Adresses IP Elastic

Une adresse IP élastique est une IPv4 adresse statique conçue pour le cloud computing dynamique. Une adresse IP élastique est attribuée à votre AWS compte et vous appartient jusqu'à ce que vous

la publiiez. En utilisant une adresse IP Elastic, vous pouvez contourner un problème de défaillance d'une instance ou d'un logiciel en remappant rapidement l'adresse à une autre instance de votre compte. Vous pouvez également spécifier l'adresse IP élastique dans un DNS enregistrement pour votre domaine, afin que celui-ci pointe vers votre instance. Pour plus d'informations, consultez la documentation de votre bureau d'enregistrement de domaines.

Une adresse IP élastique est une IPv4 adresse publique accessible depuis Internet. Si vous devez vous connecter à une instance qui ne possède pas d'IPv4adresse publique, vous pouvez associer une adresse IP élastique à votre instance pour permettre la communication avec Internet.

Table des matières

Tarification des adresses IP Elastic

AWS frais pour toutes les IPv4 adresses publiques, y compris les IPv4 adresses publiques associées aux instances en cours d'exécution et les adresses IP Elastic. Pour plus d'informations, consultez l'onglet IPv4Adresse publique sur la page de VPC tarification d'Amazon.

Principes de base d'une adresse IP Elastic

Les caractéristiques de base d'une adresse IP Elastic sont les suivantes :

- Une adresse IP Elastic est statique ; elle ne change pas au fil du temps.
- Une adresse IP Elastic est destinée uniquement à une région spécifique et ne peut pas être déplacée vers une autre région.
- Une adresse IP élastique provient du pool d'IPv4adresses d'Amazon ou d'un pool d'IPv4adresses personnalisé que vous avez intégré à votre compte Compte AWS. Nous ne prenons pas en charge les adresses IP élastiques pourIPv6.

- Pour utiliser une adresse IP Elastic, commencez par en attribuer une à votre compte, puis associez-la à votre instance ou à une interface réseau.
- Lorsque vous associez une adresse IP Elastic à une instance, elle est également associée à l'interface réseau principale de l'instance. Lorsque vous associez une adresse IP Elastic à une interface réseau attachée à une instance, elle est également associée à l'instance.
- Lorsque vous associez une adresse IP élastique à une instance ou à son interface réseau principale, si l'instance est déjà associée à une IPv4 adresse publique, cette IPv4 adresse publique est réintégrée dans le pool d'IPv4adresses publiques d'Amazon et l'adresse IP élastique est associée à l'instance à la place. Vous ne pouvez pas réutiliser l'IPv4adresse publique précédemment associée à l'instance et vous ne pouvez pas convertir cette IPv4 adresse publique en adresse IP élastique. Pour de plus amples informations, veuillez consulter IPv4Adresses publiques.
- Vous pouvez dissocier une adresse IP Elastic d'une ressource et la réassocier à une autre ressource. Pour éviter un comportement inattendu, assurez-vous que toutes les connexions actives à la ressource nommée dans l'association existante sont fermées avant d'effectuer la modification. Une fois que vous avez associé votre adresse IP Elastic à une ressource différente, vous pouvez rouvrir vos connexions à la ressource nouvellement associée.
- Une adresse IP Elastic dissociée demeure attribuée à votre compte jusqu'à ce que vous la libériez explicitement. Toutes les adresses IP Elastic de votre compte vous sont facturées, qu'elles soient associées ou non à une instance. Pour plus d'informations, consultez l'onglet IPv4Adresse publique sur la page de VPCtarification d'Amazon.
- Lorsque vous associez une adresse IP élastique à une instance qui possédait auparavant une IPv4 adresse publique, le nom d'DNShôte public de l'instance change pour correspondre à l'adresse IP élastique.
- Nous associons un nom d'DNShôte public à l'IPv4adresse publique ou à l'adresse IP élastique de l'instance en dehors du réseau de l'instance, et à l'IPv4adresse privée de l'instance depuis le réseau de l'instance.
- Lorsque vous attribuez une adresse IP élastique à partir d'un pool d'adresses IP que vous avez ajouté à votre AWS compte, elle n'est pas prise en compte dans le calcul de vos limites d'adresses IP élastiques. Pour de plus amples informations, veuillez consulter Quota appliqué aux adresses IP Elastic.
- Lorsque vous allouez les adresses IP Elastic, vous pouvez les associer à un groupe de bordure réseau. C'est à partir de cet endroit que nous annonçons le CIDR bloc. La définition du groupe frontalier du réseau limite le CIDR blocage à ce groupe. Si vous ne spécifiez pas le groupe de

bordure réseau, nous définissons le groupe de bordure contenant toutes les zones de disponibilité de la région (par exemple, `us-west-2`).

- Une adresse IP Elastic ne peut être utilisée que dans un groupe de frontière de réseau spécifique.

Quota appliqué aux adresses IP Elastic

Par défaut, toutes Comptes AWS ont un quota de cinq (5) adresses IP élastiques par région, car les adresses Internet publiques (IPv4) sont une ressource publique rare. Nous vous recommandons vivement d'utiliser les adresses IP élastiques principalement pour leur capacité à remapper l'adresse vers une autre instance en cas de défaillance de l'instance, et pour utiliser des DNSnoms d'hôte pour toutes les autres communications entre nœuds.

Si vous pensez que votre architecture justifie l'utilisation d'adresses IP Elastic supplémentaires, vous pouvez demander une augmentation de quota directement à partir de la console Service Quotas. Pour demander l'augmentation d'un quota, choisissez Demander une augmentation au niveau du compte. Pour de plus amples informations, veuillez consulter Quotas EC2 de service Amazon.

Associer une adresse IP Elastic à une instance

Après avoir alloué une adresse IP Elastic, vous pouvez l'associer à une AWS ressource, telle qu'une EC2 instance, une NAT passerelle ou un Network Load Balancer. Pour associer ultérieurement une adresse IP élastique à une autre AWS ressource, vous pouvez la dissocier de sa ressource actuelle, puis l'associer à la nouvelle ressource.

Effectuez les tâches suivantes pour associer une adresse IP élastique à une EC2 instance.

Tâches

- allouer une adresse IP Elastic ;
- Associer une adresse IP Elastic
- Dissocier une adresse IP Elastic

allouer une adresse IP Elastic ;

Suivez les étapes décrites dans cette section pour allouer une adresse IP élastique.

Console

Pour allouer une adresse IP Elastic

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network & Security, Elastic IPs.
3. Choisissez Allocate Elastic IP address (Allouer l'adresse IP Elastic).
4. (Facultatif) Lorsque vous allouez une adresse IP élastique (EIP), vous choisissez le groupe de bordure du réseau dans lequel vous souhaitez allouer laEIP. Un groupe frontalier réseau est un ensemble de zones de disponibilité (AZs), de zones locales ou de zones de longueur d'onde à partir duquel AWS une adresse IP publique est annoncée. Les zones Locales et les Zones de longueur d'onde peuvent avoir des groupes de bordure de réseau différents de ceux d'une région afin de garantir une latence minimale ou une distance physique minimale entre le AWS réseau et les clients accédant aux ressources de ces zones. AZs

   > **Important**
   >
   > Vous devez allouer un EIP dans le même groupe frontalier du réseau que la AWS ressource qui sera associée auEIP. Un groupe frontalier intégré EIP au réseau ne peut être annoncé que dans les zones de ce groupe de frontières du réseau et non dans les autres zones représentées par d'autres groupes de frontières du réseau.

   Si les zones locales ou les zones de longueur d'onde sont activées (pour plus d'informations, voir Activer une zone locale ou Activer les zones de longueur d'onde), vous pouvez choisir un groupe de bordure réseau pour les AZs zones locales ou les zones de longueur d'onde. Choisissez le groupe de bordure du réseau avec soin, car la EIP AWS ressource à laquelle il est associé doit résider dans le même groupe de bordure du réseau. Vous pouvez utiliser la EC2 console pour afficher le groupe frontalier du réseau dans lequel se trouvent vos zones de disponibilité, vos zones locales ou vos zones de longueur d'onde. En général, toutes les zones de disponibilité d'une région appartiennent au même groupe de bordures réseau, tandis que les zones locales ou les zones Wavelength appartiennent à leurs propres groupes de bordures réseau distincts.

   Si les zones Local ou Wavelength Zones ne sont pas activées, lorsque vous en allouez unEIP, le groupe de bordure du réseau qui représente l'AZsensemble de la région (par exemple`us-west-2`) est prédéfini pour vous et vous ne pouvez pas le modifier. Cela signifie

que le montant EIP que vous allouez à ce groupe frontalier du réseau sera annoncé dans l'ensemble de la région AZs dans laquelle vous vous trouvez.

5. Pour le pool IPv4 d'adresses publiques, choisissez l'une des options suivantes :

   - Le pool d'IPv4adresses d'Amazon : si vous souhaitez qu'une IPv4 adresse soit attribuée à partir du pool d'IPv4adresses d'Amazon.
   - IPv4Adresse publique que vous apportez à votre AWS compte : si vous souhaitez attribuer une adresse publique non contiguë (non séquentielle) à partir d'un pool d'IPv4adresses IP que vous avez intégré à votre compte. AWS Cette option est désactivée si vous ne disposez pas de groupes d'adresses IP. Pour plus d'informations sur l'ajout de votre propre plage d'adresses IP à votre AWS compte, consultezApportez vos propres adresses IP (BYOIP) à Amazon EC2.
   - Pool d'IPv4adresses appartenant au client : si vous souhaitez allouer une IPv4 adresse à partir d'un pool créé à partir de votre réseau local pour une utilisation avec un AWS Outpost. Cette option est désactivée si vous n'avez pas d' AWS Outpost.
   - Allouer à l'aide d'un IPAM IPv4 pool : si vous souhaitez allouer des adresses IP élastiques séquentielles à partir d'un IPv4 bloc public contigu dans un pool. IPAM L'attribution d'adresses IP élastiques séquentielles permet de réduire considérablement les frais de gestion des listes de contrôle d'accès à la sécurité et de simplifier l'allocation et le suivi des adresses IP pour les entreprises qui se développent. AWS Pour plus d'informations, consultez la section Allocation d'adresses IP élastiques séquentielles à partir d'un IPAM pool dans le guide de VPC IPAM l'utilisateur Amazon.

6. (Facultatif) Pour ajouter une balise, choisissez Ajouter une nouvelle balise et entrez une clé de balise et une valeur de balise.

AWS CLI

Pour allouer une adresse IP Elastic

Utilisez la commande allocate-address de l' AWS CLI .

```
aws ec2 allocate-address
```

PowerShell

Pour allouer une adresse IP Elastic

Utilisez la New-EC2Address AWS Tools for Windows PowerShell commande.

```
New-EC2Address -Domain Vpc
```

Associer une adresse IP Elastic

Si vous associez une adresse IP Elastic à votre instance pour permettre la communication avec Internet, vous devez également vous assurer que votre instance se trouve dans un sous-réseau public. Pour plus d'informations, consultez Activer l'accès à Internet à l'aide d'une passerelle Internet dans le guide de VPC l'utilisateur Amazon.

Console

Pour associer une adresse IP Elastic à une instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Elastic IPs.
3. Sélectionnez l'adresse IP Elastic à associer, puis choisissez Actions, Associate Elastic IP address (Associer l'adresse IP Elastic).
4. Pour Resource type (Type de ressource), choisissez Instance.
5. Par exemple, choisissez l'instance à laquelle vous souhaitez associer l'adresse IP Elastic. Vous pouvez également entrer du texte pour rechercher une instance spécifique.
6. (Facultatif) Pour Private IP address (Adresse IP privée), spécifiez une adresse IP privée à laquelle associer l'adresse IP Elastic.
7. Choisissez Associate.

Pour associer une adresse IP Elastic à une interface réseau

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Elastic IPs.
3. Sélectionnez l'adresse IP Elastic à associer, puis choisissez Actions, Associate Elastic IP address (Associer l'adresse IP Elastic).
4. Pour Type de ressource, choisissez Interface réseau.
5. Dans Network interface (Interface réseau), choisissez l'interface réseau à laquelle associer l'adresse IP Elastic. Vous pouvez également entrer du texte pour rechercher une interface réseau spécifique.

6. (Facultatif) Pour Private IP address (Adresse IP privée), spécifiez une adresse IP privée à laquelle associer l'adresse IP Elastic.
7. Choisissez Associate.

AWS CLI

Pour associer une adresse IP Elastic

Utilisez la commande associate-address AWS CLI .

```
aws ec2 associate-address --instance-id i-0b263919b6498b123 --allocation-
id eipalloc-64d5890a
```

PowerShell

Pour associer une adresse IP Elastic

Utilisez la Register-EC2Address AWS Tools for Windows PowerShell commande.

```
Register-EC2Address -InstanceId i-0b263919b6498b123 -AllocationId eipalloc-64d5890a
```

Dissocier une adresse IP Elastic

Vous pouvez dissocier une adresse IP Elastic d'une instance ou d'une interface réseau à tout moment. Après avoir dissocié l'adresse IP Elastic, vous pouvez la réassocier à une autre ressource.

Console

Pour dissocier et réassocier une adresse IP Elastic

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Elastic IPs.
3. Sélectionnez l'adresse IP Elastic à dissocier, puis choisissez Actions, Disassociate Elastic IP address (Dissocier l'adresse IP Elastic).
4. Choisissez Dissocier.

AWS CLI

Dissocier une adresse IP Elastic

Utilisez la commande disassociate-address AWS CLI .

```
aws ec2 disassociate-address --association-id eipassoc-12345678
```

PowerShell

Dissocier une adresse IP Elastic

Utilisez la Unregister-EC2Address AWS Tools for Windows PowerShell commande.

```
Unregister-EC2Address -AssociationId eipassoc-12345678
```

Transférer une adresse IP élastique entre Comptes AWS

Vous pouvez transférer une adresse IP élastique de l'un Compte AWS à l'autre. Cela peut être utile dans les situations suivantes :

- Reprise après sinistre : remappez rapidement les adresses IP pour les charges de travail Internet destinées au public en cas d'urgence.
- Restructuration organisationnelle — Déplacez rapidement une charge de travail de l'un Compte AWS à l'autre. Un transfert d'adresse évite d'avoir à attendre que les nouvelles adresses IP élastiques soient autorisées par vos groupes de sécurité et votre réseauACLs.
- Administration centralisée de la sécurité : utilisez un compte AWS de sécurité centralisé pour suivre et transférer les adresses IP élastiques dont la conformité en matière de sécurité a été vérifiée.

Tarification

Le transfert d'adresses IP Elastic est gratuit.

Tâches

- Activation du transfert d'adresses IP Elastic
- Acceptation d'une adresse IP Elastic transférée
- Désactivation du transfert d'adresses IP Elastic

Activation du transfert d'adresses IP Elastic

Cette section décrit comment accepter une adresse IP Elastic transférée. Notez les limitations suivantes en ce qui concerne l'activation des adresses IP Elastic pour le transfert :

- Vous pouvez transférer les adresses IP Elastic de n'importe quel Compte AWS (compte source) vers n'importe quel autre AWS compte de la même AWS région (compte de transfert).
- Lorsque vous transférez une adresse IP Elastic, il existe une liaison en deux étapes entre les Comptes AWS. Lorsque le compte source lance le transfert, les comptes de transfert ont sept jours pour accepter le transfert de l'adresse IP Elastic. Pendant ces sept jours, le compte source peut consulter le transfert en attente (par exemple dans la AWS console ou à l'aide de la describe-address-transfers AWS CLI commande). Au bout de sept jours, le transfert expire et la propriété de l'adresse IP Elastic revient au compte source.
- Les transferts acceptés sont visibles sur le compte source (par exemple dans la AWS console ou à l'aide de la describe-address-transfers AWS CLI commande) pendant 14 jours après l'acceptation des transferts.
- AWS n'informe pas les comptes de transfert des demandes de transfert d'adresse IP Elastic en attente. Le propriétaire du compte source doit informer le propriétaire du compte de transfert qu'il doit accepter une demande de transfert d'adresse IP Elastic.
- Toutes les balises associées à une adresse IP Elastic en cours de transfert sont réinitialisées lorsque le transfert est terminé.
- Vous ne pouvez pas transférer les adresses IP élastiques allouées à partir de pools d'IPv4adresses publics que vous apportez à votre Compte AWS compte, communément appelés pools d'adresses Bring Your Own IP (BYOIP).
- Vous ne pouvez pas transférer les adresses IP élastiques allouées à partir d'un pool public contigu d'IPv4Amazon IP Address Manager IPAM () fourni par VPC Amazon. Vous IPAM permet plutôt de partager des IPAM pools entre AWS comptes en les intégrant IPAM à AWS Organizations et en utilisant AWS RAM. Pour plus d'informations, consultez la section Allocation d'adresses IP élastiques séquentielles à partir d'un IPAM pool dans le guide de VPC IPAM l'utilisateur Amazon.
- Si vous tentez de transférer une adresse IP élastique associée à un DNS enregistrement inversé, vous pouvez commencer le processus de transfert, mais le compte de transfert ne pourra pas accepter le transfert tant que l'DNSenregistrement associé ne sera pas supprimé.
- Si vous avez activé et configuré AWS Outposts, vous avez peut-être alloué des adresses IP élastiques à partir d'un pool d'adresses IP (CoIP) appartenant au client. Vous ne pouvez pas transférer des adresses IP Elastic attribuées à partir d'un groupe CoIP. Cependant, vous pouvez

l'utiliser AWS RAM pour partager une CoIP avec un autre compte. Pour plus d'informations, voir Adresses IP appartenant au client dans le Guide de l'utilisateur AWS Outposts .

- Vous pouvez utiliser Amazon VPC IPAM pour suivre le transfert d'adresses IP élastiques vers les comptes d'une organisation à partir de AWS Organizations. Pour plus d'informations, voir Afficher l'historique des adresses IP. Si une adresse IP Elastic est transférée à un Compte AWS tiers de l'organisation, l'historique IPAM d'audit de l'adresse IP Elastic est perdu.

Cette procédure doit être suivie par le compte source.

Console

Pour activer le transfert d'adresses IP Elastic

1. Assurez-vous d'utiliser le AWS compte source.
2. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
3. Dans le volet de navigation, sélectionnez Elastic IPs.
4. Sélectionnez une ou plusieurs adresses IP Elastic à activer pour le transfert, puis choisissez Actions, Enable transfer (Activer le transfert).
5. Si vous transférez plusieurs adresses IP Elastic, l'option Transfer type (Type de transfert) s'affiche. Choisissez l'une des options suivantes :
   - Choisissez Compte unique si vous transférez les adresses IP élastiques vers un seul AWS compte.
   - Choisissez Plusieurs comptes si vous transférez les adresses IP élastiques vers plusieurs AWS comptes.
6. Sous ID de compte IDs de transfert, entrez les AWS comptes vers lesquels vous souhaitez transférer les adresses IP élastiques.
7. Confirmez le transfert en saisissant **`enable`** dans la zone de texte.
8. Sélectionnez Envoyer.
9. Pour accepter le transfert, voir Acceptation d'une adresse IP Elastic transférée. Pour désactiver le transfert, voir Désactivation du transfert d'adresses IP Elastic.

AWS CLI

Pour activer le transfert d'adresses IP Elastic

Utilisez la enable-address-transfercommande.

```
aws ec2 enable-address-transfer \
    --allocation-id eipalloc-09ad461b0d03f6aaf \
    --transfer-account-id 123456789012
```

PowerShell

Pour activer le transfert d'adresses IP Elastic

Utilisez la Enable-EC2AddressTransfercommande.

```
Enable-EC2AddressTransfer -AllocationId eipalloc-09ad461b0d03f6aaf -
TransferAccountId 123456789012
```

Acceptation d'une adresse IP Elastic transférée

Cette section décrit comment accepter une adresse IP Elastic transférée.

Lorsque vous transférez une adresse IP Elastic, il existe une liaison en deux étapes entre les Comptes AWS. Lorsque le compte source lance le transfert, les comptes de transfert ont sept jours pour accepter le transfert de l'adresse IP Elastic. Pendant ces sept jours, le compte source peut consulter le transfert en attente (par exemple dans la AWS console ou à l'aide de la describe-address-transfers AWS CLI commande). Au bout de sept jours, le transfert expire et la propriété de l'adresse IP Elastic revient au compte source.

Lorsque vous acceptez des transferts, notez les exceptions suivantes qui peuvent se produire et comment les résoudre :

- AddressLimitExceeded: Si votre compte de transfert a dépassé le quota d'adresses IP Elastic, le compte source peut activer le transfert d'adresses IP Elastic, mais cette exception se produit lorsque le compte de transfert essaie d'accepter le transfert. Par défaut, tous les AWS comptes sont limités à 5 adresses IP élastiques par région. Voir Quota appliqué aux adresses IP Elastic pour les instructions relatives à l'augmentation de la limite.
- InvalidTransfer. AddressCustomPtrSet: Si vous ou un membre de votre organisation avez configuré l'adresse IP élastique que vous essayez de transférer pour utiliser la DNS recherche inversée, le compte source peut activer le transfert de l'adresse IP élastique, mais cette exception se produit lorsque le compte de transfert essaie d'accepter le transfert. Pour résoudre ce problème, le

compte source doit supprimer l'DNSenregistrement de l'adresse IP élastique. Pour de plus amples informations, veuillez consulter Création d'un DNS enregistrement inversé pour les e-mails sur Amazon EC2.

- InvalidTransfer. AddressAssociated: Si une adresse IP élastique est associée à une EC2 instance ENI OR, le compte source peut activer le transfert pour l'adresse IP élastique, mais cette exception se produit lorsque le compte de transfert essaie d'accepter le transfert. Pour résoudre ce problème, le compte source doit dissocier l'adresse IP Elastic. Pour de plus amples informations, veuillez consulter Dissocier une adresse IP Elastic.

Pour toute autre exception, contactez AWS Support.

Cette procédure doit être suivie par le compte de transfert.

Console

Pour accepter un transfert d'adresse IP Elastic

1. Assurez-vous d'utiliser le compte de transfert.
2. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
3. Dans le volet de navigation, sélectionnez Elastic IPs.
4. Choisissez Actions, puis Accept transfer (Accepter le transfert).
5. Aucune balise associée à l'adresse IP Elastic transférée n'est transférée avec l'adresse IP Elastic lorsque vous acceptez le transfert. Si vous souhaitez définir une balise Name (Nom) pour l'adresse IP Elastic que vous acceptez, sélectionnez Create a tag with a key of 'Name' and a value that you specify (Créer une balise avec la clé « Nom » et une valeur que vous spécifiez).
6. Saisissez l'adresse IP Elastic que vous voulez transférer.
7. Si vous acceptez plusieurs adresses IP Elastic transférées, choisissez Add address (Ajouter une adresse) pour saisir une adresse IP Elastic supplémentaire.
8. Sélectionnez Envoyer.

AWS CLI

Pour accepter un transfert d'adresse IP Elastic

Utilisez la accept-address-transfercommande.

```
aws ec2 accept-address-transfer --address 100.21.184.216
```

PowerShell

Pour accepter un transfert d'adresse IP Elastic

Utilisez la Approve-EC2AddressTransfercommande.

```
Approve-EC2AddressTransfer -Address 100.21.184.216
```

Désactivation du transfert d'adresses IP Elastic

Cette section décrit comment désactiver un transfert d'adresses IP Elastic après que le transfert ait été activé.

Ces étapes doivent être effectuées par le compte source qui a activé le transfert.

Console

Pour désactiver un transfert d'adresse IP Elastic

1. Assurez-vous d'utiliser la source Compte AWS.
2. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
3. Dans le volet de navigation, sélectionnez Elastic IPs.
4. Dans la liste des ressources d'ElasticIPs, assurez-vous que la propriété indiquant la colonne Transfer status est activée.
5. Sélectionnez une ou plusieurs adresses IP Elastic dont Transfer status (État du transfert) est Pending (En attente), puis choisissez Actions, Disable transfer (Désactiver le transfert).
6. Confirmez en saisissant **`disable`** dans la zone de texte.
7. Sélectionnez Envoyer.

AWS CLI

Pour désactiver le transfert d'adresses IP Elastic

Utilisez la disable-address-transfercommande.

```
aws ec2 disable-address-transfer --allocation-id eipalloc-09ad461b0d03f6aaf
```

PowerShell

Pour désactiver le transfert d'adresses IP Elastic

Utilisez la Disable-EC2AddressTransfercommande.

```
Disable-EC2AddressTransfer -AllocationId eipalloc-09ad461b0d03f6aaf
```

Libérer une adresse IP Elastic

Si vous n'avez plus besoin d'une adresse IP Elastic, nous vous recommandons de la libérer. L'adresse IP élastique à publier ne doit pas être actuellement associée à une AWS ressource.

Console

Libérer une adresse IP Elastic

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Elastic IPs.
3. Sélectionnez l'adresse IP Elastic à libérer, puis choisissez Actions, Release Elastic IP addresses (Libérer des adresses IP Elastic).
4. Choisissez Release (Libérer).

AWS CLI

Libérer une adresse IP Elastic

Utilisez la commande release-address AWS CLI .

```
aws ec2 release-address --allocation-id eipalloc-64d5890a
```

PowerShell

Libérer une adresse IP Elastic

Utilisez la Remove-EC2Address AWS Tools for Windows PowerShell commande.

```
Remove-EC2Address -AllocationId eipalloc-64d5890a
```

Une fois que vous aurez publié votre adresse IP Elastic, vous pourrez peut-être la récupérer. Les règles suivantes s'appliquent :

- Vous ne pouvez pas récupérer une adresse IP Elastic si elle a été attribuée à un autre AWS compte ou si cela vous amène à dépasser votre limite d'adresses IP Elastic.
- Vous ne pouvez pas récupérer les balises associées à une adresse IP élastique.

AWS CLI

Pour récupérer une adresse IP Elastic

Utilisez la AWS CLI commande allocate-address et spécifiez l'adresse IP à l'aide du `--address` paramètre comme suit.

```
aws ec2 allocate-address --domain vpc --address 203.0.113.3
```

PowerShell

Pour récupérer une adresse IP Elastic

Utilisez la New-EC2Address AWS Tools for Windows PowerShell commande et spécifiez l'adresse IP à l'aide du `-Address` paramètre comme suit.

```
New-EC2Address -Address 203.0.113.3 -Domain vpc -Region us-east-1
```

Création d'un DNS enregistrement inversé pour les e-mails sur Amazon EC2

Si vous avez l'intention d'envoyer des e-mails à des tiers depuis une EC2 instance, nous vous recommandons de fournir une ou plusieurs adresses IP élastiques et d'attribuer DNS des enregistrements inverses statiques aux adresses IP élastiques que vous utilisez pour envoyer des e-mails. Cela peut vous aider à éviter que votre e-mail soit marqué comme spam par certaines organisations antispam. AWS travaille avec ISPs des organisations antispam sur Internet afin de réduire le risque que les e-mails envoyés à partir de ces adresses soient marqués comme du spam.

Considérations

- Avant de créer un DNS enregistrement inversé, vous devez définir un DNS enregistrement direct correspondant (type d'enregistrement A) qui pointe vers votre adresse IP Elastic.
- Si un DNS enregistrement inversé est associé à une adresse IP élastique, l'adresse IP élastique est verrouillée sur votre compte et ne peut pas être supprimée de votre compte tant que l'enregistrement n'est pas supprimé.
- Si vous nous avez contacté AWS Support pour configurer l'inversion DNS pour une adresse IP élastique, vous pouvez supprimer l'inverseDNS, mais vous ne pouvez pas libérer l'adresse IP élastique car elle est verrouillée par AWS Support. Pour déverrouiller l'adresse IP élastique, contactez AWS Support. Une fois l'adresse IP Elastic déverrouillée, vous pouvez la libérer.
- [AWS GovCloud (US) Region] Vous ne pouvez pas créer d'DNSenregistrement inversé. AWS doit vous attribuer les DNS enregistrements inverses statiques. Ouvrez une demande pour supprimer les restrictions relatives à l'envoi inversé DNS et à l'envoi d'e-mails et pour nous fournir vos adresses IP élastiques et vos DNS enregistrements inversés.

Création d'un DNS enregistrement inversé

Vous pouvez créer un DNS enregistrement inversé pour votre adresse IP Elastic comme suit.

Console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Elastic IPs.
3. Sélectionnez l'adresse IP élastique et choisissez Actions, Mettre à jour en sens inverse DNS.
4. Pour Nom DNS de domaine inversé, entrez le nom de domaine.
5. Saisissez **`update`** pour confirmer.
6. Sélectionnez Mise à jour.

AWS CLI

Utilisez la modify-address-attributecommande dans le AWS CLI, comme indiqué dans l'exemple suivant.

```
aws ec2 modify-address-attribute --allocation-id eipalloc-abcdef01234567890  --
domain-name example.com
```

Voici un exemple de sortie

```
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.net.",
            "PtrRecordUpdate": {
                "Value": "example.com.",
                "Status": "PENDING"
        }
    ]
}
```

Supprimer un DNS enregistrement inversé

Vous pouvez supprimer un DNS enregistrement inversé de votre adresse IP Elastic comme suit.

Si le message d'erreur suivant s'affiche, vous pouvez envoyer une demande de suppression des restrictions relatives à l'envoi d'e-mails AWS Support pour obtenir de l'aide.

```
The address cannot be released because it is locked to your account.
```

Console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Elastic IPs.
3. Sélectionnez l'adresse IP élastique et choisissez Actions, Mettre à jour en sens inverse DNS.
4. Pour Nom DNS de domaine inversé, effacez le nom de domaine.
5. Saisissez **`update`** pour confirmer.
6. Sélectionnez Mise à jour.

AWS CLI

Utilisez la reset-address-attributecommande dans le AWS CLI, comme indiqué dans l'exemple suivant.

```
aws ec2 reset-address-attribute --allocation-id eipalloc-abcdef01234567890 --
attribute domain-name
```

Voici un exemple de sortie

```
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.com.",
            "PtrRecordUpdate": {
                "Value": "example.net.",
                "Status": "PENDING"
        }
    ]
}
```

Interfaces réseau Elastic

Une interface réseau élastique est un composant réseau logique VPC qui représente une carte réseau virtuelle. Vous pouvez créer et configurer des interfaces réseau et les associer à des instances que vous lancez dans la même zone de disponibilité. Les attributs d'une interface réseau la suivent lorsque celle-ci est attachée à une instance ou détachée d'une instance, puis rattachée à une autre instance. Lorsque vous déplacez une interface réseau d'une instance à une autre, le trafic réseau est redirigé de l'instance d'origine vers la nouvelle instance.

Notez que cette AWS ressource est appelée interface réseau dans le AWS Management Console et sur Amazon EC2API. Par conséquent, nous utilisons « interface réseau » dans cette documentation au lieu d'indiquer « interface réseau Elastic ». L'expression « interface réseau » dans cette documentation signifie toujours « interface réseau Elastic ».

Attributs de l'interface réseau

Une interface réseau peut inclure les attributs suivants :

- Une IPv4 adresse privée principale issue de la plage d'IPv4adresses de votre sous-réseau
- Une IPv6 adresse principale issue de la plage d'IPv6adresses de votre sous-réseau
- IPv4Adresses privées secondaires issues de la plage d'IPv4adresses de votre sous-réseau

- Une adresse IP élastique (IPv4) pour chaque IPv4 adresse privée
- Une IPv4 adresse publique
- IPv6Adresses secondaires
- Groupes de sécurité
- Une MAC adresse
- Un indicateur de vérification origine/destination
- Une description

Surveillance du trafic

Vous pouvez activer un journal de VPC flux sur votre interface réseau pour capturer des informations sur le trafic à destination et en provenance d'une interface réseau. Après avoir créé un journal de flux, vous pouvez consulter et récupérer ses données dans Amazon CloudWatch Logs. Pour plus d'informations, consultez VPCFlow Logs dans le guide de VPC l'utilisateur Amazon.

Table des matières

Concepts d'interface réseau

Les concepts suivants sont importants à comprendre lorsque vous commencez à utiliser les interfaces réseau.

Interface réseau principale

Chaque instance a une interface réseau par défaut, appelée l'interface réseau principale. Vous ne pouvez pas détacher une interface réseau principale d'une instance.

Interfaces réseau secondaires

Vous pouvez créer et associer des interfaces réseau secondaires à votre instance. Le nombre maximal d'interfaces réseau varie selon le type d'instance. Pour de plus amples informations, veuillez consulter Nombre maximum d'adresses IP par interface réseau.

IPv4adresses pour les interfaces réseau

Lorsque vous lancez une EC2 instance dans un sous-réseau IPv4 uniquement ou à double pile, l'instance reçoit une adresse IP privée principale provenant de la plage d'IPv4adresses du sous-réseau. Vous pouvez également spécifier des IPv4 adresses privées supplémentaires, appelées IPv4 adresses privées secondaires. Contrairement aux adresses IP privées principales, les adresses IP privées secondaires peuvent être réaffectées d'une instance à une autre.

IPv4Adresses publiques pour les interfaces réseau

Tous les sous-réseaux possèdent un attribut modifiable qui détermine si une adresse publique est attribuée aux interfaces réseau créées dans ce sous-réseau (et donc aux instances lancées dans ce sous-réseau). IPv4 Pour plus d'informations, consultez la section Paramètres des sous-réseaux dans le guide de VPC l'utilisateur Amazon. Lorsque vous lancez une instance, l'adresse IP est attribuée à l'interface réseau principale. Si vous spécifiez une interface réseau existante comme interface réseau principale lorsque vous lancez une instance, l'IPv4adresse publique est déterminée par cette interface réseau.

Lorsque vous créez une interface réseau, elle hérite de l'attribut d'IPv4adressage public du sous-réseau. Si vous modifiez ultérieurement l'attribut d'IPv4adressage public du sous-réseau, l'interface réseau conserve le paramètre en vigueur lors de sa création.

IPv6adresses pour les interfaces réseau

Si vous associez des IPv6 CIDR blocs à votre sous-réseau VPC and, vous pouvez attribuer IPv6 des adresses de la plage de sous-réseaux à une interface réseau. Chaque IPv6 adresse peut être attribuée à une interface réseau.

Tous les sous-réseaux ont un attribut modifiable qui détermine si les interfaces réseau créées dans ce sous-réseau (et donc les instances lancées dans ce sous-réseau) reçoivent automatiquement une IPv6 adresse provenant de la plage du sous-réseau. Lorsque vous lancez une instance, l'IPv6adresse est attribuée à l'interface réseau principale.

Adresses IP élastiques pour les interfaces réseau

Vous pouvez associer une adresse IP élastique à l'une des IPv4 adresses privées de l'interface réseau. Vous pouvez associer une adresse IP élastique à chaque IPv4 adresse privée. Si vous dissociez une adresse IP élastique d'une interface réseau, vous pouvez la libérer ou l'associer à une autre instance.

Comportement de résiliation

Vous pouvez définir le comportement de résiliation d'une interface réseau attachée à une instance. Vous pouvez spécifier si l'interface réseau doit être supprimée automatiquement lorsque vous résiliez l'instance à laquelle celle-ci est attachée.

Vérification origine/destination

Vous pouvez activer ou désactiver les vérifications origine/destination, qui garantissent que l'instance est la source ou la destination du trafic qu'elle reçoit. Les vérifications origine/destination sont activées par défaut. Vous devez désactiver les vérifications origine/destination si l'instance exécute des services tels que la traduction d'adresses réseau, le routage ou les pare-feu.

Interfaces réseau gérées par demandeur

Ces interfaces réseau sont créées et gérées par services AWS pour vous permettre d'utiliser certaines ressources et certains services. Vous ne pouvez pas gérer vous-même ces interfaces réseau. Pour de plus amples informations, veuillez consulter Interfaces réseau gérées par demandeur.

Délégation de préfixes

Un préfixe est une IPv6 CIDR plage privée IPv4 ou privée réservée que vous allouez pour une attribution automatique ou manuelle aux interfaces réseau associées à une instance. En utilisant les préfixes délégués, vous pouvez lancer des services plus rapidement en attribuant une plage d'adresses IP sous la forme d'un préfixe unique.

Cartes réseau

La plupart des types d'instances prennent en charge une seule carte réseau. Les types d'instance qui prennent en charge plusieurs cartes réseau offrent des performances réseau supérieures, notamment des capacités de bande passante supérieures à 100 Gbit/s et des performances de débit de paquets améliorées. Lorsque vous attachez une interface réseau à une instance qui prend en charge plusieurs cartes réseau, vous pouvez sélectionner la carte réseau pour l'interface réseau. L'interface réseau principale doit être affectée à l'index de carte réseau 0.

Si vous activez Elastic Fabric Adapter (EFA) lorsque vous lancez une instance qui prend en charge plusieurs cartes réseau, toutes les cartes réseau sont disponibles. Vous pouvez en attribuer un maximum EFA par carte réseau. Et EFA compte comme une interface réseau.

Les types d'instances suivants prennent en charge plusieurs cartes réseau.

Type d'instance	Nombre de cartes réseau
c6in.32xlarge	2
c6in.metal	2
dl1.24xlarge	4
g6e.24xlarge	2
g6e.48xlarge	4
hpc6id.32xlarge	2
hpc7a.12xlarge	2
hpc7a.24xlarge	2
hpc7a.48xlarge	2
hpc7a.96xlarge	2
m6idn.32xlarge	2
m6idn.metal	2
m6in.32xlarge	2
m6in.metal	2
p4d.24xlarge	4
p4de.24xlarge	4
p5.48xlarge	32

Type d'instance	Nombre de cartes réseau
r6idn.32xlarge	2
r6idn.metal	2
r6in.32xlarge	2
r6in.metal	2
trn1.32xlarge	8
trn1n.32xlarge	16
u7in-16tb.224xlarge	2
u7in-24tb.224xlarge	2
u7in-32tb.224xlarge	2

Nombre maximum d'adresses IP par interface réseau

Chaque type d'instance prend en charge un nombre maximum d'interfaces réseau, un nombre maximum d'IPv4adresses privées par interface réseau et un nombre maximum d'IPv6adresses par interface réseau. La limite d'IPv6adresses est distincte de la limite d'IPv4adresses privées par interface réseau. Tous les types d'instances ne sont pas compatibles avec l'IPv6adressage.

Interfaces réseau disponibles

Le guide des types d'EC2instances Amazon fournit des informations sur les interfaces réseau disponibles pour chaque type d'instance. Pour plus d'informations, consultez les ressources suivantes :

- Spécifications du réseau — Usage général
- Spécifications du réseau — Optimisé pour le calcul
- Spécifications du réseau — Mémoire optimisée
- Spécifications du réseau — Stockage optimisé
- Spécifications du réseau — Calcul accéléré

- Spécifications du réseau — Calcul à haute performance
- Spécifications du réseau — Génération précédente

Pour récupérer les informations d'interface réseau à l'aide du AWS CLI

Vous pouvez utiliser la describe-instance-types AWS CLI commande pour afficher des informations sur un type d'instance, telles que les interfaces réseau prises en charge et les adresses IP par interface. L'exemple suivant affiche ces informations pour toutes les instances C5.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=c5.*" \
    --query "InstanceTypes[].{ \
        Type: InstanceType, \
        MaxENI: NetworkInfo.MaximumNetworkInterfaces, \
        IPv4addr: NetworkInfo.Ipv4AddressesPerInterface}" \
    --output table
```

Voici un exemple de sortie.

```
-------------------------------------
|        DescribeInstanceTypes      |
+----------+----------+--------------+
| IPv4addr | MaxENI   |     Type     |
+----------+----------+--------------+
|  30      |  8       |  c5.4xlarge  |
|  50      |  15      |  c5.24xlarge |
|  15      |  4       |  c5.xlarge   |
|  30      |  8       |  c5.12xlarge |
|  10      |  3       |  c5.large    |
|  15      |  4       |  c5.2xlarge  |
|  50      |  15      |  c5.metal    |
|  30      |  8       |  c5.9xlarge  |
|  50      |  15      |  c5.18xlarge |
+----------+----------+--------------+
```

Pour récupérer les informations d'interface réseau à l'aide du AWS Tools for PowerShell

Vous pouvez utiliser la Get-EC2InstanceType PowerShell commande pour afficher des informations sur un type d'instance, telles que les interfaces réseau prises en charge et les adresses IP par interface. L'exemple suivant affiche ces informations pour toutes les instances C5.

```
Get-EC2InstanceType -Filter @{Name = "instance-type"; Values = "c5.*" } | `
Select-Object `
    @{Name = 'Ipv4AddressesPerInterface'; Expression =
 {($_.Networkinfo.Ipv4AddressesPerInterface)}},
    @{Name = 'MaximumNetworkInterfaces'; Expression =
 {($_.Networkinfo.MaximumNetworkInterfaces)}},
    InstanceType | `
Format-Table -AutoSize
```

Voici un exemple de sortie.

```
Ipv4AddressesPerInterface MaximumNetworkInterfaces InstanceType
------------------------- ------------------------ ------------
                       30                        8 c5.4xlarge
                       15                        4 c5.xlarge
                       30                        8 c5.12xlarge
                       50                       15 c5.24xlarge
                       30                        8 c5.9xlarge
                       50                       15 c5.metal
                       15                        4 c5.2xlarge
                       10                        3 c5.large
                       50                       15 c5.18xlarge
```

Créez une interface réseau pour votre EC2 instance

Vous pouvez créer une interface réseau à utiliser par vos EC2 instances. Lorsque vous créez une interface réseau, vous spécifiez le sous-réseau pour lequel elle est créée. Vous ne pouvez pas déplacer une interface réseau vers un autre sous-réseau une fois qu'elle a été créée. Vous devez attacher une interface réseau à une instance dans la même zone de disponibilité. Vous pouvez détacher une interface réseau secondaire d'une instance, puis l'associer à une autre instance. Vous ne pouvez pas détacher une interface réseau principale d'une instance. Pour de plus amples informations, veuillez consulter the section called “Pièces jointes à l'interface réseau”.

Pour créer une interface réseau à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Sélectionnez Create network interface (Créer une interface réseau).
4. Sous Description, saisissez un nom descriptif.

5. Pour Sous-réseau (subnet), sélectionnez un sous-réseau. Les options disponibles dans les étapes suivantes changent en fonction du type de sous-réseau que vous sélectionnez (IPv4-only, IPv6 -only ou dual-stack (IPv4et)). IPv6
6. Pour IPv4Adresse privée, effectuez l'une des opérations suivantes :
   - Choisissez Attribuer automatiquement pour permettre EC2 à Amazon de sélectionner une IPv4 adresse dans le sous-réseau.
   - Choisissez Personnalisé et entrez une IPv4 adresse que vous sélectionnez dans le sous-réseau.
7. (Sous-réseaux avec IPv6 adresses uniquement) Pour l'IPv6adresse, effectuez l'une des opérations suivantes :
   - Choisissez Aucune si vous ne souhaitez pas attribuer d'IPv6adresse à l'interface réseau.
   - Choisissez Attribuer automatiquement pour permettre EC2 à Amazon de sélectionner une IPv6 adresse dans le sous-réseau.
   - Choisissez Personnalisé et entrez une IPv6 adresse que vous sélectionnez dans le sous-réseau.
8. (Facultatif) Si vous créez une interface réseau dans un sous-réseau à double pile ou IPv6 uniquement, vous avez la possibilité d'attribuer une adresse IP principale. IPv6 Cela attribue une adresse monodiffusion IPv6 globale principale (GUA) à l'interface réseau. L'attribution d'une IPv6 adresse principale vous permet d'éviter de perturber le trafic vers les instances ou. ENIs Choisissez Enable si l'instance à laquelle elle ENI sera attachée repose sur le fait que son IPv6 adresse ne change pas. AWS attribuera automatiquement une IPv6 adresse associée à l'adresse ENI attachée à votre instance comme IPv6 adresse principale. Une fois que vous avez activé une IPv6 GUA adresse comme adresse principaleIPv6, vous ne pouvez pas la désactiver. Lorsque vous activez une IPv6 GUA adresse comme adresse principaleIPv6, la première IPv6 GUA devient l'IPv6adresse principale jusqu'à ce que l'instance soit résiliée ou que l'interface réseau soit détachée. Si plusieurs IPv6 adresses sont associées à une adresse ENI attachée à votre instance et que vous activez une IPv6 adresse principale, la première IPv6 GUA adresse associée ENI devient l'IPv6adresse principale.
9. (Facultatif) Pour créer un Elastic Fabric Adapter (EFA), sélectionnez Elastic Fabric Adapter (EFA), puis Enable (Activer).
10. (Facultatif) Sous Paramètres avancés, pour Délai de suivi d'inactivité de la connexion, modifiez les délais d'inactivité de la connexion par défaut. Pour plus d'informations sur ces options, consultez Délai de suivi d'inactivité de la connexion.

- TCPdélai établi : délai d'expiration (en secondes) pour les TCP connexions inactives dans un état établi. Min. : 60 secondes. Max. : 432 000 secondes (5 jours). Par défaut : 432 000 secondes. Recommandé : moins de 432 000 secondes.
- UDPdélai d'attente : délai d'expiration (en secondes) pour les UDP flux inactifs qui n'ont vu du trafic que dans une seule direction ou une seule transaction demande-réponse. Min. : 30 secondes. Max. : 60 secondes. Par défaut : 30 secondes.
- UDPdélai d'expiration du flux : délai d'expiration (en secondes) pour les UDP flux inactifs classés comme des flux ayant fait l'objet de plusieurs transactions requête-réponse. Min. : 60 secondes. Max. : 180 secondes (3 minutes). Par défaut : 180 secondes.

11. Pour Groupes de sécurité, sélectionnez un ou plusieurs groupes de sécurité.
12. (Facultatif) Pour chaque balise, sélectionnez Add new tag (Ajouter une nouvelle balise) et saisissez une clé de balise et une valeur de balise facultative.
13. Sélectionnez Create network interface (Créer une interface réseau).

Pour créer une interface réseau à l'aide de la ligne de commande

Utilisez l'une des commandes suivantes.

- create-network-interface (AWS CLI)
- New-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Pièces jointes d'interface réseau pour votre EC2 instance

Vous pouvez créer des interfaces réseau à utiliser par vos EC2 instances comme interfaces réseau principales ou secondaires. Vous devez associer une interface réseau à une EC2 instance située dans la même zone de disponibilité. Le type d'instance d'une instance détermine le nombre d'interfaces réseau que vous pouvez associer à l'instance. Pour de plus amples informations, veuillez consulter the section called "Adresses IP par interface réseau".

Considérations

- Vous pouvez attacher une interface réseau à une instance lorsqu'elle est en cours d'exécution (attachement de secours), arrêtée (attachement à chaud) ou en cours de lancement (attachement à froid).

- Vous pouvez détacher les interfaces réseau secondaires lorsque l'instance s'exécute ou est arrêtée. Toutefois, vous ne pouvez pas détacher l'interface réseau principale.
- Vous pouvez déplacer une interface réseau secondaire d'une instance à une autre, si les instances se trouvent dans la même zone de disponibilité VPC mais dans des sous-réseaux différents.
- Lorsque vous lancez une instance à l'aide de CLIAPI, ou unSDK, vous pouvez spécifier l'interface réseau principale et des interfaces réseau supplémentaires.
- Le lancement d'une instance Amazon Linux ou Windows Server avec plusieurs interfaces réseau configure automatiquement les interfaces, les IPv4 adresses privées et les tables de routage sur le système d'exploitation de l'instance.
- Une connexion à chaud ou à chaud à une interface réseau supplémentaire peut vous obliger à ouvrir manuellement la deuxième interface, à configurer l'IPv4adresse privée et à modifier la table de routage en conséquence. Les instances qui exécutent Amazon Linux ou Windows Server reconnaissent automatiquement l'attachement à chaud ou de secours et se configurent elles-mêmes.
- Vous ne pouvez pas associer une autre interface réseau à une instance (par exemple, une configuration NIC d'association) pour augmenter ou doubler la bande passante réseau depuis ou vers l'instance à double hébergement.
- Si vous attachez plusieurs interfaces réseau du même sous-réseau à une instance, vous pouvez être confronté à des problèmes de mise en réseau comme le routage asymétrique. Si possible, utilisez plutôt une IPv4 adresse privée secondaire sur l'interface réseau principale.
- Pour les EC2 instances d'un sous-réseau IPv6 réservé, si vous attachez une interface réseau secondaire, le DNS nom d'hôte privé de l'interface réseau secondaire est remplacé par l'IPv6adresse principale de l'interface réseau principale.
- Instances Windows : si vous utilisez plusieurs interfaces réseau, vous devez configurer les interfaces réseau pour utiliser le routage statique.

Joindre une interface réseau

Vous pouvez associer une interface réseau à n'importe quelle instance située dans la même zone de disponibilité que l'interface réseau, en utilisant la page Instances ou Interfaces réseau de la EC2 console Amazon. Vous pouvez également attacher des interfaces réseau existantes lorsque vous lancez des instances.

> **Note**
>
> Vous pouvez associer une interface réseau située dans une autre VPC (mais dans la même zone de disponibilité) à une instance à l'aide de la attach-network-interface AWS CLI commande. Vous ne pouvez pas le faire en utilisant le AWS Management Console.

Si l'IPv4adresse publique de votre instance est publiée, elle n'en reçoit pas de nouvelle si plusieurs interfaces réseau sont associées à l'instance. Pour plus d'informations sur le comportement des IPv4 adresses publiques, consultezIPv4Adresses publiques.

Instances page

Pour attacher une interface réseau à une instance à l'aide de la page Instances

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Cochez la case correspondant à l'instance.
4. Sélectionnez Actions, Mise en réseau, Attacher l'interface réseau.
5. Choisissez unVPC. Si vous associez une interface réseau secondaire à l'instance, celle-ci peut résider dans la même instance VPC que votre instance ou dans une autre VPC que vous possédez (à condition que l'interface réseau se trouve dans un sous-réseau situé dans la même zone de disponibilité que votre instance). Cela vous permet de créer des instances multihébergées VPCs avec différentes configurations réseau et de sécurité.
6. Sélectionnez une interface réseau. Si l'instance prend en charge plusieurs cartes réseau, vous pouvez choisir une carte réseau.
7. Choisissez Attacher.

Network Interfaces page

Pour attacher une interface réseau à une instance à l'aide de la page Interfaces réseau

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau.
4. Sélectionnez Actions, puis Attach (Attacher).

5. Choisissez un type d'instance. Si l'instance prend en charge plusieurs cartes réseau, vous pouvez choisir une carte réseau.
6. Choisissez Attacher.

Pour attacher une interface réseau à une instance à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- attach-network-interface (AWS CLI)
- Add-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Détacher une interface réseau

Vous pouvez détacher une interface réseau secondaire attachée à une EC2 instance à tout moment, en utilisant la page Instances ou Interfaces réseau de la EC2 console Amazon.

Si vous essayez de détacher une interface réseau attachée à une ressource d'un autre service, tel qu'un équilibreur de charge Elastic Load Balancing, une fonction Lambda, un ou une NAT passerelle WorkSpace, vous obtenez un message d'erreur indiquant que vous n'êtes pas autorisé à accéder à la ressource. Pour trouver quel service a créé la ressource attachée à une interface réseau, consultez la description de celle-ci. Si vous supprimez la ressource, son interface réseau est supprimée.

Instances page

Pour détacher une interface réseau d'une instance à l'aide de la page instances

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Cochez la case correspondant à l'instance. Consultez la section Network interfaces (Interfaces réseau) de l'onglet Networking (Mise en réseau) pour vérifier que l'interface réseau est attachée à une instance en tant qu'interface réseau secondaire.
4. Sélectionnez Actions, Mise en réseau, Détacher l'interface réseau.
5. Sélectionnez l'interface réseau, puis choisissez Détacher.

Network Interfaces page

Pour détacher une interface réseau d'une instance à l'aide de la page Interfaces réseau

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau. Consultez la section Instance details (Détails de l'instance) de la Details (Détails) pour vérifier que l'interface réseau est attachée à une instance en tant qu'interface réseau secondaire.
4. Sélectionnez Actions, Detach (Détacher).
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Detach.
6. Si vous ne parvenez pas à détacher l'interface réseau de l'instance, choisissez Force detachment (Forcer le détachement), Enable (Activer), puis réessayez. Nous recommandons de ne forcer le détachement qu'en dernier recours. Forcer un détachement peut vous empêcher d'attacher une interface réseau différente sur le même index jusqu'à ce que vous redémarriez l'instance. Cela peut également empêcher les métadonnées de l'instance de refléter que l'interface réseau a été détachée jusqu'à ce que vous redémarriez l'instance.

Pour détacher une interface réseau à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- detach-network-interface (AWS CLI)
- Dismount-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Gérez les adresses IP de votre interface réseau

Vous pouvez gérer les adresses IP suivantes pour vos interfaces réseau :

- Adresses IP élastiques (une par IPv4 adresse privée)
- IPv4adresses
- IPv6adresses

Pour gérer les adresses IP Elastic d'une interface réseau à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau.
4. Pour associer une adresse IP Elastic, procédez comme suit :
    a. Sélectionnez Actions, Associate Address (Associer une adresse).
    b. Sous Elastic IP address (Adresse IP Elastic), sélectionnez l'adresse IP Elastic.
    c. Pour IPv4Adresse privée, sélectionnez l'IPv4adresse privée à associer à l'adresse IP élastique.
    d. (Facultatif) Sélectionnez Allow the Elastic IP address to be reassociated (Autoriser la réassociation de l'adresse IP Elastic) si l'interface réseau est actuellement associée à une autre instance ou interface réseau.
    e. Choisissez Associate.
5. Pour dissocier une adresse IP Elastic, procédez comme suit :
    a. Choisissez Actions, Disassociate address.
    b. Sous Public IP address (Adresse IP publique), sélectionnez l'adresse IP Elastic.
    c. Choisissez Dissocier.

Pour gérer les IPv6 adresses IPv4 et d'une interface réseau à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Sélectionnez l'interface réseau.
4. Sélectionnez Actions, Manage IP addresses (Gérer les adresses IP).
5. Sélectionnez l'interface réseau.
6. Pour les IPv4adresses, modifiez les adresses IP selon vos besoins. Pour attribuer une IPv4 adresse, choisissez Attribuer une nouvelle adresse IP, puis spécifiez une IPv4 adresse dans la plage de sous-réseaux ou AWS laissez-en une pour vous. Pour annuler l'attribution d'une IPv4 adresse, choisissez Annuler l'attribution à côté de l'adresse.
7. Pour attribuer ou annuler l'attribution d'une IPv4 adresse publique à une interface réseau, choisissez Attribuer automatiquement une adresse IP publique. Cette option peut être activée ou

désactivée pour n'importe quelle interface réseau, mais elle ne s'applique qu'à l'interface réseau principale (eth0).

8. Pour les IPv6adresses, modifiez les adresses IP selon vos besoins. Pour attribuer une IPv6 adresse, choisissez Attribuer une nouvelle adresse IP, puis spécifiez une IPv6 adresse dans la plage de sous-réseaux ou AWS laissez-en une pour vous. Pour annuler l'attribution d'une IPv6 adresse, choisissez Annuler l'attribution à côté de l'adresse.
9. (Facultatif) Si vous modifiez une interface réseau dans un sous-réseau à double pile ou IPv6 uniquement, vous avez la possibilité d'attribuer une adresse IP principale. IPv6 L'attribution d'une IPv6 adresse principale vous permet d'éviter de perturber le trafic vers les instances ou. ENIs Choisissez Enable si l'instance à laquelle elle ENI sera attachée repose sur le fait que son IPv6 adresse ne change pas. AWS attribuera automatiquement une IPv6 adresse associée à l'adresse ENI attachée à votre instance comme IPv6 adresse principale. Une fois que vous avez activé une IPv6 GUA adresse comme adresse principaleIPv6, vous ne pouvez pas la désactiver. Lorsque vous activez une IPv6 GUA adresse comme adresse principaleIPv6, la première IPv6 GUA devient l'IPv6adresse principale jusqu'à ce que l'instance soit résiliée ou que l'interface réseau soit détachée. Si plusieurs IPv6 adresses sont associées à une adresse ENI attachée à votre instance et que vous activez une IPv6 adresse principale, la première IPv6 GUA adresse associée ENI devient l'IPv6adresse principale.
10. Choisissez Save (Enregistrer).

Pour gérer les adresses IP d'une interface réseau à l'aide du AWS CLI

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez Accédez à Amazon EC2.

- assign-ipv6-addresses
- associate-address
- disassociate-address
- unassign-ipv6-addresses

Pour gérer les adresses IP d'une interface réseau à l'aide des outils pour Windows PowerShell

Vous pouvez utiliser l'une des commandes suivantes.

- Register-EC2Address
- Register-EC2Ipv6 AddressList

- Unregister-EC2Address
- Unregister-EC2Ipv6 AddressList

Modifier les attributs d'interface réseau

Vous pouvez modifier les attributs d'interface réseau suivants :

- Description
- Groupes de sécurité
- Supprimer à la résiliation
- Vérification origine/destination

Pour changer la description d'une interface réseau à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau.
4. Sélectionnez Actions, Change description (Modifier la description).
5. Dans Description, saisissez une description de l'interface réseau.
6. Choisissez Enregistrer.

Pour changer les groupes de sécurité d'une interface réseau à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau.
4. Sélectionnez Actions, Change security groups (Modifier les groupes de sécurité).
5. Pour Change Security Groups (Modifier les groupes de sécurité), sélectionnez les groupes de sécurité à utiliser, puis sélectionnez Save (Enregistrer).

   Le groupe de sécurité et l'interface réseau doivent être créés à cet effetVPC. Pour modifier le groupe de sécurité pour les interfaces appartenant à d'autres services, par exemple Elastic Load Balancing, faites-le via ce service.

Pour modifier le comportement de résiliation d'une interface réseau à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau.
4. Sélectionnez Actions, Change termination behavior (Modifier le comportement de résiliation).
5. Sélectionner ou désactiver Delete on termination (Supprimer à la résiliation), Enable (Activer) au besoin, puis sélectionnez Save (Enregistrer).

Pour changer la vérification origine/destination d'une interface réseau à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau.
4. Sélectionnez Actions, Change source/dest check (Modifier la vérification source/dest).
5. Sélectionnez ou désactivez Source/destination check (Vérification origine/destination), Enable (Activer) au besoin, puis sélectionnez Save (Enregistrer).

Pour modifier les délais de suivi d'inactivité de la connexion :

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau.
4. Choisissez Actions, Modifier le délai de la connexion.
5. Modifiez les délais de suivi d'inactivité de la connexion. Pour plus d'informations sur ces options, consultez Délai de suivi d'inactivité de la connexion.

   - TCPdélai établi : délai d'expiration (en secondes) pour les TCP connexions inactives dans un état établi. Min. : 60 secondes. Max. : 432 000 secondes (5 jours). Par défaut : 432 000 secondes. Recommandé : moins de 432 000 secondes.
   - UDPdélai d'attente : délai d'expiration (en secondes) pour les UDP flux inactifs qui n'ont vu du trafic que dans une seule direction ou une seule transaction demande-réponse. Min. : 30 secondes. Max. : 60 secondes. Par défaut : 30 secondes.

- UDPdélai d'expiration du flux : délai d'expiration (en secondes) pour les UDP flux inactifs classés comme des flux ayant fait l'objet de plusieurs transactions requête-réponse. Min. : 60 secondes. Max. : 180 secondes (3 minutes). Par défaut : 180 secondes.

6. Choisissez Save (Enregistrer).

Pour modifier les attributs d'interface réseau à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- modify-network-interface-attribute (AWS CLI)
- Edit-EC2NetworkInterfaceAttribute (AWS Tools for Windows PowerShell)

Plusieurs interfaces réseau pour vos EC2 instances Amazon

L'association de plusieurs interfaces réseau à une instance est utile lorsque vous avez besoin des éléments suivants :

- Un réseau de gestion.
- Appareils de réseau et de sécurité.
- Instances à double hébergement avec des charges de travail dans différents sous-réseaux ou. VPCs
- Une solution à faible budget et à haute disponibilité.

Réseau de gestion

La présentation suivante décrit un réseau de gestion créé à l'aide de plusieurs interfaces réseau.

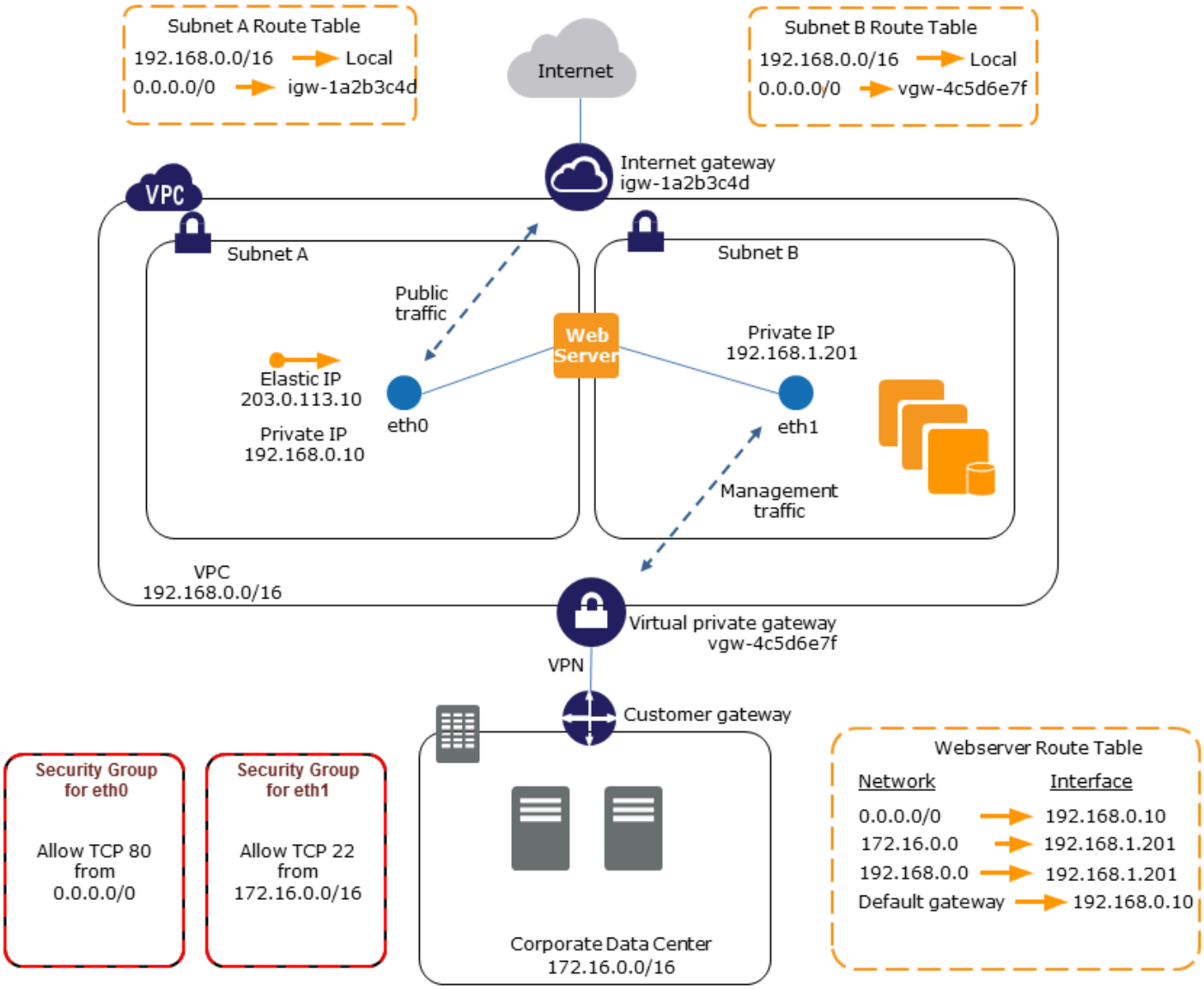
Critères

- L'interface réseau principale de l'instance (eth0) gère le trafic public.
- L'interface réseau secondaire de l'instance (eth1) gère le trafic de gestion du backend. Elle est connectée à un sous-réseau distinct qui dispose de contrôles d'accès plus restrictifs et se trouve dans la même zone de disponibilité (AZ) que l'interface réseau principale.

Paramètres

- L'interface réseau principale, qui peut ou non se trouver derrière un équilibreur de charge, a un groupe de sécurité associé qui autorise l'accès au serveur à partir d'Internet. Par exemple, autorisez les TCP ports 80 et 443 à partir de 0.0.0.0/0 ou à partir de l'équilibreur de charge.
- L'interface réseau secondaire est associée à un groupe de sécurité qui autorise uniquement l'SSHaccès, depuis l'un des emplacements suivants :
  - Plage d'adresses IP autorisée, que ce soit sur VPC Internet ou depuis Internet.
  - Sous-réseau privé au sein de la même zone de disponibilité que l'interface réseau principale.
  - Passerelle privée virtuelle.

> **Note**
>
> Pour garantir les fonctionnalités de basculement, envisagez d'utiliser un serveur privé secondaire IPv4 pour le trafic entrant sur une interface réseau. En cas de défaillance d'une instance, vous pouvez déplacer l'interface et/ou l'IPv4adresse privée secondaire vers une instance de secours.



Appareils de réseau et de sécurité

Certaines appliances réseau et de sécurité, telles que les équilibreurs de charge, les serveurs de traduction d'adresses réseau (NAT) et les serveurs proxy, préfèrent être configurées avec plusieurs interfaces réseau. Vous pouvez créer et attacher des interfaces réseau secondaires à des instances qui exécutent ces types d'applications, et configurer les interfaces supplémentaires avec leurs propres adresses IP publiques et privées, groupes de sécurité et vérification origine/destination.

Instances à double hébergement avec des charges de travail dans différents sous-réseaux

Vous pouvez placer une interface réseau sur chacun de vos serveurs web qui se connecte à un réseau de niveau intermédiaire où réside un serveur d'applications. Le serveur d'applications peut également avoir deux interfaces réseau sur le réseau backend (sous-réseau) où réside le serveur de base de données. Au lieu d'acheminer des paquets réseau via les instances à deux interfaces réseau, chaque instance à deux interfaces réseau reçoit et traite les demandes sur le serveur frontal, établit une connexion au serveur backend, puis envoie les demandes aux serveurs se trouvant sur le réseau backend.

Instances à double hébergement avec des charges de travail différentes VPCs dans le même compte

Vous pouvez lancer une EC2 instance dans l'une d'entre elles VPC et y associer une instance secondaire ENI provenant d'une autre VPC (mais dans la même zone de disponibilité). Cela vous permet de créer des instances multihébergées VPCs avec différentes configurations réseau et de sécurité. Vous ne pouvez pas créer d'instances multihébergées sur VPCs différents comptes. AWS

Vous pouvez utiliser des instances à double hébergement VPCs dans les cas d'utilisation suivants :

- Éliminez les CIDR chevauchements entre deux VPCs plages qui ne peuvent pas être comparées : vous pouvez tirer parti d'un secondaire CIDR dans un VPC et permettre à une instance de communiquer entre deux plages d'adresses IP qui ne se chevauchent pas.
- Connectez plusieurs ressources VPCs au sein d'un même compte : activez la communication entre des ressources individuelles qui seraient normalement séparées par VPC des limites.

Solution à faible budget et à haute disponibilité

Si l'une de vos instances remplissant une fonction particulière subit une défaillance, son Network Interface peut être attachée à une instance de remplacement ou de hot standby préconfigurée pour le même rôle afin de récupérer rapidement le service. Par exemple, vous pouvez utiliser une interface réseau comme interface réseau principale ou secondaire pour un service essentiel tel qu'une instance de base de données ou une NAT instance. Si une instance subit une défaillance, vous (ou, plus probablement, le code s'exécutant pour votre compte) pouvez attacher l'interface réseau à une instance de secours à chaud. Comme l'interface conserve ses adresses IP privées, ses adresses IP élastiques et son MAC adresse, le trafic réseau commence à circuler vers l'instance de secours

dès que vous attachez l'interface réseau à l'instance de remplacement. Les utilisateurs subissent une brève perte de connectivité entre le moment où l'instance tombe en panne et le moment où l'interface réseau est attachée à l'instance de secours, mais aucune modification de la table de routage ou de votre DNS serveur n'est requise.

Interfaces réseau gérées par demandeur

Une interface réseau gérée par le demandeur est une interface réseau service AWS créée en votre VPC nom. L'interface réseau est associée à une ressource pour un autre service, tel qu'une instance de base de données d'AmazonRDS, une NAT passerelle ou un point de VPC terminaison d'interface provenant de AWS PrivateLink.

Considérations

- Vous pouvez afficher les interfaces réseau gérées par demandeur dans votre compte. Vous pouvez ajouter ou supprimer des balises, mais vous ne pouvez pas modifier d'autres propriétés d'une interface réseau gérée par le demandeur.
- Vous ne pouvez pas détacher une interface réseau gérée par le demandeur.
- Lorsque vous supprimez la ressource associée à une interface réseau gérée par le demandeur, l'interface réseau service AWS est détachée et supprimée. Si le service a détaché une interface réseau, mais ne l'a pas supprimée, vous pouvez supprimer l'interface réseau détachée.

Console

Pour afficher les interfaces réseau gérées par demandeur à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Network & Security (Réseau et sécurité); Network Interfaces (Interfaces réseau).
3. Sélectionnez l'ID de l'interface réseau pour ouvrir sa page de détails.
4. Les principaux champs que vous pouvez utiliser pour déterminer l'objectif de l'interface réseau sont les suivants :
   - Description: description fournie par le service AWS ayant créé l'interface. Par exemple, « VPC Endpoint Interface vpce 089f2123488812123 ».
   - Géré par le demandeur : indique si l'interface réseau est gérée par. AWS

- ID du demandeur : alias ou identifiant de AWS compte du principal ou du service qui a créé l'interface réseau. Si vous avez créé l'interface réseau, il s'agit de votre Compte AWS identifiant. Sinon, un autre principal ou service l'a créé.

AWS CLI

Pour afficher les interfaces réseau gérées par les demandeurs à l'aide du AWS CLI

Utilisez la commande describe-network-interfaces comme suit.

```
aws ec2 describe-network-interfaces --filters Name=requester-managed,Values=true
```

Voici un exemple de sortie montrant les principaux champs que vous pouvez utiliser pour déterminer l'objectif de l'interface réseau : `Description` et `InterfaceType`.

```
{
     ...
    "Description": "VPC Endpoint Interface vpce-089f2123488812123",
    ...
    "InterfaceType": "vpc_endpoint",
    ...
    "NetworkInterfaceId": "eni-0d11e3ccd2c0e6c57",
    ...
    "RequesterId": "727180483921",
    "RequesterManaged": true,
    ...
}
```

PowerShell

Pour afficher les interfaces réseau gérées par les demandeurs à l'aide des Outils pour Windows PowerShell

Utilisez l'Get-EC2NetworkInterfaceapplet de commande comme suit.

```
Get-EC2NetworkInterface -Filter @{ Name="requester-managed"; Values="true" }
```

Voici un exemple de sortie montrant les principaux champs que vous pouvez utiliser pour déterminer l'objectif de l'interface réseau : `Description` et `InterfaceType`.

```
Description        : VPC Endpoint Interface vpce-089f2123488812123
```

```
...
InterfaceType      : vpc_endpoint
...
NetworkInterfaceId : eni-0d11e3ccd2c0e6c57
...
RequesterId        : 727180483921
RequesterManaged   : True
...
```

Délégation de préfixes pour les interfaces EC2 réseau Amazon

Vous pouvez attribuer une valeur privée IPv4 ou une IPv6 CIDR plage, automatiquement ou manuellement, à vos interfaces réseau. En attribuant des préfixes, vous mettez à l'échelle et simplifiez la gestion des applications, y compris les applications de conteneur et de réseau qui nécessitent plusieurs adresses IP sur une instance. Pour plus d'informations sur les IPv6 adresses IPv4 et les adresses, consultezAdressage IP de l'EC2instance Amazon.

Les options suivantes sont disponibles :

- Affectation automatique : AWS choisit le préfixe dans celui de votre VPC sous-réseau IPv4 ou IPv6 CIDR bloc et l'affecte à votre interface réseau.
- Affectation manuelle : vous spécifiez le préfixe à partir de votre VPC sous-réseau IPv4 ou de votre IPv6 CIDR bloc, et AWS vous vérifiez qu'il n'est pas déjà attribué à d'autres ressources avant de l'attribuer à votre interface réseau.

L'attribution de préfixes présente les avantages suivants :

- Augmentation du nombre d'adresses IP sur une interface réseau : lorsque vous utilisez un préfixe, vous attribuez un bloc d'adresses IP par opposition à des adresses IP individuelles. Cela accroît le nombre d'adresses IP d'une interface réseau.
- VPCGestion simplifiée des conteneurs : dans les applications de conteneurs, chaque conteneur nécessite une adresse IP unique. L'attribution de préfixes à votre instance simplifie la gestion de votre instanceVPCs, car vous pouvez lancer et arrêter des conteneurs sans avoir à appeler Amazon EC2 APIs pour des attributions d'adresses IP individuelles.

Table des matières

- Considérations
- Gérez les préfixes de vos interfaces réseau

Principes de base

- Vous pouvez attribuer un préfixe à des interfaces réseau nouvelles ou existantes.
- Pour utiliser des préfixes, vous devez attribuer un préfixe à votre interface réseau, puis attacher l'interface réseau à votre instance, puis configurer votre système d'exploitation.
- Lorsque vous choisissez de spécifier un préfixe, celui-ci doit répondre aux critères suivants :
  - Le IPv4 préfixe que vous pouvez spécifier est `/28`.
  - Le IPv6 préfixe que vous pouvez spécifier est `/80`.
  - Le préfixe se trouve dans le sous-réseau CIDR de l'interface réseau et ne se chevauche pas avec d'autres préfixes ou adresses IP attribués aux ressources existantes du sous-réseau.
- Vous pouvez attribuer un préfixe à l'interface réseau principale ou secondaire.
- Vous pouvez attribuer une adresse IP Elastic à une interface réseau à laquelle un préfixe est attribué.
- Vous pouvez également attribuer une adresse IP Elastic à la partie adresse IP du préfixe attribué.
- Nous convertissons le nom d'DNShôte privé d'une instance en IPv4 adresse privée principale.
- Nous attribuons à chaque IPv4 adresse privée une interface réseau, y compris celles provenant de préfixes, en utilisant le format suivant :
  - Région `us-east-1`

    ```
    ip-private-ipv4-address.ec2.internal
    ```

  - Toutes les autres régions

    ```
    ip-private-ipv4-address.region.compute.internal
    ```

Considérations

Prenez en considération les points suivants lorsque vous utilisez des préfixes :

- Les interfaces réseau avec préfixes sont prises en charge avec les instances créées sur le système AWS Nitro.

- Les préfixes des interfaces réseau sont limités aux IPv6 adresses et aux IPv4 adresses privées.
- Le nombre maximal d'adresses IP que vous pouvez attribuer à une interface réseau dépend du type d'instance. Chaque préfixe que vous attribuez à une interface réseau est considéré comme une adresse IP unique. Par exemple, le nombre d'`10`IPv4adresses d'une `c5.large` instance est limité par interface réseau. Chaque interface réseau de cette instance possède une IPv4 adresse principale. Si une interface réseau ne possède aucune IPv4 adresse secondaire, vous pouvez attribuer jusqu'à 9 préfixes à l'interface réseau. Pour chaque IPv4 adresse supplémentaire que vous attribuez à une interface réseau, vous pouvez attribuer un préfixe de moins à l'interface réseau. Pour de plus amples informations, veuillez consulter Nombre maximum d'adresses IP par interface réseau.
- Les préfixes sont inclus dans les vérifications origine/destination.
- Vous devez configurer votre système d'exploitation pour qu'il fonctionne avec des interfaces réseau avec des préfixes, des interfaces avec des préfixes. Notez ce qui suit :
  - Certains Amazon Linux AMIs contiennent des scripts supplémentaires installés par AWS, appelés`ec2-net-utils`. Ces scripts automatisent le cas échéant la configuration de vos interfaces réseau. Ils sont destinés à être utilisés uniquement sur Amazon Linux.
  - Pour les conteneurs, vous pouvez utiliser une interface réseau de conteneurs (CNI) pour le plug-in Kubernetes ou `dockerd` utiliser Docker pour gérer vos conteneurs.

Gérez les préfixes de vos interfaces réseau

Vous pouvez gérer les préfixes avec vos interfaces réseau comme suit.

Tâches

- Attribuer des préfixes pendant la création de l'interface réseau
- Attribuer des préfixes à une interface réseau existante
- Supprimer les préfixes de vos interfaces réseau

Attribuer des préfixes pendant la création de l'interface réseau

Vous pouvez attribuer des préfixes automatiques ou personnalisés lorsque vous créez une interface réseau.

Console

Pour affecter des préfixes automatiques lors de la création de l'interface réseau

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Sélectionnez Create network interface (Créer une interface réseau).
4. Entrez une description de l'interface réseau, sélectionnez le sous-réseau dans lequel créer l'interface réseau et configurez le privé IPv4 et les IPv6 adresses.
5. Développez Advanced settings (Paramètres avancés).
6. Pour la délégation de IPv4 préfixes, effectuez l'une des opérations suivantes :
   - Pour attribuer automatiquement un IPv4 préfixe, choisissez Attribuer automatiquement. Dans Nombre de IPv4 préfixes, entrez le nombre de préfixes à attribuer.
   - Pour attribuer un IPv4 préfixe spécifique, choisissez Personnalisé. Choisissez Ajouter un nouveau préfixe et entrez le préfixe.
7. Pour la délégation de IPv4 préfixes, effectuez l'une des opérations suivantes :
   - Pour attribuer automatiquement un IPv6 préfixe, choisissez Attribuer automatiquement. Dans Nombre de IPv6 préfixes, entrez le nombre de préfixes à attribuer.
   - Pour attribuer un IPv6 préfixe spécifique, choisissez Personnalisé. Choisissez Ajouter un nouveau préfixe et entrez le préfixe.

   > **Note**
   >
   > IPv6la délégation de préfixe n'apparaît que si le sous-réseau sélectionné est activé pour. IPv6

8. Sélectionnez les groupes de sécurité à associer à l'interface réseau et attribuez des balises de ressources si nécessaire.
9. Sélectionnez Create network interface (Créer une interface réseau).

AWS CLI

Pour attribuer des IPv4 préfixes automatiques lors de la création de l'interface réseau

Utilisez la create-network-interfacecommande et définissez `--ipv4-prefix-count` le nombre de préfixes que vous souhaitez AWS attribuer. Dans l'exemple suivant, AWS attribue un préfixe.

```
$ C:\> aws ec2 create-network-interface \
--subnet-id subnet-047cfed18eEXAMPLE \
--description "IPv4 automatic example" \
--ipv4-prefix-count 1
```

Pour attribuer des IPv4 préfixes spécifiques lors de la création de l'interface réseau

Utilisez la create-network-interfacecommande et définissez `--ipv4-prefixes` les préfixes. AWS sélectionne les adresses IP dans cette plage. Dans l'exemple suivant, le préfixe CIDR est`10.0.0.208/28`.

```
$ C:\> aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv4 manual example" \
    --ipv4-prefixes Ipv4Prefix=10.0.0.208/28
```

Pour attribuer des IPv6 préfixes automatiques lors de la création de l'interface réseau

Utilisez la create-network-interfacecommande et définissez `--ipv6-prefix-count` le nombre de préfixes que vous souhaitez AWS attribuer. Dans l'exemple suivant, AWS attribue un préfixe.

```
$ C:\> aws ec2 create-network-interface \
--subnet-id subnet-047cfed18eEXAMPLE \
--description "IPv6 automatic example" \
--ipv6-prefix-count 1
```

Pour attribuer des IPv6 préfixes spécifiques lors de la création de l'interface réseau

Utilisez la create-network-interfacecommande et définissez `--ipv6-prefixes` les préfixes. AWS sélectionne les adresses IP dans cette plage. Dans l'exemple suivant, le préfixe CIDR est`2600:1f13:fc2:a700:1768::/80`.

```
$ C:\> aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv6 manual example" \
    --ipv6-prefixes Ipv6Prefix=2600:1f13:fc2:a700:1768::/80
```

Attribuer des préfixes à une interface réseau existante

Vous pouvez attribuer des préfixes automatiques ou personnalisés à une interface réseau existante.

Console

Pour attribuer des préfixes automatiques à une interface réseau existante

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).
3. Sélectionnez l'interface réseau à laquelle attribuer les préfixes, puis Actions, Manage prefixes (Gérer les préfixes).
4. Pour la délégation de IPv4 préfixes, effectuez l'une des opérations suivantes :
   - Pour attribuer automatiquement un IPv4 préfixe, choisissez Attribuer automatiquement. Dans Nombre de IPv4 préfixes, entrez le nombre de préfixes à attribuer.
   - Pour attribuer un IPv4 préfixe spécifique, choisissez Personnalisé. Choisissez Ajouter un nouveau préfixe et entrez le préfixe.
5. Pour la délégation de IPv6 préfixes, effectuez l'une des opérations suivantes :
   - Pour attribuer automatiquement un IPv6 préfixe, choisissez Attribuer automatiquement. Dans Nombre de IPv6 préfixes, entrez le nombre de préfixes à attribuer.
   - Pour attribuer un IPv6 préfixe spécifique, choisissez Personnalisé. Choisissez Ajouter un nouveau préfixe et entrez le préfixe.

   > **Note**
   >
   > IPv6la délégation de préfixe n'apparaît que si le sous-réseau sélectionné est activé pour. IPv6
6. Choisissez Save (Enregistrer).

AWS CLI

Vous pouvez utiliser la commande assign-ipv6-addresses pour attribuer des IPv6 préfixes et la commande pour attribuer des préfixes aux assign-private-ip-addressesinterfaces réseau existantes. IPv4

Pour attribuer des IPv4 préfixes automatiques à une interface réseau existante

Utilisez la assign-private-ip-addressescommande et définissez `--ipv4-prefix-count` le nombre de préfixes que vous souhaitez AWS attribuer. Dans l'exemple suivant, AWS attribue un IPv4 préfixe.

```
aws ec2 assign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefix-count 1
```

Pour attribuer des IPv4 préfixes spécifiques à une interface réseau existante

Utilisez la assign-private-ip-addressescommande et définissez `--ipv4-prefixes` le préfixe. AWS sélectionne IPv4 des adresses dans cette plage. Dans l'exemple suivant, le préfixe CIDR est`10.0.0.208/28`.

```
aws ec2 assign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefixes 10.0.0.208/28
```

Pour attribuer des IPv6 préfixes automatiques à une interface réseau existante

Utilisez la commande assign-ipv6-addresses et définissez le nombre `--ipv6-prefix-count` de préfixes que vous souhaitez attribuer. AWS Dans l'exemple suivant, AWS attribue un IPv6 préfixe.

```
aws ec2 assign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefix-count 1
```

Pour attribuer des IPv6 préfixes spécifiques à une interface réseau existante

Utilisez la commande assign-ipv6-addresses et définissez le préfixe. `--ipv6-prefixes` AWS sélectionne IPv6 des adresses dans cette plage. Dans l'exemple suivant, le préfixe CIDR est`2600:1f13:fc2:a700:18bb::/80`.

```
aws ec2 assign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefixes 2600:1f13:fc2:a700:18bb::/80
```

Supprimer les préfixes de vos interfaces réseau

Vous pouvez supprimer des préfixes d'une interface réseau existante.

Console

Pour supprimer les préfixes d'une interface réseau

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Sélectionnez l'interface réseau.
4. Choisissez Actions, Gérer les préfixes.
5. Pour la délégation de IPv4 préfixes, pour supprimer des préfixes spécifiques, choisissez Annuler l'attribution à côté des préfixes à supprimer. Pour supprimer tous les préfixes, choisissez Ne pas attribuer.
6. Pour la délégation de IPv6 préfixes, pour supprimer des préfixes spécifiques, choisissez Annuler l'attribution à côté des préfixes à supprimer. Pour supprimer tous les préfixes, choisissez Ne pas attribuer.

> **Note**
>
> IPv6la délégation de préfixe n'apparaît que si le sous-réseau sélectionné est activé pour. IPv6

7. Choisissez Save (Enregistrer).

AWS CLI

Vous pouvez utiliser la commande unassign-ipv6-addresses pour supprimer des IPv6 préfixes et les unassign-private-ip-addressescommandes pour supprimer des préfixes de vos interfaces réseau existantes. IPv4

Pour supprimer des IPv4 préfixes d'une interface réseau

Utilisez la unassign-private-ip-addressescommande et définissez `--ipv4-prefix` l'adresse que vous souhaitez supprimer.

```
aws ec2 unassign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefixes 10.0.0.176/28
```

Pour supprimer des IPv6 préfixes d'une interface réseau

Utilisez la commande unassign-ipv6-addresses et spécifiez pour `--ipv6-prefix` l'adresse que vous souhaitez supprimer.

```
aws ec2 unassign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefix 2600:1f13:fc2:a700:18bb::/80
```

Supprimer une interface réseau

La suppression d'une interface réseau libère tous les attributs qui lui sont associés, ainsi que toute adresse IP privée ou adresse IP Elastic à utiliser par une autre instance.

Vous ne pouvez pas supprimer une interface réseau en cours d'utilisation. Tout d'abord, vous devez détacher l'interface réseau.

Pour supprimer une interface réseau à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau, puis sélectionnez Actions, Delete (Supprimer).
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Pour supprimer une interface réseau à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- delete-network-interface (AWS CLI)
- Remove-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Bande passante réseau des EC2 instances Amazon

Les spécifications de bande passante de l'instance s'appliquent au trafic entrant et sortant de l'instance. Par exemple, si une instance spécifie jusqu'à 10 Gbit/s de bande passante, cela signifie

qu'elle dispose d'une bande passante maximale de 10 Gbit/s pour le trafic entrant et de 10 Gbit/s pour le trafic sortant. La bande passante réseau disponible pour une EC2 instance dépend de plusieurs facteurs, comme suit.

Trafic multi-flux

La bande passante de référence pour le trafic multiflux est limitée à 50 % de la bande passante disponible pour le trafic passant par une passerelle Internet ou une passerelle locale.

Trafic à flux unique

La bande passante de référence pour le trafic à flux unique est limitée à 5 Gbit/s lorsque les instances ne sont pas dans le même groupe de placement du cluster. Pour réduire la latence et augmenter la bande passante à flux unique, essayez l'une des solutions suivantes :

- Utilisez un groupe de placement du cluster pour obtenir jusqu'à 10 Gbit/s de bande passante pour les instances au sein du même groupe.
- Configurez plusieurs chemins entre deux points de terminaison pour obtenir une bande passante plus élevée avec Multipath TCP ()MPTCP.
- Configurez ENA Express pour les instances éligibles au sein de la même zone de disponibilité afin d'atteindre jusqu'à 25 Gbit/s entre ces instances.

> **Note**
>
> Un flux unique est considéré comme un flux à 5 tuples TCP ou flux unique. UDP Pour les autres protocoles suivant l'en-tête IP, tels que `GRE` ou`IPsec`, le tuple 3 de l'adresse IP source, de l'adresse IP de destination et du protocole suivant est utilisé pour définir un flux.

Bande passante d'instance disponible

La bande passante réseau disponible d'une instance dépend vCPUs de son nombre. Par exemple, une `m5.8xlarge` instance dispose d'une bande passante réseau de 32 vCPUs et 10 Gbit/s, et une `m5.16xlarge` instance possède une bande passante réseau de 64 vCPUs et 20 Gbit/s. Les instances peuvent ne pas atteindre cette bande passante, par exemple, si elles dépassent les autorisations réseau au niveau de l'instance, tels que le paquet par seconde ou le nombre de connexions suivies. La quantité de bande passante disponible que le trafic peut utiliser dépend du

nombre vCPUs et de la destination. Par exemple, une `m5.16xlarge` instance en possède 64vCPUs, de sorte que le trafic vers une autre instance de la région peut utiliser toute la bande passante disponible (20 Gbit/s). Cependant, le trafic qui passe par une passerelle Internet ou une passerelle locale ne peut utiliser que 50 % de la bande passante disponible (10 Gbit/s).

Généralement, les instances de 16 vCPUs ou moins (taille `4xlarge` et moins) sont documentées comme ayant « jusqu'à » une bande passante spécifiée ; par exemple, « jusqu'à 10 Gbit/s ». Ces instances ont une bande passante de base. Pour répondre à une demande supplémentaire, ils peuvent utiliser un mécanisme de crédit d'I/O réseau pour surpasser leur bande passante de base. Les instances peuvent utiliser la bande passante de rafale pendant une durée limitée, généralement de 5 à 60 minutes, en fonction de la taille de l'instance.

Une instance reçoit le nombre maximal de crédits d'I/O réseau au lancement. Si l'instance épuise ses crédits d'I/O réseau, elle retourne à sa bande passante de base. Une instance en cours d'exécution gagne des crédits d'I/O réseau lorsqu'elle utilise moins de bande passante réseau que sa bande passante de base. Une instance arrêtée ne gagne pas de crédits d'I/O réseau. Le mode rafale d'une instance dépend de la mesure du possible, même lorsque l'instance dispose de crédits disponibles, car la bande passante de rafale est une ressource partagée.

Il existe des compartiments de crédits d'E/S réseau distincts pour les trafics entrants et sortants.

Performances réseau de base et de rafale

Le guide des types d'EC2instances Amazon décrit les performances réseau pour chaque type d'instance, ainsi que la bande passante réseau de base disponible pour les instances qui peuvent utiliser de la bande passante en rafale. Pour plus d'informations, consultez les ressources suivantes :

- Spécifications du réseau — Usage général
- Spécifications du réseau — Optimisé pour le calcul
- Spécifications du réseau — Mémoire optimisée
- Spécifications du réseau — Stockage optimisé
- Spécifications du réseau — Calcul accéléré
- Spécifications du réseau — Calcul à haute performance
- Spécifications du réseau — Génération précédente

Vous pouvez également utiliser un outil en ligne de commande pour obtenir ces informations.

AWS CLI

Vous pouvez utiliser la describe-instance-types AWS CLI commande pour afficher des informations sur un type d'instance. L'exemple suivant affiche les informations de performances du réseau pour toutes les instances C5.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=c5.*" \
    --query "InstanceTypes[].[InstanceType, NetworkInfo.NetworkPerformance,
 NetworkInfo.NetworkCards[0].BaselineBandwidthInGbps] | sort_by(@,&[2])" \
    --output table
```

Voici un exemple de sortie.

```
-----------------------------------------------
|           DescribeInstanceTypes             |
+--------------+--------------------+---------+
|  c5.large    |  Up to 10 Gigabit  |  0.75 |
|  c5.xlarge   |  Up to 10 Gigabit  |  1.25 |
|  c5.2xlarge  |  Up to 10 Gigabit  |  2.5  |
|  c5.4xlarge  |  Up to 10 Gigabit  |  5.0  |
|  c5.9xlarge  |  12 Gigabit        |  12.0 |
|  c5.12xlarge |  12 Gigabit        |  12.0 |
|  c5.18xlarge |  25 Gigabit        |  25.0 |
|  c5.24xlarge |  25 Gigabit        |  25.0 |
|  c5.metal    |  25 Gigabit        |  25.0 |
+--------------+--------------------+---------+
```

PowerShell

Vous pouvez utiliser la Get-EC2InstanceType PowerShell commande pour afficher des informations sur un type d'instance. L'exemple suivant affiche les informations de performances du réseau pour toutes les instances C5.

```
Get-EC2InstanceType -Filter @{Name = "instance-type"; Values = "c5.*" } | `
    Select-Object `
    InstanceType,
    @{Name = 'NetworkPerformance'; Expression =
 {($_.Networkinfo.NetworkCards.NetworkPerformance)}},
    @{Name = 'BaselineBandwidthInGbps'; Expression =
 {($_.Networkinfo.NetworkCards.BaselineBandwidthInGbps)}} | `
Format-Table -AutoSize
```

Voici un exemple de sortie.

```
InstanceType NetworkPerformance BaselineBandwidthInGbps
------------ ------------------ ----------------------
c5.4xlarge   Up to 10 Gigabit                    5.00
c5.xlarge    Up to 10 Gigabit                    1.25
c5.12xlarge  12 Gigabit                         12.00
c5.9xlarge   12 Gigabit                         12.00
c5.24xlarge  25 Gigabit                         25.00
c5.metal     25 Gigabit                         25.00
c5.2xlarge   Up to 10 Gigabit                    2.50
c5.large     Up to 10 Gigabit                    0.75
c5.18xlarge  25 Gigabit                         25.00
```

Contrôle de la bande passante de l'instance

Vous pouvez utiliser CloudWatch des métriques pour surveiller la bande passante du réseau de l'instance ainsi que les paquets envoyés et reçus. Vous pouvez utiliser les mesures de performance réseau fournies par le pilote Elastic Network Adapter (ENA) pour surveiller les cas où le trafic dépasse les allocations réseau définies par EC2 Amazon au niveau de l'instance.

Vous pouvez configurer si Amazon EC2 envoie des données métriques pour que l'instance CloudWatch utilise des périodes d'une minute ou de cinq minutes. Il est possible que les métriques de performance du réseau indiquent qu'une allocation a été dépassée et que des paquets ont été abandonnés alors que les métriques d' CloudWatch instance ne le font pas. Cela peut se produire lorsque l'instance connaît un bref pic de demande de ressources réseau (appelé microburst), mais que les CloudWatch indicateurs ne sont pas suffisamment précis pour refléter ces pics de microsecondes.

En savoir plus

- Métriques des instances
- Surveiller les performances réseau

Mise en réseau améliorée sur les EC2 instances Amazon

La mise en réseau améliorée utilise la virtualisation des E/S à racine unique (SR-IOV) pour fournir des fonctionnalités réseau hautes performances sur les types d'instances pris en charge. La SR-

IOV est une méthode de virtualisation des appareils qui fournit des performances d'E/S supérieures et un CPU taux d'utilisation réduit par rapport aux interfaces réseau virtualisées traditionnelles. La mise en réseau améliorée fournit une bande passante plus élevée, des performances de paquets par seconde (PPS) plus élevées et une latence constamment plus faible entre les instances. L'utilisation de la mise en réseau améliorée n'implique aucun coût supplémentaire.

Pour plus d'informations sur la vitesse réseau prise en charge pour chaque type d'instance, consultez Amazon EC2 Instance Types.

Tous les types d'instance de génération actuelle prennent en charge la mise en réseau améliorée, à l'exception des instances T2.

Vous pouvez activer la mise en réseau améliorée à l'aide de l'un des mécanismes suivants :

Adaptateur réseau élastique (ENA)

L'Elastic Network Adapter (ENA) prend en charge des vitesses réseau allant jusqu'à 100 Gbit/s pour les types d'instances pris en charge.

Toutes les instances basées sur le système AWS Nitro sont utilisées ENA pour améliorer la mise en réseau. En outre, les types d'instances Xen suivants sont compatibles ENA : H1, I3, G3, P2, P3`m4.16xlarge`, P3dn et R4.

Pour de plus amples informations, veuillez consulter Activez une mise en réseau améliorée avec ENA vos EC2 instances.

Interface Intel 82599 Virtual Function (VF)

L'interface Intel 82599 Virtual Function prend en charge les vitesses réseau allant jusqu'à 10 Gbit/s pour les types d'instance pris en charge.

Les types d'instance suivants utilisent l'interface Intel 82599 VF pour la mise en réseau améliorée : C3, C4, D2, I2, M4 (sauf m4.16xlarge) et R3.

Pour de plus amples informations, veuillez consulter Mise en réseau améliorée avec l'interface Intel 82599 VF.

Table des matières

- Mise en réseau améliorée avec l'interface Intel 82599 VF
- Surveillez les performances du réseau pour ENA les paramètres de votre EC2 instance
- Résoudre les problèmes liés au pilote ENA du noyau sous Linux
- Résoudre les problèmes liés au pilote Windows d'Elastic Network Adapter
- Améliorez la latence du réseau pour les EC2 instances basées sur Linux
- Considérations relatives au système Nitro pour le réglage des performances
- Optimisation des performances réseau sur les instances EC2 Windows

Activez une mise en réseau améliorée avec ENA vos EC2 instances

Amazon EC2 fournit des fonctionnalités réseau améliorées via l'Elastic Network Adapter (ENA). Pour utiliser la mise en réseau améliorée, vous devez utiliser un pilote AMI qui inclut le ENA pilote requis ou l'installer manuellement. Vous pouvez ensuite activer le ENA support sur votre instance.

Pour consulter les notes de version ou les instructions d'installation d'un ENA pilote, consultez l'onglet correspondant à la plate-forme du système d'exploitation de votre instance.

Linux

Vous pouvez consulter la documentation suivante sur GitHub :

- Consultez les notes de mise à jour du pilote du noyau ENA Linux sur GitHub.
- Pour une présentation du pilote de noyau ENA Linux qui inclut les instructions d'installation, voir le pilote de noyau Linux pour la famille Elastic Network Adapter (ENA) sur GitHub.

Windows

Vous pouvez consulter la documentation suivante dans la section Gérer les pilotes de périphériques de ce guide :

- Suivez ENA les versions des pilotes Windows.
- Installation du ENA pilote sur les instances EC2 Windows.

Pour les instances basées sur Nitro, les fonctionnalités réseau améliorées varient selon la version de Nitro implémentée par le type d'instance.

Pour consulter les spécifications réseau de votre instance, choisissez le lien de famille d'instance correspondant à votre type d'instance. Si vous ne savez pas quelle famille d'instances s'applique, consultez les conventions de dénomination dans le guide Amazon EC2 Instance Types.

- Spécifications réseau pour les instances de calcul accéléré
- Spécifications réseau pour les instances optimisées pour le calcul
- Spécifications réseau pour les instances à usage général
- Spécifications réseau pour les instances de calcul hautes performances
- Spécifications réseau pour les instances optimisées en mémoire
- Spécifications réseau pour les instances optimisées pour le stockage

Table des matières

Conditions préalables pour une mise en réseau améliorée avec ENA

Pour préparer une mise en réseau améliorée à l'aide duENA, configurez votre instance comme suit :

- Lancez une instance basée sur le système AWS Nitro.
- Vérifiez que l'instance a une connectivité Internet.
- Si vous avez des données importantes sur l'instance que vous souhaitez conserver, vous devez les sauvegarder dès maintenant en créant un AMI à partir de votre instance. La mise à jour ENA du pilote du noyau et l'activation de `enaSupport` l'attribut peuvent rendre les instances incompatibles ou les systèmes d'exploitation inaccessibles. Si cela se produit et que vous disposez d'une sauvegarde récente, vos données continueront d'être conservées.
- Instances Linux : lancez l'instance à l'aide d'une version compatible du noyau Linux et d'une distribution prise en charge, afin que la mise en réseau ENA améliorée soit automatiquement activée pour votre instance. Pour plus d'informations, consultez les notes de mise à jour du pilote ENA Linux Kernel.
- Instances Windows : si l'instance exécute Windows Server 2008 R2SP1, assurez-vous qu'elle dispose de la mise à jour de prise en charge de la signature de code SHA -2.

- AWS CloudShellUtilisez-le depuis ou installez et configurez le AWS CLIou AWS Tools for Windows PowerShellsur n'importe quel ordinateur de votre choix, de préférence sur votre ordinateur de bureau ou portable local. AWS Management Console Pour plus d'informations, consultez la section Accédez à Amazon EC2 du Guide de l'utilisateur AWS CloudShell. La mise en réseau améliorée ne peut pas être gérée depuis la EC2 console Amazon.

Tester l'activation de réseaux améliorés

Vous pouvez tester si la mise en réseau améliorée est activée dans vos instances ou dans votreAMIs.

Attribut d'instance

Pour vérifier si l'attribut de mise en réseau améliorée `enaSupport` est défini sur une instance, utilisez l'une des commandes suivantes. Si l'attribut est défini, la réponse est true.

- describe-instances (AWS CLI/AWS CloudShell)

```
aws ec2 describe-instances --instance-ids instance_id --query
 "Reservations[].Instances[].EnaSupport"
```

- Get-EC2Instance(Outils pour Windows PowerShell)

```
(Get-EC2Instance -InstanceId instance-id).Instances.EnaSupport
```

Attribut d'image

Pour vérifier si un `enaSupport` attribut de mise en réseau amélioré AMI est défini, utilisez l'une des commandes suivantes. Si l'attribut est défini, la réponse est true.

- describe-images (AWS CLI/AWS CloudShell)

```
aws ec2 describe-images --image-id ami_id --query "Images[].EnaSupport"
```

- Get-EC2Image(Outils pour Windows PowerShell)

```
(Get-EC2Image -ImageId ami_id).EnaSupport
```

pilote d'interface réseau Linux

Utilisez la commande suivante pour vérifier que le pilote `ena` du noyau est utilisé sur une interface particulière, en remplaçant le nom de l'interface que vous souhaitez vérifier. Si vous utilisez une seule interface (par défaut), ce sera `eth0`. Si le système d'exploitation prend en charge les noms de réseau prévisibles, il peut s'agir d'un nom tel que `ens5`.

Dans l'exemple suivant, le pilote `ena` du noyau n'est pas chargé, car le pilote répertorié l'est`vif`.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Dans cet exemple, le pilote `ena` du noyau est chargé et possède la version minimale recommandée. La mise en réseau améliorée est correctement configurée pour cette instance.

```
[ec2-user ~]$ ethtool -i eth0
driver: ena
version: 1.5.0g
firmware-version:
expansion-rom-version:
bus-info: 0000:00:05.0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Activer les réseaux améliorés sur une instance

La procédure que vous utilisez dépend du système d'exploitation de l'instance.

Amazon Linux

Amazon Linux 2 et les dernières versions d'Amazon Linux AMI incluent le pilote de noyau requis pour une mise en réseau améliorée, une fois le ENA support ENA installé et activé. Par conséquent, si vous lancez une instance avec une HVM version d'Amazon Linux sur un type d'instance pris en charge, la mise en réseau améliorée est déjà activée pour votre instance. Pour plus d'informations, consultez Tester l'activation de réseaux améliorés.

Si vous avez lancé votre instance à l'aide d'un ancien Amazon Linux AMI et que la mise en réseau améliorée n'est pas encore activée, suivez la procédure suivante pour activer la mise en réseau améliorée.

Pour activer la mise en réseau améliorée sur Amazon Linux AMI

1. Connectez-vous à votre instance.
2. À partir de l'instance, exécutez la commande suivante pour mettre à jour votre instance avec les derniers pilotes du noyau, notamment `ena` :

   ```
   [ec2-user ~]$ sudo yum update
   ```

3. Depuis votre ordinateur local, redémarrez votre instance à l'aide de la EC2 console Amazon ou de l'une des commandes suivantes : reboot-instances(AWS CLI), Restart-EC2Instance(AWS Tools for Windows PowerShell).
4. Connectez-vous à nouveau à votre instance et vérifiez que le pilote `ena` du noyau est installé et qu'il possède la version minimale recommandée à l'aide de la modinfo ena commande fromTester l'activation de réseaux améliorés.
5. [instance EBS sauvegardée] Depuis votre ordinateur local, arrêtez l'instance à l'aide de la EC2 console Amazon ou de l'une des commandes suivantes : stop-instances(AWS CLI), Stop-EC2Instance(AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez l'arrêter dans la AWS OpsWorks console afin que son état reste synchronisé.

   [Instance basée sur le stockage d'instance] Vous ne pouvez pas arrêter l'instance pour modifier l'attribut. Vous devez utiliser cette procédure : Pour activer la mise en réseau améliorée sur Amazon Linux AMI (instances basées sur le stockage d'instances).
6. Depuis votre ordinateur local, activez l'attribut de mise en réseau améliorée à l'aide de l'une des commandes suivantes:

- modify-instance-attribute (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
```

- Edit-EC2InstanceAttribute(Outils pour Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
```

7. (Facultatif) Créez un AMI à partir de l'instance, comme décrit dansCréez un compte soutenu EBS par Amazon AMI. AMIhérite de l'`enaSupport`attribut réseau amélioré de l'instance. Vous pouvez donc l'utiliser AMI pour lancer une autre instance avec la mise en réseau améliorée activée par défaut.
8. Depuis votre ordinateur local, démarrez l'instance à l'aide de la EC2 console Amazon ou de l'une des commandes suivantes : start-instances(AWS CLI), Start-EC2Instance(AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez démarrer l'instance dans la AWS OpsWorks console afin que son état reste synchronisé.
9. Connectez-vous à votre instance et vérifiez que le pilote `ena` du noyau est installé et chargé sur votre interface réseau à l'aide de la ethtool -i eth*n* commande fromTester l'activation de réseaux améliorés.

   Si vous ne parvenez pas à vous connecter à votre instance après avoir activé la mise en réseau améliorée, consultez Résoudre les problèmes liés au pilote ENA du noyau sous Linux.

Pour activer la mise en réseau améliorée sur Amazon Linux AMI (instances basées sur le stockage d'instances)

Suivez la procédure précédente jusqu'à l'étape à laquelle vous avez arrêté l'instance. Créez un nouveau AMI comme décrit dansCréation d'une instance sauvegardée en magasin AMI, en veillant à activer l'attribut réseau amélioré lorsque vous enregistrez leAMI.

- register-image (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

Ubuntu

La dernière version d'Ubuntu HVM AMIs inclut le pilote de noyau requis pour améliorer la mise en réseau une fois ENA installé et ENA son support activé. Par conséquent, si vous lancez une instance avec la dernière version d'Ubuntu HVM AMI sur un type d'instance pris en charge, la mise en réseau améliorée est déjà activée pour votre instance. Pour plus d'informations, consultez Tester l'activation de réseaux améliorés.

Si vous avez lancé votre instance à l'aide d'une version plus ancienne AMI et que la mise en réseau améliorée n'est pas encore activée, vous pouvez installer le package du `linux-aws` noyau pour obtenir les derniers pilotes réseau améliorés et mettre à jour l'attribut requis.

Pour installer le package du noyau **`linux-aws`** (Ubuntu 16.04 ou version ultérieure)

Ubuntu 16.04 et 18.04 sont fournis avec le noyau personnalisé Ubuntu (package du noyau `linux-aws`). Pour utiliser un autre noyau, contactez AWS Support.

Pour installer le package du noyau **`linux-aws`** (Ubuntu Trusty 14.04)

1. Connectez-vous à votre instance.
2. Mettez à jour le cache du package et les packages.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

> **Important**
>
> Si, lors d'une mise à jour, vous êtes invité à installer `grub`, utilisez `/dev/xvda` pour y installer `grub`, puis choisissez de conserver la version courante de `/boot/grub/menu.lst`.

3. [instance EBS sauvegardée] Depuis votre ordinateur local, arrêtez l'instance à l'aide de la EC2 console Amazon ou de l'une des commandes suivantes : stop-instances(AWS CLI), Stop-EC2Instance(AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez l'arrêter dans la AWS OpsWorks console afin que son état reste synchronisé.

   [Instance basée sur le stockage d'instance] Vous ne pouvez pas arrêter l'instance pour modifier l'attribut. Vous devez utiliser cette procédure : Pour activer la mise en réseau améliorée sur Ubuntu (instances basées sur le stockage d'instance).

4. Depuis votre ordinateur local, activez l'attribut de mise en réseau améliorée à l'aide de l'une des commandes suivantes:

   - modify-instance-attribute (AWS CLI)

     ```
     aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
     ```

   - Edit-EC2InstanceAttribute(Outils pour Windows PowerShell)

     ```
     Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
     ```

5. (Facultatif) Créez un AMI à partir de l'instance, comme décrit dansCréez un compte soutenu EBS par Amazon AMI. AMIhérite de l'`enaSupport`attribut réseau amélioré de l'instance. Vous pouvez donc l'utiliser AMI pour lancer une autre instance avec la mise en réseau améliorée activée par défaut.
6. Depuis votre ordinateur local, démarrez l'instance à l'aide de la EC2 console Amazon ou de l'une des commandes suivantes : start-instances(AWS CLI), Start-EC2Instance(AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez démarrer l'instance dans la AWS OpsWorks console afin que son état reste synchronisé.

Pour activer la mise en réseau améliorée sur Ubuntu (instances basées sur le stockage d'instance)

Suivez la procédure précédente jusqu'à l'étape à laquelle vous avez arrêté l'instance. Créez un nouveau AMI comme décrit dansCréation d'une instance sauvegardée en magasin AMI, en veillant à activer l'attribut réseau amélioré lorsque vous enregistrez leAMI.

- register-image (AWS CLI)

  ```
  aws ec2 register-image --ena-support ...
  ```

- Register-EC2Image (AWS Tools for Windows PowerShell)

  ```
  Register-EC2Image -EnaSupport $true ...
  ```

RHELSUSE, CentOS

Les dernières AMIs versions pour Red Hat Enterprise Linux, SUSE Linux Enterprise Server et CentOS incluent le pilote de noyau requis pour améliorer la mise en réseau avec ENA le ENA

support activé. Par conséquent, si vous lancez une instance avec la dernière version AMI d'un type d'instance pris en charge, la mise en réseau améliorée est déjà activée pour votre instance. Pour plus d'informations, consultez Tester l'activation de réseaux améliorés.

La procédure suivante fournit les étapes générales pour activer la mise en réseau améliorée sur une distribution Linux autre qu'Amazon Linux AMI ou Ubuntu. Pour plus d'informations, telles que la syntaxe détaillée des commandes, les emplacements de fichier ou la prise en charge des packages et des outils, consultez la documentation spécifique de votre distribution Linux.

Pour activer la mise en réseau améliorée sur Linux

1. Connectez-vous à votre instance.
2. Clonez le code source du pilote `ena` du noyau sur votre instance GitHub à partir dehttps://github.com/amzn/amzn-drivers. (SUSELinux Enterprise Server 12 SP2 et versions ultérieures incluent la version ENA 2.02 par défaut, vous n'êtes donc pas obligé de télécharger et de compiler le ENA pilote. Pour SUSE Linux Enterprise Server 12 SP2 et versions ultérieures, vous devez déposer une demande pour ajouter la version du pilote que vous souhaitez au noyau d'origine).

   ```
   git clone https://github.com/amzn/amzn-drivers
   ```

3. Compilez et installez le pilote `ena` du noyau sur votre instance. Ces étapes dépendent de la distribution Linux. Pour plus d'informations sur la compilation du pilote de noyau sur Red Hat Enterprise Linux, consultez Comment installer le dernier ENS pilote pour un support réseau amélioré sur une EC2 instance Amazon qui s'exécute RHEL ?
4. Exécutez la sudo depmod commande pour mettre à jour les dépendances des pilotes du noyau.
5. Effectuez une mise à jour `initramfs` sur votre instance pour vous assurer que le nouveau pilote du noyau se charge au démarrage. Par exemple, si votre distribution prend en charge dracut, vous pouvez utiliser la commande suivante :

   ```
   dracut -f -v
   ```

6. Déterminez si par défaut votre système utilise des noms d'interface réseau prévisibles. Les systèmes qui utilisent systemd ou udev version 197 ou supérieure peuvent renommer les périphériques Ethernet et ne garantissent pas qu'une seule interface réseau sera nommée `eth0`. Ce comportement peut entraîner des problèmes de connexion à votre instance. Pour plus d'informations et pour voir les autres options de configuration, consultez la section sur les noms d'interface réseau prévisibles sur le site web de freedesktop.org.

a. Vous pouvez vérifier les udev versions systemd ou sur les systèmes RPM basés sur les systèmes à l'aide de la commande suivante.

```
rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
systemd-208-11.el7_0.2.x86_64
```

Dans l'exemple Red Hat Enterprise Linux 7 ci-dessus, la version systemd est 208, de sorte que les noms d'interface réseau prévisibles doivent être désactivés.

b. Désactivez les noms d'interface réseau prévisibles en ajoutant l'option `net.ifnames=0` à la ligne `GRUB_CMDLINE_LINUX` dans `/etc/default/grub`.

```
sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /etc/default/
grub
```

c. Générez à nouveau le fichier de configuration grub.

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. [instance EBS sauvegardée] Depuis votre ordinateur local, arrêtez l'instance à l'aide de la EC2 console Amazon ou de l'une des commandes suivantes : stop-instances(AWS CLI), Stop-EC2Instance(AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez l'arrêter dans la AWS OpsWorks console afin que son état reste synchronisé.

   [Instance basée sur le stockage d'instance] Vous ne pouvez pas arrêter l'instance pour modifier l'attribut. Vous devez utiliser cette procédure : Pour activer les réseaux améliorés sur Linux (instances basées sur le stockage d'instances).

8. Depuis votre ordinateur local, activez l'attribut de mise en réseau améliorée `enaSupport` à l'aide de l'une des commandes suivantes:

   - modify-instance-attribute (AWS CLI)

     ```
     aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
     ```

   - Edit-EC2InstanceAttribute(Outils pour Windows PowerShell)

     ```
     Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
     ```

9. (Facultatif) Créez un AMI à partir de l'instance, comme décrit dansCréez un compte soutenu EBS par Amazon AMI. AMIhérite de l'`enaSupport`attribut réseau amélioré de l'instance. Vous pouvez donc l'utiliser AMI pour lancer une autre instance avec la mise en réseau améliorée activée par défaut.

   Si le système d'exploitation de votre instance contient un `/etc/udev/rules.d/70-persistent-net.rules` fichier, vous devez le supprimer avant de créer leAMI. Ce fichier contient l'MACadresse de l'adaptateur Ethernet de l'instance d'origine. Si une autre instance démarre avec ce fichier, le système d'exploitation ne pourra pas trouver le périphérique et il se peut qu'`eth0` échoue, entraînant des problèmes de démarrage. Ce fichier est régénéré lors du cycle de démarrage suivant, et toutes les instances lancées à partir de ce AMI dernier créent leur propre version du fichier.

10. Depuis votre ordinateur local, démarrez l'instance à l'aide de la EC2 console Amazon ou de l'une des commandes suivantes : start-instances(AWS CLI), Start-EC2Instance(AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez démarrer l'instance dans la AWS OpsWorks console afin que son état reste synchronisé.

11. (Facultatif) Connectez-vous à votre instance et vérifiez que le pilote du noyau est installé.

    Si vous ne parvenez pas à vous connecter à votre instance après avoir activé la mise en réseau améliorée, consultez Résoudre les problèmes liés au pilote ENA du noyau sous Linux.

Pour activer les réseaux améliorés sur Linux (instances basées sur le stockage d'instances)

Suivez la procédure précédente jusqu'à l'étape à laquelle vous avez arrêté l'instance. Créez un nouveau AMI comme décrit dansCréation d'une instance sauvegardée en magasin AMI, en veillant à activer l'attribut réseau amélioré lorsque vous enregistrez leAMI.

- register-image (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport ...
```

Ubuntu avec DKMS

Cette méthode est fournie à des fins de test et de rétroaction uniquement. Elle n'est pas destinée à être utilisée avec des déploiements en production. Pour plus d'informations sur les déploiements en production, consultez Ubuntu.

> **Important**
>
> L'utilisation DKMS annule le contrat de support de votre abonnement. Il ne doit pas être utilisé pour les déploiements de production.

Pour activer la mise en réseau améliorée ENA sous Ubuntu (instances EBS soutenues par -backed)

1. Suivez les étapes 1 et 2 dans Ubuntu.
2. Installez les `build-essential` packages pour compiler le pilote du noyau et le `dkms` package afin que votre pilote de `ena` noyau soit reconstruit chaque fois que votre noyau est mis à jour.

   ```
   ubuntu:~$ sudo apt-get install -y build-essential dkms
   ```

3. Clonez la source du pilote `ena` du noyau sur votre instance GitHub à partir dehttps://github.com/amzn/amzn-drivers.

   ```
   ubuntu:~$ git clone https://github.com/amzn/amzn-drivers
   ```

4. Déplacez le `amzn-drivers` package `/usr/src/` dans le répertoire afin de le DKMS trouver et de le compiler pour chaque mise à jour du noyau. Ajoutez le numéro de version (que vous trouverez dans les notes de version) du code source au nom du répertoire. Par exemple, la version `1.0.0` apparaît dans l'exemple suivant.

   ```
   ubuntu:~$ sudo mv amzn-drivers /usr/src/amzn-drivers-1.0.0
   ```

5. Créez le fichier DKMS de configuration avec les valeurs suivantes, en remplaçant votre version de`ena`.

   Créez le fichier.

   ```
   ubuntu:~$ sudo touch /usr/src/amzn-drivers-1.0.0/dkms.conf
   ```

Modifiez le fichier et ajoutez les valeurs suivantes.

```
ubuntu:~$ sudo vim /usr/src/amzn-drivers-1.0.0/dkms.conf
PACKAGE_NAME="ena"
PACKAGE_VERSION="1.0.0"
CLEAN="make -C kernel/linux/ena clean"
MAKE="make -C kernel/linux/ena/ BUILD_KERNEL=${kernelver}"
BUILT_MODULE_NAME[0]="ena"
BUILT_MODULE_LOCATION="kernel/linux/ena"
DEST_MODULE_LOCATION[0]="/updates"
DEST_MODULE_NAME[0]="ena"
AUTOINSTALL="yes"
```

6. Ajoutez, compilez et installez le pilote du `ena` noyau sur votre instance à l'aide deDKMS.

   Ajoutez le pilote du noyau àDKMS.

   ```
   ubuntu:~$ sudo dkms add -m amzn-drivers -v 1.0.0
   ```

   Créez le pilote du noyau à l'aide de la dkms commande.

   ```
   ubuntu:~$ sudo dkms build -m amzn-drivers -v 1.0.0
   ```

   Installez le pilote du noyau à l'aide dedkms.

   ```
   ubuntu:~$ sudo dkms install -m amzn-drivers -v 1.0.0
   ```

7. Reconstruisez `initramfs` afin que le pilote de noyau approprié soit chargé au moment du démarrage.

   ```
   ubuntu:~$ sudo update-initramfs -u -k all
   ```

8. Vérifiez que le pilote `ena` du noyau est installé à l'aide de la commande modinfo ena deTester l'activation de réseaux améliorés.

   ```
   ubuntu:~$ modinfo ena
   filename:    /lib/modules/3.13.0-74-generic/updates/dkms/ena.ko
   version:  1.0.0
   license:  GPL
   description: Elastic Network Adapter (ENA)
   ```

```
author:   Amazon.com, Inc. or its affiliates
srcversion:  9693C876C54CA64AE48F0CA
alias:    pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
depends:
vermagic:    3.13.0-74-generic SMP mod_unload modversions
parm:     debug:Debug level (0=none,...,16=all) (int)
parm:     push_mode:Descriptor / header push mode (0=automatic,1=disable,3=enable)
    0 - Automatically choose according to device capability (default)
    1 - Don't push anything to device memory
    3 - Push descriptors and header buffer to device memory (int)
parm:     enable_wd:Enable keepalive watchdog (0=disable,1=enable,default=1) (int)
parm:     enable_missing_tx_detection:Enable missing Tx completions. (default=1)
 (int)
parm:     numa_node_override_array:Numa node override map
(array of int)
parm:     numa_node_override:Enable/Disable numa node override (0=disable)
(int)
```

9. Passez à l'étape 3 dans Ubuntu.

Activer les réseaux améliorés sur Windows

Si vous avez lancé votre instance et qu'elle n'a pas la mise en réseau déjà activée, vous devez télécharger et installer le pilote de la carte réseau requis sur votre instance, puis définir l'attribut d'instance `enaSupport` pour activer la mise en réseau améliorée.

Pour activer la mise en réseau améliorée

1. Connectez-vous à votre instance en tant qu'administrateur local.
2. [Windows Server 2016 et 2019 uniquement] Exécutez le EC2Launch PowerShell script suivant pour configurer l'instance une fois le pilote installé.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

3. Depuis l'instance, installez le pilote comme suit :
   a. Téléchargez le pilote le plus récent sur l'instance.
   b. Décompressez l'archive zip.

c. Installez le pilote en exécutant le `install.ps1` PowerShell script.

> **Note**
>
> Si vous obtenez une erreur d'exécution de la stratégie, définissez la stratégie sur `Unrestricted` (par défaut, elle est définie sur `Restricted` ou `RemoteSigned`). Dans une ligne de commande, exécutez`Set-ExecutionPolicy -ExecutionPolicy Unrestricted`, puis réexécutez le `install.ps1` PowerShell script.

4. Depuis votre ordinateur local, arrêtez l'instance à l'aide de la EC2 console Amazon ou de l'une des commandes suivantes : stop-instances(AWS CLI/AWS CloudShell), Stop-EC2Instance(AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez l'arrêter dans la AWS OpsWorks console afin que son état reste synchronisé.
5. Activez le ENA support sur votre instance comme suit :

   a. Depuis votre ordinateur local, vérifiez l'attribut de ENA support d'EC2instance de votre instance en exécutant l'une des commandes suivantes. Si l'attribut n'est pas activé, la sortie indiquera « [] » ou une valeur vide. `EnaSupport` est défini sur `false` par défaut.

   - describe-instances (AWS CLI/AWS CloudShell)

```
aws ec2 describe-instances --instance-ids instance_id --query
 "Reservations[].Instances[].EnaSupport"
```

   - Get-EC2Instance(Outils pour Windows PowerShell)

```
(Get-EC2Instance -InstanceId instance-id).Instances.EnaSupport
```

   b. Pour activer ENA le support, exécutez l'une des commandes suivantes :

   - modify-instance-attribute (AWS CLI/AWS CloudShell)

```
aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
```

   - Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $true
```

Si vous rencontrez des problèmes lorsque vous redémarrez l'instance, vous pouvez également désactiver le ENA support à l'aide de l'une des commandes suivantes :

- modify-instance-attribute (AWS CLI/AWS CloudShell)

```
aws ec2 modify-instance-attribute --instance-id instance_id --no-ena-support
```

- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $false
```

c. Vérifiez que l'attribut a été défini sur `true` à l'aide de describe-instances ou Get-EC2Instance comme indiqué précédemment. Vous devriez désormais voir la sortie suivante :

```
[
 true
]
```

6. Depuis votre ordinateur local, démarrez l'instance à l'aide de la EC2 console Amazon ou de l'une des commandes suivantes : start-instances(AWS CLI/AWS CloudShell), Start-EC2Instance(AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez démarrer l'instance à l'aide de la AWS OpsWorks console afin que son état reste synchronisé.
7. Sur l'instance, vérifiez que le ENA pilote est installé et activé comme suit :

   a. Cliquez sur l'icône réseau avec le bouton droit de la souris et choisissez Open Network and Sharing Center (Ouvrir le Centre Réseau et partage).

   b. Choisissez la carte Ethernet (par exemple, Ethernet 2).

   c. Sélectionnez Details (Détails). Pour Network Connection Details (Détails de connexion réseau), vérifiez que Description a pour valeur Amazon Elastic Network Adapter.

8. (Facultatif) Créez un AMI à partir de l'instance. AMIhérite de l'`enaSupport`attribut de l'instance. Vous pouvez donc l'utiliser AMI pour lancer une autre instance ENA activée par défaut.

Améliorez les performances du réseau entre EC2 les instances avec ENA Express

ENAExpress est alimenté par la technologie AWS Scalable Reliable Datagram (SRD). SRDest un protocole de transport réseau à hautes performances qui utilise le routage dynamique pour augmenter le débit et minimiser la latence de queue. Avec ENA Express, vous pouvez communiquer entre deux EC2 instances de la même zone de disponibilité.

Avantages d'ENAExpress

- Augmente la bande passante maximale qu'un flux unique peut utiliser de 5 Gbit/s à 25 Gbit/s dans la zone de disponibilité, jusqu'à la limite d'instances agrégées.
- Réduit la latence finale du trafic réseau entre les EC2 instances, en particulier pendant les périodes de charge réseau élevée.
- Détecte et évite les chemins réseau encombrés.
- Gère certaines tâches directement dans la couche réseau, telles que la réorganisation des paquets du côté récepteur et la plupart des retransmissions nécessaires. Cela permet de libérer la couche d'application pour d'autres tâches.

> **Note**
>
> - Si votre application envoie ou reçoit un volume élevé de paquets par seconde et doit optimiser la latence la plupart du temps, en particulier pendant les périodes où il n'y a pas d'encombrement sur le réseau, Réseaux améliorés peut être mieux adaptée à votre réseau.
> - ENALe trafic express ne peut pas être envoyé à travers les sous-réseaux d'une zone locale.

Une fois que vous avez activé ENA Express pour la connexion d'interface réseau sur une instance, l'instance d'envoi initie la communication avec l'instance de réception et SRD détecte si ENA Express fonctionne à la fois sur l'instance d'envoi et sur l'instance de réception. Si ENA Express fonctionne, la communication peut utiliser SRD la transmission. Si ENA Express ne fonctionne pas, la communication revient à la ENA transmission standard.

Pendant les périodes où le trafic réseau est faible, vous remarquerez peut-être une légère augmentation de la latence des paquets (des dizaines de microsecondes) lorsque le paquet utilise ENA Express. Pendant ces périodes, les applications qui privilégient des caractéristiques de performance réseau spécifiques peuvent bénéficier d'ENAExpress comme suit :

- Les processus peuvent bénéficier d'une augmentation de la bande passante à flux unique maximale de 5 Gbit/s à 25 Gbit/s au sein d'une même zone de disponibilité, jusqu'à la limite d'instances agrégée. Par exemple, si un type d'instance spécifique prend en charge jusqu'à 12,5 Gbit/s, la bande passante à flux unique est également limitée à 12,5 Gbit/s.
- Les processus qui s'exécutent depuis longtemps devraient bénéficier d'une réduction de la latence pendant les périodes d'encombrement du réseau.
- Les processus peuvent bénéficier d'une distribution plus régulière et plus standard des temps de réponse du réseau.

Rubriques

Comment fonctionne ENA Express

ENAExpress est alimenté par la technologie AWS Scalable Reliable Datagram (SRD). Il distribue les paquets pour chaque flux réseau sur différents chemins AWS réseau et ajuste dynamiquement la distribution lorsqu'il détecte des signes de congestion. Elle gère également la réorganisation des paquets du côté récepteur.

Pour qu'ENAExpress puisse gérer le trafic réseau comme prévu, les instances d'envoi et de réception ainsi que la communication entre elles doivent répondre à toutes les exigences suivantes :

- Les types d'instance d'envoi et de réception sont pris en charge. Consultez la table Types d'instances pris en charge pour ENA Express pour plus d'informations.

- ENAExpress doit être configuré pour les instances d'envoi et de réception. S'il existe des différences dans la configuration, vous pouvez vous retrouver dans des situations où le trafic utilise par défaut la ENA transmission standard. Le scénario suivant montre ce qui peut se passer.

  Scénario : différences de configuration

Instance	ENAExpress activé	UDPutilise ENA Express
Instance 1	Oui	Oui
Instance 2	Oui	Non

  Dans ce cas, le TCP trafic entre les deux instances peut utiliser ENA Express, car les deux instances l'ont activé. Cependant, étant donné que l'une des instances n'utilise pas ENA Express pour UDP le trafic, la communication entre ces deux instances UDP utilise la ENA transmission standard.
- Les instances d'envoi et de réception doivent s'exécuter dans la même zone de disponibilité.
- Le chemin réseau entre les instances ne doit pas inclure de boîtiers intergiciels. ENAExpress ne prend actuellement pas en charge les intergiciels.
- (Instances Linux uniquement) Pour utiliser tout le potentiel de bande passante, utilisez la version 2.2.9 ou supérieure du pilote.
- (Instances Linux uniquement) Pour produire des métriques, utilisez la version 2.8 ou supérieure du pilote.

Si une exigence n'est pas satisfaite, les instances utilisent le UDP protocole standardTCP/mais sans SRD communiquer.

Pour vous assurer que le pilote réseau de votre instance est configuré pour des performances optimales, consultez les meilleures pratiques recommandées pour ENA les pilotes. Ces meilleures pratiques s'appliquent également à ENA Express. Pour plus d'informations, consultez le guide des meilleures pratiques et d'optimisation des performances des pilotes ENA Linux sur le GitHub site Web.

> **Note**
>
> Amazon EC2 fait référence à la relation entre une instance et une interface réseau qui y est attachée en tant que pièce jointe. ENALes paramètres Express s'appliquent à la pièce jointe. Si l'interface réseau est détachée de l'instance, la pièce jointe n'existe plus et les paramètres ENA Express qui s'y appliquaient ne sont plus en vigueur. Il en va de même lorsqu'une instance est résiliée, même si l'interface réseau est conservée.

Une fois que vous avez activé ENA Express pour les pièces jointes de l'interface réseau sur l'instance d'envoi et sur l'instance de réception, vous pouvez utiliser les métriques ENA Express pour vous assurer que vos instances tirent pleinement parti des améliorations de performances apportées par la SRD technologie. Pour plus d'informations sur les métriques ENA Express, consultezMétriques pour ENA Express.

Types d'instances pris en charge pour ENA Express

Les onglets suivants présentent les types d'instances compatibles avec ENA Express.

General purpose

Type d'instance	Architecture
m6a.12xlarge	x86_64
m6a.16xlarge	x86_64
m6a.24xlarge	x86_64
m6a.32xlarge	x86_64
m6a.48xlarge	x86_64
m6a.metal	x86_64
m6i.8xlarge	x86_64
m6i.12xlarge	x86_64
m6i.16xlarge	x86_64

Type d'instance	Architecture
m6i.24xlarge	x86_64
m6i.32xlarge	x86_64
m6i.metal	x86_64
m6id.8xlarge	x86_64
m6id.12xlarge	x86_64
m6id.16xlarge	x86_64
m6id.24xlarge	x86_64
m6id.32xlarge	x86_64
m6id.metal	x86_64
m7a.12xlarge	x86_64
m7a.16xlarge	x86_64
m7a.24xlarge	x86_64
m7a.32xlarge	x86_64
m7a.48xlarge	x86_64
m7a.metal-48xl	x86_64
m7g.12xlarge	arm64
m7g.16xlarge	arm64
m7g.metal	arm64
m7gd.12xlarge	arm64
m7gd.16xlarge	arm64

Type d'instance	Architecture
m7gd.metal	arm64
m7i.12xlarge	x86_64
m7i.16xlarge	x86_64
m7i.24xlarge	x86_64
m7i.48xlarge	x86_64
m7i.metal-24xl	x86_64
m7i.metal-48xl	x86_64

Compute optimized

Type d'instance	Architecture
c6a.12xlarge	x86_64
c6a.16xlarge	x86_64
c6a.24xlarge	x86_64
c6a.32xlarge	x86_64
c6a.48xlarge	x86_64
c6a.metal	x86_64
c6gn.16xlarge	arm64
c6i.8xlarge	x86_64
c6i.12xlarge	x86_64
c6i.16xlarge	x86_64

Type d'instance	Architecture
c6i.24xlarge	x86_64
c6i.32xlarge	x86_64
c6i.metal	x86_64
c6id.8xlarge	x86_64
c6id.12xlarge	x86_64
c6id.16xlarge	x86_64
c6id.24xlarge	x86_64
c6id.32xlarge	x86_64
c6id.metal	x86_64
c7a.12xlarge	x86_64
c7a.16xlarge	x86_64
c7a.24xlarge	x86_64
c7a.32xlarge	x86_64
c7a.48xlarge	x86_64
c7a.metal-48xl	x86_64
c7g.12xlarge	arm64
c7g.16xlarge	arm64
c7g.metal	arm64
c7gd.12xlarge	arm64
c7gd.16xlarge	arm64

Type d'instance	Architecture
c7gd.metal	arm64
c7i.12xlarge	x86_64
c7i.16xlarge	x86_64
c7i.24xlarge	x86_64
c7i.48xlarge	x86_64
c7i.metal-24xl	x86_64
c7i.metal-48xl	x86_64

Memory optimized

Type d'instance	Architecture
r6a.12xlarge	x86_64
r6a.16xlarge	x86_64
r6a.24xlarge	x86_64
r6a.32xlarge	x86_64
r6a.48xlarge	x86_64
r6a.metal	x86_64
r6i.8xlarge	x86_64
r6i.12xlarge	x86_64
r6i.16xlarge	x86_64
r6i.24xlarge	x86_64

Type d'instance	Architecture
r6i.32xlarge	x86_64
r6i.metal	x86_64
r6id.8xlarge	x86_64
r6id.12xlarge	x86_64
r6id.16xlarge	x86_64
r6id.24xlarge	x86_64
r6id.32xlarge	x86_64
r6id.metal	x86_64
r7a.12xlarge	x86_64
r7a.16xlarge	x86_64
r7a.24xlarge	x86_64
r7a.32xlarge	x86_64
r7a.48xlarge	x86_64
r7a.metal-48xl	x86_64
r7g.12xlarge	arm64
r7g.16xlarge	arm64
r7g.metal	arm64
r7gd.12xlarge	arm64
r7gd.16xlarge	arm64
r7gd.metal	arm64

Type d'instance	Architecture
r7i.12xlarge	x86_64
r7i.16xlarge	x86_64
r7i.24xlarge	x86_64
r7i.48xlarge	x86_64
r7i.metal-24xl	x86_64
r7i.metal-48xl	x86_64
r8g.12xlarge	arm64
r8g.16xlarge	arm64
r8g.24xlarge	arm64
r8g.48xlarge	arm64
r8g.metal-24xl	arm64
r8g.metal-48xl	arm64
u7i-12tb.224xlarge	x86_64
u7in-16tb.224xlarge	x86_64
u7in-24tb.224xlarge	x86_64
u7in-32tb.224xlarge	x86_64
x2idn.16xlarge	x86_64
x2idn.24xlarge	x86_64
x2idn.32xlarge	x86_64
x2idn.metal	x86_64

Type d'instance	Architecture
x2iedn.8xlarge	x86_64
x2iedn.16xlarge	x86_64
x2iedn.24xlarge	x86_64
x2iedn.32xlarge	x86_64
x2iedn.metal	x86_64

Accelerated computing

Type d'instance	Architecture
g6.48xlarge	x86_64

Storage optimized

Type d'instance	Architecture
i4g.4xlarge	arm64
i4g.8xlarge	arm64
i4g.16xlarge	arm64
i4i.8xlarge	x86_64
i4i.12xlarge	x86_64
i4i.16xlarge	x86_64
i4i.24xlarge	x86_64
i4i.32xlarge	x86_64
i4i.metal	x86_64

Type d'instance	Architecture
im4gn.4xlarge	arm64
im4gn.8xlarge	arm64
im4gn.16xlarge	arm64

Conditions préalables pour les instances Linux

Pour garantir le ENA bon fonctionnement d'Express, mettez à jour les paramètres de votre instance Linux comme suit.

- Si votre instance utilise des trames jumbo, exécutez la commande suivante pour définir votre unité de transmission maximale (MTU) sur8900.

```
[ec2-user ~]$ sudo ip link set dev eth0 mtu 8900
```

- Augmentez la taille de la bague du récepteur (Rx) comme suit :

```
[ec2-user ~]$ ethtool -G device rx 8192
```

- Pour optimiser la bande passante ENA Express, configurez les limites de votre TCP file d'attente comme suit :

  1. Définissez la limite des TCP petites files d'attente à 1 Mo ou plus. Cela augmente la quantité de données mises en file d'attente pour transmission sur un socket.

     ```
     sudo sh -c 'echo 1048576 > /proc/sys/net/ipv4/tcp_limit_output_bytes'
     ```

  2. Désactivez les limites de files d'attente d'octets sur le périphérique eth si elles sont activées pour votre distribution Linux. Cela augmente le nombre de données mises en file d'attente pour la transmission au niveau de la file d'attente des périphériques.

     ```
     sudo sh -c 'for txq in /sys/class/net/eth0/queues/tx-*; do echo max > ${txq}/
     byte_queue_limits/limit_min; done'
     ```

> **Note**
>
> Le ENA pilote de la distribution Amazon Linux désactive les limites de file d'octets par défaut.

Régler les performances des paramètres ENA Express sur les instances Linux

Pour vérifier la configuration de votre instance Linux afin d'optimiser les performances d'ENAExpress, vous pouvez exécuter le script suivant, disponible sur le GitHub référentiel Amazon :

https://github.com/amzn/amzn-ec2-fra-utilities/blob/main/ena-express/ .sh check-ena-express-settings

Le script exécute une série de tests et suggère les modifications de configuration recommandées et requises.

Vérifiez les paramètres ENA Express de votre EC2 instance

Cette section explique comment afficher les informations ENA Express depuis AWS Management Console ou depuis le AWS CLI. Pour de plus amples informations, choisissez l'onglet qui correspond à la méthode que vous allez utiliser.

Console

Cet onglet explique comment trouver des informations sur vos paramètres ENA Express actuels dans le AWS Management Console.

Afficher les paramètres à partir de la liste de l'interface réseau

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation de gauche, choisissez Network Interfaces (Interfaces réseau).
3. Sélectionnez une interface réseau pour afficher les détails de cette instance. Vous pouvez cliquer sur le lien Network interface ID (ID d'interface réseau) pour ouvrir la page détaillée ou cocher la case sur le côté gauche de la liste pour afficher les détails dans le volet détaillé en bas de la page.
4. Dans la section Pièce jointe à l'interface réseau de l'onglet Détails ou de la page de détails, passez en revue les paramètres d'ENAExpress et d'ENAExpress UDP.

Afficher les paramètres depuis la liste des instances

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation de gauche, sélectionnez Instances.
3. Sélectionnez une instance pour afficher les détails de cette instance. Vous pouvez cliquer sur le lien Instance ID (ID d'instance) pour ouvrir la page détaillée ou cocher la case sur le côté gauche de la liste pour afficher les détails dans le volet détaillé en bas de la page.
4. Dans la section Interfaces réseau de l'onglet Réseau, faites défiler l'écran vers la droite pour consulter les paramètres d'ENAExpress et d'ENAExpress UDP.

AWS CLI

Cet onglet explique comment trouver des informations sur vos paramètres ENA Express actuels dans le AWS CLI.

Décrire des instances

Pour plus d'informations sur la configuration ENA Express pour les instances spécifiées, exécutez la describe-instancescommande dans le AWS CLI, comme suit. Cet exemple de commande renvoie une liste de configurations ENA Express pour les interfaces réseau associées à chacune des instances en cours d'exécution spécifiées par le `--instance-ids` paramètre.

```
[ec2-user ~]$ aws ec2 describe-instances --instance-
ids i-1234567890abcdef0 i-0598c7d356eba48d7 --query 'Reservations[*].Instances[*].
[InstanceId, NetworkInterfaces[*].Attachment.EnaSrdSpecification]'[
 [
  [
   "i-1234567890abcdef0",
   [
    {
     "EnaSrdEnabled": true,
     "EnaSrdUdpSpecification": {
      "EnaSrdUdpEnabled": false
     }
    }
   ]
  ]
 ],
 [
  [
```

```
   "i-0598c7d356eba48d7",
   [
    {
     "EnaSrdEnabled": true,
     "EnaSrdUdpSpecification": {
      "EnaSrdUdpEnabled": false
     }
    }
   ]
  ]
 ]
]
```

Décrire les interfaces réseau

Pour plus d'informations sur les paramètres ENA Express d'une interface réseau, exécutez la describe-network-interfacescommande AWS CLI comme suit :

```
[ec2-user ~]$ aws ec2 describe-network-interfaces
{
"NetworkInterfaces": [
{
 "Association": {
  ....IPs, DNS...
 },
 "Attachment": {
  "AttachTime": "2022-11-17T09:04:28+00:00",
  "AttachmentId": "eni-attach-0ab1c23456d78e9f0",
  "DeleteOnTermination": true,
  "DeviceIndex": 0,
  "NetworkCardIndex": 0,
  "InstanceId": "i-1234567890abcdef0",
  "InstanceOwnerId": "111122223333",
  "Status": "attached",
  "EnaSrdSpecification": {
   "EnaSrdEnabled": true,
   "EnaSrdUdpSpecification": {
    "EnaSrdUdpEnabled": true
   }
  }
 },
 ...
 "NetworkInterfaceId": "eni-1234567890abcdef0",
```

```
 "OwnerId": "111122223333",
 ...
}
]
}
```

PowerShell

Cet onglet explique comment trouver des informations sur vos paramètres ENA Express actuels à l'aide de PowerShell.

Décrire les interfaces réseau

Pour plus d'informations sur les paramètres ENA Express d'une interface réseau, exécutez le Get-EC2NetworkInterface Cmdletà l'aide PowerShell des outils suivants :

```
PS C:\> Get-EC2NetworkInterface -NetworkInterfaceId eni-0d1234e5f6a78901b | `
Select-Object `
    Association,
    NetworkInterfaceId,
    OwnerId,
    @{Name = 'AttachTime'; Expression = { $_.Attachment.AttachTime } },
    @{Name = 'AttachmentId'; Expression = { $_.Attachment.AttachmentId } },
    @{Name = 'DeleteOnTermination'; Expression =
 { $_.Attachment.DeleteOnTermination } },
    @{Name = 'NetworkCardIndex'; Expression = { $_.Attachment.NetworkCardIndex } },
    @{Name = 'InstanceId'; Expression = { $_.Attachment.InstanceId } },
    @{Name = 'InstanceOwnerId'; Expression = { $_.Attachment.InstanceOwnerId } },
    @{Name = 'Status'; Expression = { $_.Attachment.Status } },
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled } },
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled } }

Association         :
NetworkInterfaceId  : eni-0d1234e5f6a78901b
OwnerId             : 111122223333
AttachTime          : 6/11/2022 1:13:11 AM
AttachmentId        : eni-attach-0d1234e5f6a78901b
DeleteOnTermination : True
NetworkCardIndex    : 0
InstanceId          : i-0d1234e5f6a78901b
InstanceOwnerId     : 111122223333
```

```
Status              : attached
EnaSrdEnabled       : True
EnaSrdUdpEnabled    : False
```

Configurer les paramètres ENA Express pour votre EC2 instance

Vous pouvez configurer ENA Express pour les types d'EC2instances pris en charge sans avoir à installer de logiciel supplémentaire.

Cette section explique comment configurer ENA Express depuis AWS Management Console ou depuis le AWS CLI. Pour de plus amples informations, choisissez l'onglet qui correspond à la méthode que vous allez utiliser.

Console

Cet onglet explique comment gérer les paramètres ENA Express pour les interfaces réseau associées à une instance.

Gérer ENA Express à partir de la liste des interfaces réseau

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation de gauche, choisissez Network Interfaces (Interfaces réseau).
3. Sélectionnez une interface réseau qui doit être attachée à une instance. Vous pouvez cliquer sur le lien Network interface ID (ID d'interface réseau) pour ouvrir la page détaillée ou cocher la case sur le côté gauche de la liste.
4. Choisissez Gérer ENA Express dans le menu Action en haut à droite de la page. Cela ouvre la boîte de dialogue Manage ENA Express, avec l'ID d'interface réseau sélectionné et les paramètres actuels affichés.

   > **Note**
   >
   > Si l'interface réseau que vous avez sélectionnée n'est pas associée à une instance, cette action n'apparaît pas dans le menu.

5. Pour utiliser ENAExpress, cochez la case Activer.
6. Lorsque ENA Express est activé, vous pouvez configurer UDP les paramètres. Pour utiliser ENAExpress UDP, cochez la case Activer.
7. Pour enregistrer vos paramètres, choisissez Save (Enregistrer).

Gérer ENA Express à partir de la liste des instances

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation de gauche, sélectionnez Instances.
3. Sélectionnez l'instance que vous voulez gérer. Vous pouvez choisir Instance ID (ID d'instance) pour ouvrir la page détaillée ou cocher la case sur le côté gauche de la liste.
4. Sélectionnez Network interface (Interface réseau) pour configurer pour votre instance.
5. Choisissez Gérer ENA Express dans le menu Action en haut à droite de la page.
6. Pour configurer ENA Express pour une interface réseau attachée à votre instance, sélectionnez-la dans la liste des interfaces réseau.
7. Pour utiliser ENAExpress pour la connexion d'interface réseau sélectionnée, cochez la case Activer.
8. Lorsque ENA Express est activé, vous pouvez configurer UDP les paramètres. Pour utiliser ENAExpress UDP, cochez la case Activer.
9. Pour enregistrer vos paramètres, choisissez Save (Enregistrer).

Configurer ENA Express lorsque vous attachez une interface réseau à une EC2 instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation de gauche, choisissez Network Interfaces (Interfaces réseau).
3. Sélectionnez une interface réseau qui n'est pas attachée à une instance (l'état est Available (Disponible). Vous pouvez cliquer sur le lien Network interface ID (ID d'interface réseau) pour ouvrir la page détaillée ou cocher la case sur le côté gauche de la liste.
4. Sélectionnez l'instance avec laquelle vous souhaitez effectuer l'attachement.
5. Pour utiliser ENAExpress après avoir connecté l'interface réseau à l'instance, cochez la case Activer.
6. Lorsque ENA Express est activé, vous pouvez configurer UDP les paramètres. Pour utiliser ENAExpress UDP, cochez la case Activer.
7. Pour associer l'interface réseau à l'instance et enregistrer vos paramètres ENA Express, choisissez Attach.

AWS CLI

Cet onglet explique comment configurer les paramètres ENA Express dans le AWS CLI.

Configurer ENA Express lorsque vous connectez une interface réseau

Pour configurer ENA Express lorsque vous attachez une interface réseau à une instance, exécutez la attach-network-interfacecommande dans le AWS CLI, comme indiqué dans les exemples suivants :

Exemple 1 : utiliser ENA Express pour le TCP trafic, mais pas pour le UDP trafic

Dans cet exemple, nous configurons `EnaSrdEnabled` comme true et nous autorisons`EnaSrdUdpEnabled` par défaut sur false.

```
[ec2-user ~]$ aws ec2 attach-network-interface --network-interface-
id eni-0123f4567890a1b23 --instance-id i-0f1a234b5cd67e890 --device-index 1 --ena-
srd-specification 'EnaSrdEnabled=true'
{
"AttachmentId": "eni-attach-012c3d45e678f9012"
}
```

Exemple 2 : utiliser ENA Express à la fois pour TCP le trafic et UDP le trafic

Dans cet exemple, nous configurons `EnaSrdEnabled` et `EnaSrdUdpEnabled` comme true.

```
[ec2-user ~]$ aws ec2 attach-network-interface --network-interface-
id eni-0123f4567890a1b23 --instance-id i-0f1a234b5cd67e890 --device-index 1 --ena-
srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
{
"AttachmentId": "eni-attach-012c3d45e678f9012"
}
```

Mettre à jour les paramètres ENA Express pour votre connexion d'interface réseau

Pour mettre à jour les paramètres ENA Express d'une interface réseau attachée à une instance, exécutez la modify-network-interface-attributecommande dans le AWS CLI, comme indiqué dans les exemples suivants :

Exemple 1 : utiliser ENA Express pour le TCP trafic, mais pas pour le UDP trafic

Dans cet exemple, nous configurons `EnaSrdEnabled` comme true, et nous autorisons `EnaSrdUdpEnabled` par défaut sur false si cela n'a jamais été défini auparavant.

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --network-interface-
id eni-0123f4567890a1b23 --ena-srd-specification 'EnaSrdEnabled=true'
```

Exemple 2 : utiliser ENA Express à la fois pour TCP le trafic et UDP le trafic

Dans cet exemple, nous configurons `EnaSrdEnabled` et `EnaSrdUdpEnabled` comme true.

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --
network-interface-id eni-0123f4567890a1b23 --ena-srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
```

Exemple 3 : arrêter d'utiliser ENA Express pour le UDP trafic

Dans cet exemple, nous configurons `EnaSrdUdpEnabled` comme false.

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --
network-interface-id eni-0123f4567890a1b23 --ena-srd-specification
 'EnaSrdUdpSpecification={EnaSrdUdpEnabled=false}'
```

PowerShell

Cet onglet explique comment configurer les paramètres ENA Express à l'aide de PowerShell.

Configurer ENA Express lorsque vous connectez une interface réseau

Pour configurer les paramètres ENA Express pour une interface réseau, exécutez le Add-EC2NetworkInterface Cmdletavec les outils pour, PowerShell comme indiqué dans les exemples suivants :

Exemple 1 : utiliser ENA Express pour le TCP trafic, mais pas pour le UDP trafic

Dans cet exemple, nous configurons `EnaSrdEnabled` comme true et nous autorisons`EnaSrdUdpEnabled` par défaut sur false.

```
PS C:\> Add-EC2NetworkInterface `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-InstanceId i-0f1a234b5cd67e890 `
-DeviceIndex 1 `
-EnaSrdSpecification_EnaSrdEnabled $true
```

```
eni-attach-012c3d45e678f9012
```

Exemple 2 : utiliser ENA Express à la fois pour TCP le trafic et UDP le trafic

Dans cet exemple, nous configurons `EnaSrdEnabled` et `EnaSrdUdpEnabled` comme true.

```
PS C:\> Add-EC2NetworkInterface `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-InstanceId i-0f1a234b5cd67e890 `
-DeviceIndex 1 `
-EnaSrdSpecification_EnaSrdEnabled $true `
-EnaSrdUdpSpecification_EnaSrdUdpEnabled $true

eni-attach-012c3d45e678f9012
```

Mettre à jour les paramètres ENA Express pour votre connexion d'interface réseau

Pour mettre à jour les paramètres ENA Express d'une interface réseau attachée à une instance, exécutez la Add-EC2NetworkInterface Cmdletcommande dans les outils pour PowerShell, comme indiqué dans les exemples suivants :

Exemple 1 : utiliser ENA Express pour le TCP trafic, mais pas pour le UDP trafic

Dans cet exemple, nous configurons `EnaSrdEnabled` comme true, et nous autorisons `EnaSrdUdpEnabled` par défaut sur false si cela n'a jamais été défini auparavant.

```
PS C:\> Edit-EC2NetworkInterfaceAttribute `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-EnaSrdSpecification_EnaSrdEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List

NetworkInterfaceId : eni-0123f4567890a1b23
EnaSrdEnabled      : True
EnaSrdUdpEnabled   : False
```

Exemple 2 : utiliser ENA Express à la fois pour TCP le trafic et UDP le trafic

Dans cet exemple, nous configurons `EnaSrdEnabled` et `EnaSrdUdpEnabled` comme true.

```
PS C:\> Edit-EC2NetworkInterfaceAttribute `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-EnaSrdSpecification_EnaSrdEnabled $true `
-EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List

NetworkInterfaceId : eni-0123f4567890a1b23
EnaSrdEnabled      : True
EnaSrdUdpEnabled   : True
```

Exemple 3 : arrêter d'utiliser ENA Express pour le UDP trafic

Dans cet exemple, nous configurons `EnaSrdUdpEnabled` comme false.

```
PS C:\> Edit-EC2NetworkInterfaceAttribute `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $false ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List

NetworkInterfaceId : eni-0123f4567890a1b23
EnaSrdEnabled      : True
EnaSrdUdpEnabled   : False
```

Configurer ENA Express au lancement

Vous pouvez utiliser l'une des méthodes suivantes pour configurer ENA Express directement lorsque vous lancez une instance. Les liens spécifiés renvoient aux AWS Management Console instructions relatives à ces méthodes.

- Assistant de lancement d'instance : vous pouvez configurer ENA Express au lancement à l'aide de l'assistant de lancement d'instance. Pour plus d'informations, consultez la section Configuration réseau avancée dans l'assistant Paramètres réseau de lancement de l'instance.
- Modèle de lancement : vous pouvez configurer ENA Express au lancement lorsque vous utilisez un modèle de lancement. Pour plus d'informations, consultez la Création d'un modèle de EC2 lancement Amazon page, puis développez la section Paramètres réseau et consultez la section Configuration réseau avancée.

Mise en réseau améliorée avec l'interface Intel 82599 VF

Pour les types d'EC2instances qui ne sont pas basés sur le système AWS Nitro, l'interface Intel 82599 Virtual Function (VF) fournit des fonctionnalités réseau améliorées. L'interface utilise le `ixgbevf` pilote Intel.

Les onglets suivants indiquent comment vérifier le pilote de l'adaptateur réseau installé pour le système d'exploitation de votre instance.

Linux

pilote d'interface réseau Linux

Utilisez la commande suivante pour vérifier que le module est utilisé sur une interface particulière, en remplaçant le nom de l'interface par celui que vous voulez contrôler. Si vous utilisez une seule interface (par défaut), ce sera `eth0`. Si le système d'exploitation prend en charge les noms de réseau prévisibles, il peut s'agir d'un nom tel que `ens5`.

Dans l'exemple suivant, le module `ixgbevf` n'est pas chargé, car le pilote affiché est `vif`.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
```

```
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Dans cet exemple, le module `ixgbevf` est chargé. La mise en réseau améliorée est correctement configurée pour cette instance.

```
[ec2-user ~]$ ethtool -i eth0
driver: ixgbevf
version: 4.0.3
firmware-version: N/A
bus-info: 0000:00:03.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: no
supports-register-dump: yes
supports-priv-flags: no
```

Windows

Adaptateur réseau Windows

Pour vérifier que le pilote est installé, connectez-vous à votre instance et ouvrez le Gestionnaire de périphériques. Vous devriez voir la `Intel(R) 82599 Virtual Function` liste sous Adaptateurs réseau.

Table des matières

Préparez votre instance pour une mise en réseau améliorée

Pour vous préparer à la mise en réseau améliorée à l'aide de l'interface Intel 82599 VF, configurez l'instance comme suit :

- Effectuez votre sélection parmi les types d'instances pris en charge suivants : C3, C4, D2, I2, M4 (à l'exception de `m4.16xlarge`) et R3.
- Vérifiez que l'instance a une connectivité Internet.
- Si vous avez des données importantes sur l'instance que vous souhaitez conserver, vous devez les sauvegarder dès maintenant en créant un AMI à partir de votre instance. La mise à jour des noyaux et des modules noyau, ainsi que l'activation de l'attribut `sriovNetSupport`, peuvent rendre les instances incompatibles ou les systèmes d'exploitation inaccessibles. Si cela se produit et que vous disposez d'une sauvegarde récente, vos données continueront d'être conservées.
- Instances Linux : lancez l'instance à HVM AMI partir d'une version 2.6.32 ou ultérieure du noyau Linux. Les modules requis pour une mise en réseau améliorée HVM AMIs sont installés sur les versions les plus récentes d'Amazon Linux et les attributs requis sont définis. Par conséquent, si vous lancez une instance EBS soutenue par Amazon et compatible avec la mise en réseau améliorée à l'aide d'un Amazon Linux actuel HVMAMI, la mise en réseau améliorée est déjà activée pour votre instance.

  > **Warning**
  >
  > La mise en réseau améliorée n'est prise en charge que pour HVM les instances. L'activation de la mise en réseau améliorée avec une instance de paravirtualisation peut la rendre inaccessible. La définition de cet attribut sans le module ou la version de module approprié peut rendre votre instance inaccessible.

- Instances Windows : lancez l'instance à partir d'un système 64 bits HVMAMI. Vous ne pouvez pas activer la mise en réseau améliorée sur Windows Server 2008. La mise en réseau améliorée est déjà activée pour Windows Server 2012 R2, Windows Server 2016 et versions ultérieuresAMIs. Windows Server 2012 R2 inclut le pilote Intel 1.0.15.3, et nous vous recommandons de le mettre à jour à l'aide de l'utilitaire Pnputil.exe afin d'obtenir la version la plus récente.
- AWS CloudShellUtilisez-le depuis ou installez et configurez le AWS CLIou AWS Tools for Windows PowerShellsur n'importe quel ordinateur de votre choix, de préférence sur votre ordinateur de bureau ou portable local. AWS Management Console Pour plus d'informations, consultez la section Accédez à Amazon EC2 du Guide de l'utilisateur AWS CloudShell. La mise en réseau améliorée ne peut pas être gérée depuis la EC2 console Amazon.

Tester l'activation de réseaux améliorés

Vérifiez que l'`sriovNetSupport`attribut est défini.

Attribut d'instance (sriovNetSupport)

Pour vérifier si l'attribut de mise en réseau améliorée `sriovNetSupport` est défini sur une instance, utilisez l'une des commandes suivantes. Si l'attribut est défini, la valeur est`simple`.

- describe-instance-attribute (AWS CLI) (AWS CLI/AWS CloudShell)

```
aws ec2 describe-instance-attribute --instance-id instance_id --attribute
 sriovNetSupport
```

- Get-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Get-EC2InstanceAttribute -InstanceId instance-id -Attribute sriovNetSupport
```

Attribut d'image (sriovNetSupport)

Pour vérifier si l'`sriovNetSupport`attribut réseau amélioré est AMI déjà défini, utilisez l'une des commandes suivantes. Si l'attribut est défini, la valeur est`simple`.

- describe-images (AWS CLI)

```
aws ec2 describe-images --image-id ami_id --query "Images[].SriovNetSupport"
```

- Get-EC2Image (AWS Tools for Windows PowerShell)

```
(Get-EC2Image -ImageId ami-id).SriovNetSupport
```

Activer les réseaux améliorés sur une instance

La procédure que vous utilisez dépend du système d'exploitation de l'instance.

> **Warning**
>
> Il n'existe aucun moyen de désactiver l'attribut de mise en réseau améliorée une fois que vous l'avez activé.

Amazon Linux

Le `ixgbevf` module requis pour HVM AMIs une mise en réseau améliorée est installé sur les versions les plus récentes d'Amazon Linux et les `sriovNetSupport` attributs requis sont définis. Par conséquent, si vous lancez un type d'instance à l'aide d'un Amazon Linux actuel HVMAMI, la mise en réseau améliorée est déjà activée pour votre instance. Pour de plus amples informations, veuillez consulter Tester l'activation de réseaux améliorés.

Si vous avez lancé votre instance à l'aide d'un ancien Amazon Linux AMI et que la mise en réseau améliorée n'est pas encore activée, suivez la procédure suivante pour activer la mise en réseau améliorée.

Pour activer la mise en réseau améliorée

1. Connectez-vous à votre instance.
2. Depuis l'instance, exécutez la commande suivante pour mettre à jour votre instance avec le noyau et les modules noyau les plus récents, y compris `ixgbevf` :

   ```
   [ec2-user ~]$ sudo yum update
   ```

3. Depuis votre ordinateur local, redémarrez votre instance à l'aide de la EC2 console Amazon ou de l'une des commandes suivantes : reboot-instances(AWS CLI), Restart-EC2Instance(AWS Tools for Windows PowerShell).
4. Connectez-vous à nouveau à votre instance et vérifiez que le module `ixgbevf` est installé et possède la version minimale recommandée à l'aide de la commande modinfo ixgbevf depuis Tester l'activation de réseaux améliorés.
5. [instance EBS sauvegardée] Depuis votre ordinateur local, arrêtez l'instance à l'aide de la EC2 console Amazon ou de l'une des commandes suivantes : stop-instances(AWS CLI), Stop-EC2Instance(AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez l'arrêter dans la AWS OpsWorks console afin que son état reste synchronisé.

   [Instance basée sur le stockage d'instance] Vous ne pouvez pas arrêter l'instance pour modifier l'attribut. Passez plutôt à la procédure suivante.
6. Depuis votre ordinateur local, activez l'attribut de mise en réseau améliorée à l'aide de l'une des commandes suivantes:

AWS CLI

modify-instance-attribute (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support
 simple
```

PowerShell

Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
```

7. (Facultatif) Créez un AMI à partir de l'instance, comme décrit dansCréez un compte soutenu EBS par Amazon AMI. AMIhérite de l'attribut réseau amélioré de l'instance. Vous pouvez donc l'utiliser AMI pour lancer une autre instance avec la mise en réseau améliorée activée par défaut.
8. Depuis votre ordinateur local, démarrez l'instance à l'aide de la EC2 console Amazon ou de l'une des commandes suivantes : start-instances(AWS CLI), Start-EC2Instance(AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez démarrer l'instance dans la AWS OpsWorks console afin que son état reste synchronisé.
9. Connectez-vous à votre instance et vérifiez que le module `ixgbevf` est installé et chargé sur votre interface réseau à l'aide de la commande ethtool -i eth***n*** depuis Tester l'activation de réseaux améliorés.

Pour activer la mise en réseau améliorée (instances basées sur le stockage d'instance)

Suivez la procédure précédente jusqu'à l'étape à laquelle vous avez arrêté l'instance. Créez un nouveau AMI comme décrit dansCréation d'une instance sauvegardée en magasin AMI, en veillant à activer l'attribut réseau amélioré lorsque vous enregistrez leAMI.

AWS CLI

register-image (AWS CLI/AWS CloudShell)

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Ubuntu

Avant de commencer, vérifiez si la mise en réseau améliorée est déjà activée sur votre instance.

Le Quick Start Ubuntu HVM AMIs inclut les pilotes nécessaires pour améliorer la mise en réseau. Si vous disposez d'une version du fichier `ixgbevf` antérieure à 2.16.4, vous pouvez installer le package noyau `linux-aws` pour obtenir les pilotes de mise en réseau améliorée les plus récents.

La procédure suivante fournit les étapes générales pour la compilation du module `ixgbevf` sur une instance Ubuntu.

Pour installer le package du noyau **`linux-aws`**

1. Connectez-vous à votre instance.
2. Mettez à jour le cache du package et les packages.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

> **Important**
>
> Si, lors d'une mise à jour, vous êtes invité à installer `grub`, utilisez `/dev/xvda` pour installer `grub`, puis choisissez de conserver la version actuelle de `/boot/grub/menu.lst`.

Autres distributions Linux

Avant de commencer, vérifiez si la mise en réseau améliorée est déjà activée sur votre instance. Le dernier Quick Start HVM AMIs inclut les pilotes nécessaires pour améliorer la mise en réseau. Vous n'avez donc pas besoin d'effectuer d'étapes supplémentaires.

La procédure suivante fournit les étapes générales pour si vous devez activer la mise en réseau améliorée avec l'interface Intel 82599 VF sur une distribution Linux autre qu'Amazon Linux ou Ubuntu. Pour plus d'informations, telles que la syntaxe détaillée des commandes, les emplacements de fichier ou la prise en charge des packages et des outils, consultez la documentation spécifique de votre distribution Linux.

Pour activer la mise en réseau améliorée sur Linux

1. Connectez-vous à votre instance.
2. Téléchargez la source pour le module `ixgbevf` sur votre instance depuis Sourceforge, à l'adresse https://sourceforge.net/projects/e1000/files/ixgbevf%20stable/.

   Les versions d'`ixgbevf` antérieures à 2.16.4, notamment la 2.14.2, ne sont pas générées correctement sur certaines distributions Linux, y compris certaines versions d'Ubuntu.
3. Compilez et installez le module `ixgbevf` sur votre instance.

   > **Warning**
   >
   > Si vous compilez le module `ixgbevf` pour votre noyau actuel, puis mettez à niveau le noyau sans générer à nouveau le pilote du nouveau noyau, il se peut que votre système retourne au module `ixgbevf` spécifique à la distribution lors du prochain redémarrage. Cela peut rendre votre système inaccessible si la version propre à la distribution n'est pas compatible avec la mise en réseau améliorée.
4. Exécutez la commande sudo depmod pour mettre à jour les dépendances du module.
5. Mettez à jour `initramfs` sur votre instance pour garantir que le nouveau module se charge au démarrage.
6. Déterminez si par défaut votre système utilise des noms d'interface réseau prévisibles. Les systèmes qui utilisent systemd ou udev version 197 ou supérieure peuvent renommer les périphériques Ethernet et ne garantissent pas qu'une seule interface réseau sera nommée `eth0`. Ce comportement peut entraîner des problèmes de connexion à votre instance. Pour plus d'informations et pour voir les autres options de configuration, consultez la section sur les noms d'interface réseau prévisibles sur le site web de freedesktop.org.

   a. Vous pouvez vérifier les udev versions systemd ou sur les systèmes RPM basés sur les systèmes à l'aide de la commande suivante :

   ```
   [ec2-user ~]$ rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
   systemd-208-11.el7_0.2.x86_64
   ```

   Dans l'exemple Red Hat Enterprise Linux 7 ci-dessus, la version systemd est 208, de sorte que les noms d'interface réseau prévisibles doivent être désactivés.

b. Désactivez les noms d'interface réseau prévisibles en ajoutant l'option `net.ifnames=0` à la ligne `GRUB_CMDLINE_LINUX` dans `/etc/default/grub`.

```
[ec2-user ~]$ sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /
etc/default/grub
```

c. Générez à nouveau le fichier de configuration grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. [instance EBS sauvegardée] Depuis votre ordinateur local, arrêtez l'instance à l'aide de la EC2 console Amazon ou de l'une des commandes suivantes : stop-instances (AWS CLI/AWS CloudShell), Stop-EC2Instance().AWS Tools for Windows PowerShell Si votre instance est gérée par AWS OpsWorks, vous devez l'arrêter dans la AWS OpsWorks console afin que son état reste synchronisé.

   [Instance basée sur le stockage d'instance] Vous ne pouvez pas arrêter l'instance pour modifier l'attribut. Passez plutôt à la procédure suivante.

8. Depuis votre ordinateur local, activez l'attribut de mise en réseau améliorée à l'aide de l'une des commandes suivantes:

   AWS CLI

   modify-instance-attribute (AWS CLI/AWS CloudShell)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support
    simple
   ```

   PowerShell

   Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

   ```
   Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
   ```

9. (Facultatif) Créez un AMI à partir de l'instance, comme décrit dansCréez un compte soutenu EBS par Amazon AMI. AMIhérite de l'attribut réseau amélioré de l'instance. Vous pouvez donc l'utiliser AMI pour lancer une autre instance avec la mise en réseau améliorée activée par défaut.

   Si le système d'exploitation de votre instance contient un `/etc/udev/rules.d/70-persistent-net.rules` fichier, vous devez le supprimer avant de créer leAMI. Ce fichier

contient l'MACadresse de l'adaptateur Ethernet de l'instance d'origine. Si une autre instance démarre avec ce fichier, le système d'exploitation ne pourra pas trouver le périphérique et il se peut qu'`eth0` échoue, entraînant des problèmes de démarrage. Ce fichier est régénéré lors du cycle de démarrage suivant, et toutes les instances lancées à partir de ce AMI dernier créent leur propre version du fichier.

10. Depuis votre ordinateur local, démarrez l'instance à l'aide de la EC2 console Amazon ou de l'une des commandes suivantes : start-instances(AWS CLI), Start-EC2Instance(AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez démarrer l'instance dans la AWS OpsWorks console afin que son état reste synchronisé.
11. (Facultatif) Connectez-vous à votre instance et vérifiez que le module est installé.

Pour activer les réseaux améliorés (instances basées sur le stockage d'instance)

Suivez la procédure précédente jusqu'à l'étape à laquelle vous avez arrêté l'instance. Créez un nouveau AMI comme décrit dansCréation d'une instance sauvegardée en magasin AMI, en veillant à activer l'attribut réseau amélioré lorsque vous enregistrez leAMI.

AWS CLI

register-image (AWS CLI/AWS CloudShell)

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Windows

Si vous avez lancé votre instance et qu'elle n'a pas la mise en réseau déjà activée, vous devez télécharger et installer le pilote de la carte réseau requis sur votre instance, puis définir l'attribut d'instance `sriovNetSupport` pour activer la mise en réseau améliorée. Vous ne pouvez activer cet attribut que sur les types d'instance pris en charge. Pour de plus amples informations, veuillez consulter Mise en réseau améliorée sur les EC2 instances Amazon.

> **Important**
>
> Pour consulter les dernières mises à jour des pilotes sous WindowsAMIs, consultez l'historique des AMI versions de Windows dans le manuel AWS Windows AMI Reference.

Pour activer la mise en réseau améliorée

1. Connectez-vous à votre instance en tant qu'administrateur local.
2. [Windows Server 2016 et versions ultérieures] Exécutez le PowerShell script de EC2 lancement suivant pour configurer l'instance une fois le pilote installé.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

> **Important**
>
> Le mot de passe administrateur est réinitialisé lorsque vous activez le script de EC2 lancement de l'instance d'initialisation. Vous pouvez modifier le fichier de configuration pour désactiver la réinitialisation du mot de passe administrateur en le spécifiant dans les paramètres des tâches d'initialisation.

3. À partir de l'instance, téléchargez le pilote de la carte réseau Intel adapté à votre système d'exploitation :

   - Windows Server 2022

     Visitez la page de téléchargement et téléchargez `Wired_driver_`*`version`*`_x64.zip`.
   - Windows Server 2019 notamment pour Server version 1809 ou ultérieure*

     Visitez la page de téléchargement et téléchargez `Wired_driver_`*`version`*`_x64.zip`.
   - Windows Server 2016 notamment pour Server version 1803 ou antérieure*

     Visitez la page de téléchargement et téléchargez `Wired_driver_`*`version`*`_x64.zip`.
   - Windows Server 2012 R2

     Visitez la page de téléchargement et téléchargez `Wired_driver_`*`version`*`_x64.zip`.
   - Windows Server 2012

Visitez la page de téléchargement et téléchargez `Wired_driver_version_x64.zip`.

- Windows Server 2008 R2

  Visitez la page de téléchargement et téléchargez `PROWinx64Legacy.exe`.

*Les versions 1803 et antérieures de Server, ainsi que les versions 1809 et ultérieures, ne sont pas spécifiquement traitées dans les pages relatives aux pilotes et logiciels Intel.

4. Installez le pilote de la carte réseau Intel adapté à votre système d'exploitation :

   - Windows Server 2008 R2

     1. Dans le dossier Téléchargements, localisez le fichier `PROWinx64Legacy.exe` et renommez-le `PROWinx64Legacy.zip`.
     2. Extrayez le contenu du fichier `PROWinx64Legacy.zip`.
     3. Ouvrez la ligne de commande, accédez au dossier extrait et exécutez la commande suivante pour utiliser l'`pnputil`utilitaire afin d'ajouter et d'installer le INF fichier dans le magasin de pilotes.

        ```
        C:\> pnputil -a PROXGB\Winx64\NDIS62\vxn62x64.inf
        ```

   - Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 et Windows Server 2012

     1. Dans le dossier Téléchargements, extrayez le contenu du fichier `Wired_driver_version_x64.zip`.
     2. Dans le dossier extrait, recherchez le fichier `Wired_driver_version_x64.exe` et renommez-le `Wired_driver_version_x64.zip`.
     3. Extrayez le contenu du fichier `Wired_driver_version_x64.zip`.
     4. Ouvrez la ligne de commande, accédez au dossier extrait et exécutez l'une des commandes suivantes pour utiliser l'`pnputil`utilitaire afin d'ajouter et d'installer le INF fichier dans le magasin de pilotes.

        - Windows Server 2022

          ```
          C:\> pnputil -i -a PROXGB\Winx64\WS2022\vxs.inf
          ```

        - Windows Server 2019

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS68\vxn68x64.inf
```

- Windows Server 2016

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS65\vxn65x64.inf
```

- Windows Server 2012 R2

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS64\vxn64x64.inf
```

- Windows Server 2012

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS63\vxn63x64.inf
```

5. Depuis votre ordinateur local, activez l'attribut de mise en réseau améliorée à l'aide de l'une des commandes suivantes:

   AWS CLI

   modify-instance-attribute (AWS CLI/AWS CloudShell)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support
    simple
   ```

   PowerShell

   Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

   ```
   Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
   ```

6. (Facultatif) Créez un AMI à partir de l'instance, comme décrit dansCréez un compte soutenu EBS par Amazon AMI. AMIhérite de l'attribut réseau amélioré de l'instance. Vous pouvez donc l'utiliser AMI pour lancer une autre instance avec la mise en réseau améliorée activée par défaut.
7. Depuis votre ordinateur local, démarrez l'instance à l'aide de la EC2 console Amazon ou de l'une des commandes suivantes : start-instances(AWS CLI), Start-EC2Instance(AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez démarrer l'instance dans la AWS OpsWorks console afin que son état reste synchronisé.

Résoudre les problèmes de connectivité

Si vous perdez la connexion tout en activant la mise en réseau améliorée, il se peut que le module `ixgbevf` ne soit pas compatible avec le noyau. Essayez d'installer la version du module `ixgbevf` fournie avec la distribution de Linux pour votre instance.

Si vous activez la mise en réseau améliorée pour une instance PVAMI, cela peut rendre votre instance inaccessible.

Pour plus d'informations, consultez Comment activer et configurer la mise en réseau améliorée sur mes EC2 instances ?

Surveillez les performances du réseau pour ENA les paramètres de votre EC2 instance

Le pilote Elastic Network Adapter (ENA) publie les mesures de performance du réseau à partir des instances où elles sont activées. Vous pouvez utiliser ces métriques pour résoudre les problèmes de performances d'instance, choisir la taille d'instance appropriée pour une charge de travail, planifier les activités de mise à l'échelle de manière proactive et comparer les applications afin de déterminer si elles optimisent les performances disponibles sur une instance.

Amazon EC2 définit les limites maximales du réseau au niveau de l'instance afin de garantir une expérience réseau de haute qualité, notamment des performances réseau cohérentes quelle que soit la taille des instances. AWS fournit les valeurs maximales suivantes pour chaque instance :

- Capacité de bande passante : chaque EC2 instance dispose d'une bande passante maximale pour le trafic entrant et sortant agrégé, en fonction du type et de la taille de l'instance. Certaines instances utilisent un mécanisme de crédit I/O réseau pour attribuer la bande passante réseau en fonction de l'utilisation moyenne de la bande passante. Amazon dispose EC2 également d'une bande passante maximale pour le trafic vers Internet AWS Direct Connect et vers Internet. Pour de plus amples informations, veuillez consulter Bande passante réseau des EC2 instances Amazon.
- P acket-per-second (PPS) performance — Chaque EC2 instance possède des PPS performances maximales, en fonction du type et de la taille de l'instance.
- Connexions suivies : le groupe de sécurité assure le suivi de chaque connexion établie pour s'assurer que les paquets de retour sont livrés comme prévu. Il existe un nombre maximal de connexions qui peuvent être suivies par instance. Pour plus d'informations, consultez Suivi des connexions du groupe de EC2 sécurité Amazon.

- Accès au service local par lien : Amazon EC2 fournit un maximum PPS par interface réseau pour le trafic vers des services tels que le DNS service, le service de métadonnées d'instance et le service Amazon Time Sync.

Lorsque le trafic réseau d'une instance dépasse un maximum, AWS façonne le trafic qui dépasse le maximum en mettant en file d'attente puis en supprimant les paquets réseau. Vous pouvez surveiller lorsque le trafic dépasse un maximum à l'aide des métriques de performances réseau. Ces métriques vous informent en temps réel de l'impact sur le trafic réseau et des éventuels problèmes de performances réseau.

Table des matières

Prérequis

Instances Linux

- Installez la version 2.2.10 ou ultérieure du ENA pilote. Pour vérifier la version installée, utilisez la commande ethtool. Dans l'exemple suivant, la version répond aux exigences minimales.

```
[ec2-user ~]$ ethtool -i eth0 | grep version
version: 2.2.10
```

  Pour mettre à niveau votre ENA pilote, consultez la section Mise en réseau améliorée.
- Pour importer ces métriques sur Amazon CloudWatch, installez l' CloudWatch agent. Pour plus d'informations, consultez la section Collecter les indicateurs de performance du réseau dans le guide de CloudWatch l'utilisateur Amazon.
- Pour prendre en charge les `conntrack_allowance_available` métriques, installez la version 2.8.1 du ENA pilote.

instances Windows

- Installez la version 2.2.2 ou ultérieure du ENA pilote. Pour vérifier la version installée, utilisez le Gestionnaire de périphériques comme suit.
  1. Ouvrez le Gestionnaire de périphériques en exécutant `devmgmt.msc`.
  2. Développez Network Adapters (Cartes réseau).
  3. Sélectionnez Amazon Elastic Network Adapter, puis Properties (Propriétés).
  4. Sous l'onglet Driver (Pilote), recherchez Driver Version (Version du pilote).

  Pour mettre à niveau votre ENA pilote, consultez la section Mise en réseau améliorée.
- Pour importer ces métriques sur Amazon CloudWatch, installez l' CloudWatch agent. Pour plus d'informations, consultez la section Collecter des métriques réseau avancées dans le guide de CloudWatch l'utilisateur Amazon.

Indicateurs pour le ENA conducteur

Le ENA pilote fournit les métriques suivantes à l'instance en temps réel. Ces métriques fournissent le nombre cumulé de paquets mis en file d'attente ou ignorés sur chaque interface réseau depuis la dernière réinitialisation du pilote.

Métrique	Description	Pris en charge sur
`bw_in_allowance_exceeded`	Nombre de paquets mis en file d'attente ou ignorés flottee que la bande passante agrégée entrante a dépassé le maximum de l'instance.	Tous les types d'instances
`bw_out_allowance_exceeded`	Nombre de paquets mis en file d'attente ou ignorés flottee que la bande passante agrégée sortante a dépassé le maximum de l'instance.	Tous les types d'instances
`conntrack_allowance_exceeded`	Nombre de paquets ignorés flottee que le suivi des connexions a dépassé le maximum de	Tous les types d'instances

Métrique	Description	Pris en charge sur
	l'instance et que de nouvelles connexions n'ont pas pu être établies. Cela peut entraîner une perte de paquets pour le trafic vers ou en provenance de l'instance.	
`conntrack_allowance_available`	Nombre de connexions suivies pouvant être établies par l'instance avant d'atteindre l'allocation Connexions suivies de ce type d'instance.	Instances créées uniquement sur le système AWS Nitro
`linklocal_allowance_exceeded`	Le nombre de paquets abandonnés parce que le PPS trafic vers les services proxy locaux a dépassé le maximum pour l'interface réseau. Cela a un impact sur le trafic vers le DNS service, le service de métadonnées d'instance et le service Amazon Time Sync.	Tous les types d'instances
`pps_allowance_exceeded`	Le nombre de paquets mis en file d'attente ou abandonnés parce que le mode bidirectionnel PPS a dépassé le maximum pour l'instance. Cette limite compte également les pertes de fragments de sortie supérieures à 1 024 PPS par. ENI	Tous les types d'instances

Afficher les métriques de performances réseau de votre instance

La procédure que vous utilisez dépend du système d'exploitation de l'instance.

Instances Linux

Vous pouvez publier des métriques dans vos outils favoris pour visualiser les données métriques. Par exemple, vous pouvez publier les statistiques sur Amazon à CloudWatch l'aide de l' CloudWatch agent. L'agent vous permet de sélectionner des métriques individuelles et de contrôler la publication.

Vous pouvez également utiliser la commande ethtool pour récupérer les métriques de chaque interface réseau, telles que eth0, comme suit.

```
[ec2-user ~]$ ethtool -S eth0
     bw_in_allowance_exceeded: 0
     bw_out_allowance_exceeded: 0
     pps_allowance_exceeded: 0
     conntrack_allowance_exceeded: 0
     linklocal_allowance_exceeded: 0
     conntrack_allowance_available: 136812
```

instances Windows

Vous pouvez afficher les métriques à l'aide de n'importe quel consommateur de compteurs de performances Windows. Les données peuvent être analysées en fonction du EnaPerfCounters manifeste. Il s'agit d'un XML fichier qui définit le fournisseur de compteurs de performance et ses contreensembles.

Pour installer le manifeste

Si vous avez lancé l'instance à l'aide d'un fichier AMI contenant ENA le pilote 2.2.2 ou version ultérieure, ou si vous avez utilisé le script d'installation du package de pilotes pour le ENA pilote 2.2.2, le manifeste est déjà installé. Pour installer le manifeste manuellement, procédez comme suit :

1. Supprimez le manifeste existant à l'aide de la commande suivante :

   ```
   unlodctr /m:EnaPerfCounters.man
   ```

2. Copiez `EnaPerfCounters.man`, le fichier manifeste, du package d'installation du pilote vers `%SystemRoot%\System32\drivers`.
3. Installez le nouveau manifeste à l'aide de la commande suivante :

   ```
   lodctr /m:EnaPerfCounters.man
   ```

Pour afficher les métriques à l'aide de Performance Monitor

1. Ouvrez Performance Monitor.
2. Appuyez sur Ctrl+N pour ajouter de nouveaux compteurs.
3. Choisissez ENAPackets Shaping dans la liste.
4. Sélectionnez les instances à surveiller, puis Add (Ajouter).
5. Choisissez OK.

Métriques pour ENA Express

ENAExpress est alimenté par la technologie AWS Scalable Reliable Datagram (SRD). SRDest un protocole de transport réseau à hautes performances qui utilise le routage dynamique pour augmenter le débit et minimiser la latence de queue. Si vous avez activé ENA Express pour les pièces jointes de l'interface réseau à la fois sur l'instance d'envoi et sur l'instance de réception, vous pouvez utiliser les métriques ENA Express pour vous assurer que vos instances tirent pleinement parti des améliorations de performances apportées par la SRD technologie. Par exemple :

- Évaluez vos ressources pour vous assurer qu'elles disposent d'une capacité suffisante pour établir davantage de SRD connexions.
- Identifiez les problèmes potentiels qui empêchent l'utilisation des paquets sortants éligiblesSRD.
- Calculez le pourcentage de trafic sortant utilisé par SRD l'instance.
- Calculez le pourcentage du trafic entrant utilisé par SRD l'instance.

> **Note**
>
> Pour produire des métriques, utilisez la version 2.8 ou supérieure du pilote.

Pour voir la liste des métriques de votre instance Linux filtrées pour ENA Express, exécutez la ethtool commande suivante pour votre interface réseau (illustrée ici par`eth0`). Prenez note de la valeur de la `ena_srd_mode` métrique.

```
[ec2-user ~]$ ethtool -S eth0 | grep ena_srd
NIC statistics:
 ena_srd_mode: 1
 ena_srd_tx_pkts: 0
```

```
ena_srd_eligible_tx_pkts: 0
ena_srd_rx_pkts: 0
ena_srd_resource_utilization: 0
```

Les métriques suivantes sont disponibles pour toutes les instances sur lesquelles ENA Express est activé.

ena_srd_mode

Décrit les fonctionnalités d'ENAExpress activées. Les valeurs sont les suivantes :

- `0`= ENA Désactiver ou UDP désactiver
- `1`= Activation et UDP désactivation de la fonction ENA Express
- `2`= ENA Express désactivé, UDP activé

> **Note**
>
> Cela ne se produit que lorsqu'ENAExpress a été initialement activé et UDP configuré pour l'utiliser. La valeur précédente est conservée pour le UDP trafic.

- `3`= ENA Express activé, UDP activé

ena_srd_eligible_tx_pkts

Le numéro de réseau est le suivant :

- Les types d'instance d'envoi et de réception sont pris en charge. Consultez la table Types d'instances pris en charge pour ENA Express pour plus d'informations.
- ENAExpress doit être configuré pour les instances d'envoi et de réception.
- Les instances d'envoi et de réception doivent s'exécuter dans la même zone de disponibilité.
- Le chemin réseau entre les instances ne doit pas inclure de boîtiers intergiciels. ENAExpress ne prend actuellement pas en charge les intergiciels.

> **Note**
>
> La métrique d'éligibilité d'ENAExpress couvre les exigences relatives à la source et à la destination, ainsi que le réseau entre les deux points de terminaison. Les paquets éligibles peuvent toujours être disqualifiés une fois qu'ils ont déjà été comptés. Par exemple, si un paquet éligible dépasse la limite maximale d'unités de transmission (MTU), il revient à la

ENA transmission standard, bien que le paquet soit toujours considéré comme éligible dans le compteur.

ena_srd_tx_pkts

Le nombre de SRD paquets transmis au cours d'une période donnée.

ena_srd_rx_pkts

Le nombre de SRD paquets reçus au cours d'une période donnée.

ena_srd_resource_utilization

Pourcentage de l'utilisation maximale de la mémoire autorisée pour les SRD connexions simultanées consommées par l'instance.

Pour vérifier si la transmission de paquets est utiliséeSRD, vous pouvez comparer le nombre de paquets éligibles (`ena_srd_eligible_tx_pkts`métrique) au nombre de SRD paquets transmis (`ena_srd_tx_pkts`métrique) pendant une période donnée.

Trafic sortant (paquets sortants)

Pour vous assurer que votre trafic de sortie est utilisé SRD comme prévu, comparez le nombre de paquets SRD éligibles (`ena_srd_eligible_tx_pkts`) avec le nombre de SRD paquets envoyés (`ena_srd_tx_pkts`) sur une période donnée.

Les différences importantes entre le nombre de paquets éligibles et le nombre de SRD paquets envoyés sont souvent dues à des problèmes d'utilisation des ressources. Lorsque la carte réseau attachée à l'instance a épuisé ses ressources maximales, ou si les paquets dépassent la MTU limite, les paquets éligibles ne peuvent pas être transmis via SRD et doivent revenir à la ENA transmission standard. Les paquets peuvent également tomber dans cette lacune lors de migrations en direct ou de mises à jour de serveurs en direct. Un dépannage supplémentaire est nécessaire pour déterminer la cause racine.

Note

Vous pouvez ignorer les différences mineures occasionnelles entre le nombre de paquets éligibles et le nombre de SRD paquets. Cela peut se produire lorsque votre instance établit une connexion à une autre instance pour SRD le trafic, par exemple.

Pour connaître le pourcentage de votre trafic de sortie total utilisé sur une période donnéeSRD, comparez le nombre de SRD paquets envoyés (`ena_srd_tx_pkts`) au nombre total de paquets envoyés pour l'instance (`NetworkPacketOut`) pendant cette période.

Trafic entrant (paquets entrants)

Pour connaître le pourcentage de votre trafic entrant utiliséSRD, comparez le nombre de SRD paquets reçus (`ena_srd_rx_pkts`) sur une période donnée au nombre total de paquets reçus pour l'instance (`NetworkPacketIn`) pendant cette période.

Utilisation des ressources

L'utilisation des ressources est basée sur le nombre de SRD connexions simultanées qu'une seule instance peut détenir à un moment donné. La métrique d'utilisation des ressources (`ena_srd_resource_utilization`) assure le suivi de votre utilisation actuelle pour l'instance. À mesure que l'utilisation approche les 100 %, vous pouvez vous attendre à des problèmes de performances. ENALa transmission express revient SRD à la ENA transmission standard, et le risque de perte de paquets augmente. Une utilisation élevée des ressources indique qu'il est temps de réduire la taille de l'instance afin d'améliorer les performances réseau.

> **Note**
>
> Lorsque le trafic réseau d'une instance dépasse un maximum, AWS façonne le trafic qui dépasse le maximum en mettant en file d'attente puis en supprimant les paquets réseau.

Persistance

Les métriques de sortie et d'entrée s'accumulent lorsqu'ENAExpress est activé pour l'instance. Les métriques cessent de s'accumuler si ENA Express est désactivé, mais persistent tant que l'instance est toujours en cours d'exécution. Les métriques sont réinitialisées si l'instance redémarre ou est arrêtée, ou si l'interface réseau est détachée de l'instance.

Mesures de performance du réseau avec le DPDK pilote pour ENA

La version 2.2.0 et les versions ultérieures du ENA pilote prennent en charge la génération de rapports sur les métriques du réseau. DPDKLa version 20.11 inclut le ENA pilote 2.2.0 et est la première DPDK version à prendre en charge cette fonctionnalité.

Vous pouvez utiliser un exemple d'application pour consulter les DPDK statistiques. Pour démarrer une version interactive de l'exemple d'application, exécutez la commande suivante.

```
./app/dpdk-testpmd -- -i
```

Dans cette session interactive, vous pouvez saisir une commande afin de récupérer des statistiques étendues pour un port. L'exemple de commande suivant récupère les statistiques pour le port 0.

```
show port xstats 0
```

Voici un exemple de session interactive avec l'DPDKexemple d'application.

```
[root@ip-192.0.2.0 build]# ./app/dpdk-testpmd -- -i
        EAL: Detected 4 lcore(s)
        EAL: Detected 1 NUMA nodes
        EAL: Multi-process socket /var/run/dpdk/rte/mp_socket
        EAL: Selected IOVA mode 'PA'
        EAL: Probing VFIO support...
        EAL:   Invalid NUMA socket, default to 0
        EAL:   Invalid NUMA socket, default to 0
        EAL: Probe PCI driver: net_ena (1d0f:ec20) device: 0000:00:06.0
(socket 0)
        EAL: No legacy callbacks, legacy socket not created
        Interactive-mode selected

        Port 0: link state change event
        testpmd: create a new mbuf pool <mb_pool_0>: n=171456,
size=2176, socket=0
        testpmd: preferred mempool ops selected: ring_mp_mc

        Warning! port-topology=paired and odd forward ports number, the
last port will pair with itself.

        Configuring Port 0 (socket 0)
        Port 0: 02:C7:17:A2:60:B1
        Checking link statuses...
        Done
        Error during enabling promiscuous mode for port 0: Operation
not supported - ignore
        testpmd> show port xstats 0
        ###### NIC extended statistics for port 0
        rx_good_packets: 0
        tx_good_packets: 0
        rx_good_bytes: 0
        tx_good_bytes: 0
```

```
        rx_missed_errors: 0
        rx_errors: 0
        tx_errors: 0
        rx_mbuf_allocation_errors: 0
        rx_q0_packets: 0
        rx_q0_bytes: 0
        rx_q0_errors: 0
        tx_q0_packets: 0
        tx_q0_bytes: 0
        wd_expired: 0
        dev_start: 1
        dev_stop: 0
        tx_drops: 0
        bw_in_allowance_exceeded: 0
        bw_out_allowance_exceeded: 0
        pps_allowance_exceeded: 0
        conntrack_allowance_exceeded: 0
        linklocal_allowance_exceeded: 0
        rx_q0_cnt: 0
        rx_q0_bytes: 0
        rx_q0_refill_partial: 0
        rx_q0_bad_csum: 0
        rx_q0_mbuf_alloc_fail: 0
        rx_q0_bad_desc_num: 0
        rx_q0_bad_req_id: 0
        tx_q0_cnt: 0
        tx_q0_bytes: 0
        tx_q0_prepare_ctx_err: 0
        tx_q0_linearize: 0
        tx_q0_linearize_failed: 0
        tx_q0_tx_poll: 0
        tx_q0_doorbells: 0
        tx_q0_bad_req_id: 0
        tx_q0_available_desc: 1023
        testpmd>
```

Pour plus d'informations sur l'exemple d'application et son utilisation pour récupérer des statistiques étendues, consultez le guide de l'utilisateur de l'application Testpmd dans la documentation. DPDK

Mesures relatives aux instances exécutant Free BSD

À partir de la version 2.3.0, le BSD pilote ENA Free prend en charge la collecte de mesures de performance réseau sur les instances exécutant FreeBSD. Pour activer la collecte de BSD métriques

gratuites, entrez la commande suivante et définissez *interval* à une valeur comprise entre 1 et 3 600. Cela indique la fréquence, en secondes, à laquelle les BSD métriques gratuites doivent être collectées.

```
sysctl dev.ena.network_interface.eni_metrics.sample_interval=interval
```

Par exemple, la commande suivante définit le pilote pour qu'il collecte BSD les métriques Free sur l'interface réseau 1 toutes les 10 secondes :

```
sysctl dev.ena.1.eni_metrics.sample_interval=10
```

Pour désactiver la collecte de BSD métriques gratuites, vous pouvez exécuter la commande précédente et spécifier `0` comme *interval*.

Après avoir activé la collecte de BSD métriques gratuites, vous pouvez récupérer le dernier ensemble de métriques collectées en exécutant la commande suivante.

```
sysctl dev.ena.network_interface.eni_metrics
```

Résoudre les problèmes liés au pilote ENA du noyau sous Linux

L'Elastic Network Adapter (ENA) est conçu pour améliorer l'état du système d'exploitation et réduire les risques de perturbations à long terme dues à un comportement matériel inattendu et/ou à des défaillances. L'ENAarchitecture fait en sorte que les défaillances de périphériques ou de pilotes soient aussi transparentes que possible pour le système. Cette rubrique fournit des informations de dépannage pourENA.

Si vous ne pouvez pas vous connecter à votre instance, commencez par la section Résoudre les problèmes de connectivité.

Si vous constatez une dégradation des performances après la migration vers un type d'instance de sixième génération, consultez l'article Que dois-je faire avant de migrer mon EC2 instance vers une instance de sixième génération afin de garantir des performances réseau optimales ?

Si vous ne parvenez pas à vous connecter à votre instance, recueillez des informations de diagnostic à l'aide des mécanismes de détection des défaillances et de récupération couverts dans des sections ultérieures de cette rubrique.

Sommaire

- Résoudre les problèmes de connectivité
- Mécanisme Keep-alive
- Expiration du délai d'attente des opérations de lecture
- Statistiques
- Journaux d'erreur de pilote dans syslog
- Notifications de configuration sous-optimales

Résoudre les problèmes de connectivité

Si vous perdez la connexion lors de l'activation de la mise en réseau améliorée, il se peut que le module `ena` ne soit pas compatible avec le noyau de votre instance. Cela peut se produire si vous installez le module pour une version de noyau spécifique (sans dkms ou avec un fichier dkms.conf mal configuré), puis que le noyau de votre instance est mis à jour. Si le module `ena` du noyau de l'instance qui est chargé au moment du démarrage n'est pas correctement installé, votre instance ne reconnaît pas la carte réseau et devient inaccessible.

Si vous activez la mise en réseau améliorée pour une instance PVAMI, cela peut également rendre votre instance inaccessible.

Si votre instance devient inaccessible après avoir activé la mise en réseau améliorée avecENA, vous pouvez désactiver l'`enaSupport`attribut de votre instance et l'adaptateur réseau d'origine sera rétabli.

Pour désactiver la mise en réseau améliorée avec des instances ENA (EBSsoutenues par des instances)

1. Depuis votre ordinateur local, arrêtez l'instance à l'aide de la EC2 console Amazon ou de l'une des commandes suivantes : stop-instances (AWS CLI), Stop-EC2Instance(AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez l'arrêter dans la AWS OpsWorks console afin que son état reste synchronisé.

   > **Tip**
   >
   > Si vous utilisez une instance basée sur le stockage d'instance, vous ne pouvez pas l'arrêter. Passez plutôt à Pour désactiver la mise en réseau améliorée avec ENA (instance), des instances stockées.

2. Depuis votre ordinateur local, désactivez l'attribut de mise en réseau améliorée à l'aide de la commande suivante.

   - modify-instance-attribute (AWS CLI)

   ```
   $ C:\> aws ec2 modify-instance-attribute --instance-id instance_id --no-ena-support
   ```

3. Depuis votre ordinateur local, démarrez l'instance à l'aide de la EC2 console Amazon ou de l'une des commandes suivantes : start-instances (AWS CLI), Start-EC2Instance(AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez démarrer l'instance dans la AWS OpsWorks console afin que son état reste synchronisé.
4. (Facultatif) Connectez-vous à votre instance et essayez de réinstaller le module `ena` avec votre version de noyau actuelle en suivant les étapes décrites dans la section Activez une mise en réseau améliorée avec ENA vos EC2 instances.

Pour désactiver la mise en réseau améliorée avec ENA (instances basées sur le stockage d'instance)

Si votre instance est une instance basée sur le stockage d'instances, créez-en une nouvelle AMI comme décrit dans. Création d'une instance sauvegardée en magasin AMI Assurez-vous de désactiver l'`enaSupport`attribut de mise en réseau améliorée lorsque vous enregistrez leAMI.

- register-image (AWS CLI)

```
$ C:\> aws ec2 register-image --no-ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
C:\> Register-EC2Image -EnaSupport $false ...
```

Mécanisme Keep-alive

L'ENAappareil publie des événements de maintien en vie à un rythme fixe (généralement une fois par seconde). Le ENA pilote met en œuvre un mécanisme de surveillance qui vérifie la présence de ces messages de maintien en vie. Si un ou plusieurs messages sont présents, la surveillance est réarmée. Dans le cas contraire, le pilote conclut que l'appareil a subi une défaillance et effectue alors les opérations suivantes :

- Il envoie ses statistiques dans le journal système.
- Réinitialise l'appareil ENA
- Réinitialise l'état du ENA pilote

La procédure de réinitialisation ci-dessus peut entraîner une perte de trafic pendant une courte période (TCPles connexions devraient pouvoir être rétablies), mais ne devrait pas affecter l'utilisateur.

Le ENA dispositif peut également demander indirectement une procédure de réinitialisation du dispositif, en n'envoyant pas de notification de maintien en vie, par exemple, si le ENA dispositif atteint un état inconnu après le chargement d'une configuration irrécupérable.

Voici un exemple de procédure de réinitialisation :

```
[18509.800135] ena 0000:00:07.0 eth1: Keep alive watchdog timeout. // The watchdog
 process initiates a reset
[18509.815244] ena 0000:00:07.0 eth1: Trigger reset is on
[18509.825589] ena 0000:00:07.0 eth1: tx_timeout: 0 // The driver logs the current
 statistics
[18509.834253] ena 0000:00:07.0 eth1: io_suspend: 0
[18509.842674] ena 0000:00:07.0 eth1: io_resume: 0
[18509.850275] ena 0000:00:07.0 eth1: wd_expired: 1
[18509.857855] ena 0000:00:07.0 eth1: interface_up: 1
[18509.865415] ena 0000:00:07.0 eth1: interface_down: 0
[18509.873468] ena 0000:00:07.0 eth1: admin_q_pause: 0
[18509.881075] ena 0000:00:07.0 eth1: queue_0_tx_cnt: 0
[18509.888629] ena 0000:00:07.0 eth1: queue_0_tx_bytes: 0
[18509.895286] ena 0000:00:07.0 eth1: queue_0_tx_queue_stop: 0
.......
........
[18511.280972] ena 0000:00:07.0 eth1: free uncompleted tx skb qid 3 idx 0x7 // At the
 end of the down process, the driver discards incomplete packets.
[18511.420112] [ENA_COM: ena_com_validate_version] ena device version: 0.10 //The
 driver begins its up process
[18511.420119] [ENA_COM: ena_com_validate_version] ena controller version: 0.0.1
 implementation version 1
[18511.420127] [ENA_COM: ena_com_admin_init] ena_defs : Version:[b9692e8] Build date
 [Wed Apr  6 09:54:21 IDT 2016]
[18512.252108] ena 0000:00:07.0: Device watchdog is Enabled
[18512.674877] ena 0000:00:07.0: irq 46 for MSI/MSI-X
[18512.674933] ena 0000:00:07.0: irq 47 for MSI/MSI-X
[18512.674990] ena 0000:00:07.0: irq 48 for MSI/MSI-X
[18512.675037] ena 0000:00:07.0: irq 49 for MSI/MSI-X
```

```
[18512.675085] ena 0000:00:07.0: irq 50 for MSI/MSI-X
[18512.675141] ena 0000:00:07.0: irq 51 for MSI/MSI-X
[18512.675188] ena 0000:00:07.0: irq 52 for MSI/MSI-X
[18512.675233] ena 0000:00:07.0: irq 53 for MSI/MSI-X
[18512.675279] ena 0000:00:07.0: irq 54 for MSI/MSI-X
[18512.772641] [ENA_COM: ena_com_set_hash_function] Feature 10 isn't supported
[18512.772647] [ENA_COM: ena_com_set_hash_ctrl] Feature 18 isn't supported
[18512.775945] ena 0000:00:07.0: Device reset completed successfully // The reset
 process is complete
```

Expiration du délai d'attente des opérations de lecture

L'ENAarchitecture suggère une utilisation limitée des opérations de lecture d'E/S (MMIO) mappées en mémoire. MMIOles registres ne sont accessibles par le pilote du ENA périphérique que pendant sa procédure d'initialisation.

Si les journaux du pilote (disponibles dans la sortie dmesg) indiquent une défaillance des opérations de lecture, un pilote incompatible ou mal compilé, un dispositif saturé ou une défaillance matérielle peuvent en être la cause.

Les entrées de journal intermittentes qui indiquent des défaillances des opérations de lecture ne sont pas problématiques. Dans ce cas, le pilote réessaie de les traiter. Toutefois, une série d'entrées de journal contenant des défaillances de lecture indique un problème de pilote ou de matériel.

Voici un exemple d'entrée de journal pilote indiquant une défaillance des opérations de lecture en raison de l'expiration d'un délai d'attente :

```
[ 47.113698] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
 expected: req id[1] offset[88] actual: req id[57006] offset[0]
[ 47.333715] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
 expected: req id[2] offset[8] actual: req id[57007] offset[0]
[ 47.346221] [ENA_COM: ena_com_dev_reset] Reg read32 timeout occurred
```

Statistiques

Si vous rencontrez des problèmes de latence ou si les performances réseau sont insuffisantes, vous devez récupérer les statistiques de l'appareil et les examiner. Pour obtenir ces statistiques, utilisez ethtool, comme suit.

```
[ec2-user ~]$ ethtool -S ethN
```

```
NIC statistics:
 tx_timeout: 0
 suspend: 0
 resume: 0
 wd_expired: 0
 interface_up: 1
 interface_down: 0
 admin_q_pause: 0
 bw_in_allowance_exceeded: 0
 bw_out_allowance_exceeded: 0
 pps_allowance_exceeded: 0
 conntrack_allowance_available: 450878
 conntrack_allowance_exceeded: 0
 linklocal_allowance_exceeded: 0
 queue_0_tx_cnt: 4329
 queue_0_tx_bytes: 1075749
 queue_0_tx_queue_stop: 0
 ...
```

Les paramètres de sortie de commande suivants sont décrits ci-dessous :

`tx_timeout`: *N*

Nombre de fois que la surveillance Netdev a été activée.

`suspend`: *N*

Nombre de fois que le pilote a effectué une opération de suspension.

`resume`: *N*

Nombre de fois que le pilote a effectué une opération de reprise.

`wd_expired`: *N*

Nombre de fois que le pilote n'a pas reçu l'événement keep-alive au cours des trois secondes précédentes.

`interface_up`: *N*

Le nombre de fois que l'ENAinterface a été ouverte.

`interface_down`: *N*

Le nombre de fois où l'ENAinterface a été désactivée.

`admin_q_pause`: *N*

Nombre de fois que la file d'attente d'administration n'a pas été trouvée dans un état en cours d'exécution.

`bw_in_allowance_exceeded`: *N*

Nombre de paquets mis en file d'attente ou ignorés flottee que la bande passante agrégée entrante a dépassé le maximum de l'instance.

`bw_out_allowance_exceeded`: *N*

Nombre de paquets mis en file d'attente ou ignorés flottee que la bande passante agrégée sortante a dépassé le maximum de l'instance.

`pps_allowance_exceeded`: *N*

Le nombre de paquets mis en file d'attente ou abandonnés parce que le mode bidirectionnel PPS a dépassé le maximum pour l'instance. Cette limite compte également les pertes de fragments de sortie supérieures à 1 024 PPS par. ENI

`conntrack_allowance_available`: *N*

Nombre de connexions suivies pouvant être établies par l'instance avant d'atteindre l'allocation Connexions suivies de ce type d'instance. Disponible uniquement pour les instances basées sur Nitro. Non pris en charge par BSD les instances ou DPDK les environnements gratuits.

`conntrack_allowance_exceeded`: *N*

Nombre de paquets ignorés flottee que le suivi des connexions a dépassé le maximum de l'instance et que de nouvelles connexions n'ont pas pu être établies. Cela peut entraîner une perte de paquets pour le trafic vers ou en provenance de l'instance.

`linklocal_allowance_exceeded`: *N*

Le nombre de paquets abandonnés parce que le PPS trafic vers les services proxy locaux a dépassé le maximum pour l'interface réseau. Cela a un impact sur le trafic vers le DNS service, le service de métadonnées d'instance et le service Amazon Time Sync.

`queue_`*N*`_tx_cnt`: *N*

Nombre de paquets transmis pour cette file d'attente.

`queue_`*N*`_tx_bytes`: *N*

Nombre d'octets transmis pour cette file d'attente.

`queue_N_tx_queue_stop`: *N*

Le nombre de fois que cette file d'attente *N* était plein et s'est arrêté.

`queue_N_tx_queue_wakeup`: *N*

Le nombre de fois que cette file d'attente *N* repris après avoir été arrêté.

`queue_N_tx_dma_mapping_err`: *N*

Nombre d'erreurs d'accès direct à la mémoire. Si cette valeur ne correspond pas à 0, les ressources système sont faibles.

`queue_N_tx_linearize`: *N*

Nombre de tentatives de SKB linéarisation pour cette file d'attente.

`queue_N_tx_linearize_failed`: *N*

Nombre de fois où la SKB linéarisation a échoué pour cette file d'attente.

`queue_N_tx_napi_comp`: *N*

Nombre de fois que le gestionnaire `napi` a appelé `napi_complete` pour cette file d'attente.

`queue_N_tx_tx_poll`: *N*

Nombre de fois que le gestionnaire `napi` a été planifié pour cette file d'attente.

`queue_N_tx_doorbells`: *N*

Nombre de portes de transmission pour cette file d'attente.

`queue_N_tx_prepare_ctx_err`: *N*

Nombre de fois que `ena_com_prepare_tx` a échoué pour cette file d'attente.

`queue_N_tx_bad_req_id`: *N*

`req_id` non valide pour cette file d'attente. La valeur `req_id` valide est égale à zéro, moins la valeur `queue_size`, moins 1.

`queue_N_tx_llq_buffer_copy`: *N*

Nombre de paquets dont la taille des en-têtes est supérieure à l'entrée llq pour cette file d'attente.

`queue_N_tx_missed_tx`: *N*

Nombre de paquets qui n'ont pas été traités entièrement pour cette file d'attente.

`queue_N_tx_unmask_interrupt`: *N*

Nombre de fois que tx interrupt a été démasqué pour cette file d'attente.

`queue_N_rx_cnt`: *N*

Nombre de paquets reçus pour cette file d'attente.

`queue_N_rx_bytes`: *N*

Nombre d'octets reçus pour cette file d'attente.

`queue_N_rx_rx_copybreak_pkt`: *N*

Nombre de fois que la file d'attente rx a reçu un paquet inférieur à la taille de paquet rx_copybreak pour cette file d'attente.

`queue_N_rx_csum_good`: *N*

Nombre de fois que la file d'attente rx a reçu un paquet dont le total de contrôle a été vérifié comme étant correct pour cette file d'attente.

`queue_N_rx_refil_partial`: *N*

Nombre de fois que le pilote n'a pas réussi à remplir la portion vide de la file d'attente rx avec les tampons pour cette file d'attente. Si cette valeur n'est pas égale à zéro, les ressources mémoire sont faibles.

`queue_N_rx_bad_csum`: *N*

Nombre de fois que la file d'attente `rx` a reçu un mauvais total de contrôle pour cette file d'attente (uniquement si le déchargement du total de contrôle rx est pris en charge).

`queue_N_rx_page_alloc_fail`: *N*

Nombre de fois que l'allocation des pages a échoué pour cette file d'attente. Si cette valeur n'est pas égale à zéro, les ressources mémoire sont faibles.

`queue_N_rx_skb_alloc_fail`: *N*

Nombre de fois où l'SKBallocation a échoué pour cette file d'attente. Si cette valeur n'est pas égale à zéro, les ressources système sont faibles.

`queue_N_rx_dma_mapping_err`: *N*

Nombre d'erreurs d'accès direct à la mémoire. Si cette valeur ne correspond pas à 0, les ressources système sont faibles.

`queue_N_rx_bad_desc_num`: *N*

Trop de tampons par paquet. Si cette valeur n'est pas égale à 0, cela indique l'utilisation de très petits tampons.

`queue_N_rx_bad_req_id`: *N*

Le req_id de cette file d'attente n'est pas valide. Le req_id valide est de [0, queue_size - 1].

`queue_N_rx_empty_rx_ring`: *N*

Nombre de fois que la file d'attente rx était vide pour cette file d'attente.

`queue_N_rx_csum_unchecked`: *N*

Nombre de fois que la file d'attente rx a reçu un paquet dont le total de contrôle n'a pas été vérifié pour cette file d'attente.

`queue_N_rx_xdp_aborted`: *N*

Le nombre de fois qu'un XDP paquet a été classé comme XDP _ABORT.

`queue_N_rx_xdp_drop`: *N*

Le nombre de fois qu'un XDP paquet a été classé comme XDP _DROP.

`queue_N_rx_xdp_pass`: *N*

Le nombre de fois qu'un XDP paquet a été classé comme XDP _PASS.

`queue_N_rx_xdp_tx`: *N*

Le nombre de fois qu'un XDP paquet a été classé en tant que XDP _TX.

`queue_N_rx_xdp_invalid`: *N*

Le nombre de fois où le code de XDP retour du paquet n'était pas valide.

`queue_N_rx_xdp_redirect`: *N*

Le nombre de fois qu'un XDP paquet a été classé comme XDP _REDIRECT.

`queue_N_xdp_tx_cnt`: *N*

Nombre de paquets transmis pour cette file d'attente.

