開發人員指南

AWS WAFAWS Firewall Manager、和 AWS Shield Advanced

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS WAFAWS Firewall Manager、和 AWS Shield Advanced: 開發人員指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是 AWS WAFAWS Shield Advanced、和 AWS Firewall Manager？

您可以使用AWS WAFAWS Shield、和AWS Firewall Manager一起建立全方位的安全性解決方案。AWS WAF 是一種 Web 應用程式防火牆，可用來監控使用者傳送至應用程式的 Web 要求，以及控制對內容的存取。Shield Advanced 可在網路和傳輸層 (第 3 層和第 4 層DDoS) 和應用程式層 (第 7 層) 上針對 AWS 資源進行分散式拒絕服務 () 攻擊提供保護。 AWS Firewall Manager 提供跨帳戶和資源的保護管理，例如 AWS WAF 和 Shield Advanced，即使添加了新資源也是如此。

主題

什麼是 AWS WAF？

AWS WAF 是一種 Web 應用程式防火牆，可讓您監控轉寄至受保護 Web 應用程式資源的HTTP和HTTPS要求。您可以保護下列資源類型：

- Amazon CloudFront 分佈
- Amazon API 网关 REST API
- Application Load Balancer
- AWS AppSync GraphQL API
- Amazon Cognito 使用者集區
- AWS App Runner 服務
- AWS 驗證存取實例

AWS WAF 可讓您控制內容的存取權。根據您指定的條件 (例如請求來源的 IP 位址或查詢字串的值)，受保護的資源會以要求的內容、HTTP 403 狀態碼 (禁止) 或自訂回應來回應要求。

在最簡單的層級中， AWS WAF 可讓您選擇下列其中一個行為：

- 允許除您指定的請求以外的所有請求 — 當您希望 Amazon CloudFront、Amazon API 閘道、應用程式負載平衡器 AWS AppSync、Amazon Cognito 或 AWS 已驗證存取權限為公用網站提供內容時，這非常有用，但您也想封鎖攻擊者的請求。 AWS App Runner
- 封鎖除您指定的要求以外的所有要求 — 當您想要提供受限制網站的內容時，這個網站的使用者可以容易透過網頁要求中的屬性識別 (例如他們用來瀏覽網站的 IP 位址) 提供內容時，這會很有用。
- 計算符合條件的請求 — 您可以使用Count動作來追蹤網路流量，而無需修改處理方式。您可以將其用於一般監視，也可以測試新的 Web 請求處理規則。當您想要根據 Web 要求中的新屬性來允許或封鎖要求時，您可以先設定 AWS WAF 為計算符合這些屬性的要求。這可讓您在切換規則以允許或封鎖相符要求之前，先確認新的組態設定。
- 針對符合您準則的要求執行CAPTCHA或挑戰檢查 — 您可以針對要求實作CAPTCHA和無訊息的挑戰控制，以協助減少機器人流量到受保護的資源。

使用 AWS WAF 有幾個好處：

- 使用您指定的準則抵禦 Web 攻擊的其他防護。您可以使用 Web 請求的特性來定義條件，如下所示：
  - 發出請求的 IP 地址。
  - 發出請求的國家/地區。
  - 請求標頭中的值。
  - 要求中出現的字串，可能是符合規則運算式 (regex) 模式的特定字串或字串。
  - 請求的長度。
  - 存在可能是惡意的SQL代碼（稱為SQL插入）。
  - 指令碼的存在很可能為惡意 (稱為跨網站指令碼)。
- 可允許、封鎖或計算符合指定條件的 Web 要求的規則。或者，規則可以封鎖或計算不僅符合指定條件，而且在一分鐘或五分鐘內超過指定要求數目的 Web 要求。
- 規則，您可以重複在多個 web 應用程式上使用。
- 來自 AWS 和 AWS Marketplace 賣家的受管規則群組。
- 即時指標和採樣的 Web 請求。
- 自動化管理使用 AWS WAF API.

如果您希望對添加到資源的保護進行細微控制，那麼 AWS WAF 單獨可能是正確的選擇。如需有關的更多資訊 AWS WAF，請參閱AWS WAF。

什麼是 AWS Shield Advanced？

您可以使用 AWS WAF Web 存取控制清單 (WebACLs)，將分散式拒絕服務 (DDoS) 攻擊的影響降到最低。為了防止DDoS攻擊的額外保護， AWS 還提供 AWS Shield Standard 和 AWS Shield Advanced。 AWS Shield Standard 除了您已經支付的費用 AWS WAF 和其他 AWS 服務之外，會自動包含在內，無需額外費用。

Shield Advanced 為您的 Amazon EC2 執行個體、Elastic Load Balancing 負載平衡器、 CloudFront 分佈、Route 53 託管區域和 AWS Global Accelerator 標準加速器提供擴充的DDoS攻擊防護。護 Shield 進階會產生額外費用。Shield 進階選項和功能包括自動應用程式層DDoS緩解功能、進階事件可見性，以及 Shield 回應團隊的專屬支援 (SRT)。如果您擁有高可見度的網站，或者容易遭受頻繁DDoS攻擊，請考慮購買 Shield Advanced 提供的其他保護。有關其他訊息，請參閱AWS Shield Advanced 功能和選項和決定是否訂閱 AWS Shield Advanced 及套用其他保護。

什麼是 AWS Firewall Manager？

AWS Firewall Manager 簡化多個帳戶和資源的管理和維護任務，以提供各種保護 AWS WAF， AWS Shield Advanced包括 Amazon VPC 安全群組和網路 ACLs AWS Network Firewall，以及 Amazon Route 53 解析器DNS防火牆。有了 Firewall Manager，您只需設定一次保護，服務就會自動將其套用至您的帳戶和資源，即使您新增了新的帳戶和資源也一樣。

如需防火牆管理員的詳細資訊，請參閱AWS Firewall Manager。

設定您的帳戶以使用服務

本主題說明初步步驟，例如建立帳戶，以便準備使用 AWS WAF AWS Firewall Manager、和 AWS Shield Advanced。這些初步物品不會向你收取費用。我們只會針對您使用的 AWS 服務向您收費。

主題

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊時 AWS 帳戶，會建立AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理權限的使用者

註冊後，請保護 AWS 帳戶 AWS 帳戶根使用者、啟用和建立系統管理使用者 AWS IAM Identity Center，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

1. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。AWS Management Console在下一頁中，輸入您的密碼。

如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

   如需指示，請參閱《IAM 使用者指南》中的為 AWS 帳戶 根使用者啟用虛擬 MFA 裝置 (主控台)。

建立具有管理權限的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。

2. 在 IAM 身分中心中，將管理存取權授予使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。

以具有管理權限的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

  如需使用 IAM 身分中心使用者登入的說明，請參閱使用AWS 登入 者指南中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「建立權限集」。

2. 將使用者指派給群組，然後將單一登入存取權指派給群組。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「新增群組」。

下載工具

AWS Management Console 包含、和的主控台 AWS WAF AWS Shield Advanced AWS Firewall Manager，但如果您想要以程式設計方式存取服務，請參閱下列內容：

- API 指南記錄了服務支持的操作，並提供相關 SDK 和 CLI 文檔的鏈接：
  - AWS WAF API 參考
  - AWS Shield Advanced API 參考
  - AWS Firewall Manager API 參考
- 要調用 API 而不必處理低級別的詳細信息（例如組合原始 HTTP 請求），可以使用 AWS SDK。AWS SDK 提供封裝服務功能的 AWS 函數和資料類型。若要下載 AWS SDK 並存取安裝說明，請參閱適用的頁面：
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

  如需開 AWS 發套件的完整清單，請參閱 Amazon Web Services 的工具。
- 您可以使用 AWS Command Line Interface (AWS CLI) 從命令列控制多個 AWS 服務。您也可以使用指令碼自動執行命令。如需詳細資訊，請參閱 AWS Command Line Interface。
- AWS Tools for Windows PowerShell 支持這些 AWS 服務。如需詳細資訊，請參閱 AWS Tools for PowerShell Cmdlet 參考。

AWS WAF

AWS WAF 是一種 Web 應用程式防火牆，可讓您監視轉寄至受保護 Web 應用程式資源的 HTTP (S) 要求。您可以保護下列資源類型：

- Amazon CloudFront 分佈
- Amazon API Gateway 其他 API
- Application Load Balancer
- AWS AppSync GraphQL API
- Amazon Cognito 使用者集區
- AWS App Runner 服務
- AWS 已驗證存取實例

AWS WAF 可讓您控制內容的存取權。根據您指定的準則 (例如請求來源的 IP 位址或查詢字串的值)，與受保護資源關聯的服務會以要求的內容、HTTP 403 狀態碼 (禁止) 或自訂回應來回應要求。

> **Note**
>
> 您也可以使用 AWS WAF 來保護在 Amazon Elastic Container Service (Amazon ECS) 容器中託管的應用程式。Amazon ECS 是可高度擴展、快速的容器管理服務，可讓您輕鬆執行、停止和管理叢集上的 Docker 容器。若要使用此選項，您可以將 Amazon ECS 設定為使用應用程式負載平衡器，該應用程式負載平衡器可在服務中的任務中路由和保護 HTTP (S) 第 7 層流量。AWS WAF 如需詳細資訊，請參閱 Amazon 彈性容器服務開發人員指南中的服務負載平衡。

主題

- IP 集和正則表達式模式集 AWS WAF
- 定制的 Web 請求和響應 AWS WAF
- AWS WAF 標籤, 上, 网, 請求
- AWS WAF 智慧型威脅緩解
- 記錄 AWS WAF 網頁 ACL 流量
- 測試和調整您的 AWS WAF 保護
- 如何 AWS WAF 使用 Amazon CloudFront 功能
- 您使用 AWS WAF 服務時的安全
- AWS WAF 配額
- 將您的 AWS WAF 傳統資源遷移到 AWS WAF

如何 AWS WAF 工作

您可 AWS WAF 以用來控制受保護的資源如何回應 HTTP (S) Web 要求。您可以透過定義 Web 存取控制清單 (ACL)，然後將其與您要保護的一或多個 Web 應用程式資源產生關聯，以達到此目的。相關聯的資源會將傳入的請求轉寄至 AWS WAF Web ACL 進行檢查。

在 Web ACL 中，您可以建立規則來定義要在要求中尋找的流量模式，並指定要對相符請求採取的動作。動作選擇包括下列項目：

- 允許請求轉到受保護的資源進行處理和響應。
- 阻止請求。
- 計算請求。
- 針對要求執行 CAPTCHA 或挑戰檢查，以驗證人類使用者和標準瀏覽器使用。

AWS WAF 元件

以下是的中心組成部分 AWS WAF：

- Web ACL — 您可以使用 Web 存取控制清單 (ACL) 來保護一組資 AWS 源。您可以建立一個 Web ACL，並透過新增規則來定義其保護策略。規則定義檢查 Web 請求的準則，並指定要對符合其準則的請求採取的動作。您也可以為 Web ACL 設定預設動作，指出是否要封鎖或允許透過規則尚未封鎖或允許的任何要求。如需 Web ACL 的詳細資訊，請參閱AWS WAF 網頁存取控制清單 (網路 ACL)。

網頁 ACL 是一種 AWS WAF 資源。

- 規則 — 每個規則都包含定義檢驗條件的陳述式，以及 Web 請求符合條件時要採取的動作。當 Web 請求符合準則時，這是一個相符。您可以配置規則以阻止匹配請求，允許它們通過，計算它們，或對使用 CAPTCHA 難題或無聲客戶端瀏覽器挑戰的對象運行機器人控制。如需規則的詳細資訊，請參閱AWS WAF 規則。