`queue_N_xdp_tx_bytes`: *N*

Nombre d'octets transmis pour cette file d'attente.

`queue_N_xdp_tx_queue_stop`: *N*

Nombre de fois que cette file d'attente était pleine et qu'elle a été arrêtée.

`queue_N_xdp_tx_queue_wakeup`: *N*

Nombre de fois que cette file d'attente a repris après avoir été arrêtée.

`queue_N_xdp_tx_dma_mapping_err`: *N*

Nombre d'erreurs d'accès direct à la mémoire. Si cette valeur ne correspond pas à 0, les ressources système sont faibles.

`queue_N_xdp_tx_linearize`: *N*

Nombre de tentatives de linéarisation de la XDP mémoire tampon pour cette file d'attente.

`queue_N_xdp_tx_linearize_failed`: *N*

Nombre de fois où la linéarisation de la XDP mémoire tampon a échoué pour cette file d'attente.

`queue_N_xdp_tx_napi_comp`: *N*

Nombre de fois que le gestionnaire napi a appelé napi_complete pour cette file d'attente.

`queue_N_xdp_tx_tx_poll`: *N*

Nombre de fois que le gestionnaire napi a été planifié pour cette file d'attente.

`queue_N_xdp_tx_doorbells`: *N*

Nombre de portes de transmission pour cette file d'attente.

`queue_N_xdp_tx_prepare_ctx_err`: *N*

Nombre de fois que ena_com_prepar_tx a échoué pour cette file d'attente. Cette valeur doit toujours être égale à zéro. Si ce n'est pas le cas, consultez les journaux du pilote.

`queue_N_xdp_tx_bad_req_id`: *N*

Le req_id de cette file d'attente n'est pas valide. Le req_id valide est de [0, queue_size - 1].

`queue_N_xdp_tx_llq_buffer_copy`: *N*

Nombre de paquets dont les en-têtes ont été copiés à l'aide de la copie tampon llq pour cette file d'attente.

`queue_N_xdp_tx_missed_tx`: *N*

Nombre de fois qu'une entrée de file d'attente tx a dépassé un délai de résiliation pour cette file d'attente.

`queue_N_xdp_tx_unmask_interrupt`: *N*

Nombre de fois que tx interrupt a été démasqué pour cette file d'attente.

`ena_admin_q_aborted_cmd`: *N*

Nombre de commandes d'administration qui ont été abandonnées. Généralement, cela se produit lors de la procédure de récupération automatique.

`ena_admin_q_submitted_cmd`: *N*

Nombre de portes d'administration de la file d'attente.

`ena_admin_q_completed_cmd`: *N*

Nombre de finalisations de la file d'attente d'administration.

`ena_admin_q_out_of_space`: *N*

Nombre de fois que le pilote a essayé de présenter la nouvelle commande d'administration, mais que la file d'attente était pleine.

`ena_admin_q_no_completion`: *N*

Nombre de fois que l'administration du pilote n'a pas été terminée pour une commande.

Journaux d'erreur de pilote dans syslog

Le ENA pilote écrit des messages de journal syslog pendant le démarrage du système. Vous pouvez examiner ces journaux pour rechercher les erreurs si vous rencontrez des problèmes. Vous trouverez ci-dessous un exemple d'informations enregistrées par le ENA pilote syslog lors du démarrage du système, ainsi que des annotations pour certains messages.

```
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  478.416939] [ENA_COM:
 ena_com_validate_version] ena device version: 0.10
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  478.420915] [ENA_COM:
 ena_com_validate_version] ena controller version: 0.0.1 implementation version 1
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.256831] ena 0000:00:03.0: Device
 watchdog is Enabled
```

```
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.672947] ena 0000:00:03.0: creating 8 io
 queues. queue size: 1024
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.680885] [ENA_COM:
 ena_com_init_interrupt_moderation] Feature 20 isn't supported  // Interrupt moderation
 is not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.691609] [ENA_COM:
 ena_com_get_feature_ex] Feature 10 isn't supported // RSS HASH function configuration
 is not supported by the
 device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.694583] [ENA_COM:
 ena_com_get_feature_ex] Feature 18 isn't supported //RSS HASH input source
 configuration is not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.697433] [ENA_COM:
 ena_com_set_host_attributes] Set host attribute isn't supported
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.701064] ena 0000:00:03.0 (unnamed
 net_device) (uninitialized): Cannot set host attributes
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.704917] ena 0000:00:03.0: Elastic
 Network Adapter (ENA) found at mem f3000000, mac addr 02:8a:3c:1e:13:b5 Queues 8
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  480.805037] EXT4-fs (xvda1): re-mounted.
 Opts: (null)
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  481.025842] NET: Registered protocol family
 10
```

Quelles sont les erreurs que je peux ignorer ?

Les avertissements suivants qui peuvent apparaître dans les journaux d'erreur de votre système peuvent être ignorées pour Elastic Network Adapter :

Set host attribute isn't supported

Les attributs de l'hôte ne sont pas pris en charge pour cet appareil.

failed to alloc buffer for rx queue

Il s'agit d'une erreur récupérable. Elle indique qu'il y a peut-être eu un problème de pression de mémoire lorsque l'erreur a été lancée.

Fonctionnalité *X* n'est pas pris en charge

La fonctionnalité référencée n'est pas prise en charge par Elastic Network Adapter. Valeurs possibles pour *X* inclure :

- **10**: La configuration de la fonction de RSS hachage n'est pas prise en charge pour cet appareil.
- **12**: La configuration de RSS la table d'indirection n'est pas prise en charge pour cet appareil.

- **18**: La configuration de l'entrée de RSS hachage n'est pas prise en charge pour cet appareil.
- **20** : la modération d'interruption n'est pas prise en charge pour cet appareil.
- **27** : le pilote ENA (Elastic Network Adapter) ne prend pas en charge l'interrogation des fonctions Ethernet à partir de snmpd.

Impossible de configurer AENQ

L'Elastic Network Adapter ne prend pas en charge AENQ la configuration.

Essayer de définir des événements non pris en charge AENQ

Cette erreur indique une tentative de définition d'un groupe d'AENQévénements non pris en charge par l'Elastic Network Adapter.

Notifications de configuration sous-optimales

Le ENA périphérique détecte des paramètres de configuration sous-optimaux dans le pilote que vous pouvez modifier. Le périphérique avertit le ENA pilote et enregistre un avertissement sur la console. L'exemple suivant montre le format du message d'avertissement.

```
Sub-optimal configuration notification code: 1. Refer to AWS ENA documentation for
 additional details and mitigation options.
```

La liste suivante indique les détails du code de notification et les actions recommandées pour les résultats de configuration sous-optimaux.

- Code **1** : ENA Express avec une LLQ configuration étendue n'est pas recommandé

  ENAExpress ENI est configuré avec WideLLQ. Cette configuration n'est pas optimale et peut avoir un impact sur les performances d'ENAExpress. Nous vous recommandons de désactiver les LLQ paramètres étendus lorsque vous utilisez ENA Express ENIs comme suit.

  ```
  sudo rmmod ena && sudo modprobe ena force_large_llq_header=0
  ```

  Pour plus d'informations sur la configuration optimale pour ENA Express, consultezAméliorez les performances du réseau entre EC2 les instances avec ENA Express.
- Code **2** : ENA Express ENI avec une profondeur de file Tx sous-optimale n'est pas recommandé

  ENAExpress ENI est configuré avec une profondeur de file d'attente Tx sous-optimale. Cette configuration peut avoir un impact sur les performances d'ENAExpress. Nous vous recommandons

d'agrandir toutes les files d'attente Tx à la valeur maximale de l'interface réseau lorsque vous utilisez ENA Express ENIs comme suit.

Vous pouvez exécuter les ethtool commandes suivantes pour ajuster LLQ la taille. Pour en savoir plus sur la façon de contrôler, d'interroger et d'activer le Wide-LLQ, consultez la rubrique Grande file d'attente à faible latence (LargeLLQ) du pilote du noyau Linux pour obtenir de la ENA documentation dans le GitHub référentiel Amazon Drivers.

```
ethtool -g interface
```

Réglez vos files d'attente Tx à la profondeur maximale :

```
ethtool -G interface tx depth
```

Pour plus d'informations sur la configuration optimale pour ENA Express, consultezAméliorez les performances du réseau entre EC2 les instances avec ENA Express.

- Code **3** : ENA avec une LLQ taille normale et un trafic de paquets Tx supérieur à la taille maximale d'en-tête prise en charge

  Par défaut, ENA LLQ prend en charge la taille d'en-tête de paquet Tx jusqu'à 96 octets. Si la taille de l'en-tête du paquet est supérieure à 96 octets, le paquet est supprimé. Pour atténuer ce problème, nous vous recommandons d'activer Wide-LLQ, qui augmente la taille d'en-tête de paquet Tx prise en charge à un maximum de 224 octets.

  Toutefois, lorsque vous activez Wide-LLQ, la taille maximale de l'anneau Tx est réduite de 1 000 à 512 entrées. Wide- LLQ est activé par défaut pour tous les types d'instances de Nitro v4 et versions ultérieures.

  - Les types d'instances Nitro v4 ont une taille d'anneau LLQ Wide-Tx maximale par défaut de 512 entrées, qui ne peut pas être modifiée.
  - Les types d'instances Nitro v5 ont une taille d'anneau LLQ Wide-Tx par défaut de 512 entrées, que vous pouvez augmenter jusqu'à 1 000 entrées.

  Vous pouvez exécuter les ethtool commandes suivantes pour ajuster LLQ la taille. Pour en savoir plus sur la façon de contrôler, d'interroger et d'activer le Wide-LLQ, consultez la rubrique Grande file d'attente à faible latence (LargeLLQ) du pilote du noyau Linux pour obtenir de la ENA documentation dans le GitHub référentiel Amazon Drivers.

  Trouvez la profondeur maximale de vos files d'attente Tx :

```
ethtool -g interface
```

Réglez vos files d'attente Tx à la profondeur maximale :

```
ethtool -G interface tx depth
```

Résoudre les problèmes liés au pilote Windows d'Elastic Network Adapter

L'Elastic Network Adapter (ENA) est conçu pour améliorer l'état du système d'exploitation et pour réduire les comportements matériels inattendus ou les défaillances susceptibles de perturber le fonctionnement de votre instance Windows. L'ENAarchitecture permet de rendre les défaillances de périphériques ou de pilotes aussi transparentes que possible pour le système d'exploitation.

Collecter des informations de diagnostic sur l'instance

Les étapes pour ouvrir les outils du système d'exploitation Windows varient en fonction de la version du système d'exploitation installée sur votre instance. Dans les sections suivantes, nous utilisons la boîte de dialogue Exécuter pour ouvrir les outils. Celle-ci fonctionne de la même manière sur toutes les versions du système d'exploitation. Toutefois, vous pouvez accéder à ces outils en suivant n'importe quelle méthode de votre choix.

Accéder à la boîte de dialogue Exécuter

- À l'aide de la combinaison de touches avec le logo Windows : `Windows + R`
- À l'aide de la barre de recherche :
  - Entrez `run` dans la barre de recherche.
  - Sélectionnez l'application Exécuter à partir des résultats de recherche.

Certaines étapes nécessitent le menu contextuel pour accéder aux propriétés ou aux actions contextuelles. Il existe plusieurs méthodes pour le faire, qui dépendent de la version de système d'exploitation et du matériel dont vous disposez.

Accéder au menu contextuel

- À l'aide de la souris : cliquez avec le bouton droit sur un élément pour afficher son menu contextuel.

- À l'aide de votre clavier :
  - selon la version de votre système d'exploitation, utilisez `Shift` + `F10` ou `Ctrl` + `Shift` + `F10`.
  - Si votre clavier contient la touche contextuelle (trois lignes horizontales dans un carré), sélectionnez l'élément souhaité, puis appuyez sur la touche contextuelle.

Si vous pouvez vous connecter à votre instance, utilisez les techniques suivantes pour collecter des informations de diagnostic à des fins de dépannage.

Vérifier l'état ENA de l'appareil

Pour vérifier l'état de votre pilote ENA Windows à l'aide du Gestionnaire de périphériques Windows, procédez comme suit :

1. Ouvrez Exécuter à l'aide de l'une des méthodes décrites dans la section précédente.
2. Pour ouvrir le Gestionnaire de périphériques Windows, saisissez `devmgmt.msc` la fenêtre Exécuter.
3. Choisissez OK. La fenêtre du Gestionnaire de périphériques s'ouvre.
4. Sélectionnez la flèche qui apparaît à gauche de Cartes réseau pour développer la liste.
5. Choisissez le nom ou ouvrez le menu contextuel pour Amazon Elastic Network Adapter, puis choisissez Propriétés. Cela ouvre la boîte de dialogue Propriétés d'Amazon Elastic Network Adapter.
6. Vérifiez que le message de l'onglet Général indique « Ce périphérique fonctionne correctement. »

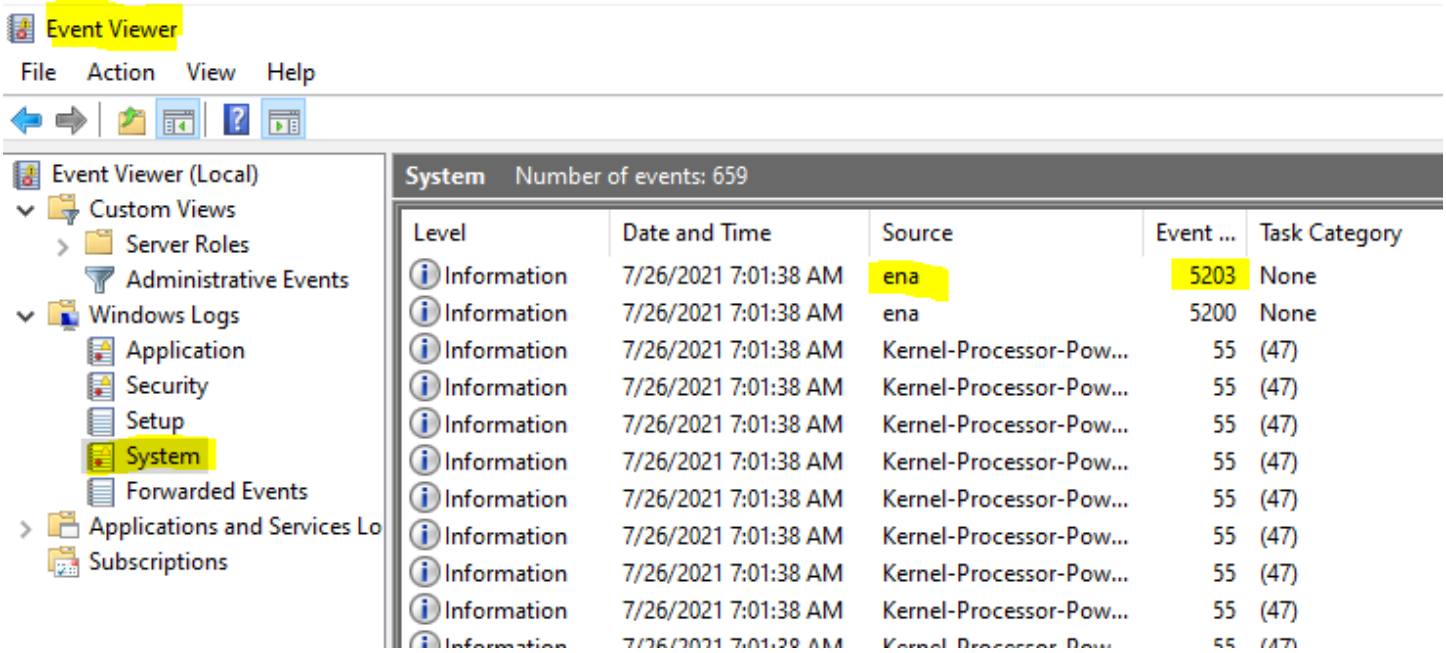
Examiner les messages d'événements du pilote

Pour consulter les journaux des événements des pilotes ENA Windows à l'aide de l'Observateur d'événements Windows, procédez comme suit :

1. Ouvrez Exécuter à l'aide de l'une des méthodes décrites dans la section précédente.
2. Pour ouvrir l'Observateur d'événements Windows, saisissez `eventvwr.msc` dans la fenêtre Exécuter.
3. Choisissez OK. La fenêtre de l'Observateur d'événements s'ouvre.
4. Développez le menu Journaux Windows, puis choisissez Système.
5. Sous Actions, dans le panneau supérieur droit, choisissez Créer une vue personnalisée. La boîte de dialogue Filtrer s'affiche.

6. Dans la zone Sources d'événements, saisissez `ena`. Cela limite les résultats aux événements générés par le pilote ENA Windows.
7. Choisissez OK. Les résultats du journal d'événements filtrés s'affichent dans les sections des détails de la fenêtre.
8. Pour explorer les détails, sélectionnez un message d'événement dans la liste.

L'exemple suivant montre un événement ENA pilote dans la liste des événements système de l'Observateur d'événements Windows :



Résumé des messages d'événement

Le tableau suivant indique les messages d'événement générés par le pilote ENA Windows.

Entrée

ID de l'événement	ENAdescription de l'événement du conducteur	Type
`5001`	Hardware is out of resources (Le matériel est à court de ressources)	Erreur

ID de l’événement	ENAdescription de l'événement du conducteur	Type
5002	Adapter has detected a hardware error (Le dispositif a détecté une erreur matérielle)	Erreur
5005	L'adaptateur a expiré pour une NDIS opération qui ne s'est pas terminée dans les délais	Erreur
5032	Adapter has failed to reset the device (Le dispositif n’a pas réussi à réinitialiser le périphérique)	Erreur
5200	Adapter has been initialized (Le dispositif a été initialisé)	Informationnel
5201	Adapter has been halted (Le dispositif a été interrompu)	Informationnel
5202	Adapter has been paused (Le dispositif a été mis en pause)	Informationnel
5203	Adapter has been restarted (Le dispositif a été redémarré)	Informationnel
5204	Adapter has been shut down (Le dispositif a été arrêté)	Informationnel
5205	Adapter has been reset (Le dispositif a été réinitialisé)	Erreur
5206	Adapter has been surprise removed (Le dispositif a été retiré par surprise)	Erreur

ID de l'événement	ENAdescription de l'événement du conducteur	Type
5208	Adapter initialization routine has failed (La routine d'initialisation du dispositif a échoué)	Erreur
5210	Adapter has encountered and successfully recovered an internal issue (Le dispositif a rencontré un problème interne et a réussi à récupérer)	Erreur

Vérifier les métriques de performance

Le pilote ENA Windows publie les mesures de performance du réseau à partir des instances où les mesures sont activées. Vous pouvez afficher et activer les métriques sur l'instance à l'aide de l'application Performance Monitor native. Pour plus d'informations sur les métriques produites par le pilote ENA Windows, consultezSurveillez les performances du réseau pour ENA les paramètres de votre EC2 instance.

Sur les instances où les ENA métriques sont activées et où l' CloudWatch agent Amazon est installé, CloudWatch collecte les métriques associées aux compteurs dans Windows Performance Monitor, ainsi que certaines métriques avancées pourENA. Ces métriques sont collectées en plus des métriques activées par défaut sur les EC2 instances. Pour plus d'informations sur les statistiques, consultez la section Mesures collectées par l' CloudWatch agent dans le guide de CloudWatch l'utilisateur Amazon.

> **Note**
>
> Les mesures de performance sont disponibles pour les versions 2.4.0 et ultérieures du ENA pilote (également pour la version 2.2.3). ENAla version 2.2.4 du pilote a été annulée en raison d'une dégradation potentielle des performances sur les EC2 instances de sixième génération. Nous vous recommandons de mettre à niveau vers la version actuelle du pilote afin de disposer des mises à niveau les plus récentes.

Voici quelques exemples d'utilisation des métriques de performance :

- Résoudre les problèmes de performance d'instance.
- Choisir la taille d'instance appropriée pour une charge de travail.
- Planifier de manière proactive des activités de mise à l'échelle.
- Définir des points de référence pour les applications afin de déterminer si elles optimisent les performances disponibles sur une instance.

Taux de rafraîchissement

Par défaut, le pilote actualise les métriques à l'aide d'un intervalle d'une seconde. Toutefois, l'application qui récupère les métriques peut utiliser un autre intervalle pour l'interrogation. Vous pouvez modifier l'intervalle d'actualisation dans le Gestionnaire de périphériques à l'aide des propriétés avancées du pilote.

Pour modifier l'intervalle d'actualisation des métriques pour le pilote ENA Windows, procédez comme suit :

1. Ouvrez Exécuter à l'aide de l'une des méthodes décrites dans la section précédente.
2. Pour ouvrir le Gestionnaire de périphériques Windows, saisissez `devmgmt.msc` la fenêtre Exécuter.
3. Choisissez OK. La fenêtre du Gestionnaire de périphériques s'ouvre.
4. Sélectionnez la flèche qui apparaît à gauche de Cartes réseau pour développer la liste.
5. Choisissez le nom ou ouvrez le menu contextuel pour Amazon Elastic Network Adapter, puis choisissez Propriétés. Cela ouvre la boîte de dialogue Propriétés d'Amazon Elastic Network Adapter.
6. Ouvrez l'onglet Avancé dans la fenêtre contextuelle.
7. Dans la liste Propriété, choisissez Intervalle d'actualisation des métriques pour modifier la valeur.
8. Une fois que vous avez terminé, choisissez OK.

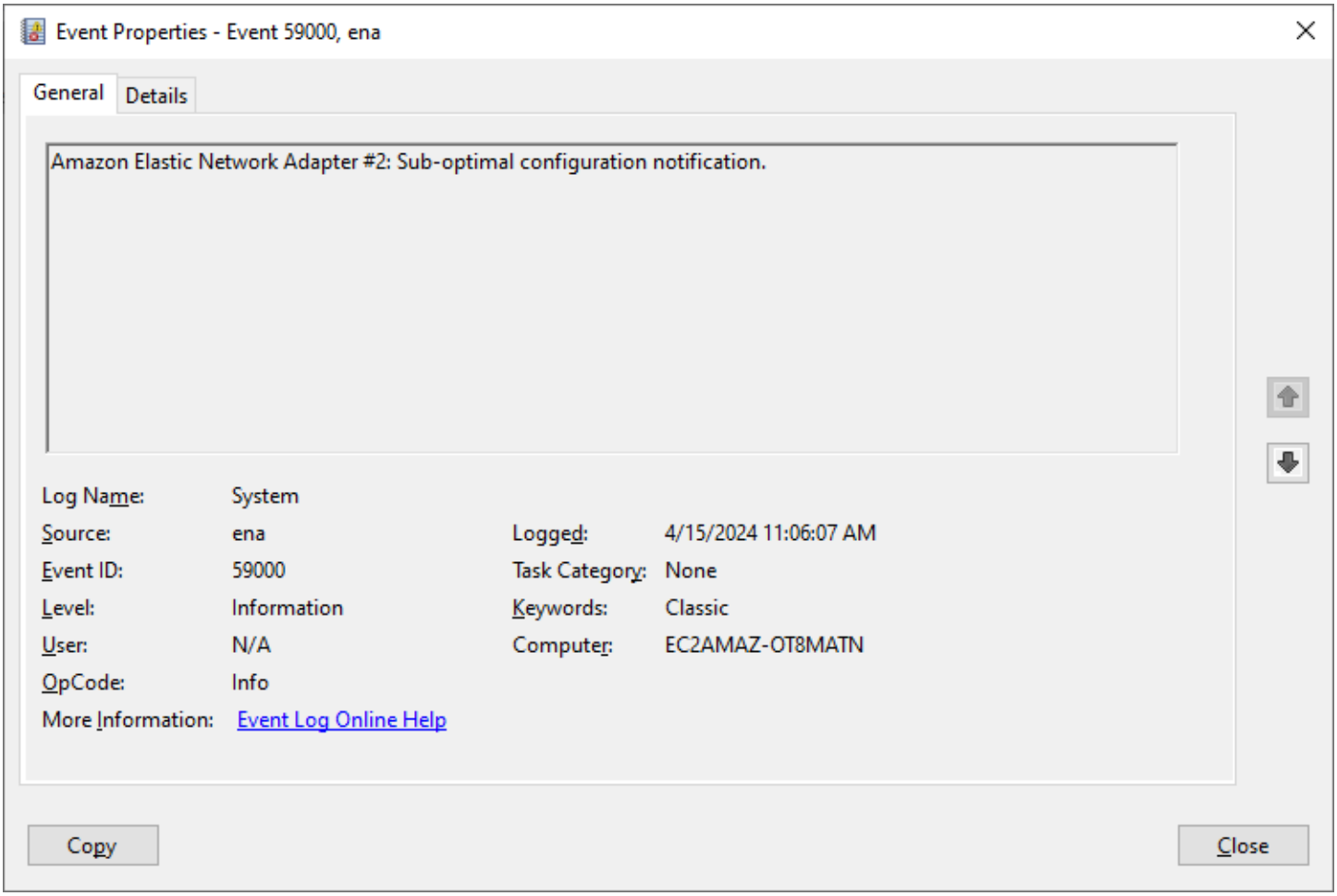
Étudier les notifications de configuration sous-optimales

Le ENA périphérique détecte des paramètres de configuration sous-optimaux dans le pilote que vous pouvez modifier. L'appareil avertit le ENA conducteur et enregistre une notification d'événement. Pour examiner les événements sous-optimaux dans l'Observateur d'événements Windows

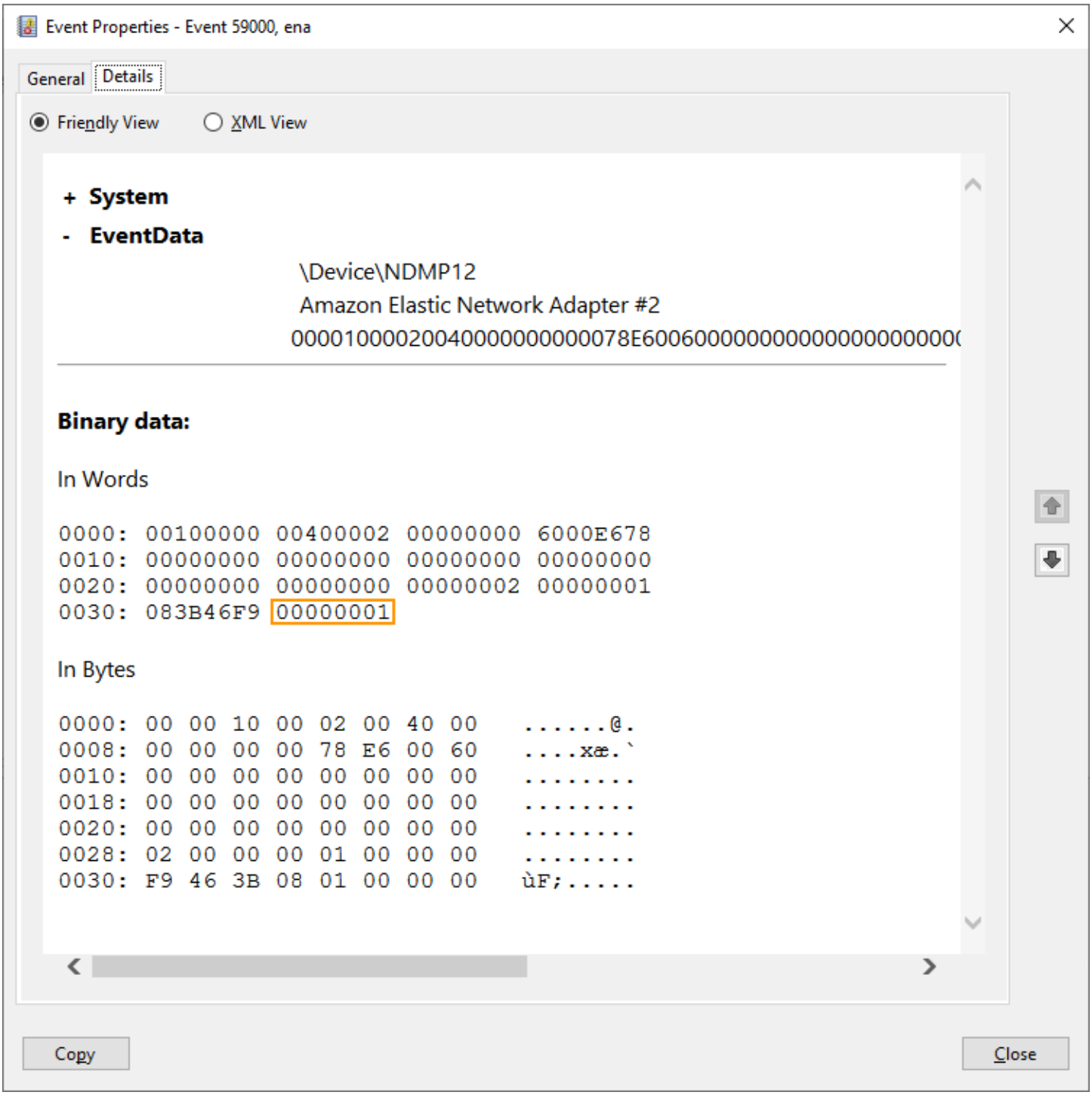
1. Ouvrez Exécuter à l'aide de l'une des méthodes décrites dans la section précédente.

2. Pour ouvrir l'Observateur d'événements Windows, saisissez `eventvwr.msc` dans la fenêtre Exécuter.
3. Choisissez OK. La fenêtre de l'Observateur d'événements s'ouvre.
4. Développez le menu Journaux Windows, puis choisissez Système.
5. Sous Actions, dans le panneau supérieur droit, choisissez Créer une vue personnalisée. La boîte de dialogue Filtrer s'affiche.
6. Dans la zone Sources d'événements, saisissez `ena`. Cela limite les résultats aux événements générés par le pilote ENA Windows.
7. Choisissez OK. Les résultats du journal d'événements filtrés s'affichent dans les sections des détails de la fenêtre.

Les événements associés à un ID vous `59000` signalent des résultats de configuration sous-optimaux. Cliquez avec le bouton droit sur un événement et choisissez Propriétés de l'événement pour ouvrir une vue détaillée, ou sélectionnez Volet d'aperçu dans le menu Affichage pour voir les mêmes détails.



Ouvrez l'onglet Détails pour voir le code de l'événement. Dans la section Données binaires : en mots, le dernier mot est le code.



La liste suivante indique les détails du code de notification et les actions recommandées pour les résultats de configuration sous-optimaux.

- Code **1** : ENA Express avec une LLQ configuration étendue n'est pas recommandé

ENAExpress ENI est configuré avec WideLLQ. Cette configuration n'est pas optimale et peut avoir un impact sur les performances d'ENAExpress. Nous vous recommandons de désactiver les LLQ paramètres étendus lorsque vous utilisez ENA Express ENIs comme suit.

1. Pour ouvrir le Gestionnaire de périphériques Windows, saisissez `devmgmt.msc` la fenêtre Exécuter.
2. Choisissez OK. La fenêtre du Gestionnaire de périphériques s’ouvre.
3. Sélectionnez la flèche qui apparaît à gauche de Cartes réseau pour développer la liste.
4. Ouvrez les propriétés de l'appareil pour`Amazon Elastic Network Adapter`.
5. À partir de là, ouvrez l'onglet Avancé pour apporter vos modifications.
6. Sélectionnez la propriété Politique de taille d'LLQen-tête et définissez sa valeur sur`Normal (128 Bytes)`.
7. Choisissez OK pour enregistrer vos modifications.

- Code **2** : ENA Express ENI avec une profondeur de file Tx sous-optimale n'est pas recommandé

  ENAExpress ENI est configuré avec une profondeur de file d'attente Tx sous-optimale. Cette configuration peut avoir un impact sur les performances d'ENAExpress. Nous vous recommandons d'agrandir toutes les files d'attente Tx à la valeur maximale de l'interface réseau lorsque vous utilisez ENA Express ENIs comme suit.

  Procédez comme suit pour agrandir les files d'attente Tx à la profondeur maximale :

  1. Pour ouvrir le Gestionnaire de périphériques Windows, saisissez `devmgmt.msc` la fenêtre Exécuter.
  2. Choisissez OK. La fenêtre du Gestionnaire de périphériques s’ouvre.
  3. Sélectionnez la flèche qui apparaît à gauche de Cartes réseau pour développer la liste.
  4. Ouvrez les propriétés de l'appareil pour`Amazon Elastic Network Adapter`.
  5. À partir de là, ouvrez l'onglet Avancé pour apporter vos modifications.
  6. Sélectionnez la propriété Transmit Buffers et définissez sa valeur sur le maximum pris en charge.
  7. Choisissez OK pour enregistrer vos modifications.

ENAréinitialisation de l'adaptateur

Le processus de réinitialisation démarre lorsque le pilote ENA Windows détecte une erreur sur un adaptateur et indique que celui-ci est défectueux. Le pilote ne peut pas se réinitialiser lui-même. Il dépend donc du système d'exploitation pour vérifier l'état de santé de l'adaptateur et appeler la poignée de réinitialisation du pilote ENA Windows. Le processus de réinitialisation peut entraîner une perte de traffic pendant une brève période. Cependant, TCP les connexions devraient pouvoir être rétablies.

L'ENAadaptateur peut également demander indirectement une procédure de réinitialisation de l'appareil, en omettant d'envoyer une notification de maintien en vie. Par exemple, si l'ENAadaptateur atteint un état inconnu après avoir chargé une configuration irrécupérable, il peut arrêter d'envoyer des notifications de maintien en vie.

Causes courantes de réinitialisation de ENA l'adaptateur

- Il manque des messages « keep-alive »

  L'ENAadaptateur publie les événements Keep-Alive à un rythme fixe (généralement une fois par seconde). Le pilote ENA Windows implémente un mécanisme de surveillance qui vérifie périodiquement la présence de ces messages de maintien en vie. S'il détecte un ou plusieurs nouveaux messages depuis la dernière vérification, il enregistre un résultat réussi. Sinon, le pilote conclut que le périphérique a subi une défaillance et lance une séquence de réinitialisation.
- Des paquets sont bloqués dans les files d'attente de transmission

  L'ENAadaptateur vérifie que les paquets circulent dans les files d'attente de transmission comme prévu. Le pilote ENA Windows détecte si des paquets sont bloqués et lance une séquence de réinitialisation s'ils le sont.
- Délai de lecture pour les registres d'E/S mappés en mémoire () MMIO

  Pour limiter les opérations de lecture des E/S mappées en mémoire (MMIO), le pilote ENA Windows accède aux MMIO registres uniquement pendant les processus d'initialisation et de réinitialisation. Si le pilote détecte un délai d'attente, il effectue l'une des actions suivantes, en fonction du processus en cours d'exécution :

  - Si un délai d'attente est détecté lors de l'initialisation, le flux échoue, ce qui entraîne l'affichage par le pilote d'un point d'exclamation jaune à côté de l'ENAadaptateur dans le Gestionnaire de périphériques Windows.

- Si un délai d'attente est détecté lors de la réinitialisation, le flux échoue. Le système d'exploitation lance alors un retrait surprise de l'ENAadaptateur et le récupère en arrêtant et en redémarrant l'adaptateur qui a été retiré. Pour plus d'informations sur le retrait surprise d'une carte d'interface réseau (NIC), consultez la section Gestion de la suppression surprise d'une carte NIC dans la documentation Microsoft Windows Hardware Developer.

Scénarios de résolution des problèmes

Les scénarios suivants peuvent vous aider à résoudre les problèmes que vous pourriez rencontrer avec le pilote ENA Windows. Nous vous recommandons de commencer par mettre à jour votre ENA pilote, si vous ne disposez pas de la dernière version. Pour trouver le pilote le plus récent pour la version de votre système d'exploitation Windows, consultez Suivez ENA les versions des pilotes Windows.

Version ENA du pilote installée de manière inattendue

Description

Après avoir suivi les étapes d'installation d'une version spécifique du ENA pilote, le Gestionnaire de périphériques Windows indique que Windows a installé une version différente du ENA pilote.

Cause

Lorsque vous exécutez l'installation d'un package de pilotes, Windows classe tous les packages de pilotes valides pour le périphérique concerné dans le magasin de pilotes local avant qu'elle ne commence. Il sélectionne ensuite le package ayant la valeur de classement la plus faible comme étant le mieux adapté. Il peut être différent du package que vous aviez l'intention d'installer. Pour plus d'informations sur le processus de sélection du package de pilotes de périphériques, consultez Comment Windows sélectionne un package de pilotes pour un périphérique sur le site Web de documentation de Microsoft.

Solution

Pour vous assurer que Windows installe la version du package de pilotes que vous avez choisie, vous pouvez supprimer les packages de pilotes de rang inférieur du magasin de pilotes à l'aide de l'outil de ligne de nPUtil commande P.

Pour mettre à jour le ENA pilote, procédez comme suit :

1. Connectez-vous à votre instance en tant qu'administrateur local.

2. Ouvrez la fenêtre Propriétés du Gestionnaire de périphériques, comme décrit dans la section Vérifier l'état ENA de l'appareil. L'onglet Général de la fenêtre Propriétés Amazon Elastic Network Adapter s'ouvre.
3. Ouvrez l'onglet Pilote.
4. Choisissez Mettre à jour le pilote. La boîte de dialogue Mettre à jour le logiciel du pilote – Amazon Elastic Network Adapter s'ouvre.
   a. Dans la section Comment voulez-vous rechercher le pilote ?, choisissez Rechercher un pilote sur mon ordinateur.
   b. Sur la page Rechercher des pilotes sur votre ordinateur, choisissez Laissez-moi choisir dans une liste de pilotes de périphériques sur mon ordinateur, située sous la barre de recherche.
   c. Sur la page Sélectionner le pilote de périphérique que vous voulez installer pour ce matériel, choisissez Je dispose d'un disque….
   d. Dans la fenêtre Installer à partir du disque, choisissez Parcourir…, à côté de l'emplacement de fichier de la liste déroulante.
   e. Accédez à l'emplacement où vous avez téléchargé le package de ENA pilotes cible. Sélectionnez le fichier nommé `ena.inf` et choisissez Ouvrir.
   f. Pour démarrer l'installation, cliquez sur OK, puis sur Suivant.
5. Si le programme d'installation ne redémarre pas automatiquement votre instance, exécutez l'Restart-Computer PowerShell applet de commande.

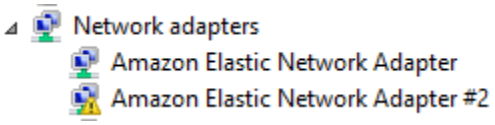
```
PS C:\> Restart-Computer
```

Avertissement relatif à l'appareil destiné au ENA conducteur

Description

L'icône de l'ENAadaptateur dans la section Adaptateurs réseau du Gestionnaire de périphériques affiche un panneau d'avertissement (un triangle jaune avec un point d'exclamation à l'intérieur).

L'exemple suivant montre un ENA adaptateur avec l'icône d'avertissement dans le Gestionnaire de périphériques Windows :



Cause

Cet avertissement est généralement dû à des problèmes d'environnement, qui peuvent nécessiter plus de recherches et requièrent généralement un processus d'élimination pour déterminer la cause sous-jacente. Pour obtenir la liste complète des erreurs du périphérique, consultez Gestionnaire de périphériques des messages d'erreur dans la documentation Microsoft Windows Hardware Developer.

Solution

La solution à cet avertissement de périphérique dépend de la cause racine. Le processus d'élimination décrit ici comprend des étapes de base pour identifier et résoudre les problèmes les plus courants et pouvant être simples à résoudre. Une analyse supplémentaire des causes racines est nécessaire lorsque ces étapes ne résolvent pas le problème.

Suivez ces étapes pour essayer d'identifier et de résoudre les problèmes courants :

1. Arrêter et démarrer le périphérique

   Ouvrez la fenêtre Propriétés du Gestionnaire de périphériques, comme décrit dans la section Vérifier l'état ENA de l'appareil. L'onglet Général de la fenêtre Propriétés de Amazon Elastic Network Adapter s'ouvre, et Statut de l'appareilaffiche le code d'erreur et un court message.

   a. Ouvrez l'onglet Pilote.
   b. Choisissez Désactiver l'appareil, et répondez Oui au message d'avertissement qui s'affiche.
   c. Choisissez Activer l'appareil.

2. Arrêtez et démarrez l'EC2instance

   Si l'adaptateur affiche toujours l'icône d'avertissement dans le Gestionnaire de périphériques, l'étape suivante consiste à arrêter et à démarrer l'EC2instance. Cette opération redémarre l'instance sur différents matériels dans la plupart des cas.

3. Examiner les problèmes possibles avec les ressources de l'instance

   Si vous avez arrêté et démarré votre EC2 instance et que le problème persiste, cela peut indiquer un problème de ressources sur votre instance, tel qu'une mémoire insuffisante.

Délai de connexion avec réinitialisation du dispositif (codes d’erreur 5007, 5205)

Description

L'Observateur d'événements Windows affiche les événements de temporisation et de réinitialisation des adaptateurs qui se produisent conjointement pour les ENA adaptateurs. Les messages ressemblent aux exemples suivants :

- Event ID 5007: Amazon Elastic Network Adapter : Timed out during an operation.
- Event ID 5205: Amazon Elastic Network Adapter : Adapter reset has been started.

Les réinitialisations du dispositif entraînent une perturbation minime du trafic. Même lorsqu’il y a plusieurs réinitialisations, il serait inhabituel qu’elles provoquent une perturbation grave du réseau.

Cause

Cette séquence d'événements indique que le pilote ENA Windows a initié une réinitialisation pour un ENA adaptateur qui ne répondait pas. Cependant, le mécanisme utilisé par le pilote du périphérique pour détecter ce problème est sujet à des faux positifs résultant d'une privation de nourriture CPU nulle.

Solution

Si cette combinaison d’erreurs se produit souvent, vérifiez les allocations de ressources pour voir où des ajustements peuvent être utiles.

1. Ouvrez Exécuter à l’aide de l’une des méthodes décrites dans la section précédente.
2. Pour ouvrir le Moniteur de ressources Windows, saisissez `resmon` dans la fenêtre Exécuter.
3. Choisissez OK. La fenêtre Moniteur de ressources s’ouvre alors.
4. Ouvrez l'CPUonglet. Les graphiques par CPU utilisation sont affichés sur le côté droit de la fenêtre Resource Monitor.
5. Vérifiez les niveaux d'utilisation à CPU 0 pour voir s'ils sont trop élevés.

Nous vous recommandons de configurer RSS pour exclure CPU 0 pour l'ENAadaptateur sur les types d'instances plus importants (plus de 16 vCPU). Pour les types d'instances plus petits, la configuration RSS peut améliorer l'expérience, mais en raison du nombre réduit de cœurs disponibles, des tests sont nécessaires pour garantir que le fait de limiter les CPU cœurs n'a pas d'impact négatif sur les performances.

Utilisez la Set-NetAdapterRss commande RSS pour configurer votre ENA adaptateur, comme indiqué dans l'exemple suivant.

```
Set-NetAdapterRss -name (Get-NetAdapter | Where-Object {$_.InterfaceDescription -like
 "*Elastic*"}).Name -Baseprocessorgroup 0 -BaseProcessorNumber 1
```

La migration vers une infrastructure d'instance de sixième génération a un impact sur les performances ou les attachements

Description

Si vous migrez vers une EC2 instance de sixième génération, vous risquez de rencontrer une baisse des performances ou des défaillances de ENA pièces jointes si vous n'avez pas mis à jour la version de votre pilote ENA Windows.

Cause

Les types d'EC2instance de sixième génération nécessitent la version minimale suivante du pilote ENA Windows, en fonction du système d'exploitation (OS) de l'instance.

Version minimale

Version Windows Server	Version du pilote ENA
Windows Server 2008 R2	2.2.3 ou 2.4.0
Windows Server 2012 et versions ultérieures	2.2.3 et ultérieures
Station de travail Windows	2.2.3 et ultérieures

Solution

Avant de passer à une instance de sixième génération, assurez-vous que l'EC2instance à partir de laquelle AMI vous lancez dispose de pilotes compatibles basés sur le système d'exploitation de l'instance, comme indiqué dans le tableau précédent. Pour plus d'informations, consultez Que dois-je faire avant de migrer mon EC2 instance vers une instance de sixième génération afin de garantir des performances réseau optimales ? dans le AWS re:Post Knowledge Center.

Performances sous-optimales de l'interface réseau Elastic

Description

L'ENAinterface ne fonctionne pas comme prévu.

Cause

L'analyse des causes racines des problèmes de performance est un processus d'élimination. Trop de variables sont impliquées pour nommer une cause commune.

Solution

La première étape de votre analyse des causes racines consiste à examiner les informations de diagnostic de l'instance qui ne fonctionne pas comme prévu afin de déterminer si des erreurs peuvent être à l'origine du problème. Pour plus d'informations, consultez la section Collecter des informations de diagnostic sur l'instance.

Il se peut que vous ayez besoin de modifier la configuration par défaut du système d'exploitation pour obtenir des performances réseau optimales sur les instances dont la mise en réseau est améliorée. Certaines optimisations, telles que l'activation et l'activation du déchargement par checksumRSS, sont configurées par défaut dans Windows officiel. AMIs Pour les autres optimisations que vous pouvez appliquer à l'ENAadaptateur, consultez les réglages de performance présentés dans. ENAréglages des performances de l'adaptateur

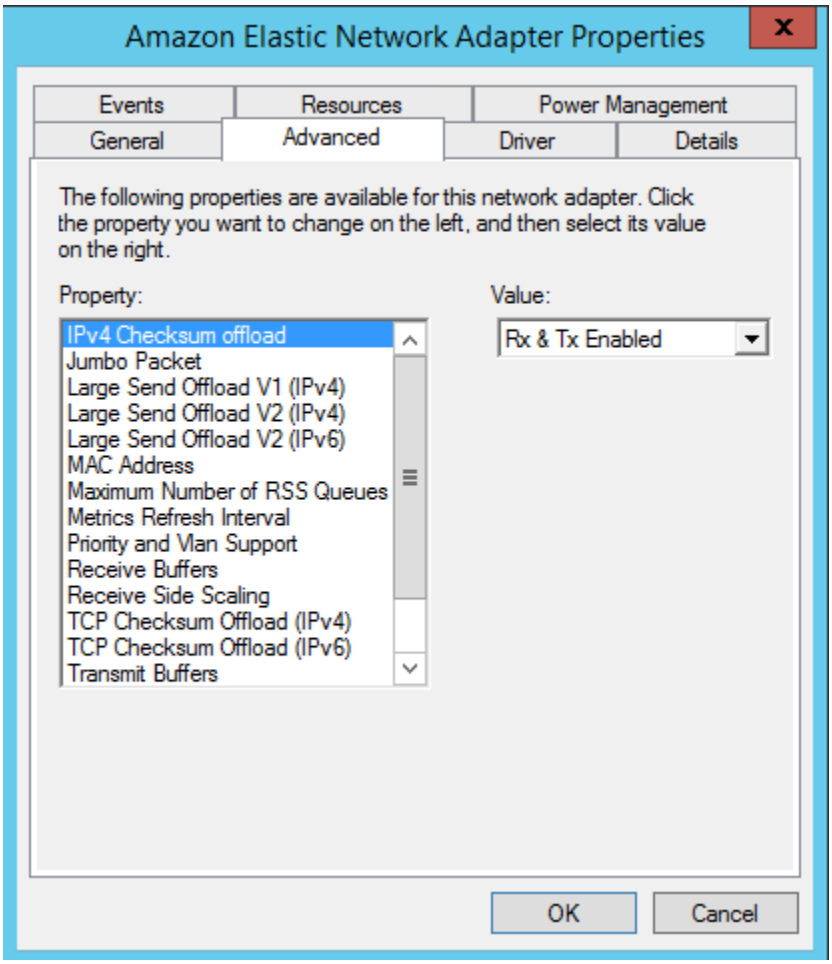
Nous vous recommandons de procéder avec prudence et de limiter les modifications des propriétés de l'appareil à celles répertoriées dans cette section ou aux modifications spécifiques recommandées par l'équipe d' AWS assistance.

Pour modifier les propriétés de l'ENAadaptateur, procédez comme suit :

1. Ouvrez Exécuter à l'aide de l'une des méthodes décrites dans la section précédente.
2. Pour ouvrir le Gestionnaire de périphériques Windows, saisissez `devmgmt.msc` la fenêtre Exécuter.
3. Choisissez OK. La fenêtre du Gestionnaire de périphériques s'ouvre.
4. Sélectionnez la flèche qui apparaît à gauche de Cartes réseau pour développer la liste.
5. Choisissez le nom ou ouvrez le menu contextuel pour Amazon Elastic Network Adapter, puis choisissez Propriétés. Cela ouvre la boîte de dialogue Propriétés d'Amazon Elastic Network Adapter.
6. Pour effectuer vos modifications, ouvrez l'onglet Avancé.

7. Lorsque vous avez terminé, sélectionnez OK pour enregistrer les modifications.

L'exemple suivant montre une propriété d'ENAadaptateur dans le Gestionnaire de périphériques Windows :



ENAréglages des performances de l'adaptateur

Le tableau suivant inclut les propriétés qui peuvent être ajustées pour améliorer les performances de l'ENAinterface.

Entrée

Propriété	Description	Valeur par défaut	Ajustement
Tampons de réception	Contrôle le nombre d'entrées dans les	1 024	Peut être augmenté jusqu'à 8 192 au maximum.

Propriété	Description	Valeur par défaut	Ajustement
	files d'attente de réception du logiciel.		
Dimensionnement côté réception (RSS)	Permet de répartir efficacement le traitement de réception réseau sur plusieurs CPUs systèmes multiprocesseurs.	Activées	Vous pouvez répartir la charge sur plusieurs processeurs. Pour en savoir plus, veuillez consulter la section Optimisation des performances réseau sur les instances EC2 Windows.

Propriété	Description	Valeur par défaut	Ajustement
Nombre maximum de files d'RSSattente	Définit le nombre maximum de RSS files d'attente autorisées lorsque cette option RSS est activée.	32	Le nombre de RSS files d'attente est déterminé lors de l'initialisation du pilote et inclut les limitations suivantes (entre autres) : • RSSlimite de file d'attente définie par cette propriété • Limites d'instances (CPUnombre de v) • Limites de génération de matériel (jusqu'à 8 RSS files d'attente ENAv1 entrantes et jusqu'à 32 RSS files d'attente entrantes) ENAv2 Vous pouvez définir une valeur entre 1 et 32, en fonction des limites de génération de votre instance et de votre matériel. Pour en savoir plus, veuillez consulter

Propriété	Description	Valeur par défaut	Ajustement
			la section Optimisation des performances réseau sur les instances EC2 Windows.
Paquet jumbo	Permet l'utilisation de trames ethernet jumbo (plus de 1 500 octets de charge utile).	Désactivé (cela limite la charge utile à 1 500 octets)	La valeur peut être configurée sur `9015`, ce qui se traduit par 9 001 octets de charge utile. Il s'agit de la charge utile maximale pour les trames ethrnet jumbo. veuillez consulter Considérations relatives à l'utilisation de trames ethernet jumbo.

Considérations relatives à l'utilisation de trames ethernet jumbo

Les trames jumbo permettent d'utiliser plus de 1 500 octets de données en augmentant la charge utile par paquet, et donc en augmentant le pourcentage de paquet qui ne constitue pas des frais supplémentaires. Moins de paquets sont nécessaires pour envoyer le même volume de données utilisables. Toutefois, le trafic est limité à un maximum MTU de 1 500 dans les cas suivants :

- Trafic en dehors d'une AWS région donnée pour EC2 Classic.
- Trafic extérieur à un singleVPC.
- Trafic via une connexion de VPC peering interrégionale.
- Trafic sur VPN les connexions.
- Trafic sur une passerelle Internet.

> **Note**
>
> Les paquets de plus de 1 500 octets sont fragmentés. Si vous avez l'indicateur `Don't Fragment` défini dans l'en-tête IP, ces paquets sont supprimés.
> Les cadres Jumbo doivent être utilisés avec prudence pour le trafic lié à Internet ou pour tout trafic sortant d'un. VPC Les paquets sont fragmentés par des systèmes intermédiaires, ce qui ralentit le trafic. Pour utiliser des trames jumbo à l'intérieur d'un VPC sans affecter le trafic sortant duVPC, essayez l'une des options suivantes :
>
> - Configurez la MTU taille par itinéraire.
> - Utilisez plusieurs interfaces réseau de différentes MTU tailles et de différents itinéraires.

Cas d'utilisation recommandés pour les trames jumbo

Les cadres Jumbo peuvent être utiles pour le trafic à l'intérieur et entre les deuxVPCs. Nous vous recommandons d'utiliser des trames jumbo pour les cas d'utilisation suivants :

- Pour les instances situées dans un même groupe de placement du cluster, les trames jumbo permettent d'atteindre le débit réseau maximum possible. Pour plus d'informations, consultez Groupes de placement pour vos EC2 instances Amazon.
- Vous pouvez utiliser des trames jumbo pour le trafic entre votre réseau VPCs et votre réseau local. AWS Direct Connect Pour plus d'informations sur l'utilisation AWS Direct Connect et la vérification de la fonctionnalité des trames jumbo, voir Configurer le réseau MTU pour les interfaces virtuelles privées ou les interfaces virtuelles de transit dans le guide de l'AWS Direct Connect utilisateur.
- Pour plus d'informations sur les MTU tailles prises en charge pour les passerelles de transit, consultez la section Quotas pour vos passerelles de transit dans Amazon VPC Transit Gateways.

Améliorez la latence du réseau pour les EC2 instances basées sur Linux

La latence réseau est le temps nécessaire à un paquet de données pour voyager de sa source à sa destination. Les applications qui envoient des données via le réseau ont besoin de réponses rapides pour offrir une expérience utilisateur positive. Une latence réseau élevée peut entraîner divers problèmes, tels que les suivants :

- Temps de chargement lents des pages Web
- Retard des flux vidéo

- Difficulté d'accès aux ressources en ligne

Cette section décrit les mesures que vous pouvez prendre pour améliorer la latence du réseau sur les EC2 instances Amazon qui s'exécutent sous Linux. Pour obtenir une latence optimale, suivez ces étapes pour configurer les paramètres de votre instance, de votre noyau et de votre ENA pilote. Pour obtenir des conseils de configuration supplémentaires, consultez le guide des meilleures pratiques et d'optimisation des performances des pilotes ENA Linux surGitHub.

> **Note**
>
> Les étapes et les paramètres peuvent varier légèrement en fonction de votre matériel réseau spécifique, de l'appareil AMI à partir duquel vous avez lancé votre instance et du cas d'utilisation de votre application. Avant d'apporter des modifications, testez et surveillez minutieusement les performances de votre réseau pour vous assurer d'obtenir les résultats souhaités.

Réduisez le nombre de sauts réseau pour les paquets de données

Chaque saut effectué par un paquet de données lorsqu'il passe d'un routeur à l'autre augmente la latence du réseau. En général, le trafic doit effectuer plusieurs sauts pour atteindre votre destination. Il existe deux méthodes pour réduire les sauts de réseau pour vos EC2 instances Amazon, comme suit :

- Groupe de placement de clusters : lorsque vous spécifiez un groupe de placement de clusters, Amazon EC2 lance des instances situées à proximité les unes des autres, physiquement au sein de la même zone de disponibilité (AZ) avec un emballage plus serré. La proximité physique des instances du groupe leur permet de profiter d'une connectivité à haut débit, ce qui se traduit par une faible latence et un débit de flux unique élevé.
- Hôte dédié : un hôte dédié est un serveur physique qui vous est dédié. Avec un hôte dédié, vous pouvez lancer vos instances pour qu'elles s'exécutent sur le même serveur physique. La communication entre les instances qui s'exécutent sur le même hôte dédié peut se faire sans sauts réseau supplémentaires.

Comment la configuration du noyau Linux affecte la latence

La configuration du noyau Linux peut augmenter ou diminuer la latence du réseau. Pour atteindre vos objectifs d'optimisation de la latence, il est important d'affiner la configuration du noyau Linux en fonction des exigences spécifiques de votre charge de travail.

Il existe de nombreuses options de configuration du noyau Linux qui peuvent contribuer à réduire la latence du réseau. Les options les plus efficaces sont les suivantes.

- Activer le mode d'interrogation occupé : le mode d'interrogation occupé réduit la latence sur le chemin de réception du réseau. Lorsque vous activez le mode d'interrogation occupé, le code de la couche de socket peut interroger directement la file d'attente de réception d'un périphérique réseau. L'inconvénient d'un sondage chargé est CPU l'augmentation de l'utilisation sur l'hôte, due à la recherche de nouvelles données en boucle étroite. Il existe deux paramètres globaux qui contrôlent le nombre de microsecondes d'attente des paquets pour toutes les interfaces.

  `busy_read`

  Un délai d'interrogation intensive de faible latence pour les lectures de sockets. Cela contrôle le nombre de microsecondes à attendre pour que la couche de socket lise les paquets dans la file d'attente du périphérique. Pour activer la fonction globalement avec la commande sysctl, l'organisation Linux Kernel recommande une valeur de 50 microsecondes. Pour plus d'informations, consultez busy_read dans le guide de l'utilisateur et de l'administrateur du noyau Linux.

  ```
  $ C:\> sudo sysctl -w net.core.busy_read=50
  ```

  `busy_poll`

  Un délai d'interrogation intensive de faible latence pour poll et select. Cela contrôle le nombre de microsecondes à attendre pour que les événements se produisent. La valeur recommandée se situe entre 50 et 100 microsecondes, en fonction du nombre de sockets que vous interrogez. Plus vous ajoutez de sockets, plus la valeur doit être élevée.

  ```
  $ C:\> sudo sysctl -w net.core.busy_poll=50
  ```

- Configurer les états CPU d'alimentation (états C) — Les états C contrôlent les niveaux de sommeil dans lesquels un cœur peut entrer lorsqu'il est inactif. Il se peut que vous vouliez contrôler les états

« C-state » pour ajuster la latence de votre système par rapport aux performances. Dans les états C plus profonds, CPU il est essentiellement « endormi » et ne peut pas répondre aux demandes tant qu'il ne se réveille pas et ne revient pas à un état actif. La mise en veille de cœurs prend du temps. Même si un cœur en veille donne plus de marge pour qu'un autre cœur fonctionne à une fréquence plus élevée, ce cœur en veille prend du temps pour se remettre en route et fonctionner.

Par exemple, si un cœur qui est assigné à la gestion des interruptions de paquets est en veille, il se peut que la prise en charge de cette interruption soit retardée. Vous pouvez configurer le système de manière à ce qu'il n'utilise pas d'états C profonds. Cependant, si cette configuration réduit la latence de réaction du processeur, elle réduit également la marge de manœuvre dont disposent les autres cœurs pour Turbo Boost.

Pour réduire la latence de réaction du processeur, vous pouvez limiter les états C-states plus approfondis. Pour plus d'informations, consultez la section Performances élevées et faible latence en limitant les états C plus profonds dans le guide de l'utilisateur Amazon Linux 2.

ENAconfiguration du pilote réseau

Le pilote ENA réseau permet la communication entre une instance et un réseau. Le pilote traite les paquets réseau et les transmet à la pile réseau ou à la carte Nitro. Lorsqu'un paquet réseau arrive, la carte Nitro génère une interruption CPU pour informer le logiciel d'un événement.

Interruption

Une interruption est un signal qu'un périphérique ou une application envoie au processeur. L'interruption indique au processeur qu'un événement s'est produit ou qu'une condition qui a été remplie nécessite une attention immédiate. Les interruptions peuvent gérer des tâches sensibles au temps, telles que la réception de données d'une interface réseau, la gestion d'événements matériels ou le traitement de demandes émanant d'autres périphériques.

Modération des interruptions

La modération des interruptions est une technique qui réduit le nombre d'interruptions générées par un périphérique en les regroupant ou en les retardant. L'objectif de la modération d'interruptions est d'améliorer les performances du système en réduisant la surcharge associée à la gestion d'un grand nombre d'interruptions. Trop d'interruptions augmentent CPU l'utilisation, ce qui a un impact négatif sur le débit, tandis que trop peu d'interruptions augmentent la latence.

Modération dynamique des interruptions

La modération dynamique des interruptions est une forme améliorée de modération des interruptions qui ajuste dynamiquement le taux d'interruption en fonction de la charge actuelle du système et des modèles de trafic. Elle vise à trouver un équilibre entre la réduction du nombre d'interruptions et le nombre de paquets par seconde, ou bande passante.

> **Note**
>
> La modération dynamique des interruptions est activée par défaut dans certains AMIs cas (mais elle peut être activée ou désactivée dans tousAMIs).

Pour minimiser la latence réseau, il peut être nécessaire de désactiver la modération des interruptions Toutefois, cela peut également augmenter la charge de traitement des interruptions. Il est important de trouver le juste équilibre entre la réduction de la latence et la réduction de la charge. Les commandes `ethtool` peuvent vous aider à configurer la modération des interruptions. Par défaut, `rx-usecs` a la valeur de `20`, et `tx-usecs` a la valeur `64`.

Pour obtenir la configuration actuelle de modification des interruptions, utilisez la commande suivante.

```
$ C:\> ethtool -c interface | egrep "rx-usecs:|tx-usecs:|Adaptive RX"
Adaptive RX: on  TX: off
rx-usecs: 20
tx-usecs: 64
```

Pour désactiver la modification des interruptions et la modération dynamique des interruptions, utilisez la commande suivante.

```
$ C:\> sudo ethtool -C interface adaptive-rx off rx-usecs 0 tx-usecs 0
```

Considérations relatives au système Nitro pour le réglage des performances

Le Système Nitro est un ensemble de composants matériels et logiciels élaborés par AWS qui garantissent des performances élevées, une haute disponibilité et un niveau de sécurité élevé. Le système Nitro fournit des fonctionnalités similaires au bare metal qui éliminent les frais de virtualisation et prennent en charge les charges de travail qui nécessitent un accès complet au matériel hôte. Pour des informations plus détaillées, consultez AWS Nitro System.

Tous les types d'EC2instances de la génération actuelle exécutent le traitement des paquets réseau sur les cartes EC2 Nitro. Cette rubrique traite de la gestion des paquets de haut niveau sur la carte Nitro, des aspects courants de l'architecture et de la configuration du réseau qui ont un impact sur les performances de traitement des paquets, et des mesures que vous pouvez prendre pour optimiser les performances de vos instances basées sur Nitro.

Les cartes Nitro gèrent toutes les interfaces d'entrée et de sortie (E/S), telles que celles nécessaires aux clouds privés virtuels ()VPCs. Pour tous les composants qui envoient ou reçoivent des informations sur le réseau, les cartes Nitro agissent comme un dispositif informatique autonome pour le trafic d'E/S, physiquement distinct de la carte mère du système sur laquelle s'exécutent les charges de travail des clients.

Flux de paquets réseau sur les cartes Nitro

EC2les instances basées sur le système Nitro disposent de capacités d'accélération matérielle qui permettent un traitement des paquets plus rapide, tel que mesuré par le débit de paquets par seconde (PPS). Lorsqu'une carte Nitro effectue l'évaluation initiale d'un nouveau flux, elle enregistre des informations identiques pour tous les paquets du flux, telles que les groupes de sécurité, les listes de contrôle d'accès et les entrées des tables de routage. Lorsqu'il traite des paquets supplémentaires pour le même flux, il peut utiliser les informations enregistrées pour réduire la surcharge associée à ces paquets.

Votre débit de connexion est mesuré par la métrique de connexions par seconde (CPS). Chaque nouvelle connexion nécessite une surcharge de traitement supplémentaire qui doit être prise en compte dans les estimations de capacité de charge de travail. Il est important de prendre en compte à la fois les PPS indicateurs CPS et les indicateurs lorsque vous concevez vos charges de travail.

Comment établir une connexion

Lorsqu'une connexion est établie entre une instance basée sur Nitro et un autre point de terminaison, la carte Nitro évalue le flux complet du premier paquet envoyé ou reçu entre les deux points de terminaison. Pour les paquets suivants du même flux, une réévaluation complète n'est généralement pas nécessaire. Il existe toutefois des exceptions. Pour plus d'informations sur les exceptions, consultezPaquets qui n'utilisent pas l'accélération matérielle.

Les propriétés suivantes définissent les deux points de terminaison et le flux de paquets entre eux. Ensemble, ces cinq propriétés sont connues sous le nom de flux à 5 tuples.

- IP Source

- Port source
- IP de destination
- Port de destination
- Protocole de communication

La direction du flux de paquets est appelée entrée (entrée) et sortie (sortie). Les descriptions de haut niveau suivantes résument le flux de paquets réseau de bout en bout.

- Entrée : lorsqu'une carte Nitro gère un paquet réseau entrant, elle l'évalue par rapport aux règles de pare-feu dynamiques et aux listes de contrôle d'accès. Il suit la connexion, la mesure et effectue d'autres actions, le cas échéant. Il transmet ensuite le paquet à sa destination sur l'hôteCPU.
- Sortie : lorsqu'une carte Nitro gère un paquet réseau sortant, elle recherche la destination de l'interface distante, évalue diverses VPC fonctions, applique des limites de débit et effectue les autres actions applicables. Il transmet ensuite le paquet à sa destination de saut suivant sur le réseau.

Concevez votre réseau pour des performances optimales

Pour tirer parti des capacités de performance de votre système Nitro, vous devez comprendre quels sont vos besoins en matière de traitement réseau et comment ces besoins affectent la charge de travail de vos ressources Nitro. Vous pouvez ensuite concevoir des performances optimales pour votre environnement réseau. Les paramètres de votre infrastructure ainsi que la conception et la configuration de la charge de travail des applications peuvent avoir un impact à la fois sur le traitement des paquets et sur les taux de connexion. Par exemple, si votre application présente un taux d'établissement de connexion élevé, tel qu'un DNS service, un pare-feu ou un routeur virtuel, elle aura moins de chances de tirer parti de l'accélération matérielle qui ne se produit qu'une fois la connexion établie.

Vous pouvez configurer les paramètres de l'application et de l'infrastructure pour rationaliser les charges de travail et améliorer les performances du réseau. Cependant, tous les paquets ne sont pas éligibles à l'accélération. Le système Nitro utilise l'intégralité du flux réseau pour les nouvelles connexions et pour les paquets qui ne sont pas éligibles à l'accélération.

Le reste de cette section se concentrera sur les considérations relatives à la conception des applications et de l'infrastructure afin de garantir que les paquets circulent autant que possible selon le chemin accéléré.

Considérations relatives à la conception du réseau pour le système Nitro

Lorsque vous configurez le trafic réseau pour votre instance, de nombreux aspects peuvent affecter les PPS performances à prendre en compte. Une fois qu'un flux est établi, la majorité des paquets qui entrent ou sortent régulièrement sont éligibles à l'accélération. Cependant, des exceptions existent pour garantir que les conceptions d'infrastructure et les flux de paquets continuent de répondre aux normes du protocole.

Pour tirer le meilleur parti de votre carte Nitro, vous devez examiner attentivement les avantages et les inconvénients des détails de configuration suivants pour votre infrastructure et vos applications.

Considérations relatives aux infrastructures

La configuration de votre infrastructure peut affecter le flux de paquets et l'efficacité du traitement. La liste suivante inclut quelques points importants à prendre en compte.

Configuration de l'interface réseau avec asymétrie

- Les groupes de sécurité utilisent le suivi des connexions pour suivre les informations relatives au trafic entrant et sortant de l'instance. Le routage asymétrique, selon lequel le trafic entre dans une instance via une interface réseau et en sort par une interface réseau différente, peut réduire les performances maximales qu'une instance peut atteindre si les flux sont suivis. Pour plus d'informations sur le suivi des connexions des groupes de sécurité, les connexions non suivies et les connexions suivies automatiquement, consultezSuivi des connexions du groupe de EC2 sécurité Amazon.

Pilotes réseau

- Les pilotes réseau sont régulièrement mis à jour et publiés. Si vos pilotes ne sont pas à jour, cela peut nuire considérablement aux performances. Maintenez vos pilotes à jour pour vous assurer que vous disposez des derniers correctifs et que vous pouvez tirer parti des améliorations de performances, telles que la fonction de trajectoire accélérée qui n'est disponible que pour la dernière génération de pilotes. Les pilotes antérieurs ne prennent pas en charge la fonction de trajectoire accélérée.

  Pour tirer parti de la fonctionnalité de chemin accéléré, nous vous recommandons d'installer le dernier ENA pilote sur vos instances.

  Instances Linux : pilote ENA Linux 2.2.9 ou version ultérieure. Pour installer ou mettre à jour le pilote ENA Linux depuis le GitHub référentiel Amazon Drivers, consultez la section Compilation du pilote du fichier readme.

Instances Windows : pilote ENA Windows 2.0.0 ou version ultérieure. Pour installer ou mettre à jour le pilote ENA Windows, voirInstallation du ENA pilote sur les instances EC2 Windows.

Distance entre les points de terminaison

Une connexion entre deux instances de la même zone de disponibilité peut traiter plus de paquets par seconde qu'une connexion entre régions en raison du TCP fenêtrage de la couche application, qui détermine la quantité de données pouvant être en vol à un moment donné. Les longues distances entre les instances augmentent la latence et diminuent le nombre de paquets que les points de terminaison peuvent traiter.

Considérations relatives à la conception de

Certains aspects de la conception et de la configuration des applications peuvent affecter l'efficacité de votre traitement. La liste suivante inclut quelques points importants à prendre en compte.

Taille du paquet

Des paquets de plus grande taille peuvent augmenter le débit des données qu'une instance peut envoyer et recevoir sur le réseau. Des paquets de plus petite taille peuvent augmenter le taux de traitement des paquets, mais cela peut réduire la bande passante maximale atteinte lorsque le nombre de paquets dépasse les limites PPS autorisées.

Si la taille d'un paquet dépasse l'unité de transmission maximale (MTU) d'un saut réseau, un routeur situé le long du chemin peut le fragmenter. Les fragments de paquets qui en résultent sont considérés comme des exceptions et sont traités au rythme standard (et non accéléré). Cela peut entraîner des variations dans vos performances. Amazon EC2 prend en charge les trames jumbo de 9001 octets, mais tous les services ne le prennent pas en charge. Nous vous recommandons d'évaluer votre topologie lors de la configurationMTU.

Compromis liés au protocole

Les protocoles fiables de TCP ce type ont plus de surcharge que les protocoles peu UDP fiables. La réduction des frais généraux et la simplification du traitement réseau pour le protocole de UDP transport peuvent entraîner un PPS débit plus élevé, mais au détriment de la fiabilité de la livraison des paquets. Si la fiabilité de la livraison des paquets n'est pas essentielle pour votre application, UDP cela peut être une bonne option.

Micro-éclatement

La micro-explosion se produit lorsque le trafic dépasse les limites pendant de brèves périodes au lieu d'être réparti uniformément. Cela se produit généralement à l'échelle de la microseconde.

Supposons, par exemple, que vous disposiez d'une instance capable d'envoyer jusqu'à 10 Gbit/s et que votre application envoie la totalité des 10 Go en une demi-seconde. Cette micro-rafale dépasse la limite autorisée pendant la première demi-seconde et ne laisse rien pour le reste de la seconde. Même si vous avez envoyé 10 Go au cours de la période d'une seconde, les allocations pendant la première demi-seconde peuvent entraîner la mise en file d'attente ou le rejet de paquets.

Vous pouvez utiliser un planificateur réseau tel que Linux Traffic Control pour accélérer votre débit et éviter de provoquer des mises en file d'attente ou des pertes de paquets à la suite de microrafales.

Nombre de flux

Un flux unique est limité à 5 Gbit/s, sauf s'il fait partie d'un groupe de placement de clusters prenant en charge jusqu'à 10 Gbit/s, ou s'il utilise ENA Express, qui prend en charge jusqu'à 25 Gbit/s.

De même, une carte Nitro peut traiter un plus grand nombre de paquets sur plusieurs flux au lieu d'utiliser un seul flux. Pour atteindre le taux de traitement de paquets maximal par instance, nous recommandons d'utiliser au moins 100 flux sur les instances dont la bande passante cumulée est supérieure ou égale à 100 Gbit/s. À mesure que les capacités de bande passante agrégée augmentent, le nombre de flux nécessaires pour atteindre des taux de traitement de pointe augmente également. L'analyse comparative vous aidera à déterminer la configuration dont vous avez besoin pour atteindre des débits de pointe sur votre réseau.

Nombre de files d'attente d'Elastic Network Adapter (ENA)

Par défaut, le nombre maximum de ENA files d'attente est alloué à une interface réseau en fonction de la taille et du type de votre instance. La réduction du nombre de files d'attente peut réduire le PPS taux maximal réalisable. Nous vous recommandons d'utiliser l'allocation de file d'attente par défaut pour de meilleures performances.

Pour Linux, une interface réseau est configurée avec le maximum par défaut. Pour les applications basées sur le kit de développement du plan de données (DPDK), nous vous recommandons de configurer le nombre maximum de files d'attente disponibles.

Fonctionnalité : surcharge du processus

Des fonctionnalités telles que Traffic Mirroring et ENA Express peuvent augmenter la charge de traitement, ce qui peut réduire les performances absolues de traitement des paquets. Vous pouvez limiter l'utilisation des fonctionnalités ou les désactiver pour augmenter les taux de traitement des paquets.

Suivi des connexions pour maintenir l'état

Vos groupes de sécurité utilisent le suivi des connexions pour stocker des informations sur le trafic à destination et en provenance de l'instance. Le suivi des connexions applique des règles à chaque flux individuel de trafic réseau afin de déterminer si le trafic est autorisé ou refusé. La carte Nitro utilise le suivi du flux pour maintenir l'état du flux. À mesure que de plus en plus de règles de groupe de sécurité sont appliquées, davantage de travail est nécessaire pour évaluer le flux.

> **Note**
>
> Les flux de trafic réseau ne sont pas tous suivis. Si une règle de groupe de sécurité est configurée avecConnexions non suivies, aucune tâche supplémentaire n'est requise, à l'exception des connexions qui sont automatiquement suivies pour garantir un routage symétrique lorsqu'il existe plusieurs chemins de réponse valides.

Paquets qui n'utilisent pas l'accélération matérielle

Tous les paquets ne peuvent pas tirer parti de l'accélération matérielle. La gestion de ces exceptions implique une certaine surcharge de traitement, nécessaire pour garantir l'intégrité de vos flux réseau. Les flux réseau doivent respecter de manière fiable les normes de protocole, se conformer aux modifications de VPC conception et acheminer les paquets uniquement vers les destinations autorisées. Cependant, les frais généraux réduisent vos performances.

Fragments de paquets

Comme indiqué dans la section Considérations relatives aux applications, les fragments de paquets résultant de paquets dépassant le réseau MTU sont traités comme des exceptions et ne peuvent pas tirer parti de l'accélération matérielle.

Connexions inactives

Lorsqu'une connexion n'est pas active pendant un certain temps, même si le délai d'expiration de la connexion n'est pas atteint, le système peut annuler sa priorité. Ensuite, si les données arrivent après que la connexion n'a plus été priorisée, le système doit les traiter comme une exception pour pouvoir se reconnecter.

Pour gérer vos connexions, vous pouvez utiliser les délais de suivi des connexions pour fermer les connexions inactives. Vous pouvez également utiliser TCP keepalives pour maintenir ouvertes

les connexions inactives. Pour de plus amples informations, veuillez consulter Délai de suivi d'inactivité de la connexion.

VPCmutation

Les mises à jour des groupes de sécurité, des tables de routage et des listes de contrôle d'accès doivent toutes être réévaluées dans le processus de traitement afin de garantir que les entrées de routage et les règles des groupes de sécurité s'appliquent toujours comme prévu.

ICMPflux

Le protocole Internet Control Message Protocol (ICMP) est un protocole de couche réseau utilisé par les périphériques réseau pour diagnostiquer les problèmes de communication réseau. Ces paquets utilisent toujours le flux complet.

Optimisez les performances du réseau sur votre système Nitro

Avant de prendre des décisions de conception ou d'ajuster les paramètres réseau de votre instance, nous vous recommandons de suivre les étapes suivantes pour obtenir les meilleurs résultats :

1. Comprenez les avantages et les inconvénients des mesures que vous pouvez prendre pour améliorer les performances en procédant à un examenConsidérations relatives à la conception du réseau pour le système Nitro.

   Pour en savoir plus et connaître les meilleures pratiques relatives à la configuration de votre instance sous Linux, consultez le Guide des meilleures pratiques et de l'optimisation des performances des pilotes ENA Linux sur GitHub.
2. Comparez vos charges de travail avec le nombre de flux actifs de pointe afin de déterminer une base de référence pour les performances de votre application. Avec une référence de performance, vous pouvez tester les variations de vos paramètres ou de la conception de votre application afin de déterminer quelles considérations auront le plus d'impact, en particulier si vous prévoyez de procéder à une mise à l'échelle ou à une extension externe.

La liste suivante contient les actions que vous pouvez entreprendre pour optimiser vos PPS performances, en fonction des besoins de votre système.

- Réduisez la distance physique entre deux instances. Lorsque les instances d'envoi et de réception sont situées dans la même zone de disponibilité ou utilisent des groupes de placement de clusters,

vous pouvez réduire le nombre de sauts qu'un paquet doit effectuer pour se déplacer d'un point de terminaison à un autre.

- Utilisez Connexions non suivies.
- Utilisez le UDP protocole pour le trafic réseau.
- Pour les EC2 instances dont la bande passante cumulée est supérieure ou égale à 100 Gbit/s, répartissez la charge de travail sur au moins 100 flux individuels afin de répartir le travail de manière uniforme sur la carte Nitro.

Surveiller les performances sur les instances Linux

Vous pouvez utiliser les métriques Ethtool sur les instances Linux pour surveiller les indicateurs de performance réseau des instances tels que la bande passante, le débit de paquets et le suivi des connexions. Pour de plus amples informations, veuillez consulter Surveillez les performances du réseau pour ENA les paramètres de votre EC2 instance.

Optimisation des performances réseau sur les instances EC2 Windows

Pour optimiser les performances réseau de vos instances Windows grâce à une mise en réseau améliorée, vous devrez peut-être modifier la configuration par défaut du système d'exploitation. Nous recommandons les modifications de configuration suivantes pour les applications nécessitant des performances réseau élevées. D'autres optimisations (telles que l'activation du déchargement par checksum et son activationRSS, par exemple) sont déjà configurées sur Windows officiel. AMIs

> **Note**
>
> TCPle déchargement par cheminée doit être désactivé dans la plupart des cas d'utilisation et est devenu obsolète depuis Windows Server 2016.

Outre ces optimisations du système d'exploitation, vous devez également prendre en compte l'unité de transmission maximale (MTU) de votre trafic réseau et l'ajuster en fonction de votre charge de travail et de votre architecture réseau. Pour plus d'informations, consultez Unité de transmission maximale du réseau (MTU) pour votre EC2 instance.

AWS mesure régulièrement les latences aller-retour moyennes entre les instances lancées dans un groupe de placement en cluster de 50 µs et les latences finales de 200 µs au 99,9 centile. Si vos applications nécessitent des latences constamment faibles, nous vous recommandons d'utiliser la dernière version des ENA pilotes sur les instances à performances fixes basées sur le système Nitro.

Configurer l'CPUaffinité de dimensionnement côté réception

Le dimensionnement côté réception (RSS) est utilisé pour répartir la CPU charge du trafic réseau entre plusieurs processeurs. Par défaut, les versions officielles d'Amazon Windows AMIs sont configurées avec RSS Activé. ENAles interfaces réseau élastiques fournissent jusqu'à huit RSS files d'attente. En définissant l'CPUaffinité pour les RSS files d'attente, ainsi que pour les autres processus du système, il est possible de répartir la CPU charge sur les systèmes multicœurs, ce qui permet de traiter davantage de trafic réseau. Pour les types d'instances comportant plus de 16vCPUs, nous vous recommandons d'utiliser l'`Set-NetAdapterRSS` PowerShell applet de commande, qui exclut manuellement le processeur de démarrage (processeurs logiques 0 et 1 lorsque l'hyperthreading est activé) de la RSS configuration de toutes les interfaces réseau Elastic, afin d'éviter tout conflit avec les différents composants du système.

Windows est sensible à l'hyperthread et veille à ce que les RSS files d'attente d'une seule carte d'interface réseau (NIC) soient toujours placées sur des cœurs physiques différents. Par conséquent, à moins que l'hyperthreading ne soit désactivé, afin d'éviter tout conflit avec d'autres processeursNICs, répartissez la RSS configuration de chacun NIC sur une gamme de 16 processeurs logiques. L'`Set-NetAdapterRss`applet de commande vous permet de définir par NIC plage de processeurs logiques valides en définissant les valeurs de BaseProcessorGroup,, BaseProcessorNumber MaxProcessingGroup MaxProcessorNumber, et NumaNode (facultatif). S'il n'y a pas suffisamment de cœurs physiques pour éliminer complètement les interférences, minimiser les plages qui se chevauchent ou réduire le nombre de processeurs logiques dans les plages d'Elastic Network Interface en fonction de la charge de travail attendue de l'interface (en d'autres termes, une interface réseau administrative à faible volume peut ne pas avoir besoin d'autant de RSS files d'attente assignées). NIC En outre, comme indiqué précédemment, divers composants doivent fonctionner sur CPU 0. Nous vous recommandons donc de l'exclure de toutes les RSS configurations lorsque suffisamment de composants vCPUs sont disponibles.

Par exemple, lorsqu'il existe trois interfaces réseau élastiques sur une CPU instance 72 v avec 2 NUMA nœuds avec l'hyperthreading activé, les commandes suivantes répartissent la charge réseau entre les deux CPUs sans chevauchement et empêchent complètement l'utilisation du noyau 0.

```
Set-NetAdapterRss -Name NIC1 -BaseProcessorGroup 0 -BaseProcessorNumber 2 -
MaxProcessorNumber 16
Set-NetAdapterRss -Name NIC2 -BaseProcessorGroup 1 -BaseProcessorNumber 0 -
MaxProcessorNumber 14
Set-NetAdapterRss -Name NIC3 -BaseProcessorGroup 1 -BaseProcessorNumber 16 -
MaxProcessorNumber 30
```

Notez que ces paramètres sont persistants pour chaque adaptateur réseau. Si une instance est redimensionnée avec un nombre différent devCPUs, vous devez réévaluer la RSS configuration pour chaque interface Elastic network activée. La documentation Microsoft complète relative à l'`Set-NetAdapterRss`applet de commande se trouve ici : powershell/module/netadapter/set-netadapterrsshttps://docs.microsoft.com/en-us/.

Remarque spéciale concernant les SQL charges de travail : nous vous recommandons également de revoir vos paramètres d'affinité des threads d'E/S ainsi que la RSS configuration de votre interface Elastic Network afin de minimiser les interférences entre les E/S et le réseau. CPUs Consultez Option de configuration de serveur de masque d'affinité.

Adaptateur Elastic Fabric pour les charges de travail ML HPC et ML sur Amazon EC2

Un adaptateur Elastic Fabric (EFA) est un périphérique réseau que vous pouvez connecter à votre EC2 instance Amazon pour accélérer les applications de calcul haute performance (HPC) et d'apprentissage automatique. EFAvous permet d'atteindre les performances applicatives d'un HPC cluster sur site, grâce à l'évolutivité, à la flexibilité et à l'élasticité offertes par le AWS cloud.

EFAsfournissent une latence plus faible et plus constante et un débit plus élevé que le TCP transport traditionnellement utilisé dans les HPC systèmes basés sur le cloud. Il améliore les performances de la communication entre instances, essentielle pour le dimensionnement HPC et les applications d'apprentissage automatique. Il est optimisé pour fonctionner sur l'infrastructure AWS réseau existante et peut évoluer en fonction des exigences de l'application.

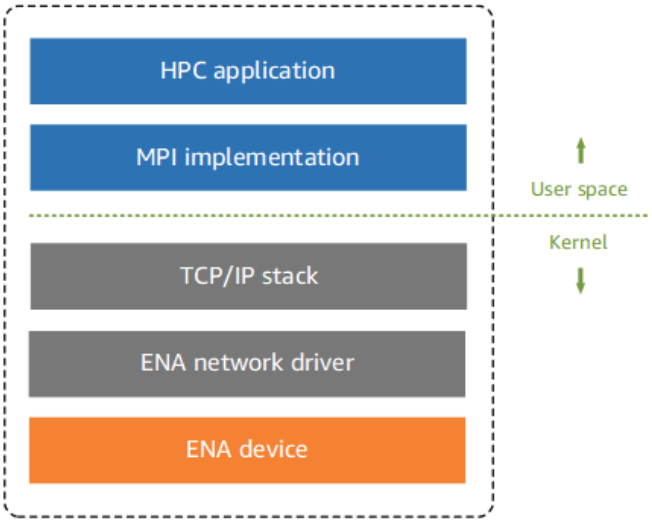
EFAss'intègre à Libfabric 1.7.0 et versions ultérieures et prend en charge Open MPI 5 et versions ultérieures, Intel MPI 2019 Update 5 et versions ultérieures pour les HPC applications, et Nvidia Collective Communications Library (NCCL) pour les applications d'apprentissage automatique.

> **Note**
>
> Les fonctionnalités de contournement du système d'exploitation de ne EFAs sont pas prises en charge sur les instances Windows. Si vous attachez un EFA à une instance Windows, celle-ci fonctionne comme un adaptateur réseau élastique, sans les EFA fonctionnalités supplémentaires.

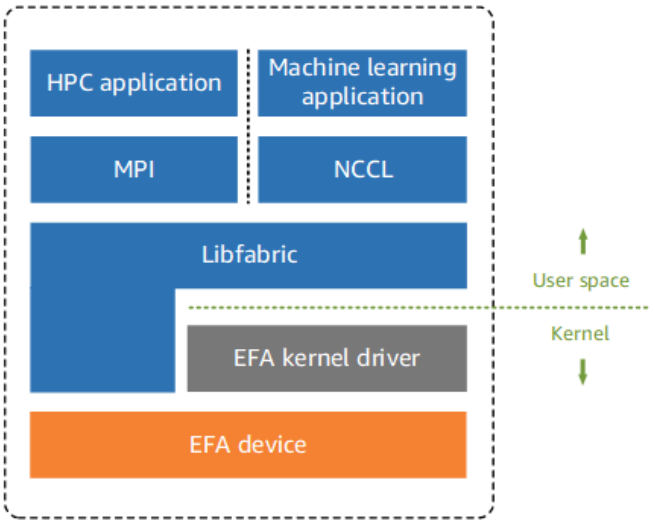
Table des matières

EFAles bases

An EFA est un adaptateur réseau élastique (ENA) doté de fonctionnalités supplémentaires. Il fournit toutes les fonctionnalités d'unENA, avec une fonctionnalité supplémentaire de contournement du système d'exploitation. OS-Bypass est un modèle d'accès qui permet aux applications d'apprentissage automatique de communiquer directement avec le matériel d'interface réseau afin de fournir des fonctionnalités de transport fiables HPC et à faible latence.



Traditional HPC software stack in EC2



HPC software stack in EC2 with EFA

Traditionnellement, HPC les applications utilisent l'interface de passage de message (MPI) pour s'interfacer avec le transport réseau du système. Dans le AWS cloud, cela signifie que les applications s'interfacent avecMPI, qui utilise ensuite la pile TCP /IP du système d'exploitation et le pilote de ENA périphérique pour permettre la communication réseau entre les instances.

Avec unEFA, HPC les applications utilisent MPI ou NCCL pour s'interfacer avec le Libfabric. API Le Libfabric API contourne le noyau du système d'exploitation et communique directement avec le EFA périphérique pour mettre des paquets sur le réseau. Cela réduit les frais généraux et permet à l'HPCapplication de fonctionner plus efficacement.

> **Note**
>
> Libfabric est un composant essentiel du framework OpenFabrics Interfaces (OFI), qui définit et exporte l'espace utilisateur API de. OFI Pour plus d'informations, consultez le OpenFabrics site Web de Libfabric.

Différences entre EFAs et ENAs

Les adaptateurs réseau Elastic (ENAs) fournissent les fonctionnalités de réseau IP traditionnelles requises pour prendre en charge la VPC mise en réseau. EFAsfournissent toutes les mêmes fonctionnalités de réseau IP traditionnelles queENAs, et ils prennent également en charge les fonctionnalités de contournement du système d'exploitation. OS-Bypass permet HPC aux applications d'apprentissage automatique de contourner le noyau du système d'exploitation et de communiquer directement avec l'EFAappareil.

Interfaces et bibliothèques prises en charge

EFAsprend en charge les interfaces et bibliothèques suivantes :

- Open MPI 5 et versions ultérieures
- Open MPI 4.0 ou version ultérieure est préférable pour Graviton
- Intel MPI 2019 Update 5 et versions ultérieures
- NVIDIACollective Communications Library (NCCL) 2.4.2 et versions ultérieures

Types d'instance pris en charge

Les types d'instance suivants prennent en charge EFAs :

- Usage général : m5dn.24xlarge m5dn.metal m5n.24xlarge | m5n.metal m5zn.12xlarge | m5zn.metal | m6a.48xlarge | m6a.metal | m6i.32xlarge m6i.metal | m6id.32xlarge | m6id.metal | m6idn.32xlarge | m6idn.metal | m6in.32xlarge m6in.metal | m7a.48xlarge | m7a.metal-48xl | m7g.16xlarge | m7g.metal m7gd.16xlarge | m7gd.metal | m7i.48xlarge | m7i.metal-48xl
- Optimisé pour le calcul : c5n.9xlarge c5n.18xlarge c5n.metal c6a.48xlarge | c6a.metal | c6gn.16xlarge | c6i.32xlarge | c6i.metal c6id.32xlarge | c6id.metal | c6in.32xlarge | c6in.metal | c7a.48xlarge | c7a.metal-48xl | c7g.16xlarge | c7g.metal | c7gd.16xlarge | c7gd.metal | c7gn.16xlarge | c7gn.metal | c7i.48xlarge | c7i.metal-48xl
- Mémoire optimisée : r5dn.24xlarge | r5dn.metal | r5n.24xlarge | r5n.metal || r6a.48xlarge | r6a.metal | r6i.32xlarge | r6i.metal | r6idn.32xlarge | r6idn.metal | r6in.32xlarge | r6in.metal | r6id.32xlarge | r6id.metal | r7a.48xlarge | r7a.metal-48xl | r7g.16xlarge || r7g.metal | r7gd.16xlarge | r7gd.metal | r7i.48xlarge | r7i.metal-48xl | r7iz.32xlarge | r7iz.metal-32xl | r8g.24xlarge | r8g.48xlarge | r8g.metal-24xl | r8g.metal-48xl | u7i-12tb.224xlarge | u7in-16tb.224xlarge || u7in-24tb.224xlarge | u7in-32tb.224xlarge | x2idn.32xlarge | x2idn.metal | x2iedn.32xlarge | x2iedn.metal | x2iezn.12xlarge | x2iezn.metal
- Stockage optimisé : i3en.12xlarge | i3en.24xlarge | i3en.metal | i4g.16xlarge | i4i.32xlarge | i4i.metal | im4gn.16xlarge
- Calcul accéléré : dl1.24xlarge dl2q.24xlarge g4dn.8xlarge | g4dn.12xlarge | g4dn.16xlarge | g4dn.metal g5.8xlarge | g5.12xlarge | g5.16xlarge | g5.24xlarge | g5.48xlarge | g6.8xlarge | g6.12xlarge g6.16xlarge | g6.24xlarge | g6.48xlarge | g6e.8xlarge | g6e.12xlarge | g6e.16xlarge g6e.24xlarge | g6e.48xlarge | gr6.8xlarge | inf1.24xlarge | p3dn.24xlarge | p4d.24xlarge p4de.24xlarge | p5.48xlarge | trn1.32xlarge | trn1n.32xlarge | vt1.24xlarge
- Calcul haute performance : hpc6a.48xlarge hpc6id.32xlarge | hpc7a.12xlarge | hpc7a.24xlarge | hpc7a.48xlarge | hpc7a.96xlarge | hpc7g.4xlarge | hpc7g.8xlarge | hpc7g.16xlarge

Pour voir les types d'instances disponibles qui sont pris EFAs en charge dans une région spécifique

Les types d'instance disponibles varient selon la région. Pour voir les types d'instances disponibles qui sont pris EFAs en charge dans une région, utilisez la describe-instance-typescommande

avec le `--region` paramètre. Incluez le `--filters` paramètre pour étendre les résultats aux types d'instances pris en charge EFA et le `--query` paramètre pour étendre la sortie à la valeur de`InstanceType`.

```
aws ec2 describe-instance-types  --region us-east-1  --filters Name=network-info.efa-supported,Values=true  --query "InstanceTypes[*].[InstanceType]"  --output text | sort
```

Systèmes d'exploitation pris en charge

La prise en charge du système d'exploitation varie en fonction du type de processeur. Le tableau suivant indique les systèmes d'exploitation pris en charge.

Système d'exploitation	Types d'instances Intel/ AMD (**`x86_64`**)	AWS Types d'instances de Graviton (**`arm64`**)
Amazon Linux 202	✓	✓
Amazon Linux 2	✓	✓
RHEL8 et 9	✓	✓
Debian 10 et 11	✓	✓
Rocky Linux 8 et 9	✓	✓
Ubuntu 20.04, 22.04 et 24.04	✓	✓
SUSELinux Enterprise 15 SP2 et versions ultérieures	✓	✓
Ouvrez SUSE Leap 15.5 et versions ultérieures	✓	

> **Note**
>
> Ubuntu 20.04 prend en charge l'assistance directe entre pairs lorsqu'il est utilisé avec les instances `dl1.24xlarge`.

EFAlimites

EFAsprésentent les limites suivantes :

- Tous les types d'instances P4d et P5 prennent en charge l'accès direct NVIDIA GPUDirect à distance à la mémoire ()RDMA.
- EFAle trafic entre les instances P4D/P4de/ et les autres types d'DL1instances n'est actuellement pas pris en charge.
- Les types d'instance qui prennent en charge plusieurs cartes réseau peuvent être configurés avec EFA une seule carte réseau. Tous les autres types d'instances pris en charge n'en prennent en charge qu'une seule EFA par instance.
- Pour`c7g.16xlarge`, `m7g.16xlarge` et les instances `r7g.16xlarge` dédiées et les hôtes dédiés ne sont pas pris en charge lorsqu'un EFA est attaché.
- EFALe trafic de contournement du système d'exploitation ne peut pas traverser les zones de disponibilité ou VPCs AWS les comptes. En d'autres termes, le trafic de EFA contournement du système d'exploitation ne peut pas circuler d'une zone de disponibilité VPC (avec ou sans connexion d'VPCappairage) ou d'un AWS compte à un autre. Cela ne s'applique pas au trafic IP normal provenant duEFA.
- EFALe trafic de contournement du système d'exploitation ne peut pas être envoyé via les sous-réseaux d'une zone locale.
- EFALe trafic de contournement du système d'exploitation n'est pas routable. Le trafic IP normal en provenance du EFA reste routable.
- EFAIl doit être membre d'un groupe de sécurité qui autorise tout le trafic entrant et sortant à destination et en provenance du groupe de sécurité lui-même.
- EFAn'est pas pris en charge sur les instances Windows.
- EFAn'est pas compatible avec AWS Outposts.

EFAtarification

EFAest disponible en tant que fonctionnalité EC2 réseau Amazon optionnelle que vous pouvez activer sur n'importe quelle instance prise en charge sans frais supplémentaires.

Maximisez la bande passante réseau sur les instances de calcul accéléré avec EFA

Pour optimiser la bande passante sur les types d'instances accélérées suivants, vous pouvez utiliser plusieurs interfaces Elastic Fabric Adapter (EFA).

- Les instances P5 prennent en charge jusqu'à 32 cartes réseau et peuvent fournir jusqu'à 3 200 Gbit/s de bande passante réseau.
- Les instances G6e prennent en charge jusqu'à quatre cartes réseau et peuvent fournir jusqu'à 400 Gbit/s de bande passante réseau

Pour plus d'informations sur la prise en main des instances GPU accélérées, consultezAccélération des performances grâce aux GPU instances.

Nous vous recommandons de définir une seule interface EFA réseau par carte réseau. Pour configurer ces interfaces au lancement, nous recommandons les paramètres suivants :

- Pour l'interface réseau `0`, spécifiez l'index d'appareils `0`.
- Pour les interfaces réseaux `1` à `31`, spécifiez l'index d'appareils `1`.

Si vous utilisez la EC2 console Amazon, dans l'assistant de lancement d'instance, choisissez Modifier dans la section Paramètres réseau. Développez Configuration réseau avancée et choisissez Ajouter une interface réseau pour ajouter le nombre requis d'interfaces réseau. Pour chaque interface réseau EFA, sélectionnez Activer pour. Pour toutes les interfaces réseau, à l'exception de l'interface réseau principale, pour Index d'appareils, spécifiez `1`. Configurez les paramètres restants selon les besoins.

Si vous utilisez la commande run-instances AWS CLI, pour`--network-interfaces`, spécifiez le nombre requis d'interfaces réseau. Pour chaque interface réseau, pour `InterfaceType`, spécifiez `efa`. Pour l'interface réseau principale, pour `NetworkCardIndex` et `DeviceIndex`, spécifiez `0`. Pour les autres interfaces réseau, pour `NetworkCardIndex`, spécifiez une valeur unique comprise entre `1` et `31`, et pour `DeviceIndex`, spécifiez `1`.

L'exemple d'extrait de commande suivant montre une demande comportant 32 interfaces EFA réseau.

```
$ aws --region $REGION ec2 run-instances \
 --instance-type p5.48xlarge \
 --count 1 \
 --key-name key_pair_name \
 --image-id ami_id \
 --network-interfaces
 "NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=1,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=2,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=3,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=4,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=5,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=6,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=7,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=8,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=9,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=10,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
```

```
"NetworkCardIndex=11,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=12,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=13,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=14,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=15,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=16,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=17,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=18,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=19,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=20,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=21,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=22,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=23,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=24,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
```

```
 "NetworkCardIndex=25,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=26,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=27,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=28,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=29,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=30,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=31,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
...
```

Si vous utilisez un modèle de lancement, spécifiez le nombre requis d'interfaces réseau dans le modèle de lancement. Pour chaque interface réseau, pour `InterfaceType`, spécifiez `efa`. Pour l'interface réseau principale, pour `NetworkCardIndex` et `DeviceIndex`, spécifiez `0`. Pour les autres interfaces réseau, pour `NetworkCardIndex`, spécifiez une valeur unique comprise entre 1 et 31, et pour `DeviceIndex`, spécifiez 1. L'extrait de code suivant montre un exemple avec 3 interfaces réseau sur 32 possibles.

```
"NetworkInterfaces":[
{
  "NetworkCardIndex":0,
  "DeviceIndex":0,
  "InterfaceType": "efa",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 1,
```

```
  "DeviceIndex": 1,
  "InterfaceType": "efa",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 2,
  "DeviceIndex": 1,
  "InterfaceType": "efa",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
}
...
```

Lorsque vous lancez une instance P5 avec plusieurs interfaces réseau, vous ne pouvez pas attribuer automatiquement des adresses IP publiques. Toutefois, vous pouvez associer une adresse IP élastique à l'interface réseau principale (NetworkCardIndex=0, DeviceIndex =0) après le lancement pour la connectivité Internet. Ubuntu 20.04 et versions ultérieures ainsi qu'Amazon Linux 2 et versions ultérieures sont configurés pour utiliser l'interface réseau principale pour le trafic Internet lorsque l'instance est lancée, comme recommandé sur cette page.

Pour obtenir les meilleures performances réseau sur les instances G6e, vous pouvez IMDS cartographier les interfaces réseau connectées et les optimiser en utilisant des instances réseau NetworkCardIndexes disjointes.

L'exemple de script suivant rassemble les détails de la pièce jointe NetworkCardIndexes.

```
$ TOKEN=$(curl -s -X PUT "http://169.254.169.254/latest/api/token" -H "X-
 aws-ec2-metadata-token-ttl-seconds: 21600")
 count=$(ls -l /sys/class/net/eth* | wc -l)

 for ((i = 0 ; i < ${count} ; i++)); do
  mac=$(cat /sys/class/net/eth$i/address)

  network_card=$(curl -s -H "X-aws-ec2-metadata-token: $TOKEN"
"http://169.254.169.254/latest/meta-data/network/interfaces/macs/$mac/
```

```
network-card")

   device_number=$(curl -s -H "X-aws-ec2-metadata-token: $TOKEN"
"http://169.254.169.254/latest/meta-data/network/interfaces/macs/$mac/
device-number")

   device_bdf=$(realpath /sys/class/net/eth${i}/device)

   echo "eth${i} ${network_card} ${device_number} ${device_bdf}"
done
```

Commencez avec EFA et MPI pour les HPC charges de travail sur Amazon EC2

Ce didacticiel vous aide à lancer un cluster d'instances MPI activé EFA et pour les charges HPC de travail.

Tâches

- Étape 1 : préparer un groupe EFA de sécurité activé
- Étape 2 : Lancer une instance temporaire
- Étape 3 : Installer le logiciel EFA
- Étape 4 : (Facultatif) Activez Open MPI 5
- Étape 5 : (Facultatif) Installez Intel MPI
- Étape 6 : Désactiver la protection ptrace
- Étape 7. Confirmer l'installation
- Étape 8 : installez votre HPC application
- Étape 9 : Création d'un système EFA activé AMI
- Étape 10 : Lancer des instances EFA activées dans un groupe de placement de clusters
- Étape 11 : Résilier l'instance temporaire
- Étape 12 : activer le mode sans mot de passe SSH

Étape 1 : préparer un groupe EFA de sécurité activé

Un EFA nécessite un groupe de sécurité qui autorise tout le trafic entrant et sortant à destination et en provenance du groupe de sécurité lui-même. La procédure suivante crée un groupe de sécurité

qui autorise tout le trafic entrant et sortant à destination et en provenance de lui-même, et qui autorise le SSH trafic entrant depuis n'importe quelle IPv4 adresse à des fins de connectivité. SSH

> **Important**
>
> Ce groupe de sécurité n'est destiné qu'à des fins de test. Pour vos environnements de production, nous vous recommandons de créer une SSH règle entrante qui autorise le trafic uniquement en provenance de l'adresse IP à partir de laquelle vous vous connectez, telle que l'adresse IP de votre ordinateur ou d'une plage d'adresses IP de votre réseau local.

Pour d'autres scénarios, consultez Règles de groupe de sécurité pour différents cas d'utilisation.

Pour créer un groupe EFA de sécurité activé

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité), puis Create security group (Créer un groupe de sécurité).
3. Dans la fenêtre Create security group (Créer un groupe de sécurité), procédez comme suit :
   a. Pour Nom du groupe de sécurité, saisissez un nom descriptif pour le groupe de sécurité, tel que `EFA-enabled security group`.
   b. (Facultatif) Pour Description, saisissez une brève description du groupe de sécurité.
   c. Pour VPC, sélectionnez l'instance VPC dans laquelle vous souhaitez lancer vos instances EFA activées.
   d. Sélectionnez Create security group (Créer un groupe de sécurité).
4. Sélectionnez le groupe de sécurité que vous avez créé et dans l'onglet Details (Détails), copiez le Security group ID (ID du groupe de sécurité).
5. En conservant la sélection du groupe de sécurité, choisissez Actions, Edit inbound rules (Modifier les règles entrantes), puis procédez comme suit :
   a. Choisissez Ajouter une règle.
   b. Pour Type, sélectionnez Tout le trafic.
   c. Pour Source type (Type de source), choisissez Custom (Personnalisée) et collez l'ID du groupe de sécurité que vous avez copié dans le champ.
   d. Choisissez Ajouter une règle.

e. Pour Type, sélectionnez SSH.

f. Pour Type de source, choisissez N'importe où- IPv4.

g. Sélectionnez Enregistrer les règles.

6. En conservant la sélection du groupe de sécurité, choisissez Actions, Edit outbound rules (Modifier les règles sortantes), puis procédez comme suit :

   a. Choisissez Ajouter une règle.

   b. Pour Type, sélectionnez Tout le trafic.

   c. Pour Destination type (Type de destination), choisissez Custom (Personnalisée) et collez l'ID du groupe de sécurité que vous avez copié dans le champ.

   d. Sélectionnez Enregistrer les règles.

Étape 2 : Lancer une instance temporaire

Lancez une instance temporaire que vous pouvez utiliser pour installer et configurer les composants EFA logiciels. Vous utilisez cette instance pour créer une instance EFA activée à AMI partir de laquelle vous pouvez lancer vos instances EFA activées.

Pour lancer une instance temporaire

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Instances, puis Launch Instances (Lancer des instances) pour ouvrir le nouvel assistant de lancement d'instance.
3. (Facultatif) Dans la section Name and tags (Noms et identifications), fournissez un nom pour l'instance, tel que `EFA-instance`. Le nom est attribué à l'instance en tant qu'identification de ressource (`Name=EFA-instance`).
4. Dans la section Images de l'application et du système d'exploitation, sélectionnez un AMI pour l'un des systèmes d'exploitation pris en charge.
5. Dans la section Instance type (Type d'instance), sélectionnez un type d'instance pris en charge.
6. Dans la section Key pair (Paire de clés), sélectionnez la paire de clés à utiliser pour l'instance.
7. Dans la section Network settings (Paramètres réseau), choisissez Edit (Modifier), puis procédez comme suit :

   a. Pour Sous-réseau, choisissez le sous-réseau dans lequel lancer l'instance. Si vous ne sélectionnez aucun sous-réseau, vous ne pouvez pas activer l'instance pourEFA.

b. Pour Firewall (security groups) (Pare-feu (groupes de sécurité)), choisissez Sélectionner un groupe de sécurité existant (Select existing security group), puis sélectionnez le groupe de sécurité que vous avez créé à l'étape précédente.

c. Développez la section Advanced network configuration (Configuration réseau avancée) et pour Elastic Fabric Adapter (EFA), sélectionnez Enable (Activer).

8. Dans la section Storage (Stockage), configurez les volumes selon vos besoins.

9. Dans le panneau Summary (Récapitulatif) à droite, choisissez Launch instance (Lancer l'instance).

> **Note**
>
> Envisagez d'exiger l'utilisation de IMDSv2 pour l'instance temporaire ainsi AMI que celle que vous allez créer à l'étape 9, sauf si vous l'avez déjà définie IMDSv2 comme instance par défaut pour le compte. Pour plus d'informations sur les étapes IMDSv2 de configuration, consultezConfigurer les options de métadonnées d'instance pour les nouvelles instances.

Étape 3 : Installer le logiciel EFA

Installez le noyau EFA activé, EFA les pilotes, Libfabric et Open MPI Stack nécessaires à la prise en charge de votre EFA instance temporaire.

Les étapes varient selon que vous avez l'intention de l'utiliser EFA avec OpenMPI, avec Intel MPI ou avec Open MPI et IntelMPI.

Pour installer le logiciel EFA

1. Connectez-vous à l'instance que vous avez lancée. Pour de plus amples informations, veuillez consulter Connectez-vous à votre instance Linux à l'aide de SSH.

2. Pour vous assurer que tous vos packages logiciels sont mis à jour, effectuez une mise à jour logicielle rapide sur votre instance. Ce processus peut prendre quelques minutes.

   - Amazon Linux 2023, Amazon Linux 2, RHEL 8/9, Rocky Linux 8/9

     ```
     $ sudo yum update -y
     ```

   - Ubuntu et Debian

```
$ sudo apt-get update && sudo apt-get upgrade -y
```

- SUSELinux Entreprise

```
$ sudo zypper update -y
```

3. Redémarrez l'instance et reconnectez-vous à celle-ci.
4. Téléchargez les fichiers d'installation du logiciel EFA. Les fichiers d'installation du logiciel sont packagés dans un fichier d'archive compressé (`.tar.gz`). Pour télécharger la version stable la plus récente, utilisez la commande suivante.

```
$ curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.34.0.tar.gz
```

Vous pouvez aussi obtenir la dernière version en remplaçant le numéro de version par `latest` dans la commande ci-dessus.

5. (Facultatif) Vérifiez l'authenticité et l'intégrité du fichier EFA tarball (`.tar.gz`).

Nous vous recommandons de le faire pour vérifier l'identité de l'éditeur du logiciel et pour vérifier que le fichier n'a pas été modifié ou endommagé depuis sa publication. Si vous ne souhaitez pas vérifier le fichier d'archive, ignorez cette étape.

> **Note**
>
> Sinon, si vous préférez vérifier le fichier tarball en utilisant plutôt une SHA256 somme de contrôle MD5 ou, consultez. Vérifiez le EFA programme d'installation à l'aide d'une somme de contrôle

a. Téléchargez la GPG clé publique et importez-la dans votre trousseau de clés.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --
import aws-efa-installer.key
```

La commande doit renvoyer une valeur clé. Notez la valeur clé, car vous en aurez besoin lors de l'étape suivante.

b. Vérifiez l'empreinte digitale de la GPG clé. Exécutez la commande suivante et spécifiez la valeur clé que vous avez obtenue à l'étape précédente.

```
$ gpg --fingerprint key_value
```

La commande doit renvoyer une empreinte digitale identique à `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC`. Si l'empreinte digitale ne correspond pas, n'exécutez pas le script EFA d'installation et contactez AWS Support.

c. Téléchargez le fichier de signature et vérifiez la signature du fichier EFA tarball.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.34.0.tar.gz.sig
 && gpg --verify ./aws-efa-installer-1.34.0.tar.gz.sig
```

Voici un exemple de sortie.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1  5E59 A054 80B1 DD2D 3CCC
```

Si le résultat inclut `Good signature` et que l'empreinte digitale correspond à l'empreinte digitale renvoyée à l'étape précédente, passez à l'étape suivante. Si ce n'est pas le cas, n'exécutez pas le script EFA d'installation et contactez AWS Support.

6. Procédez à l'extraction des fichiers à partir du fichier compressé `.tar.gz` et accédez au répertoire extrait.

```
$ tar -xf aws-efa-installer-1.34.0.tar.gz && cd aws-efa-installer
```

7. Installez le logiciel EFA. Effectuez l'une des actions suivantes en fonction de votre cas d'utilisation.

> **Note**
>
> EFAn'est pas compatible NVIDIA GPUDirect avec SUSE Linux. Si vous utilisez SUSE Linux, vous devez également spécifier l'`--skip-kmod`option pour empêcher l'installation de kmod. Par défaut, SUSE Linux n'autorise pas les modules out-of-tree du noyau.

Open MPI and Intel MPI

Si vous avez l'intention de l'utiliser EFA avec Open MPI et IntelMPI, vous devez installer le EFA logiciel avec Libfabric et OpenMPI, et vous devez effectuer l'étape 5 : Installer Intel MPI.

Pour installer le EFA logiciel avec Libfabric et OpenMPI, exécutez la commande suivante.

> **Note**
>
> À partir de la version EFA 1.30.0, Open MPI 4 et Open MPI 5 sont installés par défaut. Vous pouvez éventuellement spécifier la version d'Open MPI que vous souhaitez installer. Pour installer uniquement Open MPI 4, incluez`--mpi=openmpi4`. Pour installer uniquement Open MPI 5, incluez`--mpi=openmpi5`. Pour installer les deux, omettez l'option `--mpi`.

```
$ sudo ./efa_installer.sh -y
```

Libfabric est installé dans `/opt/amazon/efa`. Open MPI 4 est installé sur`/opt/amazon/openmpi`. Open MPI 5 est installé sur`/opt/amazon/openmpi5`.

Open MPI only

Si vous avez l'intention de l'utiliser MPI uniquement EFA avec Open, vous devez installer le EFA logiciel avec Libfabric et OpenMPI, et vous pouvez ignorer l'étape 5 : Installation d'Intel MPI. Pour installer le EFA logiciel avec Libfabric et OpenMPI, exécutez la commande suivante.

> **Note**
>
> À partir de la version EFA 1.30.0, Open MPI 4 et Open MPI 5 sont installés par défaut. Vous pouvez éventuellement spécifier la version d'Open MPI que vous souhaitez installer. Pour installer uniquement Open MPI 4, incluez`--mpi=openmpi4`. Pour installer uniquement Open MPI 5, incluez`--mpi=openmpi5`. Pour installer les deux, omettez l'option `--mpi`.

```
$ sudo ./efa_installer.sh -y
```

Libfabric est installé dans `/opt/amazon/efa`. Open MPI 4 est installé sur`/opt/amazon/openmpi`. Open MPI 5 est installé sur`/opt/amazon/openmpi5`.

Intel MPI only

Si vous avez l'intention de l'utiliser MPI uniquement EFA avec Intel, vous pouvez installer le EFA logiciel sans Libfabric et OpenMPI. Dans ce cas, Intel MPI utilise son Libfabric intégré. Si vous choisissez cette option, vous devez effectuer l'étape 5 : Installation d'Intel MPI.

Pour installer le EFA logiciel sans Libfabric et OpenMPI, exécutez la commande suivante.

```
$ sudo ./efa_installer.sh -y --minimal
```

8. Si le EFA programme d'installation vous invite à redémarrer l'instance, faites-le, puis reconnectez-vous à l'instance. Sinon, déconnectez-vous de l'instance, puis reconnectez-vous pour terminer l'installation.

Étape 4 : (Facultatif) Activez Open MPI 5

> **Note**
>
> Effectuez cette étape uniquement si vous avez l'intention d'utiliser Open MPI 5.

À partir de la version EFA 1.30.0, Open MPI 4 et Open MPI 5 sont installés par défaut. Vous pouvez également choisir d'installer uniquement Open MPI 4 ou Open MPI 5.

Si vous avez choisi d'installer Open MPI 5 à l'étape 3 : Installation du EFA logiciel et que vous avez l'intention de l'utiliser, vous devez effectuer les étapes suivantes pour l'activer.

Pour activer Open MPI 5

1. Ajoutez Open MPI 5 à la variable d'PATHenvironnement.

```
$ module load openmpi5
```

2. Vérifiez qu'Open MPI 5 est activé pour être utilisé.

```
$ which mpicc
```

   La commande doit renvoyer le répertoire d'installation d'Open MPI 5 `-/opt/amazon/openmpi5`.

3. (Facultatif) Pour vous assurer qu'Open MPI 5 est ajouté à la variable d'PATHenvironnement à chaque démarrage de l'instance, procédez comme suit :

   bash shell

   Ajoutez `module load openmpi5` à `/home/username/.bashrc` et `/home/username/.bash_profile`.

   csh and tcsh shells

   Ajoutez `module load openmpi5` à `/home/username/.cshrc`.

Si vous devez supprimer Open MPI 5 de la variable d'PATHenvironnement, exécutez la commande suivante et supprimez-la des scripts de démarrage du shell.

```
$ module unload openmpi5
```

Étape 5 : (Facultatif) Installez Intel MPI

> **Important**
>
> Effectuez cette étape uniquement si vous avez l'intention d'utiliser IntelMPI. Si vous avez l'intention de n'utiliser qu'OpenMPI, ignorez cette étape.

Intel MPI nécessite une installation supplémentaire et une configuration variable d'environnement.

Prérequis

Vérifiez que l'utilisateur qui exécute les étapes suivantes dispose des autorisations sudo.

Pour installer Intel MPI

1. Pour télécharger le script MPI d'installation Intel, procédez comme suit

a. Visitez le site web d'Intel.

b. Dans la section MPIBibliothèque Intel de la page Web, cliquez sur le lien du programme d'installation hors ligne de la MPIbibliothèque Intel pour Linux.

2. Exécutez le script d'installation que vous avez téléchargé à l'étape précédente.

```
$ sudo bash installation_script_name.sh
```

3. Dans le programme d'installation, choisissez Accept & install (Accepter et installer).

4. Lisez le programme Intel Improvement Program, choisissez l'option appropriée, puis choisissez Begin Installation (Démarrer l'installation).

5. Une fois l'installation terminée, choisissez Fermer.

6. Par défaut, Intel MPI utilise son Libfabric intégré (interne). Vous pouvez configurer Intel MPI pour qu'il utilise plutôt le Libfabric fourni avec le EFA programme d'installation. Généralement, le EFA programme d'installation est fourni avec une version de Libfabric ultérieure à celle d'IntelMPI. Dans certains cas, le Libfabric fourni avec le EFA programme d'installation est plus performant que celui d'IntelMPI. Pour configurer Intel MPI afin d'utiliser le Libfabric fourni avec le EFA programme d'installation, effectuez l'une des opérations suivantes en fonction de votre shell.

   bash shells

   Ajoutez la déclaration suivante à /home/*username*/.bashrc et /home/*username*/.bash_profile.

   ```
   export I_MPI_OFI_LIBRARY_INTERNAL=0
   ```

   csh and tcsh shells

   Ajoutez la déclaration suivante à /home/*username*/.cshrc.

   ```
   setenv I_MPI_OFI_LIBRARY_INTERNAL 0
   ```

7. Ajoutez la commande source suivante à votre script shell afin d'extraire le script `vars.sh` du répertoire d'installation pour configurer l'environnement du compilateur à chaque démarrage de l'instance. Effectuez l'une des actions suivantes en fonction de votre shell.

bash shells

Ajoutez la déclaration suivante à /home/*username*/.bashrc et /home/*username*/.bash_profile.

```
source /opt/intel/oneapi/mpi/latest/env/vars.sh
```

csh and tcsh shells

Ajoutez la déclaration suivante à /home/*username*/.cshrc.

```
source /opt/intel/oneapi/mpi/latest/env/vars.csh
```

8. Par défaut, si elle n'EFAest pas disponible en raison d'une mauvaise configuration, Intel MPI utilise par défaut la pile réseau TCP /IP, ce qui peut ralentir les performances des applications. Vous pouvez empêcher cela en définissant I_MPI_OFI_PROVIDER sur efa. Cela provoque l'échec MPI d'Intel avec le message d'erreur suivant s'il n'EFAest pas disponible :

```
Abort (XXXXXX) on node 0 (rank 0 in comm 0): Fatal error in PMPI_Init: OtherMPI
 error,
MPIR_Init_thread (XXX).......:
MPID_Init (XXXX).............:
MPIDI_OFI_mpi_init_hook (XXXX):
open_fabric (XXXX)...........:
find_provider (XXXX).........:
OFI fi_getinfo() failed (ofi_init.c:2684:find_provider:
```

Effectuez l'une des actions suivantes en fonction de votre shell.

bash shells

Ajoutez la déclaration suivante à /home/*username*/.bashrc et /home/*username*/.bash_profile.

```
export I_MPI_OFI_PROVIDER=efa
```

csh and tcsh shells

Ajoutez la déclaration suivante à /home/*username*/.cshrc.

```
setenv I_MPI_OFI_PROVIDER efa
```

9. Par défaut, Intel MPI n'imprime pas les informations de débogage. Vous pouvez spécifier différents niveaux de verbosité pour contrôler les informations de débogage. Les valeurs possibles (dans l'ordre de la quantité de détails qu'elles fournissent) sont : `0` (par défaut), `1`, `2`, `3`, `4`, `5`. Le niveau 1 et les niveaux supérieurs impriment le résultat de `libfabric version` et de `libfabric provider`. `libfabric version`À utiliser pour vérifier si Intel MPI utilise le Libfabric interne ou le Libfabric fourni avec le EFA programme d'installation. S'il utilise la bibliothèque Libfabric interne, la version est suffixée par `impi`. `libfabric provider`À utiliser pour vérifier si Intel MPI utilise EFA ou si le réseau TCP /IP. S'il utiliseEFA, la valeur est`efa`. S'il utilise TCP /IP, la valeur est`tcp;ofi_rxm`.

   Pour activer les informations de débogage, effectuez l'une des opérations suivantes en fonction de votre shell.

   bash shells

   Ajoutez la déclaration suivante à /home/*username*/`.bashrc` et /home/*username*/`.bash_profile`.

   ```
   export I_MPI_DEBUG=value
   ```

   csh and tcsh shells

   Ajoutez la déclaration suivante à /home/*username*/`.cshrc`.

   ```
   setenv I_MPI_DEBUG value
   ```

10. Par défaut, Intel MPI utilise la mémoire partagée du système d'exploitation (`shm`) pour les communications intra-nœuds et utilise Libfabric (`ofi`) uniquement pour les communications entre nœuds. En général, cette configuration fournit les meilleures performances. Cependant, dans certains cas, l'Intel MPI Shm Fabric peut entraîner le blocage indéfini de certaines applications.

    Pour résoudre ce problème, vous pouvez obliger Intel MPI à utiliser Libfabric pour les communications intra-nœuds et inter-nœuds. Pour ce faire, effectuez l'une des opérations suivantes en fonction de votre shell.

bash shells

Ajoutez la déclaration suivante à /home/*username*/.bashrc et /home/*username*/.bash_profile.

```
export I_MPI_FABRICS=ofi
```

csh and tcsh shells

Ajoutez la déclaration suivante à /home/*username*/.cshrc.

```
setenv I_MPI_FABRICS ofi
```

> **Note**
>
> Le fournisseur EFA Libfabric utilise la mémoire partagée du système d'exploitation pour les communications intra-nœuds. Cela signifie que la définition de `I_MPI_FABRICS` sur `ofi` donne des performances similaires à la configuration par défaut `shm:ofi`.

11. Déconnectez-vous de l'instance, puis reconnectez-vous.

Si vous ne souhaitez plus utiliser IntelMPI, supprimez les variables d'environnement des scripts de démarrage du shell.

Étape 6 : Désactiver la protection ptrace

Pour améliorer les performances de votre HPC application, Libfabric utilise la mémoire locale de l'instance pour les communications interprocessus lorsque les processus s'exécutent sur la même instance.

La fonctionnalité de mémoire partagée utilise Cross Memory Attach (CMA), qui n'est pas compatible avec la protection ptrace. Si vous utilisez une distribution Linux dans laquelle la protection ptrace est activée par défaut, telle que Ubuntu, vous devez la désactiver. Si la protection ptrace n'est pas activée par défaut dans votre distribution Linux, ignorez cette étape.

Pour désactiver la protection ptrace

Effectuez l'une des actions suivantes :

- Pour désactiver temporairement la protection ptrace à des fins de test, exécutez la commande suivante.

```
$ sudo sysctl -w kernel.yama.ptrace_scope=0
```

- Pour désactiver définitivement la protection ptrace, ajoutez `kernel.yama.ptrace_scope = 0` à `/etc/sysctl.d/10-ptrace.conf` et redémarrez l'instance.

Étape 7. Confirmer l'installation

Pour confirmer la réussite de l'installation

1. Pour vérifier que l'installation MPI a bien été effectuée, exécutez la commande suivante :

   ```
   $ which mpicc
   ```

   - Pour OpenMPI, le chemin renvoyé doit inclure `/opt/amazon/`
   - Pour IntelMPI, le chemin renvoyé doit inclure`/opt/intel/`. Si vous n'obtenez pas le résultat attendu, assurez-vous d'avoir obtenu le MPI `vars.sh` script Intel.
2. Pour vérifier que les composants EFA logiciels et Libfabric ont été correctement installés, exécutez la commande suivante.

   ```
   $ fi_info -p efa -t FI_EP_RDM
   ```

   La commande doit renvoyer des informations sur les EFA interfaces Libfabric. L'exemple suivant illustre la sortie de la commande.

   ```
   provider: efa
       fabric: EFA-fe80::94:3dff:fe89:1b70
       domain: efa_0-rdm
       version: 2.0
       type: FI_EP_RDM
       protocol: FI_PROTO_EFA
   ```

Étape 8 : installez votre HPC application

Installez l'HPCapplication sur l'instance temporaire. La procédure d'installation varie en fonction de l'HPCapplication spécifique. Pour plus d'informations, consultez Gérer le logiciel sur votre AL2 instance dans le guide de l'utilisateur Amazon Linux 2.

> **Note**
>
> Reportez-vous à la documentation de votre HPC application pour obtenir des instructions d'installation.

Étape 9 : Création d'un système EFA activé AMI

Après avoir installé les composants logiciels requis, vous en créez un AMI que vous pouvez réutiliser pour lancer vos instances EFA compatibles.

Pour créer un fichier AMI à partir de votre instance temporaire

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance temporaire que vous avez créée et choisissez Actions, Image, Créer une image.
4. Pour Créer une image, procédez comme suit :
   a. Dans Nom de l'image, entrez un nom descriptif pourAMI.
   b. (Facultatif) Dans Description de l'image, entrez une brève description de l'objectif duAMI.
   c. Choisissez Create image (Créer une image).
5. Dans le volet de navigation, choisissez AMIs.
6. Localisez le AMI fichier que vous avez créé dans la liste. Attendez que le statut passe de `pending` à `available` avant de poursuivre avec l'étape suivante.

Étape 10 : Lancer des instances EFA activées dans un groupe de placement de clusters

Lancez vos instances EFA activées dans un groupe de placement de clusters en utilisant le groupe de sécurité EFA activé AMI que vous avez créé à l'étape 7 et le groupe de sécurité EFA activé que vous avez créé à l'étape 1.

> **Note**
>
> - Il n'est pas obligatoire de lancer vos instances EFA activées dans un groupe de placement de clusters. Toutefois, nous vous recommandons d'exécuter vos instances EFA activées dans un groupe de placement de clusters, car cela les lance dans un groupe à faible latence dans une seule zone de disponibilité.
> - Pour vous assurer que la capacité est disponible lorsque vous mettez à l'échelle les instances de votre cluster, vous pouvez créer une réserve de capacité pour votre groupe de placement du cluster. Pour de plus amples informations, veuillez consulter Création de réservations de capacité dans des groupes de placement de clusters.

Pour lancer une instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Instances, puis Launch Instances (Lancer des instances) pour ouvrir le nouvel assistant de lancement d'instance.
3. (Facultatif) Dans la section Name and tags (Noms et identifications), fournissez un nom pour l'instance, tel que `EFA-instance`. Le nom est attribué à l'instance en tant qu'identification de ressource (`Name=`*`EFA-instance`*).
4. Dans la section Images de l'application et du système d'exploitationAMIs, choisissez Mon, puis sélectionnez celle AMI que vous avez créée à l'étape précédente.
5. Dans la section Instance type (Type d'instance), sélectionnez un type d'instance pris en charge.
6. Dans la section Key pair (Paire de clés), sélectionnez la paire de clés à utiliser pour l'instance.
7. Dans la section Network settings (Paramètres réseau), choisissez Edit (Modifier), puis procédez comme suit :

   a. Pour Sous-réseau, choisissez le sous-réseau dans lequel lancer l'instance. Si vous ne sélectionnez aucun sous-réseau, vous ne pouvez pas activer l'instance pourEFA.

b. Pour Firewall (security groups) (Pare-feu (groupes de sécurité)), choisissez Sélectionner un groupe de sécurité existant (Select existing security group), puis sélectionnez le groupe de sécurité que vous avez créé à l'étape précédente.

c. Développez la section Advanced network configuration (Configuration réseau avancée) et pour Elastic Fabric Adapter (EFA), sélectionnez Enable (Activer).

8. (Facultatif) Dans la section Storage (Stockage), configurez les volumes selon vos besoins.
9. Dans la section Advanced details (Détails avancés), pour Placement group name (Nom du groupe de placement), sélectionnez le groupe de placement du cluster dans lequel lancer les instances. Si vous avez besoin de créer un groupe de placement du cluster, choisissez Create new placement group (Créer un groupe de placement).
10. Dans le panneau Résumé de droite, pour Nombre d'instances, entrez le nombre d'instances EFA activées que vous souhaitez lancer, puis choisissez Launch instance.

Étape 11 : Résilier l'instance temporaire

À ce stade, vous n'avez plus besoin de l'instance que vous avez lancée à l'étape 2. Vous pouvez résilier l'instance pour arrêter d'être facturé pour celle-ci.

Pour résilier l'instance temporaire

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance temporaire que vous avez créée, puis choisissez Actions, État de l'instance, Terminer (supprimer) l'instance.
4. Lorsque vous êtes invité à confirmer, choisissez Terminate (delete).

Étape 12 : activer le mode sans mot de passe SSH

Pour permettre à vos applications de s'exécuter sur toutes les instances de votre cluster, vous devez activer l'SSHaccès sans mot de passe entre le nœud principal et les nœuds membres. Le nœud principal est l'instance à partir de laquelle vous exécutez vos applications. Les instances restantes du cluster sont les nœuds membres.

Pour activer le mode sans mot de passe SSH entre les instances du cluster

1. Sélectionnez une instance dans le cluster en tant que nœud principal et connectez-vous à celle-ci.
2. Désactivez `strictHostKeyChecking` et activez `ForwardAgent` sur le nœud principal. Ouvrez le fichier `~/.ssh/config` à l'aide de l'éditeur de texte de votre choix et ajoutez ce qui suit.

   ```
   Host *
       ForwardAgent yes
   Host *
       StrictHostKeyChecking no
   ```

3. Générez une paire de RSA clés.

   ```
   $ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
   ```

   La paire de clés est créée dans le répertoire `$HOME/.ssh/`.
4. Modifiez les autorisations de la clé privée sur le nœud principal.

   ```
   $ chmod 600 ~/.ssh/id_rsa
   chmod 600 ~/.ssh/config
   ```

5. Ouvrez `~/.ssh/id_rsa.pub` à l'aide de l'éditeur de texte de votre choix et copiez la clé.
6. Pour chaque nœud membre du cluster, procédez comme suit :

   a. Connectez-vous à l'instance.

   b. Ouvrez `~/.ssh/authorized_keys` à l'aide de l'éditeur de texte de votre choix et ajoutez la clé publique que vous avez copiée plus tôt.
7. Pour vérifier que le système sans mot de passe SSH fonctionne comme prévu, connectez-vous à votre nœud principal et exécutez la commande suivante.

   ```
   $ ssh member_node_private_ip
   ```

   Vous devez vous connecter au nœud membre sans être invité à entrer une clé ou un mot de passe.

Commencez avec EFA et NCCL pour les charges de travail ML sur Amazon EC2

La bibliothèque de communications NVIDIA collectives (NCCL) est une bibliothèque de routines de communication collective standard pour GPUs plusieurs nœuds sur un ou plusieurs nœuds. NCCLpeut être utilisé avec EFA Libfabric et MPI pour prendre en charge diverses charges de travail d'apprentissage automatique. Pour plus d'informations, consultez le NCCLsite Web.

Les étapes suivantes vous aideront à démarrer EFA et à NCCL utiliser une base AMI pour l'un des systèmes d'exploitation pris en charge.

> **Note**
>
> - Seuls les types d'instance `p3dn.24xlarge`, `p4d.24xlarge`et `p5.48xlarge` sont pris en charge.
> - Seuls Amazon Linux 2 et Ubuntu 20.04/22.04 base AMIs sont pris en charge.
> - Seule la NCCL version 2.4.2 et les versions ultérieures sont prises en charge avecEFA.
> - Pour plus d'informations sur l'exécution de charges de travail de machine learning avec EFA et NCCL à l'aide d'un AWS Deep Learning AMIs, consultez EFAla DLAMI section Utilisation du manuel du AWS Deep Learning AMIs développeur.

Étapes

Étape 1 : préparer un groupe EFA de sécurité activé

Un EFA nécessite un groupe de sécurité qui autorise tout le trafic entrant et sortant à destination et en provenance du groupe de sécurité lui-même. La procédure suivante crée un groupe de sécurité qui autorise tout le trafic entrant et sortant à destination et en provenance de lui-même, et qui autorise le SSH trafic entrant depuis n'importe quelle IPv4 adresse à des fins de connectivité. SSH

> **Important**
>
> Ce groupe de sécurité n'est destiné qu'à des fins de test. Pour vos environnements de production, nous vous recommandons de créer une SSH règle entrante qui autorise le trafic uniquement en provenance de l'adresse IP à partir de laquelle vous vous connectez, telle que l'adresse IP de votre ordinateur ou d'une plage d'adresses IP de votre réseau local.

Pour d'autres scénarios, consultez Règles de groupe de sécurité pour différents cas d'utilisation.

Pour créer un groupe EFA de sécurité activé

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité), puis Create security group (Créer un groupe de sécurité).
3. Dans la fenêtre Create security group (Créer un groupe de sécurité), procédez comme suit :
   a. Pour Nom du groupe de sécurité, saisissez un nom descriptif pour le groupe de sécurité, tel que `EFA-enabled security group`.
   b. (Facultatif) Pour Description, saisissez une brève description du groupe de sécurité.
   c. Pour VPC, sélectionnez l'instance VPC dans laquelle vous souhaitez lancer vos instances EFA activées.
   d. Sélectionnez Create security group (Créer un groupe de sécurité).
4. Sélectionnez le groupe de sécurité que vous avez créé et dans l'onglet Details (Détails), copiez le Security group ID (ID du groupe de sécurité).

5. En conservant la sélection du groupe de sécurité, choisissez Actions, Edit inbound rules (Modifier les règles entrantes), puis procédez comme suit :
   a. Choisissez Ajouter une règle.
   b. Pour Type, sélectionnez Tout le trafic.
   c. Pour Source type (Type de source), choisissez Custom (Personnalisée) et collez l'ID du groupe de sécurité que vous avez copié dans le champ.
   d. Choisissez Ajouter une règle.
   e. Pour Type, sélectionnez SSH.
   f. Pour Type de source, choisissez N'importe où- IPv4.
   g. Sélectionnez Enregistrer les règles.
6. En conservant la sélection du groupe de sécurité, choisissez Actions, Edit outbound rules (Modifier les règles sortantes), puis procédez comme suit :
   a. Choisissez Ajouter une règle.
   b. Pour Type, sélectionnez Tout le trafic.
   c. Pour Destination type (Type de destination), choisissez Custom (Personnalisée) et collez l'ID du groupe de sécurité que vous avez copié dans le champ.
   d. Sélectionnez Enregistrer les règles.

Étape 2 : Lancer une instance temporaire

Lancez une instance temporaire que vous pouvez utiliser pour installer et configurer les composants EFA logiciels. Vous utilisez cette instance pour créer une instance EFA activée à AMI partir de laquelle vous pouvez lancer vos instances EFA activées.

Pour lancer une instance temporaire

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Instances, puis Launch Instances (Lancer des instances) pour ouvrir le nouvel assistant de lancement d'instance.
3. (Facultatif) Dans la section Name and tags (Noms et identifications), fournissez un nom pour l'instance, tel que `EFA-instance`. Le nom est attribué à l'instance en tant qu'identification de ressource (`Name=`*`EFA-instance`*).

4. Dans la section Images de l'application et du système d'exploitation, sélectionnez un AMI pour l'un des systèmes d'exploitation pris en charge. Seuls Amazon Linux 2, Ubuntu 20.04 et Ubuntu 22.04 sont pris en charge.
5. Dans la section Type d'instance, sélectionnez `p3dn.24xlarge`, `p4d.24xlarge` ou `p5.48xlarge`.
6. Dans la section Key pair (Paire de clés), sélectionnez la paire de clés à utiliser pour l'instance.
7. Dans la section Network settings (Paramètres réseau), choisissez Edit (Modifier), puis procédez comme suit :
   a. Pour Sous-réseau, choisissez le sous-réseau dans lequel lancer l'instance. Si vous ne sélectionnez aucun sous-réseau, vous ne pouvez pas activer l'instance pourEFA.
   b. Pour Firewall (security groups) (Pare-feu (groupes de sécurité)), choisissez Sélectionner un groupe de sécurité existant (Select existing security group), puis sélectionnez le groupe de sécurité que vous avez créé à l'étape précédente.
   c. Développez la section Advanced network configuration (Configuration réseau avancée) et pour Elastic Fabric Adapter (EFA), sélectionnez Enable (Activer).
8. Dans la section Storage (Stockage), configurez les volumes selon vos besoins.

   > **Note**
   >
   > Vous devez fournir 10 à 20 GiB de stockage supplémentaires pour le Nvidia CUDA Toolkit. Si vous ne fournissez pas suffisamment de stockage, vous recevrez un `insufficient disk space` message d'erreur lorsque vous tenterez d'installer les pilotes et le CUDA kit d'outils Nvidia.

9. Dans le panneau Summary (Récapitulatif) à droite, choisissez Launch instance (Lancer l'instance).

Étape 3 : Installation des GPU pilotes Nvidia, du CUDA kit d'outils Nvidia et du processeur DNN

Amazon Linux 2

Pour installer les GPU pilotes Nvidia, le CUDA kit d'outils Nvidia et cu DNN

1. Pour vous assurer que tous vos packages logiciels sont mis à jour, effectuez une mise à jour logicielle rapide sur votre instance.

   ```
   $ sudo yum upgrade -y && sudo reboot
   ```

   Reconnectez-vous à votre instance après son redémarrage.

2. Installez les utilitaires nécessaires à l'installation des GPU pilotes Nvidia et du CUDA kit d'outils Nvidia.

   ```
   $ sudo yum groupinstall 'Development Tools' -y
   ```

3. Désactiver le`nouveau`pilotes Open Source.

   a. Installez les utilitaires requis et le package d'en-têtes de noyau correspondant à la version du noyau que vous exécutez actuellement.

   ```
   $ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -
   r)
   ```

   b. Ajoutez nouveau au fichier de liste de refus `/etc/modprobe.d/blacklist.conf` .

   ```
   $ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
   blacklist vga16fb
   blacklist nouveau
   blacklist rivafb
   blacklist nvidiafb
   blacklist rivatv
   EOF
   ```

   c. Ajouter`GRUB_CMDLINE_LINUX="rdblacklist=nouveau"`vers le`grub` fichier et générez à nouveau la configuration Grub.

```
$ echo 'GRUB_CMDLINE_LINUX="rdblacklist=nouveau"' | sudo tee -a /etc/
default/grub \
&& sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Redémarrez l'instance et reconnectez-vous à celle-ci.
5. Préparer les référentiels requis

   a. Installez le EPEL référentiel pour votre distribution Linux DKMS et activez tous les dépôts facultatifs pour celle-ci.

   ```
   $ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-
   latest-7.noarch.rpm
   ```

   b. Installez la GPG clé publique du CUDA référentiel.

   ```
   $ distribution='rhel7'
   ```

   c. Configurez le référentiel CUDA réseau et mettez à jour le cache du référentiel.

   ```
   $ ARCH=$( /bin/arch ) \
   && sudo yum-config-manager --add-repo http://developer.download.nvidia.com/
   compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \
   && sudo yum clean expire-cache
   ```

   d. (Noyau version 5.10 uniquement) Effectuez ces étapes uniquement si vous utilisez Amazon Linux 2 avec le noyau version 5.10. Si vous utilisez Amazon Linux 2 avec le noyau version 4.12, ignorez ces étapes. Pour vérifier la version de votre noyau, exécutezuname -r.

      i. Créez le fichier de configuration du pilote Nvidia nommé`/etc/dkms/nvidia.conf`.

      ```
      $ sudo mkdir -p /etc/dkms \
      && echo "MAKE[0]=\"'make' -j2 module SYSSRC=\${kernel_source_dir}
       IGNORE_XEN_PRESENCE=1 IGNORE_PREEMPT_RT_PRESENCE=1 IGNORE_CC_MISMATCH=1
       CC=/usr/bin/gcc10-gcc\"" | sudo tee /etc/dkms/nvidia.conf
      ```

      ii. (`p4d.24xlarge` et `p5.48xlarge` uniquement) Copiez le fichier de configuration du pilote Nvidia.

```
$ sudo cp /etc/dkms/nvidia.conf /etc/dkms/nvidia-open.conf
```

6. Installez les GPU pilotes, le kit d'NVIDIACUDAoutils et le processeur NvidiaDNN.

   - `p3dn.24xlarge`

     ```
     $ sudo yum clean all \
     && sudo yum -y install kmod-nvidia-latest-dkms nvidia-driver-latest-dkms \
     && sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
     ```

   - `p4d.24xlarge` et `p5.48xlarge`

     ```
     $ sudo yum clean all \
     && sudo yum -y install kmod-nvidia-open-dkms nvidia-driver-latest-dkms \
     && sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
     ```

7. Redémarrez l'instance et reconnectez-vous à celle-ci.
8. (`p4d.24xlarge` et `p5.48xlarge` uniquement) Démarrez le service Nvidia Fabric Manager et assurez-vous qu'il démarre automatiquement au démarrage de l'instance. Nvidia Fabric Manager est requis pour la gestion des commutateurs NV.

   ```
   $ sudo systemctl enable nvidia-fabricmanager && sudo systemctl start nvidia-
   fabricmanager
   ```

9. Assurez-vous que les CUDA chemins sont définis à chaque démarrage de l'instance.

   - Pour les shells bash , ajoutez les instructions suivantes à /home/*username*/`.bashrc` et /home/*username*/`.bash_profile`.

     ```
     export PATH=/usr/local/cuda/bin:$PATH
     export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

   - Pour les shells tcsh , ajoutez les instructions suivantes à /home/*username*/`.cshrc`.

     ```
     setenv PATH=/usr/local/cuda/bin:$PATH
     setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

10. Pour vérifier que les GPU pilotes Nvidia fonctionnent, exécutez la commande suivante.

```
$ nvidia-smi -q | head
```

La commande doit renvoyer des informations sur NvidiaGPUs, les GPU pilotes Nvidia et le CUDA kit d'outils Nvidia.

Ubuntu 20.04/22.04

Pour installer les GPU pilotes Nvidia, le CUDA kit d'outils Nvidia et cu DNN

1. Pour vous assurer que tous vos packages logiciels sont mis à jour, effectuez une mise à jour logicielle rapide sur votre instance.

```
$ sudo apt-get update && sudo apt-get upgrade -y
```

2. Installez les utilitaires nécessaires à l'installation des GPU pilotes Nvidia et du CUDA kit d'outils Nvidia.

```
$ sudo apt-get update && sudo apt-get install build-essential -y
```

3. Pour utiliser le GPU pilote Nvidia, vous devez d'abord désactiver les pilotes `nouveau` open source.

   a. Installez les utilitaires requis et le package d'en-têtes de noyau correspondant à la version du noyau que vous exécutez actuellement.

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

   b. Ajoutez `nouveau` au fichier de liste de refus `/etc/modprobe.d/blacklist.conf` .

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   c. Ouvrez le fichier `/etc/default/grub` à l'aide de l'éditeur de texte de votre choix et ajoutez ce qui suit.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

d. Générez à nouveau la configuration Grub.

```
$ sudo update-grub
```

4. Redémarrez l'instance et reconnectez-vous à celle-ci.
5. Ajoutez le CUDA référentiel et installez les GPU pilotes Nvidia, la NVIDIA CUDA boîte à outils et le processeurDNN.

   - `p3dn.24xlarge`

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
ubuntu2004_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
compute/cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/ /' \
&& sudo apt update \
&& sudo apt install nvidia-dkms-535 \
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535
 cuda-toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

   - `p4d.24xlarge` et `p5.48xlarge`

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
ubuntu2004_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
```

```
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
compute/cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/ /' \
&& sudo apt update \
&& sudo apt install nvidia-kernel-open-535 \
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535
 cuda-toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

6. Redémarrez l'instance et reconnectez-vous à celle-ci.
7. (`p4d.24xlarge` et `p5.48xlarge` uniquement) Installez Nvidia Fabric Manager.

   a. Vous devez installer la version de Nvidia Fabric Manager qui correspond à la version du module de noyau Nvidia que vous avez installée à l'étape précédente.

      Exécutez la commande suivante pour déterminer la version du module de noyau Nvidia.

      ```
      $ cat /proc/driver/nvidia/version | grep "Kernel Module"
      ```

      Voici un exemple de sortie.

      ```
      NVRM version: NVIDIA UNIX x86_64 Kernel Module  450.42.01  Tue Jun 15
       21:26:37 UTC 2021
      ```

      Dans l'exemple ci-dessus, la version principale `450` du module de noyau a été installée. Cela signifie que vous devez installer la version `450` de Nvidia Fabric Manager.

   b. Installez Nvidia Fabric Manager. Exécutez la commande suivante et spécifiez la version principale identifiée à l'étape précédente.

      ```
      $ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
      fabricmanager-major_version_number
      ```

      Par exemple, si la version majeure `450` du module de noyau a été installée, utilisez la commande suivante pour installer la version correspondante de Nvidia Fabric Manager.

      ```
      $ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
      fabricmanager-450
      ```

c. Démarrez le service et assurez-vous qu'il démarre automatiquement au démarrage de l'instance. Nvidia Fabric Manager est requis pour la gestion des commutateurs NV.

```
$ sudo systemctl start nvidia-fabricmanager && sudo systemctl enable nvidia-
fabricmanager
```

8. Assurez-vous que les CUDA chemins sont définis à chaque démarrage de l'instance.

   - Pour les shells bash , ajoutez les instructions suivantes à /home/*username*/.bashrc et /home/*username*/.bash_profile.

   ```
   export PATH=/usr/local/cuda/bin:$PATH
   export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
   lib64:$LD_LIBRARY_PATH
   ```

   - Pour les shells tcsh , ajoutez les instructions suivantes à /home/*username*/.cshrc.

   ```
   setenv PATH=/usr/local/cuda/bin:$PATH
   setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
   lib64:$LD_LIBRARY_PATH
   ```

9. Pour vérifier que les GPU pilotes Nvidia fonctionnent, exécutez la commande suivante.

   ```
   $ nvidia-smi -q | head
   ```

   La commande doit renvoyer des informations sur NvidiaGPUs, les GPU pilotes Nvidia et le CUDA kit d'outils Nvidia.

Étape 4 : installation de GDRCopy

Installez GDRCopy pour améliorer les performances de Libfabric. Pour plus d'informationsGDRCopy, consultez le GDRCopyréférentiel.

Amazon Linux 2

Pour installer GDRCopy

1. Installez les dépendances obligatoires.

```
$ sudo yum -y install dkms rpm-build make check check-devel subunit subunit-
devel
```

2. Téléchargez et extrayez le GDRCopy package.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
&& tar xf v2.4.tar.gz ; cd gdrcopy-2.4/packages
```

3. Créez le GDRCopy RPM package.

```
$ CUDA=/usr/local/cuda ./build-rpm-packages.sh
```

4. Installez le GDRCopy RPM package.

```
$ sudo rpm -Uvh gdrcopy-kmod-2.4-1dkms.noarch*.rpm \
&& sudo rpm -Uvh gdrcopy-2.4-1.x86_64*.rpm \
&& sudo rpm -Uvh gdrcopy-devel-2.4-1.noarch*.rpm
```

Ubuntu 20.04/22.04

Pour installer GDRCopy

1. Installez les dépendances obligatoires.

```
$ sudo apt -y install build-essential devscripts debhelper check libsubunit-dev
 fakeroot pkg-config dkms
```

2. Téléchargez et extrayez le GDRCopy package.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
&& tar xf v2.4.tar.gz \
&& cd gdrcopy-2.4/packages
```

3. Créez le GDRCopy RPM package.

```
$ CUDA=/usr/local/cuda ./build-deb-packages.sh
```

4. Installez le GDRCopy RPM package.

```
$ sudo dpkg -i gdrdrv-dkms_2.4-1_amd64.*.deb \
```

```
&& sudo dpkg -i libgdrapi_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy-tests_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy_2.4-1_amd64.*.deb
```

Étape 5 : Installation du EFA logiciel

Installez le noyau EFA activé, EFA les pilotes, Libfabric et Open MPI Stack nécessaires à la prise en charge de votre EFA instance temporaire.

Pour installer le logiciel EFA

1. Connectez-vous à l'instance que vous avez lancée. Pour de plus amples informations, veuillez consulter Connectez-vous à votre instance Linux à l'aide de SSH.
2. Téléchargez les fichiers d'installation du logiciel EFA. Les fichiers d'installation du logiciel sont packagés dans un fichier d'archive compressé (`.tar.gz`). Pour télécharger la version stable la plus récente, utilisez la commande suivante.

   ```
   $ curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.34.0.tar.gz
   ```

   Vous pouvez aussi obtenir la dernière version en remplaçant le numéro de version par `latest` dans la commande ci-dessus.
3. (Facultatif) Vérifiez l'authenticité et l'intégrité du fichier EFA tarball (`.tar.gz`).

   Nous vous recommandons de le faire pour vérifier l'identité de l'éditeur du logiciel et pour vérifier que le fichier n'a pas été modifié ou endommagé depuis sa publication. Si vous ne souhaitez pas vérifier le fichier d'archive, ignorez cette étape.

   > **Note**
   >
   > Sinon, si vous préférez vérifier le fichier tarball en utilisant plutôt une SHA256 somme de contrôle MD5 ou, consultez. Vérifiez le EFA programme d'installation à l'aide d'une somme de contrôle

   a. Téléchargez la GPG clé publique et importez-la dans votre trousseau de clés.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --
import aws-efa-installer.key
```

La commande doit renvoyer une valeur clé. Notez la valeur clé, car vous en aurez besoin lors de l'étape suivante.

b. Vérifiez l'empreinte digitale de la GPG clé. Exécutez la commande suivante et spécifiez la valeur clé que vous avez obtenue à l'étape précédente.

```
$ gpg --fingerprint key_value
```

La commande doit renvoyer une empreinte digitale identique à `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC`. Si l'empreinte digitale ne correspond pas, n'exécutez pas le script EFA d'installation et contactez AWS Support.

c. Téléchargez le fichier de signature et vérifiez la signature du fichier EFA tarball.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.34.0.tar.gz.sig
 && gpg --verify ./aws-efa-installer-1.34.0.tar.gz.sig
```

Voici un exemple de sortie.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1  5E59 A054 80B1 DD2D 3CCC
```

Si le résultat inclut `Good signature` et que l'empreinte digitale correspond à l'empreinte digitale renvoyée à l'étape précédente, passez à l'étape suivante. Si ce n'est pas le cas, n'exécutez pas le script EFA d'installation et contactez AWS Support.

4. Procédez à l'extraction des fichiers à partir du fichier compressé `.tar.gz` et accédez au répertoire extrait.

```
$ tar -xf aws-efa-installer-1.34.0.tar.gz && cd aws-efa-installer
```

5. Exécutez le script d'installation du logicielEFA.

> **Note**
>
> À partir de la version EFA 1.30.0, Open MPI 4 et Open MPI 5 sont installés par défaut. À moins que vous n'ayez besoin d'Open MPI 5, nous vous recommandons de n'installer qu'Open MPI 4. La commande suivante installe uniquement Open MPI 4. Si vous souhaitez installer Open MPI 4 et Open MPI 5, supprimez-les`--mpi=openmpi4`.

```
$ sudo ./efa_installer.sh -y --mpi=openmpi4
```

Libfabric est installé dans le `/opt/amazon/efa` répertoire, tandis qu'Open MPI est installé dans le `/opt/amazon/openmpi` répertoire.

6. Si le EFA programme d'installation vous invite à redémarrer l'instance, faites-le, puis reconnectez-vous à l'instance. Sinon, déconnectez-vous de l'instance, puis reconnectez-vous pour terminer l'installation.
7. Vérifiez que les composants EFA logiciels ont été correctement installés.

```
$ fi_info -p efa -t FI_EP_RDM
```

La commande doit renvoyer des informations sur les EFA interfaces Libfabric. L'exemple suivant illustre la sortie de la commande.

- `p3dn.24xlarge` avec interface réseau unique

```
provider: efa
fabric: EFA-fe80::94:3dff:fe89:1b70
domain: efa_0-rdm
version: 2.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

- `p4d.24xlarge` et `p5.48xlarge` avec plusieurs interfaces réseau

```
provider: efa
fabric: EFA-fe80::c6e:8fff:fef6:e7ff
domain: efa_0-rdm
version: 111.0
```

```
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c34:3eff:feb2:3c35
domain: efa_1-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c0f:7bff:fe68:a775
domain: efa_2-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::ca7:b0ff:fea6:5e99
domain: efa_3-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

Étape 6 : Installation NCCL

InstallezNCCL. Pour plus d'informationsNCCL, consultez le NCCLréférentiel.

Pour installer NCCL

1. Accédez au répertoire `/opt`.

```
$ cd /opt
```

2. Clonez le NCCL référentiel officiel sur l'instance et accédez au référentiel cloné local.

```
$ sudo git clone https://github.com/NVIDIA/nccl.git && cd nccl
```

3. Compilez, installez NCCL et spécifiez le répertoire CUDA d'installation.

```
$ sudo make -j src.build CUDA_HOME=/usr/local/cuda
```

Étape 7 : Installation du aws-ofi-nccl plugin

Le aws-ofi-nccl plugin fait correspondre le transport orienté connexion NCCL de Libfabric APIs à l'interface fiable sans connexion de Libfabric. Cela vous permet d'utiliser Libfabric en tant que fournisseur de réseau lors de l'exécution d'applications NCCL basées sur des applications. Pour plus d'informations sur le aws-ofi-nccl plugin, consultez le aws-ofi-nccl référentiel.

Pour installer le aws-ofi-nccl plugin

1. Accédez à votre répertoire de base.

```
$ cd $HOME
```

2. Installez les utilitaires requis.

   - Amazon Linux 2

```
$ sudo yum install hwloc-devel
```

   - Ubuntu

```
$ sudo apt-get install libhwloc-dev
```

3. Téléchargez les fichiers du aws-ofi-nccl plugin. Les fichiers sont packagés dans un fichier d'archive compressé (`.tar.gz`).

```
$ wget https://github.com/aws/aws-ofi-nccl/releases/download/v1.11.0-aws/aws-ofi-nccl-1.11.0-aws.tar.gz
```

4. Procédez à l'extraction des fichiers à partir du fichier compressé .tar.gz et accédez au répertoire extrait.

```
$ tar -xf aws-ofi-nccl-1.11.0-aws.tar.gz && cd aws-ofi-nccl-1.11.0-aws
```

5. Pour générer les fichiers make, exécutez le `configure` script et spécifiez les répertoiresMPI, Libfabric NCCL et CUDA d'installation.

```
$ ./configure --prefix=/opt/aws-ofi-nccl --with-mpi=/opt/amazon/openmpi \
--with-libfabric=/opt/amazon/efa \
--with-cuda=/usr/local/cuda \
--enable-platform-aws
```

6. Ajoutez le MPI répertoire Open à la PATH variable.

```
$ export PATH=/opt/amazon/openmpi/bin/:$PATH
```

7. Installez le aws-ofi-nccl plugin.

```
$ make && sudo make install
```

Étape 8 : Installation des NCCL tests

Installez les NCCL tests. Les NCCL tests vous permettent de confirmer qu'il NCCL est correctement installé et qu'il fonctionne comme prévu. Pour plus d'informations sur les NCCL tests, consultez le référentiel nccl-tests.

Pour installer les NCCL tests

1. Accédez à votre répertoire de base.

```
$ cd $HOME
```

2. Clonez le référentiel officiel nccl-tests dans l'instance et accédez au référentiel cloné local.

```
$ git clone https://github.com/NVIDIA/nccl-tests.git && cd nccl-tests
```

3. Ajoutez le répertoire Libfabric à la variable LD_LIBRARY_PATH.

   - Amazon Linux 2

   ```
   $ export LD_LIBRARY_PATH=/opt/amazon/efa/lib64:$LD_LIBRARY_PATH
   ```

   - Ubuntu

   ```
   $ export LD_LIBRARY_PATH=/opt/amazon/efa/lib:$LD_LIBRARY_PATH
   ```

4. Installez les NCCL tests et spécifiez les répertoires CUDA d'installation MPINCCL, et.

```
$ make MPI=1 MPI_HOME=/opt/amazon/openmpi NCCL_HOME=/opt/nccl/build CUDA_HOME=/usr/
local/cuda
```

Étape 9 : Testez votre NCCL configuration EFA et

Exécutez un test pour vous assurer que votre instance temporaire est correctement configurée pour EFA etNCCL.

Pour tester votre NCCL configuration EFA et

1. Créez un fichier hôte qui spécifie les hôtes sur lesquels les tests doivent être exécutés. La commande suivante crée un fichier hôte nommé `my-hosts` qui inclut une référence à l'instance elle-même.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
   meta-data/local-ipv4 >> my-hosts
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4 >> my-
   hosts
   ```

2. Exécutez le test et spécifiez le fichier hôte (`--hostfile`) et le nombre de fichiers GPUs à utiliser (`-n`). La commande suivante exécute le `all_reduce_perf` test sur 8 GPUs sur l'instance elle-même et spécifie les variables d'environnement suivantes.

   - `FI_EFA_USE_DEVICE_RDMA=1`— utilise (`p4d.24xlarge`uniquement) les RDMA fonctionnalités de l'appareil pour les transferts unilatéraux et recto verso.
   - `NCCL_DEBUG=INFO` : permet des sorties de débogage détaillées. Vous pouvez également spécifier `VERSION` d'imprimer uniquement la NCCL version au début du test ou de ne `WARN` recevoir que des messages d'erreur.

   Pour plus d'informations sur les arguments de NCCL test, consultez les NCCLtests README dans le référentiel officiel nccl-tests.

   - `p3dn.24xlarge`

   ```
   $ /opt/amazon/openmpi/bin/mpirun \
   ```

```
-x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
lib:/opt/amazon/openmpi/lib:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \
-x NCCL_DEBUG=INFO \
--hostfile my-hosts -n 8 -N 8 \
--mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-to
 none \
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

- `p4d.24xlarge` et `p5.48xlarge`

```
$ /opt/amazon/openmpi/bin/mpirun \
-x FI_EFA_USE_DEVICE_RDMA=1 \
-x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
lib:/opt/amazon/openmpi/lib:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \
-x NCCL_DEBUG=INFO \
--hostfile my-hosts -n 8 -N 8 \
--mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-to
 none \
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

3. Vous pouvez confirmer qu'il EFA est actif en tant que fournisseur sous-jacent NCCL lorsque le `NCCL_DEBUG` journal est imprimé.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Selected Provider is efa*
```

Les informations supplémentaires suivantes s'affichent lors de l'utilisation d'une instance `p4d.24xlarge`.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Running on P4d platform, Setting
 NCCL_TOPO_FILE environment variable to /home/ec2-user/install/plugin/share/aws-
ofi-nccl/xml/p4d-24xl-topo.xml
```

Étape 10 : Installer vos applications de Machine Learning

Installez les applications de machine learning sur l'instance temporaire. La procédure d'installation varie selon l'application de machine learning spécifique. Pour plus d'informations sur l'installation de logiciels sur votre instance Linux, consultez Gérer les logiciels sur votre instance Amazon Linux 2.

> **Note**
>
> Reportez-vous à la documentation de votre application de machine learning pour obtenir des instructions d'installation.

Étape 11 : Création EFA d'NCCLun AMI

Après avoir installé les composants logiciels requis, vous en créez un AMI que vous pouvez réutiliser pour lancer vos instances EFA compatibles.

Pour créer un fichier AMI à partir de votre instance temporaire

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance temporaire que vous avez créée et choisissez Actions, Image, Créer une image.
4. Pour Créer une image, procédez comme suit :
   a. Dans Nom de l'image, entrez un nom descriptif pourAMI.
   b. (Facultatif) Dans Description de l'image, entrez une brève description de l'objectif duAMI.
   c. Choisissez Create image (Créer une image).
5. Dans le volet de navigation, choisissez AMIs.
6. Localisez le AMI fichier que vous avez créé dans la liste. Attendez que le statut passe de `pending` à `available` avant de poursuivre avec l'étape suivante.

Étape 12 : Résilier l'instance temporaire

À ce stade, vous n'avez plus besoin de l'instance temporaire que vous avez lancée. Vous pouvez résilier l'instance pour arrêter d'être facturé pour celle-ci.

Pour résilier l'instance temporaire

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance temporaire que vous avez créée puis choisissez Actions, État de l'instance, Résilier l'instance.

4. Lorsque vous êtes invité à confirmer, choisissez Terminate (Mettre fin).

Étape 13 : Lancer EFA et NCCL activer des instances dans un groupe de placement de clusters

Lancez vos instances NCCL activées EFA et activées dans un groupe de placement de clusters à l'aide du groupe de sécurité EFA activé AMI et du groupe de sécurité EFA activé que vous avez créés précédemment.

> **Note**
>
> - Il n'est pas obligatoire de lancer vos instances EFA activées dans un groupe de placement de clusters. Toutefois, nous vous recommandons d'exécuter vos instances EFA activées dans un groupe de placement de clusters, car cela les lance dans un groupe à faible latence dans une seule zone de disponibilité.
> - Pour vous assurer que la capacité est disponible lorsque vous mettez à l'échelle les instances de votre cluster, vous pouvez créer une réserve de capacité pour votre groupe de placement du cluster. Pour plus d'informations, consultez Création de réservations de capacité dans des groupes de placement de clusters.

New console

Pour lancer une instance temporaire

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Instances, puis Launch Instances (Lancer des instances) pour ouvrir le nouvel assistant de lancement d'instance.
3. (Facultatif) Dans la section Name and tags (Noms et identifications), fournissez un nom pour l'instance, tel que `EFA-instance`. Le nom est attribué à l'instance en tant qu'identification de ressource (`Name=`*`EFA-instance`*).
4. Dans la section Images de l'application et du système d'exploitationAMIs, choisissez Mon, puis sélectionnez celle AMI que vous avez créée à l'étape précédente.
5. Dans la section Instance type (Type d'instance), sélectionnez `p3dn.24xlarge` ou `p4d.24xlarge`.

6. Dans la section Key pair (Paire de clés), sélectionnez la paire de clés à utiliser pour l'instance.
7. Dans la section Network settings (Paramètres réseau), choisissez Edit (Modifier), puis procédez comme suit :

   a. Pour Sous-réseau, choisissez le sous-réseau dans lequel lancer l'instance. Si vous ne sélectionnez aucun sous-réseau, vous ne pouvez pas activer l'instance pourEFA.

   b. Pour Firewall (security groups) (Pare-feu (groupes de sécurité)), choisissez Sélectionner un groupe de sécurité existant (Select existing security group), puis sélectionnez le groupe de sécurité que vous avez créé à l'étape précédente.

   c. Développez la section Advanced network configuration (Configuration réseau avancée) et pour Elastic Fabric Adapter (EFA), sélectionnez Enable (Activer).
8. (Facultatif) Dans la section Storage (Stockage), configurez les volumes selon vos besoins.
9. Dans la section Advanced details (Détails avancés), pour Placement group name (Nom du groupe de placement), sélectionnez le groupe de placement du cluster dans lequel lancer l'instance. Si vous avez besoin de créer un groupe de placement du cluster, choisissez Create new placement group (Créer un groupe de placement).
10. Dans le panneau Résumé de droite, pour Nombre d'instances, entrez le nombre d'instances EFA activées que vous souhaitez lancer, puis choisissez Launch instance.

Old console

Pour lancer vos instances NCCL compatibles EFA et dans un groupe de placement de clusters

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Choisissez Launch Instances (Lancer les instances).
3. Sur la AMI page Choisir un, choisissez Mon AMIs, recherchez celui AMI que vous avez créé précédemment, puis sélectionnez Sélectionner.
4. Sur la page Choisir un type d'instance, sélectionnez p3dn.24xlarge, puis choisissez Suivant : configurer les détails d'instance.
5. Sur la page Configurer les détails de l'instance, procédez de la façon suivante :

   a. Dans le champ Nombre d'instances, entrez le nombre EFA d'instances NCCL activées que vous souhaitez lancer.

b. Pour Réseau et sous-réseau, sélectionnez le sous-réseau VPC et dans lequel vous souhaitez lancer les instances.

c. Pour le Groupe de placement, sélectionnez Ajoutez une instance au groupe de placement.

d. Pour Nom du groupe de placement, sélectionnez Ajouter à un nouveau groupe de placement, puis saisissez un nom descriptif pour le groupe de placement. Ensuite, pour Stratégie du groupe de placement, sélectionnez Cluster.

e. Pour EFA, choisissez Enable (Activer).

f. Dans la section Interfaces réseau, pour l'appareil eth0, choisissez Nouvelle interface réseau. Vous pouvez éventuellement spécifier une IPv4 adresse principale et une ou plusieurs IPv4 adresses secondaires. Si vous lancez l'instance dans un sous-réseau associé à un IPv6 CIDR bloc, vous pouvez éventuellement spécifier une IPv6 adresse principale et une ou plusieurs IPv6 adresses secondaires.

g. Choisissez Next: Add Storage (Suivant : Ajouter le stockage).

6. Sur la page Ajouter du stockage, spécifiez les volumes à associer aux instances en plus des volumes spécifiés par le AMI (comme le volume du périphérique racine). Choisissez ensuite Suivant : Ajouter des balises.
7. Sur la page Ajouter des balises, spécifiez des balises pour l'instance, par exemple un nom évocateur, puis sélectionnez Suivant : Configurer le groupe de sécurité.
8. Sur la page Configurer le groupe de sécurité, cliquez sur Attribuer un groupe de sécurité, choisissez Sélectionner un groupe de sécurité existant, puis le groupe de sécurité que vous avez créé précédemment.
9. Choisissez Vérifier et lancer.
10. Sur la page Examiner le lancement de l'instance, vérifiez les paramètres, puis choisissez Lancer pour sélectionner une paire de clés et lancer votre instance.

Étape 14 : activer le mode sans mot de passe SSH

Pour permettre à vos applications de s'exécuter sur toutes les instances de votre cluster, vous devez activer l'SSHaccès sans mot de passe entre le nœud principal et les nœuds membres. Le nœud principal est l'instance à partir de laquelle vous exécutez vos applications. Les instances restantes du cluster sont les nœuds membres.

Pour activer le mode sans mot de passe SSH entre les instances du cluster

1. Sélectionnez une instance dans le cluster en tant que nœud principal et connectez-vous à celle-ci.
2. Désactivez `strictHostKeyChecking` et activez `ForwardAgent` sur le nœud principal. Ouvrez le fichier `~/.ssh/config` à l'aide de l'éditeur de texte de votre choix et ajoutez ce qui suit.

   ```
   Host *
       ForwardAgent yes
   Host *
       StrictHostKeyChecking no
   ```

3. Générez une paire de RSA clés.

   ```
   $ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
   ```

   La paire de clés est créée dans le répertoire `$HOME/.ssh/`.
4. Modifiez les autorisations de la clé privée sur le nœud principal.

   ```
   $ chmod 600 ~/.ssh/id_rsa
   chmod 600 ~/.ssh/config
   ```

5. Ouvrez `~/.ssh/id_rsa.pub` à l'aide de l'éditeur de texte de votre choix et copiez la clé.
6. Pour chaque nœud membre du cluster, procédez comme suit :

   a. Connectez-vous à l'instance.

   b. Ouvrez `~/.ssh/authorized_keys` à l'aide de l'éditeur de texte de votre choix et ajoutez la clé publique que vous avez copiée plus tôt.
7. Pour vérifier que le système sans mot de passe SSH fonctionne comme prévu, connectez-vous à votre nœud principal et exécutez la commande suivante.

   ```
   $ ssh member_node_private_ip
   ```

   Vous devez vous connecter au nœud membre sans être invité à entrer une clé ou un mot de passe.

Création et attachement d'un adaptateur Elastic Fabric à une EC2 instance Amazon

Vous pouvez créer une instance Amazon EFA et l'attacher à une EC2 instance Amazon de la même manière que n'importe quelle autre interface Elastic Network d'AmazonEC2. Cependant, contrairement aux interfaces réseau élastiques, elles ne EFAs peuvent pas être attachées ou détachées d'une instance dans un `running` état.

Considérations

- Vous pouvez modifier le groupe de sécurité associé à unEFA. Pour activer la fonctionnalité de contournement du système d'exploitation, EFA il doit être membre d'un groupe de sécurité qui autorise tout le trafic entrant et sortant à destination et en provenance du groupe de sécurité lui-même. Pour de plus amples informations, veuillez consulter Étape 1 : préparer un groupe EFA de sécurité activé.

  Vous modifiez le groupe de sécurité associé à un EFA de la même manière que vous modifiez le groupe de sécurité associé à une interface elastic network. Pour plus d'informations, consultez Modification du groupe de sécurité.
- Vous pouvez modifier les adresses IP associées à unEFA. Si vous possédez une adresse IP élastique, vous pouvez l'associer à unEFA. Si vous EFA êtes approvisionné dans un sous-réseau associé à un IPv6 CIDR bloc, vous pouvez attribuer une ou plusieurs IPv6 adresses au. EFA

  Vous attribuez une adresse IP élastique (IPv4) et une IPv6 adresse EFA à un de la même manière que vous attribuez une adresse IP à une interface réseau élastique. Pour plus d'informations, consultez Gestion des adresses IP.

Tâches

- Créez un EFA
- Attacher un EFA à une instance arrêtée
- Joindre un EFA lors du lancement d'une instance
- Ajouter un EFA à un modèle de lancement

Créez un EFA

Vous pouvez créer un EFA dans un sous-réseau dans unVPC. Vous ne pouvez pas le déplacer EFA vers un autre sous-réseau une fois qu'il a été créé, et vous ne pouvez l'attacher qu'aux instances arrêtées dans la même zone de disponibilité.

Pour en créer un nouveau à EFA l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Sélectionnez Créer une interface réseau.
4. Dans Description, entrez un nom descriptif pourEFA.
5. Pour Sous-réseau, sélectionnez le sous-réseau dans lequel vous souhaitez créer le. EFA
6. Pour IP privée, entrez l'IPv4adresse privée principale. Si vous ne spécifiez aucune IPv4 adresse, nous sélectionnons une IPv4 adresse privée disponible dans le sous-réseau sélectionné.
7. (IPv6uniquement) Si vous avez sélectionné un sous-réseau associé à un IPv6 CIDR bloc, vous pouvez éventuellement spécifier une IPv6 adresse dans le champ IPv6IP.
8. Pour Security groups (Groupes de sécurité), sélectionnez un ou plusieurs groupes de sécurité.
9. Pour EFA, choisissez Activé.
10. Choisissez Yes, Create.

Pour en créer un nouveau EFA à l'aide du AWS CLI

Utilisez la create-network-interfacecommande et pour`interface-type`, spécifiez`efa`, comme indiqué dans l'exemple suivant.

```
aws ec2 create-network-interface --subnet-id subnet-01234567890 --
description example_efa --interface-type efa
```

Attacher un EFA à une instance arrêtée

Vous pouvez attacher un EFA à n'importe quelle instance prise en charge qui est dans l'`stopped`état. Vous ne pouvez pas attacher un EFA à une instance qui est dans `running` cet état. Pour plus d'informations sur les types d'instance pris en charge, consultez Types d'instance pris en charge.

Vous attachez un EFA à une instance de la même manière que vous attachez une interface réseau à une instance. Pour de plus amples informations, veuillez consulter Joindre une interface réseau.

Joindre un EFA lors du lancement d'une instance

Pour attacher une instance existante EFA lors du lancement d'une instance (AWS CLI)

Utilisez la commande run-instances et pour NetworkInterfaceId, spécifiez l'ID duEFA, comme indiqué dans l'exemple suivant.

```
aws ec2 run-instances --image-id ami_id --count 1 --instance-
type c5n.18xlarge --key-name my_key_pair --network-interfaces
 DeviceIndex=0,NetworkInterfaceId=efa_id,Groups=sg_id,SubnetId=subnet_id
```

Pour attacher une nouvelle instance EFA lors du lancement d'une instance (AWS CLI)

Utilisez la commande run-instances et pour InterfaceType, spécifiez`efa`, comme indiqué dans l'exemple suivant.

```
aws ec2 run-instances --image-id ami_id --count 1 --instance-
type c5n.18xlarge --key-name my_key_pair --network-interfaces
 DeviceIndex=0,InterfaceType=efa,Groups=sg_id,SubnetId=subnet_id
```

Ajouter un EFA à un modèle de lancement

Vous pouvez créer un modèle de lancement contenant les informations de configuration nécessaires pour lancer des instances EFA compatibles. Pour créer un modèle de lancement EFA activé, créez un nouveau modèle de lancement et spécifiez un type d'instance pris en charge, votre groupe de EFA sécurité activé AMI et un groupe de sécurité EFA activé. Pour de plus amples informations, veuillez consulter Commencez avec EFA et MPI pour les HPC charges de travail sur Amazon EC2.

Vous pouvez utiliser les modèles de lancement pour lancer des instances EFA compatibles avec d'autres AWS services, tels que AWS Batchou AWS ParallelCluster.

Pour plus d'informations sur la création de modèles de lancement, consultez Création d'un modèle de EC2 lancement Amazon.

Détacher et supprimer un élément EFA d'une instance Amazon EC2

Vous pouvez détacher un élément EFA d'une EC2 instance Amazon et le supprimer de la même manière que n'importe quelle autre interface Elastic Network d'AmazonEC2.

Détacher un EFA

Pour détacher un agent EFA d'une instance, vous devez d'abord arrêter l'instance. Vous ne pouvez pas détacher un EFA élément d'une instance en cours d'exécution.

Vous détachez un élément EFA d'une instance de la même manière que vous détachez une interface elastic network d'une instance. Pour de plus amples informations, veuillez consulter Détacher une interface réseau.

Supprimer un EFA

Pour supprimer unEFA, vous devez d'abord le détacher de l'instance. Vous ne pouvez pas le supprimer EFA tant qu'il est attaché à une instance.

Vous supprimez EFAs de la même manière que vous supprimez les interfaces réseau élastiques. Pour de plus amples informations, veuillez consulter Supprimer une interface réseau.

Surveillez un adaptateur Elastic Fabric sur Amazon EC2

Vous pouvez utiliser les fonctions suivantes pour surveiller les performances de vos Elastic Fabric Adapters.

Journaux VPC de flux Amazon

Vous pouvez créer un journal Amazon VPC Flow pour recueillir des informations sur le trafic à destination et en provenance d'unEFA. Les données des journaux de flux peuvent être publiées sur Amazon CloudWatch Logs et Amazon S3. Une fois que vous avez créé un journal de flux, vous pouvez extraire et afficher ses données dans la destination choisie. Pour plus d'informations, consultez VPCFlow Logs dans le guide de VPC l'utilisateur Amazon.

Vous créez un journal de flux pour un EFA de la même manière que vous créez un journal de flux pour une interface Elastic Network. Pour plus d'informations, consultez la section Créer un journal de flux dans le guide de VPC l'utilisateur Amazon.

Dans les entrées du journal de flux, le EFA trafic est identifié par le `srcAddress` et`destAddress`, qui sont tous deux formatés sous forme d'MACadresses, comme indiqué dans l'exemple suivant.

```
version accountId  eniId        srcAddress        destAddress       sourcePort destPort
 protocol packets bytes start      end        action log-status
2       3794735123 eni-10000001 01:23:45:67:89:ab 05:23:45:67:89:ab -          -
 -        9       5689  1521232534 1524512343 ACCEPT OK
```

Amazon CloudWatch

Amazon CloudWatch fournit des statistiques qui vous permettent de surveiller votre EFAs activité en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Pour de plus amples informations, veuillez consulter Surveillez vos instances à l'aide de CloudWatch.

Vérifiez le EFA programme d'installation à l'aide d'une somme de contrôle

Vous pouvez éventuellement vérifier l'archive tar (fichier EFA .tar.gz) à l'aide d'une somme de contrôle ou. MD5 SHA256 Nous vous recommandons de le faire pour vérifier l'identité de l'éditeur du logiciel et pour vérifier que l'application n'a pas été modifiée ou endommagée depuis sa publication.

Pour vérifier l'archive

Utilisez l'utilitaire md5sum pour la somme de MD5 contrôle ou l'utilitaire sha256sum pour la somme de SHA256 contrôle, et spécifiez le nom de fichier de l'archive. Vous devez exécuter la commande à partir du répertoire dans lequel vous avez enregistré le fichier tarball.

- MD5

```
$  md5sum tarball_filename.tar.gz
```

- SHA256

```
$  sha256sum tarball_filename.tar.gz
```

Les commandes doivent renvoyer une valeur du total de contrôle au format suivant.

```
checksum_value tarball_filename.tar.gz
```

Comparez la valeur du total de contrôle renvoyée par la commande avec la valeur du total de contrôle fournie dans le tableau ci-dessous. Si les totaux de contrôle correspondent, on peut alors exécuter le script d'installation en toute sécurité. Si les totaux de contrôle ne correspondent pas, n'exécutez pas le script d'installation et contactez AWS Support.

Par exemple, la commande suivante vérifie l'archive EFA 1.9.4 à l'aide de la somme de contrôle. SHA256

```
$  sha256sum aws-efa-installer-1.9.4.tar.gz
```

Exemple de sortie :

```
1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14 aws-efa-
installer-1.9.4.tar.gz
```

Le tableau suivant répertorie les checksums des versions récentes deEFA.

Version	Télécharger URL	Totaux de contrôle
EFA1,34,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.34.0.tar.gz	MD5: `5cd4b28d27a31677c16139b54c9acb45` SHA256: `bd68839e741b0afd3ec2e37d50603803cfa7a279c120f0a736cc57c2ff2d7fdc`
EFA1,33,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.33.0.tar.gz	MD5: `e2f61fccbcaa11e2ccfddd3660522276` SHA256: `0372877b87c6a7337bb7791d255e1053b907d030489fb2c3732ba70069185fce`
EFA1,32,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.32.0.tar.gz	MD5: `db8d65cc028d8d08b5a9f2d88881c1b1` SHA256: `5f7233760be57f6fee6de8c09acbfbf59238de848e06048dc54d156ef578fc66`
EFA1,31,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.31.0.tar.gz	MD5: `856352f12bef2ccbadcd75e35aa52aaf`

Version	Télécharger URL	Totaux de contrôle
		SHA256: 943325bd37902a4300 ac9e5715163537d56e cb4e7b87b37827c3e5 47aa1897bf
EFA1,30,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.30.tar.gz	MD5: 31f48e1a47fe93ede8 ebd273fb747358 SHA256: 876ab9403e07a0c3c9 1a1a34685a52eced89 0ae052df94857f6081 c5f6c78a0a
EFA1,29.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.29.1.tar.gz	MD5: e1872ca815d752c1d7 c2b5c175e52a16 SHA256: 178b263b8c25845b63 dc93b25bcdff5870df 5204ec509af26f43e8 d283488744
EFA1,29,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.29.0.tar.gz	MD5: 39d06a002154d94cd9 82ed348133f385 SHA256: 836655f87015547e73 3e7d9f7c760e4e2469 7f8bbc261bb5f3560a bd4206bc36
EFA1,28,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.28.0.tar.gz	MD5: 9dc13b744666582260 5e66febe074035 SHA256: 2e625d2d6d3e073b51 78e8e861891273d896 b66d03cb1a32244fd5 6789f1c435

Version	Télécharger URL	Totaux de contrôle
EFA1,27,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.27.0.tar.gz	MD5: 98bfb515ea3e8d93f554020f3837fa15 SHA256: 1d49a97b0bf8d964d91652a79ac851f2550e33a5bf9d0cf86ec9357ff6579aa3
EFA1,26,1	https://efa-installer.amazonaws.com/aws-efa-installer-1.26.1.tar.gz	MD5: 884e74671fdef4725501f7cd2d451d0c SHA256: c616994c924f54ebfabfab32b7fe8ac56947fae00a0ff453d975e298d174fc96
EFA1,26,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.26.0.tar.gz	MD5: f8839f12ff2e3b9ba09ae8a82b30e663 SHA256: bc1abc1f76e97d204d3755d2a9ca307fc423e51c63141f798c2f15be3715aa11
EFA1.25.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.25.1.tar.gz	MD5: 6d876b894547847a45bb8854d4431f18 SHA256: d2abc553d22b89a4ce92882052c1fa6de450d3a801fe005da718b7d4b9602b06

Version	Télécharger URL	Totaux de contrôle
EFA1,25,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.25.0.tar.gz	MD5: 1993836ca749596051da04694ea0d00c SHA256: 98b7b26ce031a2d6a93de2297cc71b03af647194866369ca53b60d82d45ad342
EFA1.24.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.24.1.tar.gz	MD5: 211b249f39d53086f3cb0c07665f4e6f SHA256: 120cfeec233af0955623ac7133b674143329f9561a9a8193e473060f596aec62
EFA1,24,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.24.0.tar.gz	MD5: 7afe0187951e2dd2c9cc4b572e62f924 SHA256: 878623f819a0d9099d76ecd41cf4f569d4c3aac0c9bb7ba9536347c50b6bf88e
EFA1.23.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.23.1.tar.gz	MD5: 22491e114b6ee7160a8290145dca0c28 SHA256: 5ca848d8e0ff4d1571cd443c36f8d27c8cdf2a0c97e9068ebf000c303fc40797

Version	Télécharger URL	Totaux de contrôle
EFA1,23,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.23.0.tar.gz	MD5: 38a6d7c1861f5038dba4e441ca7683ca SHA256: 555d497a60f22e3857fdeb3dfc53aa86d05926023c68c916d15d2dc3df6525bd
EFA1.22.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.22.1.tar.gz	MD5: 600c0ad7cdbc06e8e846cb763f92901b SHA256: f90f3d5f59c031b9a964466b5401e86fd0429272408f6c207c3f9048254e9665
EFA1,2,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.22.0.tar.gz	MD5: 8f100c93dc8ab519c2aeb5dab89e98f8 SHA256: f329e7d54a86a03ea51da6ea9a5b68fb354fbae4a57a02f9592e21fce431dc3a
EFA1,21.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.21.0.tar.gz	MD5: 959ccc3a4347461909ec02ed3ba7c372 SHA256: c64e6ca34ccfc3ebe8e82d08899ae8442b3ef552541cf5429c43d11a04333050

Version	Télécharger URL	Totaux de contrôle
EFA1,20,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.20.0.tar.gz	MD5: `7ebfbb8e85f1b94709df4ab3db47913b` SHA256: `aeefd2681ffd5c4c631d1502867db5b831621d6eb85b61fe3ec80df983d1dcf0`
EFA1,19,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.19.0.tar.gz	MD5: `2fd45324953347ec5518da7e3fefa0ec` SHA256: `99b77821b9e72c8dea015cc92c96193e8db307deee05b91a58094cc331f16709`
EFA1,18,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.18.0.tar.gz	MD5: `fc2571a72f5d3c7b7b576ce2de38d91e` SHA256: `acb18a0808aedb9a5e485f1469225b9ac97f21db9af78e4cd6939700debe1cb6`
EFA1,17.3	https://efa-installer.amazonaws.com/aws-efa-installer-1.17.3.tar.gz	MD5: `0517df4a190356ab559235147174cafd` SHA256: `5130998b0d2883bbae189b21ab215ecbc1b01ae0231659a9b4a17b0a33ebc6ca`

Version	Télécharger URL	Totaux de contrôle
EFA1,17,2	https://efa-installer.amazonaws.com/aws-efa-installer-1.17.2.tar.gz	MD5: a329dedab53c4832df218a24449f4c9a SHA256: bca1fdde8b32b00346e175e597ffab32a09a08ee9ab136875fb38283cc4cd099
EFA1.17.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.17.1.tar.gz	MD5: 733ae2cfc9d14b52017eaf0a2ab6b0ff SHA256: f29322640a88ae9279805993cb836276ea240623820848463ca686c8ce02136f
EFA1,17,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.17.0.tar.gz	MD5: d430fc841563c11c3805c5f82a4746b1 SHA256: 75ab0cee4fb6bd38889dce313183f5d3a83bd233e0a6ef6205d8352821ea901d
EFA1,16,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.16.0.tar.gz	MD5: 399548d3b0d2e812d74dd67937b696b4 SHA256: cecec36495a1bc6fdc82f97761a541e4fb6c9a3cbf3cfcb145acf25ea5dbd45b

Version	Télécharger URL	Totaux de contrôle
EFA1.15.2	https://efa-installer.amazonaws.com/aws-efa-installer-1.15.2.tar.gz	MD5: 955fea580d5170b05823d51acde7ca21 SHA256: 84df4fbc1b3741b6c073176287789a601a589313accc8e6653434e8d4c20bd49
EFA1.15.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.15.1.tar.gz	MD5: c4610267039f72bbe4e35d7bf53519bc SHA256: be871781a1b9a15fca342a9d169219260069942a8bda7a8ad06d4baeb5e2efd7
EFA1,15,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.15.0.tar.gz	MD5: 9861694e1cc00d884fadac07d22898be SHA256: b329862dd5729d2d098d0507fb486bf859d7c70ce18b61c302982234a3a5c88f
EFA1.14.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.14.1.tar.gz	MD5: 50ba56397d359e57872fde1f74d4168a SHA256: c7b1b48e86fe4b3eaa4299d3600930919c4fe6d88cc6e2c7e4a408a3f16452c7

Version	Télécharger URL	Totaux de contrôle
EFA1,14.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.14.0.tar.gz	MD5: 40805e7fd842c36ececb9fd7f921b1ae SHA256: 662d62c12de85116df33780d40e0533ef7dad92709f4f613907475a7a1b60a97
EFA1,13,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.13.0.tar.gz	MD5: c91d16556f4fd53becadbb345828221e SHA256: ad6705eb23a3fce44af3afc0f7643091595653a723ad0374084f4f2b715192e1
EFA1.12.3	https://efa-installer.amazonaws.com/aws-efa-installer-1.12.3.tar.gz	MD5: 818aee81f097918cfaebd724eddea678 SHA256: 2c225321824788b8ca3fbc118207b944cdb096b847e1e0d1d853ef2f0d727172
EFA1.12.2	https://efa-installer.amazonaws.com/aws-efa-installer-1.12.2.tar.gz	MD5: 956bb1fc5ae0d6f0f87d2e481d49fccf SHA256: 083a868a2c212a5a4fcf3e4d732b685ce39cceb3ca7e5d50d0b74e7788d06259

Version	Télécharger URL	Totaux de contrôle
EFA1.12.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.12.1.tar.gz	MD5: `f5bfe52779df435188b0a2874d0633ea` SHA256: `5665795c2b4f09d5f3f767506d4d4c429695b36d4a17e5758b27f033aee58900`
EFA1,12,0	https://efa-installer.amazonaws.com/aws-efa-installer-1.12.0.tar.gz	MD5: `d6c6b49fafb39b770297e1cc44fe68a6` SHA256: `28256c57e9ecc0b0778b41c1f777a9982b4e8eae782343dfe1246079933dca59`
EFA 1.11.2	https://efa-installer.amazonaws.com/aws-efa-installer-1.11.2.tar.gz	MD5: `2376cf18d1353a4551e35c33d269c404` SHA256: `a25786f98a3628f7f54f7f74ee2b39bc6734ea9374720507d37d3e8bf8ee1371`
EFA 1.11.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.11.1.tar.gz	MD5: `026b0d9a0a48780cc7406bd51997b1c0` SHA256: `6cb04baf5ffc58ddf319e956b5461289199c8dd805fe216f8f9ab8d102f6d02a`

Version	Télécharger URL	Totaux de contrôle
EFA 1.11.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.11.0.tar.gz	MD5: 7d9058e010ad65bf2e14259214a36949 SHA256: 7891f6d45ae33e822189511c4ea1d14c9d54d000f6696f97be54e915ce2c9dfa
EFA 1.10.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.10.1.tar.gz	MD5: 78521d3d668be22976f46c6fecc7b730 SHA256: 61564582de7320b21de319f532c3a677d26cc46785378eb3b95c636506b9bcb4
EFA 1.10.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.10.0.tar.gz	MD5: 46f73f5a7afe41b4bb918c81888fefa9 SHA256: 136612f96f2a085a7d98296da0afb6fa807b38142e2fc0c548fa986c41186282
EFA 1.9.5	https://efa-installer.amazonaws.com/aws-efa-installer-1.9.5.tar.gz	MD5: 95edb8a209c18ba8d250409846eb6ef4 SHA256: a4343308d7ea4dc943ccc21bcebed913e8868e59bfb2ac93599c61a7c87d7d25

Version	Télécharger URL	Totaux de contrôle
EFA 1.9.4	https://efa-installer.amazonaws.com/aws-efa-installer-1.9.4.tar.gz	MD5: `f26dd5c350422c1a985e35947fa5aa28` SHA256: `1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14`
EFA 1.9.3	https://efa-installer.amazonaws.com/aws-efa-installer-1.9.3.tar.gz	MD5: `95755765a097802d3e6d5018d1a5d3d6` SHA256: `46ce732d6f3fcc9edf6a6e9f9df0ad136054328e24675567f7029edab90c68f1`
EFA 1.8.4	https://efa-installer.amazonaws.com/aws-efa-installer-1.8.4.tar.gz	MD5: `85d594c41e831afc6c9305263140457e` SHA256: `0d974655a09b213d7859e658965e56dc4f23a0eee2dc44bb41b6d039cc5bab45`

Topologie des EC2 instances Amazon

La description de la topologie de votre instance fournit une vue hiérarchique de la proximité relative entre les instances. Vous pouvez utiliser ces informations pour gérer l'infrastructure informatique de calcul à haute performance (HPC) et d'apprentissage automatique (ML) à grande échelle, tout en optimisant le placement professionnel. HPCet les tâches ML sont sensibles à la latence et au débit. Vous pouvez utiliser la topologie des instances pour détecter l'emplacement de vos instances, puis utiliser ces informations pour optimiser HPC les tâches ML en les exécutant sur des instances physiquement plus proches les unes des autres.

Vous pouvez utiliser la topologie d'instance pour détecter l'emplacement de vos instances existantes, mais vous ne pouvez pas l'utiliser pour choisir de lancer une nouvelle instance physiquement proche

d'une instance existante. Pour influencer le placement des instances, vous pouvez utiliserCréation de réservations de capacité dans des groupes de placement de clusters.

Tarification

La description de la topologie de votre instance n'entraîne aucun coût supplémentaire.

Table des matières

Considérations

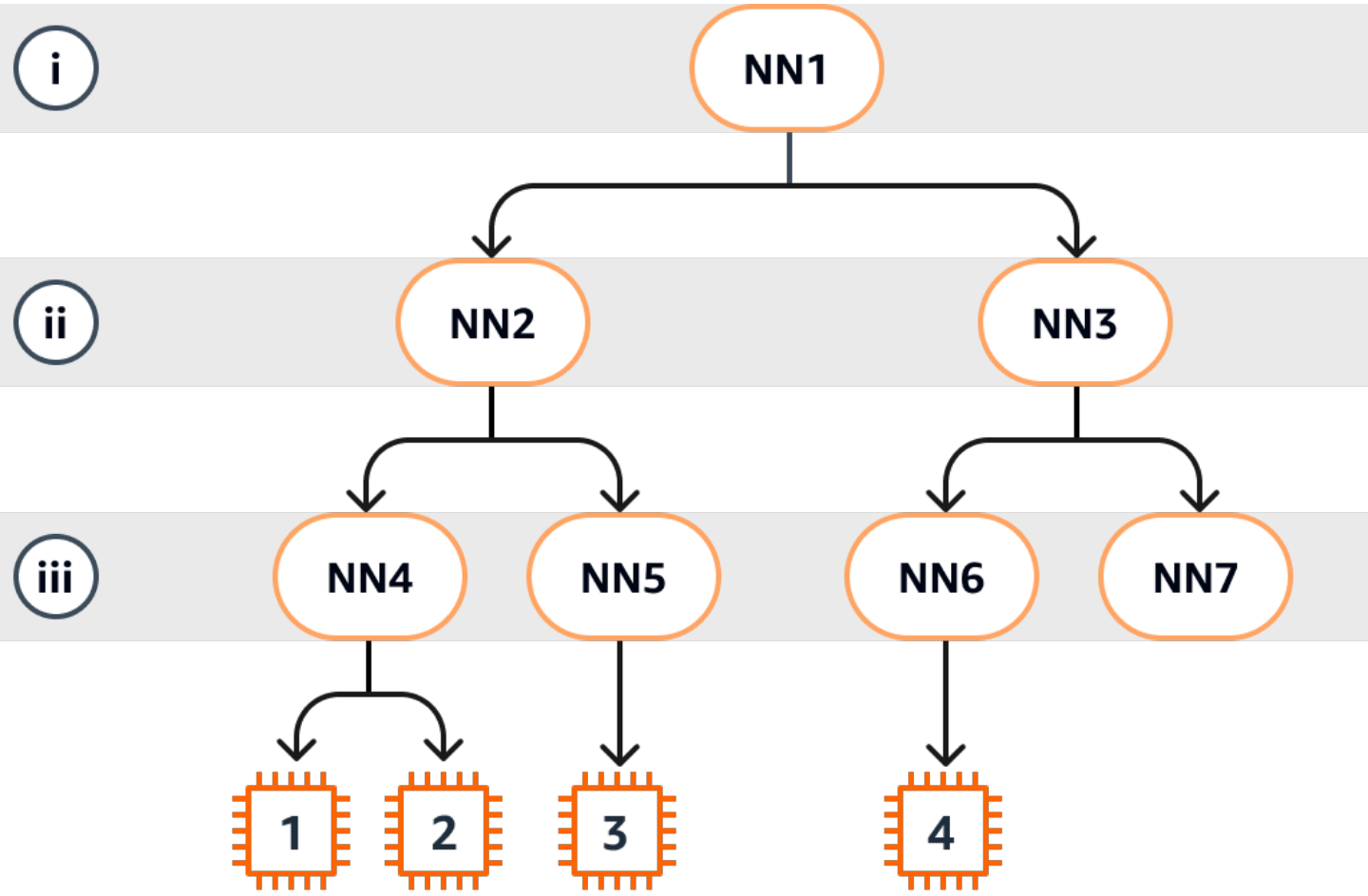
- Les instances doivent être conformes à l'`running`état.
- Chaque vue de topologie d'instance est unique par compte.
- AWS Management Console Ne prend pas en charge l'affichage de la topologie de l'instance.

Comment fonctionne la topologie des EC2 instances Amazon

Chaque EC2 instance se connecte à un ensemble de nœuds. Un ensemble de nœuds comprend trois nœuds de réseau, chaque nœud représentant une couche différente du AWS réseau. Les couches du réseau sont organisées selon une hiérarchie de 3 couches ou plus. L'ensemble de nœuds fournit une vue de haut en bas de cette hiérarchie, la couche inférieure étant connectée la plus proche d'une instance.

Les informations relatives à l'ensemble de nœuds sont appelées topologie d'instance.

Le schéma suivant fournit une représentation visuelle que vous pouvez utiliser pour comprendre la topologie de l'instance. Les nœuds du réseau sont identifiés comme NN1— NN7. Les chiffres i, ii et iii identifient les couches du réseau. Les chiffres 1, 2, 3 et 4 identifient les EC2 instances. Les instances se connectent à un nœud de la couche inférieure, identifié par iii. Plusieurs instances peuvent se connecter au même nœud.



Dans cet exemple :

- L'instance 1 se connecte au nœud de réseau 4 (NN4) de la couche iii. NN4se connecte au nœud de réseau 2 (NN2) de la couche ii et NN2 se connecte au nœud de réseau 1 (NN1) de la couche i, qui est le haut de la hiérarchie du réseau dans cet exemple. L'ensemble de nœuds de réseau comprend NN1NN2, etNN4, exprimés hiérarchiquement des couches supérieures à la couche inférieure.
- L'instance 2 se connecte également au nœud de réseau 4 (NN4). L'instance 1 et l'instance 2 partagent le même ensemble de nœuds réseau :NN1,NN2, etNN4.
- L'instance 3 se connecte au nœud de réseau 5 (NN5). NN5se connecte àNN2, et NN2 se connecte àNN1. Le nœud de réseau défini pour l'instance 3 est NN1NN2, etNN5.
- L'instance 4 se connecte au nœud de réseau 6 (NN6). Son ensemble de nœuds de réseau est NN1NN3, etNN6.

Si l'on considère la proximité des instances 1, 2 et 3, les instances 1 et 2 sont plus proches l'une de l'autre car elles se connectent au même nœud de réseau (NN4), tandis que l'instance 3 est plus éloignée car elle se connecte à un nœud de réseau différent (NN5).

Si l'on considère la proximité de toutes les instances de ce diagramme, les instances 1, 2 et 3 sont plus proches les unes des autres que de l'instance 4 car elles partagent NN2 leur ensemble de nœuds de réseau.

En règle générale, si le nœud de réseau connecté à deux instances est le même, ces instances sont physiquement proches l'une de l'autre, comme c'est le cas pour les instances 1 et 2. En outre, moins il y a de sauts entre les nœuds de réseau, plus les instances sont proches les unes des autres. Par exemple, les instances 1 et 3 effectuent moins de sauts vers un nœud de réseau commun (NN2) que vers le nœud de réseau (NN1) qu'elles ont en commun avec l'instance 4, et sont donc plus proches l'une de l'autre qu'elles ne le sont de l'instance 4.

Aucune instance ne s'exécute sous le nœud de réseau 7 (NN7) dans cet exemple, et la API sortie ne sera donc pas incluseNN7.

Comment interpréter le résultat

Vous pouvez obtenir les informations de topologie de l'instance à l'aide du DescribeInstanceTopologyAPI. La sortie fournit une vue hiérarchique de la topologie du réseau sous-jacent pour une instance.

L'exemple de sortie suivant correspond aux informations de topologie de réseau des quatre instances du schéma précédent. Les commentaires sont inclus dans l'exemple de sortie pour les besoins de cet exemple.

Il est important de noter les informations suivantes figurant dans la sortie :

- `NetworkNodes` décrit l'ensemble de nœuds de réseau d'une instance.
- Dans chaque ensemble de nœuds de réseau, les nœuds de réseau sont répertoriés par ordre hiérarchique de haut en bas.
- Le nœud de réseau connecté à l'instance est le dernier nœud de réseau de la liste (la couche inférieure).
- Pour déterminer quelles instances sont proches les unes des autres, recherchez d'abord les nœuds de réseau communs dans la couche inférieure. S'il n'existe aucun nœud de réseau commun dans la couche inférieure, recherchez des nœuds de réseau communs dans les couches supérieures.

Dans l'exemple de sortie suivant, `i-1111111111example` et `i-2222222222example` sont situées le plus près les uns des autres par rapport aux autres instances de cet exemple, car elles ont le nœud de réseau `nn-4444444444example` en commun dans la couche inférieure.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",  //Corresponds to instance 1
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 in layer i
                "nn-2222222222example",           //Corresponds to NN2 in layer ii
                "nn-4444444444example"            //Corresponds to NN4 in layer iii -
 bottom layer, connected to the instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",  //Corresponds to instance 2
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 - layer i
                "nn-2222222222example",           //Corresponds to NN2 - layer ii
                "nn-4444444444example"            //Corresponds to NN4 - layer iii -
 connected to instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",  //Corresponds to instance 3
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 - layer i
                "nn-2222222222example",           //Corresponds to NN2 - layer ii
                "nn-5555555555example"            //Corresponds to NN5 - layer iii -
 connected to instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
```

```
        {
            "InstanceId": "i-444444444example",  //Corresponds to instance 4
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",          //Corresponds to NN1 - layer i
                "nn-3333333333example",          //Corresponds to NN3 - layer ii
                "nn-6666666666example"           //Corresponds to NN6 - layer iii -
 connected to instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Conditions préalables à la topologie des EC2 instances Amazon

Avant de décrire la topologie de vos instances, assurez-vous que celles-ci répondent aux exigences suivantes.

Exigences relatives à la description de la topologie de vos instances

- Régions AWS
- Types d'instances
- État de l'instance
- IAMautorisation

Régions AWS

Pris en charge Régions AWS :

- USA Est (Virginie du Nord), USA Est (Ohio), USA Ouest (Californie du Nord), USA Ouest (Oregon)
- Asie-Pacifique (Séoul), Asie-Pacifique (Tokyo)
- Canada (Centre)
- Europe (Francfort), Europe (Irlande), Europe (Stockholm)

Types d'instances

Types d'instances pris en charge :

- `hpc6a.48xlarge` | `hpc6id.32xlarge` | `hpc7a.12xlarge` | `hpc7a.24xlarge` | `hpc7a.48xlarge` | `hpc7a.96xlarge` | `hpc7g.4xlarge` | `hpc7g.8xlarge` | `hpc7g.16xlarge`
- `p3dn.24xlarge` | `p4d.24xlarge` | `p4de.24xlarge` | `p5.48xlarge`
- `trn1.2xlarge` | `trn1.32xlarge` | `trn1n.32xlarge`

Pour consulter les types d'instance disponibles dans une région spécifique

Les types d'instance disponibles varient selon la région. Pour voir si un type d'instance est disponible dans une région, utilisez la commande describe-instance-types-offerings avec le paramètre `--region`. Incluez le paramètre `--filters` pour étendre les résultats à la famille d'instances ou au type d'instance qui vous intéresse et le paramètre `--query` pour étendre la sortie à la valeur de `InstanceType`.

```
aws ec2 describe-instance-type-offerings \
    --region us-east-2 \
    --filters 'Name=instance-type, Values=trn1*' \
    --query 'InstanceTypeOfferings[].InstanceType'
```

Sortie attendue

```
[
    "trn1.2xlarge",
    "trn1.32xlarge",
    "trn1n.32xlarge"
]
```

État de l'instance

Les instances doivent être dans l'état `running`. Vous ne pouvez pas obtenir d'informations sur la topologie des instances qui se trouvent dans un autre état.

IAMautorisation

Votre IAM identité (utilisateur, groupe d'utilisateurs ou rôle) nécessite les IAM autorisations suivantes :

- `ec2:DescribeInstanceTopology`

Exemples de topologie d'EC2instance Amazon

Vous pouvez utiliser la describe-instance-topologyCLIcommande pour décrire la topologie de vos EC2 instances.

Lorsque vous utilisez la commande `describe-instance-topology` sans paramètres ni filtres, la réponse inclut toutes vos instances qui correspondent aux types d'instances pris en charge pour cette commande dans la région spécifiée. Vous pouvez spécifier la région en incluant le paramètre `--region` ou en définissant une région par défaut. Pour plus d'informations sur la définition d'une région par défaut, consultez Sélectionnez une région pour vos EC2 ressources Amazon.

Vous pouvez inclure des paramètres pour renvoyer des instances qui correspondent aux noms d'instance IDs ou de groupe de placement spécifiés. Vous pouvez également inclure des filtres pour renvoyer des instances correspondant à un type d'instance ou à une famille d'instances spécifiques, ou des instances situées dans une zone de disponibilité ou une zone locale spécifiée. Vous pouvez inclure un seul paramètre ou filtre, ou une combinaison de paramètres et de filtres.

La sortie est paginée, avec un maximum de 20 instances par page par défaut. Vous pouvez spécifier jusqu'à 100 instances par page à l'aide du paramètre `--max-results`.

Pour plus d'informations, consultez la section describe-instance-topology dans la référence des commandes AWS CLI .

Autorisations nécessaires

L'autorisation suivante est requise pour décrire la topologie de l'instance :

- `ec2:DescribeInstanceTopology`

Exemples

- Exemple 1 : pas de paramètre ni de filtre
- Exemple 2 : filtre de type d'instance
  - Exemple 2a : filtre de correspondance exacte pour un type d'instance spécifié
  - Exemple 2b : filtre générique pour une famille d'instances
  - Exemple 2c : famille d'instances combinée et filtres de correspondance exacte

Exemple 1 : pas de paramètre ni de filtre

Pour décrire la topologie de toutes vos instances

Utilisez la describe-instance-topologyCLIcommande sans spécifier de paramètres ni de filtres.

```
aws ec2 describe-instance-topology --region us-west-2
```

La réponse renvoie uniquement les instances qui correspondent aux types d'instances pris en charge pour celaAPI. Les instances peuvent se trouver dans différentes zones de disponibilité, zones locales (`ZoneId`) et groupes de placement (`GroupName`). Si une instance ne figure pas dans un groupe de placement, le champ `GroupName` n'apparaît pas dans la sortie. Dans l'exemple de sortie suivant, une seule instance se trouve dans un groupe de placement.

Exemple de sortie

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "my-ml-cpg",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
```

```
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1212121212example",
                "nn-1211122211example",
                "nn-1311133311example"
            ],
            "ZoneId": "usw2-az4",
            "AvailabilityZone": "us-west-2d"
        },
        {
            "InstanceId": "i-444444444example",
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-5434334334example",
                "nn-1235301234example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Exemple 2 : filtre de type d'instance

Vous pouvez filtrer en fonction d'un type d'instance spécifié (correspondance exacte) ou en fonction d'une famille d'instances (à l'aide d'un caractère générique). Vous pouvez également combiner un filtre de type d'instance et un filtre de famille d'instances spécifiés.

Exemple 2a : filtre de correspondance exacte pour un type d'instance spécifié

Pour décrire la topologie d'instance de toutes vos instances correspondant à un type d'instance spécifié

Utilisez la describe-instance-topologyCLIcommande avec le `instance-type` filtre. Dans cet exemple, la sortie est filtrée pour les instances `trn1n.32xlarge`. La réponse renverra uniquement les instances correspondant au type d'instance spécifié.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters Name=instance-type,Values=trn1n.32xlarge
```

Exemple de sortie

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Exemple 2b : filtre générique pour une famille d'instances

Pour décrire la topologie d'instance de toutes vos instances correspondant à une famille d'instances

Utilisez la describe-instance-topologyCLIcommande avec le `instance-type` filtre. Dans cet exemple, la sortie est filtrée pour les instances `trn1*`. La réponse renverra uniquement les instances correspondant à la famille d'instances spécifiée.

```
aws ec2 describe-instance-topology \
```

```
    --region us-west-2 \
    --filters Name=instance-type,Values=trn1*
```

Exemple de sortie


```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1212121212example",
                "nn-1211122211example",
                "nn-1311133311example"
            ],
            "ZoneId": "usw2-az4",
            "AvailabilityZone": "us-west-2d"
        },
        {
            "InstanceId": "i-444444444example",
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-5434334334example",
                "nn-1235301234example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Exemple 2c : famille d'instances combinée et filtres de correspondance exacte

Pour décrire la topologie d'instance de toutes vos instances correspondant à une famille d'instances ou à un type d'instance spécifié

Utilisez la describe-instance-topologyCLIcommande avec le `instance-type` filtre. Dans cet exemple, la sortie est filtrée pour les instances `pd4d*` ou `trn1n.32xlarge`. La réponse renverra les instances correspondant à n'importe lequel des filtres spécifiés.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge"
```

Exemple de sortie

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-4343434343example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
```

```
}
```

Exemple 3 : filtre zone-id

Vous pouvez utiliser le filtre `zone-id` pour filtrer par zone de disponibilité ou zone locale. Vous pouvez également combiner le filtre de zone de disponibilité et le filtre de zone locale.

Exemple 3a : filtre de zone de disponibilité

Pour décrire la topologie d'instance de toutes vos instances correspondant à une zone de disponibilité spécifiée

Utilisez la describe-instance-topologyCLIcommande avec le `zone-id` filtre. Dans cet exemple, la sortie est filtrée à l'aide de l'ID de zone de disponibilité`use1-az1`. La réponse renverra uniquement les instances correspondant à la zone de disponibilité spécifiée.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-az1
```

Exemple de sortie

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Exemple 3b : filtre de zone locale

Pour décrire la topologie d'instance de toutes vos instances correspondant à une zone locale spécifiée

Utilisez la describe-instance-topologyCLIcommande avec le `zone-id` filtre. Dans cet exemple, la sortie est filtrée à l'aide de l'ID de zone local`use1-atl2-az1`. La réponse renverra uniquement les instances correspondant à la zone locale spécifiée.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-atl2-az1
```

Exemple de sortie

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Exemple 3c : combinaison des filtres de zone de disponibilité et de zone locale

Pour décrire la topologie d'instance de toutes vos instances correspondant à une zone de disponibilité ou une zone locale spécifiée

Utilisez la describe-instance-topologyCLIcommande avec le `zone-id` filtre. Dans cet exemple, la sortie est filtrée à l'aide de l'ID de zone de disponibilité `use1-az1` et de l'ID de zone local`use1-atl2-az1`. La réponse renverra les instances correspondant à n'importe lequel des filtres spécifiés.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-az1,use1-atl2-az1
```

Exemple de sortie


```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```


Exemple 4 : combinaison des filtres de type d'instance et zone-id

Vous pouvez combiner tous les filtres au sein d'une même commande.