  規則不是資 AWS WAF 源。它僅存在於 Web ACL 或規則群組的前後關聯中。
- 規則群組 — 您可以直接在 Web ACL 內或可重複使用的規則群組中定義規則。 AWS 受管規則和 AWS Marketplace 賣家會提供受管規則群組供您使用。您也可以定義自己的規則群組。如需規則群組的詳細資訊，請參閱AWS WAF 規則群組。

  規則群組是 AWS WAF 資源。

主題

AWS WAF 網路 ACL 容量單位 (WCU)

AWS WAF 使用 Web ACL 容量單位 (WCU) 來計算和控制執行規則、規則群組和 Web ACL 所需的作業資源。 AWS WAF 在設定規則群組和 Web ACL 時強制執行 WCU 限制。WCU 不會影響 AWS WAF 檢查網路流量的方式。

AWS WAF 管理規則、規則群組和 Web ACL 的容量。

規則 WCU

AWS WAF 在建立或更新規則時計算規則容量。 AWS WAF 以不同方式計算每個規則類型的產能，以反映每個規則的相對成本。相較於使用更多處理能力的複雜規則，執行成本較少的簡單規則，會使用較少的 WCU。例如，大小條件約束規則陳述式使用的 WCU 比使用正則運算式模式集檢查要求的陳述式少。

規則容量需求通常以規則類型的基本成本開始，並隨著複雜性而增加，例如，當您在檢查之前新增文字轉換或檢查 JSON 主體時。如需有關規則容量需求的資訊，請參閱中的規則陳述式清單規則陳述式基礎。

規則群組 WCU

規則群組的 WCU 需求是由您在規則群組內定義的規則所決定。規則群組的最大容量為 5,000 個 WCU。

每個規則群組都有不可變的容量設定，擁有者會在建立時指派這個設定。這適用於透過建立的受管規則群組和規則群組 AWS WAF。修改規則群組時，您的變更必須將規則群組的 WCU 保持在其容量之內。如此可確保使用規則群組的 Web ACL 仍在其容量需求範圍內。

規則群組中使用的 WCU 是規則的 WCU 總和，減去可透過組合規則行為來取得的任何處理最佳化。AWS WAF 例如，如果您定義了兩個規則來檢查相同的 Web 要求元件，而且每個規則在檢查元件之前都會套用特定的轉換至元件，則 AWS WAF 可能只需向您收取一次套用轉換的費用。在 Web ACL 中使用規則群組的 WCU 成本一律是您在建立規則群組時定義的固定 WCU 設定。

建立規則群組時，請注意將容量設定得足以容納您要在規則群組生命週期中使用的規則。

網絡十字韌帶 WCU

Web ACL 的 WCU 需求由您在 Web ACL 中使用的規則和規則群組決定。

- 在 Web ACL 中使用規則群組的成本是規則群組的容量設定。
- 使用規則的成本是規則計算的 WCU 減去任何能夠從 Web ACL 規 AWS WAF 則組合取得的處理最佳化。例如，如果您定義了兩個規則來檢查相同的 Web 要求元件，而且每個規則在檢查元件之前都會套用特定的轉換至元件，則 AWS WAF 可能只需向您收取一次套用轉換的費用。

網頁 ACL 的基本價格包含最多 1,500 個 WCU。根據分級定價模式，使用 1,500 個以上的 WCU 會產生額外費用。 AWS WAF 隨著您的 Web ACL WCU 用量變更，會自動調整您的 Web ACL 定價。如需定價詳細資訊，請參閱 AWS WAF 定價。

網頁 ACL 的最大容量為 5,000 個 WCU。

決定規則群組或網路 ACL 的 WCU

如先前幾節所述，規則群組或 Web ACL 中使用的 WCU 總計將等於或小於規則群組或 Web ACL 中定義之所有規則的 WCU 總和。

在 AWS WAF 主控台中，您可以看到將規則新增至 Web ACL 或規則群組時消耗的容量。主控台會顯示您新增規則時使用的目前容量單位。

透過 API，您可以針對要在 Web ACL 或規則群組中使用的規則，檢查最大容量需求。若要這麼做，請將規則的 JSON 清單提供給檢查容量呼叫。如需詳細資訊，請參閱 AWS WAF V2 API 參考CheckCapacity中的。

您可以使用保護的資源 AWS WAF

您可以使用 AWS WAF Web ACL 來保護全域或區域資源類型。您可以透過將 Web ACL 與您要保護的資源建立關聯來達成此目的。Web ACL 及其使用的任何 AWS WAF 資源都必須位於關聯資源所在的區域中。對於 Amazon CloudFront 發行版，此設定為美國東部 (維吉尼亞北部)。

Amazon CloudFront 分佈

您可以使用 AWS WAF 控制台或 API 將 AWS WAF Web ACL 與 CloudFront 發行版產生關聯。您也可以在建立或更新 CloudFront 發佈本身時，將 Web ACL 與分佈相關聯。若要在中配置關聯 AWS CloudFormation，您必須使用 CloudFront 發佈組態。如需 Amazon 的相關資訊 CloudFront，請參閱 Amazon CloudFront 開發人員指南中的使用 AWS WAF 控制對內容的存取。

AWS WAF 可用於全球 CloudFront 發行版，但您必須使用美國東部 (維吉尼亞北部) 區域來建立 Web ACL 和 Web ACL 中使用的任何資源，例如規則群組、IP 集和正則表達式模式集。有些介面提供「Global (CloudFront)」的區域選項。選擇此選項與選擇區域美國東部 (維吉尼亞北部) 或「us-east-1」相同。

區域資源

您可以在所有可用的區域中保護區域資源。 AWS WAF 您可以在中查看AWS WAF 端點和配額的清單Amazon Web Services 一般參考。

您可以使用 AWS WAF 來保護下列區域資源類型：

- Amazon API Gateway 其他 API
- Application Load Balancer
- AWS AppSync GraphQL API
- Amazon Cognito 使用者集區
- AWS App Runner 服務
- AWS 已驗證存取實例

您只能將 Web ACL 與內部的 Application Load Balancer 相關聯 AWS 區域。例如，您無法將 Web ACL 與開啟的 Application Load Balancer 相關聯 AWS Outposts。

Web ACL 及其使用的任何其他 AWS WAF 資源必須位於與受保護資源相同的區域中。監視和管理受保護區域資源的 Web 請求時，請將所有資料保 AWS WAF 留在與受保護資源相同的區域中。

多重資源關聯的限制

您可以將單一 Web ACL 與一或多個 AWS 資源產生關聯，但有下列限制：

- 您只能將每個 AWS 資源與一個 Web ACL 相關聯。Web ACL 和 AWS 資源之間的關係是 one-to-many。
- 您可以將 Web ACL 與一個或多個 CloudFront 分佈相關聯。您無法將已與 CloudFront 發佈關聯的 Web ACL 與任何其他 AWS 資源類型相關聯。

開始使用 AWS WAF

本教學課程顯示如何使用 AWS WAF 來執行下列工作：

- 設定 AWS WAF。
- 使用 AWS WAF 主控台中的精靈建立 Web 存取控制清單 (WebACL)。
- 選擇您要 AWS WAF 檢查 Web 請求的 AWS 資源。本教程介紹了 Amazon 的步驟 CloudFront。Amazon API 閘道RESTAPI、應用程式負載平衡器、 AWS AppSync GraphQL、Amazon Cognito 使用者集區API、 AWS App Runner 服務或 AWS 驗證存取執行個體的程序基本上相同。
- 新增您要用來篩選 Web 請求的規則和規則群組。例如，您可以指定要求來源的 IP 位址，並在要求中指定僅由攻擊者使用的值。對於每個規則，您可以指定如何處理相符的 Web 要求。您可以做阻止或計算它們之類的事情，並且可以運行類似的機器人挑戰CAPTCHA。您可以為在 Web 中定義的每個規則以ACL及在規則群組中定義的每個規則定義動作。
- 指定 Web ACL 的預設動作 (Block或) Allow。當 Web ACL 中的規則沒有明確允許或阻止它時，這是對請求 AWS WAF 採取的操作。

> **Note**
>
> AWS 一般而言，對於您在本教學課程中建立的資源，每天收取的費用不到 USD $0.25。當您完成此教學課程，我們建議您刪除資源以免產生不必要的費用。

主題

步驟 1：設定 AWS WAF

如果您尚未遵循中的一般設定步驟設定您的帳戶以使用服務，請立即執行。

步驟 2：建立網頁 ACL

主 AWS WAF 控台會引導您完成設定程序， AWS WAF 以根據您指定的條件封鎖或允許 Web 要求，例如要求來源的 IP 位址或要求中的值。在此步驟中，您會建立網頁ACL。如需 AWS WAF Web 的詳細資訊ACLs，請參閱AWS WAF 網頁存取控制清單 (網路 ACL)。

建立網頁的步驟 ACL

1. 登入 AWS Management Console 並開啟 AWS WAF 主控台，位於https://console.aws.amazon.com/wafv2/。
2. 在 AWS WAF 首頁中，選擇 [建立網頁] ACL。
3. 在「名稱」中，輸入您要用來識別此網頁的名稱ACL。

   > **Note**
   >
   > 建立網頁之後，就無法變更名稱ACL。

4. (選擇性) 對於說明-選用，ACL如果需要，請輸入較長的網頁描述。
5. 若為CloudWatch 量度名稱，請變更預設名稱 (如果適用)。遵循主控台上的指引，以瞭解有效的字元。名稱不能包含特殊字元、空格或保留給 AWS WAF使用的指標名稱，包括「All」和「Default_Action」。

   > **Note**
   >
   > 建立網頁之後，您就無法變更 CloudWatch 量度名稱ACL。

6. 對於「資源型態」，請選擇CloudFront分配。「區域」會自動填入「全域」(CloudFront) 以進CloudFront 行分配。
7. (選擇性) 針對關聯 AWS 資源-選擇性，請選擇 [新增 AWS 資源]。在對話方塊中，選擇您要關聯的資源，然後選擇 [新增]。 AWS WAF 返回「描述 Web ACL 和相關 AWS 資源」頁面。

8. 選擇 Next (下一步)。

步驟 3：新增字串比對規則

在此步驟中，您會建立使用字串比對陳述式的規則，並指出如何處理比對請求。字串比對規則陳述式會識別要在 AWS WAF 要求中搜尋的字串。通常，字符串由可打印ASCII字符組成，但是您可以指定從十六進制 0x00 到 0xFF（十進制 0 到 255）的任何字符。除了指定要搜尋的字串之外，您還可以指定要搜尋的 Web 要求元件，例如標頭、查詢字串或要求主體。

此陳述式類型會在 Web 要求元件上運作，而且需要下列要求元件設定：

- 要求元件 — 要檢查的 Web 要求部分，例如查詢字串或本文。

  > **Warning**
  >
  > 如果您檢查要求元件主JSON體、內文、標頭或 Cookie，請參閱 AWS WAF 可以檢查多少內容的限制處理超大請求組件 AWS WAF。

  如需 Web 要求元件的詳細資訊，請參閱Web 請求組件規格和處理。
- 選擇性文字轉換 — 您要在檢查要求元件之前對 AWS WAF 要求元件執行的轉換。例如，您可以轉換為小寫或標準化空格。如果您指定多個轉換，則會依照列出的順 AWS WAF 序處理這些轉換。如需相關資訊，請參閱 文字轉換選項。