Pour décrire la topologie d'instance de toutes vos instances correspondant à un type d'instance, une famille d'instances, une zone de disponibilité ou une zone locale spécifiés

Utilisez la describe-instance-topologyCLIcommande avec les `zone-id` filtres `instance-type` et. Dans cet exemple, la sortie est filtrée en fonction de la famille d'`p4d*`instances, du type d'`trn1n.32xlarge`instance, de l'ID de zone de `use1-az1` disponibilité et de l'ID de zone `use1-atl2-az1` locale. La réponse renverra les instances qui correspondent aux instances `p4d*` ou `trn1n.32xlarge` situées dans les zones `us-east-1a` ou `us-east-1-atl-2a`.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge" "Name=zone-
id,Values=use1-az1,use1-atl2-az1"
```

Exemple de sortie

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Exemple 5 : paramètre de nom du groupe de placement

Pour décrire la topologie de toutes vos instances dans un groupe de placement spécifié

Utilisez la describe-instance-topologyCLIcommande avec le `group-names` paramètre. Dans l'exemple suivant, les instances peuvent se trouver dans le groupe de placement `ML-group` ou `HPC-group`. La réponse renverra les instances qui se trouvent dans l'un des groupes de placement.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --group-names ML-group HPC-group
```

Exemple de sortie

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "GroupName": "HPC-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
```

```
}
```

Exemple 6 — Instance IDs

Pour décrire la topologie d'instances spécifiées

Utilisez la describe-instance-topologyCLIcommande avec le `--instance-ids` paramètre. La réponse renverra les instances qui correspondent à l'instance spécifiéeIDs.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --instance-ids i-1111111111example i-2222222222example
```

Exemple de sortie

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "GroupName": "HPC-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
```

```
    "NextToken": "SomeEncryptedToken"
}
```

Groupes de placement pour vos EC2 instances Amazon

Pour répondre aux besoins de votre charge de travail, vous pouvez lancer un groupe d'EC2instances interdépendantes dans un groupe de placement afin d'influencer leur placement.

Selon le type de charge de travail, vous pouvez créer un groupe de placement à l'aide de l'une des stratégies de placement suivantes :

- Cluster : regroupe des instances rapprochées à l'intérieur d'une Zone de disponibilité. Cette stratégie permet aux charges de travail d'atteindre les performances réseau à faible latence nécessaires aux node-to-node communications étroitement couplées, typiques des applications de calcul haute performance (). HPC
- Partition : répartit les instances entre les partitions logiques de façon à ce que des groupes d'instances d'une partition ne partagent pas le matériel sous-jacent avec des groupes d'instances d'autres partitions. Cette stratégie est généralement utilisée par les grandes charges de travail distribuées et répliquées telles que Hadoop, Cassandra, et Kafka.
- Répartition : place strictement un petit groupe d'instances sur un matériel sous-jacent distinct pour réduire les défaillances corrélées.

Les groupes de placement sont facultatifs. Si vous ne lancez pas vos instances dans un groupe de placementEC2, essayez de les placer de manière à ce que toutes les instances soient réparties sur le matériel sous-jacent afin de minimiser les défaillances corrélées.

Tarification

Il n'y a aucuns frais pour la création d'un groupe de placement.

Règles et limitations

Avant d'utiliser des groupes de placement, vous devez être conscient des règles suivantes :

- Une instance peut être placée dans un groupe de placement à la fois ; vous ne pouvez pas placer une instance dans plusieurs groupes de placement.
- Vous ne pouvez pas fusionner des groupes de placement.

- Les réservations de capacité à la demande et les instances réservées zonales vous permettent de réserver de la capacité pour des EC2 instances situées dans des zones de disponibilité. Lorsque vous lancez une instance, si les attributs de l'instance correspondent à ceux spécifiés par une réservation de capacité à la demande ou une instance réservée zonale, la capacité réservée est automatiquement utilisée par l'instance. Cela est également vrai si vous lancez l'instance dans un groupe de placement.
- Vous ne pouvez pas lancer d'hôtes dédiés dans des groupes de placement.
- Vous ne pouvez pas lancer une instance Spot configurée pour s'arrêter ou se mettre en veille prolongée en cas d'interruption dans un groupe de placement.

Table des matières

Stratégies de placement pour vos groupes de placement

Vous pouvez créer un groupe de placement pour vos EC2 instances à l'aide de l'une des stratégies de placement suivantes.

Stratégies de placement

Groupes de placement du cluster

Un groupe de placement du cluster est un regroupement logique d'instances dans une même zone de disponibilité. Les instances ne sont pas isolées dans un seul rack. Un groupe de placement de clusters peut couvrir des réseaux privés virtuels homologues (VPCs) d'une même région. Les instances d'un même groupe de placement de clusters bénéficient d'une limite de débit par flux plus

élevée pour le trafic TCP /IP et sont placées dans le même segment de bande passante à bissection élevée du réseau.

L'image ci-après illustre les instances placées dans un groupe de placement du cluster.

Les groupes de placement de cluster sont recommandés pour les applications qui bénéficient d'une latence réseau faible, d'un débit réseau élevé, ou des deux. Ils sont également recommandés lorsque la majorité du trafic réseau est échangé entre les instances du groupe. Pour fournir la latence la plus faible et les meilleures performances packet-per-second réseau à votre groupe de placement, choisissez un type d'instance qui prend en charge la mise en réseau améliorée. Pour plus d'informations, consultez Gestion de réseau améliorée.

Nous vous recommandons de lancer vos instances de la façon suivante :

- Utilisez une seule demande de lancement pour lancer le nombre d'instances dont vous avez besoin dans le groupe de placement.
- Utilisez le même type d'instance pour toutes les instances du groupe de placement.

Si vous essayez d'ajouter ultérieurement des instances supplémentaires au groupe de placement, ou si vous essayez de lancer plusieurs types d'instance dans le groupe de placement, vous augmentez les risques d'obtenir une erreur de capacité insuffisante.

Si vous arrêtez une instance dans un groupe de placement, puis que vous la relancez, elle s'exécute encore au sein de celui-ci. Par contre, le démarrage échoue si la capacité est insuffisante pour l'instance.

Si vous recevez une erreur de capacité lorsque vous lancez une instance dans un groupe de placement dont des instances sont déjà en cours d'exécution, arrêtez et démarrez toutes les

instances dans le groupe de placement, puis réessayez le lancement. Le redémarrage des instances peut entraîner leur migration vers un matériel qui dispose d'une capacité suffisante pour toutes les instances demandées.

Règles et limitations

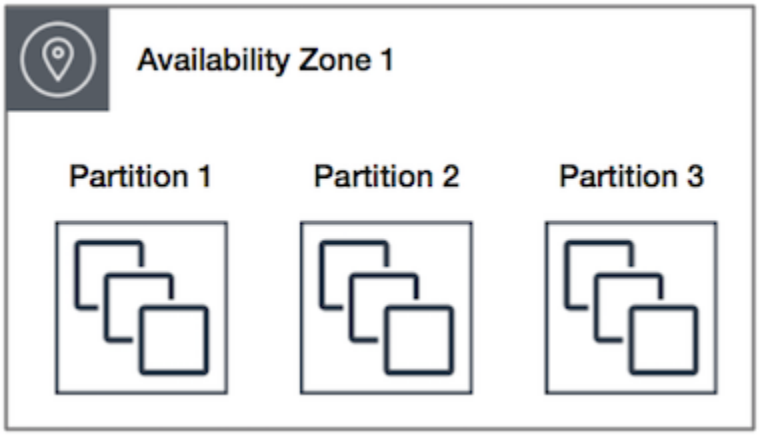
Les règles suivantes s'appliquent aux groupes de placement du cluster :

- Seuls les types d'instances suivants sont pris en charge :
  - Instances de la génération actuelle, à l'exception des instances de performance burstable (par exemple, T2), des instances Mac1 et des instances M7i-Flex.
  - Les instances de génération précédente suivantes : A1, C3, C4, I2, M4, R3 et R4.
- Un groupe de placement du cluster ne peut pas s'étendre sur plusieurs zones de disponibilité.
- La vitesse de débit réseau maximale du trafic entre deux instances au sein d'un groupe de placement du cluster est limitée par la plus lente des deux instances. Pour les applications très exigeantes en débit, choisissez un type d'instance avec une connectivité réseau qui correspond à vos besoins.
- Pour les instances pour lesquelles la mise en réseau améliorée est active, les règles suivantes s'appliquent :
  - Les instances se trouvant dans un groupe de placement du cluster peuvent utiliser jusqu'à 10 Gbit/s pour le trafic à flux unique. Les instances qui ne se trouvent pas dans un groupe de placement du cluster peuvent utiliser jusqu'à 5 Gbit/s pour le trafic à flux unique.
  - Le trafic à destination et en provenance de compartiments Amazon S3 au sein d'une même région via l'espace d'adresse IP public ou via un VPC point de terminaison peut utiliser toute la bande passante agrégée d'instance disponible.
- Vous pouvez lancer plusieurs types d'instance dans un groupe de placement du cluster. Toutefois, cela réduit la probabilité de disponibilité de la capacité requise pour que votre lancement réussisse. Nous vous recommandons d'utiliser le même type d'instance pour toutes les instances d'un groupe de placement du cluster.
- Nous vous recommandons de réserver de la capacité de manière explicite dans le groupe de placement du cluster en créant une réservation de capacité à la demande dans le groupe de placement du cluster. Notez que vous ne pouvez pas réserver de capacité à l'aide d'instances réservées zonales, car elles ne peuvent pas réserver de capacité explicitement dans un groupe de placement.
- Le trafic réseau vers Internet et via une AWS Direct Connect connexion aux ressources locales est limité à 5 Gbit/s pour les groupes de placement de clusters.

Groupes de placement par partition

Les groupes de placement de partitions permettent de réduire la probabilité de défaillances de matériel corrélé pour votre application. Lorsque vous utilisez des groupes de placement de partitions, Amazon EC2 divise chaque groupe en segments logiques appelés partitions. Amazon EC2 veille à ce que chaque partition d'un groupe de placement possède son propre ensemble de racks. Chaque rack est doté de son propre réseau et de sa propre source d'alimentation. Aucune partition dans un même groupe de placement ne dispose du même portant, ce qui vous permet ainsi d'isoler l'impact d'échecs matériels dans votre application.

L'image suivante est une représentation visuelle simplifiée d'un groupe de placement de partitions dans une seule Zone de disponibilité. Elle représente des instances placées dans un groupe de placement par partition composé de trois partitions—Partition 1, Partition 2 et Partition 3. Chaque partition comprend plusieurs instances. Les instances d'une partition ne partagent pas de portants avec les instances des autres partitions, ce qui vous permet de limiter l'impact des pannes matérielles à une seule partition.



Les groupes de placement de partitions peuvent être utilisés pour déployer de grandes charges de travail distribuées et répliquées, telles que,HDFS, et CassandraHBase, sur des racks distincts. Lorsque vous lancez des instances dans un groupe de placement de partitions, Amazon EC2 essaie de les répartir uniformément sur le nombre de partitions que vous spécifiez. Vous avez également la possibilité de lancer des instances d'une partition donnée afin de mieux contrôler l'emplacement des instances.

Un groupe de placement par partition peut disposer de partitions dans plusieurs Zones de disponibilité de la même région. Un groupe de placement par partition peut contenir jusqu'à sept partitions par zone de disponibilité. Seules les restrictions de votre compte limitent le nombre d'instances pouvant être lancées dans un groupe de placement par partition.

De plus, les groupes de placement par partition vous permettent de voir le détail des partitions — types d'instance présents dans telle ou telle partition. Vous pouvez partager ces informations avec des applications sensibles à la topologie, telles que HDFSHBase, et Cassandra. Ces applications utilisent ces informations pour prendre des décisions informées sur la réplication des données dans le but d'accroître la disponibilité et la durabilité de ces dernières.

Si vous démarrez ou lancez une instance dans un groupe de placement par partition et que le matériel nécessaire au traitement de la demande est insuffisant, la demande échoue. Amazon EC2 met à disposition un matériel plus distinct au fil du temps, afin que vous puissiez réessayer votre demande ultérieurement.

Règles et limitations

Les règles suivantes s'appliquent aux groupes de placement par partition :

- Un groupe de placement par partition prend en charge jusqu'à sept partitions par zone de disponibilité. Seules les restrictions de votre compte limitent le nombre d'instances pouvant être lancées dans un groupe de placement par partition.
- Lorsque des instances sont lancées dans un groupe de placement de partitions, Amazon EC2 essaie de les répartir uniformément sur toutes les partitions. Amazon EC2 ne garantit pas une distribution uniforme des instances sur toutes les partitions.
- Un groupe de placement par partition avec des instances dédiées peut comprendre deux partitions au maximum.
- Les réservations de capacité ne réservent pas de capacité dans un groupe de placement par partition.

Groupes de placement étendu

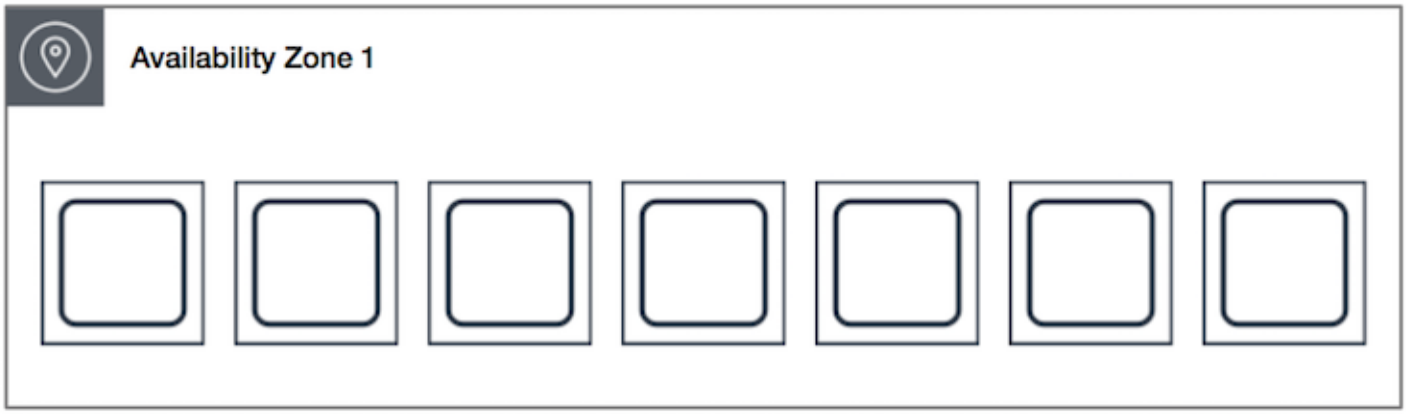
Un groupe de placement par répartition est un groupe d'instances qui sont chacune placées sur du matériel distinct.

Les groupes de placement par répartition sont recommandés pour les applications ayant un petit nombre d'instances critiques, qui doivent être séparées les unes des autres. Le lancement d'instances dans un groupe de placement par répartition réduit le risque de défaillances simultanées, qui peuvent se produire lorsque les instances partagent le même matériel. Les groupes de placement par répartition fournissent un accès à du matériel distinct et sont par conséquent adaptés à l'association de différents types d'instance et au lancement d'instances au fil du temps.

Si vous démarrez ou lancez une instance dans un groupe de placement par répartition et que le matériel nécessaire au traitement de la demande est insuffisant, la demande échoue. Amazon EC2 met à disposition un matériel plus distinct au fil du temps, afin que vous puissiez réessayer votre demande ultérieurement. Les groupes de placement peuvent répartir des instances sur des racks ou des hôtes. Les groupes de placement répartis au niveau du rack peuvent être utilisés dans AWS les régions et au-delà AWS Outposts. Les groupes de placement de spread au niveau de l'hôte ne peuvent être utilisés AWS Outposts qu'avec.

Groupes de placement répartis au niveau du rack

L'image ci-après représente sept instances au sein d'une seule zone de disponibilité qui sont placées dans un groupe de placement par répartition. Les sept instances sont placées sur sept racks différents, chaque rack ayant son propre réseau et sa propre source d'alimentation.



Un groupe de placement de spread au niveau du rack peut couvrir plusieurs zones de disponibilité dans la même région. Dans une région, un groupe de placement de spread au niveau du rack peut avoir un maximum de sept instances actives par zone de disponibilité et par groupe. Avec Outposts, un groupe de placement de spread au niveau du rack peut contenir autant d'instances que vous avez de racks dans votre déploiement d'Outposts.

Groupes de placement par répartition au niveau des hôtes

Les groupes de placement de spread au niveau de l'hôte ne sont disponibles qu'avec AWS Outposts. Un groupe de placement au niveau du spread d'hôtes peut contenir autant d'instances que vous avez d'hôtes dans votre déploiement Outpost. Pour de plus amples informations, veuillez consulter the section called "Groupes de placement sur AWS Outposts".

Règles et limitations

Les règles suivantes s'appliquent aux groupes de placement par répartition :

- Un groupe de placement par répartition sur de racks prend en charge un maximum de sept instances en cours d'exécution par zone de disponibilité. Par exemple, dans une région comportant trois zones de disponibilité, vous pouvez exécuter un total de 21 instances dans le groupe, avec sept instances dans chaque zone de disponibilité. Si vous essayez de lancer une huitième instance dans la même zone de disponibilité et dans le même groupe de placement par répartition, le lancement échoue. Si vous avez besoin de plus de sept instances dans une zone de disponibilité, nous vous recommandons d'utiliser plusieurs groupes de placement par répartition. L'utilisation de plusieurs groupes de placement par répartition ne garantit pas la répartition des instances entre les groupes, mais cela permet de garantir la répartition pour chaque groupe, limitant ainsi l'impact de certains types d'incidents.
- Les groupes de placement par répartition ne sont pas pris en charge pour les instances dédiées.
- Les groupes de placement de spread au niveau de l'hôte ne sont pris en charge que pour les groupes de placement activés AWS Outposts. Un groupe de placement de spread au niveau de l'hôte peut contenir autant d'instances que vous avez d'hôtes dans votre déploiement Outpost.
- Dans une région, un groupe de placement de spread au niveau du rack peut avoir un maximum de sept instances actives par zone de disponibilité et par groupe. Ainsi AWS Outposts, un groupe de placement de spread au niveau du rack peut contenir autant d'instances que vous avez de racks dans votre déploiement Outpost.
- Les réservations de capacité ne réservent pas de capacité dans un groupe de placement par répartition.

Créez un groupe de placement pour vos EC2 instances

Vous pouvez utiliser un groupe de placement pour contrôler le placement des instances les unes par rapport aux autres. Après avoir créé un groupe de placement, vous pouvez lancer des instances dans le groupe de placement.

Limitation

Vous pouvez créer un maximum de 500 groupes de placement par région.

Console

Pour créer un groupe de placement

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Groupes de placement.

3. Choisissez Créer un groupe de placement.
4. Spécifiez le nom du groupe.
5. Choisissez la stratégie de placement pour le groupe : Cluster, Spread ou Partition.

   Si vous avez choisi Spread, vous devez choisir le niveau de spread : Rack ou Host.

   Si vous avez choisi Partition, vous devez saisir le nombre de partitions du groupe.
6. (Facultatif) Pour ajouter une balise, choisissez Ajouter une nouvelle balise, puis entrez une clé et une valeur.
7. Choisissez Créer un groupe.

AWS CLI

Utilisez la create-placement-groupcommande.

Pour créer un groupe de placement de clusters

L'exemple suivant crée un groupe de placement qui utilise la stratégie de `cluster` placement et applique une balise avec une clé `purpose` et une valeur de`production`.

```
aws ec2 create-placement-group \
    --group-name my-cluster \
    --strategy cluster \
    --tag-specifications 'ResourceType=placement-
group,Tags={Key=purpose,Value=production}'
```

Pour créer un groupe de placement de partitions

L'exemple suivant crée un groupe de placement qui utilise la stratégie de `partition` placement et spécifie les cinq partitions à l'aide du `--partition-count` paramètre.

```
aws ec2 create-placement-group \
    --group-name HDFS-Group-A \
    --strategy partition \
    --partition-count 5
```

PowerShell

Pour créer un groupe de placement

La New-EC2PlacementGroupcommande suivante crée un groupe de placement de clusters.

```
New-EC2PlacementGroup -GroupName my-placement-group -Strategy cluster
```

Modifier l'emplacement d'une EC2 instance

Vous pouvez modifier le groupe de placement d'une instance comme suit :

- Ajouter une instance à un groupe de placement
- Déplacement d'une instance d'un groupe de placement vers un autre
- Suppression d'une instance d'un groupe de placement

Avant de pouvoir modifier le groupe de placement d'une instance, celle-ci doit être dans l'`stopped`état actuel.

Console

Pour modifier le placement de l'instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance.
4. Choisissez Actions, Paramètres de l'instance, puis Modifier le placement d'instance.
5. Pour le groupe de placement, effectuez l'une des opérations suivantes :
   - Pour ajouter l'instance à un groupe de placement, choisissez le groupe de placement.
   - Pour déplacer l'instance d'un groupe de placement à un autre, choisissez le groupe de placement.
   - Pour supprimer l'instance du groupe de placement, choisissez None.
6. Choisissez Save (Enregistrer).

AWS CLI

Déplacement d'une instance vers un groupe de placement

La modify-instance-placementcommande suivante déplace l'instance spécifiée vers le groupe de placement spécifié.

```
aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name MySpreadGroup
```

Suppression d'une instance d'un groupe de placement

La modify-instance-placementcommande suivante spécifie une chaîne vide pour le nom du groupe de placement, ce qui supprime l'instance de son groupe de placement actuel.

```
aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name ""
```

PowerShell

Déplacement d'une instance vers un groupe de placement

Utilisez la Edit-EC2InstancePlacementcommande avec le nom du groupe de placement.

Suppression d'une instance d'un groupe de placement

Utilisez la Edit-EC2InstancePlacementcommande avec une chaîne vide pour le nom du groupe de placement.

Supprimer un groupe de placement

Si vous avez besoin de supprimer un groupe de placement ou si vous n'en avez plus besoin, vous pouvez le supprimer. Vous pouvez supprimer un groupe de placement en employant l'une des méthodes suivantes.

Prérequis

Pour pouvoir être supprimé, un groupe de placement ne doit pas contenir d'instances. Vous pouvez mettre fin aux instances, les déplacer vers un autre groupe de placement ou les supprimer du groupe de placement.

Console

Suppression d'un groupe de placement

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

2. Dans le panneau de navigation, choisissez Groupes de placement.
3. Sélectionnez le groupe de placement et choisissez Actions, Supprimer.
4. Lorsque vous êtes invité à confirmer, entrez **Delete**, puis choisissez Delete (Supprimer).

AWS CLI

Suppression d'un groupe de placement

La delete-placement-groupcommande suivante supprime le groupe de placement spécifié.

```
aws ec2 delete-placement-group --group-name my-cluster
```

PowerShell

Suppression d'un groupe de placement

La Remove-EC2PlacementGroupcommande suivante supprime le groupe de placement spécifié.

```
Remove-EC2PlacementGroup -GroupName my-cluster
```

Groupes de placement partagés

Le partage de groupes de placement vous permet d'influencer le placement d'instances interdépendantes détenues par des entités distinctes Comptes AWS. Un propriétaire peut partager un groupe de placement entre plusieurs personnes Comptes AWS ou au sein de son organisation. Un participant peut lancer des instances dans un groupe de placement partagé avec son compte.

Le propriétaire d'un groupe de placement peut partager un groupe de placement avec :

- AWS Comptes spécifiques à l'intérieur ou à l'extérieur de son organisation
- Une unité d'organisation dans son organisation
- L'ensemble de son organisation

Vous pouvez utiliser le VPC peering pour connecter des instances détenues par des AWS comptes distincts et bénéficier de tous les avantages de latence offerts par les groupes de placement de clusters partagés.

Table des matières

Règles et limitations

Les règles et restrictions suivantes s'appliquent lorsque vous partagez un groupe de placement ou lorsqu'un groupe de placement est partagé avec vous.

- Pour partager un groupe de placement, vous devez en être le propriétaire dans votre AWS compte. Vous ne pouvez pas partager un groupe de placement qui a été partagé avec vous.
- Lorsque vous partagez un groupe de placement de partitions ou un groupe de placement étendu, les limites des groupes de placement ne changent pas. Un groupe de placement de partitions prend en charge un maximum de sept partitions par zone de disponibilité, tandis qu'un groupe de placement étendu prend en charge un maximum de sept instances en cours d'exécution par zone de disponibilité.
- Pour partager un groupe de placement avec votre organisation ou une unité organisationnelle de votre organisation, vous devez activer le partage avec AWS Organizations. Pour plus d'informations, consultez Partage de vos ressources AWS.
- Lorsque vous utilisez le AWS Management Console pour lancer une instance, vous pouvez sélectionner tous les groupes de placement qui ont été partagés avec vous. Lorsque vous utilisez le AWS CLI pour lancer une instance, vous devez spécifier un groupe de placement partagé par ID et non par nom. Vous ne pouvez utiliser le nom d'un groupe de placement que si vous êtes le propriétaire du groupe de placement partagé.
- Vous êtes responsable de la gestion des instances que vous possédez dans un groupe de placement partagé.
- Vous ne pouvez pas consulter ou modifier les instances et les réservations de capacité associées à un groupe de placement partagé mais dont vous n'êtes pas le propriétaire.
- Le nom de ressource Amazon (ARN) d'un groupe de placement contient l'ID du compte propriétaire du groupe de placement. Vous pouvez utiliser la partie identifiant de compte d'un groupe de placement ARN pour identifier le propriétaire d'un groupe de placement partagé avec vous.

Autorisations nécessaires

Pour partager un groupe de placement, les utilisateurs doivent disposer des autorisations nécessaires pour effectuer les actions suivantes :

- `ec2:PutResourcePolicy`
- `ec2:DeleteResourcePolicy`

Partage sur plusieurs zones de disponibilité

Pour garantir que les ressources sont réparties entre les zones de disponibilité d'une région, nous mappons indépendamment les zones de disponibilité aux noms de chaque compte. Cela peut entraîner des différences de nom de zone de disponibilité entre les comptes. Par exemple, il est possible que la zone `us-east-1a` de disponibilité de votre AWS compte ne soit pas la même que celle `us-east-1a` d'un autre AWS compte.

Pour spécifier l'emplacement de vos hôtes dédiés par rapport à vos comptes, vous devez utiliser l'ID de zone de disponibilité (AZ ID). L'ID de zone de disponibilité est un identifiant unique et cohérent pour une zone de disponibilité entre tous les comptes AWS . Par exemple, `use1-az1` est un ID de zone de disponibilité pour la région `us-east-1`, qui correspond au même emplacement dans chaque compte AWS . Pour de plus amples informations, veuillez consulter the section called "AZ IDs".

Partage de groupes de placement

Pour partager un groupe de placement, vous devez l'ajouter à un partage de ressources. Un partage de ressources est une AWS RAM ressource qui vous permet de partager vos ressources entre différents AWS comptes. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées.

Si vous faites partie d'une organisation et que le AWS Organizations partage au sein de votre organisation est activé, les clients de votre organisation ont accès au groupe de placement partagé.

Si le groupe de placement est partagé avec un AWS compte extérieur à votre organisation, le propriétaire du AWS compte recevra une invitation à rejoindre le partage des ressources. Ils peuvent accéder au groupe de placement partagé après avoir accepté l'invitation.

Vous pouvez partager un groupe de placement entre plusieurs AWS comptes à l'aide de AWS Resource Access Manager. Pour plus d'informations, consultez la section Création d'un partage de ressources dans le guide de AWS RAM l'utilisateur.

Annonce du partage du groupe de placement

Le propriétaire du groupe de placement peut annuler le partage d'un groupe de placement partagé à tout moment. Lorsque vous annulez le partage d'un groupe de placement partagé, les modifications suivantes se produisent :

- Les AWS comptes avec lesquels un groupe de placement a été partagé ne sont plus en mesure de lancer des instances ou de réserver de la capacité.
- Toutes les instances exécutées dans un groupe de placement partagé sont dissociées du groupe de placement, mais elles continuent de s'exécuter dans votre AWS compte.
- Toutes les réservations de capacité dans un groupe de placement partagé sont dissociées du groupe de placement, mais vous pouvez toujours y accéder dans votre AWS compte.

Pour plus d'informations, consultez la section Suppression d'un partage de ressources dans le guide de AWS RAM l'utilisateur.

Groupes de placement sur AWS Outposts

AWS Outposts est un service entièrement géré qui étend AWS l'infrastructureAPIs, les services et les outils aux locaux du client. En fournissant un accès local à l'infrastructure AWS gérée, il AWS Outposts permet aux clients de créer et d'exécuter des applications sur site en utilisant les mêmes interfaces de programmation que dans AWS les régions, tout en utilisant les ressources de calcul et de stockage locales pour réduire la latence et les besoins de traitement des données locaux.

Un avant-poste est un pool de capacités de AWS calcul et de stockage déployé sur le site d'un client. AWS exploite, surveille et gère cette capacité dans le cadre d'une AWS région.

Vous pouvez créer des groupes de placement sur les Outposts que vous avez créés dans votre compte. Cela vous permet de répartir les instances sur le matériel sous-jacent d'un Outpost sur votre site. Vous créez et utilisez les groupes de placement sur les Outposts de la même manière que vous créez et utilisez les groupes de placement dans les zones de disponibilité ordinaires. Lorsque vous créez un groupe de placement avec une stratégie de répartition sur un Outpost, vous pouvez choisir que le groupe de placement répartisse les instances sur des hôtes ou des racks. La répartition des

instances entre les hôtes vous permet d'utiliser une stratégie de répartition avec un Outpost à rack unique.

Considérations

- Un groupe de placement de spread au niveau du rack peut contenir autant d'instances que vous avez de racks dans votre déploiement Outpost.
- Un groupe de placement de spread au niveau de l'hôte peut contenir autant d'instances que vous avez d'hôtes dans votre déploiement Outpost.

Prérequis

Vous devez avoir un outpost installé sur votre site. Pour plus d'informations, consultez Créer un outpost et commander une capacité outpost dans le Guide de l'utilisateur AWS Outposts .

Pour utiliser un groupe de placement sur un Outpost

1. Créez un sous-réseau sur l'outpost. Pour plus d'informations, consultez Créer un sous-réseau dans le Guide de l'utilisateur AWS Outposts .
2. Créez un groupe de placement dans la région associée de l'Outpost. Si vous créez un groupe de placement avec une stratégie de spread, vous pouvez choisir un spread au niveau de l'hôte ou du rack pour déterminer comment le groupe répartira les instances sur le matériel sous-jacent de votre Outpost. Pour de plus amples informations, veuillez consulter the section called "Créer un groupe de placement.".
3. Lancez une instance dans le groupe de placement. Pour Subnet (Sous-réseau), choisissez le sous-réseau que vous avez créé à l'étape 1. Pour Placement group name (Nom du groupe de placement), sélectionnez le groupe de placement que vous avez créé à l'étape 2. Pour plus d'informations, consultez la section Lancer une instance sur votre Outpost du Guide de l'utilisateur AWS Outposts .

Unité de transmission maximale du réseau (MTU) pour votre EC2 instance

L'unité de transmission maximale (MTU) d'une connexion réseau est la taille, en octets, du plus grand paquet autorisé pouvant être transmis sur la connexion. Plus une connexion est MTU importante, plus le volume de données pouvant être transmises dans un seul paquet est important. Les trames

Ethernet se composent du paquet, ou des données réelles que vous envoyez, et des informations de surcharge du réseau qui l'entourent.

Les trames Ethernet peuvent avoir différents formats, le plus courant étant le format de trame standard Ethernet v2. Il prend en charge 1500MTU, soit la plus grande taille de paquet Ethernet prise en charge sur la majeure partie d'Internet. Le maximum pris en charge MTU pour une instance dépend de son type d'instance.

Les règles suivantes s'appliquent aux instances qui se trouvent dans des zones Wavelength :

- Le trafic qui passe d'une instance à une autre au VPC sein d'une même zone de Wavelength a un MTU de 1300.
- Le trafic qui passe d'une instance à une autre utilisant l'IP du transporteur dans une zone de Wavelength a un MTU de 1500.
- Le trafic qui passe d'une instance à l'autre entre une zone Wavelength et la région qui utilise une adresse IP publique a un MTU score de 1500.
- Le trafic qui passe d'une instance à l'autre entre une zone Wavelength et la région qui utilise une adresse IP privée a un MTU chiffre de 1300.

Les règles suivantes s'appliquent aux instances qui se trouvent dans Outposts :

- Le trafic qui passe d'une instance d'Outposts à une instance de la Région est MTU de 1 300.

Table des matières

Cadres Jumbo (9001MTU)

Les trames jumbo permettent d'utiliser plus de 1 500 octets de données en augmentant la charge utile par paquet, et donc en augmentant le pourcentage de paquet qui ne constitue pas des frais supplémentaires. Moins de paquets sont nécessaires pour envoyer le même volume de données utilisables. Toutefois, le trafic est limité à un maximum MTU de 1 500 dans les cas suivants :

- Trafic sur une passerelle Internet
- Trafic via une connexion de VPC peering interrégionale
- Trafic sur VPN les connexions
- Trafic en dehors d'une AWS région donnée

Si la taille des paquets dépasse 1 500 octets, ceux-ci sont fragmentés ou abandonnés si l'indicateur `Don't Fragment` est défini dans l'en-tête IP.

Les cadres Jumbo doivent être utilisés avec prudence pour le trafic lié à Internet ou pour tout trafic sortant d'un. VPC Les paquets sont fragmentés par des systèmes intermédiaires, ce qui ralentit le trafic. Pour utiliser des cadres géants à l'intérieur VPC d'un trafic plutôt que de ralentir à destination de l'extérieurVPC, vous pouvez configurer la MTU taille par itinéraire ou utiliser plusieurs interfaces réseau élastiques de différentes MTU tailles et de différents itinéraires.

Pour les instances situées dans un même groupe de placement du cluster, les trames jumbo permettent d'atteindre le débit réseau maximum possible et elles sont recommandées dans ce cas. Pour de plus amples informations, veuillez consulter Groupes de placement pour vos EC2 instances Amazon.

Vous pouvez utiliser des trames jumbo pour le trafic entre votre réseau VPCs et votre réseau local. AWS Direct Connect Pour plus d'informations et pour savoir comment vérifier la fonctionnalité Jumbo Frame, voir Configuration du réseau MTU dans le guide de l'AWS Direct Connect utilisateur.

Tous les types d'EC2instances Amazon prennent en charge 1 500 MTU et tous les types d'instances de la génération actuelle prennent en charge les trames jumbo. Les types d'instances de la génération précédente suivants prennent en charge les trames jumbo : A1, C3, I2, M3 et R3.

Pour plus d'informations sur les MTU tailles prises en charge :

- Pour les NAT passerelles, consultez les principes de base des NAT passerelles dans le guide de VPC l'utilisateur Amazon.
- Pour les passerelles de transit, consultez le guide MTUde l'utilisateur d'Amazon VPC Transit Gateways.
- Pour les zones locales, consultez la section Considérations dans le Guide de l'utilisateur des zones locales AWS .

MTUDécouverte du chemin

Path MTU Discovery (PMTUD) est utilisé pour déterminer le chemin MTU entre deux appareils. Le chemin MTU est la taille de paquet maximale prise en charge sur le chemin entre l'hôte d'origine et l'hôte de réception. En cas de différence de MTU taille du réseau entre deux hôtes, PMTUD permet à l'hôte récepteur de répondre à l'hôte d'origine par un ICMP message. Ce ICMP message indique à l'hôte d'origine d'utiliser la MTU taille la plus petite sur le chemin réseau et de renvoyer la demande. Sans cette négociation, un rejet de paquet peut se produire, car la demande est trop volumineuse pour l'hôte de réception.

En IPv4 effet, lorsqu'un hôte envoie un paquet plus volumineux que celui MTU de l'hôte récepteur ou supérieur à celui MTU d'un périphérique le long du chemin, l'hôte ou le périphérique récepteur abandonne le paquet, puis renvoie le ICMP message suivant : `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (Type 3, Code 4). Cela indique à l'hôte émetteur de diviser la charge utile en plusieurs paquets plus petits, puis de les retransmettre.

Le IPv6 protocole ne prend pas en charge la fragmentation du réseau. Lorsqu'un hôte envoie un paquet plus volumineux que celui MTU de l'hôte récepteur ou supérieur à celui MTU d'un périphérique le long du chemin, l'hôte ou le périphérique récepteur abandonne le paquet, puis renvoie le ICMP message suivant : `ICMPv6 Packet Too Big (PTB)` (Type 2). Cela indique à l'hôte émetteur de diviser la charge utile en plusieurs paquets plus petits, puis de les retransmettre.

Les connexions établies via certains composants, tels que les NAT passerelles et les équilibreurs de charge, sont automatiquement suivies. Cela signifie que le suivi des groupes de sécurité est automatiquement activé pour vos tentatives de connexion sortante. Si les connexions sont automatiquement suivies ou si les règles de votre groupe de sécurité autorisent le ICMP trafic entrant, vous pouvez recevoir des PMTUD réponses.

Notez que le ICMP trafic peut être bloqué même s'il est autorisé au niveau du groupe de sécurité, par exemple si vous avez une entrée de liste de contrôle d'accès réseau qui refuse le ICMP trafic vers le sous-réseau.

> **Important**
>
> Path MTU Discovery ne garantit pas que les trames jumbo ne seront pas supprimées par certains routeurs. Une passerelle Internet intégrée à votre ordinateur VPC ne transmettra que des paquets de 1 500 octets maximum. 1500 MTU paquets sont recommandés pour le trafic Internet.

Pour les MTU règles relatives aux NAT passerelles, consultez la section Unité de transmission maximale (MTU) dans le guide de l'VPCutilisateur Amazon. Pour les MTU règles relatives aux passerelles de transit, voir Unité de transmission maximale (MTU) dans le guide de l'utilisateur de AWS Transit Gateway.

Définissez le MTU pour vos EC2 instances Amazon

L'unité de transmission maximale (MTU) d'une connexion réseau est la taille, en octets, du plus grand paquet autorisé pouvant être transmis sur la connexion. Toutes les EC2 instances Amazon prennent en charge les cadres standard (1500MTU) et tous les types d'instances de la génération actuelle prennent en charge les cadres jumbo (9001MTU).

Vous pouvez consulter MTU les EC2 instances Amazon, voir le chemin MTU entre votre instance et un autre hôte, et configurer vos instances pour utiliser des cadres standard ou jumbo.

Tâches

- Vérifiez le chemin MTU entre deux hôtes
- Vérifiez le MTU pour votre instance
- Définissez le MTU pour votre instance

Vérifiez le chemin MTU entre deux hôtes

Vous pouvez vérifier le chemin MTU entre votre EC2 instance et un autre hôte. Vous pouvez spécifier un DNS nom ou une adresse IP comme destination. Si la destination est une autre EC2 instance, vérifiez que son groupe de sécurité autorise le UDP trafic entrant.

La procédure que vous utilisez dépend du système d'exploitation de l'instance.

Instances Linux

Exécutez la tracepath commande sur votre instance pour vérifier le chemin MTU entre votre EC2 instance et la destination spécifiée. Cette commande fait partie du `iputils` package, qui est disponible par défaut dans de nombreuses distributions Linux.

Cet exemple vérifie le chemin MTU entre l'EC2instance et`amazon.com`.

```
[ec2-user ~]$ tracepath amazon.com
```

Dans cet exemple de sortie, le chemin MTU est 1500.

```
 1?: [LOCALHOST]     pmtu 9001
 1:  ip-172-31-16-1.us-west-1.compute.internal (172.31.16.1)   0.187ms pmtu 1500
 1:  no reply
 2:  no reply
 3:  no reply
 4:  100.64.16.241 (100.64.16.241)                             0.574ms
 5:  72.21.222.221 (72.21.222.221)                            84.447ms asymm 21
 6:  205.251.229.97 (205.251.229.97)                          79.970ms asymm 19
 7:  72.21.222.194 (72.21.222.194)                            96.546ms asymm 16
 8:  72.21.222.239 (72.21.222.239)                            79.244ms asymm 15
 9:  205.251.225.73 (205.251.225.73)                          91.867ms asymm 16
...
31:  no reply
     Too many hops: pmtu 1500
     Resume: pmtu 1500
```

instances Windows

Pour vérifier le chemin à MTU l'aide de mturoute

1. mturoute.exeTéléchargez-le sur votre EC2 instance depuis http://www.elifulkerson.com/projects/mturoute.php.
2. Ouvrez une fenêtre d'invite de commande et modifiez l'annuaire dans lequel vous avez téléchargé mturoute.exe.
3. Utilisez la commande suivante pour vérifier le chemin MTU entre votre EC2 instance et la destination spécifiée. Cet exemple vérifie le chemin MTU entre l'EC2instance et`www.elifulkerson.com`.

   ```
   .\mturoute.exe www.elifulkerson.com
   ```

   Dans cet exemple de sortie, le chemin MTU est 1500.

   ```
   * ICMP Fragmentation is not permitted. *
   * Speed optimization is enabled. *
   * Maximum payload is 10000 bytes. *
   + ICMP payload of 1472 bytes succeeded.
   - ICMP payload of 1473 bytes is too big.
   Path MTU: 1500 bytes.
   ```

Vérifiez le MTU pour votre instance

Vous pouvez vérifier la MTU valeur de votre instance. Certaines instances sont configurées de façon à utiliser les trames jumbo, tandis que d'autres sont configurées de façon à utiliser les tailles de trame standard.

La procédure que vous utilisez dépend du système d'exploitation de l'instance.

Instances Linux

Pour vérifier le MTU paramètre sur une instance Linux

Exécutez la ip commande suivante sur votre EC2 instance. Si ce n'est pas le cas de l'interface réseau principale`eth0`, `eth0` remplacez-la par votre interface réseau.

```
[ec2-user ~]$ ip link show eth0
```

Dans cet exemple de sortie, *`mtu 9001`* indique que l'instance utilise des cadres jumbo.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP mode
 DEFAULT group default qlen 1000
    link/ether 02:90:c0:b7:9e:d1 brd ff:ff:ff:ff:ff:ff
```

instances Windows

La procédure que vous utilisez dépend du pilote de votre instance.

ENA driver

Version 2.1.0 et versions ultérieures

Pour obtenir la MTU valeur, utilisez la Get-NetAdapterAdvancedProperty commande suivante sur votre EC2 instance. Utilisez le caractère générique (astérisque) pour obtenir tous les noms Ethernet. Vérifiez la sortie pour le nom de l'interface`*JumboPacket`. La valeur 9015 indique que les trames Jumbo sont activées. Les trames Jumbo sont désactivées par défaut.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet*"
```

Version 1.5 et antérieures

Pour obtenir la MTU valeur, utilisez la Get-NetAdapterAdvancedProperty commande suivante sur votre EC2 instance. Vérifiez la sortie pour le nom de l'interfaceMTU. La valeur 9001 indique que les trames Jumbo sont activées. Les trames Jumbo sont désactivées par défaut.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

Intel SRIOV 82599 driver

Pour obtenir la MTU valeur, utilisez la Get-NetAdapterAdvancedProperty commande suivante sur votre EC2 instance. Vérifiez l'entrée pour le nom d'interface `*JumboPacket`. La valeur 9014 indique que les trames Jumbo sont activées. (Notez que la MTU taille inclut l'en-tête et la charge utile.) Les trames Jumbo sont désactivées par défaut.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

AWS PV driver

Pour obtenir la MTU valeur, utilisez la commande suivante sur votre EC2 instance. Le nom de l'interface peut varier. Dans la sortie, recherchez une entrée portant le nom « Ethernet », « Ethernet 2 » ou « Local Area Connection ». Vous aurez besoin du nom d'interface pour activer ou désactiver les trames Jumbo. La valeur 9001 indique que les trames Jumbo sont activées.

```
netsh interface ipv4 show subinterface
```

Définissez le MTU pour votre instance

Vous souhaiterez peut-être utiliser des trames jumbo pour le trafic réseau au sein de votre réseau VPC et des trames standard pour le trafic Internet. Quel que soit votre cas d'utilisation, nous vous recommandons de vérifier que votre instance se comporte comme prévu.

La procédure que vous utilisez dépend du système d'exploitation de l'instance.

Instances Linux

Pour définir la MTU valeur sur une instance Linux

1. Exécutez la ip commande suivante sur votre instance. Il définit la MTU valeur souhaitée sur 1500, mais vous pouvez utiliser 9001 à la place.

```
[ec2-user ~]$ sudo ip link set dev eth0 mtu 1500
```

2. (Facultatif) Pour conserver vos MTU paramètres réseau après un redémarrage, modifiez les fichiers de configuration suivants en fonction du type de votre système d'exploitation.

   - Pour Amazon Linux 2, ajoutez la ligne suivante au fichier `/etc/sysconfig/network-scripts/ifcfg-eth0` :

     ```
     MTU=1500
     ```

     Ajoutez la ligne suivante dans le fichier `/etc/dhcp/dhclient.conf` :

     ```
     request subnet-mask, broadcast-address, time-offset, routers, domain-name,
      domain-search, domain-name-servers, host-name, nis-domain, nis-servers, ntp-
     servers;
     ```

   - Pour Amazon LinuxAMI, ajoutez les lignes suivantes à votre `/etc/dhcp/dhclient-eth0.conf` fichier.

     ```
     interface "eth0" {
     supersede interface-mtu 1500;
     }
     ```

   - Pour les autres distributions Linux, consultez leur documentation spécifique.

3. (Facultatif) Redémarrez votre instance et vérifiez que le MTU paramètre est correct.

instances Windows

La procédure que vous utilisez dépend du pilote de votre instance.

ENA driver

Vous pouvez le modifier MTU à l'aide du Gestionnaire de périphériques ou de la Set-NetAdapterAdvancedProperty commande de votre instance.

Version 2.1.0 et versions ultérieures

Utilisez la commande suivante pour activer les cadres jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 9015
```

Utilisez la commande suivante pour désactiver les images jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 1514
```

Version 1.5 et antérieures

Utilisez la commande suivante pour activer les cadres jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -
RegistryValue 9001
```

Utilisez la commande suivante pour désactiver les images jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -
RegistryValue 1500
```

Intel SRIOV 82599 driver

Vous pouvez le modifier MTU à l'aide du Gestionnaire de périphériques ou de la Set-NetAdapterAdvancedProperty commande de votre instance.

Utilisez la commande suivante pour activer les cadres jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 9014
```

Utilisez la commande suivante pour désactiver les images jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 1514
```

AWS PV driver

Vous pouvez modifier le MTU à l'aide de la netsh commande sur votre instance. Vous ne pouvez pas le modifier à l'MTUaide du Gestionnaire de périphériques.

Utilisez la commande suivante pour activer les cadres jumbo.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=9001
```

Utilisez la commande suivante pour désactiver les images jumbo.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=1500
```

Dépannage

Si vous rencontrez des problèmes de connectivité entre votre EC2 instance et un cluster Amazon Redshift lorsque vous utilisez des trames jumbo, consultez la section Queries Appear to Hang dans le guide de gestion Amazon Redshift.

Clouds privés virtuels pour vos EC2 instances

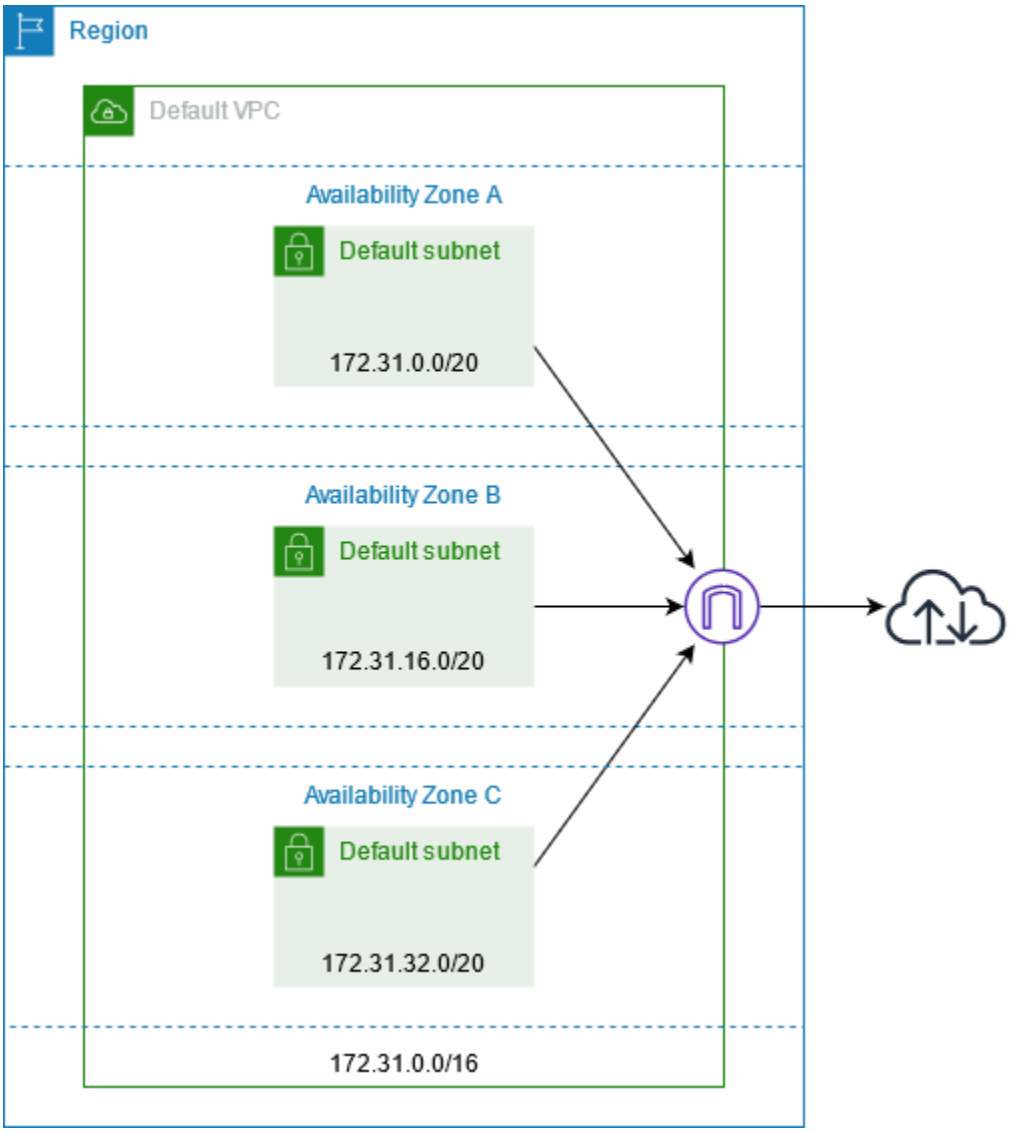
Amazon Virtual Private Cloud (AmazonVPC) vous permet de définir un réseau virtuel dans votre propre zone logiquement isolée au sein du AWS cloud, connu sous le nom de cloud privé virtuel ou VPC. Vous pouvez créer AWS des ressources, telles que EC2 des instances Amazon, dans les sous-réseaux de votreVPC. Votre réseau VPC ressemble beaucoup à un réseau traditionnel que vous pourriez exploiter dans votre propre centre de données, avec les avantages de l'utilisation d'une infrastructure évolutive AWS. Vous pouvez configurer votre VPC ; vous pouvez sélectionner sa plage d'adresses IP, créer des sous-réseaux et configurer des tables de routage, des passerelles réseau et des paramètres de sécurité. Vous pouvez connecter les instances de votre VPC ordinateur à Internet ou à votre propre centre de données.

Table des matières

Votre valeur par défaut VPCs

Lorsque vous créez votre AWS compte, nous créons un compte par défaut VPC dans chaque région. Une valeur par défaut VPC VPC est déjà configurée et prête à être utilisée. Par exemple, il existe

un sous-réseau par défaut pour chaque zone de disponibilité dans chaque zone par défautVPC, une passerelle Internet attachée auVPC, et une route dans la table de routage principale envoie tout le trafic (0.0.0.0/0) vers la passerelle Internet. Vous pouvez modifier la configuration de votre configuration par défaut VPCs selon vos besoins. Par exemple, vous pouvez ajouter des sous-réseaux et des tables de routage.



Non par défaut VPCs

Au lieu d'utiliser une valeur par défaut VPC pour vos ressources, vous pouvez créer les vôtresVPC, comme décrit dans la section Créer une ressource VPC dans le guide de VPC l'utilisateur Amazon.

Voici quelques éléments à prendre en compte lors de la création d'un VPC pour vos EC2 instances.

- Vous pouvez utiliser la suggestion par défaut pour le IPv4 CIDR bloc ou saisir le CIDR bloc requis par votre application ou votre réseau.
- Pour garantir une haute disponibilité, créez des sous-réseaux dans plusieurs zones de disponibilité.
- Si vos instances doivent être accessibles depuis Internet, effectuez l'une des actions suivantes :
  - Si vos instances peuvent se trouver dans un sous-réseau public, ajoutez-y des sous-réseaux publics. Gardez les deux DNS options activées. Vous pouvez éventuellement ajouter des sous-réseaux privés maintenant ou ultérieurement.
  - Si vos instances doivent se trouver dans un sous-réseau privé, ajoutez uniquement des sous-réseaux privés. Vous pouvez ajouter une NAT passerelle pour fournir un accès Internet aux instances des sous-réseaux privés. Si vos instances envoient ou reçoivent un volume de trafic important entre les zones de disponibilité, créez une NAT passerelle dans chaque zone de disponibilité. Sinon, vous pouvez créer une NAT passerelle dans une seule des zones de disponibilité et lancer des instances qui envoient ou reçoivent du trafic entre zones dans la même zone de disponibilité que la NAT passerelle.

Accès Internet

Les instances lancées dans un sous-réseau par défaut VPC ont accès à Internet. Par défaut, VPCs elles sont configurées pour attribuer des adresses IP et des DNS noms d'hôte publics, et la table de routage principale est configurée avec une route vers une passerelle Internet attachée au. VPC

Pour les instances que vous lancez dans des sous-réseaux autres que ceux par défautVPCs, vous pouvez utiliser l'une des options suivantes pour vous assurer que les instances que vous lancez dans ces sous-réseaux ont accès à Internet :

- Configurez une passerelle Internet. Pour plus d'informations, consultez la section Se connecter à Internet à l'aide d'une passerelle Internet dans le guide de VPC l'utilisateur Amazon.
- Configurez une NAT passerelle publique. Pour plus d'informations, consultez la section Accès à Internet depuis un sous-réseau privé dans le guide de l'VPCutilisateur Amazon.

Sous-réseaux partagés

Lorsque vous lancez EC2 des instances dans des VPC sous-réseaux partagés, tenez compte des points suivants :

- Les participants peuvent exécuter des instances dans un sous-réseau partagé en spécifiant l'ID du sous-réseau partagé. Les participants doivent posséder les groupes de sécurité ou les interfaces réseau qu'ils spécifient.
- Les participants peuvent démarrer, arrêter, terminer et décrire les instances qu'ils ont créées dans un sous-réseau partagé. Les participants ne peuvent pas démarrer, arrêter, terminer ou décrire les instances créées par le VPC propriétaire dans le sous-réseau partagé.
- VPCles propriétaires ne peuvent pas démarrer, arrêter, terminer ou décrire les instances créées par les participants dans un sous-réseau partagé.
- Les participants peuvent se connecter à une instance dans un sous-réseau partagé à l'aide d'EC2Instance Connect Endpoint. Le participant doit créer le point de terminaison EC2 Instance Connect dans le sous-réseau partagé. Les participants ne peuvent pas utiliser un point de terminaison EC2 Instance Connect créé par le VPC propriétaire dans le sous-réseau partagé.

Pour plus d'informations, consultez la section « Partagez votre compte VPC avec d'autres comptes » dans le guide de VPC l'utilisateur Amazon.

IPv6-sous-réseaux uniquement

Une EC2 instance lancée dans un sous-réseau IPv6 réservé reçoit une IPv6 adresse mais pas d'IPv4adresse. Toutes les instances que vous lancez dans un sous-réseau IPv6 réservé doivent être des instances créées sur le système AWS Nitro.

Sécurité sur Amazon EC2

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité applicables à AmazonEC2, consultez la section AWS Services concernés par programme de conformitéAWS .
- Sécurité dans le cloud : votre responsabilité englobe les domaines suivants :
  - Contrôler l'accès réseau à vos instances, par exemple en configurant vos groupes VPC et ceux de sécurité. Pour de plus amples informations, veuillez consulter Contrôle du trafic réseau.
  - Gestion des informations d'identification utilisées pour vous connecter à vos instances.
  - Gestion du système d'exploitation invité et des logiciels déployés sur le système d'exploitation invité, y compris les mises à jour et les correctifs de sécurité. Pour de plus amples informations, veuillez consulter Gestion des mises à jour pour les instances Amazon EC2 Windows.
  - Configuration des IAM rôles attachés à l'instance et des autorisations associées à ces rôles. Pour de plus amples informations, veuillez consulter IAMrôles pour Amazon EC2.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'AmazonEC2. Il vous explique comment configurer Amazon EC2 pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos EC2 ressources Amazon.

Table des matières

- Gestion des identités et des accès pour Amazon EC2
- Gestion des mises à jour pour les instances Amazon EC2 Windows
- Bonnes pratiques de sécurité pour les instances Windows
- Paires de EC2 clés Amazon et EC2 instances Amazon
- Groupes EC2 de sécurité Amazon pour vos EC2 instances
- Instances Nitro TPM pour Amazon EC2
- Credential Guard pour les instances Windows
- Accédez à Amazon à EC2 l'aide d'un point de VPC terminaison d'interface

Protection des données sur Amazon EC2

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans Amazon Elastic Compute Cloud. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la section Confidentialité des données FAQ. Pour plus d'informations sur la protection des données en Europe, consultez le modèle de responsabilitéAWS partagée et le billet de GDPR blog sur le blog sur la AWS sécurité.

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) pour chaque compte.
- UtilisezSSL/TLSpour communiquer avec les AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.

- Si vous avez besoin de FIPS 140 à 3 modules cryptographiques validés pour accéder AWS via une interface de ligne de commande ou unAPI, utilisez un point de terminaison. FIPS Pour plus d'informations sur les FIPS points de terminaison disponibles, voir Federal Information Processing Standard (FIPS) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Amazon EC2 ou un autre utilisateur services AWS à l'aide de la consoleAPI, AWS CLI, ou AWS SDKs. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez un URL à un serveur externe, nous vous recommandons vivement de ne pas y inclure d'informations d'identification URL pour valider votre demande auprès de ce serveur.

Table des matières

Sécurité EBS des données Amazon

Les EBS volumes Amazon vous sont présentés sous forme de blocs bruts et non formatés. Ces appareils sont des appareils logiques créés sur l'EBSinfrastructure et le EBS service Amazon garantit qu'ils sont logiquement vides (c'est-à-dire que les blocs bruts sont mis à zéro ou qu'ils contiennent des données cryptographiquement pseudo-aléatoires) avant toute utilisation ou réutilisation par un client.

Si vous avez des procédures qui exigent que toutes les données soient effacées à l'aide d'une méthode spécifique, après ou avant utilisation (ou les deux), telles que celles décrites dans le DoD 5220.22-M (manuel d'exploitation du programme national de sécurité industrielle) NISTou 800-88 (directives pour la désinfection des médias), vous pouvez le faire sur Amazon. EBS Cette activité au niveau des blocs sera répercutée sur le support de stockage sous-jacent au sein du service AmazonEBS.

Chiffrement au repos

EBSvolumes

Amazon EBS Encryption est une solution de chiffrement pour vos EBS volumes et vos instantanés. Il utilise AWS KMS keys. Pour plus d'informations, consultez Amazon EBS Encryption dans le guide de EBS l'utilisateur Amazon.

[Instances Windows] Vous pouvez également utiliser Microsoft EFS et NTFS les autorisations pour le chiffrement au niveau des dossiers et des fichiers.

Volumes de stockage d'instances

Les données des volumes de stockage d'NVMeinstance sont chiffrées à l'aide d'un chiffrement XTS - AES -256, implémenté sur un module matériel de l'instance. Les clés utilisées pour chiffrer les données écrites sur des périphériques de NVMe stockage connectés localement sont définies par client et par volume. Les clés sont générées par le module matériel et ne se trouvent qu'à l'intérieur de celui-ci, qui est inaccessible au personnel AWS . Les clés de chiffrement sont détruites lorsque l'instance est arrêtée ou résiliée et ne peuvent pas être récupérées. Vous ne pouvez pas désactiver le chiffrement et vous ne pouvez pas fournir votre propre clé de chiffrement.

Les données des volumes de stockage d'HDDinstance des instances H1, D3 et D3en sont chiffrées à l'aide de XTS AES -256 et de clés à usage unique.

Lorsque vous arrêtez, mettez en veille prolongée ou résiliez une instance, chaque bloc de stockage du volume de stockage d'instances est réinitialisé. Par conséquent, vos données ne sont pas accessibles via le stockage d'instances d'une autre instance.

Mémoire

Le chiffrement de la mémoire est activé sur les instances suivantes :

- Instances équipées de processeurs AWS Graviton. AWS Graviton2, AWS Graviton3 et Graviton3E prennent en charge le chiffrement permanent de la AWS mémoire. Les clés de chiffrement sont générées en toute sécurité dans le système hôte, elles ne quittent jamais le système hôte et sont détruites lorsque l'hôte est redémarré ou mis hors tension. Pour de plus amples informations, veuillez consulter Processeurs AWS Graviton.
- Les instances dotées de processeurs Intel Xeon Scalable de 3e génération (Ice Lake), telles que les instances M6i, et de processeurs Intel Xeon Scalable de 4e génération (Sapphire Rapids), tels que les instances M7i. Ces processeurs prennent en charge le chiffrement permanent de la mémoire à l'aide du protocole Intel Total Memory Encryption ()TME.
- Instances dotées de AMD EPYC processeurs de 3e génération (Milan), tels que les instances M6a, et de AMD EPYC processeurs de 4e génération (Gênes), tels que les instances M7a. Ces

processeurs prennent en charge le chiffrement permanent de la mémoire à l'aide de AMD Secure Memory Encryption ()SME. Les instances dotées de AMD EPYC processeurs de 3e génération (Milan) prennent également en charge la virtualisation cryptée AMD sécurisée et la pagination imbriquée sécurisée (-). SEV SNP

Chiffrement en transit

Chiffrement au niveau de la couche physique

Toutes les données circulant entre AWS les régions via le réseau AWS mondial sont automatiquement cryptées au niveau de la couche physique avant de quitter les installations AWS sécurisées. Tout le trafic entre les deux AZs est crypté. Des couches supplémentaires de chiffrement, y compris celles présentées dans cette section, peuvent fournir des protections supplémentaires.

Chiffrement fourni par Amazon VPC Peering et Transit Gateway Cross-Region Peering

Tout le trafic interrégional qui utilise le peering Amazon et le VPC peering Transit Gateway est automatiquement chiffré en bloc lorsqu'il quitte une région. Une couche de chiffrement supplémentaire est automatiquement fournie au niveau de la couche physique pour tout le trafic avant qu'il ne quitte les installations AWS sécurisées, comme indiqué précédemment dans cette section.

Chiffrement entre instances

AWS fournit une connectivité sécurisée et privée entre les EC2 instances de tous types. En outre, certains types d'instances utilisent les capacités de déchargement du matériel du système Nitro sous-jacent pour chiffrer automatiquement le trafic en transit entre instances. Ce chiffrement utilise des algorithmes de chiffrement authentifié avec données associées (AEAD), avec un cryptage de 256 bits. Il n'y a aucun impact sur les performances du réseau. Pour prendre en charge ce chiffrement supplémentaire du trafic en transit entre les instances, les exigences suivantes doivent être satisfaites :

- Les instances utilisent les types d'instance suivants :
  - Usage général : M5dn, M5n, M5zn, M6a, M6i, M6id, M6idn, M6in, M7a, M7g, M7GD, M7i, M7i-Flex
  - Optimisé pour le calcul : C5a, C5ad, C5n, C6a, C6gn, C6i, C6id, C6in, C7a, C7g, C7gd, C7gn, C7i, C7i-Flex

  - Mémoire optimisée : R5dn, R5n, R6a, R6i, R6idn, R6in, R6id, R7a, R7g, R7gd, R7i, R7iz, R8g, U-3tb1, U-6tb1, U-7in-12TB1, U-24TB1, U7i-12TB, U7in-12TB 16 To, U7 en 24 To, U7 en 32 To, X2IDN, X2iEDN, X2ieZN
  - Stockage optimisé : D3, D3en, i3EN, i4G, i4i, iM4GN, IS4gen
  - Calcul accéléré :DL1, G4adDL2q, G4dn, G5, G6, G6e, Gr6, Inf1, Inf2, P3dn, P4d, P4de, P5, Trn1, Trn1n, VT1
  - Calcul à hautes performances : Hpc6a, Hpc6id, Hpc7a, Hpc7g
- Les instances se trouvent dans la même région.
- Les instances sont identiques VPC ou homologuesVPCs, et le trafic ne passe pas par un périphérique ou un service réseau virtuel, tel qu'un équilibreur de charge ou une passerelle de transit.

Une couche de chiffrement supplémentaire est automatiquement fournie au niveau de la couche physique pour tout le trafic avant qu'il ne quitte les installations AWS sécurisées, comme indiqué précédemment dans cette section.

Pour afficher les types d'instance qui chiffrent le trafic en transit entre les instances à l'aide de la AWS CLI

Utilisez la commande suivante de l' describe-instance-types.

```
aws ec2 describe-instance-types \
    --filters Name=network-info.encryption-in-transit-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

Chiffrement depuis et vers AWS Outposts

Un avant-poste crée des connexions réseau spéciales appelées liens de service vers sa région d' AWS origine et, éventuellement, une connectivité privée vers un VPC sous-réseau que vous spécifiez. Tout le trafic sur ces connexions est entièrement crypté. Pour plus d'informations, consultez Connectivité via des liens de service et Chiffrement en transit dans le Guide de l'utilisateur AWS Outposts .

Chiffrement d'accès distant

Les RDP protocoles SSH and fournissent des canaux de communication sécurisés pour un accès à distance à vos instances, que ce soit directement ou via EC2 Instance Connect. L'accès à distance

à vos instances à l'aide du gestionnaire de AWS Systems Manager session ou de la commande Run est chiffré à l'aide de la version TLS 1.2, et les demandes de création de connexion sont signées à l'aide de SigV4, authentifiées et autorisées par. AWS Identity and Access Management

Il est de votre responsabilité d'utiliser un protocole de chiffrement, tel que Transport Layer Security (TLS), pour chiffrer les données sensibles en transit entre les clients et vos EC2 instances Amazon.

(Instances Windows) Assurez-vous de n'autoriser que les connexions chiffrées entre les EC2 instances et les AWS API points de terminaison ou les autres services réseau distants sensibles. Vous pouvez mettre cela en œuvre via un groupe de sécurité sortant ou des règles du Pare-feu Windows.

Sécurité de l'infrastructure sur Amazon EC2

En tant que service géré, Amazon Elastic Compute Cloud est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez les API appels AWS publiés pour accéder à Amazon EC2 via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Sécurité de la couche de transport (TLS). Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Des suites de chiffrement parfaitement confidentielles (PFS) telles que (Ephemeral Diffie-Hellman) ou DHE ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un identifiant de clé d'accès et d'une clé d'accès secrète associés à un IAM principal. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Pour plus d'informations, voir Protection de l'infrastructure dans le pilier de sécurité — AWS Well-Architected Framework.

Isolement de réseau

Un cloud privé virtuel (VPC) est un réseau virtuel situé dans votre propre zone logiquement isolée dans le AWS cloud. Utilisez la méthode séparée VPCs pour isoler l'infrastructure par charge de travail ou entité organisationnelle.

Un sous-réseau est une plage d'adresses IP dans unVPC. Lorsque vous lancez une instance, vous la lancez dans un sous-réseau de votreVPC. Utilisez des sous-réseaux pour isoler les niveaux de votre application (par exemple, le Web, l'application et la base de données) en un seulVPC. Utilisez des sous-réseaux privés pour vos instances si elles ne doivent pas être accessibles directement à partir d'Internet.

Pour appeler Amazon EC2 API depuis votre VPC adresse IP privée, utilisez AWS PrivateLink. Pour de plus amples informations, veuillez consulter Accédez à Amazon à EC2 l'aide d'un point de VPC terminaison d'interface.

Isolation sur les hôtes physiques

Les différentes EC2 instances d'un même hôte physique sont isolées les unes des autres comme si elles se trouvaient sur des hôtes physiques distincts. L'hyperviseur isole la CPU mémoire, et les instances reçoivent des disques virtualisés au lieu d'accéder aux disques bruts.

Lorsque vous arrêtez ou résiliez une instance, la mémoire qui lui est allouée est remise à zéro par l'hyperviseur avant d'être allouée à une nouvelle instance, et chaque bloc de stockage est réinitialisé. Cela permet d'être sûr que vos données ne seront pas accidentellement exposées sur une autre instance.

Les MAC adresses réseau sont attribuées dynamiquement aux instances par l'infrastructure AWS réseau. Les adresses IP sont soit attribuées dynamiquement aux instances par l'infrastructure AWS réseau, soit attribuées par un EC2 administrateur via des API demandes authentifiées. Le AWS réseau autorise les instances à envoyer du trafic uniquement à partir des adresses IP MAC et IP qui leur sont attribuées. Dans le cas contraire, le trafic est abandonné.

Par défaut, une instance ne peut pas recevoir un trafic qui ne lui est pas spécifiquement adressé. Si vous devez exécuter des services de traduction d'adresses réseau (NAT), de routage ou de pare-feu sur votre instance, vous pouvez désactiver le contrôle source/destination pour l'interface réseau.

Contrôle du trafic réseau

Envisagez les options suivantes pour contrôler le trafic réseau vers vos EC2 instances :

- Limitez l'accès à vos instances à l'aide de groupes de sécurité. Configurez des règles qui autorisent le trafic réseau minimum requis. Par exemple, vous pouvez autoriser le trafic uniquement à partir des plages d'adresses de votre réseau d'entreprise ou uniquement pour des protocoles spécifiques, tels queHTTPS. Pour les instances Windows, autorisez le trafic de gestion Windows et un minimum de connexions sortantes.
- Tirez parti des groupes de sécurité comme principal mécanisme de contrôle de l'accès réseau aux EC2 instances Amazon. Si nécessaire, utilisez le réseau ACLs avec parcimonie pour fournir un contrôle du réseau sans état et grossier. Les groupes de sécurité sont plus polyvalents que les réseaux ACLs en raison de leur capacité à effectuer un filtrage dynamique des paquets et à créer des règles faisant référence à d'autres groupes de sécurité. Cependant, le réseau ACLs peut être efficace en tant que contrôle secondaire pour refuser un sous-ensemble spécifique de trafic ou fournir des barrières de sécurité de haut niveau pour les sous-réseaux. De plus, comme le réseau ACLs s'applique à l'ensemble d'un sous-réseau, ils peuvent être utilisés comme defense-in-depth dans le cas où une instance serait lancée par inadvertance sans un groupe de sécurité approprié.
- [Instances Windows] Gérez de manière centralisée les paramètres du pare-feu Windows à l'aide des objets de stratégie de groupe (GPO) afin d'améliorer encore les contrôles réseau. Les clients utilisent souvent le Pare-feu Windows pour augmenter la visibilité sur le trafic réseau et pour compléter les filtres de groupe de sécurité, créant des règles avancées pour empêcher des applications spécifiques d'accéder au réseau ou pour filtrer le trafic à partir d'adresses IP d'un sous-ensemble. Par exemple, le pare-feu Windows peut limiter l'accès à l'adresse IP du service de EC2 métadonnées à des utilisateurs ou à des applications spécifiques. Par ailleurs, un service public peut utiliser des groupes de sécurité pour restreindre le trafic vers des ports spécifiques et le pare-feu Windows pour maintenir une liste d'adresses IP explicitement bloquées.
- Utilisez des sous-réseaux privés pour vos instances si elles ne doivent pas être accessibles directement à partir d'Internet. Utilisez un hôte bastion ou une NAT passerelle pour accéder à Internet à partir d'une instance d'un sous-réseau privé.
- [Instances Windows] Utilisez des protocoles d'administration sécurisés tels que l'RDPencapsulation surSSL/TLS. Le guide de démarrage rapide de Remote Desktop Gateway fournit les meilleures pratiques pour déployer une passerelle de bureau à distance, y compris la configuration RDP pour utiliserSSL/TLS.
- [Instances Windows] Utilisez Active Directory ou AWS Directory Service pour contrôler et surveiller de manière étroite et centralisée l'accès interactif des utilisateurs et des groupes aux instances Windows, tout en évitant les autorisations des utilisateurs locaux. Évitez également d'utiliser les administrateurs de domaine et créez plutôt des comptes basés sur des rôles plus granulaires et spécifiques à l'application. Just Enough Administration (JEA) permet de gérer les modifications

apportées aux instances Windows sans accès interactif ni accès administrateur. JEAPermet en outre aux entreprises de verrouiller l'accès administratif au sous-ensemble de PowerShell commandes Windows requis pour l'administration des instances. Pour plus d'informations, consultez la section « Gérer l'accès à Amazon au niveau du système d'exploitation EC2 » dans le livre blanc sur les meilleures pratiques AWS de sécurité.

- [Instances Windows] Les administrateurs système doivent utiliser des comptes Windows à accès limité pour effectuer leurs activités quotidiennes, et n'augmenter l'accès que lorsque cela est nécessaire pour effectuer des modifications de configuration spécifiques. En outre, n'accédez directement aux instances Windows que lorsque cela est absolument nécessaire. Tirez plutôt parti de systèmes de gestion de configuration centraux tels que EC2 Run Command, Systems Center Configuration Manager (SCCM) PowerShellDSC, Windows ou Amazon EC2 Systems Manager (SSM) pour appliquer les modifications aux serveurs Windows.
- Configurez les tables de routage des VPC sous-réseaux Amazon avec les itinéraires réseau minimaux requis. Par exemple, placez uniquement les EC2 instances Amazon nécessitant un accès direct à Internet dans des sous-réseaux dotés de routes menant à une passerelle Internet, et placez uniquement les EC2 instances Amazon nécessitant un accès direct aux réseaux internes dans des sous-réseaux dotés de routes vers une passerelle privée virtuelle.
- Envisagez d'utiliser des groupes de sécurité ou des interfaces réseau supplémentaires pour contrôler et auditer le trafic de gestion des EC2 instances Amazon séparément du trafic normal des applications. Cette approche permet aux clients de mettre en œuvre des IAM politiques spéciales pour le contrôle des modifications, ce qui facilite l'audit des modifications apportées aux règles des groupes de sécurité ou aux scripts de vérification automatique des règles. L'utilisation de plusieurs interfaces réseau fournit également des options supplémentaires pour contrôler le trafic réseau, notamment la possibilité de créer des politiques de routage basées sur l'hôte ou de tirer parti de différentes règles de routage de VPC sous-réseau en fonction du sous-réseau attribué de l'interface réseau.
- Utilisez AWS Virtual Private Network ou AWS Direct Connect pour établir des connexions privées entre vos réseaux distants et votreVPCs. Pour plus d'informations, consultez la section Options de VPCconnectivité entre le réseau et Amazon.
- Utilisez les journaux de VPC flux pour surveiller le trafic qui atteint vos instances.
- Utilisez la protection contre les GuardDuty programmes malveillants pour identifier les comportements suspects indiquant la présence de logiciels malveillants sur vos instances susceptibles de compromettre votre charge de travail, de réaffecter des ressources à des fins malveillantes et d'obtenir un accès non autorisé à vos données.

- Utilisez la surveillance du temps GuardDuty d'exécution pour identifier les menaces potentielles qui pèsent sur vos instances et y répondre. Pour plus d'informations, consultez Comment fonctionne la surveillance du temps d'exécution avec EC2 les instances Amazon.
- Utilisez AWS Security HubReachability Analyzer ou Network Access Analyzer pour vérifier l'absence d'accessibilité involontaire au réseau depuis vos instances.
- Utilisez EC2Instance Connect pour vous connecter à vos instances à l'aide de Secure Shell (SSH) sans avoir à partager ni à gérer les SSH clés.
- Utilisez le gestionnaire de AWS Systems Manager session pour accéder à distance à vos instances au lieu d'ouvrir des RDP ports SSH ou des ports entrants et de gérer des paires de clés.
- Utilisez AWS Systems Manager Run Command pour automatiser les tâches administratives courantes au lieu de vous connecter à vos instances.
- [Instances Windows] La plupart des rôles du système d'exploitation Windows et des applications professionnelles Microsoft fournissent également des fonctionnalités améliorées, telles que les restrictions de plage d'adresses IP au sein de IIS celui-ci, les politiques de filtrage TCP /IP dans Microsoft SQL Server et les politiques de filtre de connexion dans Microsoft Exchange. La fonctionnalité de restriction de réseau au sein de la couche d'application peut fournir des couches supplémentaires de défense pour les serveurs d'applications métier critiques.

Amazon VPC prend en charge des contrôles de sécurité réseau supplémentaires, tels que les passerelles, les serveurs proxy et les options de surveillance du réseau. Pour plus d'informations, consultez la section Contrôler le trafic réseau dans le guide de VPC l'utilisateur Amazon.

Résilience chez Amazon EC2

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Si vous avez besoin de répliquer vos données ou applications sur des distances géographiques plus importantes, utilisez les Local Zones AWS . Une zone AWS locale est une extension d'une AWS région située à proximité géographique de vos utilisateurs. Les Local Zones ont leurs propres

connexions à Internet et prennent en charge AWS Direct Connect. Comme toutes les AWS régions, les Zones AWS Locales sont complètement isolées des autres AWS zones.

Si vous devez répliquer vos données ou applications dans une zone AWS locale, il est AWS recommandé d'utiliser l'une des zones suivantes comme zone de basculement :

- Une autre zone locale
- Une zone de disponibilité dans la région qui n'est pas la zone parent Vous pouvez utiliser la describe-availability-zonescommande pour afficher la zone parent.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Outre l'infrastructure AWS mondiale, Amazon EC2 propose les fonctionnalités suivantes pour renforcer la résilience de vos données :

- Copier AMIs entre les régions
- Copier des EBS instantanés entre les régions
- Automatisation EBS soutenue à l'AMIsaide d'Amazon Data Lifecycle Manager
- Automatisation des EBS instantanés à l'aide d'Amazon Data Lifecycle Manager
- Maintien de la santé et de la disponibilité de votre flotte à l'aide d'Amazon EC2 Auto Scaling
- Distribution du trafic entrant sur plusieurs instances dans une ou plusieurs zones de disponibilité à l'aide d'Elastic Load Balancing

Validation de conformité pour Amazon EC2

Pour savoir si un programme services AWS de conformité service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et

réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la HIPAA sécurité et la conformité sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent AWS créer HIPAA des applications éligibles.

> **Note**
>
> Tous ne services AWS sont pas HIPAA éligibles. Pour plus d'informations, consultez la référence des services HIPAA éligibles.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation services AWS et reprennent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité PCIDSS, par exemple en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.

- AWS Audit Manager— Cela vous service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Gestion des identités et des accès pour Amazon EC2

AWS Identity and Access Management (IAM) est un outil service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. IAMles administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les EC2 ressources Amazon. IAMest un service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Vos informations de sécurité vous identifient auprès des services AWS et vous donnent accès à AWS des ressources, telles que vos EC2 ressources Amazon. Vous pouvez utiliser les fonctionnalités d'Amazon EC2 et IAM autoriser d'autres utilisateurs, services et applications à utiliser vos EC2 ressources Amazon sans partager vos informations de sécurité. Vous pouvez l'utiliser IAM pour contrôler la façon dont les autres utilisateurs utilisent les ressources de votre compte Compte AWS, et vous pouvez utiliser des groupes de sécurité pour contrôler l'accès à vos EC2 instances Amazon. Vous pouvez choisir d'autoriser l'utilisation complète ou limitée de vos EC2 ressources Amazon.

Si vous êtes développeur, vous pouvez utiliser IAM des rôles pour gérer les informations d'identification de sécurité requises par les applications que vous exécutez sur vos EC2 instances. Une fois que vous avez attaché un IAM rôle à votre instance, les applications exécutées sur l'instance peuvent récupérer les informations d'identification auprès du service de métadonnées d'instance (IMDS).

Pour connaître les meilleures pratiques en matière de sécurisation de vos AWS ressourcesIAM, consultez la section Bonnes pratiques en matière de sécurité IAM dans le guide de IAM l'utilisateur.

Table des matières

Politiques basées sur l'identité pour Amazon EC2

Par défaut, les utilisateurs ne sont pas autorisés à créer ou à modifier des EC2 ressources Amazon, ni à effectuer des tâches à l'aide d'Amazon EC2API, de EC2 la console Amazon ouCLI. Pour permettre aux utilisateurs de créer ou de modifier des ressources et d'effectuer des tâches, vous devez créer des IAM politiques qui accordent aux utilisateurs l'autorisation d'utiliser les ressources et les API actions spécifiques dont ils auront besoin, puis associer ces politiques aux utilisateurs, groupes ou IAM rôles qui nécessitent ces autorisations.

Quand vous attachez une stratégie à un utilisateur, à un groupe d'utilisateurs ou à un rôle, celle-ci accorde ou refuse aux utilisateurs l'autorisation d'exécuter les tâches spécifiées sur les ressources spécifiées. Pour plus d'informations générales sur IAM les politiques, voir Politiques et autorisations IAM dans le Guide de IAM l'utilisateur. Pour plus d'informations sur la gestion et la création de IAM politiques personnalisées, consultez la section Gestion des IAM politiques.

Une IAM politique doit accorder ou refuser l'autorisation d'utiliser une ou plusieurs EC2 actions Amazon. Elle doit aussi spécifier les ressources qui peuvent être utilisées avec l'action : il peut s'agir de toutes les ressources ou, dans certains cas, de ressources spécifiques. La politique peut aussi inclure les conditions que vous appliquez à la ressource.

Pour commencer, vous pouvez vérifier si les politiques AWS gérées pour Amazon EC2 répondent à vos besoins. Sinon, vous pouvez créer vos propres politiques personnalisées. Pour de plus amples informations, veuillez consulter the section called "AWS politiques gérées".

Table des matières

Syntaxe d'une politique

Une IAM politique est un JSON document composé d'une ou de plusieurs déclarations. Chaque déclaration est structurée comme suit :

```
{
  "Statement":[{
    "Effect":"effect",
    "Action":"action",
    "Resource":"arn",
    "Condition":{
      "condition":{
        "key":"value"
        }
      }
    }
  ]
}
```

Une déclaration se compose de différents éléments :

- Effect : effect peut avoir la valeur `Allow` ou `Deny`. Par défaut, les utilisateurs ne sont pas autorisés à utiliser les ressources et les API actions. Toutes les demandes sont donc refusées. Une autorisation explicite remplace l'autorisation par défaut. Un refus explicite remplace toute autorisation.
- Action : L'action est l'APIaction spécifique pour laquelle vous accordez ou refusez l'autorisation. Pour en savoir plus sur la spécification d'action, consultez Actions pour Amazon EC2.
- Resource : la ressource affectée par l'action. Certaines EC2 API actions Amazon vous permettent d'inclure dans votre politique des ressources spécifiques qui peuvent être créées ou modifiées par l'action. Vous spécifiez une ressource en utilisant un nom de ressource Amazon (ARN) ou en utilisant le caractère générique (*) pour indiquer que la déclaration s'applique à toutes les ressources. Pour de plus amples informations, veuillez consulter Autorisations prises en charge au niveau des ressources pour les actions Amazon EC2 API.
- Condition : les conditions sont facultatives. Elles permettent de contrôler à quel moment votre politique est effective. Pour plus d'informations sur la définition de conditions pour AmazonEC2, consultezClés de condition pour Amazon EC2.

Pour plus d'informations sur les exigences des politiques, consultez la référence des IAM JSON politiques dans le guide de IAM l'utilisateur. Pour des exemples IAM de déclarations de politique relatives à AmazonEC2, voirExemples de politiques pour contrôler l'accès à Amazon EC2 API.

Actions pour Amazon EC2

Dans une déclaration IAM de politique, vous pouvez spécifier n'importe quelle API action à partir de n'importe quel service compatibleIAM. Pour AmazonEC2, utilisez le préfixe suivant avec le nom de l'APIaction : `ec2:` Par exemple : `ec2:RunInstances` et `ec2:CreateImage`.

Pour spécifier plusieurs actions dans une seule déclaration, séparez-les par des virgules comme suit :

```
"Action": ["ec2:action1", "ec2:action2"]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques. Par exemple, vous pouvez spécifier toutes les actions dont le nom commence par le mot « Describe » comme suit :

```
"Action": "ec2:Describe*"
```

> **Note**
>
> Actuellement, les API actions Amazon EC2 Describe* ne prennent pas en charge les autorisations au niveau des ressources. Pour plus d'informations sur les autorisations au niveau des ressources pour AmazonEC2, consultez. Politiques basées sur l'identité pour Amazon EC2

Pour spécifier toutes les EC2 API actions Amazon, utilisez le caractère générique* comme suit :

```
"Action": "ec2:*"
```

Pour obtenir la liste des EC2 actions Amazon, consultez la section Actions définies par Amazon EC2 dans le Service Authorization Reference.

Autorisations prises en charge au niveau des ressources pour les actions Amazon EC2 API

Les autorisations au niveau des ressources font référence à la possibilité de spécifier les ressources sur lesquelles les utilisateurs sont autorisés à exécuter des actions. Amazon EC2 prend partiellement en charge les autorisations au niveau des ressources. Cela signifie que pour certaines EC2 actions Amazon, vous pouvez contrôler le moment où les utilisateurs sont autorisés à utiliser ces actions en fonction des conditions qui doivent être remplies ou des ressources spécifiques que les utilisateurs sont autorisés à utiliser. Par exemple, vous pouvez autoriser les utilisateurs à lancer des instances, mais uniquement d'un type spécifique et uniquement à l'aide d'une instance spécifiqueAMI.

Pour spécifier une ressource dans une déclaration IAM de politique, utilisez son Amazon Resource Name (ARN). Pour plus d'informations sur la spécification de la ARN valeur, consultezAmazon Resource Names (ARNs) pour Amazon EC2. Si une API action ne prend pas en charge un individuARNs, vous devez utiliser un caractère générique (*) pour indiquer que toutes les ressources peuvent être affectées par l'action.

Pour consulter les tableaux qui identifient les EC2 API actions Amazon qui prennent en charge les autorisations au niveau des ressources, ainsi que les clés de condition ARNs et les clés de condition que vous pouvez utiliser dans une politique, consultez Actions, ressources et clés de condition pour Amazon. EC2

N'oubliez pas que vous pouvez appliquer des autorisations au niveau des ressources basées sur des balises dans les IAM politiques que vous utilisez pour les actions Amazon. EC2 API Vous bénéficiez ainsi d'un meilleur contrôle sur les ressources qu'un utilisateur peut créer, modifier ou utiliser. Pour de plus amples informations, veuillez consulter Accorder l'autorisation de baliser les EC2 ressources Amazon lors de la création.

Amazon Resource Names (ARNs) pour Amazon EC2

Chaque déclaration IAM de politique s'applique aux ressources que vous spécifiez à l'aide de leurARNs.

An ARN possède la syntaxe générale suivante :

```
arn:aws:[service]:[region]:[account-id]:resourceType/resourcePath
```

web

Le service (par exemple, `ec2`).

region

La région de la ressource (par exemple, `us-east-1`).

id-compte

L'identifiant du AWS compte, sans tiret (par exemple,`123456789012`).

resourceType

Le type de ressource (par exemple, `instance`).

resourcePath

Un chemin qui identifie la ressource. Vous pouvez utiliser le caractère générique * dans vos chemins.

Par exemple, vous pouvez indiquer une instance spécifique (`i-1234567890abcdef0`) dans votre instruction à l'aide de ARN ce qui suit.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

Vous pouvez spécifier toutes les instances qui appartiennent à un compte spécifique à l'aide du caractère générique * comme suit :

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

Vous pouvez également spécifier toutes les EC2 ressources Amazon appartenant à un compte spécifique en utilisant le caractère générique* comme suit.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:*"
```

Pour spécifier toutes les ressources, ou si une API action spécifique n'est pas compatibleARNs, utilisez le caractère générique * dans l'`Resource`élément comme suit.

```
"Resource": "*"
```

De nombreuses EC2 API actions Amazon impliquent plusieurs ressources. Par exemple, `AttachVolume` attache un EBS volume Amazon à une instance, de sorte qu'un utilisateur doit être autorisé à utiliser le volume et l'instance. Pour spécifier plusieurs ressources dans une seule instruction, séparez-les ARNs par des virgules, comme suit.

```
"Resource": ["arn1", "arn2"]
```

Pour obtenir la liste des EC2 ressources ARNs destinées à Amazon, consultez la section Types de ressources définis par Amazon EC2.

Clés de condition pour Amazon EC2

Dans une déclaration de politique, vous pouvez, le cas échéant, spécifier des conditions qui contrôlent à quel moment la déclaration est effective. Chaque condition contient une ou plusieurs paires clé-valeur. Les clés de condition ne sont pas sensibles à la casse. Nous avons défini des clés de condition AWS globales, ainsi que des clés de condition supplémentaires spécifiques au service.

Pour obtenir la liste des clés de condition spécifiques à un service pour AmazonEC2, consultez la section Clés de condition pour Amazon. EC2 Amazon implémente EC2 également les clés de condition AWS globales. Pour plus d'informations, consultez la section Informations disponibles dans toutes les demandes dans le Guide de IAM l'utilisateur.

Toutes les EC2 actions Amazon prennent en charge les clés de `ec2:Region` condition `aws:RequestedRegion` et. Pour de plus amples informations, veuillez consulter Exemple : Restreindre l'accès à une région spécifique.

Pour utiliser une clé de condition dans votre IAM politique, utilisez l'`Condition`instruction. Par exemple, la politique suivante accorde aux utilisateurs l'autorisation d'ajouter et de supprimer des règles entrantes et sortantes pour n'importe quel groupe de sécurité. Il utilise la clé de `ec2:Vpc` condition pour spécifier que ces actions ne peuvent être effectuées que sur des groupes de sécurité spécifiquesVPC.

```
{
"Version": "2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action": [
       "ec2:AuthorizeSecurityGroupIngress",
       "ec2:AuthorizeSecurityGroupEgress",
       "ec2:RevokeSecurityGroupIngress",
       "ec2:RevokeSecurityGroupEgress"],
     "Resource": "arn:aws:ec2:region:account:security-group/*",
      "Condition": {
        "StringEquals": {
          "ec2:Vpc": "arn:aws:ec2:region:account:vpc/vpc-11223344556677889"
```

```
        }
      }
    }
  ]
}
```

Si vous spécifiez plusieurs conditions ou plusieurs clés dans une seule condition, nous les évaluons à l'aide d'une AND opération logique. Si vous spécifiez une seule condition avec plusieurs valeurs pour une clé, la condition est analysée à l'aide d'une opération logique OR. Pour que les autorisations soient accordées, toutes les conditions doivent être satisfaites.

Vous pouvez aussi utiliser des espaces réservés quand vous spécifiez des conditions. Pour plus d'informations, voir Éléments IAM de politique : variables et balises dans le guide de IAM l'utilisateur.

> **Important**
>
> De nombreuses clés de condition sont spécifiques à une ressource, et certaines API actions utilisent plusieurs ressources. Si vous écrivez une stratégie avec une clé de condition, utilisez l'élément `Resource` de la déclaration pour spécifier la ressource à laquelle la clé de condition s'applique. Dans le cas contraire, la politique peut empêcher totalement les utilisateurs d'exécuter l'action, car le contrôle de la condition échoue pour les ressources auxquelles la clé de condition ne s'applique pas. Si vous ne souhaitez pas spécifier de ressource, ou si vous avez écrit l'`Action`élément de votre politique de manière à inclure plusieurs API actions, vous devez utiliser le type de `...IfExists` condition pour vous assurer que la clé de condition est ignorée pour les ressources qui ne l'utilisent pas. Pour plus d'informations, voir... IfExists Conditions énoncées dans le guide de IAM l'utilisateur.

Clés de condition

- Clé de condition ec2:Attribute
- Clés de condition ec2:ResourceID
- Clé de condition ec2:SourceInstanceARN

Clé de condition ec2:Attribute

La clé de condition `ec2:Attribute` peut être utilisée pour les conditions qui filtrent l'accès par un attribut d'une ressource.

Cette clé de condition ne prend en charge que les propriétés de type de données primitif (telles que les chaînes ou les entiers) ou les AttributeValueobjets complexes contenant uniquement une propriété Value (telle que la description ou les ImdsSupportobjets de l'ModifyImageAttributeAPIaction). La clé de condition ne peut pas être utilisée avec des objets complexes contenant plusieurs propriétés, tels que l'LaunchPermissionobjet de ModifyImageAttribute.

Par exemple, la politique suivante utilise la clé de `ec2:Attribute/Description` condition pour filtrer l'accès en fonction de l'objet Description complexe de l'ModifyImageAttributeAPIaction. La clé de condition n'autorise que les demandes qui modifient la description d'une image pour `Production` ou `Development`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute/Description": [
            "Production",
            "Development"
          ]
        }
      }
    }
  ]
}
```

L'exemple de politique suivant utilise la clé de `ec2:Attribute` condition pour filtrer l'accès en fonction de la propriété primitive Attribute de l'ModifyImageAttributeAPIaction. La clé de condition refuse toutes les demandes qui tentent de modifier la description d'une image.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
```

```
      "Condition": {
        "StringEquals": {
          "ec2:Attribute": "Description"
        }
      }
    }
  ]
}
```

Clés de condition ec2:ResourceID

Lorsque vous utilisez les clés de `ec2:`*`Resource`*`ID` condition suivantes avec les API actions spécifiées, la valeur de la clé de condition est utilisée pour spécifier la ressource résultante créée par l'APIaction. `ec2:`*`Resource`*`ID`les clés de condition ne peuvent pas être utilisées pour spécifier une ressource source spécifiée dans la API demande. Si vous utilisez l'une des clés de `ec2:`*`Resource`*`ID` condition suivantes avec une valeur spécifiéeAPI, vous devez toujours spécifier le caractère générique (*). Si vous spécifiez une valeur différente, la condition se résout toujours en * pendant l'exécution. Par exemple, pour utiliser la clé de `ec2:ImageId` condition avec le CopyImageAPI, vous devez spécifier la clé de condition comme suit :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          ec2:ImageID": "*"
        }
      }
    }
  ]
}
```

Nous vous recommandons d'éviter d'utiliser ces clés de condition pour effectuer les API actions suivantes :

- `ec2:DhcpOptionsID` – `CreateDhcpOptions`
- `ec2:ImageID`— `CopyImage``CreateImage`,`ImportImage`, et `RegisterImage`

- `ec2:InstanceID`— `RunInstances` et `ImportInstance`
- `ec2:InternetGatewayID` – `CreateInternetGateway`
- `ec2:NetworkAclID` – `CreateNetworkAcl`
- `ec2:NetworkInterfaceID` – `CreateNetworkInterface`
- `ec2:PlacementGroupName` – `CreatePlacementGroup`
- `ec2:RouteTableID` – `CreateRouteTable`
- `ec2:SecurityGroupID` – `CreateSecurityGroup`
- `ec2:SnapshotID`— `CopySnapshot`,`CreateSnapshots`, et `ImportSnapshots`
- `ec2:SubnetID` – `CreateSubnet`
- `ec2:VolumeID`— `CreateVolume` et `ImportVolume`
- `ec2:VpcID` – `CreateVpc`
- `ec2:VpcPeeringConnectionID` – `CreateVpcPeeringConnection`

Pour filtrer l'accès en fonction d'une ressource spécifiqueIDs, nous vous recommandons d'utiliser l'élément de `Resource` politique comme suit.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-01234567890abcdef"
    }
  ]
}
```

Clé de condition ec2:SourceInstanceARN

Permet `ec2:SourceInstanceARN` de spécifier ARN l'instance à partir de laquelle une demande est effectuée. Il s'agit d'une clé de condition AWS globale, ce qui signifie que vous pouvez l'utiliser avec des services autres qu'AmazonEC2. Pour un exemple de stratégie, consultez Exemple : autoriser une instance spécifique à afficher les ressources d'autres AWS services.

Contrôlez l'accès à l'aide de l'accès basé sur les attributs

Lorsque vous créez une IAM politique qui autorise les utilisateurs à utiliser les EC2 ressources, vous pouvez inclure des informations sur les balises dans l'`Condition`élément de la stratégie afin de contrôler l'accès en fonction des balises. C'est ce que l'on appelle le contrôle d'accès basé sur les attributs ()ABAC. ABACpermet de mieux contrôler les ressources qu'un utilisateur peut modifier, utiliser ou supprimer. Pour plus d'informations, voir À quoi ça ABAC sert AWS ?

Par exemple, vous pouvez créer une stratégie qui permet aux utilisateurs de résilier une instance, mais qui refuse l'action si l'instance possède la balise `environment=production`. Pour ce faire, vous utilisez la clé de condition `aws:ResourceTag` pour autoriser ou refuser l'accès à la ressource en fonction des balises attachées à la ressource.

```
"StringEquals": { "aws:ResourceTag/environment": "production" }
```

Pour savoir si une EC2 API action Amazon permet de contrôler l'accès à l'aide de la clé de `aws:ResourceTag` condition, consultez Actions, ressources et clés de condition pour Amazon EC2. Notez que les actions `Describe` ne prennent pas en charge les autorisations au niveau des ressources, vous devez donc les spécifier dans une instruction distincte sans condition.

Pour des exemples IAM de politiques, voirExemples de politiques pour contrôler l'accès à Amazon EC2 API.

Si vous autorisez ou refusez à des utilisateurs l'accès à des ressources en fonction de balises, vous devez envisager de refuser de manière explicite la possibilité pour les utilisateurs d'ajouter ces balises ou de les supprimer des mêmes ressources. Sinon, il sera possible pour un utilisateur de contourner vos restrictions et d'obtenir l'accès à une ressource en modifiant ses balises.

Octroi d'autorisations aux utilisateurs, aux groupes et aux rôles

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .
- Utilisateurs gérés IAM via un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Suivez les instructions de la section Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le guide de IAM l'utilisateur.

- IAMutilisateurs :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la section Création d'un rôle pour un IAM utilisateur dans le Guide de IAM l'utilisateur.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la section Ajouter des autorisations à un utilisateur (console) dans le guide de IAM l'utilisateur.

Vérifier que les utilisateurs ont les autorisations requises

Une fois que vous avez créé une IAM politique, nous vous recommandons de vérifier si elle accorde aux utilisateurs les autorisations nécessaires pour utiliser les API actions et les ressources spécifiques dont ils ont besoin avant de mettre la politique en production.

Créez d'abord un utilisateur à des fins de test, puis associez la IAM politique que vous avez créée à l'utilisateur de test. Ensuite, créez une demande en tant qu'utilisateur test.

Si l'EC2action Amazon que vous testez crée ou modifie une ressource, vous devez effectuer la demande en utilisant le `DryRun` paramètre (ou exécuter la AWS CLI commande avec l'`--dry-run`option). Dans ce cas, l'appel conclut le contrôle d'autorisation, mais non l'opération. Par exemple, vous pouvez vérifier si l'utilisateur peut terminer une instance particulière sans réellement l'achever. Si l'utilisateur a les autorisations requises, la demande retourne `DryRunOperation` ; sinon, elle retourne `UnauthorizedOperation`.

Si la politique n'accorde pas à l'utilisateur les autorisations que vous escomptiez, ou si elles sont trop excessives, vous pouvez ajuster la politique selon vos besoins et la tester à nouveau jusqu'à ce que vous obteniez les résultats souhaités.

> **Important**
>
> La propagation des modifications de la politique peut durer plusieurs minutes avant qu'elles ne prennent effet. Par conséquent, il est recommandé que vous laissiez s'écouler cinq minutes avant de tester les mises à jour de votre politique.

Si un contrôle d'autorisation échoue, la demande retourne un message codé avec les informations de diagnostic. Vous pouvez décoder le message à l'aide de l'action `DecodeAuthorizationMessage`. Pour plus d'informations, reportez-vous DecodeAuthorizationMessageà la section AWS Security

Token Service APIRéférence et decode-authorization-messageà la Référence des AWS CLI commandes.

Exemples de politiques pour contrôler l'accès à Amazon EC2 API

Vous pouvez utiliser IAM des politiques pour accorder aux utilisateurs les autorisations nécessaires pour travailler avec AmazonEC2. Pour obtenir des step-by-step instructions, reportez-vous à la section Création IAM de politiques dans le guide de IAM l'utilisateur.

Les exemples suivants présentent des déclarations de politique que vous pouvez utiliser pour accorder aux utilisateurs l'autorisation d'utiliser AmazonEC2. Ces politiques sont conçues pour les demandes effectuées à l'aide du AWS CLI ou d'un AWS SDK. Dans les exemples suivants, remplacez chaque *`user input placeholder`* avec vos propres informations.

Exemples

- Exemple : accès en lecture seule
- Exemple : Restreindre l'accès à une région spécifique
- Utiliser des instances
- Instances de lancement (RunInstances)
- Utiliser instances Spot
- Exemple : Utiliser instances réservées
- Exemple : Baliser des ressources
- Exemple : Utiliser des rôles IAM
- Exemple : Utiliser des tables de routage
- Exemple : autoriser une instance spécifique à afficher les ressources d'autres AWS services
- Exemple : Utiliser des modèles de lancement
- Utiliser des métadonnées d'instance
- Travaillez avec les EBS volumes et les instantanés Amazon

Pour des exemples de politiques relatives au travail dans la EC2 console Amazon, consultezExemples de politiques pour contrôler l'accès à la EC2 console Amazon.

Exemple : accès en lecture seule

La politique suivante autorise les utilisateurs à utiliser toutes les EC2 API actions Amazon dont le nom commence par`Describe`. L'`Resource`élément utilise un caractère générique pour indiquer

que les utilisateurs peuvent spécifier toutes les ressources à l'aide de ces API actions. Le caractère générique * est également nécessaire dans les cas où l'APIaction ne prend pas en charge les autorisations au niveau des ressources. Pour plus d'informations sur les actions ARNs que vous pouvez utiliser avec quelles EC2 API actions Amazon, consultez Actions, ressources et clés de condition pour Amazon EC2.

Les utilisateurs ne sont pas autorisés à effectuer des actions sur les ressources (sauf si une autre déclaration les autorise à le faire) car l'autorisation d'utiliser des API actions leur est refusée par défaut.

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    }
   ]
}
```

Exemple : Restreindre l'accès à une région spécifique

La politique suivante refuse aux utilisateurs l'autorisation d'utiliser toutes les EC2 API actions Amazon, sauf si la région est l'Europe (Francfort). Il utilise la clé de condition globale`aws:RequestedRegion`, qui est prise en charge par toutes les EC2 API actions Amazon.

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "eu-central-1"
        }
      }
    }
  ]
```

```
}
```

Vous pouvez également utiliser la clé de conditionec2:Region, qui est spécifique à Amazon EC2 et est prise en charge par toutes les EC2 API actions Amazon.

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ec2:Region": "eu-central-1"
        }
      }
    }
  ]
}
```

Utiliser des instances

Exemples

- Exemple : Décrire, lancer, arrêter, démarrer et résilier toutes les instances
- Exemple : Décrire toutes les instances, et arrêter, démarrer et résilier uniquement des instances particulières

Exemple : Décrire, lancer, arrêter, démarrer et résilier toutes les instances

La politique suivante autorise les utilisateurs à utiliser les API actions spécifiées dans l'Actionélément. L'Resourceélément utilise un caractère générique * pour indiquer que les utilisateurs peuvent spécifier toutes les ressources à l'aide de ces API actions. Le caractère générique * est également nécessaire dans les cas où l'APIaction ne prend pas en charge les autorisations au niveau des ressources. Pour plus d'informations sur les actions ARNs que vous pouvez utiliser avec quelles EC2 API actions Amazon, consultez Actions, ressources et clés de condition pour Amazon EC2.

Les utilisateurs ne sont pas autorisés à utiliser d'autres API actions (sauf si une autre instruction les autorise à le faire) car les utilisateurs se voient refuser l'autorisation d'utiliser API des actions par défaut.

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": "*"
    }
   ]
}
```

Exemple : Décrire toutes les instances, et arrêter, démarrer et résilier uniquement des instances particulières

La stratégie suivante autorise les utilisateurs à décrire toutes les instances, à démarrer et à arrêter uniquement les instances i-1234567890abcdef0 et i-0598c7d356eba48d7, et à ne terminer que les instances de la région Région USA Est (Virginie du N.) (`us-east-1`) avec la balise de ressource "`purpose=test`".

La première déclaration utilise un caractère générique * pour l'élément `Resource` de façon à indiquer que les utilisateurs peuvent spécifier toutes les ressources avec l'action ; dans le cas présent, ils peuvent afficher toutes les instances. Le caractère générique * est également nécessaire dans les cas où l'APIaction ne prend pas en charge les autorisations au niveau des ressources (dans ce cas,). `ec2:DescribeInstances` Pour plus d'informations sur les actions ARNs que vous pouvez utiliser avec quelles EC2 API actions Amazon, consultez Actions, ressources et clés de condition pour Amazon EC2.

La deuxième déclaration utilise des permissions au niveau des ressources pour les actions `StopInstances` et `StartInstances`. Les instances spécifiques sont indiquées par leur présence ARNs dans l'`Resource`élément.

La troisième déclaration permet aux utilisateurs de résilier toutes les instances de la région USA Est (Virginie du Nord`us-east-1`) () qui appartiennent au AWS compte spécifié, mais uniquement lorsque l'instance possède le tag`"purpose=test"`. L'élément `Condition` stipule quand la déclaration de stratégie est en vigueur.

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
   "Effect": "Allow",
      "Action": "ec2:DescribeInstances",
      "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:account-id:instance/i-1234567890abcdef0",
        "arn:aws:ec2:us-east-1:account-id:instance/i-0598c7d356eba48d7"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "ec2:TerminateInstances",
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
         "StringEquals": {
            "aws:ResourceTag/purpose": "test"
         }
      }
   }

   ]
}
```

Instances de lancement (RunInstances)

L'RunInstancesAPIaction lance une ou plusieurs instances à la demande ou une ou plusieurs instances ponctuelles. `RunInstances`nécessite une instance AMI et crée une instance. Les utilisateurs peuvent spécifier une paire de clés et un groupe de sécurité dans la demande. Le lancement dans un VPC nécessite un sous-réseau et crée une interface réseau. Le lancement depuis un site EBS soutenu par Amazon AMI crée un volume. Par conséquent, l'utilisateur doit être autorisé à utiliser ces EC2 ressources Amazon. Vous pouvez créer une déclaration de stratégie qui requiert que les utilisateurs spécifient un paramètre facultatif sur `RunInstances`, ou limitent les utilisateurs à certaines valeurs pour tel ou tel paramètre.

Pour plus d'informations sur les autorisations au niveau des ressources requises pour lancer une instance, consultez Actions, ressources et clés de condition pour Amazon. EC2

Par défaut, les utilisateurs ne sont pas autorisés à décrire, démarrer, arrêter ni résilier les instances obtenues. Une solution pour accorder aux utilisateurs l'autorisation de gérer les instances obtenues consiste à créer une balise spécifique pour chaque instance, puis à créer une déclaration qui leur permet de gérer les instances avec cette balise. Pour plus d'informations, consultez Utiliser des instances.

Ressources

- AMIs
- Types d'instances
- Sous-réseaux
- EBSVolumes
- Balises
- Balises dans un modèle de lancement
- Élastique GPUs
- Modèles de lancement

AMIs

La politique suivante permet aux utilisateurs de lancer des instances en utilisant uniquement les paramètres spécifiésAMIs, `ami-9e1670f7` et`ami-45cf5c3c`. Les utilisateurs ne peuvent pas lancer une instance en utilisant un autre AMIs (sauf si une autre instruction les autorise à le faire).

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region::image/ami-9e1670f7",
        "arn:aws:ec2:region::image/ami-45cf5c3c",
        "arn:aws:ec2:region:account-id:instance/*",
        "arn:aws:ec2:region:account-id:volume/*",
        "arn:aws:ec2:region:account-id:key-pair/*",
        "arn:aws:ec2:region:account-id:security-group/*",
        "arn:aws:ec2:region:account-id:subnet/*",
        "arn:aws:ec2:region:account-id:network-interface/*"
      ]
    }
   ]
}
```

La politique suivante permet également aux utilisateurs de lancer des instances provenant de toutes les instances AMIs détenues par Amazon ou par certains partenaires fiables et vérifiés. L'élément `Condition` de la première déclaration+ teste si `ec2:Owner` est `amazon`. Les utilisateurs ne peuvent pas lancer une instance en utilisant un autre AMIs (sauf si une autre instruction les autorise à le faire).

```
{
   "Version": "2012-10-17",
   "Statement": [
         {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:Owner": "amazon"
         }
      }
   },
   {
```

```
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:instance/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
         ]
      }
   ]
}
```

Types d'instances

La stratégie suivante permet aux utilisateurs de lancer des instances uniquement à l'aide du type d'instance `t2.micro` ou `t2.small`, ce que vous pourriez faire pour contrôler les coûts. Les utilisateurs ne peuvent pas lancer d'instances plus grandes parce que l'élément `Condition` de la première déclaration teste si `ec2:InstanceType` est `t2.micro` ou `t2.small`.

```
{
   "Version": "2012-10-17",
   "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
```

```
            "arn:aws:ec2:region:account-id:volume/*",
            "arn:aws:ec2:region:account-id:key-pair/*",
            "arn:aws:ec2:region:account-id:security-group/*"
            ]
        }
    ]
}
```

Vous pouvez également créer une stratégie qui refuse aux utilisateurs l'autorisation de lancer des instances, à l'exception des types d'instance `t2.micro` et `t2.small`.

```
{
   "Version": "2012-10-17",
   "Statement": [
        {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
         "StringNotEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:instance/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
         ]
      }
   ]
}
```

Sous-réseaux

La stratégie suivante permet aux utilisateurs de lancer les instances en n'utilisant que le sous-réseau spécifié, `subnet-12345678`. Le groupe ne peut pas lancer d'instance sur un autre sous-réseau (à moins qu'une autre déclaration n'accorde aux utilisateurs l'autorisation de le faire).

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region:account-id:subnet/subnet-12345678",
        "arn:aws:ec2:region:account-id:network-interface/*",
        "arn:aws:ec2:region:account-id:instance/*",
        "arn:aws:ec2:region:account-id:volume/*",
        "arn:aws:ec2:region::image/ami-*",
        "arn:aws:ec2:region:account-id:key-pair/*",
        "arn:aws:ec2:region:account-id:security-group/*"
      ]
    }
   ]
}
```

Vous pouvez également créer une politique qui refuse aux utilisateurs l'autorisation de lancer une instance sur un autre sous-réseau. La déclaration agit ainsi en refusant l'autorisation de créer une interface réseau, à l'exception de l'emplacement où le sous-réseau `subnet-12345678` est spécifié. Ce refus se substitue à toute autre politique créée pour autoriser le lancement d'instances sur d'autres sous-réseaux.

```
{
   "Version": "2012-10-17",
   "Statement": [
         {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:network-interface/*"
      ],
      "Condition": {
         "ArnNotEquals": {
```

```
            "ec2:Subnet": "arn:aws:ec2:region:account-id:subnet/subnet-12345678"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:instance/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
         ]
      }
   ]
}
```

EBSVolumes

La politique suivante permet aux utilisateurs de lancer des instances uniquement si les EBS volumes de l'instance sont chiffrés. L'utilisateur doit lancer une instance à partir d'une AMI instance créée avec des instantanés chiffrés, afin de s'assurer que le volume racine est chiffré. N'importe quel volume supplémentaire que l'utilisateur attache à l'instance pendant le lancement doit aussi être chiffré.

```
{
    "Version": "2012-10-17",
    "Statement": [
                {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "Bool": {
                    "ec2:Encrypted": "true"
                }
            }
        },
        {
```

```
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:key-pair/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
        }
    ]
}
```

Balises

Baliser les instances lors de la création

La politique suivante permet aux utilisateurs de lancer des instances et d'attribuer des balises aux instances lors de la création. Pour les actions de création de ressources qui appliquent des balises, les utilisateurs doivent être autorisés à effectuer l'action `CreateTags`. La deuxième déclaration utilise la clé de condition `ec2:CreateAction` pour permettre aux utilisateurs de créer des balises uniquement dans le cadre de `RunInstances` et uniquement pour des instances. Les utilisateurs ne peuvent pas attribuer de balises aux ressources existantes, et ils ne peuvent pas attribuer de balises aux volumes à l'aide de la demande `RunInstances`.

Pour plus d'informations, consultez Accorder l'autorisation de baliser les EC2 ressources Amazon lors de la création.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
            "ec2:CreateTags"
         ],
         "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
         "Condition": {
            "StringEquals": {
                "ec2:CreateAction" : "RunInstances"
             }
          }
      }
   ]
}
```

Baliser des instances et des volumes lors de la création avec des balises spécifiques

La stratégie suivante inclut la clé de condition `aws:RequestTag` qui exige aux utilisateurs d'attribuer des balises aux instances et aux volumes créés par `RunInstances` avec les balises `environment=production` et `purpose=webserver`. Si les utilisateurs ne transmettent pas ces balises spécifiques ou s'ils ne spécifient pas du tout de balises, la demande échoue.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
         "arn:aws:ec2:region::image/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:security-group/*",
         "arn:aws:ec2:region:account-id:key-pair/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
          "arn:aws:ec2:region:account-id:volume/*",
          "arn:aws:ec2:region:account-id:instance/*"
```

```
      ],
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/environment": "production" ,
             "aws:RequestTag/purpose": "webserver"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Baliser des instances et des volumes lors de la création avec au moins une balise spécifique

La stratégie suivante utilise le modificateur `ForAnyValue` sur la condition `aws:TagKeys` pour indiquer qu'au moins une balise doit être spécifiée dans la demande, et elle doit comporter la clé `environment` ou `webserver`. La balise doit être appliquée à la fois aux instances et aux volumes. Toutes les valeurs de balise peuvent être spécifiées dans la demande.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
         "arn:aws:ec2:region::image/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:security-group/*",
```

```
            "arn:aws:ec2:region:account-id:key-pair/*"
        ]
      },
      {
        "Effect": "Allow",
        "Action": [
            "ec2:RunInstances"
        ],
        "Resource": [
            "arn:aws:ec2:region:account-id:volume/*",
            "arn:aws:ec2:region:account-id:instance/*"
        ],
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": ["environment","webserver"]
            }
         }
      },
      {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags"
        ],
        "Resource": "arn:aws:ec2:region:account-id:*/*",
        "Condition": {
            "StringEquals": {
                "ec2:CreateAction" : "RunInstances"
            }
         }
      }
    ]
}
```

Si les instances sont balisées lors de la création, elles doivent être balisées avec une balise spécifique

Dans la stratégie suivante, les utilisateurs ne doivent pas spécifier les balises dans la demande, mais s'ils le font, la balise doit être `purpose=test`. Aucune autre balise n'est autorisée. Les utilisateurs peuvent appliquer des balises à n'importe quelle ressource pouvant être balisée dans la demande `RunInstances`.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/purpose": "test",
             "ec2:CreateAction" : "RunInstances"
          },
          "ForAllValues:StringEquals": {
              "aws:TagKeys": "purpose"
          }
       }
    }
  ]
}
```

Pour interdire à toute personne appelée tag sur Create for RunInstances

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
```

```
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

N'autoriser que des balises spécifiques pour spot-instances-request. Incohérence surprise numéro 2 entre en jeu ici. Dans des circonstances normales, si vous ne spécifiez aucune balise, vous n'êtes pas authentifié. Dans ce cas spot-instances-request, cette politique ne sera pas évaluée s'il n'y a pas de spot-instances-request balises, de sorte qu'une demande Spot on Run sans étiquette sera acceptée.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
            ]
        },
        {
            "Sid": "VisualEditor0",
```

```
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        }
    ]
}
```

Balises dans un modèle de lancement

Dans l'exemple suivant, les utilisateurs peuvent lancer des instances, mais uniquement s'ils utilisent un modèle de lancement spécifique (`lt-09477bcd97b0d310e`). La clé de condition `ec2:IsLaunchTemplateResource` empêche les utilisateurs de remplacer les ressources spécifiées dans le modèle de lancement. La seconde partie de la déclaration permet aux utilisateurs de baliser les instances à la création. Cette partie de la déclaration est nécessaire si des balises sont spécifiées pour l'instance dans le modèle de lancement.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/
lt-09477bcd97b0d310e"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
```

```
      "Resource": "arn:aws:ec2:region:account-id:instance/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Élastique GPUs

Dans la politique suivante, les utilisateurs peuvent lancer une instance et spécifier un élastique GPU à attacher à l'instance. Les utilisateurs peuvent lancer des instances dans n'importe quelle région, mais ils ne peuvent attacher un élastique que GPU lors d'un lancement dans la `us-east-2` région.

La clé de `ec2:ElasticGpuType` condition garantit que les instances utilisent le type `eg1.medium` ou le GPU type `eg1.large` élastique.

```
{
    "Version": "2012-10-17",
    "Statement": [
             {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:account-id:elastic-gpu/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-2",
                    "ec2:ElasticGpuType": [
                        "eg1.medium",
                        "eg1.large"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
```

```
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:account-id:network-interface/*",
                "arn:aws:ec2:*:account-id:instance/*",
                "arn:aws:ec2:*:account-id:subnet/*",
                "arn:aws:ec2:*:account-id:volume/*",
                "arn:aws:ec2:*:account-id:key-pair/*",
                "arn:aws:ec2:*:account-id:security-group/*"
            ]
        }
    ]
}
```

Modèles de lancement

Dans l'exemple suivant, les utilisateurs peuvent lancer des instances, mais uniquement s'ils utilisent un modèle de lancement spécifique (`lt-09477bcd97b0d310e`). Les utilisateurs peuvent remplacer des paramètres dans le modèle de lancement en spécifiant dans l'action `RunInstances`.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/
lt-09477bcd97b0d310e"
          }
       }
    }
  ]
}
```

Dans cet exemple, les utilisateurs peuvent lancer des instances uniquement s'ils utilisent un modèle de lancement. La politique utilise la clé de `ec2:IsLaunchTemplateResource` condition pour empêcher les utilisateurs de remplacer tout élément préexistant ARNs dans le modèle de lancement.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    }
  ]
}
```

Dans l'exemple suivant, une politique permet aux utilisateurs de lancer des instances, mais uniquement s'ils utilisent un modèle de lancement. Les utilisateurs ne peuvent pas remplacer les paramètres du sous-réseau et de l'interface réseau dans la demande ; ceux-ci ne peuvent être spécifiés que dans le modèle de lancement. La première partie de l'instruction utilise l'NotResourceélément pour autoriser toutes les autres ressources à l'exception des sous-réseaux et des interfaces réseau. La seconde partie de la déclaration autorise les ressources des sous-réseaux et des interfaces réseau, mais uniquement si elles proviennent du modèle de lancement.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": ["arn:aws:ec2:region:account-id:subnet/*",
                      "arn:aws:ec2:region:account-id:network-interface/*" ],
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          }
       }
    },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
```

```
      "Resource": ["arn:aws:ec2:region:account-id:subnet/*",
                   "arn:aws:ec2:region:account-id:network-interface/*" ],
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    }
  ]
}
```

Dans l'exemple suivant, les utilisateurs sont autorisés à lancer des instances uniquement s'ils utilisent un modèle de lancement et seulement si celui-ci contient la balise `Purpose=Webservers`. Les utilisateurs ne peuvent pas remplacer les paramètres de modèle de lancement dans l'action `RunInstances`.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          },
         "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
       "StringEquals": {
           "aws:ResourceTag/Purpose": "Webservers"
        }
```

```
        }
      }
  ]
}
```

Utiliser instances Spot

Vous pouvez utiliser cette RunInstances action pour créer des demandes d'instance Spot et étiqueter les demandes d'instance Spot lors de la création. La ressource à spécifier RunInstances est`spot-instances-request`.

La `spot-instances-request` ressource est évaluée dans la IAM politique comme suit :

- Si vous ne balisez pas une demande d'instance Spot lors de la création, Amazon EC2 n'évalue pas la `spot-instances-request` ressource dans la RunInstances déclaration.
- Si vous balisez une demande d'instance Spot lors de la création, Amazon EC2 évalue la `spot-instances-request` ressource dans le RunInstances relevé.

Par conséquent, pour la `spot-instances-request` ressource, les règles suivantes s'appliquent à la IAM politique :

- Si vous avez l' RunInstances habitude de créer une demande d'instance ponctuelle et que vous n'avez pas l'intention de baliser la demande d'instance ponctuelle lors de la création, vous n'avez pas besoin d'autoriser explicitement la `spot-instances-request` ressource ; l'appel aboutira.
- Si vous avez l' RunInstances habitude de créer une demande d'instance Spot et que vous avez l'intention de baliser la demande d'instance Spot lors de sa création, vous devez inclure la `spot-instances-request` ressource RunInstances dans l'instruction d'autorisation, sinon l'appel échouera.
- Si vous avez l' RunInstances habitude de créer une demande d'instance Spot et que vous avez l'intention de baliser la demande d'instance Spot lors de sa création, vous devez spécifier la `spot-instances-request` ressource ou le `*` caractère générique dans CreateTags l'instruction d'autorisation, sinon l'appel échouera.

Vous pouvez demander des instances Spot en utilisant RunInstances ou RequestSpotInstances. Les exemples de IAM politiques suivants s'appliquent uniquement lorsque vous demandez des instances Spot à l'aide de RunInstances.

Exemple : demandez des instances ponctuelles en utilisant RunInstances

La politique suivante permet aux utilisateurs de demander des instances Spot en utilisant l' RunInstances action. La `spot-instances-request` ressource, créée par RunInstances, demande des instances Spot.

> **Note**
>
> À utiliser RunInstances pour créer des demandes d'instance Spot, vous pouvez omettre `spot-instances-request` de la `Resource` liste si vous n'avez pas l'intention de baliser les demandes d'instance Spot lors de la création. Cela est dû au fait qu'Amazon EC2 n'évalue pas la `spot-instances-request` ressource dans la RunInstances déclaration si la demande d'instance Spot n'est pas balisée lors de la création.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        }
    ]
}
```

> **Warning**
>
> NOTSUPPORTED— Exemple : refuser aux utilisateurs l'autorisation de demander des instances Spot en utilisant RunInstances

La stratégie suivante n'est pas prise en charge pour la ressource `spot-instances-request`.

La politique suivante vise à donner aux utilisateurs l'autorisation de lancer instances à la demande, mais à refuser aux utilisateurs l'autorisation de demander instances Spot. La `spot-instances-request` ressource, créée par RunInstances, est la ressource qui demande les instances Spot. La deuxième déclaration vise à refuser l' RunInstances action pour la `spot-instances-request` ressource. Toutefois, cette condition n'est pas prise en charge car Amazon EC2 n'évalue pas la `spot-instances-request` ressource dans la RunInstances déclaration si la demande d'instance Spot n'est pas balisée lors de la création.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequests - NOT SUPPORTED - DO NOT USE!",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
        }
    ]
}
```

Exemple : étiquetez les demandes d'instance Spot lors de la création

La politique suivante permet aux utilisateurs de baliser toutes les ressources créées lors du lancement de l'instance. La première instruction permet RunInstances de créer les ressources listées. La `spot-instances-request` ressource, créée par RunInstances, est la ressource qui demande les instances Spot. La deuxième instruction fournit un caractère générique * pour permettre à toutes les ressources d'être balisées lorsqu'elles sont créées au lancement de l'instance.

> **Note**
>
> Si vous balisez une demande d'instance Spot lors de la création, Amazon EC2 évalue la `spot-instances-request` ressource dans le RunInstances relevé. Par conséquent, vous devez autoriser explicitement la `spot-instances-request` ressource pour l' RunInstances action, sinon l'appel échouera.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
```

```
}
```

Exemple : refuser l'étiquette lors de la création des demandes d'instance Spot

La politique suivante refuse aux utilisateurs l'autorisation de baliser les ressources créées lors du lancement de l'instance.

La première instruction permet RunInstances de créer les ressources listées. La `spot-instances-request` ressource, créée par RunInstances, est la ressource qui demande les instances Spot. La deuxième instruction fournit un caractère générique * pour refuser toutes les ressources en cours de balisage lorsqu'elles sont créées au lancement de l'instance. Si `spot-instances-request` ou toute autre ressource est étiquetée lors de la création, l' RunInstances appel échouera.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenyTagResources",
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Warning

NOTSUPPORTED— Exemple : autoriser la création d'une demande d'instance Spot uniquement si une balise spécifique lui est attribuée
La stratégie suivante n'est pas prise en charge pour la ressource `spot-instances-request`.
La politique suivante vise à accorder RunInstances l'autorisation de créer une demande d'instance Spot uniquement si la demande est étiquetée avec une balise spécifique.
La première instruction permet RunInstances de créer les ressources listées.
La deuxième instruction est destinée à accorder aux utilisateurs l'autorisation de créer une demande d'instance Spot uniquement si la demande a l'étiquette `environment=production`. Si cette condition est appliquée à d'autres ressources créées par RunInstances, le fait de ne pas spécifier de balises entraîne une `Unauthenticated` erreur. Toutefois, si aucune balise n'est spécifiée pour la demande d'instance Spot, Amazon EC2 n'évalue pas la `spot-instances-request` ressource dans la RunInstances déclaration, ce qui entraîne la création de demandes d'instance ponctuelle non étiquetées par RunInstances.
Notez que la spécification d'une autre balise `environment=production` entraîne une `Unauthenticated` erreur, car si un utilisateur balise une demande d'instance Spot, Amazon EC2 évalue la `spot-instances-request` ressource dans la RunInstances déclaration.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
```

```
        {
            "Sid": "RequestSpotInstancesOnlyIfTagIs_environment=production - NOT
 SUPPORTED - DO NOT USE!",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }

    ]
}
```

Exemple : refuser la création d'une demande d'instance Spot si une étiquette spécifique lui est attribuée

La politique suivante refuse RunInstances l'autorisation de créer une demande d'instance Spot si la demande est étiquetée avec`environment=production`.

La première instruction permet RunInstances de créer les ressources listées.

La deuxième instruction refuse aux utilisateurs l'autorisation de créer une demande d'instance Spot si la demande a l'étiquette `environment=production`. La spécification `environment=production` en tant que balise entraîne une erreur `Unauthenticated`. La spécification d'autres étiquettes ou l'absence d'étiquettes entraînera la création d'une demande d'instance Spot.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
```

```
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequests",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Exemple : Utiliser instances réservées

La politique suivante autorise les utilisateurs à afficher, modifier et acheter les instances réservées de votre compte.

Il n'est pas possible de définir des autorisations au niveau des ressources pour les instances réservées individuelles. Cette politique signifie que les utilisateurs ont accès à toutes les instances réservées du compte.

L'élément `Resource` utilise un caractère générique * pour indiquer que les utilisateurs peuvent spécifier toutes les ressources avec l'action. Dans ce cas, ils peuvent afficher et modifier toutes les Instances réservées du compte. Ils peuvent aussi acheter des instances réservées à l'aide des informations d'identification du compte. Le caractère générique * est également nécessaire dans les cas où l'APIaction ne prend pas en charge les autorisations au niveau des ressources.

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeReservedInstancesOfferings"
      ],
      "Resource": "*"
    }
   ]
}
```

Pour permettre aux utilisateurs d'afficher et de modifier les instances réservées de votre compte, mais pas d'acheter de nouvelles instances réservées.

```
{
  "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource": "*"
    }
  ]
}
```

Exemple : Baliser des ressources

La stratégie suivante permet aux utilisateurs d'utiliser l'action `CreateTags` pour appliquer des balises à une instance uniquement si la balise contient la clé `environment` et la valeur `production`. Aucune autre identification n'est autorisée et l'utilisateur ne peut pas étiqueter d'autres types de ressources.

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        }
    ]
}
```

La politique suivante permet aux utilisateurs d'attribuer des balises à n'importe quelle ressource pouvant être balisée qui possède déjà une balise avec une clé de `owner` et une valeur du nom d'utilisateur. En outre, les utilisateurs doivent spécifier une balise avec une clé de `anycompany:environment-type` et une valeur `test` ou `prod` dans la demande. Les utilisateurs peuvent spécifier des balises supplémentaires dans la demande.

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:*/*",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/anycompany:environment-type": ["test","prod"],
                    "aws:ResourceTag/owner": "${aws:username}"
                }
            }
        }
    ]
}
```

Vous pouvez créer une IAM politique qui permet aux utilisateurs de supprimer des balises spécifiques pour une ressource. Par exemple, la stratégie suivante permet aux utilisateurs de supprimer les balises pour un volume si les clés de balise spécifiées dans la demande sont `environment` ou `cost-center`. N'importe quelle valeur peut être spécifiée pour la balise, mais la clé de balise doit correspondre à l'une des clés spécifiées.

> **Note**
>
> Si vous supprimez une ressource, toutes les balises associées à celle-ci sont également supprimées. Les utilisateurs n'ont pas besoin d'être autorisés à effectuer l'action `ec2:DeleteTags` pour supprimer une ressource comportant des balises ; ils doivent seulement être autorisés à effectuer l'action de suppression.

```
{
  "Version": "2012-10-17",
  "Statement": [
       {
      "Effect": "Allow",
      "Action": "ec2:DeleteTags",
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment","cost-center"]
        }
      }
    }
  ]
}
```

Cette politique permet aux utilisateurs de supprimer uniquement la balise `environment=prod` sur n'importe quelle ressource et uniquement si la ressource porte déjà une balise avec une clé de `owner` et une valeur du nom d'utilisateur. Les utilisateurs ne peuvent pas supprimer d'autres balises pour une ressource.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/environment": "prod",
          "aws:ResourceTag/owner": "${aws:username}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment"]
        }
      }
    }
  ]
}
```

Exemple : Utiliser des rôles IAM

La politique suivante permet aux utilisateurs d'attacher, de remplacer et de détacher un IAM rôle aux instances dotées de cette balise`department=test`. Le remplacement ou le détachement d'un IAM rôle nécessite un ID d'association. Par conséquent, la politique autorise également les utilisateurs à utiliser l'`ec2:DescribeIamInstanceProfileAssociations`action.

Les utilisateurs doivent être autorisés à utiliser l'action `iam:PassRole` pour transmettre le rôle à l'instance.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department":"test"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeIamInstanceProfileAssociations",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/DevTeam*"
    }
  ]
}
```

La politique suivante permet aux utilisateurs d'attacher ou de remplacer un IAM rôle pour n'importe quelle instance. Les utilisateurs peuvent uniquement associer ou remplacer IAM des rôles dont le nom commence par`TestRole-`. Pour l'`iam:PassRole`action, assurez-vous de spécifier le nom du IAM rôle et non le profil de l'instance (si les noms sont différents). Pour plus d'informations, consultez Profils d'instance.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateIamInstanceProfile",
                "ec2:ReplaceIamInstanceProfileAssociation"
            ],
            "Resource": "*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeIamInstanceProfileAssociations",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/TestRole-*"
        }
    ]
}
```

Exemple : Utiliser des tables de routage

La politique suivante permet aux utilisateurs d'ajouter, de supprimer et de remplacer des itinéraires pour les tables de routage associées VPC `vpc-ec43eb89` uniquement à. Pour spécifier un VPC pour la clé de `ec2:Vpc` condition, vous devez spécifier l'intégralité ARN duVPC.

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteRoute",
                "ec2:CreateRoute",
                "ec2:ReplaceRoute"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-ec43eb89"
                }
            }
        }
    ]
}
```

Exemple : autoriser une instance spécifique à afficher les ressources d'autres AWS services

Voici un exemple de politique que vous pouvez associer à un IAM rôle. La politique permet à une instance de visualiser les ressources de différents AWS services. Il utilise la clé de condition `ec2:SourceInstanceARN` globale pour spécifier que l'instance à partir de laquelle la demande est faite doit être une instance`i-093452212644b0dd6`. Si le même IAM rôle est associé à une autre instance, celle-ci ne peut effectuer aucune de ces actions.

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVolumes",
                "s3:ListAllMyBuckets",
                "dynamodb:ListTables",
                "rds:DescribeDBInstances"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "ArnEquals": {
                    "ec2:SourceInstanceARN": "arn:aws:ec2:region:account-id:instance/
i-093452212644b0dd6"
                }
            }
        }
    ]
}
```

Exemple : Utiliser des modèles de lancement

La stratégie suivante permet aux utilisateurs de créer une version du modèle de lancement et de modifier un modèle de lancement, mais uniquement pour un modèle spécifique (`lt-09477bcd97b0d3abc`). Les utilisateurs ne peuvent pas utiliser d'autres modèles de lancement.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
   {
      "Action": [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/lt-09477bcd97b0d3abc"
    }
  ]
}
```

La stratégie suivante permet aux utilisateurs de supprimer un modèle de lancement et une version du modèle de lancement, sous réserve que le modèle de lancement contienne la balise `Purpose=Testing`.

```
{
  "Version": "2012-10-17",
  "Statement": [
       {
      "Action": [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Purpose": "Testing"
        }
      }
    }
  ]
}
```

Utiliser des métadonnées d'instance

Les politiques suivantes garantissent que les utilisateurs ne peuvent récupérer les métadonnées des instances qu'à l'aide de la version 2 (IMDSv2) du service de métadonnées d'instance. Vous pouvez combiner les quatre politiques suivantes en une seule politique avec quatre instructions. Lorsqu'elle est combinée en une seule politique, vous pouvez utiliser la politique en tant que politique de contrôle des services (SCP). Elle peut fonctionner aussi bien comme politique de refus que vous appliquez à

une IAM politique existante (suppression et limitation des autorisations existantes) SCP que comme politique appliquée globalement à un compte, à une unité organisationnelle (UO) ou à l'ensemble d'une organisation.

> **Note**
>
> Les politiques d'options de RunInstances métadonnées suivantes doivent être utilisées conjointement avec une politique qui donne les autorisations principales pour lancer une instance RunInstances. Si le principal ne dispose pas également d' RunInstances autorisations, il ne sera pas en mesure de lancer une instance. Pour plus d'informations, consultez les stratégies dans Utiliser des instances et Instances de lancement (RunInstances).

> **Important**
>
> Si vous utilisez des groupes Auto Scaling et que vous devez en exiger l'utilisation IMDSv2 sur toutes les nouvelles instances, vos groupes Auto Scaling doivent utiliser des modèles de lancement.
> Lorsqu'un groupe Auto Scaling utilise un modèle de lancement, les `ec2:RunInstances` autorisations du IAM principal sont vérifiées lorsqu'un nouveau groupe Auto Scaling est créé. Elles sont également vérifiées lorsqu'un groupe Auto Scaling existant est mis à jour pour utiliser un nouveau modèle de lancement ou une nouvelle version d'un modèle de lancement. Les restrictions relatives à l'utilisation de IMDSv1 on IAM principals pour ne `RunInstances` sont vérifiées que lorsqu'un groupe Auto Scaling utilisant un modèle de lancement est créé ou mis à jour. Pour un groupe Auto Scaling configuré pour utiliser le modèle de lancement `Latest` ou `Default`, les autorisations ne sont pas vérifiées lors de la création d'une nouvelle version du modèle de lancement. Pour que les autorisations soient vérifiées, vous devez configurer le groupe Auto Scaling pour qu'il utilise une version spécifique du modèle de lancement.
>
> Pour imposer l'utilisation des instances IMDSv2 lancées par les groupes Auto Scaling, les étapes supplémentaires suivantes sont requises :
>
> 1. Désactivez l'utilisation de configurations de lancement pour tous les comptes de votre organisation en utilisant des politiques de contrôle des services (SCPs) ou des limites d'IAMautorisations pour les nouveaux principaux créés. Pour les IAM directeurs existants disposant d'autorisations de groupe Auto Scaling, mettez à jour leurs politiques associées

avec cette clé de condition. Pour désactiver l'utilisation des configurations de lancement, créez ou modifiez la limite d'autorisation ou la IAM politique pertinente SCP à l'aide de la clé de `"autoscaling:LaunchConfigurationName"` condition dont la valeur est spécifiée comme`null`.

2. Pour les nouveaux modèles de lancement, configurez les options de métadonnées d'instance dans le modèle de lancement. Pour les modèles de lancement existants, créez une nouvelle version du modèle de lancement et configurez les options de métadonnées d'instance dans la nouvelle version.
3. Dans la politique donnant à tout principal l'autorisation d'utiliser un modèle de lancement, restreignez l'association de `$latest` et de `$default` en spécifiant `"autoscaling:LaunchTemplateVersionSpecified": "true"`. En restreignant l'utilisation à une version spécifique d'un modèle de lancement, vous pouvez vous assurer que les nouvelles instances seront lancées à l'aide de la version dans laquelle les options de métadonnées d'instance sont configurées. Pour plus d'informations, consultez LaunchTemplateSpecificationl'Amazon EC2 Auto Scaling API Reference, en particulier le `Version` paramètre.
4. Pour un groupe Auto Scaling qui utilise une configuration de lancement, remplacez la configuration de lancement par un modèle de lancement. Pour plus d'informations, consultez la section Remplacer une configuration de lancement par un modèle de lancement dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.
5. Pour un groupe Auto Scaling qui utilise un modèle de lancement, assurez-vous qu'il utilise un nouveau modèle de lancement avec les options de métadonnées d'instance configurées ou qu'il utilise une nouvelle version du modèle de lancement actuel avec les options de métadonnées d'instance configurées. Pour plus d'informations, consultez update-auto-scaling-group le manuel de référence des AWS CLI commandes.

Exemples

- Exigence d'utilisation d'IMDSv2
- Refuser le désabonnement de IMDSv2
- Spécification d'une durée de vie (hop limit) maximale
- Restriction des personnes habilitées à modifier les options de métadonnées d'instance
- Exiger que les informations d'identification du rôle soient extraites de IMDSv2

Exigence d'utilisation d'IMDSv2

La politique suivante précise que vous ne pouvez pas appeler le RunInstances API à moins que l'instance ne soit également activée pour exiger l'utilisation de IMDSv2 (indiquée par`"ec2:MetadataHttpTokens": "required"`). Si vous ne spécifiez pas que l'instance l'exigeIMDSv2, une `UnauthorizedOperation` erreur s'affiche lorsque vous appelez le RunInstances API.

```
{
    "Version": "2012-10-17",
    "Statement": [
               {
            "Sid": "RequireImdsV2",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringNotEquals": {
                    "ec2:MetadataHttpTokens": "required"
                }
            }
        }
    ]
}
```

Refuser le désabonnement de IMDSv2

La politique suivante indique que vous ne pouvez pas appeler `ModifyInstanceMetadataOptions` API et autoriser l'option IMDSv1 ouIMDSv2. Si vous appelez le `ModifyInstanceMetadataOptions`API, l'`HttpTokens`attribut doit être défini sur`required`.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "DenyIMDSv1HttpTokensModification",
        "Effect": "Deny",
        "Action": "ec2:ModifyInstanceMetadataOptions",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:Attribute/HttpTokens": "required"
            },
```

```
            "Null": {
                "ec2:Attribute/HttpTokens": false
            }
        }
    }]
}
```

Spécification d'une durée de vie (hop limit) maximale

La politique suivante indique que vous ne pouvez pas appeler le RunInstances API sauf si vous spécifiez également une limite de sauts, et la limite de sauts ne peut pas être supérieure à 3. Si vous ne le faites pas, vous obtenez un `Unauthorized0peration` message d'erreur lorsque vous appelez le RunInstances API.

```
{
    "Version": "2012-10-17",
    "Statement": [
               {
            "Sid": "MaxImdsHopLimit",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "NumericGreaterThan": {
                    "ec2:MetadataHttpPutResponseHopLimit": "3"
                }
            }
        }
    ]
}
```

Restriction des personnes habilitées à modifier les options de métadonnées d'instance

La politique suivante permet uniquement aux utilisateurs ayant le rôle `ec2-imds-admins` d'apporter des modifications aux options de métadonnées de l'instance. Si un principal autre que le `ec2-imds-admins` rôle essaie d'appeler le ModifyInstanceMetadataOptions API, il obtiendra une `Unauthorized0peration` erreur. Cette instruction peut être utilisée pour contrôler l'utilisation du ModifyInstanceMetadataOptions API ; il n'existe actuellement aucun contrôle d'accès précis (conditions) pour le. ModifyInstanceMetadataOptions API

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
               {
            "Sid": "AllowOnlyImdsAdminsToModifySettings",
            "Effect": "Deny",
            "Action": "ec2:ModifyInstanceMetadataOptions",
            "Resource": "*",
            "Condition": {
                "StringNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/ec2-imds-admins"
                }
            }
        }
    ]
}
```

Exiger que les informations d'identification du rôle soient extraites de IMDSv2

La politique suivante précise que si cette politique est appliquée à un rôle, que le rôle est assumé par le EC2 service et que les informations d'identification obtenues sont utilisées pour signer une demande, la demande doit être signée à l'aide des informations d'identification de EC2 rôle extraitesIMDSv2. Sinon, tous ses API appels recevront un `UnauthorizedOperation` message d'erreur. Cette déclaration/politique peut être appliquée de manière générale car, si la demande n'est pas signée par les informations d'identification du EC2 rôle, elle n'a aucun effet.

```
{
    "Version": "2012-10-17",
    "Statement": [
               {
            "Sid": "RequireAllEc2RolesToUseV2",
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "NumericLessThan": {
                    "ec2:RoleDelivery": "2.0"
                }
            }
        }
    ]
}
```

Travaillez avec les EBS volumes et les instantanés Amazon

Pour des exemples de politiques relatives à l'utilisation des EBS volumes et des instantanés Amazon, consultez la section Exemples de politiques basées sur l'identité pour Amazon. EBS

Exemples de politiques pour contrôler l'accès à la EC2 console Amazon

Vous pouvez utiliser IAM des politiques pour accorder aux utilisateurs les autorisations nécessaires pour travailler avec AmazonEC2. Pour obtenir des step-by-step instructions, reportez-vous à la section Création IAM de politiques dans le guide de IAM l'utilisateur.

La console utilise des API actions supplémentaires pour ses fonctionnalités, de sorte que ces politiques risquent de ne pas fonctionner comme prévu. Par exemple, un utilisateur autorisé à utiliser uniquement l'`DescribeVolumes`APIaction rencontrera des erreurs lorsqu'il essaiera d'afficher des volumes dans la console. Cette section illustre les politiques qui permettent aux utilisateurs d'utiliser des parties spécifiques de la console. Pour plus d'informations sur la création de politiques pour la EC2 console Amazon, consultez le billet de blog sur la AWS sécurité suivant : Octroyer aux utilisateurs l'autorisation de travailler dans la EC2 console Amazon.

Les exemples suivants présentent des déclarations de politique que vous pouvez utiliser pour accorder aux utilisateurs l'autorisation d'utiliser AmazonEC2. Remplacez chacun *`user input placeholder`* avec vos propres informations. Ces politiques sont conçues pour les demandes effectuées à l'aide du AWS Management Console. La EC2 console Amazon peut lancer plusieurs API actions pour afficher une seule ressource, et cela peut ne pas être évident tant que l'utilisateur n'a pas tenté une tâche et que la console n'a pas affiché une erreur. Pour plus d'informations, consultez le billet de blog sur la AWS sécurité suivant : Octroyer aux utilisateurs l'autorisation de travailler dans la EC2 console Amazon.

Exemples

- Exemple : accès en lecture seule
- Exemple : utilisation de l'assistant de EC2 lancement d'instance
- Exemple : Utiliser des groupes de sécurité
- Exemple : Utiliser des adresses IP Elastic
- Exemple : Utiliser instances réservées

Pour vous aider à déterminer les API actions requises pour effectuer des tâches dans la console, vous pouvez utiliser un service qui enregistre les appels, tel que AWS CloudTrail. Si votre politique

n'accorde pas l'autorisation de créer ou de modifier une ressource spécifique, la console affiche un message codé avec les informations de diagnostic. Vous pouvez décoder le message à l'aide de l'DecodeAuthorizationMessageAPIaction pour AWS STS ou de la decode-authorization-messagecommande contenue dans le AWS CLI.

Exemple : accès en lecture seule

Pour permettre aux utilisateurs de consulter toutes les ressources de la EC2 console Amazon, vous pouvez utiliser la même politique que dans l'exemple suivant :Exemple : accès en lecture seule. Les utilisateurs ne peuvent pas exécuter d'actions sur ces ressources ou créer des ressources, à moins qu'une autre déclaration ne leur accorde l'autorisation de le faire.

Afficher les instances et AMIs les instantanés

Vous pouvez aussi fournir un accès en lecture seule à un sous-ensemble de ressources. Pour ce faire, remplacez le caractère générique * dans l'`ec2:Describe`APIaction par des `ec2:Describe` actions spécifiques pour chaque ressource. La politique suivante permet aux utilisateurs de visualiser toutes les instances et tous AMIs les instantanés dans la EC2 console Amazon. L'`ec2:DescribeTags`action permet aux utilisateurs de consulter le publicAMIs. La console a besoin des informations de balisage pour être affichées en public AMIs ; vous pouvez toutefois supprimer cette action pour permettre aux utilisateurs de n'afficher que les informations privéesAMIs.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeTags",
         "ec2:DescribeSnapshots"
      ],
      "Resource": "*"
   }
   ]
}
```

> **Note**
>
> Les EC2 `ec2:Describe*` API actions Amazon ne prennent pas en charge les autorisations au niveau des ressources. Vous ne pouvez donc pas contrôler les ressources individuelles

que les utilisateurs peuvent consulter dans la console. Par conséquent, le caractère générique * est nécessaire dans l'élément `Resource` de la déclaration ci-dessus. Pour plus d'informations sur les actions ARNs que vous pouvez utiliser avec quelles EC2 API actions Amazon, consultez Actions, ressources et clés de condition pour Amazon EC2.

Afficher les instances et CloudWatch les métriques

La politique suivante permet aux utilisateurs de consulter les instances dans la EC2 console Amazon, ainsi que les CloudWatch alarmes et les métriques dans l'onglet Surveillance de la page Instances. La EC2 console Amazon utilise le CloudWatch API pour afficher les alarmes et les métriques. Vous devez donc autoriser les utilisateurs à utiliser les `cloudwatch:GetMetricData` actions `cloudwatch:DescribeAlarms` `cloudwatch:DescribeAlarmsForMetriccloudwatch:ListMetrics`,`cloudwatch:GetMetricStat` et.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeInstanceTypes",
         "cloudwatch:DescribeAlarms",
         "cloudwatch:DescribeAlarmsForMetric",
         "cloudwatch:ListMetrics",
         "cloudwatch:GetMetricStatistics",
         "cloudwatch:GetMetricData"
      ],
      "Resource": "*"
   }
   ]
}
```

Exemple : utilisation de l'assistant de EC2 lancement d'instance

L'assistant de EC2 lancement d'instance Amazon est un écran proposant des options permettant de configurer et de lancer une instance. Votre politique doit inclure l'autorisation d'utiliser les API actions qui permettent aux utilisateurs d'utiliser les options de l'assistant. Si votre politique n'inclut

pas l'autorisation d'utiliser ces actions, certains éléments de l'Assistant ne peuvent pas se charger correctement et les utilisateurs ne peuvent pas exécuter de lancement.

Accès de base à l'assistant de lancement d'instances

Pour réussir un lancement, les utilisateurs doivent être autorisés à utiliser l'`ec2:RunInstances`APIaction, et au moins les API actions suivantes :

- `ec2:DescribeImages`: Pour afficher et sélectionner unAMI.
- `ec2:DescribeInstanceTypes` : afficher et sélectionner un type d'instance.
- `ec2:DescribeVpcs` : afficher les options réseau disponibles.
- `ec2:DescribeSubnets`: pour afficher tous les sous-réseaux disponibles pour le sous-réseau choisiVPC.
- `ec2:DescribeSecurityGroups` ou `ec2:CreateSecurityGroup` : pour afficher et sélectionner un groupe de sécurité existant, ou en créer un nouveau.
- `ec2:DescribeKeyPairs` ou `ec2:CreateKeyPair` : pour sélectionner une paire de clés existante ou en créer une nouvelle.
- `ec2:AuthorizeSecurityGroupIngress` : ajouter des règles entrantes.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateSecurityGroup",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateKeyPair"
            ],
            "Resource": "*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "*"
        }
    ]
}
```

Vous pouvez ajouter API des actions à votre politique afin d'offrir davantage d'options aux utilisateurs, par exemple :

- `ec2:DescribeAvailabilityZones` : afficher et sélectionner une zone de disponibilité spécifique.
- `ec2:DescribeNetworkInterfaces` : afficher et sélectionner les interfaces réseau existantes pour le sous-réseau sélectionné.
- Pour ajouter des règles de sortie aux groupes VPC de sécurité, les utilisateurs doivent être autorisés à utiliser l'`ec2:AuthorizeSecurityGroupEgress`APIaction. Pour modifier ou supprimer des règles existantes, les utilisateurs doivent être autorisés à utiliser l'`ec2:RevokeSecurityGroup*`APIaction correspondante.
- `ec2:CreateTags` : Pour attribuer des balises aux ressources qui sont créées par `RunInstances`. Pour plus d'informations, consultez Accorder l'autorisation de baliser les EC2 ressources Amazon lors de la création. Si les utilisateurs n'ont pas l'autorisation d'utiliser cette action et qu'ils essaient d'appliquer des balises sur la page de balisage de l'assistant de lancement d'instances, le lancement échoue.

  > **Important**
  >
  > La spécification d'un Name (Nom) lors du lancement d'une instance crée une balise et nécessite l'action `ec2:CreateTags`. Veillez à accorder aux utilisateurs l'autorisation d'utiliser l'action `ec2:CreateTags`, car cela limite votre capacité à utiliser la clé de condition `aws:ResourceTag` pour restreindre leur utilisation d'autres ressources. Si vous accordez aux utilisateurs l'autorisation d'utiliser l'action `ec2:CreateTags`, ils peuvent modifier la balise d'une ressource afin de contourner ces restrictions. Pour plus d'informations, consultez Contrôlez l'accès à l'aide de l'accès basé sur les attributs.

- Pour utiliser les paramètres de Systems Manager lors de la sélection d'unAMI, vous devez ajouter `ssm:DescribeParameters` et `ssm:GetParameters` à votre politique. `ssm:DescribeParameters`accorde à vos utilisateurs l'autorisation de visualiser et de sélectionner les paramètres de Systems Manager. `ssm:GetParameters`accorde à vos

utilisateurs l'autorisation d'obtenir les valeurs des paramètres de Systems Manager. Vous pouvez également restreindre l'accès à des paramètres Systems Manager spécifiques. Pour plus d'informations, consultez Restreindre l'accès à des paramètres Systems Manager spécifiques plus loin dans cette section.

Actuellement, les EC2 `Describe*` API actions Amazon ne prennent pas en charge les autorisations au niveau des ressources. Vous ne pouvez donc pas restreindre les ressources individuelles que les utilisateurs peuvent consulter dans l'assistant de lancement d'instance. Toutefois, vous pouvez appliquer des autorisations au niveau des ressources à l'`ec2:RunInstances`APIaction afin de limiter les ressources que les utilisateurs peuvent utiliser pour lancer une instance. Le lancement échoue si les utilisateurs sélectionnent des options qu'ils ne sont pas autorisés à utiliser.

Limiter l'accès à un type d'instance, un sous-réseau et une région spécifiques

La politique suivante permet aux utilisateurs de lancer `t2.micro` des instances en utilisant AMIs Owned by Amazon, et uniquement dans un sous-réseau spécifique (`subnet-1a2b3c4d`). Les utilisateurs ne peuvent lancer que dans la région spécifiée. Si les utilisateurs sélectionnent une autre région, un autre type d'instance ou un autre sous-réseau dans l'assistant de lancement d'instance, le lancement échoue. AMI

La première instruction accorde aux utilisateurs l'autorisation d'afficher les options dans l'assistant de lancement d'instances ou d'en créer de nouvelles, comme illustré dans l'exemple ci-dessus. La deuxième déclaration autorise les utilisateurs à utiliser l'interface réseau, le volume, la paire de clés, le groupe de sécurité et les ressources de sous-réseau pour l'`ec2:RunInstances`action, qui sont nécessaires pour lancer une instance dans unVPC. Pour plus d'informations sur l'utilisation de l'action `ec2:RunInstances`, consultez Instances de lancement (RunInstances). Les troisième et quatrième déclarations accordent aux utilisateurs l'autorisation d'utiliser respectivement l'instance et les AMI ressources, mais uniquement si l'`t2.micro`instance est une instance, et uniquement si elle appartient à Amazon ou à certains partenaires fiables et vérifiés. AMI

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeInstanceTypes",
         "ec2:DescribeKeyPairs",
```

```
            "ec2:CreateKeyPair",
            "ec2:DescribeVpcs",
            "ec2:DescribeSubnets", "ec2:DescribeSecurityGroups",
            "ec2:CreateSecurityGroup",
            "ec2:AuthorizeSecurityGroupIngress"
        ],
        "Resource": "*"
        },
        {
           "Effect": "Allow",
           "Action":"ec2:RunInstances",
           "Resource": [
              "arn:aws:ec2:region:111122223333:network-interface/*",
              "arn:aws:ec2:region:111122223333:volume/*",
              "arn:aws:ec2:region:111122223333:key-pair/*",
              "arn:aws:ec2:region:111122223333:security-group/*",
              "arn:aws:ec2:region:111122223333:subnet/subnet-1a2b3c4d"
           ]
        },
        {
           "Effect": "Allow",
           "Action": "ec2:RunInstances",
           "Resource": [
              "arn:aws:ec2:region:111122223333:instance/*"
           ],
           "Condition": {
              "StringEquals": {
                 "ec2:InstanceType": "t2.micro"
              }
           }
        },
        {
           "Effect": "Allow",
           "Action": "ec2:RunInstances",
           "Resource": [
                 "arn:aws:ec2:region::image/ami-*"
           ],
           "Condition": {
              "StringEquals": {
                 "ec2:Owner": "amazon"
              }
           }
        }
        ]
```

```
}
```

Restreindre l'accès à des paramètres Systems Manager spécifiques

La politique suivante accorde l'accès à l'utilisation des paramètres Systems Manager avec un nom spécifique.

La première instruction autorise les utilisateurs à consulter les paramètres de Systems Manager lorsqu'ils sélectionnent un AMI assistant de lancement d'instance. La deuxième instruction accorde aux utilisateurs l'autorisation d'utiliser uniquement les paramètres nommés `prod-*`.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ssm:DescribeParameters"
      ],
      "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action": [
         "ssm:GetParameters"
      ],
     "Resource": "arn:aws:ssm:region:123456123456:parameter/prod-*"
   }
   ]
}
```

Exemple : Utiliser des groupes de sécurité

Afficher les groupes de sécurité et ajouter ou supprimer des règles

La politique suivante autorise les utilisateurs à consulter les groupes de sécurité dans la EC2 console Amazon, à ajouter et à supprimer des règles entrantes et sortantes, et à répertorier et modifier les descriptions des règles pour les groupes de sécurité existants dotés de cette balise. `Department=Test`

Dans la première déclaration, l'action `ec2:DescribeTags` permet aux utilisateurs d'afficher les balises sur la console, ce qui permet aux utilisateurs d'identifier plus facilement les groupes de sécurité qu'ils sont autorisés à modifier.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeSecurityGroups",
         "ec2:DescribeSecurityGroupRules",
         "ec2:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:AuthorizeSecurityGroupIngress",
         "ec2:RevokeSecurityGroupIngress",
         "ec2:AuthorizeSecurityGroupEgress",
         "ec2:RevokeSecurityGroupEgress",
         "ec2:ModifySecurityGroupRules",
         "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
         "ec2:UpdateSecurityGroupRuleDescriptionsEgress"
      ],
      "Resource": [
         "arn:aws:ec2:region:111122223333:security-group/*"
      ],
      "Condition": {
         "StringEquals": {
            "aws:ResourceTag/Department": "Test"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": [
         "ec2:ModifySecurityGroupRules"
      ],
      "Resource": [
         "arn:aws:ec2:region:111122223333:security-group-rule/*"
      ]
   }
]}
```

Utiliser la boîte de dialogue Créer un groupe de sécurité

Vous pouvez créer une politique qui permet aux utilisateurs de travailler avec la boîte de dialogue Create Security Group de la EC2 console Amazon. Pour utiliser cette boîte de dialogue, les utilisateurs doivent être autorisés à effectuer au moins les API actions suivantes :

- `ec2:CreateSecurityGroup` : créer un groupe de sécurité.
- `ec2:DescribeVpcs`: pour afficher la liste des éléments existants VPCs dans la VPCliste.

Avec ces autorisations, les utilisateurs peuvent créer un groupe de sécurité avec succès, mais ne peuvent pas lui ajouter de règles. Pour utiliser les règles de la boîte de dialogue Créer un groupe de sécurité, vous pouvez ajouter les API actions suivantes à votre politique :

- `ec2:AuthorizeSecurityGroupIngress` : ajouter des règles entrantes.
- `ec2:AuthorizeSecurityGroupEgress`: pour ajouter des règles de sortie aux groupes VPC de sécurité.
- `ec2:RevokeSecurityGroupIngress` : modifier ou supprimer des règles entrantes existantes. Cette règle est utile pour permettre aux utilisateurs d'utiliser la fonction Copier vers le nouveau sur la console. Cette fonction ouvre la boîte de dialogue Créer un groupe de sécurité et la complète avec les mêmes règles que le groupe de sécurité sélectionné.
- `ec2:RevokeSecurityGroupEgress`: pour modifier ou supprimer les règles de sortie pour les groupes VPC de sécurité. Cette règle permet aux utilisateurs de modifier ou de supprimer la règle sortante par défaut qui autorise tout le trafic sortant.
- `ec2:DeleteSecurityGroup` : répondre lorsque les règles non valides ne peuvent pas être enregistrées. La console commence par créer le groupe de sécurité et ajoute ensuite les règles spécifiées. Si les règles ne sont pas valides, l'action échoue et la console tente de supprimer le groupe de sécurité. Comme la boîte de dialogue Créer un groupe de sécurité reste affichée, l'utilisateur peut corriger la règle non valide et essayer de recréer le groupe de sécurité. Cette API action n'est pas obligatoire, mais si un utilisateur n'est pas autorisé à l'utiliser et tente de créer un groupe de sécurité avec des règles non valides, le groupe de sécurité est créé sans aucune règle et l'utilisateur doit les ajouter par la suite.
- `ec2:UpdateSecurityGroupRuleDescriptionsIngress` : pour ajouter ou mettre à jour des descriptions des règles de trafic entrant pour les groupes de sécurité.
- `ec2:UpdateSecurityGroupRuleDescriptionsEgress` : pour ajouter ou mettre à jour des descriptions des règles de trafic sortant pour les groupes de sécurité.
- `ec2:ModifySecurityGroupRules` : pour modifier les règles de groupe de sécurité.
- `ec2:DescribeSecurityGroupRules` : pour répertorier les règles de groupe de sécurité.

La politique suivante autorise les utilisateurs à utiliser la boîte de dialogue Créer un groupe de sécurité et à créer des règles entrantes et sortantes pour les groupes de sécurité associés à un groupe de sécurité spécifique VPC ()`vpc-1a2b3c4d`. Les utilisateurs peuvent créer des groupes de sécurité pour unVPC, mais ils ne peuvent y ajouter aucune règle. De même, les utilisateurs ne peuvent pas ajouter de règles à un groupe de sécurité existant auquel il n'est pas associé VPC`vpc-1a2b3c4d`. Les utilisateurs reçoivent aussi l'autorisation d'afficher tous les groupes de sécurité sur la console. Les utilisateurs peuvent ainsi identifier plus facilement les groupes de sécurité auxquels ils peuvent ajouter des règles entrantes. Cette politique autorise également les utilisateurs à supprimer les groupes de sécurité associés à VPC`vpc-1a2b3c4d`.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSecurityGroups",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource": "arn:aws:ec2:region:111122223333:security-group/*",
      "Condition":{
         "ArnEquals": {
            "ec2:Vpc": "arn:aws:ec2:region:111122223333:vpc/vpc-1a2b3c4d"
         }
      }
    }
   ]
}
```

Exemple : Utiliser des adresses IP Elastic

Pour permettre aux utilisateurs de consulter les adresses IP élastiques dans la EC2 console Amazon, vous devez autoriser les utilisateurs à utiliser l'`ec2:DescribeAddresses`action.

Pour autoriser les utilisateurs à utiliser les adresses IP Elastic, vous pouvez ajouter les actions suivantes à votre politique.

- `ec2:AllocateAddress` : allouer une adresse IP Elastic.
- `ec2:ReleaseAddress`: libérer une adresse IP Elastic.
- `ec2:AssociateAddress` : associer une adresse IP Elastic à une instance ou une interface réseau.
- `ec2:DescribeNetworkInterfaces` et `ec2:DescribeInstances` : utiliser l'écran Associer l'adresse. Cet écran affiche les instances ou interfaces réseau disponibles auxquelles vous pouvez associer une adresse IP Elastic.
- `ec2:DisassociateAddress` : dissocier une adresse IP Elastic d'une instance ou d'une interface réseau.

La politique suivante permet aux utilisateurs d'afficher, d'allouer et d'associer des adresses IP Elastic pour les instances. Les utilisateurs ne peuvent pas associer des adresses IP Elastic à des interfaces réseau, dissocier des adresses IP Elastic ou en libérer.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAddresses",
                "ec2:AllocateAddress",
                "ec2:DescribeInstances",
                "ec2:AssociateAddress"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemple : Utiliser instances réservées

La politique suivante permet aux utilisateurs d'afficher et de modifier les instances réservées de votre compte, ainsi que d'acheter de nouvelles instances réservées dans la AWS Management Console.

Cette politique permet aux utilisateurs d'afficher tous les instances réservées, ainsi que instances à la demande, dans le compte. Il n'est pas possible de définir des autorisations au niveau des ressources pour les instances réservées individuelles.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeReservedInstances",
         "ec2:ModifyReservedInstances",
         "ec2:PurchaseReservedInstancesOffering",
         "ec2:DescribeInstances",
         "ec2:DescribeInstanceTypes",
         "ec2:DescribeAvailabilityZones",
         "ec2:DescribeReservedInstancesOfferings"
      ],
      "Resource": "*"
   }
   ]
}
```

Cette `ec2:DescribeAvailabilityZones` action est nécessaire pour garantir que la EC2 console Amazon puisse afficher des informations sur les zones de disponibilité dans lesquelles vous pouvez acheter des instances réservées. L'action `ec2:DescribeInstances` n'est pas obligatoire, mais garantit que l'utilisateur peut afficher les instances du compte et acheter des réservations pour correspondre aux spécifications exactes.

Vous pouvez ajuster les API actions pour limiter l'accès des utilisateurs, par exemple en supprimant `ec2:DescribeInstances` et en donnant `ec2:DescribeAvailabilityZones` à l'utilisateur un accès en lecture seule.

AWS politiques gérées pour Amazon EC2

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de les rédiger vous-même. Il faut du temps et de l'expertise pour créer

des politiques gérées par les IAM clients qui fournissent à votre équipe uniquement les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques AWS gérées. Ces politiques couvrent les cas d'utilisation courants et sont disponibles dans votre AWS compte. Pour plus d'informations sur les politiques AWS gérées, voir les politiques AWS gérées dans le Guide de IAM l'utilisateur.

AWS les services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent occasionnellement des autorisations à une politique gérée par AWS pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont très susceptibles de mettre à jour une politique gérée par AWS quand une nouvelle fonctionnalité est lancée ou quand de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique ReadOnlyAccess AWS gérée fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité, il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir une liste et une description des politiques relatives aux fonctions de travail, voir les politiques AWS gérées pour les fonctions de travail dans le Guide de IAM l'utilisateur.

AWS politique gérée : AmazonEC2FullAccess

Vous pouvez associer la `AmazonEC2FullAccess` politique à votre IAM identité. Cette politique accorde des autorisations permettant un accès complet à AmazonEC2.

Pour consulter les autorisations associées à cette politique, reportez-vous AmazonEC2FullAccessà la référence des politiques AWS gérées.

AWS politique gérée : AmazonEC2ReadOnlyAccess

Vous pouvez associer la `AmazonEC2ReadOnlyAccess` politique à votre IAM identité. Cette politique accorde des autorisations permettant un accès en lecture seule à Amazon. EC2

Pour consulter les autorisations associées à cette politique, reportez-vous AmazonEC2ReadOnlyAccessà la référence des politiques AWS gérées.

AWS politique gérée : AWSEC2CapacityReservationFleetRolePolicy

Cette politique est attachée au rôle lié à un service intitulé AWSServiceRoleForEC2CapacityReservationFleet pour autoriser les réserves de capacité à créer, à modifier et à annuler des réserves de capacité en votre nom. Pour plus d'informations, veuillez consulter la rubrique Rôle lié à un service pour la flotte de réserve de capacité.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSEC2CapacityReservationFleetRolePolicyà la référence des politiques AWS gérées.

AWS politique gérée : AWSEC2FleetServiceRolePolicy

Cette politique est attachée au rôle lié au service nommé AWSServiceRoleForEC2Fleetpour permettre à EC2 Fleet de demander, lancer, résilier et étiqueter des instances en votre nom. Pour plus d'informations, consultez Rôle lié au service pour Fleet EC2.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSEC2FleetServiceRolePolicyà la référence des politiques AWS gérées.

AWS politique gérée : AWSEC2SpotFleetServiceRolePolicy

Cette politique est attachée au rôle lié à un service nommé AWSServiceRoleForEC2SpotFleet pour permettre à la flotte EC2 de lancer et de gérer des instances en votre nom. Pour plus d'informations, consultez Rôle lié à un service pour un parc d'instances Spot .

Pour consulter les autorisations associées à cette politique, reportez-vous AWSEC2SpotFleetServiceRolePolicyà la référence des politiques AWS gérées.

AWS politique gérée : AWSEC2SpotServiceRolePolicy

Cette politique est associée au rôle lié au service nommé AWSServiceRoleForEC2Spotpour permettre à Amazon de lancer et EC2 de gérer des instances Spot en votre nom. Pour plus d'informations, consultez Rôle lié à un service pour les demandes d'instance Spot.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSEC2SpotServiceRolePolicyà la référence des politiques AWS gérées.

AWS politique gérée : AWSEC2VssSnapshotPolicy

Vous pouvez associer cette politique gérée au rôle de profil d'IAMinstance que vous utilisez pour vos instances Amazon EC2 Windows. La politique accorde des autorisations permettant à Amazon EC2 de créer et de gérer des VSS instantanés en votre nom.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSEC2VssSnapshotPolicyà la référence des politiques AWS gérées.

AWS politique gérée : EC2FastLaunchFullAccess

Vous pouvez associer la `EC2FastLaunchFullAccess` politique à votre profil d'instance ou à IAM un autre rôle. Cette politique accorde un accès complet aux actions EC2 Fast Launch et des autorisations ciblées comme suit.

Détails de l'autorisation

- EC2Lancement rapide : l'accès administratif est accordé afin que le rôle puisse activer ou désactiver le lancement EC2 rapide et décrire les images de lancement EC2 rapide.
- Amazon EC2 — L'accès est accordé à Amazon EC2 RunInstances, CreateTags et décrivez les actions nécessaires pour vérifier les autorisations relatives aux ressources.
- IAM— L'accès est accordé pour obtenir et utiliser des profils d'instance dont le nom contient `ec2fastlaunch` pour créer le rôle EC2FastLaunchServiceRolePolicy lié au service.

Pour consulter les autorisations associées à cette politique, reportez-vous EC2FastLaunchFullAccessà la référence des politiques AWS gérées.

AWS politique gérée : EC2FastLaunchServiceRolePolicy

Cette politique est associée au rôle lié au service nommé AWSServiceRoleForEC2FastLaunchpour permettre à Amazon EC2 de créer et de gérer un ensemble de snapshots préconfigurés afin de réduire le temps nécessaire au lancement des instances depuis votre application Fast Launch activée. EC2 AMI Pour plus d'informations, consultez the section called "Rôle lié à un service".

Pour consulter les autorisations associées à cette politique, reportez-vous EC2FastLaunchServiceRolePolicyà la référence des politiques AWS gérées.

AWS politique gérée : Ec2InstanceConnectEndpoint

Cette politique est attachée à un rôle lié à un service nommé AWSServiceRoleForEC2InstanceConnectpour permettre à Instance EC2 Connect Endpoint d'effectuer des actions en votre nom. Pour plus d'informations, consultez Rôle lié à un service pour Instance EC2 Connect Endpoint.

Pour consulter les autorisations associées à cette politique, reportez-vous Ec2InstanceConnectEndpointà la référence des politiques AWS gérées.

Amazon EC2 met à jour AWS ses politiques gérées

Consultez les informations relatives aux mises à jour des politiques AWS gérées pour Amazon EC2 depuis que ce service a commencé à suivre ces modifications.

Modification	Description	Date
EC2FastLaunchFullAccess : nouvelle politique	Amazon EC2 a ajouté cette politique pour effectuer des API actions liées à la fonctionn alité de lancement EC2 rapide à partir d'une instance. La politique peut être attachée au profil d'instance pour une instance lancée à partir d'un lancement EC2 rapide activéAMI.	14 mai 2024
AWSEC2VssSnapshotPolicy : nouvelle politique	Amazon EC2 a ajouté une `AWSEC2VssSnapshotP olicy` politique qui contient des autorisations permettan t de créer et d'ajouter des balises à Amazon Machine Images (AMIs) et aux EBS instantanés.	28 mars 2024
EC2FastLaunchServi ceRolePolicy : nouvelle politique	Amazon EC2 a ajouté la fonctionnalité EC2 Fast Launch pour permettre AMIs à Windows de lancer des instances plus rapidement en créant un ensemble de snapshots préconfigurés.	26 novembre 2021
Amazon EC2 a commencé à suivre les modifications	Amazon EC2 a commencé à suivre les modifications	1er mars 2021

Modification	Description	Date
	apportées à ses politiques AWS gérées	

IAMrôles pour Amazon EC2

Les candidatures doivent signer leurs API demandes avec des AWS informations d'identification. Par conséquent, si vous êtes développeur d'applications, vous avez besoin d'une stratégie pour gérer les informations d'identification de vos applications qui s'exécutent sur EC2 des instances. Par exemple, vous pouvez distribuer en toute sécurité vos informations d'identification AWS aux instances, en permettant ainsi aux applications de ces instances d'utiliser vos informations d'identification pour signer des demandes, tout en les protégeant des autres utilisateurs. Cependant, il est difficile de distribuer en toute sécurité les informations d'identification à chaque instance, en particulier celles AWS créées en votre nom, telles que les instances Spot ou les instances de groupes Auto Scaling. Vous devez également être en mesure de mettre à jour les informations d'identification sur chaque instance lorsque vous effectuez une rotation de vos AWS informations d'identification.

Nous avons conçu IAM des rôles pour que vos applications puissent envoyer des API demandes en toute sécurité à partir de vos instances, sans que vous ayez à gérer les informations d'identification de sécurité utilisées par les applications. Au lieu de créer et de distribuer vos AWS informations d'identification, vous pouvez déléguer l'autorisation de faire des API demandes en utilisant IAM les rôles suivants :

1. Créez un IAM rôle.
2. Définissez quels comptes ou AWS services peuvent assumer le rôle.
3. Définissez les API actions et les ressources que l'application peut utiliser après avoir assumé le rôle.
4. Spécifiez le rôle au lancement de votre instance ou attachez-le à une instance existante.
5. Demandez à l'application d'extraire un ensemble d'informations d'identification temporaires et utilisez-les.

Par exemple, vous pouvez utiliser IAM des rôles pour accorder des autorisations aux applications exécutées sur vos instances qui doivent utiliser un compartiment dans Amazon S3. Vous pouvez spécifier des autorisations pour IAM les rôles en créant une politique au JSON format. Ces politiques

sont similaires à celles que vous créez pour les utilisateurs . Si vous modifiez un rôle, la modification est répercutée sur toutes les instances.

> **Note**
>
> Les informations d'identification du EC2 IAM rôle Amazon ne sont pas soumises à la durée maximale de session configurée dans le rôle. Pour plus d'informations, consultez la section Utilisation IAM des rôles dans le Guide de IAM l'utilisateur.

Lorsque vous créez IAM des rôles, associez des IAM politiques de moindre privilège qui limitent l'accès aux API appels spécifiques requis par l'application. Pour la communication Windows vers Windows, utilisez des groupes et des rôles Windows bien définis et bien documentés pour accorder un accès au niveau de l'application entre les instances Windows. Les groupes et les rôles permettent aux clients de définir les autorisations au NTFS niveau des applications et des dossiers avec le moindre privilège afin de limiter l'accès aux exigences spécifiques à l'application.

Vous ne pouvez associer qu'un seul IAM rôle à une instance, mais vous pouvez associer le même rôle à de nombreuses instances. Pour plus d'informations sur la création et l'utilisation IAM des rôles, consultez la section Rôles du guide de IAM l'utilisateur.

Vous pouvez appliquer des autorisations au niveau des ressources à vos IAM politiques afin de contrôler la capacité des utilisateurs à associer, remplacer ou détacher IAM des rôles pour une instance. Pour plus d'informations, consultez Autorisations prises en charge au niveau des ressources pour les actions Amazon EC2 API et l'exemple suivant : Exemple : Utiliser des rôles IAM.

Sommaire

Profils d'instance

Amazon EC2 utilise un profil d'instance comme conteneur pour un IAM rôle. Lorsque vous créez un IAM rôle à l'aide de la IAM console, celle-ci crée automatiquement un profil d'instance et lui donne le même nom que le rôle auquel il correspond. Si vous utilisez la EC2 console Amazon pour lancer une instance dotée d'un IAM rôle ou pour associer un IAM rôle à une instance, vous choisissez le rôle en fonction d'une liste de noms de profils d'instance.

Si vous utilisez le AWS CLI API, ou an AWS SDK pour créer un rôle, vous créez le rôle et le profil d'instance en tant qu'actions distinctes, avec des noms potentiellement différents. Si vous utilisez ensuite le AWS CLI API, ou an AWS SDK pour lancer une instance avec un IAM rôle ou pour attacher un IAM rôle à une instance, spécifiez le nom du profil de l'instance.

Un profil d'instance ne peut contenir qu'un seul IAM rôle. Cette limite ne peut pas être augmentée.

Pour plus d'informations, consultez la section Profils d'instance dans le guide de IAM l'utilisateur.

Autorisations pour votre cas d'utilisation

Lorsque vous créez un IAM rôle pour vos applications pour la première fois, vous pouvez parfois accorder des autorisations allant au-delà de ce qui est requis. Avant de lancer votre application dans votre environnement de production, vous pouvez générer une IAM politique basée sur l'activité d'accès à un IAM rôle. IAMAccess Analyzer examine vos AWS CloudTrail journaux et génère un modèle de politique contenant les autorisations utilisées par le rôle dans la plage de dates que vous avez spécifiée. Vous pouvez utiliser le modèle pour créer une politique gérée avec des autorisations détaillées, puis l'associer au IAM rôle. Ainsi, vous n'accordez que les autorisations dont le rôle a besoin pour interagir avec les AWS ressources correspondant à votre cas d'utilisation spécifique. Cela vous permet de mieux respecter la bonne pratique qui consiste à appliquer le principe du moindre privilège. Pour plus d'informations, consultez la section Génération de politiques IAM Access Analyzer dans le guide de l'IAMutilisateur.

Extraire les informations d'identification de sécurité à partir des métadonnées d'instance

Une application de l'instance extrait les informations d'identification de sécurité fournies par le rôle à partir de l'élément `iam/security-credentials/`nom-rôle des métadonnées d'instance. L'application reçoit les autorisations pour les actions et les ressources que vous avez définies pour le rôle via les informations d'identification de sécurité associées au rôle. Ces informations de sécurité sont temporaires et nous les faisons tourner automatiquement. Nous rendons disponibles

de nouvelles informations d'identification au moins cinq minutes avant l'expiration des anciennes informations d'identification.

Pour obtenir plus d'informations sur les métadonnées d'instance, consultez Utiliser les métadonnées de l'instance pour gérer votre EC2 instance.

> **Warning**
>
> Si vous utilisez des services qui utilisent des métadonnées d'instance avec IAM des rôles, veillez à ne pas exposer vos informations d'identification lorsque les services passent des HTTP appels en votre nom. Les types de services susceptibles d'exposer vos informations d'identification incluent HTTP les proxys, les services HTML de CSS validation et les XML processeurs qui prennent en charge XML l'inclusion.

Pour vos EC2 charges de travail Amazon, nous vous recommandons de récupérer les informations d'identification de session en utilisant la méthode décrite ci-dessous. Ces informations d'identification devraient permettre à votre charge de travail de faire des AWS API demandes, sans avoir `sts:AssumeRole` à les utiliser pour assumer le même rôle que celui déjà associé à l'instance. À moins que vous n'ayez besoin de transmettre des balises de session pour le contrôle d'accès basé sur les attributs (ABAC) ou d'adopter une politique de session pour restreindre davantage les autorisations du rôle, ces appels d'attribution de rôle ne sont pas nécessaires car ils créent un nouvel ensemble d'informations d'identification de session de rôle temporaires identiques.

Si votre charge de travail utilise un rôle pour s'assumer elle-même, vous devez créer une politique de confiance qui autorise explicitement ce rôle à s'assumer lui-même. Si vous ne créez pas la politique de confiance, une `AccessDenied` erreur s'affiche. Pour plus d'informations, consultez la section Modification d'une politique d'approbation des rôles dans le Guide de IAM l'utilisateur.

La commande suivante permet de récupérer les informations d'identification de sécurité pour un IAM rôle nommés`3access`.

cURL

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/iam/security-credentials/s3access
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-
credentials/s3access
```

PowerShell

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/security-
credentials/s3access
```

Voici un exemple de sortie. Si vous ne parvenez pas à récupérer les informations de sécurité, consultez la section Je ne peux pas accéder aux informations d'identification de sécurité temporaires de mon EC2 instance dans le guide de IAM l'utilisateur.

```
{
  "Code" : "Success",
  "LastUpdated" : "2012-04-26T16:39:16Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAIOSFODNN7EXAMPLE",
  "SecretAccessKey" : "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
  "Token" : "token",
  "Expiration" : "2017-05-17T15:09:54Z"
}
```

Pour les applications et PowerShell les commandes Tools for Windows qui s'exécutent sur l'instance, il n'est pas nécessaire d'obtenir explicitement les informations d'identification de sécurité temporaires : AWS SDKs et Tools for Windows obtiennent PowerShell automatiquement les informations d'identification auprès du service de métadonnées de l'EC2instance et les utilisent. AWS CLI AWS CLI Pour passer un appel en dehors de l'instance à l'aide d'informations d'identification

de sécurité temporaires (par exemple, pour tester des IAM politiques), vous devez fournir la clé d'accès, la clé secrète et le jeton de session. Pour plus d'informations, consultez la section Utilisation d'informations d'identification de sécurité temporaires pour demander l'accès aux AWS ressources dans le guide de IAM l'utilisateur.

Accorder des autorisations pour attacher un IAM rôle à une instance

Vos identités Compte AWS, telles que IAM les utilisateurs, doivent disposer d'autorisations spécifiques pour lancer une EC2 instance Amazon avec un IAM rôle, attacher un IAM rôle à une instance, remplacer le IAM rôle par une instance ou détacher un IAM rôle d'une instance. Vous devez autoriser l'utilisation des API actions suivantes selon les besoins :

- `iam:PassRole`
- `ec2:AssociateIamInstanceProfile`
- `ec2:DisassociateIamInstanceProfile`
- `ec2:ReplaceIamInstanceProfileAssociation`

> **Note**
>
> Si vous spécifiez la ressource pour `iam:PassRole` as`*`, cela vous accordera l'accès pour transmettre n'importe lequel de vos IAM rôles à une instance. Pour suivre la meilleure pratique du moindre privilège, spécifiez les ARNs IAM rôles spécifiques avec`iam:PassRole`, comme indiqué dans l'exemple de politique ci-dessous.

Exemple de politique d'accès programmatique

La IAM politique suivante autorise le lancement d'instances dotées d'un IAM rôle, l'attachement d'un IAM rôle à une instance ou le remplacement du IAM rôle par une instance à l'aide de AWS CLI ou d'Amazon EC2API.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances",
         "ec2:AssociateIamInstanceProfile",
```

```
            "ec2:DisassociateIamInstanceProfile",
            "ec2:ReplaceIamInstanceProfileAssociation"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::123456789012:role/DevTeam*"
    }
  ]
}
```

Exigence supplémentaire pour l'accès à la console

Pour accorder l'autorisation d'effectuer les mêmes tâches à l'aide de la EC2 console Amazon, vous devez également inclure l'`iam:ListInstanceProfiles`APIaction.

Attacher un IAM rôle à une instance

Vous pouvez créer un IAM rôle et l'associer à une instance pendant ou après le lancement. Vous pouvez également remplacer ou détacher IAM des rôles.

Pour associer un IAM rôle à une instance lors du lancement à l'aide de la EC2 console Amazon, consultez la section Détails avancés. Pour le profil de l'IAMinstance, sélectionnez le IAM rôle.

> **Note**
>
> Si vous avez créé votre IAM rôle à l'aide de la IAM console, le profil d'instance a été créé pour vous et porte le même nom que le rôle. Si vous avez créé votre IAM rôle en utilisant le AWS CLI API, ou un AWS SDK, vous avez peut-être donné à votre profil d'instance un nom différent de celui du rôle.

Vous pouvez associer un IAM rôle à une instance en cours d'exécution ou arrêtée. Si un IAM rôle est déjà attaché à l'instance, vous devez le remplacer par le nouveau IAM rôle.

Console

Pour associer un IAM rôle à une instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance.
4. Choisissez Actions, Sécurité, Modifier IAM le rôle.
5. Pour IAMle rôle, sélectionnez le profil d'IAMinstance.
6. Choisissez Mettre à jour IAM le rôle.

AWS CLI

Pour associer un IAM rôle à une instance

Utilisez la associate-iam-instance-profilecommande pour attacher le IAM rôle à l'instance. Lorsque vous spécifiez le profil d'instance, vous pouvez utiliser soit le nom de ressource Amazon (ARN) du profil d'instance, soit son nom.

```
aws ec2 associate-iam-instance-profile \
    --instance-id i-1234567890abcdef0 \
    --iam-instance-profile Name="TestRole-1"
```

Voici un exemple de sortie.

```
{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-1234567890abcdef0",
        "State": "associating",
        "AssociationId": "iip-assoc-0dbd8529a48294120",
        "IamInstanceProfile": {
            "Id": "AIPAJLNLDX3AMYZNWYYAY",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-1"
        }
    }
}
```

PowerShell

Pour associer un IAM rôle à une instance

- Get-EC2Instance
- Register-EC2IamInstanceProfile

Pour remplacer le IAM rôle sur une instance à laquelle un IAM rôle est déjà attaché, l'instance doit être dans l'`running`état. Vous pouvez le faire si vous souhaitez modifier le IAM rôle d'une instance sans détacher au préalable le rôle existant. Par exemple, vous pouvez le faire pour vous assurer que API les actions effectuées par les applications exécutées sur l'instance ne sont pas interrompues.

Console

Pour remplacer un IAM rôle par une instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance.
4. Choisissez Actions, Sécurité, Modifier IAM le rôle.
5. Pour IAMle rôle, sélectionnez le profil d'IAMinstance.
6. Choisissez Mettre à jour IAM le rôle.

AWS CLI

Pour remplacer un IAM rôle par une instance

1. Si nécessaire, décrivez les associations de votre profil d'IAMinstance pour obtenir l'ID d'association du profil d'IAMinstance à remplacer.

```
aws ec2 describe-iam-instance-profile-associations
```

2. Utilisez la commande replace-iam-instance-profile-association pour remplacer le profil d'IAMinstance en spécifiant l'ID d'association pour le profil d'instance existant et le nom ARN ou du profil d'instance qui doit le remplacer.

```
aws ec2 replace-iam-instance-profile-association \
    --association-id iip-assoc-0044d817db6c0a4ba \
    --iam-instance-profile Name="TestRole-2"
```

Voici un exemple de sortie.

```
{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-087711ddaf98f9489",
```

```
        "State": "associating",
        "AssociationId": "iip-assoc-09654be48e33b91e0",
        "IamInstanceProfile": {
            "Id": "AIPAJCJEDKX7QYHWYK7GS",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
        }
    }
}
```

PowerShell

Pour remplacer un IAM rôle par une instance

- Get-EC2IamInstanceProfileAssociation
- Set-EC2IamInstanceProfileAssociation

Vous pouvez détacher un IAM rôle d'une instance en cours d'exécution ou arrêtée.

Console

Pour détacher un IAM rôle d'une instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance.
4. Choisissez Actions, Sécurité, Modifier IAM le rôle.
5. Dans le IAMchamp Rôle, sélectionnez Aucun IAM rôle.
6. Choisissez Mettre à jour IAM le rôle.
7. Lorsque vous êtes invité à confirmer, entrez Détacher, puis choisissez Détacher.

AWS CLI

Pour détacher un IAM rôle d'une instance

1. Si nécessaire, utilisez describe-iam-instance-profile-associations pour décrire les associations de votre profil d'IAMinstance et obtenir l'ID d'association du profil d'IAMinstance à détacher.

```
aws ec2 describe-iam-instance-profile-associations
```

Voici un exemple de sortie.

```
{
    "IamInstanceProfileAssociations": [
        {
            "InstanceId": "i-088ce778fbfeb4361",
            "State": "associated",
            "AssociationId": "iip-assoc-0044d817db6c0a4ba",
            "IamInstanceProfile": {
                "Id": "AIPAJEDNCAA64SSD265D6",
                "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
            }
        }
    ]
}
```

2. Utilisez la disassociate-iam-instance-profilecommande pour détacher le profil d'IAMinstance à l'aide de son ID d'association.

```
aws ec2 disassociate-iam-instance-profile --association-id iip-
assoc-0044d817db6c0a4ba
```

Voici un exemple de sortie.

```
{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-087711ddaf98f9489",
        "State": "disassociating",
        "AssociationId": "iip-assoc-0044d817db6c0a4ba",
        "IamInstanceProfile": {
            "Id": "AIPAJEDNCAA64SSD265D6",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
        }
    }
}
```

PowerShell

Pour détacher un IAM rôle d'une instance

- Get-EC2IamInstanceProfileAssociation
- Unregister-EC2IamInstanceProfile

Rôles d'identité d'instance pour les EC2 instances Amazon

Chaque EC2 instance Amazon que vous lancez possède un rôle d'identité d'instance qui représente son identité. Un rôle d'identité d'instance est un type de IAM rôle. AWS les services et fonctionnalités intégrés pour utiliser le rôle d'identité d'instance peuvent l'utiliser pour identifier l'instance auprès du service.

Les informations d'identification du rôle d'identité de l'instance sont accessibles depuis le service de métadonnées d'instance (IMDS) à l'adresse`/identity-credentials/ec2/security-credentials/ec2-instance`. Les informations d'identification se composent d'une paire de clés d'accès AWS temporaires et d'un jeton de session. Ils sont utilisés pour signer les demandes AWS Sigv4 adressées aux AWS services qui utilisent le rôle d'identité d'instance. Les informations d'identification sont présentes dans les métadonnées de l'instance, qu'un service ou une fonctionnalité utilisant les rôles d'identité d'instance soit activé ou non sur l'instance.

Les rôles d'identité d'instance sont automatiquement créés lors du lancement d'une instance, ne font l'objet d'aucun document de politique d'approbation des rôles et ne sont soumis à aucune politique d'identité ou de ressources.

Services pris en charge

Les AWS services suivants utilisent le rôle d'identité d'instance :

- Amazon EC2 — EC2Instance Connect utilise le rôle d'identité d'instance pour mettre à jour les clés d'hôte d'une instance Linux.
- Amazon GuardDuty — Runtime Monitoring utilise le rôle d'identité de l'instance pour permettre à l'agent d'exécution d'envoyer des données télémétriques de sécurité au GuardDuty VPC point de terminaison.
- AWS Security Token Service (AWS STS) — Les informations d'identification du rôle d'identité de l'instance peuvent être utilisées avec l' AWS STS `GetCallerIdentity`action.
- AWS Systems Manager— Lorsque vous utilisez la configuration de gestion d'hôte par défaut, AWS Systems Manager utilise l'identité fournie par le rôle d'identité d'instance pour

enregistrer EC2 les instances. Après avoir identifié votre instance, Systems Manager peut `AWSSystemsManagerDefaultEC2InstanceManagementRole` IAM lui transmettre votre rôle.

Les rôles d'identité d'instance ne peuvent pas être utilisés avec d'autres AWS services ou fonctionnalités car ils ne sont pas intégrés aux rôles d'identité d'instance.

Rôle d'identité de l'instance ARN

Le rôle d'identité de l'instance ARN prend le format suivant :

```
arn:aws-partition:iam::account-number:assumed-role/aws:ec2-instance/instance-id
```

Par exemple :

```
arn:aws:iam::0123456789012:assumed-role/aws:ec2-instance/i-0123456789example
```

Pour plus d'informationsARNs, consultez Amazon Resource Names (ARNs) dans le guide de IAM l'utilisateur.

Gestion des mises à jour pour les instances Amazon EC2 Windows

Nous vous recommandons de patcher, de mettre à jour et de sécuriser régulièrement le système d'exploitation et les applications de vos EC2 instances. Vous pouvez utiliser le Gestionnaire de correctifs AWS Systems Manager pour automatiser le processus d'installation des mises à jour de sécurité pour le système d'exploitation et les applications.

Pour les EC2 instances d'un groupe Auto Scaling, vous pouvez utiliser le AWS-PatchAsgInstancerunbook pour éviter le remplacement des instances soumises à des correctifs. Vous pouvez aussi utiliser n'importe quel service de mise à jour automatique ou processus recommandé pour l'installation des mises à jour fourni par le fournisseur de l'application.

Ressources

- AL2023 — Mise à jour de la AL2 version 023 dans le guide de l'utilisateur Amazon Linux 2023.
- AL2— Gérez le logiciel sur votre instance Amazon Linux 2 dans le guide de l'utilisateur Amazon Linux 2.
- Instances Windows —the section called "Gestion des mises à jour".

Bonnes pratiques de sécurité pour les instances Windows

Nous vous recommandons de suivre ces bonnes pratiques de sécurité pour vos instances Windows.

Table des matières

Bonnes pratiques de sécurité de haut niveau

Vous devez respecter les meilleures pratiques de sécurité de haut niveau suivantes pour vos instances Windows :

- Accès minimal : accordez l'accès uniquement aux systèmes et aux emplacements fiables et attendus. Cela s'applique à tous les produits Microsoft tels qu'Active Directory, les serveurs de productivité professionnels Microsoft et les services d'infrastructure tels que les services de bureau à distance, les serveurs proxy inverses, les serveurs IIS Web, etc. Utilisez AWS des fonctionnalités telles que les groupes de sécurité des EC2 instances Amazon, les listes de contrôle d'accès au réseau (ACLs) et les sous-réseaux VPC publics/privés Amazon pour renforcer la sécurité sur plusieurs sites d'une architecture. Au sein d'une instance Windows, les clients peuvent utiliser le pare-feu Windows pour renforcer defense-in-depth la stratégie de leur déploiement. Installez uniquement les composants du système d'exploitation et les applications nécessaires au fonctionnement du système aux fins pour lesquelles il a été conçu. Configurez les services d'infrastructure, par exemple IIS pour qu'ils s'exécutent sous des comptes de service ou pour utiliser des fonctionnalités telles que les identités des pools d'applications pour accéder aux ressources localement et à distance sur l'ensemble de votre infrastructure.
- Privilège minimal : déterminez l'ensemble minimal de privilèges dont les instances et les comptes ont besoin pour exécuter leurs fonctions. Restreindre ces serveurs et utilisateurs pour autoriser uniquement ces autorisations définies. Utilisez des techniques telles que les contrôles d'accès basés sur les rôles pour réduire la surface des comptes d'administration et créer les rôles les plus limités pour accomplir une tâche. Utilisez les fonctionnalités du système d'exploitation telles que le chiffrement du système de fichiers (EFS) NTFS pour chiffrer les données sensibles au repos et contrôler l'accès des applications et des utilisateurs à ces données.

- Gestion de la configuration : créez une configuration de serveur de base qui intègre des correctifs de up-to-date sécurité et des suites de protection basées sur l'hôte qui incluent un antivirus, un anti-malware, une détection/prévention des intrusions et une surveillance de l'intégrité des fichiers. Évaluez chaque serveur par rapport à la référence enregistrée actuelle pour identifier et signaler les écarts éventuels. Assurez-vous que chaque serveur est configuré pour générer et stocker en toute sécurité les données de journal et d'audit appropriées.
- Gestion des modifications : créez des processus pour contrôler les modifications apportées aux lignes de base de configuration des serveurs et optez pour des processus de modification entièrement automatisés. Tirez également parti de Just Enough Administration (JEA) avec Windows PowerShell DSC pour limiter l'accès administratif aux fonctions minimales requises.
- Gestion des correctifs : implémentez des processus qui corrigent, mettent à jour et sécurisent régulièrement le système d'exploitation et les applications de vos EC2 instances.
- Journaux d'audit : auditez l'accès et toutes les modifications apportées aux EC2 instances Amazon afin de vérifier l'intégrité du serveur et de vous assurer que seules les modifications autorisées sont apportées. Tirez parti de fonctionnalités telles que la journalisation améliorée IIS pour améliorer les fonctionnalités de journalisation par défaut. AWS des fonctionnalités telles que les journaux de VPC flux AWS CloudTrail sont également disponibles pour auditer l'accès au réseau, y compris les demandes et les API appels autorisés/refusés, respectivement.

Gestion des mises à jour

Pour garantir les meilleurs résultats lorsque vous exécutez Windows Server sur AmazonEC2, nous vous recommandons de mettre en œuvre les meilleures pratiques suivantes :

- Configure Windows Update
- Update drivers
- Use the latest Windows AMIs
- Test performance before migration
- Update launch agents
- Redémarrez votre instance Windows après avoir installé les mises à jour. Pour de plus amples informations, veuillez consulter Redémarrer votre instance.

Pour savoir comment mettre à niveau ou migrer une instance Windows vers une version plus récente de Windows Server, voir Mettre à niveau une instance EC2 Windows vers une version plus récente de Windows Server.

Configuration de Windows Update

Par défaut, les instances lancées depuis AWS Windows Server AMIs ne reçoivent pas de mises à jour via Windows Update.

Mettre à jour les pilotes Windows

Conservez les pilotes les plus récents sur toutes les EC2 instances Windows afin de garantir que les dernières corrections de problèmes et améliorations de performances sont appliquées à l'ensemble de votre parc. En fonction de votre type d'instance, vous devez mettre à jour le AWS PVENA, Amazon et AWS NVMe les pilotes.

- Utilisez SNSles rubriques pour recevoir des mises à jour concernant les nouvelles versions de pilotes.
- Utilisez le manuel AWS Systems Manager d'automatisation AWSSupport pour appliquer facilement UpgradeWindows AWSDrivers les mises à jour à toutes vos instances.

Lancer des instances à l'aide de la dernière version de Windows AMIs

AWS publie AMIs chaque mois un nouveau Windows, qui contient les derniers correctifs, pilotes et agents de lancement du système d'exploitation. Vous devez tirer parti des dernières nouveautés AMI lorsque vous lancez de nouvelles instances ou lorsque vous créez vos propres images personnalisées.

- Pour consulter les mises à jour de chaque version de AWS WindowsAMIs, consultez l'historique des AMI versions de AWS Windows.
- Pour créer avec la dernière version disponibleAMIs, voir Query for the Latest Windows AMI Using Systems Manager Parameter Store.
- Pour plus d'informations sur Windows spécialisé AMIs que vous pouvez utiliser pour lancer des instances pour votre base de données et sur les cas d'utilisation du renforcement de la conformité, consultez la section Windows spécialisés AMIs dans le Guide de AMIréférence AWS Windows.

Tester les performances du système/des applications avant la migration

La migration des applications d'entreprise vers AWS peut impliquer de nombreuses variables et configurations. Testez toujours les performances de la EC2 solution pour vous assurer que :

- Les types d'instances sont correctement configurés, y compris la taille des instances, la mise en réseau améliorée et la location (partagée ou dédiée).

- La topologie des instances est appropriée pour la charge de travail et exploite si nécessaire les fonctions hautes performances, telles que la location dédiée, les groupes de placement, les volumes de stockage d'instance et le matériel nu.

Mise à jour des agents de lancement

Passez à la dernière version de l'agent EC2Launch v2 pour vous assurer que les dernières améliorations sont appliquées à l'ensemble de votre flotte. Pour de plus amples informations, veuillez consulter the section called "Migrer vers la EC2Launch version v2".

Si vous disposez d'un parc mixte ou si vous souhaitez continuer à utiliser les agents EC2Launch (Windows Server 2016 et 2019) ou EC2 Config (ancien système d'exploitation uniquement), effectuez la mise à jour vers les dernières versions des agents respectifs.

Les mises à jour automatiques sont prises en charge sur les combinaisons suivantes de version de Windows Server et d'agents de lancement. Vous pouvez activer les mises à jour automatiques dans la console SSMQuick Setup Host Management sous Amazon EC2 Launch Agents.

Version Windows	EC2Launch v1	EC2Launch v2
2016	✓	✓
2019	✓	✓
2022		✓

- Pour plus d'informations sur la mise à jour vers la EC2Launch version v2, consultezthe section called "Installer la EC2Launch v2".
- Pour plus d'informations sur la mise à jour manuelleEC2Config, consultezthe section called "Installer EC2Config".
- Pour plus d'informations sur la mise à jour manuelleEC2Launch, consultezthe section called "Installer EC2Launch".

Gestion de la configuration

Amazon Machine Images (AMIs) fournit une configuration initiale pour une EC2 instance Amazon, qui inclut le système d'exploitation Windows et des personnalisations facultatives spécifiques au client,

telles que les applications et les contrôles de sécurité. Créez un AMI catalogue contenant des lignes de base de configuration de sécurité personnalisées pour garantir que toutes les instances Windows sont lancées avec des contrôles de sécurité standard. Les bases de sécurité peuvent être intégrées à unAMI, amorcées dynamiquement lors du lancement d'une EC2 instance, ou packagées sous forme de produit pour une distribution uniforme via les portefeuilles AWS Service Catalog. Pour plus d'informations sur la sécurisation d'unAMI, consultez Bonnes pratiques pour créer un AMI.

Chaque EC2 instance Amazon doit respecter les normes de sécurité de l'organisation. N'installez pas de rôles et de fonctionnalités Windows qui ne sont pas requis, et installez des logiciels pour vous protéger contre les codes malveillants (antivirus, antimalware, réduction de l'exploitation), surveiller l'intégrité de l'hôte et effectuer la détection des intrusions. Configurez le logiciel de sécurité pour surveiller et maintenir les paramètres de sécurité du système d'exploitation, protéger l'intégrité des fichiers critiques de ce dernier et signaler les écarts par rapport à la référence de sécurité. Envisagez de mettre en œuvre des tests de configuration de sécurité recommandés publiés par Microsoft, le Center for Internet Security (CIS) ou le National Institute of Standards and Technology (NIST). Envisagez d'utiliser d'autres outils Microsoft pour des serveurs d'applications spécifiques, tels que le Best Practice Analyzer for SQL Server.

AWS les clients peuvent également exécuter des évaluations Amazon Inspector afin d'améliorer la sécurité et la conformité des applications déployées sur des EC2 instances Amazon. Amazon Inspector évalue automatiquement les applications pour détecter les vulnérabilités ou les écarts par rapport aux meilleures pratiques et inclut une base de connaissances contenant des centaines de règles mappées selon les normes de sécurité communes (par exemple, PCIDSS) et des définitions de vulnérabilités. Les règles préintégrées prévoient, par exemple, la vérification de l'activation de la connexion distante à la racine ou la détection des versions de logiciels vulnérables installées. Ces règles sont régulièrement mises à jour par les chercheurs en AWS sécurité.

Lors de la sécurisation des instances Windows, nous vous recommandons d'implémenter les services de domaine Active Directory afin d'activer une infrastructure évolutive, sécurisée et gérable pour les emplacements distribués. En outre, après avoir lancé des instances depuis la EC2 console Amazon ou à l'aide d'un outil de EC2 provisionnement Amazon AWS CloudFormation, il est recommandé d'utiliser les fonctionnalités natives du système d'exploitation, telles que Microsoft Windows, PowerShell DSC pour maintenir l'état de la configuration en cas de dérive de configuration.

Gestion des modifications

Une fois que les bases de sécurité initiales ont été appliquées aux EC2 instances Amazon au lancement, contrôlez les EC2 modifications continues apportées par Amazon afin de garantir la

sécurité de vos machines virtuelles. Établissez un processus de gestion des modifications pour autoriser et intégrer les modifications apportées aux AWS ressources (telles que les groupes de sécurité, les tables de routage et le réseauACLs) ainsi qu'aux configurations du système d'exploitation et des applications (telles que Windows ou l'application de correctifs, les mises à niveau logicielles ou les mises à jour des fichiers de configuration).

AWS fournit plusieurs outils pour aider à gérer les modifications apportées aux AWS ressources AWS CloudTrail, notamment AWS Config, AWS CloudFormation, AWS Elastic Beanstalk AWS OpsWorks, et des packs d'administration pour Systems Center Operations Manager et System Center Virtual Machine Manager. Notez que Microsoft publie des correctifs Windows le deuxième mardi de chaque mois (ou selon les besoins) et AWS met à jour tous les systèmes Windows AMIs administrés dans les cinq jours AWS suivant la publication d'un correctif par Microsoft. Il est donc important de corriger en permanence toutes les configurations de référenceAMIs, de mettre à jour les AWS CloudFormation modèles et les configurations de groupe Auto Scaling avec les dernières nouveautés AMIIDs, et de mettre en œuvre des outils pour automatiser la gestion des correctifs d'instance en cours d'exécution.

Microsoft fournit plusieurs options pour gérer les modifications du système d'exploitation Windows et des applications. SCCM, par exemple, fournit une couverture complète du cycle de vie des modifications de l'environnement. Sélectionnez des outils qui répondent aux exigences de l'entreprise et contrôlent l'impact des modifications sur les applicationsSLAs, la capacité, la sécurité et les procédures de reprise après sinistre. Évitez les modifications manuelles et utilisez plutôt un logiciel de gestion de configuration automatisé ou des outils de ligne de commande tels que EC2 Run Command ou Windows PowerShell pour mettre en œuvre des processus de modification scriptés et répétables. Pour répondre à cette exigence, utilisez des hôtes bastion avec journalisation améliorée pour toutes les interactions avec vos instances Windows, afin de vous assurer que tous les événements et toutes les tâches sont automatiquement enregistrés.

Audit et responsabilité pour les instances Amazon EC2 Windows

AWS CloudTrail AWS Config, et AWS Config Rules fournissent des fonctionnalités d'audit et de suivi des modifications pour auditer les modifications AWS des ressources. Configurez les journaux d'événements Windows pour envoyer des fichiers journaux locaux à un système de gestion centralisée des journaux, afin de préserver les données des journaux à des fins d'analyse de la sécurité et du comportement opérationnel. Microsoft System Center Operations Manager (SCOM) regroupe les informations relatives aux applications Microsoft déployées sur des instances Windows et applique des ensembles de règles préconfigurés et personnalisés en fonction des rôles et services des applications. Les packs d'administration de System Center s'appuient sur SCOM des fonctionnalités de surveillance et de configuration spécifiques aux applications. Ces packs

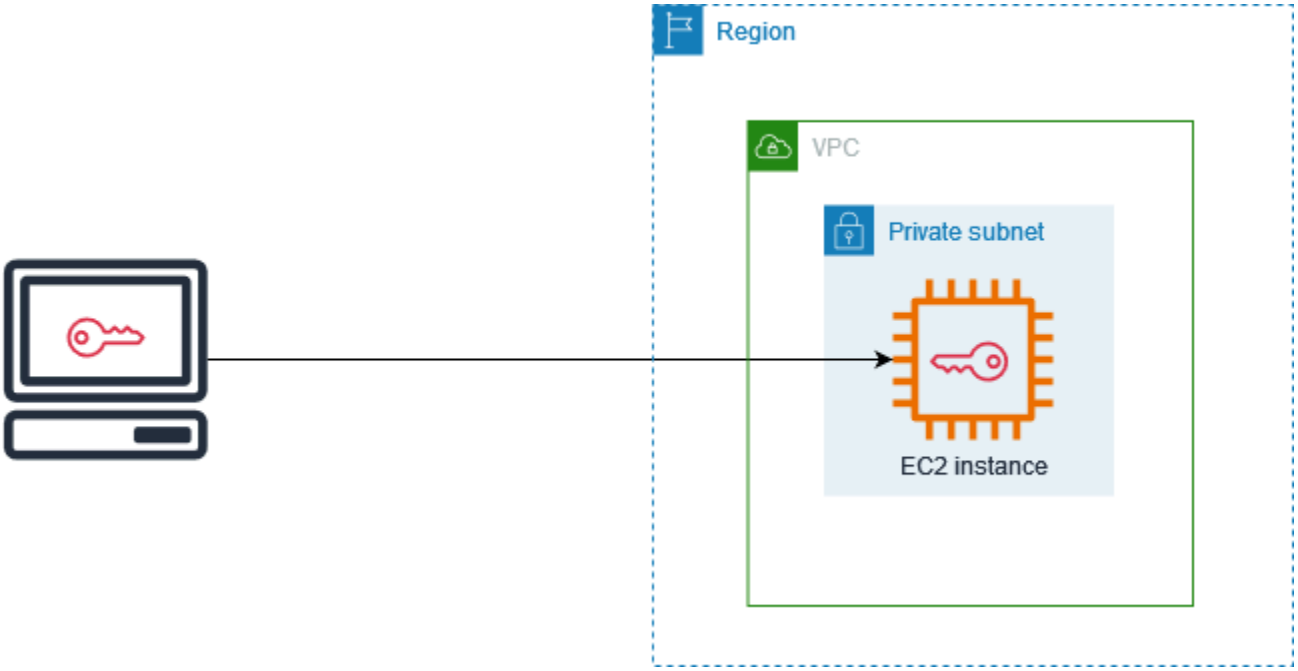
d'administration prennent en charge Windows Server Active Directory, SharePoint Server 2013, Exchange Server 2013, Lync Server 2013, SQL Server 2014, ainsi que de nombreux autres serveurs et technologies.

Outre les outils de gestion des systèmes Microsoft, les clients peuvent utiliser Amazon CloudWatch pour surveiller CPU l'utilisation des instances, les performances des disques, les E/S réseau et effectuer des vérifications de l'état des hôtes et des instances. Les agents de lancement EC2ConfigEC2Launch,, et EC2Launch v2 donnent accès à des fonctionnalités avancées supplémentaires pour les instances Windows. Par exemple, ils peuvent exporter les journaux du système Windows, de la sécurité, des applications et des services Internet (IIS) vers CloudWatch des journaux qui peuvent ensuite être intégrés aux CloudWatch métriques et aux alarmes Amazon. Les clients peuvent également créer des scripts qui exportent les compteurs de performance Windows vers des métriques CloudWatch personnalisées Amazon.

Paires de EC2 clés Amazon et EC2 instances Amazon

Une paire de clés, composée d'une clé publique et d'une clé privée, est un ensemble d'informations d'identification de sécurité que vous utilisez pour prouver votre identité lorsque vous vous connectez à une EC2 instance Amazon. Pour les instances Linux, la clé privée vous permet d'accéder à votre instance SSH en toute sécurité. Pour les instances Windows, la clé privée est requise pour déchiffrer le mot de passe administrateur, que vous utilisez ensuite pour vous connecter à votre instance.

Amazon EC2 stocke la clé publique sur votre instance, et vous stockez la clé privée, comme indiqué dans le schéma suivant. Il est important de stocker votre clé privée dans un endroit sécurisé, car toute personne possédant votre clé privée peut se connecter à vos instances qui utilisent la paire de clés.



Lorsque vous lancez une instance, vous pouvez spécifier une paire de clés afin de pouvoir vous connecter à votre instance à l'aide d'une méthode qui nécessite une paire de clés. Selon la façon dont vous gérez votre sécurité, vous pouvez spécifier la même paire de clés pour toutes vos instances ou vous pouvez spécifier différentes paires de clés.

Pour les instances Linux, lorsque votre instance démarre pour la première fois, la clé publique que vous avez spécifiée au lancement est placée sur votre instance Linux dans une entrée située à l'intérieur`~/.ssh/authorized_keys`. Lorsque vous vous connectez à votre instance Linux en utilisantSSH, pour vous connecter, vous devez spécifier la clé privée qui correspond à la clé publique.

Pour plus d'informations sur la connexion à votre EC2 instance, consultezConnect à votre EC2 instance.

> **Important**
>
> Amazon EC2 ne conservant pas de copie de votre clé privée, il est impossible de la récupérer si vous la perdez. Cependant, il peut toujours y avoir un moyen de vous connecter aux instances pour lesquelles vous avez perdu la clé privée. Pour plus d'informations, consultez J'ai perdu ma clé privée. Comment puis-je me connecter à mon instance ?.

Comme alternative aux paires de clés, vous pouvez vous connecter AWS Systems Manager Session Managerà votre instance à l'aide d'un shell interactif basé sur un navigateur en un clic ou du AWS Command Line Interface ().AWS CLI

Table des matières

Créez une paire de clés pour votre EC2 instance Amazon

Vous pouvez utiliser Amazon EC2 pour créer vos paires de clés, ou vous pouvez utiliser un outil tiers pour créer vos paires de clés, puis les importer sur AmazonEC2.

Amazon EC2 prend en charge les RSA clés SSH 2 048 bits pour les instances Linux et Windows. Amazon prend EC2 également en charge ED25519 les clés pour les instances Linux.

Pour savoir comment vous connecter à votre instance Linux SSH après avoir créé une paire de clés, consultezthe section called "Connectez-vous à votre instance Linux à l'aide de SSH".

Pour savoir comment vous connecter à votre instance Windows RDP après avoir créé une paire de clés, consultezthe section called "Connectez-vous à votre instance Windows à l'aide de RDP".

Table des matières

Créez une paire de clés à l'aide d'Amazon EC2

Lorsque vous créez une paire de clés à l'aide d'AmazonEC2, la clé publique est stockée dans Amazon EC2 et vous stockez la clé privée.

Vous pouvez créer jusqu'à 5 000 paires de clés par région. Pour demander une augmentation, créez un dossier de support. Pour obtenir plus d'informations, consultez la section Creating a support case (Création d'un cas de support) dans le Guide de l'utilisateur AWS Support .

Console

Pour créer une paire de clés à l'aide d'Amazon EC2

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sous Network & Security, choisissez Key Pairs.
3. Choisissez Créer une paire de clés.
4. Pour Name (Nom), entrez un nom descriptif pour la paire de clés. Amazon EC2 associe la clé publique au nom que vous spécifiez comme nom de clé. Le nom d'une clé peut comporter jusqu'à 255 ASCII caractères. Il ne peut pas inclure d'espaces de début ou de fin.
5. Sélectionnez un type de paire de clés adapté à votre système d'exploitation :

   (Instances Linux) Pour le type de paire de clés, choisissez RSAsoit ED25519.

   (Instances Windows) Pour le type de paire de clés, sélectionnez RSA. ED25519les clés ne sont pas prises en charge pour les instances Windows.
6. Pour le Private Key File format (Format de fichier de clé privée), sélectionnez le format dans lequel vous souhaitez enregistrer la clé privée. Pour enregistrer la clé privée dans un format utilisable avec OpenSSH, choisissez pem. Pour enregistrer la clé privée dans un format utilisable avec PuTTY, choisissez ppk.
7. Pour ajouter une balise à la clé publique, sélectionnez Add tag (Ajouter une balise), puis entrez la clé et la valeur de la balise. Répétez l'opération pour chaque étiquette.
8. Choisissez Créer une paire de clés.
9. Le fichier de clé privée est automatiquement téléchargé dans votre navigateur. Le nom de fichier de base est celui que vous avez spécifié pour votre paire de clés, et l'extension de nom de fichier est déterminée par le format de fichier que vous avez choisi. Enregistrez le fichier de clé privée en lieu sûr.

   > **Important**
   >
   > C'est votre seule occasion d'enregistrer le fichier de clé privée.

10. Si vous envisagez d'utiliser un SSH client sur un ordinateur macOS ou Linux pour vous connecter à votre instance Linux, utilisez la commande suivante pour définir les autorisations de votre fichier de clé privée afin que vous soyez le seul à pouvoir le lire.

    ```
    chmod 400 key-pair-name.pem
    ```

    Si vous ne définissez pas ces autorisations, vous ne pouvez pas vous connecter à votre instance à l'aide de cette paire de clés. Pour de plus amples informations, veuillez consulter Erreur : fichier de clé privée non protégé.

AWS CLI

Pour créer une paire de clés à l'aide d'Amazon EC2

1. Pour générer la paire de clés et enregistrer la clé privée vers un fichier `.pem`, utilisez la commande create-key-pair comme suit.

   Pour `--key-name`, indiquez un nom pour la clé publique. Le nom peut comporter jusqu'à 255 ASCII caractères.

   Pour `--key-type`, spécifiez `rsa` ou `ed25519`. Si vous n'incluez pas le paramètre `--key-type`, une clé `rsa` est créée par défaut. Notez que ED25519 les clés ne sont pas prises en charge pour les instances Windows.

   Pour `--key-format`, spécifiez `pem` ou `ppk`. Si vous n'incluez pas le paramètre `--key-format`, un fichier `pem` est créé par défaut.

   `--query "KeyMaterial"` imprime le matériel de clé privée à la sortie.

   `--output text > my-key-pair.pem` enregistre le matériel de clé privée dans un fichier avec l'extension spécifiée. L'extension peut être `.pem` ou `.ppk`. La clé privée peut avoir un nom différent de la clé publique, mais pour faciliter son utilisation, utilisez le même nom.

   ```
   aws ec2 create-key-pair \
       --key-name my-key-pair \
       --key-type rsa \
       --key-format pem \
       --query "KeyMaterial" \
       --output text > my-key-pair.pem
   ```

2. Si vous envisagez d'utiliser un SSH client sur un ordinateur macOS ou Linux pour vous connecter à votre instance Linux, utilisez la commande suivante pour définir les autorisations de votre fichier de clé privée afin que vous soyez le seul à pouvoir le lire.

```
chmod 400 key-pair-name.pem
```

Si vous ne définissez pas ces autorisations, vous ne pouvez pas vous connecter à votre instance à l'aide de cette paire de clés. Pour de plus amples informations, veuillez consulter Erreur : fichier de clé privée non protégé.

PowerShell

Pour créer une paire de clés à l'aide d'Amazon EC2

Utilisez la New-EC2KeyPair AWS Tools for Windows PowerShell commande suivante pour générer la clé et l'enregistrer dans un `.ppk` fichier `.pem` or.

Pour `-KeyName`, indiquez un nom pour la clé publique. Le nom peut comporter jusqu'à 255 ASCII caractères.

Pour `-KeyType`, spécifiez `rsa` ou `ed25519`. Si vous n'incluez pas le paramètre `-KeyType`, une clé `rsa` est créée par défaut. Notez que ED25519 les clés ne sont pas prises en charge pour les instances Windows.

Pour `-KeyFormat`, spécifiez `pem` ou `ppk`. Si vous n'incluez pas le paramètre `-KeyFormat`, un fichier `pem` est créé par défaut.

`KeyMaterial` imprime le matériel de clé privée à la sortie.

`Out-File -Encoding ascii -FilePath C:\path\my-key-pair.pem` enregistre le matériel de clé privée dans un fichier avec l'extension spécifiée. L'extension peut être `.pem` ou `.ppk`. La clé privée peut avoir un nom différent de la clé publique, mais pour faciliter son utilisation, utilisez le même nom.

```
PS C:\> (New-EC2KeyPair -KeyName "my-key-pair" -KeyType "rsa" -KeyFormat
 "pem").KeyMaterial | Out-File -Encoding ascii -FilePath C:\path\my-key-pair.pem
```

Créez une paire de clés en utilisant AWS CloudFormation

Lorsque vous créez une nouvelle paire de clés à l'aide de AWS CloudFormation, la clé privée est enregistrée dans AWS Systems Manager Parameter Store. Le nom du paramètre a le format suivant :

```
/ec2/keypair/key_pair_id
```

Pour plus d'informations, veuillez consulter la rubrique AWS Systems Manager Parameter Store dans le Guide de l'utilisateur AWS Systems Manager .

Pour créer une paire de clés en utilisant AWS CloudFormation

1. Spécifiez la KeyPair ressource AWSEC2: : : dans votre modèle.

   ```
   Resources:
     NewKeyPair:
       Type: 'AWS::EC2::KeyPair'
       Properties:
         KeyName: new-key-pair
   ```

2. Utilisez la commande describe-key-pairs comme suit pour obtenir l'ID de la paire de clés.

   ```
   aws ec2 describe-key-pairs --filters Name=key-name,Values=new-key-pair --query
    KeyPairs[*].KeyPairId --output text
   ```

   Voici un exemple de sortie.

   ```
   key-05abb699beEXAMPLE
   ```

3. Utilisez la commande get-parameter comme suit pour obtenir le paramètre de votre clé et enregistrer le contenu de la clé dans un fichier `.pem`.

   ```
   aws ssm get-parameter --name /ec2/keypair/key-05abb699beEXAMPLE --with-decryption
    --query Parameter.Value --output text > new-key-pair.pem
   ```

IAMAutorisations requises

AWS CloudFormation Pour permettre de gérer les paramètres du Parameter Store en votre nom, le IAM rôle assumé par AWS CloudFormation ou votre utilisateur doit disposer des autorisations suivantes :

- `ssm:PutParameter` : accorde l'autorisation de créer un paramètre pour le matériel de clé privée.
- `ssm:DeleteParameter` : autorise la suppression du paramètre utilisé pour stocker les éléments de clé privée. Cette autorisation est nécessaire, que la paire de clés ait été importée ou créée par AWS CloudFormation.

Lorsqu'il AWS CloudFormation supprime une paire de clés créée ou importée par une pile, il effectue une vérification des autorisations pour déterminer si vous êtes autorisé à supprimer des paramètres, même s'il AWS CloudFormation crée un paramètre uniquement lorsqu'il crée une paire de clés, et non lorsqu'il importe une paire de clés. AWS CloudFormation teste l'autorisation requise à l'aide d'un nom de paramètre fabriqué qui ne correspond à aucun paramètre de votre compte. Par conséquent, vous pouvez voir un nom de paramètre fabriqué dans le message d'erreur `AccessDeniedException`.

Créez une paire de clés à l'aide d'un outil tiers et importez la clé publique sur Amazon EC2

Instances Linux

Au lieu d'utiliser Amazon EC2 pour créer une paire de clés, vous pouvez créer une paire de ED25519 clés RSA or à l'aide d'un outil tiers, puis importer la clé publique sur AmazonEC2.

Exigences relatives aux paires de clés

- Types pris en charge : RSA etED25519. Amazon EC2 n'accepte pas les DSA clés.
- Formats pris en charge :
  - Format de clé SSH publique ouvert (format en`~/.ssh/authorized_keys`). Si vous vous connectez SSH en utilisant EC2 Instance ConnectAPI, le SSH2 format est également pris en charge.
  - SSHle format de fichier de clé privée doit être PEM ou PPK
  - (RSAuniquement) Format codé DER Base64
  - (RSAuniquement) format de fichier à clé SSH publique tel que spécifié dans RFC4716

- Longueurs prises en charge : 1024, 2048 et 4096. Si vous vous connectez SSH en utilisant EC2 Instance ConnectAPI, les longueurs prises en charge sont 2048 et 4096.

Pour créer une paire de clés à l'aide d'un outil tiers

1. Générez une paire de clés avec un outil tiers de votre choix. Par exemple, vous pouvez utiliser ssh-keygen (un outil fourni avec l'SSHinstallation standard d'Open). Java, Ruby, Python et de nombreux autres langages de programmation fournissent également des bibliothèques standard que vous pouvez utiliser pour créer une paire de ED25519 clés RSA ou.

   > **Important**
   >
   > La clé privée doit être au PPK format PEM or. Par exemple, `ssh-keygen -m PEM` utilisez-le pour générer la SSH touche Ouvrir au PEM format.

2. Enregistrez la clé publique dans un fichier local. Par exemple, `~/.ssh/my-key-pair.pub`. L'extension du nom de fichier de ce fichier n'est pas importante.
3. Enregistrez la clé privée dans un fichier local dont l'extension est `.pem` ou `.ppk`. Par exemple, `~/.ssh/my-key-pair.pem` ou `~/.ssh/my-key-pair.ppk`.

   > **Important**
   >
   > Enregistrez le fichier de clé privée en lieu sûr. Vous devez fournir le nom de votre clé publique lorsque vous lancez une instance, ainsi que la clé privée correspondante chaque fois que vous vous connectez à l'instance.

instances Windows

Au lieu d'utiliser Amazon EC2 pour créer votre paire de clés, vous pouvez créer une paire de RSA clés à l'aide d'un outil tiers, puis importer la clé publique sur AmazonEC2.

Exigences relatives aux paires de clés

- Types pris en charge :RSA. Amazon EC2 n'accepte pas les DSA clés.

> **Note**
>
> ED25519les clés ne sont pas prises en charge pour les instances Windows.

- Formats pris en charge :
  - Format de clé SSH publique ouvert
  - SSHle format de fichier de clé privée doit être PEM ou PPK
  - (RSAuniquement) Format codé DER Base64
  - (RSAuniquement) format de fichier à clé SSH publique tel que spécifié dans RFC4716
- Longueurs prises en charge : 1024, 2048 et 4096.

Pour créer une paire de clés à l'aide d'un outil tiers

1. Générez une paire de clés avec un outil tiers de votre choix. Par exemple, vous pouvez utiliser ssh-keygen (un outil fourni avec l'SSHinstallation standard d'Open). Java, Ruby, Python et de nombreux autres langages de programmation fournissent également des bibliothèques standard que vous pouvez utiliser pour créer une paire de RSA clés.

   > **Important**
   >
   > La clé privée doit être au PPK format PEM or. Par exemple, `ssh-keygen -m PEM` utilisez-le pour générer la SSH touche Ouvrir au PEM format.

2. Enregistrez la clé publique dans un fichier local. Par exemple, `C:\keys\my-key-pair.pub`. L'extension du nom de fichier de ce fichier n'est pas importante.
3. Enregistrez la clé privée dans un fichier local dont l'extension est `.pem` ou `.ppk`. Par exemple, `C:\keys\my-key-pair.pem` ou `C:\keys\my-key-pair.ppk`. L'extension du nom de fichier de ce fichier est importante car seuls `.pem` les fichiers peuvent être sélectionnés lors de la connexion à votre instance Windows depuis la EC2 console.

   > **Important**
   >
   > Enregistrez le fichier de clé privée en lieu sûr. Vous devez fournir le nom de votre clé publique lorsque vous lancez une instance, ainsi que la clé privée correspondante chaque fois que vous vous connectez à l'instance.

Après avoir créé la paire de clés, utilisez l'une des méthodes suivantes pour importer votre clé publique sur AmazonEC2.

Console

Pour importer la clé publique sur Amazon EC2

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, cliquez sur Key Pairs.
3. Choisissez Import key pair (Importer une paire de clés).
4. Pour Name (Nom), saisissez un nom descriptif pour la clé publique. Le nom peut comporter jusqu'à 255 ASCII caractères. Il ne peut pas inclure d'espaces de début ou de fin.

   > **Note**
   >
   > Lorsque vous vous connectez à votre instance depuis la EC2 console, celle-ci suggère ce nom pour le nom de votre fichier de clé privée.

5. Choisissez Browse (Parcourir) pour accéder à votre clé publique et la sélectionner, ou collez le contenu de votre clé publique dans le champ Public key contents (Contenu de la clé publique).
6. Choisissez Import key pair (Importer une paire de clés).
7. Vérifiez que la clé publique que vous avez importée apparaît dans la liste des paires de clés.

AWS CLI

Pour importer la clé publique sur Amazon EC2

Utilisez la commande import-key-pair AWS CLI .

Pour vérifier que la paire de clés a été importée correctement

Utilisez la commande describe-key-pairs AWS CLI .

PowerShell

Pour importer la clé publique sur Amazon EC2

Utilisez la commande Import-EC2KeyPair AWS Tools for Windows PowerShell .

Pour vérifier que la paire de clés a été importée correctement

Utilisez la commande Get-EC2KeyPair AWS Tools for Windows PowerShell .

Baliser une paire de clés

Pour classer et gérer les paires de clés que vous avez créées à l'aide d'Amazon EC2 ou importées sur AmazonEC2, vous pouvez les étiqueter avec des métadonnées personnalisées. Pour plus d'informations sur le fonctionnement des balises, consultez Marquez vos EC2 ressources Amazon.

Console

Pour afficher, ajouter ou supprimer le tag d'une paire de clés

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, cliquez sur Key Pairs.
3. Sélectionnez une clé publique, puis choisissez Actions, Gérer les étiquettes.
4. La page Gérer les étiquettes) affiche toutes les étiquettes affectées à la clé publique.
   - Pour ajouter une balise, choisissez Ajouter la balise, puis entrez la clé et la valeur de la balise. Vous pouvez ajouter jusqu'à 50 étiquettes par clé. Pour plus d'informations, consultez Restrictions liées aux balises.
   - Pour supprimer une balise, sélectionnez Remove (Retirer) en regard de la zone de valeur de la balise.
5. Choisissez Save (Enregistrer).

AWS CLI

Pour afficher les tags de vos paires de clés

Utilisez la commande describe-tags AWS CLI . Dans l'exemple suivant, vous décrivez les étiquettes de toutes vos clés publiques.

```
aws ec2 describe-tags --filters "Name=resource-type,Values=key-pair"
```

```
{
    "Tags": [
    {
```

```
        "Key": "Environment",
        "ResourceId": "key-0123456789EXAMPLE",
        "ResourceType": "key-pair",
        "Value": "Production"
    },
    {
        "Key": "Environment",
        "ResourceId": "key-9876543210EXAMPLE",
        "ResourceType": "key-pair",
        "Value": "Production"
    }]
}
```

Pour décrire les balises d'une paire de clés

Utilisez la commande describe-key-pairs AWS CLI .

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789EXAMPLE
```

```
{
    "KeyPairs": [
    {
        "KeyName": "MyKeyPair",
        "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
        "KeyPairId": "key-0123456789EXAMPLE",
        "Tags": [
        {
            "Key": "Environment",
            "Value": "Production"
        }]
    }]
}
```

Pour étiqueter une paire de clés

Utilisez la commande create-tags AWS CLI . Dans l'exemple suivant, la clé publique est étiquetée avec `Key=Cost-Center` et `Value=CC-123`.

```
aws ec2 create-tags --resources key-0123456789EXAMPLE --tags Key=Cost-
Center,Value=CC-123
```

Pour supprimer une balise d'une paire de clés

Utilisez la commande delete-tags AWS CLI . Pour obtenir des exemples, reportez-vous à la section Exemples dans le document AWS CLI Références des commandes.

PowerShell

Pour afficher les tags de vos paires de clés

Utilisez la commande Get-EC2Tag.

Pour décrire les balises d'une paire de clés

Utilisez la commande Get-EC2KeyPair.

Pour étiqueter une paire de clés

Utilisez la commande New-EC2Tag.

Pour supprimer une balise d'une paire de clés

Utilisez la commande Remove-EC2Tag.

Décrivez vos paires de clés

Vous pouvez décrire les paires de clés que vous avez stockées sur AmazonEC2. Vous pouvez également récupérer le contenu de la clé publique et identifier la clé publique spécifiée lors du lancement.

Rubriques

- Décrivez vos paires de clés
- Extraire le contenu de la clé publique
- Identifier la clé publique spécifiée au lancement

Décrivez vos paires de clés

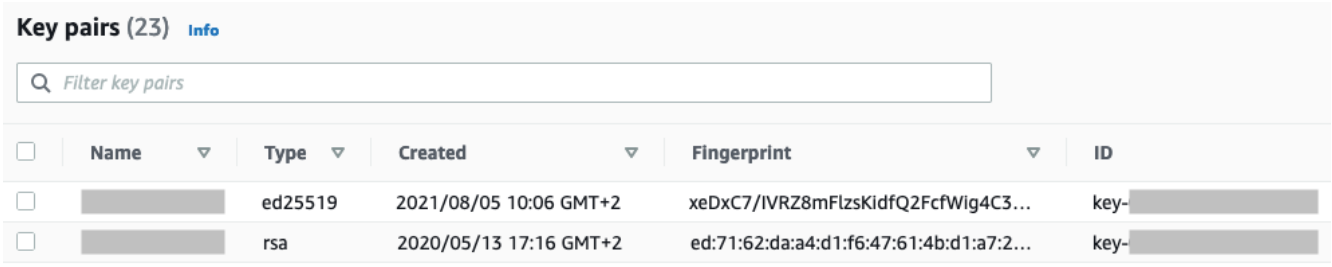
Vous pouvez consulter les informations suivantes concernant vos clés publiques stockées sur Amazon EC2 : nom de la clé publique, identifiant, type de clé, empreinte digitale, contenu de la clé publique, date et heure (dans le UTC fuseau horaire) de création de la clé par Amazon EC2 (si la clé a été créée par un outil tiers, il s'agit de la date et de l'heure auxquelles la clé a été importée sur AmazonEC2) et toutes les balises associées à la clé publique.

Vous pouvez utiliser la EC2 console Amazon ou AWS CLI consulter les informations relatives à vos clés publiques.

Console

Pour afficher des informations sur vos clés publiques

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation de gauche, choisissez Key Pairs (Paires de clés).
3. Vous pouvez afficher les informations relatives à chaque clé publique dans la table Key pairs (Paires de clés).



4. Pour afficher les identifications d'une clé publique, cochez la case à côté de la clé, puis choisissez Actions, Manage tags (Gérer les identifications).

AWS CLI

Pour décrire une clé publique

Utilisez la commande describe-key-pairs et spécifiez le paramètre `--key-names`.

```
aws ec2 describe-key-pairs --key-names key-pair-name
```

Exemple de sortie

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
```

```
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

Sinon, au lieu de `--key-names`, vous pouvez spécifier le paramètre `--key-pair-ids` pour identifier la clé publique.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example
```

Pour afficher la clé publique dans la sortie, vous devez spécifier le paramètre `--include-public-key`.

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

Exemple de sortie : dans la sortie, le champ `PublicKey` contient la clé publique.

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
            "PublicKey": "ssh-ed25519
 AAAAC3NzaC1lZDI1NTE5AAAAIIj7azlDjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

Extraire le contenu de la clé publique

Vous pouvez utiliser différentes méthodes pour accéder à la clé publique. Vous pouvez récupérer le contenu de la clé publique à partir de la clé privée correspondante sur votre ordinateur local, à partir des métadonnées de l'instance lancée avec la clé publique ou à l'aide de la `describe-key-pairs` AWS CLI commande. Pour les instances Linux, le contenu de la clé publique peut également être extrait du `authorized_keys` fichier de l'instance.

Utilisez l'une des méthodes suivantes pour récupérer le contenu de la clé publique.

Instances Linux

From the private key

Pour extraire le contenu de la clé publique de la clé privée

Sur votre ordinateur local Linux ou macOS, vous pouvez utiliser la commande ssh-keygen pour extraire la clé publique de votre paire de clés. Spécifiez le chemin où vous avez téléchargé votre clé privée (fichier `.pem`).

```
ssh-keygen -y -f /path_to_key_pair/my-key-pair.pem
```

La commande renvoie la clé publique, comme indiqué dans l'exemple suivant.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

Si la commande échoue, exécutez la commande suivante pour vous assurer d'avoir modifié les autorisations sur votre fichier de paire de clés privées afin d'être le seul à pouvoir l'afficher.

```
chmod 400 key-pair-name.pem
```

From the instance metadata

Vous pouvez utiliser le service des métadonnées d'instance Version 2 ou le service des métadonnées d'instance Version 1 pour récupérer la clé publique à partir des métadonnées de l'instance.

> **Note**
>
> Si vous modifiez la paire de clés que vous utilisez pour vous connecter à l'instance, Amazon EC2 ne met pas à jour les métadonnées de l'instance pour afficher la nouvelle clé publique. Les métadonnées d'instance continuent d'afficher la clé publique pour la paire de clés que vous avez spécifiée lors du lancement de l'instance.

Pour récupérer le contenu de la clé publique à partir des métadonnées de l'instance

Utilisez l'une des commandes suivantes pour vous connecter à votre instance.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Exemple de sortie

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

Pour obtenir plus d'informations sur les métadonnées d'instance, consultez Accéder aux métadonnées d'une EC2 instance.

From the instance

Si vous spécifiez une paire de clés lorsque vous lancez une instance Linux, lorsque l'instance démarre pour la première fois, le contenu de la clé publique est placé sur l'instance dans une entrée dans `~/.ssh/authorized_keys`.

Pour récupérer le contenu de la clé publique à partir d'une instance

1. Connectez-vous à votre instance.
2. Dans la fenêtre du terminal, ouvrez le fichier `authorized_keys` à l'aide de votre éditeur de texte préféré (tel que vim ou nano).

   ```
   [ec2-user ~]$ nano ~/.ssh/authorized_keys
   ```

Le fichier `authorized_keys` s'ouvre, affichant la clé publique, suivie du nom de la paire de clés. Voici un exemple d'entrée pour la paire de clés nommée *key-pair-name*.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

From describe-key-pairs

Pour extraire la clé publique à partir de la commande AWS CLI**`describe-key-pairs`**

Utilisez la commande describe-key-pairs et spécifiez le paramètre `--key-names` pour identifier la clé publique. Pour inclure la clé publique dans la sortie, spécifiez le paramètre `--include-public-key`.

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

Exemple de sortie : dans la sortie, le champ `PublicKey` contient la clé publique.

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
            "PublicKey": "ssh-ed25519
 AAAAC3NzaC1lZDI1NTE5AAAAIIj7azlDjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

Sinon, au lieu de `--key-names`, vous pouvez spécifier le paramètre `--key-pair-ids` pour identifier la clé publique.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example --include-public-key
```

instances Windows

From the private key

Pour extraire le contenu de la clé publique de la clé privée

Sur votre ordinateur Windows local, vous pouvez utiliser P uTTYgen pour obtenir la clé publique de votre paire de clés.

Démarrez P uTTYgen et choisissez Charger. Sélectionnez le fichier de clé privée `.ppk` ou `.pem`. P uTTYgen affiche la clé publique sous clé publique pour la coller dans le fichier Open SSH authorized_keys. Vous pouvez également visualiser la clé publique en choisissant Save public key (Enregistrer la clé publique), en spécifiant un nom pour le fichier, en enregistrant le fichier et en ouvrant le fichier.

From the instance metadata

Vous pouvez utiliser le service des métadonnées d'instance Version 2 ou le service des métadonnées d'instance Version 1 pour récupérer la clé publique à partir des métadonnées de l'instance.

> **Note**
>
> Si vous modifiez la paire de clés que vous utilisez pour vous connecter à l'instance, Amazon EC2 ne met pas à jour les métadonnées de l'instance pour afficher la nouvelle clé publique. Les métadonnées d'instance continuent d'afficher la clé publique pour la paire de clés que vous avez spécifiée lors du lancement de l'instance.

Pour récupérer le contenu de la clé publique à partir des métadonnées de l'instance

Utilisez l'une des commandes suivantes pour vous connecter à votre instance.

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri  http://169.254.169.254/latest/meta-data/public-
keys/0/openssh-key
```

Exemple de sortie

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

Pour obtenir plus d'informations sur les métadonnées d'instance, consultez Accéder aux métadonnées d'une EC2 instance.

From describe-key-pairs

Pour extraire la clé publique à partir de la commande AWS CLI**`describe-key-pairs`**

Utilisez la commande describe-key-pairs et spécifiez le paramètre `--key-names` pour identifier la clé publique. Pour inclure la clé publique dans la sortie, spécifiez le paramètre `--include-public-key`.

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

Exemple de sortie : dans la sortie, le champ `PublicKey` contient la clé publique.

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
```

```
            "PublicKey": "ssh-ed25519
 AAAAC3NzaC1lZDI1NTE5AAAAIIj7azlDjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

Sinon, au lieu de `--key-names`, vous pouvez spécifier le paramètre `--key-pair-ids` pour identifier la clé publique.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example --include-public-key
```

Identifier la clé publique spécifiée au lancement

Si vous spécifiez une clé publique lorsque vous lancez une instance, le nom de la clé publique est enregistré par l'instance.

Pour identifier la clé publique spécifiée au lancement

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez instances, puis sélectionnez votre instance.
3. Sous l'onglet Détails, sous Détails de l'instance, le champ Paire de clés assignée au lancement affiche le nom de la clé publique que vous avez spécifiée lors du lancement de l'instance.

> **Note**
>
> La valeur du champ Paire de clés assignée au lancement ne change pas même si vous modifiez la clé publique sur l'instance ou si vous ajoutez des clés publiques.

Supprimer votre paire de clés

Vous pouvez supprimer une paire de clés, ce qui supprime la clé publique stockée sur AmazonEC2. La suppression d'une paire de clés ne supprime pas la clé privée correspondante.

Lorsque vous supprimez une clé publique à l'aide des méthodes suivantes, vous supprimez uniquement la clé publique que vous avez stockée sur Amazon EC2 lorsque vous avez créé ou

importé la paire de clés. La suppression d'une clé publique ne supprime pas la clé publique des instances auxquelles vous l'avez ajoutée, que vous l'ayez ajoutée lors du lancement de l'instance ou plus tard. Elle ne supprime pas non plus la clé privée présente sur votre ordinateur local. Vous pouvez continuer à vous connecter aux instances que vous avez lancées à l'aide d'une clé publique que vous avez supprimée d'Amazon EC2 tant que vous possédez toujours le fichier de clé privée (`.pem`).

> **Important**
>
> Si vous utilisez un groupe Auto Scaling (par exemple, dans un environnement Elastic Beanstalk), assurez-vous que la clé publique que vous supprimez n'est pas spécifiée dans un modèle de lancement ou dans une configuration de lancement associé(e). Si Amazon EC2 Auto Scaling détecte une instance défectueuse, il lance une instance de remplacement. Toutefois, le lancement de l'instance échoue si la clé publique est introuvable. Pour plus d'informations, consultez la section Modèles de lancement dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.

Console

Pour supprimer votre clé publique sur Amazon EC2

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, cliquez sur Key Pairs.
3. Sélectionnez la paire de clés à supprimer et choisissez Actions, Delete (Supprimer).
4. Dans le champ de confirmation, entrez, `Delete` puis choisissez Delete (Supprimer).

AWS CLI

Pour supprimer votre clé publique sur Amazon EC2

Utilisez la commande delete-key-pair AWS CLI .

PowerShell

Pour supprimer votre clé publique sur Amazon EC2

Utilisez la commande Remove-EC2KeyPair AWS Tools for Windows PowerShell .

Ajouter ou remplacer une clé publique sur votre instance Linux

Si vous perdez une clé privée, vous perdez l'accès à toutes les instances qui utilisent la paire de clés. Pour plus d'informations sur la connexion à une instance à l'aide d'une paire de clés différent e de celle que vous avez spécifiée au lancement, voir J'ai perdu ma clé privée.

Lorsque vous lancez une instance, vous pouvez spécifier une paire de clés. Si vous spécifiez une paire de clés lors du lancement, lorsque votre instance démarre pour la première fois, le contenu de la clé publique est placé sur votre instance Linux dans une entrée dans `~/.ssh/authorized_keys`.

Vous pouvez modifier la paire de clés utilisée pour accéder au compte système par défaut de votre instance en ajoutant une nouvelle clé publique sur l'instance ou en remplaçant la clé publique (en supprimant la clé publique existante et en ajoutant une nouvelle clé) sur l'instance. Vous pouvez également supprimer toutes les clés publiques d'une instance. Pour ajouter ou remplacer une paire de clés, vous devez pouvoir vous connecter à votre instance.

Vous pouvez ajouter ou remplacer une paire de clés pour les raisons suivantes :

- Si un utilisateur de votre organisation requiert l'accès à l'utilisateur système à l'aide d'une paire de clés distincte, vous pouvez ajouter la clé publique à votre instance.
- Si quelqu'un possède une copie de la clé privée (fichier `.pem`) et que vous voulez l'empêcher de se connecter à votre instance (par exemple, si la personne a quitté votre organisation), vous pouvez supprimer la clé publique sur l'instance et la remplacer par une nouvelle.
- Si vous créez un système Linux AMI à partir d'une instance, le contenu de la clé publique est copié de l'instance vers leAMI. Si vous lancez une instance depuis leAMI, la nouvelle instance inclut la clé publique de l'instance d'origine. Pour empêcher une personne détenant la clé privée de se connecter à la nouvelle instance, vous pouvez supprimer la clé publique de l'instance d'origine avant de créer laAMI.

Utilisez les procédures suivantes pour modifier la paire de clés de l'utilisateur par défaut, par exemple`ec2-user`. Pour plus d'informations sur l'ajout d'utilisateurs à votre instance, consultez la documentation du système d'exploitation de votre instance.

Pour ajouter ou remplacer une paire de clés

1. Créez une nouvelle paire de clés à l'aide de la EC2console Amazon ou d'un outil tiers.
2. Récupérez la clé publique de votre nouvelle paire de clés. Pour plus d'informations, consultez Extraire le contenu de la clé publique.
3. Connectez-vous à votre instance à l'aide de votre clé privée existante.
4. À l'aide d'un éditeur de texte de votre choix, ouvrez le fichier `.ssh/authorized_keys` sur l'instance. Collez les informations de clé publique depuis votre nouvelle paire de clés sous les informations existantes de clé publique. Sauvegardez le fichier.
5. Déconnectez-vous de votre instance et testez que vous pouvez vous connecter à votre instance à l'aide du nouveau fichier de clé privé.
6. (Facultatif) Si vous remplacez une paire de clés existante, connectez-vous à votre instance et supprimez les informations de clé publique de la paire de clés originale du fichier `.ssh/authorized_keys`.

> **Important**
>
> Si vous utilisez un groupe Auto Scaling, assurez-vous que la paire de clés que vous remplacez n'est pas spécifiée dans votre modèle ou votre configuration de lancement. Si Amazon EC2 Auto Scaling détecte une instance défectueuse, il lance une instance de remplacement. Toutefois, le lancement de l'instance échoue si la paire de clés est introuvable. Pour plus d'informations, consultez la section Modèles de lancement dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.

Pour supprimer une clé publique d'une instance

1. Connectez-vous à votre instance.
2. À l'aide d'un éditeur de texte de votre choix, ouvrez le fichier `.ssh/authorized_keys` sur l'instance. Supprimez les informations de clé publique, puis enregistrez le fichier.

> **Warning**
>
> Une fois que vous avez supprimé toutes les clés publiques d'une instance et que vous vous êtes déconnecté de l'instance, vous ne pouvez plus vous y reconnecter à moins que cela ne AMI fournisse un autre moyen de connexion.

Vérifier l'empreinte de votre paire de clés

Pour vérifier l'empreinte de votre paire de clés, comparez l'empreinte affichée sur la page des paires de clés de la EC2 console Amazon, ou renvoyée par la describe-key-pairscommande, avec l'empreinte que vous générez à l'aide de la clé privée sur votre ordinateur local. Ces empreintes doivent correspondre.

Lorsqu'Amazon EC2 calcule une empreinte digitale, Amazon EC2 peut ajouter des caractères à l'empreinte digitale. = D'autres outils, tels que ssh-keygen, pourraient omettre ce remplissage.

Si vous essayez de vérifier l'empreinte de votre EC2 instance Linux, et non celle de votre paire de clés, consultez la section Obtenir l'empreinte de l'instance.

Comment sont calculées les empreintes

Amazon EC2 utilise différentes fonctions de hachage pour calculer les empreintes digitales RSA et les paires de ED25519 clés. En outre, pour les paires de RSA clés, Amazon EC2 calcule les empreintes différemment à l'aide de différentes fonctions de hachage selon que la paire de clés a été créée par Amazon EC2 ou importée sur Amazon. EC2

Le tableau suivant répertorie les fonctions de hachage utilisées pour calculer les empreintes digitales RSA et les paires de ED25519 clés créées par Amazon EC2 et importées sur Amazon. EC2

(Instances Linux) Fonctions de hachage utilisées pour calculer les empreintes

Source de paires de clés	RSApaires de clés (Windows et Linux)	ED25519paires de clés (Linux)
Créée par Amazon EC2	SHA-1	SHA-256
Importé sur Amazon EC2	MD5[1]	SHA-256

[1] Si vous importez une RSA clé publique sur AmazonEC2, l'empreinte digitale est calculée à l'aide d'une fonction de MD5 hachage. Cela est vrai quelle que soit la manière dont vous avez créé la paire de clés, par exemple en utilisant un outil tiers ou en générant une nouvelle clé publique à partir d'une clé privée existante créée à l'aide d'AmazonEC2.

Lorsque vous utilisez la même paire de clés dans différentes régions

Si vous prévoyez d'utiliser la même paire de clés pour vous connecter à des instances situées dans des instances différentes Régions AWS, vous devez importer la clé publique dans toutes les régions dans lesquelles vous l'utiliserez. Si vous utilisez Amazon EC2 pour créer la paire de clés, vous pouvez Extraire le contenu de la clé publique importer la clé publique dans les autres régions.

> **Note**
>
> - Si vous créez une paire de RSA clés à l'aide d'AmazonEC2, puis que vous générez une clé publique à partir de la clé EC2 privée Amazon, les clés publiques importées auront une empreinte différente de celle de la clé publique d'origine. Cela est dû au fait que l'empreinte de la RSA clé d'origine créée à l'aide d'Amazon EC2 est calculée à l'aide d'une fonction de hachage SHA -1, tandis que l'empreinte des RSA clés importées est calculée à l'aide d'une fonction de MD5 hachage.
> - Pour les paires de ED25519 clés, les empreintes seront les mêmes, qu'elles soient créées par Amazon EC2 ou importées sur AmazonEC2, car la même fonction de hachage SHA -256 est utilisée pour calculer l'empreinte digitale.

Générer une empreinte digitale à partir de la clé privée

Utilisez l'une des commandes suivantes pour générer une empreinte à partir de la clé privée sur votre machine locale.

Si vous utilisez un ordinateur local Windows, vous pouvez exécuter les commandes suivantes à l'aide du sous-système Windows pour Linux (WSL). Installez la distribution WSL et une distribution Linux en suivant les instructions du guide d'installation de Windows 10. L'exemple des instructions installe la distribution Ubuntu de Linux, mais vous pouvez installer n'importe quelle distribution. Vous êtes invité à redémarrer votre ordinateur pour que les modifications prennent effet.

- Si vous avez créé la paire de clés à l'aide d'Amazon EC2

Utilisez les SSL outils Open pour générer une empreinte digitale, comme indiqué dans les exemples suivants.

Pour les paires de RSA clés :

```
openssl pkcs8 -in path_to_private_key -inform PEM -outform DER -topk8 -nocrypt |
 openssl sha1 -c
```

(instances Linux) Pour les paires de ED25519 clés :

```
ssh-keygen -l -f path_to_private_key
```

- (paires de RSA clés uniquement) Si vous avez importé la clé publique sur Amazon EC2

  Vous pouvez suivre cette procédure quelle que soit la manière dont vous avez créé la paire de clés, par exemple en utilisant un outil tiers ou en générant une nouvelle clé publique à partir d'une clé privée existante créée à l'aide d'Amazon EC2

  Utilisez les SSL outils Open pour générer l'empreinte digitale, comme indiqué dans l'exemple suivant.

  ```
  openssl rsa -in path_to_private_key -pubout -outform DER | openssl md5 -c
  ```

- Si vous avez créé une paire de SSH clés Open à l'aide d'Open SSH 7.8 ou version ultérieure et que vous avez importé la clé publique sur Amazon EC2

  Utilisez ssh-keygen pour générer l'empreinte comme indiqué dans les exemples suivants.

  Pour les paires de RSA clés :

  ```
  ssh-keygen -ef path_to_private_key -m PEM | openssl rsa -RSAPublicKey_in -outform DER
   | openssl md5 -c
  ```

  (instances Linux) Pour les paires de ED25519 clés :

  ```
  ssh-keygen -l -f path_to_private_key
  ```

Groupes EC2 de sécurité Amazon pour vos EC2 instances

Un groupe de sécurité agit comme un pare-feu virtuel permettant à vos EC2 instances de contrôler le trafic entrant et sortant. Les règles entrantes contrôlent le trafic entrant vers votre instance, et les règles sortantes contrôlent le trafic sortant de votre instance. Lorsque vous lancez une instance, vous pouvez spécifier un ou plusieurs groupes de sécurité. Si vous ne spécifiez aucun groupe de sécurité, Amazon EC2 utilise le groupe de sécurité par défaut pour leVPC. Après avoir lancé une instance, vous pouvez modifier ses groupes de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Pour plus d'informations, consultezSécurité sur Amazon EC2. AWS fournit des groupes de sécurité comme l'un des outils de sécurisation de vos instances, et vous devez les configurer pour répondre à vos besoins en matière de sécurité. Si vous avez des exigences qui ne sont pas satisfaites par les groupes de sécurité, vous pouvez maintenir votre propre pare-feu sur l'une de vos instances, quelle qu'elle soit, en plus de l'utilisation des groupes de sécurité.

Tarification

L'utilisation de groupes de sécurité n'entraîne aucuns frais supplémentaires.

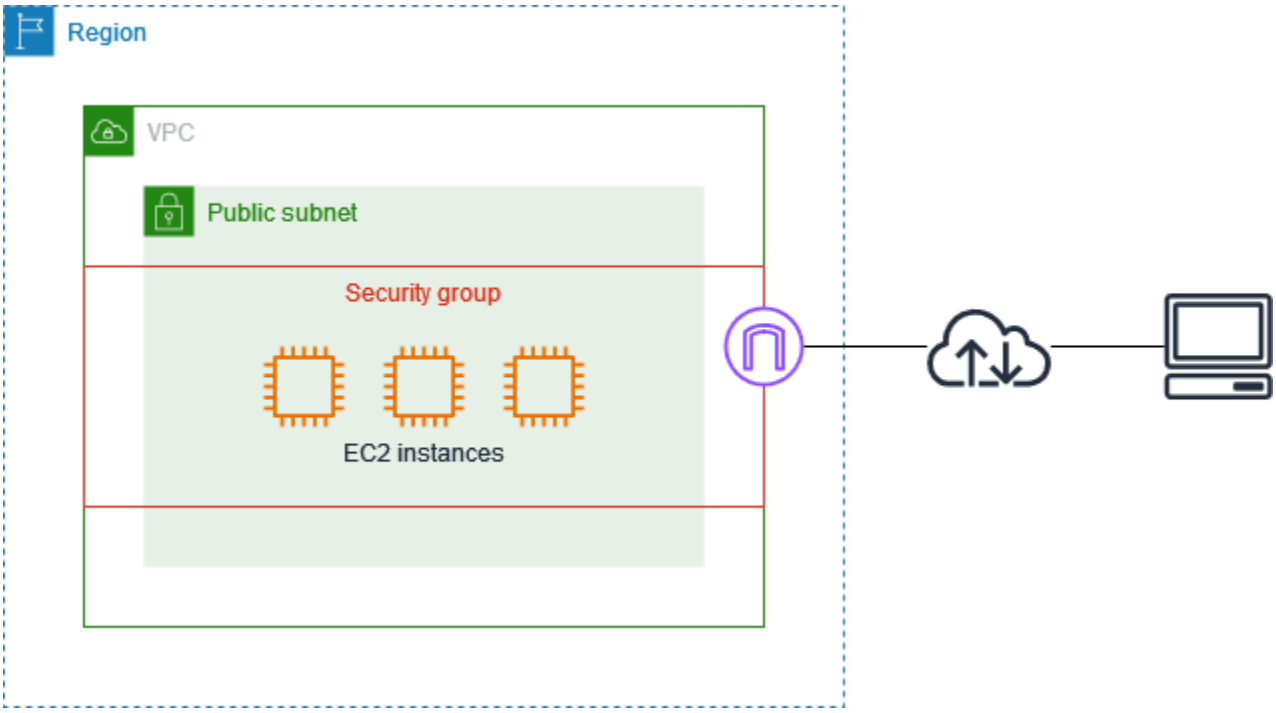
Table des matières

Présentation

Un groupe de sécurité ne peut être utilisé que dans celui VPC pour lequel il a été créé. Vous pouvez associer chaque instance à plusieurs groupes de sécurité, et vous pouvez associer chaque groupe de sécurité à plusieurs instances. Vous ajoutez des règles à chaque groupe de sécurité pour autoriser le trafic vers ou depuis ses instances associées. Vous pouvez modifier les règles pour un groupe de sécurité à la fois. Les nouvelles règles sont automatiquement appliquées à toutes les instances associées au groupe de sécurité. Lorsqu'Amazon EC2 décide d'autoriser ou non le

trafic à atteindre une instance, il évalue toutes les règles de tous les groupes de sécurité associés à l'instance. Pour plus d'informations, consultez la section Règles relatives aux groupes de sécurité dans le guide de VPC l'utilisateur Amazon.

Le schéma suivant montre VPC un sous-réseau, une passerelle Internet et un groupe de sécurité. Le sous-réseau contient des EC2 instances. Le groupe de sécurité est associé aux instances. Le seul trafic qui atteint l'instance est le trafic autorisé par les règles du groupe de sécurité. Par exemple, si le groupe de sécurité contient une règle qui autorise le SSH trafic en provenance de votre réseau, vous pouvez vous connecter à votre instance depuis votre ordinateur à l'aide deSSH. Si le groupe de sécurité contient une règle qui autorise tout le trafic provenant des ressources qui lui sont associées, chaque instance peut recevoir le trafic envoyé par les autres instances.



Les groupes de sécurité sont dynamiques. Si vous envoyez une demande à partir de votre instance, le trafic de la réponse à cette demande est autorisé, indépendamment des règles entrantes des groupes de sécurité. En outre, les réponses au trafic entrant autorisé sont autorisées à sortir, quelles que soient les règles de sortie. Pour de plus amples informations, veuillez consulter Suivi de la connexion.

Créez un groupe de sécurité pour votre EC2 instance Amazon

Les groupes de sécurité font office de pare-feu pour les instances associées, en contrôlant le trafic entrant et le trafic sortant au niveau de l'instance. Vous pouvez ajouter des règles à un groupe de sécurité qui vous permettent de vous connecter à votre instance en utilisant SSH (instances Linux) ou

RDP (instances Windows). Vous pouvez également ajouter des règles qui autorisent le trafic client, par exemple, HTTP et HTTPS le trafic destiné à un serveur Web.

Vous pouvez associer un groupe de sécurité à une instance lorsque vous lancez l'instance. Lorsque vous ajoutez ou supprimez des règles dans des groupes de sécurité associés, ces modifications sont automatiquement appliquées à toutes les instances auxquelles vous avez associé le groupe de sécurité.

Après avoir lancé une instance, vous pouvez associer des groupes de sécurité supplémentaires. Pour de plus amples informations, veuillez consulter Modifier les groupes de sécurité pour votre EC2 instance Amazon.

Vous pouvez ajouter des règles de groupe de sécurité entrant et sortant lorsque vous créez un groupe de sécurité ou vous pouvez les ajouter ultérieurement. Pour de plus amples informations, veuillez consulter Configuration des règles du groupe de sécurité. Pour obtenir des exemples de règles que vous pouvez ajouter à un groupe de sécurité, consultezRègles de groupe de sécurité pour différents cas d'utilisation.

Considérations

- Par défaut, les nouveaux groupes de sécurité commencent avec seulement une règle de trafic sortant, qui permet à la totalité du trafic de quitter la ressource. Vous devez ajouter des règles pour activer un trafic entrant ou limiter le trafic sortant.
- Lorsque vous configurez une source pour une règle autorisant SSH ou RDP accédant à vos instances, n'autorisez pas l'accès de n'importe où, car cela autoriserait cet accès à votre instance à partir de toutes les adresses IP sur Internet. Cette solution est acceptable pour une brève durée dans un environnement de test, mais n'est pas sécurisée pour les environnements de production.
- S'il existe plusieurs règles pour un port spécifique, Amazon EC2 applique la règle la plus permissive. Par exemple, si vous avez une règle qui autorise l'accès au TCP port 22 (SSH) à partir de l'adresse IP 203.0.113.1, et une autre règle qui autorise l'accès au TCP port 22 depuis n'importe où, alors tout le monde a accès au port 22. TCP
- Vous pouvez associer plusieurs groupes de sécurité à une instance. Par conséquent, une instance peut avoir des centaines de règles qui s'appliquent. Cela peut entraîner des problèmes quand vous accédez à l'instance. Nous vous recommandons de condenser vos règles autant que possible.
- Quand vous spécifiez un groupe de sécurité comme source ou destination d'une règle, celle-ci affecte toutes les instances associées au groupe de sécurité. Le trafic entrant est autorisé en fonction des adresses IP privées des instances associées au groupe de sécurité source (et non

des adresses IP Elastic ou des adresses IP publiques). Pour plus d'informations sur les adresses IP, consultez Adressage IP de l'EC2instance Amazon.

- Amazon EC2 bloque le trafic sur le port 25 par défaut. Pour de plus amples informations, veuillez consulter Restriction sur les e-mails envoyés à l'aide du port 25.

Pour créer un groupe de sécurité à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité).
3. Sélectionnez Create security group (Créer un groupe de sécurité).
4. Entrez un nom descriptif et une brève description pour le groupe de sécurité. Vous ne pouvez pas modifier le nom et la description d'un groupe de sécurité une fois celui-ci créé.
5. Pour VPCcela, choisissez l'instance VPC dans laquelle vous allez exécuter vos EC2 instances Amazon.
6. (Facultatif) Pour ajouter des règles entrantes, choisissez Règles entrantes. Pour chaque règle, choisissez Ajouter une règle et spécifiez le protocole, le port et la source. Par exemple, pour autoriser SSH le trafic, choisissez SSHType et spécifiez l'IPv4adresse publique de votre ordinateur ou de votre réseau pour Source.
7. (Facultatif) Pour ajouter des règles sortantes, choisissez Règles sortantes. Pour chaque règle, choisissez Ajouter une règle et spécifiez le protocole, le port et la destination. Sinon, vous pouvez conserver la règle par défaut, qui autorise tout le trafic sortant.
8. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
9. Sélectionnez Create security group (Créer un groupe de sécurité).

Pour créer un groupe de sécurité à l'aide de la ligne de commande

- create-security-group (AWS CLI)
- New-EC2SecurityGroup (AWS Tools for Windows PowerShell)

Modifier les groupes de sécurité pour votre EC2 instance Amazon

Vous pouvez spécifier des groupes de sécurité pour vos EC2 instances Amazon lorsque vous les lancez. Après avoir lancé une instance, vous pouvez ajouter ou supprimer des groupes de sécurité.

Vous pouvez également ajouter, supprimer ou modifier des règles de groupe de sécurité pour les groupes de sécurité associés à tout moment.

Les groupes de sécurité sont associés à des interfaces réseau. L'ajout ou la suppression de groupes de sécurité modifie les groupes de sécurité associés à l'interface réseau principale. Vous pouvez également modifier les groupes de sécurité associés à toute interface réseau secondaire. Pour de plus amples informations, veuillez consulter Modifier les attributs d'interface réseau.

Tâches

- Ajouter ou supprimer des groupes de sécurité
- Configuration des règles du groupe de sécurité

Ajouter ou supprimer des groupes de sécurité

Après avoir lancé une instance, vous pouvez ajouter ou supprimer des groupes de sécurité dans la liste des groupes de sécurité associés. Quand vous associez plusieurs groupes de sécurité à une instance, les règles de chaque groupe de sécurité sont effectivement regroupées pour créer un seul ensemble de règles. Amazon EC2 utilise cet ensemble de règles pour déterminer s'il convient d'autoriser le trafic.

Prérequis

- L'instance doit être dans l'état `running` ou `stopped`.
- Un groupe de sécurité est spécifique à unVPC. Vous pouvez associer un groupe de sécurité à une ou plusieurs instances.

Pour modifier les groupes de sécurité d'une instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez votre instance, puis Actions (Actions), Security (Sécurité), Change security groups (Modifier les groupes de sécurité).
4. Pour Associated security groups (Groupes de sécurité associés), sélectionnez un groupe de sécurité dans la liste et choisissez Add security group (Ajouter un groupe de sécurité).

   Pour supprimer un groupe de sécurité déjà associé, choisissez Remove (Supprimer) pour ce groupe de sécurité.

5. Choisissez Save (Enregistrer).

Pour modifier les groupes de sécurité d'une instance à l'aide de la ligne de commande

- modify-instance-attribute (AWS CLI)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Configuration des règles du groupe de sécurité

Après avoir créé un groupe de sécurité, vous pouvez ajouter, mettre à jour et supprimer ses règles de groupe de sécurité. Lorsque vous ajoutez, mettez à jour ou supprimez une règle, la modification est automatiquement appliquée aux ressources associées au groupe de sécurité.

Pour obtenir des exemples de règles que vous pouvez ajouter à un groupe de sécurité, consultezRègles de groupe de sécurité pour différents cas d'utilisation.

Sources et destinations

Vous pouvez spécifier les sources suivantes pour les règles entrantes ou comme destinations pour les règles sortantes.

- Personnalisé : IPv4 CIDR bloc, IPv6 CIDR bloc, autre groupe de sécurité ou liste de préfixes.
- N'importe où- IPv4 — Le bloc 0.0.0.0/0 IPv4CIDR.
- N'importe où- IPv6 — Le bloc : IPv6 CIDR :/0.
- Mon adresse IP — L'IPv4adresse publique de votre ordinateur local.

> **Warning**
>
> Si vous ajoutez des règles entrantes pour les ports 22 (SSH) ou 3389 (RDP), nous vous recommandons vivement de n'autoriser que l'adresse IP ou la plage d'adresses spécifiques qui ont besoin d'accéder à vos instances. Si vous choisissez Anywhere- IPv4, vous autorisez le trafic provenant de toutes les IPv4 adresses à accéder à vos instances en utilisant le protocole spécifié. Si vous choisissez Anywhere- IPv6, vous autorisez le trafic provenant de toutes les IPv6 adresses à accéder à vos instances en utilisant le protocole spécifié.

Pour configurer les règles des groupes de sécurité à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Groupes de sécurité.
3. Sélectionnez le groupe de sécurité.
4. Pour modifier les règles entrantes, choisissez Modifier les règles entrantes dans Actions ou dans l'onglet Règles entrantes.

   a. Pour ajouter une règle, choisissez Ajouter une règle et entrez le type, le protocole, le port et la source de la règle.

      Si le type est TCP ouUDP, vous devez saisir la plage de ports pour autoriser. Pour la personnalisationICMP, vous devez choisir le nom du ICMP type dans Protocol et, le cas échéant, le nom de code dans Port range. Pour tous les autres types, le protocole et la plage de ports sont configurés automatiquement.

   b. Pour mettre à jour une règle, modifiez son protocole, sa description et sa source selon vos besoins. Cependant, vous ne pouvez pas modifier le type de source. Par exemple, si la source est un IPv4 CIDR bloc, vous ne pouvez pas spécifier de IPv6 CIDR bloc, de liste de préfixes ou de groupe de sécurité.

   c. Pour supprimer une règle, cliquez sur le bouton Supprimer.

5. Pour modifier les règles sortantes, choisissez Modifier les règles sortantes dans Actions ou dans l'onglet Règles sortantes.

   a. Pour ajouter une règle, choisissez Ajouter une règle et entrez le type, le protocole, le port et la destination de la règle. Vous pouvez également saisir une description facultative.

      Si le type est TCP ouUDP, vous devez saisir la plage de ports pour autoriser. Pour la personnalisationICMP, vous devez choisir le nom du ICMP type dans Protocol et, le cas échéant, le nom de code dans Port range. Pour tous les autres types, le protocole et la plage de ports sont configurés automatiquement.

   b. Pour mettre à jour une règle, modifiez son protocole, sa description et sa source selon vos besoins. Cependant, vous ne pouvez pas modifier le type de source. Par exemple, si la source est un IPv4 CIDR bloc, vous ne pouvez pas spécifier de IPv6 CIDR bloc, de liste de préfixes ou de groupe de sécurité.

   c. Pour supprimer une règle, cliquez sur le bouton Supprimer.

6. Sélectionnez Enregistrer les règles.

Pour configurer les règles des groupes de sécurité à l'aide du AWS CLI

- Ajouter — Utilisez les authorize-security-group-egresscommandes authorize-security-group-ingresset.
- Supprimer — Utilisez les revoke-security-group-egresscommandes revoke-security-group-ingresset.
- Modifier — Utilisez les modify-security-group-rulescommandes update-security-group-rule-descriptions-ingress et -descriptions-egress. update-security-group-rule

Pour configurer les règles des groupes de sécurité à l'aide des Outils pour Windows PowerShell

- Ajouter — Utilisez Grant-EC2SecurityGroupIngressetGrant-EC2SecurityGroupEgress.
- Supprimer — Utilisez Revoke-EC2SecurityGroupIngressetRevoke-EC2SecurityGroupEgress.
- Modifier — Utilisez Edit-EC2SecurityGroupRuleUpdate-EC2SecurityGroupRuleIngressDescription, et Update-EC2SecurityGroupRuleEgressDescription.

Supprimer un groupe EC2 de sécurité Amazon

Lorsque vous avez terminé avec un groupe de sécurité que vous avez créé pour être utilisé avec vos EC2 instances Amazon, vous pouvez le supprimer.

Prérequis

- Le groupe de sécurité ne peut pas être associé à une instance ou à une interface réseau.
- Le groupe de sécurité ne peut pas être référencé par une règle d'un autre groupe de sécurité.

Pour supprimer un groupe de sécurité à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. (Facultatif) Pour vérifier que votre groupe de sécurité n'est pas associé à une instance, procédez comme suit :
   a. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité).
   b. Copiez l'ID du groupe de sécurité à supprimer.
   c. Dans le panneau de navigation, choisissez Instances.

   d. Dans la barre de recherche, ajouter le groupe de sécurité IDs équivaut à filtrer et collez l'ID du groupe de sécurité. S'il n'y a aucun résultat, le groupe de sécurité n'est pas associé à une instance. Dans le cas contraire, vous devez dissocier le groupe de sécurité avant de pouvoir le supprimer.

3. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité).
4. Sélectionnez le groupe de sécurité, puis choisissez Actions, Supprimer les groupes de sécurité.
5. Si vous avez sélectionné plusieurs groupes de sécurité, vous êtes invité à confirmer. Si certains groupes de sécurité ne peuvent pas être supprimés, nous affichons le statut de chaque groupe de sécurité, qui indique s'il sera supprimé. Pour confirmer la suppression, saisissez Supprimer.
6. Sélectionnez Delete (Supprimer).

Pour supprimer un groupe de sécurité à l'aide de la ligne de commande

- delete-security-group (AWS CLI)
- Remove-EC2SecurityGroup (AWS Tools for Windows PowerShell)

Suivi des connexions du groupe de EC2 sécurité Amazon

Vos groupes de sécurité utilisent le suivi de connexion pour suivre les informations sur le trafic en provenance ou à destination de l'instance. Les règles s'appliquent en fonction de l'état de connexion du trafic pour déterminer si le trafic est autorisé ou refusé. Avec cette approche, les groupes de sécurité sont avec état. Les groupes de sécurité peuvent ainsi être avec état. Les réponses au trafic entrant sont autorisées à transiter en dehors de l'instance, indépendamment des règles sortantes des groupes de sécurité (et inversement).

Supposons par exemple que vous initiez une commande telle que netcat ou similaire pour vos instances depuis votre ordinateur personnel et que les règles de votre groupe de sécurité entrant autorisent ICMP le trafic. Les informations sur la connexion (y compris sur le port) sont suivies. Le trafic de réponse provenant de l'instance pour la commande n'est pas suivi en tant que nouvelle demande, mais plutôt en tant que connexion établie, et est autorisé à sortir de l'instance, même si les règles de votre groupe de sécurité sortant limitent le trafic sortantICMP.

Pour les protocoles autres que TCPUDP, ouICMP, seuls l'adresse IP et le numéro de protocole sont suivis. Si votre instance envoie le trafic vers un autre hôte et que l'hôte envoie le même type de trafic vers votre instance dans un délai de 600 secondes, le groupe de sécurité de votre instance l'accepte

indépendamment des règles de groupe de sécurité entrantes. Le groupe de sécurité l'accepte, car il est considéré comme un trafic de réponse pour le trafic d'origine.

Lorsque vous modifiez une règle de groupe de sécurité, ses connexions suivies ne sont pas immédiatement interrompues. Le groupe de sécurité continue d'autoriser les paquets jusqu'à l'expiration des connexions existantes. Pour vous assurer que le trafic est immédiatement interrompu ou que l'ensemble du trafic est soumis à des règles de pare-feu quel que soit l'état du suivi, vous pouvez utiliser un réseau ACL pour votre sous-réseau. ACLsLes réseaux sont apatrides et n'autorisent donc pas automatiquement le trafic de réponse. L'ajout d'un réseau ACL bloquant le trafic dans les deux sens interrompt les connexions existantes. Pour plus d'informations, consultez la section Réseau ACLs dans le guide de VPC l'utilisateur Amazon.

> **Note**
>
> Les groupes de sécurité n'ont aucun effet sur le DNS trafic à destination ou en provenance du résolveur Route 53, parfois appelé « adresse IP VPC +2 » (voir Qu'est-ce qu'Amazon Route 53 Resolver ? dans le guide du développeur Amazon Route 53), ou le « AmazonProvided DNS » (voir Travailler avec des ensembles d'DHCPoptions dans le guide de l'utilisateur d'Amazon Virtual Private Cloud). Si vous souhaitez filtrer les DNS demandes via le résolveur Route 53, vous pouvez activer le DNS pare-feu Route 53 Resolver (voir Route 53 Resolver DNS Firewall dans le guide du développeur Amazon Route 53).

Connexions non suivies

Certains flux de trafic ne sont pas suivis. Si une règle de groupe de sécurité autorise TCP ou UDP circule pour tout le trafic (0.0.0.0/0 ou : :/0) et qu'il existe une règle correspondante dans l'autre sens qui autorise tout le trafic de réponse (0.0.0.0/0 ou : :/0) pour n'importe quel port (0-65535), ce flux de trafic n'est pas suivi, sauf s'il fait partie d'une connexion suivie automatiquement. Le trafic de la réponse d'un flux non suivi est autorisé en fonction de la règle entrante ou sortante qui autorise le trafic de la réponse, et non des informations de suivi.

Un flux de trafic non suivi est immédiatement interrompu si la règle qui active le flux est supprimée ou modifiée. Par exemple, si vous avez une règle sortante ouverte (0.0.0.0/0) et que vous supprimez une règle qui autorise tout le trafic entrant (0.0.0.0/0) (TCPport 22) à destination de l'instance SSH (ou si vous la modifiez pour que la connexion ne soit plus autorisée), vos connexions existantes SSH à l'instance sont immédiatement supprimées. La connexion n'était pas suivie auparavant, de sorte que la modification rompt la connexion. En revanche, si vous avez une règle entrante plus étroite

qui autorise initialement une SSH connexion (c'est-à-dire que la connexion a été suivie), mais que vous modifiez cette règle pour ne plus autoriser de nouvelles connexions à partir de l'adresse du SSH client actuel, la SSH connexion existante n'est pas interrompue car elle est suivie.

Connexions suivies automatiquement

Les connexions établies via les méthodes suivantes sont automatiquement suivies, même si la configuration du groupe de sécurité ne nécessite pas de suivi par ailleurs :

- Passerelles Internet de sortie uniquement
- Accélérateurs Global Accelerator
- NATpasserelles
- Points de terminaison de pare-feu Network Firewall
- Network Load Balancers
- AWS PrivateLink (VPCpoints de terminaison de l'interface)
- AWS Lambda (Interfaces réseau élastiques Hyperplane)

Allocations de suivi des connexions

Amazon EC2 définit le nombre maximum de connexions pouvant être suivies par instance. Une fois le maximum atteint, tous les paquets envoyés ou reçus sont abandonnées, car une nouvelle connexion ne peut pas être établie. Lorsque cela se produit, les applications qui envoient et reçoivent des paquets ne peuvent pas communiquer correctement. Utilisez la métrique de performance réseau `conntrack_allowance_available` pour déterminer le nombre de connexions suivies encore disponibles pour ce type d'instance.

Pour déterminer si des paquets ont été abandonnés parce que le trafic réseau de votre instance a dépassé le nombre maximal de connexions pouvant être suivies, utilisez la métrique de performance réseau `conntrack_allowance_exceeded`. Pour plus d'informations, consultez Surveillez les performances du réseau pour ENA les paramètres de votre EC2 instance.

Avec Elastic Load Balancing, si vous dépassez le nombre maximal de connexions pouvant être suivies par instance, nous vous recommandons de mettre à l'échelle soit le nombre d'instances enregistrées auprès de l'équilibreur de charge, soit la taille des instances enregistrées auprès de l'équilibreur de charge.

Considérations relatives aux performances du suivi des connexions

Le routage asymétrique, selon lequel le trafic entre dans une instance via une interface réseau et sort par une interface réseau différente, peut réduire les performances maximales qu'une instance peut atteindre si les flux sont suivis.

Pour maintenir des performances optimales lorsque le suivi des connexions est activé pour vos groupes de sécurité, nous recommandons la configuration suivante :

- Évitez les topologies de routage asymétriques, si possible.
- Au lieu d'utiliser des groupes de sécurité pour le filtrage, utilisez le réseauACLs.
- Si vous devez utiliser des groupes de sécurité avec suivi des connexions, configurez le délai d'expiration de connexion le plus court possible.

Pour plus d'informations sur le réglage des performances du système Nitro, consultezConsidérations relatives au système Nitro pour le réglage des performances.

Délai de suivi d'inactivité de la connexion

Le groupe de sécurité assure le suivi de chaque connexion établie pour que les paquets de retour soient livrés comme prévu. Il existe un nombre maximal de connexions qui peuvent être suivies par instance. Les connexions qui restent inactives peuvent entraîner l'épuisement du suivi des connexions, empêcher le suivi des connexions et entraîner la perte de paquets. Vous pouvez définir le délai pour le suivi d'inactivité de la connexion sur une interface réseau Elastic.

> **Note**
>
> Cette fonctionnalité n'est disponible que pour les instances créées sur le système AWS Nitro.

Il existe trois délais configurables :

- TCPdélai établi : délai d'expiration (en secondes) pour les TCP connexions inactives dans un état établi. Min. : 60 secondes. Max. : 432 000 secondes (5 jours). Par défaut : 432 000 secondes. Recommandé : moins de 432 000 secondes.
- UDPdélai d'attente : délai d'expiration (en secondes) pour les UDP flux inactifs qui n'ont vu du trafic que dans une seule direction ou une seule transaction demande-réponse. Min. : 30 secondes. Max. : 60 secondes. Par défaut : 30 secondes.

- UDPdélai d'expiration du flux : délai d'expiration (en secondes) pour les UDP flux inactifs classés comme des flux ayant fait l'objet de plusieurs transactions requête-réponse. Min. : 60 secondes. Max. : 180 secondes (3 minutes). Par défaut : 180 secondes.

Vous pouvez modifier les délais par défaut dans les cas suivants :

- Si vous surveillez les connexions suivies à l'aide des indicateurs de performance du EC2 réseau Amazon, les indicateurs conntrack_allowance_exceeded et conntrack_allowance_available vous permettent de surveiller les paquets abandonnés et de suivre l'utilisation des connexions afin de gérer de manière proactive la capacité des EC2 instances grâce à des actions d'extension ou de réduction afin de répondre à la demande de connexions réseau avant de supprimer des paquets. Si vous observez des baisses de conntrack_allowance_exceeded sur vos EC2 instances, il peut être avantageux de définir un délai d'expiration plus court pour tenir compte TCP des UDP sessions périmées résultant de clients ou de boîtiers TCP réseau inappropriés.
- Généralement, les équilibreurs de charge ou les pare-feux ont un délai d'inactivité TCP établi compris entre 60 et 90 minutes. Si vous exécutez des charges de travail censées gérer un très grand nombre de connexions (supérieures à 100 000) à partir d'appareils tels que des pare-feux réseau, il est conseillé de configurer un délai d'expiration similaire sur une interface EC2 réseau.
- Si vous exécutez une charge de travail qui utilise une topologie de routage asymétrique, nous vous recommandons de configurer un délai d'inactivité TCP établi de 60 secondes.
- Si vous exécutez des charges de travail comportant un nombre élevé de connexionsDNS, tels que Syslog SIPSNMP, Radius et d'autres services principalement utilisés UDP pour répondre aux demandes, le fait de définir le délai d'expiration « UDP -stream » sur 60 permet d'améliorer l'évolutivité et les performances de la capacité existante et d'éviter les défaillances grises.
- Pour les UDP connexionsTCP/via les équilibreurs de charge réseau (NLBs) et les équilibreurs de charge élastiques (ELB), toutes les connexions sont suivies. La valeur du délai d'inactivité pour les TCP flux est de 350 secondes et les UDP flux de 120 secondes. Elle varie en fonction des valeurs de délai d'inactivité au niveau de l'interface. Vous souhaiterez peut-être configurer les délais d'expiration au niveau de l'interface réseau afin de permettre une plus grande flexibilité que les délais par défaut pour/. ELB NLB

Vous avez la possibilité de configurer les délais du suivi des connexions lorsque vous effectuez les actions suivantes :

- Créer une interface réseau

- Modifier les attributs d'interface réseau
- Lancer une EC2 instance
- Création d'un modèle de lancement d'EC2instance

Exemple

Dans l'exemple suivant, le groupe de sécurité possède des règles entrantes qui autorisent le ICMP trafic TCP et des règles sortantes qui autorisent tout le trafic sortant.

Entrant

Type de protocole	Numéro de port	Source
TCP	22 (SSH)	203.0.113.1/32
TCP	80 (HTTP)	0.0.0.0/0
TCP	80 (HTTP)	::/0
ICMP	Tous	0.0.0.0/0

Sortant

Type de protocole	Numéro de port	Destination
Tous	Tous	0.0.0.0/0
Tous	Tous	::/0

Avec une connexion réseau directe à l'instance ou à l'interface réseau, le suivi se comporte comme suit :

- Le TCP trafic entrant et sortant sur le port 22 (SSH) est suivi, car la règle de trafic entrant n'autorise que le trafic provenant de 203.0.113.1/32, et non de toutes les adresses IP (0.0.0.0/0).
- Le TCP trafic entrant et sortant sur le port 80 (HTTP) n'est pas suivi, car les règles entrantes et sortantes autorisent le trafic provenant de toutes les adresses IP.
- ICMPle trafic est toujours suivi.

Si vous supprimez la règle de trafic sortant, tout le IPv4 trafic entrant et sortant est suivi, y compris le IPv4 trafic sur le port 80 (). HTTP Il en va de même pour IPv6 le trafic si vous supprimez la règle de trafic sortant pour le IPv6 trafic.

Règles de groupe de sécurité pour différents cas d'utilisation

Vous pouvez créer un groupe de sécurité et ajouter des règles qui reflètent le rôle de l'instance qui est associée à ce groupe. Par exemple, une instance configurée en tant que serveur Web a besoin de règles de groupe de sécurité qui autorisent l'entrée HTTP et l'HTTPSaccès. De même, une instance de base de données a besoin de règles qui autorisent l'accès au type de base de données, comme l'accès via le port 3306 pour MySQL.

Voici des exemples de types de règles que vous pouvez ajouter à des groupes de sécurité pour des types d'accès spécifiques.

Exemples

- Règles de serveur web
- Règles de serveur de base de données
- Règles pour la connexion à des instances à partir de votre ordinateur
- Règles pour la connexion à des instances à partir d'une instance avec le même groupe de sécurité
- Règles pour le ping/ ICMP
- DNSrègles du serveur
- EFSRègles d'Amazon
- Règles Elastic Load Balancing

Règles de serveur web

Les règles de trafic entrant suivantes autorisent HTTP l'HTTPSaccès à partir de n'importe quelle adresse IP. Si vous êtes VPC activé pourIPv6, vous pouvez ajouter des règles pour contrôler le HTTPS trafic entrant HTTP et en provenance des IPv6 adresses.

Type de protocole	Numéro de protocole	Port	IP Source	Remarques
TCP	6	80 (HTTP)	0.0.0.0/0	Permet l'HTTPaccès entrant depuis n'importe quelle adresse IPv4
TCP	6	443 (HTTPS)	0.0.0.0/0	Permet l'HTTPSaccès entrant depuis n'importe quelle adresse IPv4
TCP	6	80 (HTTP)	::/0	Permet l'HTTPaccès entrant depuis n'importe quelle adresse IPv6
TCP	6	443 (HTTPS)	::/0	Permet l'HTTPSaccès entrant depuis n'importe quelle adresse IPv6

Règles de serveur de base de données

Les règles entrantes suivantes sont des exemples de règles que vous pouvez ajouter pour un accès à une base de données selon le type de base de données que vous exécutez sur votre instance. Pour plus d'informations sur les RDS instances Amazon, consultez le guide de RDS l'utilisateur Amazon.

Pour l'adresse IP source, spécifiez l'une des options suivantes :

- Une adresse IP spécifique ou une plage d'adresses IP (en notation par CIDR blocs) sur votre réseau local
- Un ID de groupe de sécurité pour un groupe d'instances qui accèdent à la base de données

Type de protocole	Numéro de protocole	Port	Remarques
TCP	6	1433 (MSSQL)	Port par défaut pour accéder à une base de données Microsoft SQL

Type de protocole	Numéro de protocole	Port	Remarques
			Server, par exemple, sur une RDS instance Amazon
TCP	6	3306 (MYSQL/ Aurore)	Port par défaut pour accéder à une base de données My SQL ou Aurora, par exemple, sur une RDS instance Amazon
TCP	6	5439 (Redshift)	Port par défaut pour accéder à une base de données de cluster Amazon Redshift.
TCP	6	5432 (SQLPoster)	Le port par défaut pour accéder à une SQL base de données Postgre, par exemple, sur une instance Amazon RDS
TCP	6	1521 (Oracle)	Port par défaut pour accéder à une base de données Oracle, par exemple, sur une RDS instance Amazon

Vous pouvez éventuellement restreindre le trafic sortant de vos serveurs de base de données. Par exemple, vous pouvez autoriser l'accès à Internet pour les mises à jour logicielles, mais limiter tous les autres types de trafic. Vous devez d'abord supprimer la règle sortante par défaut qui autorise tout le trafic sortant.

Type de protocole	Numéro de protocole	Port	IP de destination	Remarques
TCP	6	80 (HTTP)	0.0.0.0/0	Permet l'HTTPaccès sortant à n'importe quelle adresse IPv4

Type de protocole	Numéro de protocole	Port	IP de destination	Remarques
TCP	6	443 (HTTPS)	0.0.0.0/0	Permet l'HTTPSaccès sortant à n'importe quelle adresse IPv4
TCP	6	80 (HTTP)	::/0	(IPv6activé VPC uniquement) Autorise l'HTTPaccès sortant à n'importe quelle adresse IPv6
TCP	6	443 (HTTPS)	::/0	(IPv6activé VPC uniquement) Autorise l'HTTPSaccès sortant à n'importe quelle adresse IPv6

Règles pour la connexion à des instances à partir de votre ordinateur

Pour se connecter à votre instance, votre groupe de sécurité doit disposer de règles entrantes autorisant l'SSHaccès (pour les instances Linux) ou l'RDPaccès (pour les instances Windows).

Type de protocole	Numéro de protocole	Port	IP Source
TCP	6	22 (SSH)	L'IPv4adresse publique de votre ordinateur ou une série d'adresses IP de votre réseau local. Si vous êtes VPC activé pour IPv6 et que votre instance possède une IPv6 adresse, vous pouvez saisir une IPv6 adresse ou une plage.
TCP	6	389 () RDP	L'IPv4adresse publique de votre ordinateur ou une série d'adresses IP de votre réseau local. Si vous êtes VPC activé pour IPv6 et que votre

Type de protocole	Numéro de protocole	Port	IP Source
			instance possède une IPv6 adresse, vous pouvez saisir une IPv6 adresse ou une plage.

Règles pour la connexion à des instances à partir d'une instance avec le même groupe de sécurité

Pour autoriser les instances associées au même groupe de sécurité à communiquer les unes avec les autres, vous devez à cette fin ajouter des règles explicitement.

> **Note**
>
> Si vous configurez des acheminements pour transférer le trafic entre deux instances de sous-réseaux différents via une appliance middlebox, vous devez vous assurer que les groupes de sécurité des deux instances autorisent le trafic à transiter entre les instances. Le groupe de sécurité de chaque instance doit faire référence à l'adresse IP privée de l'autre instance, ou à la CIDR plage du sous-réseau qui contient l'autre instance, comme source. Si vous référencez le groupe de sécurité de l'autre instance en tant que source, cela n'autorise pas le trafic à transiter entre les instances.

Le tableau suivant décrit la règle entrante pour un groupe de sécurité qui permet aux instances associées de communiquer les unes avec les autres. La règle autorise tous les types de trafic.

Type de protocole	Numéro de protocole	Ports	IP Source
-1 (Tout)	-1 (Tout)	-1 (Tout)	L'ID du groupe de sécurité ou la CIDR plage du sous-réseau qui contient l'autre instance (voir note).

Règles pour le ping/ ICMP

La ping commande est un type de ICMP trafic. Pour envoyer un ping à votre instance, vous devez ajouter l'une des ICMP règles entrantes suivantes.

Type	Protocole	Source		
Personnalisé ICMP - IPv4	Demande Echo	L'IPv4adresse publique de votre ordinateur, une IPv4 adresse spécifique ou une IPv6 adresse IPv4 OR depuis n'importe où.		
Tout ICMP - IPv4	IPv4ICMP(1)	L'IPv4adresse publique de votre ordinateur, une IPv4 adresse spécifique ou une IPv6 adresse IPv4 OR depuis n'importe où.		

Pour utiliser la ping6 commande pour envoyer un ping à l'IPv6adresse de votre instance, vous devez ajouter la ICMPv6 règle entrante suivante.

Type	Protocole	Source		
Tout ICMP - IPv6	IPv6ICMP(58)	L'IPv6adresse de votre ordinateur, une IPv4 adresse spécifique		

Type	Protocole	Source		
		ou une IPv4 adresse ou depuis n'importe quel endroit. IPv6		

DNSrègles du serveur

Si vous avez configuré votre EC2 instance en tant que DNS serveur, vous devez vous assurer que TCP le UDP trafic peut atteindre votre DNS serveur via le port 53.

Pour l'adresse IP source, spécifiez l'une des options suivantes :

- Adresse IP ou plage d'adresses IP (en notation par CIDR blocs) dans un réseau
- L'ID d'un groupe de sécurité pour l'ensemble des instances de votre réseau qui nécessitent un accès au DNS serveur

Type de protocole	Numéro de protocole	Port
TCP	6	53
UDP	17	53

EFSRègles d'Amazon

Si vous utilisez un système de EFS fichiers Amazon avec vos EC2 instances Amazon, le groupe de sécurité que vous associez à vos cibles de EFS montage Amazon doit autoriser le trafic via le NFS protocole.

Type de protocole	Numéro de protocole	Ports	IP Source	Remarques
TCP	6	2049 () NFS	ID du groupe de sécurité	Autorise l'NFSaccès entrant depuis les

Type de protocole	Numéro de protocole	Ports	IP Source	Remarques
				ressources (y compris la cible de montage) associées à ce groupe de sécurité

Pour monter un système de EFS fichiers Amazon sur votre EC2 instance Amazon, vous devez vous connecter à votre instance. Par conséquent, le groupe de sécurité associé à votre instance doit disposer de règles autorisant le trafic entrant SSH depuis votre ordinateur local ou votre réseau local.

Type de protocole	Numéro de protocole	Ports	IP Source	Remarques
TCP	6	22 (SSH)	La plage d'adresses IP de votre ordinateur local ou la plage d'adresses IP (en notation par CIDR blocs) de votre réseau.	Autorise l'SSHaccès entrant depuis votre ordinateur local.

Règles Elastic Load Balancing

Si vous enregistrez vos EC2 instances auprès d'un équilibreur de charge, le groupe de sécurité associé à votre équilibreur de charge doit autoriser la communication avec les instances. Pour plus d'informations, consultez les informations suivantes dans la documentation d'Elastic Load Balancing.

- Groupes de sécurité pour votre Application Load Balancer
- Groupes de sécurité de votre Network Load Balancer
- Configuration des groupes de sécurité pour votre Classic Load Balancer

Instances Nitro TPM pour Amazon EC2

Le Nitro Trusted Platform Module (NitroTPM) est un appareil virtuel fourni par le système AWS Nitro et conforme à la spécification 2.0. TPM Il stocke en toute sécurité les artefacts (tels que les mots

de passe, les certificats ou les clés de chiffrement) utilisés pour authentifier l'instance. Nitro TPM peut générer des clés et les utiliser pour des fonctions cryptographiques (telles que le hachage, la signature, le chiffrement et le déchiffrement).

Nitro TPM propose un démarrage mesuré, un processus par lequel le chargeur de démarrage et le système d'exploitation créent des hachages cryptographiques de chaque binaire de démarrage et les combinent avec les valeurs précédentes dans les registres de configuration de plate-forme TPM internes de Nitro (). PCRs Avec le démarrage mesuré, vous pouvez obtenir des PCR valeurs signées auprès de Nitro TPM et les utiliser pour prouver à des entités distantes l'intégrité du logiciel de démarrage de l'instance. Cela porte le nom d'attestation distante.

Avec NitroTPM, les clés et les secrets peuvent être marqués d'une PCR valeur spécifique, de sorte qu'ils ne soient jamais accessibles si la PCR valeur et donc l'intégrité de l'instance changent. Cette forme spéciale d'accès conditionnel est appelée scellement et descellement. Les technologies des systèmes d'exploitation BitLocker, telles que Nitro, peuvent utiliser Nitro TPM pour sceller une clé de déchiffrement d'un lecteur afin que le lecteur ne puisse être déchiffré que lorsque le système d'exploitation a démarré correctement et qu'il est dans un état connu comme bon.

Pour utiliser NitroTPM, vous devez sélectionner une image machine Amazon (AMI) configurée pour le TPM support Nitro, puis l'utiliser AMI pour lancer des instances basées sur le système AWS Nitro. Vous pouvez sélectionner l'un des modèles prédéfinis d'Amazon AMIs ou en créer un vous-même.

Tarification

L'utilisation de Nitro TPM n'entraîne aucun coût supplémentaire. Vous payez uniquement les ressources sous-jacentes que vous utilisez.

Table des matières

Conditions requises pour utiliser Nitro TPM avec des instances Amazon EC2

Pour lancer une instance avec Nitro TPM activé, vous devez répondre aux exigences suivantes.

Rubriques

AMIs

Nitro AMI doit être TPM activé.

Linux AMIs

Il n'y a aucune configuration préconfiguréeAMIs. Vous devez configurer le vôtreAMI. Pour de plus amples informations, veuillez consulter Activer un système Linux AMI pour Nitro TPM.

Fenêtres AMIs

Les fenêtres suivantes AMIs sont préconfigurées pour activer Nitro TPM et UEFI Secure Boot avec des clés Microsoft :

- TPM-Windows_Server-2_Anglais-Core-Base
- TPM-Windows_Server-2_Anglais-Base complète
- TPM-Windows_Server-2_Anglais-Complet- _2022_Enterprise SQL
- TPM-Windows_Server-2_Anglais-Complet- _2022_Standard SQL
- TPM-Windows_Server-2019-Anglais-Core-Base
- TPM-Windows_Server-2019-Anglais-Base complète
- TPM-Windows_Server-2019-Anglais-Complet- _2019_Enterprise SQL
- TPM-Windows_Server-2019-Anglais-Complet- _2019_Standard SQL
- TPM-Windows_Server-2016-Anglais-Core-Base
- TPM-Windows_Server-2016-Anglais-Base complète

> **Note**
>
> Système d'exploitation — Le système d'exploitation AMI doit inclure un pilote Command Response Buffer (CRB) TPM 2.0. La plupart des systèmes d'exploitation actuels incluent un CRB pilote TPM 2.0.
> UEFImode de démarrage — AMI Il doit être configuré pour le mode de UEFI démarrage. Pour de plus amples informations, veuillez consulter UEFIDémarrage sécurisé pour les EC2 instances Amazon.

Types d'instances

Vous devez utiliser l'un des types d'instances virtualisées suivants :

- Usage général : M5, M5a, M5ad, M5d, M5dn, M5n, M5zn, M6a, M6g, M6gd, M6i, M6id, M6idn, M6in, M7a, M7g, M7GD, M7i, T3, T3a, T4g
- Optimisé pour le calcul : C5, C5a, C5ad, C5d, C5n, C6a, C6g, C6gd, C6gn, C6i, C6id, C6in, C7a, C7g, C7gd, C7gn, C7i, C7i-Flex
- Mémoire optimisée : R5, R5a, R5ad, R5b, R5d, R5dn, R5n, R6a, R6g, R6gd, R6i, R6idn, R6in, R6id, R7a, R7g, R7gd, R7i, R7iZ, R8g, U7i-12TB, U7in-16TB, U7 en 24 To, U7 en 32 To, X2IDN, X2iEDN, X2ieZN, z1d
- Stockage optimisé : D3, D3en, i3EN, i4i
- Calcul accéléré : G4dn, G5, G6, G6e, Gr6, Inf1, Inf2
- Calcul à hautes performances : HPC6a, HPC6id

Considérations

Les considérations suivantes s'appliquent lors de l'utilisation de Nitro TPM :

- Après avoir lancé une instance à l'aide d'une instance AMI avec Nitro TPM activé, si vous souhaitez modifier le type d'instance, le nouveau type d'instance que vous choisissez doit également prendre en charge TPM Nitro.
- BitLocker les volumes chiffrés avec des clés TPM basées sur Nitro ne peuvent être utilisés que sur l'instance d'origine.
- L'TPMétat Nitro n'est pas affiché dans la EC2 console Amazon.

- L'TPMétat Nitro n'est pas inclus dans les EBSinstantanés Amazon.
- L'TPMétat Nitro n'est pas inclus dans les images VM Import/Export.
- Nitro n'TPMest pas pris en charge sur AWS Outposts., Local Zones ou Wavelength Zones.

Activer un système Linux AMI pour Nitro TPM

Pour activer Nitro TPM pour une instance, vous devez lancer l'instance à l'aide d'un AMI avec Nitro activéTPM. Vous devez configurer votre système Linux AMI avec le TPM support Nitro lorsque vous l'enregistrez. Vous ne pourrez pas configurer le TPM support Nitro ultérieurement.

Pour obtenir la liste des systèmes Windows AMIs préconfigurés pour le TPM support Nitro, consultez. Conditions requises pour utiliser Nitro TPM avec des instances Amazon EC2

Vous devez créer un AMI avec Nitro TPM configuré à l'aide du RegisterImageAPI. Vous ne pouvez pas utiliser la EC2 console Amazon ou VM Import/Export.

Pour activer un système Linux AMI pour Nitro TPM

1. Lancez une instance temporaire avec le système Linux requisAMI. Notez l'ID de son volume racine, que vous pouvez trouver dans la console sous l'onglet Stockage de l'instance.
2. Une fois que l'instance a atteint `running` cet état, créez un instantané du volume racine de l'instance. Vous pouvez utiliser la console ou la commande create-snapshot suivante.

```
aws ec2 create-snapshot  \
    --volume-id vol-1234567890EXAMPLE \
    --description "Snapshot of the root volume"
```

3. Enregistrez l'instantané que vous avez créé en tant queAMI. Vous devez utiliser la commande register-image. Pour `--tpm-support`, spécifiez `v2.0`. Pour `--boot-mode`, spécifiez `uefi`. Dans le mappage des périphériques en mode bloc, spécifiez le cliché que vous avez créé pour le volume racine.

```
aws ec2 register-image \
    --name my-image \
    --boot-mode uefi \
    --architecture x86_64 \
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/xvda,Ebs={SnapshotId=snapshot_id} \
    --tpm-support v2.0
```

Voici un exemple de sortie.

```
{
    "ImageId": "ami-0123456789example"
}
```

4. Mettez fin à l'instance temporaire que vous avez lancée à l'étape 1.

Vérifiez qu'un AMI est activé pour Nitro TPM

Pour activer Nitro TPM pour une instance, vous devez lancer l'instance à l'aide d'un AMI avec Nitro activéTPM. Vous pouvez utiliser l'un `describe-images` ou `describe-image-attributes` l'autre ou pour vérifier qu'un AMI est activé pour NitroTPM. Si Nitro TPM est activé pour leAMI, la valeur pour `TpmSupport` est`"v2.0"`.

Pour décrire l'image

Vous pouvez utiliser la commande describe-images comme suit.

```
aws ec2 describe-images --image-ids ami-0123456789example --query Images[*].TpmSupport
```

Si Nitro TPM est activé pour leAMI, le résultat est le suivant.

```
[
    "v2.0"
]
```

Si TPM ce n'est pas activé, la sortie est vide.

```
[
]
```

Pour décrire l'attribut image

Sinon, si vous êtes le AMI propriétaire, vous pouvez utiliser la describe-image-attributecommande comme suit, en spécifiant `tpmSupport` comme`attribute`.

```
aws ec2 describe-image-attribute \
    --region us-east-1 \
    --image-id ami-0123456789example \
```

```
    --attribute tpmSupport
```

Voici un exemple de sortie.

```
{
    "ImageId": "ami-0123456789example",
    "TpmSupport": {
        "Value": "v2.0"
    }
}
```

Activer ou arrêter d'utiliser Nitro TPM sur une instance Amazon EC2

Vous ne pouvez activer une EC2 instance Amazon pour Nitro TPM qu'au lancement. Une fois qu'une instance est activée pour NitroTPM, vous ne pouvez pas la désactiver. Si vous n'avez plus besoin d'utiliser NitroTPM, vous devez configurer le système d'exploitation pour qu'il cesse de l'utiliser.

Rubriques

- Lancer une instance avec Nitro activé TPM
- Arrêter d'utiliser Nitro TPM sur une instance

Lancer une instance avec Nitro activé TPM

Lorsque vous lancez une instance avec les prérequis, Nitro TPM est automatiquement activé sur l'instance. Vous ne pouvez activer Nitro TPM sur une instance qu'au lancement. Pour plus d'informations sur le lancement d'une instance, consultez Lancer une EC2 instance Amazon.

Arrêter d'utiliser Nitro TPM sur une instance

Après avoir lancé une instance avec Nitro TPM activé, vous ne pouvez pas désactiver Nitro TPM pour l'instance. Toutefois, vous pouvez configurer le système d'exploitation pour qu'il cesse d'utiliser Nitro TPM en désactivant le pilote de périphérique TPM 2.0 sur l'instance à l'aide des outils suivants :

- Pour les instances Linux, utilisez tpm-tools.
- Pour les instances Windows, utilisez la console TPM de gestion (tpm.msc).

Pour plus d'informations sur la désactivation du pilote de périphérique, consultez la documentation de votre système d'exploitation.

Vérifiez qu'une EC2 instance Amazon est activée pour Nitro TPM

Vous pouvez utiliser l'une des méthodes suivantes pour vérifier si une EC2 instance Amazon est activée pour NitroTPM.

Pour vérifier si une instance est activée pour Nitro TPM

Utilisez la commande describe-instances AWS CLI et spécifiez l'ID de l'instance. La EC2 console Amazon n'affiche pas le `TpmSupport` champ.

```
aws ec2 describe-instances --instance-ids i-0123456789example
```

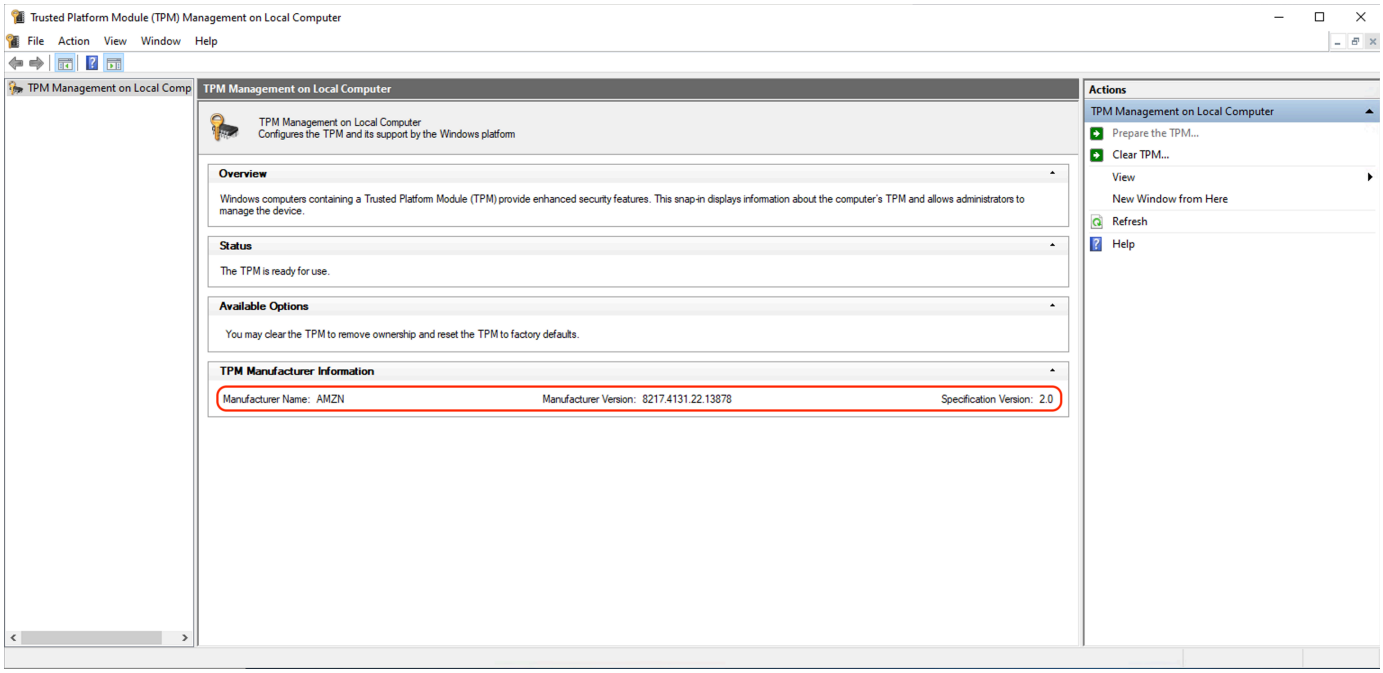
Si le TPM support Nitro est activé sur l'instance, cela `"TpmSupport": "v2.0"` apparaît dans la sortie. Par exemple :

```
"Instances": {
  "InstanceId":"0123456789example",
  "InstanceType":"c5.large",
  ...
  "BootMode": "uefi",
  "TpmSupport": "v2.0"
  ...
}
```

(Instances Windows uniquement) Pour vérifier si le Nitro TPM est accessible à Windows

1. Connectez-vous à votre instance EC2 Windows.
2. Sur l'instance, exécutez le programme tpm.msc.

   La fenêtre TPMGestion sur ordinateur local s'ouvre.
3. Vérifiez le champ Informations sur le TPM fabricant. Il contient le nom du fabricant et la version du Nitro présent TPM sur l'instance.



Récupérez la clé d'approbation publique pour une EC2 instance Amazon

Vous pouvez récupérer en toute sécurité la clé d'approbation publique d'une instance à tout moment à l'aide du AWS CLI.

Pour récupérer la clé d'approbation publique pour une instance

Utilisez la AWS CLI commande get-instance-tpm-ek-pub.

Exemple 1

L'exemple de commande suivant permet d'obtenir la clé d'approbation `rsa-2048` publique au `tpmt` format correspondant à l'instance spécifiée.

```
aws ec2 get-instance-tpm-ek-pub \--instance-id i-01234567890abcdef \
--key-format tpmt \
--key-type rsa-2048
```

Voici un exemple de sortie.

```
{
    "InstanceId": "i-01234567890abcdef",
    "KeyFormat": "tpmt",
    "KeyType": "rsa-2048",
```

```
    "KeyValue": "AAEACwADALIAIINxl2dEhLEXAMPLEUal1yT9UtduBlILZPKh2hszFGmqAAYAgABDA
    EXAMPLEAAABAOiRd7WmgtdGNoV1h/AxmW+CXExblG8pEUfNm0LOLiYnEXAMPLERqApiFa/UhvEYqN4
    Z7jKMD/usbhsQaAB1gKA5RmzuhSazHQkax7EXAMPLEzDthlS7HNGuYn5eG7qnJndRcakS+iNxT8Hvf
    0S1ZtNuItMs+Yp4SO6aU28MT/JZkOKsXIdMerY3GdWbNQz9AvYbMEXAMPLEPyHfzgVO0QTTJVGdDxh
    vxtXCOu9GYf0crbjEXAMPLEd4YTbWdDdgOKWF9fjzDytJSDhrLAOUctNzHPCd/92l5zEXAMPLEOIFA
    Ss50C0/802c17W2pMSVHvCCa9lYCiAfxH/vYKovAAE="
}
```

Exemple 2

L'exemple de commande suivant permet d'obtenir la clé d'approbation `rsa-2048` publique au `der` format correspondant à l'instance spécifiée.

```
aws ec2 get-instance-tpm-ek-pub \
--instance-id i-01234567890abcdef \
--key-format der \
--key-type rsa-2048
```

Voici un exemple de sortie.

```
{
    "InstanceId": "i-01234567890abcdef",
    "KeyFormat": "der",
    "KeyType": "rsa-2048",
    "KeyValue": "MIIBIjANBgEXAMPLEw0BAQEFAAOCAQ8AMIIBCgKCAQEA6JF3taEXAMPLEXWH8DGZb4
    JcTFuUbykRR82bQs4uJifaKSOv5NGoEXAMPLEG8Rio3hnuMowP+6xuGxBoAHWAoDlGbO6FJrMdEXAMP
    LEnYUHvMO2GVLsc0a5ifl4buqcmd1FxqRL6I3FPwe9/REXAMPLE0yz5inhI7ppTbwxP8lmQ4qxch0x6
    tjcZ1Zs1DP0EXAMPLERUYLQ/Id/OBU7RBNMlUZ0PGG/G1cI670Zh/RytuOdx9iEXAMPLEtZ0N2A4pYX
    1+PMPK0lIOGssA5Ry03Mc8J3/3aXnOD2/ASRQ4gUBKznQLT/zTZEXAMPLEJUe8IJr2VgKIB/Ef+9gqi
    8AAQIDAQAB"
}
```

Credential Guard pour les instances Windows

Le système AWS Nitro prend en charge Credential Guard pour les instances Windows Amazon Elastic Compute Cloud EC2 (Amazon). Credential Guard est une fonctionnalité de sécurité basée sur la virtualisation de Windows (VBS) qui permet de créer des environnements isolés pour protéger les actifs de sécurité, tels que les informations d'identification des utilisateurs Windows et l'application de l'intégrité du code, au-delà des protections du noyau Windows. Lorsque vous exécutez des instances EC2 Windows, Credential Guard utilise le système AWS Nitro pour empêcher l'extraction des informations de connexion Windows de la mémoire du système d'exploitation.

Table des matières

Prérequis

Votre instance Windows doit répondre aux conditions préalables suivantes pour utiliser Credential Guard.

Images de machines Amazon (AMIs)

AMIIl doit être préconfiguré pour activer Nitro TPM et UEFI Secure Boot. Pour plus d'informations sur la prise en chargeAMIs, consultezthe section called "Prérequis".

Intégrité de la mémoire

L'intégrité de la mémoire, également connue sous le nom d'intégrité du code protégée par l'hyperviseur (HVCI) ou intégrité du code renforcée par l'hyperviseur, n'est pas prise en charge. Avant d'activer Credential Guard, vous devez vous assurer que cette fonctionnalité est désactivée. Pour de plus amples informations, veuillez consulter Désactiver l'intégrité de la mémoire.

Types d'instances

Les types d'instances suivants prennent en charge Credential Guard, quelle que soit leur taille `C5` `C5dC5n`, sauf indication contraire : `C6iC6id`,`C6in`,`C7i`,`C7i-flex`,`M5`,`M5d`,,`M5dn`,`M5n`,`M5zn`,`M6i`,`M6id`,,`M6idn`,`M6in`,`M7i`,`M7i-flex`,`R5`,`R5b`,,`R5d`,`R5dn`,`R5n`,`R6i`,`R6id`,,`R6idn`, `R6in` `R7iR7iz`,`T3`.

> **Note**
>
> - Bien que Nitro TPM ait certains types d'instances obligatoires en commun, le type d'instance doit être l'un des types d'instance précédents pour prendre en charge Credential Guard.
> - Credential Guard n'est pas pris en charge pour :

- Instances en métal nu.
- Les types d'instances suivants : `C7i.48xlarge`M7i.48xlarge, et`R7i.48xlarge`.

Pour plus d'informations sur les types d'instances, consultez le guide des types d'EC2instances Amazon.

Lancer une instance prise en charge

Vous pouvez utiliser la EC2 console Amazon ou AWS Command Line Interface (AWS CLI) pour lancer une instance compatible avec Credential Guard. Vous aurez besoin d'un AMI identifiant compatible pour lancer votre instance, unique pour chaque instance Région AWS.

> **Tip**
>
> Vous pouvez utiliser le lien suivant pour découvrir et lancer des instances compatibles avec Amazon fournies AMIs dans la EC2 console Amazon : https://console.aws.amazon.com/ec2/v2/home?#Images:visibility=public-images;v=3;search=:TPM-Windows_Server;ownerAlias=amazon

Amazon EC2 console

Pour lancer une instance à l'aide de la EC2 console Amazon

Suivez les étapes pour lancer une instance, en spécifiant un type d'instance pris en charge et un système Windows AMI préconfiguré.

AWS CLI

Pour lancer une instance à l'aide du AWS CLI

Utilisez la run-instancescommande pour lancer une instance à l'aide d'un type d'instance pris en charge et d'un système Windows AMI préconfiguré.

```
aws ec2 run-instances \
    --image-id resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-English-Full-Base \
    --instance-type c6i.large \
    --region us-east-1 \
```

```
    --subnet-id subnet-id
    --key-name key-name
```

PowerShell

Pour lancer une instance à l'aide du AWS Tools for PowerShell

Utilisez la New-EC2Instancecommande pour lancer une instance à l'aide d'un type d'instance pris en charge et d'un système Windows AMI préconfiguré.

```
New-EC2Instance `
    -ImageId resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-English-Full-Base `
    -InstanceType c6i.large `
    -Region us-east-1 `
    -SubnetId subnet-id `
    -KeyName key-name
```

Désactiver l'intégrité de la mémoire

Vous pouvez utiliser l'éditeur de stratégie de groupe local pour désactiver l'intégrité de la mémoire dans les scénarios pris en charge. Les instructions suivantes peuvent être appliquées pour chaque paramètre de configuration dans le cadre de la protection de l'intégrité du code basée sur la virtualisation :

- Activé sans verrouillage : modifiez le paramètre sur Désactivé pour désactiver l'intégrité de la mémoire.
- Activé par UEFI verrouillage — L'intégrité de la mémoire a été activée par UEFI verrouillage. L'intégrité de la mémoire ne peut pas être désactivée une fois qu'elle a été activée par UEFI verrouillage. Nous vous recommandons de créer une nouvelle instance en désactivant l'intégrité de la mémoire et de résilier l'instance non prise en charge si elle n'est pas utilisée.

Pour désactiver l'intégrité de la mémoire à l'aide de l'éditeur de stratégie de groupe local

1. Connectez-vous à votre instance en tant que compte utilisateur doté de privilèges d'administrateur à l'aide du protocole Remote Desktop (RDP). Pour de plus amples informations, veuillez consulter the section called "Connect à l'aide d'un RDP client".
2. Ouvrez le menu Démarrer et recherchez **cmd** pour lancer une invite de commande.

3. Exécutez la commande suivante pour ouvrir l'éditeur de stratégie de groupe local : `gpedit.msc`
4. Dans l'éditeur de stratégie de groupe locale, choisissez Configuration de l'ordinateur, Modèles d'administration, Système, Device Guard.
5. Sélectionnez Activer la sécurité basée sur la virtualisation, puis sélectionnez Modifier le paramètre de stratégie.
6. Ouvrez la liste déroulante des paramètres de la protection de l'intégrité du code basée sur la virtualisation, choisissez Désactivé, puis sélectionnez Appliquer.
7. Redémarrez l'instance pour appliquer les modifications.

Activez Credential Guard

Après avoir lancé une instance Windows avec un type d'instance compatible AMI et confirmé que l'intégrité de la mémoire est désactivée, vous pouvez activer Credential Guard.

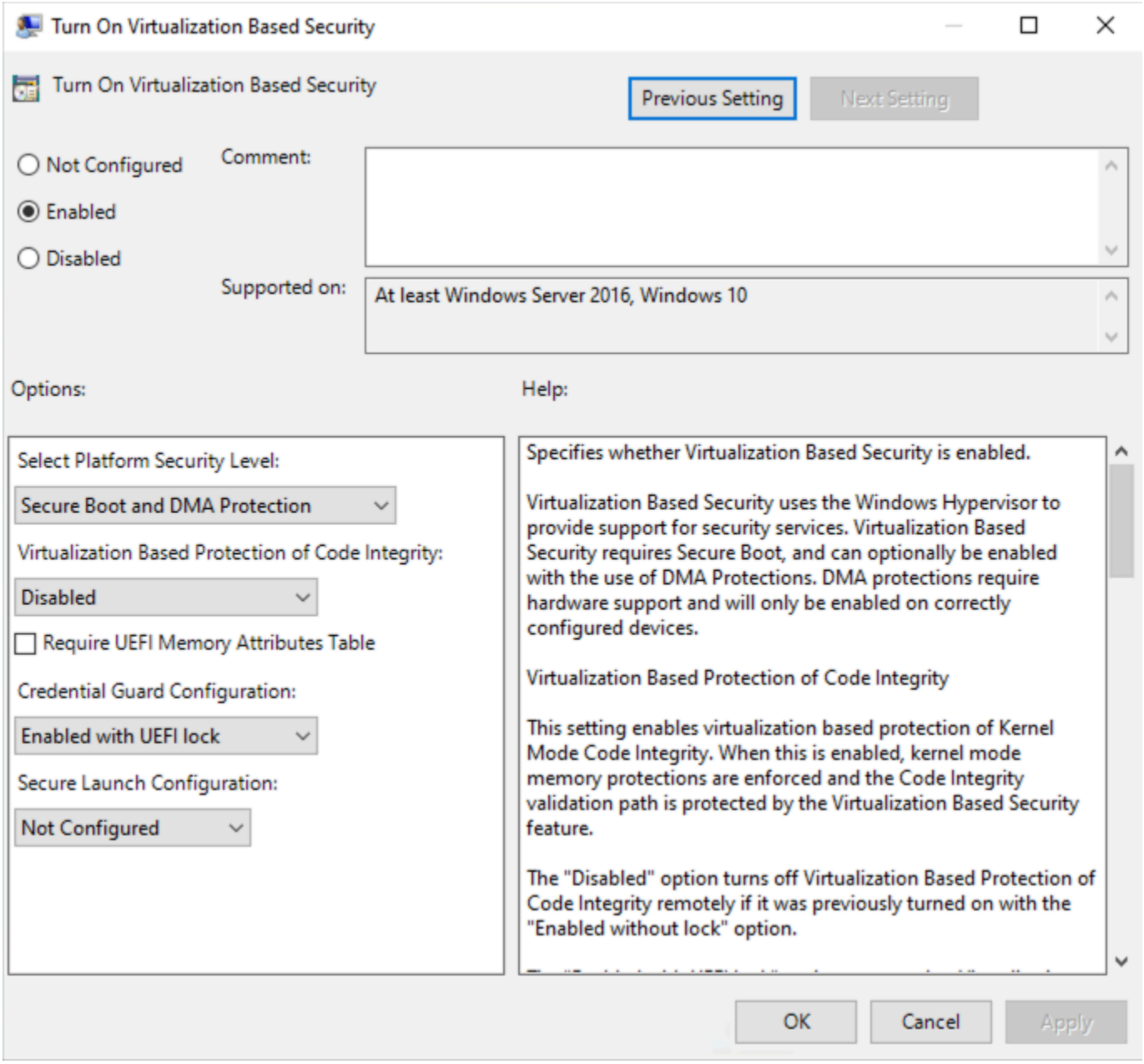
> **Important**
>
> Des privilèges d'administrateur sont nécessaires pour exécuter les étapes suivantes afin d'activer Credential Guard.

Pour activer Credential Guard

1. Connectez-vous à votre instance en tant que compte utilisateur doté de privilèges d'administrateur à l'aide du protocole Remote Desktop (RDP). Pour de plus amples informations, veuillez consulter the section called "Connect à l'aide d'un RDP client".
2. Ouvrez le menu Démarrer et recherchez **`cmd`** pour lancer une invite de commande.
3. Exécutez la commande suivante pour ouvrir l'éditeur de stratégie de groupe local : `gpedit.msc`
4. Dans l'éditeur de stratégie de groupe locale, choisissez Configuration de l'ordinateur, Modèles d'administration, Système, Device Guard.
5. Sélectionnez Activer la sécurité basée sur la virtualisation, puis sélectionnez Modifier le paramètre de stratégie.
6. Choisissez Activé dans le menu Activer la sécurité basée sur la virtualisation.
7. Pour Sélectionner le niveau de sécurité de la plate-forme, choisissez Démarrage sécurisé et DMA protection.
8. Pour la configuration de Credential Guard, choisissez Activé avec UEFI verrouillage.

> **Note**
>
> Les autres paramètres de stratégie ne sont pas nécessaires pour activer Credential Guard et peuvent être laissés comme Non configurés.

L'image suivante affiche les VBS paramètres configurés comme décrit précédemment :



9. Redémarrez l'instance pour appliquer les paramètres.

Vérifiez que Credential Guard est en cours d'exécution

Vous pouvez utiliser l'outil Microsoft System Information (`Msinfo32.exe`) pour vérifier que Credential Guard est en cours d'exécution.

> **Important**
>
> Vous devez d'abord redémarrer l'instance pour terminer l'application des paramètres de stratégie nécessaires à l'activation de Credential Guard.

Pour vérifier que Credential Guard est en cours d'exécution

1. Connectez-vous à votre instance à l'aide du protocole Remote Desktop (RDP). Pour de plus amples informations, veuillez consulter the section called "Connect à l'aide d'un RDP client".
2. Au RDP cours de la session sur votre instance, ouvrez le menu Démarrer et recherchez **`cmd`** pour démarrer une invite de commande.
3. Ouvrez System Information en exécutant la commande suivante : `msinfo32.exe`
4. L'outil Microsoft System Information répertorie les détails de VBS configuration. À côté de Services de sécurité basés sur la virtualisation, vérifiez que Credential Guard apparaît comme étant en cours d'exécution.

   Les affichages d'images suivants VBS s'exécutent comme décrit précédemment :

Virtualization-based security	Running
Virtualization-based security Required Security Properties	Base Virtualization Support, Secure Boot, DMA Protection
Virtualization-based security Available Security Properties	Base Virtualization Support, Secure Boot, DMA Protection, UEFI Code Readonly, Mode Based Execution Control
Virtualization-based security Services Configured	Credential Guard
Virtualization-based security Services Running	Credential Guard

Accédez à Amazon à EC2 l'aide d'un point de VPC terminaison d'interface

Vous pouvez améliorer votre niveau de sécurité VPC en créant une connexion privée entre vous VPC et AmazonEC2. Vous pouvez accéder à Amazon EC2 comme s'il s'agissait de votre VPC compte, sans passer par une passerelle Internet, un NAT appareil, une VPN connexion ou une AWS Direct Connect connexion. Les instances de votre VPC ordinateur n'ont pas besoin d'adresses IP publiques pour accéder à AmazonEC2.

Pour plus d'informations, consultez la section Accès services AWS par AWS PrivateLink le biais du AWS PrivateLink guide.

Table des matières

Création d'un point de VPC terminaison d'interface

Créez un point de terminaison d'interface pour Amazon EC2 en utilisant le nom de service suivant :

- com.amazonaws.***region***.ec2 — Crée un point de terminaison pour les actions Amazon EC2API.

Pour plus d'informations, consultez la section Accès et service AWS utilisation d'un point de VPC terminaison d'interface dans le AWS PrivateLink Guide.

Création d'une politique de point de terminaison

Une politique de point de terminaison est une IAM ressource que vous pouvez associer au point de terminaison de votre interface. La politique de point de terminaison par défaut autorise un accès complet à Amazon EC2 API via le point de terminaison de l'interface. Pour contrôler l'accès autorisé à Amazon EC2 API depuis votre ordinateurVPC, associez une politique de point de terminaison personnalisée au point de terminaison de l'interface.

Une politique de point de terminaison spécifie les informations suivantes :

- Le mandataire qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- La ressource sur laquelle les actions peuvent être effectuées.

> **Important**
>
> Lorsqu'une politique autre que celle par défaut est appliquée à un point de VPC terminaison d'interface pour AmazonEC2, certaines API demandes ayant échoué, telles que celles émanant de`RequestLimitExceeded`, peuvent ne pas être connectées à Amazon AWS CloudTrail ou à Amazon CloudWatch.

Pour plus d'informations, consultez Contrôle de l'accès aux services à l'aide de politiques de point de terminaison dans le Guide AWS PrivateLink .

L'exemple suivant montre une politique de point de VPC terminaison qui refuse l'autorisation de créer des volumes non chiffrés ou de lancer des instances avec des volumes non chiffrés. L'exemple de politique accorde également l'autorisation d'effectuer toutes les autres EC2 actions Amazon.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Action": "ec2:*",
        "Effect": "Allow",
        "Resource": "*",
        "Principal": "*"
    },
    {
        "Action": [
            "ec2:CreateVolume"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    },
    {
        "Action": [
            "ec2:RunInstances"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    }]
}
```

Options de stockage pour vos EC2 instances Amazon

Amazon vous EC2 propose des options de stockage de easy-to-use données flexibles et économiques pour vos instances. Chaque option est une combinaison unique de performance et de durabilité. Ces options de stockage peuvent être utilisées seules ou associées pour satisfaire vos besoins.

Stockage en mode bloc

- Amazon EBS — Amazon EBS fournit des volumes de stockage durables au niveau des blocs que vous pouvez attacher et détacher de vos instances. Vous pouvez associer plusieurs EBS volumes à une instance. Un EBS volume persiste indépendamment de la durée de vie de son instance associée. Vous pouvez chiffrer vos EBS volumes. Pour conserver une copie de sauvegarde de vos données, vous pouvez créer des instantanés à partir de vos EBS volumes. Les instantanés sont stockés dans Amazon S3. Vous pouvez créer un EBS volume à partir d'un instantané.
- Stockage d'instances Stockage par blocs temporaire pour les EC2 instances— Le magasin d'instances fournit un stockage temporaire au niveau des blocs pour les instances. Le nombre, la taille et le type des volumes de stockage d'instances sont déterminés par le type et la taille des instances. Les données sur un volume de stockage d'instances persistent uniquement pendant la vie de l'instance associée. Si vous arrêtez, mettez en veille prolongée ou résiliez une instance, toutes les données sur les volumes de stockage d'instances sont perdues.

Stockage d'objets

- Amazon S3— Amazon S3 donne accès à une infrastructure de stockage de données fiable et peu coûteuse. Il est conçu pour faciliter l'informatique à l'échelle du Web en vous permettant de stocker et de récupérer n'importe quel volume de données, à tout moment, depuis Amazon EC2 ou n'importe où sur le Web. Par exemple, vous pouvez utiliser Amazon S3 pour stocker des copies de sauvegarde de vos données et applications. Amazon EC2 utilise Amazon S3 pour stocker des EBS instantanés et des instances sauvegardées en magasinAMIs.

Stockage de fichiers

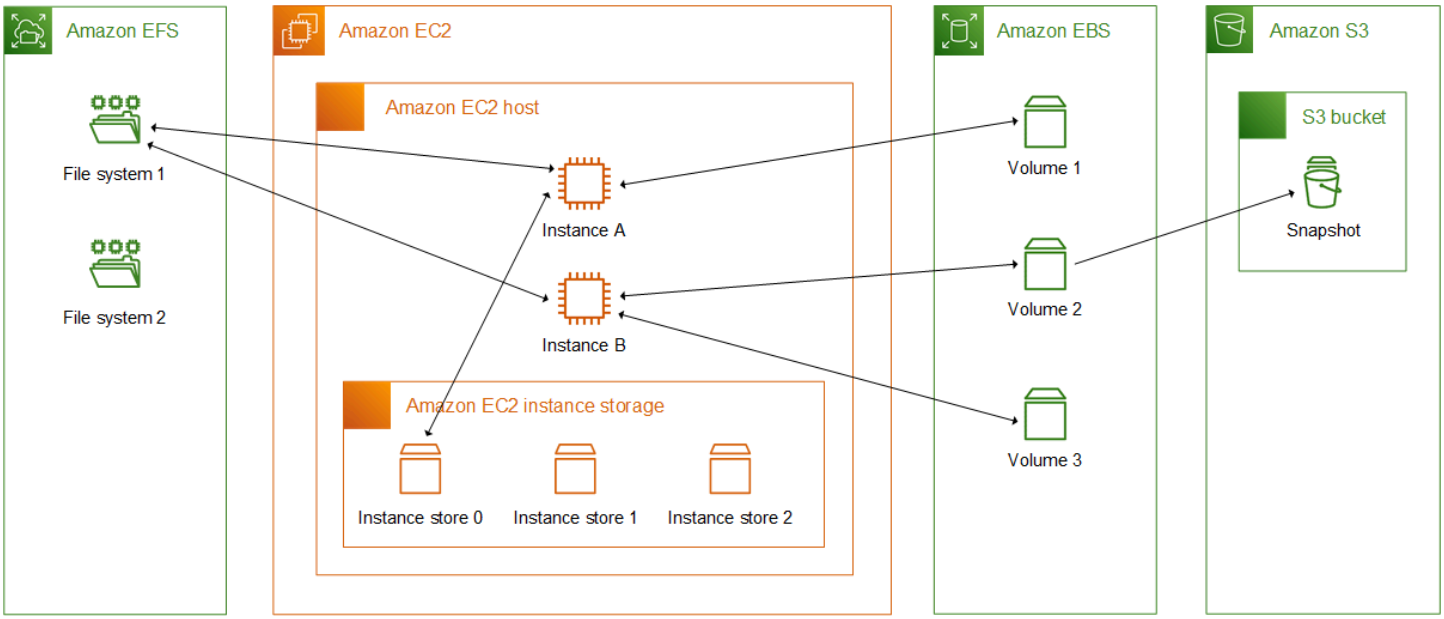
- Amazon EFS(Instances Linux uniquement) — Amazon EFS fournit un stockage de fichiers évolutif à utiliser avec AmazonEC2. Vous pouvez créer un système de EFS fichiers et configurer vos instances pour monter le système de fichiers. Vous pouvez utiliser un système de EFS fichiers comme source de données commune pour les charges de travail et les applications exécutées sur plusieurs instances.

- Amazon FSx— Avec AmazonFSx, vous pouvez lancer, exécuter et faire évoluer des systèmes de fichiers riches en fonctionnalités et à hautes performances dans le cloud. Amazon FSx est un service entièrement géré qui prend en charge un large éventail de charges de travail. Vous pouvez choisir entre les systèmes de fichiers les plus utilisés : Lustre NetApp ONTAPZFS, Open et Windows File Server.

Mise en cache de fichiers

- Utiliser Amazon File Cache avec les EC2 instances Amazon— Amazon File Cache fournit un cache temporaire à hautes performances AWS pour le traitement des données des fichiers. Le cache permet d'accéder aux données en lecture et en écriture pour calculer les charges de travail sur Amazon EC2 avec des latences inférieures à la milliseconde, des centaines de Go/s de débit et des millions de. IOPS

L'illustration suivante représente la relation entre ces options de stockage et votre instance.



AWS Tarification du stockage

Ouvrez AWS Tarification, faites défiler la page jusqu'à Tarification AWS des produits et sélectionnez Stockage. Choisissez le produit de stockage pour ouvrir sa page de tarification.

Stockage par blocs EBS persistant Amazon pour les EC2 instances Amazon

Amazon Elastic Block Store (AmazonEBS) fournit des ressources de stockage par blocs évolutives et performantes qui peuvent être utilisées avec des EC2 instances Amazon. Amazon EBS vous permet de créer et de gérer les ressources de stockage par blocs suivantes :

- EBSVolumes Amazon : il s'agit de volumes de stockage que vous associez aux EC2 instances Amazon. Une fois que vous avez attaché un volume à une instance, vous pouvez l'utiliser de la même manière que vous utiliseriez le stockage par blocs. L'instance peut interagir avec le volume comme elle le ferait avec un lecteur local.
- EBSInstantanés Amazon : il s'agit de point-in-time sauvegardes de EBS volumes Amazon qui sont conservées indépendamment du volume lui-même. Vous pouvez créer des instantanés pour sauvegarder les données de vos EBS volumes Amazon. Vous pouvez ensuite restaurer de nouveaux volumes à partir de ces instantanés à tout moment.

Vous pouvez créer et attacher des EBS volumes à une instance lors du lancement, et vous pouvez créer et attacher EBS des volumes à une instance à tout moment après le lancement. Vous pouvez également augmenter la taille ou les performances de vos EBS volumes sans les détacher ni redémarrer votre instance.

Vous pouvez créer des EBS instantanés à partir d'un EBS volume à tout moment après sa création. Vous pouvez utiliser EBS des instantanés pour sauvegarder les données stockées sur vos volumes. Vous pouvez ensuite utiliser ces instantanés pour restaurer instantanément des volumes ou pour migrer des données entre Comptes AWS des AWS régions ou des zones de disponibilité. Vous pouvez utiliser Amazon Data Lifecycle Manager ou AWS Backup automatiser la création, la conservation et la suppression de vos EBS instantanés.

Pour plus d'informations sur l'utilisation des volumes et des instantanés, consultez le guide de l'EBSutilisateur Amazon.

Limites EBS de volume Amazon pour les EC2 instances Amazon

Le nombre maximum de EBS volumes Amazon que vous pouvez attacher à une instance dépend du type et de la taille de l'instance. Lorsque vous réfléchissez au nombre de volumes à attacher à votre instance, vous devriez déterminer si vous avez besoin d'une plus grande bande passante E/S ou d'une plus grande capacité de stockage.

Bande passante et capacité

Pour des cas d'utilisation de la bande passante cohérents et prévisibles, utilisez des instances EBS optimisées pour Amazon avec des volumes à usage général ou SSD des volumes provisionnés IOPSSSD. Pour des performances optimales, faites correspondre la bande passante que IOPS vous avez allouée pour vos volumes à la bande passante disponible pour votre type d'instance.

En ce qui concerne les RAID configurations, vous constaterez peut-être que les baies de plus de 8 volumes présentent des performances réduites en raison de l'augmentation de la charge d'E/S. Testez la performance de votre application individuelle et ajustez-la si nécessaire.

Table des matières

Limites de volume pour les instances créées sur le système Nitro

Les limites de volume pour les instances créées sur le système Nitro dépendent du type d'instance. Certains types d'instances Nitro ont une limite de EBS volume dédiée, tandis que la plupart ont une limite de volume partagée.

Limite EBS de volume dédiée

Les types d'instances Nitro suivants ont une limite de EBS volume dédiée qui varie en fonction de la taille de l'instance. La limite n'est pas partagée avec les autres pièces jointes du périphérique. En d'autres termes, vous pouvez attacher n'importe quel nombre de EBS volumes jusqu'à la limite d'attachement de volume, quel que soit le nombre de périphériques connectés, tels que les volumes de stockage d'NVMeinstance et les interfaces réseau.

- Usage général : M7a, M7i, M7i-Flex
- Optimisé pour le calcul : C7a, C7i, C7i-Flex
- Mémoire optimisée : R7a, R7i, R7iz, R8g, U7i

- Calcul accéléré : G6, Gr6

Pour les types d'instances qui prennent en charge les limites de volume dédiées, les limites de volume dépendent de la taille de l'instance. Le tableau suivant indique la limite de chaque taille d'instance.

Taille d'instance	Limite de volume
`medium | large | xlarge | 2xlarge | 4xlarge | 8xlarge | 12xlarge`	32
`16xlarge`	48
`24xlarge`	64
`32xlarge`	88
`48xlarge`	128
`metal-16xl | metal-24xl`	39
`metal-32xl | metal-48xl`	79

Limite EBS de volume partagé

Tous les autres types d'instances Nitro (non répertoriés dansLimite EBS de volume dédiée) ont une limite de volume attachée qui est partagée entre les EBS volumes Amazon, les interfaces réseau et les volumes de stockage d'NVMeinstance. Vous pouvez associer n'importe quel nombre de EBS volumes Amazon jusqu'à cette limite, moins le nombre d'interfaces réseau et de volumes de stockage d'NVMeinstance attachés. N'oubliez pas que chaque instance doit disposer d'au moins une interface réseau et que les volumes de stockage d'NVMeinstance sont automatiquement attachés au lancement.

La plupart des instances Nitro prennent en charge un maximum de 28 pièces jointes. Les exemples suivants montrent comment calculer le nombre de EBS volumes que vous pouvez joindre.

Exemples

- Avec une `m5.xlarge` instance dotée uniquement de l'interface réseau principale, vous pouvez associer 27 EBS volumes.

  28 volumes - 1 interface réseau = 27
- Avec une `m5.xlarge` instance dotée de deux interfaces réseau supplémentaires, vous pouvez associer 25 EBS volumes.

  28 volumes - 3 interfaces réseau = 25
- Avec une `m5d.xlarge` instance dotée de deux interfaces réseau supplémentaires, vous pouvez associer 24 EBS volumes.

  28 volumes - 3 interfaces réseau - 1 volume de stockage d'NVMeinstance = 24

Les exceptions suivantes concernent les types d'instances dont les limites de volume sont partagées.

Exceptions

- `d3.8xlarge`et `d3en.12xlarge` les instances prennent en charge un maximum de 3 EBS volumes.
- DL2qles instances prennent en charge un maximum de 19 EBS volumes.
- `g5.48xlarge`les instances prennent en charge un maximum de 9 EBS volumes.
- `inf1.xlarge`et `inf1.2xlarge` les instances prennent en charge un maximum de 26 EBS volumes.
- `inf1.6xlarge`les instances prennent en charge un maximum de 23 EBS volumes.
- `inf1.24xlarge`les instances prennent en charge un maximum de 11 EBS volumes.
- `Mac2`, `Mac2-m2``Mac2-m2pro`, et les `Mac2-m1ultra` instances prennent en charge un maximum de 10 EBS volumes.
- `U-*tb1`les instances virtualisées prennent en charge un maximum de 27 EBS volumes.
- Par `vt1.3xlarge` exemple`vt1.6xlarge`, chaque accélérateur compte pour deux pièces jointes.
- Par exemple`vt1.24xlarge`, les accélérateurs ne sont pas pris en compte dans le calcul de la limite de volume partagé.
- Pour les instances de calcul accéléré autres que VT1 les instances, chaque accélérateur compte comme une pièce jointe. Par exemple, `p4d.24xlarge` les instances ont une limite de volume partagé de 28GPUs, 8 et 8 volumes de stockage d'NVMeinstance. Cela signifie que vous pouvez

associer jusqu'à 11 EBS volumes (28 volumes - 1 interface réseau GPUs - 8 à 8 volumes de stockage d'NVMeinstance).

- La plupart des instances bare metal prennent en charge un maximum de 31 EBS volumes. Les exceptions sont les suivantes :
  - `mac1.metal`les instances prennent en charge un maximum de 16 EBS volumes.
  - `U-*tb1`les instances bare metal prennent en charge un maximum de 19 EBS volumes.

Limites de volume pour les instances basées sur Xen

Les limites de volume pour les instances basées sur Xen dépendent du système d'exploitation.

Instances Linux

L'attachement de plus de 40 volumes à une instance Linux basée sur Xen peut provoquer des échecs de démarrage. Ce nombre inclut le volume racine, ainsi que tous les volumes de stockage d'instance attachés et les EBS volumes Amazon.

Si vous rencontrez des problèmes de démarrage sur une instance avec un grand nombre de volumes, arrêtez l'instance, détachez tous les volumes qui ne sont pas essentiels au processus de démarrage, démarrez l'instance, puis rattachez les volumes une fois que l'instance est en cours d'exécution.

> **Important**
>
> Attacher plus de 40 volumes sur une instance Linux basée sur Xen est pris en charge autant que possible et ce, sans garantie.

instances Windows

Le tableau ci-après affiche les limites de volumes pour les instances Windows basées sur Xen en fonction du pilote utilisé. Que ces chiffres incluent le volume racine, ainsi que tous les volumes de stockage d'instance attachés et les EBS volumes Amazon.

Pilote	Limite de volume
AWS PV	26

Pilote	Limite de volume
Virtualisation paravirtuelle Citrix	26
Virtualisation paravirtuelle Red Hat	17

Nous vous recommandons de ne pas associer plus de 26 volumes à une instance Windows basée sur XEN avec des pilotes AWS PV ou Citrix PV, car cela pourrait entraîner des problèmes de performances. Pour déterminer quels pilotes de virtualisation paravirtuelle sont utilisés par votre instance, ou pour passer votre instance Windows de pilotes de virtualisation paravirtuelle Red Hat à des pilotes Citrix, veuillez consulter la rubrique the section called “Mettre à niveau les pilotes PV”.

> **Important**
>
> Attacher plus que le nombre de volumes suivant sur une instance Windows basée sur Xen est pris en charge autant que possible et ce, sans garantie.

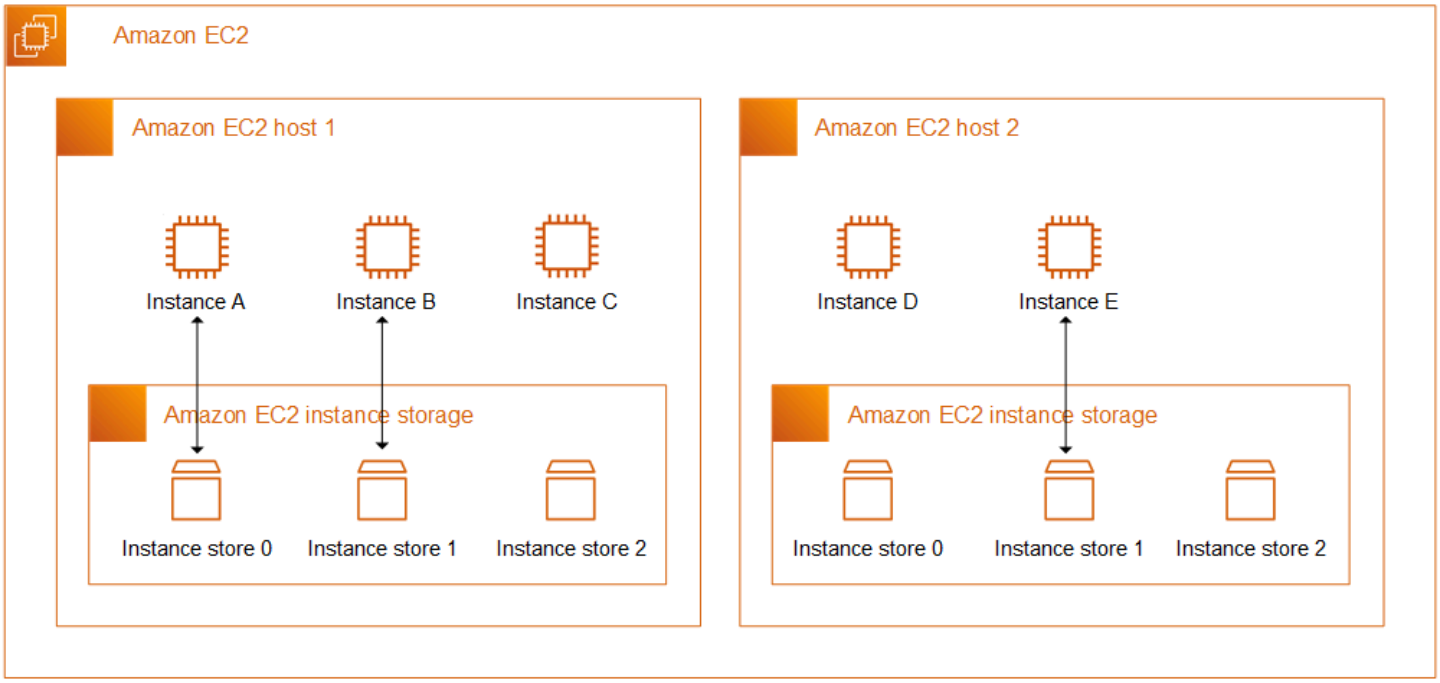
Pour plus d'informations sur la façon dont les noms de périphériques sont liés aux volumes, veuillez consulter la rubrique Comment les volumes sont attachés et mappés pour les instances Amazon EC2 Windows.

Stockage d'instances Stockage par blocs temporaire pour les EC2 instances

Un magasin d'instance fournit un stockage temporaire au niveau des blocs pour votre EC2 instance. Ce stockage est assuré par des disques physiquement connectés à l'ordinateur hôte. Le stockage d'instances est particulièrement adapté pour le stockage temporaire d'informations qui changent fréquemment, telles que les tampons, les caches, les données de travail et autres contenus temporaires. Il peut également être utilisé pour stocker des données temporaires que vous répliquez sur une flotte d'instances, comme un groupe à charge équilibrée de serveurs Web.

Un stockage d'instances se compose d'un ou de plusieurs stockages d'instance exposés comme périphériques de stockage en mode bloc. La taille d'un stockage d'instances ainsi que le nombre de périphériques disponibles varient en fonction du type et de la taille des instances. Par exemple, tous les types d'instance ne fournissent pas de volumes de stockage d'instance. Pour de plus amples informations, veuillez consulter Limites de volume de stockage d'instance pour les EC2 instances.

Les périphériques virtuels, par exemple les volumes de stockage, reçoivent des noms de périphériques virtuels dans l'ordre allant de `ephemeral0` à`ephemeral23`. Par exemple, avec un type d'instance qui prend en charge un volume de stockage d'instance, le nom de périphérique virtuel de ce volume est`ephemeral0`. Avec un type d'instance qui prend en charge quatre volumes de stockage d'instance, les noms des périphériques virtuels des quatre volumes sont les suivants : `ephemeral0`, `ephemeral1`, `ephemeral2` et`ephemeral3`.



Tarification du stockage d'instances

L'utilisation des volumes de stockage d'instance fournis pour votre instance est gratuite. Les volumes de stockage d'instance sont inclus dans le coût d'utilisation de l'instance.

Table des matières

Persistance des données pour les volumes de stockage des EC2 instances Amazon

Les volumes de stockage d'instances sont attachés uniquement au lancement de l'instance. Vous ne pouvez pas attacher des volumes de stockage d'instances après le lancement. Vous ne pouvez pas détacher un volume de stockage d'instances à partir d'une instance et l'attacher à une autre instance.

Un volume de stockage d'instances n'existe que pendant la durée de vie de l'instance à laquelle il est attaché. Vous ne pouvez pas configurer un volume de stockage d'instances pour qu'il persiste au-delà de la durée de vie de son instance associée.

Les données stockées sur un volume de stockage d'instances persistent même si l'instance est redémarrée. Toutefois, les données ne persistent pas si l'instance est arrêtée, mise en veille prolongée ou résiliée. Lorsque l'instance est arrêtée, mise en veille prolongée ou résiliée, chaque bloc du stockage d'instances est effacé de manière cryptographique.

Par conséquent, ne vous fiez pas au stockage d'instances pour les données précieuses et à long terme. Si vous devez conserver les données stockées sur un volume de stockage d'instance au-delà de la durée de vie de l'instance, vous devez les copier manuellement vers un stockage plus persistant, tel qu'un EBS volume Amazon, un compartiment Amazon S3 ou un système de EFS fichiers Amazon.

Certains événements peuvent empêcher la persistance de vos données pendant toute la durée de vie de l'instance. Le tableau suivant indique si les données relatives aux volumes de stockage d'instances sont persistées lors d'événements spécifiques, tant pour les instances virtualisées que pour les instances de matériel nu.

Événement	Qu'arrive-t-il à vos données ?
Événements du cycle de vie de l'instance initiés par l'utilisateur	
L'instance est redémarrée	Les données persistent
L'instance est arrêtée	Les données ne persistent pas
L'instance est mise en veille prolongée	Les données ne persistent pas
L'instance est terminée	Les données ne persistent pas
Le type d'instance est modifié	Les données ne persistent pas *

Événement	Qu'arrive-t-il à vos données ?
Un EBS -backed AMI est créé à partir de l'instance	Les données ne sont pas conservées dans le fichier AMI ** créé
Une instance sauvegardée en magasin AMI est créée à partir de l'instance (instances Linux)	Les données sont conservées dans le AMI bundle chargé sur Amazon S3 ***
Événements du système d'exploitation initiés par l'utilisateur	
Un arrêt est lancé	Les données ne persistent pas †
Un redémarrage est lancé	Les données persistent
AWS événements programmés	
Arrêt de l'instance	Les données ne persistent pas
Redémarrage de l'instance	Les données persistent
Redémarrage du système	Les données persistent
Retrait de l'instance	Les données ne persistent pas
Événements non planifiés	
Restauration automatique simplifiée	Les données ne persistent pas
CloudWatch restauration basée sur l'action	Les données ne persistent pas
Le disque sous-jacent tombe en panne	Les données présentes sur le disque défaillant ne sont pas conservées
Panne de courant	Les données sont conservées au redémarrage

* Si le nouveau type d'instance prend en charge le stockage d'instances, l'instance obtient le nombre de volumes de stockage d'instances pris en charge par le nouveau type d'instance, mais les données ne sont pas transférées vers la nouvelle instance. Si le nouveau type d'instance ne prend pas en charge le stockage d'instances, l'instance n'obtient pas les volumes de stockage d'instances.

** Les données ne sont pas incluses dans le EBS -backedAMI, et elles ne sont pas incluses dans les volumes de stockage d'instance attachés aux instances lancées à partir de celui-ciAMI.

*** Les données sont incluses dans le AMI bundle qui est chargé sur Amazon S3. Lorsque vous lancez une instance à partir de làAMI, l'instance intègre les volumes de stockage d'instance AMI avec les données qu'ils AMI contenaient au moment de leur création.

† La protection contre la résiliation et l'arrêt ne protègent pas les instances contre les arrêts ou les résiliations d'instances à la suite d'arrêts initiés via le système d'exploitation de l'instance. Les données stockées sur les volumes de stockage d'instances ne persistent pas lors des événements d'arrêt ni de résiliation d'instance.

Limites de volume de stockage d'instance pour les EC2 instances

Le nombre, la taille et le type des volumes de stockage d'instance sont déterminés par le type d'instance. Certains types d'instances, tels que M6, C6 et R6, ne prennent pas en charge les volumes de stockage d'instances, tandis que d'autres types d'instances, tels que M5d, C6gd et R6gd, prennent en charge les volumes de stockage d'instances. Vous ne pouvez pas attacher à une instance plus de volumes de stockage d'instances que ne le permet son type d'instance. Pour les types d'instances qui prennent en charge les volumes de stockage d'instances, le nombre et la taille des volumes de stockage d'instances varient en fonction de la taille de l'instance. Par exemple, `m5d.large` prend en charge 1 volume de stockage d'instances de 75 Go, tandis que `m5d.24xlarge` prend en charge 4 volumes de stockage d'instances de 900 Go.

Pour les types d'NVMeinstance dotés de volumes de stockage d'instance, tous les volumes de stockage d'instance pris en charge sont automatiquement attachés à l'instance au lancement. Pour les types d'instance dotés de volumes de stockage autres que les NVMe instances, tels que C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 et X1e, vous devez spécifier manuellement les mappages de périphériques de bloc pour les volumes de stockage d'instance que vous souhaitez associer au lancement. Ensuite, une fois l'instance lancée, vous devez formater et monter les volumes de stockage d'instances attachés avant de pouvoir les utiliser. Vous ne pouvez pas attacher un volume de stockage d'instances après avoir lancé l'instance.

Certains types d'instances utilisent des disques SSD () SATA basés sur NVMe ou basés sur des disques durs (SSD), tandis que d'autres utilisent des disques durs SATA basés sur ou basés sur des disques durs (HDD). SSDsoffrent des performances d'E/S aléatoires élevées avec une latence très faible, mais vous n'avez pas besoin que les données persistent lorsque l'instance se termine ou vous pouvez tirer parti d'architectures tolérantes aux pannes. Pour de plus amples informations, veuillez consulter SSDvolumes de stockage d'instance pour les EC2 instances.

Les données relatives aux volumes de stockage d'NVMeinstance et à certains volumes de stockage d'HDDinstance sont chiffrées au repos. Pour de plus amples informations, veuillez consulter Protection des données sur Amazon EC2.

Volumes de stockage d'instances disponibles

Le guide des types d'EC2instances Amazon fournit des informations sur la quantité, la taille, le type et les optimisations des performances des volumes de stockage d'instance disponibles pour chaque type d'instance pris en charge. Pour plus d'informations, consultez les ressources suivantes :

- Spécifications du magasin d'instances — Usage général
- Spécifications du magasin d'instances — Optimisé pour le calcul
- Spécifications du magasin d'instances — Mémoire optimisée
- Spécifications du magasin d'instances — Stockage optimisé
- Spécifications du magasin d'instances — Calcul accéléré
- Spécifications du magasin d'instances — Calcul à hautes performances
- Spécifications du magasin d'instances — Génération précédente

Pour récupérer les informations sur le volume de stockage de l'instance à l'aide du AWS CLI

Vous pouvez utiliser la describe-instance-types AWS CLI commande pour afficher des informations sur un type d'instance, telles que ses volumes de stockage d'instance. L'exemple suivant affiche la taille totale du stockage d'instance de toutes les instances R5 avec volumes de stockage d'instance.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r5*" "Name=instance-storage-
supported,Values=true" \
    --query "InstanceTypes[].[InstanceType, InstanceStorageInfo.TotalSizeInGB]" \
    --output table
```

Exemple de sortie

```
----------------------------
|  DescribeInstanceTypes   |
+----------------+---------+
|  r5ad.24xlarge |  3600   |
|  r5ad.12xlarge |  1800   |
```

```
|  r5dn.8xlarge  |  1200  |
|  r5ad.8xlarge  |  1200  |
|  r5ad.large    |  75    |
|  r5d.4xlarge   |  600   |
   . . .
|  r5dn.2xlarge  |  300   |
|  r5d.12xlarge  |  1800  |
+----------------+--------+
```

L'exemple suivant affiche les détails complets du stockage d'instance correspondant au type d'instance spécifié.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r5d.4xlarge" \
    --query "InstanceTypes[].InstanceStorageInfo"
```

L'exemple de sortie montre que ce type d'instance possède deux NVMe SSD volumes de 300 Go, pour un total de 600 Go de stockage d'instance.

```
[
    {
        "TotalSizeInGB": 600,
        "Disks": [
            {
                "SizeInGB": 300,
                "Count": 2,
                "Type": "ssd"
            }
        ],
        "NvmeSupport": "required"
    }
]
```

SSDvolumes de stockage d'instance pour les EC2 instances

Comme pour les autres volumes de stockage d'instance, vous devez mapper les volumes de stockage d'SSDinstance pour votre instance lorsque vous la lancez. Les données d'un volume d'SSDinstance ne sont conservées que pendant la durée de vie de l'instance associée. Pour de plus amples informations, veuillez consulter Ajouter des volumes de stockage d'instance à une EC2 instance.

NVMeSSDvolumes

Certaines instances proposent des volumes de stockage d'instance non volatils (NVMe), des disques SSD (SSD) en mémoire express (). Pour plus d'informations sur le type de volume de stockage d'instance pris en charge par chaque type d'instance, consultez Limites de volume de stockage d'instance pour les EC2 instances.

Les données du stockage de l'NVMeinstance sont chiffrées à l'aide d'un chiffrement par blocs de XTS AES -256 implémenté dans un module matériel de l'instance. Les clés de chiffrement sont générées à l'aide du module matériel et sont uniques à chaque périphérique de stockage d'NVMeinstance. Toutes les clés de chiffrement sont détruites lorsque l'instance est arrêtée ou résiliée et ne peuvent pas être récupérées. Vous ne pouvez pas désactiver le chiffrement et vous ne pouvez pas fournir votre propre clé de chiffrement.

Instances Linux

Pour accéder aux NVMe volumes, les NVMe pilotes doivent être installés. Les éléments suivants AMIs répondent à cette exigence :

- AL2023
- Amazon Linux 2
- Amazon Linux AMI 2018.03 et versions ultérieures
- Ubuntu 14.04 ou une version ultérieure avec noyau `linux-aws`

> **Note**
>
> AWS Les types d'instances basés sur Graviton nécessitent Ubuntu 18.04 ou version ultérieure avec noyau `linux-aws`

- Red Hat Enterprise Linux 7.4 ou une version ultérieure
- SUSELinux Enterprise Server 12 SP2 ou version ultérieure
- CentOS 7.4.1708 ou une version ultérieure
- Version BSD 11.1 gratuite ou version ultérieure
- GNUDebian/Linux 9 ou version ultérieure

- Bottlerocket

Une fois connecté à votre instance, vous pouvez répertorier les NVMe appareils à l'aide de la lspci commande. Voici un exemple de sortie pour une `i3.8xlarge` instance qui prend en charge quatre NVMe appareils.

```
[ec2-user ~]$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371SB PIIX3 IDE [Natoma/Triton II]
00:01.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 01)
00:02.0 VGA compatible controller: Cirrus Logic GD 5446
00:03.0 Ethernet controller: Device 1d0f:ec20
00:17.0 Non-Volatile memory controller: Device 1d0f:cd01
00:18.0 Non-Volatile memory controller: Device 1d0f:cd01
00:19.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1a.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1f.0 Unassigned class [ff80]: XenSource, Inc. Xen Platform Device (rev 01)
```

Si vous utilisez un système d'exploitation compatible mais que vous ne voyez pas les NVMe appareils, vérifiez que le NVMe module est chargé à l'aide de la commande suivante.

- Amazon Linux, Amazon Linux 2, Ubuntu 14/16, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, CentOS 7

  ```
  $ lsmod | grep nvme
  nvme           48813  0
  ```

- Ubuntu 18

  ```
  $ cat /lib/modules/$(uname -r)/modules.builtin | grep nvme
  s/nvme/host/nvme-core.ko
  kernel/drivers/nvme/host/nvme.ko
  kernel/drivers/nvmem/nvmem_core.ko
  ```

Les NVMe volumes sont conformes à la spécification NVMe 1.0e. Vous pouvez utiliser les NVMe commandes avec vos NVMe volumes. Avec Amazon Linux, vous pouvez installer le package `nvme-cli` à partir du référentiel à l'aide de la commande yum install. Avec d'autres versions de Linux prises en charge, vous pouvez télécharger le package `nvme-cli` s'il n'est pas disponible dans l'image.

instances Windows

La dernière version de AWS Windows AMIs pour les systèmes d'exploitation suivants contient les AWS NVMe pilotes utilisés pour interagir avec les volumes de stockage d'SSDinstance qui sont exposés sous forme de périphériques en mode NVMe bloc pour de meilleures performances :

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Une fois connecté à votre instance, vous pouvez vérifier que les NVMe volumes apparaissent dans le Gestionnaire de disques. Dans la barre des tâches, ouvrez le menu contextuel (via un clic droit) du logo Windows et choisissez Gestion des disques.

Le AWS Windows AMIs fourni par Amazon inclut le AWS NVMe pilote. Si vous n'utilisez pas la dernière version de AWS WindowsAMIs, vous pouvez installer le AWS NVMe pilote actuel.

Non en NVMe SSD volumes

Les instances suivantes prennent en charge les volumes de stockage d'instance qui utilisent la technologie non- NVMe SSDs pour fournir des performances d'E/S aléatoires élevées : C3, I2, M3, R3 et X1. Pour plus d'informations sur la prise en charge des volumes de stockage d'instance par chaque type d'instance, consultez Limites de volume de stockage d'instance pour les EC2 instances.

SSDperformances d'E/S du volume de stockage d'instance basées sur le volume

Au fur et à mesure que vous remplissez les volumes de stockage d'instance SSD basés sur votre instance, le nombre d'écritures IOPS que vous pouvez réaliser diminue. Cela est dû au travail supplémentaire que le SSD contrôleur doit effectuer pour trouver l'espace disponible, réécrire les données existantes et effacer l'espace inutilisé afin de pouvoir le réécrire. Ce processus de collecte des déchets entraîne une amplification interne de l'écritureSSD, exprimée sous la forme du rapport entre les opérations d'SSDécriture et les opérations d'écriture de l'utilisateur. Cette diminution des performances est encore plus importante si les opérations d'écriture ne sont pas exprimées en multiples de 4 096 octets ou ne sont pas alignées sur une limite de 4 096 octets. Si vous écrivez une petite quantité d'octets ou d'octets qui ne sont pas alignés, le SSD contrôleur doit lire les données environnantes et stocker le résultat dans un nouvel emplacement. Ce modèle se traduit par une forte

augmentation de l'amplification d'écriture, une latence accrue et une diminution considérable des performances d'I/O.

SSDles contrôleurs peuvent utiliser plusieurs stratégies pour réduire l'impact de l'amplification en écriture. L'une de ces stratégies consiste à réserver de l'espace dans le stockage de l'SSDinstance afin que le contrôleur puisse gérer plus efficacement l'espace disponible pour les opérations d'écriture. Cette solution est appelée sur-approvisionnement. Les volumes de stockage d'instance SSD basés fournis à une instance ne disposent d'aucun espace réservé au surprovisionnement. Pour réduire l'amplification en écriture, nous vous recommandons de laisser 10 % du volume non partitionné afin que le SSD contrôleur puisse l'utiliser pour le surprovisionnement. Cela diminue le stockage que vous pouvez utiliser, mais augmente les performances même si le disque est proche de sa capacité maximale.

Par exemple, stockez les volumes compatiblesTRIM, vous pouvez utiliser la TRIM commande pour avertir le SSD contrôleur chaque fois que vous n'avez plus besoin des données que vous avez écrites. Cela fournit au contrôleur plus d'espace disponible, ce qui peut réduire l'amplification d'écriture et augmenter les performances. Pour de plus amples informations, veuillez consulter Prise en TRIM charge des volumes de stockage d'instance.

Prise en TRIM charge des volumes de stockage d'instance

Certains types d'instances prennent en charge SSD les volumes avecTRIM. Pour de plus amples informations, veuillez consulter Limites de volume de stockage d'instance pour les EC2 instances.

> **Note**
>
> (Instances Windows uniquement) Les instances exécutant Windows Server 2012 R2 sont prises en charge à partir TRIM de la version 7.3.0 de AWS PV Driver. Les instances exécutant des versions antérieures de Windows Server ne sont pas prises en chargeTRIM.

Les volumes de stockage d'instance pris en charge TRIM sont entièrement réduits avant d'être alloués à votre instance. Comme ces volumes ne sont pas formatés avec un système de fichiers au lancement de l'instance, vous devez les formater avant qu'ils ne puissent être montés et utilisés. Pour accéder plus rapidement à ces volumes, vous devez ignorer l'TRIMopération lorsque vous les formatez.

(Instances Windows) Pour désactiver temporairement le TRIM support lors du formatage initial, utilisez la `fsutil behavior set DisableDeleteNotify 1` commande. Une fois le formatage

terminé, réactivez le TRIM support en utilisant`fsutil behavior set DisableDeleteNotify 0`.

Avec les volumes de stockage d'instance compatiblesTRIM, vous pouvez utiliser la TRIM commande pour avertir le SSD contrôleur lorsque vous n'avez plus besoin des données que vous avez écrites. Cela fournit au contrôleur plus d'espace disponible, ce qui peut réduire l'amplification d'écriture et augmenter les performances. Sur les instances Linux, utilisez la `fstrim` commande pour activer le périodiqueTRIM. Sur les instances Windows, utilisez la `fsutil behavior set DisableDeleteNotify 0` commande pour vous assurer que le TRIM support est activé pendant le fonctionnement normal.

Ajouter des volumes de stockage d'instance à une EC2 instance

Pour les types d'NVMeinstance dotés de volumes de stockage d'instance, tous les volumes de stockage d'instance pris en charge sont automatiquement attachés à l'instance au lancement. Ils sont automatiquement énumérés et un nom de périphérique leur est automatiquement attribué au lancement de l'instance.

Pour les types d'instance dotés de volumes de stockage autres que les NVMe instances, tels que C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 et X1e, vous devez spécifier manuellement les mappages de périphériques de bloc pour les volumes de stockage d'instance que vous souhaitez associer au lancement. Les mappages de périphériques par blocs peuvent être spécifiés dans la demande de lancement de l'instance ou dans le AMI fichier utilisé pour lancer l'instance. Le mappage de périphérique de stockage en mode bloc inclut un nom de périphérique et le volume sur lequel il est mappé. Pour plus d'informations, consultez Bloquer les mappages d'appareils pour les volumes sur les instances Amazon EC2.

> **Important**
>
> Vous ne pouvez attacher les volumes de stockage d'instances à une instance que lors de son lancement. Vous ne pouvez pas attacher des volumes de stockage d'instance à une instance après l'avoir lancée.

Après le lancement d'une instance, vous devez vous assurer que les volumes de stockage d'instance de votre instance sont formatés et montés avant que vous ne puissiez les utiliser. Le volume racine d'une instance basée sur le stockage d'instance est monté automatiquement.

À prendre en compte pour les volumes racines

Un mappage de périphérique de stockage en mode bloc spécifie toujours le volume racine de l'instance. Le volume racine est toujours monté automatiquement.

Instances Linux : le volume racine est soit un EBS volume Amazon, soit un volume de stockage d'instance. Pour les instances avec un volume de stockage d'instance pour le volume racine, la taille de ce volume varieAMI, mais la taille maximale est de 10 Go. Pour de plus amples informations, veuillez consulter Root device type.

Instances Windows : le volume racine doit être un EBS volume Amazon. Le stockage d'instance n'est pas pris en charge pour le volume racine.

Table des matières

Ajouter des volumes de stockage d'instance à un Amazon EC2 AMI

Vous pouvez créer un mappage de périphériques AMI avec un bloc qui inclut les volumes de stockage d'instance.

Si vous lancez une instance qui prend en charge les volumes de stockage autres que les NVMe instances à l'aide d'une instance AMI qui spécifie les mappages de périphériques par blocs de volumes de stockage d'instance, l'instance inclut les volumes de stockage d'instance. Si le nombre de mappages de périphériques de bloc de volume de stockage d'instance dans le est AMI supérieur au nombre de volumes de stockage d'instance disponibles pour l'instance, les mappages de périphériques de blocs de volume de stockage d'instance supplémentaires sont ignorés.

Si vous lancez une instance qui prend en charge les volumes de stockage d'NVMeinstance à l'aide d'une instance AMI qui spécifie les mappages de périphériques de bloc de volume de stockage d'instance, les mappages de périphériques de blocs de volume de stockage d'instance sont ignorés. Les instances qui prennent en charge les volumes de stockage d'NVMeinstance obtiennent tous leurs volumes de stockage d'instance pris en charge, quels que soient les mappages de périphériques par blocs spécifiés dans la demande de lancement d'instance et dans leAMI.

Considérations

- Pour les instances M3, spécifiez les volumes de stockage d'instance dans le mappage des périphériques par blocs de l'instance, et non dans leAMI. Amazon EC2 peut ignorer les mappages de périphériques par blocs de volume de stockage d'instance dans leAMI.
- Lorsque vous lancez une instance, vous pouvez omettre les volumes de stockage autres que les NVMe instances spécifiés dans le mappage des périphériques en AMI mode bloc ou ajouter des volumes de stockage d'instance.

Console

Pour ajouter des volumes de stockage d'instance à une instance EBS sauvegardée par Amazon à AMI l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Instances, puis choisissez l'instance.
3. Choisissez Actions, Image and templates (Image et modèles), Create image (Créer une image).
4. Sur la page Create Image (Créer une image), saisissez un nom et une description significatifs pour votre image.
5. Pour chaque volume de stockage d'instance à ajouter, sélectionnez Add volume (Ajouter un volume), puis dans Type de volume, sélectionnez un volume de stockage d'instance, et dans Device (Périphérique), sélectionnez un nom de périphérique. (Pour plus d'informations, consultez Noms des appareils pour les volumes sur les EC2 instances Amazon.) Le nombre de volumes de stockage d'instance disponibles dépend du type d'instance. Pour les instances comportant des volumes de stockage d'NVMeinstance, le mappage des périphériques de ces volumes dépend de l'ordre dans lequel le système d'exploitation énumère les volumes.
6. Choisissez Create image (Créer une image).

AWS CLI

Pour ajouter des volumes de stockage d'instance à un à AMI l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez Accédez à Amazon EC2.

- create-image ou register-image (AWS CLI)
- New-EC2Imageet Register-EC2Image(AWS Tools for Windows PowerShell)

Ajouter des volumes de stockage d'instance à une EC2 instance lors du lancement

Lorsque vous lancez un type d'instance avec des volumes de stockage autres que les NVMe instances, tels que C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 et X1e, vous devez spécifier les mappages de périphériques de bloc pour les volumes de stockage d'instance que vous souhaitez associer au lancement. Les mappages de périphériques en mode bloc doivent être spécifiés dans la demande de lancement de l'instance ou dans le AMI fichier utilisé pour lancer l'instance.

S'il AMI inclut des mappages de périphériques par blocs pour les volumes de stockage d'instance, il n'est pas nécessaire de spécifier des mappages de périphériques par blocs dans la demande de lancement d'instance, sauf si vous avez besoin de plus de volumes de stockage d'instance que ce qui est inclus dans le. AMI

Si les mappages de périphériques par blocs pour les volumes de stockage d'instance AMI ne sont pas inclus, vous devez spécifier les mappages de périphériques par blocs dans la demande de lancement d'instance.

Pour les types d'NVMeinstance dotés de volumes de stockage d'instance, tous les volumes de stockage d'instance pris en charge sont automatiquement attachés à l'instance au lancement.

Considérations

- Pour les instances M3, il se peut que vous receviez les volumes de stockage d'instance, même si vous ne les spécifiez pas dans le mappage de périphérique de stockage en mode bloc de l'instance.

Pour spécifier des mappages de périphérique de stockage en mode bloc dans la requête de lancement de l'instance, utilisez l'une des méthodes suivantes.

Amazon EC2 console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le tableau de bord, choisissez Lancer une instance.
3. Dans la section Images de l'application et du système d'exploitation, sélectionnez le AMI à utiliser.

4. Dans Configurer le stockage, la section Volumes de stockage d'instances répertorie les volumes de stockage d'instances qui peuvent être attachés à l'instance. Le nombre de volumes de stockage d'instance disponibles dépend du type d'instance.
5. Pour chaque volume de stockage d'instances à attacher, dans Nom du périphérique, sélectionnez le nom du périphérique à utiliser.
6. Configurez les paramètres d'instance restants selon les besoins, puis cliquez sur Lancer l'instance.

Command line

Vous pouvez utiliser l'une des commandes suivantes avec l'option correspondante.

- `--block-device-mappings` avec run-instances (AWS CLI)
- `-BlockDeviceMapping`avec New-EC2Instance(AWS Tools for Windows PowerShell)

Rendre le volume de stockage d'instance disponible pour une utilisation sur une EC2 instance

Après avoir lancé une instance avec des volumes de stockage d'instances associés, vous devez monter les volumes avant de pouvoir y accéder.

Instances Linux

Vous pouvez formater les volumes avec le système de fichiers de votre choix après avoir lancé votre instance.

Vous pouvez afficher et monter les volumes de stockage de l'instance comme décrit dans la procédure suivante.

Pour rendre disponible un volume de stockage d'instance sur Linux

1. Connectez-vous à l'instance à l'aide d'un SSH client. Pour de plus amples informations, veuillez consulter Connectez-vous à votre instance Linux à l'aide de SSH.
2. Utilisez la commande `df -h` pour afficher les volumes qui sont formatés et montés.

```
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        3.8G   72K  3.8G   1% /dev
```

```
tmpfs           3.8G     0  3.8G   0% /dev/shm
/dev/nvme0n1p1  7.9G  1.2G  6.6G  15% /
```

3. Utilisez la commande `lsblk` pour afficher les volumes qui ont été mappés au lancement, mais ne sont ni formatés ni montés.

```
$ lsblk
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme0n1       259:1    0    8G  0 disk
##nvme0n1p1   259:2    0    8G  0 part /
##nvme0n1p128 259:3    0    1M  0 part
nvme1n1       259:0    0 69.9G  0 disk
```

4. Pour formater et monter un volume de stockage d'instance qui a seulement été mappé, procédez comme suit :

   a. Créez un système de fichiers sur le périphérique avec la commande `mkfs`.

   ```
   $ sudo mkfs -t xfs /dev/nvme1n1
   ```

   b. Créez un répertoire sur lequel monter le périphérique avec la commande `mkdir`.

   ```
   $ sudo mkdir /data
   ```

   c. Montez le périphérique sur le répertoire nouvellement créé à l'aide de la commande `mount`.

   ```
   $ sudo mount /dev/nvme1n1 /data
   ```

instances Windows

Pour les instances Windows, nous reformatons les volumes de stockage des instances avec le système de NTFS fichiers.

Vous pouvez consulter les volumes de stockage des instances à l'aide de Windows Disk Management. Pour de plus amples informations, veuillez consulter Répertorier les NVMe non-disques.

Pour monter manuellement un volume de stockage d'instance

1. Choisissez Start (Démarrer), entrez Computer Management (Gestion de l'ordinateur), puis appuyez sur Entrée.

2. Dans le panneau de gauche, choisissez Disk Management (Gestion des disques).
3. Si vous êtes invité à initialiser le volume, choisissez le volume à initialiser, sélectionnez le type de partition requis en fonction de votre cas d'utilisation, puis choisissez OK.
4. Dans la liste des volumes, cliquez avec le bouton droit sur le volume à monter, puis choisissez New Simple Volume (Nouveau volume simple).
5. Dans l'assistant, choisissez Next (Suivant).
6. Dans l'écran de spécification de la taille du volume, choisissez Next (Suivant) pour utiliser la taille de volume maximale. Vous pouvez également choisir une taille de volume comprise entre l'espace disque minimal et maximal.
7. Dans l'écran d'affectation d'une lettre de lecteur ou d'un chemin, effectuez l'une des opérations suivantes et choisissez Next (Suivant).
   - Pour monter le volume avec une lettre de lecteur, choisissez Assign the following drive letter (Affecter la lettre de lecteur suivante) puis choisissez la lettre de lecteur à utiliser.
   - Pour monter le volume en tant que dossier, choisissez Monter dans le NTFS dossier vide suivant, puis choisissez Parcourir pour créer ou sélectionner le dossier à utiliser.
   - Pour monter le volume sans lettre de lecteur ou chemin d'accès, choisissez Do not assign a drive letter or drive path (Ne pas affecter de lettre ou de chemin d'accès de lecteur).
8. Dans l'écran de formatage de partition, indiquez si le volume doit être formaté ou non. Si vous choisissez de formater le volume, choisissez le système de fichiers requis et la taille de l'unité, puis spécifiez un libellé de volume.
9. Choisissez Next (Suivant), Finish (Terminer).

Pour obtenir des instructions sur le montage automatique d'un volume attaché après le redémarrage, consultez la section Montage automatique d'un volume attaché après le redémarrage dans le guide de EBS l'utilisateur Amazon.

Activer le volume d'échange de stockage d'instance pour les EC2 instances M1 et C1

> **Note**
>
> Cette rubrique s'applique uniquement `c1.medium` aux instances `m1.small` Linux.

Les types d'`m1.small`instance `c1.medium` et disposent d'une quantité limitée de mémoire physique. Par conséquent, un volume d'échange de 900 MiB leur est attribué au moment du lancement pour servir de mémoire virtuelle, ou d'espace d'échange, pour le système Linux. L'espace d'échange de Linux peut être utilisé quand un système nécessite plus de mémoire que celle qui lui a été allouée physiquement. Quand l'espace d'échange est activé, les systèmes Linux peuvent échanger exceptionnellement les pages mémoire utilisées entre la mémoire physique et l'espace d'échange (partition dédiée ou fichier d'échange d'un système de fichiers existant) et libérer cet espace pour les pages mémoire qui nécessitent un accès à haute vitesse.

> **Note**
>
> - L'utilisation de l'espace d'échange pour la pagination de la mémoire n'est ni aussi rapide ni aussi efficace que l'utilisationRAM. Si votre charge de travail injecte régulièrement de la mémoire dans de l'espace d'échange, vous devriez envisager de migrer vers un type d'instance plus important contenant davantage de mémoire. RAM Pour de plus amples informations, veuillez consulter Changements de type d'EC2instance Amazon.
> - Même si le noyau Linux considère cet espace d'échange comme une partition du périphérique racine, il s'agit réellement d'un volume de stockage d'instance distinct, quel que soit votre type de périphérique racine.

Amazon Linux active et utilise automatiquement cet espace d'échange, mais certaines étapes supplémentaires AMI peuvent être nécessaires pour reconnaître et utiliser cet espace d'échange. Pour vérifier si votre instance utilise un espace d'échange, vous pouvez utiliser la commande swapon -s.

```
[ec2-user ~]$ swapon -s
Filename                                Type            Size    Used    Priority
/dev/xvda3                              partition       917500  0       -1
```

L'instance ci-dessus possède un volume d'échange de 900 Mio attaché et activé. Si vous ne voyez aucun volume d'échange apparaître avec cette commande, vous devez peut-être activer l'espace d'échange pour le périphérique. Vérifiez vos disques disponibles à l'aide de la commande lsblk.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
```

```
xvda3 202:3    0  896M  0 disk
```

Ici, le volume d'échange `xvda3` est accessible à l'instance, mais il n'est pas activé (notez que le champ `MOUNTPOINT` est vide). Vous pouvez activer le volume d'échange avec la commande swapon.

> **Note**
>
> Vous devez préfixer par `/dev/` le nom du périphérique affiché par lsblk. Votre périphérique peut avoir un nom différent, tel que `sda3`, `sde3` ou `xvde3`. Utilisez le nom de périphérique pour votre système dans la commande ci-après.

```
[ec2-user ~]$ sudo swapon /dev/xvda3
```

L'espace d'échange apparaît désormais dans la sortie lsblk et swapon -s.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M  0 disk [SWAP]
[ec2-user ~]$ swapon -s
Filename                                Type            Size    Used    Priority
/dev/xvda3                              partition       917500  0       -1
```

Vous devez aussi modifier votre fichier `/etc/fstab` de telle sorte que cet espace d'échange soit automatiquement activé à chaque démarrage système.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Ajoutez la ligne suivante à votre fichier `/etc/fstab` (à l'aide du nom du périphérique d'échange de votre système) :

```
/dev/xvda3       none    swap    sw  0       0
```

Pour utiliser un volume de stockage d'instance comme espace d'échange

Tout volume de stockage d'instance peut être utilisé comme espace d'échange. Par exemple, le type d'`m3.medium`instance inclut un volume de stockage d'SSDinstance de 4 Go adapté à l'espace de

swap. Si votre volume de stockage d'instance est beaucoup plus grand (par exemple, 350 Go), vous pouvez envisager de partitionner le volume avec une partition d'échange plus petite de 4 à 8 Go, le reste étant affecté à un volume de données.

> **Note**
>
> Cette procédure s'applique uniquement aux types d'instance prenant en charge ce stockage d'instance. Pour obtenir la liste des types d'instances, consultez Limites de volume de stockage d'instance pour les EC2 instances.

1. Affichez les périphériques de stockage en mode bloc attachés à votre instance pour obtenir le nom de périphérique de votre volume de stockage d'instance.

```
[ec2-user ~]$ lsblk -p
NAME       MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
/dev/xvdb  202:16   0   4G  0 disk /media/ephemeral0
/dev/xvda1 202:1    0   8G  0 disk /
```

   Dans cet exemple, le volume de stockage d'instance est `/dev/xvdb`. Comme il s'agit d'une instance Amazon Linux, le volume de stockage d'instance est formaté et monté à `/media/ephemeral0` ; certains systèmes d'exploitation Linux n'opèrent pas ainsi automatiquement.

2. (Facultatif) Si votre volume de stockage d'instance est monté (il affiche un `MOUNTPOINT` dans la sortie de la commande lsblk), vous devez le démonter à l'aide de la commande suivante.

```
[ec2-user ~]$ sudo umount /dev/xvdb
```

3. Configurez une zone d'échange Linux sur le périphérique avec la commande mkswap.

```
[ec2-user ~]$ sudo mkswap /dev/xvdb
mkswap: /dev/xvdb: warning: wiping old ext3 signature.
Setting up swapspace version 1, size = 4188668 KiB
no label, UUID=b4f63d28-67ed-46f0-b5e5-6928319e620b
```

4. Activez le nouvel espace d'échange.

```
[ec2-user ~]$ sudo swapon /dev/xvdb
```

5. Vérifiez que le nouvel espace d'échange est en cours d'utilisation.

```
[ec2-user ~]$ swapon -s
Filename    Type  Size Used Priority
/dev/xvdb                               partition 4188668 0 -1
```

6. Modifiez votre fichier `/etc/fstab` de telle sorte que cet espace d'échange soit automatiquement activé à chaque démarrage système.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Si votre fichier `/etc/fstab` a une entrée pour `/dev/xvdb` (ou `/dev/sdb`), modifiez-la pour qu'elle corresponde à la ligne ci-dessous ; dans le cas contraire, ajoutez la ligne suivante à votre fichier `/etc/fstab` (à l'aide du nom de périphérique d'échange de votre système) :

```
/dev/xvdb       none    swap    sw  0       0
```

> **Important**
>
> Les données du volume de stockage d'instance sont perdues quand une instance est arrêtée ou mise en veille prolongée. Cela inclut également le formatage de l'espace d'échange du volume de stockage créé dans Step 3. Si vous arrêtez et redémarrez une instance qui a été configurée pour utiliser un espace d'échange de stockage d'instance, vous devez répéter Step 1 via Step 5 sur le nouveau volume de stockage d'instance.

Initialisation des volumes de stockage d'instance sur les EC2 instances

En raison de la façon dont Amazon EC2 virtualise les disques, la première écriture sur n'importe quel emplacement de certains volumes de stockage d'instance est plus lente que les écritures suivantes. Pour la plupart des applications, l'amortissement de ce coût sur la durée de vie de l'instance est acceptable. Cependant, si vous exigez des performances disque élevées, il est recommandé que vous initialisiez vos disques en écrivant une fois sur chaque emplacement disque avant l'utilisation en production.

> **Note**
>
> Les types d'instance dotés de disques SSD à connexion directe (SSD) et TRIM compatibles offrent des performances optimales au moment du lancement, sans initialisation. Pour plus

d'informations sur le stockage d'instance pour chaque type d'instance, consultez Limites de volume de stockage d'instance pour les EC2 instances.

Si vous avez besoin d'une plus grande flexibilité en termes de latence ou de débit, nous vous recommandons d'utiliser AmazonEBS.

Pour initialiser les volumes de stockage d'instance, utilisez les commandes dd suivantes, en fonction du stockage à initialiser (par exemple, `/dev/sdb` ou `/dev/nvme1n1`).

> **Note**
>
> Veillez bien à démonter le disque avant d'exécuter cette commande.
> L'initialisation peut durer longtemps (8 heures environ pour une grande instance supplémentaire).

Pour initialiser les volumes de stockage d'instance, utilisez les commandes suivantes sur les types d'instance `m1.large`, `m1.xlarge`, `c1.xlarge`, `m2.xlarge`, `m2.2xlarge` et `m2.4xlarge` :

```
dd if=/dev/zero of=/dev/sdb bs=1M
dd if=/dev/zero of=/dev/sdc bs=1M
dd if=/dev/zero of=/dev/sdd bs=1M
dd if=/dev/zero of=/dev/sde bs=1M
```

Pour initialiser simultanément tous les volumes de stockage d'instance, utilisez la commande suivante :

```
dd if=/dev/zero bs=1M|tee /dev/sdb|tee /dev/sdc|tee /dev/sde > /dev/sdd
```

La configuration des lecteurs pour RAID les initialiser en écrivant sur chaque emplacement du lecteur. Lors de la configuration logicielleRAID, assurez-vous de modifier la vitesse de reconstruction minimale :

```
echo $((30*1024)) > /proc/sys/dev/raid/speed_limit_min
```

Volumes root pour vos EC2 instances Amazon

Lorsque vous lancez une instance, nous créons un volume racine pour l'instance. Le volume racine contient l'image utilisée pour démarrer l'instance. Chaque instance possède un volume racine unique. Vous pouvez ajouter des volumes de stockage à vos instances pendant ou après le lancement.

Le volume AMI que vous utilisez pour lancer une instance détermine le type de volume racine. Vous pouvez lancer une instance à partir d'une instance basée sur Amazon EBS AMI (instances Linux et Windows) ou d'une instance sauvegardée en magasin AMI (instances Linux uniquement). Il existe des différences significatives entre ce que vous pouvez faire avec chaque type deAMI. Pour plus d'informations sur ces différences, consultez Root device type.

Nous vous recommandons d'utiliser AMIs Backed by AmazonEBS, car ces instances se lancent plus rapidement et utilisent un stockage persistant.

Nous réservons des noms de périphérique spécifiques aux volumes racines. Pour de plus amples informations, veuillez consulter Noms des appareils pour les volumes sur les EC2 instances Amazon.

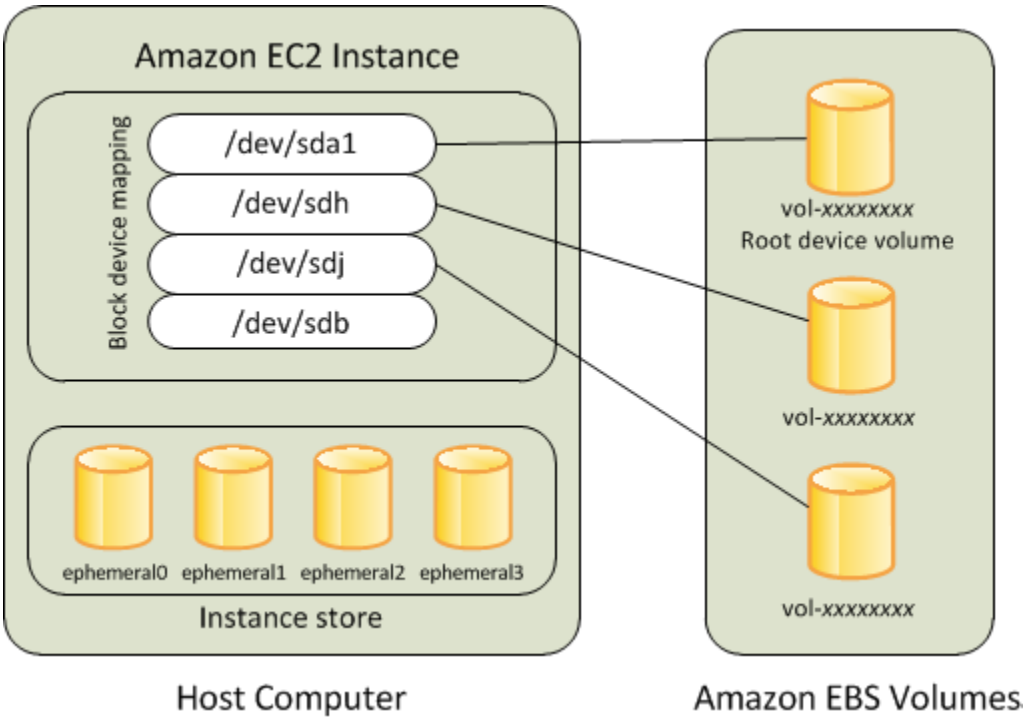
Table des matières

Instances EBS soutenues par Amazon

Les instances qui utilisent Amazon EBS pour le volume racine sont automatiquement associées à un EBS volume Amazon. Lorsque vous lancez une instance EBS basée sur Amazon, nous créons un EBS volume Amazon pour chaque EBS instantané Amazon référencé par celui AMI que vous utilisez. Vous pouvez éventuellement utiliser d'autres EBS volumes Amazon ou volumes de stockage d'instance, selon le type d'instance.

Une instance EBS basée sur Amazon peut être arrêtée puis redémarrée sans affecter les données stockées dans les volumes attachés. Il existe différentes tâches liées aux instances et aux volumes que vous pouvez effectuer lorsqu'une instance EBS basée sur Amazon est arrêtée. Par exemple, vous pouvez modifier les propriétés de l'instance, changer sa taille ou mettre à jour le noyau qu'elle

utilise, ou vous pouvez aussi attacher votre volume racine à une autre instance en cours d'exécution à des fins de débogage ou autre. Pour plus d'informations, consultez Amazon EBS Volumes.



Limitation

Vous ne pouvez pas utiliser `st1` nos `sc1` EBS volumes en tant que volumes racine.

Défaillance de l'instance

Si une instance EBS basée sur Amazon échoue, vous pouvez restaurer votre session en suivant l'une des méthodes suivantes :

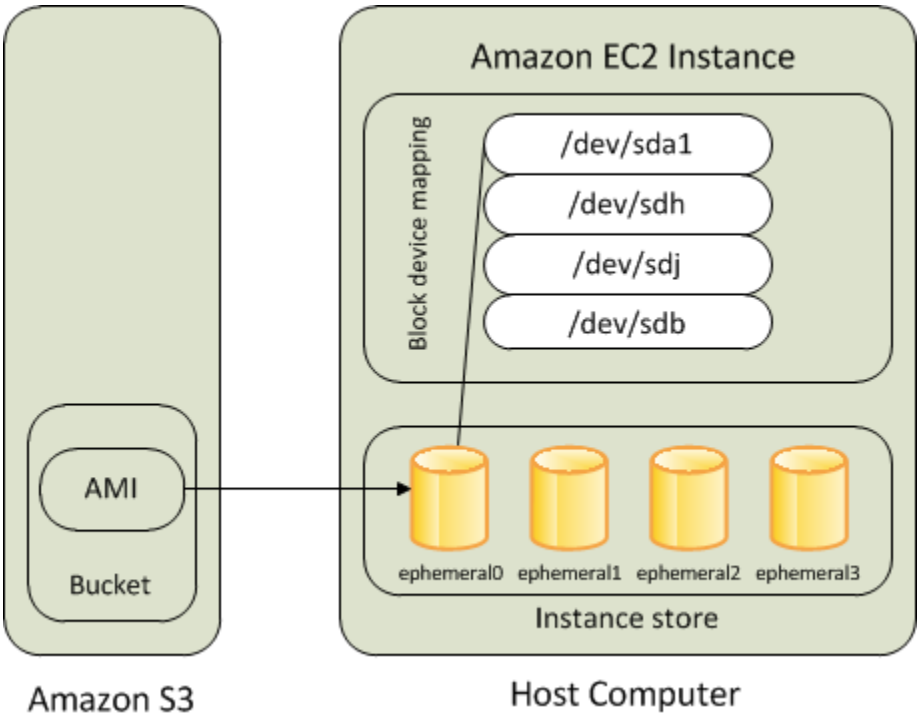
- Arrêtez l'instance et redémarrez-la (essayez cette méthode en premier).
- Capturez automatiquement tous les volumes pertinents et créez-en un nouveauAMI. Pour de plus amples informations, veuillez consulter Créez un compte soutenu EBS par Amazon AMI.
- Attachez le volume à la nouvelle instance à l'aide des étapes suivantes :
  1. Créez un instantané du volume racine.
  2. Enregistrez un nouveau AMI à l'aide de l'instantané.
  3. Lancez une nouvelle instance à partir de la nouvelleAMI.
  4. Détachez les EBS volumes Amazon restants de l'ancienne instance.
  5. Rattachez les EBS volumes Amazon à la nouvelle instance.

Instances basées sur le stockage d'instances (instances Linux uniquement)

> **Note**
>
> Les instances Windows ne prennent pas en charge les volumes racine sauvegardés par le stockage d'instances.

Les instances qui utilisent les stockages d'instance pour le volume racine ont automatiquement un ou plusieurs volumes de stockage d'instance disponibles, l'un faisant office de volume racine. Quand une instance est lancée, l'image utilisée pour démarrer l'instance est copiée sur le volume racine. Notez que vous pouvez utiliser le cas échéant des volumes de stockage d'instance supplémentaires, suivant le type d'instance.

Les données présentes sur les volumes de stockage d'instance demeurent aussi longtemps que l'instance s'exécute, mais ces données sont supprimées quand il est procédé à la terminaison de l'instance (les instances basées sur le stockage d'instance ne prennent pas en charge l'action Stop) ou en cas de défaillance de l'instance (problèmes rencontrés par un lecteur sous-jacent, par exemple). Pour de plus amples informations, veuillez consulter Stockage d'instances Stockage par blocs temporaire pour les EC2 instances.



Types d'instance pris en charge

Seuls les types d'instance suivants prennent en charge un volume de stockage d'instance en tant que volume racine : C1, C3, D2, I2, M1, M2, M3, R3 et X1.

Défaillance de l'instance

Après qu'une instance basée sur le stockage d'instances a échoué ou s'est terminée, elle ne peut pas être restaurée. Si vous envisagez d'utiliser des EC2 instances basées sur des magasins d'instances Amazon, nous vous recommandons vivement de distribuer les données de vos magasins d'instances sur plusieurs zones de disponibilité. Vous devez aussi sauvegarder régulièrement les données critiques de vos volumes de stockage d'instance sur un stockage permanent.

Conserver un volume EBS racine Amazon après la résiliation d'une EC2 instance Amazon

Par défaut, le volume EBS racine Amazon d'une instance est supprimé lorsque l'instance se termine. Vous pouvez modifier le comportement par défaut pour garantir qu'un volume EBS racine Amazon persiste après la fin de l'instance. Pour modifier le comportement par défaut, définissez l'`DeleteOnTermination`attribut sur`false`. Vous pouvez le faire au lancement de l'instance ou ultérieurement.

Tâches

- Configurer le volume racine pour qu'il persiste pendant le lancement de l'instance
- Configurer le volume racine pour qu'il persiste pour une instance existante
- Confirmer qu'un volume racine est configuré pour persister

Configurer le volume racine pour qu'il persiste pendant le lancement de l'instance

Vous pouvez configurer le volume racine pour qu'il persiste lorsque vous lancez une instance.

Console

Configurer le volume racine pour qu'il persiste lorsque vous lancez une instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances, puis Lancer une instance.
3. Choisissez une Amazon Machine Image (AMI), choisissez un type d'instance, choisissez une paire de clés et configurez vos paramètres réseau.

4. Pour Configurer le stockage, choisissez Avancé.
5. Développez le volume racine.
6. Pour Supprimer à la résiliation, choisissez Non.
7. Une fois la configuration de votre instance terminée, choisissez Lancer l'instance.

AWS CLI

Pour configurer le volume racine de manière à ce qu'il persiste lorsque vous lancez une instance à l'aide du AWS CLI

Utilisez la commande run-instances et incluez un mappage de périphérique en mode bloc qui définit l'attribut `DeleteOnTermination` avec la valeur `false`.

```
aws ec2 run-instances --block-device-mappings file://mapping.json ...other
 parameters...
```

Spécifiez les éléments suivants dans `mapping.json`.

```
[
    {
        "DeviceName": "/dev/sda1",
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
]
```

Tools for Windows PowerShell

Pour configurer le volume racine de manière à ce qu'il persiste lorsque vous lancez une instance à l'aide des Outils pour Windows PowerShell

Utilisez la New-EC2Instancecommande et incluez un mappage de périphériques en mode bloc qui définit l'`DeleteOnTermination`attribut sur`false`.

```
C:\> $ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
C:\> $ebs.DeleteOnTermination = $false
C:\> $bdm = New-Object Amazon.EC2.Model.BlockDeviceMapping
C:\> $bdm.DeviceName = "dev/xvda"
```

```
C:\> $bdm.Ebs = $ebs
C:\> New-EC2Instance -ImageId ami-0abcdef1234567890 -BlockDeviceMapping
 $bdm ...other parameters...
```

Configurer le volume racine pour qu'il persiste pour une instance existante

Vous pouvez configurer le volume racine pour qu'il persiste pendant une instance en cours d'exécution. Notez que vous ne pouvez pas effectuer cette tâche à l'aide de la EC2 console Amazon.

AWS CLI

Pour configurer le volume racine de manière à ce qu'il soit conservé pour une instance existante à l'aide du AWS CLI

Utilisez la modify-instance-attributecommande avec un mappage de périphériques en mode bloc qui définit l'`DeleteOnTermination`attribut sur`false`.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-
mappings file://mapping.json
```

Spécifiez les éléments suivants dans `mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
]
```

Tools for Windows PowerShell

Configurer le volume racine pour qu'il persiste pour une instance existante à l'aide de AWS Tools for Windows PowerShell

Utilisez la Edit-EC2InstanceAttributecommande avec un mappage de périphériques en mode bloc qui définit l'`DeleteOnTermination`attribut sur`false`.

```
C:\> $ebs = New-Object Amazon.EC2.Model.EbsInstanceBlockDeviceSpecification
```

```
C:\> $ebs.DeleteOnTermination = $false
C:\> $bdm = New-Object Amazon.EC2.Model.InstanceBlockDeviceMappingSpecification
C:\> $bdm.DeviceName = "/dev/xvda"
C:\> $bdm.Ebs = $ebs
C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -BlockDeviceMapping
 $bdm
```

Confirmer qu'un volume racine est configuré pour persister

Vous pouvez confirmer qu'un volume racine est configuré pour persister à l'aide de la EC2 console Amazon ou des outils de ligne de commande.

Console

Pour confirmer qu'un volume racine est configuré pour persister à l'aide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Instances, puis sélectionnez l'instance.
3. Dans l'onglet Stockage, sous Bloquer les appareil, recherchez l'entrée du volume racine. Si la valeur Supprimer lors de la résiliation est définie avec la valeur No, le volume est configuré pour persister.

AWS CLI

Pour confirmer qu'un volume racine est configuré pour persister à l'aide du AWS CLI

Utilisez la commande describe-instances et vérifiez que l'attribut `DeleteOnTermination` de l'élément de réponse `BlockDeviceMappings` est défini avec la valeur `false`.

```
aws ec2 describe-instances --instance-id i-1234567890abcdef0
```

```
...
    "BlockDeviceMappings": [
    {
        "DeviceName": "/dev/sda1",
        "Ebs": {
            "Status": "attached",
            "DeleteOnTermination": false,
```

```
            "VolumeId": "vol-1234567890abcdef0",
            "AttachTime": "2013-07-19T02:42:39.000Z"
        }
    }
...
```

Tools for Windows PowerShell

Pour confirmer qu'un volume racine est configuré pour persister à l'aide du AWS Tools for Windows PowerShell

Utilisez Get-EC2Instanceet vérifiez que l'`DeleteOnTermination`attribut de l'élément de `BlockDeviceMappings` réponse est défini sur`false`.

```
C:\> (Get-EC2Instance -InstanceId i-
i-1234567890abcdef0).Instances.BlockDeviceMappings.Ebs
```

Remplacez le volume racine d'une EC2 instance Amazon sans l'arrêter

Amazon vous EC2 permet de remplacer le EBS volume Amazon racine d'une instance en cours d'exécution tout en conservant les éléments suivants :

- Données stockées sur les volumes de stockage d'instance — Les volumes de stockage d'instances restent attachés à l'instance après la restauration du volume racine.
- Données stockées sur des EBS volumes Amazon (non root) — Les EBS volumes Amazon non root restent attachés à l'instance une fois le volume racine restauré.
- Configuration réseau : toutes les interfaces réseau restent attachées à l'instance et conservent leurs adresses IP, leurs identifiants et leurs pièces jointesIDs. Lorsque l'instance devient disponible, tout le trafic réseau en attente est purgé. En outre, l'instance reste sur le même hôte physique, de sorte qu'elle conserve ses adresses IP publiques et privées ainsi que son DNS nom.
- IAMpolitiques : les IAM profils et les politiques (tels que les politiques basées sur des balises) associés à l'instance sont conservés et appliqués.

Table des matières

Comment fonctionne le remplacement du volume racine

Lorsque vous remplacez le volume racine d'une instance, nous créons une tâche de remplacement du volume racine. Le volume racine d’origine est détaché de l’instance et le nouveau volume racine est attaché à l’instance à sa place. Le mappage de périphérique de stockage en mode bloc de l’instance est mis à jour pour refléter l’ID du volume racine de remplacement.

Lorsque vous remplacez le volume racine d'une instance, vous devez spécifier la source de l'instantané pour le nouveau volume. Les options possibles sont les suivantes.

Restaurer l'état d'origine d'un volume racine

Cette option remplace le volume racine actuel par un volume basé sur le cliché utilisé pour le créer.

Considérations relatives à l'utilisation de l'état de lancement

Le volume racine de remplacement a les mêmes attributs de type, de taille et de suppression à la résiliation que le volume racine d’origine.

Remplacez le volume racine à l'aide d'un instantané

Cette option remplace le volume racine actuel par un volume de remplacement basé sur le cliché que vous spécifiez. Par exemple, un instantané spécifique que vous avez créé précédemment à partir de ce volume racine. Cela est utile si vous devez résoudre des problèmes liés à la corruption du volume racine ou à des erreurs de configuration réseau dans le système d'exploitation client.

Le volume racine de remplacement a les mêmes attributs de type, de taille et de suppression à la résiliation que le volume racine d’origine.

Considérations relatives à l’utilisation d’un instantané

- Vous ne pouvez utiliser que des instantanés appartenant à la même lignée que le volume racine actuel.
- Vous ne pouvez pas utiliser de copies d’instantanés créées à partir d’instantanés provenant du volume racine.
- Après avoir remplacé le volume racine avec succès, vous pouvez toujours utiliser des instantanés pris à partir du volume racine d'origine pour remplacer le nouveau volume racine (de remplacement).

Remplacez le volume racine à l'aide d'un AMI

Cette option remplace le volume racine actuel par un volume AMI que vous spécifiez. Cela est utile si vous devez appliquer des correctifs ou des mises à niveau du système d'exploitation et des applications. Le code produit, les informations de facturation, le type d'architecture et le même type de virtualisation AMI doivent être identiques à ceux de l'instance.

Si l'instance est activée pour ENA ou sriov-net, vous devez utiliser un système AMI qui prend en charge ces fonctionnalités. Si l'instance n'est pas activée pour ENA sriov-net, vous pouvez soit sélectionner une instance AMI qui ne prend pas en charge ces fonctionnalités, soit ajouter automatiquement une assistance si vous sélectionnez une instance AMI qui prend en charge ENA ou sriov-net.

Si l'instance est activée pour NitroTPM, vous devez utiliser une instance sur AMI laquelle Nitro TPM est activé. Le TPM support Nitro n'est pas activé si l'instance n'a pas été configurée pour cela, quelle que soit celle AMI que vous avez sélectionnée.

Vous pouvez sélectionner un mode AMI de démarrage différent de celui de l'instance, à condition que l'instance prenne en charge le mode de démarrage duAMI. Si l'instance ne prend pas en charge le mode de démarrage, la demande échoue. Si l'instance prend en charge le mode de démarrage, le nouveau mode de démarrage est propagé à l'instance et ses UEFI données sont mises à jour en conséquence. Si vous avez modifié manuellement l'ordre de démarrage ou ajouté une clé de démarrage UEFI sécurisée privée pour charger les modules du noyau privé, les modifications sont perdues lors du remplacement du volume racine.

Le volume racine de remplacement obtient le même type de volume et le même attribut de suppression à la fin que le volume racine d'origine, et il obtient la taille du mappage de périphériques par blocs du volume AMI racine.

> **Note**
>
> La taille du mappage des périphériques par blocs de volume AMI racine doit être égale ou supérieure à la taille du volume racine d'origine. Si la taille du mappage du périphérique par blocs de volume AMI racine est inférieure à la taille du volume racine d'origine, la demande échoue.

Une fois la tâche de remplacement du volume racine terminée, les informations nouvelles et mises à jour suivantes sont reflétées lorsque vous décrivez l'instance à l'aide de la console, AWS CLI ou AWS SDKs :

- Nouvel AMI identifiant
- Nouvel ID de volume pour le volume racine
- Configuration du mode de démarrage mise à jour (si modifiée par leAMI)
- TPMConfiguration Nitro mise à jour (si activée par leAMI)
- ENAConfiguration mise à jour (si activée par leAMI)
- Configuration sriov-net mise à jour (si activée par le) AMI

Le nouvel AMI ID est également reflété dans les métadonnées de l'instance.

Considérations relatives à l'utilisation d'un AMI :

- Si vous utilisez un AMI qui possède plusieurs mappages de périphériques en mode bloc, seul le volume racine du AMI est utilisé. Les autres volumes (non racine) sont ignorés.
- Vous ne pouvez utiliser cette fonctionnalité que si vous êtes autorisé à accéder à l'instantané du volume racine AMI et à son instantané associé. Vous ne pouvez pas utiliser cette fonctionnalité avec AWS Marketplace AMIs.
- Vous ne pouvez utiliser une instance AMI sans code produit que si l'instance ne possède pas de code produit.
- La taille du mappage des périphériques par blocs de volume AMI racine doit être égale ou supérieure à la taille du volume racine d'origine. Si la taille du mappage du périphérique par blocs de volume AMI racine est inférieure à la taille du volume racine d'origine, la demande échoue.
- Les documents d'identité de l'instance sont automatiquement mis à jour.
- Si l'instance prend en charge NitroTPM, les TPM données Nitro de l'instance sont réinitialisées et de nouvelles clés sont générées.

Vous pouvez choisir de conserver ou non le volume racine d'origine une fois le processus de remplacement du volume racine terminé. Si vous choisissez de supprimer le volume racine d'origine une fois le processus de remplacement terminé, le volume racine d'origine est automatiquement supprimé et devient irrécupérable. Si vous choisissez de conserver le volume racine d'origine une fois le processus terminé, le volume reste approvisionné dans votre compte ; vous devez le supprimer manuellement lorsque vous n'en avez plus besoin.

La tâche de remplacement du volume racine passe par les états suivants :

- `pending`— Le volume de remplacement est en cours de création.
- `in-progress`— Le volume d'origine est en train d'être détaché et le volume de remplacement est en cours de fixation.
- `succeeded`— Le volume de remplacement a été correctement attaché à l'instance et celle-ci est disponible.
- `failing`— La tâche de remplacement est sur le point d'échouer.
- `failed`— La tâche de remplacement a échoué, mais le volume racine est toujours connecté.
- `failing-detached`— La tâche de remplacement est sur le point d'échouer et aucun volume racine n'est peut-être attaché à l'instance.
- `failed-detached`— La tâche de remplacement a échoué et aucun volume racine n'est attaché à l'instance.

Si la tâche de remplacement du volume racine échoue, l'instance est redémarrée et le volume racine d'origine reste attaché à l'instance.

Considérations

Avant de commencer, considérez les points suivants.

Prérequis

- L'instance doit être dans l'état `running`.
- L'instance est automatiquement redémarrée pendant le processus. Le contenu de la mémoire (RAM) est effacé lors du redémarrage. Aucun redémarrage manuel n'est nécessaire.
- Vous ne pouvez pas remplacer le volume racine s'il s'agit d'un volume de stockage d'instances. Seules les instances avec des volumes EBS racine Amazon sont prises en charge.
- Vous pouvez remplacer le volume racine pour tous les types d'instances virtualisées et les instances bare metal EC2 Mac. Aucun autre type d'instance bare metal n'est pris en charge.
- Vous pouvez utiliser n'importe quel instantané qui appartient à la même lignée que l'un des volumes racine précédents de l'instance.
- Si le EBS chiffrement Amazon est activé par défaut sur votre compte dans la région actuelle, le volume racine de remplacement créé par la tâche de remplacement du volume racine est toujours chiffré, quel que soit l'état de chiffrement de l'instantané spécifié ou du volume racine du volume racine spécifiéAMI.

Résultats du chiffrement

Le tableau suivant récapitule les résultats de chiffrement possibles.

	Volume racine d'origine	Instantané spécifié ou AMI	Chiffrement par défaut	Remplacement du volume racine	Clé de chiffrement utilisée pour le volume racine de remplacement
Restaurer le volume racine de remplacement à l'état de lancement initial	Chiffré	Ne s'applique pas	Non pris en compte	Chiffré	Même KMS clé que le volume racine d'origine
	Non chiffré	Ne s'applique pas	Désactivées	Non chiffré	Ne s'applique pas
	Non chiffré	Ne s'applique pas	Activées	Chiffré	KMSClé par défaut du compte pour le EBS chiffrement Amazon
Restaurez le volume racine de remplacement à partir d'un instantané ou AMI	Chiffré	Non chiffré	Non pris en compte	Chiffré	Même KMS clé que le volume racine d'origine
	Chiffré	Chiffré	Non pris en compte	Chiffré	Même KMS clé que le volume

	Volume racine d'origine	Instantané spécifié ou AMI	Chiffrement par défaut	Remplacement du volume racine	Clé de chiffrement utilisée pour le volume racine de remplacement
					racine d'origine
	Non chiffré	Non chiffré	Désactivées	Non chiffré	Ne s'applique pas
	Non chiffré	Non chiffré	Activées	Chiffré	KMSClé par défaut du compte pour le EBS chiffrement Amazon

	Volume racine d'origine	Instantané spécifié ou AMI	Chiffrement par défaut	Remplacement du volume racine	Clé de chiffrement utilisée pour le volume racine de remplacement
	Non chiffré	Chiffré	Non pris en compte	Chiffré	Si le compte AMI ou le snapshot appartient au compte, le volume de remplacement est chiffré avec la KMS clé du snapshot AMI ou du snapshot. Si AMI un instantané est partagé avec le compte, le volume de remplacement est chiffré avec la KMS clé par défaut du compte pour le EBS chiffrement Amazon.

Remplacer un volume racine

Lorsque vous remplacez le volume racine d'une instance, une tâche de remplacement du volume racine est créé. Vous pouvez utiliser la tâche de remplacement du volume racine pour surveiller la progression et le résultat du processus de remplacement.

Console

Pour remplacer le volume racine

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance dont vous souhaitez remplacer le volume racine et choisissez Actions, Surveiller et résoudre les problèmes, Remplacer le volume racine.

   > **Note**
   >
   > L'action Replace root volume (Remplacer le volume racine) est désactivée si l'instance sélectionnée n'est pas dans l'état `running`.

4. Dans l'écran Remplacer le volume racine, pour Restaurer, choisissez l'une des options suivantes :

   - État de lancement : restaurez le volume racine de remplacement à partir de l'instantané utilisé pour créer le volume racine actuel.
   - Instantané : restaurez le volume racine de remplacement sur le cliché que vous spécifiez. Pour Snapshot, sélectionnez l'instantané à utiliser.
   - Image — Restaurez le volume racine de remplacement à l'aide du volume AMI que vous spécifiez. Pour Image, sélectionnez le AMI à utiliser.

5. (Facultatif) Pour supprimer le volume racine que vous remplacez, sélectionnez Supprimer le volume racine remplacé.
6. Choisissez Créer une tâche de remplacement.
7. Pour surveiller la tâche de remplacement, choisissez l'onglet Stockage de l'instance et sélectionnez Tâches récentes de remplacement du volume racine.

AWS CLI

Pour restaurer le volume racine de remplacement à l'état de lancement

Utilisez la commande create-replace-root-volume-task. Pour `--instance-id`, spécifiez l'ID de l'instance dont le volume racine doit être remplacé. Omettez les paramètres `--snapshot-id` et `--image-id`. Pour supprimer le volume racine d'origine après qu'il ait été remplacé, incluez `--delete-replaced-root-volume` et spécifiez `true`.

```
$ aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--delete-replaced-root-volume
```

Pour restaurer le volume racine de remplacement à un instantané spécifique

Utilisez la commande create-replace-root-volume-task. Pour `--instance-id`, spécifiez l'ID de l'instance dont le volume racine doit être remplacé. Pour `--snapshot-id`, spécifiez l'ID de l'instantané à utiliser. Pour supprimer le volume racine d'origine après qu'il ait été remplacé, incluez `--delete-replaced-root-volume` et spécifiez `true`.

```
$ aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--snapshot-id snap-9876543210abcdef0 \
--delete-replaced-root-volume
```

Pour restaurer le volume racine de remplacement à l'aide d'un AMI

Utilisez la commande create-replace-root-volume-task. Pour `--instance-id`, spécifiez l'ID de l'instance dont le volume racine doit être remplacé. Pour`--image-id`, spécifiez l'ID du AMI à utiliser. Pour supprimer le volume racine d'origine après qu'il ait été remplacé, incluez `--delete-replaced-root-volume` et spécifiez `true`.

```
$ aws ec2 create-replace-root-volume-task \
--instance-id i-01234567890abcdef \
--image-id ami-09876543210abcdef \
--delete-replaced-root-volume
```

Pour afficher l'état d'une tâche de remplacement du volume racine

Utilisez la commande describe-replace-root-volume-tasks et spécifiez les tâches IDs de remplacement du volume racine à afficher.

```
$ aws ec2 describe-replace-root-volume-tasks \
--replace-root-volume-task-ids replacevol-1234567890abcdef0
```

```
{
  "ReplaceRootVolumeTasks": [
  {
    "ReplaceRootVolumeTaskId": "replacevol-1234567890abcdef0",
    "InstanceId": "i-1234567890abcdef0",
    "TaskState": "succeeded",
    "StartTime": "2020-11-06 13:09:54.0",
    "CompleteTime": "2020-11-06 13:10:14.0",
    "SnapshotId": "snap-01234567890abcdef",
    "DeleteReplacedRootVolume": "True"
  }]
}
```

Vous pouvez également utiliser le filtre `instance-id` pour filtrer les résultats par instance.

```
$ aws ec2 describe-replace-root-volume-tasks \
--filters Name=instance-id,Values=i-1234567890abcdef0
```

Tools for Windows PowerShell

Pour restaurer le volume racine de remplacement à l'état de lancement

Utilisez la New-EC2ReplaceRootVolumeTaskcommande. Pour `-InstanceId`, spécifiez l'ID de l'instance dont le volume racine doit être remplacé. Omettez les paramètres `-SnapshotId` et `-ImageId`. Pour supprimer le volume racine d'origine après qu'il ait été remplacé, incluez `-DeleteReplacedRootVolume` et spécifiez `$true`.

```
PS C:\> New-EC2ReplaceRootVolumeTask -InstanceId i-1234567890abcdef0 -
DeleteReplacedRootVolume $true
```

Pour restaurer le volume racine de remplacement à un instantané spécifique

Utilisez la New-EC2ReplaceRootVolumeTaskcommande. Pour `--InstanceId`, spécifiez l'ID de l'instance dont le volume racine doit être remplacé. Pour `-SnapshotId`, spécifiez l'ID de l'instantané à utiliser. Pour supprimer le volume racine d'origine après qu'il ait été remplacé, incluez `-DeleteReplacedRootVolume` et spécifiez `$true`.

```
PS C:\> New-EC2ReplaceRootVolumeTask -InstanceId i-1234567890abcdef0 -
SnapshotId snap-9876543210abcdef0 -DeleteReplacedRootVolume $true
```

Pour restaurer le volume racine de remplacement à l'aide d'un AMI

Utilisez la New-EC2ReplaceRootVolumeTaskcommande. Pour `-InstanceId`, spécifiez l'ID de l'instance dont le volume racine doit être remplacé. Pour`-ImageId`, spécifiez l'ID du AMI à utiliser. Pour supprimer le volume racine d'origine après qu'il ait été remplacé, incluez `-DeleteReplacedRootVolume` et spécifiez `$true`.

```
PS C:\> New-EC2ReplaceRootVolumeTask -InstanceId i-1234567890abcdef0 -
ImageId ami-09876543210abcdef -DeleteReplacedRootVolume $true
```

Pour afficher l'état d'une tâche de remplacement du volume racine

Utilisez la Get-EC2ReplaceRootVolumeTaskcommande et spécifiez les tâches IDs de remplacement du volume racine à afficher.

```
PS C:\> Get-EC2ReplaceRootVolumeTask -
ReplaceRootVolumeTaskIds replacevol-1234567890abcdef0
```

Vous pouvez également utiliser le filtre `instance-id` pour filtrer les résultats par instance.