如需 AWS WAF 規則的其他資訊，請參閱AWS WAF 規則。

建立字串比對規則陳述式

1. 在 Add rules and rule groups (新增規則和規則群組) 頁面上，選擇 Add rules (新增規則)、Add my own rules and rule groups (新增我自己的規則和規則群組)、Rule builder (規則建置器) 及 Rule visual editor (規則視覺化編輯器)。

   > **Note**
   >
   > 主控台提供「規則」視覺化編輯器以及「規則」JSON 編輯器。JSON編輯器可讓您輕鬆地在 Web 之間複製配置，ACLs並且對於更複雜的規則集（例如具有多個巢狀層級的規則集）則需要此編輯器。

此程序使用 Rule visual editor (規則視覺化編輯器)。

2. 對於 Name (名稱)，輸入您要用來識別此規則的名稱。
3. 對於 Type (類型)，選擇 Regular rule (一般規則)。
4. 對於 If a request (如果請求)，選擇 matches the statement (比對陳述式)。

   其他選項適用於邏輯規則陳述式類型。您可以使用它們來合併或否定其他規則陳述式的結果。
5. 在陳述式上，針對「檢查」，開啟下拉式清單，然後選擇您要檢查的 Web AWS WAF 要求元件。在此範例中，選擇「單一標題」。

   當您選擇「單一標題」時，您也可以指定 AWS WAF 要檢查的標頭。輸入 **`User-Agent`**。此值不會區分大小寫。
6. 對於 Match type (比對類型)，選擇指定的字串必須顯示在 `User-Agent` 標頭中的位置。

   對於此範例，選擇 Exactly matches string (完全符合字串)。這表示會 AWS WAF 檢查每個 Web 要求中的使用者代理程式標頭，找出與您指定的字串相同的字串。
7. 對於 String to match (要比對的字串)，指定您要 AWS WAF 搜尋的字串。String to match (符合值) 的長度上限為 200 個字元。如果您想要指定 base64 編碼值，可在編碼前指定最多 200 個字元。

   在此範例中，輸入MyAgent。 AWS WAF 將檢查 Web 請求中的`User-Agent`標題中的值`MyAgent`。
8. 將 Text transformation (文字轉換) 保持設定為 None (無)。
9. 針對「動作」，選取您希望規則在符合 Web 要求時採取的動作。在此範例中，選擇 [計數] 並保留其他選項不變。計數動作會為符合規則的 Web 要求建立量度，但不會影響要求是允許還是封鎖。如需有關動作選擇的詳細資訊，請參閱規則動作和Web ACL 規則和規則群組評估。
10. 選擇新增規則。

步驟 4：新增受 AWS 管規則規則群組

AWS 受管規則提供一組受管規則群組供您使用，其中大部分對 AWS WAF 客戶免費。如需規則群組的詳細資訊，請參閱AWS WAF 規則群組。我們會將 AWS 受管規則規則群組新增至此網頁ACL。

新增 AWS 受管規則規則群組

1. 在 Add rules and rule groups (新增規則和規則群組) 頁面上，選擇 Add rules (新增規則)，然後選擇 Add managed rule groups (新增受管規則群組)。

2. 在 [新增受管規則群組] 頁面上，展開AWS 受管規則群組的清單。（你也會看到為 AWS Marketplace 賣家提供的物品。 您可以訂閱其提供項目，然後以與「 AWS 受管規則」規則群組相同的方式使用它們。）
3. 針對您要新增的規則群組，執行下列動作：
   a. 在「動作」欄中，開啟「新增至網頁」ACL 切換。
   b. 選取「編輯」，然後在規則群組的「規則」清單中開啟「覆寫所有規則動作」下拉式清單，然後選取Count。這會將規則群組中所有規則的動作設定為僅計數。這可讓您在使用任何規則之前，先查看規則群組中的所有規則與 Web 要求的行為。
   c. 選擇 [儲存規則]。
4. 在 [新增受管規則群組] 頁面中，選擇 [新增規則]。您會返回「新增規則和規則群組」頁面。

步驟 5：完成您的網頁ACL設定

完成將規則和規則群組新增至 Web ACL 設定後，請在 Web 中管理規則的優先順序，並設定指標、標記ACL和記錄等設定來完成工作。

完成您的網頁ACL設定

1. 在 Add rules and rule groups (新增規則和規則群組) 頁面上，選擇 Next (下一步)。
2. 在 [設定規則優先順序] 頁面上，您可以在 Web 中查看規則和規則群組的處理順序ACL。 AWS WAF 從清單頂端開始處理它們。您可以向上或向下移動規則來變更處理順序。若要這樣做，請在清單中選取一個，然後選擇 Move up (上移) 或 Move down (下移)。如需有關規則優先順序的詳細資訊，請參閱 Web ACL 中規則和規則群組的處理順序。
3. 選擇 Next (下一步)。
4. 在設定指標頁面上，對於 Amazon CloudWatch 指標，您可以查看規則和規則群組的計劃指標，並且可以查看 Web 請求取樣選項。如需檢視取樣請求的資訊，請參閱。檢視 Web 請求的範例如需 Amazon CloudWatch 指標的相關資訊，請參閱使用 Amazon 監控 CloudWatch。

   您可以在 AWS WAF 主控台的「流量概觀」索引標籤下，存取網ACL頁流量指標的摘要。主控台儀表板提供近乎即時的網路 ACL Amazon CloudWatch 指標摘要。如需詳細資訊，請參閱網頁 ACL 流量概觀儀表板。
5. 選擇 Next (下一步)。
6. 在 [檢閱並建立網ACL頁] 上，檢閱您的設定，然後選擇 [建立網頁] ACL。

精靈會返回列出新網ACL頁ACL的網頁。

步驟 6：清除您的資源

現在，您已成功完成教學課程。若要避免帳戶產生額外 AWS WAF 費用，請清除您建立的 AWS WAF 物件。或者，您可以更改配置以匹配您真正想要使用管理的 Web 請求 AWS WAF。

> **Note**
>
> AWS 一般而言，對於您在本教學課程中建立的資源，每天收取的費用不到 USD $0.25。當您完成時，我們建議您刪除資源以免產生不必要的費用。

若要刪除 AWS WAF 收費的物件

1. 在網ACL頁中，ACL從清單中選取您的網頁，然後選擇 [編輯]。
2. 在 [關聯的 AWS 資源] 索引標籤上，針對每個關聯的資源選取資源名稱旁的選項按鈕，然後選擇 [取消關聯]。這會將網路ACL與您的 AWS 資源斷開關聯。
3. 在下列每個畫面中，選擇 [下一步]，直到您返回網ACL頁。

   在網ACL頁中，ACL從清單中選取您的網頁，然後選擇 [刪除]。

規則和規則陳述式不存在於規則群組和 Web ACL 定義之外。如果您刪除網頁ACL，這會刪除您在 Web 中定義的所有個別規則ACL。從網頁移除規則群組時ACL，只要移除該群組的參照即可。

AWS WAF 網頁存取控制清單 (網路 ACL)

Web 訪問控制列表（Web ACL）使您可以對受保護的資源響應的所有 HTTP（S）Web 請求進行更細微的控制。您可以保護亞馬遜 CloudFront、Amazon API 閘道、Application Load Balancer AWS AppSync、Amazon Cognito 和 AWS 驗證存取資源。 AWS App Runner

您可以使用如下的準則來允許或封鎖請求：

- 請求的 IP 地址來源
- 請求的來源國家/地區
- 字串比對或規則運算式 (regex) 在請求的一部分比對
- 請求的特定部分的大小
- 偵測惡意 SQL 程式碼或指令碼

您也可以測試這些條件的任何組合。您可以封鎖或計算不僅符合指定條件，還可以在一分鐘內超過指定要求數目的 Web 要求。您可以使用邏輯運算子結合條件。您還可以針對請求運行 CAPTCHA 難題和無聲客戶端會話挑戰。

您可以提供比對條件，以及在 AWS WAF 規則陳述式中對相符項目採取的動作。您可以直接在 Web ACL 內以及在 Web ACL 中使用的可重複使用規則群組中定義規則陳述式。如需選項的完整清單，請參閱規則陳述式基礎和規則動作。

若要指定 Web 請求檢查與處理條件，請執行下列作業：

1. 針對不符合您指定的任何規則的 Web 請求，選擇 Web ACL 預設動作Block，Allow或。如需詳細資訊，請參閱 網頁 ACL 預設動作。
2. 新增您要在 Web ACL 中使用的任何規則群組。受管規則群組通常包含封鎖 Web 請求的規則。如需規則群組的詳細資訊，請參閱 AWS WAF 規則群組。
3. 在一或多個規則中指定其他符合條件和處理指示。若要新增多個規則，請使用AND或規OR則陳述式開頭，然後將您要合併的規則嵌套在這些規則之下。如果您要否定某個規則選項，請將巢狀在 NOT 陳述式中規則化。您可以選擇性地使用速率型規則來取代一般規則，限制來自任何單一 IP 地址且符合條件的請求數量。如需規則的詳細資訊，請參閱 AWS WAF 規則。

如果您將多個規則新增至 Web ACL，請按照規則針對 Web ACL 列出的順序來 AWS WAF 評估規則。如需詳細資訊，請參閱 Web ACL 規則和規則群組評估。

建立 Web ACL 時，您可以指定要與其搭配使用的資源類型。如需相關資訊，請參閱建立 Web ACL。定義 Web ACL 之後，您可以將它與您的資源產生關聯，以開始為它們提供保護。如需詳細資訊，請參閱 建立 Web ACL 與資源的關聯或取消關聯 AWS。

AWS 資源如何處理回應延遲 AWS WAF

在某些情況下， AWS WAF 可能會遇到內部錯誤，延遲對關聯 AWS 資源的回應，關於是否允許或封鎖要求。在這些情況下， CloudFront 通常允許請求或提供內容，而區域服務通常會拒絕請求並且不提供內容。

主題

- Web ACL 規則和規則群組評估
- 網頁 ACL 預設動作
- 管理車身檢查尺寸限制
- 驗證碼，挑戰和令牌的配置

- 使用 Web ACL

Web ACL 規則和規則群組評估

Web ACL 處理 Web 請求的方式取決於下列各項：

- Web ACL 和規則群組內規則的數字優先順序設定
- 規則和 Web ACL 上的動作設定
- 您在新增的規則群組中放置的規則上的任何覆寫

如需規則動作設定的清單，請參閱規則動作。

您可以在規則動作設定和預設 Web ACL 動作設定中自訂要求和回應處理。如需相關資訊，請參閱定制的 Web 請求和響應 AWS WAF。

主題

- Web ACL 中規則和規則群組的處理順序
- 如何 AWS WAF 處理 Web ACL 中的規則和規則群組動作
- 規則群組的動作覆寫選項

Web ACL 中規則和規則群組的處理順序

在 Web ACL 和任何規則群組中，您可以使用數字優先順序設定來決定規則的評估順序。您必須為 Web ACL 中的每個規則指定該 Web ACL 中唯一的優先順序設定，並且必須為規則群組中的每個規則指定該規則群組中唯一的優先順序設定。

> **Note**
>
> 當您透過主控台管理規則群組和 Web ACL 時， AWS WAF 會根據清單中規則的順序為您指派唯一的數字優先順序設定。 AWS WAF 會將最低的數字優先順序指派給清單頂端的規則，並將最高的數字優先順序指派給底部的規則。

當 AWS WAF 根據 Web 要求評估任何 Web ACL 或規則群組時，它會從最低數值優先順序設定開始評估規則，直到找到終止評估的相符項目或耗盡所有規則為止。