```
PS C:\> Get-EC2ReplaceRootVolumeTask -Filters @{Name = 'instance-id'; Values =
 'i-1234567890abcdef0'} | Format-Table
```

Noms des appareils pour les volumes sur les EC2 instances Amazon

Lorsque vous associez un volume à votre instance, vous incluez un nom d'appareil pour le volume. Ce nom d'appareil est utilisé par AmazonEC2. Le pilote de périphérique de bloc de l'instance attribue le nom réel du volume lors du montage du volume, et le nom attribué peut être différent du nom EC2 utilisé par Amazon.

Le nombre maximum de volumes que votre instance peut prendre en charge dépend du système d'exploitation. Pour plus d'informations, consultez Limites EBS de volume Amazon pour les EC2 instances Amazon.

Table des matières

Noms d'appareil disponibles

Instances Linux

Deux types de virtualisation sont disponibles pour les instances Linux : la virtualisation paravirtuelle (PV) et la machine virtuelle matérielle (HVM). Le type de virtualisation d'une instance est déterminé par le type AMI utilisé pour lancer l'instance. Tous les types d'instances sont pris en charge HVMAMIs. Certains types d'instances de la génération précédente prennent en charge le PVAMIs. N'oubliez pas de noter le type de virtualisation de votre instance, AMI car les noms de périphériques recommandés et disponibles que vous pouvez utiliser dépendent du type de virtualisation de votre instance. Pour plus d'informations, consultez Types de virtualisation.

Le tableau suivant répertorie les noms de périphériques disponibles que vous pouvez spécifier dans un mappage de périphériques en mode bloc ou lors de l'attachement d'un EBS volume.

Type de virtualisation	Disponible	Réservé pour le volume racine	Recommandé pour les EBS volumes	Volumes de stockage d'instances
Paravirtuel	/dev/sd[a-z] /dev/sd[a-z][1-15] /dev/hd[a-z] /dev/hd[a-z][1-15]	/dev/sda1	/dev/sd[f-p] /dev/sd[f-p][1-6]	/dev/sd[b-e]
HVM	/dev/sd[a-z] /dev/xvd [a-d] [a-x] /dev/xvd[e-z]	Diffère par AMI /dev/sda1 or /dev/xvda	/dev/sd[f-p] *	/dev/sd[b-e] /dev/sd[b-h] (h1.16xlarge)

Type de virtualisation	Disponible	Réservé pour le volume racine	Recommandé pour les EBS volumes	Volumes de stockage d'instances
				/dev/sd[b-y] (d2.8xlarge) /dev/sd[b-i] (i2.8xlarge) **

* Les noms de périphérique que vous spécifiez pour les NVMe EBS volumes dans un mappage de périphériques en mode bloc sont renommés à l'aide des noms de NVMe périphériques (`/dev/nvme[0-26]n1`). Le pilote de périphérique en mode bloc peut attribuer des noms de NVMe périphériques dans un ordre différent de celui que vous avez spécifié pour les volumes dans le mappage de périphériques en mode bloc.

** les volumes de stockage d'NVMeinstance sont automatiquement énumérés et un nom de NVMe périphérique leur est attribué.

instances Windows

Windows AMIs utilise l'un des ensembles de pilotes suivants pour autoriser l'accès au matériel virtualisé : AWS PV, Citrix PV et RedHat PV. Pour plus d'informations, consultez the section called "Pilotes PV Windows".

Le tableau suivant répertorie les noms de périphériques disponibles que vous pouvez spécifier dans un mappage de périphériques en mode bloc ou lors de l'attachement d'un EBS volume.

Type de pilote	Disponible	Réservé pour le volume racine	Recommandé pour les EBS volumes	Volumes de stockage d'instances
AWS PV, Citrix PV	xvd[b-z] xvd[b-c][a-z] /dev/sda1	/dev/sda1	xvd[f-z] *	xvdc[a-x] xvd[a-e] **

Type de pilote	Disponible	Réservé pour le volume racine	Recommandé pour les EBS volumes	Volumes de stockage d'instances
	/dev/sd[b-e]			
Virtualisation paravirtuelle Red Hat	xvd[a-z] xvd[b-c][a-z] /dev/sda1 /dev/sd[b-e]	/dev/sda1	xvd[f-p]	xvdc[a-x] xvd[a-e]

* Pour Citrix PV et Red Hat PV, si vous EBS mappez un volume avec son nom`xvda`, Windows ne le reconnaît pas (le volume est visible pour AWS PV ou AWS NVMe).

** les volumes de stockage d'NVMeinstance sont automatiquement énumérés et une lettre de lecteur Windows leur est attribuée.

Pour plus d'informations sur les volumes de stockage d'instance, consultez Stockage d'instances Stockage par blocs temporaire pour les EC2 instances. Pour plus d'informations sur les NVMe EBS volumes (instances basées sur Nitro), notamment sur la manière d'identifier l'EBSappareil, consultez Amazon EBS et NVMe le guide de l'EBSutilisateur Amazon.

Considérations sur les noms d'appareil

Gardez les points suivants à l'esprit lorsque vous sélectionnez un nom d'appareil :

- La fin des noms d'appareils que vous utilisez ne doit pas se chevaucher, car cela peut entraîner des problèmes au démarrage de votre instance. Par exemple, évitez d'utiliser des combinaisons telles que `/dev/xvdf` et `xvdf` pour les volumes attachés à la même instance.
- Bien que vous puissiez attacher vos EBS volumes en utilisant les noms de périphériques utilisés pour attacher les volumes de stockage d'instance, nous vous recommandons vivement de ne pas le faire car le comportement peut être imprévisible.
- Le nombre de NVMe volumes de stockage d'instance pour une instance dépend de sa taille. NVMeles volumes de stockage d'instance sont automatiquement énumérés et on leur attribue un nom de NVMe périphérique (instances Linux) ou une lettre de lecteur Windows (instances Windows).

- (Instances Windows) AWS Windows AMIs est fourni avec un logiciel supplémentaire qui prépare une instance lors de son premier démarrage. Il s'agit du EC2Config service (Windows AMIs antérieur à Windows Server 2016) ou EC2Launch (Windows Server 2016 et versions ultérieures). Une fois que les appareils ont été mappés aux lecteurs, ils sont initialisés et montés. Le lecteur racine est initialisé et monté en tant que `C:\`. Par défaut, lorsqu'un EBS volume est attaché à une instance Windows, il peut s'afficher sous la forme de n'importe quelle lettre de lecteur sur l'instance. Vous pouvez modifier les paramètres afin de définir les lettres de lecteur des volumes EBS selon vos spécifications. Par exemple, les volumes de stockage, la valeur par défaut dépend du pilote. AWS Les pilotes PV et Citrix PV attribuent aux volumes de stockage des instances des lettres de lecteur allant de Z : à A :. Les pilotes Red Hat attribuent les lettres de lecteurs de volumes de stockage d'instances allant de D: à A:. Pour plus d'informations, consultez Agents de lancement Windows sur les instances Amazon EC2 Windows et Comment les volumes sont attachés et mappés pour les instances Amazon EC2 Windows.
- (Instances Linux) Selon le pilote de périphérique en mode bloc du noyau, le périphérique peut être attaché sous un nom différent de celui que vous avez spécifié. Par exemple, si vous spécifiez un nom de périphérique de `/dev/sdh`, votre appareil peut être renommé `/dev/xvdh` ou `/dev/hdh`. Dans la plupart des cas, la lettre finale reste la même. Dans certaines versions de Red Hat Enterprise Linux (et ses variantes, telles que CentOS), la lettre finale peut changer (`/dev/sda` peut devenir `/dev/xvde`). Dans ces cas, la lettre finale de chaque nom de périphérique est incrémentée le même nombre de fois. Par exemple, si `/dev/sdb` est renommé `/dev/xvdf`, alors `/dev/sdc` est renommé `/dev/xvdg`. Amazon Linux crée un lien symbolique pour le nom que vous avez spécifié pour le périphérique renommé. D'autres systèmes d'exploitation peuvent avoir un comportement différent.
- (instances Linux) HVM AMIs ne prennent pas en charge l'utilisation de chiffres de fin sur les noms de périphériques, à l'exception de`/dev/sda1`, qui est réservé au périphérique racine, et`/dev/sda2`. Bien que l'utilisation `/dev/sda2` soit possible, nous vous déconseillons d'utiliser ce mappage de périphériques avec des HVM instances.
- (Instances Linux) Lorsque vous utilisez PVAMIs, vous ne pouvez pas joindre des volumes qui partagent les mêmes lettres de périphérique, avec ou sans chiffres de fin. Par exemple, si vous attachez un premier volume en tant que `/dev/sdc` et un autre volume en tant que `/dev/sdc1`, seul `/dev/sdc` sera visible pour l'instance. Pour utiliser des chiffres à la fin des noms de périphériques, vous devez y avoir recours pour tous les noms de périphériques qui partagent les mêmes lettres de base (par exemple `/dev/sdc1`, `/dev/sdc2`, `/dev/sdc3`).
- (Instances Linux) Certains noyaux personnalisés peuvent comporter des restrictions qui limitent leur utilisation à `/dev/sd[f-p]` ou`/dev/sd[f-p][1-6]`. Si vous rencontrez des difficultés en

utilisant `/dev/sd[q-z]` ou `/dev/sd[q-z][1-6]`, essayez avec `/dev/sd[f-p]` ou `/dev/sd[f-p][1-6]`.

Avant de spécifier le nom de l'appareil que vous avez sélectionné, vérifiez qu'il est disponible. Sinon, vous recevrez un message d'erreur indiquant que le nom de l'appareil est déjà utilisé. Pour afficher les unités de disque et leurs points de montage, utilisez la lsblk commande (instances Linux), l'utilitaire de gestion des disques ou la diskpart commande (instances Windows).

Bloquer les mappages d'appareils pour les volumes sur les instances Amazon EC2

Chaque instance que vous lancez est associée à un volume de périphérique racine, qui est soit un EBS volume Amazon, soit un volume de stockage d'instance. Vous pouvez utiliser le mappage des périphériques en mode bloc pour spécifier des EBS volumes supplémentaires ou des volumes de stockage d'instance à associer à une instance lors de son lancement. Vous pouvez également associer des EBS volumes supplémentaires à une instance en cours d'exécution. Cependant, le seul moyen d'attacher des volumes de stockage d'instance à une instance est d'utiliser le mappage de périphérique de stockage en mode bloc pour les attacher lors du lancement de l'instance.

Table des matières

Concepts de mappage de périphérique de stockage en mode bloc

Un périphérique de stockage en mode bloc est un dispositif de stockage qui déplace des données en séquence d'octets ou bits (blocs). Ces périphériques prennent en charge l'accès aléatoire et utilisent généralement des E/S mises en mémoire tampon. Les exemples incluent les disques durs, les ROM lecteurs de CD et les lecteurs flash. Un périphérique de stockage en mode bloc peut être physiquement attaché à un ordinateur ou accessible à distance comme s'il était physiquement attaché à l'ordinateur.

Amazon EC2 prend en charge deux types de dispositifs de blocage :

- Les volumes de stockage d'instance (périphériques virtuels dont le matériel sous-jacent est physiquement attaché à l'ordinateur hôte de l'instance)
- EBSvolumes (périphériques de stockage distants)

Un mappage de périphériques en mode bloc définit les périphériques en mode bloc (volumes de stockage d'instance et EBS volumes) à associer à une instance. Vous pouvez spécifier un mappage de périphériques en mode bloc dans le cadre de la création d'un AMI afin que le mappage soit utilisé par toutes les instances lancées depuis leAMI. Vous pouvez également spécifier un mappage de périphériques en mode bloc lorsque vous lancez une instance, afin que ce mappage remplace celui spécifié dans le mappage à AMI partir duquel vous avez lancé l'instance. Notez que tous les volumes de stockage d'NVMeinstance pris en charge par un type d'instance sont automatiquement énumérés et qu'un nom de périphérique leur est attribué lors du lancement de l'instance ; leur inclusion dans le mappage de périphériques par blocs n'a aucun effet.

Table des matières

Entrées du mappage de périphérique de stockage en mode bloc

Lorsque vous créez un mappage de périphérique de stockage en mode bloc, vous spécifiez les informations suivantes pour chaque périphérique de stockage en mode bloc qui doit être attaché à l'instance :

- Le nom de l'appareil utilisé dans AmazonEC2. Le pilote du périphérique de stockage en mode bloc de l'instance attribue le nom de volume réel lors du montage du volume. Le nom attribué peut être différent du nom EC2 recommandé par Amazon. Pour de plus amples informations, veuillez consulter Noms des appareils pour les volumes sur les EC2 instances Amazon.

Pour les volumes de stockage d'instance, vous spécifiez également les informations suivantes :

- Le nom du périphérique virtuel : `ephemeral[0-23]`. Notez que le nombre et la taille des volumes de stockage d'instance disponibles pour votre instance varient en fonction du type d'instance.

Par NVMe exemple, les informations suivantes s'appliquent également aux volumes de stockage :

- Ces volumes sont automatiquement énumérés et un nom de périphérique leur est automatiquement attribué. Le fait de les ajouter dans votre mappage de périphérique de stockage en mode bloc n'a aucun effet.

Pour les EBS volumes, vous devez également spécifier les informations suivantes :

- L'ID de l'instantané à utiliser pour créer le périphérique de stockage en mode bloc (snap-xxxxxxxx). Cette valeur est facultative si vous spécifiez une taille de volume. Vous ne pouvez pas spécifier l'ID d'instantané archivé.
- Taille du volume en Gio La taille spécifiée doit être supérieure ou égale à la taille de l'instantané spécifié.
- Suppression ou non du volume lors de l'arrêt de l'instance (`true` ou `false`). La valeur par défaut est `true` pour le volume du périphérique racine et `false` pour les volumes attachés. Lorsque vous créez unAMI, son mappage de périphériques par blocs hérite de ce paramètre de l'instance. Lorsque vous lancez une instance, elle hérite de ce paramètre duAMI.
- Le type de volume, qui peut être `gp2` `gp3` destiné à un usage SSD général IOPSSSD, provisionné, optimisé `st1` pour le débit HDDHDD, `sc1` froid ou magnétique`standard`. `io1` `io2`
- Nombre d'opérations d'entrée/sortie par seconde (IOPS) prises en charge par le volume. (Utilisé uniquement avec les volumes `io1` et `io2`.)

Mises en garde sur le stockage d'instance du mappage de périphérique de stockage en mode bloc

Plusieurs mises en garde doivent être prises en compte lors du lancement d'instances AMIs dont les mappages de périphériques en mode bloc contiennent des volumes de stockage d'instance.

- Certains types d'instance comprennent un plus grand nombre de volumes de stockage d'instance que d'autres et certains types d'instance ne contiennent aucun volume de stockage d'instance. Si votre type d'instance prend en charge un volume de stockage d'instance et que vous AMI disposez de mappages pour deux volumes de stockage d'instance, l'instance est lancée avec un volume de stockage d'instance.
- Les volumes de stockage d'instance peuvent uniquement être mappés au moment du lancement. Vous ne pouvez pas arrêter une instance sans volume de stockage d'instance (comme `t2.micro`), modifier le type de l'instance par un type prenant en charge les volumes de stockage

d'instance, puis redémarrer l'instance avec des volumes de stockage d'instance. Toutefois, vous pouvez créer une instance AMI à partir de l'instance et la lancer sur un type d'instance qui prend en charge les volumes de stockage d'instance, puis mapper ces volumes de stockage d'instance à l'instance.

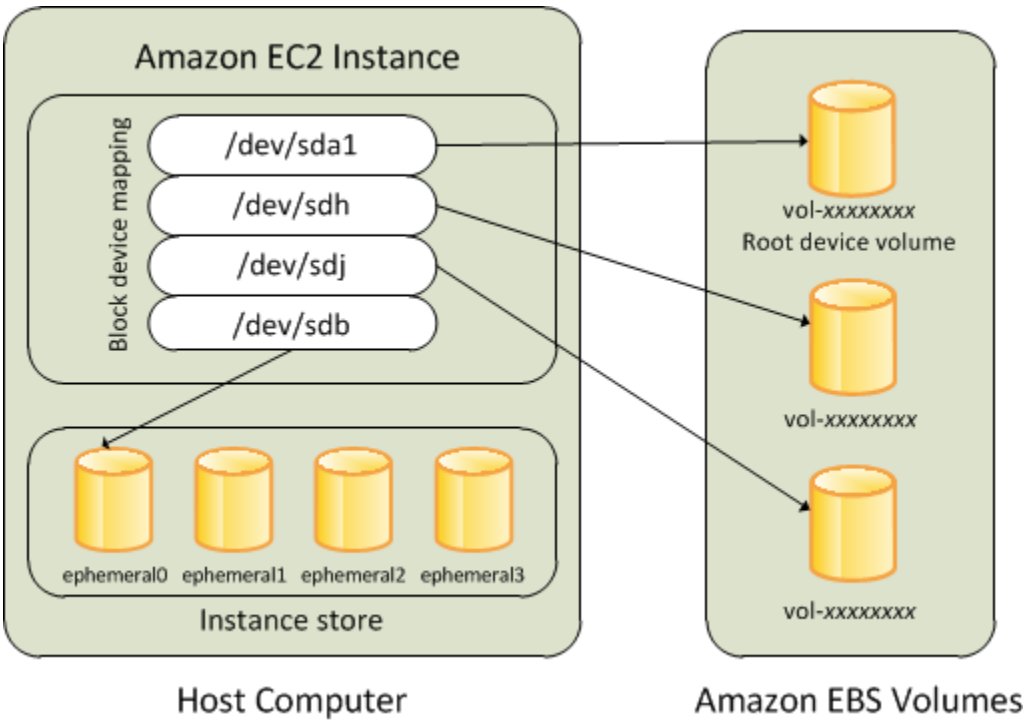
- Si vous lancez une instance à laquelle sont mappés des volumes de stockage d'instance, puis arrêtez l'instance, en modifiez le type avec un nombre inférieur de volumes de stockage d'instance et redémarrez l'instance, les mappages des volumes de stockage d'instance du lancement initial apparaissent toujours dans les métadonnées de l'instance. Cependant, l'instance n'a accès qu'au nombre maximum de volumes de stockage d'instance pris en charge pour ce type d'instance.

  > **Note**
  >
  > Lorsqu'une instance est arrêtée, toutes les données stockées sur les volumes de stockage d'instance sont perdues.

- En fonction de la capacité de stockage de l'instance au moment du lancement, les instances M3 peuvent ignorer les mappages de périphériques par blocs de stockage d'AMIinstance au lancement, sauf s'ils sont spécifiés lors du lancement. Vous devez spécifier les mappages de périphériques de stockage d'instance au moment du lancement, même si les volumes de stockage d'instance que AMI vous lancez sont mappés dans leAMI, afin de garantir que les volumes de stockage d'instance sont disponibles au lancement de l'instance.

Exemple de mappage de périphérique de stockage en mode bloc

Cette figure montre un exemple de mappage de périphériques en mode bloc pour une instance EBS basée sur un support. Il cartographie `/dev/sdb` `ephemeral0` et mappe deux EBS volumes, l'un vers `/dev/sdh` et l'autre vers`/dev/sdj`. Il indique également le EBS volume qui est le volume du périphérique racine,`/dev/sda1`.



Notez que cet exemple de mappage de périphériques par blocs est utilisé dans les exemples de commandes et APIs dans cette rubrique. Vous pouvez trouver des exemples de commandes APIs qui créent des mappages de périphériques par blocs dans Spécifiez un mappage de périphériques en mode bloc pour un AMI etMettre à jour le mappage de périphérique de stockage en mode bloc lors du lancement d'une instance.

Mise à disposition d'appareils dans le système d'exploitation

Des noms d'appareils similaires à `/dev/sdh` et `xvdh` sont utilisés par Amazon EC2 pour décrire les appareils en mode bloc. Le mappage des périphériques en mode bloc est utilisé par Amazon EC2 pour spécifier les périphériques en mode bloc à associer à une EC2 instance. Lorsqu'un périphérique de stockage en mode bloc est attaché à une instance, il doit être monté par le système d'exploitation pour que vous puissiez accéder au dispositif de stockage. Lorsqu'un périphérique de stockage en mode bloc est détaché d'une instance, il doit être démonté par le système d'exploitation. Ainsi, vous ne pouvez plus accéder au dispositif de stockage.

Instances Linux : les noms des périphériques spécifiés dans le mappage des périphériques par blocs sont mappés aux périphériques par blocs correspondants lors du premier démarrage de l'instance. Le type d'instance détermine les volumes de stockage d'instance qui sont formatés et montés par défaut. Vous pouvez monter des volumes de stockage d'instance supplémentaires au moment du lancement, à condition de ne pas dépasser le nombre de volumes de stockage d'instance disponibles pour votre type d'instance. Pour plus d'informations, consultez Stockage d'instances Stockage par

blocs temporaire pour les EC2 instances. Le pilote du périphérique de stockage en mode bloc pour l'instance détermine les périphériques utilisés lorsque les volumes sont formatés et montés.

Instances Windows : les noms des périphériques spécifiés dans le mappage des périphériques par blocs sont mappés aux périphériques par blocs correspondants lorsque l'instance démarre pour la première fois, puis le service Ec2Config initialise et monte les lecteurs. Le volume du périphérique racine est monté en tant que `C:\`. Les volumes de stockage d'instance sont montés en tant que `Z:\`, `Y:\`, etc. Lorsqu'un EBS volume est monté, il peut être monté à l'aide de n'importe quelle lettre de lecteur disponible. Vous pouvez toutefois configurer la manière dont les lettres de lecteur sont attribuées aux EBS volumes ; pour plus d'informations, consultezthe section called "Agents de lancement Windows".

Ajoutez des mappages de périphériques en mode bloc à un AMI

Chacun AMI possède un mappage de périphériques en mode bloc qui spécifie les périphériques en mode bloc à associer à une instance lorsqu'elle est lancée depuis leAMI. Pour ajouter d'autres appareils de blocage à unAMI, vous devez créer les vôtresAMI.

Table des matières

Spécifiez un mappage de périphériques en mode bloc pour un AMI

Il existe deux manières de spécifier des volumes en plus du volume racine lorsque vous créez unAMI. Si vous avez déjà attaché des volumes à une instance en cours d'exécution avant de créer un volume AMI à partir de l'instance, le mappage des périphériques par blocs AMI inclut ces mêmes volumes. Pour les EBS volumes, les données existantes sont enregistrées dans un nouvel instantané, et c'est ce nouvel instantané qui est spécifié dans le mappage des périphériques en mode bloc. Pour les volumes de stockage d'instance, les données ne sont pas conservées.

Dans le cas d'un EBS -backedAMI, vous pouvez ajouter des EBS volumes et des volumes de stockage d'instance à l'aide d'un mappage de périphériques en mode bloc. Pour une instance sauvegardée par le stockageAMI, vous pouvez ajouter des volumes de stockage d'instance uniquement en modifiant les entrées de mappage des périphériques par blocs dans le fichier manifeste de l'image lors de l'enregistrement de l'image.

> **Note**
>
> Pour les instances M3, vous devez spécifier les volumes de stockage d'instance dans le mappage de périphérique de stockage en mode bloc de l'instance lorsque cette dernière est lancée. Lorsque vous lancez une instance M3, les volumes de stockage d'instance spécifiés dans le mappage de périphériques par blocs pour le AMI peuvent être ignorés s'ils ne sont pas spécifiés dans le cadre du mappage de périphériques par blocs d'instance.

Console

Pour ajouter des volumes à une AMI utilisation de la console

1. Ouvrez la EC2 console Amazon.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez une instance, puis Actions, Image and templates (Image et modèles), Create image (Créer une image).
4. Saisissez un nom et une description pour l'image.
5. Les volumes d'instance apparaissent sous Instance volumes (Volumes d'instance). Pour ajouter un autre volume, sélectionnez Add volume (Ajouter un volume).
6. Pour Volume type (Type de volume), sélectionnez le type de volume. Pour Device (Périphérique), sélectionnez le nom du périphérique. Pour un EBS volume, vous pouvez spécifier des détails supplémentaires, tels qu'un instantané, la taille du volume, le type de volume et l'état de chiffrement. IOPS
7. Choisissez Create image (Créer une image).

Command line

Pour ajouter des volumes à un à AMI l'aide de la ligne de commande

Utilisez la AWS CLI commande create-image pour spécifier un mappage de périphériques en mode bloc pour un EBS -backed. AMI Utilisez la AWS CLI commande register-image pour spécifier un mappage de périphériques en mode bloc pour une instance sauvegardée en magasin. AMI

Spécifiez le mappage de périphérique de stockage en mode bloc à l'aide du paramètre `--block-device-mappings`. Les arguments encodés JSON peuvent être fournis soit directement sur la ligne de commande, soit par référence à un fichier :

```
--block-device-mappings [mapping, ...]
--block-device-mappings [file://mapping.json]
```

Pour ajouter un volume de stockage d'instance, utilisez le mappage suivant :

```
{
    "DeviceName": "device_name",
    "VirtualName": "ephemeral0"
}
```

Pour ajouter un volume gp2 vide de 100 Gio, utilisez le mappage suivant :

```
{
    "DeviceName": "device_name",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

Pour ajouter un EBS volume basé sur un instantané, utilisez le mappage suivant.

```
{
    "DeviceName": "device_name",
    "Ebs": {
      "SnapshotId": "snap-xxxxxxxx"
    }
}
```

Pour omettre un mappage pour un périphérique, utilisez le mappage suivant :

```
{
    "DeviceName": "device_name",
    "NoDevice": ""
}
```

Vous pouvez aussi utiliser le paramètre `-BlockDeviceMapping` avec les commandes suivantes (AWS Tools for Windows PowerShell) :

- New-EC2Image
- Register-EC2Image

Afficher les EBS volumes dans un mappage de périphériques en mode AMI bloc

Vous pouvez facilement énumérer les EBS volumes dans le mappage des périphériques en mode bloc pour unAMI.

Console

Pour afficher les EBS volumes et AMI utiliser la console

1. Ouvrez la EC2 console Amazon.
2. Dans le volet de navigation, choisissez AMIs.
3. Choisissez EBSdes images dans la liste des filtres pour obtenir la liste des images EBS sauvegardées par -backedAMIs.
4. Sélectionnez la valeur souhaitéeAMI, puis consultez l'onglet Détails. Au minimum, les informations suivantes sont disponibles pour le périphérique racine :

   - Type de périphérique racine (`ebs`)
   - Nom du périphérique racine (par exemple, `/dev/sda1`)
   - Block Devices (par exemple, `/dev/sda1=snap-1234567890abcdef0:8:true`)

   Si le AMI a été créé avec des EBS volumes supplémentaires à l'aide d'un mappage de périphériques par blocs, le champ Block Devices affiche également le mappage pour ces volumes supplémentaires. Notez que cet écran n'affiche pas les volumes de stockage d'instance.

Command line

Pour afficher les EBS volumes à l'AMIaide de la ligne de commande

Utilisez la commande describe-images (AWS CLI) ou la commande Get-EC2Image(AWS Tools for Windows PowerShell) pour énumérer les EBS volumes dans le mappage de périphériques en mode bloc pour un. AMI

Ajouter des mappages de périphériques en mode bloc à une instance Amazon EC2

Par défaut, une instance que vous lancez inclut tous les périphériques de stockage spécifiés dans le mappage des périphériques par blocs de l'instance AMI à partir de laquelle vous avez lancé l'instance. Vous pouvez modifier le mappage des périphériques en mode bloc pour une instance lorsque vous la lancez, et ces mises à jour remplacent ou fusionnent avec le mappage des périphériques en mode bloc duAMI.

Limites

- Pour le volume racine, vous pouvez uniquement modifier les données informations suivantes : taille du volume, type de volume et indicateur Delete on Termination.
- Lorsque vous modifiez un EBS volume, vous ne pouvez pas réduire sa taille. Par conséquent, vous devez spécifier un instantané dont la taille est égale ou supérieure à la taille du cliché spécifié dans le mappage des périphériques en mode bloc duAMI.

Table des matières

Mettre à jour le mappage de périphérique de stockage en mode bloc lors du lancement d'une instance

Vous pouvez ajouter des EBS volumes et des volumes de stockage d'instance à une instance lorsque vous la lancez. Notez que la mise à jour du mappage des périphériques en mode bloc pour une instance n'entraîne pas de modification permanente du mappage des périphériques en mode bloc de l'instance AMI à partir de laquelle elle a été lancée.

Console

Pour ajouter des volumes à une instance à l'aide de la console

1. Ouvrez la EC2 console Amazon.
2. Sur le tableau de bord, choisissez Lancer une instance.
3. Sur la page Choose an Amazon Machine Image (AMI), sélectionnez l'image AMI à utiliser, puis sélectionnez Select.
4. Suivez l'Assistant pour compléter les pages Choisir un type d'instance et Configurer les détails de l'instance.
5. Sur la page Ajouter du stockage, vous pouvez modifier le volume racine, les EBS volumes et les volumes de stockage d'instance comme suit :
   - Pour modifier la taille du volume racine, recherchez le volume Root dans la colonne Type, et modifiez le champ Size.
   - Pour supprimer un EBS volume spécifié par le mappage de périphériques par blocs du périphérique AMI utilisé pour lancer l'instance, localisez le volume et cliquez sur son icône Supprimer.
   - Pour ajouter un EBS volume, choisissez Ajouter un nouveau volume, EBSsélectionnez-le dans la liste Type et renseignez les champs (Appareil, Instantané, etc.).
   - Pour supprimer un volume de stockage d'instance spécifié par le mappage de périphériques par blocs du volume AMI utilisé pour lancer l'instance, localisez le volume et cliquez sur son icône Supprimer.
   - Pour ajouter un volume de stockage d'instance, choisissez Add New Volume, sélectionnez Instance Store dans la liste Type, puis choisissez un nom de périphérique dans la liste Device.
6. Complétez les pages restantes de l'Assistant, puis sélectionnez Launch.

Command line

Pour ajouter des volumes à une instance à l'aide du AWS CLI

Utilisez la AWS CLI commande run-instances avec l'`--block-device-mappings`option permettant de spécifier un mappage de périphériques en mode bloc pour une instance au lancement.

Supposons, par exemple, qu'un EBS -backed AMI spécifie le mappage de périphériques par blocs suivant pour une instance Linux :

- `/dev/sdb` = `ephemeral0`
- `/dev/sdh` = `snap-1234567890abcdef0`
- `/dev/sdj` = `100`

Pour éviter `/dev/sdj` de vous attacher à une instance lancée à partir de làAMI, utilisez le mappage suivant.

```
{
    "DeviceName": "/dev/sdj",
    "NoDevice": ""
}
```

Pour augmenter la taille de `/dev/sdh` à`300 GiB`, spécifiez le mappage suivant. Notez que vous ne devez pas spécifier l'ID d'instantané pour `/dev/sdh`, car le fait de spécifier le nom du périphérique suffit à identifier le volume.

```
{
    "DeviceName": "/dev/sdh",
    "Ebs": {
      "VolumeSize": 300
    }
}
```

Pour augmenter la taille du volume racine au lancement de l'instance, appelez d'abord describe-images avec l'ID du AMI afin de vérifier le nom du périphérique du volume racine. Par exemple, `"RootDeviceName": "/dev/xvda"`. Pour modifier la taille du volume racine, spécifiez le nom du périphérique racine utilisé par le volume AMI ainsi que la nouvelle taille du volume.

```
{
    "DeviceName": "/dev/xvda",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

Pour attacher un volume de stockage d'instance supplémentaire, `/dev/sdc`, spécifiez le mappage suivant. Si le type d'instance ne prend pas en charge plusieurs volumes de stockage d'instance, ce mappage n'a aucun effet. Si l'NVMeinstance prend en charge les volumes de stockage d'instance, ils sont automatiquement énumérés et un nom de NVMe périphérique leur est attribué.

```
{
    "DeviceName": "/dev/sdc",
    "VirtualName": "ephemeral1"
}
```

Pour ajouter des volumes à une instance à l'aide du AWS Tools for Windows PowerShell

Utilisez le `-BlockDeviceMapping` paramètre avec la New-EC2Instancecommande (AWS Tools for Windows PowerShell).

Mettre à jour le mappage de périphérique de stockage en mode bloc d'une instance en cours d'exécution

Vous pouvez utiliser la modify-instance-attribute AWS CLI commande pour mettre à jour le mappage des périphériques en mode bloc d'une instance en cours d'exécution. Vous n'avez pas besoin d'arrêter l'instance avant de modifier cet attribut.

```
aws ec2 modify-instance-attribute --instance-id i-1a2b3c4d --block-device-mappings
 file://mapping.json
```

Par exemple, pour conserver le volume racine à la clôture de l'instance, spécifiez les informations suivantes dans le fichier `mapping.json`.

```
[
  {
    "DeviceName": "/dev/sda1",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

Vous pouvez également utiliser le `-BlockDeviceMapping` paramètre avec la Edit-EC2InstanceAttributecommande (AWS Tools for Windows PowerShell).

Afficher les EBS volumes dans un mappage de périphériques par blocs d'instance

Vous pouvez facilement énumérer les EBS volumes mappés à une instance.

> **Note**
>
> Pour les instances lancées avant la sortie du 31/10/2009API, impossible d'afficher le AWS mappage des périphériques en mode bloc. Vous devez détacher et rattacher les volumes afin de AWS pouvoir afficher le mappage des périphériques en mode bloc.

Console

Pour afficher les EBS volumes d'une instance à l'aide de la console

1. Ouvrez la EC2 console Amazon.
2. Dans le panneau de navigation, choisissez Instances.
3. Dans la zone de recherche, entrez le type de périphérique racine, puis choisissez EBS. Cela affiche une liste des instances EBS sauvegardées.
4. Sélectionnez l'instance souhaitée, puis consultez les informations affichées dans l'onglet Storage (Stockage). Au minimum, les informations suivantes sont disponibles pour le périphérique racine :
   - Type de périphérique racine (par exemple, EBS)
   - Root device name (Nom du périphérique racine) (par exemple, `/dev/xvda`)
   - Block devices (Périphériques de stockage en mode bloc) (par exemple, `/dev/xvda`, `/dev/sdf` et `/dev/sdj`)

   Si l'instance a été lancée avec des EBS volumes supplémentaires à l'aide d'un mappage de périphériques en mode bloc, ils apparaissent sous Bloquer les appareils. Aucun volume de stockage d'instance n'apparaît sur cet onglet.
5. Pour afficher des informations supplémentaires sur un EBS volume, choisissez son ID de volume pour accéder à la page du volume.

Command line

Pour afficher les EBS volumes d'une instance à l'aide de la ligne de commande

Utilisez la commande describe-instances (AWS CLI) ou la commande Get-EC2Instance(AWS Tools for Windows PowerShell) pour énumérer les EBS volumes dans le mappage de périphériques en mode bloc pour une instance.

Afficher le mappage de périphérique de stockage en mode bloc d'une instance pour les volumes de stockage d'instances

Le type d'instance détermine le nombre et le type de volumes de stockage d'instance disponibles pour l'instance. Si le nombre de volumes de stockage d'instances dans un mappage d'appareils en bloc dépasse le nombre de volumes de stockage d'instances disponibles pour une instance, les volumes supplémentaires sont ignorés. Pour afficher les volumes de stockage de votre instance, exécutez la lsblk commande (instances Linux) ou ouvrez Windows Disk Management (instances Windows). Pour savoir combien de volumes de stockage d'instance sont pris en charge par chaque type d'instance, consultez les spécifications des types d'EC2instance Amazon.

Lorsque vous consultez le mappage des périphériques en mode bloc pour votre instance, vous ne pouvez voir que les EBS volumes, pas les volumes de stockage de l'instance. La méthode que vous utilisez pour afficher les volumes de stockage d'instance disponibles pour votre instance dépend du type de volume.

NVMevolumes de stockage d'instances

Instances Linux

Vous pouvez utiliser le package de ligne de NVMe commande, nvme-cli, pour interroger les volumes de stockage d'NVMeinstance dans le mappage des périphériques en mode bloc. Téléchargez et installez le package sur votre instance, puis exécutez la commande suivante.

```
[ec2-user ~]$ sudo nvme list
```

L'exemple ci-dessous présente la sortie pour une instance. Le texte de la colonne Modèle indique si le volume est un EBS volume ou un volume de stockage d'instance. Dans cet exemple, `/dev/nvme1n1` et `/dev/nvme2n1` sont des volumes de stockage d'instance.

```
Node             SN                   Model
 Namespace
---------------- -------------------- ----------------------------------------
 ---------
/dev/nvme0n1     vol06afc3f8715b7a597 Amazon Elastic Block Store              1

/dev/nvme1n1     AWS2C1436F5159EB6614 Amazon EC2 NVMe Instance Storage        1

/dev/nvme2n1     AWSB1F4FF0C0A6C281EA Amazon EC2 NVMe Instance Storage        1
  ...
```

instances Windows

Vous pouvez utiliser la gestion des disques ou PowerShell répertorier les deux EBS et les NVMe volumes de stockage d'instance. Pour de plus amples informations, veuillez consulter the section called “Mappez NVME des disques à des volumes”.

HDDou volumes de stockage d'SSDinstance

Vous pouvez utiliser les métadonnées d'instance pour interroger les volumes de stockage d'SSDinstance HDD ou d'instance dans le mappage des périphériques en mode bloc. NVMeles volumes de stockage d'instance ne sont pas inclus.

La base URI de toutes les demandes de métadonnées d'instance est`http://169.254.169.254/latest/`. Pour de plus amples informations, veuillez consulter Utiliser les métadonnées de l'instance pour gérer votre EC2 instance.

Instances Linux

Commencez par vous connecter à votre instance en cours d'exécution. Utilisez cette requête à partir de l'instance pour obtenir son mappage de périphérique de stockage en mode bloc.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/block-device-mapping/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/
```

La réponse inclut les noms des périphériques de stockage en mode bloc de l'instance. Par exemple, la sortie pour une instance `m1.small` basée sur un stockage d'instances ressemble à cela :

```
ami
ephemeral0
root
swap
```

Le périphérique `ami` est le périphérique racine tel que le voit l'instance. Les volumes de stockage d'instance sont nommés `ephemeral[0-23]`. Le périphérique `swap` est utilisé pour le fichier d'échange. Si vous avez également mappé EBS des volumes, ils apparaissent sous la forme `ebs1ebs2`,, etc.

Pour obtenir des détails relatifs à un périphérique de stockage en mode bloc individuel dans le mappage de périphérique de stockage en mode bloc, ajoutez son nom à la requête précédente, comme illustré ici.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

instances Windows

Commencez par vous connecter à votre instance en cours d'exécution. Utilisez cette requête à partir de l'instance pour obtenir son mappage de périphérique de stockage en mode bloc.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-mapping/
```

La réponse inclut les noms des périphériques de stockage en mode bloc de l'instance. Par exemple, la sortie pour une instance `m1.small` basée sur un stockage d'instances ressemble à cela :

```
ami
ephemeral0
root
swap
```

Le périphérique `ami` est le périphérique racine tel que le voit l'instance. Les volumes de stockage d'instance sont nommés `ephemeral[0-23]`. Le périphérique `swap` est utilisé pour le fichier d'échange. Si vous avez également mappé EBS des volumes, ils apparaissent sous la forme `ebs1ebs2`,, etc.

Pour obtenir des détails relatifs à un périphérique de stockage en mode bloc individuel dans le mappage de périphérique de stockage en mode bloc, ajoutez son nom à la requête précédente, comme illustré ici.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

Comment les volumes sont attachés et mappés pour les instances Amazon EC2 Windows

> **Note**
>
> Cette rubrique s'applique uniquement aux instances Windows.

Votre instance Windows est fournie avec un EBS volume qui fait office de volume racine. Si votre instance Windows utilise des pilotes AWS PV ou Citrix PV, vous pouvez éventuellement ajouter jusqu'à 25 volumes, soit un total de 26 volumes. Pour de plus amples informations, veuillez consulter Limites EBS de volume Amazon pour les EC2 instances Amazon.

En fonction du type de votre instance, vous disposerez de 0 à 24 volumes de stockage d'instance possibles disponibles pour l'instance. Pour utiliser l'un des volumes de stockage d'instance

disponibles pour votre instance, vous devez le spécifier lors de la création AMI ou du lancement de votre instance. Vous pouvez également ajouter des EBS volumes lorsque vous créez AMI ou lancez votre instance, ou les attacher pendant que votre instance est en cours d'exécution.

Lorsque vous ajoutez un volume à votre instance, vous spécifiez le nom de l'appareil EC2 utilisé par Amazon. Pour de plus amples informations, Noms des appareils pour les volumes sur les EC2 instances Amazonconsultez AWS . Windows Amazon Machine Images (AMIs) contient un ensemble de pilotes utilisés par Amazon pour EC2 mapper le stockage et les EBS volumes des instances à des disques Windows et à des lettres de lecteur.

Méthodes pour mapper des disques à des EBS volumes

- NVMeMappez les disques d'une instance Amazon EC2 Windows à des volumes
- Mappez des objets non NVMe disques sur une instance Amazon EC2 Windows à des volumes

NVMeMappez les disques d'une instance Amazon EC2 Windows à des volumes

Avec les instances créées sur le système AWS Nitro, les EBS volumes sont exposés en tant que NVMe périphériques. Cette rubrique explique comment afficher les NVMedisques disponibles pour le système d'exploitation Windows sur votre instance. Il explique également comment mapper ces NVMe disques aux EBS volumes Amazon sous-jacents et aux noms d'appareils spécifiés pour les mappages de périphériques en mode bloc utilisés par AmazonEC2.

Rubriques

- Lister NVMe les disques
- Mappez NVMe des disques à des volumes

Lister NVMe les disques

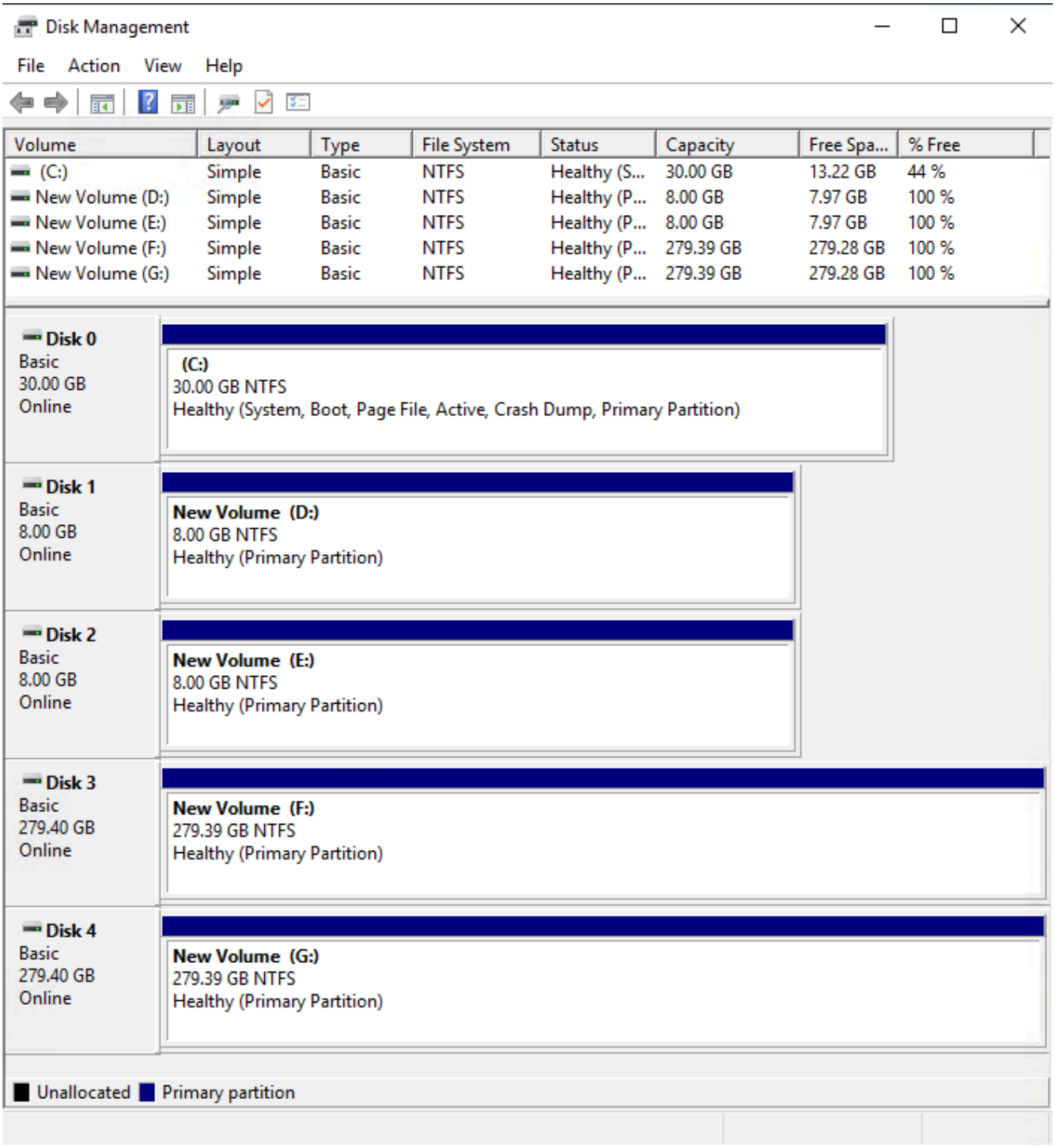
Vous pouvez utiliser la gestion de disques ou Powershell pour rechercher les disques sur votre instance Windows.

Disk Management

Pour rechercher les disques sur votre instance Windows

1. Connectez-vous à votre instance Windows en utilisant les services Bureau à distance. Pour plus d'informations, consultez Connectez-vous à votre instance Windows à l'aide de RDP.
2. Démarrez l'utilitaire Gestion des disques.
3. Examinez les disques. Le volume racine est un EBS volume monté en tant que`C:\`. Si aucun autre disque n'est affiché, cela signifie que vous n'avez pas spécifié de volumes supplémentaires lors de la création AMI ou du lancement de l'instance.

   L'exemple suivant montre les disques disponibles si vous lancez une `r5d.4xlarge` instance avec deux EBS volumes supplémentaires.



PowerShell

Le PowerShell script suivant répertorie chaque disque ainsi que le nom de périphérique et le volume correspondants. Il est destiné à être utilisé avec des instances basées sur le système AWS Nitro, qui utilisent NVMe EBS et stockent des volumes.

Connectez-vous à votre instance Windows et exécutez la commande suivante pour activer l'exécution du PowerShell script.

```
Set-ExecutionPolicy RemoteSigned
```

Copiez le script suivant et enregistrez-le en tant que `mapping.ps1` sur votre instance Windows.

```
# List the disks for NVMe volumes

function Get-EC2InstanceMetadata {
    param([string]$Path)
    (Invoke-WebRequest -Uri "http://169.254.169.254/latest/$Path").Content
}

function GetEBSVolumeId {
    param($Path)
    $SerialNumber = (Get-Disk -Path $Path).SerialNumber
    if($SerialNumber -clike 'vol*'){
        $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("vol","vol-")
    }
    else {
       $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("AWS","AWS-")
    }
    return $EbsVolumeId
}

function GetDeviceName{
    param($EbsVolumeId)
    if($EbsVolumeId -clike 'vol*'){

        $Device  = ((Get-EC2Volume -VolumeId $EbsVolumeId ).Attachment).Device
        $VolumeName = ""
    }
     else {
        $Device = "Ephemeral"
        $VolumeName = "Temporary Storage"
    }
    Return $Device,$VolumeName
}

function GetDriveLetter{
    param($Path)
    $DiskNumber =  (Get-Disk -Path $Path).Number
```

```
    if($DiskNumber -eq 0){
        $VirtualDevice = "root"
        $DriveLetter = "C"
        $PartitionNumber = (Get-Partition -DriveLetter C).PartitionNumber
    }
    else
    {
        $VirtualDevice = "N/A"
        $DriveLetter = (Get-Partition -DiskNumber $DiskNumber).DriveLetter
        if(!$DriveLetter)
        {
            $DriveLetter = ((Get-Partition -DiskId $Path).AccessPaths).Split(",")[0]
        }
        $PartitionNumber = (Get-Partition -DiskId $Path).PartitionNumber
    }

    return $DriveLetter,$VirtualDevice,$PartitionNumber

}

$Report = @()
foreach($Path in (Get-Disk).Path)
{
    $Disk_ID = ( Get-Partition -DiskId $Path).DiskId
    $Disk = ( Get-Disk -Path $Path).Number
    $EbsVolumeId  = GetEBSVolumeId($Path)
    $Size =(Get-Disk -Path $Path).Size
    $DriveLetter,$VirtualDevice, $Partition = (GetDriveLetter($Path))
    $Device,$VolumeName = GetDeviceName($EbsVolumeId)
    $Disk = New-Object PSObject -Property @{
      Disk          = $Disk
      Partitions    = $Partition
      DriveLetter   = $DriveLetter
      EbsVolumeId   = $EbsVolumeId
      Device        = $Device
      VirtualDevice = $VirtualDevice
      VolumeName= $VolumeName
    }
 $Report += $Disk
}

$Report | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions,
 DriveLetter, EbsVolumeId, Device, VirtualDevice, VolumeName
```

Exécutez le script comme suit :

```
PS C:\> .\mapping.ps1
```

Voici un exemple de sortie pour une instance avec un volume racine, deux EBS volumes et deux volumes de stockage d'instance.

```
Disk Partitions DriveLetter EbsVolumeId           Device    VirtualDevice VolumeName
---- ---------- ----------- -----------           ------    ------------- ----------
   0          1 C           vol-03683f1d861744bc7 /dev/sda1 root
   1          1 D           vol-082b07051043174b9 xvdb      N/A
   2          1 E           vol-0a4064b39e5f534a2 xvdc      N/A
   3          1 F           AWS-6AAD8C2AEEE1193F0 Ephemeral N/A           Temporary
 Storage
   4          1 G           AWS-13E7299C2BD031A28 Ephemeral N/A           Temporary
 Storage
```

Si vous n'avez pas configuré vos informations d'identification pour Tools for Windows PowerShell sur l'instance Windows, le script ne peut pas obtenir l'ID du EBS volume et utilise N/A dans la `EbsVolumeId` colonne.

Mappez NVMe des disques à des volumes

Vous pouvez utiliser la commande Get-Disk pour mapper les numéros de disque Windows au EBS volume. IDs

```
PS C:\> Get-Disk
Number Friendly Name Serial Number                    HealthStatus
 OperationalStatus      Total Size Partition

                      Style
------ ------------- -------------                    ------------
 -----------------      ---------- ----------
3      NVMe Amazo... AWS6AAD8C2AEEE1193F0_00000001.   Healthy              Online
              279.4 GB MBR
4      NVMe Amazo... AWS13E7299C2BD031A28_00000001.   Healthy              Online
              279.4 GB MBR
2      NVMe Amazo... vol0a4064b39e5f534a2_00000001.   Healthy              Online
                8 GB MBR
0      NVMe Amazo... vol03683f1d861744bc7_00000001.   Healthy              Online
                30 GB MBR
```

```
1      NVMe Amazo... vol082b07051043174b9_00000001.   Healthy              Online
                8 GB MBR
```

Vous pouvez également exécuter la ebsnvme-id commande pour mapper les numéros de NVMe disque aux noms de EBS volumes IDs et de périphériques.

```
PS C:\> C:\PROGRAMDATA\Amazon\Tools\ebsnvme-id.exe
Disk Number: 0
Volume ID: vol-03683f1d861744bc7
Device Name: sda1

Disk Number: 1
Volume ID: vol-082b07051043174b9
Device Name: xvdb

Disk Number: 2
Volume ID: vol-0a4064b39e5f534a2
Device Name: xvdc
```

Mappez des objets non NVMe disques sur une instance Amazon EC2 Windows à des volumes

Pour les instances lancées depuis un Windows AMI qui utilise des pilotes AWS PV ou Citrix PV, vous pouvez utiliser les relations décrites sur cette page pour mapper vos disques Windows à votre magasin d'instances et à vos EBS volumes. Cette rubrique explique comment afficher les NVMenon-disques disponibles pour le système d'exploitation Windows sur votre instance. Il explique également comment mapper ces objets non liés aux NVMe disques aux EBS volumes Amazon sous-jacents et aux noms d'appareils spécifiés pour les mappages de périphériques en mode bloc utilisés par AmazonEC2.

> **Note**
>
> Si vous lancez une instance Si votre Windows AMI utilise des pilotes PV Red Hat, vous pouvez mettre à jour votre instance pour utiliser les pilotes Citrix. Pour de plus amples informations, veuillez consulter the section called “Mettre à niveau les pilotes PV”.

Rubriques

- Mappez des objets autres que NVMe des disques à des volumes

Répertorier les NVMe non-disques

Vous pouvez trouver les disques de votre instance Windows à l'aide de la gestion des disques ou PowerShell.

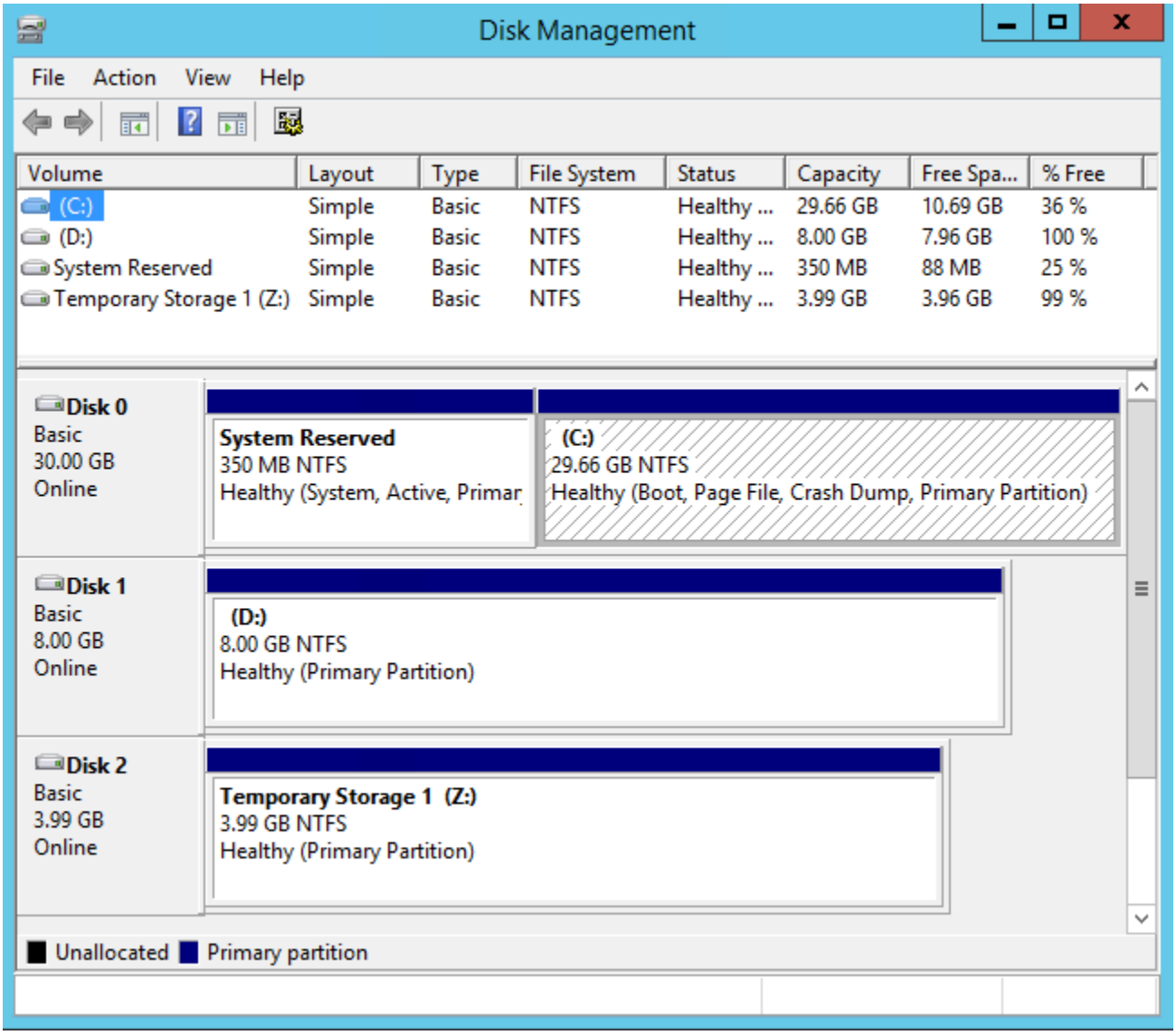
Disk Management

Pour rechercher les disques sur votre instance Windows

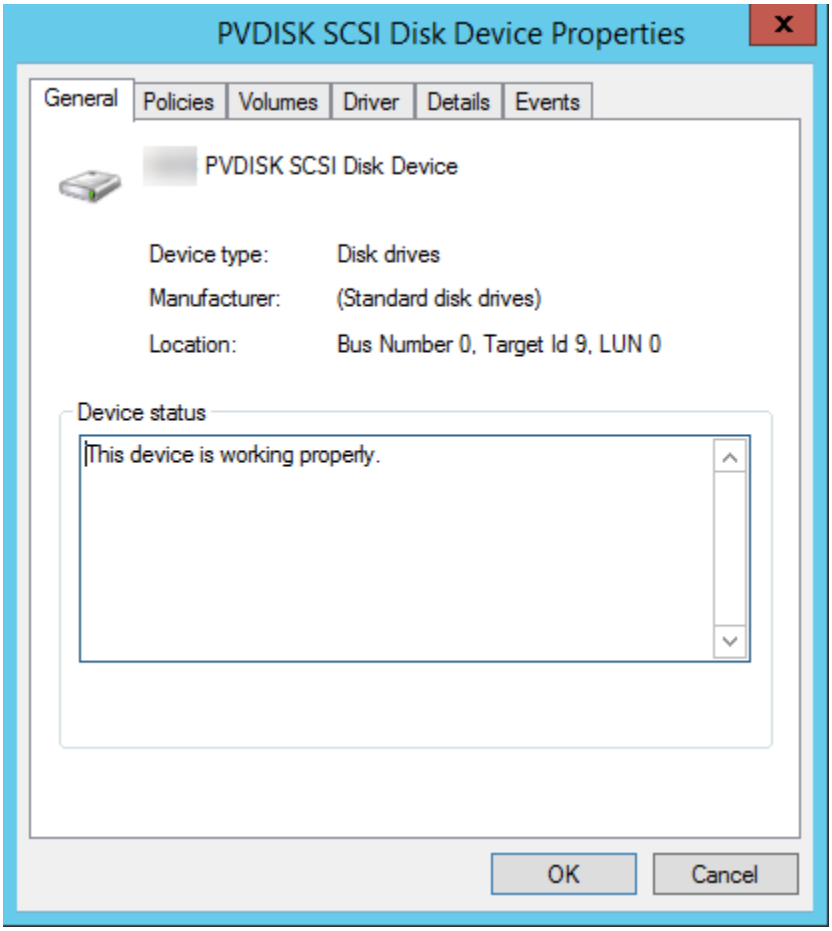
1. Connectez-vous à votre instance Windows en utilisant les services Bureau à distance. Pour plus d'informations, consultez Connectez-vous à votre instance Windows à l'aide de RDP.
2. Démarrez l'utilitaire Gestion des disques.

   Dans la barre des tâches, cliquez avec le bouton droit sur le logo Windows, puis sélectionnez Gestion des disques.
3. Examinez les disques. Le volume racine est un EBS volume monté en tant que`C:\`. Si aucun autre disque n'est affiché, cela signifie que vous n'avez pas spécifié de volumes supplémentaires lors de la création AMI ou du lancement de l'instance.

   L'exemple suivant montre les disques disponibles si vous lancez une `m3.medium` instance avec un volume de stockage d'instance (disque 2) et un EBS volume supplémentaire (disque 1).



4. Cliquez avec le bouton droit sur le disque 1 étiqueté dans le volet grisé, puis cliquez sur Propriétés. Prenez note de la valeur de l'Emplacement et recherchez-le dans les tables de Mappez des objets autres que NVMe des disques à des volumes. Par exemple, le disque suivant possède l'emplacement Bus numéro 0, ID cible 9, LUN 0. Selon le tableau des EBS volumes, le nom du périphérique pour cet emplacement est `xvdj`.



PowerShell

Le PowerShell script suivant répertorie chaque disque ainsi que le nom de périphérique et le volume correspondants.

Exigences et limitations

- Nécessite Windows Server 2012 ou une version ultérieure.
- Nécessite des informations d'identification pour obtenir l'ID EBS du volume. Vous pouvez configurer un profil à l'aide des outils pour PowerShell l'instance ou y associer un IAM rôle.
- Ne prend pas en charge NVMe les volumes.
- Ne prend pas en charge les disques dynamiques.

Connectez-vous à votre instance Windows et exécutez la commande suivante pour activer l'exécution du PowerShell script.

```
Set-ExecutionPolicy RemoteSigned
```

Copiez le script suivant et enregistrez-le en tant que `mapping.ps1` sur votre instance Windows.

```
# List the disks
function Convert-SCSITargetIdToDeviceName {
  param([int]$SCSITargetId)
  If ($SCSITargetId -eq 0) {
    return "sda1"
  }
  $deviceName = "xvd"
  If ($SCSITargetId -gt 25) {
    $deviceName += [char](0x60 + [int]($SCSITargetId / 26))
  }
  $deviceName += [char](0x61 + $SCSITargetId % 26)
  return $deviceName
}

[string[]]$array1 = @()
[string[]]$array2 = @()
[string[]]$array3 = @()
[string[]]$array4 = @()

Get-WmiObject Win32_Volume | Select-Object Name, DeviceID | ForEach-Object {
  $array1 += $_.Name
  $array2 += $_.DeviceID
}

$i = 0
While ($i -ne ($array2.Count)) {
  $array3 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-
Disk).SerialNumber) -replace "_[^ ]*$" -replace "vol", "vol-"
  $array4 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-
Disk).FriendlyName)
  $i ++
}

[array[]]$array = $array1, $array2, $array3, $array4

Try {
  $InstanceId = Get-EC2InstanceMetadata -Category "InstanceId"
  $Region = Get-EC2InstanceMetadata -Category "Region" | Select-Object -
ExpandProperty SystemName
```

```
}
Catch {
  Write-Host "Could not access the instance Metadata using AWS Get-
EC2InstanceMetadata CMDLet.
Verify you have AWSPowershell SDK version '3.1.73.0' or greater installed and
 Metadata is enabled for this instance." -ForegroundColor Yellow
}
Try {
  $BlockDeviceMappings = (Get-EC2Instance -Region $Region -Instance
 $InstanceId).Instances.BlockDeviceMappings
  $VirtualDeviceMap = (Get-EC2InstanceMetadata -Category
 "BlockDeviceMapping").GetEnumerator() | Where-Object { $_.Key -ne "ami" }
}
Catch {
  Write-Host "Could not access the AWS API, therefore, VolumeId is not available.
Verify that you provided your access keys or assigned an IAM role with adequate
 permissions." -ForegroundColor Yellow
}

Get-disk | ForEach-Object {
  $DriveLetter = $null
  $VolumeName = $null
  $VirtualDevice = $null
  $DeviceName = $_.FriendlyName

  $DiskDrive = $_
  $Disk = $_.Number
  $Partitions = $_.NumberOfPartitions
  $EbsVolumeID = $_.SerialNumber -replace "_[^ ]*$" -replace "vol", "vol-"
  if ($Partitions -ge 1) {
    $PartitionsData = Get-Partition -DiskId $_.Path
    $DriveLetter = $PartitionsData.DriveLetter | Where-object { $_ -notin @("",
 $null) }
    $VolumeName = (Get-PSDrive | Where-Object { $_.Name -in
 @($DriveLetter) }).Description | Where-object { $_ -notin @("", $null) }
  }
  If ($DiskDrive.path -like "*PROD_PVDISK*") {
    $BlockDeviceName = Convert-SCSITargetIdToDeviceName((Get-WmiObject -Class
 Win32_Diskdrive | Where-Object { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" +
 $DiskDrive.Number) }).SCSITargetId)
    $BlockDeviceName = "/dev/" + $BlockDeviceName
    $BlockDevice = $BlockDeviceMappings | Where-Object { $BlockDeviceName -like "*"
 + $_.DeviceName + "*" }
    $EbsVolumeID = $BlockDevice.Ebs.VolumeId
```

```
    $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -
eq $BlockDeviceName }).Key | Select-Object -First 1
  }
  ElseIf ($DiskDrive.path -like "*PROD_AMAZON_EC2_NVME*") {
    $BlockDeviceName = (Get-EC2InstanceMetadata -Category
 "BlockDeviceMapping")."ephemeral$((Get-WmiObject -Class Win32_Diskdrive | Where-
Object { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" + $DiskDrive.Number) }).SCSIPort - 2)"
    $BlockDevice = $null
    $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -
eq $BlockDeviceName }).Key | Select-Object -First 1
  }
  ElseIf ($DiskDrive.path -like "*PROD_AMAZON*") {
    if ($DriveLetter -match '[^a-zA-Z0-9]') {
      $i = 0
      While ($i -ne ($array3.Count)) {
        if ($array[2][$i] -eq $EbsVolumeID) {
          $DriveLetter = $array[0][$i]
          $DeviceName = $array[3][$i]
        }
        $i ++
      }
    }
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.ebs.VolumeId -eq
 $EbsVolumeID }).DeviceName
  }
  ElseIf ($DiskDrive.path -like "*NETAPP*") {
    if ($DriveLetter -match '[^a-zA-Z0-9]') {
      $i = 0
      While ($i -ne ($array3.Count)) {
        if ($array[2][$i] -eq $EbsVolumeID) {
          $DriveLetter = $array[0][$i]
          $DeviceName = $array[3][$i]
        }
        $i ++
      }
    }
    $EbsVolumeID = "FSxN Volume"
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.ebs.VolumeId -eq
 $EbsVolumeID }).DeviceName
  }
  Else {
    $BlockDeviceName = $null
```

```
    $BlockDevice = $null
  }
  New-Object PSObject -Property @{
    Disk          = $Disk;
    Partitions    = $Partitions;
    DriveLetter   = If ($DriveLetter -eq $null) { "N/A" } Else { $DriveLetter };
    EbsVolumeId   = If ($EbsVolumeID -eq $null) { "N/A" } Else { $EbsVolumeID };
    Device        = If ($BlockDeviceName -eq $null) { "N/A" } Else
 { $BlockDeviceName };
    VirtualDevice = If ($VirtualDevice -eq $null) { "N/A" } Else { $VirtualDevice };
    VolumeName    = If ($VolumeName -eq $null) { "N/A" } Else { $VolumeName };
    DeviceName    = If ($DeviceName -eq $null) { "N/A" } Else { $DeviceName };
  }
} | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions,
 DriveLetter, EbsVolumeId, Device, VirtualDevice, DeviceName, VolumeName
```

Exécutez le script comme suit :

```
PS C:\> .\mapping.ps1
```

Voici un exemple de sortie.

```
Disk  Partitions  DriveLetter   EbsVolumeId            Device      VirtualDevice
 DeviceName              VolumeName
----  ----------  -----------   -----------            ------      -------------
 ----------              ----------
   0           1            C   vol-0561f1783298efedd   /dev/sda1   N/A
 NVMe Amazon Elastic B   N/A
   1           1            D   vol-002a9488504c5e35a   xvdb        N/A
 NVMe Amazon Elastic B   N/A
   2           1            E   vol-0de9d46fcc907925d   xvdc        N/A
 NVMe Amazon Elastic B   N/A
```

Si vous n'avez pas fourni vos informations d'identification sur l'instance Windows, le script ne peut pas obtenir l'ID du EBS volume et utilise N/A dans la `EbsVolumeId` colonne.

Mappez des objets autres que NVMe des disques à des volumes

Le pilote du périphérique de stockage en mode bloc de l'instance attribue les noms de volume réels lors du montage des volumes.

Mappages

- Volumes de stockage d'instance
- EBSvolumes

Volumes de stockage d'instance

Le tableau suivant décrit comment les pilotes PV et AWS PV Citrix mappent les volumes de stockage autres que les NVMe instances aux volumes Windows. Le nombre de volumes de stockage d'instance disponibles est déterminé par le type d'instance. Pour plus d'informations, consultez Limites de volume de stockage d'instance pour les EC2 instances.

Emplacement	Nom d'appareil
Bus numéro 0, ID cible 78, LUN 0	xvdca
Bus numéro 0, ID cible 79, LUN 0	xvdcb
Bus numéro 0, ID cible 80, LUN 0	xvdcc
Bus numéro 0, ID cible 81, LUN 0	xvdcd
Bus numéro 0, ID cible 82, LUN 0	xvdce
Bus numéro 0, ID cible 83, LUN 0	xvdcf
Bus numéro 0, ID cible 84, LUN 0	xvdcg
Bus numéro 0, ID cible 85, LUN 0	xvdch
Bus numéro 0, ID cible 86, LUN 0	xvdci
Bus numéro 0, ID cible 87, LUN 0	xvdcj
Bus numéro 0, ID cible 88, LUN 0	xvdck
Bus numéro 0, ID cible 89, LUN 0	xvdcl

EBSvolumes

Le tableau suivant décrit comment les pilotes PV et AWS PV Citrix mappent les NVME EBS non-volumes aux volumes Windows.

Emplacement	Nom d'appareil
Bus numéro 0, ID cible 0, LUN 0	/dev/sda1
Bus numéro 0, ID cible 1, LUN 0	xvdb
Bus numéro 0, ID cible 2, LUN 0	xvdc
Bus numéro 0, ID cible 3, LUN 0	xvdd
Bus numéro 0, ID cible 4, LUN 0	xvde
Bus numéro 0, ID cible 5, LUN 0	xvdf
Bus numéro 0, ID cible 6, LUN 0	xvdg
Bus numéro 0, ID cible 7, LUN 0	xvdh
Bus numéro 0, ID cible 8, LUN 0	xvdi
Bus numéro 0, ID cible 9, LUN 0	xvdj
Bus numéro 0, ID cible 10, LUN 0	xvdk
Bus numéro 0, ID cible 11, LUN 0	xvdl
Bus numéro 0, ID cible 12, LUN 0	xvdm
Bus numéro 0, ID cible 13, LUN 0	xvdn
Bus numéro 0, ID cible 14, LUN 0	xvdo
Bus numéro 0, ID cible 15, LUN 0	xvdp
Bus numéro 0, ID cible 16, LUN 0	xvdq
Bus numéro 0, ID cible 17, LUN 0	xvdr

Emplacement	Nom d'appareil
Bus numéro 0, ID cible 18, LUN 0	xvds
Bus numéro 0, ID cible 19, LUN 0	xvdt
Bus numéro 0, ID cible 20, LUN 0	xvdu
Bus numéro 0, ID cible 21, LUN 0	xvdv
Bus numéro 0, ID cible 22, LUN 0	xvdw
Bus numéro 0, ID cible 23, LUN 0	xvdx
Bus numéro 0, ID cible 24, LUN 0	xvdy
Bus numéro 0, ID cible 25, LUN 0	xvdz

Prévention de l'écriture déchirée sur les instances Amazon EC2 Linux

> **Note**
>
> La prévention de l'écriture déchirée est prise en charge uniquement avec les instances Linux.

La prévention de l'écriture déchirée est une fonctionnalité de stockage par blocs conçue AWS pour améliorer les performances de vos charges de travail de base de données relationnelles intensives en E/S et réduire la latence sans affecter négativement la résilience des données. Les bases de données relationnelles qui utilisent InnoDB ou XtraDB comme moteur de base de données, telles que My SQL et MariaDB, bénéficieront de la prévention de l'écriture déchirée.

En règle générale, les bases de données relationnelles qui utilisent des pages plus grandes que l'atomicité en cas de panne du périphérique de stockage utilisent des mécanismes de journalisation de données pour se protéger contre les écritures déchirées. MariaDB et SQL My utilisent un fichier tampon à double écriture pour enregistrer les données avant de les écrire dans des tables de données. En cas d'écritures incomplètes ou déchirées, à la suite d'une panne du système d'exploitation ou d'une panne de courant pendant les transactions d'écriture, la base de

données peut récupérer les données de la mémoire tampon à double écriture. La surcharge d'E/S supplémentaire associée à l'écriture dans la mémoire tampon à double écriture a un impact sur les performances de la base de données et la latence des applications. De plus, elle réduit le nombre de transactions pouvant être traitées par seconde. Pour plus d'informations sur le tampon doublewrite, consultez les documentations MariaDB et My. SQL

Grâce à la protection contre l'écriture déchirée, les données sont enregistrées dans le stockage sous all-or-nothingforme de transactions d'écriture, ce qui élimine le besoin d'utiliser la mémoire tampon à double écriture. Cela empêche l'écriture de données partielles ou déchirées dans le stockage en cas de panne du système d'exploitation ou de panne de courant lors des transactions d'écriture. Le nombre de transactions traitées par seconde peut être augmenté jusqu'à 30 % et la latence d'écriture peut être réduite jusqu'à 50 %, sans compromettre la résilience de vos charges de travail.

Tarification

L'utilisation de la solution de prévention des écritures déchirées est disponible sans coûts supplémentaires.

Table des matières

Tailles de bloc pour empêcher l'écriture déchirée sur Amazon EC2

La prévention des écritures déchirées prend en charge les opérations d'écriture pour des blocs de données de 4 Kio, 8 Kio et 16 Kio. L'adresse du bloc logique de début du bloc de données (LBA) doit être alignée sur la taille de limite de bloc respective de 4 KiB, 8 KiB ou 16 KiB. Par exemple, pour les opérations d'écriture de 16 KiB, le début du bloc de données LBA doit être aligné sur une taille de limite de bloc de 16 KiB.

Le tableau suivant présente la prise en charge des différents types de stockage et d'instance.

	Blocs de 4 Kio	Blocs de 8 Kio	Blocs de 16 Kio
Volumes de	Toutes les NVMe instances stockent des	Instances i4i, IM4GN et IS4gen prises en charge par Nitro. AWS SSD	

	Blocs de 4 Kio	Blocs de 8 Kio	Blocs de 16 Kio
stockage d'instances	volumes attachés aux instances de la famille I de la génération actuelle.		
EBSVolumes Amazon	Tous les EBS volumes Amazon attachés à des instances basées sur le système AWS Nitro.		

Pour vérifier si votre instance et votre volume prennent en charge la prévention des écritures déchirées, adressez une requête afin de vérifier si l'instance prend en charge la prévention des écritures déchirées et fournissez d'autres informations, telles que les tailles de blocs et de limites prises en charge. Pour de plus amples informations, veuillez consulter Vérifiez le support des EC2 instances Amazon pour empêcher l'écriture déchirée.

Conditions requises pour utiliser la protection contre l'écriture déchirée sur Amazon EC2

Pour que la prévention des écritures déchirées fonctionne correctement, une opération d'E/S doit respecter les exigences de taille, d'alignement et de limites, telles que spécifiées dans les champs `NTWPU`, `NTWGU` et `NTWBU`. Vous devez configurer votre système d'exploitation de manière à ce que le sous-système de stockage spécifique (système de fichiers LVMRAID, etc.) ne modifie pas les propriétés d'E/S dans la pile de stockage, notamment les fusions de blocs, les scissions ou la relocalisation d'adresses de blocs, avant d'être soumis au périphérique.

La prévention des écritures déchirées a été testée avec la configuration suivante :

- Type d'instance et type de stockage qui prennent en charge la taille de bloc requise.
- Amazon Linux 2 avec la version du noyau 5.10 ou version ultérieure.
- ext4 avec `bigalloc` activé et une taille de cluster de 16 Kio, ainsi que les utilitaires ext4 les plus récents (e2fsprogs 1.46.5 ou version ultérieure).
- Mode d'accès aux fichiers `O_DIRECT` pour contourner le cache tampon du noyau Linux.

> **Note**
>
> Il n'est pas nécessaire de désactiver la fusion d'E/S pour les charges de travail My et SQL MariaDB.

Vérifiez le support des EC2 instances Amazon pour empêcher l'écriture déchirée

Pour vérifier si votre instance et votre volume prennent en charge la prévention de l'écriture déchirée et pour consulter les données spécifiques au fournisseur de l'NVMeespace de noms contenant des informations de prévention de l'écriture déchirée, utilisez la commande suivante.

```
$ sudo nvme id-ns -v device_name
```

> **Note**
>
> La commande renvoie les informations spécifiques au fournisseur sous forme hexadécimale avec interprétation. ASCII Il se peut que vous deviez intégrer à vos applications un outil similaire à `ebsnvme-id` capable de lire et d'analyser les résultats.

Par exemple, la commande suivante renvoie les données spécifiques au fournisseur de l'NVMeespace de noms contenant des informations de prévention de l'écriture déchirée pour`/dev/nvme1n1`.

```
$ sudo nvme id-ns -v /dev/nvme1n1
```

Si votre instance et votre volume prennent en charge la prévention de l'écriture déchirée, ils renvoient les informations de prévention de l'écriture AWS déchirée suivantes dans les données spécifiques au fournisseur de l'NVMeespace de noms.

> **Note**
>
> Les octets du tableau suivant représentent le décalage en octets par rapport au début des données spécifiques au fournisseur de l'NVMeespace de noms.

Octets	Description
0:31	Le nom du point de montage de l'attachement du périphérique, par exemple /dev/xvda . Vous le fournissez lors de la demande de pièce jointe au volume et il peut être utilisé par l'EC2instance Amazon pour créer un lien symbolique vers le périphérique en NVMe mode bloc (nvmeXn1).
32:63	ID du volume. Par exemple, vol01234567890abcdef . Ce champ peut être utilisé pour mapper le NVMe périphérique au volume attaché.
64:255	Réservé pour un usage futur.
256:257	Taille de l'unité de prévention de l'écriture déchirée dans l'espace de noms (NTWPU). Ce champ indique la taille spécifique à l'espace de noms de l'opération d'écriture dont l'écriture est garantie de manière atomique en cas de panne de NVM courant ou d'erreur. Ce champ est spécifié dans des blocs logiques représentés par des valeurs basées sur zéro.
258:259	Taille de granularité de prévention de l'écriture déchirée par l'espace de noms ()NTWPG. Ce champ indique les incréments de taille spécifiques à l'espace de noms ci-dessous NTWPU de l'opération d'écriture dont l'écritur e est garantie de manière atomique en cas de panne de NVM courant ou d'erreur. C'est-à-dire que la taille doit être NTWPG * n <= NTWPU, où n est un entier positif. Le LBA décalage de l'opération d'écriture doit également être aligné sur ce champ. Ce champ est spécifié dans des blocs logiques représentés par des valeurs basées sur zéro.
260:263	Taille de la limite de prévention de l'écriture déchirée par l'espace de noms (NTWPB). Ce champ indique la taille de la limite atomique pour cet espace de noms pour la valeur NTWPU. Il n'est pas garanti que les écritures dans cet espace de noms qui franchissent les limites atomiques soient écrites de manière atomique en cas de panne de NVM courant ou d'erreur. Une valeur de 0h indique qu'il n'existe pas de limites atomiques pour les conditions de panne ou d'erreur. Toutes les autres valeurs

Octets	Description
	indiquent une taille en termes de blocs logiques utilisant le même codage que le champ NTWPU.

Configurez votre charge de travail sur Amazon EC2 pour éviter les erreurs d'écriture

La prévention des écritures déchirées est activée par défaut sur les types d'instances pris en charge avec des volumes pris en charge. Vous n'avez pas besoin d'activer de paramètres supplémentaires pour activer la prévention des écritures déchirées sur votre volume ou votre instance.

> **Note**
>
> Il n'y a aucun impact sur les performances quant aux charges de travail qui ne prennent pas en charge la prévention des écritures déchirées. Vous n'avez pas besoin d'apporter des modifications pour ces charges de travail.
> Les charges de travail qui prennent en charge la prévention des erreurs d'écriture, mais qui ne sont pas configurées pour l'utiliser, continuent à utiliser la mémoire tampon à double écriture et ne bénéficient d'aucun avantage en termes de performances.

Pour configurer votre pile logicielle My SQL ou MariaDB afin de désactiver le tampon d'écriture double et d'utiliser la prévention de l'écriture déchirée, procédez comme suit :

1. Configurez votre volume pour utiliser le système de fichiers ext4 avec l' BigAlloc option et définissez la taille du cluster sur 4 KiB, 8 KiB ou 16 KiB. L'utilisation BigAlloc d'une taille de cluster de 4 KiB, 8 KiB ou 16 KiB garantit que le système de fichiers alloue les fichiers conformément à la limite correspondante.

   ```
   $  mkfs.ext4 -O bigalloc -C 4096|8192|16384 device_name
   ```

   > **Note**
   >
   > Pour My SQL et MariaDB, vous devez `-C 16384` utiliser pour correspondre à la taille de page de la base de données. La définition de la granularité d'allocation sur une valeur autre qu'un multiple de la taille de page peut entraîner des allocations qui peuvent ne

pas correspondre aux limites de prévention des écritures déchirées du périphérique de stockage.

Par exemple :

```
$  mkfs.ext4 -O bigalloc -C 16384 /dev/nvme1n1
```

2. Configurez InnoDB pour utiliser la méthode de vidage `O_DIRECT` et désactivez la double écriture d'InnoDB. Utilisez l'éditeur de texte de votre choix pour ouvrir `/etc/my.cnf` et mettez à jour les paramètres `innodb_flush_method` et `innodb_doublewrite` comme suit :

```
innodb_flush_method=O_DIRECT
innodb_doublewrite=0
```

Important

Si vous utilisez Logical Volume Manager (LVM) ou une autre couche de virtualisation du stockage, assurez-vous que les décalages de départ des volumes sont alignés sur des multiples de 16 KiB. Cela est relatif au NVMe stockage sous-jacent pour prendre en compte les en-têtes de métadonnées et les superblocs utilisés par la couche de virtualisation du stockage. Si vous ajoutez un décalage au volume LVM physique, cela peut entraîner un désalignement entre les allocations du système de fichiers et les décalages du NVMe périphérique, ce qui annulerait la prévention de l'écriture déchirée. Pour plus d'informations, veuillez consulter `--dataalignmentoffset` dans la page Amazon Linux.

EBSInstantanés Amazon VSS basés sur Windows cohérents avec les applications

Vous pouvez prendre des instantanés cohérents avec les applications de tous les EBS volumes Amazon attachés à vos instances Amazon EC2 Windows à l'aide AWS Systems Manager de Run Command. Le processus de capture instantanée utilise le service Windows Volume Shadow Copy (VSS) pour effectuer des sauvegardes au niveau du EBS volume des applications VSS compatibles. Les instantanés incluent des données de transactions en attente entre ces applications

et le disque. Vous n'avez pas besoin de fermer vos instances ni de les déconnecter lorsque vous devez sauvegarder tous les volumes attachés.

L'utilisation des EBS instantanés VSS basés sur des instantanés n'entraîne aucun coût supplémentaire. Vous ne payez que pour les EBS instantanés créés par le processus de sauvegarde. Pour plus d'informations, consultez Comment me sont facturés mes EBS instantanés Amazon ?

> **Note**
>
> Les instantanés VSS basés sur Windows cohérents avec les applications ne sont pris en charge qu'avec les instances Windows.

Table des matières

Qu'est-ce qu'VSS ?

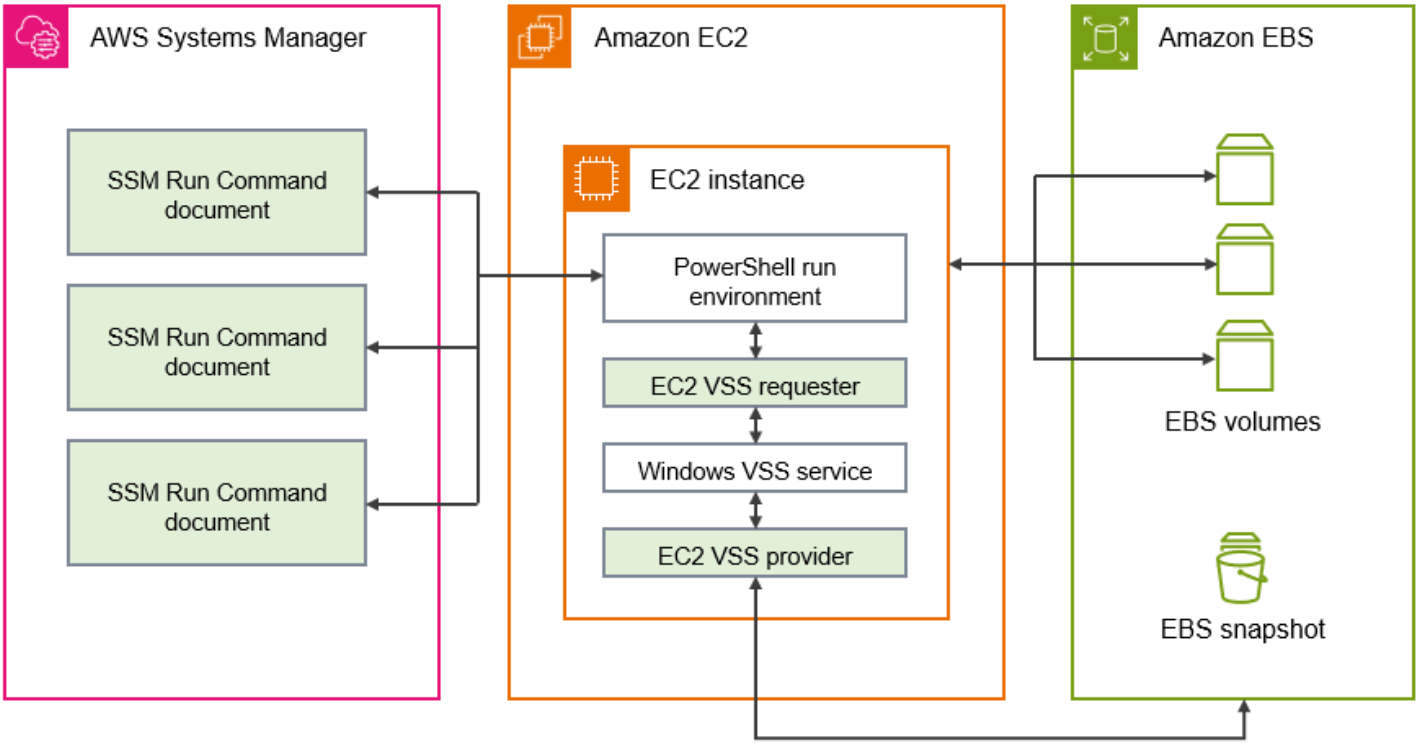
Volume Snapshot Copy Service (VSS) est une technologie de sauvegarde et de restauration incluse dans Microsoft Windows. Elle peut créer des copies de sauvegarde, ou des instantanés, de fichiers ou de volumes informatiques pendant leur utilisation. Pour plus d'informations, consultez Volume Shadow Copy Service.

Pour créer un instantané de la cohérence de l'application, les composants logiciels suivants sont impliqués.

- VSSservice — Fait partie du système d'exploitation Windows
- VSSdemandeur — Le logiciel qui demande la création de copies instantanées
- VSSrédacteur : généralement fourni dans le cadre d'une application, telle qu'un SQL serveur, pour garantir un ensemble de données cohérent à sauvegarder

- VSSprovider — Le composant qui crée les copies instantanées des volumes sous-jacents

La solution Amazon EBS Snapshot VSS basée sur Windows se compose de plusieurs documents Systems Manager (SSM) Run Command qui facilitent la création de sauvegardes, et d'un [package Systems Manager Distributor](#)`AwsVssComponents`, appelé, qui inclut un EC2VSSdemandeur et un EC2VSSfournisseur. Le `AwsVssComponents` package doit être installé sur des instances EC2 Windows pour prendre des instantanés de volumes cohérents avec les applications. EBS Le schéma suivant illustre la relation entre ces composants logiciels.



Comment fonctionne la solution Amazon EBS Snapshot VSS basée sur Amazon

Le processus de création de scripts de EBS capture d'écran cohérents avec les applications comprend les étapes suivantes. VSS

1. Terminez le [Conditions requises pour créer des instantanés VSS basés sur EBS Windows](#).
2. Entrez les paramètres du `AWSEC2-VssInstallAndSnapshot` SSM document et exécutez-le à l'aide de la commande Exécuter. Pour de plus amples informations, veuillez consulter [Exécuter le document VssInstallAndSnapshot de commande AWSEC2 - (recommandé)](#).

3. Le VSS service Windows de votre instance coordonne toutes les opérations d'E/S en cours pour exécuter des applications.
4. Le système vide tous les tampons I/O et suspend provisoirement toutes les opérations d'I/O. Cette interruption dure, au maximum, dix secondes.
5. Pendant cette suspension, le système crée des instantanés de tous les volumes attachés à l'instance.
6. La suspension est ensuite levée et les I/O reprennent leurs opérations.
7. Le système ajoute tous les instantanés nouvellement créés à la liste des instantanés. EBS Le système étiquette tous les EBS instantanés VSS basés avec succès créés avec succès par ce processus AppConsistent avec:true.
8. Si vous devez effectuer une restauration à partir d'un instantané, vous pouvez utiliser le EBS processus standard de création d'un volume à partir d'un instantané, ou vous pouvez restaurer tous les volumes sur une instance à l'aide d'un exemple de script, comme décrit dansRestaurez EBS des volumes pour votre instance Windows à partir de snapshots VSS basés.

Conditions requises pour créer des instantanés VSS basés sur EBS Windows

Vous pouvez créer des EBS instantanés VSS basés sur Systems Manager Run Command ou Amazon Data Lifecycle Manager. AWS Backup Les conditions suivantes s'appliquent à toutes les solutions.

Configuration système requise

Assurez-vous que votre instance EC2 Windows répond à toutes les exigences du système pour créer des instantanés VSS basés, y compris les versions prises en charge du système d'exploitation Windows. NETframework, PowerShell AWS Tools for Windows PowerShell, et l' AWS Systems Manager agent.

IAMautorisations

Le IAM rôle associé à votre instance Amazon EC2 Windows doit être autorisé à créer des instantanés cohérents avec les applications avec. VSS Pour accorder les autorisations nécessaires, vous pouvez associer la politique `AWSEC2VssSnapshotPolicy` gérée à votre profil d'instance.

VSScomposants

Pour créer des instantanés cohérents avec les applications sur les systèmes d'exploitation Windows, le package `AwsVssComponents` doit être installé sur l'instance. Le package contient un EC2 VSS agent sur instance qui fonctionne en tant que VSS demandeur et un EC2 VSS fournisseur de EBS volumes.

Configuration système requise

Installation de l'agent Systems Manager

VSSest orchestré par l'agent Systems Manager à l'aide PowerShell de. Assurez-vous d'avoir installé la version de SSM l'agent `3.0.502.0` ou une version ultérieure sur votre EC2 instance. Si vous utilisez déjà une ancienne version de l'SSMagent, mettez-la à jour à l'aide de Run Command. Pour plus d'informations, consultez les sections Configuration de Systems Manager pour les EC2 instances Amazon et Working with SSM Agent on Amazon EC2 instances for Windows Server dans le guide de AWS Systems Manager l'utilisateur.

Exigences relatives aux instances Amazon EC2 Windows

VSSles EBS instantanés basés sur Windows Server sont pris en charge pour les instances exécutant Windows Server 2016 et versions ultérieures.

. NETVersion du framework

Le `AwsVssComponents` package nécessite. NETVersion du framework `4.6` ou version ultérieure. Les versions du système d'exploitation Windows antérieures à Windows Server 2016 utilisent par défaut une version antérieure de. NETCadre. Si votre instance utilise une version antérieure du. NETFramework, vous devez installer la version `4.6` ou ultérieure à l'aide de Windows Update.

AWS Tools for Windows PowerShell version

Assurez-vous que votre instance exécute la AWS Tools for Windows PowerShell version `3.3.48.0` ou une version ultérieure. Pour vérifier votre version, exécutez la commande suivante dans le PowerShell terminal de l'instance.

```
C:\> Get-AWSPowerShellVersion
```

Si vous devez effectuer une mise à jour AWS Tools for Windows PowerShell sur votre instance, consultez la section Installation du AWS Tools for Windows PowerShell dans le guide de AWS Tools for Windows PowerShell l'utilisateur.

PowerShell Version Windows

Assurez-vous que votre instance exécute la version PowerShell majeure de Windows `3`, `4`, ou `5`. Pour vérifier votre version, exécutez la commande suivante dans un PowerShell terminal de l'instance.

```
C:\> $PSVersionTable.PSVersion
```

PowerShell mode de langue

Assurez-vous que le mode de PowerShell langue de votre instance est défini sur`FullLanguage`. Pour plus d'informations, veuillez consulter about_Language_Modes dans la documentation Microsoft.

Utiliser une politique IAM gérée pour accorder des autorisations pour les instantanés VSS basés

La politique AWSEC2VssSnapshotPolicy gérée permet à Systems Manager d'effectuer les actions suivantes sur votre instance Windows :

- Création et balisage d'EBSinstantanés
- Créez et étiquetez Amazon Machine Images (AMIs)
- Attachez des métadonnées, telles que l'ID de l'appareil, aux balises de capture par défaut qui sont VSS créées.

Cette rubrique décrit les détails des autorisations pour la politique VSS gérée et explique comment l'associer à votre IAM rôle de profil d'EC2instance.

Table des matières

AWSEC2VssSnapshotPolicydétails de la politique gérée

Une politique AWS gérée est une politique autonome proposée par Amazon aux AWS clients. AWS les politiques gérées sont conçues pour accorder des autorisations pour les cas d'utilisation courants. Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Toutefois, vous pouvez copier la politique et l'utiliser comme référence pour une politique gérée par le client spécifique à votre cas d'utilisation.

Pour plus d'informations sur les politiques AWS gérées, voir les politiques AWS gérées dans le Guide de IAM l'utilisateur.

Pour utiliser la politique AWSEC2VssSnapshotPolicygérée, vous pouvez l'associer au IAM rôle associé à vos instances EC2 Windows. Cette politique permet à la EC2 VSS solution de créer et d'ajouter des balises aux Amazon Machine Images (AMIs) et aux EBS Snapshots. Pour joindre la politique, voirAssociez la politique gérée par VSS snapshot à votre rôle de profil d'instance.

Autorisations octroyées par AWSEC2VssSnapshotPolicy

La AWSEC2VssSnapshotPolicypolitique inclut les EC2 autorisations Amazon suivantes pour permettre à Amazon de EC2 créer et de gérer des VSS instantanés en votre nom. Vous pouvez associer cette politique gérée au rôle de profil d'IAMinstance que vous utilisez pour vos instances EC2 Windows.

- ec2 : CreateTags — Ajoutez des balises aux EBS instantanés pour aider AMIs à identifier et à classer les ressources.
- ec2 : DescribeInstanceAttribute — Récupérez les EBS volumes et les mappages de périphériques de blocs correspondants attachés à l'instance cible.
- ec2 : CreateSnapshots — Créez des instantanés de volumes. EBS
- ec2 : CreateImage — Créez un à AMI partir d'une EC2 instance en cours d'exécution.
- ec2 : DescribeImages — Récupère les informations EC2 AMIs et les instantanés.
- ec2 : DescribeSnapshots — Déterminez l'heure de création et le statut des instantanés afin de vérifier la cohérence de l'application.

> **Note**
>
> Pour consulter les détails des autorisations relatives à cette politique, reportez-vous AWSEC2VssSnapshotPolicyà la référence des politiques AWS gérées.

Simplifier les autorisations pour des cas d'utilisation spécifiques - avancé

La politique `AWSEC2VssSnapshotPolicy` gérée inclut des autorisations pour toutes les manières dont vous pouvez créer des instantanés VSS basés sur des instantanés. Vous pouvez créer une politique personnalisée qui inclut uniquement les autorisations dont vous avez besoin.

Cas d'utilisation : CréerAMI, Cas d'utilisation : Utiliser AWS Backup un service

Si vous utilisez exclusivement `CreateAmi` cette option, ou si vous créez des instantanés VSS basés uniquement via le AWS Backup service, vous pouvez rationaliser les déclarations de politique comme suit.

- Omettez les déclarations de politique identifiées par l'énoncé suivant IDs (SIDs) :
  - `CreateSnapshotsWithTag`
  - `CreateSnapshotsAccessInstance`
  - `CreateSnapshotsAccessVolume`
- Ajustez l'`CreateTagsOnResourceCreation`énoncé comme suit :
  - Supprimer `arn:aws:ec2:*:*:snapshot/*` des ressources.
  - Supprimer `CreateSnapshots` de la `ec2:CreateAction` condition.
- Ajustez l'`CreateTagsAfterResourceCreation`instruction pour la `arn:aws:ec2:*:*:snapshot/*` supprimer des ressources.
- Ajustez l'`DescribeImagesAndSnapshots`instruction à supprimer `ec2:DescribeSnapshots` de l'action de la déclaration.

Cas d'utilisation : Snapshot uniquement

Si vous n'utilisez pas `CreateAmi` cette option, vous pouvez rationaliser les déclarations de politique comme suit.

- Omettez les déclarations de politique identifiées par l'énoncé suivant IDs (SIDs) :
  - `CreateImageAccessInstance`
  - `CreateImageWithTag`
- Ajustez l'`CreateTagsOnResourceCreation`énoncé comme suit :
  - Supprimer `arn:aws:ec2:*:*:image/*` des ressources.
  - Supprimer `CreateImage` de la `ec2:CreateAction` condition.

- Ajustez l'`CreateTagsAfterResourceCreation`instruction pour la `arn:aws:ec2:*:*:image/*` supprimer des ressources.
- Ajustez l'`DescribeImagesAndSnapshots`instruction à supprimer `ec2:DescribeImages` de l'action de la déclaration.

> **Note**
>
> Pour garantir que votre politique personnalisée fonctionne comme prévu, nous vous recommandons de consulter et d'intégrer régulièrement des mises à jour à la politique gérée.

Associez la politique gérée par VSS snapshot à votre rôle de profil d'instance

Pour accorder des autorisations pour les instantanés VSS basés sur votre instance EC2 Windows, vous pouvez associer la politique AWSEC2VssSnapshotPolicygérée à votre rôle de profil d'instance comme suit. Il est important de vous assurer que votre instance répond à toutes les exigencesConfiguration système requise.

> **Note**
>
> Pour utiliser la politique gérée, la version `AwsVssComponents` du package `2.3.1` ou une version ultérieure doit être installée sur votre instance. Pour l'historique des versions, voirAwsVssComponents versions du package.

1. Ouvrez la IAM console à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, choisissez Rôles pour afficher la liste des IAM rôles auxquels vous avez accès.
3. Sélectionnez le lien Nom du rôle associé à votre instance. Cela ouvre la page détaillée du rôle.
4. Pour joindre la politique gérée, choisissez Ajouter des autorisations, dans le coin supérieur droit du panneau de liste. Sélectionnez ensuite Joindre des politiques dans la liste déroulante.
5. Pour rationaliser les résultats, entrez le nom de la politique dans la barre de recherche (`AWSEC2VssSnapshotPolicy`).
6. Cochez la case à côté du nom de la politique à joindre, puis choisissez Ajouter des autorisations.

Package de VSS composants de gestion pour les EBS instantanés VSS basés sur Windows

Avant de créer des EBS instantanés VSS basés, assurez-vous que la dernière version du package de VSS composants est installée sur votre instance Windows. Vous pouvez installer le `AwsVssComponents` package sur une instance existante de plusieurs manières, comme suit :

- (Recommandé) Exécuter le document VssInstallAndSnapshot de commande AWSEC2 - (recommandé). Cela s'installe ou se met à jour automatiquement si nécessaire à chaque exécution.
- Installation manuelle des VSS composants sur une instance EC2 Windows.
- Mettez à jour le package de VSS composants sur votre instance EC2 Windows.

Vous pouvez également créer un AMI with EC2 Image Builder qui utilise le composant `aws-vss-components-windows` géré pour installer le `AwsVssComponents` package de l'image. Le composant géré utilise AWS Systems Manager Distributor pour installer le package. Une fois qu'Image Builder a créé l'image, le VSS package est installé sur chaque instance que vous lancez à partir de l'instance associéeAMI. Pour plus d'informations sur la façon dont vous pouvez créer un AMI avec le VSS package installé, consultez la section Composants gérés par le package Distributor pour Windows dans le guide de l'utilisateur d'EC2Image Builder.

Table des matières

Installation manuelle des VSS composants sur une instance EC2 Windows

Des VSS composants doivent être installés sur votre instance EC2 Windows pour que vous puissiez créer des instantanés cohérents avec les applications avec Systems Manager. Si vous n'exécutez pas le document de commande `AWSEC2-VssInstallAndSnapshot` pour installer ou mettre à jour automatiquement le package chaque fois que vous créez des instantanés cohérents avec les applications, vous devez installer le package manuellement.

Vous devez également effectuer l'installation manuellement si vous prévoyez d'utiliser l'une des méthodes suivantes pour créer des instantanés cohérents avec les applications à partir de votre instance. EC2

- Créez des VSS instantanés à l'aide de AWS Backup

- Créez des VSS instantanés à l'aide d'Amazon Data Lifecycle Manager

Si vous devez effectuer une installation manuelle, nous vous recommandons d'utiliser le dernier package de AWS VSS composants pour améliorer la fiabilité et les performances des instantanés cohérents avec les applications sur vos EC2 instances Windows.

> **Note**
>
> Pour installer ou mettre à jour automatiquement le package `AwsVssComponents` chaque fois que vous créez des instantanés cohérents avec les applications, nous vous recommandons d'utiliser Systems Manager pour exécuter le document. `AWSEC2-VssInstallAndSnapshot` Pour de plus amples informations, veuillez consulter Exécuter le document VssInstallAndSnapshot de commande AWSEC2 - (recommandé).

Pour installer les VSS composants sur une instance Amazon EC2 Windows, suivez les étapes correspondant à votre environnement préféré.

Console

Pour installer les VSS composants à l'aide du SSM distributeur

1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.
2. Dans le panneau de navigation, choisissez Fonctionnalité Exécuter la commande.
3. Choisissez Run Command (Exécuter la commande).
4. Pour le document de commande, cliquez sur le bouton à côté de AWS-C onfigureAWSPackage.
5. Dans Command parameters (Paramètres de la commande), procédez comme suit :
   a. Vérifiez que l'option Action est définie sur Install (Installer).
   b. Pour Nom, saisissez `AwsVssComponents`.
   c. Pour Version, saisissez un numéro de version ou laissez le champ vide pour que Systems Manager installe la dernière version.
6. Dans la section Targets (Cibles), identifiez les instances sur lesquelles vous souhaitez exécuter cette opération en spécifiant les balises ou en sélectionnant manuellement les instances.

> **Note**
>
> Si vous choisissez de sélectionner les instances manuellement et qu'une instance que vous vous attendez à voir ne figure pas dans la liste, consultez Où sont mes instances ? dans le Guide de l'utilisateur AWS Systems Manager pour obtenir des conseils de résolution d'incident.

7. Pour Autres paramètres :

   - (Facultatif) Pour Comment (Commentaire), saisissez les informations relatives à cette commande.
   - Pour Délai (secondes), précisez le nombre de secondes durant lesquelles le système doit attendre avant de mettre en échec l'exécution de la commande globale.

8. (Facultatif) Pour Contrôle du débit :

   - Pour Concurrency (Simultanéité), spécifiez un nombre ou un pourcentage d'instances sur lesquelles exécuter simultanément la commande.

     > **Note**
     >
     > Si vous avez sélectionné des cibles en choisissant les EC2 balises Amazon et que vous n'êtes pas certain du nombre d'instances utilisant les balises sélectionnées, limitez le nombre d'instances pouvant exécuter le document en même temps en spécifiant un pourcentage.

   - Pour Seuil d'erreur, spécifiez quand arrêter l'exécution de la commande sur d'autres instances après son échec sur un nombre ou un pourcentage d'instances. Si, par exemple, vous spécifiez trois erreurs, Systems Manager cesse d'envoyer la commande à la réception de la quatrième erreur. Les instances sur lesquelles la commande est en cours de traitement peuvent également envoyer des erreurs.

9. (Facultatif) Dans la section Output options (Options de sortie), si vous souhaitez enregistrer la sortie de la commande dans un fichier, sélectionnez Enable writing to an S3 bucket (Autoriser l'écriture dans un compartiment S3) Spécifiez les noms du compartiment et (facultatif) du préfixe (dossier).

> **Note**
>
> Les autorisations S3 qui accordent la possibilité d'écrire les données dans un compartiment S3 sont celles du profil d'instance attribué à l'instance, et non celles de l'utilisateur qui effectue cette tâche. Pour plus d'informations, consultez la section Créer un profil d'IAMinstance pour Systems Manager dans le guide de AWS Systems Manager l'utilisateur.

10. (Facultatif) Spécifiez les options pour SNSles notifications.

    Pour plus d'informations sur la configuration SNS des notifications Amazon pour Run Command, consultez Configuration SNS des notifications Amazon pour AWS Systems Manager.

11. Cliquez sur Exécuter.

AWS CLI

Utilisez la procédure suivante pour télécharger et installer le package `AwsVssComponents` sur vos instances en utilisant Run Command depuis AWS CLI. Le package installe deux composants : un VSS demandeur et un VSS fournisseur. Le système copie ces composants dans un répertoire de l'instance, puis enregistre le fournisseur DLL en tant que VSS fournisseur.

Pour installer le VSS package à l'aide du AWS CLI

- Exécutez la commande suivante pour télécharger et installer les VSS composants requis pour Systems Manager.

```
aws ssm send-command \
--document-name "AWS-ConfigureAWSPackage" \
--instance-ids "i-01234567890abcdef" \
--parameters '{"action":["Install"],"name":["AwsVssComponents"]}'
```

PowerShell

Suivez la procédure ci-dessous pour télécharger et installer le `AwsVssComponents` package sur vos instances à l'aide de la commande Exécuter la commande depuis les outils pour Windows PowerShell. Le package installe deux composants : un VSS demandeur et un VSS fournisseur.

Le système copie ces composants dans un répertoire de l'instance, puis enregistre le fournisseur DLL en tant que VSS fournisseur.

Pour installer le VSS package à l'aide du AWS Tools for Windows PowerShell

- Exécutez la commande suivante pour télécharger et installer les VSS composants requis pour Systems Manager.

```
Send-SSMCommand -DocumentName AWS-ConfigureAWSPackage -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'action'='Install';'name'='AwsVssComponents'}
```

Vérifier la signature sur les AWS VSS composants

Utilisez la procédure suivante pour vérifier la signature sur le package `AwsVssComponents`.

1. Connectez-vous à votre instance Windows. Pour de plus amples informations, veuillez consulter Connectez-vous à votre instance Windows à l'aide de RDP.
2. Accédez à C:\Program Files \ Amazon \AwsVssComponents.
3. Ouvrez le menu contextuel (clic droit) pour `ec2-vss-agent.exe`, puis choisissez Propriétés.
4. Accédez à l'onglet Signatures numériques et vérifiez que le nom du signataire est Amazon Web Services Inc.
5. Suivez les étapes précédentes pour vérifier la signature sur `Ec2VssInstaller` et `Ec2VssProvider.dll`.

Mettez à jour le package de VSS composants sur votre instance EC2 Windows

Nous vous recommandons de maintenir les VSS composants à jour avec la dernière version recommandée. Il existe plusieurs façons de mettre à jour les composants lorsqu'une nouvelle version du package `AwsVssComponents` est publiée.

Méthodes de mise à jour

- Vous pouvez répéter les étapes décrites Installation manuelle des VSS composants sur une instance EC2 Windows lors de la publication d'une nouvelle version des AWS VSS composants.
- Vous pouvez configurer une association Systems Manager State Manager pour télécharger et installer automatiquement des VSS composants nouveaux ou mis à jour lorsque le `AwsVssComponents` package est disponible.

- Vous pouvez installer ou mettre à jour automatiquement le package `AwsVssComponents` chaque fois que vous créez des instantanés cohérents avec les applications, lorsque vous utilisez Systems Manager pour exécuter le document `AWSEC2-VssInstallAndSnapshot`.

> **Note**
>
> Nous vous recommandons d'utiliser Systems Manager pour exécuter le document de commande `AWSEC2-VssInstallAndSnapshot`, qui installe ou met à jour automatiquement le package `AwsVssComponents` avant qu'il ne crée les instantanés cohérents avec les applications. Pour de plus amples informations, veuillez consulter Exécuter le document VssInstallAndSnapshot de commande AWSEC2 - (recommandé).

Pour créer une association Systems Manager State Manager, suivez les étapes correspondant à votre environnement préféré.

Console

Pour créer une association State Manager à l'aide de la console

1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.
2. Dans le volet de navigation, sélectionnez State Manager.

   Ou, si la page d'accueil de Systems Manager s'ouvre en premier, ouvrez le volet de navigation, puis choisissez State Manager.
3. Sélectionnez Créer une association.
4. Dans le champ Name (Nom), saisissez un nom évocateur.
5. Dans la liste des documents, choisissez AWS-C onfigureAWSPackage.
6. Dans la section Paramètres, sélectionnez Installer dans la liste Action.
7. Pour Installation type (Type d'installation), sélectionnez Uninstall and reinstall (Désinstaller et réinstaller).
8. Dans le champ Nom, saisissez `AwsVssComponents`. Vous pouvez ne rien inscrire dans les champs Version et Additional Arguments (Arguments supplémentaires).
9. Dans la section Targets (Cibles), sélectionnez une option.

> **Note**
>
> Si vous choisissez de cibler les instances à l'aide de balises, et que vous spécifiez des balises qui correspondent à des instances Linux, l'association réussit sur l'instance Windows, mais échoue sur les instances Linux. Le statut global de l'association indique Failed.

10. Dans la section Spécifier le programme, sélectionnez une option.
11. Dans la section Advanced options (Options avancées), pour Compliance severity (Sévérité de conformité), sélectionnez un niveau de sévérité pour l'association. Pour de plus amples informations, consultez A propos de la conformité des associations State Manager. Pour les Calendriers de modifications, sélectionnez un calendrier de modifications préconfiguré. Pour de plus amples informations, consultez AWS Systems Manager Change Calendar.
12. Pour Contrôle du débit, procédez comme suit :
    - Dans Concurrency (Simultanéité), spécifiez un nombre ou un pourcentage de nœuds gérés sur lesquels exécuter simultanément la commande.
    - Dans Error threshold (Seuil d'erreur), indiquez quand arrêter l'exécution de la commande sur les autres nœuds gérés après l'échec de celle-ci sur un certain nombre ou un certain pourcentage de nœuds.
13. (Facultatif) Dans Options de sortie, pour enregistrer la sortie de la commande dans un fichier, sélectionnez Autoriser l'écriture dans un compartiment S3. Saisissez les noms de compartiment et de préfixe (dossier) dans les zones.
14. Sélectionnez Create association (Créer une association), puis Close (Fermer). Le système tente de créer l'association sur les instances et applique immédiatement l'état.

> **Note**
>
> Si les EC2 instances de Windows Server affichent le statut Failed, vérifiez que l'SSMagent est en cours d'exécution sur l'instance et vérifiez que l'instance est configurée avec un rôle AWS Identity and Access Management (IAM) pour Systems Manager. Pour plus d'informations, consultez la section Configuration AWS Systems Manager.

AWS CLI

Vous pouvez exécuter la AWS CLI commande create-association pour mettre à jour un package de distributeur selon un calendrier sans mettre l'application associée hors ligne. Seuls les fichiers nouveaux ou mis à jour dans le package sont remplacés.

Pour créer une association State Manager à l'aide du AWS CLI

1. Installez et configurez le AWS CLI, si ce n'est pas déjà fait. Pour de plus amples informations, consultez Install or update the latest version of the AWS CLI.
2. Exécutez la commande suivante pour créer une association. La valeur de `--name`, le nom du document, est toujours `AWS-ConfigureAWSPackage`. La commande suivante utilise la clé `InstanceIds` pour spécifier les instances cibles.

```
aws ssm create-association \
--name "AWS-ConfigureAWSPackage" \
--parameters '{"action":["Install"],"installationType":["Uninstall and
 reinstall"],"name":["AwsVssComponents"]}' \
--targets [{\"Key\":\"InstanceIds\",\"Values\":[\"i-01234567890abcdef\",
\"i-000011112222abcde\"]}]
```

Pour plus d'informations sur les autres options que vous pouvez utiliser avec la `create-association` commande, voir create-association dans la AWS Systems Manager section de la référence des AWS CLI commandes.

Créez des EBS instantanés VSS basés sur votre instance EC2 Windows

Une fois que vous avez satisfait à toutes les Conditions requises pour créer des instantanés VSS basés sur EBS Windows exigences, vous pouvez utiliser l'une des méthodes suivantes pour créer des instantanés VSS basés sur votre EC2 instance.

AWS Systems Manager documents de commande

Utiliser les documents de commande de Systems Managerpour créer des instantanés VSS basés.

Pour automatiser les sauvegardes, vous pouvez créer une tâche de fenêtre de AWS Systems Manager maintenance qui utilise le document de `AWSEC2-VssInstallAndSnapshot` commande. Pour plus d'informations, consultez Utilisation des fenêtres de maintenance (console) dans le Guide de l'utilisateur AWS Systems Manager .

AWS Backup

Vous pouvez créer une VSS sauvegarde lors de l'utilisation VSS en AWS Backup activant dans la console ouCLI. Pour plus d'informations, consultez la section Création de VSS sauvegardes Windows dans le Guide du AWS Backup développeur.

> **Note**
>
> AWS Backup n'installe pas automatiquement le `AwsVssComponents` package sur votre instance. Vous devez effectuer une installation manuelle sur votre instance. Pour de plus amples informations, veuillez consulter Installation manuelle des VSS composants sur une instance EC2 Windows.

Amazon Data Lifecycle Manager

Vous pouvez créer des VSS instantanés à l'aide d'Amazon Data Lifecycle Manager en activant les scripts pré et post dans vos politiques de cycle de vie des instantanés. Pour plus d'informations, consultez Automatiser les instantanés cohérents avec les applications dans le guide de l'utilisateur Amazon. EBS

> **Note**
>
> Amazon Data Lifecycle Manager n'installe pas automatiquement le package `AwsVssComponents` sur votre instance. Vous devez effectuer une installation manuelle sur votre instance. Pour de plus amples informations, veuillez consulter Installation manuelle des VSS composants sur une instance EC2 Windows.

Utilisez les documents de commande de Systems Manager pour créer des instantanés VSS basés

Vous pouvez utiliser des documents de AWS Systems Manager commande pour créer des instantanés VSS basés. Le contenu suivant présente les documents de commande disponibles et les paramètres d'exécution utilisés par ces documents pour créer vos instantanés.

Avant d'utiliser l'un des documents de commande de Systems Manager, assurez-vous d'avoir respecté toutes les Conditions requises pour créer des instantanés VSS basés sur EBS Windows.

Rubriques

Paramètres des documents VSS instantanés de Systems Manager

Les documents Systems Manager qui créent des VSS instantanés utilisent tous les paramètres suivants, sauf indication contraire :

ExcludeBootVolume(chaîne, facultatif)

Ce paramètre exclut les volumes de démarrage du processus de sauvegarde si vous créez des instantanés. Pour exclure les volumes de démarrage de vos instantanés, définissez ExcludeBootVolumeles paramètres sur `True` et CreateAmisur`False`.

Si vous créez un AMI pour votre sauvegarde, ce paramètre doit être défini sur`False`. La valeur par défaut de ce paramètre est `False`.

NoWriters(chaîne, facultatif)

Pour exclure les VSS rédacteurs d'applications du processus de capture instantanée, définissez ce paramètre sur`True`. L'exclusion VSS des rédacteurs d'applications peut vous aider à résoudre les conflits avec des composants VSS de sauvegarde tiers. La valeur par défaut de ce paramètre est `False`.

CopyOnly(chaîne, facultatif)

Si vous utilisez en plus la sauvegarde native SQL du serveur AWS VSS, l'exécution d'une sauvegarde par copie uniquement AWS VSS empêche de rompre la chaîne de sauvegarde différentielle native. Pour effectuer une opération de sauvegarde par copie uniquement, définissez ce paramètre sur `True`.

La valeur par défaut de ce paramètre est`False`, ce qui AWS VSS entraîne l'exécution d'une opération de sauvegarde complète.

CreateAmi(chaîne, facultatif)

Pour créer une Amazon Machine Image (AMI) VSS basée sur laquelle sauvegarder votre instance, définissez ce paramètre sur`True`. La valeur par défaut de ce paramètre est`False`, qui sauvegarde votre instance avec un EBS instantané à la place.

Pour plus d'informations sur la création d'une instance AMI à partir d'une instance, consultezCréez un compte soutenu EBS par Amazon AMI.

AmiName(chaîne, facultatif)

Si l'CreateAmioption est définie sur`True`, spécifiez le nom du fichier AMI créé par la sauvegarde.

description : (chaîne, facultatif)

Spécifiez une description pour les instantanés ou les images créés par ce processus.

tags (chaîne, facultatif)

Nous vous recommandons de baliser vos instantanés et vos images pour vous aider à localiser et à gérer vos ressources, par exemple pour restaurer des volumes à partir d'une liste d'instantanés. Le système ajoute la `Name` clé, avec une valeur vide dans laquelle vous pouvez spécifier le nom que vous souhaitez appliquer à vos instantanés ou images de sortie.

Si vous souhaitez spécifier des balises supplémentaires, séparez-les par un point-virgule entre les deux. Par exemple, `Key=Environment,Value=Test;Key=User,Value=TestUser1`.

Par défaut, le système ajoute les balises réservées suivantes pour les instantanés et les images VSS basés.

- Appareil : pour les instantanés VSS basés, il s'agit du nom de périphérique du EBS volume capturé par l'instantané.
- AppConsistent— Cette balise indique la création réussie d'un instantané VSS basé ouAMI.
- AwsVssConfig— Cela identifie les instantanés et ceux AMIs qui sont créés avec cette VSS option activée. La balise inclut des méta-informations telles que la `AwsVssComponents` version.

> **Warning**
>
> La spécification de l'une de ces balises réservées dans votre liste de paramètres provoquera une erreur.

executionTimeout(chaîne, facultatif)

Spécifiez la durée maximale en secondes pour exécuter le processus de création d'un instantané sur l'instance ou pour en créer un à AMI partir de l'instance. L'augmentation de ce délai permet à la commande d'attendre plus longtemps avant de commencer VSS à geler et de terminer le

balisage des ressources qu'elle crée. Ce délai d'attente s'applique uniquement à l'instantané ou aux étapes AMI de création. L'étape initiale d'installation ou de mise à jour du package `AwsVssComponents` n'est pas incluse dans le délai d'expiration.

CollectDiagnosticLogs(chaîne, facultatif)

Pour collecter plus d'informations lors des étapes de capture d'écran et de AMI création, définissez ce paramètre sur « `True` ». La valeur par défaut de ce paramètre est « `False` ». Les journaux de diagnostic consolidés sont enregistrés sous `.zip` forme d'archive au format à l'emplacement suivant sur votre instance :

`C:\ProgramData\Amazon\AwsVss\Logs\`*`timestamp`*`.zip`

VssVersion(chaîne, facultatif)

Pour le document `AWSEC2-VssInstallAndSnapshot` uniquement, vous pouvez spécifier le paramètre `VssVersion` pour installer une version spécifique du package `AwsVssComponents` sur votre instance. Laissez ce paramètre vide pour installer la version par défaut recommandée.

Si la version spécifiée du package `AwsVssComponents` est déjà installée, le script ignore l'étape d'installation et passe à l'étape de sauvegarde. Pour obtenir la liste des versions de package `AwsVssComponents` et du support d'exploitation, consultez AWS VSShistorique des versions de la solution.

Exécutez les documents de commande de VSS capture instantanée de Systems Manager

Vous pouvez créer des EBS instantanés VSS basés sur des documents de AWS Systems Manager commande comme suit.

Exécuter le document VssInstallAndSnapshot de commande AWSEC2 - (recommandé)

Lorsque vous exécutez AWS Systems Manager le `AWSEC2-VssInstallAndSnapshot` document, le script exécute les étapes suivantes.

1. Le script commence par installer ou mettre à jour le package `AwsVssComponents` sur votre instance, selon qu'il est déjà installé ou non.
2. Le script crée les instantanés cohérents avec l'application une fois la première étape terminée.

Pour exécuter le document `AWSEC2-VssInstallAndSnapshot`, suivez les étapes correspondant à votre environnement préféré.

Console

Créez des EBS instantanés VSS basés sur la console

1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.
2. Dans le volet de navigation, sélectionnez Exécuter une commande. Cela permet d'afficher une liste des commandes en cours d'exécution dans votre compte, le cas échéant.
3. Sélectionnez Run Command (Exécuter la commande). Cela permet d'ouvrir la liste des documents de commande auxquels vous avez accès.
4. Sélectionnez `AWSEC2-VssInstallAndSnapshot` dans la liste des documents de commande. Pour rationaliser les résultats, vous pouvez saisir tout ou partie du nom du document. Vous pouvez également filtrer par propriétaire, par type de plateforme ou par balise.

   Lorsque vous sélectionnez un document de commande, les détails apparaissent sous la liste.
5. Sélectionnez `Default version at runtime` dans la liste Version du document.
6. Configurez les paramètres de commande pour définir comment `AWSEC2-VssInstallAndSnapshot` installer le `AwsVssComponents` package et le sauvegarder avec des VSS instantanés ou unAMI. Pour plus de détails sur les paramètres, veuillez consulter la rubrique Paramètres des documents VSS instantanés de Systems Manager.
7. Pour Sélection de la cible, spécifiez des balises ou sélectionnez des instances manuellement afin d'identifier les instances sur lesquelles vous souhaitez exécuter cette opération.

   > **Note**
   >
   > Si vous sélectionnez les instances manuellement et qu'une instance que vous vous attendez à voir ne figure pas dans la liste, consultez Où sont mes instances ? pour obtenir des conseils de résolution d'incident.
8. Pour des paramètres supplémentaires permettant de définir le comportement de Exécuter la commande Systems Manager, tels que Contrôle du débit, entrez des valeurs comme décrit dans Exécution des commande à partir de la console.
9. Cliquez sur Exécuter.

   En cas de succès, la commande remplit la liste des EBS instantanés avec les nouveaux instantanés. Vous pouvez localiser ces instantanés dans la liste des EBS instantanés en

recherchant les balises que vous avez spécifiées ou en recherchant. `AppConsistent` Si l'exécution de la commande a échoué, consultez la sortie de commande Systems Manager pour en connaître les raisons. Si la commande s'est correctement exécutée, mais qu'une sauvegarde de volume spécifique a échoué, vous pouvez résoudre le problème dans la liste des EBS volumes.

AWS CLI

Vous pouvez exécuter les commandes suivantes dans le AWS CLI pour créer des EBS instantanés VSS basés et obtenir l'état de la création de vos instantanés.

Créez des EBS instantanés VSS basés

Exécutez la commande suivante pour créer des EBS instantanés VSS basés. Pour créer les instantanés, vous devez identifier les instances à l'aide du paramètre `--instance-ids`. Pour plus d'informations sur les autres paramètres que vous pouvez utiliser, veuillez consulter la rubrique Paramètres des documents VSS instantanés de Systems Manager.

```
aws ssm send-command \
 --document-name "AWSEC2-VssInstallAndSnapshot" \
 --instance-ids "i-01234567890abcdef" \
 --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":
["Key=key_name,Value=tag_value"],"VssVersion":[""]}'
```

En cas de succès, le document de commande remplit la liste des EBS instantanés avec les nouveaux instantanés. Vous pouvez localiser ces instantanés dans la liste des EBS instantanés en recherchant les balises que vous avez spécifiées ou en recherchant. `AppConsistent` Si l'exécution de la commande a échoué, consultez la sortie de commande pour en connaître les raisons.

Obtenir le statut de la commande

Pour obtenir l'état actuel des instantanés, exécutez la commande suivante à l'aide de l'ID de commande renvoyé par send-command.

```
aws ssm get-command-invocation
 --instance-ids "i-01234567890abcdef" \
 --command-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
 --plugin-name "CreateVssSnapshot"
```

PowerShell

Exécutez les commandes suivantes AWS Tools for Windows PowerShell pour créer des EBS instantanés VSS basés et obtenir l'état d'exécution actuel pour la création de votre sortie. Spécifiez les paramètres décrits dans la liste précédente pour modifier le comportement du processus de capture instantanée.

Créez des EBS instantanés VSS basés sur Tools for Windows PowerShell

Exécutez la commande suivante pour créer des EBS instantanés VSS basés sur. AMIs

```
Send-SSMCommand -DocumentName "AWSEC2-VssInstallAndSnapshot" -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'ExcludeBootVolume'='False';'description'='a_description'
 ;'tags'='Key=key_name,Value=tag_value';'VssVersion'=''}
```

Obtenir le statut de la commande

Pour obtenir l'état actuel des instantanés, exécutez la commande suivante à l'aide de l'ID de commande renvoyé par Send-SSMCommand.

```
Get-SSMCommandInvocationDetail -InstanceId "i-01234567890abcdef" -CommandId
 "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" -PluginName "CreateVssSnapshot"
```

En cas de succès, la commande remplit la liste des EBS instantanés avec les nouveaux instantanés. Vous pouvez localiser ces instantanés dans la liste des EBS instantanés en recherchant les balises que vous avez spécifiées ou en recherchant. `AppConsistent` Si l'exécution de la commande a échoué, consultez la sortie de commande pour en connaître les raisons.

Exécutez le document de CreateVssSnapshot commande à AWSEC 2

Pour exécuter le document `AWSEC2-CreateVssSnapshot`, suivez les étapes correspondant à votre environnement préféré.

Console

Créez des EBS instantanés VSS basés sur la console

1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.

2. Dans le volet de navigation, sélectionnez Exécuter une commande. Cela permet d'afficher une liste des commandes en cours d'exécution dans votre compte, le cas échéant.
3. Sélectionnez Run Command (Exécuter la commande). Cela permet d'ouvrir la liste des documents de commande auxquels vous avez accès.
4. Sélectionnez `AWSEC2-CreateVssSnapshot` dans la liste des documents de commande. Pour rationaliser les résultats, vous pouvez saisir tout ou partie du nom du document. Vous pouvez également filtrer par propriétaire, par type de plateforme ou par balise.

   Lorsque vous sélectionnez un document de commande, les détails apparaissent sous la liste.
5. Sélectionnez `Default version at runtime` dans la liste Version du document.
6. Configurez les paramètres de commande pour définir le mode de `AWSEC2-CreateVssSnapshot` sauvegarde à l'aide de VSS snapshots ou d'unAMI. Pour plus de détails sur les paramètres, veuillez consulter la rubrique Paramètres des documents VSS instantanés de Systems Manager.
7. Pour Sélection de la cible, spécifiez des balises ou sélectionnez des instances manuellement afin d'identifier les instances sur lesquelles vous souhaitez exécuter cette opération.

   > **Note**
   >
   > Si vous sélectionnez les instances manuellement et qu'une instance que vous vous attendez à voir ne figure pas dans la liste, consultez Où sont mes instances ? pour obtenir des conseils de résolution d'incident.
8. Pour des paramètres supplémentaires permettant de définir le comportement de Exécuter la commande Systems Manager, tels que Contrôle du débit, entrez des valeurs comme décrit dans Exécution des commande à partir de la console.
9. Cliquez sur Exécuter.

   En cas de succès, la commande remplit la liste des EBS instantanés avec les nouveaux instantanés. Vous pouvez localiser ces instantanés dans la liste des EBS instantanés en recherchant les balises que vous avez spécifiées ou en recherchant. `AppConsistent` Si l'exécution de la commande a échoué, consultez la sortie de commande Systems Manager pour en connaître les raisons. Si la commande s'est correctement exécutée, mais qu'une sauvegarde de volume spécifique a échoué, vous pouvez résoudre le problème dans la liste des EBS volumes.

AWS CLI

Vous pouvez exécuter la commande suivante dans le AWS CLI pour créer des EBS instantanés VSS basés.

Créez des EBS instantanés VSS basés

Exécutez la commande suivante pour créer des EBS instantanés VSS basés. Pour créer les instantanés, vous devez identifier les instances à l'aide du paramètre `--instance-ids`. Pour plus d'informations sur les autres paramètres que vous pouvez utiliser, veuillez consulter la rubrique Paramètres des documents VSS instantanés de Systems Manager.

```
aws ssm send-command \
 --document-name "AWSEC2-CreateVssSnapshot" \
 --instance-ids "i-01234567890abcdef" \
 --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":
["Key=key_name,Value=tag_value"]}'
```

En cas de succès, le document de commande remplit la liste des EBS instantanés avec les nouveaux instantanés. Vous pouvez localiser ces instantanés dans la liste des EBS instantanés en recherchant les balises que vous avez spécifiées ou en recherchant. `AppConsistent` Si l'exécution de la commande a échoué, consultez la sortie de commande pour en connaître les raisons.

PowerShell

Exécutez la commande suivante avec AWS Tools for Windows PowerShell pour créer des EBS instantanés VSS basés.

Créez des EBS instantanés VSS basés sur Tools for Windows PowerShell

Exécutez la commande suivante pour créer des EBS instantanés VSS basés. Pour créer les instantanés, vous devez identifier les instances à l'aide du paramètre `InstanceId`. Vous pouvez spécifier plusieurs instances pour lesquelles créer des instantanés. Pour plus d'informations sur les autres paramètres que vous pouvez utiliser, veuillez consulter la rubrique Paramètres des documents VSS instantanés de Systems Manager.

```
Send-SSMCommand -DocumentName AWSEC2-CreateVssSnapshot -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'ExcludeBootVolume'='False';'description'='a_description'
```

```
;'tags'='Key=key_name,Value=tag_value'}
```

En cas de succès, la commande remplit la liste des EBS instantanés avec les nouveaux instantanés. Vous pouvez localiser ces instantanés dans la liste des EBS instantanés en recherchant les balises que vous avez spécifiées ou en recherchant. `AppConsistent` Si l'exécution de la commande a échoué, consultez la sortie de commande pour en connaître les raisons. Si la commande s'est correctement exécutée, mais qu'une sauvegarde de volume spécifique a échoué, vous pouvez résoudre le problème dans la liste des EBS instantanés.

Exécuter des documents de commande pour un cluster Windows Failover avec stockage partagé EBS

Vous pouvez utiliser l'une des procédures de ligne de commande décrites dans la section précédente pour créer un instantané VSS basé sur un instantané. Le document de commande (`AWSEC2-VssInstallAndSnapshot` ou `AWSEC2-CreateVssSnapshot`) doit être exécuté sur le nœud primaire de votre cluster. Le document échoue sur les nœuds secondaires, car ils n'ont pas accès aux disques partagés. Si vos paramètres principal et secondaire changent de manière dynamique, vous pouvez exécuter le document AWS Systems Manager Exécuter la commande sur plusieurs nœuds en espérant que la commande réussira sur le nœud principal et échouera sur les nœuds secondaires.

> **Note**
>
> Pour automatiser les sauvegardes, vous pouvez créer une tâche de fenêtre de AWS Systems Manager maintenance qui utilise le `AWSEC2-VssInstallAndSnapshot` document. Pour plus d'informations, consultez Utilisation des fenêtres de maintenance (console) dans le Guide de l'utilisateur AWS Systems Manager .

Résoudre les problèmes liés aux instantanés VSS basés sur EBS Windows

Avant d'essayer d'autres étapes de résolution des problèmes, nous vous recommandons de vérifier les informations suivantes.

- Assurez-vous d'avoir respecté toutes les Conditions requises pour créer des instantanés VSS basés sur EBS Windows.
- Vérifiez que vous utilisez la dernière version de Prise en charge de la version du système d'exploitation Windows du package `AwsVssComponents` correspondant à votre système

d'exploitation. Le problème que vous avez observé a peut-être été résolu dans les versions plus récentes.

Rubriques

Vérifier les fichiers journaux

Si vous rencontrez des problèmes ou recevez des messages d'erreur lorsque vous créez des EBS instantanés VSS basés, vous pouvez consulter le résultat de la commande dans la console Systems Manager.

Pour les documents Systems Manager qui créent des VSS instantanés, vous pouvez définir le `CollectDiagnosticLogs` paramètre sur « `True` » lors de l'exécution. Lorsque le `CollectDiagnosticLogs` paramètre est défini sur `True` « », VSS collecte des journaux supplémentaires pour faciliter le débogage. Pour de plus amples informations, veuillez consulter Collectez des journaux de diagnostic supplémentaires.

Si vous collectez des journaux de diagnostic, le document Systems Manager les stocke sur votre instance à l'emplacement suivant : `C:\ProgramData\Amazon\AwsVss\Logs\`*`timestamp`*`.zip` La valeur par défaut du `CollectDiagnosticLogs` paramètre est « `False` ».

> **Note**
>
> Pour obtenir de l'aide supplémentaire pour le débogage, vous pouvez envoyer le `.zip` fichier à AWS Support.

Les journaux supplémentaires suivants sont disponibles, que vous recueilliez des journaux de diagnostic ou non :

- `%ProgramData%\Amazon\SSM\InstanceData\`*`InstanceID`*`\document\orchestration\`*`SSMCommandID`*`\awsrunPowerShellScript\runPowerShellScript\stdout`
- `%ProgramData%\Amazon\SSM\InstanceData\`*`InstanceID`*`\document\orchestration\`*`SSMCommandID`*`\awsrunPowerShellScript\runPowerShellScript\stderr`

Vous pouvez également ouvrir l'application Observateur d'événements de Windows et sélectionner Journaux Windows, Application pour afficher les journaux supplémentaires. Pour voir les événements provenant spécifiquement du VSS fournisseur EC2 Windows et du service Volume Shadow Copy, filtrez par source selon les termes **`Ec2VssSoftwareProvider`** et**`VSS`**.

Si vous utilisez Systems Manager avec des VPC points de terminaison et que l'SendCommandAPIaction Systems Manager (Exécuter la commande dans la console) a échoué, vérifiez que vous avez correctement configuré le point de terminaison suivant : com.amazonaws.***`region`***.ec2.

Si le point de EC2 terminaison Amazon n'est pas défini, l'appel pour énumérer les EBS volumes attachés échoue, ce qui entraîne l'échec de la commande Systems Manager. Pour plus d'informations sur la configuration des VPC points de terminaison avec Systems Manager, voir Create a Virtual Private Cloud Endpoint dans le guide de l'AWS Systems Manager utilisateur.

Collectez des journaux de diagnostic supplémentaires

Pour collecter des journaux de diagnostic supplémentaires lorsque vous utilisez la commande d'envoi de Systems Manager pour exécuter le document VSS instantané, définissez le paramètre `CollectDiagnosticLogs` d'entrée sur « `True` » lors de l'exécution. Nous vous recommandons de définir ce paramètre sur « `True` » lors de la résolution des problèmes.

Pour voir un exemple de ligne de commande, sélectionnez l'un des onglets suivants.

AWS CLI

L'exemple suivant exécute le document `AWSEC2-CreateVssSnapshot` Systems Manager dans le AWS CLI :

```
aws ssm send-command \
--document-name "AWSEC2-CreateVssSnapshot" \
--instance-ids "i-1234567890abcdef0" \
```

```
--parameters '{"description":["Example - create diagnostic logs at
 runtime."],"tags":["Key=tag_name,Value=tag_value"],"CollectDiagnosticLogs":
["True"]}'
```

PowerShell

L'exemple suivant exécute le document `AWSEC2-CreateVssSnapshot` Systems Manager dans PowerShell :

```
Send-SSMCommand -DocumentName AWSEC2-CreateVssSnapshot -InstanceId
 "i-1234567890abcdef0" -Parameter @{'description'='Example - create diagnostic logs
 at runtime.';'tags'='Key=tag_name,Value=tag_value';'CollectDiagnosticLogs'='True'}
```

Utilisation VSS sur des instances avec un proxy configuré

Si vous rencontrez des problèmes lors de la création de EBS snapshots VSS basés sur des instances qui utilisent un proxy pour atteindre les EC2 points de terminaison, vérifiez les paramètres suivants sur votre instance :

- Vérifiez que le proxy est configuré de manière à ce que les points de terminaison du EC2 service situés dans la région de l'instance IMDS soient accessibles en AWS Tools for Windows PowerShell exécutant sous SYSTEM le nom de.
- Pour prendre en charge l'utilisation du HTTP proxy Win configuré par le système, assurez-vous d'avoir installé la dernière `AwsVssComponents` version sur votre instance. Pour plus d'informations sur la configuration du HTTP proxy Win, consultez la section Commandes Netsh pour le protocole de transfert hypertexte Windows (WINHTTP) sur le site Web de Microsoft.

Erreur : le délai de connexion au canal de dégel a expiré, erreur lors du dégel, délai d'attente pour le VSS gel ou autres erreurs de délai

Le VSS fournisseur EC2 Windows peut expirer en raison d'une activité ou de services sur l'instance empêchant le traitement des instantanés VSS basés dans les délais impartis. Le Windows VSS Framework fournit une fenêtre non configurable de 10 secondes pendant laquelle la communication avec le système de fichiers est interrompue. Pendant ce temps, `AWSEC2-CreateVssSnapshot` crée des instantanés de vos volumes.

Les problèmes suivants peuvent faire en sorte que le VSS fournisseur EC2 Windows se heurte à des limites de temps lors d'un instantané :

- I/O excessives vers un volume
- Faible réactivité de EC2 API l'instance
- Volumes fragmentés
- Incompatibilité avec certains logiciels antivirus
- Problèmes avec un rédacteur VSS d'applications
- Lorsque la journalisation des modules est activée pour un grand nombre de PowerShell modules, cela peut entraîner un ralentissement de l'exécution PowerShell des scripts

La plupart des délais d'expiration qui se produisent lorsque vous exécutez le document de commande `AWSEC2-CreateVssSnapshot` sont liés au fait que la charge de travail sur l'instance est trop élevée au moment de la sauvegarde. Pour vous aider à créer un instantané avec succès, vous pouvez procéder comme suit :

- Réessayez la commande `AWSEC2-CreateVssSnapshot` pour voir si la tentative d'instantané réussit. Si une nouvelle tentative réussit dans certains cas, la réduction de la charge de l'instance peut favoriser la réussite des instantanés.
- Patientez le temps que la charge globale sur l'instance diminue, puis réessayez la commande `AWSEC2-CreateVssSnapshot`. Vous pouvez également essayer des instantanés lorsque vous savez que l'instance est soumise à une faible contrainte.
- Essayez de VSS créer des instantanés lorsque le logiciel antivirus du système est éteint. Si cela résout le problème, reportez-vous aux instructions du logiciel antivirus et configurez-le pour autoriser les VSS instantanés.
- S'il y a un volume élevé d'EC2APIappels Amazon sur votre compte dans la même région que celle où vous exécutez un instantané, la API limitation peut retarder les opérations de capture instantanée. Pour réduire l'impact de la régulation, utilisez le package le plus récent`AwsVssComponents`. Ce package utilise cette EC2 `CreateSnapshots` API action pour réduire le nombre d'actions mutantes telles que la création et le balisage d'instantanés par volume.
- Si plusieurs scripts de commande `AWSEC2-CreateVssSnapshot` s'exécutent en même temps, vous pouvez suivre les étapes suivantes pour réduire les problèmes de simultanéité.
  - Envisagez de planifier des instantanés pendant les périodes de faible API activité.
  - Si vous exécutez le script de commande Run Command dans la console Systems Manager (ou SendCommand dans leAPI), vous pouvez utiliser les contrôles de débit de Systems Manager pour réduire la simultanéité.

Vous pouvez également utiliser les contrôles de débit de Systems Manager pour réduire la simultanéité des services tels AWS Backup que ceux qui utilisent Systems Manager pour exécuter le script de commande.

- Exécutez la commande `vssadmin list writers` dans un shell et voyez si celle-ci signale des erreurs dans le champ Last error pour tous les enregistreurs sur le système. Si des enregistreurs signalent une erreur time out, vous pouvez éventuellement réessayer de créer des instantanés lorsque l'instance sera moins chargée.
- Lorsque vous utilisez des types d'instances plus petits tels que *t2 | t3 | t3a*.nano ou *t2 | t3 | t3a*.micro, des délais d'attente dus à la mémoire et à des CPU contraintes peuvent survenir. Les actions suivantes peuvent contribuer à réduire les problèmes de délai d'expiration.
  - Essayez de fermer la mémoire ou de fermer les applications CPU intensives avant de prendre des instantanés.
  - Essayez de prendre des instantanés pendant les périodes de faible activité de l'instance.

Erreur : impossible d'invoquer la méthode. L'invocation de méthodes n'est prise en charge que sur les types principaux dans ce mode de langue.

Vous rencontrerez cette erreur lorsque le mode de PowerShell langue n'est pas défini sur`FullLanguage`. Le `AWSEC2-CreateVssSnapshot` SSM document doit PowerShell être configuré en `FullLanguage` mode.

Pour vérifier le mode de langue, exécutez la commande suivante sur l'instance dans une PowerShell console :

```
$ExecutionContext.SessionState.LanguageMode
```

Pour plus d'informations sur les modes de langue, veuillez consulter la rubrique about_Language_Modes dans la documentation Microsoft.

Restaurez EBS des volumes pour votre instance Windows à partir de snapshots VSS basés

Vous pouvez utiliser le `RestoreVssSnapshotSampleScript.ps1` script pour restaurer des volumes sur une instance à partir de EBS snapshots VSS basés sur des instantanés. Ce script effectue les tâches suivantes :

- Arrête une instance
- Supprime tous les disques existants de l'instance (à l'exception du volume de démarrage, s'il a été exclu)
- Crée de nouveaux volumes à partir des instantanés
- Attache les volumes à l'instance en utilisant la balise d'ID de périphérique sur l'instantané
- Redémarre l'instance

> **Important**
>
> Le script suivant détache tous les volumes attachés à une instance, puis crée de nouveaux volumes à partir d'un instantané. Vérifiez que vous avez correctement sauvegardé l'instance. Les anciens volumes ne sont pas supprimés. Si vous le souhaitez, vous pouvez modifier le script afin de supprimer les anciens volumes.

Pour restaurer des volumes à partir de EBS snapshots VSS basés

1. Téléchargez le fichier RestoreVssSnapshotSampleScript.zip et extrayez le contenu du fichier.
2. Ouvrez `RestoreVssSnapshotSampleScript.ps1` dans un éditeur de texte et modifiez l'exemple d'appel au bas du script avec un ID d'EC2instance et un ID de EBS capture valides, puis exécutez le script depuis PowerShell.

AWS VSShistorique des versions de la solution

Cette page inclut les notes de mise à jour par version pour le package de AWS VSS composants, ainsi que les exigences de version des composants et des scripts pour chaque version prise en charge de Windows Server.

Rubriques

- AwsVssComponents versions du package
- Prise en charge de la version du système d'exploitation Windows

AwsVssComponents versions du package

Le tableau suivant décrit les versions publiées du package de AWS VSS composants.

Version	Détails	Date de publication
2.3.3	L'VSSagent a été mis à jour pour garantir qu'il `Ec2VssProvider` est utilisé lors de la création du snapshot.	25 juin 2024
2.3.2	Correction d'un cas où l'enregistrement du VSS fournisseur n'était pas supprimé lors de la désinstallation.	9 mai 2024
2.3.1	Ajout d'une nouvelle balise par défaut `AwsVssConfig` pour identifier les instantanés et AMIs créée par AWS VSS.	7 mars 2024
2.2.1	• Ajout de la prise en charge de l'utilisation du `DescribeInstanceAttribute` API. • Correctifs de bogues et améliorations de fiabilité. • Support obsolète pour Windows Server 2012 et 2012 R2. AWS VSSL'installation des composants version 2.2.1 sur Windows Server 2012 et 2012 R2 échouera. AWS VSSLa version 2.1.0 des composants est la dernière version compatible avec Windows Server 2012 et 2012 R2.	18 janvier 2024
2.1.0	Ajout de la prise en charge de l'utilisation du `CreateSnapshots` API.	6 novembre 2023
2.0.1	Ajout de la prise en charge de l'utilisation des paramètres de HTTP proxy Win.	26 octobre 2023
2.0.0	Possibilité ajoutée au AWS VSS composant de créer des instantanésAMIs, ce qui permet la compatibilité avec les fonctionnalités de journalisation des PowerShell modules, de journalisation par blocs de scripts et de transcription.	28 avril 2023

Version	Détails	Date de publication
1.3.2.0	Correction d'un cas où l'échec de l'installation n'était pas signalé correctement.	10 mai 2022
1.3.1.0	• Correction d'un échec des snapshots sur les contrôleurs de domaine en raison d'une erreur de journalisation du NTDS VSS rédacteur. • Correction d'une erreur d'VSSagent lors de la désinstallation du VSS fournisseur de la version 1.0.	6 février 2020
1.3.00	• Amélioration de la journalisation par la réduction du niveau de détail indésirable. • Correction des problèmes de régionalisation lors de l'install ation. • Correction des codes de retour pour certaines conditions d'erreur d'enregistrement du fournisseur. • Correction de divers problèmes d'installation.	19 mars 2019
1.2.00	• Ajout de paramètres de ligne de commande `-nw` (no-writers) et `-copy` (copy-only) à l'agent. • Correction EventLog d'erreurs causées par des appels d'allocation de mémoire incorrects.	le 15 novembre 2018
1.1	AWS VSSComposants corrigés qui n'étaient pas utilisés correctement en tant que fournisseur Windows Backup and Restore par défaut.	12 décembre 2017

Version	Détails	Date de publication
1.0	Première version.	le 20 novembre 2017

Prise en charge de la version du système d'exploitation Windows

Le tableau suivant indique les versions de AWS VSS solution que vous devez exécuter sur chaque version de Windows Server sur AmazonEC2.

Version Windows Server	AwsVssComponents version	AWSEC2-nom de VssInstallAndSnapshot version	AWSEC2-nom de CreateVssSnapshot version
Windows Server 2022	default	default	default
Windows Server 2019	default	default	default
Windows Server 2016	default	default	default
Windows Ser	2.1.0	non pris en charge	2012R2
Windows Server 2012	2.1.0	non pris en charge	2012R2
Windows Ser	1.3.1.0	non pris en charge	2008R2

Stockage d'objets, stockage de fichiers et mise en cache de fichiers sur Amazon EC2

Le stockage de fichiers dans le cloud est une méthode de stockage des données dans le cloud qui permet aux serveurs et aux applications d'accéder aux données via des systèmes de fichiers partagés. Cette compatibilité rend le stockage de fichiers dans le cloud idéal pour les charges de travail reposant sur des systèmes de fichiers partagés et offre une intégration simple sans modification de code.

Il existe de nombreuses solutions de stockage de fichiers, allant d'un serveur de fichiers à nœud unique sur une instance de calcul utilisant le stockage par blocs comme base, sans évolutivité ou peu de redondances pour protéger les données, à une solution en do-it-yourself cluster ou à une solution entièrement gérée. Le contenu suivant présente certains des services de stockage fournis AWS pour une utilisation avec les EC2 instances Amazon.

Table des matières

Utiliser Amazon S3 avec des EC2 instances Amazon

Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets qui offre une évolutivité, une disponibilité des données, une sécurité et des performances de pointe. Vous pouvez utiliser Amazon S3 pour stocker et récupérer n'importe quelle quantité de données pour différents cas d'utilisation, tels que les lacs de données, les sites Web, les sauvegardes et les analyses de mégadonnées, à partir d'une EC2 instance Amazon ou de n'importe où sur Internet. Pour plus d'informations, consultez Qu'est-ce qu'Amazon S3 ?

Les objets sont les entités fondamentales stockées dans Amazon S3. Chaque objet stocké dans Amazon S3 se trouve dans un compartiment. Les compartiments organisent l'espace de noms Amazon S3 au plus haut niveau et identifient le compte qui assure ce stockage. Les compartiments Amazon S3 sont similaires aux noms de domaine Internet. Les objets stockés dans les compartiments ont une valeur clé unique et sont récupérés à l'aide d'unURL. Par exemple, si un objet avec une valeur clé `/photos/mygarden.jpg` est stocké dans le `amzn-`

`s3-demo-bucket1` compartiment, il est adressable à l'aide du URL`https://amzn-s3-demo-bucket1.s3.amazonaws.com/photos/mygarden.jpg`. Pour plus d'informations, consultez Comment fonctionne Amazon S3.

Exemples d'utilisation :

Compte tenu des avantages d'Amazon S3 en matière de stockage, vous pouvez décider d'utiliser ce service pour stocker des fichiers et des ensembles de données destinés à être utilisés avec des EC2 instances. Vous pouvez déplacer des données entre Amazon S3 et vos instances de différentes façons. En plus des exemples présentés ci-après, vous pouvez utiliser de nombreux outils conçus par des utilisateurs pour accéder à vos données dans Amazon S3 depuis votre ordinateur ou votre instance. Certains des plus courants sont présentés dans les forums AWS .

Si vous y êtes autorisé, vous pouvez copier un fichier vers ou depuis Amazon S3 et votre instance en utilisant l'une des méthodes suivantes.

GET or wget (Linux)

> **Note**
>
> Cette méthode ne fonctionne que pour les objets publics. Si l'objet n'est pas public, vous recevez un message `ERROR 403: Forbidden`. Si vous recevez cette erreur, vous devez utiliser la console Amazon S3, AWS CLI, AWS API, AWS SDK, ou AWS Tools for Windows PowerShell, et vous devez disposer des autorisations requises. Pour plus d'informations, consultez Identity and Access Management dans Amazon S3 et Téléchargement d'un objet dans le Guide de l'utilisateur Amazon S3.

L'wgetutilitaire est un FTP client HTTP et qui vous permet de télécharger des objets publics depuis Amazon S3. Il est installé par défaut dans Amazon Linux et la plupart des autres distributions, et est disponible en téléchargement sur Windows. Pour télécharger un objet Amazon S3, utilisez la commande suivante en remplaçant URL l'objet à télécharger.

```
[ec2-user ~]$ wget https://my_bucket.s3.amazonaws.com/path-to-file
```

AWS Tools for Windows PowerShell (Windows)

Les instances Windows bénéficient d'un navigateur graphique que vous pouvez utiliser pour accéder directement à la console Amazon S3. Toutefois, dans le cadre du scripting, les

utilisateurs Windows peuvent également utiliser AWS Tools for Windows PowerShell pour déplacer les objets depuis et vers Amazon S3.

Utilisez la commande suivante pour copier un objet Amazon S3 vers votre instance Windows.

```
PS C:\> Copy-S3Object -BucketName my_bucket -Key path-to-file -
LocalFile my_copied_file.ext
```

AWS CLI (Linux and Windows)

Le AWS Command Line Interface (AWS CLI) est un outil unifié permettant de gérer vos AWS services. AWS CLI permet aux utilisateurs de s'authentifier et de télécharger des éléments restreints depuis Amazon S3, et également de charger des éléments. Pour plus d'informations notamment sur l'installation et la configuration des outils, consultez la page détaillée sur l'AWS Command Line Interface.

La commande aws s3 cp est similaire à la commande Unix cp. Vous pouvez copier des fichiers depuis Amazon S3 vers votre instance, copier des fichiers depuis votre instance vers Amazon S3 et même copier des fichiers d'un emplacement Amazon S3 vers un autre.

Utilisez la commande suivante pour copier un objet depuis Amazon S3 vers votre instance.

```
aws s3 cp s3://my_bucket/my_folder/my_file.ext my_copied_file.ext
```

Utilisez la commande suivante pour copier un objet depuis votre instance vers Amazon S3.

```
aws s3 cp my_copied_file.ext s3://my_bucket/my_folder/my_file.ext
```

La commande aws s3 sync peut synchroniser un compartiment Amazon S3 entier vers un répertoire local. Cela peut être utile pour télécharger un ensemble de données et conserver la copie locale up-to-date avec la télécommande. Si vous disposez des autorisations adéquates sur le compartiment Amazon S3, vous pouvez renvoyer votre répertoire local sur le cloud lorsque vous avez terminé, en inversant les emplacements source et de destination dans la commande.

Utilisez la commande suivante pour télécharger un bucket Amazon S3 entier vers un répertoire local sur votre instance.

```
aws s3 sync s3://remote_S3_bucket local_directory
```

Amazon S3 API

Si vous êtes développeur, vous pouvez utiliser un API pour accéder aux données d'Amazon S3. Vous pouvez l'utiliser API pour développer votre application et l'intégrer à d'autres APIs etSDKs. Pour plus d'informations, consultez les exemples de code pour Amazon S3 utilisés AWS SDKs dans le guide de l'utilisateur Amazon S3.

Utiliser Amazon EFS avec des instances Amazon EC2 Linux

> **Note**
>
> Amazon n'EFSest pas pris en charge sur les instances Windows.

Amazon EFS fournit un stockage de fichiers évolutif à utiliser avec AmazonEC2. Vous pouvez utiliser un système de EFS fichiers comme source de données commune pour les charges de travail et les applications exécutées sur plusieurs instances. Pour en savoir plus, consultez la page produit d'Amazon Elastic File System.

Ce didacticiel explique comment créer et joindre un système de EFS fichiers Amazon à l'aide de l'assistant Amazon EFS Quick Create lors du lancement de l'instance. Pour un didacticiel sur la création d'un système de fichiers à l'aide de la EFS console Amazon, consultez Getting started with Amazon Elastic File System dans le manuel Amazon Elastic File System User Guide.

> **Note**
>
> Lorsque vous créez un système de EFS fichiers à l'aide de EFS Quick Create, le système de fichiers est créé avec les paramètres recommandés par le service suivants :
>
> - Sauvegardes automatiques activées.
> - Montez les cibles dans chaque sous-réseau par défaut du sous-réseau sélectionnéVPC.
> - Mode de performance à usage général.
> - Mode de débit exceptionnel.
> - Le chiffrement des données au repos est activé à l'aide de votre clé par défaut pour Amazon EFS (`aws/elasticfilesystem`).
> - La gestion EFS du cycle de vie d'Amazon est activée avec une politique de 30 jours.

Tâches

- Création d'un système de EFS fichiers à l'aide d'Amazon EFS Quick Create
- Testez le système EFS de fichiers
- Supprimer le système EFS de fichiers

Création d'un système de EFS fichiers à l'aide d'Amazon EFS Quick Create

Vous pouvez créer un système de EFS fichiers et le monter sur votre instance lorsque vous lancez votre instance à l'aide de la fonction Amazon EFS Quick Create de l'assistant de EC2 lancement d'instance Amazon.

Pour créer un système de EFS fichiers à l'aide d'Amazon EFS Quick Create

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Sélectionnez Launch instance (Lancer une instance).
3. (Facultatif) Sous Name and tags (Noms et identifications), pour Name (Nom), saisissez un nom pour identifier votre instance.
4. Sous Images de l'application et du système d'exploitation (Amazon Machine Image), choisissez un système d'exploitation Linux, puis pour Amazon Machine Image (AMI), sélectionnez un LinuxAMI.
5. Sous Instance type (Type d'instance), pour Instance type (Type d'instance), sélectionnez un type d'instance ou conservez la valeur par défaut.
6. Sous Key pair (login) (Paire de clés (connexion)), pour Key pair name (Nom de la paire de clés), choisissez une paire de clés existante ou créez-en une.
7. Sous Network settings (Paramètres réseau), choisissez Edit (Modifier) (à droite), puis pour Subnet (Sous-réseau), sélectionnez un sous-réseau.

   > **Note**
   >
   > Vous devez sélectionner un sous-réseau avant de pouvoir ajouter un système de EFS fichiers.

8. Sous Configure storage (Configurer le stockage), choisissez Edit (Modifier) (en bas à droite), puis procédez comme suit :

a. Pour les systèmes de fichiers, assurez-vous que cette option EFSest sélectionnée, puis choisissez Créer un nouveau système de fichiers partagé.

b. Dans Nom du système de fichiers, entrez le nom du système de EFS fichiers Amazon, puis choisissez Create file system.

c. Pour Point de montage, spécifiez un point de montage personnalisé ou conservez le point de montage par défaut.

d. Pour permettre l'accès au système de fichiers, sélectionnez Automatically create and attach security groups (Créer et attacher automatiquement des groupes de sécurité). En cochant cette case, les groupes de sécurité suivants seront automatiquement créés et attachés à l'instance et aux cibles de montage du système de fichiers :

   - Groupe de sécurité d'instance : inclut une règle sortante qui autorise le trafic sur le NFS port 2049, mais n'inclut aucune règle entrante.
   - Le montage du système de fichiers cible le groupe de sécurité : inclut une règle entrante qui autorise le trafic via le port NFS 2049 depuis le groupe de sécurité d'instance (décrit ci-dessus), et une règle sortante qui autorise le trafic via le NFS port 2049.

   > **Note**
   >
   > Vous pouvez également créer et associer manuellement les groupes de sécurité. Si vous voulez créer et attacher manuellement les groupes de sécurité, décochez la case Automatically create and attach the required security groups (Créer et attacher automatiquement les groupes de sécurité requis).

e. Pour monter automatiquement le système de fichiers partagé lors du lancement de l'instance, sélectionnez Automatically mount shared file system by attaching required user data script (Monter automatiquement le système de fichiers partagé en attachant le script de données utilisateur requis). Pour afficher les données utilisateur générées automatiquement, développez Advanced details (Détails avancés), puis faites défiler vers le bas jusqu'à User data (Données utilisateur).

> **Note**
>
> Si vous avez ajouté des données utilisateur avant de cocher cette case, les données utilisateur d'origine sont remplacées par les données utilisateur générées automatiquement.

9. Configurez les autres paramètres de configuration de l'instance si nécessaire.
10. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance). Pour plus d'informations, consultez Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console.

Testez le système EFS de fichiers

Vous pouvez vous connecter à votre instance et vérifier que le système de fichiers est bien monté dans le répertoire que vous avez indiqué (par exemple, /mnt/efs).

Pour vérifier que le système de fichiers est bien monté

1. Connectez-vous à votre instance. Pour plus d'informations, consultez Connectez-vous à votre instance Linux à l'aide de SSH.
2. Dans la fenêtre du terminal de l'instance, exécutez la df -T commande pour vérifier que le système de EFS fichiers est monté.

```
$ df -T
Filesystem     Type              1K-blocks    Used          Available Use% Mounted
 on
/dev/xvda1     ext4                8123812 1949800            6073764  25% /
devtmpfs       devtmpfs            4078468      56            4078412   1% /dev
tmpfs          tmpfs               4089312       0            4089312   0% /dev/shm
efs-dns        nfs4       9007199254740992       0   9007199254740992   0% /mnt/efs
```

   Notez que le nom du système de fichiers, indiqué dans l'exemple de sortie sous la forme *efs-dns*, se présente sous la forme suivante.

```
file-system-id.efs.aws-region.amazonaws.com:/
```

3. (Facultatif) Créez un fichier dans le système de fichiers à partir de l'instance, et vérifiez ensuite que vous pouvez consulter ce fichier à partir d'une autre instance.

a. Depuis l'instance, exécutez la commande suivante pour créer le fichier.

```
$ sudo touch /mnt/efs/test-file.txt
```

b. Depuis l'autre instance, exécutez la commande suivante pour afficher le fichier.

```
$ ls /mnt/efs
test-file.txt
```

Supprimer le système EFS de fichiers

Si vous n'avez plus besoin de votre système de fichiers, vous pouvez le supprimer.

Pour supprimer le système de fichiers

1. Ouvrez la console Amazon Elastic File System à l'adresse https://console.aws.amazon.com/efs/.
2. Sélectionnez le système de fichiers à supprimer.
3. Choisissez Actions, Delete file system.
4. Lorsque vous êtes invité à confirmer, entrez l'ID du système de fichiers et choisissez Delete file system (Supprimer le système de fichiers).

Utiliser Amazon FSx avec des EC2 instances Amazon

La FSx gamme de services Amazon facilite le lancement, l'exécution et le dimensionnement du stockage partagé alimenté par des systèmes de fichiers commerciaux et open source populaires. Vous pouvez utiliser le nouvel assistant de lancement d'instance pour associer automatiquement les types de systèmes de FSx fichiers Amazon suivants à vos EC2 instances Amazon lors du lancement :

- Amazon FSx for NetApp ONTAP fournit un stockage partagé entièrement géré dans le AWS cloud avec les fonctionnalités populaires d'accès et de gestion des données de NetApp ONTAP.
- Amazon FSx for Open ZFS fournit un stockage partagé rentable entièrement géré, alimenté par le célèbre système de ZFS fichiers Open.

> **Note**
>
> - Cette fonctionnalité est disponible uniquement dans l'assistant de lancement d'instance. Pour plus d'informations, consultez Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console.
> - Les systèmes de fichiers Amazon FSx pour Windows et Amazon FSx for Lustre ne peuvent pas être montés au lancement. Vous devez monter ces systèmes de fichiers manuellement après le lancement.

Vous pouvez choisir de monter un système de fichiers existant que vous avez créé précédemment, ou vous pouvez créer un nouveau système de fichiers à monter sur une instance au lancement.

Rubriques

- Groupes de sécurité et script de données utilisateur
- Monter un système de FSx fichiers Amazon au lancement

Groupes de sécurité et script de données utilisateur

Lorsque vous montez un système de FSx fichiers Amazon sur une instance à l'aide de l'assistant de lancement d'instance, vous pouvez choisir de créer et d'associer automatiquement les groupes de sécurité nécessaires pour permettre l'accès au système de fichiers, ou d'inclure automatiquement les scripts de données utilisateur nécessaires pour monter le système de fichiers et le rendre disponible à l'utilisation.

Rubriques

- Groupes de sécurité
- Script de données utilisateur

Groupes de sécurité

Si vous choisissez de créer automatiquement les groupes de sécurité nécessaires pour activer l'accès au système de fichiers, l'assistant de lancement d'instance de lancement crée et attache deux groupes de sécurité : un groupe de sécurité est attaché à l'instance et l'autre est attaché au système de fichiers. Pour plus d'informations sur les exigences relatives aux groupes de sécurité, consultez

FSxpour ONTAP le contrôle d'accès au système de fichiers avec Amazon VPC et FSxpour le contrôle d'accès au système de ZFS fichiers ouvert avec Amazon VPC.

Nous ajoutons la balise `Name=instance-sg-1` au groupe de sécurité créé et attaché à l'instance. La valeur de la balise est automatiquement incrémentée chaque fois que l'assistant de lancement d'instance crée un groupe de sécurité pour les systèmes de FSx fichiers Amazon.

Le groupe de sécurité comprend les règles de sortie suivantes, mais aucune règle d'entrée.

Règles sortantes

Type de protocole	Numéro de port	Destination
UDP	111	*file system security group*
UDP	2001 - 2003	*file system security group*
UDP	4049	*file system security group*
UDP	2049	*file system security group*
UDP	635	*file system security group*
UDP	4045 - 4046	*file system security group*
TCP	4049	*file system security group*
TCP	635	*file system security group*
TCP	2049	*file system security group*
TCP	111	*file system security group*
TCP	4045 - 4046	*file system security group*
TCP	2001 - 2003	*file system security group*
Tous	Tous	*file system security group*

Le groupe de sécurité créé et attaché au système de fichiers est balisé avec `Name=fsx-sg-1`. La valeur de la balise est automatiquement incrémentée chaque fois que l'assistant de lancement d'instance crée un groupe de sécurité pour les systèmes de FSx fichiers Amazon.

Le groupe de sécurité comprend les règles suivantes.

Règles entrantes

Type de protocole	Numéro de port	Source
UDP	2049	*instance security group*
UDP	2001 - 2003	*instance security group*
UDP	4049	*instance security group*
UDP	111	*instance security group*
UDP	635	*instance security group*
UDP	4045 - 4046	*instance security group*
TCP	4045 - 4046	*instance security group*
TCP	635	*instance security group*
TCP	2049	*instance security group*
TCP	4049	*instance security group*
TCP	2001 - 2003	*instance security group*
TCP	111	*instance security group*

Règles sortantes

Type de protocole	Numéro de port	Destination
Tous	Tous	0.0.0.0/0

Script de données utilisateur

Si vous choisissez d'attacher automatiquement des scripts de données utilisateur, l'assistant de lancement d'instance ajoute les données utilisateur suivantes à l'instance. Ce script installe les packages nécessaires, monte le système de fichiers et met à jour les paramètres de votre instance afin que le système de fichiers soit automatiquement remonté chaque fois que l'instance redémarre.

```
#cloud-config
package_update: true
package_upgrade: true
runcmd:
- yum install -y nfs-utils
- apt-get -y install nfs-common
- svm_id_1=svm_id
- file_system_id_1=file_system_id
- vol_path_1=/vol1
- fsx_mount_point_1=/mnt/fsx/fs1
- mkdir -p "${fsx_mount_point_1}"
- if [ -z "$svm_id_1" ]; then printf "\n${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev
 0 0\n" >> /etc/fstab; else printf "\n${svm_id_1}.${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev 0
 0\n" >> /etc/fstab; fi
- retryCnt=15; waitTime=30; while true; do mount -a -t nfs4 defaults; if [ $? = 0 ] ||
 [ $retryCnt -lt 1 ]; then echo File system mounted successfully; break; fi; echo File
 system not available, retrying to mount.; ((retryCnt--)); sleep $waitTime; done;
```

Monter un système de FSx fichiers Amazon au lancement

Pour monter un système de FSx fichiers Amazon nouveau ou existant au lancement

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances, Launch instance (Lancer l'instance) pour ouvrir l'assistant de lancement d'instance.
3. Dans la section Images de l'application et du système d'exploitation, sélectionnez le AMI à utiliser.
4. Dans la section Instance type (Type d'instance), sélectionnez le type d'instance.

5. Pour la section Key pair (Paire de clés), sélectionnez une paire de clés existante ou créez-en une nouvelle.
6. Dans la section Network settings (Paramètres réseau), procédez comme suit :

   a. Choisissez Modifier.

   b. Si vous souhaitez monter un système de fichiers existant, pour Subnet (Sous-réseau), choisissez le sous-réseau préféré du système de fichiers. Nous vous recommandons de lancer l'instance dans la même zone de disponibilité que le sous-réseau préféré du système de fichiers afin d'optimiser les performances.

      Si vous souhaitez créer un nouveau système de fichiers à monter sur une instance, pour Subnet (Sous-réseau), choisissez le sous-réseau dans lequel lancer l'instance.

      > **Important**
      >
      > Vous devez sélectionner un sous-réseau pour activer la FSx fonctionnalité Amazon dans le nouvel assistant de lancement d'instance. Si vous ne sélectionnez pas de sous-réseau, vous ne pourrez pas monter un système de fichiers existant ou en créer un nouveau.

7. Dans la section Storage (Stockage), procédez comme suit :

   a. Configurez les volumes au besoin.

   b. Développez la section Systèmes de fichiers et sélectionnez FSx.

   c. Choisissez Add shared file system (Ajouter un système de fichiers partagé).

   d. Pour File system (Système de fichiers), sélectionnez le système de fichiers à monter.

      > **Note**
      >
      > La liste affiche tous les systèmes de ZFS fichiers Amazon FSx FSx for NetApp ONTAP et Amazon for Open de votre compte dans la région sélectionnée.

   e. Pour créer et attacher automatiquement les groupes de sécurité nécessaires à l'accès au système de fichiers, sélectionnez Automatically create and attach security groups (Créer et attacher automatiquement des groupes de sécurité). Si vous préférez créer manuellement les groupes de sécurité, décochez la case. Pour plus d'informations, consultez Groupes de sécurité.

f. Pour attacher automatiquement les scripts de données utilisateur nécessaires au montage du système de fichiers, sélectionnez Automatically mount shared file system by attaching required user data script (Monter automatiquement le système de fichiers partagé en attachant le script de données utilisateur requis). Si vous préférez fournir manuellement les scripts de données utilisateur, décochez la case. Pour plus d'informations, consultez Script de données utilisateur.

8. Dans Advanced (Avancé), configurez les paramètres d'instance supplémentaires au besoin.
9. Choisissez Lancer.

Utiliser Amazon File Cache avec les EC2 instances Amazon

Amazon File Cache fournit un cache haut débit entièrement géré AWS qui facilite le traitement des données des fichiers, quel que soit leur emplacement de stockage. Amazon File Cache sert d'emplacement de stockage temporaire à hautes performances pour les données stockées dans des systèmes de fichiers locaux, des systèmes de AWS fichiers et des compartiments Amazon Simple Storage Service (Amazon S3). Vous pouvez utiliser cette fonctionnalité pour mettre des ensembles de données dispersés à la disposition des applications basées sur des fichiers AWS avec une vue unifiée et à des vitesses élevées (latences inférieures à la milliseconde et débit élevé). Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur Amazon File Cache.

Amazon File Cache fonctionne avec le système Linux AMIs le plus populaire et est compatible avec les types d'instances x86 et les types d'instances Graviton. Vous pouvez accéder à votre cache depuis vos EC2 instances Amazon à l'aide du client open source Lustre. Vous pouvez monter votre cache, puis utiliser les fichiers et les répertoires qu'il contient à l'aide des commandes Linux standard. EC2Les instances Amazon peuvent accéder à votre cache depuis d'autres zones de disponibilité du même cloud privé virtuel (VPC), à condition que la configuration de votre réseau autorise l'accès à travers les sous-réseaux duVPC. Vous pouvez également créer un cache dans un espace partagéVPC.

Pour commencer, consultez Getting started with Amazon File Cache dans le guide de l'utilisateur d'Amazon File Cache.

Gérez vos EC2 ressources Amazon

Une ressource est une entité avec laquelle vous pouvez travailler. Amazon EC2 crée des ressources lorsque vous utilisez les fonctionnalités du service. Par exemple, les EC2 ressources Amazon incluent des images, des instances, des flottes, des paires de clés et des groupes de sécurité. Tous les types de EC2 ressources Amazon incluent des attributs décrivant les ressources. Par exemple, les noms, les descriptions, les identificateurs de ressources et les noms de ressources Amazon (ARN).

Les EC2 ressources Amazon sont spécifiques à la AWS région ou à la zone dans laquelle elles se trouvent. Par exemple, une Amazon Machine Image (AMI) est spécifique à une AWS région, mais l'instance que vous lancez à partir d'une AMI est spécifique à la zone dans laquelle vous la lancez. Vous pouvez spécifier une EC2 ressource Amazon dans une politique d'autorisation à l'aide de sonARN.

Vous Compte AWS avez des quotas par défaut pour AmazonEC2. Ces quotas définissent le nombre maximum de ressources que vous pouvez créer. Par exemple, il existe des quotas pour le nombre maximum d'vCPUsinstances en cours d'exécution. Si le lancement d'une instance ou le démarrage d'une instance arrêtée vous amène à dépasser votre quota, l'opération échoue.

Vous pouvez rechercher des ressources spécifiques dans votre région Compte AWS à l'aide de ressources IDs ou de balises. Pour rechercher des ressources ou des types de ressources spécifiques dans plusieurs régions, utilisez Amazon EC2 Global View.

Table des matières

Sélectionnez une région pour vos EC2 ressources Amazon

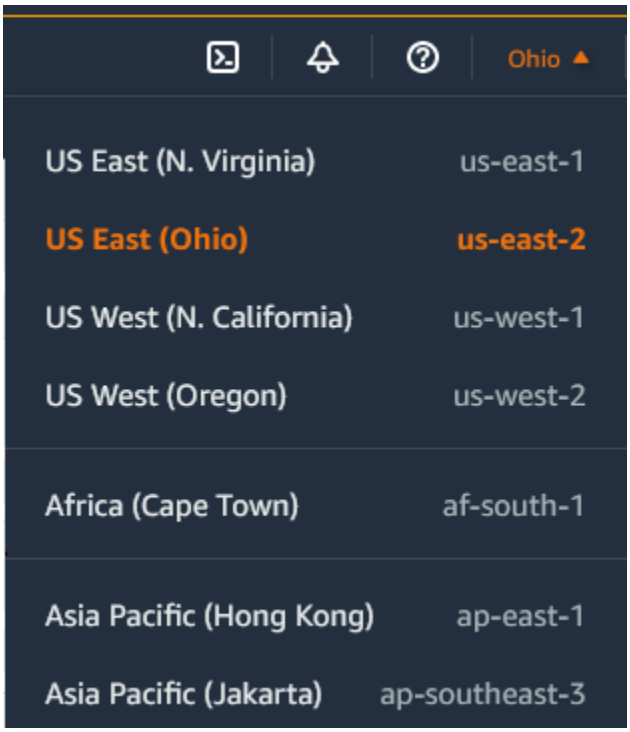
Les EC2 ressources Amazon sont spécifiques à la AWS région ou à la zone dans laquelle elles se trouvent. Lorsque vous créez une EC2 ressource Amazon, vous sélectionnez la région pour la ressource.

Considérations

Certaines AWS ressources peuvent ne pas être disponibles dans toutes les régions. Assurez-vous de pouvoir créer toutes les AWS ressources dont vous avez besoin dans la région sélectionnée avant de lancer vos EC2 instances Amazon.

Pour sélectionner une région pour une ressource à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation, choisissez le sélecteur Regions (Régions), puis sélectionnez la région.



3. Le sélecteur de régions inclut toutes les ressources pouvant être utilisées dans votre Compte AWS. Choisissez le texte souligné en bas de la liste pour afficher les régions qui ne sont pas activées pour votre compte. Pour activer une région qui n'est pas activée, voir Spécifier AWS les régions que votre compte peut utiliser dans le Guide de AWS Account Management référence.

Trouvez vos EC2 ressources Amazon

Vous pouvez obtenir une liste de certains types de ressources à l'aide de la EC2 console Amazon. Vous pouvez obtenir une liste de chaque type de ressource à l'aide de la commande ou de API

l'action correspondante. Si vous avez plusieurs ressources, vous pouvez filtrer les résultats pour n'inclure ou n'exclure que les ressources qui correspondent à certains critères.

Sommaire

Lister et filtrer des ressources à l'aide de la console

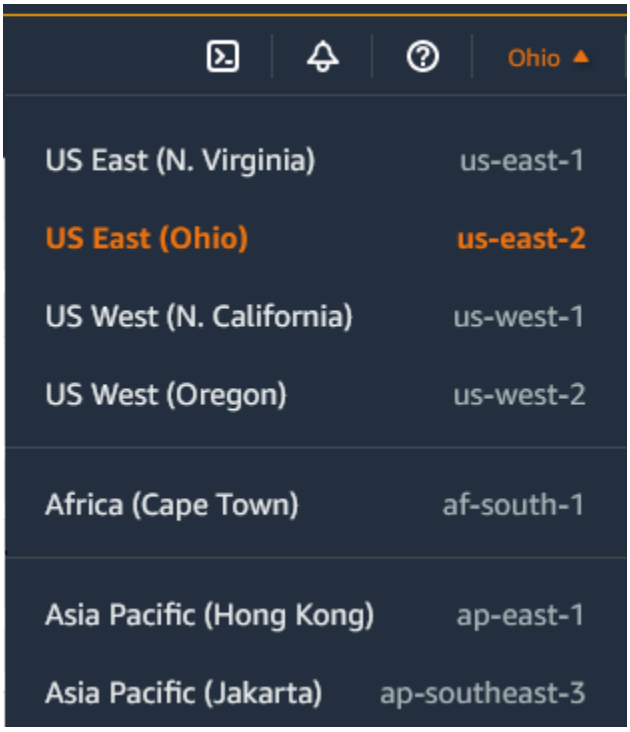
Table des matières

Lister des ressources à l'aide de la console

Vous pouvez consulter les types de EC2 ressources Amazon les plus courants à l'aide de la console. Pour afficher des ressources supplémentaires, utilisez l'interface de ligne de commande ou les API actions.

Pour répertorier EC2 les ressources à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Les EC2 ressources Amazon sont spécifiques à un Région AWS. Dans la barre de navigation, choisissez une région dans le sélecteur de régions.

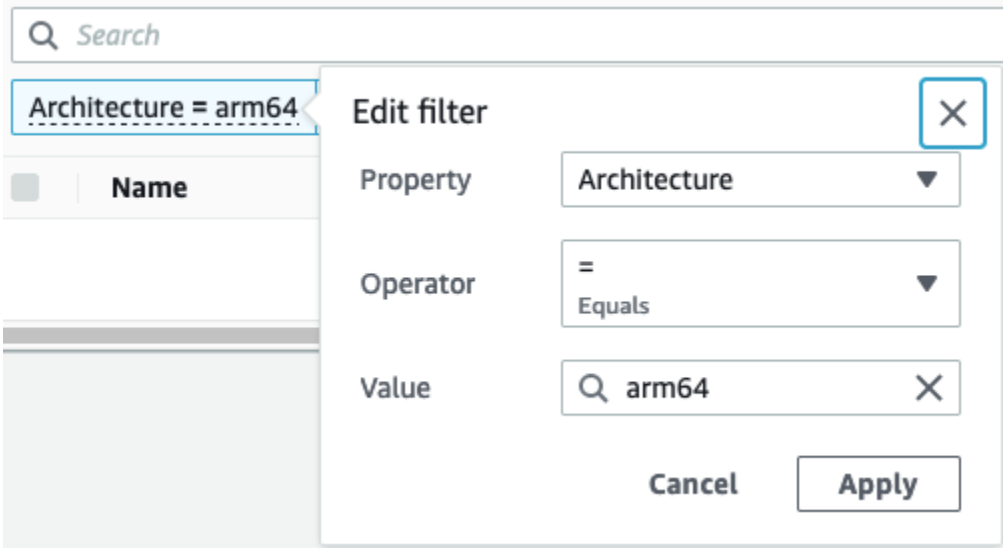


3. Dans le volet de navigation, choisissez l'option qui correspond à la ressource. Par exemple, pour répertorier toutes vos instances, choisissez Instances.

Filtrer des ressources à l'aide de la console

Pour filtrer une liste de ressources

1. Dans le panneau de navigation, sélectionnez un type de ressource (par exemple, Instances).
2. Choisissez le champ de recherche.
3. Sélectionnez le filtre dans la liste.
4. Sélectionnez un opérateur, par exemple,= (Equals (égal à)). Certains attributs ont plus d'opérateurs disponibles à sélectionner. Notez que tous les écrans ne prennent pas en charge la sélection d'un opérateur.
5. Sélectionnez une valeur de filtre.
6. Pour modifier un filtre sélectionné, choisissez le jeton de filtre (zone bleue), apportez les modifications requises, puis choisissezAppliquer. Notez que tous les écrans ne prennent pas en charge la modification du filtre sélectionné.



7. Lorsque vous avez terminé, retirez le filtre.

Filtres pris en charge

La EC2 console Amazon prend en charge deux types de filtrage.

- APIle filtrage se fait côté serveur. Le filtrage est appliqué lors de l'APIappel, ce qui réduit le nombre de ressources renvoyées par le serveur. Il permet un filtrage rapide sur des ensembles volumineux de ressources et peut réduire le temps et le coût du transfert de données entre le serveur et le navigateur. APIle filtrage prend en charge les opérateurs = (égal) et : (contient) et distingue toujours les majuscules et minuscules.
- Le filtrage client se produit du côté du client. Il vous permet de filtrer les données déjà disponibles dans le navigateur (en d'autres termes, les données qui ont déjà été renvoyées par leAPI). Le filtrage client fonctionne bien en conjonction avec un API filtre permettant de filtrer des ensembles de données plus petits dans le navigateur. En plus des opérateurs =(equals (égal à)) et :(contains (contient)) opérateurs, le filtrage client peut également prendre en charge les opérateurs de plage, tels que>=(greater than or equal (supérieur ou égal à)) et les opérateurs de négation (inverse), tels que ! =(does not equal (n'est pas égal à)).

La EC2 console Amazon prend en charge les types de recherches suivants :

Recherche par mot-clé

La recherche par mot clé est une recherche de texte libre qui vous permet de rechercher une valeur parmi tous les attributs de vos ressources ou balises, sans spécifier l'attribut ou la balise à rechercher.

> **Note**
>
> Toutes les recherches par mots-clés utilisent le filtrage client.

Pour rechercher par mot-clé, entrez ou collez ce que vous recherchez dans la zone de recherche, puis choisissez Enter (Entrer). Par exemple, la recherche 123 correspond à toutes les instances dont l'un des attributs, tel qu'une adresse IP, un ID, un ID ou un VPC ID d'instance, ou AMI l'une de leurs balises, telle que le nom, contient 123. Si votre recherche de texte libre renvoie des correspondances inattendues, appliquez des filtres supplémentaires.

Recherche par attribut

La recherche par attribut vous permet de rechercher un attribut spécifique parmi toutes vos ressources.

> **Note**
>
> Les recherches d'attributs utilisent le APIfiltrage ou le filtrage client, selon l'attribut sélectionné. Lors d'une recherche par attribut, les attributs sont regroupés en conséquence.

Par exemple, vous pouvez rechercher l'attribut État de l'instance pour toutes vos instances afin de renvoyer uniquement les instances dont l'état est `stopped`. Pour cela :

1. Dans le champ de recherche de l'écran Instances, commencez à saisir `Instance state`. Lorsque vous entrez les caractères, les deux types de filtres apparaissent pour l'état de l'instance : APIles filtres et les filtres clients.
2. Pour effectuer une recherche côté serveur, choisissez État de l'instance sous APIfiltres. Pour effectuer une recherche côté client, choisissez État de l'instance (client) sous Filtres client.

   Une liste d'opérateurs possibles pour l'attribut sélectionné s'affiche.
3. Cliquez sur l'onglet=opérateur (Equals (égal à)).

Une liste des valeurs possibles pour l'attribut et l'opérateur sélectionné s'affiche.

4. Sélectionnez Arrêté dans la liste.

Rechercher par identification

La recherche par balise permet de filtrer les ressources du tableau actuellement affiché par une clé de balise ou une valeur de balise.

Les recherches par balises utilisent le APIfiltrage ou le filtrage client, selon les paramètres de la fenêtre Préférences.

Pour garantir API le filtrage des balises

1. Ouvrir l'onglet Preferences (Préférences).
2. Effacer la case Utiliser la mise en correspondance d'expressions régulières. Si cette case est cochée, le filtrage client est effectué.
3. Sélectionnez la case Correspondance avec respect des casse. Si cette case est cochée, le filtrage client est effectué.
4. Choisissez Confirmer.

Lorsque vous effectuez une recherche par balise, vous pouvez utiliser les valeurs suivantes :

- (vide)— Recherchez toutes les ressources avec la clé de balise spécifiée, mais il ne doit pas y avoir de valeur de balise.
- Toutes les valeurs— Recherchez toutes les ressources avec la clé de balise spécifiée et n'importe quelle valeur de balise.
- Non balisé – Pour rechercher toutes les ressources qui n'ont pas la clé de balise spécifiée.
- La valeur affichée : permet de rechercher toutes les ressources avec la clé de balise spécifiée et la valeur de balise spécifiée.

Vous pouvez utiliser les techniques suivantes pour améliorer ou affiner vos recherches.

Recherche inversée

Les recherches inverses vous permettent de rechercher des ressources qui ne correspondent pas à une valeur spécifiée. Dans les instances et AMIsles écrans, les recherches inversées sont effectuées en sélectionnant le ! = (N'est pas égal à) ou ! : (Ne contient pas) opérateur, puis

sélection d'une valeur. Dans d'autres écrans, les recherches inverses s'effectuent en préfixant le mot clé de recherche d'un caractère point d'exclamation (!).

> **Note**
>
> La recherche inverse est prise en charge avec des recherches par mot-clé et des recherches par attribut uniquement sur des filtres client. Elle n'est pas prise en charge par les recherches d'attributs dans les API filtres.

Par exemple, vous pouvez rechercher l'attribut État de l'instance pour toutes vos instances afin de renvoyer uniquement les instances dont l'état est `terminated`. Pour cela :

1. Dans le champ de recherche de l'écran Instances, commencez à saisir `Instance state`. Lorsque vous entrez les caractères, les deux types de filtres apparaissent pour l'état de l'instance : APIles filtres et les filtres clients.
2. Sous Filtres client, choisissez État de l'instance (client). La recherche inverse n'est prise en charge que sur les filtres client.

   Une liste d'opérateurs possibles pour l'attribut sélectionné s'affiche.
3. Choisissez ! =(Does not equal (N'est pas égal à)), puis choisissezrésilié.

Pour filtrer les instances en fonction d'un attribut d'état d'instance, vous pouvez également utiliser les icônes de recherche (

) dans la colonne État de l'instance. L'icône de recherche avec un signe plus (+) affiche toutes les instances correspondant à cet attribut. L'icône de recherche avec un signe moins (-) exclut toutes les instances correspondant à cet attribut.

Voici un autre exemple d'utilisation de la recherche inverse : pour répertorier toutes les instances qui ne sont pas affectées au groupe de sécurité nommé `launch-wizard-1`, sous Filtres client, effectuez une recherche via l'attribut Security group name (Nom du groupe de sécurité), choisissez !=, et dans la barre de recherche entrez `launch-wizard-1`.

Recherche partielle

Avec les recherches partielles, vous pouvez rechercher des valeurs de chaîne partielles. Pour effectuer une recherche partielle, entrez uniquement une partie du mot-clé que vous souhaitez rechercher. Sur les instances et AMIsles écrans, les recherches partielles ne peuvent être

effectuées qu'avec l'opérateur : (Contient). Sur d'autres écrans, vous pouvez sélectionner l'attribut de filtre client et entrer immédiatement uniquement une partie du mot-clé que vous souhaitez rechercher. Par exemple, dans l'écran Type d'instance , pour rechercher toutes les instances , et `t2.micro`, effectuez une recherche par l'attribut `t2.small`Instance Type (Type d'instance)`t2.medium` puis saisissez `t2`.

Recherche d'expression régulière

Pour utiliser les recherches d'expression régulière, vous devez sélectionner la case à cocher Use regular expression matching (Utiliser la correspondance d'expression régulière) dans la fenêtre Preferences (préférences).

Les expressions régulières sont utiles quand vous avez besoin de faire correspondre les valeurs d'un champ à un modèle spécifique. Par exemple, pour rechercher une valeur qui commence par `s`, recherchez `^s`. Pour rechercher une valeur qui se termine par `xyz`, recherchez `xyz$`. Pour rechercher une valeur commençant par un nombre suivi d'un ou de plusieurs caractères, recherchez `[0-9]+.*`.

> **Note**
>
> La recherche par expression régulière est prise en charge avec les recherches par mot-clé et les recherches par attribut uniquement sur les filtres client. Elle n'est pas prise en charge par les recherches d'attributs dans les API filtres.

Recherche sensible à la casse

Pour utiliser des recherches sensibles à la casse, vous devez sélectionner leCorrespondance avec respect des cassedans la fenêtrePreferences (Préférences). La préférence sensible à la casse s'applique uniquement aux filtres des clients et des balises.

> **Note**
>
> APIles filtres distinguent toujours les majuscules et minuscules.

Recherche par caractère générique

Utilisez le caractère générique * pour faire correspondre zéro ou plusieurs caractères. Utilisez le caractère générique ? pour faire correspondre zéro ou un caractère. Par exemple, si vous

disposez d'un ensemble de données contenant les valeurs`prod`,`prods`, et`production`, une recherche de`prod*`correspond à toutes les valeurs, tandis que`prod?`correspondances uniquement`prod`et`prods`. Pour utiliser les valeurs littérales, échappez-les avec une barre oblique inverse (\). Par exemple, "`prod\*`" correspondrait à `prod*`.

> **Note**
>
> La recherche par caractères génériques est prise en charge uniquement pour les recherches par attributs et balises sur API les filtres. Elle n'est pas prise en charge avec les recherches par mot-clé et les recherches par attribut et balise uniquement sur les filtres client.

Combinaison de recherches

En général, plusieurs filtres avec le même attribut sont automatiquement joints avec `OR`. Par exemple, la recherche `Instance State : Running` et `Instance State : Stopped` renvoie toutes les instances en cours d'exécution OU arrêtées. Pour joindre la recherche avec `AND`, recherchez sur différents attributs. Par exemple, rechercher `Instance State : Running` et `Instance Type : c4.large` renvoyer uniquement les instances dont le type `c4.large` AND est en cours d'exécution.

Répertorier et filtrer à l'aide des touches CLI et API

Chaque type de ressource possède une CLI commande et une API action correspondantes que vous utilisez pour répertorier les ressources de ce type. Les listes de ressources qui en résultent peuvent être longues, de sorte qu'il peut être plus rapide et plus utile de filtrer les résultats pour inclure uniquement les ressources qui répondent à des critères spécifiques.

Considérations relatives au filtrage

- Vous pouvez spécifier jusqu'à 50 filtres et jusqu'à 200 valeurs par filtre en une seule demande.
- Les chaînes de filtre peuvent comporter jusqu'à 255 caractères.
- Vous pouvez aussi utiliser des caractères génériques avec les valeurs de filtre. Un astérisque (*) correspond à zéro ou plusieurs caractères, et un point d'interrogation (?) correspond à zéro ou un caractère.
- Les valeurs de filtre sont sensibles à la casse.

- Votre recherche peut inclure les valeurs littérales des caractères génériques ; vous devez simplement leur associer une séquence d'échappement avec une barre oblique inverse devant le caractère. Par exemple, la valeur `\*amazon\?\\` recherche la chaîne littérale `*amazon?\`.

Filtres pris en charge

Pour connaître les filtres pris en charge pour chaque EC2 ressource Amazon, consultez la documentation suivante :

- AWS CLI: Les `describe` commandes du AWS CLI Command Reference-Amazon EC2.
- Outils pour Windows PowerShell : les `Get` commandes de l'AWS Tools for PowerShell applet de commande Reference-Amazon. EC2
- Requête API : les `Describe` API actions décrites dans la EC2APIréférence Amazon.

Example Exemple : spécifier un filtre unique

Vous pouvez répertorier vos EC2 instances Amazon à l'aide de describe-instances. Sans aucun filtre, la réponse contient les informations pour toutes vos ressources. Vous pouvez utiliser la commande suivante pour inclure uniquement les instances en cours d'exécution dans votre sortie.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=running
```

Pour répertorier uniquement l'instance IDs de vos instances en cours d'exécution, ajoutez le `--query` paramètre comme suit.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=running --query
 "Reservations[*].Instances[*].InstanceId" --output text
```

Voici un exemple de sortie.

```
i-0ef1f57f78d4775a4
i-0626d4edd54f1286d
i-04a636d18e83cfacb
```

Example Exemple : spécifier plusieurs filtres ou valeurs de filtre

Si vous spécifiez plusieurs filtres ou plusieurs valeurs de filtre, la ressource doit correspondre à tous les filtres pour pouvoir apparaître dans les résultats.

Vous pouvez utiliser la commande suivante pour répertorier toutes les instances dont le type est `m5.large` ou `m5d.large`.

```
aws ec2 describe-instances --filters Name=instance-type,Values=m5.large,m5d.large
```

Vous pouvez utiliser la commande suivante pour répertorier toutes les instances arrêtées dont le type est `t2.micro`.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=stopped
 Name=instance-type,Values=t2.micro
```

Example Exemple : utiliser des caractères génériques dans une valeur de filtre

Si vous spécifiez `database` comme valeur de filtre pour le `description` filtre lorsque vous décrivez des EBS instantanés à l'aide de describe-snapshots, la commande renvoie uniquement les instantanés dont la description est « base de données ».

```
aws ec2 describe-snapshots --filters Name=description,Values=database
```

Le caractère générique * correspond à zéro ou plusieurs caractères. Si vous spécifiez `*database*` comme valeur de filtre, la commande renvoie uniquement les instantanés dont la description inclut ce terme.

```
aws ec2 describe-snapshots --filters Name=description,Values=*database*
```

Le caractère générique ? correspond à 1 seul caractère. Si vous spécifiez `database?` comme valeur de filtre, la commande renvoie uniquement les instantanés dont la description correspond à « database » ou à ce terme, suivi d'un caractère.

```
aws ec2 describe-snapshots --filters Name=description,Values=database?
```

Si vous indiquez `database????`, la commande renvoie uniquement les instantanés dont la description correspond à « database », suivi d'un maximum de quatre caractères. Elle exclut les descriptions contenant le terme « database » suivi de cinq caractères ou plus.

```
aws ec2 describe-snapshots --filters Name=description,Values=database????
```

Example Exemple : filtre basé sur la date

Avec le AWS CLI, vous pouvez filtrer JMESPath les résultats à l'aide d'expressions. Par exemple, la describe-snapshotscommande suivante affiche tous IDs les instantanés créés par votre Compte AWS (représenté par *123456789012*) avant la date spécifiée (représentée par *2020-03-31*). Si vous ne spécifiez pas le propriétaire, les résultats incluent tous les instantanés publics.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query
 "Snapshots[?(StartTime<='2020-03-31')].[SnapshotId]" --output text
```

La commande suivante affiche tous IDs les instantanés créés dans la plage de dates spécifiée.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query
 "Snapshots[?(StartTime>='2019-01-01') && (StartTime<='2019-12-31')].[SnapshotId]" --
output text
```

Filtre basé sur les balises

Pour obtenir des exemples de filtrage d'une liste de ressources en fonction de leurs balises, consultez Filtrer EC2 les ressources Amazon par tag.

Afficher les ressources de différentes régions à l'aide d'Amazon EC2 Global View

Amazon EC2 Global View vous permet de consulter et de rechercher VPC des ressources Amazon EC2 et Amazon dans une seule AWS région ou dans plusieurs régions simultanément sur une seule console. Pour de plus amples informations, veuillez consulter Afficher les ressources de différentes régions à l'aide d'Amazon EC2 Global View.

Afficher les ressources de différentes régions à l'aide d'Amazon EC2 Global View

Amazon EC2 Global View vous permet de consulter certaines de vos VPC ressources Amazon EC2 et Amazon dans une seule AWS région ou dans plusieurs régions dans une seule console. Amazon EC2 Global View fournit également une fonctionnalité de recherche globale qui vous permet de rechercher des ressources spécifiques ou des types de ressources spécifiques dans plusieurs régions simultanément.

Amazon EC2 Global View ne vous permet en aucun cas de modifier les ressources.

Ressources prises en charge

À l'aide d'Amazon EC2 Global View, vous pouvez consulter un résumé global des ressources suivantes dans toutes les régions pour lesquelles votre compte Compte AWS est activé.

- Groupes Auto Scaling
- DHCPjeu d'options
- Passerelles Internet de sortie uniquement
- Élastique IPs
- Services de point de terminaison
- instances
- Passerelles Internet
- Listes de préfixes gérées
- NATpasserelles
- Réseau ACLs
- Interfaces réseau
- Tables de routage
- Groupes de sécurité
- Sous-réseaux
- Volumes
- VPCs
- VPCpoints de terminaison
- VPCconnexions de peering

Autorisations nécessaires

Un utilisateur doit disposer des autorisations suivantes pour utiliser Amazon EC2 Global View.

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
```

```
    "autoscaling:DescribeAutoScalingGroups",
    "ec2:DescribeRegions",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeEgressOnlyInternetGateways",
    "ec2:DescribeAddresses",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribePrefixLists",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections"
  ],
  "Resource": "*"
  }]
}
```

Pour utiliser Amazon EC2 Global View

Ouvrez la console Amazon EC2 Global View à la https://console.aws.amazon.com/ec2globalview/maison.

> **Important**
>
> Vous ne pouvez pas utiliser une fenêtre privée dans Firefox pour accéder à Amazon EC2 Global View.

La console comprend les éléments suivants :

- Region explorer (Explorateur de région). Cet onglet comprend les sections suivantes :
  - Synthèse : offre un aperçu général de vos ressources dans toutes les régions.

    Les régions activées indiquent le nombre de régions pour lesquelles la vôtre Compte AWS est activée. Les champs restants indiquent le nombre de ressources dont vous disposez

actuellement dans ces Régions. Sélectionnez l'un des liens pour afficher les ressources de ce type dans toutes les Régions. Par exemple, si le lien situé sous l'étiquette instances est 29 dans 10 Regions (29 dans 10 Régions), cela indique que vous avez actuellement 29 instances à travers10 Régions. Cliquez sur ce lien pour afficher la liste des 29 instances.

- Nombre de régions de ressources : répertorie toutes les Régions AWS (y compris celles pour lesquelles votre compte n'est pas activé) et fournit des totaux pour chaque type de ressource pour chaque région.

  Sélectionnez un nom de Région pour afficher toutes les ressources de tous les types pour cette Région donnée. Par exemple, choisissez Africa (Cape Town) af-south-1 pour afficher VPCs tous les sous-réseaux, les instances, les groupes de sécurité, les volumes et les groupes Auto Scaling de cette région. Vous pouvez également sélectionner une Région et sélectionner View resources for selected Region (Afficher les ressources pour la Région sélectionnée).

  Sélectionnez la valeur d'un type de ressource spécifique dans une Région spécifique pour afficher uniquement les ressources de ce type dans cette Région. Par exemple, sélectionnez la valeur pour instances pour Africa (Cape Town) af-south-1 (Afrique (Le Cap) af-south-1) pour afficher uniquement les instances dans cette Région.

- Recherche globale : cet onglet vous permet de rechercher des ressources spécifiques ou des types de ressources spécifiques dans une seule région ou dans plusieurs régions. Il vous permet également d'afficher les détails d'une ressource spécifique.

  Pour rechercher des ressources, entrez les critères de recherche dans le champ précédant la grille. Vous pouvez effectuer une recherche par Région, par type de ressource et par balises affectées aux ressources.

  Pour afficher les détails d'une ressource spécifique, sélectionnez-la dans la grille. Vous pouvez également sélectionner l'ID ressource d'une ressource pour l'afficher dans sa console. Par exemple, choisissez un ID d'instance pour ouvrir l'instance dans la EC2 console Amazon, ou choisissez un ID de sous-réseau pour ouvrir le sous-réseau dans la console AmazonVPC.

> **Tip**
>
> Si vous utilisez uniquement des régions ou des types de ressources spécifiques, vous pouvez personnaliser Amazon EC2 Global View pour n'afficher que ces régions et ces types de ressources. Pour personnaliser les régions et les types de ressources affichés, dans le panneau de navigation, choisissez Paramètres, puis dans les onglets Ressources et Régions,

sélectionnez les régions et les types de ressources que vous ne souhaitez pas voir apparaître dans Amazon EC2 Global View.

Marquez vos EC2 ressources Amazon

Pour vous aider à gérer vos instances, images et autres EC2 ressources Amazon, vous pouvez attribuer vos propres métadonnées à chaque ressource sous forme de balises. Les balises vous permettent de classer vos AWS ressources de différentes manières, par exemple par objectif, propriétaire ou environnement. Cette approche est utile lorsque vous avez de nombreuses ressources de même type. Elle vous permet d'identifier rapidement une ressource spécifique en fonction des balises que vous lui avez attribuées. Cette rubrique décrit les balises et vous montre comment les créer.

Warning

Les clés de balise et leurs valeurs sont renvoyées par de nombreux API appels différents. Le fait de refuser l'accès à `DescribeTags` ne refuse pas automatiquement l'accès aux balises renvoyées par d'autresAPIs. Nous vous recommandons de ne pas inclure de données sensibles dans vos balises.

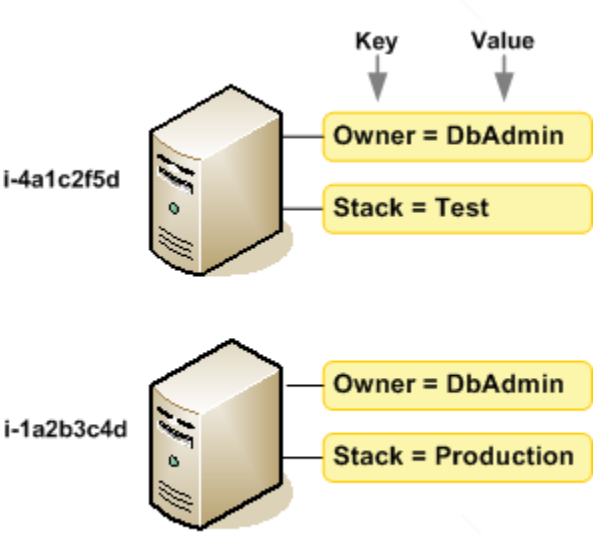
Sommaire

Principes de base des balises

Une étiquette est une étiquette que vous attribuez à une AWS ressource. Chaque balise est constituée d'une clé et d'une valeur facultative que vous définissez.

Les balises vous permettent de classer vos AWS ressources de différentes manières, par exemple par objectif, propriétaire ou environnement. Par exemple, vous pouvez définir un ensemble de balises pour les EC2 instances Amazon de votre compte afin de suivre le propriétaire et le niveau de pile de chaque instance.

Le graphique suivant illustre le fonctionnement du balisage. Dans cet exemple, vous avez affecté deux balises à chacune de vos instances : une balise avec la clé `Owner` et une autre avec la clé `Stack`. Chaque balise possède également une valeur associée.



Nous vous recommandons de concevoir un ensemble de clés de balise répondant à vos besoins pour chaque type de ressource. L'utilisation d'un ensemble de clés de balise cohérent facilite la gestion de vos ressources. Vous pouvez rechercher et filtrer les ressources en fonction des étiquettes que vous ajoutez. Pour plus d'informations sur la mise en œuvre d'une stratégie de balisage des ressources efficace, consultez le livre blanc sur les meilleures pratiques AWS en matière de balisage.

Les tags n'ont aucune signification sémantique pour Amazon EC2 et sont interprétés strictement comme des chaînes de caractères. De plus, les étiquettes ne sont pas automatiquement affectées à vos ressources. Vous pouvez modifier les clés et valeurs de balise, et vous pouvez retirer des balises d'une ressource à tout moment. Vous pouvez définir la valeur d'une balise sur une chaîne vide, mais vous ne pouvez pas définir la valeur d'une balise sur null. Si vous ajoutez une balise ayant la même

clé qu'une balise existante sur cette ressource, la nouvelle valeur remplace l'ancienne valeur. Si vous supprimez une ressource, ses balises sont également supprimées.

> **Note**
>
> Une fois que vous avez supprimé une ressource, ses balises peuvent rester visibles dans la console et être CLI affichées pendant une courte période. API Ces balises seront progressivement dissociées de la ressource et seront définitivement supprimées.

Etiqueter vos ressources

Lorsque vous utilisez la EC2 console Amazon, vous pouvez appliquer des balises aux ressources en utilisant l'onglet Tags sur l'écran des ressources concerné, ou vous pouvez utiliser l'éditeur de balises dans la AWS Resource Groups console. Certains écrans de ressource vous permettent de spécifier des balises pour une ressource lors de la création de cette ressource ; par exemple, une balise avec une clé de `Name` et une valeur que vous indiquez. Dans la plupart des cas, la console applique les balises immédiatement après la création de la ressource (plutôt qu'au cours de la création de ressources). La console peut organiser les ressources en fonction de la `Name` balise, mais cette balise n'a aucune signification sémantique pour le EC2 service Amazon.

Si vous utilisez Amazon EC2API, le ou un AWS CLI AWS SDK, vous pouvez utiliser cette `CreateTags` EC2 API action pour appliquer des balises aux ressources existantes. En outre, certaines actions de création de ressources vous permettent de spécifier des balises pour une ressource lors de la création de cette dernière. Si les balises ne peuvent pas être appliquées au cours de la création de ressources, nous restaurons le processus de création de ressources. Cela permet de s'assurer que les ressources sont créées avec des balises ou qu'elles ne sont pas créées du tout, et qu'aucune ressource ne demeurent sans balise à tout moment. En attribuant des balises aux ressources au moment de la création, vous pouvez supprimer la nécessité d'exécuter des scriptes de balisage personnalisés après la création de ressources. Pour plus d'informations sur la façon de permettre aux utilisateurs de baliser des ressources lors de la création, consultez Accorder l'autorisation de baliser les EC2 ressources Amazon lors de la création.

Vous pouvez appliquer des autorisations au niveau des ressources basées sur des balises dans vos IAM politiques aux EC2 API actions Amazon qui prennent en charge le balisage lors de la création afin de mettre en œuvre un contrôle granulaire sur les utilisateurs et les groupes autorisés à étiqueter les ressources lors de la création. Vos ressources sont correctement sécurisées depuis la création. Les balises sont appliquées immédiatement à vos ressources. Les autorisations de niveau ressource

basées sur des balises sont donc effectives immédiatement. Vos ressources peuvent être suivies et signalées avec plus de précision. Vous pouvez appliquer l'utilisation du balisage sur les nouvelles ressources et contrôler que les clés et valeurs de balise sont définies sur vos ressources.

Vous pouvez également appliquer des autorisations au niveau des ressources aux actions `CreateTags` Amazon et aux EC2 API actions `DeleteTags` Amazon de vos IAM politiques afin de contrôler les clés et les valeurs de balise définies sur vos ressources existantes. Pour de plus amples informations, veuillez consulter Exemple : Baliser des ressources.

Pour plus d'informations sur l'étiquetage de vos ressources pour la facturation, consultez Utilisation des étiquettes de répartition des coûts dans le AWS Billing Guide de l'utilisateur.

Restrictions liées aux balises

Les restrictions de base suivantes s'appliquent aux balises :

- Nombre maximal de balises par ressource : 50
- Pour chaque ressource, chaque clé de balise doit être unique, et chaque clé de balise peut avoir une seule valeur.
- Longueur de clé maximale : 128 caractères Unicode en UTF -8
- Longueur maximale de la valeur : 256 caractères Unicode en UTF -8
- Caractères autorisés
  - Bien qu'il EC2 autorise n'importe quel caractère dans ses balises, d'autres AWS services sont plus restrictifs. Les caractères autorisés dans tous les AWS services sont : les lettres (`a-z`,`A-Z`), les chiffres (`0-9`) et les espaces représentables en UTF -8, ainsi que les caractères suivants :. `+ - = . _ : / @`
  - Si vous activez les identifications d'instance dans les métadonnées d'instance, les clés d'identification d'instance ne peuvent utiliser que des lettres (`a-z`, `A-Z`), des nombres (`0-9`), ainsi que les caractères suivants : `+ - = . , _ : @`. Les clés d'identification des instances ne peuvent pas contenir d'espaces ou de `/`, et ne peuvent pas comprendre uniquement `.` (un point), `..` (deux points) ou `_index`. Pour de plus amples informations, veuillez consulter Afficher les balises de vos EC2 instances à l'aide des métadonnées de l'instance.
- Les clés et valeurs d'étiquette sont sensibles à la casse.
- Le `aws:` préfixe est réservé à l' AWS usage. Lorsque la balise possède une clé de balise avec ce préfixe, vous ne pouvez pas modifier ou supprimer sa clé ou sa valeur. Les balises avec le préfixe `aws:` ne sont pas comptabilisées comme vos balises pour la limite de ressources.

Vous ne pouvez pas mettre fin à une ressource, ou l'arrêter ou la supprimer uniquement en fonction de ses balises ; vous devez spécifier l'identificateur de ressource. Par exemple, pour supprimer des instantanés (snapshot) que vous avez balisés avec une clé de balise appelée `DeleteMe`, vous devez utiliser l'action `DeleteSnapshots` avec les identificateurs de ressource des instantanés, tels que `snap-1234567890abcdef0`.

Lorsque vous balisez des ressources publiques ou partagées, les balises que vous attribuez ne sont disponibles que pour votre AWS compte ; aucun autre AWS compte n'a accès à ces balises. Pour le contrôle d'accès basé sur des balises aux ressources partagées, chaque AWS compte doit attribuer son propre ensemble de balises pour contrôler l'accès à la ressource.

Gestion des balises et des accès

Si vous utilisez AWS Identity and Access Management (IAM), vous pouvez contrôler quels utilisateurs de votre AWS compte sont autorisés à créer, modifier ou supprimer des tags. Pour de plus amples informations, veuillez consulter Accorder l'autorisation de baliser les EC2 ressources Amazon lors de la création.

Vous pouvez également utiliser des balises de ressources pour implémenter le contrôle basé sur les attributs ()ABAC. Vous pouvez créer des IAM politiques qui autorisent les opérations en fonction des balises de la ressource. Pour de plus amples informations, veuillez consulter Contrôlez l'accès à l'aide de l'accès basé sur les attributs.

Baliser vos ressources pour facturation

Vous pouvez utiliser des balises pour organiser votre AWS facture afin de refléter votre propre structure de coûts. Pour ce faire, inscrivez-vous pour obtenir la facture de votre AWS compte avec les valeurs clés du tag incluses. Pour plus d'informations sur la configuration d'un rapport de répartition des coûts avec des étiquettes, consultez Rapport de répartition des coûts mensuel dans le Guide de l'utilisateur AWS Billing . Pour voir le coût de vos ressources combinées, vous pouvez organiser vos informations de facturation en fonction des ressources possédant les mêmes valeurs de clé d'étiquette. Par exemple, vous pouvez baliser plusieurs ressources avec un nom d'application spécifique, puis organiser vos informations de facturation pour afficher le coût total de cette application dans plusieurs services. Pour plus d'informations, veuillez consulter Utilisation des étiquettes de répartition des coûts dans le AWS Billing Guide de l'utilisateur.

> **Note**
>
> Si vous venez d'activer la création de rapports, les données du mois en cours peuvent être consultées après 24 heures.

Les balises de répartition des coûts peuvent indiquer quelles ressources contribuent aux coûts, mais la suppression ou la désactivation des ressources ne réduit pas toujours les coûts. Par exemple, des données d'instantané qui sont référencées par un autre instantané sont conservées, même si l'instantané qui contient les données d'origine est supprimé. Pour plus d'informations, consultez Volumes et instantanés Amazon Elastic Block Store dans le AWS Billing Guide de l'utilisateur.

> **Note**
>
> Les adresses IP Elastic étiquetées ne sont pas affichées dans votre rapport de répartition des coûts.

Accorder l'autorisation de baliser les EC2 ressources Amazon lors de la création

Certaines EC2 API actions Amazon qui créent des ressources vous permettent de spécifier des balises lors de la création de la ressource. Vous pouvez utiliser des balises de ressources pour implémenter le contrôle basé sur les attributs ()ABAC. Pour plus d'informations, consultez Etiqueter vos ressources et Contrôlez l'accès à l'aide de l'accès basé sur les attributs.

Pour permettre aux utilisateurs d'attribuer des balises aux ressources au moment de la création, ils doivent avoir les autorisations d'utiliser l'action qui crée la ressource (par exemple, `ec2:RunInstances` ou `ec2:CreateVolume`). Si les balises sont spécifiées dans l'action de création de ressources, Amazon effectue une autorisation supplémentaire sur l'action `ec2:CreateTags` pour vérifier si les utilisateurs sont autorisés à créer des balises. Par conséquent, les utilisateurs doivent également avoir des autorisations explicites d'utiliser l'action `ec2:CreateTags`.

Dans la définition IAM de la politique de l'`ec2:CreateTags`action, utilisez l'`Condition`élément associé à la clé de `ec2:CreateAction` condition pour accorder des autorisations de balisage à l'action qui crée la ressource.

L'exemple suivant illustre une politique qui permet aux utilisateurs de lancer des instances et d'appliquer des balises aux instances et aux volumes pendant le lancement. Les utilisateurs ne sont pas autorisés à attribuer des balises aux ressources existantes (ils ne peuvent pas appeler l'action `ec2:CreateTags` directement).

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

De même, la politique suivante permet aux utilisateurs de créer des volumes et appliquer des balises à des volumes pendant la création de volume. Les utilisateurs ne sont pas autorisés à attribuer des balises aux ressources existantes (ils ne peuvent pas appeler l'action `ec2:CreateTags` directement).