例如，假設您的 Web ACL 中有下列規則和規則群組，如下所示的優先順序：

- 規則 1 — 優先順序 0
- RuleGroupA — 優先順序 100
  - 規則 1 — 優先順序 10,000
  - 規則 2-2 萬優先順序
- 規則 2 — 優先順序 200
- RuleGroup乙級 — 優先順序
  - 規則 B1 — 優先順序 0
  - 規則 B2 — 優先順序 1

AWS WAF 會以下列順序評估此 Web ACL 的規則：

- 規則 1
- RuleGroup一條規則 1
- RuleGroup一條規則 2
- 規則 2
- RuleGroupB 規則 B1
- RuleGroupB 規則 B2

如何 AWS WAF 處理 Web ACL 中的規則和規則群組動作

設定規則和規則群組時，您可以選擇要如 AWS WAF 何處理相符的 Web 要求：

- Allow和Block正在終止動作 — Allow 並且Block動作會停止相符 Web 請求上對 Web ACL 的所有其他處理。如果 Web ACL 中的規則找到與請求相符的項目，而規則動作為Allow或Block，則該相符項目會決定 Web ACL 的 Web 要求的最終處理方式。 AWS WAF 不會處理 Web ACL 中位於相符項目之後的任何其他規則。對於您直接新增至 Web ACL 的規則和在規則群組內新增的規則，正是如此。透過此Block動作，受保護的資源不會接收或處理 Web 要求。
- Count為非終止動作 — 當具有動作的規則符合要求時，會 AWS WAF 計算要求，然後繼續處理 Web ACL 規則集中後續的規則。Count
- CAPTCHA且Challenge可以是非終止或終止動作 — 當具有這些動作之一的規則符合要求時，會 AWS WAF 檢查其 Token 狀態。如果要求具有有效權杖，則會 AWS WAF 將相符項目視為與相Count符項目類似，然後繼續處理 Web ACL 規則集中遵循的規則。如果請求沒有有效的令牌，則 AWS WAF 終止評估並向客戶端發送 CAPTCHA 難題或無聲後台客戶端會話挑戰以解決。

如果規則評估不會產生任何終止動作，則會將 Web ACL 預設動作 AWS WAF 套用至要求。如需相關資訊，請參閱網頁 ACL 預設動作。

在 Web ACL 中，您可以覆寫規則群組內規則的動作設定，也可以覆寫規則群組傳回的動作。如需相關資訊，請參閱規則群組的動作覆寫選項。

動作與優先權設定之間的互動

AWS WAF 套用至 Web 要求的動作會受 Web ACL 中規則的數字優先順序設定影響。例如，假設您的 Web ACL 具有Allow動作和數字優先順序為 50 的規則，另一個具有Count動作且數字優先順序為 100 的規則。 AWS WAF 從最低設定開始，依其優先順序來評估 Web ACL 中的規則，因此它會在計數規則之前評估允許規則。符合這兩個規則的 Web 要求會先符合 allow 規則。由於Allow是終止動作，因此 AWS WAF 會在此比對中停止評估，並且不會根據計數規則評估要求。

- 如果您只想在計數規則量度中包含與 allow 規則不相符的要求，則規則的優先順序設定就可以使用。
- 另一方面，如果您想要計數規則中的計數量度，即使是符合 allow 規則的請求，則需要將計數規則指定為低於 allow 規則的數字優先順序設定，以便先執行。

如需優先順序設定的更多資訊，請參閱Web ACL 中規則和規則群組的處理順序。

規則群組的動作覆寫選項

將規則群組新增至 Web ACL 時，您可以覆寫對相符 Web 要求所採取的動作。覆寫 Web ACL 配置中規則群組的動作並不會改變規則群組本身。它只會改變在 Web ACL 環境中 AWS WAF 使用規則群組的方式。

規則群組規則動作覆寫

您可以將規則群組內的規則動作覆寫為任何有效的規則動作。當您執行此操作時，系統會完全像處理已設定規則的動作是覆寫設定一樣處理相符的要求。

> **Note**
>
> 規則動作可以是終止或非終止。終止動作會停止要求的 Web ACL 評估，並允許該要求繼續執行受保護的應用程式或封鎖該要求。

以下是規則動作選項：

- Allow- AWS WAF 允許將請求轉發到受保護的 AWS 資源以進行處理和響應。這是終止動作。在您定義的規則中，您可以在要求中插入自訂標頭，然後再將其轉寄至受保護的資源。
- Block- AWS WAF 阻止請求。這是終止動作。根據預設，受保護的 AWS 資源會以 HTTP `403 (Forbidden)` 狀態碼回應。在您定義的規則中，您可以自訂回應。 AWS WAF 封鎖要求時，Block 處理行動設定會決定受保護資源傳送回用戶端的回應。
- Count— AWS WAF 計算請求，但不確定是否允許或阻止它。這是非終止動作。 AWS WAF 繼續處理網頁 ACL 中的其餘規則。在您定義的規則中，您可以將自訂標題插入要求中，也可以新增其他規則可以符合的標籤。
- CAPTCHA並且 Challenge — AWS WAF 使用 CAPTCHA 謎題和無聲挑戰來驗證請求是否來自機器人，並 AWS WAF 使用令牌來跟踪最近成功的客戶響應。

  驗證碼謎題和無聲挑戰只能在瀏覽器訪問 HTTPS 端點時運行。瀏覽器客戶端必須在安全上下文中運行才能獲取令牌。

  > **Note**
  >
  > 如果您在其中一項規則中使用CAPTCHA或規Challenge則動作，或是規則群組中的規則動作覆寫，系統會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

  這些規則動作可以終止或非終止，具體取決於請求中令牌的狀態：

  - 非終止有效，未過期的令牌-如果令牌根據配置的 CAPTCHA 或挑戰免疫時間有效且未過期，則 AWS WAF 處理類似於操作的請求。Count AWS WAF 繼續根據 Web ACL 中剩餘的規則檢查 Web 請求。與Count組態類似，在您定義的規則中，您可以選擇性地使用要插入要插入要求的自訂標頭來設定這些動作，也可以新增其他規則可符合的標籤。
  - 以無效或過期權杖的封鎖要求終止 — 如果 Token 無效或指定的時間戳記已過期， AWS WAF 會終止 Web 要求的檢查並封鎖要求，類似於動作。Block AWS WAF 然後使用自定義響應代碼響應客戶端。對於CAPTCHA，如果請求內容表明客戶端瀏覽器可以處理它，則以 JavaScript 插入式方式 AWS WAF 發送 CAPTCHA 難題，該謎題旨在區分人類客戶端和機器人。對於該Challenge動作， AWS WAF 發送帶有無聲挑戰的 JavaScript 插頁式挑戰，該挑戰旨在區分普通瀏覽器和由漫遊器運行的會話。

  如需其他資訊，請參閱 CAPTCHA並Challenge在 AWS WAF。

若要取得有關如何使用此選項的資訊，請參閱〈〉覆寫規則群組中的規則動作。

將規則動作覆寫為 Count

規則動作覆寫最常見的使用案例是覆寫部分或全部規則動作Count，以測試和監視規則群組的行為，然後再將規則群組置入生產環境。

您也可以使用此功能對產生誤判的規則群組進行疑難排解。當規則群組封鎖您不預期封鎖的流量時，就會發生誤判。如果您在規則群組中識別會封鎖您要允許的請求的規則，您可以保留該規則的計數動作覆寫，以排除該規則不會對您的請求採取行動。

如需在測試中使用規則動作覆寫的詳細資訊，請參閱測試和調整您的 AWS WAF 保護。

清單：**RuleActionOverrides**取代 **ExcludedRules**

如果您Count在 2022 年 10 月 27 日之前在 Web ACL 組態中將規則群組規則動作設定為，則在 Web ACL JSON 中將覆寫 AWS WAF 儲存為ExcludedRules。現在，用於覆蓋規則的 JSON 設置位於CountRuleActionOverrides設置中。

當您使用 AWS WAF 主控台編輯現有的規則群組設定時，主控台會自動將 JSON 中的任何ExcludedRules設定轉換為RuleActionOverrides設定，覆寫動作設定為Count。

- 目前設定範例：

```
       "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesAdminProtectionRuleSet",
          "RuleActionOverrides": [
            {
              "Name": "AdminProtection_URIPATH",
              "ActionToUse": {
                "Count": {}
              }
            }
          ]
```

- 舊的設置示例：

```
OLD SETTING
       "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesAdminProtectionRuleSet",
          "ExcludedRules": [
            {
              "Name": "AdminProtection_URIPATH"
            }
```

```
            ]
OLD SETTING
```

建議您將 JSON 刊登物品中的所有`ExcludedRules`設定更新為`RuleActionOverrides`設定，並將動作設定為Count。API 接受任何一項設定，但如果您只使用新設定，您的主控台工作和 API 工作之間的 JSON 清單會保持一致`RuleActionOverrides`性。

規則群組傳回動作覆寫為 Count

您可以覆寫規則群組傳回的動作，並將其設定為Count。

> **Note**
>
> 這不是測試規則群組中規則的好選擇，因為它不會改變規則群組本身的 AWS WAF 評估方式。它只會影響 AWS WAF 處理從規則群組評估傳回至 Web ACL 之結果的方式。如果您要測試規則群組中的規則，請使用前一節所述的選項規則群組規則動作覆寫。

當您將規則群組動作覆寫為時Count，會正常 AWS WAF 處理規則群組評估。

如果規則群組中沒有相符的規則，或所有相符規則都有Count動作，則此覆寫對規則群組或 Web ACL 的處理沒有影響。

規則群組中符合 Web 要求且具有終止規則動作的第一個規則會導 AWS WAF 致停止評估規則群組，並將終止動作結果傳回 Web ACL 評估層級。此時，在 Web ACL 評估中，此取代會生效。 AWS WAF 會覆寫終止動作，使規則群組評估的結果只是一個Count動作。 AWS WAF 然後繼續處理 Web ACL 中的其餘規則。

若要取得有關如何使用此選項的資訊，請參閱〈〉將規則群組的評估結果覆寫為 Count。

網頁 ACL 預設動作

當您建立和設定 Web ACL 時，必須設定 Web ACL 預設動作。 AWS WAF 將此動作套用至任何透過 Web ACL 規則評估的 Web 請求，而不套用終止動作。終止動作會停止要求的 Web ACL 評估，並允許該要求繼續執行受保護的應用程式或封鎖該要求。如需有關規則動作的資訊，請參閱規則動作。

Web ACL 預設動作必須決定 Web 要求的最終處理方式，因此它是終止動作：

- Allow— 如果您想要允許大多數使用者存取您的網站，但想要封鎖對其請求來自指定 IP 位址的攻擊者的存取，或其要求似乎包含惡意 SQL 程式碼或指定值的攻擊者，請選擇Allow預設動作。然後，當

您將規則新增至 Web ACL 時，請新增可識別並封鎖您要封鎖的特定請求的規則。透過此動作，您可以在要求中插入自訂標頭，然後再將其轉寄至受保護的資源。

- Block— 如果您想要防止大多數使用者存取您的網站，但您想要允許存取來自指定 IP 位址的要求，或其要求包含指定值的使用者，請選擇Block預設動作。然後，當您將規則新增至 Web ACL 時，請新增可識別並允許您要允許的特定請求的規則。根據預設，對於Block動作，資 AWS 源會使用 HTTP `403 (Forbidden)` 狀態碼回應，但您可以自訂回應。

如需有關自訂請求和回應的資訊，請參閱定制的 Web 請求和響應 AWS WAF。

您自己的規則和規則群組的組態部分取決於您要允許還是封鎖多數的 Web 請求。例如，如果您想要允許大部分的要求，您可以將 Web ACL 預設動作設定為Allow，然後新增規則來識別您要封鎖的 Web 要求，如下所示：

- 來自發出異常數量 IP 地址的請求
- 來自您不常交涉、或時常受到攻擊國家/地區的請求
- `User-agent` 標題中包含虛假值的請求
- 似乎含有惡意 SQL 程式碼的請求

受管規則群組規則通常會使用Block動作，但並非所有規則都會使用。例如，用於機器人控制的某些規則會使用CAPTCHA和Challenge動作設定。如需受管規則群組的相關資訊，請參閱 受管規則群組。

管理車身檢查尺寸限制

主體檢查大小限制是 AWS WAF 可以檢查的最大請求主體大小。當 Web 要求主體大於限制時，基礎主機服務只會將限制範圍內的內容轉寄給以 AWS WAF 供檢查。

- 對於 Application Load Balancer AWS AppSync，限制固定為 8 KB (8,192 位元組)。
- 對於 CloudFront API Gateway、Amazon Cognito、應用程式執行器和驗證存取，預設限制為 16 KB (16,384 位元組)，您可以增加任何資源類型的限制，以 16 KB 的增量增加，最大為 64 KB。設定選項包括 16 KB、32 KB、48 KB 和 64 KB。

超大身體處理

如果您的 Web 流量包含大於限制的主體，則會套用您設定的超大處理。如需有關超大處理選項的資訊，請參閱處理超大請求組件 AWS WAF。

提高限制設定的定價考量

AWS WAF 針對檢查資源類型預設限制範圍內的流量收取基本費率的費用。

對於 CloudFront API Gateway、Amazon Cognito、應用程式執行器和驗證存取資源，如果您增加限制設定，則 AWS WAF 可檢查的流量會包括最大到新限制的主體大小。只有針對檢查內文大小大於預設 16 KB 的要求，您才需支付額外費用。如需定價的詳細資訊，請參閱AWS WAF 定價。

修改主體檢驗大小限制的選項

您可以設定 API Gateway、Amazon Cognito CloudFront、應用程式執行器或已驗證存取資源的主體檢查大小限制。

建立或編輯 Web ACL 時，可以修改資源關聯規劃中的主體檢查大小限制。如需 API 的相關資訊，請參閱網頁 ACL 的關聯設定，網址為AssociationConfig。對於主控台，請參閱您指定 Web ACL 相關資源的頁面上的組態。如需有關主控台設定的指引，請參閱使用 Web ACL。

驗證碼，挑戰和令牌的配置

您可以在 Web ACL 中針對使用CAPTCHA或Challenge規則動作的規則，以及管理 AWS WAF 受管理保護的無訊息用戶端挑戰的應用程式整合 SDK 設定選項。

這些功能通過向最終用戶挑戰 CAPTCHA 難題並通過向客戶端會話提出沉默挑戰來減輕機器人活動。當客戶端成功響應時，為他們 AWS WAF 提供一個令牌，供他們在他們的 Web 請求中使用，時間戳上最後一個成功的謎題和挑戰響應。如需詳細資訊，請參閱 AWS WAF 智慧型威脅緩解。

在 Web ACL 配置中，您可以配置如何 AWS WAF 管理這些令牌：

- CAPTCHA 和挑戰免疫時間 — 這些指定 CAPTCHA 或挑戰時間戳記保持有效的時間長度。Web ACL 設定會由未設定其自身免疫時間設定的所有規則繼承，也會由應用程式整合 SDK 繼承。如需詳細資訊，請參閱 時間戳記到期： AWS WAF 權杖豁免時間。
- 權杖網域 — 依預設，僅 AWS WAF 接受 Web ACL 相關聯之資源網域的權杖。如果您設定 Token 網域清單，請 AWS WAF 接受清單中所有網域的權杖，以及相關資源的網域。如需更多詳細資訊，請參閱 AWS WAF 網絡 ACL 令牌域列表配置。

使用 Web ACL

本節提供透過 AWS 主控台建立、管理和使用 Web ACL 的程序。

對於您正在使用的任何 Web ACL，您可以在 AWS WAF 主控台的「流量概觀」標籤下的 Web ACL 頁面上存取 Web 流量指標摘要。主控台儀表板提供近乎即時的 Amazon CloudWatch 指標摘要，這些指

標會在評估應用程式 Web 流量時 AWS WAF 收集到。如需有關儀表板的更多資訊，請參閱網頁 ACL 流量概觀儀表板。如需監視 Web ACL 流量的其他資訊，請參閱監控和調整。

> **⚠ 生產流量風險**
>
> 在 Web ACL 中針對生產流量部署變更之前，請先在測試或測試環境中對其進行測試和調整，直到您熟悉對流量的潛在影響為止。然後在啟用生產流量之前，在計數模式下測試和調整您更新的規則。如需準則，請參閱測試和調整您的 AWS WAF 保護。

> **Note**
>
> 在網頁 ACL 中使用超過 1,500 個 WCU 會產生超出基本網頁 ACL 價格的成本。如需詳細資訊，請參閱 AWS WAF 網路 ACL 容量單位 (WCU) 和 AWS WAF 定價。

更新期間暫時不一致

當您建立或變更 Web ACL 或其他 AWS WAF 資源時，變更需要少量時間才能傳播到儲存資源的所有區域。傳輸時間可以是幾秒鐘到分鐘數。

以下是您在變更傳播期間可能會注意到的暫時性不一致的範例：

- 建立 Web ACL 之後，如果您嘗試將其與資源建立關聯，可能會出現例外狀況，指出 Web ACL 無法使用。
- 將規則群組新增至 Web ACL 後，新規則群組規則可能會在使用 Web ACL 的某個區域中生效，而不會在另一個區域中生效。
- 變更規則動作設定後，您可能會在某些地方看到舊動作，而在其他地方看到新動作。
- 將 IP 位址新增至封鎖規則中使用的 IP 集後，該新位址可能會在某個區域遭到封鎖，而另一個區域仍允許使用該 IP 位址。

主題

- 建立 Web ACL
- 編輯網路 ACL
- 管理 Web ACL 中的規則群組行為
- 建立 Web ACL 與資源的關聯或取消關聯 AWS
- 刪除網頁 ACL

建立 Web ACL

若要建立新的 Web ACL，請按照此頁面上的程序使用 Web ACL 建立精靈。

> **⚠ 生產流量風險**
>
> 在 Web ACL 中針對生產流量部署變更之前，請先在測試或測試環境中對其進行測試和調整，直到您熟悉對流量的潛在影響為止。然後在啟用生產流量之前，在計數模式下測試和調整您更新的規則。如需準則，請參閱測試和調整您的 AWS WAF 保護。

> **Note**
>
> 在網頁 ACL 中使用超過 1,500 個 WCU 會產生超出基本網頁 ACL 價格的成本。如需詳細資訊，請參閱 AWS WAF 網路 ACL 容量單位 (WCU) 和 AWS WAF 定價。

建立 Web ACL

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中，選擇 Web ACL，然後選擇 Create web ACL (建立 Web ACL)。
3. 對於 Name (名稱)，輸入您要用來識別此 Web ACL 的名稱。

   > **Note**
   >
   > 建立 Web ACL 後無法修改名稱。

4. (選擇性) 對於 Description - optional (描述 - 選用性)，如果需要，請為 Web ACL 輸入較長的描述。
5. 若為CloudWatch 量度名稱，請變更預設名稱 (如果適用)。遵循主控台上的指引，以瞭解有效的字元。名稱不能包含特殊字元、空格或為其保留的量度名稱 AWS WAF，包括「全部」和「Default_Action」。

   > **Note**
   >
   > 建立 Web ACL 之後，您就無法變更 CloudWatch 量度名稱。

6. 在 [資源類型] 下，選擇您要與此 Web ACL 建立關聯的 AWS 資源類別 (Amazon CloudFront 分發或區域資源)。如需詳細資訊，請參閱 建立 Web ACL 與資源的關聯或取消關聯 AWS。
7. 對於「地區」，如果您已選擇區域資源類型，請選擇 AWS WAF 要儲存 Web ACL 的地區。

   您只需要針對區域資源類型選擇此選項。對於 CloudFront 分發，針對全球 () 應用程式，區域會硬式編碼至美國東部 (維吉尼亞北部CloudFront) 區域。`us-east-1`
8. (CloudFront、API Gateway、Amazon Cognito、應用程式執行器和驗證存取) 對於 Web 請求檢查大小限制-選用，如果您想要指定不同的本體檢查大小限制，請選取限制。檢測超過預設 16 KB 的機身尺寸可能會產生額外費用。如需此選項的詳細資訊，請參閱管理車身檢查尺寸限制。
9. (選擇性) 針對關聯 AWS 資源-選用，如果您要立即指定資源，請選擇 [新增 AWS 資源]。在對話方塊中，選擇您要關聯的資源，然後選擇 [新增]。 AWS WAF 返回「描述 Web ACL 和相關 AWS 資源」頁面。
10. 選擇下一步。
11. (選用) 如果您要新增受管規則群組，在 Add rules and rule groups (新增規則和規則群組) 頁面上，選擇 Add rules (新增規則)，然後選擇 Add managed rule groups (新增受管規則群組)。對於您要新增的每個受管規則群組執行下列動作：

    a. 在「新增受管規則群組」頁面上，展開 AWS 受管規則群組或您選擇的 AWS Marketplace 賣家的刊登物品。

    b. 針對您要新增的規則群組，在「動作」欄中，開啟「新增至 Web ACL」切換。

       若要自訂 Web ACL 使用規則群組的方式，請選擇 [編輯]。以下是常見的自訂設定：

       - 覆寫部分或所有規則的規則動作。如果您未定義規則的覆寫動作，則評估會使用規則群組內定義的規則動作。如需此選項的詳細資訊，請參閱規則群組的動作覆寫選項。
       - 新增範圍向下陳述式，以減少規則群組檢查的 Web 要求範圍。如需此選項的詳細資訊，請參閱範圍向下語句。
       - 某些受管規則群組會要求您提供其他組態。請參閱受管規則群組提供者的說明文件。如需 AWS 受管規則規則群組的特定資訊，請參閱AWS 的受管規則 AWS WAF。

       完成設定後，請選擇 [儲存規則]。

    選擇 Add rules (新增規則) 以完成新增受管規則，並回到 Add rules and rule group (新增規則和規則群組) 頁面。

12. (選用) 如果您要新增自己的規則群組，在 Add rules and rule groups (新增規則和規則群組) 頁面上，選擇 Add rules (新增規則)，然後選擇 Add my own rules and rule groups (新增我自己的規則和規則群組)。對於您要新增的每個規則群組執行下列動作：

    a. 在 Add my own rules and rule groups (新增我自己的規則和規則群組) 頁面上，選擇 Rule group (規則群組)。

    b. 在名稱中，輸入要用於此 Web ACL 中規則群組規則的名稱。請勿使用以`AWS`、`Shield`、`PreFM`或開頭的名稱`PostFM`。這些字串是保留的，或者可能會與其他服務為您管理的規則群組造成混淆。請參閱由其他服務提供的規則群組。

    c. 從清單中選擇您的規則群組。

    > **Note**
    >
    > 如果您要覆寫自己的規則群組的規則動作，請先將其儲存到 Web ACL，然後在 Web ACL 的規則清單中編輯 Web ACL 和規則群組參考陳述式。您可以將規則動作覆寫為任何有效的動作設定，就像您對受管規則群組執行的操作一樣。

    d. 選擇新增規則。

13. (選用) 如果您要新增自己的規則，在 Add rules and rule groups (新增規則和規則群組) 頁面上，選擇 Add rules (新增規則)、Add my own rules and rule groups (新增我自己的規則和規則群組)、Rule builder (規則建置器) 及 Rule visual editor (規則視覺化編輯器)。