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateVolume"
      ],
      "Resource": "*"
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "CreateVolume"
          }
       }
    }
  ]
}
```

L'action `ec2:CreateTags` est uniquement évaluée si les balises sont appliquées pendant l'action de création de ressources. Par conséquent, un utilisateur qui est autorisé à créer une ressource (en supposant qu'il n'existe aucune condition de balisage) n'a pas besoin des autorisations d'utiliser l'action `ec2:CreateTags` si aucune balise n'est spécifié dans la demande. Toutefois, si l'utilisateur essaie de créer une ressource avec des balises, la demande échoue s'il n'a pas les autorisations d'utiliser l'action `ec2:CreateTags`.

L'action `ec2:CreateTags` est également évaluée si des balises sont fournies dans un modèle de lancement. Pour un exemple de politique, consultez Balises dans un modèle de lancement.

Contrôler l'accès à des balises spécifiques

Vous pouvez utiliser des conditions supplémentaires dans l'`Condition`élément de vos IAM politiques pour contrôler les clés de balise et les valeurs qui peuvent être appliquées aux ressources.

Les clés de condition suivantes peuvent être utilisées avec les exemples de la section précédente :

- `aws:RequestTag` : Pour indiquer qu'une clé de balise ou une clé et valeur de balise particulière doit être présente dans une demande. D'autres balises peuvent également être spécifiées dans la demande.
  - Utilisez avec l'opérateur de condition `StringEquals` pour appliquer une combinaison de clé de balise et de valeur spécifique ; par exemple, pour appliquer la balise `cost-center=cc123` :

    ```
    "StringEquals": { "aws:RequestTag/cost-center": "cc123" }
    ```

- A utiliser avec l'opération de condition `StringLike` pour appliquer une clé de balise spécifique dans la demande ; par exemple, pour appliquer la clé de balise `purpose`:

```
"StringLike": { "aws:RequestTag/purpose": "*" }
```

- `aws:TagKeys` : Pour appliquer les clés de balise qui sont utilisées dans la demande.
  - A utiliser avec le modificateur `ForAllValues` pour appliquer des clés de balise spécifiques si celles-ci sont fournies dans la demande (si les balises sont spécifiées dans la demande, seules les clés de balise spécifiques sont autorisées ; aucune autre balise n'est autorisée). Par exemple, les clés de balise `environment` ou `cost-center` sont autorisées :

```
"ForAllValues:StringEquals": { "aws:TagKeys": ["environment","cost-center"] }
```

  - A utiliser avec le modificateur `ForAnyValue` pour appliquer la présence d'au moins l'une des clés de balise spécifiées dans la demande. Par exemple, au moins l'une des clés de balise `environment` ou `webserver` doit être présente dans la demande :

```
"ForAnyValue:StringEquals": { "aws:TagKeys": ["environment","webserver"] }
```

Ces clés de condition peuvent être appliqués aux actions de création de ressources qui prennent en charge le balisage ainsi qu'aux actions `ec2:CreateTags` et `ec2:DeleteTags`. Pour savoir si une EC2 API action Amazon prend en charge le balisage, consultez Actions, ressources et clés de condition pour Amazon EC2.

Pour forcer les utilisateurs à spécifier des balises quand ils créent une ressource, vous devez utiliser la clé de condition `aws:RequestTag` ou la clé de condition `aws:TagKeys` avec le modificateur `ForAnyValue` sur l'action de création de ressources. L'action `ec2:CreateTags` n'est pas évaluée si un utilisateur ne spécifie pas de balises pour l'action de création de ressources.

Pour les conditions, la clé de condition n'est pas sensible à la casse et la valeur de la condition est sensible à la casse. Par conséquent pour forcer la sensibilité à la casse d'une clé de balise, utilisez la clé de condition `aws:TagKeys`, où la clé de balise est indiquée comme une valeur dans la condition.

Pour des exemples IAM de politiques, voirExemples de politiques pour contrôler l'accès à Amazon EC2 API. Pour plus d'informations sur les conditions à valeurs multiples, voir Création d'une condition qui teste plusieurs valeurs clés dans le guide de l'IAMutilisateur.

Ajouter et supprimer des balises pour les EC2 ressources Amazon

Lorsque vous créez une EC2 ressource Amazon, telle qu'une EC2 instance Amazon, vous pouvez spécifier les balises à ajouter à la ressource. Vous pouvez également utiliser la EC2 console Amazon pour afficher les balises d'une EC2 ressource Amazon spécifique. Vous pouvez également ajouter ou supprimer des balises dans une EC2 ressource Amazon existante.

Vous pouvez utiliser l'éditeur de balises de la AWS Resource Groups console pour afficher, ajouter ou supprimer des balises pour toutes vos AWS ressources dans toutes les régions. Vous pouvez appliquer ou supprimer des balises pour plusieurs types de ressources en même temps. Pour plus d'informations, consultez le Guide de l'utilisateur AWS des ressources de balisage.

Tâches

- Ajouter et supprimer des tags à l'aide de la console
- Ajoutez des balises à l'aide du AWS CLI
- Ajoutez des balises à l'aide de CloudFormation

Ajouter et supprimer des tags à l'aide de la console

Vous pouvez gérer les balises d'une ressource existante directement depuis la page de la ressource.

Pour gérer les balises d'une ressource existante

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation, sélectionnez la région où se trouve la ressource.
3. Dans le panneau de navigation, sélectionnez un type de ressource (par exemple, Instances).
4. Sélectionnez la ressource dans la liste.
5. Dans l'onglet Tags, sélectionnez Gérer les tags.
6. Pour ajouter une étiquette, choisissez Ajouter une nouvelle balise et entrez une clé et une valeur pour la balise. Pour supprimer une identification, choisissez Supprimer.
7. Choisissez Save (Enregistrer).

Ajoutez des balises à l'aide du AWS CLI

Les exemples suivants montrent comment ajouter des balises à une ressource existante à l'aide de la commande create-tags.

Example Exemple : Ajout d'une balise à une ressource

La commande suivante ajoute la balise **`Stack=production`** à l'image spécifiée ou remplace une balise existante pour l'AMIendroit où se trouve la clé de balise. **`Stack`** Si la commande réussit, aucune sortie n'est renvoyée.

```
aws ec2 create-tags \
    --resources ami-78a54011 \
    --tags Key=Stack,Value=production
```

Example Exemple : Ajout de balises à plusieurs ressources

Cet exemple ajoute (ou remplace) deux balises pour une instance AMI et une instance. L'une des balises contient simplement une clé (**`webserver`**), sans valeur (nous avons défini une chaîne vide comme valeur). L'autre balise est constituée d'une clé (**`stack`**) et d'une valeur (**`Production`**). Si la commande réussit, aucune sortie n'est renvoyée.

```
aws ec2 create-tags \
    --resources ami-1a2b3c4d i-1234567890abcdef0 \
    --tags Key=webserver,Value=  Key=stack,Value=Production
```

Example Exemple : Ajout de balises avec des caractères spéciaux

Cet exemple ajoute la balise **`[Group]=test`** à une instance. Les crochets (**`[`** et **`]`**) sont des caractères spéciaux, qui doivent être échappés.

Si vous utilisez Linux ou OS X, pour échapper les caractères spéciaux, placez l'élément avec le caractère spécial entre des guillemets doubles (**`"`**), puis placez toute la structure de clé et de valeur entre des guillemets simples (**`'`**).

```
aws ec2 create-tags \
    --resources i-1234567890abcdef0 \
    --tags 'Key="[Group]",Value=test'
```

Si vous utilisez Windows, pour échapper les caractères spéciaux, placez l'élément qui a des caractères spéciaux entre des guillemets doubles ("), puis faites précéder chaque guillemet double d'une barre oblique inverse (**`\`**), comme suit :

```
aws ec2 create-tags ^
    --resources i-1234567890abcdef0 ^
```

```
    --tags Key=\"[Group]\",Value=test
```

Si vous utilisez Windows PowerShell, pour éviter les caractères spéciaux, placez la valeur contenant des caractères spéciaux entre guillemets (**"**), faites précéder chaque guillemet d'une barre oblique inverse (****), puis placez l'ensemble de la structure des clés et des valeurs entre guillemets simples () comme suit : **'**

```
aws ec2 create-tags `
    --resources i-1234567890abcdef0 `
    --tags 'Key=\"[Group]\",Value=test'
```

Ajoutez des balises à l'aide de CloudFormation

Avec les types de EC2 ressources Amazon, vous spécifiez des balises à l'aide de la `TagSpecifications` propriété a `Tags` ou.

Les exemples suivants ajoutent la balise **`Stack=Production`** à AWS: : EC2 : :Instance à l'aide de sa `Tags` propriété.

Example Exemple : Tags YAML

```
Tags:
  - Key: "Stack"
    Value: "Production"
```

Example Exemple : Tags JSON

```
"Tags": [
    {
        "Key": "Stack",
        "Value": "Production"
    }
]
```

Les exemples suivants ajoutent la balise **`Stack=Production`** à AWS: : : EC2 : LaunchTemplate LaunchTemplateData en utilisant sa `TagSpecifications` propriété.

Example Exemple : TagSpecifications dans YAML

```
TagSpecifications:
  - ResourceType: "instance"
```

```
    Tags:
    - Key: "Stack"
      Value: "Production"
```

Example Exemple : TagSpecifications dans JSON

```
"TagSpecifications": [
    {
        "ResourceType": "instance",
        "Tags": [
            {
                "Key": "Stack",
                "Value": "Production"
            }
        ]
    }
]
```

Filtrer EC2 les ressources Amazon par tag

Après avoir ajouté des balises, vous pouvez filtrer vos EC2 ressources Amazon en fonction des clés de balise et des valeurs de balise.

Pour filtrer les ressources par tag à l'aide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez un type de ressource (par exemple, Instances).
3. Choisissez le champ de recherche.
4. Dans la liste, sous Balises, choisissez la clé de balise.
5. Choisissez la valeur de balise correspondante dans la liste.
6. Lorsque vous avez terminé, retirez le filtre.

Pour plus d'informations sur l'utilisation des filtres dans la EC2 console Amazon, consultezTrouvez vos EC2 ressources Amazon.

Pour filtrer les ressources par balise à l'aide du AWS CLI

Les exemples suivants montrent comment utiliser des filtres avec describe-instances pour afficher des instances avec des balises spécifiques. Toutes les commandes de EC2 description utilisent

cette syntaxe pour filtrer par balise sur un seul type de ressource. Vous pouvez également utiliser la commande describe-tags pour filtrer les types de EC2 ressources par balise.

Example Exemple 1 : Décrire les instances avec la clé de balise spécifiée

La commande suivante décrit les instances avec une balise **`Stack`**, quelle que soit la valeur de la balise.

```
aws ec2 describe-instances \
    --filters Name=tag-key,Values=Stack
```

Example Exemple 2 : Décrire les instances avec la balise spécifiée

La commande suivante décrit les instances avec la balise **`Stack=production`**.

```
aws ec2 describe-instances \
    --filters Name=tag:Stack,Values=production
```

Example Exemple 3 : Décrire les instances avec la valeur de balise spécifiée

La commande suivante décrit les instances à l'aide d'une balise avec la valeur **`production`**, quelle que soit la clé de balise.

```
aws ec2 describe-instances \
    --filters Name=tag-value,Values=production
```

Example Exemple 4 : Décrire toutes les EC2 ressources avec le tag spécifié

La commande suivante décrit toutes les EC2 ressources associées à la balise**`Stack=Test`**.

```
aws ec2 describe-tags \
    --filters Name=key,Values=Stack Name=value,Values=Test
```

Afficher les balises de vos EC2 instances à l'aide des métadonnées de l'instance

Vous pouvez accéder aux identifications d'une instance à partir des métadonnées de l'instance. En accédant aux balises à partir des métadonnées de l'instance, vous n'avez plus besoin d'utiliser les `DescribeTags` API appels `DescribeInstances` ou pour récupérer les informations relatives aux balises, ce qui réduit le nombre de API transactions par seconde et permet à vos recherches

de balises d'évoluer en fonction du nombre d'instances que vous contrôlez. En outre, les processus locaux exécutés sur une instance peuvent afficher les informations d'identification de l'instance directement à partir des métadonnées de l'instance.

Par défaut, les identifications ne sont pas disponibles à partir des métadonnées de l'instance. Vous devez explicitement autoriser l'accès. Vous pouvez autoriser l'accès au lancement de l'instance ou après le lancement sur une instance en cours d'exécution ou arrêtée. Vous pouvez également autoriser l'accès aux identifications en le spécifiant dans un modèle de lancement. Les instances lancées à l'aide du modèle permettent d'accéder aux identifications dans les métadonnées de l'instance.

Si vous ajoutez ou supprimez une balise d'instance, les métadonnées de l'instance sont mises à jour pendant que l'instance est exécutée, sans avoir besoin d'arrêter puis de démarrer l'instance.

Tâches

- Autoriser l'accès aux identifications dans les métadonnées d'instance
- Extraire les identifications à partir des métadonnées d'instance
- Désactiver l'accès aux identifications dans les métadonnées d'instance

Autoriser l'accès aux identifications dans les métadonnées d'instance

Par défaut, il n'y a pas d'accès aux balises d'instance dans les métadonnées de l'instance. Pour chaque instance, vous devez explicitement autoriser l'accès en utilisant l'une des méthodes suivantes.

Pour autoriser l'accès aux identifications dans les métadonnées d'instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez une instance, puis choisissez Actions, Instance settings (Paramètres de l'instance), Allow tags in instance metadata (Autoriser les identifications dans les métadonnées d'instance).
4. Pour autoriser l'accès aux identifications dans les métadonnées d'instance, cochez la case Allow (Autoriser).
5. Choisissez Save (Enregistrer).

Pour autoriser l'accès aux identifications dans les métadonnées d'instance lors du lancement à l'aide de la AWS CLI

Utilisez la commande run-instances et définissez le paramètre `InstanceMetadataTags` sur `enabled`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c3.large \
    ...
    --metadata-options "InstanceMetadataTags=enabled"
```

Pour autoriser l'accès aux identifications dans les métadonnées d'instance sur une instance en cours d'exécution ou arrêtée à l'aide de la AWS CLI

Utilisez la modify-instance-metadata-optionscommande et réglez `--instance-metadata-tags` sur`enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-123456789example \
    --instance-metadata-tags enabled
```

Extraire les identifications à partir des métadonnées d'instance

Après avoir autorisé l'accès aux balises d'instance dans les métadonnées de l'instance, vous pouvez accéder à la `tags/instance` catégorie à partir des métadonnées de l'instance. Pour de plus amples informations, veuillez consulter Accéder aux métadonnées d'une EC2 instance.

Instance Metadata Service Version 2

Exécutez les exemples suivants sur votre EC2 instance Amazon pour récupérer les métadonnées de l'instance pourIMDSv2.

cURL

Cet exemple permet d'obtenir toutes les clés de balise d'une instance.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/tags/instance
Name
Environment
```

Cet exemple obtient la valeur de la Name clé obtenue dans l'exemple précédent. La IMDSv2 demande utilise le jeton stocké créé à l'aide de la commande de l'exemple précédent. Le jeton ne doit pas avoir expiré.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/tags/instance/Name
MyInstance
```

PowerShell

Cet exemple permet d'obtenir toutes les clés de balise d'une instance.

```
PS C:\> $token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/tags/instance
Name
Environment
```

Cet exemple obtient la valeur de la Name clé obtenue dans l'exemple précédent. La IMDSv2 demande utilise le jeton stocké créé à l'aide de la commande de l'exemple précédent. Le jeton ne doit pas avoir expiré.

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/tags/instance/Name
MyInstance
```

Service de métadonnées d'instance, version 1

Exécutez les exemples suivants sur votre EC2 instance Amazon pour récupérer les métadonnées de l'instance pourIMDSv1.

cURL

Cet exemple permet d'obtenir toutes les clés de balise d'une instance.

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/tags/instance
Name
```

```
Environment
```

Cet exemple obtient la valeur de la Name clé obtenue dans l'exemple précédent.

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/tags/instance/Name
MyInstance
```

PowerShell

Cet exemple permet d'obtenir toutes les clés de balise d'une instance.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/tags/instance
Name
Environment
```

Cet exemple obtient la valeur de la Name clé obtenue dans l'exemple précédent.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/tags/
instance/Name
MyInstance
```

Désactiver l'accès aux identifications dans les métadonnées d'instance

Pour désactiver l'accès aux identifications d'instance dans les métadonnées d'instance, utilisez l'une des méthodes suivantes. Il n'est pas nécessaire de désactiver l'accès aux identifications d'instance sur les métadonnées d'instance au lancement car il est désactivé par défaut.

Pour désactiver l'accès aux identifications dans les métadonnées d'instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez une instance, puis choisissez Actions, Instance settings (Paramètres de l'instance), Allow tags in instance metadata (Autoriser les identifications dans les métadonnées d'instance).
4. Pour désactiver l'accès aux identifications dans les métadonnées d'instance, décochez la case Allow (Autoriser).
5. Choisissez Save (Enregistrer).

Pour désactiver l'accès aux balises dans les métadonnées de l'instance à l'aide du AWS CLI

Utilisez la modify-instance-metadata-optionscommande et réglez `--instance-metadata-tags` sur`disabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-123456789example \
    --instance-metadata-tags disabled
```

Pour savoir si l'accès aux balises dans les métadonnées de l'instance est autorisé à l'aide du AWS CLI

Utilisez la commande describe-instances et spécifiez l'ID de l'instance. Utilisez le `--query` paramètre pour afficher uniquement les options de métadonnées de l'instance dans les résultats.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[*].Instances[*].MetadataOptions"
```

Voici un exemple de sortie. La valeur de `InstanceMetadataTags` indique si l'accès aux balises dans les métadonnées de l'instance est autorisé. Si la valeur est`enabled`, elle est autorisée. Si la valeur est positive`disabled`, elle n'est pas autorisée.

```
[
    [
        {
            "State": "applied",
            "HttpTokens": "required",
            "HttpPutResponseHopLimit": 2,
            "HttpEndpoint": "enabled",
            "HttpProtocolIpv6": "disabled",
            "InstanceMetadataTags": "enabled"
        }
    ]
]
```

Quotas EC2 de service Amazon

Lorsque vous créez votre Compte AWS, nous définissons des quotas par défaut (également appelés limites) pour vos AWS ressources par région. Si vous essayez de dépasser le quota d'une ressource, la demande échoue. Par exemple, il existe un nombre maximum d'Amazon EC2 vCPUs

que vous pouvez approvisionner pour les instances à la demande dans une région. Si vous tentez de lancer une instance dans une région et que cette demande entraîne un dépassement de ce quota d'utilisation, la demande échoue. Dans ce cas, vous pouvez réduire l'utilisation de vos ressources ou demander une augmentation de quota.

La console Service Quotas est un emplacement central où vous pouvez consulter et gérer vos quotas de AWS services, et demander une augmentation des quotas pour la plupart des ressources que vous utilisez. Utilisez les informations de quota que nous fournissons pour gérer votre AWS infrastructure. Prévoyez de demander les augmentations de quota avant le moment où vous en aurez besoin.

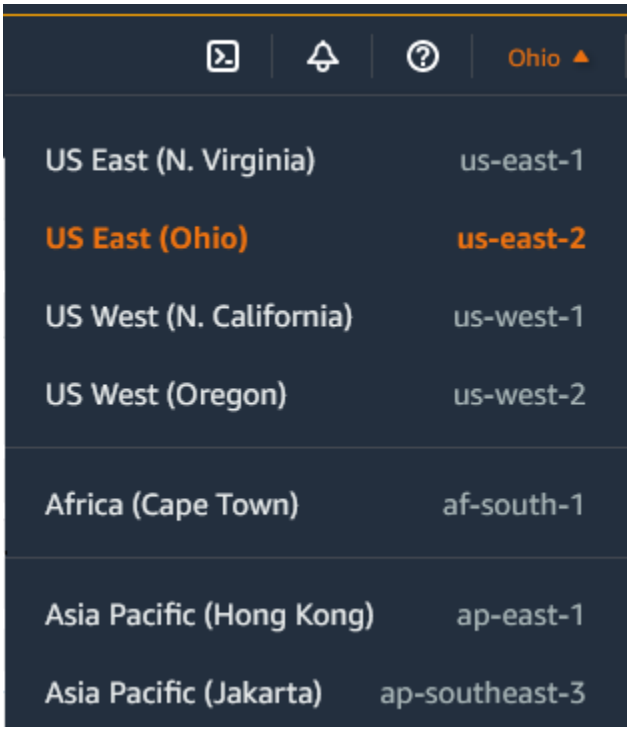
Pour plus d'informations, consultez les sections EC2Points de terminaison et quotas Amazon et EBS Points de terminaison et quotas Amazon dans le. Référence générale d'Amazon Web Services

Afficher vos quotas actuels

Vous pouvez consulter vos quotas pour chaque région à l'aide de la EC2 console Service Quotas.

Pour afficher vos quotas actuels à l'aide de la console Service Quotas

1. Ouvrez la console Service Quotas à l'adresse https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Dans la barre de navigation (en haut de l'écran), sélectionnez une région.



3. Utilisez le champ de filtre pour filtrer la liste par nom de ressource. Par exemple, saisissez **`On-Demand`** pour connaître les quotas des instances à la demande.
4. Pour plus d'informations, choisissez le nom du quota afin d'ouvrir la page de détails du quota.

Demander une augmentation

Vous pouvez demander une augmentation de quota pour chaque région.

Pour demander une augmentation à l'aide de la console Service Quotas

1. Ouvrez la console Service Quotas à l'adresse https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Dans la barre de navigation (en haut de l'écran), sélectionnez une région.
3. Utilisez le champ de filtre pour filtrer la liste par nom de ressource. Par exemple, saisissez **`On-Demand`** pour connaître les quotas des instances à la demande.
4. Si le quota est ajustable, sélectionnez-le, puis choisissez Demander une augmentation de quota.
5. Pour Modifier la valeur du quota, saisissez la nouvelle valeur du quota.
6. Choisissez Request (Demander).
7. Pour afficher les demandes en attente ou récemment résolues dans la console, choisissez Tableau de bord dans le volet de navigation. Pour les demandes en attente, choisissez l'état de la demande pour ouvrir le reçu de la demande. L'état initial d'une demande est Pending (En attente). Une fois que le statut est passé au quota demandé, vous verrez le numéro de dossier avec AWS Support. Choisissez le numéro de dossier pour ouvrir le billet pour votre demande.

Pour plus d'informations, notamment sur la manière d'utiliser AWS CLI ou de SDKs demander une augmentation de quota, consultez la section Demander une augmentation de quota dans le Guide de l'utilisateur du Service Quotas.

Restriction sur les e-mails envoyés à l'aide du port 25

Sur toutes les instances, Amazon EC2 limite le trafic sortant aux adresses IP publiques via le port 25 par défaut. Vous pouvez demander que cette restriction soit supprimée. Pour plus d'informations, consultez Comment supprimer la restriction sur le port 25 de mon EC2 instance Amazon ou de ma fonction Lambda ?

Note

Cette restriction ne s'applique pas au trafic sortant envoyé sur le port 25 aux :

- Adresses IP dans le CIDR bloc principal du bloc VPC dans lequel se trouve l'interface réseau d'origine.
- Les adresses IP CIDRs sont définies en RFC1918, RFC6598 et RFC 4193.

Surveillez les EC2 ressources Amazon

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de vos EC2 instances Amazon et de vos AWS solutions. Vous devez collecter des données de surveillance provenant de tous les composants de vos AWS solutions afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant.

AWS fournit différents outils que vous pouvez utiliser pour surveiller AmazonEC2. Les tableaux de bord Amazon EC2 et de CloudWatch la console fournissent une at-a-glance vue d'ensemble de l'état de votre EC2 environnement Amazon. En outre, nous fournissons les services suivants :

- Contrôles de l'état du système : surveillez les AWS systèmes requis pour utiliser votre instance afin de vous assurer qu'ils fonctionnent correctement. Ces vérifications détectent les problèmes liés à votre instance qui nécessitent une AWS intervention pour les réparer. Lorsqu'un contrôle de statut échoue, vous pouvez choisir d'attendre qu' AWS résolve le problème ou le résoudre vous-même (par exemple, en arrêtant et en redémarrant une instance, ou en y mettant fin et en la remplaçant). Voici quelques exemples de problèmes entraînant l'échec des contrôles de statut du système :
  - Perte de connectivité réseau
  - Perte d'alimentation système
  - Problèmes logiciels sur un hôte physique
  - Problèmes matériels sur un hôte physique ayant un impact sur l'accessibilité du réseau

  Pour plus d'informations, veuillez consulter Contrôles de statut pour les EC2 instances Amazon.
- Contrôles de l'état de l'instance : surveillez la configuration logicielle et réseau de votre instance individuelle. Ces contrôles détectent les problèmes nécessitant votre intervention pour les résoudre. Lorsqu'un contrôle du statut de l'instance échoue, vous devez généralement résoudre le problème vous-même (en redémarrant par exemple l'instance ou en apportant des modifications à votre système d'exploitation). Voici quelques exemples de problèmes susceptibles d'entraîner l'échec des contrôles du statut de l'instance :
  - Échec de contrôles de statut de système
  - Configuration de mise en réseau ou de démarrage incorrecte
  - Mémoire épuisée
  - Système de fichiers corrompu
  - Noyau incompatible

Pour de plus amples informations, veuillez consulter Contrôles de statut pour les EC2 instances Amazon.

- CloudWatch Alarmes Amazon : surveillez une seule métrique sur une période que vous spécifiez et effectuez une ou plusieurs actions en fonction de la valeur de la métrique par rapport à un seuil donné sur un certain nombre de périodes. L'action est une notification envoyée à une rubrique Amazon Simple Notification Service (AmazonSNS) ou à une politique Amazon EC2 Auto Scaling. Les alarmes déclenchent des actions uniquement pour les changements d'état prolongés. CloudWatch les alarmes ne déclencheront pas d'actions simplement parce qu'elles sont dans un état particulier ; l'état doit avoir changé et être maintenu pendant un certain nombre de périodes. Pour de plus amples informations, veuillez consulter Surveillez vos instances à l'aide de CloudWatch.
- Amazon EventBridge events — Automatisez vos AWS services et répondez automatiquement aux événements du système. Les événements issus AWS des services sont transmis EventBridge en temps quasi réel, et vous pouvez spécifier des actions automatisées à effectuer lorsqu'un événement correspond à une règle que vous avez écrite. Pour de plus amples informations, veuillez consulter the section called “Automatisez l'utilisation EventBridge”.
- AWS CloudTrail journaux — Capturez des informations détaillées sur les appels passés à Amazon EC2 API et stockez-les sous forme de fichiers journaux dans Amazon S3. Vous pouvez utiliser CloudTrail les journaux pour déterminer quels appels ont été passés, l'adresse IP source de l'appel, l'auteur de l'appel et la date de l'appel. Pour de plus amples informations, veuillez consulter the section called “Enregistrez les API appels en utilisant CloudTrail”.
- CloudWatch agent : collectez les journaux et les mesures au niveau du système auprès des hôtes et des invités sur vos EC2 instances et sur vos serveurs sur site. Pour plus d'informations, consultez la section Collecte de métriques et de journaux à partir d'EC2instances Amazon et de serveurs sur site avec l' CloudWatch agent dans le guide de l' CloudWatch utilisateur Amazon.

Surveillez l'état de vos EC2 instances Amazon

Vous pouvez surveiller le statut de vos instances en affichant les contrôles de statut et les événements planifiés pour vos instances.

Une vérification de statut vous fournit les informations qui résultent des contrôles automatisés effectués par AmazonEC2. Ces contrôles automatisés détectent si des problèmes spécifiques concernent vos instances. Les informations de vérification du statut, associées aux données fournies

par Amazon CloudWatch, vous offrent une visibilité opérationnelle détaillée sur chacune de vos instances.

Vous pouvez également consulter le statut d' événements spécifiques planifiés pour vos instances. Les statuts des événements fournissent des informations sur les activités à venir planifiées pour vos instances, comme le redémarrage ou la mise hors service. Ils fournissent aussi les heures prévues de début et de fin de chaque événement.

Table des matières

Contrôles de statut pour les EC2 instances Amazon

Grâce à la surveillance de l'état des instances, vous pouvez rapidement déterminer si Amazon EC2 a détecté des problèmes susceptibles d'empêcher vos instances d'exécuter des applications. Amazon EC2 effectue des contrôles automatisés sur chaque EC2 instance en cours d'exécution afin d'identifier les problèmes matériels et logiciels. Vous pouvez afficher les résultats de ces contrôles de statut pour identifier des problèmes spécifiques et détectables. Les données d'état des événements complètent les informations EC2 déjà fournies par Amazon sur l'état de chaque instance (telles que`pending`,`running`,`stopping`) et les indicateurs d'utilisation CloudWatch surveillés par Amazon (CPUutilisation, trafic réseau et activité du disque).

Les contrôles de statut sont exécutés toutes les minutes et chacun d'entre eux renvoie un statut de réussite ou d'échec. Si tous les contrôles réussissent, le statut global de l'instance est OK. Si un ou plusieurs contrôles échouent, le statut global de l'instance est dégradé. Les vérifications de statut sont intégrées à AmazonEC2, elles ne peuvent donc pas être désactivées ou supprimées.

Lorsqu'une vérification de statut échoue, la CloudWatch métrique correspondante pour les vérifications de statut est incrémentée. Pour de plus amples informations, veuillez consulter Métriques de contrôle de statut. Vous pouvez utiliser ces mesures pour créer des CloudWatch alarmes déclenchées en fonction du résultat des vérifications d'état. Par exemple, vous pouvez créer une alarme pour vous avertir si des contrôles de statut échouent sur une instance spécifique. Pour de plus amples informations, veuillez consulter Créez des CloudWatch alarmes pour les EC2 instances Amazon qui échouent aux vérifications de statut.

Vous pouvez également créer une CloudWatch alarme Amazon qui surveille une EC2 instance Amazon et la récupère automatiquement si elle est altérée en raison d'un problème sous-jacent. Pour de plus amples informations, veuillez consulter Résilience des instances.

Sommaire

Types de contrôles de statut

Il existe trois types de contrôles de statuts.

- Contrôles de statut de système
- Contrôles de statut des instances
- Contrôles EBS d'état joints

Contrôles de statut de système

Les vérifications de l'état du système surveillent les AWS systèmes sur lesquels votre instance s'exécute. Ces contrôles détectent les problèmes sous-jacents liés à votre instance qui nécessitent une intervention de résolution d' AWS . Lorsqu'une vérification de l'état du système échoue, vous pouvez choisir AWS d'attendre que le problème soit résolu ou de le résoudre vous-même. Pour les instances soutenues par AmazonEBS, vous pouvez arrêter et démarrer l'instance vous-même, ce qui entraîne dans la plupart des cas la migration de l'instance vers un nouvel hôte. Pour les instances Linux basées sur le stockage d'instance, vous pouvez mettre l'instance hors service et la remplacer. Pour les instances Windows, le volume racine doit être un EBS volume Amazon ; le magasin d'instances n'est pas pris en charge pour le volume racine. Notez que les volumes de stockage d'instance sont éphémères et que toutes les données sont perdues lorsque l'instance est arrêtée.

Voici des exemples de problèmes pouvant entraîner l'échec des contrôles de statut :

- Perte de connectivité réseau
- Perte d'alimentation système

- Problèmes logiciels sur un hôte physique
- Problèmes matériels sur un hôte physique ayant un impact sur l'accessibilité du réseau

Si la vérification de l'état du système échoue, nous incrémentons la métrique StatusCheckFailed_System.

Instances nues

Si vous effectuez un redémarrage à partir du système d'exploitation sur une instance nue (bare metal), la vérification de l'état du système peut renvoyer temporairement un état d'échec. Lorsque l'instance devient disponible, la vérification de l'état du système doit renvoyer un état de succès.

Contrôles de statut des instances

Contrôles du statut de l'instance Surveillez la configuration logicielle et réseau de votre instance. Amazon EC2 vérifie l'état de l'instance en envoyant une demande de protocole de résolution d'adresses (ARP) à l'interface réseau (NIC). Ces contrôles détectent les problèmes nécessitant votre intervention pour les résoudre. Lorsqu'un contrôle de statut d'instance échoue, vous devez généralement résoudre le problème vous-même (par exemple, en redémarrant l'instance ou en effectuant des changements de configuration sur l'instance).

> **Note**
>
> Les distributions Linux récentes utilisées `systemd-networkd` pour la configuration réseau peuvent rendre compte des vérifications de santé différemment des distributions précédentes. Au cours du processus de démarrage, ce type de réseau peut démarrer plus tôt et éventuellement se terminer avant d'autres tâches de démarrage susceptibles d'affecter l'état de l'instance. Les vérifications d'état qui dépendent de la disponibilité du réseau peuvent signaler un état sain avant que les autres tâches ne soient terminées.

Voici des exemples de problèmes pouvant entraîner l'échec des contrôles d'instance :

- Échec de contrôles de statut de système
- Configuration de mise en réseau ou de démarrage incorrecte
- Mémoire épuisée
- Système de fichiers corrompu

- Noyau incompatible
- [Instances Windows] Lors du redémarrage de l'instance ou lorsqu'une instance basée sur le stockage d'une instance Windows est groupée, une vérification de l'état de l'instance signale un échec jusqu'à ce que l'instance soit de nouveau disponible.

Si la vérification de l'état d'une instance échoue, nous incrémentons la métrique StatusCheckFailed_Instance.

Instances nues

Si vous effectuez un redémarrage à partir du système d'exploitation sur une instance nue (bare metal), la vérification de l'état de l'instance peut renvoyer temporairement un état d'échec. Lorsque l'instance devient disponible, la vérification de l'état de l'instance doit renvoyer un état de succès.

Contrôles EBS d'état joints

Les contrôles de EBS statut attachés vérifient si les EBS volumes Amazon attachés à une instance sont accessibles et capables d'effectuer des opérations d'E/S. La `StatusCheckFailed_AttachedEBS` métrique est une valeur binaire qui indique une altération si un ou plusieurs EBS volumes attachés à l'instance ne sont pas en mesure d'effectuer les opérations d'E/S. Ces vérifications d'état détectent les problèmes sous-jacents liés au calcul ou à EBS l'infrastructure Amazon. Lorsque la métrique de vérification de EBS statut jointe échoue, vous pouvez soit AWS attendre que le problème soit résolu, soit prendre des mesures, telles que le remplacement des volumes concernés ou l'arrêt et le redémarrage de l'instance.

Voici des exemples de problèmes susceptibles d'entraîner l'échec des vérifications de EBS statut des pièces jointes :

- Problèmes matériels ou logiciels sur les sous-systèmes de stockage sous-jacents aux volumes EBS
- Problèmes matériels sur l'hôte physique qui ont un impact sur l'accessibilité des volumes EBS
- Problèmes de connectivité entre l'instance et les EBS volumes

Vous pouvez utiliser la métrique `StatusCheckFailed_AttachedEBS` pour améliorer la résilience de votre charge de travail. Vous pouvez utiliser cette métrique pour créer des CloudWatch alarmes Amazon déclenchées en fonction du résultat de la vérification de statut. Par exemple, vous pouvez basculer vers une instance secondaire ou une zone de disponibilité lorsque vous détectez un impact prolongé. Vous pouvez également surveiller les performances d'E/S de chaque volume connecté

à l'aide de EBS CloudWatch métriques pour détecter et remplacer le volume endommagé. Si votre charge de travail ne génère d'E/S vers aucun des EBS volumes attachés à votre instance et que la vérification de l'EBSétat associée indique un dysfonctionnement, vous pouvez arrêter et démarrer l'instance pour résoudre les problèmes liés à l'hôte physique qui ont un impact sur l'accessibilité des volumes. EBS Pour plus d'informations, consultez CloudWatch les statistiques Amazon pour Amazon EBS.

Vous pouvez également configurer vos groupes Amazon EC2 Auto Scaling pour détecter les échecs de vérification de EBS statut associés, puis remplacer l'instance affectée par une nouvelle instance. Pour plus d'informations, consultez la section Surveiller et remplacer les instances Auto Scaling par des EBS volumes Amazon altérés dans le manuel Amazon EC2 Auto Scaling User Guide.

> **Note**
>
> La métrique de vérification de EBS statut ci-jointe n'est disponible que pour les instances Nitro.

Afficher les vérifications de statut pour les EC2 instances Amazon

Pour consulter les contrôles de statut, utilisez l'une des méthodes suivantes.

Console

Pour afficher les contrôles de statut

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sur la page instances, la colonne Status check (Vérification de statut) répertorie le statut opérationnel de chaque instance.
4. Pour afficher le statut d'une instance spécifique, sélectionnez-la, puis choisissez l'onglet Statuts et alarmes.

   Lorsqu'un contrôle de statut d'instance échoue, vous devez généralement résoudre le problème vous-même (par exemple, en redémarrant l'instance ou en effectuant des changements de configuration sur celle-ci). Pour résoudre vous-même des échecs de contrôle de statut de système ou d'instance, consultez Résoudre les problèmes des instances Amazon EC2 Linux dont les vérifications d'état ont échoué.

5. Pour consulter les CloudWatch mesures relatives aux vérifications de statut, dans l'onglet État et alarmes, développez Métriques pour afficher les graphiques des mesures suivantes :

   - Échec du contrôle de statut au niveau du système
   - Échec du contrôle de statut au niveau de l'instance
   - La vérification de l'état de la pièce jointe a échoué EBS

   Pour de plus amples informations, veuillez consulter the section called "Métriques de contrôle de statut".

Command line

Vous pouvez consulter les vérifications d'état des instances en cours d'exécution à l'aide de la commande describe-instance-status(AWS CLI).

Pour afficher le statut de toutes les instances, utilisez la commande suivante :

```
aws ec2 describe-instance-status
```

Pour obtenir le statut de toutes les instances avec un statut d'instance `impaired`, utilisez la commande suivante.

```
aws ec2 describe-instance-status \
--filters Name=instance-status.status,Values=impaired
```

Pour obtenir le statut d'une seule instance, utilisez la commande suivante.

```
aws ec2 describe-instance-status \
--instance-ids i-1234567890abcdef0
```

Vous pouvez également utiliser les commandes suivantes :

- Get-EC2InstanceStatus (AWS Tools for Windows PowerShell)
- DescribeInstanceStatus(EC2Requête AmazonAPI)

Si vous avez une instance avec un statut d'échec (failed), consultez Résoudre les problèmes des instances Amazon EC2 Linux dont les vérifications d'état ont échoué.

Créez des CloudWatch alarmes pour les EC2 instances Amazon qui échouent aux vérifications de statut

Vous pouvez utiliser les métriques de vérification de statut pour créer des CloudWatch alarmes afin de vous avertir en cas d'échec de la vérification de statut d'une instance.

> **Important**
>
> Les contrôles d'état et les alarmes de contrôle d'état peuvent temporairement passer à un état de données insuffisant s'il manque des points de données métriques. Bien que cela soit rare, cela peut se produire en cas d'interruption des systèmes de reporting des métriques, même lorsqu'une instance est saine. Nous vous recommandons de traiter cet état comme une donnée manquante plutôt que comme un échec de vérification du statut ou comme une violation d'alarme, en particulier lorsque vous effectuez des actions d'arrêt, de terminaison, de redémarrage ou de restauration sur l'instance en réponse.

Pour créer une alarme de contrôle de statut, utilisez l'une des méthodes suivantes :

Console

Utilisez la procédure suivante pour configurer une alarme qui vous envoie une notification par e-mail, ou arrête, met fin ou récupère une instance en cas d'échec du contrôle de statut de cette dernière.

Pour créer une alarme de contrôle de statut

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance, choisissez l'onglet Status Checks (Contrôles des statuts), puis choisissez Actions, Create status check alarm (Créer une alarme de contrôle de statut).
4. Sur la page Gérer les CloudWatch alarmes, sous Ajouter ou modifier une alarme, choisissez Créer une alarme.
5. Pour les notifications d'alarme, activez le bouton pour configurer les notifications Amazon Simple Notification Service (AmazonSNS). Sélectionnez un SNS sujet Amazon existant ou entrez un nom pour créer un nouveau sujet.

Si vous ajoutez une adresse e-mail à la liste des destinataires ou si vous créez un nouveau sujet, Amazon SNS envoie un e-mail de confirmation d'abonnement à chaque nouvelle adresse. Chaque destinataire doit confirmer l'abonnement en choisissant le lien contenu dans ce message. Les notifications d'alerte sont envoyées uniquement aux adresses confirmées.

6. Activez Alarm action (Action d'alarme) pour spécifier une action à effectuer lorsque l'alarme est déclenchée. Sélectionnez l'action.
7. Pour Alarm thresholds (Seuils d'alarme), sélectionnez la métrique et les critères de l'alarme.

   Vous pouvez laisser les paramètres par défaut pourRegrouper les échantillons par (moyenne) et Type de données à échantillonner (échec de la vérification de statut : soit), ou vous pouvez les modifier en fonction de vos besoins.

   Dans Consecutive period (Période consécutive), définissez le nombre de périodes que vous souhaitez évaluer et, dans Period (Période), sélectionnez la période d'évaluation avant de déclencher l'alarme et d'envoyer un e-mail.
8. (Facultatif) Pour Exemple de données de métrique, choisissez Ajouter au tableau de bord.
9. Sélectionnez Create (Créer).

Si vous devez apporter des modifications à une alarme de statut d'instance, vous pouvez modifier celle-ci.

Pour modifier une alarme de contrôle de statut

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance et choisissez Actions, Surveillance, Gestion des CloudWatch alarmes.
4. Sur la page Gérer les CloudWatch alarmes, sous Ajouter ou modifier une alarme, choisissez Modifier une alarme.
5. Dans Search for alarm (Rechercher une alarme), sélectionnez l'alarme.
6. Une fois les modifications terminées, sélectionnez Update (Mettre à jour).

Command line

Dans l'exemple suivant, l'alarme publie une notification dans un SNS sujet lorsque l'instance échoue à la vérification de l'instance ou à la vérification de l'état du système pendant au moins

deux périodes consécutives. `arn:aws:sns:us-west-2:111122223333:my-sns-topic` La CloudWatch métrique utilisée est`StatusCheckFailed`.

Pour créer une alarme de vérification de statut à l'aide du AWS CLI

1. Sélectionnez un SNS sujet existant ou créez-en un nouveau. Pour plus d'informations, consultez la section Utilisation du AWS CLI avec Amazon SNS dans le guide de AWS Command Line Interface l'utilisateur.
2. Utilisez la commande list-metrics suivante pour afficher les CloudWatch métriques Amazon disponibles pour Amazon. EC2

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

3. Utilisez la put-metric-alarmcommande suivante pour créer l'alarme.

```
aws cloudwatch put-metric-alarm \
--alarm-name StatusCheckFailed-Alarm-for-i-1234567890abcdef0 \
--metric-name StatusCheckFailed \
--namespace AWS/EC2 \
--statistic Maximum \
--dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
--unit Count \
--period 300 \
--evaluation-periods 2 \
--threshold 1 \
--comparison-operator GreaterThanOrEqualToThreshold \
--alarm-actions arn:aws:sns:us-west-2:111122223333:my-sns-topic
```

La période est la période, en secondes, pendant laquelle CloudWatch les métriques Amazon sont collectées. Dans cet exemple, 300, qui correspond à 60 secondes multipliées par 5 minutes, est utilisé. La période d'évaluation est le nombre de périodes consécutives pour lesquelles la valeur de la métrique doit être comparée au seuil. Dans cet exemple, 2 est utilisé. Les actions d'alarme correspondent aux actions à exécuter lors du déclenchement de cette alarme. Cet exemple configure l'alarme pour envoyer un e-mail via AmazonSNS.

Événements de changement d'état pour les EC2 instances Amazon

Amazon EC2 envoie un `EC2 Instance State-change Notification` événement à Amazon EventBridge lorsque l'état d'une instance change.

Voici un exemple de données pour cet événement. Dans cet exemple, l'instance est entrée dans l'état `pending`.

```
{
   "id":"7bf73129-1428-4cd3-a780-95db273d1602",
   "detail-type":"EC2 Instance State-change Notification",
   "source":"aws.ec2",
   "account":"123456789012",
   "time":"2021-11-11T21:29:54Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111"
   ],
   "detail":{
      "instance-id":"i-abcd1111",
      "state":"pending"
   }
}
```

Les valeurs possibles pour `state` sont :

- `pending`
- `running`
- `stopping`
- `stopped`
- `shutting-down`
- `terminated`

Lorsque vous lancez ou démarrez une instance, elle entre dans l'état `pending`, puis dans l'état `running`. Lorsque vous arrêtez une instance, elle entre dans l'état `stopping`, puis dans l'état `stopped`. Lorsque vous résiliez une instance, elle entre dans l'état `shutting-down`, puis dans l'état `terminated`.

Créez une alarme qui envoie un e-mail lorsqu'une EC2 instance Amazon change d'état

Pour recevoir des notifications par e-mail lorsque votre instance change d'état, créez un SNS sujet Amazon, puis une EventBridge règle pour l'`EC2 Instance State-change Notification`événement.

Pour créer une rubrique SNS

1. Ouvrez la SNS console Amazon sur https://console.aws.amazon.com/sns/v3/home.
2. Dans le volet de navigation, choisissez Rubriques.
3. Choisissez Créer une rubrique.
4. Pour Type, choisissez Standard.
5. Pour Nom, saisissez un nom pour votre rubrique.
6. Choisissez Créer une rubrique.
7. Choisissez Créer un abonnement.
8. Pour Protocole, choisissez E-mail.
9. Pour Point de terminaison, saisissez l'adresse e-mail qui reçoit les notifications.
10. Choisissez Créer un abonnement.
11. Vous recevrez un e-mail avec l'objet suivant : AWS Notification - Subscription Confirmation. Suivez les instructions pour confirmer votre abonnement.

Pour créer une EventBridge règle

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Choisissez Créer une règle.
3. Pour Nom, saisissez un nom pour votre règle.
4. Pour Type de règle, choisissez Règle avec un modèle d'événement.
5. Choisissez Suivant.
6. Pour Event pattern (Modèle d'événement), procédez comme suit :
   a. Pour Event source (Source d'événement), choisissez services AWS.
   b. Pour service AWS, choisissez EC2.
   c. Pour Type d'événement, choisissez Notification de changement d'état de l'EC2instance.
   d. Par défaut, nous envoyons des notifications pour tout changement d'état pour n'importe quelle instance. Si vous préférez, vous pouvez sélectionner des états ou des instances spécifiques.
7. Choisissez Suivant.
8. Spécifiez une cible comme suit :

a. Pour Target types (Types de cibles), choisissez service AWS.

b. Pour Sélectionner une cible, choisissez un SNSsujet.

c. Dans le champ Sujet, choisissez le SNS sujet que vous avez créé lors de la procédure précédente.

9. Choisissez Suivant.
10. (Facultatif) Ajoutez des identifications à votre règle.
11. Choisissez Suivant.
12. Choisissez Créer une règle.
13. Pour tester votre règle, déclenchez un changement d'état. Par exemple, démarrez une instance arrêtée, arrêtez une instance en cours d'exécution ou lancez une instance. Vous recevrez des e-mails avec l'objet suivant : AWS Notification Message. Le corps de l'e-mail contient les données de l'événement.

Événements planifiés pour les EC2 instances Amazon

AWS peut planifier des événements pour vos instances, tels qu'un redémarrage, un arrêt/démarrage ou une mise hors service. Ces événements ne se produisent pas fréquemment. Si l'une de vos instances est affectée par un événement programmé, AWS envoie un e-mail à l'adresse e-mail associée à votre AWS compte avant l'événement prévu. Cet e-mail fournit des détails concernant l'événement, y compris les dates de début et de fin. En fonction de l'événement, vous pourrez peut-être prendre des mesures pour contrôler le calendrier de l'événement. AWS envoie également un AWS Health événement, que vous pouvez surveiller et gérer à l'aide d'Amazon CloudWatch Events. Pour plus d'informations sur la surveillance des AWS Health événements avec CloudWatch, consultez la section Surveillance AWS Health des événements avec CloudWatch des événements.

Les événements planifiés sont gérés par AWS ; vous ne pouvez pas planifier d'événements pour vos instances. Vous pouvez consulter les événements planifiés par AWS, personnaliser les notifications d'événements planifiés pour inclure ou supprimer des balises dans la notification par e-mail, et effectuer des actions lorsqu'il est prévu de redémarrer, de retirer ou d'arrêter une instance.

Pour mettre à jour les informations de contact de votre compte afin d'être sûr d'être averti à propos d'événements planifiés, accédez à la page Account Settings (Paramètres du compte).

> **Note**
>
> Lorsqu'une instance est affectée par un événement planifié et qu'elle fait partie d'un groupe Auto Scaling, Amazon EC2 Auto Scaling la remplace finalement dans le cadre de ses bilans de santé, sans qu'aucune autre action de votre part ne soit nécessaire. Pour plus d'informations sur les contrôles de santé effectués par Amazon EC2 Auto Scaling, consultez la section Contrôles de santé des instances Auto Scaling dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.

Types d'événements planifiés

Amazon EC2 peut créer les types d'événements suivants pour vos instances, lorsque l'événement se produit à une heure planifiée :

- Instance stop (Arrêt de l'instance) : à l'heure planifiée, l'instance est arrêté. Lorsque vous la redémarrez, elle est migrée vers un nouvel hôte. S'applique uniquement aux instances soutenues par AmazonEBS.
- Retrait de l'instance : à l'heure prévue, l'instance est arrêtée si elle est soutenue par AmazonEBS, ou résiliée si elle est soutenue par un magasin d'instances.
- Instance reboot (Redémarrage de l'instance) : à l'heure planifiée, l'instance est redémarrée.
- System reboot (Redémarrage du système) : à l'heure planifiée, l'hôte de l'instance est redémarré.
- System maintenance (Maintenance du système) : à l'heure planifiée, l'instance peut être temporairement affectée par une maintenance du réseau ou une maintenance de l'alimentation.

Table des matières

Actions recommandées pour les EC2 instances Amazon affectées par des événements planifiés

La rubrique suivante explique les mesures que vous devez prendre lorsque votre EC2 instance Amazon est affectée par un événement planifié.

Rubriques

Actions pour les instances dont l'arrêt ou la mise hors service sont prévus

Lorsqu'il AWS détecte une défaillance irréparable de l'hôte sous-jacent de votre instance, il planifie l'arrêt ou la résiliation de l'instance, en fonction du type de périphérique racine de l'instance. Si le périphérique racine est un EBS volume, l'arrêt de l'instance est programmé. Si le périphérique racine est un volume de stockage d'instance, la fin de l'instance est planifiée. Pour plus d'informations, veuillez consulter Mise hors service d'instance.

> **Important**
>
> Les données stockées sur des volumes de stockage d'instance sont perdues lorsque l'instance est arrêtée, mise en veille prolongée ou résiliée. Cela inclut les volumes de stockage d'instance attachés à une instance dont le périphérique racine est un EBS volume. Veillez à enregistrer les données de vos volumes de stockage d'instance dont vous aurez besoin ultérieurement avant que l'instance ne soit arrêtée, mise en veille prolongée ou résiliée.

Actions pour les instances soutenues par Amazon EBS

Vous pouvez attendre que l'instance s'arrête comme planifié. Sinon, vous pouvez arrêter et démarrer l'instance vous-même, ce qui la migre vers un nouvel ordinateur hôte. Pour plus d'informations sur l'arrêt de votre instance, ainsi que des informations sur les changements apportés à la configuration de votre instance lorsque celle-ci est arrêtée, consultez Arrêtez et démarrez les EC2 instances Amazon.

Vous pouvez automatiser un arrêt immédiat et un démarrage en réponse à un événement planifié d'arrêt d'instance. Pour plus d'informations, consultez Automatiser les actions pour les EC2 instances Amazon dans le Guide de l'AWS Health utilisateur.

Actions pour les instances basées sur le stockage d'instance

Nous vous recommandons de lancer une instance de remplacement à partir de votre instance la plus récente AMI et de migrer toutes les données nécessaires vers l'instance de remplacement avant la date prévue de mise hors service de l'instance. Ensuite, vous pouvez mettre fin à l'instance d'origine ou attendre que l'instance prenne fin comme planifié.

Actions pour les instances dont le redémarrage est prévu

Lorsqu' AWS il doit effectuer des tâches telles que l'installation de mises à jour ou la maintenance de l'hôte sous-jacent, il peut planifier le redémarrage de l'instance ou de l'hôte sous-jacent. Vous pouvez reprogrammer la plupart des événements de redémarrage afin que votre instance soit redémarrée à une date et une heure spécifiques qui vous conviennent.

Afficher le type d'événement de reboot

Vous pouvez déterminer si l'événement de redémarrage est un redémarrage d'instance ou de système à l'aide de l'une des méthodes suivantes.

Console

Pour afficher le type d'événement de redémarrage planifié

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Événements.
3. Choisissez Type de ressource : instance dans la liste des filtres.
4. Pour chaque instance, affichez la valeur dans la colonne Type d'événement. La valeur est soit system-reboot (redémarrage du système), soit instance-reboot (redémarrage de l'instance).

AWS CLI

Pour afficher le type d'événement de redémarrage planifié

Utilisez la describe-instance-statuscommande.

```
aws ec2 describe-instance-status \
```

```
    --instance-id i-1234567890abcdef0
```

Pour les événements de redémarrage programmés, la valeur de `Code` est soit `system-reboot` ou `instance-reboot`. L'exemple de sortie suivant affiche un événement `system-reboot`.

```
[
    "Events": [
                {
                    "InstanceEventId": "instance-event-0d59937288b749b32",
                    "Code": "system-reboot",
                    "Description": "The instance is scheduled for a reboot",
                    "NotAfter": "2019-03-14T22:00:00.000Z",
                    "NotBefore": "2019-03-14T20:00:00.000Z",
                    "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
                }
            ]
]
```

Actions pour le redémarrage d'une instance

Vous pouvez attendre que le redémarrage d'instance se produise dans sa fenêtre de maintenance planifiée, reprogrammer le redémarrage d'instance à une date et heure qui vous conviennent, ou redémarrer vous-même l'instance au moment qui vous convient.

Après le redémarrage de votre instance, l'événement planifié pour le redémarrage d'instance est annulé et la description de l'événement est mise à jour. La maintenance en attente pour l'hôte sous-jacent est effectuée et vous pouvez recommencer à utiliser votre instance après son démarrage complet.

Actions pour le redémarrage du système

Vous ne pouvez pas redémarrer le système vous-même. Vous pouvez attendre que le redémarrage de système se produise dans sa fenêtre de maintenance planifiée, ou vous pouvez reprogrammer le redémarrage de système à une date et heure qui vous conviennent. Un redémarrage de système se termine généralement en quelques minutes. Après le redémarrage du système, l'instance conserve son adresse IP et son DNS nom, et toutes les données présentes sur les volumes de stockage d'instance locaux sont préservées. Une fois le redémarrage du système achevé, l'événement planifié pour l'instance est effacé et vous pouvez vérifier que les logiciels sur votre instance fonctionnent comme prévu.

Sinon, s'il est nécessaire de maintenir l'instance à un autre moment et que vous ne pouvez pas reprogrammer le redémarrage du système, vous pouvez arrêter et démarrer une instance EBS soutenue par Amazon, qui la migre vers un nouvel hôte. Par contre, les données sur les volumes de stockage d'instance locaux ne sont pas conservées. Vous pouvez également automatiser un arrêt d'instance immédiat et un démarrage en réponse à un événement planifié de réinitialisation du système. Pour plus d'informations, consultez la section Automatisation des actions pour les EC2 instances dans le guide de l'AWS Health utilisateur. Pour une instance sauvegardée par un stockage d'instance, si vous ne pouvez pas reprogrammer le redémarrage du système, vous pouvez lancer une instance de remplacement à partir de la plus récenteAMI, migrer toutes les données nécessaires vers l'instance de remplacement avant la période de maintenance planifiée, puis mettre fin à l'instance d'origine.

Actions pour les instances dont la maintenance est planifiée

Lorsqu' AWS il doit gérer l'hôte sous-jacent d'une instance, il planifie la maintenance de l'instance. Il existe deux types d'événements de maintenance : maintenance du réseau et maintenance de l'alimentation.

Lors d'une maintenance du réseau, les instances planifiées perdent leur connectivité réseau pendant une courte période. La connectivité réseau normale vers votre instance est restaurée une fois la maintenance terminée.

Lors d'une maintenance de l'alimentation, les instances planifiées sont mises hors ligne pendant une courte période, puis redémarrées. Lorsqu'un redémarrage est effectué, les paramètres de configuration de votre instance sont conservés.

Une fois que votre instance a redémarré (cela prend normalement quelques minutes), vérifiez que votre application fonctionne comme prévu. À ce stade, votre instance ne devrait plus avoir d'événement planifié associé. Dans le cas contraire, la description de l'événement planifié commence par [Terminé]. Cela peut parfois prendre jusqu'à 1 heure pour que la description de statut de cette instance soit actualisée. Les événements de maintenance terminés sont affichés sur le tableau de bord de EC2 la console Amazon pendant une semaine au maximum.

Actions pour les instances soutenues par Amazon EBS

Vous pouvez attendre que la maintenance ait lieu comme planifié. Sinon, vous pouvez arrêter et démarrer l'instance, ce qui la migre vers un nouvel hôte. Pour plus d'informations sur l'arrêt de votre instance, ainsi que des informations sur les changements apportés à la configuration de votre instance lorsque celle-ci est arrêtée, consultez Arrêtez et démarrez les EC2 instances Amazon.

Vous pouvez automatiser un arrêt immédiat et un démarrage en réponse à un événement planifié de maintenance. Pour plus d'informations, consultez la section Automatisation des actions pour les EC2 instances dans le guide de l'AWS Health utilisateur.

Actions pour les instances basées sur le stockage d'instance

Vous pouvez attendre que la maintenance ait lieu comme planifié. Sinon, si vous souhaitez maintenir un fonctionnement normal pendant une période de maintenance planifiée, vous pouvez lancer une instance de remplacement à partir de la plus récenteAMI, migrer toutes les données nécessaires vers l'instance de remplacement avant la fenêtre de maintenance planifiée, puis mettre fin à l'instance d'origine.

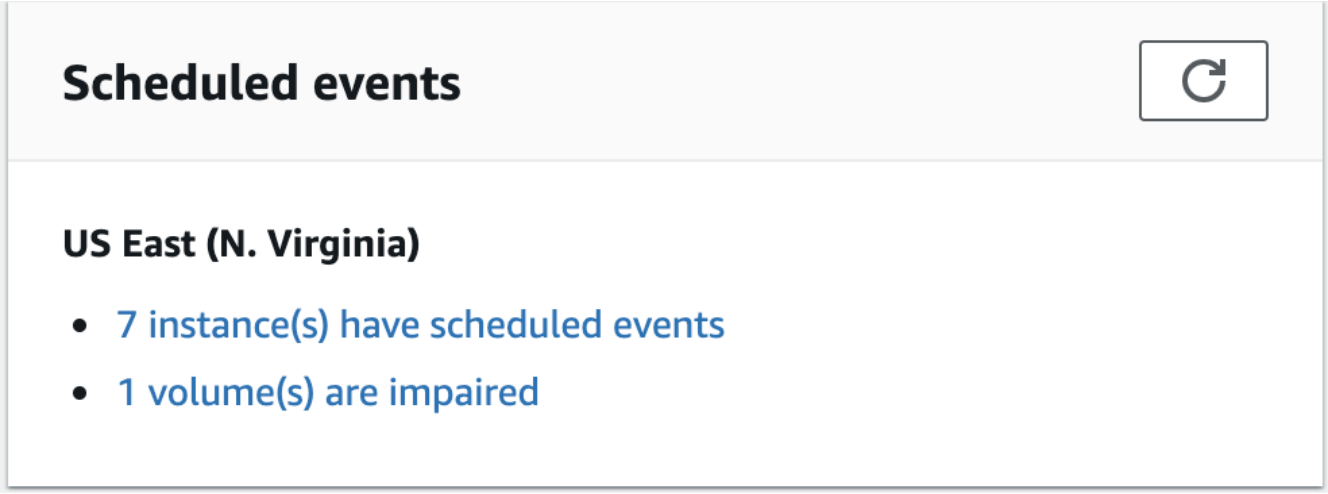
Afficher les événements planifiés qui affectent vos EC2 instances Amazon

En plus de recevoir une notification des événements planifiés par e-mail, vous pouvez consulter les événements planifiés en utilisant une des méthodes suivantes.

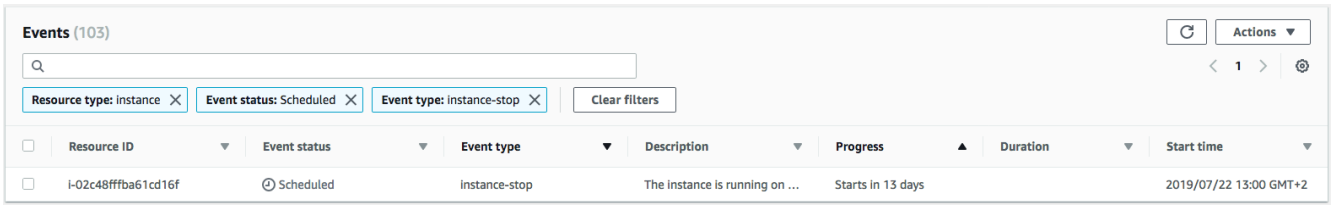
Console

Pour afficher les événements planifiés pour vos instances

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Le tableau de bord affiche toutes les ressources avec un événement associé sous Événements planifiés.



3. Pour obtenir plus de détails, sélectionnez Événements dans le volet de navigation. Toutes les ressources avec un événement associé sont affichées. Vous pouvez filtrer par caractéristiques telles que le type d'événement, le type de ressource et la zone de disponibilité.



AWS CLI

Pour afficher les événements planifiés pour vos instances

Utilisez la describe-instance-statuscommande.

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0 \
    --query "InstanceStatuses[].Events"
```

L'exemple de sortie suivant montre un événement de redémarrage :

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0d59937288b749b32",
            "Code": "system-reboot",
            "Description": "The instance is scheduled for a reboot",
            "NotAfter": "2019-03-15T22:00:00.000Z",
            "NotBefore": "2019-03-14T20:00:00.000Z",
            "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
         }

    ]
]
```

Voici un exemple de sortie montrant un événement de mise hors service d'instance.

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0e439355b779n26",

            "Code": "instance-stop",
            "Description": "The instance is running on degraded hardware",
            "NotBefore": "2015-05-23T00:00:00.000Z"
```

```
        }
    ]
]
```

PowerShell

Pour afficher les événements planifiés pour vos instances à l'aide de la AWS Tools for Windows PowerShell

Utilisez la commande Get-EC2InstanceStatus suivante.

```
PS C:\> (Get-EC2InstanceStatus -InstanceId i-1234567890abcdef0).Events
```

Voici un exemple de sortie montrant un événement de mise hors service d'instance.

```
Code         : instance-stop
Description  : The instance is running on degraded hardware
NotBefore    : 5/23/2015 12:00:00 AM
```

Instance metadata

Pour afficher les événements planifiés pour vos instances à l'aide des métadonnées de l'instance

Vous pouvez récupérer des informations sur les événements de maintenance actifs pour vos instances à partir des métadonnées de l'instance à l'aide de Service des métadonnées d'instance Version 2 ou Service des métadonnées d'instance Version 1.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/events/maintenance/scheduled
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/
scheduled
```

Voici un exemple de sortie contenant des informations sur un événement de redémarrage programmé du système, au JSON format.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "active"
  }
]
```

Pour afficher l'historique des événements terminés ou annulés pour vos instances à l'aide des métadonnées de l'instance

Vous pouvez récupérer des informations sur les événements terminés ou annulés pour vos instances à partir des métadonnées de l'instance à l'aide de Service des métadonnées d'instance Version 2 ou Service des métadonnées d'instance Version 1.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/maintenance/history
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/history
```

Voici un exemple de sortie contenant des informations sur un événement de redémarrage du système annulé et un événement de redémarrage du système terminé, au JSON format.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Canceled] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
```

```
    "State" : "canceled"
  },
  {
    "NotBefore" : "29 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Completed] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "29 Jan 2019 09:17:23 GMT",
    "State" : "completed"
  }
]
```

AWS Health

Vous pouvez utiliser le AWS Health Dashboard pour en savoir plus sur les événements susceptibles d'affecter votre instance. Il AWS Health Dashboard organise les problèmes en trois groupes : les problèmes ouverts, les modifications planifiées et les autres notifications. Le groupe des modifications planifiées contient des éléments qui sont en cours ou à venir.

Pour plus d'informations, consultez Premiers pas avec le AWS Health Dashboard dans le Guide de l'utilisateur AWS Health .

Personnalisez les notifications par e-mail pour les événements planifiés qui affectent les EC2 instances Amazon

Vous pouvez personnaliser les notifications d'événements planifiés pour inclure des balises dans la notification par e-mail. Cela facilite l'identification de la ressource affectée (instances ou Hôtes dédiés) et la hiérarchisation des actions pour l'événement à venir.

Lorsque vous personnalisez les notifications d'événements pour inclure des balises, vous pouvez choisir d'inclure :

- Toutes les balises associées à la ressource affectée
- Seules les balises spécifiques associées à la ressource affectée

Par exemple, supposons que vous assignez les balises `application`, `costcenter`, `project` et `owner` à toutes vos instances. Vous pouvez choisir d'inclure toutes les balises dans les notifications d'événements. Sinon, si vous souhaitez afficher uniquement les balises `owner` et `project` dans les notifications d'événements, vous pouvez choisir d'inclure uniquement ces balises.

Après avoir sélectionné les balises à inclure, les notifications d'événement incluront l'ID de ressource (ID d'instance ou Hôte dédié) et les paires clé de balise et valeur associées à la ressource affectée.

Tâches

- Inclure des balises dans les notifications d'événements
- Supprimer les balises des notifications d'événements
- Afficher les balises à inclure dans les notifications d'événements

Inclure des balises dans les notifications d'événements

Les balises que vous choisissez d'inclure s'appliquent à toutes les ressources (instances et Hôtes dédiés) de la région sélectionnée. Pour personnaliser les notifications d'événements dans d'autres régions, sélectionnez d'abord la région requise, puis effectuez les étapes suivantes.

Vous pouvez inclure des étiquettes dans les notifications d'événements à l'aide de l'une des méthodes suivantes.

Console

Pour inclure des balises dans les notifications d'événements

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Événements.
3. Choisissez Actions, Manage event notifications (Gérer les notifications d'événements).
4. Activez Inclure des balises dans les notifications d'événements.
5. Faites l'une des opérations suivantes, en fonction des balises que vous souhaitez inclure dans les notifications d'événement :
   - Pour inclure toutes les balises associées à l'instance affectée ou Hôte dédié, sélectionnez Inclure toutes les balises de ressource.
   - Pour sélectionner les balises à inclure, sélectionnez Choisir les balises à inclure, puis sélectionnez ou saisissez les clés de balise.
6. Choisissez Save (Enregistrer).

AWS CLI

Pour inclure toutes les balises dans les notifications d'événements

Utilisez la AWS CLI commande register-instance-event-notification-attributes et définissez le `IncludeAllTagsOfInstance` paramètre sur. `true`

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute "IncludeAllTagsOfInstance=true"
```

Pour inclure des balises spécifiques dans les notifications d'événements

Utilisez la AWS CLI commande register-instance-event-notification-attributes et spécifiez les balises à inclure à l'aide du `InstanceTagKeys` paramètre.

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute 'InstanceTagKeys=["tag_key_1", "tag_key_2",
 "tag_key_3"]'
```

Supprimer les balises des notifications d'événements

Vous pouvez supprimer les étiquettes des notifications d'événements à l'aide de l'une des méthodes suivantes.

Console

Pour supprimer les balises des notifications d'événements

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Événements.
3. Choisissez Actions, Manage event notifications (Gérer les notifications d'événements).
4. Pour supprimer toutes les balises des notifications d'événement, désactivez Inclure des balises dans les notifications d'événement.
5. Pour supprimer des balises spécifiques des notifications d'événements, sélectionnez le X) pour les clés de balise correspondantes.
6. Choisissez Save (Enregistrer).

AWS CLI

Pour supprimer toutes les balises des notifications d'événements

Utilisez la AWS CLI commande deregister-instance-event-notification-attributes et définissez le `IncludeAllTagsOfInstance` paramètre sur. `false`

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute "IncludeAllTagsOfInstance=false"
```

Pour supprimer des balises spécifiques des notifications d'événements

Utilisez la AWS CLI commande deregister-instance-event-notification-attributes et spécifiez les balises à supprimer à l'aide du `InstanceTagKeys` paramètre.

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute 'InstanceTagKeys=["tag_key_1", "tag_key_2",
 "tag_key_3"]'
```

Afficher les balises à inclure dans les notifications d'événements

Vous pouvez afficher les étiquettes qui doivent être incluses dans les notifications d'événement à l'aide de l'une des méthodes suivantes.

Console

Pour afficher les balises à inclure dans les notifications d'événements

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Événements.
3. Choisissez Actions, Manage event notifications (Gérer les notifications d'événements).

AWS CLI

Pour afficher les balises à inclure dans les notifications d'événements

Utilisez la commande describe-instance-event-notification AWS CLI -attributes.

```
aws ec2 describe-instance-event-notification-attributes
```

Replanifiez les événements planifiés qui affectent vos instances Amazon EC2

Vous pouvez replanifier un événement de sorte qu'il se produise à une date et une heure spécifiques qui vous conviennent. Seuls les événements ayant une date d'échéance peuvent être reprogrammés. Il existe d'autres restrictions pour la reprogrammation d'un événement.

Vous pouvez replanifier un événement à l'aide de l'une des méthodes suivantes.

Console

Pour replanifier un événement

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Événements.
3. Choisissez Type de ressource : instance dans la liste des filtres.
4. Sélectionnez une ou plusieurs instances, puis sélectionnez Actions, Schedule Event (Programmer un événement).

   Seuls les événements ayant une date d'échéance, indiquée par la valeur Event Deadline (Échéance de l'événement), peuvent être reprogrammés. Si l'un des événements sélectionnés n'a pas de date d'échéance, Actions, Schedule Event (Programmer un événement) est désactivé.
5. Dans New start time (Nouvelle heure de début), saisissez une nouvelle date et une nouvelle heure pour l'événement. La nouvelle date et la nouvelle heure doivent être antérieures à la valeur de Event Deadline (Échéance de l'événement).
6. Choisissez Save (Enregistrer).

   L'heure de démarrage mise à jour peut prendre une à deux minutes pour s'afficher dans la console.

AWS CLI

Pour replanifier un événement

1. Seuls les événements dotés d'une date d'échéance d'événement, indiquée par la valeur pour `NotBeforeDeadline`, peuvent être reprogrammés. Utilisez la describe-instance-statuscommande pour afficher la valeur du `NotBeforeDeadline` paramètre.

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0
```

L'exemple de sortie suivant illustre un événement `system-reboot` qui peut être reprogrammé, car `NotBeforeDeadline` contient une valeur.

```
[
    "Events": [
                {
                    "InstanceEventId": "instance-event-0d59937288b749b32",
                    "Code": "system-reboot",
                    "Description": "The instance is scheduled for a reboot",
                    "NotAfter": "2019-03-14T22:00:00.000Z",
                    "NotBefore": "2019-03-14T20:00:00.000Z",
                    "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
                }
            ]
]
```

2. Pour replanifier l'événement, utilisez la commande modify-instance-event-start-time. Spécifiez la nouvelle heure de début de l'événement à l'aide du paramètre `not-before`. La nouvelle heure de début doit se situer avant la `NotBeforeDeadline`.

```
aws ec2 modify-instance-event-start-time \
    --instance-id i-1234567890abcdef0 \
    --instance-event-id instance-event-0d59937288b749b32 \
    --not-before 2019-03-25T10:00:00.000
```

Cela peut prendre une minute ou deux avant que la describe-instance-statuscommande ne renvoie la valeur de `not-before` paramètre mise à jour.

Limites

- Seuls les événements dotés d'une date d'échéance d'événement peuvent être reprogrammés. L'événement peut être reprogrammé jusqu'à la date d'échéance de celui-ci. La colonne Date limite de la console et le `NotBeforeDeadline` champ de la colonne AWS CLI indiquent si l'événement a une date limite.

- Seuls les événements n'ayant pas encore démarré peuvent être reprogrammés. La colonne Heure de début de la console et le `NotBefore` champ de la AWS CLI indiquent l'heure de début de l'événement. Les événements programmés pour un lancement dans les 5 prochaines minutes ne peuvent pas être reprogrammés.
- La nouvelle heure de début doit être au moins 60 minutes après l'heure actuelle.
- Si vous reprogrammez plusieurs événements à l'aide de la console, la date d'échéance de l'événement est déterminée par l'événement avec la date d'échéance d'événement la plus proche.

Créez des fenêtres d'événements personnalisées pour les événements planifiés qui affectent vos EC2 instances Amazon

Vous pouvez définir des fenêtres d'événements personnalisées qui se reproduisent chaque semaine pour les événements planifiés qui redémarrent, arrêtent ou mettent fin à vos EC2 instances Amazon. Vous pouvez associer une ou plusieurs instances à une fenêtre d'événements. Si un événement est planifié pour ces instances, AWS planifiera les événements dans la fenêtre d'événements associée.

Vous pouvez utiliser des fenêtres d'événements afin d'optimiser la disponibilité de la charge de travail globale en spécifiant des fenêtres d'événements pendant des périodes creuses pour cette charge de travail. Vous pouvez également aligner les fenêtres d'événements avec vos planifications de maintenance internes.

Vous définissez une fenêtre d'événements en spécifiant un ensemble de plages de temps. La plage de temps minimale est de 2 heures. Les plages de temps combinées doivent totaliser au moins 4 heures.

Vous pouvez associer une ou plusieurs instances à une fenêtre d'événements à l'aide d'instances IDs ou de balises d'instance. Vous pouvez également associer des hôtes dédiés à une fenêtre d'événements en utilisant l'ID d'hôte.

> **Warning**
>
> Les fenêtres d'événements s'appliquent uniquement à des événements planifiés qui arrêtent, redémarrent ou résilient des instances.
> Les fenêtres d'événements ne sont pas applicables aux événements suivants :
>
> - Événements planifiés accélérés et événements de maintenance du réseau.
> - Maintenance imprévue, telle que AutoRecovery redémarrages imprévus.

Utiliser les fenêtres d'événements

Considérations

- Toutes les heures de créneau des événements sont passéesUTC.
- La durée minimale d'une fenêtre d'événements hebdomadaire est de 4 heures.
- Les plages de temps au sein d'une fenêtre d'événements doivent être d'au moins 2 heures chacune.
- Un seul type de cible (ID d'instance, ID d'hôte dédié ou étiquette d'instance) peut être associé à une fenêtre d'événements.
- Une cible (ID d'instance, ID d'hôte dédié ou étiquette d'instance) ne peut être associée qu'à à une fenêtre d'événements.
- Un maximum de 100 instancesIDs, 50 hôtes IDs dédiés ou 50 balises d'instance peuvent être associées à une fenêtre d'événements. Les étiquettes d'instance peuvent être associées à un nombre quelconque d'instances.
- Un maximum de 200 fenêtres d'événements peuvent être créées par AWS région.
- Plusieurs instances associées à des fenêtres d'événements peuvent avoir des événements planifiés se produisant en même temps.
- Si vous avez AWS déjà planifié un événement, la modification d'une fenêtre d'événements ne changera pas l'heure de l'événement planifié. Si l'événement a une date d'échéance, vous pouvez replanifier l'événement.
- Vous pouvez arrêter et démarrer une instance avant l'événement planifié. Cela a pour effet de migrer l'instance vers un nouvel hôte, de sorte que l'événement planifié n'aura plus lieu.

Créer des fenêtres d'événements

Vous pouvez créer une ou plusieurs fenêtres d'événements. Pour chaque fenêtre d'événements, vous spécifiez un ou plusieurs blocs de temps. Par exemple, vous pouvez créer une fenêtre

d'événements avec des blocs de temps qui se produisent tous les jours à 4 heures du matin pendant 2 heures. Ou vous pouvez créer une fenêtre d'événements avec des blocs de temps qui se produisent les dimanches de 2 à 4 heures et les mercredis de 3 à 5 heures.

Pour connaître les contraintes de fenêtre d'événements, consultez Considérations plus haut dans cette rubrique.

Les fenêtres d'événements se reproduisent à une fréquence hebdomadaire jusqu'à ce que vous les supprimiez.

Pour créer une fenêtre d'événements, utilisez l'une des méthodes suivantes.

Console

Pour créer une fenêtre d'événements

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Events (Évènements).
3. Choisissez Actions, Gérer les fenêtres d'événements.
4. Choisissez Créer une fenêtre d'événements d'instance.
5. Pour Nom de la fenêtre d'événements, saisissez un nom descriptif.
6. Pour Planification de la fenêtre d'événements, choisissez de spécifier les blocs de temps dans la fenêtre d'événements à l'aide du générateur de planification cron ou en spécifiant des plages de temps.

   - Si vous choisissez Générateur de planification Cron, spécifiez les paramètres suivants :
     1. Pour Days (UTC), spécifiez les jours de la semaine pendant lesquels la fenêtre d'événements apparaît.
     2. Pour Heure de début (UTC), spécifiez l'heure à laquelle la fenêtre d'événements commence.
     3. Pour Durée, spécifiez la durée des blocs de temps dans la fenêtre d'événements. La durée minimale par bloc de temps est de 2 heures. La durée minimale de la fenêtre d'événements doit être égale ou supérieure à 4 heures au total. Tous les temps sont écoulésUTC.
   - Si vous choisissez Plages de temps, choisissez Ajouter une nouvelle plage de temps, puis spécifiez le jour et l'heure de début, ainsi que le jour et l'heure de fin. Répétez l'opération pour chaque plage de temps. La durée minimale par plage de temps est de 2 heures. La

durée minimale pour toutes les plages de temps combinées doit être égale ou supérieure à 4 heures au total.

7. (Facultatif) Pour Détails de la cible, associez une ou plusieurs instances à la fenêtre d'événements afin que, si les instances sont planifiées pour maintenance, l'événement planifié se produise durant la fenêtre d'événement associée. Vous pouvez associer une ou plusieurs instances à une fenêtre d'événements à l'aide d'instances IDs ou de balises d'instance. Vous pouvez associer des hôtes dédiés avec une fenêtre d'événements en utilisant l'ID d'hôte.

   Notez que vous pouvez créer la fenêtre d'événements sans y associer de cible. Plus tard, vous pourrez modifier la fenêtre pour associer une ou plusieurs cibles.
8. (Facultatif) Pour Etiquettes de la fenêtre d'événements, choisissez Ajouter une étiquette, puis saisissez la clé et la valeur de l'étiquette. Répétez l'opération pour chaque étiquette.
9. Choisissez Créer une fenêtre d'événements.

AWS CLI

Pour créer une fenêtre d'événements à l'aide de AWS CLI, vous devez d'abord créer la fenêtre d'événements, puis vous associez une ou plusieurs cibles à la fenêtre d'événements.

Créer une fenêtre d'événements

Lors de la création de la fenêtre d'événements, vous pouvez définir un ensemble de plages de temps ou une expression cron, mais pas les deux.

Pour créer une fenêtre d'événements avec une plage de temps

Utilisez la create-instance-event-windowcommande et spécifiez le `--time-range` paramètre. Vous ne pouvez pas également spécifier le paramètre `--cron-expression`.

```
aws ec2 create-instance-event-window \
    --region us-east-1 \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8 \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

Sortie attendue

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Pour créer une fenêtre d'événements avec une expression cron à

Utilisez la create-instance-event-windowcommande et spécifiez le `--cron-expression` paramètre. Vous ne pouvez pas également spécifier le paramètre `--time-range`.

```
aws ec2 create-instance-event-window \
    --region us-east-1 \
    --cron-expression "* 21-23 * * 2,3" \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

Sortie attendue

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "State": "creating",
```

```
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Associer une cible à une fenêtre d'événements

Vous ne pouvez associer qu'un seul type de cible (instance IDsIDs, hôte dédié ou balises d'instance) à une fenêtre d'événements.

Pour associer des étiquettes d'instance à une fenêtre d'événements

Utilisez la associate-instance-event-windowcommande et spécifiez le `instance-event-window-id` paramètre pour définir la fenêtre d'événements. Pour associer des étiquettes d'instance, spécifiez le paramètre `--association-target`, et pour les valeurs de paramètre, spécifiez une ou plusieurs étiquettes.

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Sortie attendue

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [
                {
                    "Key": "k2",
                    "Value": "v2"
                },
                {
                    "Key": "k1",
```

```
                    "Value": "v1"
                }
            ],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Pour associer une ou plusieurs instances à une fenêtre d'événements

Utilisez la associate-instance-event-windowcommande et spécifiez le `instance-event-window-id` paramètre pour définir la fenêtre d'événements. Pour associer des instances, spécifiez le `--association-target` paramètre, et pour les valeurs des paramètres, spécifiez une ou plusieurs instancesIDs.

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Sortie attendue

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-1234567890abcdef0",
                "i-0598c7d356eba48d7"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Pour associer un hôte dédié à une fenêtre d'événements

Utilisez la associate-instance-event-windowcommande et spécifiez le `instance-event-window-id` paramètre pour définir la fenêtre d'événements. Pour associer un hôte dédié, spécifiez le `--association-target` paramètre, et pour les valeurs des paramètres, spécifiez un ou plusieurs hôtes dédiésIDs.

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "DedicatedHostIds=h-029fa35a02b99801d"
```

Sortie attendue

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": [
                "h-029fa35a02b99801d"
            ]
        },
        "State": "creating"
    }
}
```

Afficher les fenêtres d'événements

Vous pouvez afficher les fenêtres d'événements à l'aide de l'une des méthodes suivantes.

Console

Pour afficher les fenêtres d'événements

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Events (Évènements).
3. Choisissez Actions, Gérer les fenêtres d'événements.
4. Sélectionnez une fenêtre d'événements pour voir ses détails.

AWS CLI

Pour décrire toutes les fenêtres d'événements

Utilisez la describe-instance-event-windowscommande.

```
aws ec2 describe-instance-event-windows \
    --region us-east-1
```

Sortie attendue

```
{
    "InstanceEventWindows": [
        {
            "InstanceEventWindowId": "iew-0abcdef1234567890",
            "Name": "myEventWindowName",
            "CronExpression": "* 21-23 * * 2,3",
            "AssociationTarget": {
                "InstanceIds": [
                    "i-1234567890abcdef0",
                    "i-0598c7d356eba48d7"
                ],
                "Tags": [],
                "DedicatedHostIds": []
            },
            "State": "active",
            "Tags": []
        }

        ...

    ],
    "NextToken": "9d624e0c-388b-4862-a31e-a85c64fc1d4a"
}
```

Pour décrire une fenêtre d'événements spécifique

Utilisez la describe-instance-event-windowscommande avec le `--instance-event-window-id` paramètre pour décrire une fenêtre d'événements spécifique.

```
aws ec2 describe-instance-event-windows \
    --region us-east-1 \
```

```
    --instance-event-window-id iew-0abcdef1234567890
```

Pour décrire des fenêtres d'événements correspondant à un ou plusieurs filtres

Utilisez la describe-instance-event-windowscommande avec le `--filters` paramètre. Dans l'exemple suivant, le filtre `instance-id` est utilisé pour décrire toutes les fenêtres d'événements associées à l'instance spécifiée.

Quand un filtre est utilisé, il recherche une correspondance directe. Cependant, le filtre `instance-id` est différent. À défaut de correspondance directe avec l'ID d'instance, il recherche des associations indirectes avec la fenêtre d'événements, telles que les étiquettes ou l'ID d'hôte dédié de l'instance (si celle-ci se trouve sur un hôte dédié).

Pour la liste des filtres pris en charge, reportez-vous describe-instance-event-windowsà la section AWS CLI Référence.

```
aws ec2 describe-instance-event-windows \
    --region us-east-1 \
    --filters Name=instance-id,Values=i-1234567890abcdef0 \
    --max-results 100 \
    --next-token <next-token-value>
```

Sortie attendue

Dans l'exemple suivant, l'instance se trouve sur un hôte dédié qui est associé à la fenêtre d'événements.

```
{
    "InstanceEventWindows": [
        {
            "InstanceEventWindowId": "iew-0dbc0adb66f235982",
            "TimeRanges": [
                {
                    "StartWeekDay": "sunday",
                    "StartHour": 2,
                    "EndWeekDay": "sunday",
                    "EndHour": 8
                }
            ],
            "Name": "myEventWindowName",
            "AssociationTarget": {
                "InstanceIds": [],
```

```
                "Tags": [],
                "DedicatedHostIds": [
                    "h-0140d9a7ecbd102dd"
                ]
            },
            "State": "active",
            "Tags": []
        }
    ]
}
```

Modifier des fenêtres d'événements

Vous pouvez modifier tous les champs d'une fenêtre d'événements à l'exception de son ID. Par exemple, quand l'heure d'été commence, vous pouvez modifier la planification de la fenêtre d'événements. Pour des fenêtres d'événements existantes, vous pouvez ajouter ou supprimer des cibles.

Pour modifier une fenêtre d'événements, utilisez l'une des méthodes suivantes.

Console

Pour modifier une fenêtre d'événements

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Events (Évènements).
3. Choisissez Actions, Gérer les fenêtres d'événements.
4. Sélectionnez la fenêtre d'événements à modifier, puis choisissez Actions, Modifier la fenêtre d'événements d'instance.
5. Modifiez les champs de la fenêtre d'événements, puis choisissez Modifier la fenêtre d'événements.

AWS CLI

Pour modifier une fenêtre d'événements à l'aide de AWS CLI, vous pouvez modifier la plage de temps ou l'expression cron, et associer ou dissocier une ou plusieurs cibles à la fenêtre d'événements.

Modifier l'heure de la fenêtre d'événements

Lors de la modification de la fenêtre d'événements, vous pouvez modifier une plage de temps ou une expression cron, mais pas les deux.

Pour modifier la plage de temps d'une fenêtre d'événements

Utilisez la modify-instance-event-windowcommande et spécifiez la fenêtre d'événements à modifier. Spécifiez le paramètre `--time-range` pour modifier la plage de temps. Vous ne pouvez pas également spécifier le paramètre `--cron-expression`.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8
```

Sortie attendue

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
```

```
        ]
    }
}
```

Pour modifier une ensemble de plages de temps pour une fenêtre d'événements

Utilisez la modify-instance-event-windowcommande et spécifiez la fenêtre d'événements à modifier. Spécifiez le paramètre `--time-range` pour modifier la plage de temps. Vous ne pouvez pas spécifier également le paramètre `--cron-expression` dans le même appel.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range '[{"StartWeekDay": "monday", "StartHour": 2, "EndWeekDay":
 "wednesday", "EndHour": 8},
   {"StartWeekDay": "thursday", "StartHour": 2, "EndWeekDay": "friday",
 "EndHour": 8}]'
```

Sortie attendue

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            },
            {
                "StartWeekDay": "thursday",
                "StartHour": 2,
                "EndWeekDay": "friday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
```

```
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Pour modifier l'expression cron d'une fenêtre d'événements

Utilisez la modify-instance-event-windowcommande et spécifiez la fenêtre d'événements à modifier. Spécifiez le paramètre `--cron-expression` pour modifier l'expression cron. Vous ne pouvez pas également spécifier le paramètre `--time-range`.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --cron-expression "* 21-23 * * 2,3"
```

Sortie attendue

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
```

```
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Modifier les cibles associées à une fenêtre d'événements

Vous pouvez associer des cibles supplémentaires à une fenêtre d'événements. Vous pouvez également dissocier des cibles existantes d'une fenêtre d'événements. Toutefois, un seul type de cible (instance IDsIDs, hôte dédié ou balises d'instance) peut être associé à une fenêtre d'événements.

Pour associer des cibles supplémentaires à une fenêtre d'événements

Pour obtenir des instructions sur la façon d'associer des cibles à une fenêtre d'événements, consultez Associate a target with an event window.

Pour dissocier des étiquettes d'instance d'une fenêtre d'événements

Utilisez la disassociate-instance-event-windowcommande et spécifiez le `instance-event-window-id` paramètre pour définir la fenêtre d'événements. Pour dissocier des étiquettes d'instance, spécifiez le paramètre `--association-target`, et pour les valeurs de paramètre, spécifiez une ou plusieurs étiquettes.

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Sortie attendue

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
```

```
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Pour dissocier une ou plusieurs instances d'une fenêtre d'événements

Utilisez la disassociate-instance-event-windowcommande et spécifiez le `instance-event-window-id` paramètre pour définir la fenêtre d'événements. Pour dissocier les instances, spécifiez le `--association-target` paramètre, et pour les valeurs des paramètres, spécifiez une ou plusieurs instancesIDs.

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Sortie attendue

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Pour dissocier un hôte dédié d'une fenêtre d'événements

Utilisez la disassociate-instance-event-windowcommande et spécifiez le `instance-event-window-id` paramètre pour définir la fenêtre d'événements. Pour dissocier un hôte dédié, spécifiez le `--association-target` paramètre, et pour les valeurs des paramètres, spécifiez un ou plusieurs hôtes IDs dédiés.

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target DedicatedHostIds=h-029fa35a02b99801d
```

Sortie attendue

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Supprimer des fenêtres d'événements

Vous pouvez supprimer une fenêtre d'événements à la fois à l'aide de l'une des méthodes suivantes.

Console

Pour supprimer une fenêtre d'événements

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Events (Évènements).
3. Choisissez Actions, Gérer les fenêtres d'événements.
4. Sélectionnez la fenêtre d'événements à supprimer, puis choisissez Actions, Supprimer la fenêtre d'événements d'instance.
5. Lorsque vous y êtes invité, tapez **`delete`**, puis choisissez Supprimer.

AWS CLI

Pour supprimer une fenêtre d'événements

Utilisez la delete-instance-event-windowcommande et spécifiez la fenêtre d'événements à supprimer.

```
aws ec2 delete-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890
```

Pour supprimer de force une fenêtre d'événements

Utilisez le paramètre `--force-delete` si la fenêtre d'événements est actuellement associée à des cibles.

```
aws ec2 delete-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --force-delete
```

Sortie attendue

```
{
    "InstanceEventWindowState": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "State": "deleting"
    }
}
```

Etiqueter des fenêtres d'événements

Vous pouvez étiqueter une fenêtre d'événements lorsque vous la créez, ou ultérieurement.

Pour étiqueter une fenêtre d'événements lorsque vous la créez, consultez Créer des fenêtres d'événements.

Pour étiqueter une fenêtre d'événements, utilisez l'une des méthodes suivantes.

Console

Pour étiqueter une fenêtre d'événements existante

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Events (Évènements).

3. Choisissez Actions, Gérer les fenêtres d'événements.
4. Sélectionnez la fenêtre d'événements à étiqueter, puis choisissez Actions, Etiqueter la fenêtre d'événements d'instance.
5. Pour ajouter une étiquette, choisissez Ajouter une étiquette. Répétez l'opération pour chaque étiquette.
6. Choisissez Save (Enregistrer).

AWS CLI

Pour étiqueter une fenêtre d'événements existante

Utilisez la commande create-tags pour baliser les ressources existantes. Dans l'exemple suivant, la fenêtre d'événements existante est étiquetée avec Key=purpose et Value=test.

```
aws ec2 create-tags \
    --resources iew-0abcdef1234567890 \
    --tags Key=purpose,Value=test
```

Surveillez vos instances à l'aide de CloudWatch

Vous pouvez surveiller vos instances à l'aide d'Amazon CloudWatch, qui collecte et traite les données brutes d'Amazon pour EC2 en faire des indicateurs lisibles en temps quasi réel. Ces statistiques sont enregistrées pour une durée de 15 mois et, par conséquent, vous pouvez accéder aux informations historiques et acquérir un meilleur point de vue de la façon dont votre service ou application web s'exécute.

Par défaut, Amazon EC2 envoie les données métriques CloudWatch à des intervalles de 5 minutes. Pour envoyer les données métriques de votre instance par périodes CloudWatch d'une minute, vous pouvez activer la surveillance détaillée de l'instance. Pour de plus amples informations, veuillez consulter Gérez la surveillance détaillée de vos EC2 instances.

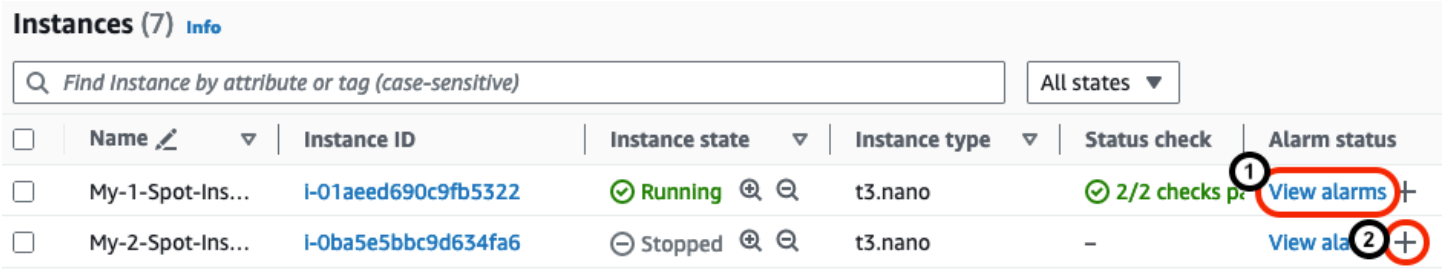
La EC2 console Amazon affiche une série de graphiques basés sur les données brutes d'Amazon CloudWatch. Selon vos besoins, vous préférerez peut-être obtenir les données de vos instances auprès d'Amazon CloudWatch plutôt que de consulter les graphiques de la console.

Pour obtenir des informations sur la CloudWatch facturation et les coûts d'Amazon, consultez la section CloudWatch facturation et coûts dans le guide de CloudWatch l'utilisateur Amazon.

Table des matières

Gérez les CloudWatch alarmes pour vos EC2 instances dans la EC2 console Amazon

Depuis l'écran Instances de la EC2 console Amazon, vous pouvez gérer les CloudWatch alarmes Amazon pour vos instances. Dans le tableau Instances, la colonne État de l'alarme fournit deux commandes de console : une commande pour afficher les alarmes et une autre pour les créer ou les modifier. La capture d'écran suivante indique ces commandes de console, numérotées 1 (Afficher les alarmes) et 2 (signe + pour créer ou modifier une alarme).



Afficher les alarmes depuis l'écran Instances

Vous pouvez consulter les alarmes de chaque instance depuis l'écran Instances.

Pour afficher l'alarme d'une instance depuis l'écran Instances

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.

3. Dans le tableau Instances, pour l'instance que vous avez choisie, choisissez Afficher les alarmes (numérotée 1 dans la capture d'écran précédente).
4. Dans les détails de l'alarme pour ***i-0123456789example***fenêtre, choisissez le nom de l'alarme pour afficher l'alarme dans la CloudWatch console.

Créez des alarmes à partir de l'écran Instances

Vous pouvez créer une alarme pour chaque instance à partir de l'écran Instances.

Pour créer une alarme pour une instance à partir de l'écran Instances

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Dans le tableau Instances, pour l'instance que vous avez choisie, choisissez le signe plus (numéroté 2 dans la capture d'écran précédente).
4. Dans l'écran Gérer les CloudWatch alarmes, créez votre alarme. Pour de plus amples informations, veuillez consulter Création d'une CloudWatch alarme pour une instance.

Modifier les alarmes depuis l'écran Instances

Vous pouvez modifier l'alarme d'une instance depuis l'écran Instances.

Pour modifier une alarme pour une instance depuis l'écran Instances

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Dans le tableau Instances, pour l'instance que vous avez choisie, choisissez le signe plus (numéroté 2 dans la capture d'écran précédente).
4. Dans l'écran Gérer les CloudWatch alarmes, modifiez votre alarme. Pour plus d'informations, consultez Modifier ou supprimer une CloudWatch alarme dans le guide de CloudWatch l'utilisateur Amazon.

Gérez la surveillance détaillée de vos EC2 instances

Amazon CloudWatch propose deux catégories de surveillance : la surveillance de base et la surveillance détaillée. Par défaut, votre instance est configurée pour une surveillance de base. Vous

pouvez éventuellement activer une surveillance détaillée pour vous aider à identifier les problèmes opérationnels et à y remédier plus rapidement. Vous pouvez activer ou désactiver la surveillance détaillée au lancement ou lorsque l'instance est en cours d'exécution ou arrêtée.

L'activation de la surveillance détaillée sur une instance n'a aucune incidence sur la surveillance de ses EBS volumes attachés. Pour plus d'informations, consultez CloudWatch les statistiques Amazon pour Amazon EBS.

Le tableau suivant met en évidence les différences entre la surveillance de base et la surveillance détaillée pour vos instances.

Type de surveillance	Description	Frais
Surveillance de base	Les mesures de vérification du statut sont disponibles par périodes d'une minute. Toutes les autres métriques sont disponibles par périodes de cinq minutes.	Aucuns frais.
Surveillance détaillée	Toutes les métriques, y compris les métriques de contrôle de statut, sont disponibles par périodes d'une minute. Pour obtenir le niveau de données, vous devez l'activer spécifiquement pour l'instance. Pour les instances où vous avez activé la surveillance détaillée, vous pouvez également obtenir les donnés agrégées à partir de groupes d'instances similaires.	Vous êtes débité par métrique envoyée EC2 par Amazon CloudWatch. Vous n'êtes pas facturé pour le stockage des données. Pour plus d'informations, consultez le niveau payant et l'exemple 1 - Surveillance EC2 détaillée sur la page de CloudWatch tarification d'Amazon.

Table des matières

Autorisations requises

Pour activer la surveillance détaillée d'une instance, votre utilisateur doit être autorisé à utiliser l'MonitorInstancesAPIaction. Pour désactiver la surveillance détaillée d'une instance, votre utilisateur doit être autorisé à utiliser l'UnmonitorInstancesAPIaction.

Activez une surveillance détaillée au lancement

Utilisez les procédures suivantes pour activer la surveillance détaillée au lancement. Par défaut, votre instance utilise la surveillance de base.

Console

Pour activer la surveillance détaillée lors du lancement d'une instance

Lorsque vous lancez une instance à l'aide de la EC2 console Amazon, sous Détails avancés, cochez la case CloudWatch Surveillance détaillée.

AWS CLI

Pour activer la surveillance détaillée lors du lancement d'une instance

Utilisez la commande run-instances avec l'indicateur `--monitoring` pour activer la surveillance détaillée.

```
aws ec2 run-instances --image-id ami-09092360 --monitoring Enabled=true...
```

Gérez le suivi détaillé

Utilisez les procédures suivantes pour gérer la surveillance détaillée d'une instance en cours d'exécution ou arrêtée.

Console

Pour gérer la surveillance détaillée d'une instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance.
4. Choisissez Actions, Surveiller et résoudre les problèmes, Gérer la surveillance détaillée.

5. Sur la page Surveillance détaillée, pour Surveillance détaillée, effectuez l'une des opérations suivantes :
   - Surveillance détaillée : sélectionnez Activer.
   - Surveillance de base — Clear Enable.
6. Choisissez Confirmer.

AWS CLI

Activation de la surveillance détaillée d'une instance

Utilisez la commande monitor-instances suivante pour activer la surveillance détaillée des instances spécifiées.

```
aws ec2 monitor-instances --instance-ids i-1234567890abcdef0
```

Pour désactiver la surveillance détaillée d'une instance

Utilisez la commande unmonitor-instances suivante pour désactiver la surveillance détaillée des instances spécifiées.

```
aws ec2 unmonitor-instances --instance-ids i-1234567890abcdef0
```

CloudWatch métriques disponibles pour vos instances

Amazon EC2 envoie des métriques à Amazon CloudWatch. Vous pouvez utiliser le AWS Management Console AWS CLI, le ou un API pour répertorier les métriques auxquelles Amazon EC2 envoie des données CloudWatch. Par défaut, chaque point de données couvre les 5 minutes suivant l'heure de début d'activité de l'instance. Si vous avez activé la surveillance détaillée, chaque point de données couvre la minute suivant l'activité à compte de l'heure de début. Notez que pour les statistiques minimale, maximale et moyenne, la granularité minimale des mesures EC2 fournies est de 1 minute.

Pour plus d'informations sur la façon de consulter les statistiques disponibles à l'aide du AWS Management Console ou du AWS CLI, consultez la section Afficher les mesures disponibles dans le guide de CloudWatch l'utilisateur Amazon.

Pour plus d'informations sur la façon d'obtenir les statistiques pour ces métriques, consultez Statistiques pour les CloudWatch métriques relatives à vos instances.

Sommaire

Métriques des instances

L'espace de nom `AWS/EC2` inclut les métriques d'instance suivantes.

Métrique	Description	Unité	Statistiques significatives
`CPUUtilization`	Le pourcentage de CPU temps physique EC2 utilisé par Amazon pour exécuter l'EC2instance, qui inclut le temps passé à exécuter à la fois le code utilisateur et le EC2 code Amazon. À un niveau très élevé, `CPUUtilization` est la somme de l'invité `CPUUtilization` et de l'hyperviseur `CPUUtilization` . Les outils de votre système d'exploitation peuvent afficher un pourcentage différent de celui CloudWatch dû à des facteurs tels que la simulation d'appareils existants, la configuration d'appareils non existants, les charges de travail nécessitant de nombreuses interruptions, la migration en direct et la mise à jour en direct.	Pourcentage	• Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
`DiskReadOps`	Opérations de lecture terminées de tous les volumes de stockage d'instance disponibles pour l'instance, au cours de la période spécifiée. Pour calculer la moyenne des opérations d'E/S par seconde (IOPS) pour la période, divisez le total des opérations de la période par le nombre de secondes de cette période. S'il n'y a pas de volumes de stockage d'instance, la valeur est 0 ou la métrique n'est pas prise en charge.	Nombre	• Somme • Moyenne • Minimum • Maximum
`DiskWriteOps`	Opérations d'écriture terminées dans tous les volumes de stockage d'instance disponibles pour l'instance, au cours de la période spécifiée. Pour calculer la moyenne des opérations d'E/S par seconde (IOPS) pour la période, divisez le total des opérations de la période par le nombre de secondes de cette période. S'il n'y a pas de volumes de stockage d'instance, la valeur est 0 ou la métrique n'est pas prise en charge.	Nombre	• Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
`DiskReadBytes`	Octets lus à partir de tous les volumes de stockage d'instance disponibles pour l'instance. Cette métrique permet de déterminer le volume de données que l'application lit à partir du disque dur de l'instance. Il est ainsi possible de déterminer la vitesse de l'application. Le nombre mentionné correspond au nombre d'octets reçus pendant la période. Si vous utilisez une surveillance de base (cinq minutes), vous pouvez diviser ce nombre par 300 pour trouver le nombre d'octets/seconde. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique `DIFF_TIME` pour déterminer les octets par seconde. Par exemple, si vous avez représenté graphiquement `DiskReadBytes` CloudWatch comme `m1`, la formule mathématique de la métrique `m1/(DIFF_TIME(m1))` renvoie la métrique en octets/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques `DIFF_TIME` et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon. S'il n'y a pas de volumes de stockage d'instance, la valeur est 0 ou la métrique n'est pas prise en charge.	Octets	• Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
`DiskWriteBytes`	Octets écrits dans tous les volumes de stockage d'instance disponibles pour l'instance. Cette métrique permet de déterminer le volume de données que l'application écrit sur le disque dur de l'instance. Il est ainsi possible de déterminer la vitesse de l'application. Le nombre mentionné correspond au nombre d'octets reçus pendant la période. Si vous utilisez une surveillance de base (cinq minutes), vous pouvez diviser ce nombre par 300 pour trouver le nombre d'octets/seconde. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique `DIFF_TIME` pour déterminer les octets par seconde. Par exemple, si vous avez représenté graphiquement `DiskWriteBytes` CloudWatch comme `m1`, la formule mathématique de la métrique `m1/(DIFF_TIME(m1))` renvoie la métrique en octets/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques `DIFF_TIME` et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon. S'il n'y a pas de volumes de stockage d'instance, la valeur est 0 ou la métrique n'est pas prise en charge.	Octets	• Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
`MetadataNoToken`	Le nombre de fois où le service de métadonnées d'instance (IMDS) a été accédé avec succès à l'aide d'une méthode qui n'utilise pas de jeton. Cette métrique est utilisée pour déterminer s'il existe des processus accédant aux métadonnées d'instance qui utilisent le service de métadonnées d'instance version 1 (IMDSv1), qui n'utilise pas de jeton. Si toutes les demandes utilisent des sessions basées sur des jetons, c'est-à-dire le service de métadonnées d'instance version 2 (IMDSv2), la valeur est 0. Pour de plus amples informations, veuillez consulter Passer à l'utilisation de Service des métadonnées d'instance Version 2.	Nombre	• Somme • Centiles
`MetadataNoTokenRejected`	Le nombre de tentatives d'IMDSv1appel après avoir IMDSv1 été désactivé. Si cette métrique apparaît, elle indique qu'un IMDSv1 appel a été tenté et rejeté. Vous pouvez soit réactiver, IMDSv1 soit vous assurer que tous vos appels sont utilisésIMDSv2. Pour de plus amples informations, veuillez consulter Passer à l'utilisation de Service des métadonnées d'instance Version 2.	Nombre	• Somme • Centiles

Métrique	Description	Unité	Statistiques significatives
`NetworkIn`	Nombre d'octets reçus par l'instance sur toutes les interfaces réseau. Cette métrique identifie le volume du trafic réseau entrant d'une seule instance. Le nombre mentionné correspond au nombre d'octets reçus pendant la période. Si vous utilisez une surveillance de base (cinq minutes) et que la statistique est Somme, vous pouvez diviser ce nombre par 300 pour trouver le nombre d'octets/seconde. Si vous utilisez une surveillance détaillée (une minute) et que la statistique est Somme, divisez-la par 60. Vous pouvez également utiliser la fonction mathémati que CloudWatch métrique `DIFF_TIME` pour déterminer les octets par seconde. Par exemple, si vous avez représenté graphique ment `NetworkIn` CloudWatch comme`m1`, la formule mathématique de la métrique `m1/(DIFF_TIME(m1))` renvoie la métrique en octets/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques `DIFF_TIME` et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.	Octets	• Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
`NetworkOut`	Nombre d'octets envoyés par l'instance sur toutes les interfaces réseau. Cette métrique identifie le volume du trafic réseau sortant d'une seule instance. Le nombre mentionné correspond au nombre d'octets envoyés pendant la période. Si vous utilisez une surveillance de base (cinq minutes) et que la statistique est Somme, vous pouvez diviser ce nombre par 300 pour trouver le nombre d'octets/seconde. Si vous utilisez une surveillance détaillée (une minute) et que la statistique est Somme, divisez-la par 60. Vous pouvez également utiliser la fonction mathémati que CloudWatch métrique `DIFF_TIME` pour déterminer les octets par seconde. Par exemple, si vous avez représenté graphique ment `NetworkOut` CloudWatch comme`m1`, la formule mathématique de la métrique `m1/(DIFF_TIME(m1))` renvoie la métrique en octets/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques `DIFF_TIME` et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.	Octets	• Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
`NetworkPacketsIn`	Nombre de paquets reçus par l'instance sur toutes les interfaces réseau. Cette métrique identifie le volume du trafic entrant en ce qui concerne le nombre de paquets sur une seule instance. Cette métrique est disponible uniquement pour la surveillance basique (périodes de cinq minutes). Pour calculer le nombre de paquets par seconde (PPS) que votre instance a reçus pendant les 5 minutes, divisez la valeur de la statistique Sum par 300. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique `DIFF_TIME` pour trouver les paquets par seconde. Par exemple, si vous avez représenté graphiquement `NetworkPacketsIn` CloudWatch comme `m1`, la formule mathématique de la métrique `m1/(DIFF_TIME(m1))` renvoie la métrique en paquets/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques `DIFF_TIME` et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.	Nombre	• Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
`NetworkPackets0ut`	Nombre de paquets envoyés par l'instance sur toutes les interfaces réseau. Cette métrique identifie le volume du trafic sortant en ce qui concerne le nombre de paquets sur une seule instance. Cette métrique est disponible uniquement pour la surveillance basique (périodes de cinq minutes). Pour calculer le nombre de paquets par seconde (PPS) envoyés par votre instance pendant les 5 minutes, divisez la valeur de la statistique Sum par 300. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique `DIFF_TIME` pour trouver les paquets par seconde. Par exemple, si vous avez représenté graphiquement `NetworkPackets0ut` CloudWatch comm`em1`, la formule mathématique de la métrique `m1/(DIFF_TIME(m1))` renvoie la métrique en paquets/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques `DIFF_TIME` et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.	Nombre	• Somme • Moyenne • Minimum • Maximum

CPUindicateurs de crédit

L'espace de `AWS/EC2` noms inclut les indicateurs CPU de crédit suivants pour vos instances de performance burstable.

Métrique	Description	Unité	Statistiques significatives
`CPUCreditUsage`	Le nombre de CPU crédits dépensés par l'instance pour être CPU utilisés. Un CPU crédit équivaut à un v CPU fonctionnant à 100 % d'utilisation pendant une minute ou une combinaison équivalente d'vCPUsutilisation et de temps (par exemple, un v CPU fonctionnant à 50 % d'utilisation pendant deux minutes ou deux vCPUs fonctionnant à 25 % d'utilisation pendant deux minutes). CPUles indicateurs de crédit ne sont disponibles qu'à une fréquence de 5 minutes. Si vous spécifiez une période supérieure à cinq minutes, utilisez la statistique `Sum` au lieu de la statistique `Average`.	Crédits (v CPU - minutes)	• Somme • Moyenne • Minimum • Maximum
`CPUCreditBalance`	Le nombre de CPU crédits accumulés par une instance depuis son lancement ou son démarrage. Pour les instances T2 Standard, le `CPUCreditBalance` inclut également le nombre de crédits de lancement qui ont été accumulés. Les crédits sont accumulés dans le solde de crédits quand ils sont gagnés et supprimés du solde de crédits lorsqu'ils sont dépensés. Le solde de crédits présente une limite maximum qui est déterminée par la taille de l'instance. Une fois que la limite est atteinte, tous les nouveaux crédits gagnés sont rejetés. Pour les instances T2 Standard, les crédits de lancement ne sont pas comptés dans la limite.	Crédits (v CPU - minutes)	• Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
	Les crédits contenus dans le `CPUCredit Balance` sont disponibles pour que l'instanc e puisse les dépenser au-delà de son CPU utilisation de base. Les crédits figurant dans le `CPUCredit Balance` d'une instance en cours d'exécuti on n'expirent pas. Lorsqu'une instance T3 ou T3a s'arrête, la valeur `CPUCreditBalance` est conservée pendant sept jours. Au-delà, tous les crédits accumulés sont perdus. Lorsqu'une instance T2 s'arrête, la valeur de `CPUCredit Balance` n'est pas conservée, et tous les crédits accumulés sont perdus. CPUles indicateurs de crédit ne sont disponibl es qu'à une fréquence de 5 minutes.		
`CPUSurplu sCreditBa lance`	Nombre de crédits excédentaires ayant été dépensés par une instance `unlimited` lorsque la valeur `CPUCreditBalance` est nulle. La `CPUSurplusCreditBalance` valeur est remboursée sous forme de CPU crédits gagnés. Si le nombre de crédits excédenta ires dépasse le nombre maximum de crédits que l'instance peut gagner en 24 heures, les crédits excédentaires dépensés au-dessus du maximum génèrent des frais supplémentaires. CPUles indicateurs de crédit ne sont disponibl es qu'à une fréquence de 5 minutes.	Crédits (v CPU - minutes)	• Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
`CPUSurplusCreditsCharged`	Le nombre de crédits excédentaires dépensés qui ne sont pas remboursés par les CPU crédits gagnés et qui entraînent donc des frais supplémentaires. Les crédits excédentaires dépensés sont facturés lorsque l'une des situations suivantes se produit : • Les crédits excédentaires dépensés dépassent le nombre maximum de crédits que l'instance peut gagner sur une période de 24 heures. Les crédits excédentaires dépensés au-dessus de ce maximum sont facturés à la fin de l'heure. • L'instance est arrêtée ou résiliée. • L'instance bascule du mode `unlimited` au mode `standard`. CPUles indicateurs de crédit ne sont disponibles qu'à une fréquence de 5 minutes.	Crédits (v CPU - minutes)	• Somme • Moyenne • Minimum • Maximum

Métriques d'hôte dédié

L'espace de noms `AWS/EC2` inclut les métriques suivantes pour les hôtes dédiés T3.

Métrique	Description	Unité	Statistiques significatives
`DedicatedHostCPUUtilization`	Pourcentage de capacité de calcul allouée actuellement utilisée par les instances exécutées sur l'hôte dédié.	Pourcentage	• Somme • Moyenne • Minimum

Métrique	Description	Unité	Statistiques significatives
			• Maximum

EBSMétriques Amazon pour les instances basées sur Nitro

L'espace de `AWS/EC2` noms inclut des EBS métriques Amazon supplémentaires pour les volumes attachés à des instances basées sur Nitro qui ne sont pas des instances bare metal.

Métrique	Description	Unité	Statistiques significatives
`EBSReadOps`	Opérations de lecture terminées à partir de tous les EBS volumes Amazon attachés à l'instance dans un délai spécifié. Pour calculer la moyenne des opérations d'E/S de lecture par seconde (lectureIOPS) pour la période, divisez le nombre total d'opérations de la période par le nombre de secondes de cette période. Si vous utilisez une surveillance de base (5 minutes), vous pouvez diviser ce nombre par 300 pour calculer le ReadIOPS. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique `DIFF_TIME` pour déterminer les opérations par seconde. Par exemple, si vous avez représenté graphiquement `EBSReadOps` CloudWatch comme `m1`, la formule mathématique de la métrique `m1/(DIFF_TIME(m1))` renvoie la métrique en opérations/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques `DIFF_TIME` et sur d'autres, consultez la section Utiliser les mathématiques	Nombre	• Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
	métriques dans le guide de CloudWatch l'utilisateur Amazon.		
`EBSWriteOps`	Opérations d'écriture terminées sur tous les EBS volumes attachés à l'instance au cours d'une période spécifiée. Pour calculer la moyenne des opérations d'E/S d'écriture par seconde (écritureIOPS) pour la période, divisez le total des opérations de la période par le nombre de secondes de cette période. Si vous utilisez une surveillance de base (5 minutes), vous pouvez diviser ce nombre par 300 pour calculer le WriteIOPS. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique `DIFF_TIME` pour déterminer les opérations par seconde. Par exemple, si vous avez représenté graphiquement `EBSWriteOps` CloudWatch comme `m1`, la formule mathématique de la métrique `m1/(DIFF_TIME(m1))` renvoie la métrique en opérations/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques `DIFF_TIME` et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.	Nombre	• Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
`EBSReadBytes`	Octets lus à partir de tous les EBS volumes attachés à l'instance au cours d'une période spécifiée. Le nombre mentionné correspond au nombre d'octets lus pendant la période. Si vous utilisez une surveillance de base (cinq minutes), vous pouvez diviser ce nombre par 300 pour trouver le nombre d'octets/seconde en lecture. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathémati que CloudWatch métrique `DIFF_TIME` pour déterminer les octets par seconde. Par exemple, si vous avez représenté graphique ment `EBSReadBytes` CloudWatch comme `m1`, la formule mathématique de la métrique `m1/(DIFF_TIME(m1))` renvoie la métrique en octets/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques `DIFF_TIME` et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.	Octets	• Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
`EBSWriteBytes`	Octets écrits sur tous les EBS volumes attachés à l'instance au cours d'une période spécifiée. Le nombre mentionné correspond au nombre d'octets écrits pendant la période. Si vous utilisez une surveillance de base (cinq minutes), vous pouvez diviser ce nombre par 300 pour trouver le nombre d'octets/seconde en écriture. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique `DIFF_TIME` pour déterminer les octets par seconde. Par exemple, si vous avez représenté graphiquement `EBSWriteBytes` CloudWatch comme `m1`, la formule mathématique de la métrique `m1/(DIFF_TIME(m1))` renvoie la métrique en octets/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques `DIFF_TIME` et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.	Octets	• Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
`EBSIOBalance%`	Fournit des informations sur le pourcentage de crédits d'I/O restant dans le compartiment en rafales. Cette métrique est disponible uniquement pour la surveillance basique. Cette métrique n'est disponible que pour certaines tailles d'instance `*.4xlarge` et plus petites qui atteignent leur performance maximale pendant 30 minutes au moins une fois par 24 heures. La statistique `Sum` n'est pas applicable pour cette métrique.	Pourcentage	• Minimum • Maximum
`EBSByteBalance%`	Fournit des informations sur le pourcentage de crédits de débit restant dans le compartiment en rafales. Cette métrique est disponible uniquement pour la surveillance basique. Cette métrique n'est disponible que pour certaines tailles d'instance `*.4xlarge` et plus petites qui atteignent leur performance maximale pendant 30 minutes au moins une fois par 24 heures. La statistique `Sum` n'est pas applicable pour cette métrique.	Pourcentage	• Minimum • Maximum

Pour plus d'informations sur les mesures fournies pour vos EBS volumes, consultez la section Mesures relatives aux EBS volumes Amazon dans le guide de EBS l'utilisateur Amazon. Pour plus d'informations sur les mesures fournies pour vos EC2 flottes et vos flottes ponctuelles, consultez. Surveillez votre EC2 flotte ou repérez votre flotte en utilisant CloudWatch

Métriques de contrôle de statut

Par défaut, les métriques de contrôle de statut sont disponibles à la fréquence d'1 minute sans frais supplémentaires. Pour une instance nouvellement lancée, les données de métriques de contrôle de statut sont disponibles uniquement une fois que l'état d'initialisation de l'instance a pris fin (dans les quelques minutes qui suivent l'entrée de l'instance dans l'état `running`). Pour plus d'informations sur les vérifications de EC2 statut, consultezContrôles de statut pour les EC2 instances Amazon.

L'espace de nom `AWS/EC2` inclut les métriques de contrôle de statut suivantes.

Métrique	Description	Unité	Statistiques significatives
`StatusCheckFailed`	Indique si l'instance a passé avec succès toutes les vérifications de statut au cours de la dernière minute. Cette métrique peut avoir la valeur `0` (succès) ou 1 (échec). Par défaut, cette métrique est disponible à la fréquence d'1 minute sans frais supplémentaires.	Nombre	• Somme • Moyenne
`StatusCheckFailed_Instance`	Indique si l'instance a passé avec succès le contrôle de statut de l'instance de la dernière minute. Cette métrique peut avoir la valeur `0` (succès) ou 1 (échec). Par défaut, cette métrique est disponible à la fréquence d'1 minute sans frais supplémentaires.	Nombre	• Somme • Moyenne
`StatusCheckFailed_System`	Indique si l'instance a passé avec succès le contrôle de statut du système de la dernière minute.	Nombre	• Somme • Moyenne

Métrique	Description	Unité	Statistiques significatives
	Cette métrique peut avoir la valeur `0` (succès) ou 1 (échec). Par défaut, cette métrique est disponible à la fréquence d'1 minute sans frais supplémentaires.		
`StatusCheckFailed_AttachedEBS`	Indique si l'instance a passé avec succès le contrôle de EBS statut joint au cours de la dernière minute. Cette métrique peut avoir la valeur `0` (succès) ou 1 (échec). Par défaut, cette métrique est disponible à la fréquence d'1 minute sans frais supplémentaires.	Nombre	• Somme • Moyenne

L'`AWS/EBS`espace de noms inclut la métrique de vérification de statut suivante.

Métrique	Description	Unité	Statistiques significatives
`VolumeStalledIOCheck`	Remarque : pour les instances Nitro uniquement. Non publié pour les volumes attachés à Amazon ECS et AWS Fargate les tâches. Indique si un volume a réussi ou échoué à une vérification d'E/S bloquée au cours de la dernière minute. Cette métrique peut avoir la valeur `0` (succès) ou 1 (échec).	Aucun	• Somme • Moyenne • Minimum • Maximum

Métriques de mise en miroir du trafic

L'espace de noms `AWS/EC2` inclut des métriques pour le trafic mis en miroir. Pour plus d'informations, consultez la section Surveiller le trafic miroir à l'aide d'Amazon CloudWatch dans le guide Amazon VPC Traffic Mirroring.

Métriques du groupe Auto Scaling

L'espace de noms `AWS/AutoScaling` inclut des métriques pour les groupes Auto Scaling. Pour plus d'informations, consultez la section Surveillance CloudWatch des métriques pour vos groupes et instances Auto Scaling dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.

Dimensions EC2 métriques d'Amazon

Vous pouvez utiliser les dimensions suivantes pour affiner les métriques répertoriées dans les tableaux précédents.

Dimension	Description
`AutoScalingGroupName`	Cette dimension filtre les données que vous demandez pour toutes les instances dans un groupe de capacité donné. Un groupe Auto Scaling est un ensemble d'instances que vous définissez si vous utilisez Auto Scaling. Cette dimension n'est disponible que pour les EC2 métriques Amazon lorsque les instances font partie d'un tel groupe Auto Scaling. Disponibl e pour les instances avec la surveillance détaillée ou basique activée.
`ImageId`	Cette dimension filtre les données que vous demandez pour toutes les instances exécutant cette EC2 Amazon Machine Image (AMI). Disponible pour les instances avec la surveillance détaillée activée.
`InstanceId`	Cette dimension filtre les données que vous demandez de l'instance identifiée uniquement. Cela vous aide à identifier une instance exacte à partir de laquelle surveiller les données.
`InstanceType`	Cette dimension filtre les données que vous demandez pour toutes les instances s'exécutant avec ce type d'instance

Dimension	Description
	spécifiée. Cela vous permet de classer vos données selon le type d'instance en cours d'exécution. Par exemple, vous pouvez comparer les données issues d'une instance m1.small et d'une instance m1.large pour déterminer qui a la meilleure valeur commerciale pour votre application. Disponible pour les instances avec la surveillance détaillée activée.

Statistiques EC2 d'utilisation d'Amazon

Vous pouvez utiliser les statistiques CloudWatch d'utilisation pour obtenir une visibilité sur l'utilisation des ressources par votre compte. Utilisez ces indicateurs pour visualiser l'utilisation actuelle de vos services sur CloudWatch des graphiques et des tableaux de bord.

Les statistiques EC2 d'utilisation d'Amazon correspondent aux quotas AWS de service. Vous pouvez configurer des alarmes qui vous alertent lorsque votre utilisation approche d'un quota de service. Pour plus d'informations sur CloudWatch l'intégration avec les quotas de service, consultez les statistiques AWS d'utilisation dans le guide de CloudWatch l'utilisateur Amazon.

Amazon EC2 publie les métriques suivantes dans l'espace de `AWS/Usage` noms.

Métrique	Description
`ResourceCount`	Nombre des ressources spécifiées exécutées dans votre compte. Les ressources sont définies par les dimensions associées à la métrique. La statistique la plus utile pour cette métrique est `MAXIMUM`, qui représente le nombre maximal de ressources utilisées pendant la période d'une minute.

Les dimensions suivantes sont utilisées pour affiner les statistiques d'utilisation publiées par AmazonEC2.

Dimension	Description
`Service`	Nom du AWS service contenant la ressource. Pour les statistiq ues EC2 d'utilisation d'Amazon, la valeur de cette dimension est`EC2`.
`Type`	Type d'entité faisant l'objet d'un rapport. Actuellement, la seule valeur valide pour les métriques EC2 d'utilisation d'Amazon est`Resource`.
`Resource`	Type de ressource en cours d'exécution. Actuellement, la seule valeur valide pour les métriques EC2 d'utilisation d'Amazon est`vCPU`, qui renvoie des informations sur les instances en cours d'exécution.
`Class`	Classe de ressource suivie. Pour les métriques EC2 d'utilisa tion d'Amazon dont la valeur de la `Resource` dimension est la valeur`Standard/OnDemand` , les valeurs valides sont `F/ OnDemand` `G/OnDemand` ,`Inf/OnDemand` ,`P/OnDemand` , et`X/OnDemand` . `vCPU` Les valeurs de cette dimension définissent la première lettre des types d'instance signalés par la métrique. Par exemple, `Standard/OnDemand` renvoie des informations sur toutes les instances en cours d'exécution dont les types commencen t par A, C, D, H, I, M, R, T et Z, et `G/OnDemand` renvoie des informations sur toutes les instances en cours d'exécution dont les types commencent par G.

Installez et configurez l' CloudWatchagent à l'aide de la EC2 console Amazon pour ajouter des métriques supplémentaires

L'installation et la configuration de l' CloudWatch agent à l'aide de la EC2 console Amazon sont en version bêta pour Amazon EC2 et sont susceptibles d'être modifiées.

Par défaut, Amazon CloudWatch fournit des mesures de base, telles que `CPUUtilization` et`NetworkIn`, pour surveiller vos EC2 instances Amazon. Pour collecter des métriques supplémentaires, vous pouvez installer l' CloudWatch agent sur vos EC2 instances, puis configurer l'agent pour qu'il émette les métriques sélectionnées. Au lieu d'installer et de configurer manuellement l' CloudWatch agent sur chaque EC2 instance, vous pouvez utiliser la EC2 console Amazon pour le faire à votre place.

Cette rubrique explique comment utiliser la EC2 console Amazon pour installer l' CloudWatch agent sur vos instances et configurer l'agent pour qu'il émette des métriques sélectionnées.

Pour les étapes manuelles de ce processus, consultez la section Installation de l' CloudWatch agent AWS Systems Managerà l'aide du guide de CloudWatch l'utilisateur Amazon. Pour plus d'informations sur l' CloudWatch agent, consultez la section Collecter les métriques, les journaux et les traces avec l' CloudWatch agent.

Rubriques

Prérequis

Pour utiliser Amazon EC2 pour installer et configurer l' CloudWatch agent, vous devez satisfaire aux exigences relatives à l'utilisateur et à l'instance décrites dans cette section.

Conditions requises pour l'utilisateur

Pour utiliser cette fonctionnalité, l'utilisateur ou le rôle de votre IAM console doit disposer des autorisations requises pour utiliser Amazon EC2 et des IAM autorisations suivantes :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter",
                "ssm:PutParameter"
```

```
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/EC2-Custom-Metrics-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:ListCommandInvocations",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetInstanceProfile",
                "iam:SimulatePrincipalPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Conditions préalables à l'instance

- État de l'instance : `running`
- Système d'exploitation pris en charge : Linux
- AWS Systems Manager Agent (SSMagent) : installé. Deux remarques à propos de SSM l'agent :
  - SSML'agent est préinstallé sur certaines Amazon Machine Images (AMIs) fournies par AWS des tiers de confiance. Pour plus d'informations sur le support AMIs et les instructions d'installation de SSM l'agent, consultez Amazon Machine Images (AMIs) avec SSM agent préinstallé dans le guide de l'AWS Systems Manager utilisateur.
  - Si vous rencontrez des problèmes avec l'SSMagent, consultez la section Dépannage de SSM l'agent dans le guide de AWS Systems Manager l'utilisateur.
- IAMautorisations pour l'instance : les politiques AWS gérées suivantes doivent être ajoutées à un IAM rôle attaché à l'instance :
  - A mazonSSMManaged InstanceCore — Permet à une instance d'utiliser Systems Manager pour installer et configurer l' CloudWatch agent.

- CloudWatchAgentServerPolicy— Permet à une instance d'utiliser l' CloudWatchagent pour y écrire des données CloudWatch.

Pour plus d'informations sur la façon d'ajouter IAM des autorisations à votre instance, consultez la section Utilisation des profils d'instance dans le Guide de IAM l'utilisateur.

Comment ça marche

Avant de pouvoir utiliser la EC2 console Amazon pour installer et configurer l' CloudWatch agent, vous devez vous assurer que votre IAM utilisateur ou votre rôle, ainsi que les instances sur lesquelles vous souhaitez ajouter des métriques, répondent à certaines conditions préalables. Vous pouvez ensuite utiliser la EC2 console Amazon pour installer et configurer l' CloudWatch agent sur les instances que vous avez sélectionnées.

Répondez d'abord aux prérequis

- Vous avez besoin des IAM autorisations requises : avant de commencer, assurez-vous que l'utilisateur ou le rôle de votre console dispose des IAM autorisations requises pour utiliser cette fonctionnalité.
- Instances : pour utiliser cette fonctionnalité, vos EC2 instances doivent être des instances Linux, l'SSMagent doit être installé, disposer des IAM autorisations requises et être en cours d'exécution.

Ensuite, vous pouvez utiliser la fonctionnalité

1. Sélectionnez vos instances : dans la EC2 console Amazon, vous sélectionnez les instances sur lesquelles vous souhaitez installer et configurer l' CloudWatch agent. Vous lancez ensuite le processus en choisissant Configurer CloudWatch l'agent.
2. Valider SSM l'agent : Amazon EC2 vérifie que l'SSMagent est installé et démarré sur chaque instance. Toutes les instances qui échouent à cette vérification sont exclues du processus. L'SSMagent est utilisé pour effectuer des actions sur l'instance au cours de ce processus.
3. Valider IAM les autorisations : Amazon EC2 vérifie que chaque instance dispose des IAM autorisations requises pour ce processus. Toutes les instances qui échouent à cette vérification sont exclues du processus. Les IAM autorisations permettent à l' CloudWatch agent de collecter des métriques à partir de l'instance et de les intégrer AWS Systems Manager pour utiliser l'SSMagent.
4. Valider CloudWatch l'agent : Amazon EC2 vérifie que l' CloudWatch agent est installé et s'exécute sur chaque instance. Si une instance échoue à cette vérification, Amazon EC2 propose d'installer

et de démarrer l' CloudWatch agent pour vous. L' CloudWatch agent collectera les métriques sélectionnées sur chaque instance une fois ce processus terminé.

5. Sélectionnez la configuration des métriques : vous sélectionnez les métriques que l' CloudWatch agent doit émettre depuis vos instances. Une fois sélectionné, Amazon EC2 stocke un fichier de configuration dans Parameter Store, où il est conservé jusqu'à la fin du processus. Amazon EC2 supprimera le fichier de configuration de Parameter Store à moins que le processus ne soit interrompu. Notez que si vous ne sélectionnez pas de métrique, mais que vous l'avez déjà ajoutée à votre instance, elle sera supprimée de votre instance une fois ce processus terminé.
6. Mettre à jour la configuration de l' CloudWatch agent : Amazon EC2 envoie la configuration métrique à l' CloudWatch agent. Il s'agit de la dernière étape du processus. En cas de succès, vos instances peuvent émettre des données pour les métriques sélectionnées et Amazon EC2 supprime le fichier de configuration de Parameter Store.

Coûts

Les mesures supplémentaires que vous ajoutez au cours de ce processus sont facturées en tant que mesures personnalisées. Pour plus d'informations sur la tarification des CloudWatch métriques, consultez Amazon CloudWatch Pricing.

Installation et configuration de l' CloudWatch agent

Vous pouvez utiliser la EC2 console Amazon pour installer et configurer l' CloudWatch agent afin d'ajouter des métriques supplémentaires.

> **Note**
>
> Chaque fois que vous effectuez cette procédure, vous remplacez la configuration de l' CloudWatch agent existante. Si vous ne sélectionnez aucune métrique sélectionnée précédemment, elle sera supprimée de l'instance.

Pour installer et configurer l' CloudWatch agent à l'aide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez les instances sur lesquelles vous souhaitez installer et configurer l' CloudWatch agent.

4. Choisissez Actions, Surveillance et résolution des problèmes, Configuration de CloudWatch l'agent.

> **Tip**
>
> Cette fonctionnalité n'est pas disponible du tout Régions AWS. Si CloudWatchl'agent de configuration n'est pas disponible, essayez une autre région.

5. Pour chaque étape du processus, lisez le texte de la console, puis choisissez Next.
6. Pour terminer le processus, dans la dernière étape, sélectionnez Terminer.

Statistiques pour les CloudWatch métriques relatives à vos instances

Vous pouvez obtenir des statistiques relatives aux CloudWatch métriques de vos instances. Les statistiques sont des agrégations de données métriques sur des périodes spécifiques. CloudWatch fournit des statistiques basées sur les points de données métriques fournis par vos données personnalisées ou fournis par d'autres services AWS connexes CloudWatch. Les regroupements sont effectués en utilisant l'espace de noms, le nom métrique, les dimensions et l'unité de mesure des points de données, pendant la période spécifiée. Le tableau suivant décrit les statistiques disponibles.

Statistique	Description
`Minimum`	La valeur la plus basse observée pendant la période spécifiée. Vous pouvez utiliser cette valeur pour déterminer les faibles volumes d'activité pour votre application.
`Maximum`	La valeur la plus haute observée pendant la période spécifiée. Vous pouvez utiliser cette valeur pour déterminer les volumes d'activité élevés pour votre application.
`Sum`	Toutes les valeurs soumises pour la métrique correspondante ajoutées ensemble. Cette statistique peut être utile pour déterminer le volume total d'une métrique.
`Average`	La valeur de `Sum` / `SampleCount` pendant la période spécifiée. En comparant cette statistique à `Minimum` et à `Maximum`, vous pouvez déterminer l'ampleur d'une métrique et si l'utilisation moyenne est proche de `Minimum` ou de `Maximum`.

Statistique	Description
	Cette comparaison vous permet de savoir quand augmenter ou diminuer vos ressources en fonction des besoins.
`SampleCount`	Le compte (nombre) des points de données utilisé pour le calcul statistique.
`pNN.NN`	Valeur du centile spécifié. Vous pouvez spécifier un centile en utilisant jusqu'à deux décimales (par exemple, p95.45).

Table des matières

Obtenir les statistiques d'une instance spécifique

Vous pouvez utiliser le AWS Management Console ou le AWS CLI pour obtenir des statistiques pour une instance spécifique. Les exemples suivants vous montrent comment utiliser le AWS Management Console ou le AWS CLI pour déterminer l'CPUutilisation maximale d'une EC2 instance spécifique.

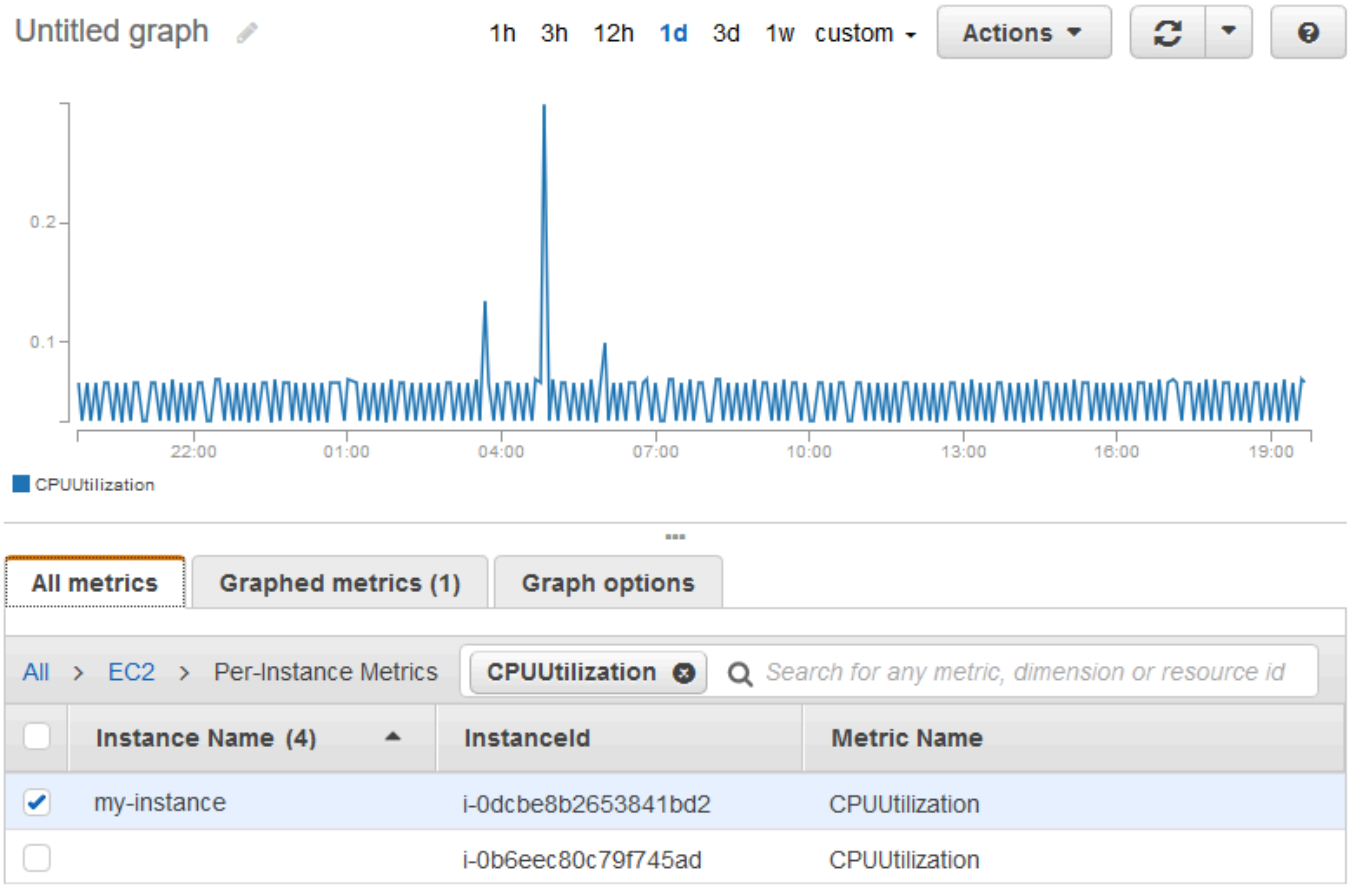
Prérequis

- Vous devez avoir l'ID de l'instance. Vous pouvez obtenir l'ID d'instance en utilisant AWS Management Console ou la commande describe-instances.
- Par défaut, la surveillance basique est activée, mais vous pouvez activer la surveillance détaillée. Pour de plus amples informations, veuillez consulter Gérez la surveillance détaillée de vos EC2 instances.

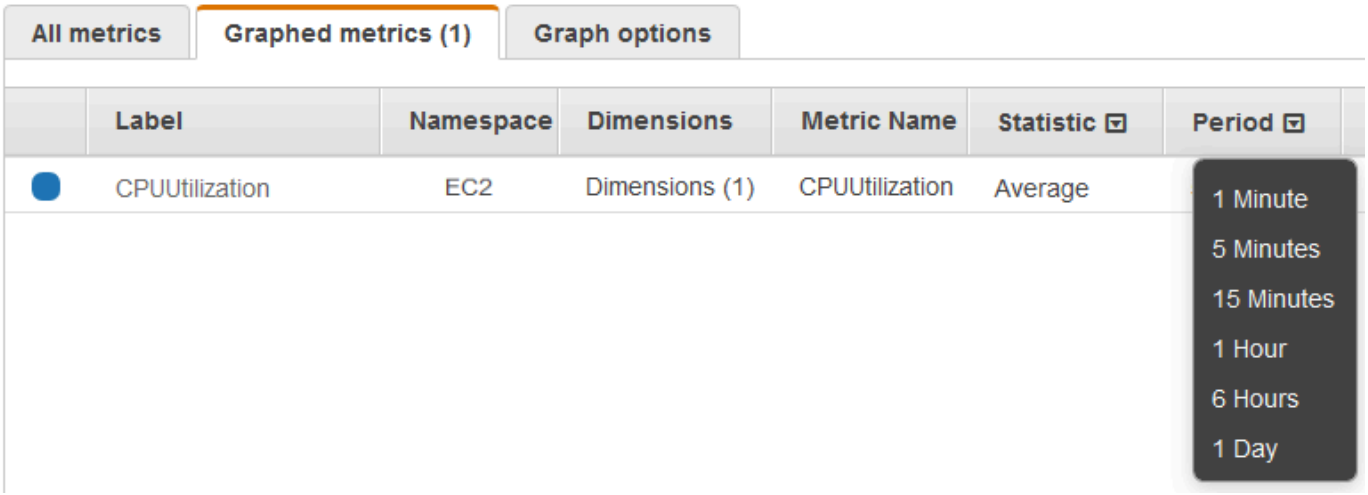
Pour afficher l'CPUutilisation d'une instance spécifique (console)

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Choisissez l'espace de noms de la EC2métrique.

4. Choisissez la dimension Per-Instance Metrics (Métriques par instance).
5. Dans le champ de recherche, entrez **`CPUUtilization`**, puis appuyez sur Entrée. Choisissez la ligne pour l'instance spécifique, qui affiche un graphique pour la CPUUtilizationmétrique de l'instance. Pour nommer le graphique, choisissez l'icône en forme de crayon. Pour modifier la plage de temps, sélectionnez l'une des valeurs prédéfinies ou choisissez custom.



6. Pour modifier la statistique ou la période pour la métrique, choisissez l'onglet Graphed metrics. Sélectionnez l'en-tête de colonne ou une valeur individuelle et choisissez une autre valeur.



Pour obtenir le CPU taux d'utilisation d'une instance spécifique (AWS CLI)

Utilisez la get-metric-statisticscommande suivante pour obtenir la CPUUtilizationmétrique pour l'instance spécifiée, en utilisant la période et l'intervalle de temps spécifiés :

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
 --period 3600 \
--statistics Maximum --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
--start-time 2022-10-18T23:18:00 --end-time 2022-10-19T23:18:00
```

Voici un exemple de sortie. Chaque valeur représente le pourcentage CPU d'utilisation maximal pour une EC2 instance unique.

```
{
    "Datapoints": [
        {
            "Timestamp": "2022-10-19T00:18:00Z",
            "Maximum": 0.33000000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T03:18:00Z",
            "Maximum": 99.670000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T07:18:00Z",
            "Maximum": 0.34000000000000002,
```

```
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T12:18:00Z",
            "Maximum": 0.34000000000000002,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```

Regrouper les statistiques à travers les instances

Les statistiques agrégées sont disponibles pour des instances pour lesquelles la surveillance détaillée a été activée. Les instances qui utilisent la surveillance basique ne sont pas incluses dans les regroupements. Avant de pouvoir obtenir des statistiques regroupées entre les instances, vous devez activer la surveillance détaillée (avec coût additionnel) qui fournit des données toutes les minutes.

Notez qu'Amazon CloudWatch ne peut pas agréger les données entre AWS les régions. Les métriques sont totalement séparées d'une région à une autre.

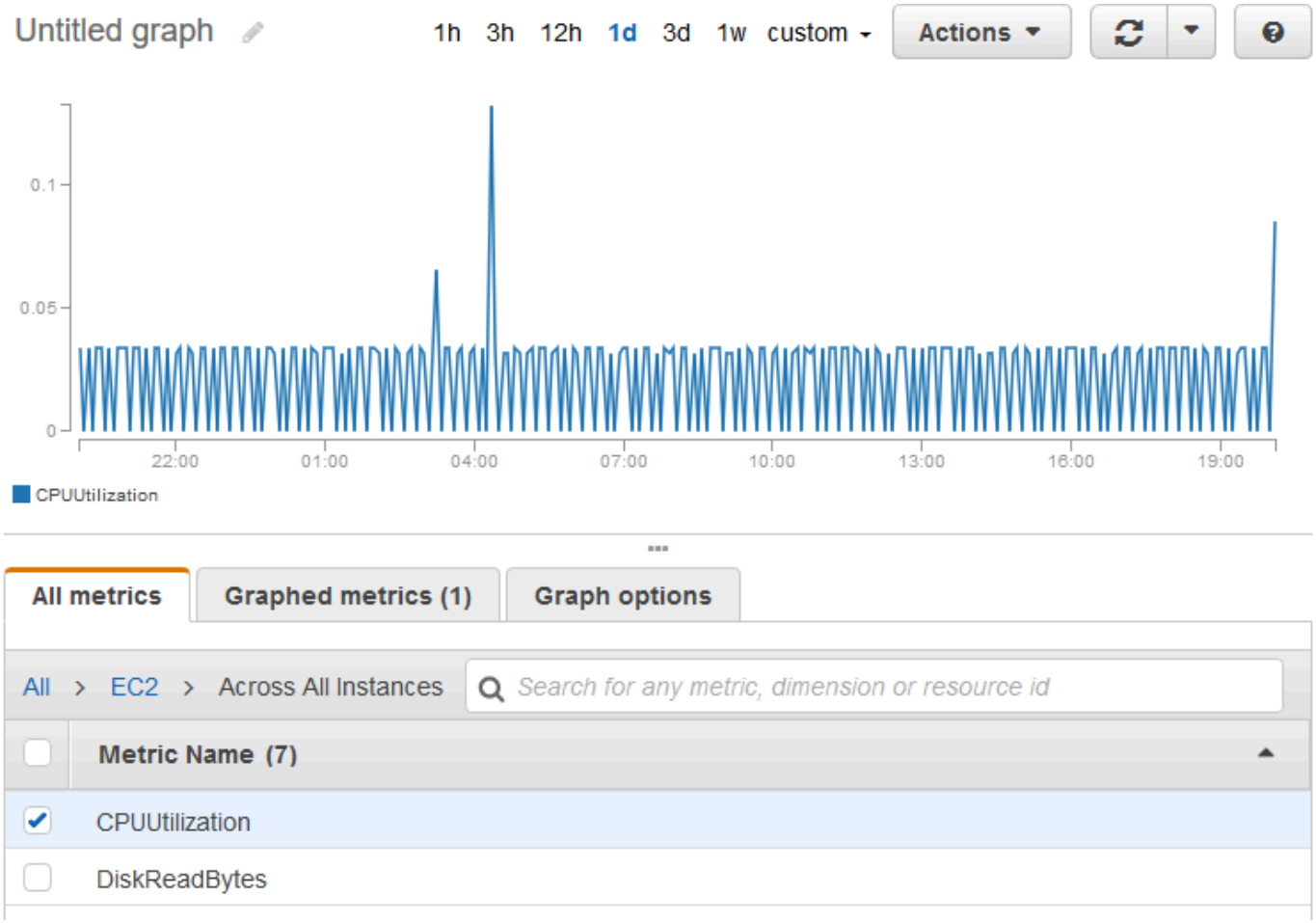
Cet exemple vous montre comment utiliser une surveillance détaillée pour obtenir l'CPUutilisation moyenne de vos EC2 instances. Aucune dimension n'étant spécifiée, CloudWatch renvoie des statistiques pour toutes les dimensions de l'espace de `AWS/EC2` noms.

> **Important**
>
> Cette technique de récupération de toutes les dimensions d'un espace de AWS noms ne fonctionne pas pour les espaces de noms personnalisés que vous publiez sur Amazon. CloudWatch Avec les espaces de noms personnalisés, vous devez spécifier l'ensemble complet des dimensions associées à un point de données particulier pour pouvoir extraire les statistiques qui incluent le point de données.

Pour afficher le taux d'CPUutilisation moyen sur l'ensemble de vos instances (console)

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Métriques.

3. Choisissez l'espace de EC2noms, puis choisissez Across All Instances.
4. Choisissez la ligne qui contient CPUUtilization, qui affiche un graphique pour la métrique pour toutes vos EC2 instances. Pour nommer le graphique, choisissez l'icône en forme de crayon. Pour modifier la plage de temps, sélectionnez l'une des valeurs prédéfinies ou choisissez custom.



5. Pour modifier la statistique ou la période pour la métrique, choisissez l'onglet Graphed metrics. Sélectionnez l'en-tête de colonne ou une valeur individuelle et choisissez une autre valeur.

Pour obtenir un CPU taux d'utilisation moyen sur l'ensemble de vos instances (AWS CLI)

Utilisez la get-metric-statisticscommande suivante pour obtenir la moyenne de la CPUUtilizationmétrique sur vos instances.

```
aws cloudwatch get-metric-statistics \
    --namespace AWS/EC2 \
    --metric-name CPUUtilization \
    --period 3600  --statistics "Average" "SampleCount" \
```

```
    --start-time 2022-10-11T23:18:00 \
    --end-time 2022-10-12T23:18:00
```

Voici un exemple de sortie :

```
{
    "Datapoints": [
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-12T07:18:00Z",
            "Average": 0.038235294117647062,
            "Unit": "Percent"
        },
        {
            "SampleCount": 240.0,
            "Timestamp": "2022-10-12T09:18:00Z",
            "Average": 0.16670833333333332,
            "Unit": "Percent"
        },
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-11T23:18:00Z",
            "Average": 0.041596638655462197,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```

Regroupement de statistiques par groupe Auto Scaling

Vous pouvez agréger les statistiques des EC2 instances d'un groupe Auto Scaling. Notez qu'Amazon CloudWatch ne peut pas agréger les données entre AWS les régions. Les métriques sont totalement séparées d'une région à une autre.

Cet exemple vous montre comment récupérer le nombre total d'octets écrits sur disque pour un groupe Auto Scaling. Le total est calculé pour des périodes d'une minute pour un intervalle de 24 heures sur toutes les EC2 instances du groupe Auto Scaling spécifié.

DiskWriteBytes Pour afficher les instances d'un groupe Auto Scaling (console)

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Choisissez l'espace de EC2noms, puis choisissez By Auto Scaling Group.
4. Choisissez la ligne pour la DiskWriteBytesmétrique et le groupe Auto Scaling spécifique, qui affiche un graphique pour la métrique pour les instances du groupe Auto Scaling. Pour nommer le graphique, choisissez l'icône en forme de crayon. Pour modifier la plage de temps, sélectionnez l'une des valeurs prédéfinies ou choisissez custom.
5. Pour modifier la statistique ou la période pour la métrique, choisissez l'onglet Graphed metrics. Sélectionnez l'en-tête de colonne ou une valeur individuelle et choisissez une autre valeur.

DiskWriteBytes Pour afficher les instances d'un groupe Auto Scaling (AWS CLI)

Utilisez la commande get-metric-statistics comme suit.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name DiskWriteBytes
 --period 360 \
--statistics "Sum" "SampleCount" --dimensions Name=AutoScalingGroupName,Value=my-asg --
start-time 2022-10-16T23:18:00 --end-time 2022-10-18T23:18:00
```

Voici un exemple de sortie :

```
{
    "Datapoints": [
        {
            "SampleCount": 18.0,
            "Timestamp": "2022-10-19T21:36:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "SampleCount": 5.0,
            "Timestamp": "2022-10-19T21:42:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        }
    ],
    "Label": "DiskWriteBytes"
```

```
}
```

Statistiques agrégées par AMI

Vous pouvez agréger les statistiques AMI pour les instances pour lesquelles la surveillance détaillée est activée. Les instances qui utilisent la surveillance basique ne sont pas incluses dans les regroupements. Avant de pouvoir obtenir des statistiques regroupées entre les instances, vous devez activer la surveillance détaillée (avec coût additionnel) qui fournit des données toutes les minutes.

Notez qu'Amazon CloudWatch ne peut pas agréger les données entre AWS les régions. Les métriques sont totalement séparées d'une région à une autre.

Cet exemple vous montre comment déterminer le CPU taux d'utilisation moyen pour toutes les instances qui utilisent une Amazon Machine Image (AMI) spécifique. La moyenne est calculée par intervalles de 60 secondes pour une période d'un jour.

Pour afficher l'CPUutilisation moyenne par AMI (console)

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Choisissez l'espace de EC2noms, puis choisissez By Image (AMI) Id.
4. Choisissez la ligne pour la CPUUtilizationmétrique et la ligne spécifiqueAMI, qui affiche un graphique pour la métrique spécifiéeAMI. Pour nommer le graphique, choisissez l'icône en forme de crayon. Pour modifier la plage de temps, sélectionnez l'une des valeurs prédéfinies ou choisissez custom.
5. Pour modifier la statistique ou la période pour la métrique, choisissez l'onglet Graphed metrics. Sélectionnez l'en-tête de colonne ou une valeur individuelle et choisissez une autre valeur.

Pour obtenir l'CPUutilisation moyenne d'un ID d'image (AWS CLI)

Utilisez la commande get-metric-statistics comme suit.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
 --period 3600 \
--statistics Average --dimensions Name=ImageId,Value=ami-3c47a355 --start-
time 2022-10-10T00:00:00 --end-time 2022-10-11T00:00:00
```

Voici un exemple de sortie. Chaque valeur représente un pourcentage d'CPUutilisation moyen pour les EC2 instances exécutant la valeur spécifiéeAMI.

```
{
    "Datapoints": [
        {
            "Timestamp": "2022-10-10T07:00:00Z",
            "Average": 0.041000000000000009,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T14:00:00Z",
            "Average": 0.079579831932773085,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T06:00:00Z",
            "Average": 0.036000000000000011,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```


Afficher les graphiques de surveillance de vos instances

Après avoir lancé une instance, vous pouvez ouvrir la EC2 console Amazon et consulter les graphiques de surveillance de l'instance dans l'onglet Surveillance. Chaque graphique est basé sur l'une des EC2 statistiques Amazon disponibles.

Les graphiques suivants sont disponibles :

- CPUUtilisation moyenne (pourcentage)
- Lectures moyennes sur disque (octets)
- Ecritures moyennes sur disque (octets)
- Nombre maximal entrées réseau (octets)
- Nombre maximal sorties réseau (octets)
- Récapitulatif des opérations de lecture sur disque (nombre)
- Récapitulatif des opérations d'écriture sur disque (nombre)
- Récapitulatif des statuts (quels qu'il soient)
- Récapitulatif des statuts d'instance (nombre)

- Récapitulatif des statuts système (nombre)

Pour plus d'informations sur les métriques et les données qu'elles leur fournissent, consultez CloudWatch métriques disponibles pour vos instances.

Représentez graphiquement les métriques à l'aide CloudWatch de

Vous pouvez également utiliser la CloudWatch console pour représenter graphiquement les données métriques générées par Amazon EC2 et d'autres AWS services. Pour plus d'informations, consultez la section Représentation graphique des métriques dans le guide de CloudWatch l'utilisateur Amazon.

Création d'une CloudWatch alarme pour une instance

Vous pouvez créer une CloudWatch alarme qui surveille les CloudWatch métriques de l'une de vos instances. CloudWatchvous enverra automatiquement une notification lorsque la métrique atteindra le seuil que vous spécifiez. Vous pouvez créer une CloudWatch alarme à l'aide de la EC2 console Amazon ou à l'aide des options plus avancées proposées par la CloudWatch console.

Pour créer une alarme à l'aide de la CloudWatch console

Pour des exemples, consultez la section Création d' CloudWatchalarmes Amazon dans le guide de CloudWatch l'utilisateur Amazon.

Pour créer une alarme à l'aide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance et choisissez Actions, Surveiller et dépanner, Gérer les CloudWatch alarmes.
4. Sur la page détaillée de gestion des CloudWatch alarmes, sous Ajouter ou modifier une alarme, sélectionnez Créer une alarme.
5. Pour les notifications d'alarme, choisissez si vous souhaitez configurer les notifications Amazon Simple Notification Service (AmazonSNS). Entrez un SNS sujet Amazon existant ou entrez un nom pour créer un nouveau sujet.
6. Pour Action d'alarme, choisissez si vous souhaitez spécifier une action à effectuer lorsque l'alarme est déclenchée. Choisissez une action dans la liste.

7. Pour Seuils d'alarme, sélectionnez la métrique et les critères de l'alarme. Par exemple, pour créer une alarme qui se déclenche lorsque le CPU taux d'utilisation atteint 80 % pendant une période de 5 minutes, procédez comme suit :

   a. Conservez le paramètre par défaut pour Regrouper les échantillons par (moyenne) et Type de données à échantillonner (CPUutilisation).

   b. Choisissez **>=** pour Alarme quand et saisissez **`0.80`** pour Pourcentage.

   c. Saisissez **`1`** pour Période consécutive et sélectionnez 5 minutes pour Période.

8. (Facultatif) Pour Exemple de données de métrique, choisissez Ajouter au tableau de bord.

9. Sélectionnez Create (Créer).

Vous pouvez modifier les paramètres de votre CloudWatch alarme depuis la EC2 console Amazon ou depuis la CloudWatch console. Si vous souhaitez supprimer votre alarme, vous pouvez le faire depuis la CloudWatch console. Pour plus d'informations, consultez Modifier ou supprimer une CloudWatch alarme dans le guide de CloudWatch l'utilisateur Amazon.

Créer des alarmes qui arrêtent, finissent, redémarrent ou récupèrent une instance

À l'aide des actions CloudWatch d'alarme Amazon, vous pouvez créer des alarmes qui arrêtent, mettent fin, redémarrent ou restaurent automatiquement vos instances. Vous pouvez utiliser les actions d'arrêt ou de terminaison pour vous permettre d'économiser de l'argent quand vous n'avez plus besoin qu'une instance s'exécute. De même, les actions de redémarrage et de récupération vous permettent de redémarrer automatiquement ces instances ou de les récupérer sur un nouveau matériel en cas de déficience du nouveau matériel.

> **Note**
>
> Pour les informations de facturation et de tarification d'Amazon CloudWatch Alarmes, consultez la section CloudWatch facturation et coûts dans le guide de CloudWatch l'utilisateur Amazon.

Le rôle `AWSServiceRoleForCloudWatchEvents` lié au service permet d' AWS effectuer des actions d'alarme en votre nom. La première fois que vous créez une alarme dans le AWS Management Console, le AWS CLI, ou le IAMAPI, CloudWatch crée le rôle lié au service pour vous.

Il existe un certain nombre de scénarios dans lesquels vous pourriez vouloir arrêter ou terminer automatiquement votre instance. Par exemple, vous pourriez avoir des instances dédiées aux tâches de traitement différé de la paie ou de calcul scientifique qui s'exécutent pendant une durée, puis achèvent leur travail. Plutôt que de laisser ces instances demeurer inactives (et d'accumuler les frais), vous pouvez les arrêter ou les terminer, ce qui peut vous aider à économiser de l'argent. La principale différence entre l'utilisation des actions d'alarme « stop » et « terminate » est que vous pouvez facilement démarrer une instance arrêtée si vous devez l'exécuter à nouveau ultérieurement, et que vous pouvez conserver les mêmes ID d'instance et volume racine. Cependant, vous ne pouvez pas démarrer une instance résiliée. Vous devez à la place lancer une nouvelle instance. Lorsqu'une instance est arrêtée ou résiliée, les données sur les volumes de stockage d'instances sont perdues.

Vous pouvez ajouter les actions d'arrêt, de résiliation, de redémarrage ou de restauration à toute alarme définie sur une métrique Amazon EC2 par instance, y compris les mesures de surveillance de base et détaillées fournies par Amazon CloudWatch (dans l'`AWS/EC2`espace de noms), ainsi que toutes les mesures personnalisées qui incluent la `InstanceId` dimension, à condition que sa valeur fasse référence à une instance Amazon EC2 en cours d'exécution valide.

> **Important**
>
> Les alarmes de vérification d'état peuvent entrer temporairement dans l'`INSUFFICIENT_DATA`état s'il manque des points de données métriques. Bien que cela soit rare, cela peut se produire en cas d'interruption des systèmes de reporting des métriques, même lorsqu'une instance est saine. Nous vous recommandons de traiter l'`INSUFFICIENT_DATA`état comme une donnée manquante plutôt que comme une violation d'alarme, en particulier lorsque vous configurez l'alarme pour arrêter, arrêter, redémarrer ou récupérer une instance.

Prise en charge de la console

Vous pouvez créer des alarmes à l'aide de la EC2 console Amazon ou de la CloudWatch console. Les procédures décrites dans cette documentation utilisent la EC2 console Amazon. Pour les procédures utilisant la CloudWatch console, consultez la section Créer des alarmes qui arrêtent, mettent fin, redémarrent ou restaurent une instance dans le guide de CloudWatch l'utilisateur Amazon.

Autorisations

Vous devez disposer du `iam:CreateServiceLinkedRole` pour créer ou modifier une alarme qui exécute des actions EC2 d'alarme. Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, consultez la section Création d'un rôle auquel déléguer des autorisations service AWS dans le Guide de IAM l'utilisateur.

Table des matières

Ajouter des actions d'arrêt aux CloudWatch alarmes Amazon

Vous pouvez créer une alarme qui arrête une EC2 instance Amazon lorsqu'un certain seuil est atteint. Par exemple, vous pouvez exécuter des instances de développement ou de test, et, à l'occasion, oublier de les fermer. Vous pouvez créer une alarme qui se déclenche lorsque le pourcentage CPU d'utilisation moyen est inférieur à 10 % pendant 24 heures, signalant qu'elle est inactive et qu'elle n'est plus utilisée. Vous pouvez ajuster le seuil, la durée et la période en fonction de vos besoins, et vous pouvez également ajouter une notification Amazon Simple Notification Service (AmazonSNS) afin de recevoir un e-mail lorsque l'alarme est déclenchée.

Les instances qui utilisent un EBS volume Amazon comme périphérique racine peuvent être arrêtées ou résiliées, tandis que les instances qui utilisent le magasin d'instances comme périphérique racine peuvent uniquement être résiliées. Les données stockées sur des volumes de stockage d'instance sont perdues lorsque l'instance est résiliée ou arrêtée.

Pour créer une alarme afin d'arrêter une instance inactive (EC2console Amazon)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance et choisissez Actions, Surveiller et dépanner, Gérer les CloudWatch alarmes.

Vous pouvez également sélectionner le signe plus (

) dans la colonne Alarm status (Statut de l'alarme) .

4. Sur la page Gérer les CloudWatch alarmes, procédez comme suit :

   a. Sélectionnez Create an alarm (Créer une alarme).

   b. Pour recevoir un e-mail lorsque l'alarme est déclenchée, pour la notification d'alarme, choisissez un SNS sujet Amazon existant. Vous devez d'abord créer un SNS sujet Amazon à l'aide de la SNS console Amazon. Pour plus d'informations, consultez la section Utilisation d'Amazon SNS pour la messagerie application-to-person (A2P) dans le manuel du développeur Amazon Simple Notification Service.

   c. Activer l'option Alarm action (Action d'alarme), puis sélectionnez Stop (Arrêter).

   d. Pour Group samples by (Regrouper les échantillons par) et Type of data to sample (Type de données à échantillonner), sélectionnez une statistique et une métrique. Dans cet exemple, sélectionnez Moyenne et CPUutilisation.

   e. Pour Alarm When (Alarme Quand) et Percent (Pourcentage), spécifiez le seuil de la métrique. Dans cet exemple, spécifiez <= et 10 pour cent.

   f. Pour Consecutive period (Période consécutive) et Period (Période), spécifiez la période d'évaluation de l'alarme. Dans cet exemple, spécifiez 1 période consécutive de 5 Minutes.

   g. Amazon crée CloudWatch automatiquement un nom d'alarme pour vous. Pour modifier le nom, saisissez un nouveau nom dans Alarm name (Nom de l'alarme). Les noms des alarmes ne doivent contenir que ASCII des caractères.

      > **Note**
      >
      > Vous pouvez régler la configuration de l'alarme en fonction de vos propres besoins avant de créer l'alarme, ou pouvez la modifier ultérieurement. Les paramètres de configuration incluent ceux de métrique, de seuil, de durée, d'action et de notification. Cependant, après avoir créé une alarme, vous ne pourrez pas modifier son nom par la suite.

   h. Sélectionnez Create (Créer).

Ajouter des actions de résiliation aux CloudWatch alarmes Amazon

Vous pouvez créer une alarme qui met automatiquement fin à une EC2 instance lorsqu'un certain seuil est atteint (tant que la protection contre la résiliation n'est pas activée pour l'instance). Par exemple, il se peut que vous vouliez finir une instance quand elle a terminé son travail et que vous n'avez pas besoin de l'instance à nouveau. Si vous souhaitez utiliser l'instance par la suite, vous devez arrêter l'instance, et non y mettre fin. Les données stockées sur des volumes de stockage d'instance sont perdues lorsque l'instance est résiliée. Pour plus d'informations sur l'activation et la désactivation de la protection contre la résiliation pour une instance, consultez Activer la protection de la résiliation.

Pour créer une alarme afin de mettre fin à une instance inactive (EC2console Amazon)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance et choisissez Actions, Surveiller et dépanner, Gérer les CloudWatch alarmes.

   Vous pouvez également sélectionner le signe plus (

) dans la colonne Alarm status (Statut de l'alarme) .
4. Sur la page Gérer les CloudWatch alarmes, procédez comme suit :

   a. Sélectionnez Create an alarm (Créer une alarme).

   b. Pour recevoir un e-mail lorsque l'alarme est déclenchée, pour la notification d'alarme, choisissez un SNS sujet Amazon existant. Vous devez d'abord créer un SNS sujet Amazon à l'aide de la SNS console Amazon. Pour plus d'informations, consultez la section Utilisation d'Amazon SNS pour la messagerie application-to-person (A2P) dans le manuel du développeur Amazon Simple Notification Service.

   c. Activer l'option Alarm action (Action d'alarme), puis sélectionnez Terminate (Résilier).

   d. Pour Group samples by (Regrouper les échantillons par) et Type of data to sample (Type de données à échantillonner), sélectionnez une statistique et une métrique. Dans cet exemple, sélectionnez Moyenne et CPUutilisation.

   e. Pour Alarm When (Alarme Quand) et Percent (Pourcentage), spécifiez le seuil de la métrique. Dans cet exemple, spécifiez => et 10 pour cent.

f. Pour Consecutive period (Période consécutive) et Period (Période), spécifiez la période d'évaluation de l'alarme. Dans cet exemple, spécifiez 24 périodes consécutives de 1 heure.

g. Amazon crée CloudWatch automatiquement un nom d'alarme pour vous. Pour modifier le nom, saisissez un nouveau nom dans Alarm name (Nom de l'alarme). Les noms des alarmes ne doivent contenir que ASCII des caractères.

> **Note**
>
> Vous pouvez régler la configuration de l'alarme en fonction de vos propres besoins avant de créer l'alarme, ou pouvez la modifier ultérieurement. Les paramètres de configuration incluent ceux de métrique, de seuil, de durée, d'action et de notification. Cependant, après avoir créé une alarme, vous ne pourrez pas modifier son nom par la suite.

h. Sélectionnez Create (Créer).

Ajouter des actions de redémarrage aux CloudWatch alarmes Amazon

Vous pouvez créer une CloudWatch alarme Amazon qui surveille une EC2 instance Amazon et la redémarre automatiquement. L'action d'alarme de redémarrage est recommandée pour les défaillances de vérification de l'état d'instance (par opposition à l'action d'alarme de récupération, qui convient aux défaillances de la vérification de l'état du système). Le redémarrage d'une instance est similaire à celui d'un système d'exploitation. Dans la plupart des cas, il suffit de quelques minutes pour redémarrer votre instance. Lorsque vous redémarrez une instance, celle-ci reste sur le même hôte physique, de sorte que votre instance conserve son DNS nom public, son adresse IP privée et toutes les données présentes sur ses volumes de stockage d'instance.

Le redémarrage d'une instance ne déclenche pas de nouvelle période de facturation d'instance (avec frais d'une minute minimum), contrairement à l'arrêt, puis au redémarrage d'une instance. Les données des volumes de stockage d'instances sont conservées lorsque l'instance est redémarrée. Les volumes de stockage d'instances doivent être remontés dans le système de fichiers après un redémarrage. Pour de plus amples informations, veuillez consulter Redémarrer votre instance.

> **Important**
>
> Pour prévenir toute condition de concurrence entre les actions de redémarrage et de récupération, évitez de définir le même nombre de périodes d'évaluation pour une alarme

de redémarrage et une alarme de récupération. Nous vous recommandons de définir des alarmes de redémarrage sur trois périodes d'évaluation d'une minute chacune. Pour plus d'informations, consultez la section Évaluation d'une alarme dans le guide de CloudWatch l'utilisateur Amazon.

Pour créer une alarme afin de redémarrer une instance (EC2console Amazon)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance et choisissez Actions, Surveiller et dépanner, Gérer les CloudWatch alarmes.

   Vous pouvez également sélectionner le signe plus (

) dans la colonne Alarm status (Statut de l'alarme) .
4. Sur la page Gérer les CloudWatch alarmes, procédez comme suit :

   a. Sélectionnez Create an alarm (Créer une alarme).
   b. Pour recevoir un e-mail lorsque l'alarme est déclenchée, pour la notification d'alarme, choisissez un SNS sujet Amazon existant. Vous devez d'abord créer un SNS sujet Amazon à l'aide de la SNS console Amazon. Pour plus d'informations, consultez la section Utilisation d'Amazon SNS pour la messagerie application-to-person (A2P) dans le manuel du développeur Amazon Simple Notification Service.
   c. Activer l'option Alarm action (Action d'alarme), puis sélectionnez Reboot (Redémarrer).
   d. Pour Group samples by (Regrouper les échantillons par) et Type of data to sample (Type de données à échantillonner), sélectionnez une statistique et une métrique. Dans cet exemple, sélectionnez Average (Moyenne) et Status check failed: instance (Échec du contrôle de statut : instance).
   e. Pour Consecutive period (Période consécutive) et Period (Période), spécifiez la période d'évaluation de l'alarme. Dans cet exemple, entrez 3 périodes consécutives de 1 minute. Si 1 minute est désactivé, vous devez activer la surveillance détaillée, ou vous pouvez choisir 5 minutes à la place.
   f. Amazon crée CloudWatch automatiquement un nom d'alarme pour vous. Pour modifier le nom, saisissez un nouveau nom dans Alarm name (Nom de l'alarme). Les noms des alarmes ne doivent contenir que ASCII des caractères.

g. Sélectionnez Create (Créer).

Ajouter des actions de restauration aux CloudWatch alarmes Amazon

Vous pouvez créer une CloudWatch alarme Amazon qui surveille une EC2 instance Amazon. Si l'instance est altérée en raison d'une défaillance matérielle sous-jacente ou d'un problème nécessitant une AWS intervention pour être réparée, vous pouvez la récupérer automatiquement. Les instances mises hors service ne peuvent pas être récupérées. Une instance récupérée est identique à l'instance d'origine, y compris pour l'ID d'instance, les adresses IP privées, les adresses IP Elastic et toutes les métadonnées de l'instance.

CloudWatch vous empêche d'ajouter une action de restauration à une alarme qui se trouve sur une instance qui ne prend pas en charge les actions de restauration.

Lorsque l'`StatusCheckFailed_System`alarme est déclenchée et que l'action de restauration est lancée, vous êtes averti par le SNS sujet Amazon que vous avez choisi lorsque vous avez créé l'alarme et associé l'action de restauration. Lors de la récupération d'instance, l'instance est migrée pendant un redémarrage d'instance, et toutes les données en mémoire sont perdues. Lorsque le processus est terminé, les informations sont publiées dans la SNS rubrique que vous avez configurée pour l'alarme. Toute personne abonnée à cette SNS rubrique reçoit une notification par e-mail indiquant l'état de la tentative de restauration et toute autre instruction. Vous remarquez un redémarrage d'instance sur l'instance récupérée.

> **Note**
>
> L'action de récupération ne peut être utilisée qu'avec `StatusCheckFailed_System`, pas avec `StatusCheckFailed_Instance`.

Les problèmes suivants peuvent entraîner l'échec des contrôles de statut de système :

- Perte de connectivité réseau
- Perte d'alimentation système
- Problèmes logiciels sur un hôte physique
- Problèmes matériels sur un hôte physique ayant un impact sur l'accessibilité du réseau

L'opération de récupération est prise en charge uniquement sur les instances présentant certaines caractéristiques. Pour de plus amples informations, veuillez consulter Résilience des instances.

Si votre instance a une adresse IP publique, elle la conserve après la récupération.

> **Important**
>
> Pour prévenir toute condition de concurrence entre les actions de redémarrage et de récupération, évitez de définir le même nombre de périodes d'évaluation pour une alarme de redémarrage et une alarme de récupération. Nous vous recommandons de définir des alarmes de récupération sur deux périodes d'évaluation d'une minute chacune. Pour plus d'informations, consultez la section Évaluation d'une alarme dans le guide de CloudWatch l'utilisateur Amazon.

Pour créer une alarme afin de récupérer une instance (EC2console Amazon)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance et choisissez Actions, Surveiller et dépanner, Gérer les CloudWatch alarmes.

   Vous pouvez également sélectionner le signe plus (

) dans la colonne Alarm status (Statut de l'alarme) .
4. Sur la page Gérer les CloudWatch alarmes, procédez comme suit :

   a. Sélectionnez Create an alarm (Créer une alarme).

   b. Pour recevoir un e-mail lorsque l'alarme est déclenchée, pour la notification d'alarme, choisissez un SNS sujet Amazon existant. Vous devez d'abord créer un SNS sujet Amazon à l'aide de la SNS console Amazon. Pour plus d'informations, consultez la section Utilisation d'Amazon SNS pour la messagerie application-to-person (A2P) dans le manuel du développeur Amazon Simple Notification Service.

   > **Note**
   >
   > Les utilisateurs doivent s'abonner à la SNS rubrique spécifiée pour recevoir des notifications par e-mail lorsque l'alarme est déclenchée. Il reçoit Utilisateur racine

d'un compte AWS toujours des notifications par e-mail lorsque des actions de restauration automatique d'instance se produisent, même si aucun SNS sujet n'est spécifié ou si l'utilisateur root n'est pas abonné au SNS sujet spécifié.

c. Activer l'option Alarm action (Action d'alarme), puis sélectionnez Recover (Récupérer).

d. Pour Group samples by (Regrouper les échantillons par) et Type of data to sample (Type de données à échantillonner), sélectionnez une statistique et une métrique. Dans cet exemple, sélectionnez Average (Moyenne) et Status check failed: system (Échec du contrôle de statut : système).

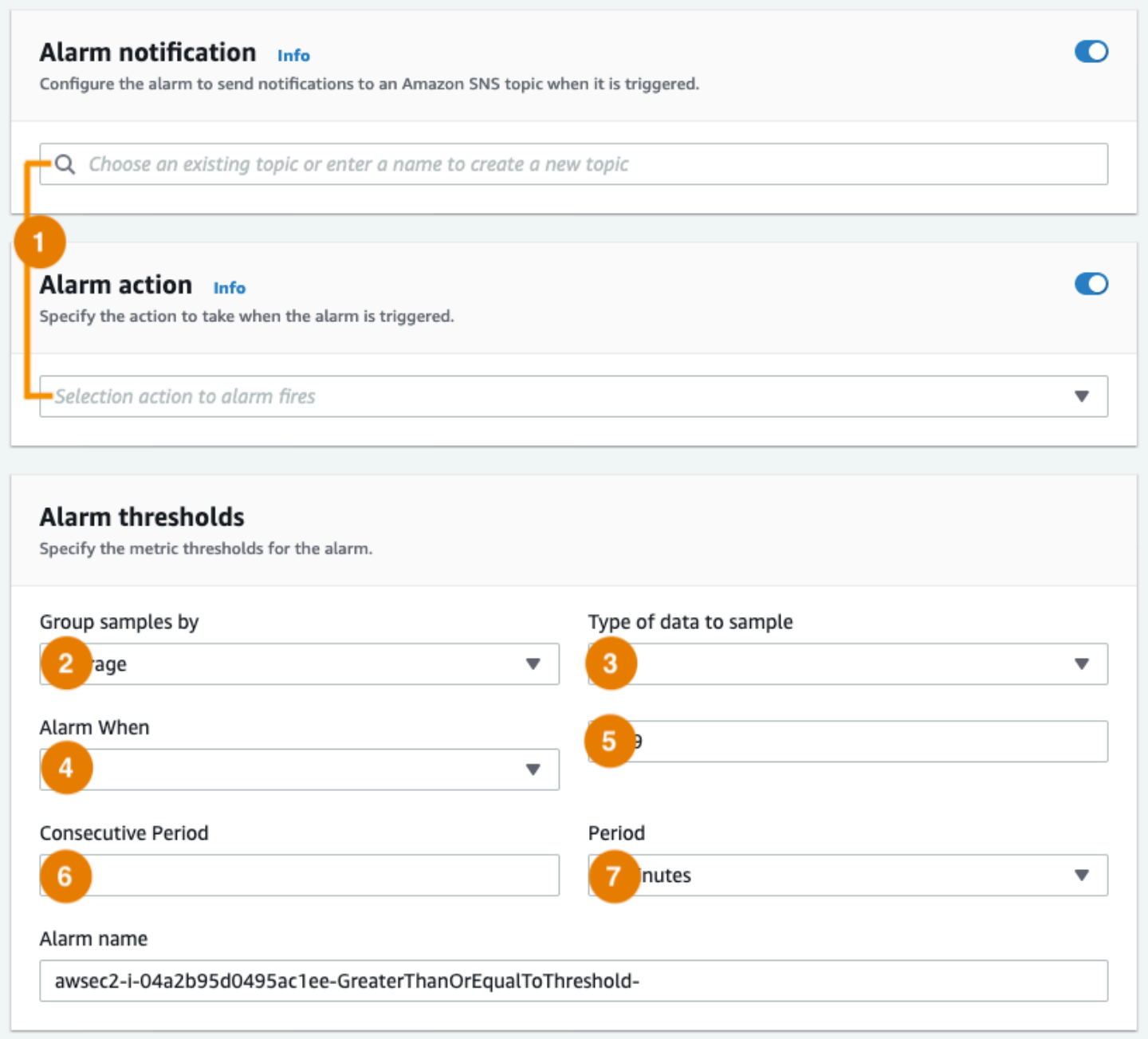
e. Pour Consecutive period (Période consécutive) et Period (Période), spécifiez la période d'évaluation de l'alarme. Dans cet exemple, entrez 2 périodes consécutives de 1 minute. Si 1 minute est désactivé, vous devez activer la surveillance détaillée, ou vous pouvez choisir 5 minutes à la place.

f. Amazon crée CloudWatch automatiquement un nom d'alarme pour vous. Pour modifier le nom, saisissez un nouveau nom dans Alarm name (Nom de l'alarme). Les noms des alarmes ne doivent contenir que ASCII des caractères.

g. Sélectionnez Create (Créer).

Scénarios CloudWatch d'action d'alarme Amazon

Vous pouvez utiliser la EC2 console Amazon pour créer des actions d'alarme qui arrêtent ou mettent fin à une EC2 instance Amazon lorsque certaines conditions sont remplies. Dans la capture d'écran suivante de la page de la console où vous avez défini les actions d'alarme, nous avons numéroté les paramètres. Nous avons également numéroté les paramètres des scénarios qui suivent afin de vous aider à créer les actions appropriées.



Scénario 1 : arrêter le développement inactif et tester les instances

Créez une alarme qui arrête une instance utilisée pour le développement ou le test de logiciels quand elle a été inactive pendant au moins une heure.

Paramètre	Value
1	Arrêter

Paramètre	Value
2	Maximum
3	CPUUtilisation
4	<=
5	10 %
6	1
7	1 heure

Scénario 2 : arrêter les instances inactives

Créez une alarme qui arrête une instance et envoie un courrier électronique quand l'instance est inactive depuis 24 heures.

Paramètre	Value
1	Arrêter et envoyer un e-mail
2	Moyenne
3	CPUUtilisation
4	<=
5	5 %
6	24
7	1 heure

Scénario 3 : envoyer un e-mail relatif aux serveurs Web ayant un trafic inhabituellement élevé

Créez une alarme qui envoie un courrier électronique quand une instance dépasse 10 Go de trafic réseau sortant par jour.

Paramètre	Value
1	E-mail
2	Somme
3	Réseau sortant
4	>
5	10 Go
6	24
7	1 heure

Scénario 4 : arrêter les serveurs Web avec un trafic inhabituellement élevé

Créez une alarme qui arrête une instance et envoyez un message texte (SMS) si le trafic sortant dépasse 1 Go par heure.

Paramètre	Value
1	Arrêtez et envoyez SMS
2	Somme
3	Réseau sortant
4	>
5	1 Go
6	1
7	1 heure

Scénario 5 : arrêter une instance déficiente

Créez une alarme qui arrête une instance après qu'elle a échoué à trois contrôles de statut consécutifs (exécutés à 5 minutes d'intervalle).

Paramètre	Value
1	Arrêter
2	Moyenne
3	Échec du contrôle de du statut : Système
4	-
5	-
6	1
7	15 minutes

Scénario 6 : résilier les instances quand les tâches de traitement par batch sont terminés

Créez une alarme qui finit une instance exécutant des traitements par batch quand elle n'envoie plus de données de résultat.

Paramètre	Value
1	Terminer
2	Maximum
3	Réseau sortant
4	<=
5	100,000 bytes
6	1

Paramètre	Value
7	5 minutes

Automatisez Amazon EC2 en utilisant EventBridge

Vous pouvez utiliser Amazon EventBridge pour automatiser services AWS et répondre automatiquement aux événements du système, tels que les problèmes de disponibilité des applications ou les modifications des ressources. Les événements AWS liés aux services sont diffusés EventBridge en temps quasi réel. Vous pouvez créer des règles pour indiquer quels événements vous intéressent et les actions à effectuer quand un événement correspond à une règle. Les actions pouvant être déclenchées automatiquement sont les suivantes :

- Invoquer une AWS Lambda fonction
- Appelez la commande Amazon EC2 Run
- Relayer l'événement à Amazon Kinesis Data Streams
- Activer une machine à AWS Step Functions états
- Notifier un SNS sujet Amazon
- Notifier une SQS file d'attente Amazon

Voici des exemples d'utilisation que vous pouvez utiliser EventBridge avec Amazon EC2 :

- Activer une fonction Lambda chaque fois qu'une instance entre dans l'état d'exécution.
- Notifier un SNS sujet Amazon lorsqu'un EBS volume Amazon est créé ou modifié.
- Envoyez une commande à une ou plusieurs EC2 instances Amazon à l'aide d'Amazon EC2 Run Command chaque fois qu'un certain événement se produit dans un autre AWS service.

Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.

Types d'EC2événements Amazon

Amazon EC2 prend en charge les types d'événements suivants :

- EC2AMIChangement d'état
- EC2Notification de changement d'état de lancement rapide

- EC2Erreur de flotte
- EC2Informations sur la flotte
- EC2Changement d'instance de flotte
- EC2Demande de modification de l'instance Fleet Spot
- EC2Modification de l'état de la flotte
- EC2Recommandation de rééquilibrage des instances
- EC2Notification de changement d'état de l'instance
- EC2Repérez une erreur de flotte
- EC2Informations sur la flotte Spot
- EC2Changement d'instance de Spot Fleet
- EC2Modification de la demande d'instance Spot Fleet Spot
- EC2Changement d'état du parc de véhicules Spot
- EC2Avertissement d'interruption d'une instance ponctuelle
- EC2Traitement des demandes d'instance Spot
- EC2ODCRNotification de sous-utilisation

Pour plus d'informations sur les types d'événements pris en charge par AmazonEBS, consultez Amazon EventBridge pour Amazon EBS.

Enregistrez les EC2 API appels Amazon en utilisant AWS CloudTrail

Amazon EC2 API est intégré à AWS CloudTrailun service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un service AWS. CloudTrail capture tous les EC2 API appels Amazon sous forme d'événements. Les appels capturés incluent les appels passés par la console. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Amazon EC2API, l'adresse IP à partir de laquelle la demande a été faite et la date à laquelle elle a été faite.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou d'utilisateur root.

- Si la demande a été faite au nom d'un utilisateur de IAM l'Identity Center.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre service AWS.

CloudTrail est actif dans votre compte Compte AWS lorsque vous créez le compte et vous avez automatiquement accès à l'historique des CloudTrail événements. L'historique des CloudTrail événements fournit un enregistrement consultable, consultable, téléchargeable et immuable des 90 derniers jours des événements de gestion enregistrés dans un. Région AWS Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur. La consultation de CloudTrail l'historique des événements est gratuite.

Pour un enregistrement continu des événements de vos 90 Compte AWS derniers jours, créez un magasin de données sur les événements de Trail ou CloudTrailLake.

CloudTrail sentiers

Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Tous les sentiers créés à l'aide du AWS Management Console sont multirégionaux. Vous pouvez créer un parcours à région unique ou multirégionale à l'aide du. AWS CLI Il est recommandé de créer un parcours multirégional, car vous capturez l'activité dans l'ensemble Régions AWS de votre compte. Si vous créez un parcours à région unique, vous ne pouvez voir que les événements enregistrés dans le parcours. Région AWS Pour plus d'informations sur les sentiers, consultez les sections Création d'un sentier pour votre organisation Compte AWS et Création d'un sentier pour une organisation dans le guide de AWS CloudTrail l'utilisateur.

Vous pouvez envoyer une copie de vos événements de gestion en cours dans votre compartiment Amazon S3 gratuitement CloudTrail en créant un journal. Toutefois, des frais de stockage Amazon S3 sont facturés. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification. Pour obtenir des informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

CloudTrail Stockages de données sur les événements du lac

CloudTrail Lake vous permet d'exécuter SQL des requêtes basées sur vos événements. CloudTrail Lake convertit les événements existants au JSON format basé sur les lignes au ORC format Apache. ORCest un format de stockage en colonnes optimisé pour une extraction rapide des données. Les événements sont agrégés dans des magasins de données d'événement.

Ceux-ci constituent des collections immuables d'événements basées sur des critères que vous sélectionnez en appliquant des sélecteurs d'événements avancés. Les sélecteurs que vous appliquez à un magasin de données d'événement contrôlent les événements qui persistent et que vous pouvez interroger. Pour plus d'informations sur CloudTrail Lake, consultez la section Travailler avec AWS CloudTrail Lake dans le guide de AWS CloudTrail l'utilisateur.

CloudTrail Les stockages et requêtes de données sur les événements de Lake entraînent des coûts. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Événements EC2 API de gestion Amazon dans CloudTrail

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre Compte AWS. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, CloudTrail enregistre les événements de gestion.

Toutes les EC2 API actions Amazon sont enregistrées en tant qu'événements de gestion. Pour obtenir la liste des API actions auxquelles vous êtes connecté CloudTrail, consultez le Amazon EC2 API Reference. Par exemple, les appels au RunInstancesDescribeInstances, et les StopInstancesactions sont enregistrés en tant qu'événements de gestion.

Exemples d'EC2APIévénements Amazon

Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'APIopération demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des API appels publics, de sorte que les événements n'apparaissent pas dans un ordre spécifique.

L'enregistrement de fichier journal suivant montre qu'un utilisateur a résilié une instance.


```
{
   "Records":[
      {
         "eventVersion":"1.03",
         "userIdentity":{
            "type":"Root",
            "principalId":"123456789012",
```

```
            "arn":"arn:aws:iam::123456789012:root",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"user"
         },
         "eventTime":"2016-05-20T08:27:45Z",
         "eventSource":"ec2.amazonaws.com",
         "eventName":"TerminateInstances",
         "awsRegion":"us-west-2",
         "sourceIPAddress":"198.51.100.1",
         "userAgent":"aws-cli/1.10.10 Python/2.7.9 Windows/7botocore/1.4.1",
         "requestParameters":{
            "instancesSet":{
               "items":[{
                  "instanceId":"i-1a2b3c4d"
               }]
            }
         },
         "responseElements":{
            "instancesSet":{
               "items":[{
                  "instanceId":"i-1a2b3c4d",
                  "currentState":{
                     "code":32,
                     "name":"shutting-down"
                  },
                  "previousState":{
                     "code":16,
                     "name":"running"
                  }
               }]
            }
         },
         "requestID":"be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
         "eventID":"6e12345-2a4e-417c-aa78-7594fEXAMPLE",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```


Pour plus d'informations sur le contenu des CloudTrail enregistrements, voir le contenu des CloudTrail enregistrements dans le Guide de AWS CloudTrail l'utilisateur.

Audit des connexions établies à l'aide d'EC2Instance Connect

Vous pouvez l'utiliser AWS CloudTrail pour auditer les utilisateurs qui se connectent à vos instances à l'aide d'EC2Instance Connect.

Pour auditer SSH l'activité via EC2 Instance Connect à l'aide de la AWS CloudTrail console

1. Ouvrez la CloudTrail console à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Vérifiez que vous êtes dans la région correcte.
3. Dans le volet de navigation, sélectionnez Event history (Historique des événements).
4. Pour Filter (Filtre), choisissez Event source (Source de l'événement), ec2-instance-connect.amazonaws.com.
5. (Facultatif) Pour Time range (Plage de temps), sélectionnez une plage de temps.
6. Choisissez l'icône Refresh events (Actualiser les événements).
7. La page affiche les événements correspondant aux SendSSHPublicKeyAPIappels. Développez un événement à l'aide de la flèche pour afficher des détails supplémentaires, tels que le nom d'utilisateur et la clé d' AWS accès utilisés pour établir la SSH connexion, ainsi que l'adresse IP source.
8. Pour afficher les informations complètes de l'événement sous forme de JSON format, choisissez Afficher l'événement. Le requestParameterschamp contient l'ID de l'instance de destination, le nom d'utilisateur du système d'exploitation et la clé publique utilisés pour établir la SSH connexion.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
        "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
        "accountId": "123456789012",
        "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
        "userName": "IAM-friendly-name",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-09-21T21:37:58Z"}
        }
    },
```

```
    "eventTime": "2018-09-21T21:38:00Z",
    "eventSource": "ec2-instance-connect.amazonaws.com",
    "eventName": "SendSSHPublicKey ",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "123.456.789.012",
    "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
    "requestParameters": {
        "instanceId": "i-0123456789EXAMPLE",
        "osUser": "ec2-user",
        "SSHKey": {
            "publicKey": "ssh-rsa ABCDEFGHIJKLMNO01234567890EXAMPLE"
        }
     },
    "responseElements": null,
    "requestID": "1a2s3d4f-bde6-11e8-a892-f7ec64543add",
    "eventID": "1a2w3d4r5-a88f-4e28-b3bf-30161f75be34",
    "eventType": "AwsApiCall",
    "recipientAccountId": "0987654321"
}
```


Si vous avez configuré votre AWS compte pour collecter des CloudTrail événements dans un compartiment S3, vous pouvez télécharger et auditer les informations par programmation. Pour plus d'informations, consultez la section Obtenir et consulter vos fichiers CloudTrail journaux dans le guide de AWS CloudTrail l'utilisateur.

Moniteur. NETet applications SQL de serveur utilisant CloudWatch Application Insights

CloudWatch Application Insights vous aide à surveiller votre. NETet des applications de SQL serveur qui utilisent EC2 des instances Amazon ainsi que d'autres ressources AWS applicatives. Il identifie et configure les indicateurs clés, les journaux et les alarmes pour l'ensemble des ressources de votre application et de votre infrastructure technologique (par exemple, votre base de données Microsoft SQL Server, vos serveurs Web (IIS) et d'applications, votre système d'exploitation, vos équilibreurs de charge et vos files d'attente). Elle surveille en permanence les métriques et les journaux afin de détecter et de corréler les anomalies et les erreurs. Lorsque des erreurs et des anomalies sont détectées, Application Insights génère CloudWatch des événements que vous pouvez utiliser pour configurer des notifications ou prendre des mesures. Pour faciliter le dépannage, elle crée des tableaux de bord automatisés qui retracent les problèmes détectés, les anomalies métriques, les erreurs de journalisation corrélées, ainsi que des informations supplémentaires vous indiquant la

cause potentielle. Les tableaux de bord automatisés vous aident à prendre rapidement des mesures correctives pour vous assurer que vos applications sont saines et que les utilisateurs finaux ne sont pas affectés.

Pour consulter la liste complète des journaux et mesures pris en charge, consultez la section Journaux et mesures pris en charge par Amazon CloudWatch Application Insights.

Informations fournies sur les problèmes détectés

- Un bref résumé du problème
- La date et l'heure de début du problème
- La gravité du problème : High/Medium/Low (Haute/Moyenne/Basse)
- Le statut du problème détecté : In-progress/Resolved (En cours/Résolu)
- Analyses : génération automatique d'analyses concernant le problème détecté et sa possible cause
- Commentaires sur les informations : commentaires que vous avez fournis sur l'utilité des informations générées par CloudWatch Application Insights for. NETet SQL serveur
- Observations connexes : une vue détaillée des anomalies métriques et des extraits pertinents de journaux d'erreurs liés au problème, parmi différents composants d'application

Commentaires

Vous pouvez fournir des commentaires sur les analyses générées automatiquement relatives aux problèmes détectés en les qualifiant d'utiles ou d'inutiles. Les commentaires que vous laissez sur les analyses, ainsi que vos diagnostics d'application (anomalies métriques et exceptions de journaux) sont utilisés pour améliorer les futures détections de problèmes similaires.

Pour plus d'informations, consultez la documentation CloudWatchApplication Insights dans le guide de CloudWatch l'utilisateur Amazon.

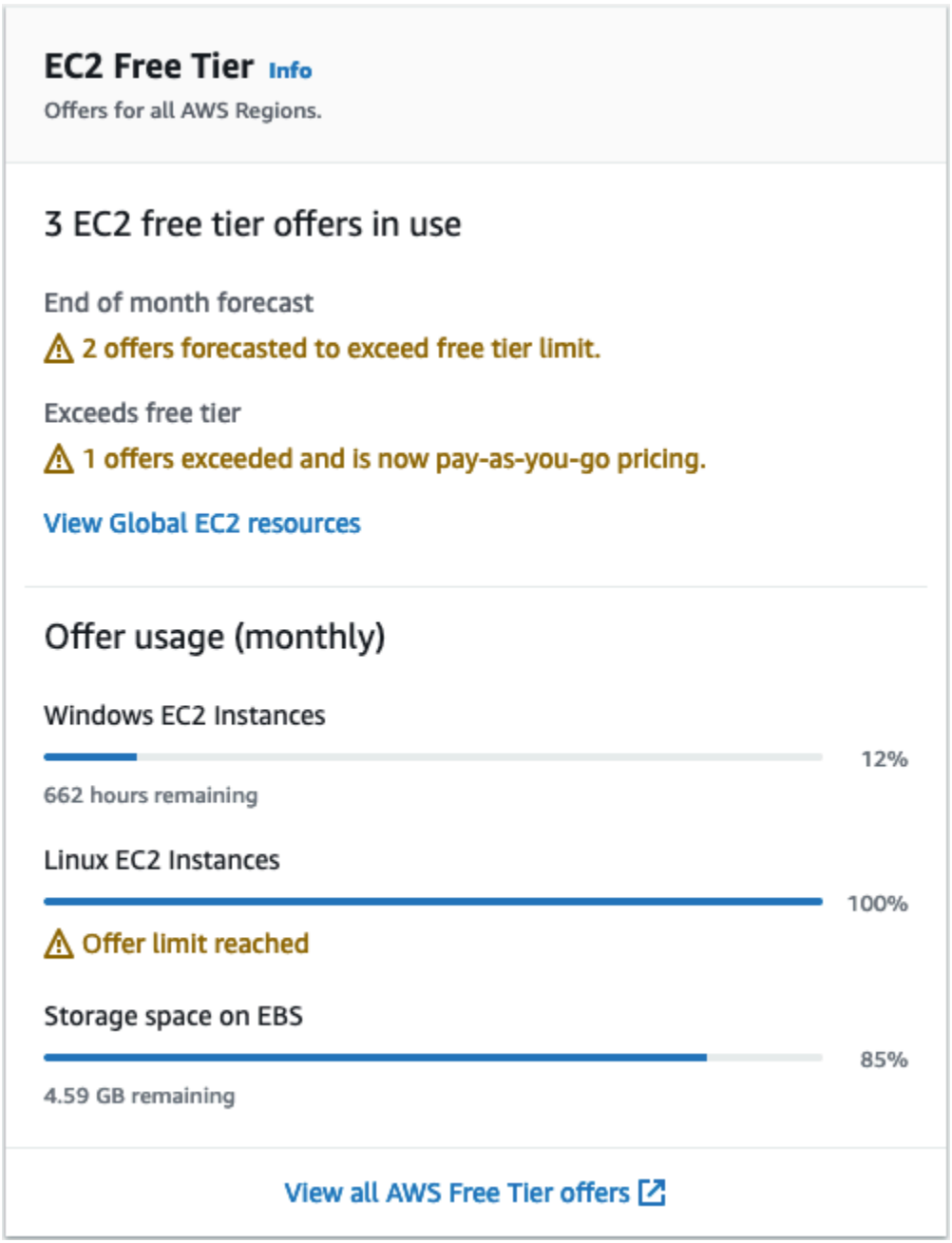
Suivez votre utilisation du niveau gratuit pour Amazon EC2

Vous pouvez utiliser Amazon EC2 sans frais si vous êtes AWS client depuis moins de 12 mois et si vous respectez les limites Niveau gratuit d'AWS d'utilisation. Il est important de suivre votre utilisation de l'offre gratuite pour éviter les surprises liées à la facturation. Si vous dépassez les limites du niveau gratuit, vous devrez payer des pay-as-go frais standard. Pour de plus amples informations, veuillez consulter Niveau gratuit d'AWS.

> **Note**
>
> Si vous êtes AWS client depuis plus de 12 mois, vous n'êtes plus éligible à l'utilisation du niveau gratuit et vous ne verrez pas la case correspondant à l'offre EC2gratuite décrite dans la procédure suivante.

Pour suivre votre utilisation de l'offre gratuite

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez EC2Dashboard.
3. Trouvez la case EC2Free Tier (en haut à droite).



4. Dans la case EC2Free Tier, vérifiez votre utilisation du Free Tier, comme suit :

   - Dans le cadre des offres de niveau EC2 gratuit en cours d'utilisation, prenez note des avertissements suivants :
     - Prévisions de fin de mois : vous avertit que des frais vous seront facturés ce mois si vous continuez avec votre modèle d'utilisation actuel.
     - Dépasse l'offre gratuite : indique que vous avez dépassé les limites de l'offre gratuite et que vous avez déjà engagé des frais.

- Sous Utilisation de l'offre (mensuelle), notez votre utilisation des instances Linux, des instances Windows et du EBS stockage. Le pourcentage indique la part des limites de l'offre gratuite que vous avez utilisée ce mois-ci. Si vous êtes à 100 %, des frais vous seront facturés pour toute utilisation ultérieure.

> **Note**
>
> Ces informations apparaissent uniquement une fois que vous avez créé une instance. Toutefois, les informations relatives à l'utilisation ne sont pas mises à jour en temps réel, mais trois fois par jour.

5. Pour éviter d'encourir des frais supplémentaires, supprimez toutes les ressources qui sont actuellement facturées ou qui le seront si vous dépassez la limite d'utilisation de votre offre gratuite.

   - Pour obtenir les instructions relatives à la suppression de votre instance, consultezMettre fin aux EC2 instances Amazon.
   - Pour vérifier si vous avez des ressources dans d'autres régions susceptibles d'être facturées, dans la case Niveau EC2 gratuit, choisissez Afficher les EC2 ressources mondiales pour ouvrir la vue EC2globale. Pour de plus amples informations, veuillez consulter Afficher les ressources de différentes régions à l'aide d'Amazon EC2 Global View.

6. Pour voir l'utilisation de vos ressources pour tous services AWS dans le champ « Free Tier » Niveau gratuit d'AWS, en bas de la case EC2Free Tier, sélectionnez Afficher toutes les Niveau gratuit d'AWS offres. Pour plus d'informations, consultez Utilisation de la Niveau gratuit d'AWS dans le Guide de l'utilisateur de la facturation AWS .

Résoudre les problèmes liés aux instances Amazon EC2

Les procédures et conseils suivants peuvent vous aider à résoudre les problèmes liés à vos EC2 instances Amazon.

Problèmes

- Résoudre les problèmes de lancement des EC2 instances Amazon
- Résoudre les problèmes d'arrêt des EC2 instances Amazon
- Résoudre les problèmes de résiliation d'EC2une instance Amazon
- Résoudre les problèmes liés à une instance Amazon inaccessible EC2
- Résoudre les problèmes de connexion à votre instance Amazon EC2 Linux
- Résoudre les problèmes des instances Amazon EC2 Linux dont les vérifications d'état ont échoué
- Résoudre les problèmes liés au démarrage d'une instance Amazon EC2 Linux à partir du mauvais volume
- Résoudre les problèmes de connexion à votre instance Amazon EC2 Windows
- Résoudre les problèmes de démarrage des instances Amazon EC2 Windows
- Résoudre les problèmes liés aux instances Amazon EC2 Windows
- Réinitialisation du mot de passe administrateur Windows pour une instance Amazon EC2 Windows
- Résoudre les problèmes liés à Sysprep avec les instances Amazon Windows EC2
- Résolvez les problèmes liés à une instance Amazon EC2 Linux défectueuse à l'aide de EC2Rescue
- Résoudre les problèmes liés à une instance Amazon EC2 Windows défectueuse à l'aide de EC2Rescue
- EC2Console série pour instances
- Envoyer une interruption de diagnostic pour déboguer une instance Amazon inaccessible EC2

Résoudre les problèmes de lancement des EC2 instances Amazon

Vous trouverez ci-dessous des conseils de dépannage qui vous aideront à résoudre les problèmes lors du lancement d'une EC2 instance Amazon.

Problèmes de lancement

Nom de périphérique non valide

Description

Vous obtenez l'erreur `Invalid device name` *`device_name`* lorsque vous essayez de lancer une nouvelle instance.

Cause

Si vous obtenez cette erreur lorsque vous essayez de lancer une instance, le nom de périphérique spécifié pour un ou plusieurs volumes dans la demande comporte un nom de périphérique non valide. Les causes possibles incluent :

- Le nom de l'appareil est peut-être utilisé par la personne sélectionnéeAMI.
- Le nom de périphérique peut être réservé aux volumes racine.
- Le nom de périphérique peut être utilisé pour un autre volume dans la demande.
- Le nom de périphérique peut ne pas être valide pour le système d'exploitation.

Solution

Pour résoudre le problème :

- Assurez-vous que le nom de l'appareil n'est pas utilisé dans celui AMI que vous avez sélectionné. Exécutez la commande suivante pour afficher les noms de périphériques utilisés parAMI.

```
aws ec2 describe-images --image-id ami_id --query
 'Images[*].BlockDeviceMappings[].DeviceName'
```

- Assurez-vous que vous n'utilisez pas un nom de périphérique qui est réservé aux volumes racine. Pour de plus amples informations, veuillez consulter Noms d'appareil disponibles.
- Assurez-vous que chaque volume spécifié dans votre demande possède un nom de périphérique unique.
- Assurez-vous que les noms de périphériques que vous avez spécifiés sont au format correct. Pour de plus amples informations, veuillez consulter Noms d'appareil disponibles.

Dépassement de la limite d'instance

Description

Vous obtenez l'erreur `InstanceLimitExceeded` lorsque vous essayez de lancer une nouvelle instance ou de redémarrer une instance arrêtée.

Cause

Si vous obtenez une erreur `InstanceLimitExceeded` lorsque vous essayez de lancer une nouvelle instance ou de redémarrer une instance arrêté, vous avez atteint la limite du nombre d'instances que vous pouvez lancer dans une région. Lorsque vous créez votre AWS compte, nous fixons des limites par défaut quant au nombre d'instances que vous pouvez exécuter par région.

Solution

Vous pouvez demander une augmentation de la limite d'instance par région. Pour de plus amples informations, veuillez consulter Quotas EC2 de service Amazon.

Capacité d'instance insuffisante

Description

Vous obtenez l'erreur `InsufficientInstanceCapacity` lorsque vous essayez de lancer une nouvelle instance ou de redémarrer une instance arrêtée.

Cause

Si vous obtenez cette erreur lorsque vous essayez de lancer une instance ou de redémarrer une instance arrêtée, AWS n'a actuellement pas assez de capacité à la demande disponible pour répondre à votre demande.

Solution

Pour résoudre ce problème, essayez ce qui suit :

- Attendez quelques minutes, puis renvoyez votre demande. La capacité peut changer fréquemment.
- Envoyez une nouvelle demande avec un nombre réduit d'instances. Par exemple, si vous faites une demande simple pour lancer 15 instances, essayez de faire 3 demandes pour 5 instances ou 15 demandes pour 1 instance à la place.
- Si vous lancez une instance, soumettez une nouvelle demande sans spécifier de zone de disponibilité.
- Si vous lancez une instance, envoyez une nouvelle demande en utilisant un type d'instance différent (que vous pouvez redimensionner à un stade ultérieur). Pour de plus amples informations, veuillez consulter Changements de type d'EC2instance Amazon.
- Si vous lancez des instances dans un groupe de placement du cluster, vous pouvez recevoir une erreur de capacité insuffisante.

La configuration demandée n'est actuellement pas prise en charge. Consultez la documentation pour voir les configurations prises en charge.

Description

Vous obtenez l'erreur `Unsupported` lorsque vous essayez de lancer une nouvelle instance, car la configuration de l'instance n'est pas prise en charge.

Cause

Le message d'erreur fournit des informations supplémentaires. Par exemple, un type d'instance ou une option d'achat d'instance peut ne pas être prise en charge dans la région ou la zone de disponibilité spécifiée.

Solution

Essayez une autre configuration d'instance. Pour rechercher un type d'instance qui répond à vos besoins, consultez Rechercher un type d'EC2instance Amazon.

Mise hors service immédiate de l'instance

Description

Votre instance passe de l'état `pending` à l'état `terminated`.

Cause

Voici quelques raisons qui expliquent pourquoi une instance peut se terminer immédiatement :

- Vous avez dépassé vos limites de EBS volume. Pour de plus amples informations, veuillez consulter Limites EBS de volume Amazon pour les EC2 instances Amazon.
- Un EBS instantané est endommagé.
- Le EBS volume racine est chiffré et vous n'êtes pas autorisé à accéder à la KMS clé pour le déchiffrer.
- Un instantané spécifié dans le mappage des périphériques en mode bloc pour le AMI est chiffré et vous n'êtes pas autorisé à accéder à la KMS clé pour le déchiffrer ou vous n'avez pas accès à la KMS clé pour chiffrer les volumes restaurés.
- Il manque une partie obligatoire (un fichier image.part) à l'instance sauvegardée par le stockage AMI que vous avez utilisée pour lancer l'instance. (fichier xx).

Pour de plus amples informations, veuillez récupérer le motif de résiliation à l'aide de l'une des méthodes suivantes.

Pour obtenir le motif de résiliation à l'aide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez instances, puis choisissez l'instance.
3. Dans le premier onglet, recherchez le motif en regard de State transition reason (Motif de transition de l'état).

Pour obtenir le motif du licenciement à l'aide du AWS Command Line Interface

1. Utilisez la commande describe-instances et spécifiez l'ID de l'instance.

```
aws ec2 describe-instances --instance-id instance_id
```

2. Passez en revue la JSON réponse renvoyée par la commande et notez les valeurs de l'élément de `StateReason` réponse.

   Le bloc de code suivant présente un exemple d'élément de réponse `StateReason`.

   ```
   "StateReason": {
     "Message": "Client.VolumeLimitExceeded: Volume limit exceeded",
     "Code": "Server.InternalError"
   },
   ```

Pour obtenir le motif du licenciement en utilisant AWS CloudTrail

Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements dans le Guide de AWS CloudTrail l'utilisateur.

Solution

En fonction de la cause de la résiliation, exécutez l'une des actions suivantes :

- **`Client.VolumeLimitExceeded: Volume limit exceeded`** — Supprimez les volumes inutilisés. Vous pouvez envoyer une demande d'augmentation de votre limite de volumes.
- **`Client.InternalError: Client error on launch`**— Assurez-vous que vous disposez des autorisations requises pour accéder aux volumes AWS KMS keys utilisés pour déchiffrer et chiffrer. Pour de plus amples informations, veuillez consulter Utilisation des politiques de clé AWS KMS dans le AWS Key Management Service Guide du développeur.

Autorisations insuffisantes

Description

Vous obtenez l'erreur `"errorMessage": "You are not authorized to perform this operation."` lorsque vous essayez de lancer une nouvelle instance et que le lancement échoue.

Cause

Si cette erreur s'affiche lorsque vous essayez de lancer une instance, cela signifie que vous ne disposez pas IAM des autorisations requises pour lancer l'instance.

Les autorisations manquantes possibles incluent :

- `ec2:RunInstances`
- `iam:PassRole`

D'autres autorisations peuvent également être manquantes. Pour obtenir la liste des autorisations requises pour lancer une instance, consultez les exemples de IAM politiques sous Exemple : utilisation de l'assistant de EC2 lancement d'instance etInstances de lancement (RunInstances).

Solution

Pour résoudre le problème :

- Si vous faites des demandes en tant qu'IAMutilisateur, vérifiez que vous disposez des autorisations suivantes :
  - `ec2:RunInstances` avec une ressource générique (« * »)
  - `iam:PassRole`avec la ressource correspondant au rôle ARN (par exemple,`arn:aws:iam::999999999999:role/ExampleRoleName`)
- Si vous ne disposez pas des autorisations précédentes, modifiez la IAM politique associée au IAM rôle ou à l'utilisateur pour ajouter les autorisations requises manquantes.

Si votre problème persiste et que vous recevez toujours un message d'erreur d'échec de lancement, vous pouvez décoder le message d'échec d'autorisation inclus dans l'erreur. Le message décodé inclut les autorisations absentes de la IAM politique. Pour plus d'informations, consultez Comment décoder un message d'échec d'autorisation après avoir reçu une erreur « UnauthorizedOperation » lors du lancement d'une EC2 instance ?

CPUUtilisation élevée peu après le démarrage de Windows (instances Windows uniquement)

> **Note**
>
> Ce conseil de résolution des problèmes concerne uniquement les instances Windows.

Si Windows Update est configuré sur Vérifier les mises à jour, mais que je peux choisir de les télécharger et de les installer (paramètre d'instance par défaut), cette vérification peut consommer entre 50 et 99 % du CPU temps de l'instance. Si cette CPU consommation pose des problèmes à

vos applications, vous pouvez modifier manuellement les paramètres de Windows Update dans le Panneau de configuration ou utiliser le script suivant dans le champ des données EC2 utilisateur Amazon :

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v
 AUOptions /t REG_DWORD /d 3 /f net stop wuauserv net start wuauserv
```

Lorsque vous exécutez ce script, spécifiez une valeur pour /d. La valeur par défaut est 3. Les valeurs possibles sont notamment les suivantes :

1. Ne jamais rechercher des mises à jour
2. Rechercher des mises à jour mais me laisser choisir s'il convient de les télécharger et de les installer
3. Télécharger des mises à jour mais me laisser choisir s'il convient de les installer
4. Installer les mises à jour automatiquement

Après avoir modifié les données utilisateur de votre instance, vous pouvez exécuter celle-ci. Pour plus d'informations, consultez Exécuter des commandes sur votre instance Windows au lancement.