    > **Note**
    >
    > 主控台 Rule visual editor (規則視覺化編輯器) 支援一個層級的巢狀化。例如，您可以使用單一邏輯`AND`或`OR`陳述式，並在其中嵌套一個層級的其他陳述式，但您無法在邏輯陳述式中巢狀化邏輯陳述式。若要管理更複雜的規則陳述式，請使用 Rule JSON editor(規則 JSON 編輯器)。如需有關規則的所有選項的資訊，請參閱 AWS WAF 規則。
    > 此程序涵蓋 Rule visual editor (規則視覺化編輯器)。

    a. 對於 Name (名稱)，輸入您要用來識別此規則的名稱。請勿使用以`AWS`、`Shield`、`PreFM`或開頭的名稱`PostFM`。這些字串是保留的，或者可能會與其他服務為您管理的規則群組造成混淆。

    b. 根據您的需求輸入規則定義。您可以在邏輯陳述式`AND`和規則陳述式中結合規`OR`則。精靈會根據內容，引導您完成每個規則的選項。如需規則選項的相關資訊，請參閱 AWS WAF 規則。

c. 對於 Action (動作)，選取規則在比對到 Web 請求時要採取的動作。如需有關您的選擇的相關資訊，請參閱 規則動作和 Web ACL 規則和規則群組評估。

如果您正在使用CAPTCHA或Challenge動作，請根據規則的需要調整豁免時間組態。如果未指定設定，則規則會從 Web ACL 繼承該設定。若要修改 Web ACL 免疫時間設定，請在建立 Web ACL 之後對其進行編輯。有關免疫時間的更多信息，請參閱時間戳記到期： AWS WAF 權杖豁免時間。

> **Note**
>
> 如果您在其中一項規則中使用CAPTCHA或規Challenge則動作，或是規則群組中的規則動作覆寫，系統會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

如果您想要自訂要求或回應，請選擇該要求或回應的選項，然後填入您的自訂詳細資訊。如需詳細資訊，請參閱 定制的 Web 請求和響應 AWS WAF。

如果您希望規則為匹配的 Web 請求添加標籤，請選擇相應的選項並填寫標籤詳細信息。如需詳細資訊，請參閱 AWS WAF 標籤, 上, 网, 請求。

d. 選擇新增規則。

14. 選擇 Web ACL 的預設動作，Block或Allow。當 Web ACL 中的規則未明確允許或封鎖 AWS WAF 要求時，這是針對要求所採取的動作。如需詳細資訊，請參閱 網頁 ACL 預設動作。

    如果要自定義默認操作，請選擇該操作的選項並填寫自定義的詳細信息。如需詳細資訊，請參閱 定制的 Web 請求和響應 AWS WAF。

15. 您可以定義 Token 網域清單，以啟用受保護應用程式之間的權杖共用。當您將 AWS 受管規則規則群組用於詐騙控制帳戶建立詐騙預防 (ACFP)、 AWS WAF AWS WAF 詐騙控制帳戶接管預防 (ATP) 和機器人控制時，您實Challenge作的和動作以及 AWS WAF 應用程式整合 SDK 會使用 Token。CAPTCHA

    不允許使用公共後綴。例如，您無法使用`gov.au`或`co.uk`做為權杖網域。

    默認情況下，僅 AWS WAF 接受保護資源的域令牌。如果您在此清單中新增 Token 網域，請 AWS WAF 接受清單中所有網域和相關資源網域的權杖。如需詳細資訊，請參閱 AWS WAF 網絡 ACL 令牌域列表配置。

16. 選擇下一步。

17. 在「設定規則優先順序」頁面中，選取規則和規則群組，並將其移至您要 AWS WAF 處理它們的順序。 AWS WAF 處理從清單頂端開始的規則。儲存 Web ACL 時，會依照規則的列示順序，AWS WAF 將數字優先順序設定指定給規則。如需詳細資訊，請參閱 Web ACL 中規則和規則群組的處理順序。
18. 選擇下一步。
19. 在「設定測量結果」頁面中，檢閱選項並套用您需要的任何更新。您可以為多個來源提供相同的量度名稱，以合併來自多個來源的CloudWatch 量度。
20. 選擇下一步。
21. 在 Review and create web ACL (檢閱並建立 Web ACL) 頁面中，檢查您的定義。如果您要變更任何區域，請針對區域選擇 Edit (編輯)。這會帶您回到 Web ACL 精靈中的頁面。進行任何變更，然後在頁面中選擇 Next (下一步)，直到您返回 Review and create web ACL (檢閱並建立 Web ACL) 頁面為止。
22. 選擇 建立 Web ACL。您的新 Web ACL 會列在 Web ACL 頁面中。

編輯網路 ACL

若要從 Web ACL 新增或移除規則，或變更組態設定，請使用此頁面上的程序存取 Web ACL。更新 Web ACL 時， AWS WAF 提供您與 Web ACL 相關聯的資源的持續涵蓋範圍。

> **生產流量風險**
>
> 在 Web ACL 中針對生產流量部署變更之前，請先在測試或測試環境中對其進行測試和調整，直到您熟悉對流量的潛在影響為止。然後在啟用生產流量之前，在計數模式下測試和調整您更新的規則。如需準則，請參閱測試和調整您的 AWS WAF 保護。

> **Note**
>
> 在網頁 ACL 中使用超過 1,500 個 WCU 會產生超出基本網頁 ACL 價格的成本。如需詳細資訊，請參閱 AWS WAF 網路 ACL 容量單位 (WCU) 和 AWS WAF 定價。

編輯 Web ACL

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

2. 在導覽窗格中，選擇 Web ACL。
3. 選擇您要編輯的 Web ACL 名稱。主控台會帶您前往 Web ACL 的說明。

> **Note**
>
> 由管理的網頁 ACL AWS Firewall Manager 的名稱開頭FMManagedWebACLV2-為。Firewall Manager 員管理員可以在 Firewall Manager 員 AWS WAF 策略中管理 這些 Web ACL 可能包含指定為在 Web ACL 中第一個和最後一個執行的規則群組集，位在您新增和管理的任何規則或規則群組的前面或後面。您無法變更任何第一個和最後一個規則群組規格。第一個和最後一個規則群組的名稱分別以PREFMManaged-和POSTFMManaged-開頭。如需這些政策的詳細資訊，請參閱AWS WAF 政策。

4. 視需要編輯網頁 ACL。選擇您感興趣的配置區域的標籤，然後編輯可變設置。對於您編輯的每個設定，當您選擇 [儲存] 並返回 Web ACL 的描述頁面時，主控台會儲存您對 Web ACL 的變更。

   以下列出包含 Web ACL 組態元件的索引標籤。

   - 規則標籤
     - 在 Web ACL 中定義的規則 — 您可以編輯和管理在 Web ACL 中定義的規則，類似於建立 Web ACL 期間的規則。

       > **Note**
       >
       > 請勿變更您未手動新增至 Web ACL 的任何規則名稱。如果您使用其他服務來管理規則，變更其名稱可能會移除或降低其提供預期保護的能力。 AWS Shield Advanced 並且 AWS Firewall Manager 兩者都在您的 Web ACL 中創建規則。如需相關資訊，請參閱由其他服務提供的規則群組。

       > **Note**
       >
       > 如果您變更規則的名稱，並希望規則的量度名稱反映變更，您也必須更新量度名稱。AWS WAF 變更規則名稱時，不會自動更新規則的度量名稱。您可以在主控台中編輯規則時，使用規則 JSON 編輯器變更量度名稱。您也可以透過 API 和任何用來定義 Web ACL 或規則群組的 JSON 清單中變更名稱。

如需有關規則和規則群組設定的資訊，請參閱AWS WAF 規則和AWS WAF 規則群組。

- 使用的 Web ACL 規則容量單位 — Web ACL 目前的容量使用量。這是僅供檢視。
- 不符合任何規則之請求的預設 Web ACL 動作 — 如需有關此設定的詳細資訊，請參閱網頁 ACL 預設動作。
- Web ACL 驗證碼和挑戰配置 — 這些免疫時間決定了 CAPTCHA 或挑戰令牌在獲取後仍然有效的時間。您只能在建立 Web ACL 之後，在此修改此設定。如需這些設定的資訊，請參閱時間戳記到期： AWS WAF 權杖豁免時間。
- Token 網域清單 — AWS WAF 接受清單中所有網域的權杖，以及相關資源的網域。如需詳細資訊，請參閱 AWS WAF 網絡 ACL 令牌域列表配置。

- 關聯的 AWS 資源標籤
  - Web 請求檢查大小限制 — 僅適用於保護 CloudFront 散佈的 Web ACL。本體檢查尺寸限制決定了要轉送到多少主體組件進 AWS WAF 行檢查。如需有關此設定的詳細資訊，請參閱 管理車身檢查尺寸限制。
  - 關聯 AWS 資源 — Web ACL 目前與之關聯並保護的資源清單。您可以找到與 Web ACL 位於相同區域內的資源，並將其與 Web ACL 相關聯。如需詳細資訊，請參閱 建立 Web ACL 與資源的關聯或取消關聯 AWS。
- 自訂回應主體標籤
  - 可供動作設定為的 Web ACL 規則使用的自訂回應主體Block。如需詳細資訊，請參閱 Block動作的自訂回應。
- 記錄和指標索引標籤
  - 記錄 — Web ACL 評估之流量的記錄。如需相關資訊，請參閱記錄 AWS WAF 網頁 ACL 流量。
  - 取樣請求 — 與 Web 請求相符之規則的相關資訊。如需檢視取樣請求的資訊，請參閱。檢視 Web 請求的範例
  - CloudWatch 度量 — Web ACL 中規則的度量。如需 Amazon CloudWatch 指標的相關資訊，請參閱使用 Amazon 監控 CloudWatch。

更新期間暫時不一致

當您建立或變更 Web ACL 或其他 AWS WAF 資源時，變更需要少量時間才能傳播到儲存資源的所有區域。傳輸時間可以是幾秒鐘到分鐘數。

以下是您在變更傳播期間可能會注意到的暫時性不一致的範例：

- 建立 Web ACL 之後，如果您嘗試將其與資源建立關聯，可能會出現例外狀況，指出 Web ACL 無法使用。
- 將規則群組新增至 Web ACL 後，新規則群組規則可能會在使用 Web ACL 的某個區域中生效，而不會在另一個區域中生效。
- 變更規則動作設定後，您可能會在某些地方看到舊動作，而在其他地方看到新動作。
- 將 IP 位址新增至封鎖規則中使用的 IP 集後，該新位址可能會在某個區域遭到封鎖，而另一個區域仍允許使用該 IP 位址。

管理 Web ACL 中的規則群組行為

本節說明用於修改您如何在 Web ACL 中使用規則群組的選項。此資訊適用於所有規則群組類型。將規則群組新增至 Web ACL 後，您可以將規則群組中個別規則的動作覆寫至任何其他有效規則動作設定，Count或覆寫至任何其他有效的規則動作設定。您也可以將規則群組的產生動作覆寫為Count，這不會影響規則群組內的規則評估方式。

如需這些選項的資訊，請參閱 規則群組的動作覆寫選項。

覆寫規則群組中的規則動作

對於 Web ACL 中的每個規則群組，您可以針對部分或所有規則覆寫包含規則的動作。

最常見的使用案例是覆寫規則動作，以測試新Count的或更新的規則。如果您已啟用量度，則會收到覆寫之每個規則的量度。如需測試的詳細資訊，請參閱 測試和調整您的 AWS WAF 保護。