Résoudre les problèmes d'arrêt des EC2 instances Amazon

Si vous avez arrêté votre instance basée sur Amazon EBS et qu'elle semble bloquée, il se peut qu'il y ait un problème avec l'ordinateur hôte sous-jacent. `stopping` Essayez d'abord de forcer l'arrêt de l'instance. Si l'instance ne s'arrête pas, vous pouvez demander de l'aide pour résoudre ce problème.

L'utilisation d'une instance est gratuite tant que l'instance est à l'état `stopping` ou à n'importe quel autre état, sauf `running`. L'utilisation d'une instance est payante uniquement lorsqu'elle est à l'état `running`.

Table des matières

Forcer l'arrêt d'une instance

Forcez l'arrêt de l'instance à l'aide de la console ou de l AWS CLI.

> **Note**
>
> Vous pouvez forcer une instance à cesser d'utiliser la console uniquement lorsque l'instance est dans l'état `stopping`. Vous pouvez forcer une instance à cesser d'utiliser la AWS CLI lorsque l'instance est dans n'importe quel état, sauf `shutting-down` et `terminated`.

Console

Pour forcer l'arrêt de l'instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez instances et choisissez l'instance bloquée.
3. Sélectionnez État de l'instance, Forcer l'arrêt de l'instance, Arrêter.

   Notez que Forcer l'arrêt de l'instance n'est disponible dans la console que si votre instance se trouve dans l'état `stopping`. Si votre instance est dans un autre état (sauf `shutting-down` et`terminated`), vous pouvez utiliser le AWS CLI pour forcer l'arrêt de votre instance.

AWS CLI

Pour forcer l'arrêt de l'instance à l'aide du AWS CLI

Utilisez la commande stop-instances et l'option `--force` comme suit :

```
aws ec2 stop-instances --instance-ids i-0123ab456c789d01e --force
```

Si l'instance ne s'est pas arrêtée après 10 minutes, publiez une demande d'aide sur le AWS re:Post. Pour contribuer à une résolution rapide du problème, incluez l'ID d'instance et décrivez les étapes que vous avez déjà effectuées. Sinon, si vous disposez d'un plan de support, créez une demande d'assistance technique dans le Centre de support.

(Facultatif) Créez une instance de remplacement

Pendant que vous attendez l'assistance du AWS re:PostSupport Center, vous pouvez créer une instance de remplacement si nécessaire. Créez une instance AMI à partir de l'instance bloquée et lancez une nouvelle instance en utilisant la nouvelleAMI.

> **Important**
>
> Vous pouvez créer une instance de remplacement si l'instance bloquée produit uniquement des vérifications de l'état du système, car les vérifications de l'état de l'instance entraîneront la AMI copie d'une réplique exacte du système d'exploitation défectueux. Après avoir confirmé le message d'état, créez-le AMI et lancez-en une nouvelle en utilisant le nouveauAMI.

Console

Pour créer une instance de remplacement à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez instances et choisissez l'instance bloquée.
3. Choisissez Actions, Image and templates (Image et modèles), Create image (Créer une image).
4. Sur la page Créer une image, procédez comme suit :

   a. Entrez un nom et une description pourAMI.

   b. Effacez l'instance de redémarrage.

   c. Choisissez Create image (Créer une image).

   Pour de plus amples informations, veuillez consulter the section called “Créer et à AMI partir d'une instance”.
5. Lancez une nouvelle instance depuis le AMI et vérifiez qu'elle fonctionne.
6. Sélectionnez l'instance bloquée, puis choisissez Actions, État de l'instance, Terminer (supprimer) l'instance. Si l'instance est également bloquée en cours de résiliation, Amazon l'oblige EC2 automatiquement à se terminer en quelques heures.

AWS CLI

Pour créer une instance de remplacement à l'aide du CLI

1. Créez une instance AMI à partir de l'instance bloquée à l'aide de la commande create-image (AWS CLI) et de l'`--no-reboot`option suivantes :.

```
aws ec2 create-image --instance-id i-0123ab456c789d01e --name "AMI" --
description "AMI for replacement instance" --no-reboot
```

2. Lancez une nouvelle instance à l'AMIaide de la commande run-instances (AWS CLI) comme suit :

```
aws ec2 run-instances --image-id ami-1a2b3c4d --count 1 --instance-type c3.large
 --key-name MyKeyPair --security-groups MySecurityGroup
```

3. Vérifiez que la nouvelle instance fonctionne.
4. Mettez fin à l'instance bloquée en utilisant la commande terminate-instances (AWS CLI) de la façon suivante :

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0
```

Si vous ne parvenez pas à créer une instance à AMI partir de l'instance comme décrit dans la procédure précédente, vous pouvez configurer une instance de remplacement comme suit :

(Alternative) Pour créer une instance de remplacement à l'aide de la console

1. Sélectionnez l'instance et choisissez Description, Périphériques de stockage en mode bloc. Sélectionnez chaque volume et notez leur ID de volume. Assurez-vous de noter quel volume correspond au volume racine.
2. Dans le panneau de navigation, choisissez Volumes. Sélectionnez chaque volume pour l'instance et sélectionnez Actions, Créer un instantané.
3. Dans le panneau de navigation, choisissez Snapshots. Sélectionnez l'instantané que vous venez de créer et choisissez Actions, Créer un volume.
4. Lancez une instance avec le même système d'exploitation que l'instance bloqué. Notez l'ID du volume et le nom de périphérique de son volume racine.
5. Dans le panneau de navigation, sélectionnez instances, puis l'instance que vous venez de lancer, et État de l'instance, Arrêter l'instance.
6. Dans le panneau de navigation, sélectionnez Volumes, choisissez le volume racine de l'instance arrêtée, et sélectionnez Actions, Détacher un volume.
7. Sélectionnez le volume racine que vous avez créé à partir de l'instance bloquée, puis Actions, Attacher un volume et attachez-le à la nouvelle instance comme volume racine (en utilisant

le nom de périphérique que vous avez noté). Attachez n'importe quel volume non-racine supplémentaire à l'instance.

8. Dans le panneau de navigation, sélectionnez instances et choisissez l'instance de remplacement. Choisissez État de l'instance, Démarrer l'instance. Vérifiez que l'instance fonctionne.
9. Sélectionnez l'instance bloquée, choisissez État de l'instance, Terminer (supprimer) l'instance. Si l'instance est également bloquée en cours de résiliation, Amazon l'oblige EC2 automatiquement à se terminer en quelques heures.

Résoudre les problèmes de résiliation d'EC2une instance Amazon

L'arrêt ou la suppression de votre instance s'appelle la résiliation de l'instance. Les informations suivantes peuvent vous aider à résoudre les problèmes lorsque vous mettez fin à votre instance.

Vous n'êtes pas facturé pour l'utilisation d'une instance tant que l'instance n'est pas à l'état `running`. En d'autres termes, lorsque vous mettez fin à une instance, l'instance ne vous est plus facturée dès que son état passe à `shutting-down`.

Mise hors service immédiate de l'instance

Plusieurs problèmes peuvent entraîner la résiliation immédiate de votre instance au démarrage. Pour plus d'informations, consultez Mise hors service immédiate de l'instance.

Mise à fin d'instance retardée

Si votre instance reste à l'état `shutting-down` pendant plus que quelques minutes, elle peut être retardée à cause des scripts d'arrêt exécutés par l'instance.

Un autre cause possible est un problème avec l'ordinateur hôte sous-jacent. Si votre instance reste dans `shutting-down` cet état pendant plusieurs heures, Amazon la EC2 traite comme une instance bloquée et y met fin de force.

S'il semble que votre instance soit bloquée pendant la mise à fin et que cela dure depuis plus de quelques heures, envoyez une demande d'aide à AWS re:Post. Pour aider à accélérer la résolution d'un problème, incluez l'ID d'instance et décrivez les étapes que vous avez déjà effectuées. Sinon, si vous disposez d'un plan de support, créez une demande d'assistance technique dans le Centre de support.

Instance terminée toujours affichée

Après avoir mis fin à une instance, elle reste visible pendant un court instant avant d'être supprimée. L'état indique `terminated`. Si l'entrée n'est pas supprimée après plusieurs heures, contactez le support.

Erreur : il se peut que l'instance ne soit pas résiliée. Modifier son attribut d'instance disableApiTermination « »

Si vous essayez de résilier une instance et que le message d'erreur `The instance` *`instance_id`* `may not be terminated. Modify its 'disableApiTermination' instance attribute` s'affiche, cela signifie que la protection contre la résiliation de l'instance a été activée. La protection contre la résiliation empêche la résiliation accidentelle de l'instance. Pour de plus amples informations, veuillez consulter Activer la protection de la résiliation.

Vous devez désactiver la protection contre la résiliation avant de pouvoir résilier l'instance.

Pour désactiver la protection contre la résiliation à l'aide de la EC2 console Amazon, sélectionnez l'instance, puis choisissez Actions, Paramètres de l'instance, Modifier la protection contre la résiliation.

Pour désactiver la protection contre le licenciement à l'aide de AWS CLI, utilisez la commande suivante.

```
aws ec2 modify-instance-attribute --instance-id instance_id --no-disable-api-
termination
```

instances lancées ou terminées automatiquement

En général, les comportements suivants signifient que vous avez utilisé Amazon EC2 Auto Scaling, EC2 Fleet ou Spot Fleet pour dimensionner automatiquement vos ressources informatiques en fonction de critères que vous avez définis :

- Vous mettez fin à une instance et une nouvelle instance se lance automatiquement.
- Vous lancez une instance et l'une de vos instances se termine automatiquement.
- Vous arrêtez une instance, elle se termine et une nouvelle instance se lance automatiquement.

Pour arrêter le dimensionnement automatique, recherchez le groupe Auto Scaling ou le parc qui lance les instances et définissez sa capacité sur 0 ou supprimez-le.

Résoudre les problèmes liés à une instance Amazon inaccessible EC2

Les informations suivantes peuvent vous aider à résoudre les problèmes liés aux instances Amazon EC2 inaccessibles. Vous pouvez prendre des captures d'écran ou accéder aux sorties de console pour diagnostiquer les problèmes et déterminer si vous devez redémarrer votre instance. Pour les instances Windows inaccessibles, résolvez les problèmes en consultant les captures d'écran renvoyées par le service.

Table des matières

Redémarrage d'instance

La capacité de redémarrer des instances qui sont généralement inaccessibles est précieuse pour le dépannage et la gestion générale des instances.

Tout comme vous pouvez réinitialiser un ordinateur en appuyant sur le bouton de réinitialisation, vous pouvez réinitialiser EC2 les instances à l'aide de la EC2 console AmazonCLI, ouAPI. Pour de plus amples informations, veuillez consulter Redémarrer votre instance.

Sortie de la console de l'instance

La sortie de la console est un outil de valeur pour le diagnostic des problèmes. Il est particulièrement utile pour résoudre les problèmes liés au noyau et à la configuration des services susceptibles de provoquer la fermeture d'une instance ou de la rendre inaccessible avant le démarrage de son SSH daemon.

- Instances Linux : la sortie de la console d'instance affiche exactement la sortie de console qui serait normalement affichée sur un moniteur physique connecté à un ordinateur. La sortie de la

console renvoie des informations mises en mémoire tampon qui ont été publiées après un état de transition d'instance (démarrage, arrêt, redémarrage et résiliation). La sortie publiée n'est pas continuellement mise à jour, uniquement lorsqu'elle est probablement très bénéfique.

- Instances Windows : le résultat de la console d'instance inclut les trois dernières erreurs du journal des événements du système.

Seul le propriétaire de l'instance peut accéder à la sortie de la console.

Vous pouvez récupérer les derniers résultats de la console série pendant le cycle de vie de l'instance. Cette option n'est prise en charge que sur les instances créées sur le système AWS Nitro. Il n'est pas pris en charge via la EC2 console Amazon.

Console

Pour obtenir la sortie de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation de gauche, sélectionnez Instances.
3. Sur la page Instances, sélectionnez Actions, Surveiller et dépanner, puis Obtenir le journal système.

Command line

Pour obtenir la sortie de la console

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- get-console-output (AWS CLI)
- Get-EC2ConsoleOutput (AWS Tools for Windows PowerShell)

Création d'une capture d'écran d'une instance inaccessible

Si vous ne parvenez pas à vous connecter à votre instance, vous pouvez en faire une capture d'écran et l'afficher sous forme d'image. Cette image permet de voir le statut de l'instance et de résoudre le problème plus rapidement.

Vous pouvez générer des captures d'écran pendant que l'instance s'exécute ou après son blocage. L'image est générée dans un JPG format ne dépassant pas 100 ko. Aucun coût de transfert de données n'est facturé pour la capture d'écran.

Limites

Cette fonctionnalité n'est pas prise en charge dans les cas suivants :

- Instances matériel nu (instances de type `*.metal`)
- L'instance utilise un NVIDIA GRID pilote
- Instances alimentées par des processeurs Graviton basés sur ARM
- Instances Windows activées AWS Outposts
- Instances Windows sur les Zones AWS Locales

Régions prises en charge

Cette fonction est disponible dans les régions suivantes :

- US East (N. Virginia) Region
- Région US East (Ohio)
- Région US West (N. California)
- Région US West (Oregon)
- Région Afrique (Le Cap)
- Région Asie-Pacifique (Hong Kong)
- Région Asie-Pacifique (Hyderabad)
- Région Asie-Pacifique (Jakarta)
- Région Asie-Pacifique (Melbourne)
- Région Asie-Pacifique (Mumbai)
- Région Asie-Pacifique (Osaka)
- Région Asie-Pacifique (Séoul)
- Région Asie-Pacifique (Singapour)
- Région Asie-Pacifique (Sydney)
- Région Asie-Pacifique (Tokyo)
- Région Canada (Centre)

- Région Canada Ouest (Calgary)
- Région Chine (Beijing)
- Région Chine (Ningxia)
- Région Europe (Frankfurt)
- Région Europe (Irlande)
- Région Europe (London)
- Europe (Milan) Region
- Région Europe (Paris)
- Région Europe (Espagne)
- Région Europe (Stockholm)
- Région Europe (Zurich)
- Région Israël (Tel Aviv)
- Région Amérique du Sud (São Paulo)
- Middle East (Bahrain) Region
- Région du Moyen-Orient (UAE)

Console

Obtention d'une capture d'écran d'une instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation de gauche, choisissez Instances.
3. Sélectionnez l'instance à capturer.
4. Sélectionnez Actions, Surveiller et dépanner puis Obtenir la capture d'écran d'instance.
5. Sélectionnez Téléchargerou cliquez avec le bouton droit sur l'image pour la télécharger et l'enregistrer.

Command line

Création d'une capture d'écran d'instance

Vous pouvez utiliser l'une des commandes suivantes. Le contenu renvoyé est codé en base64. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel Accédez à Amazon EC2.

- get-console-screenshot (AWS CLI)
- GetConsoleScreenshot(EC2Requête AmazonAPI)

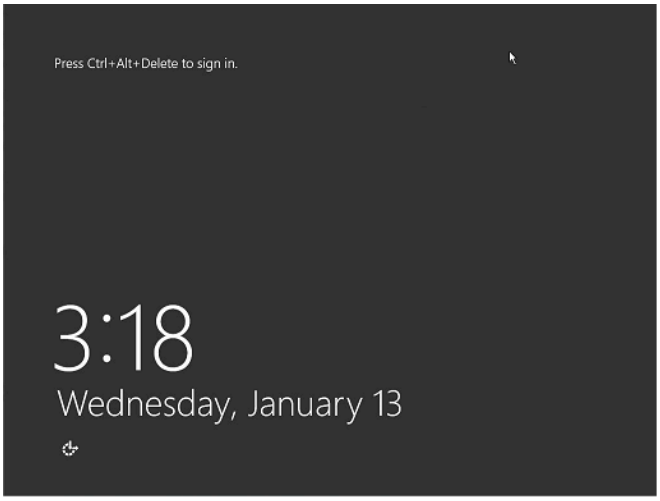
Captures d'écran courantes pour résoudre les problèmes liés aux instances Windows inaccessibles

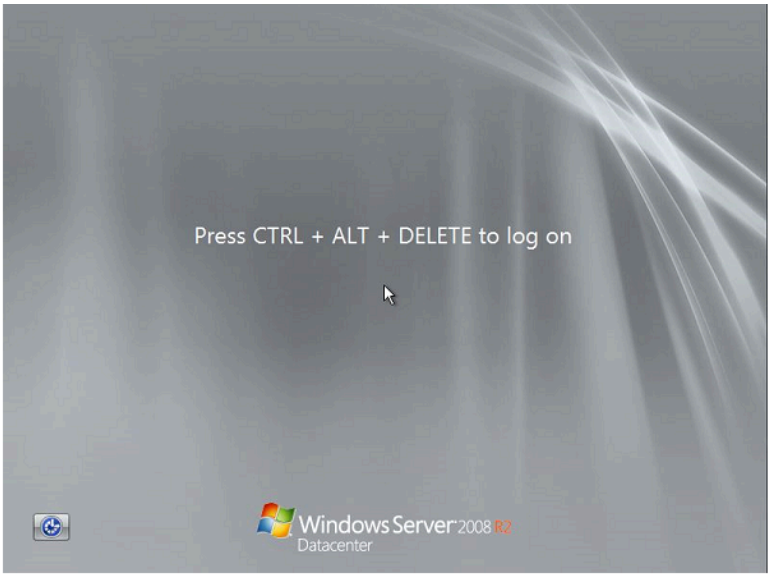
Aidez-vous des informations suivantes pour faciliter le dépannage d'une instance Windows inaccessible grâce aux captures d'écran renvoyées par le service.

- Écran de connexion (Ctrl+Alt+Suppr)
- Écran de la console de récupération
- Écran du gestionnaire de démarrage Windows
- Écran Sysprep
- Écran de préparation
- Écran Windows Update
- Chkdsk

Écran de connexion (Ctrl+Alt+Suppr)

Le service de capture d'écran de la console a renvoyé ce qui suit.





Si une instance devient inaccessible au cours de la connexion, le problème peut venir de votre configuration réseau ou des services Bureau à distance de Windows. Une instance peut également ne pas répondre si un processus utilise de grandes quantités deCPU.

Configuration réseau

Utilisez les informations suivantes pour vérifier que votre configuration réseau AWS, celle de Microsoft Windows et celle de votre réseau local (ou local) ne bloquent pas l'accès à l'instance.

AWS configuration réseau

Configuration	Vérifier
Configuration du groupe de sécurité	Vérifiez que le port 3389 est ouvert pour votre groupe de sécurité. Vérifiez que vous vous connectez à l'adresse IP publique appropriée. Si l'instance n'a pas été associée à une EIP, l'adresse IP publique change après l'arrêt ou le démarrage de l'instance. Pour de plus amples informations, veuillez consulter Le service Bureau à distance ne peut pas se connecter à l'ordinateur distant.
VPCconfiguration (réseauACLs)	Vérifiez que la liste de contrôle d'accès (ACL) de votre Amazon VPC ne bloque pas l'accès. Pour plus d'informations, consultez la section Réseau ACLs dans le guide de VPC l'utilisateur Amazon.
VPNconfiguration	Si vous vous connectez VPC via un réseau privé virtuel (VPN), vérifiez la connectivité VPN du tunnel. Pour plus d'informations, consultez Comment résoudre les problèmes de connectivité d'un VPN tunnel vers un Amazon VPC ?

Configuration du réseau Windows

Configuration	Vérifier
Pare-feu Windows	Vérifiez que le pare-feu Windows ne bloque pas les connexions à votre instance. Désactive z le pare-feu Windows, comme décrit à l'étape 7 de la section de résolution des problèmes liés au service Bureau à distance, Le service Bureau à distance ne peut pas se connecter à l'ordinateur distant.
Configuration TCP /IP avancée (utilisation d'une adresse IP statique)	L'instance peut ne pas réagir flottee que vous avez configuré une adresse IP statique. Dans le cas d'unVPC, créez une interface réseau et attachez-la à l'instance.

Configuration réseau locale ou sur site

Vérifiez qu'une configuration réseau locale ne bloque pas l'accès. Essayez de vous connecter à une autre instance identique à VPC celle de votre instance inaccessible. Si vous ne parvenez pas à accéder à une autre instance, contactez votre administrateur de réseau local pour déterminer si une politique locale restreint l'accès.

Problème lié aux services Bureau à distance

Si l'instance n'est pas joignable lors de l'ouverture de session, il se peut qu'il y ait un problème avec Remote Desktop Services (RDS) sur l'instance.

> **Tip**
>
> Vous pouvez utiliser le `AWSSupport-TroubleshootRDP` runbook pour vérifier et modifier les différents paramètres susceptibles d'affecter les connexions Remote Desktop Protocol (RDP). Pour plus d'informations, consultez `AWSSupport-TroubleshootRDP` dans la référence AWS Systems Manager Automation runbook.

Configuration des services Bureau à distance (RDS)

Configuration	Vérifier
RDSest en cours d'exécution	Vérifiez qu'il RDS est en cours d'exécution sur l'instance. Connectez-vous à l'instance à l'aide du composant logiciel enfichable Microsoft Management Console (MMC) Services (`services.msc`). Dans la liste des services, vérifiez que Services Bureau à distance est défini sur En cours d'exécution. Si ce n'est pas le cas, démarrez-le, puis définissez le type de démarrage sur Automatique. Si vous ne parvenez pas à vous connecter à l'instance à l'aide du composant logiciel enfichabl e Services, détachez le volume racine de l'instance, prenez un instantané du volume ou créez-en un à AMI partir de celui-ci, attachez le volume d'origine à une autre instance située dans la même zone de disponibilité qu'un volume secondaire et modifiez la clé de registre Start. Lorsque vous avez terminé, rattachez le volume racine à l'instance d'origine.
RDSest activé	Même si le service a été lancé, il peut être désactivé. Détachez le volume racine de l'instance, prenez un instantané du volume ou créez-en un à AMI partir de celui-ci, attachez le volume d'origine à une autre instance située dans la même zone de disponibilité qu'un volume secondaire et activez le service en modifiant la clé de registre du serveur Terminal Server comme décrit dansActiver le bureau à distance sur une EC2 instance dotée d'un registre distant. Lorsque vous avez terminé, rattachez le volume racine à l'instance d'origine.

CPUUsage élevé

Vérifiez la métrique CPUUtilization(maximale) sur votre instance à l'aide d'Amazon CloudWatch. Si CPUUtilization(Maximum) est un nombre élevé, attendez qu'il baisse et CPU essayez de vous reconnecter. Une CPU utilisation élevée peut être causée par :

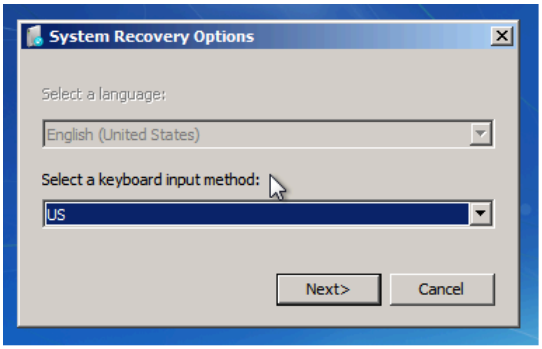
- Windows Update

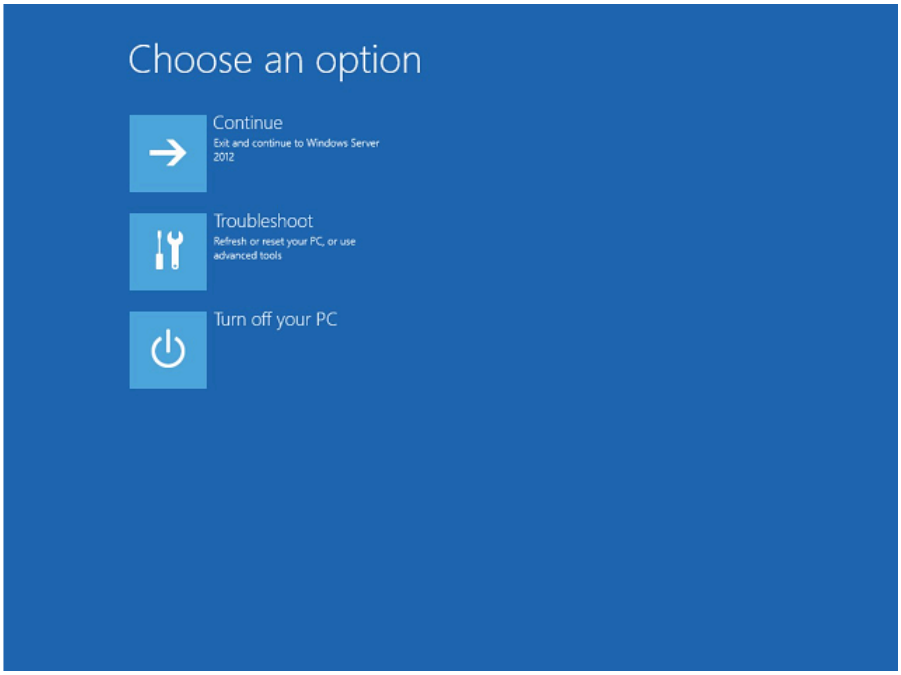
- Analyse des logiciels de sécurité
- Script de démarrage personnalisé
- Planificateur de tâches

Pour plus d'informations, consultez Obtenir des statistiques pour une ressource spécifique dans le guide de CloudWatch l'utilisateur Amazon. Pour des conseils de dépannage supplémentaires, consultez la page CPUUtilisation élevée peu après le démarrage de Windows (instances Windows uniquement).

Écran de la console de récupération

Le service de capture d'écran de la console a renvoyé ce qui suit.





Le système d'exploitation peut démarrer dans la console de récupération et rester bloqué dans cet état si la stratégie `bootstatuspolicy` n'est pas définie sur `ignoreallfailures`. Utilisez la procédure suivante pour remplacer la configuration `bootstatuspolicy` par `ignoreallfailures`.

Par défaut, la configuration de politique pour les fenêtres publiques AMIs fournie par AWS est définie sur`ignoreallfailures`.

1. Arrêtez l'instance inaccessible.
2. Créez un instantané du volume racine. Le volume racine est attaché à l'instance en tant que `/dev/sda1`.

Détachez le volume racine de l'instance inaccessible, prenez un instantané du volume ou créez-en un à AMI partir de celui-ci, puis attachez-le à une autre instance dans la même zone de disponibilité qu'un volume secondaire.

> **Warning**
>
> Si votre instance temporaire et l'instance d'origine ont été lancées de la même manièreAMI, vous devez effectuer des étapes supplémentaires, sinon vous ne pourrez pas démarrer l'instance d'origine après avoir restauré son volume racine en raison d'une collision de signature de disque. Si vous devez créer une instance temporaire à l'aide de celui-ciAMI, pour éviter une collision de signature de disque, suivez les étapes décrites dansCollision de signature de disque.
> Vous pouvez également en sélectionner une autre AMI pour l'instance temporaire. Par exemple, si l'instance d'origine utilise un AMI pour Windows Server 2016, lancez l'instance temporaire à l'aide d'un AMI pour Windows Server 2019.

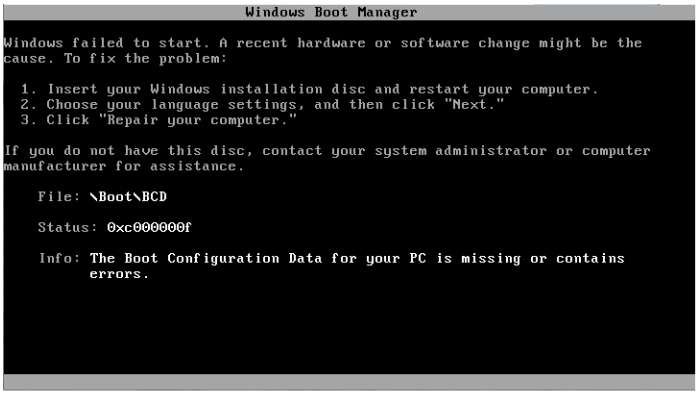
3. Connectez-vous à l'instance et exécutez la commande suivante à partir d'une invite de commande pour remplacer la configuration `bootstatuspolicy` par `ignoreallfailures`.

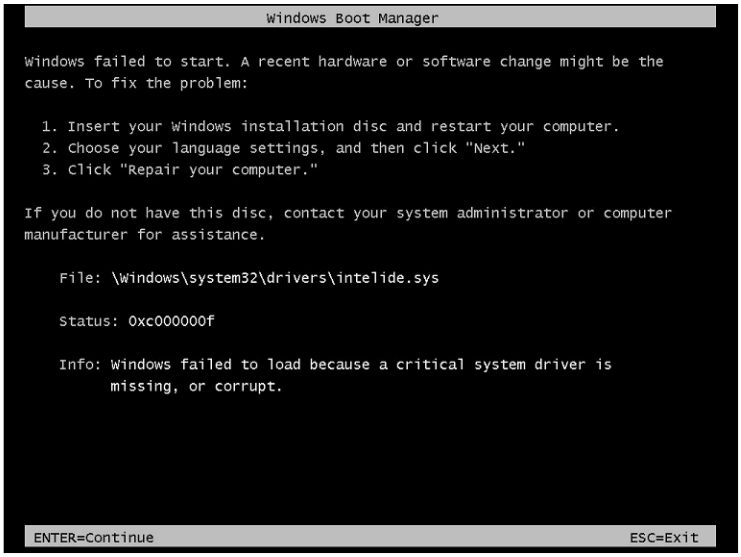
```
bcdedit /store Drive Letter:\boot\bcd /set {default} bootstatuspolicy
 ignoreallfailures
```

4. Rattachez le volume à l'instance inaccessible et redémarrez cette dernière.

Écran du gestionnaire de démarrage Windows

Le service de capture d'écran de la console a renvoyé ce qui suit.

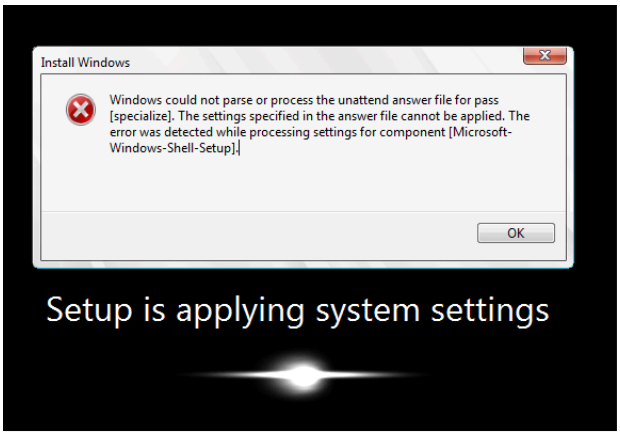


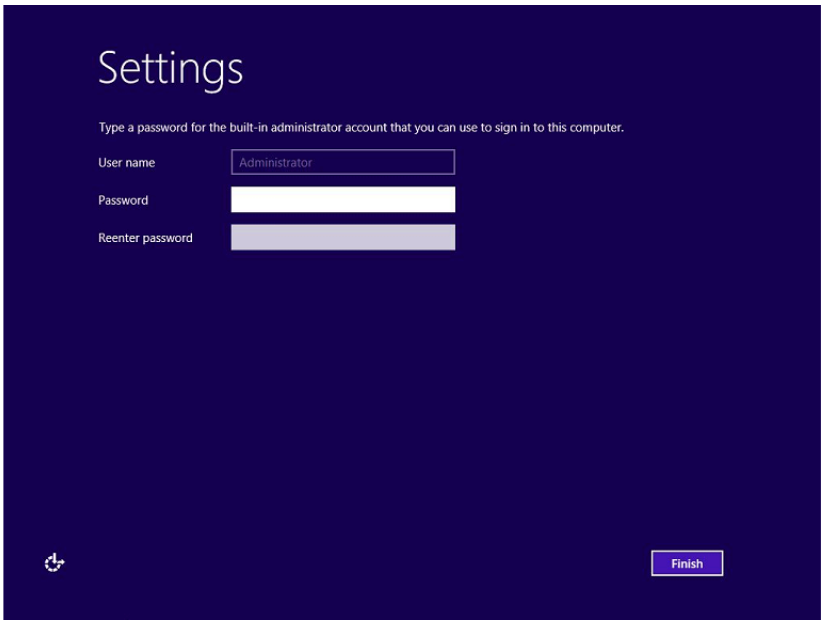


Le système d'exploitation a subi une corruption irrécupérable dans le système de fichier et/ou le registre. Lorsque l'instance est bloquée dans cet état, vous devez la récupérer à partir d'une sauvegarde récente AMI ou lancer une instance de remplacement. Si vous devez accéder aux données de l'instance, détachez les volumes racines de l'instance inaccessible, prenez un instantané de ces volumes ou créez-en un à AMI partir de ceux-ci, puis attachez-les à une autre instance dans la même zone de disponibilité qu'un volume secondaire.

Écran Sysprep

Le service de capture d'écran de la console a renvoyé ce qui suit.

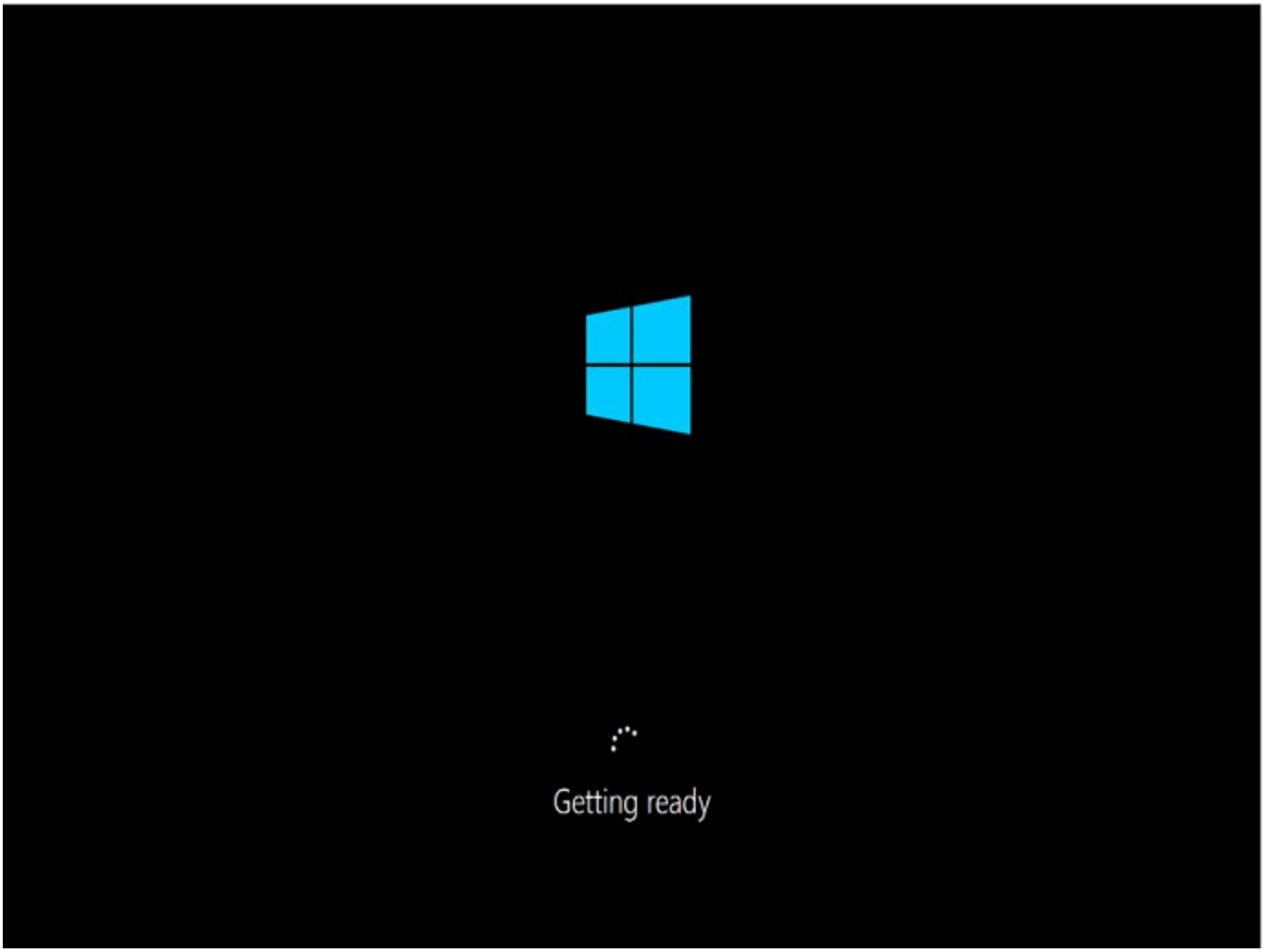




Cet écran peut s'afficher si vous n'avez pas utilisé le EC2Config Service pour appeler Sysprep ou si le système d'exploitation a échoué lors de l'exécution de Sysprep. Vous pouvez réinitialiser le mot de passe en utilisant EC2Rescue. Sinon, consultez Créez un Amazon à EC2 AMI l'aide de Windows Sysprep.

Écran de préparation

Le service de capture d'écran de la console a renvoyé ce qui suit.

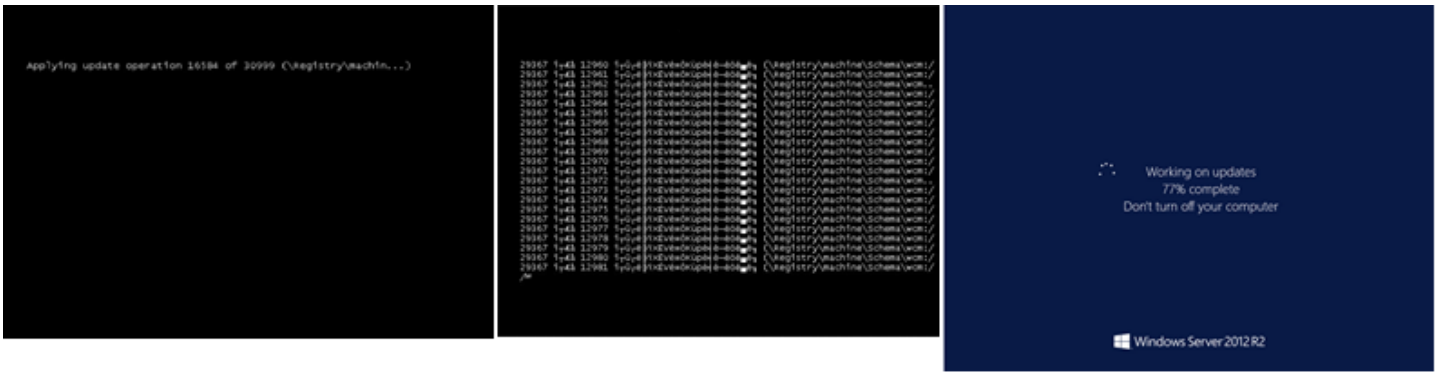


Actualisez le service de capture d'écran de la console d'instance plusieurs fois pour vérifier que l'anneau de progression tourne. Si l'anneau tourne, attendez que le système d'exploitation démarre. Vous pouvez également vérifier la métrique CPUUtilization(maximale) sur votre instance en utilisant Amazon CloudWatch pour vérifier si le système d'exploitation est actif. Si l'anneau de progression ne tourne pas, l'instance est peut-être bloquée au niveau du processus de démarrage. Redémarrez l'instance. Si le redémarrage ne résout pas le problème, restaurez l'instance à partir d'une sauvegarde récente AMI ou lancez une instance de remplacement. Si vous devez accéder aux

données de l'instance, détachez le volume racine de l'instance inaccessible, prenez un instantané du volume ou créez-en un AMI à partir de celui-ci. Attachez-le ensuite à une autre instance de la même zone de disponibilité en tant que volume secondaire.

Écran Windows Update

Le service de capture d'écran de la console a renvoyé ce qui suit.

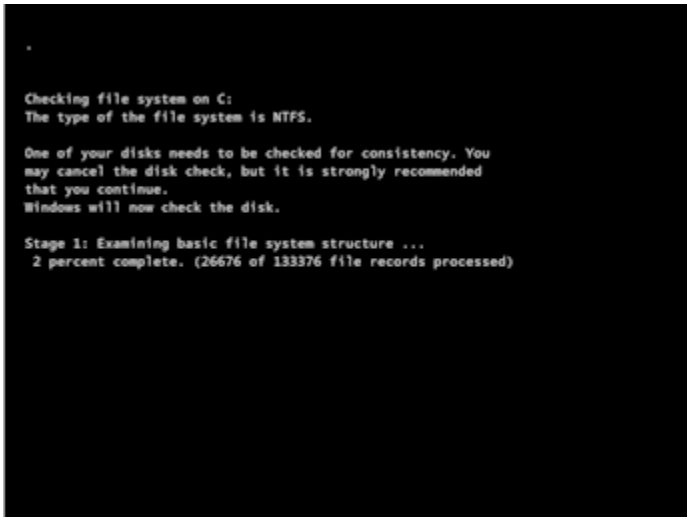


Le processus Windows Update met à jour le registre. Attendez que la mise à jour soit terminée. Ne redémarrez ou n'arrêtez pas l'instance, car cela peut entraîner une corruption des données au cours de la mise à jour.

> **Note**
>
> Le processus Windows Update peut utiliser des ressources sur le serveur au cours de la mise à jour. Si vous rencontrez souvent ce problème, pensez à utiliser des types d'instance et des EBS volumes plus rapides.

Chkdsk

Le service de capture d'écran de la console a renvoyé ce qui suit.



Windows exécute l'outil système chkdsk sur le disque pour vérifier l'intégrité du système de fichiers et pour corriger les erreurs système des fichiers logiques. Attendez que le processus se termine.

Récupération d'instance en cas de plantage de l'ordinateur hôte

S'il existe un problème irrécupérable lié au matériel d'un ordinateur hôte sous-jacent, AWS peut planifier un évènement d'arrêt d'instance. Vous êtes averti d'un tel événement en avance par e-mail.

Pour récupérer une instance EBS basée sur Amazon exécutée sur un ordinateur hôte en panne

1. Sauvegardez toutes les données importantes relatives aux volumes de stockage de votre instance sur Amazon EBS ou Amazon S3.
2. Arrêtez l'instance.
3. Démarrez l'instance.
4. Restaurez toutes les données importantes.

Pour de plus amples informations, veuillez consulter Arrêtez et démarrez les EC2 instances Amazon.

Pour récupérer une instance basée sur le stockage d'instance et exécutée sur un ordinateur hôte qui a planté

1. Créez un AMI à partir de l'instance.
2. Chargez l'image vers Amazon S3.
3. Sauvegardez les données importantes sur Amazon EBS ou Amazon S3.
4. Mettez fin à l'instance.

5. Lancez une nouvelle instance depuis leAMI.
6. Restaurez toutes les données importantes sur la nouvelle instance.

Résoudre les problèmes de connexion à votre instance Amazon EC2 Linux

Les informations suivantes et les erreurs courantes peuvent vous aider à résoudre les problèmes de connexion à votre instance Linux.

Problèmes de connexion

- Causes courantes des problèmes de connexion
- Erreur de connexion à votre instance : connexion expirée
- Erreur : impossible de charger la clé... Attendant : ANY PRIVATE KEY
- Erreur : clé de l'utilisateur non reconnue par le serveur
- Erreur : autorisation refusée ou connexion fermée par [instance] port 22
- Erreur : fichier de clé privée non protégé
- Erreur : la clé privée doit commencer par « ----- BEGIN RSA PRIVATE KEY ----- » et se terminer par « ----- ----- » END RSA PRIVATE KEY
- Erreur : le serveur a refusé notre clé ou Aucune méthode d'authentification prise en charge disponible
- Impossible d'envoyer une commande ping à l'instance
- Erreur : le serveur a fermé la connexion réseau de manière inopinée
- Erreur : échec de la validation de la clé d'hôte pour EC2 Instance Connect
- Impossible de se connecter à une instance Ubuntu à l'aide d'EC2Instance Connect
- J'ai perdu ma clé privée. Comment puis-je me connecter à mon instance ?

Causes courantes des problèmes de connexion

Nous vous recommandons de commencer à résoudre les problèmes de connexion aux instances en vérifiant que vous avez correctement effectué les tâches suivantes.

Vérifiez le nom d'utilisateur de votre instance

Vous pouvez vous connecter à votre instance en utilisant le nom d'utilisateur de votre compte utilisateur ou le nom d'utilisateur par défaut de AMI celui que vous avez utilisé pour lancer votre instance.

- Obtenez le nom d'utilisateur de votre compte utilisateur.

  Pour plus d'informations sur la création d'un compte utilisateur, consultez Gérez les utilisateurs du système sur votre instance Amazon EC2 Linux.
- Obtenez le nom d'utilisateur par défaut pour celui AMI que vous avez utilisé pour lancer votre instance.

AMIutilisé pour lancer l'instance	Nom d'utilisateur par défaut
Amazon Linux	`ec2-user`
CentOS	`centos` ou `ec2-user`
Debian	`admin`
Fedora	`fedora` ou `ec2-user`
RHEL	`ec2-user` ou `root`
SUSE	`ec2-user` ou `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Autre	Vérifiez auprès du AMI fournisseur

Vérifiez que les règles de votre groupe de sécurité autorisent le trafic

Assurez-vous que le groupe de sécurité associé à votre instance autorise le SSH trafic entrant depuis votre adresse IP. Le groupe de sécurité par défaut pour le VPC n'autorise pas le SSH trafic entrant par défaut. Le groupe de sécurité créé par l'assistant de lancement d'instance active

SSH le trafic par défaut. Pour savoir comment ajouter une règle pour le SSH trafic entrant à votre instance Linux, consultezRègles pour la connexion à des instances à partir de votre ordinateur. Pour connaître les étapes à vérifier, consultez Erreur de connexion à votre instance : connexion expirée.

Vérifiez que votre instance est prête

Après le lancement d'une instance, quelques minutes peuvent s'écouler avant qu'elle soit prête à accepter les demandes de connexion. Vérifiez votre instance pour vous assurer qu'elle est en cours d'exécution et qu'elle a réussi ses vérifications d'état.

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez instances, puis sélectionnez votre instance.
3. Vérifiez les paramètres suivants :
   a. Dans la colonne État de l'instance, vérifiez que l'état de votre instance est `running`.
   b. Dans la colonne Contrôle des statuts, vérifiez que votre instance a passé avec succès les deux vérifications de statut.

Vérifiez que vous avez répondu à toutes les conditions préalables pour vous connecter.

Assurez-vous de disposer de toutes les informations dont vous avez besoin pour vous connecter. Pour de plus amples informations, veuillez consulter Connectez-vous à votre instance Linux à l'aide de SSH.

Connect depuis Linux ou macOS X

Si le système d'exploitation de votre ordinateur local est Linux ou macOS X, vérifiez les points suivants pour connaître les conditions préalables spécifiques à la connexion à une instance Linux :

- SSHclient
- EC2Instance Connect
- AWS Systems Manager Gestionnaire de sessions

Connexion à partir de Windows

Si le système d'exploitation de votre ordinateur local est Windows, vérifiez les points suivants pour connaître les conditions préalables spécifiques à la connexion à une instance Linux :

- Ouvert SSH

- Pu TTY
- AWS Systems Manager Gestionnaire de sessions
- WSL (Windows Subsystem for Linux)

Erreur de connexion à votre instance : connexion expirée

Si vous essayez de vous connecter à votre instance et vous obtenez le message d'erreur `Network error: Connection timed out` ou `Error connecting to [instance], reason: -> Connection timed out: connect`, essayez ce qui suit :

Vérifiez les règles du groupe de sécurité.

Vous avez besoin d'une règle de groupe de sécurité qui autorise le trafic entrant depuis l'IPv4adresse publique de votre ordinateur local sur le port approprié.

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez instances, puis sélectionnez votre instance.
3. Sous l'onglet Sécurité au bas de la page de la console, sous Règles entrantes, vérifiez la liste des règles en vigueur pour l'instance sélectionnée. Vérifiez qu'une règle autorise le trafic de votre ordinateur local vers le port 22 (SSH).

   Si votre groupe de sécurité ne possède pas de règle qui permet le trafic entrant à partir de votre ordinateur local, ajoutez une règle à votre règle de sécurité. Pour de plus amples informations, veuillez consulter Règles pour la connexion à des instances à partir de votre ordinateur.
4. Pour connaître la règle qui autorise le trafic entrant, consultez laSource. Si la valeur est une adresse IP unique et si l'adresse IP n'est pas statique, une nouvelle adresse IP sera attribuée chaque fois que vous redémarrerez votre ordinateur. Cela aura pour conséquence que la règle n'inclut pas le trafic d'adresses IP de votre ordinateur. L'adresse IP peut ne pas être statique si votre ordinateur est connecté à un réseau d'entreprise, si vous vous connectez via un fournisseur de services Internet (ISP), ou si l'adresse IP de votre ordinateur est dynamique et change chaque fois que vous redémarrez votre ordinateur. Pour vous assurer que votre règle de groupe de sécurité autorise le trafic entrant provenant de votre ordinateur local, au lieu de spécifier une adresse IP unique pourSource, au lieu de spécifier la plage d'adresses IP utilisées par vos ordinateurs clients.

   Pour plus d'informations sur les règles des groupes de sécurité, consultez la section Règles des groupes de sécurité dans le guide de VPC l'utilisateur Amazon.

Vérifiez la table de routage pour le sous-réseau.

Vous avez besoin d'un itinéraire qui envoie tout le trafic destiné VPC à l'extérieur vers la passerelle Internet duVPC.

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez instances, puis sélectionnez votre instance.
3. Dans l'onglet Mise en réseau, notez les valeurs de l'VPCID et de l'ID de sous-réseau.
4. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
5. Dans le panneau de navigation, choisissez Passerelles Internet. Vérifiez qu'une passerelle Internet est connectée à votreVPC. Sinon, choisissez Créer une passerelle Internet, entrez un nom pour la passerelle Internet et choisissez Créer une passerelle Internet. Ensuite, pour la passerelle Internet que vous avez créée, choisissez Actions, Joindre à VPC, sélectionnez votreVPC, puis choisissez Attacher la passerelle Internet pour l'associer à votreVPC.
6. Dans le panneau de navigation, sélectionnez Sous-réseaux, puis sélectionnez votre sous-réseau.
7. Dans l'onglet Table de routage, vérifiez qu'il existe un itinéraire avec `0.0.0.0/0` comme destination et la passerelle Internet correspondant à votre destination VPC comme cible. Si vous vous connectez à votre instance à l'aide de son IPv6 adresse, vérifiez qu'il existe un itinéraire pour tout le IPv6 trafic (`::/0`) qui pointe vers la passerelle Internet. Sinon, procédez comme suit :

    a. Choisissez l'ID de la table de routage (rtb-xxxxxxxx) pour accéder à cette dernière.

    b. Dans l'onglet Routes, choisissez Edit routes (Modifier les routes). Choisissez Add route (Ajouter une route) et utilisez `0.0.0.0/0` comme destination et la passerelle Internet comme cible. PourIPv6, choisissez Ajouter un itinéraire, utilisez `::/0` comme destination et la passerelle Internet comme cible.

    c. Choisissez Save routes (Enregistrer les acheminements).

Vérifiez la liste de contrôle d'accès réseau (ACL) du sous-réseau.

Le réseau ACLs doit autoriser le SSH trafic entrant depuis votre adresse IP locale sur le port 22. Elles doivent également autoriser le trafic sortant vers les ports éphémères (1024-65535).

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Subnets.

3. Sélectionnez votre sous-réseau.
4. Dans l'ACLonglet Réseau, pour les règles entrantes, vérifiez que les règles autorisent le trafic entrant depuis votre ordinateur sur le port requis. Sinon, supprimez ou modifiez la règle qui bloque le trafic.
5. Pour Règles sortantes, vérifiez que les règles autorisent le trafic vers votre ordinateur sur les ports éphémères. Sinon, supprimez ou modifiez la règle qui bloque le trafic.

Si votre ordinateur se trouve sur un réseau d'entreprise

Demandez à votre administrateur réseau si le pare-feu interne autorise le trafic entrant et sortant de votre ordinateur sur le port 22.

Si votre ordinateur est doté d'un pare-feu, vérifiez qu'il autorise le trafic entrant et sortant de votre ordinateur sur le port 22.

Vérifiez que votre instance possède une IPv4 adresse publique.

Si non, vous pouvez associer une adresse IP Elastic à votre instance. Pour de plus amples informations, veuillez consulter Adresses IP Elastic.

Vérifiez la CPU charge de votre instance ; le serveur est peut-être surchargé.

AWS fournit automatiquement des données telles que CloudWatch les métriques Amazon et le statut de l'instance, que vous pouvez utiliser pour connaître le CPU niveau de charge de votre instance et, si nécessaire, ajuster la manière dont vos charges sont gérées. Pour de plus amples informations, veuillez consulter Surveillez vos instances à l'aide de CloudWatch.

- Si votre charge est variable, vous pouvez automatiquement effectuer des mises à l'échelle ascendantes et descendantes de vos instances en utilisant l'Auto Scaling et l'Elastic Load Balancing.
- Si votre charge augmente régulièrement, vous pouvez passer à un type d'instance plus important. Pour de plus amples informations, veuillez consulter Changements de type d'EC2instance Amazon.

Pour vous connecter à votre instance à l'aide d'une IPv6 adresse, vérifiez les points suivants :

- Votre sous-réseau doit être associé à une table de routage comportant une route pour le IPv6 trafic (`::/0`) vers une passerelle Internet.

- Les règles de votre groupe de sécurité doivent autoriser le trafic entrant depuis votre IPv6 adresse locale sur le port 22.
- ACLLes règles de votre réseau doivent autoriser le trafic entrant et sortantIPv6.
- Si vous avez lancé votre instance à partir d'une ancienne instanceAMI, elle n'est peut-être pas configurée pour DHCPv6 (les IPv6 adresses ne sont pas automatiquement reconnues sur l'interface réseau). Pour plus d'informations, consultez la section Configurer IPv6 sur vos instances dans le guide de VPC l'utilisateur Amazon.
- Votre ordinateur local doit avoir une IPv6 adresse et doit être configuré pour être utiliséIPv6.

Erreur : impossible de charger la clé... Attendant : ANY PRIVATE KEY

Si vous essayez de vous connecter à votre instance et obtenez le message d'erreur `unable to load key ... Expecting: ANY PRIVATE KEY`, le fichier dans lequel la clé privée est stockée est mal configuré. Si le fichier de clé privée se termine par `.pem`, il est peut-être toujours mal configuré. Une cause possible de configuration incorrecte d'un fichier de clé privée est l'absence d'un certificat.

Si le fichier de clé privée est mal configuré, suivez ces étapes pour corriger l'erreur.

1. Créez une nouvelle paire de clés. Pour de plus amples informations, veuillez consulter Créez une paire de clés à l'aide d'Amazon EC2.

   > **Note**
   >
   > Sinon, vous pouvez créer une nouvelle key pair à l'aide d'un outil tiers. Pour de plus amples informations, veuillez consulter Créez une paire de clés à l'aide d'un outil tiers et importez la clé publique sur Amazon EC2.

2. Ajoutez la nouvelle paire de clés à votre instance. Pour de plus amples informations, veuillez consulter J'ai perdu ma clé privée. Comment puis-je me connecter à mon instance ?.
3. Connectez-vous à votre instance à l'aide de la nouvelle paire de clés.

Erreur : clé de l'utilisateur non reconnue par le serveur

Si vous vous connectez SSH à votre instance

- Utilisez `ssh -vvv` pour obtenir des informations très détaillées sur le débogage en vous connectant :

```
ssh -vvv -i path/key-pair-name.pem instance-user-
name@ec2-203-0-113-25.compute-1.amazonaws.com
```

L'exemple de données de sortie suivant montre que vous pouvez voir si vous étiez en train de vous connecter à votre instance avec une clé qui n'était pas reconnue par le serveur.

```
open/ANT/myusername/.ssh/known_hosts).
debug2: bits set: 504/1024
debug1: ssh_rsa_verify: signature correct
debug2: kex_derive_keys
debug2: set_newkeys: mode 1
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug2: set_newkeys: mode 0
debug1: SSH2_MSG_NEWKEYS received
debug1: Roaming not allowed by server
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug2: service_accept: ssh-userauth
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug2: key: boguspem.pem ((nil))
debug1: Authentications that can continue: publickey
debug3: start over, passed a different list publickey
debug3: preferred gssapi-keyex,gssapi-with-mic,publickey,keyboard-
interactive,password
debug3: authmethod_lookup publickey
debug3: remaining preferred: keyboard-interactive,password
debug3: authmethod_is_enabled publickey
debug1: Next authentication method: publickey
debug1: Trying private key: boguspem.pem
debug1: read PEM private key done: type RSA
debug3: sign_and_send_pubkey: RSA 9c:4c:bc:0c:d0:5c:c7:92:6c:8e:9b:16:e4:43:d8:b2
debug2: we sent a publickey packet, wait for reply
debug1: Authentications that can continue: publickey
debug2: we did not send a packet, disable method
debug1: No more authentication methods to try.
```

```
Permission denied (publickey).
```

Si vous utilisez Pu TTY pour vous connecter à votre instance

- Vérifiez que votre fichier de clé privée (.pem) a été converti au format reconnu par Pu TTY (.ppk). Pour plus d'informations sur la conversion de votre clé privée, consultez Connectez-vous à votre instance Linux à l'aide de Pu TTY.

> **Note**
>
> Dans PuTTYgen, chargez votre fichier de clé privée et sélectionnez Enregistrer la clé privée plutôt que Générer.

- Vérifiez que vous vous connectez avec le nom d'utilisateur approprié pour votreAMI. Entrez le nom d'utilisateur dans le champ Nom de l'hôte de la fenêtre TTYde configuration Pu.

AMIutilisé pour lancer l'instance	Nom d'utilisateur par défaut
Amazon Linux	`ec2-user`
CentOS	`centos` ou `ec2-user`
Debian	`admin`
Fedora	`fedora` ou `ec2-user`
RHEL	`ec2-user` ou `root`
SUSE	`ec2-user` ou `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Autre	Vérifiez auprès du AMI fournisseur

- Vérifiez que vous avez une règle entrante de groupe de sécurité pour permettre le trafic entrant vers le port approprié. Pour de plus amples informations, veuillez consulter Règles pour la connexion à des instances à partir de votre ordinateur.

Erreur : autorisation refusée ou connexion fermée par [instance] port 22

Si vous vous connectez à votre instance en utilisant SSH et obtenez l'une des erreurs suivantes,`Host key not found in [directory]`,`Permission denied (publickey)`, ou`Authentication failed, permission denied`, ou`Connection closed by [instance] port 22`, vérifiez que vous vous connectez avec le nom d'utilisateur approprié pour votre instance AMI et que vous avez spécifié la clé privée (`.pem`)fichier) appropriée pour votre instance.

Les noms d'utilisateur appropriés sont les suivants :

AMIutilisé pour lancer l'instance	Nom d'utilisateur par défaut
Amazon Linux	`ec2-user`
CentOS	`centos` ou `ec2-user`
Debian	`admin`
Fedora	`fedora` ou `ec2-user`
RHEL	`ec2-user` ou `root`
SUSE	`ec2-user` ou `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Autre	Vérifiez auprès du AMI fournisseur

Par exemple, pour utiliser un SSH client pour se connecter à une instance Amazon Linux, utilisez la commande suivante :

```
ssh -i /path/key-pair-name.pem instance-user-
name@ec2-203-0-113-25.compute-1.amazonaws.com
```

Confirmez que vous utilisez le fichier de clé privée qui correspond à la paire de clés que vous avez sélectionnée lorsque vous avez lancé l'instance.

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances, puis sélectionnez votre instance.
3. Sous l'onglet Détails, sous Détails de l'instance, vérifiez la valeur Nom de la paire de clés.
4. Si vous n'avez pas spécifié une paire de clés lorsque vous avez lancé l'instance, vous pouvez mettre fin à l'instance et lancer une nouvelle instance en vous assurant de spécifier une paire de clés. S'il s'agit d'une instance que vous avez utilisée, mais que vous n'avez plus le fichier `.pem` pour votre paire de clés, vous pouvez remplacer la paire de clés par une nouvelle. Pour de plus amples informations, veuillez consulter J'ai perdu ma clé privée. Comment puis-je me connecter à mon instance ?.

Si vous avez généré votre propre paire de clés, assurez-vous que votre générateur de clés est configuré pour créer des RSA clés. DSAles clés ne sont pas acceptées.

Si vous obtenez une erreur `Permission denied (publickey)` et qu'aucune des réponses ci-dessus ne s'applique (par exemple, vous avez pu vous connecter précédemment), les autorisations sur le répertoire de base de votre instance a peut-être été modifiées. Les autorisations pour `/home/instance-user-name/.ssh/authorized_keys` doivent être limitées au propriétaire uniquement.

Pour vérifier les autorisations sur votre instance

1. Arrêtez votre instance et détachez le volume racine. Pour de plus amples informations, veuillez consulter Arrêtez et démarrez les EC2 instances Amazon.
2. Lancez une instance temporaire dans la même zone de disponibilité que votre instance actuelle (utilisez une instance similaire ou AMI identique à celle que vous avez utilisée pour votre instance actuelle) et attachez le volume racine à l'instance temporaire.
3. Connectez-vous à l'instance temporaire, créez un point de montage et montez le volume que vous avez joint.

4. A partir de l'instance temporaire, vérifiez les autorisations du répertoire /home/*instance-user-name*/ du volume attaché. Si nécessaire, modifiez les autorisations comme suit :

```
[ec2-user ~]$ chmod 600 mount_point/home/instance-user-name/.ssh/authorized_keys
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name/.ssh
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name
```

5. Démontez le volume, détachez-le de l'instance temporaire et attachez-le de nouveau à l'instance originale. Assurez-vous que vous avez spécifié le bon nom de périphérique pour le volume racine, par exemple, /dev/xvda.
6. Démarrez votre instance. Si vous n'avez plus besoin de l'instance temporaire, vous pouvez la mettre en service.

Erreur : fichier de clé privée non protégé

Votre fichier de clé privée doit être protégé des opérations de lecture et d'écriture des autres utilisateurs. Si votre clé privée peut être lue ou écrite par quelqu'un d'autre que vous, alors elle est SSH ignorée et le message d'avertissement suivant s'affiche ci-dessous.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0777 for '.ssh/my_private_key.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
bad permissions: ignore key: .ssh/my_private_key.pem
Permission denied (publickey).
```

Si vous voyez un message similaire lorsque vous essayez de vous connecter à votre instance, examinez la première ligne du message d'erreur pour vérifier que vous utilisez la bonne clé publique pour votre instance. L'exemple ci-dessus utilise la clé privée .ssh/my_private_key.pem avec les autorisations sur les fichiers de 0777 ce qui permet à n'importe qui de lire ou écrire sur ce fichier. Ce niveau d'autorisation est très précaire et SSH ignore donc cette clé.

Si vous vous connectez à partir de macOs ou Linux, exécutez la commande suivante pour corriger cette erreur en remplaçant le chemin par celui de votre fichier de clé privée.

```
[ec2-user ~]$ chmod 0400 .ssh/my_private_key.pem
```

Si vous vous connectez à une instance Linux depuis Windows, effectuez les étapes suivantes sur votre ordinateur local.

1. Accédez au fichier .pem.
2. Cliquez avec le bouton droit de la souris sur le fichier .pem et sélectionnezPropriétés.
3. Choisissez l'onglet Security (Sécurité).
4. Sélectionnez Avancé.
5. Vérifiez que vous êtes le propriétaire du fichier. Si ce n'est pas le cas, changez le propriétaire avec votre nom d'utilisateur.
6. Sélectionnez Désactiver l'héritage et Supprimer toutes les autorisations héritées de cet objet.
7. Sélectionnez Ajouter, Sélectionnez un principal, saisissez votre nom d'utilisateur et sélectionnez OK.
8. À partir de la fenêtre Entrée d'autorisation, attribuez les autorisations Lire et sélectionnez OK.
9. Cliquez sur Apply (Appliquer) afin de garantir l'enregistrement de tous les paramètres.
10. Sélectionnez OK pour fermer la fenêtre Paramètres de sécurité avancés.
11. Sélectionnez OK pour fermer la fenêtre Propriétés.
12. Vous devriez pouvoir vous connecter à votre instance Linux depuis Windows à l'aide deSSH.

À partir d'une invite de commande Windows, exécutez la commande suivante.

1. À partir de l'invite de commande, accédez à l'emplacement du chemin de fichier de votre fichier .pem.
2. Exécutez la commande suivante pour réinitialiser et supprimer les autorisations explicites :

   ```
   icacls.exe $path /reset
   ```

3. Exécutez la commande suivante pour accorder à l'utilisateur actuel les autorisations de lecture :

   ```
   icacls.exe $path /GRANT:R "$($env:USERNAME):(R)"
   ```

4. Exécutez la commande suivante pour désactiver l'héritage et supprimer les autorisations héritées.

```
icacls.exe $path /inheritance:r
```

5. Vous devriez pouvoir vous connecter à votre instance Linux depuis Windows à l'aide deSSH.

Erreur : la clé privée doit commencer par « ----- BEGIN RSA PRIVATE KEY ----- » et se terminer par « ----- ----- » END RSA PRIVATE KEY

Si vous utilisez un outil tiers, par exemple ssh-keygen pour créer une paire de RSA clés, il génère la clé privée au format Open SSH key. Lorsque vous vous connectez à votre instance, si vous utilisez la clé privée SSH au format Open pour déchiffrer le mot de passe, le message d'erreur `Private key must begin with "-----BEGIN RSA PRIVATE KEY-----" and end with "-----END RSA PRIVATE KEY-----"` s'affiche.

Pour résoudre l'erreur, la clé privée doit être au PEM format. Utilisez la commande suivante pour créer la clé privée au PEM format :

```
ssh-keygen -m PEM
```

Erreur : le serveur a refusé notre clé ou Aucune méthode d'authentification prise en charge disponible

Si vous utilisez Pu TTY pour vous connecter à votre instance et que vous obtenez l'une des erreurs suivantes, Erreur : le serveur a refusé notre clé ou Erreur : aucune méthode d'authentification prise en charge n'est disponible, vérifiez que vous vous connectez avec le nom d'utilisateur approprié pour votreAMI. Tapez le nom d'utilisateur dans Nom d'utilisateur dans la fenêtre TTYde configuration Pu.

Les noms d'utilisateur appropriés sont les suivants :

AMIutilisé pour lancer l'instance	Nom d'utilisateur par défaut
Amazon Linux	`ec2-user`
CentOS	`centos` ou `ec2-user`
Debian	`admin`
Fedora	`fedora` ou `ec2-user`

AMIutilisé pour lancer l'instance	Nom d'utilisateur par défaut
RHEL	`ec2-user` ou `root`
SUSE	`ec2-user` ou `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Autre	Vérifiez auprès du AMI fournisseur

Vous devez également vérifier que :

- Vous utilisez la dernière version de PuTTY. Pour plus d'informations, consultez la page TTY Web de Pu.
- Votre fichier de clé privée (.pem) a été correctement converti au format reconnu par Pu TTY (.ppk). Pour plus d'informations sur la conversion de votre clé privée, consultez Connectez-vous à votre instance Linux à l'aide de Pu TTY.

Impossible d'envoyer une commande ping à l'instance

La `ping` commande est un type de ICMP trafic. Si vous ne parvenez pas à envoyer un ping à votre instance, assurez-vous que les règles de votre groupe de sécurité entrant autorisent le ICMP trafic provenant `Echo Request` de toutes les sources, ou de l'ordinateur ou de l'instance à partir duquel vous émettez la commande.

Si vous ne parvenez pas à émettre de `ping` commande depuis votre instance, assurez-vous que les règles de votre groupe de sécurité sortant autorisent le ICMP trafic du `Echo Request` message vers toutes les destinations ou vers l'hôte auquel vous essayez d'envoyer un ping.

Les commandes `Ping` peuvent également être bloquées par un pare-feu ou un délai d'attente en raison de latence réseau ou de problèmes matériels. Vous devez consulter votre réseau local ou votre administrateur système pour obtenir de l'aide sur la résolution des problèmes supplémentaires.

Erreur : le serveur a fermé la connexion réseau de manière inopinée

Si vous vous connectez à votre instance via Pu TTY et que vous recevez le message d'erreur « Le serveur a fermé la connexion réseau de manière inattendue », vérifiez que vous avez activé les keepalives sur la page de connexion de la TTY configuration Pu pour éviter d'être déconnecté. Certains serveurs déconnectent les clients lorsqu'ils n'ont pas reçu de données dans une période de temps spécifiée. Réglez les secondes entre keepalives à 59 secondes.

Si vous rencontrez toujours des problèmes après avoir activé keepalives, essayez de désactiver l'algorithme de Nagle sur la page de connexion de la configuration Pu. TTY

Erreur : échec de la validation de la clé d'hôte pour EC2 Instance Connect

Si vous faites pivoter les clés d'hôte de votre instance, les nouvelles clés d'hôte ne sont pas automatiquement téléchargées dans la base de données de clés d'hôte AWS fiables. Cela entraîne l'échec de la validation de la clé d'hôte lorsque vous essayez de vous connecter à votre instance à l'aide du client basé sur le navigateur EC2 Instance Connect, et vous ne parvenez pas à vous connecter à votre instance.

Pour résoudre l'erreur, vous devez exécuter le `eic_harvest_hostkeys` script sur votre instance, qui télécharge votre nouvelle clé d'hôte sur EC2 Instance Connect. Le script se trouve sur `/opt/aws/bin/` sur les instances Amazon Linux 2 et sur `/usr/share/ec2-instance-connect/` sur les instances Ubuntu.

Amazon Linux 2

Pour résoudre l'erreur de validation de clé d'hôte ayant échoué sur une instance Amazon Linux 2

1. Connectez-vous à votre instance à l'aide deSSH.

   Vous pouvez vous connecter à l'aide d'EC2Instance Connect CLI ou à l'aide de la paire de SSH clés attribuée à votre instance lorsque vous l'avez lancée et du nom d'utilisateur par défaut AMI que vous avez utilisé pour lancer votre instance. Pour Amazon Linux 2, le nom d'utilisateur par défaut est`ec2-user`.

   Par exemple, si votre instance a été lancée à l'aide d'Amazon Linux 2, le DNS nom public de votre instance est`ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, et la paire de clés est`my_ec2_private_key.pem`, utilisez la commande suivante pour SSH accéder à votre instance :

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Pour plus d'informations sur la connexion à votre instance, consultez Connectez-vous à votre instance Linux à l'aide d'un SSH client.

2. Accédez au dossier suivant.

```
[ec2-user ~]$ cd /opt/aws/bin/
```

3. Exécutez la commande suivante sur votre instance.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Notez qu'un appel réussi n'entraîne pas obligatoirement une sortie.

Vous pouvez désormais utiliser le client basé sur le navigateur EC2 Instance Connect pour vous connecter à votre instance.

Ubuntu

Pour résoudre l'erreur de validation de clé d'hôte ayant échoué sur une instance Ubuntu

1. Connectez-vous à votre instance à l'aide deSSH.

   Vous pouvez vous connecter à l'aide d'EC2Instance Connect CLI ou à l'aide de la paire de SSH clés attribuée à votre instance lorsque vous l'avez lancée et du nom d'utilisateur par défaut AMI que vous avez utilisé pour lancer votre instance. Pour Ubuntu, le nom d'utilisateur par défaut est`ubuntu`.

   Par exemple, si votre instance a été lancée avec Ubuntu, le DNS nom public de votre instance est`ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, et la paire de clés est`my_ec2_private_key.pem`, utilisez la commande suivante pour accéder à SSH votre instance :

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Pour plus d'informations sur la connexion à votre instance, consultez Connectez-vous à votre instance Linux à l'aide d'un SSH client.

2. Accédez au dossier suivant.

```
[ec2-user ~]$ cd /usr/share/ec2-instance-connect/
```

3. Exécutez la commande suivante sur votre instance.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Notez qu'un appel réussi n'entraîne pas obligatoirement une sortie.

Vous pouvez désormais utiliser le client basé sur le navigateur EC2 Instance Connect pour vous connecter à votre instance.

Impossible de se connecter à une instance Ubuntu à l'aide d'EC2Instance Connect

Si vous utilisez EC2 Instance Connect pour vous connecter à votre instance Ubuntu et qu'une erreur s'affiche lorsque vous tentez de vous connecter, vous pouvez utiliser les informations suivantes pour tenter de résoudre le problème.

Cause possible

Le package `ec2-instance-connect` sur l'instance n'est pas la dernière version.

Solution

Mettre à jour le package `ec2-instance-connect` sur l'instance vers la dernière version, comme suit :

1. Connectez-vous à votre instance à l'aide d'une méthode autre qu'EC2Instance Connect.
2. Exécuter la commande suivante sur votre instance pour mettre à jour le package `ec2-instance-connect` vers la dernière version.

```
apt update && apt upgrade
```

J'ai perdu ma clé privée. Comment puis-je me connecter à mon instance ?

Si vous perdez la clé privée d'une instance EBS sauvegardée, vous pouvez à nouveau accéder à votre instance. Vous devez arrêter l'instance, détacher son volume racine et l'attacher à une autre instance en tant que volume de données, modifier le fichier `authorized_keys` avec une nouvelle clé publique, replacer le volume dans l'instance d'origine et redémarrer l'instance. Pour plus d'informations sur le lancement et l'arrêt des instances, ainsi que sur la connexion aux instances, consultez Modifications de l'état de l'EC2instance Amazon.

Cette procédure n'est prise en charge que pour les instances avec des volumes EBS racine. Si l'appareil racine est un volume de stockage d'instance, vous ne pouvez pas utiliser cette procédure pour rétablir l'accès à votre instance ; vous devez disposer de la clé privée pour vous connecter à l'instance. Pour déterminer le type de périphérique racine de votre instance, ouvrez la EC2 console Amazon, choisissez Instances, sélectionnez l'instance, choisissez l'onglet Stockage et, dans la section Détails du périphérique racine, vérifiez la valeur du type d'appareil racine.

La valeur est `EBS` ou `INSTANCE-STORE`.

En plus des étapes suivantes, il existe d'autres façons de vous connecter à votre instance Linux en cas de perte de votre clé privée. Pour plus d'informations, consultez Comment puis-je me connecter à mon EC2 instance Amazon si j'ai perdu ma paire de SSH clés après son lancement initial ?

Étapes de connexion à une instance EBS basée sur -back avec une paire de clés différente

- Étape 1 : Créer une nouvelle paire de clés
- Étape 2 : Obtenir des informations sur l'instance d'origine et son volume racine
- Étape 3 : Arrêter l'instance d'origine
- Étape 4 : Lancer une instance temporaire
- Étape 5 : Détacher le volume racine de l'instance d'origine et l'attacher à l'instance temporaire
- Étape 6 : Ajouter la nouvelle clé publique authorized_keys sur le volume d'origine monté sur l'instance temporaire
- Étape 7 : Démonter et détacher le volume d'origine de l'instance temporaire, puis le reconnecter à l'instance d'origine
- Étape 8 : Se connecter à l'instance d'origine à l'aide de la nouvelle paire de clés
- Étape 9 : nettoyer

Étape 1 : Créer une nouvelle paire de clés

Créez une nouvelle paire de clés à l'aide de la EC2 console Amazon ou d'un outil tiers. Si vous souhaitez nommer votre nouvelle paire de clés exactement comme la clé privée perdue, vous devez commencer par supprimer la paire de clés existante. Pour de plus amples informations sur la création d'une paire de clés, veuillez consulter Créez une paire de clés à l'aide d'Amazon EC2 ou Créez une paire de clés à l'aide d'un outil tiers et importez la clé publique sur Amazon EC2.

Étape 2 : Obtenir des informations sur l'instance d'origine et son volume racine

Notez les informations suivantes, car vous en aurez besoin pour effectuer cette procédure.

Pour obtenir des informations sur votre instance d'origine

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Choisissez Instances dans le panneau de navigation, puis sélectionnez l'instance à laquelle vous souhaitez vous connecter. (Cette instance est qualifiée d'instance d'origine.)
3. Dans l'onglet Détails, notez l'ID et AMI l'ID de l'instance.
4. Sous l'onglet Networking (Réseaux), notez la zone de disponibilité.
5. Sous l'onglet Storage (Stockage), sous Root device name (Nom du périphérique racine), notez le nom du périphérique pour le volume racine (par exemple, `/dev/xvda`). Ensuite, sous Block devices (Bloquer les périphériques), recherchez le nom du périphérique et notez l'ID de volume (par exemple, vol-0a1234b5678c910de).

Étape 3 : Arrêter l'instance d'origine

Choisissez État de l'instance, Arrêter l'instance. Si cette option est désactivée, l'instance est déjà arrêtée ou son périphérique racine est un volume de stockage d'instance.

> **Warning**
>
> Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instance sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

Étape 4 : Lancer une instance temporaire

Pour lancer une instance temporaire

1. Dans le volet de navigation, choisissez Instances, puis Launch instances (Lancer des instances).
2. Dans la section Name and tags (Noms et identifications), pour Name (Nom), saisissez Temporary (Temporaire).
3. Dans la section Images de l'application et du système d'exploitation, sélectionnez celle AMI que vous avez utilisée pour lancer l'instance d'origine. S'il n'AMIest pas disponible, vous pouvez en créer un AMI que vous pouvez utiliser à partir de l'instance arrêtée. Pour de plus amples informations, veuillez consulter Créez un compte soutenu EBS par Amazon AMI.
4. Dans la section Instance type (Type d'instance), sélectionnez le type d'instance par défaut.
5. Dans la section Key pair (Paire de clés), pour Key pair name (Nom de la paire de clés), sélectionnez une paire de clés existante ou créez-en une.
6. Dans la section Network settings (Paramètres réseau), choisissez Edit (Modifier), puis pour Subnet (Sous-réseau), sélectionnez un sous-réseau dans la même zone de disponibilité que celle de l'instance d'origine.
7. Dans le panneau Summary (Récapitulatif), choisissez Launch (Lancer).

Étape 5 : Détacher le volume racine de l'instance d'origine et l'attacher à l'instance temporaire

1. Dans le panneau de navigation, sélectionnez Volumes, puis le volume du périphérique racine pour l'instance d'origine (vous avez noté l'ID de volume au cours d'une étape précédente). Choisissez Actions, Detach Volume (Détacher un volume), puis choisissez Detach (Détacher). Attendez que l'état du volume devienne `available`. (Vous devrez peut-être sélectionner l'icône Actualiser.)
2. Tandis que le volume est toujours sélectionné, choisissez Actions, puis choisissez Attach volume (Attacher un volume). Sélectionnez l'ID d'instance de l'instance temporaire, notez le nom du périphérique spécifié dans Device name (Nom du périphérique) (par exemple, `/dev/sdf`), puis sélectionnez Attach volume (Attacher un volume).

> **Note**
>
> Si vous avez lancé votre instance d'origine à partir d'un AWS Marketplace AMI et que votre volume contient des AWS Marketplace codes, vous devez d'abord arrêter l'instance temporaire avant de pouvoir attacher le volume.

Étape 6 : Ajouter la nouvelle clé publique **authorized_keys** sur le volume d'origine monté sur l'instance temporaire

1. Connectez-vous à l'instance temporaire.
2. À partir de l'instance temporaire, montez le volume que vous avez attaché à l'instance afin de pouvoir accéder au système de fichiers. Par exemple, si le nom du périphérique est `/dev/sdf`, utilisez les commandes suivantes pour monter le volume en tant que `/mnt/tempvol`.

   > **Note**
   >
   > Le nom du périphérique peut apparaître différemment sur votre instance. Par exemple, les périphériques montés en tant que `/dev/sdf` peuvent également s'afficher en tant que `/dev/xvdf` sur l'instance. Certaines versions de Red Hat (ou ses variantes, comme CentOS) peuvent même incrémenter la lettre finale de quatre caractères, et `/dev/sdf` devient `/dev/xvdk`.

   a. Utilisez la commande lsblk pour déterminer si le volume est divisé.

   ```
   [ec2-user ~]$ lsblk
   NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
   xvda    202:0    0    8G  0 disk
   ##xvda1 202:1    0    8G  0 part /
   xvdf    202:80   0  101G  0 disk
   ##xvdf1 202:81   0  101G  0 part
   xvdg    202:96   0   30G  0 disk
   ```

   Dans l'exemple précédent, `/dev/xvda` et `/dev/xvdf` sont des volumes partitionnés, mais `/dev/xvdg` ne l'est pas. Si votre volume est partitionné, vous montez la partition (`/dev/xvdf1`)) au lieu du périphérique brut (`/dev/xvdf`) au cours des étapes suivantes.

b. Créez un répertoire temporaire pour monter le volume.

```
[ec2-user ~]$ sudo mkdir /mnt/tempvol
```

c. Montez le volume (ou la partition) sur le point de montage temporaire, en utilisant le nom du volume ou du périphérique que vous avez identifié plus tôt. La commande requise dépend du système de fichiers de votre système d'exploitation. Notez que le nom du périphérique peut apparaître différemment sur votre instance. Reportez-vous à l'étape 6 de note pour plus d'informations.

- Amazon Linux, Ubuntu et Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

- Amazon Linux 2, CentOS, SUSE Linux 12 et 7.x RHEL

```
[ec2-user ~]$ sudo mount -o nouuid /dev/xvdf1 /mnt/tempvol
```

> **Note**
>
> Si vous obtenez une erreur indiquant que le système de fichiers est endommagé, exécutez la commande suivante pour utiliser l'utilitaire fsck afin de rechercher les erreurs dans votre système de fichiers et de les résoudre.
>
> ```
> [ec2-user ~]$ sudo fsck /dev/xvdf1
> ```

3. À partir de l'instance temporaire, utilisez la commande suivante pour mettre à jour `authorized_keys` sur le volume monté avec la nouvelle clé publique de `authorized_keys` pour l'instance temporaire.

> **Important**
>
> Les exemples suivants utilisent le nom d'utilisateur Amazon Linux`ec2-user`. Il se peut que vous deviez remplacer un nom d'utilisateur différent, par exemple `ubuntu` pour les instances Ubuntu.

```
[ec2-user ~]$ cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Une fois que cette étape est correctement effectuée, vous pouvez passer à l'étape suivante.

(Facultatif) Sinon, si vous n'êtes pas autorisé à modifier des fichiers dans `/mnt/tempvol`, vous devez mettre à jour le fichier à l'aide de la commande sudo, puis vérifier les autorisations sur le fichier afin de vous assurer que vous êtes en mesure de vous connecter à l'instance d'origine. Pour vérifier les autorisations sur le fichier, utilisez la commande suivante.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
total 4
-rw------- 1 222 500 398 Sep 13 22:54 authorized_keys
```

Dans cet exemple de sortie, *222* est le nom d'utilisateur et *500* est l'identifiant du groupe. Utilisez ensuite la commande sudo pour ré-exécuter la commande copy ayant échoué.

```
[ec2-user ~]$ sudo cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Exécutez à nouveau la commande suivante pour déterminer si les autorisations ont été modifiées.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

Si l'ID d'utilisateur et l'ID de groupe ont été modifiés, utilisez la commande suivante pour les restaurer.

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

Étape 7 : Démonter et détacher le volume d'origine de l'instance temporaire, puis le reconnecter à l'instance d'origine

1. À partir de l'instance temporaire, démontez le volume que vous avez attaché afin de pouvoir l'attacher à nouveau à l'instance d'origine. Par exemple, utilisez la commande suivante pour démonter le volume situé dans `/mnt/tempvol`.

   ```
   [ec2-user ~]$ sudo umount /mnt/tempvol
   ```

2. Détachez le volume de l'instance temporaire (vous l'avez démonté à l'étape précédente) : depuis la EC2 console Amazon, choisissez Volumes dans le volet de navigation, sélectionnez le volume du périphérique racine pour l'instance d'origine (vous avez pris note de l'ID du volume à l'étape précédente), choisissez Actions, Détacher le volume, puis choisissez Détacher. Attendez que l'état du volume devienne `available`. (Vous devrez peut-être sélectionner l'icône Actualiser.)
3. Rattachez le volume à l'instance d'origine : le volume étant toujours sélectionné, choisissez Actions, Attach volume (Attacher un volume). Sélectionnez l'ID d'instance de l'instance d'origine, précisez le nom de l'appareil que vous avez noté précédemment au cours de l'étape 2 pour l'attachement de l'appareil racine d'origine (`/dev/sda1` ou `/dev/xvda`), puis choisissez Attach volume (Attacher un volume).

   > **Important**
   >
   > Si vous ne spécifiez pas le même nom de périphérique que pour l'attachement original, vous ne pourrez pas démarrer l'instance d'origine. Amazon EC2 s'attend à ce que le volume du périphérique racine `sda1` soit égal à ou`/dev/xvda`.

Étape 8 : Se connecter à l'instance d'origine à l'aide de la nouvelle paire de clés

Sélectionnez l'instance d'origine, choisissez État de l'instance, Démarrer l'instance. Lorsque l'état de l'instance est `running`, vous pouvez vous y connecter à l'aide du fichier de clé privée de votre nouvelle paire de clés.

> **Note**
>
> Si le nom de votre paire de clés et du fichier de clé privée correspondant est différent du nom de la paire de clés initiale, veillez à spécifier le nom du nouveau fichier de clé privée lorsque vous vous connectez à votre instance.

Étape 9 : nettoyer

(Facultatif) Vous pouvez mettre fin à l'instance temporaire si vous n'en avez plus besoin. Sélectionnez l'instance temporaire, puis choisissez État de l'instance, Terminer (supprimer) l'instance.

Résoudre les problèmes des instances Amazon EC2 Linux dont les vérifications d'état ont échoué

Les informations suivantes peuvent vous aider à résoudre les problèmes si la vérification de statut de votre instance Linux échoue. Commencez par déterminer si vos applications présentent des problèmes. Si vous constatez que l'instance n'exécute pas vos applications comme prévu, passez en revue les informations de contrôle de statut et les journaux système.

Pour des exemples de problèmes pouvant entraîner l'échec des vérifications d'état, consultez Contrôles de statut pour les EC2 instances Amazon.

Sommaire

- « FATAL : Impossible de charger /lib/modules" ou "BusyBox" (modules de noyau manquants)
- ERRORNoyau non valide (noyau EC2 incompatible)
- fsck : aucun fichier ou répertoire de ce type lors de la tentative d'ouverture... (système de fichiers non trouvé)
- General error mounting filesystems (Montage en échec)
- VFS: Impossible de monter le fichier root fs sur un bloc inconnu (incompatibilité du système de fichiers racine)
- Erreur : Unable to determine major/minor number of root device... (décalage du système de fichiers/périphérique racine)
- XENBUS: Appareil sans pilote...
- ... days without being checked, check forced (Contrôle du système de fichiers nécessaire)
- fsck a échoué à l'état de sortie... (périphérique manquant)
- GRUBprompt (grubdom>)
- Affichage de l'interface eth0 : le périphérique eth0 a une MAC adresse différente de celle attendue, ignorée. (MACAdresse codée en dur)
- Impossible de charger la SELinux politique. L'appareil est en mode d'exécution. Arrêt maintenant. (SELinuxmauvaise configuration)
- XENBUS: délai de connexion aux appareils (délai d'expiration Xenbus)

Examen des informations de contrôle de statut

Pour étudier les instances défectueuses à l'aide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez instances, puis sélectionnez votre instance.
3. Sélectionnez l'onglet État et alarmes pour voir les résultats individuels de toutes les vérifications d'état du système, des vérifications de l'état des instances et des vérifications de EBSstatut des pièces jointes.

Si la vérification du statut a échoué, vous pouvez essayer l'une des options suivantes :

- Créez une alarme pour récupérer l'instance en réponse à l'échec de la vérification de statut. Pour de plus amples informations, veuillez consulter Créer des alarmes qui arrêtent, finissent, redémarrent ou récupèrent une instance.

- (Vérifications de l'état de l'instance) Si vous avez changé le type d'instance pour une instance basée sur le système AWS Nitro, les vérifications de statut échouent si vous avez migré depuis une instance qui ne possède pas les pilotes ENA et NVMe pilotes requis. Pour de plus amples informations, veuillez consulter Compatibilité pour modifier le type d'instance.
- Pour une instance EBS sauvegardée, arrêtez et redémarrez l'instance. Pour de plus amples informations, veuillez consulter Arrêtez et démarrez les EC2 instances Amazon.
- Pour une instance basée sur un magasin d'instances, mettez fin à l'instance et lancez une instance de remplacement. Pour de plus amples informations, veuillez consulter Mettre fin aux EC2 instances Amazon.
- Attendez qu'Amazon EC2 résolve le problème.
- Contactez AWS Support ou publiez votre problème sur AWS Re:post.
- Si votre instance fait partie d'un groupe Auto Scaling :
  - (Vérifications de l'état du système et vérifications de l'état des instances) Par défaut, Amazon EC2 Auto Scaling lance automatiquement une instance de remplacement. Pour plus d'informations, consultez Health Checks for Auto Scaling Instances dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.
  - (Vérifications de EBS statut jointes) Vous devez configurer Amazon EC2 Auto Scaling pour lancer automatiquement une instance de remplacement. Pour plus d'informations, consultez la section Surveiller et remplacer les instances Auto Scaling par des EBS volumes Amazon altérés dans le manuel Amazon EC2 Auto Scaling User Guide.
- Récupérez le journal du système et recherchez les erreurs. Pour de plus amples informations, veuillez consulter Récupération des journaux système.

Récupération des journaux système

Si un contrôle de statut d'instance échoue, vous pouvez relancer l'instance et récupérer les journaux du système. Les journaux peuvent révéler une erreur que peut vous aider à résoudre le problème. Le redémarrage efface les informations inutiles des journaux.

Pour redémarrer une instance et récupérer le journal du système

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez instances, puis choisissez votre instance.
3. Sélectionnez État de l'instance, puis Redémarrer l'instance. Le redémarrage de votre instance peut prendre quelques minutes.

4. Vérifiez si le problème existe encore. Dans certains cas, le redémarrage peut résoudre le problème.
5. Lorsque l'état de l'instance est `running`, sélectionnez Actions, Surveiller et dépanner, Obtenir le journal système.
6. Consultez le journal qui apparaît à l'écran et utilisez la liste ci-dessous des déclarations d'erreurs connues du journal du système afin de résoudre votre problème.
7. Si votre problème n'est pas résolu, vous pouvez le publier sur AWS re:Post.

Résoudre les erreurs du journal système pour les instances Linux

Pour les instances Linux qui ont échoué à une vérification de l'état de l'instance, telle que la vérification de l'accessibilité de l'instance, vérifiez que vous avez suivi les étapes ci-dessus pour récupérer le journal système. La liste suivante contient certaines erreurs communes du journal du système et les actions suggérées que vous pouvez prendre pour résoudre le problème correspondant à chaque erreur.

Memory Errors

- Mémoire insuffisante : processus d'arrêt
- ERROR: échec de mmu_update (échec de la mise à jour de la gestion de la mémoire)

Device Errors

- Erreur d'E/S (échec du périphérique de stockage en mode bloc)
- E/S ERROR : ni disque local ni disque distant (périphérique à blocs distribués cassé)

Kernel Errors

- request_module: runaway loop modprobe (modprobe en boucle sur le noyau hérité sur des versions Linux plus anciennes)
- « FATAL : kernel too old » et « fsck : aucun fichier ou répertoire de ce type lors de la tentative d'ouverture de /dev » (Kernel et incompatibilité) AMI
- « FATAL : Impossible de charger /lib/modules" ou "BusyBox" (modules de noyau manquants)
- ERRORNoyau non valide (noyau EC2 incompatible)

File System Errors

- fsck : aucun fichier ou répertoire de ce type lors de la tentative d'ouverture... (système de fichiers non trouvé)
- General error mounting filesystems (Montage en échec)
- VFS: Impossible de monter le fichier root fs sur un bloc inconnu (incompatibilité du système de fichiers racine)
- Erreur : Unable to determine major/minor number of root device... (décalage du système de fichiers/périphérique racine)
- XENBUS: Appareil sans pilote...
- ... days without being checked, check forced (Contrôle du système de fichiers nécessaire)
- fsck a échoué à l'état de sortie... (périphérique manquant)

Operating System Errors

- GRUBprompt (grubdom>)
- Affichage de l'interface eth0 : le périphérique eth0 a une MAC adresse différente de celle attendue, ignorée. (MACAdresse codée en dur)
- Impossible de charger la SELinux politique. L'appareil est en mode d'exécution. Arrêt maintenant. (SELinuxmauvaise configuration)
- XENBUS: délai de connexion aux appareils (délai d'expiration Xenbus)

Mémoire insuffisante : processus d'arrêt

Une out-of-memory erreur est indiquée par une entrée du journal système similaire à celle illustrée ci-dessous.

```
[115879.769795] Out of memory: kill process 20273 (httpd) score 1285879
or a child
[115879.769795] Killed process 1917 (php-cgi) vsz:467184kB, anon-
rss:101196kB, file-rss:204kB
```

Cause potentielle

Mémoire épuisée

Actions suggérées

Pour ce type d'instance	Faites ceci
Soutenu EBS par Amazon	Effectuez l'une des actions suivantes : • Arrêtez l'instance et modifiez l'instance pour utiliser un type d'instance différent, puis relancez l'instance. Par exemple, un type d'instance plus importante ou optimisée pour la mémoire. • Redémarrez l'instance pour la renvoyer vers un statut non-défaillant. Le problème se reproduira probablement à moins que vous ne changiez de type d'instance.
Basée sur le stockage d'instance	Effectuez l'une des actions suivantes : • Arrêtez l'instance et lancez une nouvelle instance en spécifiant un type d'instance différent. Par exemple, un type d'instanc e plus importante ou optimisée pour la mémoire. • Redémarrez l'instance pour la renvoyer vers un statut non-défaillant. Le problème se reproduira probablement à moins que vous ne changiez de type d'instance.

ERROR: échec de mmu_update (échec de la mise à jour de la gestion de la mémoire)

Les échecs de la mise à jour de la gestion de la mémoire sont indiqués par une entrée du journal du système qui est similaire à ce qui suit :

```
...
Press `ESC' to enter the menu... 0   [H[J  Booting 'Amazon Linux 2011.09
 (2.6.35.14-95.38.amzn1.i686)'
```

```
root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /boot/vmlinuz-2.6.35.14-95.38.amzn1.i686 root=LABEL=/ console=hvc0 LANG=

en_US.UTF-8 KEYTABLE=us

initrd /boot/initramfs-2.6.35.14-95.38.amzn1.i686.img

ERROR: mmu_update failed with rc=-22
```

Cause potentielle

Problème avec Amazon Linux

Action suggérée

Publiez votre problème sur Forums dédiés aux développeurs ou contactez AWS Support.

Erreur d'E/S (échec du périphérique de stockage en mode bloc)

Une erreur d'entrée/sortie est indiquée par une entrée du journal du système qui est similaire à l'exemple suivant :

```
[9943662.053217] end_request: I/O error, dev sde, sector 52428288
[9943664.191262] end_request: I/O error, dev sde, sector 52428168
[9943664.191285] Buffer I/O error on device md0, logical block 209713024
[9943664.191297] Buffer I/O error on device md0, logical block 209713025
[9943664.191304] Buffer I/O error on device md0, logical block 209713026
[9943664.191310] Buffer I/O error on device md0, logical block 209713027
[9943664.191317] Buffer I/O error on device md0, logical block 209713028
[9943664.191324] Buffer I/O error on device md0, logical block 209713029
[9943664.191332] Buffer I/O error on device md0, logical block 209713030
[9943664.191339] Buffer I/O error on device md0, logical block 209713031
[9943664.191581] end_request: I/O error, dev sde, sector 52428280
[9943664.191590] Buffer I/O error on device md0, logical block 209713136
[9943664.191597] Buffer I/O error on device md0, logical block 209713137
[9943664.191767] end_request: I/O error, dev sde, sector 52428288
[9943664.191970] end_request: I/O error, dev sde, sector 52428288
```

```
[9943664.192143] end_request: I/O error, dev sde, sector 52428288
[9943664.192949] end_request: I/O error, dev sde, sector 52428288
[9943664.193112] end_request: I/O error, dev sde, sector 52428288
[9943664.193266] end_request: I/O error, dev sde, sector 52428288
...
```

Causes potentielles

Type d'instance	Cause potentielle
Soutenu EBS par Amazon	Un EBS volume Amazon défaillant
Basée sur le stockage d'instance	Un lecteur physique en échec

Actions suggérées

Pour ce type d'instance	Faites ceci
Soutenu EBS par Amazon	Utilisez la procédure suivante. 1. Arrêtez l'instance. 2. Dissociez le volume. 3. Essayez de récupérer le volume. **Note** Il est recommandé de prendre régulièrement des photos de vos EBS volumes Amazon. Cela diminue considérablement le risque de perte de données suite à un échec. 4. Attachez de nouveau le volume à l'instance. 5. Démarrez l'instance.
Basée sur le stockage d'instance	Mettez fin à l'instance et lancez une nouvelle instance.

Pour ce type d'instance	Faites ceci
	Note Les données ne peuvent pas être récupérées. Récupérez-les grâce aux sauvegardes.
	Note Il est recommandé d'utiliser Amazon S3 ou Amazon EBS pour les sauvegard es. Les volumes de stockage d'instance sont directement reliés aux échecs d'un hôte et d'un disque uniques.

E/S ERROR : ni disque local ni disque distant (périphérique à blocs distribués cassé)

Une erreur d'entrée/sortie sur le périphérique est indiquée par une entrée du journal du système qui est similaire à l'exemple suivant :

```
...
block drbd1: Local IO failed in request_timer_fn. Detaching...

Aborting journal on device drbd1-8.

block drbd1: IO ERROR: neither local nor remote disk

Buffer I/O error on device drbd1, logical block 557056

lost page write due to I/O error on drbd1

JBD2: I/O error detected when updating journal superblock for drbd1-8.
```

Causes potentielles

Type d'instance	Cause potentielle
Soutenu EBS par Amazon	Un EBS volume Amazon défaillant
Basée sur le stockage d'instance	Un lecteur physique en échec

Action suggérée

Mettez fin à l'instance et lancez une nouvelle instance.

Pour une instance basée sur AmazonEBS, vous pouvez récupérer les données d'un instantané récent en créant une image à partir de celui-ci. Toutes les données ajoutées après l'instantané ne peuvent pas être récupérées.

request_module: runaway loop modprobe (modprobe en boucle sur le noyau hérité sur des versions Linux plus anciennes)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous. L'utilisation d'un noyau Linux instable ou ancien (par exemple, 2.6.16-xenU) peut entraîner une condition de boucle interminable au démarrage.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007

BIOS-provided physical RAM map:

 Xen: 0000000000000000 - 0000000026700000 (usable)

0MB HIGHMEM available.
...

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c
```

```
request_module: runaway loop modprobe binfmt-464c
```

Actions suggérées

Pour ce type d'instance	Faites ceci
Soutenu EBS par Amazon	Utilisez un noyau plus récent, GRUB basé ou statique, en utilisant l'une des options suivantes : Option 1 : Arrêtez l'instance et lancez une nouvelle instance en spécifiant les paramètres `-kernel` et `-ramdisk`. Option 2 : 1. Arrêtez l'instance. 2. Modifiez les attributs de noyau et de ramdisk pour utiliser un noyau plus récent. 3. Démarrez l'instance.
Basée sur le stockage d'instance	Arrêtez l'instance et lancez une nouvelle instance en spécifiant les paramètres `-kernel` et `-ramdisk`.

« FATAL : kernel too old » et « fsck : aucun fichier ou répertoire de ce type lors de la tentative d'ouverture de /dev » (Kernel et incompatibilité) AMI

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
Linux version 2.6.16.33-xenU (root@dom0-0-50-45-1-a4-ee.z-2.aes0.internal)
(gcc version 4.1.1 20070105 (Red Hat 4.1.1-52)) #2 SMP Wed Aug 15 17:27:36 SAST 2007
...
FATAL: kernel too old
Kernel panic - not syncing: Attempted to kill init!
```

Causes potentielles

Noyau et identifiant incompatibles

Actions suggérées

Pour ce type d'instance	Faites ceci
Soutenu EBS par Amazon	Utilisez la procédure suivante. 1. Arrêtez l'instance. 2. Modifiez la configuration pour utiliser un noyau plus récent. 3. Démarrez l'instance.
Basée sur le stockage d'instance	Utilisez la procédure suivante. 1. Créez un code AMI qui utilise un noyau plus récent. 2. Mettez fin à l'instance. 3. Démarrez une nouvelle instance à partir de celle AMI que vous avez créée.

« FATAL : Impossible de charger /lib/modules" ou "BusyBox" (modules de noyau manquants)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
[    0.370415] Freeing unused kernel memory: 1716k freed
Loading, please wait...
WARNING: Couldn't open directory /lib/modules/2.6.34-4-virtual: No such file or
 directory
FATAL: Could not open /lib/modules/2.6.34-4-virtual/modules.dep.temp for writing: No
 such file or directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
Couldn't get a file descriptor referring to the console
```

```
Begin: Loading essential drivers... ...
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
Done.
Begin: Running /scripts/init-premount ...
Done.
Begin: Mounting root file system... ...
Begin: Running /scripts/local-top ...
Done.
Begin: Waiting for root file system... ...
Done.
Gave up waiting for root device.  Common problems:
 - Boot args (cat /proc/cmdline)
   - Check rootdelay= (did the system wait long enough?)
   - Check root= (did the system wait for the right device?)
 - Missing modules (cat /proc/modules; ls /dev)
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
ALERT! /dev/sda1 does not exist. Dropping to a shell!


BusyBox v1.13.3 (Ubuntu 1:1.13.3-1ubuntu5) built-in shell (ash)
Enter 'help' for a list of built-in commands.

(initramfs)
```

Causes potentielles

Une ou plusieurs conditions suivantes peuvent entraîner ce problème :

- Ramdisk manquant
- Modules corrects manquants pour le ramdisk
- Le volume EBS racine Amazon n'est pas correctement attaché en tant que `/dev/sda1`

Actions suggérées

Pour ce type d'instance	Faites ceci
Soutenu EBS par Amazon	Utilisez la procédure suivante. 1. Sélectionnez le ramdisk corrigé pour le EBS volume Amazon. 2. Arrêtez l'instance. 3. Détachez le volume et réparez-le. 4. Attachez le volume à l'instance. 5. Démarrez l'instance. 6. Modifiez le AMI pour utiliser le ramdisk corrigé.
Basée sur le stockage d'instance	Utilisez la procédure suivante. 1. Arrêtez l'instance et lancez une nouvelle instance avec le bon ramdisk. 2. Créez-en un nouveau AMI avec le bon ramdisk.

ERRORNoyau non valide (noyau EC2 incompatible)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
...
root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz root=/dev/sda1 ro

initrd /initrd.img

ERROR Invalid kernel: elf_xen_note_check: ERROR: Will only load images
built for the generic loader or Linux images
```

```
xc_dom_parse_image returned -1

Error 9: Unknown boot failure

  Booting 'Fallback'

root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz.old root=/dev/sda1 ro

Error 15: File not found
```

Causes potentielles

Une ou deux des conditions suivantes peuvent entraîner ce problème :

- Le noyau fourni n'est pas pris en charge par GRUB
- Le noyau de rechange n'existe pas

Actions suggérées

Pour ce type d'instance	Faites ceci
Soutenu EBS par Amazon	Utilisez la procédure suivante. 1. Arrêtez l'instance. 2. Remplacez-le avec un noyau qui fonctionne. 3. Installez un noyau de rechange. 4. Modifiez le AMI en corrigeant le noyau.
Basée sur le stockage d'instance	Utilisez la procédure suivante. 1. Arrêtez l'instance et lancez une nouvelle instance avec le bon noyau. 2. Créez un AMI avec le bon noyau.

Pour ce type d'instance	Faites ceci
	3. (Facultatif) Demandez une assistance technique pour la récupération des données en utilisant AWS Support.

fsck : aucun fichier ou répertoire de ce type lors de la tentative d'ouverture... (système de fichiers non trouvé)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
  Welcome to Fedora
  Press 'I' to enter interactive startup.
Setting clock : Wed Oct 26 05:52:05 EDT 2011 [  OK  ]

Starting udev: [  OK  ]

Setting hostname localhost:  [  OK  ]

No devices found
Setting up Logical Volume Management: File descriptor 7 left open
  No volume groups found
[  OK  ]

Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1: clean, 82081/1310720 files, 2141116/2621440 blocks
[/sbin/fsck.ext3 (1) -- /mnt/dbbackups] fsck.ext3 -a /dev/sdh
fsck.ext3: No such file or directory while trying to open /dev/sdh

/dev/sdh:
The superblock could not be read or does not describe a correct ext2
filesystem.  If the device is valid and it really contains an ext2
filesystem (and not swap or ufs or something else), then the superblock
is corrupt, and you might try running e2fsck with an alternate superblock:
    e2fsck -b 8193 <device>

[FAILED]
```

```
*** An error occurred during the file system check.
*** Dropping you to a shell; the system will reboot
*** when you leave the shell.
Give root password for maintenance
(or type Control-D to continue):
```

Causes potentielles

- Un bogue existe dans les définitions du système de fichiers ramdisk /etc/fstab
- Définitions du système de fichiers mal configurées dans /etc/fstab
- Lecteur manquant/en échec

Actions suggérées

Pour ce type d'instance	Faites ceci
Soutenu EBS par Amazon	Utilisez la procédure suivante. 1. Arrêtez l'instance, détachez le volume racine, réparez/modifiez le volume dans le fichier /etc/fstab, attachez le volume à l'instance et lancez l'instance. 2. Corrigez le ramdisk pour inclure le fichier /etc/fstab modifié (le cas échéant). 3. Modifiez le AMI pour utiliser un disque RAM plus récent. Le sixième champ de fstab définit les exigences de disponibilité du montage. Une valeur non nulle implique qu'un fsck sera effectué sur ce volume et doit réussir. L'utilisation de ce champ peut s'avérer problématique sur Amazon, EC2 car une défaillance entraîne généralement l'affichage d'une invite de console interacti ve qui n'est actuellement pas disponible sur AmazonEC2. Faites attention avec cette

Pour ce type d'instance	Faites ceci
	fonction et lisez la page sur la commande man Linux en ce qui concerne fstab.
Basée sur le stockage d'instance	Utilisez la procédure suivante. 1. Mettez fin à l'instance et lancez une nouvelle instance. 2. Détachez tous les EBS volumes Amazon erronés et l'instance de redémarrage. 3. (Facultatif) Demandez une assistance technique pour la récupération des données en utilisant AWS Support.

General error mounting filesystems (Montage en échec)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
Loading xenblk.ko module
xen-vbd: registered block device major 8

Loading ehci-hcd.ko module
Loading ohci-hcd.ko module
Loading uhci-hcd.ko module
USB Universal Host Controller Interface driver v3.0

Loading mbcache.ko module
Loading jbd.ko module
Loading ext3.ko module
Creating root device.
Mounting root filesystem.
kjournald starting.  Commit interval 5 seconds

EXT3-fs: mounted filesystem with ordered data mode.

Setting up other filesystems.
Setting up new root fs
no fstab.sys, mounting internal defaults
```

```
Switching to new root and running init.
unmounting old /dev
unmounting old /proc
unmounting old /sys
mountall:/proc: unable to mount: Device or resource busy
mountall:/proc/self/mountinfo: No such file or directory
mountall: root filesystem isn't mounted
init: mountall main process (221) terminated with status 1

General error mounting filesystems.
A maintenance shell will now be started.
CONTROL-D will terminate this shell and re-try.
Press enter for maintenance
(or type Control-D to continue):
```

Causes potentielles

Type d'instance	Cause potentielle
Soutenu EBS par Amazon	• EBSVolume Amazon détaché ou défaillant. • Système de fichiers corrompu. • Ramdisk et AMI combinaison incompatibles (comme Debian ramdisk avec a). SUSE AMI
Basée sur le stockage d'instance	• Un lecteur en échec. • Un système de fichiers corrompu. • Un disque RAM et une combinaison incompatibles (par exemple, un disque RAM Debian avec un). SUSE AMI

Actions suggérées

Pour ce type d'instance	Faites ceci
Soutenu EBS par Amazon	Utilisez la procédure suivante. 1. Arrêtez l'instance.

Pour ce type d'instance	Faites ceci
	2. Détachez le volume racine. 3. Attachez le volume racine à une instance connue en fonctionnement. 4. Exécutez le contrôle du système de fichiers (fsck –a /dev/...). 5. Corrigez toutes les erreurs. 6. Détachez le volume de l'instance connue en fonctionnement. 7. Attachez le volume à l'instance arrêtée. 8. Démarrez l'instance. 9. Revérifiez le statut de l'instance.
Basée sur le stockage d'instance	Essayez l'une des actions suivantes : • Démarrez une nouvelle instance. • (Facultatif) Demandez une assistance technique pour la récupération des données en utilisant AWS Support.

VFS: Impossible de monter le fichier root fs sur un bloc inconnu (incompatibilité du système de fichiers racine)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
 20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
Kernel command line:  root=/dev/sda1 ro 4
...
Registering block device major 8
...
Kernel panic - not syncing: VFS: Unable to mount root fs on unknown-block(8,1)
```

Causes potentielles

Type d'instance	Cause potentielle
Soutenu EBS par Amazon	• Le périphérique n'est pas attaché correctem ent. • Le périphérique racine n'est pas attaché au bon point périphérique. • Le système de fichiers n'est pas au format attendu. • Utilisez le noyau hérité (par exemple, 2.6.16-XenU). • Mise à jour récente du noyau sur votre instance (mise à jour défaillante ou bogue de mise à jour)
Basée sur le stockage d'instance	Échec du périphérique matériel.

Actions suggérées

Pour ce type d'instance	Faites ceci
Soutenu EBS par Amazon	Effectuez l'une des actions suivantes : • Arrêtez puis redémarrez l'instance. • Modifiez le volume racine pour l'attacher au bon point périphérique, comme /dev/sda1 au lieu de /dev/sda. • Arrêtez et modifiez pour le noyau moderne. • Pour plus d'informations sur les bogues de mise à jour connus, consultez la documenta tion de votre distribution Linux. Modifiez ou réinstallez le noyau.

Pour ce type d'instance	Faites ceci
Basée sur le stockage d'instance	Arrêtez l'instance et lancez une nouvelle instance en utilisant un noyau moderne.

Erreur : Unable to determine major/minor number of root device... (décalage du système de fichiers/périphérique racine)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
...
XENBUS: Device with no driver: device/vif/0
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#
```

Causes potentielles

- Pilote du périphérique de stockage en mode bloc virtuel manquant ou configuré de façon incorrecte
- Conflit de l'énumération du périphérique (sda versus xvda ou sda au lieu de sda1)
- Choix incorrect du noyau de l'instance

Actions suggérées

Pour ce type d'instance	Faites ceci
Soutenu EBS par Amazon	Utilisez la procédure suivante. 1. Arrêtez l'instance. 2. Dissociez le volume. 3. Corrigez le problème du mappage du périphérique. 4. Démarrez l'instance. 5. Modifiez le AMI pour résoudre les problèmes de mappage des appareils.
Basée sur le stockage d'instance	Utilisez la procédure suivante. 1. Créez-en un nouveau AMI avec le correctif approprié (cartographiez correctement le périphérique). 2. Mettez fin à l'instance et lancez une nouvelle instance à partir de celle AMI que vous avez créée.

XENBUS: Appareil sans pilote...

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
```

```
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#
```

Causes potentielles

- Pilote du périphérique de stockage en mode bloc virtuel manquant ou configuré de façon incorrecte
- Conflit de l'énumération du périphérique (sda versus xvda)
- Choix incorrect du noyau de l'instance

Actions suggérées

Pour ce type d'instance	Faites ceci
Soutenu EBS par Amazon	Utilisez la procédure suivante. 1. Arrêtez l'instance. 2. Dissociez le volume. 3. Corrigez le problème du mappage du périphérique. 4. Démarrez l'instance. 5. Modifiez le AMI pour résoudre les problèmes de mappage des appareils.
Basée sur le stockage d'instance	Utilisez la procédure suivante. 1. Créez un AMI avec le correctif approprié (cartographiez correctement le périphérique). 2. Mettez fin à l'instance et lancez-en une nouvelle à l'aide de celle AMI que vous avez créée.

... days without being checked, check forced (Contrôle du système de fichiers nécessaire)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
...
Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1 has gone 361 days without being checked, check forced
```

Causes potentielles

La durée de contrôle du système de fichiers est dépassée ; un contrôle du système de fichiers est en train d'être forcé.

Actions suggérées

- Patientez jusqu'à ce que le contrôle du système de fichiers se termine. Un contrôle de système de fichiers peut prendre longtemps en fonction de la taille du système de fichiers racine.
- Modifiez vos systèmes de fichiers pour supprimer l'application du contrôle du système de fichiers (fsck) en utilisant tune2fs ou des outils appropriés pour votre système de fichiers.

fsck a échoué à l'état de sortie... (périphérique manquant)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
Cleaning up ifupdown....
Loading kernel modules...done.
...
Activating lvm and md swap...done.
Checking file systems...fsck from util-linux-ng 2.16.2
/sbin/fsck.xfs: /dev/sdh does not exist
fsck died with exit status 8
[31mfailed (code 8).[39;49m
```

Causes potentielles

- Ramdisk à la recherche d'un lecteur manquant
- Contrôle de cohérence forcé du système de fichiers
- Lecteur en échec ou détaché

Actions suggérées

Pour ce type d'instance	Faites ceci
Soutenu EBS par Amazon	Essayez une ou plusieurs des solutions suivants pour résoudre le problème : • Arrêtez l'instance, attachez le volume à une instance existante en cours d'exécution. • Exécutez manuellement des contrôles de cohérence. • Corrigez le ramdisk pour inclure les utilitaires pertinents. • Modifiez les paramètres de réglage du système de fichiers pour supprimer les exigences de cohérence (non recommandé).
Basée sur le stockage d'instance	Essayez une ou plusieurs des solutions suivants pour résoudre le problème : • Regrouper le ramdisk avec les bons outils. • Modifiez les paramètres de réglage du système de fichiers pour supprimer les exigences de cohérence (non recommandé). • Mettez fin à l'instance et lancez une nouvelle instance. • (Facultatif) Demandez une assistance technique pour la récupération des données en utilisant AWS Support.

GRUBprompt (grubdom>)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
    GNU GRUB  version 0.97  (629760K lower / 0K upper memory)

       [ Minimal BASH-like line editing is supported.   For

         the   first   word,  TAB  lists  possible  command

         completions.  Anywhere else TAB lists the possible

         completions of a device/filename. ]

grubdom>
```

Causes potentielles

Type d'instance	Causes potentielles
Soutenu EBS par Amazon	• Fichier GRUB de configuration manquant. • GRUBImage utilisée incorrecte, le fichier GRUB de configuration attendu se trouve à un autre emplacement. • Système de fichiers non pris en charge utilisé pour stocker votre fichier de GRUB configuration (par exemple, pour convertir votre système de fichiers racine en un type non pris en charge par une version antérieur e deGRUB).
Basée sur le stockage d'instance	• Fichier GRUB de configuration manquant. • GRUBImage utilisée incorrecte, le fichier GRUB de configuration attendu se trouve à un autre emplacement. • Système de fichiers non pris en charge utilisé pour stocker votre fichier de GRUB

Type d'instance	Causes potentielles
	configuration (par exemple, pour convertir votre système de fichiers racine en un type non pris en charge par une version antérieur e deGRUB).

Actions suggérées

Pour ce type d'instance	Faites ceci
Soutenu EBS par Amazon	Option 1 : modifiez l'instance AMI et relancez-la : 1. Modifiez la source AMI pour créer un fichier de GRUB configuration à l'emplacement standard (/boot/grub/menu.lst). 2. Vérifiez que votre version de GRUB prend en charge le type de système de fichiers sous-jacent et effectuez une mise à niveau GRUB si nécessaire. 3. Choisissez l'GRUBimage appropriée (hd0-1er lecteur ou hd00 — 1er lecteur, 1re partition). 4. Mettez fin à l'instance et lancez-en une nouvelle en utilisant celle AMI que vous avez créée. Option 2 : Corrigez l'instance existante: 1. Arrêtez l'instance. 2. Détachez le système de fichiers racine. 3. Attachez le système de fichiers racine à une instance connue en fonctionnement. 4. Montez le système de fichiers.

Pour ce type d’instance	Faites ceci
	5. Créez un fichier GRUB de configuration. 6. Vérifiez que votre version de GRUB prend en charge le type de système de fichiers sous-jacent et effectuez une mise à niveau GRUB si nécessaire. 7. Détachez le système de fichiers. 8. Attachez-le à l’instance originale. 9. Modifiez l'attribut du noyau pour utiliser l'GRUBimage appropriée (1er disque ou 1ère partition sur le 1er disque). 10. Démarrez l’instance.

Pour ce type d'instance	Faites ceci
Basée sur le stockage d'instance	Option 1 : modifiez l'instance AMI et relancez-la : 1. Créez le nouveau AMI avec un fichier de GRUB configuration à l'emplacement standard (/boot/grub/menu.lst). 2. Choisissez l'GRUBimage appropriée (hd0-1er lecteur ou hd00 — 1er lecteur, 1re partition). 3. Vérifiez que votre version de GRUB prend en charge le type de système de fichiers sous-jacent et effectuez une mise à niveau GRUB si nécessaire. 4. Mettez fin à l'instance et lancez-en une nouvelle à l'aide de celle AMI que vous avez créée. Option 2 : Arrêtez l'instance et lancez une nouvelle instance en spécifiant le noyau correct. **Note** Pour récupérer les données de l'instanc e existante, contactez AWS Support.

Affichage de l'interface eth0 : le périphérique eth0 a une MAC adresse différente de celle attendue, ignorée. (MACAdresse codée en dur)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
. . .
```

```
Bringing up loopback interface:  [  OK  ]

Bringing up interface eth0:  Device eth0 has different MAC address than expected,
 ignoring.
[FAILED]

Starting auditd: [  OK  ]
```

Causes potentielles

Il existe une interface codée en dur MAC dans la configuration AMI

Actions suggérées

Pour ce type d'instance	Faites ceci
Soutenu EBS par Amazon	Effectuez l'une des actions suivantes : • Modifiez le AMI pour supprimer le codage en dur et relancer l'instance. • Modifiez l'instance pour supprimer l'MACadresse codée en dur. OU Utilisez la procédure suivante. 1. Arrêtez l'instance. 2. Détachez le volume racine. 3. Attachez le volume à une autre instance et modifiez-le pour supprimer l'MACadresse codée en dur. 4. Attachez le volume à l'instance originale. 5. Démarrez l'instance.
Basée sur le stockage d'instance	Effectuez l'une des actions suivantes : • Modifiez l'instance pour supprimer l'MACadresse codée en dur.

Pour ce type d'instance	Faites ceci
	• Mettez fin à l'instance et lancez une nouvelle instance.

Impossible de charger la SELinux politique. L'appareil est en mode d'exécution. Arrêt maintenant. (SELinuxmauvaise configuration)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
audit(1313445102.626:2): enforcing=1 old_enforcing=0 auid=4294967295
Unable to load SELinux Policy. Machine is in enforcing mode. Halting now.
Kernel panic - not syncing: Attempted to kill init!
```

Causes potentielles

SELinuxa été activé par erreur :

- Le noyau fourni n'est pas pris en charge par GRUB
- Le noyau de rechange n'existe pas

Actions suggérées

Pour ce type d'instance	Faites ceci
Soutenu EBS par Amazon	Utilisez la procédure suivante. 1. Arrêtez l'instance en échec. 2. Détachez le volume racine de l'instance en échec. 3. Attachez le volume racine à une autre instance Linux en fonctionnement (appelée plus tard instance de récupération).

Pour ce type d'instance	Faites ceci
	4. Connectez-vous à l'instance de récupération et montez le volume racine de l'instance en échec. 5. SELinuxDésactivez-le sur le volume racine monté. Ce processus varie selon les distributions Linux. Pour plus d'informations, consultez la documentation spécifique à votre système d'exploitation. **Note** Sur certains systèmes, vous pouvez le désactiver `SELINUX=disabled` en SELinux définissant dans le `/mount_point /etc/sysconfig/selinux` fichier l'emplacement où *`mount_point`* vous avez monté le volume sur votre instance de restauration. 6. Démontez et détachez le volume racine à partir de l'instance de récupération et attachez-le de nouveau à l'instance originale. 7. Démarrez l'instance.
Basée sur le stockage d'instance	Utilisez la procédure suivante. 1. Mettez fin à l'instance et lancez une nouvelle instance. 2. (Facultatif) Demandez une assistance technique pour la récupération des données en utilisant AWS Support.

XENBUS: délai de connexion aux appareils (délai d'expiration Xenbus)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
XENBUS: Timeout connecting to devices!
...
Kernel panic - not syncing: No init found.  Try passing init= option to kernel.
```

Causes potentielles

- Le périphérique de stockage en mode bloc n'est pas connecté à l'instance
- Cette instance utilise un ancien noyau de l'instance

Actions suggérées

Pour ce type d'instance	Faites ceci
Soutenu EBS par Amazon	Effectuez l'une des actions suivantes : • Modifiez l'instance AMI et pour utiliser un noyau moderne et relancez l'instance. • Redémarrez l'instance.
Basée sur le stockage d'instance	Effectuez l'une des actions suivantes : • Mettez fin à l'instance. • Modifiez le AMI pour utiliser un noyau moderne et lancez une nouvelle instance à l'aide de celui-ciAMI.

Résoudre les problèmes liés au démarrage d'une instance Amazon EC2 Linux à partir du mauvais volume

Dans certains cas, un volume autre que le volume attaché à une instance Linux `/dev/xvda` ou en `/dev/sda` devient le volume racine. Cela peut arriver lorsque vous avez attaché le volume racine d'une autre instance, ou un volume créé à partir de l'instantané d'un volume racine, à une instance avec un volume racine existant.

Ceci est dû à la façon de fonctionner du ramdisk initial dans Linux. Il choisit le volume définit comme `/` dans le fichier `/etc/fstab`, et dans certaines distributions. Ceci est déterminé par l'étiquette attachée à la partition du volume. Plus spécifiquement, vous trouvez que le fichier `/etc/fstab` ressemble à ce qui suit :

```
LABEL=/ / ext4 defaults,noatime 1 1
tmpfs /dev/shm tmpfs defaults 0 0
devpts /dev/pts devpts gid=5,mode=620 0 0
sysfs /sys sysfs defaults 0 0
proc /proc proc defaults 0 0
```

Si vous vérifiez l'étiquette des deux volumes, vous verrez qu'ils contiennent tous les deux l'étiquette `/` :

```
[ec2-user ~]$ sudo e2label /dev/xvda1
/
[ec2-user ~]$ sudo e2label /dev/xvdf1
/
```

Dans cet exemple, `/dev/xvdf1` pourrait devenir le périphérique racine où votre instance démarre après l'exécution initiale de ramdisk, au lieu du volume `/dev/xvda1` à partir duquel vous aviez essayé de démarrer. Pour résoudre ce problème, utilisez la même commande e2label pour changer l'étiquette du volume attaché à partir duquel vous ne souhaitez pas démarrer.

Dans certains cas, le fait de spécifier un UUID in `/etc/fstab` peut résoudre ce problème. Toutefois, si les deux volumes proviennent du même instantané, ou si le volume secondaire est créé à partir d'un instantané du volume principal, ils partagent unUUID.

```
[ec2-user ~]$ sudo blkid
/dev/xvda1: LABEL="/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
 PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
```

```
/dev/xvdf1: LABEL="old/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
 PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
```

Pour changer l'étiquette d'un volume ext4 attaché

1. Utilisez la commande e2label pour remplacer l'étiquette du volume par autre chose que /.

   ```
   [ec2-user ~]$ sudo e2label /dev/xvdf1 old/
   ```

2. Vérifiez que le volume possède la nouvelle étiquette.

   ```
   [ec2-user ~]$ sudo e2label /dev/xvdf1
   old/
   ```

Pour changer l'étiquette d'un volume xfs attaché

- Utilisez la commande xfs_admin pour remplacer l'étiquette du volume par autre chose que /.

  ```
  [ec2-user ~]$ sudo xfs_admin -L old/ /dev/xvdf1
  writing all SBs
  new label = "old/"
  ```

Après avoir modifié l'étiquette du volume comme indiqué, vous devriez pouvoir redémarrer l'instance et avoir le bon volume sélectionné par le ramdisk initial lorsque l'instance démarre.

> **Important**
>
> Si vous prévoyez de détacher le volume avec la nouvelle étiquette et de le renvoyer vers une autre instance pour l'utiliser comme volume racine, vous devez ré-exécuter la procédure ci-dessus et réattribuer à l'étiquette du volume sa valeur d'origine. Sinon, l'autre instance ne démarre pas, car le ramdisk ne peut pas trouver le volume avec l'étiquette /.

Résoudre les problèmes de connexion à votre instance Amazon EC2 Windows

Les informations suivantes et les erreurs courantes peuvent vous aider à résoudre les problèmes lors de la connexion à votre instance Windows.

Problèmes de connexion

- Le service Bureau à distance ne peut pas se connecter à l'ordinateur distant
- Erreur lors de l'utilisation du RDP client macOS
- RDPaffiche un écran noir au lieu du bureau
- Impossible de se connecter à distance à une instance avec un utilisateur autre qu'un administrateur
- Résolution des problèmes de bureau à distance à l'aide de AWS Systems Manager
- Activer le bureau à distance sur une EC2 instance dotée d'un registre distant
- J'ai perdu ma clé privée. Comment puis-je me connecter à mon instance Windows ?

Le service Bureau à distance ne peut pas se connecter à l'ordinateur distant

Essayez d'exécuter l'opération suivante pour résoudre les problèmes liés à votre connexion à votre instance :

- Vérifiez que vous utilisez le bon DNS nom d'hôte public. (Dans la EC2 console Amazon, sélectionnez l'instance et cochez Public DNS (IPv4) dans le volet de détails.) Si votre instance se trouve dans un VPC et que vous ne voyez pas de DNS nom public, vous devez activer les DNS noms d'hôte. Pour plus d'informations, consultez DNSles attributs correspondants VPC dans le guide de VPC l'utilisateur Amazon.
- Vérifiez que votre instance possède une IPv4 adresse publique. Si non, vous pouvez associer une adresse IP Elastic à votre instance. Pour plus d'informations, consultez Adresses IP Elastic.
- Pour vous connecter à votre instance à l'aide d'une IPv6 adresse, vérifiez que votre ordinateur local possède une IPv6 adresse et qu'il est configuré pour l'utiliserIPv6. Pour plus d'informations, consultez la section Configurer IPv6 sur vos instances dans le guide de VPC l'utilisateur Amazon.
- Vérifiez que votre groupe de sécurité dispose d'une règle autorisant RDP l'accès sur le port 3389.
- Si vous avez copié le mot de passe, mais que vous obtenez l'erreur `Your credentials did not work`, essayez de le saisir manuellement lorsque vous y êtes invité. Il est possible que vous

ayez oublié un caractère ou ajouté une espace supplémentaire lorsque vous avez copié le mot de passe.

- Vérifiez que l'instance a réussi les contrôles d'état. Pour plus d'informations, consultez Contrôles de statut pour les EC2 instances Amazon et the section called "Les vérifications d'état de l'instance Linux ont échoué".
- Vérifiez que la table de routage du sous-réseau comporte un itinéraire qui envoie tout le trafic destiné à l'extérieur VPC vers la passerelle Internet duVPC. Pour plus d'informations, consultez la section Création d'une table de routage personnalisée (passerelles Internet) dans le guide de l'VPCutilisateur Amazon.
- Vérifiez que le pare-feu Windows ou un autre logiciel de pare-feu ne bloque pas le RDP trafic vers l'instance. Nous vous recommandons de désactiver le pare-feu Windows et le contrôle d'accès à votre instance à l'aide des règles des groupes de sécurité. Vous pouvez AWSSupport-TroubleshootRDP utiliser pour disable the Windows Firewall profiles using SSM Agent. Pour désactiver le pare-feu Windows sur une instance Windows qui n'est pas configurée pour AWS Systems ManagerAWSSupport-ExecuteEC2Rescue, utilisez ou suivez les étapes manuelles suivantes :

Étapes manuelles

1. Arrêtez l'instance affectée et détachez son volume racine.
2. Lancez une instance temporaire dans la même zone de disponibilité que l'instance affectée.

   > **Warning**
   >
   > Si votre instance temporaire est basée sur la même base AMI que l'instance d'origine, vous devez effectuer des étapes supplémentaires, sinon vous ne pourrez pas démarrer l'instance d'origine après avoir restauré son volume racine en raison d'une collision de signatures de disque. Vous pouvez également en sélectionner une autre AMI pour l'instance temporaire. Par exemple, si l'instance d'origine utilise AWS Windows AMI pour Windows Server 2016, lancez l'instance temporaire à l'aide de AWS Windows AMI pour Windows Server 2019.

3. Attachez le volume racine de l'instance affectée à cette instance temporaire. Connectez-vous à l'instance temporaire, ouvrez l'utilitaire Gestion des disques et mettez le lecteur en ligne.

4. Ouvrez Regedit et sélectionnez HKEY_ LOCAL _ MACHINE. Dans le menu File (Fichier), choisissez Load Hive (Charger Hive). Sélectionnez le lecteur, ouvrez le fichier `Windows\System32\config\SYSTEM` et spécifiez un nom de clé lorsque vous y êtes invité (vous pouvez utiliser n'importe quel nom).
5. Sélectionnez la clé que vous venez de charger et naviguez jusqu'à `ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy`. Pour chaque clé portant un nom au format xxxxProfile, sélectionnez la clé et passez `EnableFirewall` de 1 à 0. Sélectionnez à nouveau la clé, puis dans le menu File (Fichier), sélectionnez Unload Hive (Décharger Hive).
6. (Facultatif) Si votre instance temporaire est basée sur la même base AMI que l'instance d'origine, vous devez effectuer les étapes suivantes, sinon vous ne pourrez pas démarrer l'instance d'origine après avoir restauré son volume racine en raison d'une collision de signature de disque.

   > **Warning**
   >
   > La procédure suivante décrit comment modifier le Registre Windows à l'aide de l'Éditeur de Registre. Si vous n'êtes pas familier avec le Registre Windows ou comment apporter des modifications en toute sécurité à l'aide de l'Éditeur de Registre, consultez Configurer le registre.

   a. Ouvrez une invite de commande, saisissez regedit.exe, puis appuyez sur Entrée.
   b. Dans l'éditeur du registre, choisissez HKEYLOCAL_ _ dans le MACHINE menu contextuel (clic droit), puis choisissez Rechercher.
   c. Cliquez sur Windows Boot Manager, puis.choisissez Rechercher suivant.
   d. Choisissez la clé nommée `11000001`. Cette clé est apparentée à la clé que vous avez trouvée à l'étape précédente.
   e. Dans le volet droit, choisissez `Element`, puis.Modifier à partir du menu contextuel (clic droit).
   f. Localisez la signature du disque de quatre octets au décalage 0x38 dans les données. Inversez les octets pour créer la signature du disque et l'écrire. Par exemple, la signature de disque représentée par les données suivantes est `E9EB3AA5` :

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
```

```
...
```

g. Dans une fenêtre d'invite de commandes, exécutez la commande suivante pour démarrer Microsoft DiskPart.

```
diskpart
```

h. Exécutez la DiskPart commande suivante pour sélectionner le volume. (Vous pouvez vérifier que le numéro de disque est 1 à l'aide de l'utilitaire Gestion des disques.

```
DISKPART> select disk 1

Disk 1 is now the selected disk.
```

i. Exécutez la DiskPart commande suivante pour obtenir la signature du disque.

```
DISKPART>  uniqueid disk

Disk ID: 0C764FA8
```

j. Si la signature de disque affichée à l'étape précédente ne correspond pas à BCD celle que vous avez notée précédemment, utilisez la DiskPart commande suivante pour modifier la signature de disque afin qu'elle corresponde :

```
DISKPART> uniqueid disk id=E9EB3AA5
```

7. À l'aide de l'utilitaire Gestion des disques, déconnectez le lecteur.

> **Note**
>
> Le lecteur est automatiquement hors ligne si l'instance temporaire exécute le même système d'exploitation que l'instance concernée. Vous n'aurez donc pas besoin de le mettre hors ligne manuellement.

8. Détachez le volume de l'instance temporaire. Vous pouvez mettre l'instance temporaire hors service si vous n'en avez plus besoin.
9. Restaurez le volume racine de l'instance affectée en attachant celui-ci en tant que `/dev/sda1`.
10. Démarrez l'instance.

- Vérifiez que l'authentification au niveau du réseau est désactivée sur les instances qui ne font pas partie d'un domaine Active Directory (utilisez AWSSupport-TroubleshootRDP pour disable NLA).
- Vérifiez que le type de démarrage du service Remote Desktop (TermService) est automatique et que le service est démarré (utilisé AWSSupport-TroubleshootRDPpourenable and start the RDP service).
- Vérifiez que vous vous connectez au port RDP (Remote Desktop Protocol) approprié, qui est par défaut le port 3389 (utilisez AWSSupport-TroubleshootRDP pour read the current RDP port et change it back to 3389).
- Vérifiez que les connexions via le service Bureau à distance sont autorisées sur votre instance (utilisez AWSSupport-TroubleshootRDP pour enable Remote Desktop connections).
- Vérifiez que le mot de passe n'a pas expiré. Si c'est le cas, vous pouvez le réinitialiser. Pour plus d'informations, consultez Réinitialisation du mot de passe administrateur Windows pour une instance Amazon EC2 Windows.
- Si vous tentez de vous connecter à l'aide d'un utilisateur que vous avez créé sur l'instance et que vous recevez le message d'erreur `The user cannot connect to the server due to insufficient access privileges`, vérifiez que vous avez autorisé l'utilisateur à se connecter localement. Pour plus d'informations, consultez Accorder à un membre le droit de se connecter localement.
- Si vous tentez de dépasser le nombre maximal de RDP sessions simultanées autorisées, votre session est interrompue `Your Remote Desktop Services session has ended. Another user connected to the remote computer, so your connection was lost.` par le message Par défaut, vous êtes autorisé à utiliser deux RDP sessions simultanées sur votre instance.

Erreur lors de l'utilisation du RDP client macOS

Si vous vous connectez à une instance Windows Server à l'aide du client Remote Desktop Connection sur le site Web de Microsoft, le message d'erreur suivant peut s'afficher :

```
Remote Desktop Connection cannot verify the identity of the computer that you want to
 connect to.
```

Téléchargez l'application Microsoft Remote Desktop à partir du Mac App Store et utilisez cette application pour vous connecter à votre instance.

RDPaffiche un écran noir au lieu du bureau

Essayez ce qui suit pour résoudre ce problème :

- Consultez la sortie de la console pour plus d'informations. Pour obtenir la sortie de console de votre instance à l'aide de la EC2 console Amazon, sélectionnez l'instance, puis choisissez Actions, Surveiller et dépanner, puis Obtenir le journal du système.
- Vérifiez que vous utilisez la dernière version de votre RDP client.
- Essayez les paramètres par défaut du RDP client. Pour plus d'informations, consultez Remote Session Environment.
- Si vous utilisez la connexion au Bureau à distance, essayez de la démarrer avec l'option `/admin` comme suit.

```
mstsc /v:instance /admin
```

- Si le serveur exécute une application plein écran, il se peut qu'elle ait cessé de répondre. Utilisez Ctrl+Shift+Esc pour démarrer le Gestionnaire des tâches de Windows, puis fermez l'application.
- Si le serveur est sur-utilisé, il peut avoir cessé de répondre. Pour surveiller l'instance à l'aide de la EC2 console Amazon, sélectionnez l'instance, puis sélectionnez l'onglet Surveillance. Si vous avez besoin d'attribuer une taille supérieure au type d'instance, consultez Changements de type d'EC2instance Amazon.

Impossible de se connecter à distance à une instance avec un utilisateur autre qu'un administrateur

Si vous ne pouvez pas vous connecter à distance à une instance Windows avec un utilisateur qui n'est pas un compte administrateur, vérifiez que l'utilisateur est autorisé à se connecter localement. Consultez Accorder à un utilisateur ou à un groupe le droit de se connecter localement aux contrôleurs de domaine du domaine.

Résolution des problèmes de bureau à distance à l'aide de AWS Systems Manager

Vous pouvez l'utiliser AWS Systems Manager pour résoudre les problèmes de connexion à votre instance Windows à l'aide RDP de.

AWSSupport-Résoudre les problèmes RDP

Le document RDP d'automatisation AWSSupport -Troubleshoot permet à l'utilisateur de vérifier ou de modifier les paramètres courants de l'instance cible susceptibles d'avoir un impact sur les connexions Remote Desktop Protocol (RDP), tels que le RDPport, l'authentification de la couche réseau (NLA) et les profils de pare-feu Windows. Par défaut, le document lit et produit les valeurs de ces paramètres.

Le document RDP d'automatisation AWSSupport -Troubleshoot peut être utilisé avec EC2 des instances, des instances locales et des machines virtuelles (VMs) activées pour être utilisées avec AWS Systems Manager (instances gérées). En outre, il peut également être utilisé avec des EC2 instances de Windows Server qui ne sont pas activées pour être utilisées avec Systems Manager. Pour plus d'informations sur l'activation des instances à utiliser avec AWS Systems Manager, consultez la section Nœuds gérés dans le guide de AWS Systems Manager l'utilisateur.

Pour résoudre les problèmes à l'aide du document AWSSupport RDP -Troubleshoot

1. Connectez-vous à la console Systems Manager.
2. Vérifiez que vous êtes dans la même région que l'instance dégradée.
3. Dans le volet de navigation de gauche, choisissez Documents.
4. Sur l'onglet Owned by Amazon (Propriété d'Amazon), saisissez `AWSSupport-TroubleshootRDP` dans le champ de recherche. Lorsque le document `AWSSupport-TroubleshootRDP` apparaît, sélectionnez-le.
5. Sélectionnez Execute automation (Exécuter l'automatisation).
6. Pour Mode d'exécution, choisissez Exécution simple.
7. Pour les paramètres d'entrée InstanceId, activez Afficher le sélecteur d'instance interactif.
8. Choisissez votre EC2 instance Amazon.
9. Consultez les exemples, puis choisissez Exécuter.
10. Pour surveiller la progression de l'exécution, dans Statut de l'exécution, attendez que le statut passe de En attente à Réussite. Développez Sorties pour afficher les résultats. Pour afficher la sortie de chaque étape, dans Étapes exécutées, choisissez l'ID d'étape.

AWSSupport-Exemples de résolution des problèmes RDP

Les exemples suivants vous montrent comment effectuer des tâches de dépannage courantes à l'aide de AWSSupport -TroubleshootRDP. Vous pouvez utiliser l'exemple de AWS CLI start-automation-executioncommande ou le lien fourni vers le AWS Management Console.

Example Exemple : vérifier l'RDPétat actuel

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=instance_id, Action=Custom" --region region_code
```

AWS Systems Manager console :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region#documentVersion=$LATEST
```

Example Exemple : Désactiver le pare-feu Windows

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, Firewall=Disable" --
region region_code
```

AWS Systems Manager console :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&Firewall=Disable
```

Example Exemple : Désactiver l'authentification au niveau du réseau

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, NLASettingAction=Disable" --
region region_code
```

AWS Systems Manager console :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion
```

Example Exemple : définir le type RDP de démarrage du service sur Automatique et démarrer le RDP service

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, RDPServiceStartupType=Auto,
 RDPServiceAction=Start" --region region_code
```

AWS Systems Manager console :

```
https://console.aws.amazon.com/systems-manager/automation/execute/
AWSSupport-TroubleshootRDP?region=region_code#documentVersion=
$LATEST&RDPServiceStartupType=Auto&RDPServiceAction=Start
```

Example Exemple : restauration du RDP port par défaut (3389)

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, RDPPortAction=Modify" --
region region_code
```

AWS Systems Manager console :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RDPPortAction=Modify
```

Example Exemple : Autoriser les connexions à distance

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, RemoteConnections=Enable" --
region region_code
```

AWS Systems Manager console :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RemoteConnections=Enable
```

AWSSupport-Exécuter EC2Rescue

Le document AWSSupport d'EC2Rescueautomatisation -Execute utilise Windows Server EC2Rescue pour résoudre et restaurer automatiquement la connectivité et les problèmes de connectivité des EC2 RDP instances. Pour plus d'informations, voir Exécuter l'EC2Rescueoutil sur des instances inaccessibles.

Le document AWSSupport d'EC2Rescueautomatisation -Execute nécessite l'arrêt et le redémarrage de l'instance. Systems Manager Automation arrête l'instance et crée une Amazon Machine Image (AMI). Les données stockées sur les volumes de stockage d'instance sont perdues. L'adresse IP publique est modifiée si vous n'utilisez pas une adresse IP Elastic. Pour plus d'informations, voir Exécuter l'EC2Rescueoutil sur des instances inaccessibles dans le Guide de l'AWS Systems Manager utilisateur.

Pour résoudre les problèmes liés à l'utilisation du document AWSSupport -Execute EC2Rescue

1. Ouvrez la console Systems Manager.
2. Vérifiez que vous vous trouvez dans la même région que l'EC2instance Amazon défectueuse.
3. Dans le panneau de navigation, choisissez Documents.
4. Recherchez et sélectionnez le document `AWSSupport-ExecuteEC2Rescue`, puis choisissez Exécuter l'automatisation.
5. Dans Execution mode (Mode d'exécution), choisissez Simple Execution (Exécution simple).
6. Dans la section Paramètres d'entrée, pour UnreachableInstanceId, entrez l'ID d'EC2instance Amazon de l'instance inaccessible.
7. (Facultatif) Pour LogDestination, entrez le nom du bucket Amazon Simple Storage Service (Amazon S3) si vous souhaitez collecter les journaux du système d'exploitation pour le dépannage de votre instance AmazonEC2. Les journaux sont chargés automatiquement dans le compartiment spécifié.
8. Sélectionnez Execute (Exécuter).
9. Pour surveiller la progression de l'exécution, dans Execution statut (Statut de l'exécution), attendez que le statut passe de Pending (En attente) à Success (Succès). Développez Sorties pour afficher les résultats. Pour afficher la sortie de chaque étape, dans Executed Steps (Étapes exécutées), choisissez l'ID d'étape.

Activer le bureau à distance sur une EC2 instance dotée d'un registre distant

Si votre instance inaccessible n'est pas gérée par le gestionnaire de session de AWS Systems Manager, vous pouvez utiliser le registre distant pour activer Remote Desktop.

1. Depuis la EC2 console, arrêtez l'instance inaccessible.
2. Détachez le volume racine de l'instance inaccessible et attachez-le à une instance accessible dans la même zone de disponibilité que le volume de stockage. Si vous n'avez pas d'instance accessible dans la même zone de disponibilité, lancez-en une. Notez le nom du périphérique du volume racine de l'instance inaccessible.
3. Sur l'instance accessible, ouvrez la Gestion des disques. Vous pouvez le faire en exécutant la commande suivante dans une fenêtre d'invite de commande.

   ```
   diskmgmt.msc
   ```

4. Cliquez avec le bouton droit sur le volume récemment attaché provenant de l'instance inaccessible, puis sélectionnez En ligne.
5. Ouvrez l'Éditeur du Registre Windows. Vous pouvez le faire en exécutant la commande suivante dans une fenêtre d'invite de commande.

   ```
   regedit
   ```

6. Dans l'éditeur du registre, choisissez HKEY_ LOCAL _ MACHINE, puis sélectionnez Fichier, Load Hive.
7. Sélectionnez le lecteur du volume attaché, accédez à `\Windows\System32\config\`, sélectionnez `SYSTEM`, puis choisissez Ouvrir.
8. Dans Nom de clé, entrez un nom unique pour le répertoire de stockage et choisissez OK.
9. Sauvegardez la ruche du registre avant d'apporter des modifications au registre.

   a. Dans l'arborescence de la console de l'éditeur de registre, sélectionnez la ruche que vous avez chargée : HKEY_ LOCAL _ \ MACHINE*your-key-name*.

   b. Choisissez Fichier, Exporter.

   c. Dans la boîte de dialogue Exporter un fichier du Registre, choisissez l'emplacement vers lequel vous souhaitez enregistrer la copie de sauvegarde, puis tapez un nom pour le fichier de sauvegarde dans le champ Nom du fichier.

d. Choisissez Enregistrer.

10. Dans l'éditeur du registre, naviguez jusqu'à`HKEY_LOCAL_MACHINE\your key name\ControlSet001\Control\Terminal Server`, puis double-cliquez dans le volet de détails fDenyTSConnections.
11. Dans le champ Modifier DWORD la valeur, saisissez le champ Données relatives **`0`** à la valeur.
12. Choisissez OK.

> **Note**
>
> Si la valeur du champ Données de valeur est `1`, l'instance refusera les connexions au bureau à distance. La valeur `0` autorise les connexions au bureau à distance.

13. Dans l'éditeur du registre, choisissez HKEY_ LOCAL _ MACHINE *your-key-name*, puis sélectionnez Fichier, Décharger la ruche.
14. Fermez l'Éditeur du Registre et la Gestion des disques.
15. À partir de la EC2 console, détachez le volume de l'instance accessible, puis attachez-le à nouveau à l'instance inaccessible. Lorsque vous attachez le volume à l'instance inaccessible, saisissez le nom du périphérique que vous avez enregistré précédemment dans le champ Périphérique.
16. Redémarrez l'instance inaccessible.

J'ai perdu ma clé privée. Comment puis-je me connecter à mon instance Windows ?

Lorsque vous vous connectez à une instance Windows lancée récemment, vous déchiffrez le mot de passe du compte administrateur à l'aide de la clé privée de la paire de clés que vous avez spécifiée lors du lancement de l'instance.

Si vous perdez le mot de passe administrateur et que vous n'avez plus de clé privée, vous devez réinitialiser le mot de passe ou créer une nouvelle instance. Pour plus d'informations, consultez Réinitialisation du mot de passe administrateur Windows pour une instance Amazon EC2 Windows. Pour connaître les étapes de réinitialisation du mot de passe à l'aide d'un document Systems Manager, voir Réinitialiser les mots de passe et SSH les clés EC2 des instances dans le Guide de AWS Systems Manager l'utilisateur.

Résoudre les problèmes de démarrage des instances Amazon EC2 Windows

Vous trouverez ci-dessous des conseils de dépannage pour vous aider à résoudre les problèmes de mot de passe et d'activation liés aux instances Amazon EC2 Windows.

Problèmes

- « Le mot de passe n'est pas disponible »
- « Mot de passe pas encore disponible »
- « Récupération du mot de passe Windows impossible »
- « En attente du service de métadonnées »
- « L'activation de Windows est impossible »
- « Windows n'est pas authentique (0x80070005) »
- « Aucun serveur de licences Terminal Server n'est disponible pour fournir une licence »
- « Certains paramètres sont gérés par votre organisation »

« Le mot de passe n'est pas disponible »

Pour vous connecter à une instance Windows à l'aide des services Bureau à distance, vous devez spécifier un compte et un mot de passe. Les comptes et mots de passe fournis sont basés sur ceux AMI que vous avez utilisés pour lancer l'instance. Vous pouvez soit récupérer le mot de passe généré automatiquement pour le compte administrateur, soit utiliser le compte et le mot de passe utilisés dans l'instance d'origine à partir de laquelle le compte AMI a été créé.

Vous pouvez générer un mot de passe pour le compte administrateur pour les instances lancées à l'aide d'un système Windows personnaliséAMI. Pour générer le mot de passe, vous devez configurer certains paramètres du système d'exploitation avant de AMI le créer. Pour de plus amples informations, veuillez consulter Créez un compte soutenu EBS par Amazon AMI.

Si votre instance Windows n'est pas configurée pour générer un mot de passe aléatoire, vous recevez le message suivant lorsque vous extrayez le mot de passe généré automatiquement à l'aide de la console :

```
Password is not available.
The instance was launched from a custom AMI, or the default password has changed. A
```

```
password cannot be retrieved for this instance. If you have forgotten your password,
 you can
reset it using the Amazon EC2 configuration service. For more information, see
 Passwords for a
Windows Server instance.
```

Vérifiez la sortie de console de l'instance pour voir si AMI celle que vous avez utilisée pour la lancer a été créée avec la génération de mot de passe désactivée. Si la génération de mot de passe est désactivée, la sortie de la console contient ce qui suit :

```
Ec2SetPassword: Disabled
```

Si la génération de mot de passe est désactivée et que vous avez oublié le mot de passe de l'instance originale, vous pouvez réinitialiser le mot de passe de cette instance. Pour de plus amples informations, veuillez consulter Réinitialisation du mot de passe administrateur Windows pour une instance Amazon EC2 Windows.

« Mot de passe pas encore disponible »

Pour vous connecter à une instance Windows à l'aide des services Bureau à distance, vous devez spécifier un compte et un mot de passe. Les comptes et mots de passe fournis sont basés sur ceux AMI que vous avez utilisés pour lancer l'instance. Vous pouvez soit récupérer le mot de passe généré automatiquement pour le compte administrateur, soit utiliser le compte et le mot de passe utilisés dans l'instance d'origine à partir de laquelle le compte AMI a été créé.

Votre mot de passe devrait être disponible d'ici quelques minutes. Si le mot de passe n'est pas disponible, vous recevrez le message suivant lorsque vous extrayez le mot de passe généré automatiquement à l'aide de la console :

```
Password not available yet.
Please wait at least 4 minutes after launching an instance before trying to retrieve
 the
auto-generated password.
```

Si cela fait plus de quatre minutes et que vous ne pouvez toujours pas obtenir le mot de passe, il est possible que l'agent de lancement de votre instance ne soit pas configuré pour générer un mot de passe. Pour cela, vérifiez si sortie de la console est vide. Pour de plus amples informations, veuillez consulter Impossible d'obtenir la sortie de la console.

Vérifiez également que l'`ec2:GetPasswordData`action est autorisée sur le compte AWS Identity and Access Management (IAM) utilisé pour accéder au portail de gestion. Pour plus d'informations sur IAM les autorisations, voir Qu'est-ce que c'est IAM ? .

« Récupération du mot de passe Windows impossible »

Pour récupérer le mot de passe généré automatiquement pour le compte d'administrateur, vous devez utiliser la clé privée de la paire de clés que vous avez spécifiée lors du lancement de l'instance. Si vous n'avez pas spécifié de paire de clés existante au lancement de l'instance, vous recevez le message suivant.

```
Cannot retrieve Windows password
```

Vous pouvez mettre fin à cette instance et lancer une nouvelle instance en l'utilisantAMI, en veillant à spécifier une paire de clés.

« En attente du service de métadonnées »

Une instance Windows doit obtenir des informations auprès des métadonnées de son instance avant qu'elle puisse s'activer. Par défaut, le `WaitForMetaDataAvailable` paramètre garantit que le EC2Config service attend que les métadonnées de l'instance soient accessibles avant de poursuivre le processus de démarrage. Pour de plus amples informations, veuillez consulter Utiliser les métadonnées de l'instance pour gérer votre EC2 instance.

Si l'instance échoue au test d'accessibilité de l'instance, essayez la solution suivante pour résoudre le problème.

- Vérifiez que le CIDR bloc correspond à votreVPC. Une instance Windows ne peut pas démarrer correctement si elle est lancée dans une zone VPC dont la plage d'adresses IP est comprise entre `224.0.0.0` et `255.255.255.255` (plages d'adresses IP de classe D et de classe E). Ces plages d'adresses IP sont réservées et ne doivent pas être attribuées aux périphériques hôtes. Nous vous recommandons de créer un bloc VPC avec un CIDR bloc à partir des plages d'adresses IP privées (non routables publiquement) telles que spécifiées en RFC 1918.
- Il est possible que le système ait été configuré avec une adresse IP statique. Essayez de créer une interface réseau et de l'attacher à l'instance.
- Pour l'activer DHCP sur une instance Windows à laquelle vous ne pouvez pas vous connecter

  1. Arrêtez l'instance affectée et détachez son volume racine.

2. Lancez une instance temporaire dans la même zone de disponibilité que l'instance affectée.

> **Warning**
>
> Si votre instance temporaire est basée sur la même base AMI que l'instance d'origine, vous devez effectuer des étapes supplémentaires, sinon vous ne pourrez pas démarrer l'instance d'origine après avoir restauré son volume racine en raison d'une collision de signatures de disque. Vous pouvez également en sélectionner une autre AMI pour l'instance temporaire. Par exemple, si l'instance d'origine utilise AWS Windows AMI pour Windows Server 2016, lancez l'instance temporaire à l'aide de AWS Windows AMI pour Windows Server 2019.

3. Attachez le volume racine de l'instance affectée à cette instance temporaire. Connectez-vous à l'instance temporaire, ouvrez l'utilitaire Gestion des disques et mettez le lecteur en ligne.
4. Depuis l'instance temporaire, ouvrez Regedit et sélectionnez HKEY_ LOCAL _ MACHINE. Dans le menu File (Fichier), choisissez Load Hive (Charger Hive). Sélectionnez le lecteur, ouvrez le fichier `Windows\System32\config\SYSTEM` et spécifiez un nom de clé lorsque vous y êtes invité (vous pouvez utiliser n'importe quel nom).
5. Sélectionnez la clé que vous venez de charger et naviguez jusqu'à `ControlSet001\Services\Tcpip\Parameters\Interfaces`. Chaque interface réseau est répertoriée par unGUID. Sélectionnez l'interface réseau correcte. S'il DHCP est désactivé et qu'une adresse IP statique est attribuée, `EnableDHCP` il est défini sur 0. Pour l'activerDHCP, définissez `EnableDHCP` la valeur 1 et supprimez les clés suivantes si elles existent : `NameServerSubnetMask`,`IPAddress`, et`DefaultGateway`. Sélectionnez à nouveau la clé, puis dans le menu File (Fichier), sélectionnez Unload Hive (Décharger Hive).

> **Note**
>
> Si vous disposez de plusieurs interfaces réseau, vous devez identifier l'interface appropriée à activerDHCP. Pour identifier l'interface réseau appropriée, consultez les valeurs de clé `NameServer`, `SubnetMask`, `IPAddress` et `DefaultGateway`. Ces valeurs affichent la configuration statique de l'instance précédente.

6. (Facultatif) S'il DHCP est déjà activé, il est possible que vous n'ayez pas de route vers le service de métadonnées. La mise à jour EC2Config peut résoudre ce problème.

a. Téléchargez et installez la dernière version du EC2Config service. Pour en savoir plus sur l'installation de ce service, consultez the section called "Installer EC2Config".

b. Extrayez les fichiers du fichier `.zip` dans le répertoire `Temp` du lecteur que vous avez attaché.

c. Ouvrez Regedit et sélectionnez HKEY_ LOCAL _ MACHINE. Dans le menu File (Fichier), choisissez Load Hive (Charger Hive). Sélectionnez le lecteur, ouvrez le fichier `Windows\System32\config\SOFTWARE` et spécifiez un nom de clé lorsque vous y êtes invité (vous pouvez utiliser n'importe quel nom).

d. Sélectionnez la clé que vous venez de charger et naviguez jusqu'à `Microsoft\Windows\CurrentVersion`. Sélectionnez la clé `RunOnce`. (Si elle n'existe pas, cliquez avec le bouton droit sur `CurrentVersion`, pointez la souris vers Nouveau, sélectionnez Clé et nommez la clé `RunOnce`.) Cliquez avec le bouton droit, pointez la souris vers Nouveau et sélectionnez Valeur de chaîne. Entrez le nom `Ec2Install` et les données `C:\Temp\Ec2Install.exe -q`.

e. Sélectionnez à nouveau la clé, puis dans le menu File (Fichier), sélectionnez Unload Hive (Décharger Hive).

7. (Facultatif) Si votre instance temporaire est basée sur la même base AMI que l'instance d'origine, vous devez effectuer les étapes suivantes, sinon vous ne pourrez pas démarrer l'instance d'origine après avoir restauré son volume racine en raison d'une collision de signature de disque.

> **Warning**
>
> La procédure suivante décrit comment modifier le Registre Windows à l'aide de l'Éditeur de Registre. Si vous n'êtes pas familier avec le Registre Windows ou comment apporter des modifications en toute sécurité à l'aide de l'Éditeur de Registre, consultez Configurer le registre.

a. Ouvrez une invite de commande, saisissez regedit.exe, puis appuyez sur Entrée.

b. Dans l'éditeur du registre, choisissez HKEYLOCAL_ _ dans le MACHINE menu contextuel (clic droit), puis choisissez Rechercher.

c. Cliquez sur Windows Boot Manager, puis.choisissez Rechercher suivant.

d. Choisissez la clé nommée `11000001`. Cette clé est apparentée à la clé que vous avez trouvée à l'étape précédente.

e. Dans le volet droit, choisissez `Element`, puis.Modifier à partir du menu contextuel (clic droit).

f. Localisez la signature du disque de quatre octets au décalage 0x38 dans les données. Inversez les octets pour créer la signature du disque et l'écrire. Par exemple, la signature de disque représentée par les données suivantes est `E9EB3AA5` :

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

g. Dans une fenêtre d'invite de commandes, exécutez la commande suivante pour démarrer Microsoft DiskPart.

```
diskpart
```

h. Exécutez la DiskPart commande suivante pour sélectionner le volume. (Vous pouvez vérifier que le numéro de disque est 1 à l'aide de l'utilitaire Gestion des disques.

```
DISKPART> select disk 1

Disk 1 is now the selected disk.
```

i. Exécutez la DiskPart commande suivante pour obtenir la signature du disque.

```
DISKPART>  uniqueid disk

Disk ID: 0C764FA8
```

j. Si la signature de disque affichée à l'étape précédente ne correspond pas à BCD celle que vous avez notée précédemment, utilisez la DiskPart commande suivante pour modifier la signature de disque afin qu'elle corresponde :

```
DISKPART> uniqueid disk id=E9EB3AA5
```

8. À l'aide de l'utilitaire Gestion des disques, déconnectez le lecteur.

> **Note**
>
> Le lecteur est automatiquement hors ligne si l'instance temporaire exécute le même système d'exploitation que l'instance concernée. Vous n'aurez donc pas besoin de le mettre hors ligne manuellement.

9. Détachez le volume de l'instance temporaire. Vous pouvez mettre l'instance temporaire hors service si vous n'en avez plus besoin.
10. Restaurez le volume racine de l'instance affectée en attachant le volume en tant que `/dev/sda1`.
11. Démarrez l'instance concernée.

Si vous êtes connecté à l'instance, ouvrez un navigateur Internet depuis l'instance et entrez les informations suivantes URL pour le serveur de métadonnées :

```
http://169.254.169.254/latest/meta-data/
```

Si vous ne pouvez pas contacter le serveur de métadonnées, essayez la solution suivante pour résoudre le problème :

- Téléchargez et installez la dernière version du EC2Config service. Pour en savoir plus sur l'installation de ce service, consultez the section called "Installer EC2Config".
- Vérifiez si l'instance Windows exécute des pilotes RedHat PV. Si c'est le cas, mettez à jour les pilotes PV Citrix. Pour de plus amples informations, veuillez consulter the section called "Mettre à niveau les pilotes PV".
- Vérifiez que les paramètres du pare-feu et du proxy ne bloquent pas le trafic sortant vers le service de métadonnées (`169.254.169.254`) ou les AWS KMS serveurs (les adresses sont spécifiées dans les `TargetKMSServer` éléments dans`C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml`). IPSec
- Vérifiez que vous disposez d'une route vers le service de métadonnées (`169.254.169.254`) à l'aide de la commande suivante.

  ```
  route print
  ```

- Vérifiez les problèmes de réseau susceptibles d'affecter la zone de disponibilité de votre instance. Accédez à http://status.aws.amazon.com/.

« L'activation de Windows est impossible »

Les instances Windows utilisent l' AWS KMS activation Windows. Vous pouvez recevoir ce message :`A problem occurred when Windows tried to activate. Error Code 0xC004F074`, si votre instance ne parvient pas à atteindre le AWS KMS serveur. Windows doit être activé tous les 180 jours. EC2Configtente de contacter le AWS KMS serveur avant l'expiration de la période d'activation pour s'assurer que Windows reste activé.

Si vous rencontrez un problème d'activation Windows, utilisez la procédure suivante pour le résoudre.

Pour EC2Config (Windows Server 2012 R2 AMIs et versions antérieures)

1. Téléchargez et installez la dernière version du EC2Config service. Pour en savoir plus sur l'installation de ce service, consultez the section called "Installer EC2Config".
2. Connectez-vous à l'instance et ouvrez le fichier suivant : `C:\Program Files\Amazon\Ec2ConfigService\Settings\config.xml`.
3. Localisez le WindowsActivate plugin Ec2 dans le `config.xml` fichier. Remplacez l'état par Activé, puis enregistrez vos modifications.
4. Dans le composant logiciel enfichable Windows Services, redémarrez le EC2Config service ou redémarrez l'instance.

Si cette procédure ne résout pas le problème d'activation, suivez ces étapes supplémentaires.

1. Définissez l' AWS KMS objectif : C:\> slmgr.vbs /skms 169.254.169.250:1688
2. Activez Windows : C:\> slmgr.vbs /ato

Pour EC2Launch (Windows Server 2016 AMIs et versions ultérieures)

1. À partir d'une PowerShell invite indiquant les droits d'administration, importez le EC2Launch module :

```
PS C:\> Import-Module "C:\ProgramData\Amazon\EC2-Windows\Launch\Module
\Ec2Launch.psd1"
```

2. Appelez la fonction Add-Routes pour voir la liste des nouvelles routes :

```
PS C:\> Add-Routes
```

3. Appelez la ActivationSettings fonction Set- :

```
PS C:\> Set-Activationsettings
```

4. Ensuite, exécutez le script suivant pour activer Windows :

```
PS C:\> cscript "${env:SYSTEMROOT}\system32\slmgr.vbs" /ato
```

Dans les deux casEC2Launch, EC2Config et si vous recevez toujours un message d'erreur d'activation, vérifiez les informations suivantes.

- Vérifiez que vous disposez de routes vers les AWS KMS serveurs. Ouvrez `C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml` et recherchez les éléments `TargetKMSServer`. Exécutez la commande suivante et vérifiez si les adresses de ces AWS KMS serveurs sont répertoriées.

  ```
  route print
  ```

- Vérifiez que la clé AWS KMS client est définie. Exécutez la commande suivante et consultez la sortie.

  ```
  C:\Windows\System32\slmgr.vbs /dlv
  ```

  Si le résultat contient le message d'erreur : clé de produit introuvable, la clé AWS KMS client n'est pas définie. Si la clé AWS KMS client n'est pas définie, recherchez-la comme décrit dans cet article de Microsoft : Clés de configuration du AWS KMS client, puis exécutez la commande suivante pour définir la clé AWS KMS client.

  ```
  C:\Windows\System32\slmgr.vbs /ipk client_key
  ```

- Vérifiez que le système dispose de l'heure et du fuseau horaires adéquats. Si vous utilisez un fuseau horaire autre queUTC, ajoutez la clé de registre suivante et configurez-la 1 pour vous assurer que l'heure est correcte :`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\RealTimeIsUniversal`.
- Si le pare-feu Windows est activé, désactivez-le temporairement à l'aide de la commande suivante.

  ```
  netsh advfirewall set allprofiles state off
  ```

« Windows n'est pas authentique (0x80070005) »

Les instances Windows utilisent l' AWS KMS activation Windows. Si une instance ne parvient pas à terminer le processus d'activation, elle signale que la copie de Windows n'est pas authentique.

Essayez les suggestions de la section « L'activation de Windows est impossible ».

« Aucun serveur de licences Terminal Server n'est disponible pour fournir une licence »

Par défaut, la licence Windows Server autorise deux utilisateurs simultanés via les services Bureau à distance. Si vous devez fournir à plus de deux utilisateurs un accès simultané à votre instance Windows via Remote Desktop, vous pouvez acheter une licence d'accès client Remote Desktop Services (CAL) et installer les rôles Remote Desktop Session Host et Remote Desktop Licensing Server.

Vérifiez les problèmes suivants :

- Vous avez dépassé le nombre maximal de RDP sessions simultanées.
- Vous avez installé le rôle des services Bureau à distance Windows.
- Le Gestionnaire de licences a expiré. Le cas échéant, vous ne pouvez pas vous connecter à votre instance Windows en tant qu'utilisateur. Vous pouvez essayer l'une des actions suivantes :
  - Connectez-vous à l'instance à partir de la ligne de commande à l'aide du paramètre `/admin`, par exemple :

    ```
    mstsc /v:instance /admin
    ```

    Pour plus d'informations, consultez l'article Microsoft suivant : Access Remote Desktop Via Command Line.
  - Arrêtez l'instance, détachez ses EBS volumes Amazon et associez-les à une autre instance de la même zone de disponibilité pour récupérer vos données.

« Certains paramètres sont gérés par votre organisation »

Les instances lancées à partir de la dernière version de Windows Server AMIs peuvent afficher un message de dialogue Windows Update indiquant « Certains paramètres sont gérés par votre

organisation ». Ce message apparaît en réponse à des changements dans Windows Server et n'affecte pas le comportement de Windows Update, ni votre capacité à gérer les paramètres de mise à jour.

Pour supprimer l'avertissement

1. Ouvrez `gpedit.msc` et accédez à Configuration ordinateur, Modèles d'administration, Composants Windows, Mises à jour Windows. Modifiez Configurer la mise à jour automatique et définissez la valeur activé.
2. Dans une invite de commandes, mettez à jour la politique de groupe avec gpupdate /force.
3. Fermez et rouvrez les Paramètres de Windows Update. Vous verrez le message ci-dessus indiquant que vos paramètres sont gérés par votre organisation, suivi par « Nous téléchargerons automatiquement les mises à jour, sauf si vous disposez d'une connexion limitée (où des frais s'appliquent). Dans ce cas, nous ne téléchargerons automatiquement que les mises à jour nécessaires au bon fonctionnement de Windows. »
4. Revenez à `gpedit.msc` et redéfinissez la stratégie de groupe sur la valeur non configuré. Exécutez à nouveau gpupdate /force.
5. Fermez l'invite de commande et patientez quelques minutes.
6. Rouvrez les Paramètres de Windows Update. Le message « Certains paramètres sont gérés par votre organisation. » ne doit pas s'afficher.

Résoudre les problèmes liés aux instances Amazon EC2 Windows

Vous trouverez ci-dessous des conseils de dépannage destinés à vous aider à résoudre les problèmes liés aux instances Amazon EC2 Windows.

Problèmes

- EBSles volumes ne s'initialisent pas sous Windows Server 2016 et 2019
- Démarrez une instance EC2 Windows en mode restauration des services d'annuaire (DSRM)
- L'instance perd la connectivité réseau ou les tâches programmées ne s'exécutent pas au moment prévu
- Impossible d'obtenir la sortie de la console
- Windows Server 2012 R2 non disponible sur le réseau
- Collision de signature de disque

EBSles volumes ne s'initialisent pas sous Windows Server 2016 et 2019

Les instances créées à partir d'Amazon Machine Images (AMIs) pour Windows Server 2016 et 2019 utilisent l'agent EC2Launch v1 pour diverses tâches de démarrage, notamment l'initialisation de EBS volumes. Par défaut, la EC2Launch v1 n'initialise pas les volumes secondaires. Cependant, vous pouvez configurer la EC2Launch version 1 pour initialiser automatiquement ces disques, comme suit.

Mapper les lettres de lecteur avec les volumes

1. Connectez-vous à l'instance que vous voulez configurer et ouvrez le fichier `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` dans un éditeur de texte.
2. Spécifiez les paramètres du volume, comme suit :

   ```
   {
   "driveLetterMapping": [
    {
      "volumeName": "sample volume",
      "driveLetter": "H"
    }]
   }
   ```
3. Enregistrez les modifications, puis fermez le fichier.
4. Ouvrez Windows PowerShell et utilisez la commande suivante pour exécuter le script EC2Launch v1 qui initialise les disques :

   ```
   PS C:\>  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
   ```

   Pour initialiser les disques chaque fois que l'instance démarre, ajoutez l'indicateur `-Schedule` comme suit :

   ```
   PS C:\>  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -
   Schedule
   ```

   L'agent EC2Launch v1 peut exécuter des scripts d'initialisation d'instance, par exemple `initializeDisks.ps1` en parallèle avec le `InitializeInstance.ps1` script. Si le script `InitializeInstance.ps1` redémarre l'instance, il peut interrompre d'autres tâches planifiées qui s'exécutent au démarrage de l'instance. Pour éviter tout conflit potentiel, nous vous

recommandons d'ajouter de la logique à votre script `initializeDisks.ps1`pour vous assurer que l'initialisation de l'instance est terminée en premier.

> **Note**
>
> Si le EC2Launch script n'initialise pas les volumes, assurez-vous qu'ils sont en ligne. Si les volumes sont hors ligne, exécutez la commande suivante pour mettre tous les disques en ligne.
>
> ```
> PS C:\> Get-Disk | Where-Object IsOffline -Eq $True | Set-Disk -IsOffline
>  $False
> ```

Démarrez une instance EC2 Windows en mode restauration des services d'annuaire (DSRM)

Si une instance exécutant Microsoft Active Directory rencontre une défaillance du système ou d'autres problèmes critiques, vous pouvez dépanner l'instance en démarrant dans une version spéciale du mode sans échec appelée Mode de restauration des services d'annuaire ()DSRM. DSRMVous pouvez y réparer ou récupérer Active Directory.

Assistance au conducteur pour DSRM

La façon dont vous activez DSRM et démarrez l'instance dépend des pilotes exécutés par l'instance. Dans la EC2 console, vous pouvez consulter les détails de la version du pilote pour une instance à partir du journal système. Le tableau suivant indique quels pilotes sont pris en chargeDSRM.

Versions des pilotes	DSRMSoutenu ?	Étapes suivantes
PV Citrix 5.9	Non	Restaurez l'instance à partir d'une sauvegarde. Vous ne pouvez pas l'activerDSRM.
AWS PC 7.2.0	Non	Bien que ce pilote ne DSRM soit pas pris en charge, vous pouvez toujours détacher le volume racine de l'instance, prendre un instantané du volume ou en créer un à AMI partir de celui-ci, et l'associer à une autre instance dans la même zone de disponibilité qu'un volume secondaire.

Versions des pilotes	DSRMSoutenu ?	Étapes suivantes
		Vous pouvez ensuite l'activer DSRM (comme décrit dans cette section).
AWS PV 7.2.2 et versions ultérieures	Oui	Détachez le volume racine, attachez-le à une autre instance et activez-le DSRM (comme décrit dans cette section).
Mise en réseau améliorée	Oui	Détachez le volume racine, attachez-le à une autre instance et activez-le DSRM (comme décrit dans cette section).

Pour plus d'informations sur la façon d'activer la mise en réseau améliorée, consultezthe section called "Adaptateur réseau élastique (ENA)". Pour plus d'informations sur la mise à niveau des pilotes AWS PV, voir Mettre à niveau les pilotes PV sur les instances Windows.

Configurer une instance dans laquelle démarrer DSRM

EC2Les instances Windows ne disposent pas de connectivité réseau avant l'exécution du système d'exploitation. C'est pourquoi vous ne pouvez pas appuyer sur la touche F8 de votre clavier pour sélectionner une option de démarrage. Vous devez utiliser l'une des procédures suivantes pour démarrer une instance EC2 Windows Server dansDSRM.

Si vous pensez qu'Active Directory a été endommagé et que l'instance est toujours en cours d'exécution, vous pouvez configurer l'instance pour qu'elle démarre à DSRM l'aide de la boîte de dialogue de configuration du système ou de l'invite de commande.

Pour démarrer une instance en ligne à DSRM l'aide de la boîte de dialogue de configuration du système

1. Dans la boîte de dialogue Exécuter, tapez `msconfig` et appuyez sur Entrée.
2. Choisissez l'onglet Démarrage.
3. Sous Options de démarrage, choisissez Démarrage sécurisé.
4. Choisissez Réparer Active Directory, puis OK. Le système vous invite à redémarrer le serveur.

Pour démarrer une instance en ligne à DSRM l'aide de la ligne de commande

A partir d'une fenêtre d'invite de commande, exécutez la commande suivante :

```
bcdedit /set safeboot dsrepair
```

Si une instance est hors ligne et inaccessible, vous devez détacher le volume racine et l'attacher à une autre instance pour activer DSRM le mode.

Pour démarrer une instance hors ligne dans DSRM

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Recherchez et sélectionnez l'instance affectée. Choisissez État de l'instance, Arrêter l'instance.
4. Choisissez Lancer les instances et créez une instance temporaire dans la même zone de disponibilité que l'instance affectée. Choisissez un type d'instance qui utilise une autre version de Windows. Par exemple, si votre instance est Windows Server 2016, choisissez une instance Windows Server 2019.

   > **Important**
   >
   > Si vous ne créez pas l'instance dans la même zone de disponibilité que l'instance affectée, vous ne pourrez pas attacher le volume racine de celle-ci à la nouvelle instance.

5. Dans le panneau de navigation, choisissez Volumes.
6. Recherchez le volume racine de l'instance affectée. Détachez le volume et attachez-le à l'instance temporaire que vous avez créée précédemment. Attachez-le avec le nom du périphérique par défaut (xvdf).
7. Utilisez les services Bureau à distance pour vous connecter à l'instance temporaire, puis utilisez l'utilitaire Gestion des disques pour rendre le volume disponible.
8. Ouvrez une invite de commande et exécutez la commande suivante. Remplacez D par la lettre de lecteur réelle du volume secondaire que vous venez d'attacher :

   ```
   bcdedit /store D:\Boot\BCD /set {default} safeboot dsrepair
   ```

9. Dans l'utilitaire Gestion des disques, choisissez le lecteur que vous avez attaché précédemment, ouvrez le menu contextuel (clic droit) et choisissez Hors connexion.

10. Dans la EC2 console, détachez le volume concerné de l'instance temporaire et attachez-le à nouveau à votre instance d'origine avec le nom de l'appareil. `/dev/sda1` Vous devez spécifier ce nom de périphérique pour désigner le volume en tant que volume racine.
11. Démarrez l'instance.
12. Une fois que l'instance a passé les tests de santé dans la EC2 console, connectez-vous à l'instance à l'aide de Remote Desktop et vérifiez qu'elle démarre en DSRM mode.
13. (Facultatif) Supprimez ou arrêtez l'instance temporaire que vous avez créée au cours de cette procédure.

L'instance perd la connectivité réseau ou les tâches programmées ne s'exécutent pas au moment prévu

Si vous redémarrez votre instance et qu'elle perd sa connectivité réseau, il est possible que l'instance ne soit pas à l'heure.

Par défaut, les instances Windows utilisent le temps universel coordonné (UTC). Si vous définissez l'heure de votre instance sur un autre fuseau horaire et que vous la redémarrez, l'heure se décale et l'instance perd temporairement son adresse IP. L'instance finit par rétablir sa connectivité réseau, mais cela peut prendre plusieurs heures. Le temps nécessaire à l'instance pour rétablir la connectivité réseau dépend de la différence entre le fuseau horaire UTC et l'autre.

Ce problème peut également entraîner l'absence d'exécution de tâches planifiées au moment prévu. Dans ce cas, les tâches planifiées ne s'exécutent pas au moment prévu, car l'heure de l'instance est incorrecte.

Pour utiliser un fuseau horaire autre que UTC permanent, vous devez définir la clé de RealTimeIsUniversalregistre. Sans cette clé, une instance est utilisée une UTC fois que vous l'avez redémarrée.

Pour résoudre les problèmes d'heure qui entraînent une perte de la connectivité réseau

1. Vérifiez que vous exécutez les pilotes PV recommandés. Pour plus d'informations, consultez the section called "Mettre à niveau les pilotes PV".
2. Vérifiez que la clé de registre suivante existe et qu'elle est définie sur 1 : HKEYLOCAL_ _ MACHINE SYSTEM \ CurrentControlSet \ \ Control \ TimeZoneInformation \ RealTimeIsUniversal

Impossible d'obtenir la sortie de la console

Pour les instances Windows, la sortie de la console de l'instance affiche la sortie des tâches exécutées à l'aide du processus d'amorçage Windows. Si Windows démarre correctement, le dernier message enregistré est `Windows is Ready to use`. Vous pouvez également afficher les messages du journal des événements dans la console, mais cette fonctionnalité peut ne pas être activée par défaut en fonction de votre version de Windows. Pour plus d'informations, consultez the section called "Agents de lancement Windows".

Pour obtenir la sortie de console de votre instance à l'aide de la EC2 console Amazon, sélectionnez l'instance, puis choisissez Actions, Surveiller et dépanner, puis Obtenir le journal du système. Pour obtenir le résultat de la console à l'aide de la ligne de commande, utilisez l'une des commandes suivantes : get-console-output(AWS CLI) ou Get-EC2ConsoleOutput(AWS Tools for Windows PowerShell).

Pour les instances exécutant Windows Server 2012 R2 et versions antérieures, si la sortie de la console est vide, cela peut indiquer un problème avec le EC2Config service, tel qu'un fichier de configuration mal configuré ou un échec du démarrage de Windows. Pour résoudre le problème, téléchargez et installez la dernière version deEC2Config. Pour plus d'informations, consultez the section called "Installer EC2Config".

Windows Server 2012 R2 non disponible sur le réseau

Pour plus d'informations sur le dépannage d'une instance Windows Server 2012 R2 qui n'est pas disponible sur le réseau, voir Windows Server 2012 R2 perd la connectivité réseau et de stockage après le redémarrage d'une instance.

Collision de signature de disque

Vous pouvez vérifier et résoudre les collisions de signatures de disque à l'aide EC2Rescuede Windows Server. Vous pouvez également résoudre manuellement les problèmes de signature de disque en effectuant les opérations suivantes :

> **Warning**
>
> La procédure suivante décrit comment modifier le Registre Windows à l'aide de l'Éditeur de Registre. Si vous n'êtes pas familier avec le Registre Windows ou comment apporter

des modifications en toute sécurité à l'aide de l'Éditeur de Registre, consultez Configurer le registre.

1. Ouvrez une invite de commande, saisissez regedit.exe, puis appuyez sur Entrée.
2. Dans l'éditeur du registre, choisissez HKEYLOCAL_ _ dans le MACHINE menu contextuel (clic droit), puis choisissez Rechercher.
3. Cliquez sur Windows Boot Manager, puis.choisissez Rechercher suivant.
4. Choisissez la clé nommée `11000001`. Cette clé est apparentée à la clé que vous avez trouvée à l'étape précédente.
5. Dans le volet droit, choisissez `Element`, puis.Modifier à partir du menu contextuel (clic droit).
6. Localisez la signature du disque de quatre octets au décalage 0x38 dans les données. Il s'agit de la signature de la base de données de configuration de démarrage (BCD). Inversez les octets pour créer la signature du disque et l'écrire. Par exemple, la signature de disque représentée par les données suivantes est `E9EB3AA5` :

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

7. Dans une fenêtre d'invite de commandes, exécutez la commande suivante pour démarrer Microsoft DiskPart.

```
diskpart
```

8. Exécutez la `select disk` DiskPart commande et spécifiez le numéro de disque du volume concerné par la collision de signature de disque.

> **Tip**
>
> Pour vérifier le numéro de disque du volume présentant la collision de signature de disque, utilisez l'utilitaire Gestion des disques. Ouvrez une invite de commande, saisissez `compmgmt.msc`, puis appuyez sur Entrée. Dans le volet de navigation de gauche, double-cliquez sur Gestion des disques. Dans l'utilitaire Gestion des disques, vérifiez le numéro de disque du volume présentant la collision de signature de disque.

```
DISKPART> select disk 1
Disk 1 is now the selected disk.
```

9. Exécutez la DiskPart commande suivante pour obtenir la signature du disque.

```
DISKPART>  uniqueid disk
Disk ID: 0C764FA8
```

10. Si la signature de disque affichée à l'étape précédente ne correspond pas à la signature de disque que vous avez notée précédemment, utilisez la DiskPart commande suivante pour modifier la signature de disque afin qu'elle corresponde :

```
DISKPART> uniqueid disk id=E9EB3AA5
```

Réinitialisation du mot de passe administrateur Windows pour une instance Amazon EC2 Windows

Si vous ne parvenez plus à vous connecter à votre instance Amazon EC2 Windows en raison de la perte ou de l'expiration du mot de passe administrateur Windows, vous pouvez le réinitialiser.

> **Note**
>
> Il existe un document AWS Systems Manager d'automatisation qui applique automatiquement les étapes manuelles nécessaires pour réinitialiser le mot de passe de l'administrateur local. Pour plus d'informations, consultez la section Réinitialiser les mots de passe et SSH les clés EC2 des instances dans le Guide de AWS Systems Manager l'utilisateur.

Les méthodes manuelles pour réinitialiser le mot de passe administrateur utilisent la EC2Launch version v2 ouEC2Launch. EC2Config

- Pour tous les systèmes Windows pris en charge AMIs qui incluent l'agent EC2Launch v2, utilisez EC2Launch v2.
- Pour les versions de Windows AMIs antérieures à Windows Server 2016, utilisez le EC2Config service.

- Pour Windows Server 2016 et versions ultérieuresAMIs, utilisez le EC2Launch service.

Ces procédures expliquent aussi comment vous connecter à une instance, si vous avez perdu la paire de clés qui a été utilisée pour créer l'instance. Amazon EC2 utilise une clé publique pour chiffrer une donnée, telle qu'un mot de passe, et une clé privée pour déchiffrer les données. La clé publique et la clé privée constituent une paire de clés. Avec les instances Windows, vous utilisez une paire de clés pour obtenir le mot de passe administrateur, puis vous vous connectez à l'aide deRDP.

> **Note**
>
> Si vous avez désactivé le compte d'administrateur local sur l'instance et que celle-ci est configurée pour Systems Manager, vous pouvez également réactiver et réinitialiser votre mot de passe d'administrateur local en utilisant EC2Rescue and Run Command. Pour plus d'informations, consultez la section Utiliser EC2Rescue pour Windows Server avec la commande d'exécution de Systems Manager.

Table des matières

Réinitialisez le mot de passe administrateur Windows, EC2 par exemple en utilisant la EC2Launch version 2

Si vous avez perdu votre mot de passe administrateur Windows et AMI que vous utilisez un système Windows compatible incluant l'agent EC2Launch v2, vous pouvez utiliser la EC2Launch version v2 pour générer un nouveau mot de passe.

Si vous utilisez un Windows Server 2016 ou une version ultérieure AMI qui n'inclut pas l'agent EC2Launch v2, consultezRéinitialisez le mot de passe administrateur Windows, EC2 par exemple en utilisant EC2Launch.

Si vous utilisez un Windows Server AMI antérieur à Windows Server 2016 qui n'inclut pas l'agent EC2Launch v2, consultezRéinitialisez le mot de passe administrateur Windows, EC2 par exemple en utilisant EC2Config.

> **Note**
>
> Si vous avez désactivé le compte d'administrateur local sur l'instance et que celle-ci est configurée pour Systems Manager, vous pouvez également réactiver et réinitialiser votre mot de passe d'administrateur local en utilisant EC2Rescue and Run Command. Pour plus d'informations, consultez la section Utiliser EC2Rescue pour Windows Server avec la commande d'exécution de Systems Manager.

> **Note**
>
> Il existe un document AWS Systems Manager d'automatisation qui applique automatiquement les étapes manuelles nécessaires pour réinitialiser le mot de passe de l'administrateur local. Pour plus d'informations, consultez la section Réinitialiser les mots de passe et SSH les clés EC2 des instances dans le Guide de AWS Systems Manager l'utilisateur.

Pour réinitialiser votre mot de passe administrateur Windows à l'EC2Launchaide de la version 2, vous devez effectuer les opérations suivantes :

- Étape 1 : vérifier que l'agent EC2Launch v2 est en cours d'exécution
- Étape 2 : Détacher le volume racine de l'instance
- Étape 3 : Attacher le volume à une instance temporaire
- Étape 4 : Supprimer le fichier .run-once.
- Étape 5 : Redémarrer l'instance originale

Étape 1 : vérifier que l'agent EC2Launch v2 est en cours d'exécution

Avant de tenter de réinitialiser le mot de passe administrateur, vérifiez que l'agent EC2Launch v2 est installé et en cours d'exécution. Vous utiliserez l'agent EC2Launch v2 pour réinitialiser le mot de passe administrateur plus loin dans cette section.

Pour vérifier que l'agent EC2Launch v2 est en cours d'exécution

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

2. Dans le panneau de navigation, sélectionnez Instances, puis sélectionnez l'instance dont le mot de passe doit être réinitialisé. Cette instance s'appelle l'instance originale dans cette procédure.
3. Sélectionnez Actions, Surveiller et dépanner, Obtenir le journal système.
4. Localisez l'entrée EC2 Launch, par exemple Launch : EC2Launch v2 service v2.0.124. Si vous voyez cette entrée, le service EC2Launch v2 est en cours d'exécution.

   Si le résultat du journal système est vide ou si l'agent EC2Launch v2 n'est pas en cours d'exécution, dépannez l'instance à l'aide du service Instance Console Screenshot. Pour de plus amples informations, veuillez consulter Création d'une capture d'écran d'une instance inaccessible.

Étape 2 : Détacher le volume racine de l'instance

Vous ne pouvez pas utiliser la EC2Launch version v2 pour réinitialiser un mot de passe administrateur si le volume sur lequel le mot de passe est stocké est attaché à une instance en tant que volume racine. Vous devez détacher le volume de l'instance originale avant de pouvoir l'attacher à une instance temporaire en tant que volume secondaire.

Détacher le volume racine de l'instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance qui nécessite une réinitialisation du mot de passe et choisissez État de l'instance, Arrêter l'instance. Une fois que le statut de l'instance est passé à Arrêtée, passez à l'étape suivante.
4. (Facultatif) Si vous disposez de la clé privée que vous avez spécifiée lors du lancement de cette instance, passez à l'étape suivante. Sinon, procédez comme suit pour remplacer l'instance par une nouvelle instance que vous lancez par une nouvelle paire de clés.

   a. Créez une nouvelle paire de clés à l'aide de la EC2 console Amazon. Si vous souhaitez nommer votre nouvelle paire de clés exactement comme la clé privée perdue, vous devez commencer par supprimer la paire de clés existante.

   b. Sélectionnez l'instance à remplacer. Notez le type d'instanceVPC, le sous-réseau, le groupe de sécurité et le IAM rôle de l'instance.

   c. Une fois l'instance sélectionnée, choisissez Actions, Image et modèles, puis Créer une image. Saisissez le nom et la description de l'image, puis choisissez Créer l'image.

d. Dans le volet de navigation, choisissez AMIs. Attendez que le statut de l'image passe à disponible. Sélectionnez ensuite l'image et choisissez Launch instance from AMI.

e. Renseignez les champs pour lancer une instance, en veillant à sélectionner le même type d'instance, VPC le même sous-réseau, le même groupe de sécurité et le même IAM rôle que l'instance à remplacer, puis choisissez Launch instance.

f. Lorsque vous y êtes invité, choisissez la paire de clés que vous avez créée pour la nouvelle instance, puis choisissez Launch instance.

g. (Facultatif) Si l'instance d'origine a une adresse IP Elastic associée, associez-la à la nouvelle instance. Si l'instance d'origine possède EBS des volumes en plus du volume racine, transférez-les vers la nouvelle instance.

5. Détachez le volume racine de l'instance d'origine comme suit :

   a. Sélectionnez l'instance d'origine et cliquez sur l'onglet Stockage. Notez le nom du périphérique racine sous Nom du périphérique racine. Recherchez le volume portant ce nom de périphérique sous Bloquer les appareils et notez l'ID du volume.

   b. Dans le panneau de navigation, choisissez Volumes.

   c. Dans la liste des volumes, sélectionnez le volume que vous avez noté comme périphérique racine, puis choisissez Actions, Détacher le volume. Une fois le statut du volume passé à disponible, passez à l'étape suivante.

6. Si vous avez créé une nouvelle instance pour remplacer votre instance d'origine, vous pouvez mettre fin à l'instance d'origine dès maintenant. Ce n'est plus nécessaire. Pour le reste de cette procédure, toutes les références à l'instance d'origine s'appliquent à la nouvelle instance que vous avez créée.

Étape 3 : Attacher le volume à une instance temporaire

Ensuite, lancez une instance temporaire et attachez-lui le volume en tant que volume secondaire. Il s'agit de l'instance que vous utilisez pour modifier le fichier de configuration.

Pour lancer une instance temporaire et attacher le volume

1. Lancez l'instance temporaire comme suit :

   a. Dans le volet de navigation, choisissez Instances, Launch instances, puis sélectionnez unAMI.

> **Important**
>
> Pour éviter les collisions entre les signatures de disque, vous devez sélectionner un AMI pour une autre version de Windows. Par exemple, si l'instance d'origine exécute Windows Server 2019, lancez l'instance temporaire à l'aide de la base AMI pour Windows Server 2016.

b. Quittez le type d'instance par défaut, puis choisissez Suivant : configurer les détails de l'instance.

c. Dans la page Configurer les détails d'instance, pour Sous-réseau, sélectionnez la même zone de disponibilité que l'instance d'origine et choisissez Revoir et lancer.

> **Important**
>
> Lancez une instance temporaire dans la même zone de disponibilité que l'instance d'origine. Si votre instance temporaire se trouve dans une zone de disponibilité différente, vous ne pouvez pas y attacher le volume racine de l'instance d'origine.

d. Sur la page Review Instance Launch, sélectionnez Launch.

e. Lorsque vous y êtes invité, créez une nouvelle paire de clés, téléchargez-la dans un emplacement sûr de votre ordinateur, puis choisissez Lancer des instances.

2. Attachez le volume à l'instance temporaire en tant que volume secondaire, comme suit :

a. Dans le panneau de navigation, sélectionnez Volumes, choisissez le volume que vous avez détaché de l'instance d'origine, et sélectionnez Actions, Attacher un volume.

b. Dans la boîte de dialogue Attacher un volume, pour Instances, commencez par saisir le nom ou l'ID de votre instance temporaire, puis sélectionnez-la dans la liste.

c. Pour Appareil, saisissez **`xvdf`** (s'il n'est pas déjà présent), puis choisissezAttacher.

Étape 4 : Supprimer le fichier .run-once.

Vous devez à présent supprimer le fichier `.run-once` du volume hors ligne attaché à l'instance. Cela indique à la EC2Launch v2 d'exécuter toutes les tâches avec une fréquence de`once`, y compris la définition du mot de passe administrateur. Le chemin du fichier dans le volume secondaire que vous avez joint est similaire à `D:\ProgramData\Amazon\EC2Launch\state\.run-once`.

Pour supprimer le fichier .run-once

1. Ouvrez l'utilitaire de gestion des disques et mettez le lecteur en ligne en suivant ces instructions : Rendre un EBS volume Amazon disponible pour utilisation.
2. Localisez le fichier `.run-once` sur le disque que vous avez mis en ligne.
3. Supprimez le fichier .run-once.

> **Important**
>
> Tous les scripts définis comme devant être exécutés une fois seront déclenchés par cette action.

Étape 5 : Redémarrer l'instance originale

Après avoir supprimé le fichier `.run-once`, rattachez le volume à l'instance originale en tant que volume racine et connectez-vous à l'instance en utilisant sa paire de clés pour récupérer le mot de passe administrateur.

1. Rattachez le volume à l'instance originale comme suit :
   a. Dans le panneau de navigation, choisissez Volumes, sélectionnez le volume que vous avez détaché de l'instance temporaire, et sélectionnez Actions, Attacher un volume.
   b. Dans la boîte de dialogue Attacher un volume, pour Instances, saisissez le nom ou l'ID de votre instance d'origine, puis sélectionnez l'instance.
   c. Pour Appareil, saisissez **`/dev/sda1`**.
   d. Choisissez Attacher. Une fois le statut du volume passé à `in-use`, passez à l'étape suivante.
2. Dans le panneau de navigation, choisissez Instances. Sélectionnez l'instance d'origine et choisissez État de l'instance, Démarrer l'instance. Après que l'état de l'instance est passé à `Running`, passez à l'étape suivante.
3. Récupérez votre nouveau mot de passe administrateur Windows à l'aide de la clé privée de la nouvelle paire de clés et connectez-vous à l'instance. Pour de plus amples informations, veuillez consulter Connectez-vous à votre instance Windows à l'aide de RDP.

> **Important**
>
> L'instance reçoit une nouvelle adresse IP publique après que vous l'arrêtiez et la redémarriez. Assurez-vous de vous connecter à l'instance en utilisant son DNS nom public actuel. Pour de plus amples informations, veuillez consulter Modifications de l'état de l'EC2instance Amazon.

4. (Facultatif) Vous pouvez résilier l'instance temporaire si vous n'en avez plus besoin. Sélectionnez l'instance temporaire, puis choisissez État de l'instance et Résilier l'instance.

Réinitialisez le mot de passe administrateur Windows, EC2 par exemple en utilisant EC2Launch

Si vous avez perdu votre mot de passe administrateur Windows et que vous utilisez Windows Server 2016 ou version ultérieureAMI, vous pouvez utiliser l'EC2Rescueoutil, qui utilise le EC2Launch service pour générer un nouveau mot de passe.

Si vous utilisez un Windows Server 2016 ou une version ultérieure AMI qui n'inclut pas l'agent EC2Launch v2, vous pouvez utiliser la EC2Launch version v2 pour générer un nouveau mot de passe.

Si vous utilisez un Windows Server AMI antérieur à Windows Server 2016, consultezRéinitialisez le mot de passe administrateur Windows, EC2 par exemple en utilisant EC2Config.

> **Warning**
>
> Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instance sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

> **Note**
>
> Si vous avez désactivé le compte d'administrateur local sur l'instance et que celle-ci est configurée pour Systems Manager, vous pouvez également réactiver et réinitialiser votre mot de passe d'administrateur local en utilisant EC2Rescue and Run Command. Pour

plus d'informations, consultez la section Utiliser EC2Rescue pour Windows Server avec la commande d'exécution de Systems Manager.

> **Note**
>
> Il existe un document AWS Systems Manager d'automatisation qui applique automatiquement les étapes manuelles nécessaires pour réinitialiser le mot de passe de l'administrateur local. Pour plus d'informations, consultez la section Réinitialiser les mots de passe et SSH les clés EC2 des instances dans le Guide de AWS Systems Manager l'utilisateur.

Pour réinitialiser votre mot de passe administrateur Windows à l'aide deEC2Launch, vous devez procéder comme suit :

- Étape 1 : Détacher le volume racine de l'instance
- Étape 2 : Attacher le volume à une instance temporaire
- Étape 3 : Réinitialiser le mot de passe administrateur
- Étape 4 : Redémarrer l'instance originale

Étape 1 : Détacher le volume racine de l'instance

Vous ne pouvez pas l'utiliser EC2Launch pour réinitialiser un mot de passe administrateur si le volume sur lequel le mot de passe est stocké est attaché à une instance en tant que volume racine. Vous devez détacher le volume de l'instance originale avant de pouvoir l'attacher à une instance temporaire en tant que volume secondaire.

Détacher le volume racine de l'instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance qui nécessite une réinitialisation du mot de passe et choisissez État de l'instance, Arrêter l'instance. Une fois que le statut de l'instance est passé à Arrêtée, passez à l'étape suivante.

4. (Facultatif) Si vous disposez de la clé privée que vous avez spécifiée lors du lancement de cette instance, passez à l'étape suivante. Sinon, procédez comme suit pour remplacer l'instance par une nouvelle instance que vous lancez par une nouvelle paire de clés.

   a. Créez une nouvelle paire de clés à l'aide de la EC2 console Amazon. Si vous souhaitez nommer votre nouvelle paire de clés exactement comme la clé privée perdue, vous devez commencer par supprimer la paire de clés existante.

   b. Sélectionnez l'instance à remplacer. Notez le type d'instanceVPC, le sous-réseau, le groupe de sécurité et le IAM rôle de l'instance.

   c. Une fois l'instance sélectionnée, choisissez Actions, Image et modèles, puis Créer une image. Saisissez le nom et la description de l'image, puis choisissez Créer l'image.

   d. Dans le volet de navigation, choisissez AMIs. Attendez que le statut de l'image passe à disponible. Sélectionnez ensuite l'image et choisissez Launch instance from AMI.

   e. Renseignez les champs pour lancer une instance, en veillant à sélectionner le même type d'instance, VPC le même sous-réseau, le même groupe de sécurité et le même IAM rôle que l'instance à remplacer, puis choisissez Launch instance.

   f. Lorsque vous y êtes invité, choisissez la paire de clés que vous avez créée pour la nouvelle instance, puis choisissez Launch instance.

   g. (Facultatif) Si l'instance d'origine a une adresse IP Elastic associée, associez-la à la nouvelle instance. Si l'instance d'origine possède EBS des volumes en plus du volume racine, transférez-les vers la nouvelle instance.

5. Détachez le volume racine de l'instance d'origine comme suit :

   a. Sélectionnez l'instance d'origine et cliquez sur l'onglet Stockage. Notez le nom du périphérique racine sous Nom du périphérique racine. Recherchez le volume portant ce nom de périphérique sous Bloquer les appareils et notez l'ID du volume.

   b. Dans le panneau de navigation, choisissez Volumes.

   c. Dans la liste des volumes, sélectionnez le volume que vous avez noté comme périphérique racine, puis choisissez Actions, Détacher le volume. Une fois le statut du volume passé à disponible, passez à l'étape suivante.

6. Si vous avez créé une nouvelle instance pour remplacer votre instance d'origine, vous pouvez mettre fin à l'instance d'origine dès maintenant. Ce n'est plus nécessaire. Pour le reste de cette procédure, toutes les références à l'instance d'origine s'appliquent à la nouvelle instance que vous avez créée.

Étape 2 : Attacher le volume à une instance temporaire

Ensuite, lancez une instance temporaire et attachez-lui le volume en tant que volume secondaire. Il s'agit de l'instance que vous utilisez pour exécuterEC2Launch.

Pour lancer une instance temporaire et attacher le volume

1. Lancez l'instance temporaire comme suit :

   a. Dans le volet de navigation, choisissez Instances, Launch instances, puis sélectionnez unAMI.

   > **Important**
   >
   > Pour éviter les collisions entre les signatures de disque, vous devez sélectionner un AMI pour une autre version de Windows. Par exemple, si l'instance d'origine exécute Windows Server 2019, lancez l'instance temporaire à l'aide de la base AMI pour Windows Server 2016.

   b. Quittez le type d'instance par défaut, puis choisissez Suivant : configurer les détails de l'instance.

   c. Dans la page Configurer les détails d'instance, pour Sous-réseau, sélectionnez la même zone de disponibilité que l'instance d'origine et choisissez Revoir et lancer.

   > **Important**
   >
   > Lancez une instance temporaire dans la même zone de disponibilité que l'instance d'origine. Si votre instance temporaire se trouve dans une zone de disponibilité différente, vous ne pouvez pas y attacher le volume racine de l'instance d'origine.

   d. Sur la page Review Instance Launch, sélectionnez Launch.

   e. Lorsque vous y êtes invité, créez une nouvelle paire de clés, téléchargez-la dans un emplacement sûr de votre ordinateur, puis choisissez Lancer des instances.

2. Attachez le volume à l'instance temporaire en tant que volume secondaire, comme suit :

   a. Dans le panneau de navigation, sélectionnez Volumes, choisissez le volume que vous avez détaché de l'instance d'origine, et sélectionnez Actions, Attacher un volume.

b. Dans la boîte de dialogue Attacher un volume, pour Instances, commencez par saisir le nom ou l'ID de votre instance temporaire, puis sélectionnez-la dans la liste.

c. Pour Appareil, saisissez **xvdf** (s'il n'est pas déjà présent), puis choisissezAttacher.

Étape 3 : Réinitialiser le mot de passe administrateur

Ensuite, connectez-vous à l'instance temporaire et utilisez-la EC2Launch pour réinitialiser le mot de passe administrateur.

Pour réinitialiser le mot de passe administrateur

1. Connectez-vous à l'instance temporaire et utilisez l'outil EC2Rescue pour Windows Server sur l'instance pour réinitialiser le mot de passe administrateur comme suit :

   a. Téléchargez le fichier zip EC2Rescuepour Windows Server, extrayez le contenu et exécutez le fichier EC2Rescue.exe.

   b. Sur l'écran License Agreement (Contrat de licence), lisez le contrat de licence et, si vous acceptez les conditions, choisissez I agree (J'accepte).

   c. Sur l'écran Bienvenue EC2Rescue sur Windows Server, choisissez Next.

   d. Sur l'écran Select mode, choisissez Offline instance.

   e. Sur l'écran Select a disk, sélectionnez le périphérique xvdf et choisissez Next.

   f. Confirmez la sélection de disque et choisissez Yes (Oui).

   g. Une fois le volume chargé, choisissez OK.

   h. Sur l'écran Select Offline Instance Option, choisissez Diagnose and Rescue.

   i. Sur l'écran Summary, vérifiez les informations, puis choisissez Next.

   j. Sur l'écran Detected possible issues, sélectionnez Reset Administrator Password et choisissez Next.

   k. Sur l'écran Confirm, choisissez Rescue, OK.

   l. Sur l'écran Done, choisissez Finish.

   m. Fermez l'outil EC2Rescue pour Windows Server, déconnectez-vous de l'instance temporaire, puis revenez à la EC2 console Amazon.

2. Détachez le volume (`xvdf`) secondaire de l'instance temporaire comme suit :

   a. Dans le panneau de navigation, sélectionnez Instances et choisissez l'instance temporaire.

b. Dans l'onglet Stockage de l'instance temporaire, notez l'ID du EBS volume répertorié sous la forme xvdf.

c. Dans le panneau de navigation, choisissez Volumes.

d. Dans la liste des volumes, sélectionnez le volume noté à l'étape précédente, puis choisissez Actions et Détacher un volume. Une fois le statut du volume passé à disponible, passez à l'étape suivante.

Étape 4 : Redémarrer l'instance originale

Après avoir réinitialisé le mot de passe administrateurEC2Launch, rattachez le volume à l'instance d'origine en tant que volume racine et connectez-vous à l'instance à l'aide de sa paire de clés pour récupérer le mot de passe administrateur.

Pour redémarrer l'instance originale

1. Rattachez le volume à l'instance originale comme suit :

   a. Dans le panneau de navigation, choisissez Volumes, sélectionnez le volume que vous avez détaché de l'instance temporaire, et sélectionnez Actions, Attacher un volume.

   b. Dans la boîte de dialogue Attacher un volume, pour Instances, saisissez le nom ou l'ID de votre instance d'origine, puis sélectionnez l'instance.

   c. Pour Appareil, saisissez **`/dev/sda1`**.

   d. Choisissez Attacher. Une fois le statut du volume passé à `in-use`, passez à l'étape suivante.

2. Dans le panneau de navigation, choisissez Instances. Sélectionnez l'instance d'origine et choisissez État de l'instance, Démarrer l'instance. Après que l'état de l'instance est passé à `Running`, passez à l'étape suivante.

3. Récupérez votre nouveau mot de passe administrateur Windows à l'aide de la clé privée de la nouvelle paire de clés et connectez-vous à l'instance. Pour de plus amples informations, veuillez consulter Connectez-vous à votre instance Windows à l'aide de RDP.

4. (Facultatif) Vous pouvez résilier l'instance temporaire si vous n'en avez plus besoin. Sélectionnez l'instance temporaire, puis choisissez État de l'instance et Résilier l'instance.

Réinitialisez le mot de passe administrateur Windows, EC2 par exemple en utilisant EC2Config

Si vous avez perdu votre mot de passe administrateur Windows et que vous utilisez un système Windows AMI antérieur à Windows Server 2016, vous pouvez utiliser l'EC2Configagent pour générer un nouveau mot de passe.

Si vous utilisez Windows Server 2016 ou version ultérieureAMI, consultez Réinitialisez le mot de passe administrateur Windows, EC2 par exemple en utilisant EC2Launch ou vous pouvez utiliser l'EC2Rescueoutil, qui utilise le EC2Launch service pour générer un nouveau mot de passe.

> **Note**
>
> Si vous avez désactivé le compte d'administrateur local sur l'instance et que celle-ci est configurée pour Systems Manager, vous pouvez également réactiver et réinitialiser votre mot de passe d'administrateur local en utilisant EC2Rescue and Run Command. Pour plus d'informations, consultez la section Utiliser EC2Rescue pour Windows Server avec la commande d'exécution de Systems Manager.

> **Note**
>
> Il existe un document AWS Systems Manager d'automatisation qui applique automatiquement les étapes manuelles nécessaires pour réinitialiser le mot de passe de l'administrateur local. Pour plus d'informations, consultez la section Réinitialiser les mots de passe et SSH les clés EC2 des instances dans le Guide de AWS Systems Manager l'utilisateur.

Pour réinitialiser votre mot de passe administrateur Windows à l'aide deEC2Config, vous devez procéder comme suit :

- Étape 1 : vérifier que le EC2Config service est en cours d'exécution
- Étape 2 : Détacher le volume racine de l'instance
- Étape 3 : Attacher le volume à une instance temporaire
- Étape 4 : Modifier le fichier de configuration
- Étape 5 : Redémarrer l'instance originale

Étape 1 : vérifier que le EC2Config service est en cours d'exécution

Avant de tenter de réinitialiser le mot de passe administrateur, vérifiez que le EC2Config service est installé et en cours d'exécution. Vous utiliserez le EC2Config service pour réinitialiser le mot de passe administrateur plus loin dans cette section.

Pour vérifier que le EC2Config service est en cours d'exécution

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Instances, puis sélectionnez l'instance dont le mot de passe doit être réinitialisé. Cette instance s'appelle l'instance originale dans cette procédure.
3. Sélectionnez Actions, Surveiller et dépanner, Obtenir le journal système.
4. Localisez l'entrée EC2 Agent, par exemple EC2Agent : Ec2Config service v3.18.1118. Si vous voyez cette entrée, le EC2Config service est en cours d'exécution.

   Si le résultat du journal système est vide ou si le EC2Config service n'est pas en cours d'exécution, dépannez l'instance à l'aide du service Instance Console Screenshot. Pour de plus amples informations, veuillez consulter Création d'une capture d'écran d'une instance inaccessible.

Étape 2 : Détacher le volume racine de l'instance

Vous ne pouvez pas l'utiliser EC2Config pour réinitialiser un mot de passe administrateur si le volume sur lequel le mot de passe est stocké est attaché à une instance en tant que volume racine. Vous devez détacher le volume de l'instance originale avant de pouvoir l'attacher à une instance temporaire en tant que volume secondaire.

Détacher le volume racine de l'instance

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance qui nécessite une réinitialisation du mot de passe et choisissez État de l'instance, Arrêter l'instance. Une fois que le statut de l'instance est passé à Arrêtée, passez à l'étape suivante.
4. (Facultatif) Si vous disposez de la clé privée que vous avez spécifiée lors du lancement de cette instance, passez à l'étape suivante. Sinon, procédez comme suit pour remplacer l'instance par une nouvelle instance que vous lancez par une nouvelle paire de clés.

a. Créez une nouvelle paire de clés à l'aide de la EC2 console Amazon. Si vous souhaitez nommer votre nouvelle paire de clés exactement comme la clé privée perdue, vous devez commencer par supprimer la paire de clés existante.

b. Sélectionnez l'instance à remplacer. Notez le type d'instanceVPC, le sous-réseau, le groupe de sécurité et le IAM rôle de l'instance.

c. Une fois l'instance sélectionnée, choisissez Actions, Image et modèles, puis Créer une image. Saisissez le nom et la description de l'image, puis choisissez Créer l'image.

d. Dans le volet de navigation, choisissez AMIs. Attendez que le statut de l'image passe à disponible. Sélectionnez ensuite l'image et choisissez Launch instance from AMI.

e. Renseignez les champs pour lancer une instance, en veillant à sélectionner le même type d'instance, VPC le même sous-réseau, le même groupe de sécurité et le même IAM rôle que l'instance à remplacer, puis choisissez Launch instance.

f. Lorsque vous y êtes invité, choisissez la paire de clés que vous avez créée pour la nouvelle instance, puis choisissez Launch instance.

g. (Facultatif) Si l'instance d'origine a une adresse IP Elastic associée, associez-la à la nouvelle instance. Si l'instance d'origine possède EBS des volumes en plus du volume racine, transférez-les vers la nouvelle instance.