若要覆寫規則群組中的規則動作

您可以在將受管規則群組新增至 Web ACL 時進行這些變更，而且可以在編輯 Web ACL 時將其設定到任何類型的規則群組。這些指示適用於已新增至 Web ACL 的規則群組。請參閱中有關此選項的其他資訊規則群組規則動作覆寫。

1. 編輯網路 ACL。
2. 在 Web ACL 頁面的「規則」標籤中，選取規則群組，然後選擇「編輯」。
3. 在規則群組的「規則」區段中，視需要管理動作設定。

    - 所有規則 — 若要為規則群組中的所有規則設定覆寫動作，請開啟「覆寫所有規則動作」下拉式清單，然後選取覆寫動作。若要移除所有規則的覆寫，請選取「移除所有取代」。
    - 單一規則 — 若要設定單一規則的覆寫動作，請開啟規則的下拉式清單，然後選取覆寫動作。若要移除規則的覆寫，請開啟規則的下拉式清單，然後選取 [移除覆寫]。

4. 完成變更後，請選擇 [儲存規則]。規則動作和覆寫動作設定會列在規則群組頁面中。

下列範例 JSON 清單顯示 Web ACL 內的規則群組宣告，該規則群組宣告會覆寫規則`CategoryVerifiedSearchEngine`與`Count`的規則動作`CategoryVerifiedSocialMedia`。在 JSON 中，您可以為每個個別規則提供一個`RuleActionOverrides`項目來覆寫所有規則動作。

```
{
    "Name": "AWS-AWSBotControl-Example",
   "Priority": 5,
   "Statement": {
    "ManagedRuleGroupStatement": {
        "VendorName": "AWS",
        "Name": "AWSManagedRulesBotControlRuleSet",
        "RuleActionOverrides": [
          {
            "ActionToUse": {
              "Count": {}
            },
            "Name": "CategoryVerifiedSearchEngine"
          },
          {
            "ActionToUse": {
              "Count": {}
            },
            "Name": "CategoryVerifiedSocialMedia"
          }
        ],
        "ExcludedRules": []
    },
   "VisibilityConfig": {
       "SampledRequestsEnabled": true,
       "CloudWatchMetricsEnabled": true,
       "MetricName": "AWS-AWSBotControl-Example"
   }
}
```

將規則群組的評估結果覆寫為 Count

您可以覆寫規則群組評估所產生的動作，而不必改變規則群組中規則的設定或評估方式。這個選項不常用。如果規則群組中的任何規則導致相符，此覆寫會將規則群組中產生的動作設定為Count。

> **Note**
>
> 這是一個不常見的用例。大多數動作覆寫都是在規則群組內的規則層級完成，如中所述覆寫規則群組中的規則動作。

您可以在新增或編輯規則群組時覆寫規則群組在 Web ACL 中產生的動作。在主控台中，開啟規則群組的 [覆寫規則群組] 動作-選用窗格，並啟用覆寫。在規則群組陳述式`OverrideAction`中設定的 JSON 中，如下列範例所示：

```
{
   "Name": "AWS-AWSBotControl-Example",
   "Priority": 5,
   "Statement": {
    "ManagedRuleGroupStatement": {
     "VendorName": "AWS",
     "Name": "AWSManagedRulesBotControlRuleSet"
     }
   },
    "OverrideAction": {
       "Count": {}
    },
   "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSBotControl-Example"
   }
}
```

建立 Web ACL 與資源的關聯或取消關聯 AWS

您可以使 AWS WAF 用在 Web ACL 和資源之間建立下列關聯：

- 將地區 Web ACL 與以下列出的任何區域資源建立關聯。對於此選項，Web ACL 必須與您的資源位於相同的區域中。
  - Amazon API Gateway 其他 API
  - Application Load Balancer
  - AWS AppSync GraphQL API
  - Amazon Cognito 使用者集區

  - AWS App Runner 服務
  - AWS 已驗證存取實例
- 將全球 Web ACL 與 Amazon CloudFront 分發相關聯。全球 Web ACL 將具有美國東部 (維吉尼亞北部) 區域的硬式編碼區域。

您也可以在建立或更新 CloudFront 發佈本身時，將 Web ACL 與分佈相關聯。如需詳細資訊，請參閱 Amazon CloudFront 開發人員指南中的使用 AWS WAF 控制對內容的存取。

有關多個關聯的限制

您可以根據下列限制，將單一 Web ACL 與一或多個 AWS 資源相關聯：

- 您只能將每個 AWS 資源與一個 Web ACL 相關聯。Web ACL 和 AWS 資源之間的關係是 one-to-many。
- 您可以將 Web ACL 與一個或多個 CloudFront 分佈相關聯。您無法將已與 CloudFront 發佈關聯的 Web ACL 與任何其他 AWS 資源類型相關聯。

其他限制

下列其他限制適用於 Web ACL 關聯：

- 您只能將 Web ACL 與中的應用程式負載平衡器相關聯 AWS 區域。例如，您無法將 Web ACL 與開啟的 Application Load Balancer 相關聯 AWS Outposts。
- 您無法將 Amazon Cognito 使用者集區與使用 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 受管規則群組`AWSManagedRulesACFPRuleSet`或詐騙控制帳戶接管預防 (ATP) 受管規則群組的 Web ACL 建立關聯。 AWS WAF `AWSManagedRulesATPRuleSet`如需有關帳戶建立詐騙預防的資訊，請參閱AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）。如需有關防止帳戶接管的資訊，請參閱AWS WAF 防止欺詐控制帳戶接管（ATP）。

> ⚠ 生產流量風險
>
> 在為生產流量部署 Web ACL 之前，請在測試或測試環境中對其進行測試和調整，直到您熟悉流量的潛在影響為止。然後在啟用規則之前，使用生產流量在計數模式下測試和調整規則。如需準則，請參閱測試和調整您的 AWS WAF 保護。

將 Web ACL 與 AWS 資源相關聯的步驟

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中，選擇 Web ACL。
3. 選擇您要與資源關聯的 Web ACL 名稱。主控台會將您帶到 Web ACL 的描述，您可以在其中編輯它。
4. 在關聯的 AWS 資源標籤上，選擇新增 AWS 資源。
5. 出現提示時，請選擇資源類型，選取要關聯的資源旁邊的圓鈕，然後選擇 [新增]。

取消 Web ACL 與資源的關聯的步驟 AWS

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中，選擇 Web ACL。
3. 選擇您要取消與資源關聯的 Web ACL 名稱。主控台會將您帶到 Web ACL 的描述，您可以在其中編輯它。
4. 在 [關聯的 AWS 資源] 索引標籤上，選取要取消此 Web ACL 與之關聯的資源。

   > **Note**
   >
   > 您必須一次取消一個資源的關聯。請勿選擇多個資源。

5. 選擇取消關聯。控制台打開一個確認對話框。確認您選擇取消 Web ACL 與 AWS 資源的關聯。

刪除網頁 ACL

若要刪除網頁ACL，請先取消所有 AWS 資源與網路ACL的關聯。請執行以下程序。

若要刪除網頁 ACL

1. 登入 AWS Management Console 並開啟 AWS WAF 主控台，位於https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中，選擇 [Web] ACLs。
3. 選取您要刪除ACL的網頁名稱。主控台會帶您前往網頁ACL說明，您可以在其中進行編輯。

> **Note**
>
> 如果您沒有看到要刪除的網頁，請ACL確定「網頁」區ACLs段中的「地區」選取項目正確無誤。ACLs保護 Amazon CloudFront 分佈的網絡位於全球（CloudFront）。

4. 在 [關聯的 AWS 資源] 索引標籤上，針對每個關聯的資源選取資源名稱旁的選項按鈕，然後選擇 [取消關聯]。這會將網路ACL與您的 AWS 資源斷開關聯。
5. 在導覽窗格中，選擇 [Web] ACLs。
6. 選取要刪除之網頁ACL旁邊的圓形按鈕，然後選擇 [刪除]。

AWS WAF 規則群組

規則群組是一組您可以新增至 Web ACL 的可重複使用的規則。如需 Web ACL 的詳細資訊，請參閱AWS WAF 網頁存取控制清單 (網路 ACL)。

規則群組分為下列主要類別：

- 您自己建立和維護的規則群組。
- 受管規則團隊為您建立和維護的 AWS 受管規則群組。
- AWS Marketplace 賣家為您建立和維護的受管規則群組。
- 由其他服務（例如和 Shield 進階）擁有 AWS Firewall Manager 和管理的規則群組。

規則群組與 Web ACL 之間的差異

規則群組和 Web ACL 都包含規則，這些規則在兩個位置都以相同的方式定義。規則群組與 Web ACL 的不同之處如下：

- 規則群組不能包含規則群組參考陳述式。
- 您可以將規則群組參考陳述式新增至每個 Web ACL，重複使用多個 Web ACL 中的單一規則群組。您無法重複使用 Web ACL。
- 規則群組沒有預設動作。在 Web ACL 中，您可以為您包含的每個規則或規則群組設定預設動作。規則群組或 Web ACL 內的每個個別規則都有定義的動作。
- 您不會直接將規則群組與 AWS 資源建立關聯。若要使用規則群組保護資源，請在 Web ACL 中使用規則群組。

- 網頁 ACL 具有系統定義的最大容量為 5,000 個網頁 ACL 容量單位 (WCU)。每個規則群組都有 WCU 設定，必須在建立時進行設定。您可以使用此設定來計算使用規則群組會新增至您的 Web ACL 的額外容量需求。如需 WCU 的詳細資訊，請參閱AWS WAF 網路 ACL 容量單位 (WCU)。

如需規則的詳細資訊，請參閱 AWS WAF 規則。

本節提供建立和管理您自己的規則群組的指引、說明您可以使用的受管規則群組，以及提供使用受管規則群組的指引。

主題

受管規則群組

受管規則群組是預先定義的 ready-to-use 規則集合，以 AWS 及 AWS Marketplace 賣家為您撰寫和維護的規則。基本 AWS WAF 定價適用於您對任何受管規則群組的使用。如需 AWS WAF 定價資訊，請參閱AWS WAF 定價。

- 除了基本 AWS WAF 費用外，還提供 AWS WAF 機器人控制、防 AWS WAF 欺詐控制帳戶接 AWS 管（ATP）和 AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）的受管規則群組，需支付額外費用。如需定價詳細資訊，請參閱 AWS WAF 定價。
- 所有其他 AWS 受管規則群組均可供 AWS WAF 客戶使用，無須額外付費。
- AWS Marketplace 受管規則群組可透過訂閱使用 AWS Marketplace。這些規則群組中的每一個都是由 AWS Marketplace 賣家擁有和管理。如需使用 AWS Marketplace 受管規則群組的定價資訊，請聯絡 AWS Marketplace 賣家。

某些受管規則群組的設計目的是協助保護特定類型的 Web 應用程式WordPress，例如 Joomla 或 PHP。其他提供廣泛的保護，防範已知威脅或常見 Web 應用程式弱點，包括 OWASP 前 10 名中列出的部分弱點。如果您受限於法規合規，例如 PCI 或 HIPAA，您可以使用受管規則群組以達到 Web 應用程式防火牆的需求。

自動更新

為了保持在最新狀態以了解不斷變化的威脅趨勢，不僅費時而且耗錢。實作和使用受管規則群組可以節省您的時間 AWS WAF。許多人 AWS 和 AWS Marketplace 銷售商會在出現新漏洞和威脅時自動更新受管規則群組，並提供新版本的規則群組。