5. Détachez le volume racine de l'instance d'origine comme suit :

a. Sélectionnez l'instance d'origine et cliquez sur l'onglet Stockage. Notez le nom du périphérique racine sous Nom du périphérique racine. Recherchez le volume portant ce nom de périphérique sous Bloquer les appareils et notez l'ID du volume.

b. Dans le panneau de navigation, choisissez Volumes.

c. Dans la liste des volumes, sélectionnez le volume que vous avez noté comme périphérique racine, puis choisissez Actions, Détacher le volume. Une fois le statut du volume passé à disponible, passez à l'étape suivante.

6. Si vous avez créé une nouvelle instance pour remplacer votre instance d'origine, vous pouvez mettre fin à l'instance d'origine dès maintenant. Ce n'est plus nécessaire. Pour le reste de cette procédure, toutes les références à l'instance d'origine s'appliquent à la nouvelle instance que vous avez créée.

Étape 3 : Attacher le volume à une instance temporaire

Ensuite, lancez une instance temporaire et attachez-lui le volume en tant que volume secondaire. Il s'agit de l'instance que vous utilisez pour modifier le fichier de configuration.

Pour lancer une instance temporaire et attacher le volume

1. Lancez l'instance temporaire comme suit :

   a. Dans le volet de navigation, choisissez Instances, Launch instances, puis sélectionnez unAMI.

   > **Important**
   >
   > Pour éviter les collisions entre les signatures de disque, vous devez sélectionner un AMI pour une autre version de Windows. Par exemple, si l'instance d'origine exécute Windows Server 2019, lancez l'instance temporaire à l'aide de la base AMI pour Windows Server 2016.

   b. Quittez le type d'instance par défaut, puis choisissez Suivant : configurer les détails de l'instance.

   c. Dans la page Configurer les détails d'instance, pour Sous-réseau, sélectionnez la même zone de disponibilité que l'instance d'origine et choisissez Revoir et lancer.

   > **Important**
   >
   > Lancez une instance temporaire dans la même zone de disponibilité que l'instance d'origine. Si votre instance temporaire se trouve dans une zone de disponibilité différente, vous ne pouvez pas y attacher le volume racine de l'instance d'origine.

   d. Sur la page Review Instance Launch, sélectionnez Launch.

   e. Lorsque vous y êtes invité, créez une nouvelle paire de clés, téléchargez-la dans un emplacement sûr de votre ordinateur, puis choisissez Lancer des instances.

2. Attachez le volume à l'instance temporaire en tant que volume secondaire, comme suit :

   a. Dans le panneau de navigation, sélectionnez Volumes, choisissez le volume que vous avez détaché de l'instance d'origine, et sélectionnez Actions, Attacher un volume.

b. Dans la boîte de dialogue Attacher un volume, pour Instances, commencez par saisir le nom ou l'ID de votre instance temporaire, puis sélectionnez-la dans la liste.

c. Pour Appareil, saisissez **`xvdf`** (s'il n'est pas déjà présent), puis choisissezAttacher.

Étape 4 : Modifier le fichier de configuration

Après avoir attaché le volume à une instance temporaire en tant que volume secondaire, modifiez le plug-in `Ec2SetPassword` dans le fichier de configuration.

Pour modifier le fichier de configuration

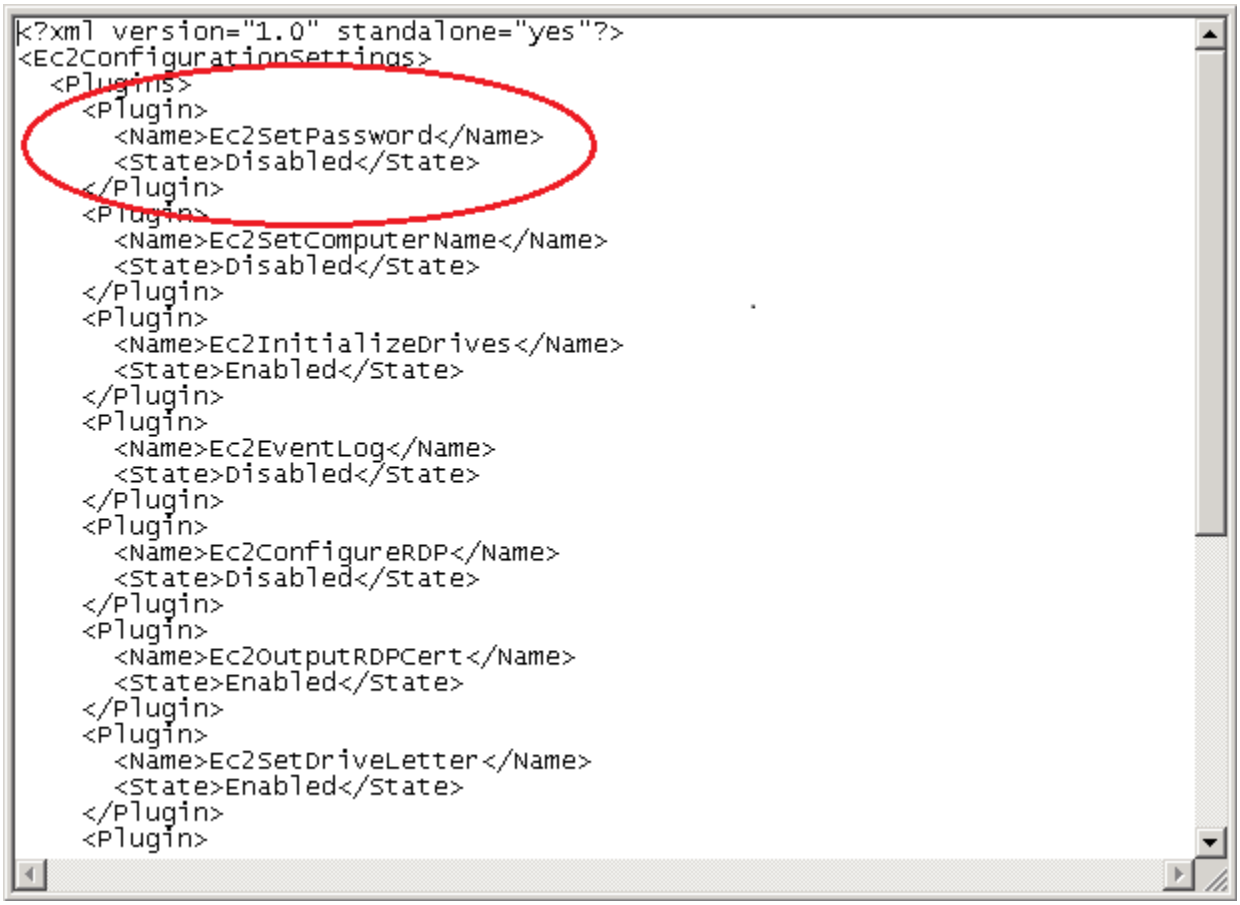
1. Dans l'instance temporaire, modifiez le fichier de configuration sur le volume secondaire comme suit :

   a. Lancez et connectez-vous à l'instance temporaire.

   b. Suivez les instructions suivantes pour mettre le lecteur en ligne : Rendre un EBS volume Amazon disponible pour utilisation.

   c. Accédez au volume secondaire et ouvrez `\Program Files\Amazon \Ec2ConfigService\Settings\config.xml` à l'aide d'un éditeur de texte comme le Bloc-notes.

   d. En haut du fichier, recherchez le plug-in portant le nom `Ec2SetPassword`, comme illustré dans la capture d'écran. Remplacez la valeur `Disabled` de l'état par `Enabled` et enregistrez le fichier.



2. Après avoir modifié le fichier de configuration, détachez le volume secondaire de l'instance temporaire comme suit :

   a. À l'aide de l'utilitaire Gestion des disques, déconnectez le volume.

   b. Déconnectez-vous de l'instance temporaire et revenez sur la EC2 console Amazon.

   c. Dans le panneau de navigation, sélectionnez Volumes, choisissez le volume, puis sélectionnez Actions, Détacher un volume. Une fois le statut du volume passé à disponible, passez à l'étape suivante.

Étape 5 : Redémarrer l'instance originale

Après avoir modifié le fichier de configuration, rattachez le volume à l'instance originale en tant que volume racine et connectez-vous à l'instance en utilisant sa paire de clés pour récupérer le mot de passe administrateur.

1. Rattachez le volume à l'instance originale comme suit :

a. Dans le panneau de navigation, choisissez Volumes, sélectionnez le volume que vous avez détaché de l'instance temporaire, et sélectionnez Actions, Attacher un volume.

b. Dans la boîte de dialogue Attacher un volume, pour Instances, saisissez le nom ou l'ID de votre instance d'origine, puis sélectionnez l'instance.

c. Pour Appareil, saisissez **`/dev/sda1`**.

d. Choisissez Attacher. Une fois le statut du volume passé à `in-use`, passez à l'étape suivante.

2. Dans le panneau de navigation, choisissez Instances. Sélectionnez l'instance d'origine et choisissez État de l'instance, Démarrer l'instance. Après que l'état de l'instance est passé à `Running`, passez à l'étape suivante.

3. Récupérez votre nouveau mot de passe administrateur Windows à l'aide de la clé privée de la nouvelle paire de clés et connectez-vous à l'instance. Pour de plus amples informations, veuillez consulter Connectez-vous à votre instance Windows à l'aide de RDP.

> **Important**
>
> L'instance reçoit une nouvelle adresse IP publique après que vous l'arrêtiez et la redémarriez. Assurez-vous de vous connecter à l'instance en utilisant son DNS nom public actuel. Pour de plus amples informations, veuillez consulter Modifications de l'état de l'EC2instance Amazon.

4. (Facultatif) Vous pouvez résilier l'instance temporaire si vous n'en avez plus besoin. Sélectionnez l'instance temporaire, puis choisissez État de l'instance et Résilier l'instance.

Résoudre les problèmes liés à Sysprep avec les instances Amazon Windows EC2

Si vous rencontrez des problèmes ou que vous recevez des messages d'erreur pendant les préparations d'images, consultez les journaux suivants : L'emplacement du journal varie selon que vous utilisez EC2Config Sysprep en version EC2Launch v1 ou EC2Launch v2.

- `%WINDIR%\Panther\Unattendgc`(EC2Config, EC2Launch v1 et EC2Launch v2)
- `%WINDIR%\System32\Sysprep\Panther`(EC2Config, EC2Launch v1 et EC2Launch v2)

- `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt`(EC2Configuniquement)
- `C:\ProgramData\Amazon\Ec2Config\Logs`(EC2Configuniquement)
- `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\EC2Launch.log`(EC2Launchv1 uniquement)
- `%ProgramData%\Amazon\EC2Launch\log\agent.log`(EC2Launchv2 uniquement)

Si vous recevez un message d'erreur pendant la préparation de l'image avec Sysprep, il se peut que le système d'exploitation ne soit pas disponible. Pour consulter les fichiers journaux, vous devez arrêter l'instance, attacher son volume racine à une autre instance sain sur un volume secondaire, puis consulter les journaux mentionnés précédemment sur le volume secondaire. Pour plus d'informations sur l'objectif des fichiers journaux par nom, veuillez consulter Windows Setup-Related Log Files dans la documentation Microsoft.

Si vous trouvez des erreurs dans le fichier journal Unattendgc, utilisez l'outil Error Lookup de Microsoft pour en savoir plus sur les erreurs. Le problème suivant signalé dans le fichier journal Unattendgc est généralement dû à un ou plusieurs profils utilisateur corrompus sur l'instance :

```
Error [Shell Unattend] _FindLatestProfile failed (0x80070003) [gle=0x00000003]
Error [Shell Unattend] CopyProfile failed (0x80070003) [gle=0x00000003]
```

Vous avez deux options à votre disposition pour le résoudre :

Option 1

Utilisez Regedit sur l'instance pour rechercher la clé suivante. Vérifiez qu'il n'existe aucune clé de registre de profil d'utilisateur supprimé.

`[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\`

Option 2

1. Modifiez le fichier concerné, comme suit :

   - Windows Server 2012 R2 et versions antérieures : modifiez le fichier de EC2Config réponses (`C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml`).
   - Windows Server 2016 et 2019 – Modifiez le fichier de réponses unattend.xml (`C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml`).

- Windows Server 2022 – Modifiez le fichier de réponse unattend.xml (`C:\ProgramData\Amazon\EC2Launch\sysprep\unattend.xml`).

2. Remplacez `<CopyProfile>true</CopyProfile>` par `<CopyProfile>false</CopyProfile>`
3. Exécutez à nouveau Sysprep. Notez que cette modification apportée à la configuration entraîne la suppression du profil utilisateur de l'administrateur intégré une fois Sysprep terminé.

Résolvez les problèmes liés à une instance Amazon EC2 Linux défectueuse à l'aide de EC2Rescue

EC2Rescuefor Linux est un easy-to-use outil open source qui peut être exécuté sur une instance Amazon EC2 Linux pour diagnostiquer, résoudre et résoudre les problèmes courants à l'aide de sa bibliothèque de plus de 100 modules. Les modules sont des YAML fichiers contenant un script BASH ou un script Python ainsi que les métadonnées nécessaires.

Voici quelques cas d'utilisation généralisés EC2Rescue pour les instances Linux :

- Collecte des journaux Syslog et du gestionnaire de paquets
- Collecte de données sur l'utilisation des ressources
- Diagnostic et correction des paramètres de noyau problématiques connus et des problèmes courants en suspens SSH

> **Note**
>
> Le runbook `AWSSupport-TroubleshootSSH` AWS Systems Manager Automation s'installe EC2Rescue pour Linux, puis utilise l'outil pour vérifier ou tenter de résoudre les problèmes courants qui empêchent la SSH connexion à une instance Linux. Pour plus d'informations, consultez AWSSupport-Troubleshoot SSH.

Si vous utilisez une instance Windows, consultezthe section called "EC2Rescuepour les instances Windows".

Rubriques

- Installation EC2Rescue sur une instance Amazon EC2 Linux

- Exécuter EC2Rescue des commandes sur une instance Amazon EC2 Linux
- Développez EC2Rescue des modules pour les instances Amazon EC2 Linux

Installation EC2Rescue sur une instance Amazon EC2 Linux

L'outil EC2Rescue pour Linux peut être installé sur une instance Amazon EC2 Linux qui répond aux exigences suivantes.

Prérequis

- Systèmes d'exploitation pris en charge :
  - Amazon Linux 2
  - Amazon Linux 2016.09+
  - SUSEServeur Linux Enterprise 12+
  - RHEL7 ans et plus
  - Ubuntu 16.04+
- Configuration logicielle requise :
  - Python 2.7.9+ ou 3.2+

Installer EC2Rescue

Le `AWSSupport-TroubleshootSSH` runbook s'installe EC2Rescue pour Linux, puis utilise l'outil pour vérifier ou tenter de résoudre les problèmes courants qui empêchent une connexion à distance à une machine Linux via. SSH Pour plus d'informations et pour exécuter cette automatisation, consultez AWS Support-Troubleshoot SSH.

Si votre système dispose de la version Python requise, vous pouvez installer la build standard. Dans le cas contraire, vous pouvez installer la build de la solution groupée, qui inclut une copie minimale de Python.

Pour installer la build standard

1. À partir d'une instance Linux fonctionnelle, téléchargez l'outil EC2Rescuepour Linux :

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz
```

2. (Facultatif) Vérifiez la signature du fichier d'installation EC2Rescue pour Linux. Pour de plus amples informations, veuillez consulter (Facultatif) Vérifiez la signature de EC2Rescue pour Linux.
3. Téléchargez le fichier de hachage sha256 :

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sha256
```

4. Vérifiez l'intégrité du tarball :

```
sha256sum -c ec2rl.tgz.sha256
```

5. Déballez le tarball :

```
tar -xzvf ec2rl.tgz
```

6. Vérifiez l'installation en énumérant le fichier d'aide :

```
cd ec2rl-<version_number>
./ec2rl help
```

Pour installer la build de la solution groupée

Pour un lien vers le téléchargement et une liste des limitations, consultez EC2RescueLinux sur github.

(Facultatif) Vérifiez la signature de EC2Rescue pour Linux

Voici le processus recommandé pour vérifier la validité du package EC2Rescue pour Linux pour les systèmes d'exploitation basés sur Linux.

Lorsque vous téléchargez une application à partir d'Internet, nous vous recommandons d'authentifier l'identité de l'éditeur du logiciel et de vérifier que l'application n'a pas été modifiée ou corrompue depuis sa publication. Cela vous évitera d'installer une version de l'application contenant un virus ou tout autre code malveillant.

Si, après avoir exécuté les étapes décrites dans cette rubrique, vous constatez que le logiciel EC2Rescue pour Linux est altéré ou endommagé, n'exécutez pas le fichier d'installation. Contactez plutôt Amazon Web Services.

EC2Rescuepour Linux, les fichiers pour les systèmes d'exploitation basés sur Linux sont signés à l'aide de GnuPG, une implémentation open source du standard Pretty Good Privacy (Open) pour les signatures numériques sécurisées. PGP GnuPG (également connu sous GPG le nom de) fournit une authentification et une vérification d'intégrité par le biais d'une signature numérique. AWS publie une clé publique et des signatures que vous pouvez utiliser pour vérifier le package téléchargé EC2Rescue pour Linux. Pour plus d'informations sur PGP GnuPG GPG (), consultez http://www.gnupg.org.

La première étape consiste à établir une approbation avec l'éditeur du logiciel. Téléchargez la clé publique de l'éditeur du logiciel, vérifiez que le propriétaire de cette clé publique est bien celui qu'il prétend être, puis ajoutez la clé publique à votre porte-clés. Votre porte-clés est un ensemble de clés publiques connues. Après avoir établi l'authenticité de la clé publique, vous pouvez l'utiliser pour vérifier la signature de l'application.

Tâches

- Authentification et importation de la clé publique
- Vérification de la signature du package

Authentification et importation de la clé publique

L'étape suivante du processus consiste à authentifier la clé publique EC2Rescue pour Linux et à l'ajouter en tant que clé fiable dans votre GPG trousseau de clés.

Pour authentifier et importer la clé publique EC2Rescue pour Linux

1. À l'invite de commande, utilisez la commande suivante pour obtenir une copie de notre clé de GPG compilation publique :

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.key
   ```

2. À l'invite de commande dans le répertoire où vous avez enregistré`ec2rl.key`, utilisez la commande suivante pour importer la clé publique EC2Rescue pour Linux dans votre trousseau de clés :

   ```
   gpg2 --import ec2rl.key
   ```

   La commande renvoie un résultat semblable à ce qui suit :

```
gpg: /home/ec2-user/.gnupg/trustdb.gpg: trustdb created
gpg: key 2FAE2A1C: public key "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
 imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

> **Tip**
>
> Si vous voyez un message d'erreur indiquant que la commande est introuvable, installez l'utilitaire GnuPG `apt-get install gnupg2` avec (Linux basé sur Debian) `yum install gnupg2` ou (Linux basé sur Red Hat).

Vérification de la signature du package

Après avoir installé les GPG outils, authentifié et importé la clé publique EC2Rescue pour Linux, et vérifié que la clé publique EC2Rescue pour Linux est fiable, vous êtes prêt à vérifier la signature du script d'installation EC2Rescue pour Linux.

Pour vérifier la signature du script d'installation EC2Rescue pour Linux

1. À l'invite de commande, exécutez la commande suivante pour télécharger le fichier signature du script d'installation :

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sig
   ```

2. Vérifiez la signature en exécutant la commande suivante à l'invite de commande dans le répertoire où vous l'avez enregistrée `ec2rl.tgz.sig` et dans le fichier d'installation EC2Rescue pour Linux. Ces deux fichiers doivent être présents.

   ```
   gpg2 --verify ./ec2rl.tgz.sig
   ```

   Le résultat doit ressembler à ce qui suit :

   ```
   gpg: Signature made Thu 12 Jul 2018 01:57:51 AM UTC using RSA key ID 6991ED45
   gpg: Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
   gpg: WARNING: This key is not certified with a trusted signature!
   gpg:          There is no indication that the signature belongs to the owner.
   Primary key fingerprint: E528 BCC9 0DBF 5AFA 0F6C  C36A F780 4843 2FAE 2A1C
   ```

```
Subkey fingerprint: 966B 0D27 85E9 AEEC 1146  7A9D 8851 1153 6991 ED45
```

Si la sortie contient cette phraseGood `signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"`, cela signifie que la signature a été vérifiée avec succès et que vous pouvez exécuter le script d'installation EC2Rescue pour Linux.

Si le résultat inclut l'expression `BAD signature`, vérifiez si vous avez effectué la procédure correctement. Si vous continuez à obtenir cette réponse, contactez Amazon Web Services et n'exécutez pas le fichier d'installation que vous avez précédemment téléchargé.

Voici les informations détaillées sur les avertissements qui peuvent s'afficher :

- WARNING: This key is not certified with a trusted signature! There is no indication that the signature belongs to the owner.Cela fait référence à votre niveau de confiance personnel dans votre conviction que vous possédez une clé publique authentique EC2Rescue pour Linux. Dans un monde idéal, vous visiteriez un bureau Amazon Web Services et recevriez la clé en personne. Cependant, vous la téléchargez le plus souvent à partir d'un site Web. Dans le cas présent, le site Web est un site Amazon Web Services.
- gpg2: no ultimately trusted keys found. Cela signifie que la clé spécifique n'est pas « approuvée en dernier lieu » par vous-même (ou par d'autres personnes de confiance).

Pour plus d'informations, consultez http://www.gnupg.org.

Exécuter EC2Rescue des commandes sur une instance Amazon EC2 Linux

EC2Rescueest un outil en ligne de commande. Après l'avoir installé EC2Rescue sur votre instance Linux, vous pouvez obtenir de l'aide générale sur l'utilisation de l'outil en exécutant `./ec2rl help`. Vous pouvez consulter les modules disponibles en exécutant `./ec2rl list`, et vous pouvez obtenir de l'aide sur un module spécifique en exécutant `./ec2rl help` *`module_name`*.

Les tâches suivantes sont des tâches courantes que vous pouvez effectuer pour commencer à utiliser cet outil.

Tâches

- Exécuter EC2Rescue des modules
- Téléchargez les résultats EC2Rescue du module
- Création de sauvegardes d'une instance Amazon EC2 Linux

Exécuter EC2Rescue des modules

Pour exécuter tous les EC2Rescue modules

Utilisez la ./ec2rl run commande sans spécifier de paramètres supplémentaires. Certains modules nécessitent un accès racine. Si vous n'êtes pas un utilisateur root, sudo utilisez-le lorsque vous exécutez la commande.

```
./ec2rl run
```

Pour exécuter un EC2Rescue module spécifique

Utilisez la ./ec2rl run commande et pour`--only-modules`, spécifiez le nom du module à exécuter. Certains modules nécessitent des arguments pour les utiliser.

```
./ec2rl run --only-modules=module_name --arguments
```

Par exemple, pour exécuter le dig module afin d'interroger le `amazon.com` domaine, utilisez la commande suivante.

```
./ec2rl run --only-modules=dig --domain=amazon.com
```

Pour consulter les résultats d'un EC2Rescue module

Lancez le module puis visualisez le fichier journal`cat /var/tmp/ec2rl/logfile_location`. Par exemple, le fichier journal du dig module se trouve à l'emplacement suivant :

```
cat /var/tmp/ec2rl/timestamp/mod_out/run/dig.log
```

Téléchargez les résultats EC2Rescue du module

Si vous avez AWS Support demandé les résultats d'un EC2Rescue module, vous pouvez télécharger le fichier journal à l'aide de l'EC2Rescueoutil. Vous pouvez télécharger les résultats soit vers un emplacement fourni par, AWS Support soit vers un compartiment Amazon S3 dont vous êtes le propriétaire.

Pour télécharger les résultats vers un emplacement fourni par AWS Support

Utilisez la commande ./ec2rl upload. Pour`--upload-directory`, spécifiez l'emplacement du fichier journal. Pour`--support-url`, spécifiez le URL fourni par AWS Support.

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/logfile_location --support-
url="url_provided_by_aws_support"
```

Pour télécharger les résultats dans un compartiment Amazon S3

Utilisez la commande ./ec2rl upload. Pour`--upload-directory`, spécifiez l'emplacement du fichier journal. Pour`--presigned-url`, spécifiez un présigné URL pour le compartiment S3. Pour plus d'informations sur la génération de documents pré-signés URLs pour Amazon S3, consultez la section Chargement d'objets à l'aide de systèmes pré-signés. URLs

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/logfile_location --presigned-
url="presigned_s3_url"
```

Création de sauvegardes d'une instance Amazon EC2 Linux

Vous pouvez l'utiliser EC2Rescue pour sauvegarder votre instance Linux en créant un AMI ou en créant des instantanés de ses volumes attachés.

Pour créer un AMI

Utilisez la `./ec2rl run` commande et pour `--backup`, spécifie`ami`.

```
./ec2rl run --backup=ami
```

Pour créer des instantanés multivolumes de tous les volumes attachés

Utilisez la `./ec2rl run` commande et pour `--backup`, spécifie`allvolumes`.

```
./ec2rl run --backup=allvolumes
```

Pour créer un instantané d'un volume attaché spécifique

Utilisez la `./ec2rl run` commande et pour `--backup`, spécifiez l'ID du volume à sauvegarder.

```
./ec2rl run --backup=volume_id
```

Développez EC2Rescue des modules pour les instances Amazon EC2 Linux

Les modules sont écrits dans YAML une norme de sérialisation des données. Le YAML fichier d'un module se compose d'un seul document représentant le module et ses attributs.

Ajouter des attributs de module

Le tableau suivant répertorie les attributs de module disponibles.

Attribut	Description
name	Nom du module. La longueur du nom doit être inférieure ou égale à 18 caractères.
Version	Numéro de version du module.
title	Titre court et descriptif du module. La longueur de cette valeur doit être inférieure ou égale à 50 caractères.

helptext	Description étendue du module. La longueur de chaque ligne doit être inférieure ou égale à 75 caractères. Si le module consomme des arguments, obligatoires ou facultatifs, incluez-les dans la valeur helptext.
	
	Exemples :
	
	`helptext: !!str |`
	`  Collect output from ps for system analysis`
	`  Consumes --times= for number of times to repeat`
	`  Consumes --period= for time period between repetition`

placement	Étape dans laquelle le module doit être exécuté. Valeurs prises en charge :

Attribut	Description
	• prediagnostic • run • postdiagnostic
langage	Langage dans lequel le code du module est écrit. Valeurs prises en charge : • bash • python **Note** Le code Python doit être compatible avec Python 2.7.9+ et Python 3.2+.
remediation	Indique si le module prend en charge la correction. Les valeurs prises en charge sont `True` ou `False`. Le module utilise par défaut `False` si aucune valeur n'est indiquée. Il s'agit donc d'un attribut facultatif pour les modules qui ne prennent pas en charge la correction.
content	Intégralité du code de script.
contrainte	Nom de l'objet contenant les valeurs de contrainte.

Attribut	Description
domaine	Descripteur de la façon dont le module est regroupé ou classé. L'ensemble de modules inclus utilise les domaines suivants : • application • net • os • performances
class	Descripteur du type de tâche effectué par le module. L'ensemble de modules inclus utilise les classes suivantes : • collect (collecte la sortie des programmes) • diagnose (réussite/échec en fonction d'un ensemble de critères) • gather (copie les fichiers et écrit dans un fichier spécifique)
distro	Liste des distributions Linux que ce module prend en charge. L'ensemble de modules inclus utilise les distributions suivantes : • alami (Amazon Linux) • rhel • ubuntu • suse
obligatoire	Les arguments requis que le module consomme à partir des CLI options.
facultatif	Arguments facultatifs que le module peut utiliser.

Attribut	Description
logiciel	Exécutables logiciels utilisés dans le module. Cet attribut a pour but de spécifier un logiciel qui n'est pas installé par défaut. La logique EC2Rescue pour Linux garantit que ces programmes sont présents et exécutables avant d'exécuter le module.
package	Package logiciel source pour un exécutable. Cet attribut est destiné à fournir des informati ons détaillées sur le package contenant le logiciel, y compris un outil URL permettant de télécharger ou d'obtenir des informations supplémentaires.
sudo	Indique si l'accès racine est obligatoire pour exécuter le module. Vous n'avez pas besoin d'implémenter des vérifications sudo dans le script du module. Si la valeur est vraie, la logique EC2Rescue pour Linux n'exécute le module que lorsque l'utilisa teur exécutant dispose d'un accès root.
perfimpact	Indique si le module peut avoir un impact important sur les performances qui affecte l'environnement dans lequel il est exécuté. Si la valeur est true et que l'argument `--perfimp act=true` n'est pas présent, le module est ignoré.
parallelexclusive	Spécifie un programme qui requiert une exclusivité mutuelle. Par exemple, tous les modules qui spécifient « bpf » sont exécutés en série.

Ajouter des variables d'environnement

Le tableau suivant répertorie les variables d'environnement disponibles.

Variable d'environnement	Description
`EC2RL_CALLPATH`	Chemin vers `ec2rl.py`. Ce chemin peut être utilisé pour localiser le répertoire lib et utiliser les modules Python fournis.
`EC2RL_WORKDIR`	Répertoire tmp principal pour l'outil de diagnostic. Valeur par défaut: `/var/tmp/ec2rl` .
`EC2RL_RUNDIR`	Répertoire dans lequel toutes les sorties sont stockées. Valeur par défaut: `/var/tmp/ec2rl/<date&timestamp>` .
`EC2RL_GATHEREDDIR`	Répertoire racine dans lequel placer les données collectées sur le module. Valeur par défaut:`/var/tmp/ec2rl/<date&timestamp>/mod_out/gathered/` .
`EC2RL_NET_DRIVER`	Pilote utilisé pour la première interface réseau non virtuelle, triée par ordre alphabétique, de l'instance. Exemples : • xen_netfront • ixgbevf • ena

Variable d'environnement	Description
`EC2RL_SUDO`	True si EC2Rescue for Linux est exécuté en tant que root ; sinon, faux.
`EC2RL_VIRT_TYPE`	Type de virtualisation, tel que fourni par les métadonnées d'instance. Exemples : • default-hvm • default-paravirtual
`EC2RL_INTERFACES`	Liste énumérée des interfaces du système. La valeur est une chaîne contenant des noms, tels que `eth0`, `eth1`, etc. Elle est générée via `functions.bash` et est disponibl e uniquement pour les modules dont elle provient.

Utiliser YAML la syntaxe

Les points suivants doivent être pris en compte lors de la construction de vos YAML fichiers de module :

- Le triple trait d'union (`---`) indique le début explicite d'un document.
- La `!ec2rlcore.module.Module` balise indique à l'YAMLanalyseur quel constructeur appeler lors de la création de l'objet à partir du flux de données. Vous trouverez le constructeur dans le fichier `module.py`.
- La `!!str` balise indique à l'YAMLanalyseur de ne pas tenter de déterminer le type de données, mais d'interpréter le contenu comme une chaîne littérale.
- Le caractère pipe (`|`) indique à l'YAMLanalyseur que la valeur est un scalaire de style littéral. Dans ce cas, l'analyseur inclut tous les espaces. C'est important pour les modules car les caractères de mise en retrait et de saut de ligne sont conservés.
- Le retrait YAML standard est constitué de deux espaces, comme le montrent les exemples suivants. Veillez à conserver la mise en retrait standard (par exemple, quatre espaces pour Python)

pour votre script, puis mettez en retrait l'intégralité du contenu à l'aide de deux espaces dans le fichier du module.

Exemples de modules

Example un (`mod.d/ps.yaml`):

```
--- !ec2rlcore.module.Module
# Module document. Translates directly into an almost-complete Module object
name: !!str ps
path: !!str
version: !!str 1.0
title: !!str Collect output from ps for system analysis
helptext: !!str |
  Collect output from ps for system analysis
  Requires --times= for number of times to repeat
  Requires --period= for time period between repetition
placement: !!str run
package:
  - !!str
language: !!str bash
content: !!str |
  #!/bin/bash
  error_trap()
  {
      printf "%0.s=" {1..80}
      echo -e "\nERROR: "$BASH_COMMAND" exited with an error on line ${BASH_LINENO[0]}"
      exit 0
  }
  trap error_trap ERR

  # read-in shared function
  source functions.bash
  echo "I will collect ps output from this $EC2RL_DISTRO box for $times times every
 $period seconds."
  for i in $(seq 1 $times); do
      ps auxww
      sleep $period
  done
constraint:
  requires_ec2: !!str False
  domain: !!str performance
  class: !!str collect
```

```
  distro: !!str alami ubuntu rhel suse
  required: !!str period times
  optional: !!str
  software: !!str
  sudo: !!str False
  perfimpact: !!str False
  parallelexclusive: !!str
```

Résoudre les problèmes liés à une instance Amazon EC2 Windows défectueuse à l'aide de EC2Rescue

EC2Rescuefor Windows Server est un easy-to-use outil que vous exécutez sur une instance Amazon EC2 Windows Server pour diagnostiquer et résoudre d'éventuels problèmes. Il est utile non seulement pour collecter les fichiers journaux et résoudre les problèmes, mais aussi pour rechercher de manière proactive les éventuels sujets de préoccupation. Il peut même examiner les volumes EBS racine Amazon provenant d'autres instances et collecter les journaux pertinents pour le dépannage des instances Windows Server utilisant ce volume. Voici quelques problèmes courants qui EC2Rescue peuvent être résolus :

- Problèmes de connectivité de l'instance dus à la configuration du pare-feu, du protocole Remote Desktop (RDP) ou de l'interface réseau
- Problèmes de démarrage du système d'exploitation dus à une erreur d'arrêt, à une boucle de démarrage ou à un registre endommagé
- Problèmes susceptibles de nécessiter une analyse et un dépannage avancés des journaux

EC2Rescuepour Windows Server comporte deux modules différents :

- Un module de collecte de données qui collecte des données provenant de différentes sources
- Un module d'analyse qui analyse les données collectées par rapport à une série de règles prédéfinies pour identifier les problèmes et fournir des suggestions

L'outil EC2Rescue pour Windows Server s'exécute uniquement sur les EC2 instances Amazon exécutant Windows Server 2012 et versions ultérieures. Lorsque l'outil démarre, il vérifie s'il s'exécute sur une EC2 instance Amazon.

> **Note**
>
> Le runbook `AWSSupport-ExecuteEC2Rescue` AWS Systems Manager Automation utilise l'EC2Rescueoutil pour dépanner et, dans la mesure du possible, résoudre les problèmes de connectivité courants avec l'instance spécifiéeEC2. Pour plus d'informations et pour exécuter cette automatisation, voir > AWSSupport -Execute EC2Rescue.

Si vous utilisez une instance Linux, consultezthe section called "EC2Rescuepour les instances Linux".

Rubriques

- Résoudre les problèmes liés à une instance Windows défectueuse à l'aide du EC2Rescue GUI
- Résoudre les problèmes liés à une instance Windows défectueuse à l'aide du EC2Rescue CLI
- Résoudre les problèmes liés à une instance Windows avec EC2Rescue and Systems Manager

Résoudre les problèmes liés à une instance Windows défectueuse à l'aide du EC2Rescue GUI

EC2Rescuepour Windows Server, vous pouvez effectuer l'analyse suivante sur des instances hors ligne :

Option	Description
Diagnostic et résolution des problèmes	EC2Rescuepour Windows Server peut détecter et résoudre les problèmes liés aux paramètres de service suivants : • Heure du système • RealTimeisUniversal- Détecte si la clé de `RealTimeisUniversal` registre est activée. Si cette option est désactivé e, l'heure du système Windows dérive lorsque le fuseau horaire est défini sur une valeur autre que. UTC • Pare-feu Windows

Option	Description
	• Réseaux de domaine : détectent si ce profil de pare-feu Windows est activé ou désactivé. • Réseaux privés : détectent si ce profil de pare-feu Windows est activé ou désactivé. • Réseaux invités ou publics : détectent si ce profil de pare-feu Windows est activé ou désactivé. • Bureau à distance • Démarrage du service : détecte si le service bureau à distance est activé. • Connexions réseau à distance : détectent si cette option est activée. • TCPPort - Détecte le port sur lequel le service Remote Desktop écoute. • EC2Config(Windows Server 2012 R2 et versions antérieures) • Installation - Détecte EC2Config la version installée. • Service Start - Détecte si le EC2Config service est activé. • Ec2 SetPassword - Génère un nouveau mot de passe administrateur. • Ec2 HandleUserData - Vous permet d'exécuter un script de données utilisateur lors du prochain démarrage de l'instance. • EC2Launch(Windows Server 2016 et versions ultérieures)

Option	Description

	• Installation - Détecte EC2Launch la version installée.
	• Ec2 SetPassword - Génère un nouveau mot de passe administrateur.
	
	• Interface réseau
	  • DHCPDémarrage du service - Détecte si le DHCP service est activé.
	  • Détails Ethernet : affiche des informations détaillées sur la version de pilote réseau, si elle est détectée.
	  • DHCPsur Ethernet - Détecte si DHCP c'est activé.
	• État de signature de disque
	  • Signature sur disque et signature sur la base de données de configuration au démarrage (BCD) - Détecte si la signature du disque et la BCD signature sont identiques. Si les valeurs sont différent es, EC2Rescue tente de remplacer la signature du disque par la signature activéeBCD.

Restaurer	Effectuez l'une des opérations suivantes : • Dernière configuration correcte connue : tente de démarrer l'instance avec son dernier état de démarrage connu. • Restaurer le registre à partir de la sauvegard e : restaure le registre à partir de `\Windows\System32\config\RegBack` .

Option	Description
Capture Logs	Permet de capturer des journaux sur l'instance en vue de les analyser.

EC2Rescuepour Windows Server peut collecter les données suivantes à partir d'instances actives et hors ligne :

Élément	Description
Event Log	Collecte les journaux des applications, du système et des EC2Config événements.
Registre	Collecte les ruches `SYSTEM` et `SOFTWARE`.
Windows Update Log	Permet de collecter les fichiers journaux générés par Windows Update. **Note** Dans Windows Server 2016 et versions ultérieures, le journal est collecté au format Event Tracing for Windows (ETW).
Sysprep Log	Permet de collecter les fichiers journaux générés par l'outil Windows System Preparati on.
Journal de configuration du pilote	Collecte les API journaux d'installation de Windows (`setupapi.dev.log` et`setupapi.setup.log`).
Boot Configuration	Collecte la ruche `HKEY_LOCAL_MACHINE\BCD00000000` .

Élément	Description
Memory Dump	Permet de collecter les fichiers de vidage de mémoire existant sur l'instance.
EC2ConfigDossier	Collecte les fichiers journaux générés par le EC2Config service.
EC2LaunchDossier	Collecte les fichiers journaux générés par les EC2Launch scripts.
SSMFichier d'agent	Collecte les fichiers journaux générés par les journaux de SSM l'agent et du gestionnaire de correctifs.
EC2lasticGPUs Fichier E	Collecte les journaux d'événements liés à ElasticGPUs.
ECS	Collecte les journaux relatifs à AmazonECS.
CloudEndure	Collecte les fichiers journaux relatifs à CloudEndure l'agent.

EC2Rescuepour Windows Server peut collecter les données supplémentaires suivantes à partir d'instances actives :

Élément	Description
System Information	RecueilleMSInfo32.
Résultat de la politique de groupe	Collecte un rapport de politique de groupe.

Analyser une instance hors connexion

L'option Offline Instance (Instance hors ligne) est pratique pour déboguer les problèmes de démarrage liés aux instances Windows.

Pour effectuer une action sur une instance hors ligne

1. À partir d'une instance Windows Server fonctionnelle, téléchargez l'outil EC2Rescuepour Windows Server et extrayez les fichiers.

   Vous pouvez exécuter la PowerShell commande suivante pour télécharger EC2Rescue sans modifier votre configuration de sécurité renforcée d'Internet Explorer (ESC) :

   ```
   Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -
   OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
   ```

   Cette commande téléchargera le fichier EC2Rescue .zip sur le bureau de l'utilisateur actuellement connecté.

   > **Note**
   >
   > Si un message d'erreur s'affiche lors du téléchargement du fichier et que vous utilisez Windows Server 2016 ou une version antérieure, il est possible que la version TLS 1.2 doive être activée sur votre PowerShell terminal. Vous pouvez activer la TLS version 1.2 pour la PowerShell session en cours à l'aide de la commande suivante, puis réessayer :
   >
   > ```
   > [Net.ServicePointManager]::SecurityProtocol =
   >  [Net.SecurityProtocolType]::Tls12
   > ```

2. Arrêtez l'instance défaillante si ce n'est pas déjà fait.
3. Détachez le volume EBS racine de l'instance défectueuse et attachez-le à une instance Windows fonctionnelle sur laquelle Windows Server est EC2Rescue installé.
4. Exécutez l'outil EC2Rescue pour Windows Server sur l'instance de travail et choisissez Instance hors ligne.
5. Sélectionnez le disque du volume nouvellement monté et choisissez Next (Suivant).
6. Confirmez la sélection de disque et choisissez Yes (Oui).
7. Choisissez l'option d'instance en ligne à exécuter puis sélectionnez Next (Suivant).

L'outil EC2Rescue pour Windows Server analyse le volume et collecte des informations de dépannage en fonction des fichiers journaux sélectionnés.

Collecter des données à partir d'une instance active

Vous pouvez collecter des journaux et d'autres données à partir d'une instance active

Pour collecter des données à partir d'une instance active

1. Connectez-vous à votre instance Windows.
2. Téléchargez l'outil EC2Rescuepour Windows Server sur votre instance Windows et extrayez les fichiers.

   Vous pouvez exécuter la PowerShell commande suivante pour télécharger EC2Rescue sans modifier votre configuration de sécurité renforcée d'Internet Explorer (ESC) :

   ```
   Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -
   OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
   ```

   Cette commande téléchargera le fichier EC2Rescue .zip sur le bureau de l'utilisateur actuellement connecté.

   > **Note**
   >
   > Si un message d'erreur s'affiche lors du téléchargement du fichier et que vous utilisez Windows Server 2016 ou une version antérieure, il est possible que la version TLS 1.2 doive être activée sur votre PowerShell terminal. Vous pouvez activer la TLS version 1.2 pour la PowerShell session en cours à l'aide de la commande suivante, puis réessayer :
   >
   > ```
   > [Net.ServicePointManager]::SecurityProtocol =
   >  [Net.SecurityProtocolType]::Tls12
   > ```

3. Ouvrez l'application EC2Rescue pour Windows Server et acceptez le contrat de licence.
4. Choisissez Next (Suivant), Current instance (Instance actuelle), Capture logs (Capturer les journaux).
5. Sélectionnez les éléments de données à collecter et choisissez Collect... (Collecter...). Lisez l'avertissement et choisissez Yes (Oui) pour continuer.
6. Choisissez un nom de fichier et un emplacement pour le ZIP fichier, puis cliquez sur Enregistrer.

7. Une fois EC2Rescue Windows Server terminé, choisissez Ouvrir le dossier contenant pour afficher le ZIP fichier.
8. Choisissez Finish (Terminer).

Résoudre les problèmes liés à une instance Windows défectueuse à l'aide du EC2Rescue CLI

L'interface de ligne de commande EC2Rescue pour Windows Server (CLI) vous permet d'exécuter un plug-in EC2Rescue pour Windows Server (appelé « action ») par programmation.

L'outil EC2Rescue pour Windows Server dispose de deux modes d'exécution :

- /online —Cela vous permet d'agir sur l'instance sur laquelle Windows Server est installé, par EC2Rescue exemple de collecter des fichiers journaux.
- /offline : <device_id>—Cela vous permet d'agir sur le volume racine hors ligne attaché à une instance Amazon EC2 Windows distincte, sur laquelle vous avez installé Windows EC2Rescue Server.

Téléchargez l'outil EC2Rescuepour Windows Server EC2Rescue sur votre instance Windows et extrayez les fichiers. Vous pouvez afficher le fichier d'aide avec la commande suivante :

```
EC2RescueCmd.exe /help
```

EC2Rescuepour Windows Server peut effectuer les actions suivantes sur une instance Amazon EC2 Windows :

- Action de collecte
- Action de résolution
- Action de restauration

Action de collecte

> **Note**
>
> Vous pouvez collecter tous les journaux, un groupe de journaux complet ou un journal individuel au sein d'un groupe.

EC2Rescuepour Windows Server peut collecter les données suivantes à partir d'instances actives et hors ligne.

Groupe de journaux	Journaux disponibles	Description
`all`		Collecte tous les journaux disponibles.
`eventlog`	• `'Application'` • `'System'` • `'EC2ConfigService'`	Collecte les journaux des applications, du système et des EC2Config événements.
`memory-dump`	• `'Memory Dump File'` • `'Mini Dump Files'`	Permet de collecter les fichiers de vidage de mémoire existant sur l'instance.
`ec2config`	• `'Log Files'` • `'Configuration Files'`	Collecte les fichiers journaux générés par le EC2Config service.
`ec2launch`	• `'Logs'` • `'Config'`	Collecte les fichiers journaux générés par les EC2Launch scripts.
`ssm-agent`	• `'Log Files'` • `'Patch Baseline Logs'` • `'InstanceData'`	Collecte les fichiers journaux générés par les journaux de SSM l'agent et du gestionnaire de correctifs.
`sysprep`	`'Log Files'`	Permet de collecter les fichiers journaux générés par l'outil Windows System Preparation.
`driver-setup`	• `'SetupAPI Log Files'` • `'DPInst Log File'` • `'AWS PV Setup Log File'`	Collecte les API journaux d'installation de Windows (`setupapi.dev.log` et`setupapi.setup.log`).

Groupe de journaux	Journaux disponibles	Description
`registry`	• `'SYSTEM'` • `'SOFTWARE'` • `'BCD'`	Collecte les ruches `SYSTEM` et `SOFTWARE`.
`egpu`	• `'Event Log'` • `'System Files'`	Collecte les journaux d'événements liés à ElasticGPUs.
`boot-config`	`'BCDEDIT Output'`	Collecte la ruche `HKEY_LOCAL_MACHINE\BCD00000000` .
`windows-update`	`'Log Files'`	Permet de collecter les fichiers journaux générés par Windows Update. **Note** Dans Windows Server 2016 et versions ultérieures, le journal est collecté au format Event Tracing for Windows (ETW).
`cloudendure`	• `'Migrate Script Logs'` • `'Driver Logs'` • `'CloudEndure File List'`	Collecte les fichiers journaux relatifs à CloudEndure l'agent.

EC2Rescuepour Windows Server peut collecter les données supplémentaires suivantes à partir d'instances actives.

Groupe de journaux	Journaux disponibles	Description
`system-info`	`'MSInfo32 Output'`	Collecte `MSInfo32`.
`gpresult`	`'GPResult Output'`	Collecte un rapport de politique de groupe.

Les options suivantes sont disponibles :

- /output : < outputFilePath > - Emplacement du chemin du fichier de destination requis pour enregistrer les fichiers journaux collectés au format zip.
- /no-offline : attribut facultatif utilisé en mode hors ligne. Ne met pas le volume hors connexion après avoir exécuté l'action.
- /no-fix-signature- Attribut facultatif utilisé en mode hors ligne. Ne corrige pas une collision de signature de disque possible après avoir exécuté l'action.

Exemples

Voici des exemples d'utilisation de EC2Rescue pour Windows ServerCLI.

Exemples en mode en ligne

Collecter tous les journaux disponibles :

```
EC2RescueCmd /accepteula /online /collect:all /output:<outputFilePath>
```

Collecter uniquement un groupe de journaux spécifique :

```
EC2RescueCmd /accepteula /online /collect:ec2config /output:<outputFilePath>
```

Collecter des journaux individuels au sein d'un groupe de journaux :

```
EC2RescueCmd /accepteula /online /collect:'ec2config.Log Files,driver-setup.SetupAPI
 Log Files' /output:<outputFilePath>
```

Exemples de mode hors connexion

Collectez tous les journaux disponibles à partir d'un EBS volume. Le volume est spécifié par la valeur d'ID de périphérique.

```
EC2RescueCmd /accepteula /offline:xvdf /collect:all /output:<outputFilePath>
```

Collecter uniquement un groupe de journaux spécifique :

```
EC2RescueCmd /accepteula /offline:xvdf /collect:ec2config /output:<outputFilePath>
```

Action de résolution

EC2Rescuepour Windows Server peut détecter et résoudre les problèmes liés aux paramètres de service suivants :

Groupe de services	Actions disponibles	Description
`all`		
`system-time`	`'RealTimeIsUniversal'`	Heure du système • RealTimeisUniversal- Détecte si la clé de `RealTimeisUniversal` registre est activée. Si cette option est désactivée, l'heure du système Windows dérive lorsque le fuseau horaire est défini sur une valeur autre que. UTC
`firewall`	• `'Domain networks'` • `'Private networks'` • `'Guest or public networks'`	Pare-feu Windows • Réseaux de domaine : détectent si ce profil de pare-feu Windows est activé ou désactivé.

Groupe de services	Actions disponibles	Description
		• Réseaux privés : détectent si ce profil de pare-feu Windows est activé ou désactivé. • Réseaux invités ou publics : détectent si ce profil de pare-feu Windows est activé ou désactivé.
rdp	• `'Service Start'` • `'Remote Desktop Connections'` • `'TCP Port'`	Bureau à distance • Démarrage du service : détecte si le service bureau à distance est activé. • Connexions réseau à distance : détectent si cette option est activée. • TCPPort - Détecte le port sur lequel le service Remote Desktop écoute.
`ec2config`	• `'Service Start'` • `'Ec2SetPassword'` • `'Ec2HandleUserData'`	EC2Config • Service Start - Détecte si le EC2Config service est activé. • Ec2 SetPassword - Génère un nouveau mot de passe administrateur. • Ec2 HandleUserData - Vous permet d'exécuter un script de données utilisateur lors du prochain démarrage de l'instance.

Groupe de services	Actions disponibles	Description
`ec2launch`	`'Reset Administrator Password'`	Génère un nouveau mot de passe administrateur Windows.
`network`	`'DHCP Service Startup'`	Interface réseau • DHCPDémarrage du service - Détecte si le DHCP service est activé.

Les options suivantes sont disponibles :

- /level:<level> : attribut facultatif pour le niveau de contrôle que l'action doit déclencher. Les valeurs autorisées sont les suivantes: `information`, `warning`, `error`, `all`. Par défaut, l'attribut est défini sur `error`.
- /check-only : attribut facultatif qui génère un rapport mais n'effectue aucune modification sur le volume hors ligne.

> **Note**
>
> Si EC2Rescue Windows Server détecte une possible collision de signature de disque, il corrige la signature une fois le processus hors ligne terminé par défaut, même lorsque vous utilisez l'`/check-only`option. Vous devez utiliser `/no-fix-signature` cette option pour empêcher la correction.

- /no-offline : attribut facultatif qui empêche la mise hors ligne du volume une fois l'action exécutée.
- /no-fix-signature- Attribut facultatif qui ne corrige pas une éventuelle collision de signature de disque une fois l'action terminée.

Exemples de résolution

Voici des exemples d'utilisation de EC2Rescue pour Windows ServerCLI. Le volume est spécifié à l'aide de la valeur d'ID de périphérique.

Tenter de corriger tous les problèmes identifiés sur un volume :

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:all
```

Tenter de corriger tous les problèmes identifiés au sein d'un groupe de services sur un volume :

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:firewall
```

Tenter de corriger un élément spécifique au sein d'un groupe de services sur un volume :

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:rdp.'Service Start'
```

Spécifier plusieurs problèmes à tenter de corriger sur un volume :

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:'system-
time.RealTimeIsUniversal,ec2config.Service Start'
```

Action de restauration

EC2Rescuepour Windows Server peut détecter et résoudre les problèmes liés aux paramètres de service suivants :

Groupe de services	Actions disponibles	Description
Restaurer la dernière configuration correcte connue	`lkgc`	Dernière configuration correcte connue : tente de démarrer l'instance avec son dernier état de démarrage connu.
Restaurer le registre Windows à partir de la dernière sauvegarde	`regback`	Restaurer le registre à partir de la sauvegarde : restaure le registre à partir de `\Windows\System32\config\RegBack .`

Les options suivantes sont disponibles :

- /no-offline — Attribut facultatif qui empêche la mise hors connexion du volume une fois l'action exécutée.

- /no-fix-signature—Attribut facultatif qui ne corrige pas une éventuelle collision de signatures de disque une fois l'action terminée.

Exemples de restauration

Voici des exemples d'utilisation de EC2Rescue pour Windows ServerCLI. Le volume est spécifié à l'aide de la valeur d'ID de périphérique.

Restaurer la dernière configuration correcte connue sur un volume :

```
EC2RescueCmd /accepteula /offline:xvdf /restore:lkgc
```

Restaurer la dernière sauvegarde du registre Windows sur un volume :

```
EC2RescueCmd /accepteula /offline:xvdf /restore:regback
```

Résoudre les problèmes liés à une instance Windows avec EC2Rescue and Systems Manager

AWS Support vous fournit un document de commande d'exécution de Systems Manager pour vous interfacer avec votre instance compatible avec Systems Manager afin de l'exécuter EC2Rescue pour Windows Server. Le document Exécuter la commande s'appelle `AWSSupport-RunEC2RescueForWindowsTool`.

Le document Exécuter la commande Systems Manager effectue les tâches suivantes :

- Télécharge et vérifie EC2Rescue pour Windows Server.
- Importe un PowerShell module pour faciliter votre interaction avec l'outil.
- S'exécute EC2RescueCmd avec la commande et les paramètres fournis.

Le document Exécuter la commande Systems Manager accepte trois paramètres :

- Commande : EC2Rescue pour l'action de Windows Server. Les valeurs autorisées actuelles sont :
  - ResetAccess—Réinitialise le mot de passe de l'administrateur local. Le mot de passe administrateur local de l'instance actuelle sera réinitialisé et le mot de passe généré de manière aléatoire sera stocké de manière sécurisée dans le Parameter Store en tant que `/EC2Rescue/Password/<INSTANCE_ID>`. Si vous sélectionnez cette action sans fournir de paramètres, les mots de passe sont chiffrés automatiquement avec la KMS clé par défaut. Vous pouvez

éventuellement spécifier un identifiant de KMS clé dans Paramètres pour chiffrer le mot de passe avec votre propre clé.

- CollectLogs—Fonctionne EC2Rescue pour Windows Server avec l'`/collect:all`action. Si vous sélectionnez cette action, `Parameters` doit inclure le nom d'un compartiment Amazon S3 dans lequel les journaux seront chargés.
- FixAll—Fonctionne EC2Rescue pour Windows Server avec l'`/rescue:all`action. Si vous sélectionnez cette action, `Parameters` doit inclure le nom du périphérique de stockage en mode bloc à corriger.

- Paramètres : PowerShell paramètres à transmettre pour la commande spécifiée.

> **Note**
>
> Pour que l'ResetAccessaction fonctionne, votre EC2 instance Amazon doit être associée à la politique suivante afin d'écrire le mot de passe crypté dans Parameter Store. Patientez quelques minutes avant de tenter de réinitialiser le mot de passe d'une instance après avoir associé cette politique au IAM rôle correspondant.
> À l'aide de la KMS clé par défaut :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:region:account_id:parameter/EC2Rescue/
Passwords/<instanceid>"
      ]
    }
  ]
}
```

> À l'aide d'une KMS clé personnalisée :

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:region:account_id:parameter/EC2Rescue/
Passwords/<instanceid>"
        ]
      },
      {
      "Effect": "Allow",
      "Action": [
      "kms:Encrypt"
      ],
      "Resource": [
        "arn:aws:kms:region:account_id:key/<kmskeyid>"
      ]
    }
  ]
}
```

La procédure suivante explique comment afficher le document correspondant JSON à ce document dans la EC2 console Amazon.

Pour consulter le document JSON pour le Systems Manager Run Command

1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.
2. Dans le panneau de navigation, développez Shared Services (Services partagés) et choisissez Documents.
3. Dans la barre de recherche, définissez Propriétaire sur M'appartenant ou appartenant à Amazon et définissez Document name prefix (Préfixe du nom du document) sur `AWSSupport-RunEC2RescueForWindowsTool`.
4. Sélectionnez le `AWSSupport-RunEC2RescueForWindowsTool` document, choisissez Sommaire, puis affichez leJSON.

Exemples

Voici quelques exemples d'utilisation du document Run Command de Systems Manager EC2Rescue pour exécuter Windows Server, à l'aide du AWS CLI. Pour plus d'informations sur l'envoi de commandes avec le AWS CLI, consultez la référence des AWS CLI commandes.

Tentative de correction de tous les problèmes identifiés sur un volume racine hors connexion

Essayez de résoudre tous les problèmes identifiés sur un volume racine hors ligne connecté à une instance Amazon EC2 Windows :

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue offline volume xvdf" --parameters
 "Command=FixAll, Parameters='xvdf'" --output text
```

Collectez les journaux de l'instance Amazon EC2 Windows actuelle

Collectez tous les journaux de l'instance Amazon EC2 Windows en ligne actuelle et chargez-les dans un compartiment Amazon S3 :

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue online log collection to S3" --
parameters "Command=CollectLogs, Parameters='amzn-s3-demo-bucket'" --output text
```

Collectez des journaux à partir d'un volume d'instance Amazon EC2 Windows hors ligne

Collectez tous les journaux d'un volume hors ligne connecté à une instance Amazon EC2 Windows et chargez-les sur Amazon S3 avec un document présigné URL :

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue offline log collection to S3"
 --parameters "Command=CollectLogs, Parameters=\"-Offline -BlockDeviceName xvdf -
S3PreSignedUrl 'YOURS3PRESIGNEDURL'\"" --output text
```

Réinitialisez le mot de passe administrateur local

Les exemples suivants illustrent les méthodes vous permettant de réinitialiser le mot de passe administrateur local. La sortie fournit un lien vers Parameter Store, où vous pouvez trouver le mot de passe sécurisé généré de manière aléatoire que vous pouvez ensuite utiliser pour RDP accéder à votre instance Amazon EC2 Windows en tant qu'administrateur local.

Réinitialiser le mot de passe administrateur local d'une instance en ligne à l'aide de la AWS KMS key par défaut alias/aws/ssm :

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue online password reset" --parameters
 "Command=ResetAccess" --output text
```

Réinitialisez le mot de passe administrateur local d'une instance en ligne à l'aide d'une KMS clé :

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue online password reset" --parameters
 "Command=ResetAccess, Parameters=a133dc3c-a2g4-4fc6-a873-6c0720104bf0" --output text
```

> **Note**
>
> Dans cet exemple, la KMS clé esta133dc3c-a2g4-4fc6-a873-6c0720104bf0.

EC2Console série pour instances

Avec la console EC2 série, vous avez accès au port série de votre EC2 instance Amazon, que vous pouvez utiliser pour résoudre les problèmes de démarrage, de configuration réseau et autres. La console série ne requiert pas que votre instance possède des capacités de mise en réseau. La console série vous permet de commander une instance comme si votre clavier et votre moniteur étaient directement connectés au port série de cette dernière. La session de la console série dure du redémarrage à l'arrêt de l'instance. Pendant le redémarrage, vous pouvez afficher tous les messages de démarrage depuis le début.

L'accès à la console série n'est pas disponible par défaut. Votre organisation doit autoriser le compte à accéder à la console série et configurer des IAM politiques pour accorder à vos utilisateurs l'accès à la console série. L'accès à la console série peut être contrôlé à un niveau granulaire à l'aide d'instancesIDs, de balises de ressources et d'autres IAM leviers. Pour de plus amples informations, veuillez consulter Configuration de l'accès à la console EC2 série.

La console série est accessible à l'aide de la EC2 console ou du AWS CLI.

La console série est disponible sans frais supplémentaires.

Rubriques

Conditions requises pour la console EC2 série

Pour vous connecter à la console EC2 série et utiliser l'outil de dépannage de votre choix, les conditions préalables suivantes doivent être réunies :

- Régions AWS
- Zones Wavelength et AWS Outposts
- Zones locales
- Types d'instances
- Octroi de l'accès
- Prise en charge d'un client basé sur un navigateur
- État de l'instance
- Amazon EC2 Systems Manager
- Configuration de l'outil de dépannage de votre choix

Régions AWS

Pris en charge dans tous les Régions AWS domaines.

Zones Wavelength et AWS Outposts

Non pris en charge.

Zones locales

Prise en charge dans toutes les zones locales.

Types d'instances

Types d'instances pris en charge :

- Linux
  - Toutes les instances virtualisées créées sur la base de Nitro System.
  - Toutes les instances de matériel nu à l'exception de :
    - Usage général : `a1.metal`, `mac1.metal`, `mac2.metal`
    - Calcul accéléré : `g5g.metal`
    - Mémoire optimisée : `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal`, `u-24tb1.metal`
- Windows

  Toutes les instances virtualisées créées sur la base de Nitro System. Non pris en charge par les instances à matériel nu.

Octroi de l'accès

Vous devez effectuer les tâches de configuration pour autoriser l'accès à la console EC2 série. Pour de plus amples informations, veuillez consulter Configuration de l'accès à la console EC2 série.

Prise en charge d'un client basé sur un navigateur

Pour vous connecter à la console série à l'aide du client basé sur un navigateur, votre navigateur doit être compatible. WebSocket Si votre navigateur ne le prend pas en charge WebSocket, connectez-vous à la console série à l'aide de votre propre clé et d'un SSH client.

État de l'instance

Doit indiquer `running`.

Vous ne pouvez pas vous connecter à la console série si l'instance est à l'état `pending`, `stopping`, `stopped`, `shutting-down` ou `terminated`.

Pour plus d'informations sur les états de l'instance, consultez Modifications de l'état de l'EC2instance Amazon.

Amazon EC2 Systems Manager

Si l'instance utilise Amazon EC2 Systems Manager, la version 3.0.854.0 ou ultérieure de l'SSMagent doit être installée sur l'instance. Pour plus d'informations sur SSM l'agent, consultez la section Utilisation de SSM l'agent dans le guide de AWS Systems Manager l'utilisateur.

Configuration de l'outil de dépannage de votre choix

Pour dépanner votre instance via la console série, vous pouvez utiliser GRUB ou SysRq sur des instances Linux, et la console d'administration spéciale (SAC) sur des instances Windows. Avant de pouvoir utiliser ces outils, vous devez d'abord effectuer des étapes de configuration sur chaque instance sur laquelle vous allez les utiliser.

Utilisez les instructions relatives au système d'exploitation de votre instance pour configurer l'outil de dépannage que vous avez choisi.

(instances Linux) Configurer GRUB

Pour configurerGRUB, choisissez l'une des procédures suivantes en fonction de celle AMI qui a été utilisée pour lancer l'instance.

Amazon Linux 2

Pour configurer GRUB sur une instance Amazon Linux 2

1. Connectez-vous à votre instance Linux à l'aide de SSH
2. Ajoutez ou modifiez les options suivantes dans `/etc/default/grub`:
   - Configurez `GRUB_TIMEOUT=1`.
   - Addition `GRUB_TERMINAL="console serial"`.
   - Addition `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

   Voici un exemple de `/etc/default/grub`. Vous devrez peut-être modifier la configuration en fonction de la configuration de votre système.

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0
    biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.shell=0"
   GRUB_TIMEOUT=1
   GRUB_DISABLE_RECOVERY="true"
   GRUB_TERMINAL="console serial"
   GRUB_SERIAL_COMMAND="serial --speed=115200"
   ```
3. Appliquez la configuration mise à jour en exécutant la commande suivante.

   ```
   [ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

Ubuntu

Pour configurer GRUB sur une instance Ubuntu

1. Connectez-vous à votre instance.
2. Ajoutez ou modifiez les options suivantes dans `/etc/default/grub.d/50-cloudimg-settings.cfg`:
   - Configurez `GRUB_TIMEOUT=1`.
   - Addition `GRUB_TIMEOUT_STYLE=menu`.
   - Addition `GRUB_TERMINAL="console serial"`.
   - Supprimez `GRUB_HIDDEN_TIMEOUT`.
   - Addition `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

   Voici un exemple de `/etc/default/grub.d/50-cloudimg-settings.cfg`. Vous devrez peut-être modifier la configuration en fonction de la configuration de votre système.

```
# Cloud Image specific Grub settings for Generic Cloud Images
# CLOUD_IMG: This file was created/modified by the Cloud Image build process

# Set the recordfail timeout
GRUB_RECORDFAIL_TIMEOUT=0

# Do not wait on grub prompt
GRUB_TIMEOUT=1
GRUB_TIMEOUT_STYLE=menu

# Set the default commandline
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
 nvme_core.io_timeout=4294967295"

# Set the grub console type
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed 115200"
```

3. Appliquez la configuration mise à jour en exécutant la commande suivante.

```
[ec2-user ~]$ sudo update-grub
```

RHEL

Pour configurer GRUB sur une RHEL instance

1. Connectez-vous à votre instance.
2. Ajoutez ou modifiez les options suivantes dans `/etc/default/grub`:
   - Supprimez `GRUB_TERMINAL_OUTPUT`.
   - Addition `GRUB_TERMINAL="console serial"`.
   - Addition `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

   Voici un exemple de `/etc/default/grub`. Vous devrez peut-être modifier la configuration en fonction de la configuration de votre système.

   ```
   GRUB_TIMEOUT=1
   GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
   GRUB_DEFAULT=saved
   GRUB_DISABLE_SUBMENU=true
   GRUB_CMDLINE_LINUX="console=tty0 console=ttyS0,115200n8 net.ifnames=0
    rd.blacklist=nouveau nvme_core.io_timeout=4294967295 crashkernel=auto"
   GRUB_DISABLE_RECOVERY="true"
   GRUB_ENABLE_BLSCFG=true
   GRUB_TERMINAL="console serial"
   GRUB_SERIAL_COMMAND="serial --speed=115200"
   ```
3. Appliquez la configuration mise à jour en exécutant la commande suivante.

   ```
   [ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

CentOS

Pour les instances lancées à l'aide d'un CentOSAMI, GRUB est configuré par défaut pour la console série.

Voici un exemple de `/etc/default/grub`. En fonction de la configuration de votre système, il se peut que votre configuration soit différente.

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
```

```
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL="serial console"
GRUB_SERIAL_COMMAND="serial --speed=115200"
GRUB_CMDLINE_LINUX="console=tty0 crashkernel=auto console=ttyS0,115200"
GRUB_DISABLE_RECOVERY="true"
```

(instances Linux) Configurer SysRq

Pour configurer SysRq, vous devez activer les SysRq commandes pour le cycle de démarrage en cours. Pour que la configuration soit persistante, vous pouvez également activer les SysRq commandes pour les démarrages suivants.

Pour activer toutes les SysRq commandes pour le cycle de démarrage en cours

1. Connectez-vous à votre instance.
2. Exécutez la commande suivante.

```
[ec2-user ~]$ sudo sysctl -w kernel.sysrq=1
```

> **Note**
>
> Ce paramètre est effacé au prochain redémarrage.

Pour activer toutes les SysRq commandes pour les démarrages suivants

1. Créez le fichier `/etc/sysctl.d/99-sysrq.conf` et ouvrez-le dans votre éditeur préféré.

```
[ec2-user ~]$ sudo vi /etc/sysctl.d/99-sysrq.conf
```

2. Ajoutez la ligne suivante.

```
kernel.sysrq=1
```

3. Redémarrez l'instance pour appliquer les modifications.

```
[ec2-user ~]$ sudo reboot
```

4. À l'**`login`**invite, entrez le nom d'utilisateur de l'utilisateur basé sur un mot de passe que vous avez configuré précédemment, puis appuyez sur Entrée.
5. À l'invite `Password`, entrez le mot de passe, puis appuyez sur Entrée.

(instances Windows) Activer SAC et menu de démarrage

> **Note**
>
> Si vous l'activez SAC sur une instance, les EC2 services qui reposent sur la récupération du mot de passe ne fonctionneront pas depuis la EC2 console Amazon. Les agents de EC2 lancement de Windows on Amazon (EC2ConfigEC2Launchv1 et EC2Launch v2) s'appuient sur la console série pour exécuter diverses tâches. Ces tâches ne s'exécutent pas correctement lorsque vous SAC les activez sur une instance. Pour plus d'informations sur les agents de EC2 lancement de Windows sur Amazon, consultezthe section called "Configuration des instances Windows". Si vous l'activezSAC, vous pourrez le désactiver ultérieurement. Pour de plus amples informations, veuillez consulter Désactiver SAC et menu de démarrage.

Utilisez l'une des méthodes suivantes pour activer SAC et activer le menu de démarrage sur une instance.

PowerShell

Pour activer SAC et activer le menu de démarrage sur une instance Windows

1. Connectez-vous à votre instance et effectuez les étapes suivantes à partir d'une ligne de PowerShell commande élevée.
2. ActiverSAC.

```
bcdedit /ems '{current}' on
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Activez le menu de démarrage.

```
bcdedit /set '{bootmgr}' displaybootmenu yes
bcdedit /set '{bootmgr}' timeout 15
bcdedit /set '{bootmgr}' bootems yes
```

4. Appliquez la configuration mise à jour en redémarrant l'instance.

```
shutdown -r -t 0
```

Command prompt

Pour activer SAC et activer le menu de démarrage sur une instance Windows

1. Connectez-vous à votre instance et exécutez les étapes suivantes à partir de l'invite de commandes.
2. ActiverSAC.

```
bcdedit /ems {current} on
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Activez le menu de démarrage.

```
bcdedit /set {bootmgr} displaybootmenu yes
bcdedit /set {bootmgr} timeout 15
bcdedit /set {bootmgr} bootems yes
```

4. Appliquez la configuration mise à jour en redémarrant l'instance.

```
shutdown -r -t 0
```

Configuration de l'accès à la console EC2 série

Pour configurer l'accès à la console série, vous devez accorder l'accès à la console série au niveau du compte, puis configurer des IAM politiques pour accorder l'accès à vos utilisateurs. Pour les instances Linux, vous devez également configurer un utilisateur basé sur un mot de passe pour chaque instance afin que vos utilisateurs puissent utiliser la console série pour le dépannage.

Avant de commencer, assurez-vous de vérifier les conditions préalables.

Rubriques

- Niveaux d'accès à la console EC2 série
- Gérer l'accès du compte à la console EC2 série

- Configuration IAM des politiques d'accès à la console EC2 série
- Définir un mot de passe utilisateur du système d'exploitation sur une instance Linux

Niveaux d'accès à la console EC2 série

Par défaut, il n'est pas possible d'accéder à la console série au niveau du compte. Vous devez accorder explicitement l'accès à la console série au niveau du compte. Pour de plus amples informations, veuillez consulter Gérer l'accès du compte à la console EC2 série.

Vous pouvez utiliser une politique de contrôle des services (SCP) pour autoriser l'accès à la console série au sein de votre organisation. Vous pouvez ensuite avoir un contrôle d'accès granulaire au niveau de l'utilisateur en utilisant une IAM politique de contrôle d'accès. En utilisant une combinaison de IAM politiques SCP et, vous disposez de différents niveaux de contrôle d'accès à la console série.

Niveau de l'organisation

Vous pouvez utiliser une politique de contrôle des services (SCP) pour autoriser l'accès à la console série aux comptes des membres de votre organisation. Pour plus d'informationsSCPs, consultez la section Politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.

Niveau de l'instance

Vous pouvez configurer les politiques d'accès à la console série en utilisant IAM PrincipalTag des ResourceTag constructions et en spécifiant les instances par leur identifiant. Pour de plus amples informations, veuillez consulter Configuration IAM des politiques d'accès à la console EC2 série.

Niveau utilisateur

Vous pouvez configurer l'accès au niveau de l'utilisateur en configurant une IAM politique pour autoriser ou refuser à un utilisateur spécifié l'autorisation d'envoyer la clé SSH publique au service de console série d'une instance donnée. Pour de plus amples informations, veuillez consulter Configuration IAM des politiques d'accès à la console EC2 série.

Niveau du système d'exploitation (instances Linux uniquement)

Vous pouvez définir un mot de passe utilisateur au niveau du système d'exploitation invité. Cela permet d'accéder à la console série pour certains cas d'utilisation. Toutefois, pour surveiller les journaux, vous n'avez pas besoin d'un utilisateur avec un mot de passe. Pour de plus amples informations, veuillez consulter Définir un mot de passe utilisateur du système d'exploitation sur une instance Linux.

Gérer l'accès du compte à la console EC2 série

Par défaut, il n'est pas possible d'accéder à la console série au niveau du compte. Vous devez accorder explicitement l'accès à la console série au niveau du compte.

Rubriques

Autoriser les utilisateurs à gérer l'accès du compte

Pour permettre à vos utilisateurs de gérer l'accès de leur compte à la console EC2 série, vous devez leur accorder les IAM autorisations requises.

La politique suivante accorde des autorisations pour consulter l'état du compte, ainsi que pour autoriser ou empêcher l'accès du compte à la console EC2 série.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:EnableSerialConsoleAccess",
                "ec2:DisableSerialConsoleAccess"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour plus d'informations, consultez la section Création IAM de politiques dans le guide de IAM l'utilisateur.

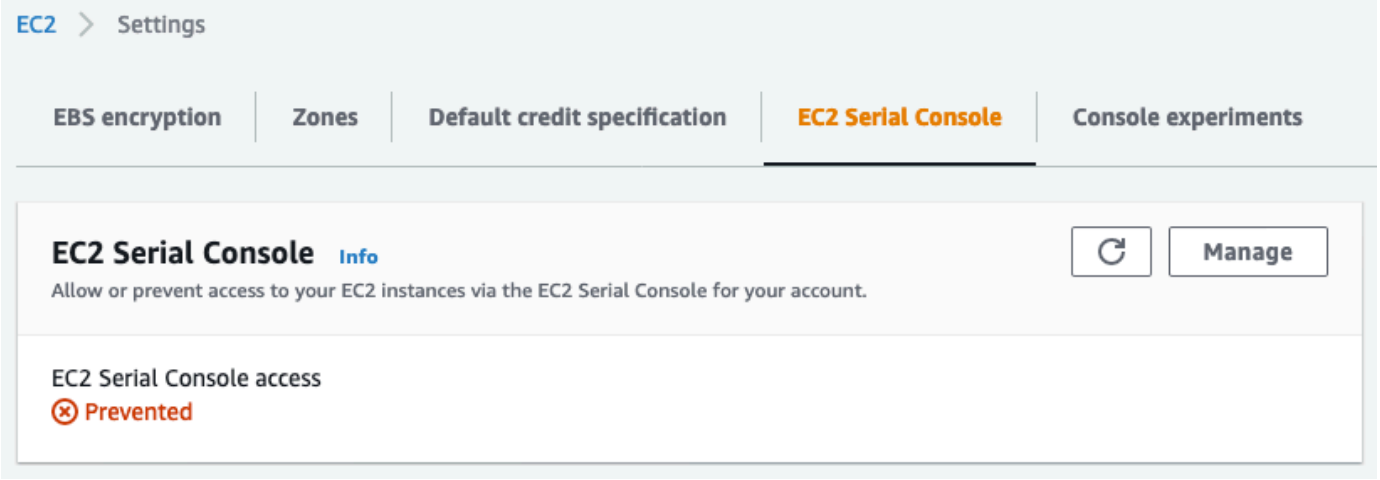
Afficher l'état de l'accès du compte à la console série

Pour afficher l'état de l'accès du compte à la console série (console)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation de gauche, choisissez EC2Dashboard.
3. Dans Attributs du compte, sélectionnez EC2Serial Console.

   Le champ Accès à la console EC2 série indique si l'accès au compte est autorisé ou interdit.

   La capture d'écran suivante montre que le compte ne peut pas utiliser la console EC2 série.



Pour afficher l'état d'accès du compte à la console série (AWS CLI)

Utilisez la commande get-serial-console-access-status pour afficher l'état d'accès du compte à la console série.

```
aws ec2 get-serial-console-access-status --region us-east-1
```

Dans le résultat suivant, `true` indique que le compte est autorisé à accéder à la console série.

```
{
    "SerialConsoleAccessEnabled": true
}
```

Autoriser le compte à accéder à la console série

Pour autoriser le compte à accéder à la console série (console)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation de gauche, choisissez EC2Dashboard.
3. Dans Attributs du compte, sélectionnez EC2Serial Console.
4. Choisissez Gérer.
5. Pour autoriser l'accès à la console EC2 série de toutes les instances du compte, cochez la case Autoriser.
6. Sélectionnez Mise à jour.

Pour autoriser le compte à accéder à la console série (AWS CLI)

Utilisez la enable-serial-console-accesscommande pour autoriser l'accès du compte à la console série.

```
aws ec2 enable-serial-console-access --region us-east-1
```

Dans le résultat suivant, `true` indique que le compte est autorisé à accéder à la console série.

```
{
    "SerialConsoleAccessEnabled": true
}
```

Interdire au compte l'accès à la console série

Pour interdire au compte l'accès à la console série (console)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation de gauche, choisissez EC2Dashboard.
3. Dans Attributs du compte, sélectionnez EC2Serial Console.
4. Choisissez Gérer.
5. Pour empêcher l'accès à la console EC2 série de toutes les instances du compte, décochez la case Autoriser.
6. Sélectionnez Mise à jour.

Pour interdire au compte l'accès à la console série (AWS CLI)

Utilisez la disable-serial-console-accesscommande pour empêcher l'accès du compte à la console série.

```
aws ec2 disable-serial-console-access --region us-east-1
```

Dans le résultat suivant, `false` indique que le compte n'est pas autorisé à accéder à la console série.

```
{
    "SerialConsoleAccessEnabled": false
}
```

Configuration IAM des politiques d'accès à la console EC2 série

Par défaut, vos utilisateurs n'ont pas accès à la console série. Votre organisation doit configurer IAM des politiques pour accorder à vos utilisateurs l'accès requis. Pour plus d'informations, consultez la section Création IAM de politiques dans le guide de IAM l'utilisateur.

Pour accéder à la console série, créez un document de JSON politique qui inclut l'`ec2-instance-connect:SendSerialConsoleSSHPublicKey`action. Cette action accorde à un utilisateur l'autorisation d'envoyer la clé publique en mode push au service de console série, qui démarre une session de console série. Nous recommandons de restreindre l'accès à des EC2 instances spécifiques. Sinon, tous les utilisateurs disposant de cette autorisation peuvent se connecter à la console série de toutes les EC2 instances.

Exemples de IAM politiques

- Autoriser explicitement l'accès à la console série
- Refuser explicitement l'accès à la console série
- Utiliser des balises de ressources pour contrôler l'accès à la console série

Autoriser explicitement l'accès à la console série

Par défaut, personne n'a accès à la console série. Pour accorder l'accès à la console série, vous devez configurer une politique pour autoriser explicitement cet accès. Nous vous recommandons de configurer une politique qui restreint l'accès à des instances spécifiques.

La politique suivante permet d'accéder à la console série d'une instance spécifique, identifiée par son ID d'instance.

Notez que les actions `DescribeInstances`, `DescribeInstanceTypes` et `GetSerialConsoleAccessStatus` ne prennent pas en charge les autorisations au niveau des ressources. Par conséquent, toutes les ressources, indiquées par un astérisque *, doivent être spécifiées pour ces actions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
             "Resource": "*"
        },
        {
            "Sid": "AllowinstanceBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

Refuser explicitement l'accès à la console série

La IAM politique suivante autorise l'accès à la console série de toutes les instances, désignée par un * (astérisque), et refuse explicitement l'accès à la console série d'une instance spécifique, identifiée par son identifiant.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "AllowSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DenySerialConsoleAccess",
            "Effect": "Deny",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

Utiliser des balises de ressources pour contrôler l'accès à la console série

Vous pouvez utiliser des balises de ressource pour contrôler l'accès à la console série d'une instance.

Le contrôle d'accès basé sur les attributs est une stratégie d'autorisation qui définit les autorisations en fonction de balises pouvant être associées aux utilisateurs et AWS aux ressources. Par exemple, la politique suivante permet à un utilisateur d'initier une connexion à la console série pour une seule instance si la balise de ressource de cette instance et la balise du principal possèdent la même valeur `SerialConsole` en clé de balise.

Pour plus d'informations sur l'utilisation de balises pour contrôler l'accès à vos AWS ressources, consultez la section Contrôle de l'accès aux AWS ressources dans le Guide de IAM l'utilisateur.

Notez que les actions `DescribeInstances`, `DescribeInstanceTypes` et `GetSerialConsoleAccessStatus` ne prennent pas en charge les autorisations au niveau des ressources. Par conséquent, toutes les ressources, indiquées par un astérisque `*`, doivent être spécifiées pour ces actions.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowTagBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/SerialConsole":
 "${aws:PrincipalTag/SerialConsole}"
                }
            }
        }
    ]
}
```

Définir un mot de passe utilisateur du système d'exploitation sur une instance Linux

> **Note**
>
> Cette section s'applique uniquement aux instances Linux.

Vous pouvez vous connecter à la console série sans mot de passe. Toutefois, pour utiliser la console série pour le dépannage d'une instance Linux, celle-ci doit disposer d'un utilisateur du système d'exploitation basé sur un mot de passe.

Vous pouvez définir le mot de passe pour n'importe quel utilisateur du système d'exploitation, y compris l'utilisateur racine. Notez que l'utilisateur racine peut modifier tous les fichiers, tandis que chaque utilisateur du système d'exploitation peut avoir des autorisations limitées.

Vous devez définir un mot de passe utilisateur pour chaque instance pour laquelle vous utilisez la console série. Vous n'aurez besoin d'effectuer cette opération qu'une seule fois pour chaque instance.

> **Note**
>
> Les instructions suivantes ne s'appliquent que si vous avez lancé votre instance à l'aide d'un système Linux AMI fourni par AWS car, par défaut, le système AMIs fourni par AWS n'est pas configuré avec un utilisateur basé sur un mot de passe. Si vous avez lancé votre instance à l'aide d'une instance AMI dont le mot de passe utilisateur root est déjà configuré, vous pouvez ignorer ces instructions.

Pour définir un mot de passe utilisateur du système d'exploitation sur une instance Linux

1. Connectez-vous à votre instance. Vous pouvez utiliser n'importe quelle méthode pour vous connecter à votre instance, à l'exception de la méthode de connexion par console EC2 série.
2. Pour définir le mot de passe d'un utilisateur, utilisez la commande passwd. Dans l'exemple suivant, l'utilisateur est `root`.

   ```
   [ec2-user ~]$ sudo passwd root
   ```

   Voici un exemple de sortie.

   ```
   Changing password for user root.
   New password:
   ```
3. À l'invite `New password`, entrez le nouveau mot de passe.
4. À l'invite, saisissez à nouveau le mot de passe.

Connect à la console EC2 série

Vous pouvez vous connecter à la console série de votre EC2 instance à l'aide de la EC2 console Amazon ou viaSSH. Une fois connecté à la console série, vous pouvez l'utiliser pour résoudre les problèmes de démarrage, de configuration réseau et autres. Pour plus d'informations sur la résolution des problèmes, consultez Résoudre les problèmes liés à votre EC2 instance Amazon à l'aide de la console EC2 série.

Considérations

- Une seule connexion de console série active est prise en charge par instance.
- La connexion à la console série dure généralement une heure, à moins que vous ne vous déconnectiez. Toutefois, pendant la maintenance du système, Amazon EC2 déconnectera la session de console série.
- 30 secondes sont nécessaires pour déconnecter une session après la déconnexion de la console série afin d'autoriser une nouvelle session.
- Ports de console série pris en charge : `ttyS0` (instances Linux) et `COM1` (instances Windows)
- Lorsque vous vous connectez à la console série, vous pouvez observer une légère baisse de débit de votre instance.

Rubriques

Connexion à l'aide du client basé sur un navigateur

Vous pouvez vous connecter à la console série de votre EC2 instance à l'aide du client basé sur un navigateur. Pour ce faire, sélectionnez l'instance dans la EC2 console Amazon et choisissez de vous connecter à la console série. Le client basé sur le navigateur gère les autorisations et fournit une connexion réussie.

EC2la console série fonctionne à partir de la plupart des navigateurs et prend en charge la saisie au clavier et à la souris.

Avant d'établir la connexion, assurez-vous d'avoir réuni les conditions préalables.

Pour vous connecter au port série de votre instance à l'aide du client basé sur un navigateur (console AmazonEC2)

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance et choisissez Actions, Monitor and troubleshoot, EC2Serial Console, Connect.

Vous pouvez également sélectionner l'instance et choisir Connect, EC2Serial Console, Connect.

Une fenêtre de terminal dans le navigateur s'ouvre.

4. Appuyez sur Entrée. Si une invite de connexion est retournée, vous êtes connecté à la console série.

   Si l'écran reste noir, vous pouvez utiliser les informations suivantes pour résoudre les problèmes de connexion à la console série :

   - Vérifiez que vous avez configuré l'accès à la console série. Pour de plus amples informations, veuillez consulter Configuration de l'accès à la console EC2 série.
   - (Instances Linux uniquement) SysRq À utiliser pour se connecter à la console série. SysRq ne nécessite pas que vous vous connectiez via le client basé sur un navigateur. Pour de plus amples informations, veuillez consulter (Instances Linux) SysRq À utiliser pour dépanner votre instance.
   - (Instances Linux uniquement) Redémarrez getty. Si vous avez SSH accès à votre instance, connectez-vous à votre instance en utilisant SSH et redémarrez getty à l'aide de la commande suivante.

     ```
     [ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
     ```

   - Redémarrez votre instance. Vous pouvez redémarrer votre instance en utilisant SysRq (instances Linux), la EC2 console ou le AWS CLI. Pour plus d'informations, consultez (Instances Linux) SysRq À utiliser pour dépanner votre instance (instances Linux) ouRedémarrer votre instance.
5. (Instances Linux uniquement) À l'**`login`**invite, entrez le nom d'utilisateur de l'utilisateur basé sur un mot de passe que vous avez configuré précédemment, puis appuyez sur Entrée.
6. (Instances Linux uniquement) À l'`Password`dinvite, entrez le mot de passe, puis appuyez sur Entrée.

Vous êtes maintenant connecté à l'instance et pouvez utiliser la console série pour résoudre les problèmes.

Connectez-vous à l'aide de votre propre clé et de votre propre SSH client

Vous pouvez utiliser votre propre SSH clé et vous connecter à votre instance depuis le SSH client de votre choix tout en utilisant la console sérieAPI. Vous bénéficiez ainsi de la capacité de la console série d'envoyer une clé publique en mode push à l'instance.

Avant d'établir la connexion, assurez-vous d'avoir réuni les conditions préalables.

Pour vous connecter à la console série d'une instance à l'aide de SSH

1. Envoyez votre clé SSH publique à l'instance pour démarrer une session de console série

   Utilisez la commande send-serial-console-ssh-public-key pour transmettre votre clé SSH publique à l'instance. Une session de console série démarre.

   Si une session de console série a déjà été démarrée pour cette instance, la commande échoue car vous ne pouvez avoir qu'une seule session ouverte à la fois. 30 secondes sont nécessaires pour déconnecter une session après la déconnexion de la console série afin d'autoriser une nouvelle session.

   ```
   aws ec2-instance-connect send-serial-console-ssh-public-key \
       --instance-id i-001234a4bf70dec41EXAMPLE \
       --serial-port 0 \
       --ssh-public-key file://my_key.pub \
       --region us-east-1
   ```

2. Connexion à la console série à l'aide de votre clé privée

   Utilisez la commande ssh pour vous connecter à la console série avant que la clé publique ne soit supprimée du service de console série. Vous avez 60 secondes avant sa suppression.

   Utilisez la clé privée qui correspond à la clé publique.

   Le format du nom d'utilisateur est`instance-id.port0`, qui comprend l'ID de l'instance et le port 0. Dans l'exemple suivant, le nom d'utilisateur est`i-001234a4bf70dec41EXAMPLE.port0`.

   Le point de terminaison du service Serial Console est différent pour chaque région. Consultez le tableau EC2Points de terminaison et empreintes digitales de la console série pour le point de terminaison de chaque région. Dans l'exemple suivant, le service de console série se trouve dans la région *us-east-1*.

```
ssh -i my_key i-001234a4bf70dec41EXAMPLE.port0@serial-console.ec2-instance-connect.us-east-1.aws
```

3. (Facultatif) Vérification de l'empreinte digitale

   Lorsque vous vous connectez pour la première fois à la console série, vous êtes invité à vérifier l'empreinte digitale. Vous pouvez comparer l'empreinte digitale de la console série avec l'empreinte digitale affichée pour vérification. Si ces empreintes ne correspondent pas, quelqu'un est peut-être en train de tenter une attaque « man-in-the-middle ». Si elles correspondent, vous pouvez vous connecter en toute confiance à la console série.

   L'empreinte digitale suivante concerne le service de console série dans la région us-east-1. Pour obtenir les empreintes digitales de chaque région, consultez EC2Points de terminaison et empreintes digitales de la console série.

   ```
   SHA256:dXwn5ma/xadVMeBZGEru5l2gx+yI5LDiJaLUcz0FMmw
   ```

   > **Note**
   >
   > L'empreinte digitale n'apparaît que la première fois que vous vous connectez à la console série.

4. Appuyez sur Entrée. Si une invite est retournée, vous êtes connecté à la console série.

   Si l'écran reste noir, vous pouvez utiliser les informations suivantes pour résoudre les problèmes de connexion à la console série :

   - Vérifiez que vous avez configuré l'accès à la console série. Pour de plus amples informations, veuillez consulter Configuration de l'accès à la console EC2 série.
   - (Instances Linux uniquement) SysRq À utiliser pour se connecter à la console série. SysRq ne nécessite pas que vous vous connectiez viaSSH. Pour de plus amples informations, veuillez consulter (Instances Linux) SysRq À utiliser pour dépanner votre instance.
   - (Instances Linux uniquement) Redémarrez getty. Si vous avez SSH accès à votre instance, connectez-vous à votre instance en utilisant SSH et redémarrez getty à l'aide de la commande suivante.

     ```
     [ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
     ```

- Redémarrez votre instance. Vous pouvez redémarrer votre instance en utilisant SysRq (instances Linux uniquement), la EC2 console ou le AWS CLI. Pour plus d'informations, consultez (Instances Linux) SysRq À utiliser pour dépanner votre instance (instances Linux uniquement) ouRedémarrer votre instance.

5. (Instances Linux uniquement) À l'**`login`**invite, entrez le nom d'utilisateur de l'utilisateur basé sur un mot de passe que vous avez configuré précédemment, puis appuyez sur Entrée.
6. (Instances Linux uniquement) À l'`Password`dinvite, entrez le mot de passe, puis appuyez sur Entrée.

Vous êtes maintenant connecté à l'instance et pouvez utiliser la console série pour résoudre les problèmes.

EC2Points de terminaison et empreintes digitales de la console série

Vous trouverez ci-dessous les points de terminaison de service et les empreintes digitales de la console EC2 série. Pour vous connecter par programmation à la console série d'une instance, vous utilisez un point de terminaison de console EC2 série. Les points de terminaison et les empreintes digitales de la console EC2 série sont uniques pour chaque AWS région.

Nom de la région	Région	Point de terminaison	Empreinte digitale
USA Est (Ohio)	us-east-2	serial-console.ec2-instance-connect.us-east-2.aws	SHA256: EhwPkTzRt TY7TRSzz26XbB 0/HVV9J 0xw/d/0 RM7mCZN
US East (Virginie du Nord)	us-east-1	serial-console.ec2-instance-connect.us-east-1.aws	SHA256: dXwn 5 mA/+yI5 xadVMe BZGEru5l2gx 0 LDiJaLUcz FMmw
USA Ouest (Californie du Nord)	us-west-1	serial-console.ec2-instance-connect.us-west-1.aws	SHA256:OH ldlcMET8u 7QLSX3jmR TRAPFHVtq byoLZBMUCqiH3Y

Nom de la région	Région	Point de terminaison	Empreinte digitale
USA Ouest (Oregon)	us-west-2	serial-console.ec2-instance-connect.us-west-2.aws	SHA256:EM CIe23TqKaBI6yGHain qZcMwqNkD hhAVHa1O2JxVUc
Afrique (Le Cap)	af-south-1	ec2-serial-console.af-south-1.api.aws	SHA256: RMWWZ2fVe PeJUqzjO5jL2KIgXsc zoHlz21Ed 00 BiiWi
Asie-Pacifique (Hong Kong)	ap-east-1	ec2-serial-console.ap-east-1.api.aws	SHA256:T0Q1 lpiXxCho ZHplnAkjb P7tkm2xXViC9bJFsjY nifk
Asie-Pacifique (Hyderabad)	ap-south-2	ec2-serial-console.ap-south-2.api.aws	SHA256WJg PBSwV4:/SHn + OPITValoe wAuYj15DV W845JEhDKRs
Asie-Pacifique (Jakarta)	ap-southeast-3	ec2-serial-console.ap-southeast-3.api.aws	SHA2565 : ZwgrCh XITqL +lfns32/4 O0 4 zIfbx bZgs YFqy3o8mIk
Asie-Pacifique (Melbourne)	ap-southeast-4	ec2-serial-console.ap-southeast-4.api.aws	SHA256:Avaq27 5 Z0oV7H90P0 hFgLvjn gTSSh GG46wfOeT 6ZJvM
Asie-Pacifique (Mumbai)	ap-south-1	serial-console.ec2-instance-connect.ap-south-1.aws	SHA256: oBLXc Y mklqHHEbli ARxEgH8IsO51rezTPi SM35BsU4 0

Nom de la région	Région	Point de terminaison	Empreinte digitale
Asie-Pacifique (Osaka)	ap-northeast-3	ec2-serial-console.ap-northeast-3.api.aws	SHA256:Am 0/9 /v jiBKBn BuFnHr /3UCyJSQ aXsg EV3G8Tu VHFXE
Asie-Pacifique (Séoul)	ap-northeast-2	serial-console.ec2-instance-connect.ap-northeast-2.aws	SHA256WXNX:Foq +DZ+G 9+Frc uNTztg PK49WYMqBX ZM2dSrqrI
Asie-Pacifique (Singapour)	ap-southeast-1	serial-console.ec2-instance-connect.ap-southeast-1.aws	SHA256: PLFNn7WnC QDHx3qmwLu1Gy / O8 TUX7LQgZu aC6L45CoY
Asie-Pacifique (Sydney)	ap-southeast-2	serial-console.ec2-instance-connect.ap-southeast-2.aws	SHA256yFv MwUK9lEUQ jQTRoXXzuN:+CW9/ VSe9W984Cf5Tgzo4
Asie-Pacifique (Tokyo)	ap-northeast-1	serial-console.ec2-instance-connect.ap-northeast-1.aws	SHA256:RQ fsDCZTOfQ awewTRDV1t9Em/ HMrFQe+CRlIOT 5um4k
Canada (Centre)	ca-central-1	serial-console.ec2-instance-connect.ca-central-1.aws	SHA256: P2O2 MWKPO6 jOZwmp YW738FIOT HdUTyEv2g czYMMO7s4

Nom de la région	Région	Point de terminaison	Empreinte digitale
Chine (Beijing)	cn-north-1	ec2-serial-console.cn-north-1.api.amazonwebservices.com.cn	SHA2562 : 47UU3+WgHVFy D28V/LGGT+Y aFUx ggMeqjvSlgngpg
Chine (Ningxia)	cn-northwest-1	ec2-serial-console.cn-northwest-1.api.amazonwebservices.com.cn	SHA256T : 90 dgrNZki QOdVfYEBU hO4SzUA VWI5rYOZG TogpwmiM
Europe (Francfort)	eu-central-1	serial-console.ec2-instance-connect.eu-central-1.aws	SHA256: aCMFS/ yIcOdOlkXvOl bBnrJJ3Fy8AmZ1ToE + 0k0De2C
Europe (Irlande)	eu-west-1	serial-console.ec2-instance-connect.eu-west-1.aws	SHA256: H2AA GAWO4Hath htm6ezs3Bj7udgUxi2 qTrHjZAwCW6E
Europe (Londres)	eu-west-2	serial-console.ec2-instance-connect.eu-west-2.aws	SHA256:A69RD5CE// AEG4Amm53I 6lkD1ZPvS BCV3tTPW2RnJg8
Europe (Milan)	eu-south-1	ec2-serial-console.eu-south-1.api.aws	SHA256:Lc0 kOVJnpg F 0A7N99 yBVrxn 0 ecLb XSX95cuuS7X7QK3
Europe (Paris)	eu-west-3	serial-console.ec2-instance-connect.eu-west-3.aws	SHA256:q8 IdnAf 9 pymeNe nFVng 8B Y3/RPArkxswJUzfrlx eEWs

Nom de la région	Région	Point de terminaison	Empreinte digitale
Europe (Espagne)	eu-south-2	ec2-serial-console.eu-south-2.api.aws	SHA256:Go /4F4N7T45 CW2DFRlu6 69QNxqFxEcsR6fZUz ZcwoEc
Europe (Stockholm)	eu-north-1	serial-console.ec2-instance-connect.eu-north-1.aws	SHA256: tkGFFUVUD voc Oui GSS3Cu8Gd l6w2uI32E PNpKFKLwX84
Europe (Zurich)	eu-central-2	ec2-serial-console.eu-central-2.api.aws	SHA256: 8 ppx2 mBMf 6 0/4 O WdCw NUlzKfwM4 IfRz aXFut QXWp6mk
Israël (Tel Aviv)	il-central-1	ec2-serial-console.il-central-1.api.aws	SHA256:JR 6q8v6kNNP i8+QSFQ4d j5dimNmZP TgwgsM1SNvtYyU
Moyen-Orient (Bahreïn)	me-south-1	ec2-serial-console .me-south-1.api.aws	SHA256:nP jLLKHu2Qn LdUq2kVAr soK5xvPJO MRJKCBzCDqC3k8
Moyen-Orient (UAE)	me-central-1	ec2-serial-console .me-central-1.api.aws	SHA256:zpb5 Bz+L0 B4/X duKi dFwPeyyk MPBYhI zXNe FSDKBvLE

Nom de la région	Région	Point de terminaison	Empreinte digitale
Amérique du Sud (São Paulo)	sa-east-1	serial-console.ec2-instance-connect.sa-east-1.aws	SHA256: RD2+/32 OGNJeW1+B otbih62O 1Di yVIem ENaQzC qAPDq
AWS GovCloud (USA Est)	us-gov-east-1	serial-console.ec2-instance-connect.us-gov-east-1.amazonaws.com	SHA256: tIwe 19 ANS ET GWsoyLClr tvu38YEEh PLUS DHIkqnDcZ nmtebvF28
AWS GovCloud (US-Ouest)	us-gov-west-1	serial-console.ec2-instance-connect.us-gov-west-1.amazonaws.com	SHA256: kfOFRWLa OZfB bRf +utbd3 8 8 n OlPf GO2YZLqXZ iIw5DQ

Déconnectez-vous de la console EC2 série

Si vous n'avez plus besoin d'être connecté à la console EC2 série de votre instance, vous pouvez vous en déconnecter. Lorsque vous vous déconnectez de la console série, toutes les sessions shell en cours d'exécution sur l'instance continuent de s'exécuter. Si vous souhaitez mettre fin à la session du shell, vous devez y mettre fin avant de vous déconnecter de la console série.

Considérations

- La connexion à la console série dure généralement une heure, à moins que vous ne vous déconnectiez. Toutefois, pendant la maintenance du système, Amazon EC2 déconnectera la session de console série.
- 30 secondes sont nécessaires pour déconnecter une session après la déconnexion de la console série afin d'autoriser une nouvelle session.

La méthode de déconnexion de la console série dépend du client.

Client basé sur le navigateur

Pour vous déconnecter de la console série, fermez la fenêtre du terminal du navigateur de la console.

SSHClient ouvert standard

Pour vous déconnecter de la console série, utilisez la commande suivante pour fermer la SSH connexion. Cette commande doit être exécutée immédiatement après une nouvelle ligne.

```
~.
```

La commande que vous utilisez pour fermer une SSH connexion peut être différente selon le SSH client que vous utilisez.

Résoudre les problèmes liés à votre EC2 instance Amazon à l'aide de la console EC2 série

À l'aide de la console EC2 série, vous pouvez résoudre les problèmes de démarrage, de configuration réseau et autres en vous connectant au port série de votre instance.

Utilisez les instructions relatives au système d'exploitation de votre instance et à l'outil que vous avez configuré sur votre instance.

> **Note**
>
> Avant de commencer, assurez-vous d'avoir rempli les conditions requises, y compris la configuration de l'outil de dépannage que vous avez choisi.

(Instances Linux) GRUB À utiliser pour dépanner votre instance

GNUGRUB(abréviation de GNU GRand Unified Bootloader, communément appeléGRUB) est le chargeur de démarrage par défaut pour la plupart des systèmes d'exploitation Linux. GRUBDans le menu, vous pouvez sélectionner le noyau dans lequel démarrer ou modifier les entrées du menu pour changer le mode de démarrage du noyau. Cela peut être utile lors de la résolution des problèmes d'une instance défaillante.

Le GRUB menu s'affiche pendant le processus de démarrage. Le menu n'est pas accessible en mode normalSSH, mais vous pouvez y accéder via la console EC2 série.

Vous pouvez démarrer en mode mono-utilisateur ou en mode d'urgence. Le mode utilisateur unique démarre le noyau à un niveau d'exécution inférieur. Par exemple, il peut monter le système de fichiers mais pas activer le réseau, ce qui vous permet d'effectuer la maintenance nécessaire pour

réparer l'instance. Le mode d'urgence est similaire au mode utilisateur unique, sauf que le noyau fonctionne au niveau d'exécution le plus bas possible.

Pour démarrer en mode utilisateur unique

1. Connectez-vous à la console série de l'instance.
2. Redémarrez l'instance à l'aide de la commande suivante.

```
[ec2-user ~]$ sudo reboot
```

3. Pendant le redémarrage, lorsque le GRUB menu apparaît, appuyez sur n'importe quelle touche pour arrêter le processus de démarrage.
4. Dans le GRUB menu, utilisez les flèches pour sélectionner le noyau dans lequel démarrer, puis appuyez e sur votre clavier.
5. Utilisez les touches fléchées pour localiser votre curseur sur la ligne contenant le noyau. La ligne commence par l'un `linux` ou l'autre ou `linux16` en fonction de AMI celui qui a été utilisé pour lancer l'instance. Pour Ubuntu, deux lignes commençant par `linux` doivent toutes deux être modifiées à l'étape suivante.
6. À la fin de la ligne, ajoutez le mot `single`.

   Voici un exemple pour Amazon Linux 2.

```
linux /boot/vmlinuz-4.14.193-149.317.amzn2.aarch64 root=UUID=d33f9c9a-\
dadd-4499-938d-ebbf42c3e499 ro  console=tty0 console=ttyS0,115200n8 net.ifname\
s=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.she\
ll=0 single
```

7. Appuyez sur Ctrl+X pour démarrer en mode utilisateur unique.
8. À l'**`login`**invite, entrez le nom d'utilisateur de l'utilisateur basé sur un mot de passe que vous avez configuré précédemment, puis appuyez sur Entrée.
9. À l'invite `Password`, entrez le mot de passe, puis appuyez sur Entrée.

Pour démarrer en mode d'urgence

Suivez les mêmes étapes que le mode utilisateur unique, mais à l'étape 6, ajoutez le mot à la `emergency` place de`single`.

(Instances Linux) SysRq À utiliser pour dépanner votre instance

La touche System Request (SysRq), parfois qualifiée de SysRq « magique », peut être utilisée pour envoyer directement une commande au noyau, en dehors d'un shell, et le noyau répondra, indépendamment de ce que fait le noyau. Par exemple, si l'instance ne répond plus, vous pouvez utiliser la SysRq clé pour indiquer au noyau de se bloquer ou de redémarrer. Pour plus d'informations, voir Magic SysRq key sur Wikipedia.

Vous pouvez utiliser des SysRq commandes dans le client basé sur le navigateur EC2 Serial Console ou dans un SSH client. La commande d'envoi d'une requête d'interruption est différente pour chaque client.

Pour l'utiliser SysRq, choisissez l'une des procédures suivantes en fonction du client que vous utilisez.

Browser-based client

À utiliser SysRq dans le client basé sur le navigateur de la console série

1. Connectez-vous à la console série de l'instance.
2. Pour envoyer une demande d'interruption, appuyez sur `CTRL+0` (zéro). Si votre clavier prend cette fonctionnalité en charge, vous pouvez également envoyer une demande d'interruption à l'aide de la touche Pause ou Attn.

   ```
   [ec2-user ~]$ CTRL+0
   ```

3. Pour émettre une SysRq commande, appuyez sur la touche de votre clavier correspondant à la commande requise. Par exemple, pour afficher une liste de SysRq commandes, appuyez surh.

   ```
   [ec2-user ~]$ h
   ```

   Le résultat de la commande h est similaire à ce qui suit.

   ```
   [ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
   tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
   (j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
   tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
   ) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
   buffer(z)
   ```

SSH client

À utiliser SysRq dans un SSH client

1. Connectez-vous à la console série de l'instance.
2. Pour envoyer une demande d'interruption, appuyez sur ~B (tilde, suivi de B majuscule).

```
[ec2-user ~]$ ~B
```

3. Pour émettre une SysRq commande, appuyez sur la touche de votre clavier correspondant à la commande requise. Par exemple, pour afficher une liste de SysRq commandes, appuyez surh.

```
[ec2-user ~]$ h
```

Le résultat de la commande h est similaire à ce qui suit.

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
buffer(z)
```

> **Note**
>
> La commande que vous utilisez pour envoyer une demande d'interruption peut être différente selon le SSH client que vous utilisez.

(Instances Windows) SAC À utiliser pour dépanner votre instance

La fonctionnalité Special Admin Console (SAC) de Windows permet de dépanner une instance Windows. En vous connectant à la console série de l'instance et en l'utilisantSAC, vous pouvez interrompre le processus de démarrage et démarrer Windows en mode sans échec.

> **Note**
>
> Si vous l'activez SAC sur une instance, les EC2 services qui reposent sur la récupération du mot de passe ne fonctionneront pas depuis la EC2 console Amazon. Les agents de EC2 lancement de Windows on Amazon (EC2ConfigEC2Launchv1 et EC2Launch v2) s'appuient sur la console série pour exécuter diverses tâches. Ces tâches ne s'exécutent pas correctement lorsque vous SAC les activez sur une instance. Pour plus d'informations sur les agents de EC2 lancement de Windows sur Amazon, consultezthe section called "Configuration des instances Windows". Si vous l'activezSAC, vous pourrez le désactiver ultérieurement. Pour de plus amples informations, veuillez consulter Désactiver SAC et menu de démarrage.

Rubriques

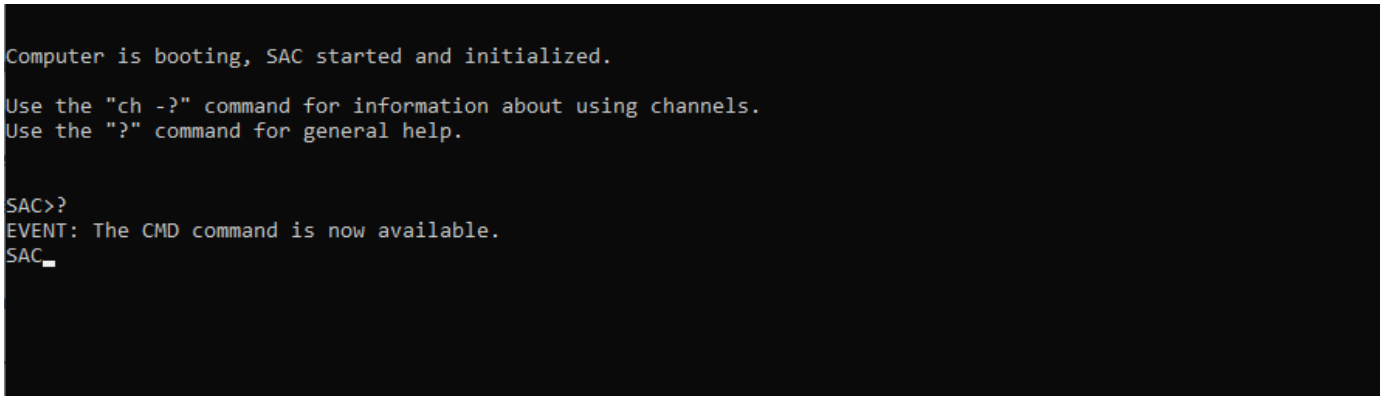
- Utiliser SAC
- Utiliser le menu de démarrage
- Désactiver SAC et menu de démarrage

Utiliser SAC

À utiliser SAC

1. Connectez-vous à la console série

   Si cette option SAC est activée sur l'instance, la console série affiche l'SAC>invite.

2. Pour afficher les SAC commandes, entrez**?**, puis appuyez sur Entrée.

   Sortie attendue

```
SAC>?
ch                    Channel management commands.  Use ch -? for more help.
cmd                   Create a Command Prompt channel.
d                     Dump the current kernel log.
f                     Toggle detailed or abbreviated tlist info.
? or help             Display this list.
i                     List all IP network numbers and their IP addresses.
i <#> <ip> <subnet> <gateway> Set IPv4 addr., subnet and gateway.
id                    Display the computer identification information.
k <pid>               Kill the given process.
l <pid>               Lower the priority of a process to the lowest possible.
lock                  Lock access to Command Prompt channels.
m <pid> <MB-allow>    Limit the memory usage of a process to <MB-allow>.
p                     Toggle paging the display.
r <pid>               Raise the priority of a process by one.
s                     Display the current time and date (24 hour clock used).
s mm/dd/yyyy hh:mm    Set the current time and date (24 hour clock used).
t                     Tlist.
restart               Restart the system immediately.
shutdown              Shutdown the system immediately.
crashdump             Crash the system. You must have crash dump enabled.
```

3. Pour créer un canal d'invite de commandes (tel que `cmd0001` ou `cmd0002`), saisissez **`cmd`**, puis appuyez sur Entrée.
4. Pour afficher le canal d'invite de commandes, appuyez sur ESC, puis appuyez sur TAB.

   Sortie attendue

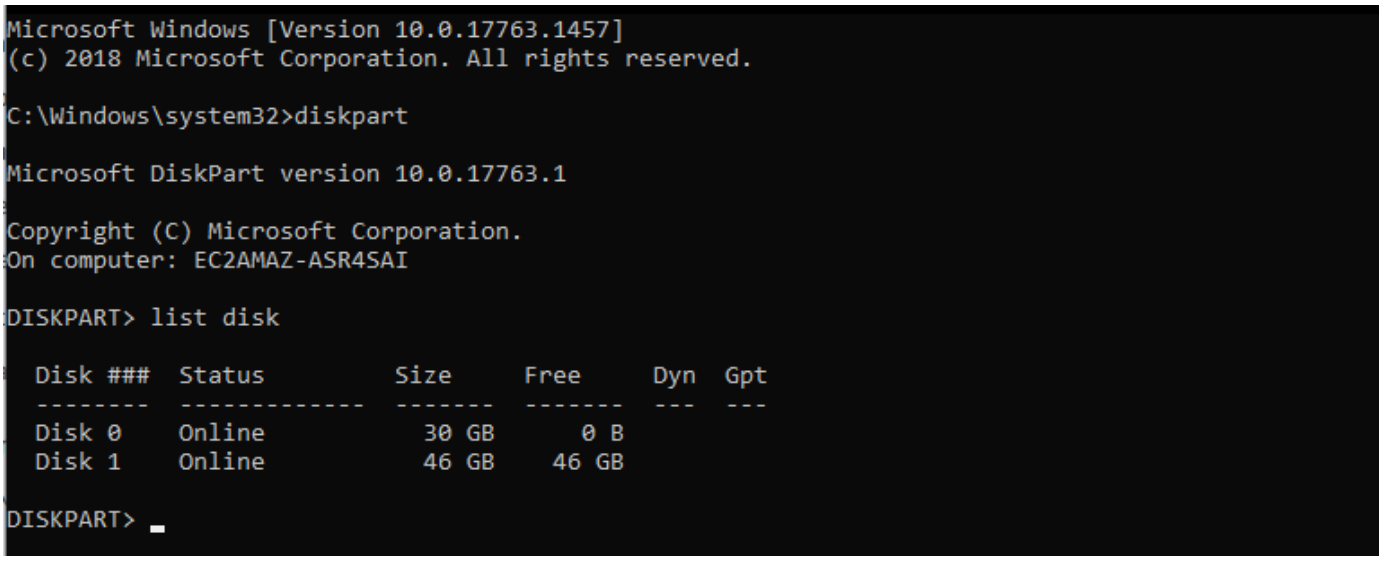
```
Name:                 Cmd0001
Description:          Command
Type:                 VT-UTF8
Channel GUID:         ef9f20a0-1287-11eb-82b0-0e4ba51872e5
Application Type GUID: 63d02271-8aa4-11d5-bccf-00b0d014a2d0

Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.
```

5. Pour changer de chaîne, appuyez simultanément sur ESC+ TAB +numéro de chaîne. Par exemple, pour passer à la `cmd0002` chaîne (si elle a été créée), appuyez sur ESC+ TAB +2.
6. Entrez les informations d'identification requises par le canal d'invite de commandes.

```
Please enter login credentials.
Username: Administrator
Domain  : .
Password: *******
```

L'invite de commande correspond au shell de commande complet que vous obtenez sur un bureau, mais ne permet toutefois pas la lecture des caractères déjà envoyés.



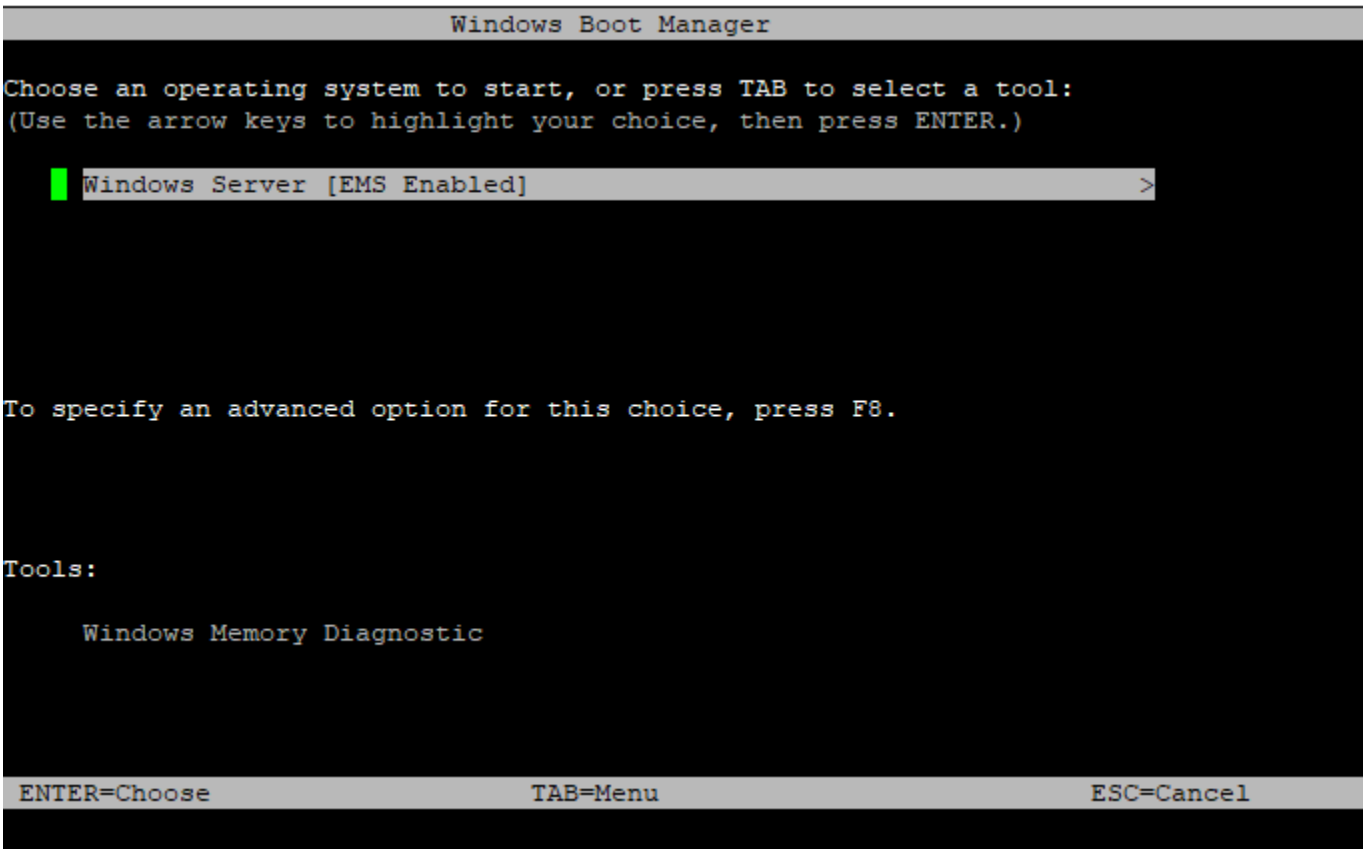
PowerShell peut également être utilisé à partir de l'invite de commande.

Notez que vous devrez peut-être définir la préférence de progression en mode silencieux.

```
PS C:\Windows\system32> $ProgressPreference="SilentlyContinue"
PS C:\Windows\system32> $computerInfo = Get-ComputerInfo
PS C:\Windows\system32> $computerInfo.Csprocessors[0].Name
Intel(R) Xeon(R) Platinum 8124M CPU @ 3.00GHz
PS C:\Windows\system32> $computerInfo.Csprocessors[0].Description
Intel64 Family 6 Model 85 Stepping 4
PS C:\Windows\system32>
```

Utiliser le menu de démarrage

Si le menu de démarrage de l'instance est activé et qu'elle est redémarrée après la connexion viaSSH, le menu de démarrage devrait s'afficher, comme suit.



Commandes du menu de démarrage

ENTER

Démarre l'entrée sélectionnée du système d'exploitation.

TAB

Bascule vers le menu Outils.

ESC

Annule et redémarre l'instance.

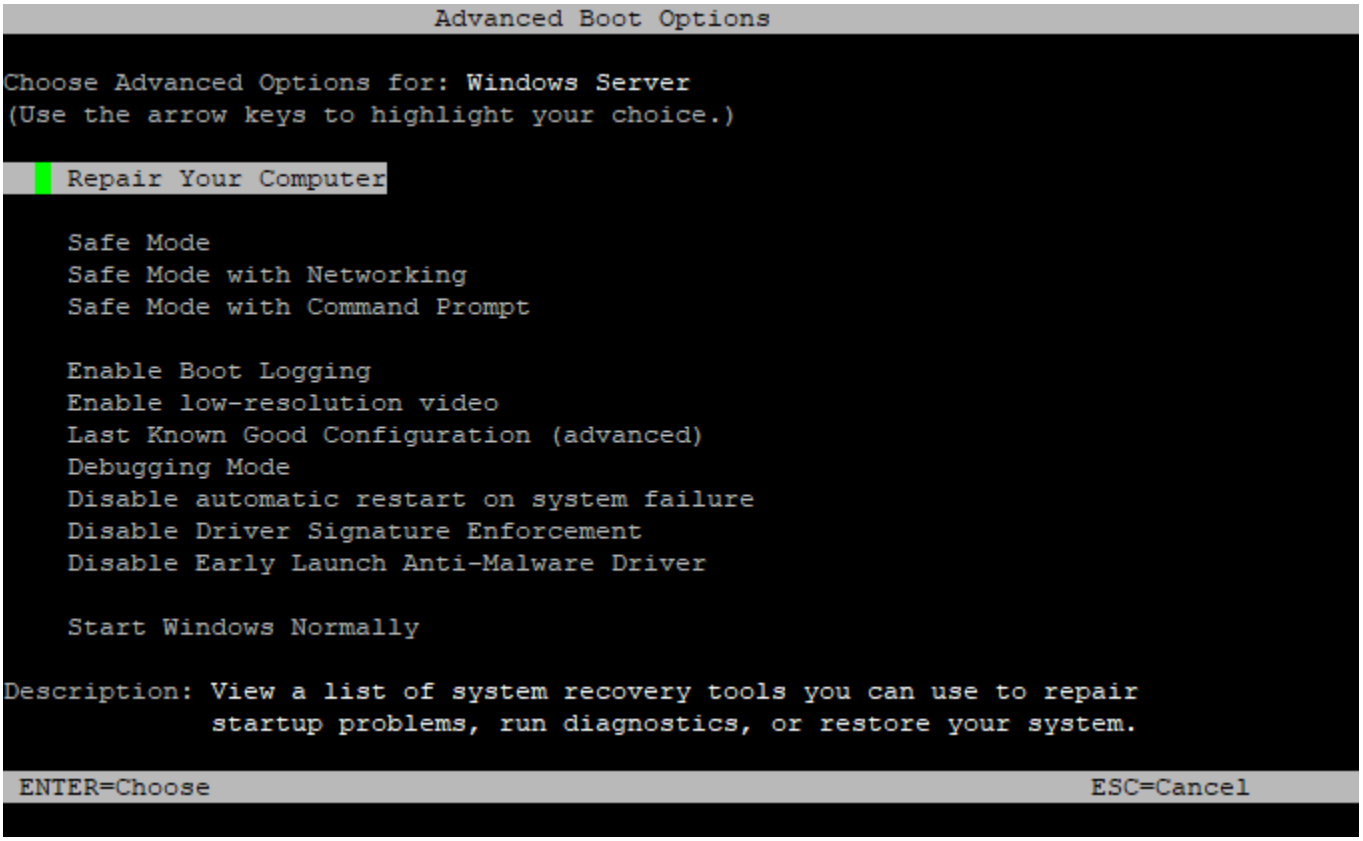
ESCsuivie par 8

Revient à appuyer sur F8. Affiche les options avancées de l'élément sélectionné.

ESCtouche + flèche gauche

Retourne au menu de démarrage initial.

> **Note**
>
> La ESC touche à elle seule ne vous ramène pas au menu principal car Windows attend de voir si une séquence d'échappement est en cours.



Désactiver SAC et menu de démarrage

Si vous activez SAC le menu de démarrage, vous pourrez désactiver ces fonctionnalités ultérieurement.

Utilisez l'une des méthodes suivantes pour désactiver SAC le menu de démarrage d'une instance.

PowerShell

Pour désactiver SAC et le menu de démarrage sur une instance Windows

1. Connectez-vous à votre instance et effectuez les étapes suivantes à partir d'une ligne de PowerShell commande élevée.
2. Désactivez d'abord le menu de démarrage en changeant la valeur en no.

```
bcdedit /set '{bootmgr}' displaybootmenu no
```

3. Désactivez-le ensuite en SAC modifiant la valeur en`off`.

```
bcdedit /ems '{current}' off
```

4. Appliquez la configuration mise à jour en redémarrant l'instance.

```
shutdown -r -t 0
```

Command prompt

Pour désactiver SAC et le menu de démarrage sur une instance Windows

1. Connectez-vous à votre instance et exécutez les étapes suivantes à partir de l'invite de commandes.
2. Désactivez d'abord le menu de démarrage en changeant la valeur en `no`.

```
bcdedit /set {bootmgr} displaybootmenu no
```

3. Désactivez-le ensuite en SAC modifiant la valeur en`off`.

```
bcdedit /ems {current} off
```

4. Appliquez la configuration mise à jour en redémarrant l'instance.

```
shutdown -r -t 0
```

Envoyer une interruption de diagnostic pour déboguer une instance Amazon inaccessible EC2

Warning

Les interruptions de diagnostic sont destinées à être utilisées par les utilisateurs avancés. Une utilisation incorrecte pourrait avoir un impact négatif sur votre instance. L'envoi d'une

interruption de diagnostic à une instance peut déclencher un plantage et un redémarrage d'une instance, ce qui peut entraîner la perte de données.

Vous pouvez envoyer une interruption de diagnostic à une instance inaccessible ou ne répondant pas pour déclencher manuellement une panique au niveau du noyau pour une instance Linux, ou une erreur d'arrêt (communément appelée erreur d'écran bleu) pour une instance Windows.

Instances Linux

Les systèmes d'exploitation Linux tombent généralement en panne et redémarrent en cas de panique de noyau. Le comportement spécifique du système d'exploitation dépend de sa configuration. Vous pouvez aussi utiliser une panique de noyau pour que le noyau système du système d'exploitation de l'instance effectue des tâches telles que la génération d'un fichier de vidage sur incident. Vous pouvez alors utiliser les informations du fichier de vidage sur incident pour effectuer l'analyse de la cause de la panne et le débogage de l'instance. Les données de vidage sur incident sont générées localement par le système d'exploitation sur l'instance elle-même.

instances Windows

En général, les systèmes d'exploitation Windows tombent en panne et redémarrent en cas d'erreur d'arrêt, mais le comportement du système dépend de sa configuration. Une erreur d'arrêt peut également provoquer l'écriture d'informations de débogage dans un fichier par le système d'exploitation (par exemple, vidage mémoire du noyau). Vous pouvez ensuite utiliser ces informations pour effectuer une analyse de la cause racine et déboguer l'instance. Les données de vidage mémoire sont générées localement par le système d'exploitation sur l'instance elle-même.

Avant d'envoyer une interruption de diagnostic à votre instance, nous vous recommandons de consulter la documentation de votre système d'exploitation, puis d'apporter les modifications nécessaires à la configuration.

Sommaire

Types d'instance pris en charge

L'interruption diagnostique est prise en charge sur tous les types d'instances basées sur Nitro, à l'exception de celles alimentées par des processeurs AWS Graviton. Pour plus d'informations, consultez les instances basées sur le système AWS Nitro et AWS Graviton.

Prérequis

Avant d'utiliser une interruption de diagnostic, vous devez configurer le système d'exploitation de votre instance. Cela garantit qu'il exécute les actions dont vous avez besoin en cas de panique du noyau (instances Linux) ou d'erreur d'arrêt (instances Windows).

Instances Linux

Pour configurer Amazon Linux 2 pour générer un vidage sur incident en cas de panique de noyau

1. Connectez-vous à votre instance.
2. Installez kexec et kdump.

```
[ec2-user ~]$ sudo yum install kexec-tools -y
```

3. Configurez le noyau afin qu'il réserve une quantité appropriée de mémoire pour le noyau secondaire. La quantité de mémoire à réserver dépend de la quantité de mémoire totale disponible de votre instance. Ouvrez le fichier `/etc/default/grub` à l'aide de votre éditeur de texte préféré, localisez la ligne commençant par `GRUB_CMDLINE_LINUX_DEFAULT`, puis ajoutez le paramètre `crashkernel` au format suivant : `crashkernel=`*`memory_to_reserve`*. Par exemple, pour réserver `160MB`, modifiez le fichier `grub` comme suit :

```
GRUB_CMDLINE_LINUX_DEFAULT="crashkernel=160M console=tty0 console=ttyS0,115200n8
 net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
 rd.shell=0"
GRUB_TIMEOUT=0
GRUB_DISABLE_RECOVERY="true"
```

4. Enregistrez les modifications, puis fermez le fichier `grub`.
5. Reconstruisez le fichier GRUB2 de configuration.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

6. Sur les instances basées sur Intel et les AMD processeurs, la `send-diagnostic-interrupt` commande envoie une interruption non masquable inconnue (NMI) à l'instance. Vous devez configurer le noyau pour qu'il se bloque lorsqu'il reçoit l'inconnuNMI. Ouvrez le fichier `/etc/sysctl.conf` à l'aide de l'éditeur de texte de votre choix et ajoutez ce qui suit.

```
kernel.unknown_nmi_panic=1
```

7. Redémarrez votre instance et reconnectez-la.
8. Vérifiez que le noyau a été démarré avec le paramètre `crashkernel` correct.

```
$ grep crashkernel /proc/cmdline
```

L'exemple de sortie suivant illustre une configuration réussie.

```
BOOT_IMAGE=/boot/vmlinuz-4.14.128-112.105.amzn2.x86_64 root=UUID=a1e1011e-
e38f-408e-878b-fed395b47ad6 ro crashkernel=160M console=tty0 console=ttyS0,115200n8
 net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
 rd.shell=0
```

9. Vérifiez que le service kdump est en cours d'exécution.

```
[ec2-user ~]$ systemctl status kdump.service
```

L'exemple de sortie suivant présente le résultat lorsque le service kdump est en cours d'exécution.

```
kdump.service - Crash recovery kernel arming
   Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled; vendor preset:
 enabled)
   Active: active (exited) since Fri 2019-05-24 23:29:13 UTC; 22s ago
  Process: 2503 ExecStart=/usr/bin/kdumpctl start (code=exited, status=0/SUCCESS)
 Main PID: 2503 (code=exited, status=0/SUCCESS)
```

> **Note**
>
> Par défaut, le fichier de vidage sur incident est enregistré dans `/var/crash/`. Pour modifier cet emplacement, modifiez le fichier `/etc/kdump.conf` à l'aide de l'éditeur de texte de votre choix.

Pour configurer Amazon Linux pour générer un vidage sur incident en cas de panique de noyau

1. Connectez-vous à votre instance.
2. Installez kexec et kdump.

   ```
   [ec2-user ~]$ sudo yum install kexec-tools -y
   ```

3. Configurez le noyau afin qu'il réserve une quantité appropriée de mémoire pour le noyau secondaire. La quantité de mémoire à réserver dépend de la quantité de mémoire totale disponible de votre instance.

   ```
   $ sudo grubby --args="crashkernel=memory_to_reserve" --update-kernel=ALL
   ```

   Par exemple, pour réserver `160MB` pour le noyau d'incident, utilisez la commande qui suit.

   ```
   $ sudo grubby --args="crashkernel=160M" --update-kernel=ALL
   ```

4. Sur les instances basées sur Intel et les AMD processeurs, la `send-diagnostic-interrupt` commande envoie une interruption non masquable inconnue (NMI) à l'instance. Vous devez configurer le noyau pour qu'il se bloque lorsqu'il reçoit l'inconnuNMI. Ouvrez le fichier `/etc/sysctl.conf` à l'aide de l'éditeur de texte de votre choix et ajoutez ce qui suit.

   ```
   kernel.unknown_nmi_panic=1
   ```

5. Redémarrez votre instance et reconnectez-la.
6. Vérifiez que le noyau a été démarré avec le paramètre `crashkernel` correct.

   ```
   $ grep crashkernel /proc/cmdline
   ```

   L'exemple de sortie suivant illustre une configuration réussie.

```
root=LABEL=/ console=tty1 console=ttyS0 selinux=0 nvme_core.io_timeout=4294967295
 LANG=en_US.UTF-8 KEYTABLE=us crashkernel=160M
```

7. Vérifiez que le service kdump est en cours d'exécution.

```
[ec2-user ~]$ sudo service kdump status
```

Si le service est en cours d'exécution, la commande renvoie la réponse `Kdump is operational`.

> **Note**
>
> Par défaut, le fichier de vidage sur incident est enregistré dans `/var/crash/`. Pour modifier cet emplacement, modifiez le fichier `/etc/kdump.conf` à l'aide de l'éditeur de texte de votre choix.

Pour configurer SUSE Linux Enterprise, Ubuntu ou Red Hat Enterprise Linux

Sur les instances basées sur Intel et les AMD processeurs, la `send-diagnostic-interrupt` commande envoie une interruption non masquable inconnue (NMI) à l'instance. Vous devez configurer le noyau pour qu'il se bloque lorsqu'il reçoit l'inconnu NMI en ajustant le fichier de configuration de votre système d'exploitation. Pour plus d'informations sur la façon de configurer le noyau pour qu'il plante, consultez la documentation de votre système d'exploitation :

- SUSELinux Entreprise
- Ubuntu
- Red Hat Enterprise Linux (RHEL)

instances Windows

Pour configurer Windows afin qu'il génère un vidage mémoire en d'erreur d'arrêt

1. Connectez-vous à votre instance.
2. Ouvrez le Panneau de configuration, choisissez Système, Paramètres système avancés.
3. Dans la boîte de dialogue Propriétés, choisissez l'onglet Paramètres système avancés.

4. Dans la section Démarrage et récupération, choisissez Paramètres....
5. Dans la section System failure (Échec système), configurez les paramètres comme vous le souhaitez, puis choisissez OK.

Pour plus d'informations sur la configuration des erreurs d'arrêt de Windows, veuillez consulter Overview of memory dump file options for Windows.

Envoi d'une interruption de diagnostic

Une fois que vous avez effectué les modifications de configuration nécessaires, vous pouvez envoyer une interruption de diagnostic à votre instance à l'aide de AWS CLI ou Amazon EC2API.

AWS CLI

Pour envoyer une interruption de diagnostic à votre instance (AWS CLI)

Utilisez la send-diagnostic-interruptcommande et spécifiez l'ID de l'instance.

```
aws ec2 send-diagnostic-interrupt --instance-id i-1234567890abcdef0
```

PowerShell

Pour envoyer une interruption de diagnostic à votre instance (AWS Tools for Windows PowerShell)

Utilisez le Send-EC2DiagnosticInterruptcmdlt et spécifiez l'ID de l'instance.

```
PS C:\> Send-EC2DiagnosticInterrupt -InstanceId i-1234567890abcdef0
```

Historique du document pour le guide de EC2 l'utilisateur Amazon

Le tableau suivant décrit les ajouts importants au guide de EC2 l'utilisateur Amazon à compter de 2019. Nous mettons également fréquemment à jour le guide pour répondre aux commentaires que vous nous envoyez.

Modification	Description	Date
Nouvelles fonctionnalités pour gérer les réservations de capacité à la demande	Vous pouvez désormais diviser votre réservation de capacité, déplacer la capacité entre les réservations de capacité et modifier l'attribut d'éligibilité des instances de votre réservation de capacité.	14 août 2024
Support d'hibernation pour C6g, C6gn, C6gd, C7g, C7gd, M6g, M6gd, M7g, M7gd, R6g et R6gd	Mettez en veille prolongée vos instances récemment lancées qui s'exécutent sur les types d'instances C6g, C6gn, C6gD, M6g, M6gD, M7g, M7gD, M7gD, R6g et R6gd.	30 juillet 2024
Support d'hibernation pour les types AMIs d'instances de Graviton compatibles	Mettez en veille prolongée vos instances récemment lancées depuis un Amazon Linux ou Ubuntu compatible avec les types d'instances AMI Graviton.	30 juillet 2024
Types d'instances supplémentaires pris en charge pour Credential Guard	Vous pouvez désormais activer Credential Guard pour les instances C7i, C7-flex, M7i, M7i-Flex, R7i, R7i-Flex et T3.	26 juin 2024

EC2Instances M1 Ultra Mac	Nouveau type d'instance à usage général doté de processeurs Apple M1 Ultra.	17 juin 2024
EC2outil de recherche de type d'instance — paramètres supplémentaires	L'outil de recherche de type d'EC2instance fournit désormais des paramètre s supplémentaires vous permettant de définir des exigences plus détaillées pour votre charge de travail.	5 juin 2024
Instances U7i-12TB, U7in-16TB, U7in-24TB et U7in-32TB	Nouveaux types d'instanc es à mémoire élevée dotés de processeurs Intel Xeon Scalable de 4e génération.	28 mai 2024
Nouvelle politique gérée pour EC2 Fast Launch	Ajout de la EC2FastLa unchFullAccess politique permettant d'effectuer API des actions liées à la fonctionnalité de lancement EC2 rapide à partir d'une instance.	14 mai 2024
AMIprotection contre le désenregistrement	Vous pouvez activer la protection de désinscription AMI pour empêcher toute suppression accidentelle ou malveillante.	23 avril 2024
PTPhorloge matérielle — prise en charge des types d'instanc e	L'horloge PTP matérielle est désormais disponible sur les types d'instance C7a, C7i, M7a, M7g, M7i, R7a et R7i.	22 avril 2024

Ajout de considérations relatives aux performances de Nitro pour une mise en réseau améliorée	Cette page se concentre sur les considérations relatives au réseau afin de vous aider à optimiser les performances de vos EC2 instances Amazon basées sur Nitro.	4 avril 2024
Nouvelle politique gérée pour les EBS instantanés VSS basés	Amazon EC2 VSS dispose d'une nouvelle politique IAM gérée que vous pouvez ajouter à votre rôle de profil d'instanc e afin de garantir le maintien de vos autorisations up-to-dat e et de respecter les meilleure s pratiques.	28 mars 2024
PTPhorloge matérielle — USA Est (Virginie du Nord)	L'horloge PTP matérielle est désormais disponible dans la région de l'est des États-Unis (Virginie du Nord).	26 mars 2024
Définir IMDSv2 comme compte par défaut	Vous pouvez configurer tous les nouveaux lancements d'EC2instances dans votre compte pour utiliser le service de métadonnées d'instance version 2 (IMDSv2) par défaut.	25 mars 2024
Tag : nouveau Linux AMIs créé à partir d'un instantané	Lorsque vous créez un Linux AMI à partir d'un instantan é, vous pouvez étiqueter le nouveauAMI.	7 mars 2024

Marquer les nouveautés AMIs et les instantanés lors de la copie	Lorsque vous copiez unAMI, vous pouvez étiqueter les nouveaux AMI et les nouveaux instantanés avec les mêmes balises, ou vous pouvez les étiqueter avec des balises différentes.	7 mars 2024
Supprimer les pages AWS du pack d'administration	Le pack d' AWS administration était principalement utilisé avec Windows Server 2012 et versions antérieures. Ces anciennes versions de plate-forme de système d'exploitation ne sont plus prises en charge. Pour gérer et dépanner votre parc de serveurs fonctionnant sur site ou sur site, consultez AWS AWS Systems Manager Fleet Manager.	12 février 2024
EC2Instance Connect préinstallée sur macOS AMIs	EC2Instance Connect est désormais préinstallé sur macOS Sonoma 14.2.1 ou version ultérieure, macOS Ventura 13.6.3 ou version ultérieure et macOS Monterey 12.7.2 ou version ultérieure. AMIs	26 janvier 2024
EC2Support d'Instance Connect pour CentOS, macOS et RHEL	Vous pouvez désormais installer EC2 Instance Connect sur les systèmes CentOS, macOS et. RHEL AMIs	6 décembre 2023

Prise en charge de la mise en veille prolongée pour C7a, C7i, R7a, R7i et R7iz	Désormais, vous pouvez mettre en veille prolongée les instances que vous venez de lancer et qui s’exécutent sur les types d’instances C7a, C7i, R7a, R7i et R7iz.	1er décembre 2023
Sélecteur de type d'EC2instance Amazon Q	Le sélecteur de type d'EC2instance Amazon Q prend en compte votre cas d'utilisation, votre type de charge de travail et les préférences CPU du fabricant, ainsi que la façon dont vous hiérarchisez le prix et les performances. Il utilise ensuite ces données pour fournir des conseils et des suggestions concernant les types d'EC2instances Amazon les mieux adaptés à vos nouvelles charges de travail.	28 novembre 2023
EC2 Offre gratuite	Vous pouvez suivre votre utilisation du niveau EC2 gratuit depuis le EC2 tableau de bord.	26 novembre 2023

Console-to-Code	Console-to-Code peut vous aider à faire vos premiers avec le code d'automatisation. Console-to-Code enregistre les actions de votre console, puis utilise l'IA générative pour suggérer du code dans votre infrastructure préférée au format de code. Vous pouvez utiliser le code comme point de départ, en le personnal isant pour qu'il soit prêt pour la production en fonction de votre cas d'utilisation spécifique.	26 novembre 2023
Délais de suivi d'inactivité de connexion configurables	Les connexions de groupe de sécurité qui restent inactives peuvent entraîner l'épuisem ent du suivi des connexion s, empêcher le suivi des connexions et entraîner la perte de paquets. Vous pouvez désormais définir le délai en secondes pour le suivi de connexion de groupe de sécurité sur une interface réseau Elastic.	17 novembre 2023
PTPhorloge matérielle	Les instances prises en charge disposent désormais d'une horloge matérielle Precision Time Protocol (PTP). L'horloge PTP matérielle prend en charge une connexion NTP ou une PTP connexion directe.	16 novembre 2023

Modification du type d'instance d'une instance dont la mise en veille prolongée est activée	Vous pouvez désormais modifier le type d'une instance dont la mise en veille prolongée est activée lorsqu'elle est à l'état `stopped`.	16 novembre 2023
Topologie d'instance	Vous pouvez utiliser le DescribeInstanceTopology API pour détecter l'emplacement de vos instances, puis utiliser ces informations pour optimiser HPC les tâches ML en les exécutant sur des instances physiquement plus proches les unes des autres.	13 novembre 2023
EC2AMISupport partagé Fast Launch	Vous pouvez désormais activer le lancement EC2 rapide sur AMI un fichier partagé avec vous. Lorsque vous activez EC2 Fast Launch sur un partageAMI, les instantanés préconfigurés pour un lancement plus rapide sont créés dans votre compte.	6 novembre 2023
Blocs de capacité pour ML	Vous pouvez désormais réserver GPU des instances à une date future pour prendre en charge vos charges de travail d'apprentissage automatique (ML) de courte durée.	31 octobre 2023

Mise en veille prolongée d'instances Spot	Vous pouvez désormais mettre en veille prolongée vos instances Spot en utilisant la même expérience de mise en veille prolongée et les mêmes familles d'instances que celles actuellement disponibles pour les instances à la demande.	24 octobre 2023
Paramètres par défaut pour bloquer l'accès public pour AMIs	Bloquer l'accès public pour AMIs est désormais activé par défaut pour tous les nouveaux comptes et pour les comptes existants qui ne sont pas publicsAMIs.	20 octobre 2023
Vue EC2 globale d'Amazon	Amazon EC2 Global View prend en charge des types de ressources supplémen taires et des options d'afficha ge personnalisables.	18 octobre 2023
Support d'hibernation pour Ubuntu 22.04.2 LTS (Jammy Jellyfish)	Mettez en veille prolongée vos instances récemment lancées depuis Ubuntu LTS 22.04.2 (Jammy Jellyfish). AMI	16 octobre 2023
Désactiver un AMI	Vous pouvez désactiver an AMI pour l'empêcher d'être utilisé pour les lancements d'instances.	12 octobre 2023
Contrôles EBS d'état joints	Vous pouvez utiliser les vérifications de EBS statut jointes pour vérifier si les EBS volumes Amazon attachés à une instance sont accessibles.	11 octobre 2023

Prise en charge de la mise en veille prolongée pour Red Hat Enterprise Linux 9	Mettez en veille prolongée les instances que vous venez de lancer depuis Red Hat Enterprise Linux 9. AMI	2 octobre 2023
Prise en charge de la mise en veille prolongée pour Microsoft Windows Server 2022	Mettez en veille prolongée vos instances récemment lancées depuis Microsoft Windows Server 2022. AMI	2 octobre 2023
Support d'hibernation pour 2023 AL2	Hibernez vos instances nouvellement lancées qui ont été lancées à partir du 023. AL2 AMI	2 octobre 2023
Lancer l'interruption des instances Spot dans un parc d'instances Spot	Vous pouvez sélectionner un parc Spot dans la EC2 console Amazon et initier une interrupt ion des instances Spot dans le parc afin de pouvoir tester la façon dont les applications de vos instances Spot gèrent les interruptions.	21 septembre 2023
Bloquer l'accès public à AMIs	Vous pouvez activer le blocage de l'accès public AMIs au niveau du compte pour bloquer toute tentative de rendre votre compte AMIs public.	12 septembre 2023
Prise en charge de la mise en veille prolongée pour M7i et M7i-flex	Désormais, vous pouvez mettre en veille prolongée les instances que vous venez de lancer et qui s'exécutent sur les types d'instances M7i et M7i-flex	22 août 2023

EC2-Classic est obsolète	Avec EC2 -Classic, EC2 les instances s'exécutaient sur un réseau unique et plat partagé avec d'autres clients. Amazon VPC remplace EC2 -Classic. Avec AmazonVPC , vos instances s'exécutent dans un cloud privé virtuel (VPC) qui est logiquement isolé de votre AWS compte.	08 août 2023
Hôtes dédiés	Vous pouvez allouer des hôtes dédiés sur des actifs matériels spécifiques sur un Outpost.	20 juin 2023
EC2Point de terminaison Instance Connect	Vous pouvez désormais vous connecter à une instance via SSH ou RDP sans que l'instance ait une IPv4 adresse publique.	13 juin 2023
IMDSAnalyseur de packages	Vous pouvez désormais utiliser l'analyseur de IMDS paquets pour identifier les sources d'IMDSv1appels sur vos EC2 instances.	1er juin 2023
EC2Instances bare metal de console série	La console EC2 série prend désormais en charge la connectivité au port série de certaines instances bare metal.	11 avril 2023

Quotas de modèles de lancement	Vous pouvez désormais consulter vos quotas pour les modèles de lancement et les versions des modèles de lancement dans la console Service Quotas et en utilisant les Quotas de ServiceCLI.	3 avril 2023
Notifications d'utilisation des réserves de capacité	AWS Health envoie désormais des notifications lorsque le taux d'utilisation des capacités pour les réservations de capacité de votre compte tombe en dessous de 20 %.	3 avril 2023
Groupes de réserve de capacité	Vous pouvez désormais ajouter des réserves de capacité qui sont partagées avec vous aux groupes de réserves de capacité qui vous appartiennent.	30 mars 2023
Modifier les options des métadonnées d'instance	Vous pouvez désormais utiliser la EC2 console Amazon pour modifier les options de métadonnées de l'instance.	20 mars 2023
Mises à jour du système d'exploitation macOS sur place	Vous pouvez désormais effectuer des mises à jour sur place du système d'exploit ation macOS d'Apple sur les instances Mac M1.	14 mars 2023

UEFIpréféré	Vous pouvez désormais en créer un AMI qui prend en charge à la fois les modes de BIOS démarrage Unified Extensible Microware Interface (UEFI) et Legacy.	3 mars 2023
Modifier un AMI formulaire IMDSv2	Modifiez votre instance existante AMI afin que les instances soient lancées à partir de l'option AMI requise IMDSv2 par défaut.	28 février 2023
Sécurité basée sur la virtualisation de Windows – Credential Guard	Vous pouvez activer Credential Guard, une fonctionnalité de sécurité basée sur la virtualisation (VBS), sur les instances Amazon prises en charge. EC2	31 janvier 2023
AMIalias dans les modèles de lancement	Vous pouvez spécifier un AWS Systems Manager paramètre au lieu de l'AMIID dans vos modèles de lancement pour éviter d'avoir à mettre à jour les modèles chaque fois que l'AMIID change.	19 janvier 2023
Prise en charge de la mise en veille prolongée pour C6i, i3en et M6i	Désormais, vous pouvez mettre en veille prolongée les instances que vous venez de lancer et qui s'exécutent sur les types d'instances C6i, I3en et M6i.	19 décembre 2022

Prévention des écritures déchirées	Améliorez les performances de vos charges de travail de bases de données relationnelles gourmandes en E/S et réduisez la latence sans affecter négativement la résilience des données grâce à la fonction de prévention des écritures déchirées, une fonctionnalité de stockage par blocs.	29 novembre 2022
ENAExpress	Augmentez le débit et minimisez la latence finale du trafic réseau entre les EC2 instances avec ENA Express.	28 novembre 2022
Copier les AMI tags	Lorsque vous copiez unAMI, vous pouvez copier vos AMI balises définies par l'utilisateur en même temps.	18 novembre 2022
AMItaille pour le stockage et la restauration	La taille d'un paquet AMI (avant compression) pouvant être stocké et restauré depuis et vers un compartiment Amazon S3 peut désormais atteindre 5 000 Go.	16 novembre 2022

priceCapacityOptimizedstratégie d'allocation pour les instances Spot	Un parc d'instances Spot qui utilise la stratégie d'allocation `priceCapacityOptimized` examine à la fois le prix et la capacité pour sélectionner les groupes d'instances Spot les moins susceptibles d'être interrompus et dont le prix est le plus bas possible.	10 novembre 2022
price-capacity-optimizedstratégie d'allocation pour les instances Spot	Une EC2 flotte qui utilise la stratégie d'`price-capacity-optimized` allocation examine à la fois le prix et la capacité pour sélectionner les pools d'instances ponctuelles les moins susceptibles d'être interrompus et dont le prix est le plus bas possible.	10 novembre 2022
Annuler un AMI partage avec votre compte	Si un compte AMI a été partagé avec vous Compte AWS et que vous ne souhaitez plus le partager avec votre compte, vous pouvez supprimer les autorisations de lancement AMI de votre compte.	4 novembre 2022
Transfert d'adresses IP Elastic	Vous pouvez désormais transférer des adresses IP Elastic de l'une Compte AWS à l'autre.	31 octobre 2022

Remplacement d'un volume racine	Vous pouvez remplacer le EBS volume Amazon racine d'une instance en cours d'exécution à l'aide d'unAMI.	27 octobre 2022
Connexion automatique d'une instance à une base de données	Utilisez la fonction de connexion automatique pour connecter rapidement une ou plusieurs EC2 instances à une RDS base de données afin d'autoriser le trafic entre elles.	10 octobre 2022
AMIquotas	Les quotas s'appliquent désormais à la création et au partageAMIs.	10 octobre 2022
Configurer AMI pour IMDSv2	Configurez votre instance de AMI telle sorte que les instances soient lancées à partir de l'option AMI requise IMDSv2 par défaut.	3 octobre 2022
Lancer une interruption d'instance Spot	Vous pouvez sélectionner une instance Spot dans la EC2 console Amazon et lancer une interruption afin de tester la façon dont les applications de vos instances Spot gèrent les interruptions.	26 septembre 2022
AMIFournisseur vérifié	Dans la EC2 console Amazon, AMIs les entités publiques appartenant à Amazon ou à un partenaire Amazon vérifié sont marquées comme fournisseur vérifié.	22 juillet 2022

Groupes de placement sur AWS Outposts	Ajout d'une stratégie de répartition des hôtes pour les groupes de placement sur un Outpost.	30 juin 2022
Volumes `io2` Block Express	Vous pouvez modifier la taille et le provisionnement IOPS des volumes `io2` Block Express et vous pouvez les activer pour une restauration rapide des instantanés.	31 mai 2022
Hôtes dédiés sur AWS Outposts	Vous pouvez allouer des hôtes dédiés sur AWS Outposts.	31 mai 2022
Protection contre l'arrêt d'instance	Pour éviter que votre instance ne soit arrêtée accidente llement, vous pouvez activer la protection contre l'arrêt de l'instance.	24 mai 2022
UEFIDémarrage sécurisé	UEFISecure Boot s'appuie sur le processus de démarrage sécurisé de longue date d'Amazon EC2 et fournit des fonctionnalités supplémen taires defense-in-depth qui aident les clients à protéger leurs logiciels contre les menaces qui persistent après les redémarrages.	10 mai 2022

Nitro TPM	Le Nitro Trusted Platform Module (NitroTPM) est un appareil virtuel fourni par le système AWS Nitro et conforme à la spécification 2.0. TPM	10 mai 2022
AMIévénements de changement d'état	Amazon génère EC2 désormais un événement lorsqu'un élément AMI change d'état. Vous pouvez utiliser Amazon EventBridge pour détecter ces événements et y réagir.	9 mai 2022
Décrire les clés publiques	Vous pouvez demander la clé publique et la date de création d'une paire de EC2 clés Amazon.	28 avril 2022
Création des paires de clés	Vous pouvez spécifier le format de clé (PEMouPPK) lors de la création d'une nouvelle paire de clés.	28 avril 2022
Montez les systèmes de FSx fichiers Amazon au lancement	Vous pouvez monter un système de ZFS fichiers Amazon FSx for NetApp ONTAP ou Amazon FSx for Open nouveau ou existant au lancement à l'aide du nouvel assistant de lancement d'instance.	12 avril 2022

Nouvel assistant de lancement d'instance	Une expérience de lancement nouvelle et améliorée dans la EC2 console Amazon, qui permet de lancer une EC2 instance plus rapidement et plus facilement.	5 avril 2022
Déprécier automatiquement le public AMIs	Par défaut, la date d'obsoles cence de tous les publics AMIs est fixée à deux ans à compter de la date de AMI création.	31 mars 2022
Catégorie de métadonné es d'instance : autoscaling/ target-lifecycle-state	Lorsque vous utilisez des groupes Auto Scaling, vous pouvez accéder à l'état du cycle de vie cible d'une instance à partir des métadonnées de l'instance.	24 mars 2022
AMIheure du dernier lancement	`lastLaunchedTime` Indique la date à laquelle vous AMI avez été utilisé pour la dernière fois pour lancer une instance.	28 février 2022
ED25519clés	ED25519les clés sont désormais prises en charge pour EC2 Instance Connect et EC2 Serial Console.	20 janvier 2022
RHELPlateformes supplémen taires pour les réservations de capacité	Plateformes Red Hat Enterpris e Linux supplémentaires pour les réserves de capacité à la demande.	11 janvier 2022

Configuration de Windows AMIs pour un lancement plus rapide	Configurez Windows AMIs pour lancer des instances jusqu'à 65 % plus rapidement, à l'aide de snapshots préprovisionnés.	10 janvier 2022
Identifications d'instance dans les métadonnées d'instance	Vous pouvez accéder aux identifications d'une instance à partir des métadonnées de l'instance.	6 janvier 2022
Réserves de capacité dans des groupes de placement de cluster	Vous pouvez créer des réserves de capacité dans des groupes de placement de cluster.	6 janvier 2022
Parc d'instances Spot launch-before-terminate	Un parc d'instances Spot peut mettre fin aux instances Spot qui reçoivent une notification de rééquilibrage après le lancement de nouvelles instances Spot de remplacement.	4 novembre 2021
EC2Flotte launch-before-terminate	EC2Fleet peut résilier les instances Spot qui reçoivent une notification de rééquilibrage après le lancement de nouvelles instances Spot de remplacement.	4 novembre 2021
Comparer les horodatages	Vous pouvez déterminer l'heure réelle d'un événement en comparant l'horodatage de votre instance Amazon EC2 Linux avec. ClockBound	2 novembre 2021

Partagez AMIs avec des organisations et OUs	Vous pouvez désormais partager AMIs avec les AWS ressources suivantes : organisations et unités organisationnelles (OUs).	29 octobre 2021
Score de placement Spot	Obtenez une recommand ation pour une AWS région ou une zone de disponibilité en fonction de vos besoins en matière de capacité Spot.	27 octobre 2021
Sélection de type d'instance basée sur des attributs pour un parc d'instances Spot	Spécifiez les attributs qu'une instance doit posséder, et Amazon EC2 identifiera tous les types d'instances dotés de ces attributs.	27 octobre 2021
Sélection du type d'instance basée sur les attributs pour Fleet EC2	Spécifiez les attributs qu'une instance doit posséder, et Amazon EC2 identifiera tous les types d'instances dotés de ces attributs.	27 octobre 2021
Flotte de réservation de capacité à la demande	Vous pouvez utiliser une flotte de réservations de capacité pour lancer un groupe, ou une flotte, de réservations de capacité.	5 octobre 2021
Support d'hibernation pour Ubuntu 20.04 - Focal LTS	Mettez en veille prolongée vos instances récemment lancées depuis Ubuntu 20.04 - Focal. LTS AMI	4 octobre 2021

EC2Réservations de capacité de flotte et ciblées à la demande	EC2Fleet peut lancer des instances à la demande dans le cadre `targeted` de réservations de capacité.	22 septembre 2021
instances T3 sur les hôtes dédiés	Support pour les instances T3 sur Amazon EC2 Dedicated Host.	14 septembre 2021
Support d'hibernation pour RHEL Fedora et CentOS	Mettez en veille prolongée vos instances récemment lancées depuis Fedora et RHEL CentOS. AMIs	9 septembre 2021
Vue EC2 globale d'Amazon	Amazon EC2 Global View vous permet de visualiser les sous-réseauxVPCs, les instances, les groupes de sécurité et les volumes dans plusieurs AWS régions dans une seule console.	1er septembre 2021
AMIsupport de dépréciation pour Amazon Data Lifecycle Manager	Les AMI politiques EBS soutenues par Amazon Data Lifecycle Manager peuvent être AMIs déconseillées. La politique AWSDataLi fecycleManagerServiceRoleFo rAMIManagement AWS gérée a été mise à jour pour prendre en charge cette fonctionnalité.	23 août 2021
Prise en charge de la mise en veille prolongée pour C5d, M5d et R5d	Vous pouvez mettre en veille prolongée les instances nouvellement lancées et qui s'exécutent sur les types d'instances C5d, M5d et R5d.	19 août 2021

Paires EC2 de clés Amazon	Amazon prend EC2 désormais en charge ED25519 les clés sur les instances Linux et Mac.	17 août 2021
Préfixes pour les interfaces réseau	Vous pouvez attribuer une valeur privée IPv4 ou une IPv6 CIDR plage, automatiq uement ou manuellement, à vos interfaces réseau.	22 juillet 2021
Fenêtres d'événements	Vous pouvez définir des fenêtres d'événements hebdomadaires récurrent es personnalisées pour les événements planifiés qui redémarrent, arrêtent ou mettent fin à vos instances AmazonEC2.	15 juillet 2021
Support des ressources IDs et du balisage pour les règles des groupes de sécurité	Vous pouvez faire référence aux règles des groupes de sécurité par ID de ressource . Vous pouvez également ajouter des étiquettes aux règles de vos groupes de sécurité.	7 juillet 2021
Déprécier un AMI	Vous pouvez désormais spécifier quand un AMI est obsolète.	11 juin 2021
Facturation à la seconde Windows	Amazon EC2 facture l'utilisa tion SQL basée sur Windows et sur un serveur à la seconde, avec un minimum d'une minute.	10 juin 2021

Réservations de capacité sur AWS Outposts	Vous pouvez désormais utiliser les réservations de capacité sur AWS Outposts.	24 mai 2021
Partage d'une Réservation de capacité	Les réservations de capacité créés dans Local Zones et zones Wavelength peuvent maintenant être partagées.	24 mai 2021
Remplacement du volume racine	Vous pouvez désormais utiliser les tâches de remplacement du volume racine pour remplacer le EBS volume racine pour les instances en cours d'exécuti on.	22 avril 2021
Stockage et restauration à l'AMIaide de S3	Stockez les EBS fichiers sauvegardés AMIs dans S3 et restaurez-les à partir de S3 pour permettre la copie entre partitions de. AMIs	6 avril 2021
EC2Console série	Résolvez les problèmes de démarrage et de connectiv ité réseau en établissant une connexion au port série d'une instance.	30 mars 2021
Modes de démarrage	Amazon prend EC2 désormais en charge le UEFI démarrage sur des EC2 instances sélectionnées AMD et basées sur Intel.	22 mars 2021

Création d'un DNS enregistrement inversé	Vous pouvez désormais configurer la DNS recherche inversée pour vos adresses IP Elastic.	3 février 2021
Tag AMIs et instantanés lors de la création AMI	Lorsque vous créez unAMI, vous pouvez étiqueter AMI les instantanés avec les mêmes balises, ou vous pouvez les étiqueter avec des balises différentes.	4 décembre 2020
Utilisez Amazon EventBridge pour surveiller les événements de Spot Fleet	Créez des EventBridge règles qui déclenchent des actions programmatiques en réponse aux changements d'état et aux erreurs de Spot Fleet.	20 novembre 2020
Utilisez Amazon EventBridge pour surveiller les événements EC2 de la flotte	Créez des EventBridge règles qui déclenchent des actions programmatiques en réponse aux changements et aux erreurs de l'état de la EC2 flotte.	20 novembre 2020
Supprimer instant les flottes	Supprimez un type de EC2 flotte `instant` et mettez fin à toutes les instances de la flotte en un seul API appel.	18 novembre 2020
Prise en charge de la mise en veille prolongée pour T3 et T3a	Mettez en veille prolongée les instances que vous venez de lancer et qui s'exécutent sur les types d'instance T3 et T3a.	17 novembre 2020

Amazon EFS Quick Create	Vous pouvez créer et monter un système de EFS fichiers Amazon sur une instance au lancement à l'aide d'Amazon EFS Quick Create.	9 novembre 2020
Catégorie de métadonnées d'instance : events/recommendations/rebalance	Heure approximative, enUTC, à laquelle la notification de recommandation de rééquilibrage d'EC2instance est émise pour l'instance.	4 novembre 2020
EC2recommandation de rééquilibrage des instances	Signal qui vous avertit en cas de risque élevé d'interruption d'instance Spot.	4 novembre 2020
Réservations de capacité dans les zones Wavelength	Les réservations de capacité peuvent maintenant être créées et utilisées dans les zones Wavelength.	4 novembre 2020
Rééquilibrage de la capacité	Configurez Spot EC2 Fleet ou Fleet pour lancer une instance Spot de remplacement lorsqu'Amazon EC2 émet une recommandation de rééquilibrage.	4 novembre 2020
Prise en charge de la mise en veille prolongée pour les types d'instance I3, M5ad et R5ad	Mettez en veille prolongée les instances que vous venez de lancer et qui s'exécutent sur les types d'instances I3, M5ad et R5ad.	21 octobre 2020

CPULimites de l'instance Spot v	Les limites d'instances Spot sont désormais gérées en fonction du nombre d'instances Spot vCPUs que vos instances Spot en cours d'exécution utilisent ou utiliseront en attendant le traitement des demandes ouvertes.	1er octobre 2020
Réservations de capacité dans Local Zones	Réservations de capacité peut maintenant être créé et utilisé dans Local Zones.	30 septembre 2020
Prise en charge de la mise en veille prolongée pour M5a et R5a	Désormais, vous pouvez mettre en veille prolongée les instances que vous venez de lancer et qui s'exécutent sur les types d'instances M5a et 5Ra.	28 août 2020
Les métadonnées d'instance fournissent des informations sur l'emplacement et le placement	Nouveaux champs de métadonnées d'instance dans la catégorie `placement` : région, nom du groupe de placement, numéro de partition, ID d'hôte et ID de zone de disponibilité.	24 août 2020
Groupes de réserve de capacité	Vous pouvez utiliser AWS Resource Groups pour créer des collections logiques de réservations de capacité, puis lancer des instances cibles dans ces groupes.	29 juillet 2020

EC2Launchv2	Vous pouvez utiliser la EC2Launch version 2 pour effectuer des tâches lors du démarrage de l'instance, si une instance est arrêtée puis redémarrée, si une instance est redémarrée, et à la demande. EC2LaunchLa v2 prend en charge toutes les versions de Windows Server et remplace EC2Launch etEC2Config.	30 juin 2020
Apportez vos propres IPv6 adresses	Vous pouvez transférer une partie ou la totalité de votre plage d'IPv6adresses de votre réseau local vers votre AWS compte.	21 mai 2020
Lancement des instances à l'aide d'un paramètre Systems Manager	Vous pouvez spécifier un AWS Systems Manager paramètre au lieu d'un AMI lorsque vous lancez une instance.	5 mai 2020
Personnaliser les notifications d'événements planifiés	Vous pouvez personnaliser les notifications d'événeme nts planifiés pour inclure des balises dans la notification par e-mail.	4 mai 2020

Amazon Linux 2 Kernel Live Patching	Kernel Live Patching pour Amazon Linux 2 vous permet d'appliquer des correctifs de vulnérabilité de sécurité et de bogues critiques à un noyau Linux en cours d'exécution, sans redémarrer ni interrompre les applications en cours d'exécution.	28 avril 2020
Windows Server sur les hôtes dédiés	Vous pouvez utiliser Windows Server AMIs fourni par Amazon pour exécuter les dernières versions de Windows Server sur des hôtes dédiés.	7 avril 2020
Arrêter et démarrer une instance Spot	Arrêtez vos instances Spot soutenues par Amazon EBS et démarrez-les comme bon vous semble, au lieu de vous fier au comportement d'arrêt des interruptions.	13 janvier 2020

Étiquette des ressources	Vous pouvez baliser les passerelles Internet de sortie uniquement, les passerelles locales, les tables de routage de passerelles locales, les interfaces virtuelles de passerelle locale, les groupes d'interfaces virtuelles de passerelle locale, les associations de tables de routage de passerelles locales et les VPC associations de groupes d'interfaces virtuelles de tables de routage de passerelles locales.	10 janvier 2020
Connexion à votre instance à l'aide du Gestionnaire de session	Vous pouvez démarrer une session de gestionnaire de session avec une instance depuis la EC2 console Amazon.	18 décembre 2019
Hôtes dédiés et groupes de ressources hôte	Les Hôtes dédiés peuvent désormais être utilisés avec des groupes de ressources hôte.	2 décembre 2019
Partage d'hôte dédié	Vous pouvez désormais partager vos hôtes dédiés entre plusieurs AWS comptes.	2 décembre 2019
Spécification de crédits par défaut au niveau du compte	Vous pouvez définir la spécification de crédit par défaut par famille d'instances de performance burstable au niveau du compte par AWS région.	25 novembre 2019

Découverte du type d'instance	Vous pouvez identifier un type d'instance qui répond à vos besoins.	22 novembre 2019
Hôtes dédiés	Vous pouvez désormais configurer un Hôte dédié pour prendre en charge plusieurs types d'instances au sein d'une famille d'instances.	21 novembre 2019
Instance Metadata Service Version 2	Vous pouvez utiliser Service des métadonnées d'instanc e Version 2, qui est une méthode orientée session de demande de métadonnées d'instance.	19 novembre 2019
Elastic Fabric Adapter (EFA)	Les adaptateurs Elastic Fabric peuvent désormais être utilisés avec Intel MPI 2019 Update 6.	15 novembre 2019
Prise en charge de la mise en veille pour les instances Windows à la demande	Vous pouvez mettre en veille les instances Windows à la demande	14 octobre 2019
Achats d'instances réservées mis en file d'attente	Vous pouvez mettre l'achat d'une Instance réservée en file d'attente jusqu'à trois ans en avance.	4 octobre 2019
Interruption de diagnostic	Vous pouvez envoyer une interruption de diagnostic à une instance inaccessible ou qui ne répond pas afin de déclencher une panique de noyau.	14 août 2019

Stratégie d'allocation optimisée pour la capacité	À l'aide de EC2 Fleet ou de Spot Fleet, vous pouvez lancer des instances Spot à partir de pools Spot dont la capacité est optimale compte tenu du nombre d'instances lancées.	12 août 2019
Partage de réserve de capacité à la demande	Vous pouvez désormais partager vos réservations de capacité entre différents AWS comptes.	29 juillet 2019
Elastic Fabric Adapter (EFA)	EFAprend désormais en charge Open MPI 3.1.4 et Intel MPI 2019 Update 4.	26 juillet 2019
EC2Instance Connect	EC2Instance Connect est un moyen simple et sécurisé de se connecter à vos instances à l'aide de Secure Shell (SSH).	27 juin 2019
Resturation de l'hôte	Redémarre automatiquement vos instances sur un nouvel hôte en cas de panne matériell e soudaine sur un Hôte dédié.	5 juin 2019
VSSinstantanés cohérents avec les applications	Prenez des instantanés cohérents avec les applicati ons de tous les EBS volumes Amazon attachés à vos instances Windows à l'aide AWS Systems Manager de Run Command.	13 mai 2019

Assistant de replateforme Windows vers Linux pour les bases de données Microsoft Server SQL	Déplacez les charges de travail Microsoft SQL Server existantes d'un système d'exploitation Windows vers un système d'exploitation Linux. Le lien mis à jour pointe vers le guide de l'EC2utilisateur de Microsoft SQL Server on Amazon.	8 mai 2019
Mise à niveau automatisée de Windows	Effectuez des mises à niveau automatisées des instances EC2 Windows à l'aide de AWS Systems Manager.	6 mai 2019
Elastic Fabric Adapter (EFA)	Vous pouvez associer un adaptateur Elastic Fabric à vos instances pour accélérer les applications de calcul haute performance (HPC).	29 avril 2019

Pour plus d'informations sur les versions des types d'instance pour AmazonEC2, consultez l'historique des documents dans le guide des types d'EC2instances Amazon.

Historique pour 2018 et les années antérieures

Le tableau suivant décrit les ajouts importants apportés au guide de EC2 l'utilisateur Amazon en 2018 et dans les années antérieures.

Fonctionnalité	APIversion	Description	Date de publication
Groupes de placement par partition	2016-11-15	Les groupes de placement par partition répartissent les instances entre les partitions logiques, en s'assurant que les instances d'une	20 décembre 201

Fonctionnalité	APIversion	Description	Date de publication
		partition ne partagent pas le matériel sous-jacent avec les instances d'autres partitions. Pour plus d'informations, consultez Groupes de placement par partition.	
Instances Linux Hibernate EC2	2016-11-15	Vous pouvez mettre en veille une instance Linux si cette dernière a été activée pour la mise en veille et répond aux exigences de la mise en veille. Pour plus d'informations, consultez Hibernez votre instance Amazon EC2.	28 novembre 2018
Accélérateurs Amazon Elastic Inference	2016-11-15	Vous pouvez associer un accélérateur Amazon EI à vos instances pour ajouter une accélération GPU optimisée afin de réduire le coût d'exécution de l'inférence basée sur le deep learning.	28 novembre 2018
Parc d'instances recommandé par la console Spot	2016-11-15	La console Spot recommande un parc d'instances basé sur les meilleures pratiques Spot (diversification des instances) afin de répondre aux spécifications matérielles minimales (vCPUsmémoire et stockage) adaptées aux besoins de votre application. Pour de plus amples informations, veuillez consulter Créer une flotte Spot.	20 novembre 2018

Fonctionnalité	APIversion	Description	Date de publication
Nouveau type EC2 de demande de flotte : instant	2016-11-15	EC2Fleet prend désormais en charge un nouveau type de demande`instant`, que vous pouvez utiliser pour allouer de la capacité de manière synchrone entre les types d'instances et les modèles d'achat. La `instant` demande renvoie les instances lancées dans la API réponse et ne prend aucune autre mesure, ce qui vous permet de contrôler si et quand les instances sont lancées. Pour de plus amples informations, veuillez consulter EC2Types de demandes relatives aux flottes et aux flottes ponctuelles.	14 novembre 2018
Informations d'économies Spot	2016-11-15	Vous pouvez afficher les économies réalisées grâce à l'utilisation d'instances Spot pour un seul parc d'instances Spot ou pour toutes les instances Spot. Pour plus d'informations, consultez Économies réalisées grâce à l'achat d'instances Spot.	5 novembre 2018
Support de console pour l'optimisation des CPU options	2016-11-15	Lorsque vous lancez une instance, vous pouvez optimiser les CPU options en fonction de charges de travail ou de besoins commerciaux spécifiques à l'aide de la EC2 console Amazon. Pour de plus amples informations, veuillez consulter CPUoptions pour les EC2 instances Amazon.	31 octobre 2018

Fonctionnalité	APIversion	Description	Date de publication
Prise en charge de la console pour la création d'un modèle de lancement à partir d'une instance	2016-11-15	Vous pouvez créer un modèle de lancement en utilisant une instance comme base pour un nouveau modèle de lancement à l'aide de la EC2 console Amazon. Pour de plus amples informations, veuillez consulter Création d'un modèle de EC2 lancement Amazon.	30 octobre 2018
On-Demand Capacity Reservations	2016-11-15	Vous pouvez réserver de la capacité pour vos EC2 instances Amazon dans une zone de disponibilité spécifique pour n'importe quelle durée. Cela vous permet de créer et de gérer des réservations de capacité indépendamment des remises de facturation offertes par les instances réservées (IR). Pour plus d'informations, consultez Réservez de la capacité de calcul grâce aux réservations de capacité à la demande.	25 octobre 2018
Apportez vos propres adresses IP (BYOIP)	2016-11-15	Vous pouvez transférer une partie ou la totalité de votre plage d'IPv4adresses publiques de votre réseau local vers votre AWS compte. Une fois que vous avez transféré la plage d'adresses AWS, elle apparaît dans votre compte sous forme de pool d'adresses. Vous pouvez créer une adresse IP Elastic à partir de votre groupe d'adresses et l'utiliser avec vos ressources AWS . Pour plus d'informations, consultez Apportez vos propres adresses IP (BYOIP) à Amazon EC2.	23 octobre 2018

Fonctionnalité	APIversion	Description	Date de publication
Balisage de Hôte dédié à la création et prise en charge de la console	2016-11-15	Vous pouvez étiqueter vos hôtes dédiés lors de leur création, et vous pouvez gérer vos tags d'hôtes dédiés à l'aide de la EC2 console Amazon. Pour de plus amples informations, veuillez consulter Attribuez un hôte EC2 dédié Amazon à utiliser sur votre compte.	08 octobre 2018
Prise en charge par la console de la mise à l'échelle planifiée pour le parc d'instances Spot	2016-11-15	Augmente ou réduit la capacité actuelle du flotte en fonction de la date et de l'heure. Pour plus d'informations, consultez Mise à l'échelle planifiée : adaptez votre flotte Spot selon un calendrier.	20 septembre 201
Stratégies d'allocation pour les EC2 flottes	2016-11-15	Vous pouvez spécifier si l'affectation de capacité à la demande est traitée par prix (prix le plus bas en premier) ou par priorité (priorité la plus élevée en premier). Vous pouvez spécifier le nombre de groupes d'instances Spot auxquels allouer votre capacité Spot cible. Pour plus d'informations, consultez Utilisez des stratégies d'allocation pour déterminer comment EC2 Fleet ou Spot Fleet exploite les capacités sur place et à la demande.	26 juillet 2018

Fonctionnalité	APIversion	Description	Date de publication
Stratégies d'allocation pour les Parcs d'instances Spot	2016-11-15	Vous pouvez spécifier si l'affectation de capacité à la demande est traitée par prix (prix le plus bas en premier) ou par priorité (priorité la plus élevée en premier). Vous pouvez spécifier le nombre de groupes d'instances Spot auxquels allouer votre capacité Spot cible. Pour plus d'informations, consultez Utilisez des stratégies d'allocation pour déterminer comment EC2 Fleet ou Spot Fleet exploite les capacités sur place et à la demande.	26 juillet 2018
Automatisation du cycle de vie des instantanés	2016-11-15	Vous pouvez utiliser Amazon Data Lifecycle Manager pour automatiser la création et la suppression de snapshots pour vos EBS volumes. Pour plus d'informations, consultez Amazon Data Lifecycle Manager.	12 juillet 2018
CPUOptions du modèle de lancement	2016-11-15	Lorsque vous créez un modèle de lancement à l'aide des outils de ligne de commande, vous pouvez optimiser les CPU options en fonction de charges de travail ou de besoins commerciaux spécifiques. Pour de plus amples informations, veuillez consulter Création d'un modèle de EC2 lancement Amazon.	11 juillet 2018
Balisage des Hôtes dédiés	2016-11-15	Vous pouvez baliser vos Hôtes dédiés.	3 juillet 2018
Obtenir la dernière sortie de console	2016-11-15	Vous pouvez récupérer la dernière sortie de console pour certains types d'instances lorsque vous utilisez la get-console-output AWS CLI commande.	9 mai 2018

Fonctionnalité	APIversion	Description	Date de publication
Optimisez CPU les options	2016-11-15	Lorsque vous lancez une instance, vous pouvez optimiser les CPU options pour les adapter à des charges de travail ou à des besoins commerciaux spécifiques. Pour de plus amples informations, veuillez consulter CPUoptions pour les EC2 instances Amazon.	8 mai 2018
EC2Flotte	2016-11-15	Vous pouvez utiliser EC2 Fleet pour lancer un groupe d'instances dans différents EC2 types d'instances et zones de disponibilité, ainsi que dans le cadre de modèles d'achat d'instances à la demande, d'instances réservées et d'instances ponctuelles. Pour de plus amples informations, veuillez consulter EC2Fleet et Spot Fleet.	2 mai 2018
instances à la demande dans des Parcs d'instances Spot	2016-11-15	Vous pouvez inclure une demande de capacité à la demande dans votre demande de parc d'instances Spot pour garantir que vous avez toujours la capacité d'instance. Pour de plus amples informations, veuillez consulter EC2Fleet et Spot Fleet.	2 mai 2018
Marquer les EBS instantanés lors de leur création	2016-11-15	Vous pouvez appliquer des balises aux instantanés au moment de la création.	2 avril 2018
Modifier les groupes de placement	2016-11-15	Vous pouvez déplacer une instance à l'intérieur ou à l'extérieur d'un groupe de placement, ou modifier son groupe de placement. Pour plus d'informations, consultez Modifier l'emplacement d'une EC2 instance.	1 mars 2018
Ressource plus longue IDs	2016-11-15	Vous pouvez activer le format d'ID long pour d'autres types de ressource.	9 février 2018

Fonctionnalité	APIversion	Description	Date de publication
Améliorations des performances réseau	2016-11-15	Les instances qui se trouvent en dehors d'un groupe de placement de cluster peuvent à présent profiter d'une bande passante plus élevée pour l'envoi ou la réception de trafic réseau entre d'autres instances ou Amazon S3.	24 janvier 2018
Balisage de vos adresses IP Elastic	2016-11-15	Vous pouvez baliser vos adresses IP Elastic.	21 décembre 2017
Amazon Time Sync Service	2016-11-15	Amazon Time Sync Service permet de garder une heure précise sur votre instance. Pour de plus amples informations, veuillez consulter Synchronisation précise de l'heure et de l'heure sur votre EC2 instance.	29 novembre 2017
T2 illimité	2016-11-15	Les instances T2 illimité peuvent dépasser le niveau de base aussi longtemps que nécessaire. Pour plus d'informations, consultez Instances de performance à capacité extensible.	29 novembre 2017
Modèles de lancement	2016-11-15	Un modèle de lancement peut contenir tout ou partie des paramètres permettant de lancer une instance. Il est donc inutile de les spécifier à chaque lancement d'une instance. Pour plus d'informations, consultez Stockez les paramètres de lancement de l'instance dans les modèles de EC2 lancement Amazon.	29 novembre 2017
Placement par répartition	2016-11-15	Les groupes de placement par répartition sont recommandés pour les applications ayant un petit nombre d'instances critiques, qui doivent être séparées les unes des autres. Pour plus d'informations, consultez Groupes de placement étendu.	29 novembre 2017

Fonctionnalité	APIversion	Description	Date de publication
Mise en veille prolongée d'instances Spot	2016-11-15	Le service d'instances Spot peut mettre les instances Spot en veille prolongée en cas d'interruption. Pour plus d'informations, consultez Mettre les instances Spot interrompues en veille prolongée.	28 novembre 2017
Suivi de cible du parc d'instances Spot	2016-11-15	Vous pouvez configurer des politiques de suivi des objectifs et d'échelonnement pour votre parc d'instances Spot Pour plus d'informations, consultez Mise à l'échelle du suivi des cibles : dimensionnez le parc de spots en ciblant une valeur pour une métrique spécifique.	17 novembre 2017
Le parc d'instances Spot s'intègre avec Elastic Load Balancing	2016-11-15	Vous pouvez attacher un ou plusieurs équilibreurs de charge à un parc d'instances Spot .	10 novembre 2017
Fusionner et diviser des instances réservées convertibles	2016-11-15	Vous pouvez échanger (ou fusionner) deux instances réservées convertibles ou plus pour obtenir une nouvelle Instance réservée convertible. Vous pouvez également utiliser le processus de modification pour diviser une Instance réservée convertible en plus petites réservations. Pour plus d'informations, consultez Échanger des instances réservées convertibles.	6 novembre 2017
Modifier le VPC bail	2016-11-15	Vous pouvez modifier l'attribut de location d'instance d'un format VPC de `dedicated` à`default`. Pour de plus amples informations, veuillez consulter Modifier la location d'instance d'un VPC.	16 octobre 2017

Fonctionnalité	APIversion	Description	Date de publication
Facturation par seconde	2016-11-15	Amazon EC2 facture l'utilisation basée sur Linux à la seconde, avec un minimum d'une minute.	2 octobre 2017
Arrêt sur une interruption	2016-11-15	Vous pouvez spécifier si Amazon EC2 doit arrêter ou résilier les instances Spot lorsqu'elles sont interrompues. Pour de plus amples informations, veuillez consulter Comportement des interruptions des instances Spot.	18 septembre 201
NATPasserelles de balises	2016-11-15	Vous pouvez étiqueter votre NAT passerelle. Pour de plus amples informations, veuillez consulter Etiqueter vos ressources .	7 septembre 2017
Descriptions des règles des groupes de sécurité	2016-11-15	Vous pouvez ajouter des descriptions aux règles des groupes de sécurité.	31 août 2017
Elastic Graphics	2016-11-15	Attachez des accélérateurs Elastic Graphics à vos instances pour accélérer les performances graphiques de vos applications.	29 août 2017
Récupération d'adresses IP Elastic	2016-11-15	Si vous publiez une adresse IP élastique pour une utilisation dans unVPC, vous pourrez peut-être la récupérer.	11 août 2017
Identifier les instances du parc d'instances Spot	2016-11-15	Vous pouvez configurer votre parc d'instances Spot pour identifier automatiquement les instances qu'il lance.	24 juillet 2017

Fonctionnalité	APIversion	Description	Date de publication
Baliser des ressources pendant la création	2016-11-15	Vous pouvez appliquer des balises à des instances et des volumes au moment de la création. Pour plus d'informations, consultez Etiqueter vos ressources . De plus, vous pouvez utiliser des autorisations de niveau ressources basées sur des balises pour contrôler les balises appliquées. Pour plus d'informations, consultez Accorder l'autorisation de baliser les EC2 ressources Amazon lors de la création.	28 mars 2017
Effectuer des modifications sur les EBS volumes attachés	2016-11-15	La plupart des EBS volumes étant attachés à la plupart des EC2 instances, vous pouvez modifier la taille et le type du volume, IOPS sans détacher le volume ni arrêter l'instance.	13 février 2017
Attachement d'un rôle IAM	2016-11-15	Vous pouvez attacher, détacher ou remplacer un IAM rôle pour une instance existante. Pour de plus amples informations, veuillez consulter IAMrôles pour Amazon EC2.	9 février 2017
instances Spot dédiées	2016-11-15	Vous pouvez exécuter des instances Spot sur du matériel à locataire unique dans un cloud privé virtuel (VPC). Pour de plus amples informations, veuillez consulter Lancement sur du matériel à locataire unique.	19 janvier 2017
IPv6soutien	2016-11-15	Vous pouvez IPv6 CIDR associer un à vos sous-réseaux VPC et et attribuer des IPv6 adresses aux instances de votreVPC. Pour de plus amples informations, veuillez consulter Adressage IP de l'EC2instance Amazon.	1er décembre 201

Fonctionnalité	APIversion	Description	Date de publication
Scalabilité automatique du parc d'instances Spot		Vous pouvez désormais configurer des politiques de mise à l'échelle pour votre parc d'instances Spot . Pour plus d'informations, consultez Découvrez le dimensionnement automatique pour Spot Fleet.	1 septembre 2016
Adaptateur réseau élastique (ENA)	01-04-2016	Vous pouvez désormais l'utiliser ENA pour améliorer la mise en réseau. Pour de plus amples informations, veuillez consulter Mise en réseau améliorée sur les EC2 instances Amazon.	28 juin 2016
Support amélioré pour une visualisation et une modification plus longues IDs	01-04-2016	Vous pouvez désormais afficher et modifier les paramètres d'identification plus longs pour IAM les autres utilisateurs, IAM les rôles ou l'utilisateur root.	23 juin 2016
Copiez des EBS instantanés Amazon cryptés entre les comptes AWS	01-04-2016	Vous pouvez désormais copier des EBS instantanés chiffrés entre AWS comptes.	21 juin 2016
Création d'une capture d'écran d'une console d'instance	01-10-2015	Vous pouvez désormais obtenir des informations supplémentaires lors du débogage d'instances inaccessibles. Pour de plus amples informations, veuillez consulter Création d'une capture d'écran d'une instance inaccessible.	24 mai 2016
Deux nouveaux types de EBS volumes	01-10-2015	Vous pouvez désormais créer des volumes optimisés pour le débit HDD (st1) et des volumes froids HDD (sc1).	19 avril 2016

Fonctionnalité	APIversion	Description	Date de publication
Ajout de nouveautés NetworkPacketsIn et de NetworkPacketsOut statistiques pour Amazon EC2		Ajout de nouvelles NetworkPacketsIn NetworkPacketsOut statistiques pour AmazonEC2. Pour de plus amples informations, veuillez consulter Métriques des instances.	23 mars 2016
CloudWatch métriques pour Spot Fleet		Vous pouvez désormais obtenir CloudWatch des statistiques pour votre parc de spots. Pour de plus amples informations, veuillez consulter Surveillez votre EC2 flotte ou repérez votre flotte en utilisant CloudWatch.	21 mars 2016
instances planifiées	01-10-2015	Les instances réservées planifiées (instances planifiées) vous permettent d'acheter des réservations de capacité récurrentes sur une base quotidienne, hebdomadaire ou mensuelle, avec une date de début et une durée spécifiées.	13 janvier 2016
Ressource plus longue IDs	01-10-2015	Nous introduisons progressivement des longueurs plus longues IDs pour certains types de EBS ressources Amazon EC2 et Amazon. Durant la période d'abonnement, vous pouvez activer le format d'ID plus long pour les types de ressources pris en charge.	13 janvier 2016
ClassicLink DNSsoutien	01-10-2015	Vous pouvez activer la prise en ClassicLink DNS charge de votre nom d'DNShôte VPC afin que les noms d'hôtes adressés entre les instances EC2 -Classic liées et les instances soient VPC résolus en adresses IP privées et non en adresses IP publiques.	11 janvier 2016

Fonctionnalité	APIversion	Description	Date de publication
Hôtes dédiés	01-10-2015	Un hôte Amazon EC2 Dedicated est un serveur physique dont la capacité d'instance est dédiée à votre usage. Pour de plus amples informations, veuillez consulter Hôtes EC2 dédiés Amazon.	23 novembre 2015
Durée d'instance Spot	01-10-2015	Vous pouvez désormais spécifier une durée pour vos instances Spot. Les blocs d'instances Spot ne sont pas pris en charge (janvier 2023).	6 octobre 2015
Demande de modification de parc d'instances Spot	01-10-2015	Vous pouvez désormais modifier la capacité cible de votre demande de parc d'instances Spot. Pour plus d'informations, consultez Modifier une demande de parc d'instances Spot.	29 septembre 201
Stratégie d'allocation diversifiée de parc d'instances Spot	15-04-2015	Vous pouvez désormais allouer des instances Spot dans plusieurs groupes d'instances Spot à l'aide d'une seule demande de parc d'instances Spot. Pour de plus amples informations, veuillez consulter Utilisez des stratégies d'allocation pour déterminer comment EC2 Fleet ou Spot Fleet exploite les capacités sur place et à la demande.	15 septembre 201

Fonctionnalité	APIversion	Description	Date de publication
Pondération d'instance de parc d'instances Spot	15-04-2015	Vous pouvez désormais définir les unités de capacité par lesquelles chaque type d'instance contribue aux performances de votre application et ajuster en conséquence le montant que vous êtes prêt à payer pour des instances Spot pour chaque pool d'instances Spot. Pour de plus amples informations, veuillez consulter Utilisez la pondération des instances pour gérer les coûts et les performances de votre EC2 flotte ou de votre flotte ponctuelle.	31 août 2015
Nouvelle action d'alarme de redémarrage et nouveau IAM rôle à utiliser avec les actions d'alarme		Ajout de l'action d'alarme de redémarrage et d'IAMun nouveau rôle à utiliser avec les actions d'alarme. Pour de plus amples informations, veuillez consulter Créer des alarmes qui arrêtent, finissent, redémarrent ou récupèrent une instance.	23 juillet 2015
Spot Fleets	15-04-2015	Vous pouvez gérer un ensemble, ou une flotte d'instances Spot au lieu de gérer des demandes d'instance Spot distinctes. Pour de plus amples informations, veuillez consulter EC2Fleet et Spot Fleet.	18 mai 2015
Migrer les adresses IP Elastic vers EC2 - Classic	15-04-2015	Vous pouvez migrer une adresse IP élastique que vous avez allouée pour être utilisée dans EC2 -Classic afin de l'utiliser dans un... VPC	15 mai 2015

Fonctionnalité	APIversion	Description	Date de publication
Importation VMs avec plusieurs disques en tant que AMIs	01-03-2015	Le processus VM Import prend désormais en charge l'importation VMs avec plusieurs disques en tant queAMIs. Pour plus d'informations, consultez Importation d'un ordinateur virtuel comme image à l'aide de VM Import/Export dans le VM Import/Export Guide de l'utilisateur.	23 avril 2015
Systems Manager		Systems Manager vous permet de configurer et de gérer vos EC2 instances.	17 février 2015
Systems Manager pour Microsoft SCVMM 1.5		Vous pouvez désormais utiliser Systems Manager for Microsoft SCVMM pour lancer une instance et importer une machine virtuelle depuis SCVMM AmazonEC2.	21 janvier 2015
Restauration automatique pour les EC2 instances		Vous pouvez créer une CloudWatch alarme Amazon qui surveille une EC2 instance Amazon et la récupère automatiquement si elle est endommagée en raison d'une défaillance matérielle sous-jacente ou d'un problème nécessitant une AWS intervention pour être réparée. Une instance récupérée est identique à l'instance d'origine, y compris son ID d'instance, les adresses IP privées et toutes les métadonnées d'instance. Pour plus d'informations, consultez Résilience des instances.	12 janvier 2015

Fonctionnalité	APIversion	Description	Date de publication
ClassicLink	01-10-2014	ClassicLink vous permet de lier votre instance EC2 -Classic à une instance VPC de votre compte. Vous pouvez associer des groupes VPC de sécurité à l'instance EC2 -Classic, permettant ainsi la communication entre votre instance EC2 -Classic et les instances de vos adresses IP privées VPC d'utilisation.	7 janvier 2015
Avis de résiliation d'instance Spot		Le meilleur moyen de vous protéger contre une interruption d'instance Spot est de faire en sorte que votre application soit tolérante aux pannes au niveau de son architecture. En outre, vous pouvez profiter des avis de résiliation d'une instance Spot, qui fournissent un avertissement de deux minutes avant qu'Amazon ne EC2 doive résilier votre instance Spot. Pour de plus amples informations, veuillez consulter Avis d'interruption d'instance Spot..	5 janvier 2015
Systems Manager pour Microsoft SCVMM		Systems Manager for Microsoft SCVMM fournit une easy-to-use interface simple pour gérer les AWS ressources, telles que EC2 les instances, de MicrosoftSCVMM.	29 octobre 2014
Prise en charge de la pagination `DescribeVolumes`	01-09-2014	L'`DescribeVolumes` APIappel prend désormais en charge la pagination des résultats avec les `NextToken` paramètres `MaxResults` et. Pour plus d'informations, consultez DescribeVolumesle manuel Amazon EC2 API Reference.	23 octobre 2014

Fonctionnalité	APIversion	Description	Date de publication
Ajout de la prise en charge d'Amazon CloudWatch Logs		Vous pouvez utiliser Amazon CloudWatch Logs pour surveiller, stocker et accéder à votre système, à votre application et aux fichiers journaux personnalisés à partir de vos instances ou d'autres sources. Vous pouvez ensuite récupérer les données de journal associées dans CloudWatch Logs à l'aide de la CloudWatch console Amazon, CloudWatch des commandes Logs du AWS CLI ou CloudWatch des LogsSDK.	10 juillet 2014
Nouvelle page sur les limites de EC2 service		Utilisez la page EC2Service Limits de la EC2 console Amazon pour consulter les limites actuelles des ressources fournies par Amazon EC2 et AmazonVPC, par région.	19 juin 2014
SSDVolumes à usage EBS général d'Amazon	01-05-2014	SSDLes volumes à usage général offrent un stockage rentable, idéal pour un large éventail de charges de travail. Ces volumes offrent des latences à un chiffre en millisecondes, la capacité d'atteindre 3 000 IOPS points pendant de longues périodes et une performance de base de 3 /Gib. IOPS SSDLes volumes à usage général peuvent avoir une taille comprise entre 1 GiB et 1 TiB.	16 juin 2014
AWS Pack de gestion		AWS Le pack d'administration est désormais compatible avec System Center Operations Manager 2012 R2.	22 mai 2014

Fonctionnalité	APIversion	Description	Date de publication
EBSChiffrement Amazon	01-05-2014	Amazon EBS Encryption permet un chiffrement fluide des volumes de EBS données et des instantanés, éliminant ainsi le besoin de créer et de maintenir une infrastructure de gestion des clés sécurisée. EBSle chiffrement assure la sécurité des données au repos en cryptant vos données à l'aide Clés gérées par AWS de. Le chiffrement est effectué sur les serveurs hébergeant les EC2 instances, ce qui permet de chiffrer les données lors de leur transfert entre les EC2 instances et le EBS stockage.	21 mai 2014
Rapports EC2 d'utilisation d'Amazon		Les rapports EC2 d'utilisation Amazon sont un ensemble de rapports qui présentent les données de coût et d'utilisation relatives à votre utilisation deEC2.	28 janvier 2014
Importation de machines virtuelles Linux	15-10-2013	Le processus VM Import prend désormais en charge l'importation d'instances Linux. Pour plus d'informations, consultez le VM Import/Export Guide de l'utilisateur.	16 décembre 2013
Autorisations au niveau des ressources pour RunInstances	15-10-2013	Vous pouvez désormais créer des politiques AWS Identity and Access Management pour contrôler les autorisations au niveau des ressources pour l'action Amazon EC2 RunInstances API. Pour plus d'informations et obtenir des exemples de stratégie, consultez Gestion des identités et des accès pour Amazon EC2.	20 novembre 2013

Fonctionnalité	APIversion	Description	Date de publication
Lancement d'une instance à partir du AWS Marketplace		Vous pouvez désormais lancer une instance à l' AWS Marketplace aide de l'assistant de EC2 lancement Amazon. Pour de plus amples informations, veuillez consulter Lancez une EC2 instance Amazon à partir d'un AWS Marketplace AMI.	11 novembre 2013
Nouvel Assistant de lancement		Il existe un nouvel assistant de EC2 lancement repensé. Pour de plus amples informations, veuillez consulter Lancer une EC2 instance à l'aide de l'assistant de lancement d'instance de la console.	10 octobre 2013
Modification des types d'instances réservées	01-10-2013	Vous pouvez désormais modifier le type d'instances des instances réservées Linux d'une même famille (par exemple, M1, M2, M3, C1). Pour plus d'informations, consultez Modifier instances réservées.	09 octobre 2013
Modifier les instances EC2 réservées Amazon	15-08-2013	Vous pouvez désormais modifier les instances réservées d'une région. Pour de plus amples informations, veuillez consulter Modifier instances réservées.	11 septembre 201
Attribution d'une adresse IP publique	15-07-2013	Vous pouvez désormais attribuer une adresse IP publique lorsque vous lancez une instance dans unVPC. Pour de plus amples informations, veuillez consulter Attribuer une IPv4 adresse publique lors du lancement de l'instance.	20 août 2013

Fonctionnalité	APIversion	Description	Date de publication
Attribution d'autorisations au niveau des ressources	15-06-2013	Amazon EC2 prend en charge les nouveaux Amazon Resource Names (ARNs) et les nouvelles clés de condition. Pour de plus amples informations, veuillez consulter Politiques basées sur l'identité pour Amazon EC2.	8 juillet 2013
Copies d'instantané incrémentielles	01-02-2013	Vous pouvez désormais effectuer des copies d'instantané incrémentielles.	11 juin 2013
AWS Pack de gestion		Le pack d' AWS administration relie EC2 les instances Amazon aux systèmes d'exploitation Windows ou Linux qui y sont exécutés. Le pack d' AWS administration est une extension de Microsoft System Center Operations Manager.	8 mai 2013
Nouvelle page Balises		Il existe une nouvelle page de tags dans la EC2 console Amazon. Pour de plus amples informations, veuillez consulter Marquez vos EC2 ressources Amazon.	04 avril 2013
Copier et AMI d'une région à l'autre	01-02-2013	Vous pouvez copier un fichier AMI d'une région à l'autre, ce qui vous permet de lancer des instances cohérentes dans plusieurs AWS régions rapidement et facilement. Pour de plus amples informations, veuillez consulter Copier un Amazon EC2 AMI.	11 mars 2013

Fonctionnalité	APIversion	Description	Date de publication
Lancer des instances dans une instance par défaut VPC	01-02-2013	Votre AWS compte est capable de lancer des instances dans EC2 -Classic ou aVPC, ou uniquement dans aVPC, sur une region-by -region base. Si vous ne pouvez lancer des instances que dans unVPC, nous créons une instance par défaut VPC pour vous. Lorsque vous lancez une instance, nous la lançons dans votre instance par défautVPC, sauf si vous créez une instance autre que celle par défaut VPC et que vous la spécifiez lorsque vous lancez l'instance.	11 mars 2013
EBScopie instantanée	01-12-2012	Vous pouvez utiliser des copies instantanées pour créer des sauvegardes de données, pour créer de nouveaux EBS volumes Amazon ou pour créer des Amazon Machine Images (AMIs).	17 décembre 2012
EBSMesures et contrôles de statut mis à jour pour les volumes provisionnés IOPS SSD	01-10-2012	Les EBS métriques ont été mises à jour pour inclure deux nouvelles métriques pour les IOPS SSD volumes provisionnés. De nouvelles vérifications de statut ont également été ajoutées pour les IOPS SSD volumes provisionnés.	20 novembre 2012
État de demande d'instance Spot	01-10-2012	L'état de demande d'instance Spot simplifie la détermination de l'état de vos demandes Spot.	14 octobre 2012

Fonctionnalité	APIversion	Description	Date de publication
Amazon EC2 Reserved Instances Marketplace	15-08-2012	La Reserved Instance Marketplace met en relation les vendeurs qui possèdent des instances EC2 réservées Amazon dont ils n'ont plus besoin avec des acheteurs qui cherchent à acheter de la capacité supplémentaire. Les instances réservées achetées et vendues via le Marketplace d'instance réservée fonctionnent comme toute autre instance réservée, si ce n'est qu'il peut ne leur rester qu'une durée standard complète et qu'elles peuvent être vendues à différents prix.	11 septembre 201
Provisionné IOPS SSD pour Amazon EBS	20-07-2012	IOPSSSDLes volumes provisionnés offrent des performances élevées et prévisibles pour les charges de travail intensives en E/S, telles que les applications de base de données, qui reposent sur des temps de réponse constants et rapides.	31 juillet 2012
IAMrôles sur les EC2 instances Amazon	01-06-2012	IAMles rôles pour Amazon EC2 fournissent : • AWS clés d'accès pour les applications exécutées sur EC2 des instances Amazon. • Rotation automatique des clés AWS d'accès sur l'EC2instance Amazon. • Autorisations granulaires pour les applications exécutées sur des EC2 instances Amazon qui adressent des demandes à vos AWS services.	11 juin 2012

Fonctionnalité	APIversion	Description	Date de publication
Fonctions d'instance Spot qui facilitent le démarrage et la gestion d'une interruption potentielle.		Vous pouvez désormais gérer vos instances Spot comme suit : • Spécifiez le montant que vous êtes prêt à payer pour des instances Spot à l'aide de configurations de lancement Auto Scaling et configurez un calendrier pour indiquer ce montant pour des instances Spot. Pour plus d'informations, consultez Launching Spot Instances in Your Auto Scaling Group dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling. • Obtenez des notifications quand les instances sont lancées ou terminées. • Utilisez AWS CloudFormation des modèles pour lancer des instances Spot dans une pile contenant AWS des ressources.	7 juin 2012
EC2exportation d'instances et horodatage pour les vérifications de statut pour Amazon EC2	01-05-2012	Ajout de la prise en charge de l'exportation des instances Windows Server dans lesquelles vous avez initialement effectué l'importationEC2. Ajout de la prise en charge des horodatages sur le statut d'instance et le statut système pour indiquer la date et l'heure auxquelles un contrôle d'état a échoué.	25 mai 2012

Fonctionnalité	APIversion	Description	Date de publication
EC2exportation d'instances et horodatage lors des vérifications de l'état des instances et du système pour Amazon VPC	01-05-2012	Ajout de la prise en charge de l'exportation EC2 par exemple vers Citrix Xen, Microsoft Hyper-V et. VMware vSphere Ajout de la prise en charge des horodatages dans les contrôles de statut d'instance et de statut système.	25 mai 2012
AWS Marketplace AMIs	01-04-2012	Ajout du support pour AWS Marketplace AMIs.	19 avril 2012
Niveaux de tarification des instances réservées	15-12-2011	Ajout d'une nouvelle section expliquant comment tirer parti de la tarification des remises intégrée aux niveaux de tarification des instances réservées.	5 mars 2012
Interfaces réseau élastiques (ENIs) pour les EC2 instances dans Amazon Virtual Private Cloud	01-12-2011	Ajout d'une nouvelle section sur les interfaces réseau élastiques (ENIs) pour les EC2 instances d'unVPC. Pour de plus amples informations, veuillez consulter Interfaces réseau Elastic.	21 décembre 2011
Nouveaux types d'offres pour les instances EC2 réservées Amazon	01-11-2011	Vous avez le choix entre différentes offres d'instances réservées qui prennent en compte votre utilisation projetée de l'instance.	01 décembre 2011

Fonctionnalité	APIversion	Description	Date de publication
État de l'EC2instance Amazon	01-11-2011	Vous pouvez consulter des informations supplémentaires sur le statut de vos instances , y compris les événements planifiés par et AWS susceptibles d'avoir un impact sur vos instances. Ces activités opérationnelles incluent les redémarrages d'instance requis pour appliquer les mises à jour logicielles ou les correctifs de sécurité, ou les exigences d'instance requises en cas de problèmes matériels. Pour plus d'informations, consultez Surveillez l'état de vos EC2 instances Amazon.	16 novembre 2011
Instances ponctuelles sur Amazon VPC	15-07-2011	Ajout d'informations sur la prise en charge des instances Spot sur AmazonVPC. Avec cette mise à jour, les utilisateurs peuvent lancer des instances Spot, un cloud privé virtuel (VPC). En lançant des instances Spot dans unVPC, les utilisateurs d'instances Spot peuvent profiter des avantages d'AmazonVPC.	11 octobre 2011
Processus d'importation de machines virtuelles simplifié pour les utilisateurs des CLI outils	15-07-2011	Le processus d'importation de VM est simplifié grâce aux fonctionnalités améliorées de `ImportInstance` et`ImportVolume` , qui effectuera désormais le téléchargement des images sur Amazon EC2 après avoir créé la tâche d'importation. De plus, avec l'introduction de la commande `ResumeImport` , les utilisateurs peuvent redémarrer un chargement incomplet au point où la tâche s'est arrêtée.	15 septembre 201

Fonctionnalité	APIversion	Description	Date de publication
Support pour l'importation au format de VHD fichier		VM Import peut désormais importer des fichiers image de machine virtuelle au VHD format. Le format de VHD fichier est compatible avec les plateformes de virtualisation Citrix Xen et Microsoft Hyper-V. Avec cette version, VM Import prend désormais en charge RAW VHD et VMDK (VMwareESXcompatible) les formats d'image. Pour plus d'informations, consultez le VM Import/Export Guide de l'utilisateur.	24 août 2011
Mise à jour du connecteur Amazon EC2 VM Import pour VMware vCenter		Ajout d'informations sur la version 1.1 du connecteur Amazon EC2 VM Import pour appareil VMware vCenter virtuel (Connecto r). Cette mise à jour inclut la prise en charge du proxy pour l'accès Internet, une meilleure gestion des erreurs, une précision accrue de la barre d'avancement des tâches et plusieurs correctifs de bogue.	27 juin 2011
Modifications de tarification des zones de disponibilité des instances Spot	15-05-2011	Ajout d'informations sur la fonction de tarification des zones de disponibilité des instances Spot. Dans cette version, nous avons ajouté les options de tarification des zones de disponibilité, comme parties intégrantes des informations retournées quand vous interrogez les demandes d'instance Spot et l'historique des prix Spot. Ces ajouts permettent de déterminer plus facilement le prix requis pour lancer une instance Spot dans une zone de disponibilité particulière.	26 mai 2011

Fonctionnalité	APIversion	Description	Date de publication
AWS Identity and Access Management		Ajout d'informations sur AWS Identity and Access Management (IAM), qui permettent aux utilisateurs de spécifier les EC2 actions Amazon qu'ils peuvent utiliser avec les EC2 ressources Amazon en général. Pour de plus amples informations, veuillez consulter Gestion des identités et des accès pour Amazon EC2.	26 avril 2011
instances dédiées		Lancées au sein de votre Amazon Virtual Private Cloud (AmazonVPC), les instances dédiées sont des instances physiquement isolées au niveau du matériel hôte. Les instances dédiées vous permettent de tirer parti d'Amazon VPC et du AWS cloud, avec des avantages tels que le provisionnement élastique à la demande et le paiement uniquement pour ce que vous utilisez, tout en isolant vos instances de EC2 calcul Amazon au niveau matériel. Pour de plus amples informations, veuillez consulter Instances EC2 dédiées Amazon.	27 mars 2011
Mises à jour de la console de AWS gestion relatives aux instances réservées		Les mises à jour AWS de la console de gestion permettent aux utilisateurs de consulter plus facilement leurs instances réservées et d'acheter des instances réservées supplémentaires, y compris des instances réservées dédiées.	27 mars 2011

Fonctionnalité	APIversion	Description	Date de publication
Informations de métadonnées	2011-01-01	Ajout d'informations sur les métadonnées pour refléter les modifications de la version 2011-01-01. Pour plus d'informations, consultez Utiliser les métadonnées de l'instance pour gérer votre EC2 instance et Catégories de métadonnées d'instance.	11 mars 2011
Connecteur Amazon EC2 VM Import pour VMware vCenter		Ajout d'informations sur le connecteur Amazon EC2 VM Import pour appareil VMware vCenter virtuel (Connector). Le Connector est un plug-in VMware vCenter qui s'intègre au VMware vSphere client et fournit une interface utilisateur graphique que vous pouvez utiliser pour importer vos machines VMware virtuelles sur AmazonEC2.	3 mars 2011
Forcer le détachement du volume		Vous pouvez désormais utiliser le AWS Management Console pour forcer le détachement d'un EBS volume Amazon d'une instance.	23 février 2011
Protection de la fin d'instance		Vous pouvez désormais utiliser la console AWS de gestion pour empêcher la mise hors service d'une instance. Pour de plus amples informations, veuillez consulter Activer la protection de la résiliation.	23 février 2011
VM Import	15-11-2010	Ajout d'informations sur VM Import, qui vous permet d'importer une machine virtuelle ou un volume dans AmazonEC2. Pour plus d'informations, consultez le VM Import/Export Guide de l'utilisateur.	15 décembre 2010
Surveillance basique pour les instances	31-08-2010	Ajout d'informations sur la surveillance de base pour les EC2 instances.	12 décembre 2010

Fonctionnalité	APIversion	Description	Date de publication
Filtres et balises	31-08-2010	Ajout d'informations sur les ressources d'affichage, de filtrage et de balisage. Pour plus d'informations, consultez Trouvez vos EC2 ressources Amazon et Marquez vos EC2 ressources Amazon.	19 septembre 201
Lancement d'instance idempotente	31-08-2010	Ajout d'informations pour garantir l'idempotence lors de l'exécution des instances.	19 septembre 201
AWS Identity and Access Management pour Amazon EC2		Amazon s'intègre EC2 désormais à AWS Identity and Access Management (IAM). Pour de plus amples informations, veuillez consulter Gestion des identités et des accès pour Amazon EC2.	2 septembre 2010
Désignation de l'adresse VPC IP Amazon	15-06-2010	VPCLes utilisateurs d'Amazon peuvent désormais spécifier l'adresse IP à attribuer à une instance lancée dans unVPC.	12 juillet 2010
CloudWatch Surveillance d'Amazon pour Amazon EBS Volumes		La CloudWatch surveillance Amazon est désormais automatiquement disponible pour les EBS volumes Amazon.	14 juin 2010
instances réservées avec Windows		Amazon prend EC2 désormais en charge les instances réservées sous Windows.	22 février 2010

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.