在某些情況下，由於其參與了許多私人披露社區，因 AWS 此在公開披露之前會收到新漏洞的通知。在這些情況下，即使在廣為人知的新安全威脅之前，仍 AWS 可更新 AWS 受管規則群組並為您部署。

受管規則群組中規則的限制存取

每個受管規則群組都會針對其設計用來防範的攻擊類型和弱點提供完整描述。若要保護規則群組提供者的智慧財產權，您無法檢視規則群組中個別規則的所有詳細資料。此限制也有助於防止惡意使用者利用規避發佈的規則設計攻擊威脅。

主題

- 版本化的受管理規則群組
- 使用受管規則群組
- AWS 的受管規則 AWS WAF
- AWS Marketplace 受管規則群組

版本化的受管理規則群組

許多受管規則群組提供者會使用版本控制來更新規則群組的選項和功能。通常，特定版本的受管規則群組是靜態的。有時候，提供者可能需要更新受管規則群組的部分或全部靜態版本，例如，為了回應新興的安全威脅。

當您在 Web ACL 中使用版本化的受管理規則群組時，可以選取預設版本並讓提供者管理您使用的靜態版本，或者您可以選取特定的靜態版本。

找不到您想要的版本？

如果您在規則群組的版本清單中沒有看到某個版本，表示該版本可能已排定到期或已過期。排定版本到期後，您就 AWS WAF 不再允許為規則群組選擇該版本。

AWS 受管規則規則群組的 SNS 通知

「受 AWS 管規則」規則群組除了 IP 信譽規則群組外，所有群組都會提供版本控制和 SNS 更新通知。提供通知的 AWS 受管規則規則群組都使用相同的 SNS 主題 Amazon 資源名稱 (ARN)。若要註冊 SNS 通知，請參閱取得新版本和更新的通知。

主題

受管規則群組的版本生命週期

提供者會處理受管規則群組靜態版本的下列生命週期階段：

- 發行和更新 — 受管規則群組供應商透過 Amazon Simple Notification Service (Amazon SNS) 主題的通知，宣布其受管規則群組的即將推出和新的靜態版本。提供者也可能會使用此主題來傳達有關其規則群組的其他重要資訊，例如緊急必要的更新。

  您可以訂閱規則群組的主題，並設定接收通知的方式。如需更多資訊，請參閱取得新版本和更新的通知。
- 到期排程 — 受管規則群組提供者會將舊版規則群組排程到期。排程到期的版本無法新增至您的 Web ACL 規則。在某個版本排程到期後，使用 Amazon 中的倒數指標 AWS WAF 追蹤到期時間 CloudWatch。
- 版本到期 — 如果您將 Web ACL 設定為使用受管理規則群組的過期版本，則在 Web ACL 評估期間， AWS WAF 會使用規則群組的預設版本。此外，會 AWS WAF 封鎖 Web ACL 的任何更新，這些更新不會移除規則群組或將其版本變更為未過期的規則群組。

如果您使用 AWS Marketplace 受管規則群組，請向提供者詢問有關版本生命週期的任何其他資訊。

受管規則群組的版本到期日

如果您使用特定版本的規則群組，請確定您不會繼續使用超過其到期日期的版本。您可以透過規則群組的 SNS 通知和 Amazon CloudWatch 指標來監控版本到期日。

如果您在 Web ACL 中使用的版本已過期，則會 AWS WAF 封鎖對 Web ACL 的任何更新，而這些更新不包括將規則群組移至未過期的版本。您可以將規則群組更新為可用版本，或將其從 Web ACL 中移除。

受管規則群組的到期處理取決於規則群組提供者。對於 AWS 受管規則規則群組，過期版本會自動變更為規則群組的預設版本。對於 AWS Marketplace 規則群組，請詢問提供者如何處理到期日。

當提供者建立規則群組的新版本時，會設定版本的預測存留期。雖然版本未排定到期，但 Amazon CloudWatch 指標值會設定為預測的存留期設定，在中 CloudWatch，您會看到指標的固定值。提供者

排定量度到期後，指標值會每天減少，直到到期日達到零為止。如需監視到期日的相關資訊，請參閱追蹤版本到期日。

處理受管規則群組版本的最佳作法

當您使用版本控制的受管理規則群組時，請遵循此最佳作法指引來處理版本控制。

當您在 Web ACL 中使用受管規則群組時，您可以選擇使用規則群組的特定靜態版本，或選擇使用預設版本：

- 預設版本 — AWS WAF 一律將預設版本設定為提供者目前建議的靜態版本。當提供者更新其建議的靜態版本時， AWS WAF 會自動更新 Web ACL 中規則群組的預設版本設定。

  當您使用受管規則群組的預設版本時，請執行下列最佳作法：

  - 訂閱通知 — 訂閱規則群組變更的通知，並留意這些變更。大多數提供商都會發送新靜態版本和默認版本更改的高級通知。這些可讓您在將預設版本 AWS 切換至新靜態版本之前檢查新靜態版本的效果。如需更多資訊，請參閱取得新版本和更新的通知。
  - 檢閱靜態版本設定的效果，並視需要進行調整，然後再將預設值設為新的靜態版本。在預設值設定為新的靜態版本之前，請先檢閱靜態版本對監視和管理 Web 要求的影響。新的靜態版本可能有新規則需要檢閱。尋找誤報或其他未預期的行為，以防您需要修改規則群組的使用方式。您可以設定要計數的規則，例如，在您弄清楚要如何處理新行為時，阻止它們封鎖流量。如需詳細資訊，請參閱 測試和調整您的 AWS WAF 保護。
- 靜態版本 — 如果您選擇使用靜態版本，則必須在準備採用新版本的規則群組時手動更新版本設定。

  當您使用受管規則群組的靜態版本時，請執行下列最佳作法：

  - 保持版本為最新狀態 — 讓您的受管規則群組盡可能接近最新版本。發布新版本時，請對其進行測試，根據需要調整設置並及時實施。如需有關測試的資訊，請參閱測試和調整您的 AWS WAF 保護。
  - 訂閱通知 — 訂閱規則群組變更的通知，以便您知道提供者何時發佈新的靜態版本。大多數提供商會提供版本更改的高級通知。此外，您的提供商可能需要更新您正在使用的靜態版本，以關閉安全漏洞或其他緊急原因。如果您訂閱了提供商的通知，您將知道發生了什麼。如需詳細資訊，請參閱取得新版本和更新的通知。
  - 避免版本過期-不要讓靜態版本在您使用時過期。過期版本的提供者處理可能會有所不同，可能包括強制升級到可用版本或其他可能導致意外後果的變更。追蹤到 AWS WAF 期指標並設定警示，讓您有足夠的天數成功升級至支援的版本。如需更多詳細資訊，請參閱 追蹤版本到期日。

使用受管規則群組

本節提供存取和管理受管規則群組的指引。

將受管規則群組新增至 Web ACL 時，您可以選擇與您自己的規則群組相同的組態選項，以及其他設定。

在 Web ACL 中新增和編輯規則的過程中，您可以透過主控台存取受管規則群組資訊。透過 API 和命令列介面 (CLI)，您可以直接要求受管規則群組資訊。

當您在 Web ACL 中使用受管規則群組時，您可以編輯下列設定：

- 版本-只有在規則群組已建立版本時，才能使用此選項。如需詳細資訊，請參閱 版本化的受管理規則群組。
- 覆寫規則動作 — 您可以將規則群組中規則的動作覆寫為任何動作。將其設定為對Count於在使用規則群組管理 Web 要求之前測試規則群組非常有用。如需詳細資訊，請參閱 規則群組規則動作覆寫。
- ScopeDown 陳述式 — 您可以新增範圍向下陳述式，以篩選出您不想使用規則群組評估的 Web 要求。如需詳細資訊，請參閱 範圍向下語句。
- 覆寫規則群組動作 — 您可以覆寫規則群組評估所產生的動作，並將其設定為Count僅。此選項不常用。它不會改變規則群組中規則的 AWS WAF 評估方式。如需詳細資訊，請參閱 規則群組傳回動作覆寫為 Count。

編輯 Web ACL 中的受管規則群組設定

- 主控台
  - (選項) 當您將受管規則群組新增至 Web ACL 時，您可以選擇 「編輯」 來檢視和編輯設定。
  - (選項) 將受管規則群組新增至 Web ACL 之後，從 Web ACL 頁面選擇剛建立的 Web ACL。這將帶您前往 Web ACL 編輯頁面。
    - 選擇 Rules (規則)。
    - 選取規則群組，然後選擇編輯以檢視和編輯設定。
- API 和 CLI — 在主控台之外，您可以在建立和更新 Web ACL 時管理受管規則群組設定。

擷取受管規則群組清單

您可以擷取可供您在 Web ACL 中使用的受管規則群組清單。該列表包括以下內容：

- 所有 AWS 受管規則規則群組。

- 您已訂閱的 AWS Marketplace 規則群組。

> **Note**
>
> 如需有關訂閱 AWS Marketplace 規則群組的資訊，請參閱AWS Marketplace 受管規則群組。

擷取受管規則群組清單時，您取回的清單取決於您使用的介面：

- 主控台 — 透過主控台，您可以查看所有受管規 AWS Marketplace 則群組，包括尚未訂閱的規則群組。對於您尚未訂閱的那些，該界面提供了可以按照訂閱的鏈接。
- API 和 CLI — 在主控台外部，您的請求只會傳回可供您使用的規則群組。

擷取受管規則群組的清單

- 主控台 — 在建立 Web ACL 的過程中，在 [新增規則和規則群組] 頁面上，選擇 [新增受管規則群組]。會在最上層列出提供者名稱。展開每個提供者清單以查看受管規則群組的清單。對於已建立版本的規則群組，此層級顯示的資訊適用於預設版本。當您將受管規則群組新增至 Web ACL 時，主控台會根據命名配置 `<Vendor Name>-<Managed Rule Group Name>` 列出該群組。
- API —
  - `ListAvailableManagedRuleGroups`
- CLI —
  - `aws wafv2 list-available-managed-rule-groups --scope=<CLOUDFRONT|REGIONAL>`

擷取受管規則群組中的規則

您可以擷取受管規則群組中的規則清單。API 和 CLI 呼叫會傳回您可以在 JSON 模型中或透過參考的規則規格 AWS CloudFormation。

擷取受管規則群組中的規則清單

- 主控台
  - (選項) 當您將受管規則群組新增至 Web ACL 時，您可以選擇 「編輯」 來檢視規則。
  - (選項) 將受管規則群組新增至 Web ACL 之後，從 Web ACL 頁面選擇剛建立的 Web ACL。這將帶您前往 Web ACL 編輯頁面。

    - 選擇 Rules (規則)。
    - 選取您要查看其規則清單的規則群組，然後選擇「編輯」。 AWS WAF 顯示規則群組中的規則清單。
- API — `DescribeManagedRuleGroup`
- CLI — `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

擷取受管規則群組的可用版本

受管規則群組的可用版本是尚未排程到期的版本。此清單會指出哪個版本是規則群組的目前預設版本。

擷取受管規則群組的可用版本清單

- 主控台
    - (選項) 當您將受管規則群組新增至 Web ACL 時，請選擇 「編輯」 以查看規則群組的資訊。展開 [版本] 下拉式清單以查看可用版本的清單。
    - (選項) 將受管規則群組新增至 Web ACL 後，請在 Web ACL 上選擇 [編輯]，然後選取並編輯規則群組規則。展開 [版本] 下拉式清單以查看可用版本的清單。
- API —
    - `ListAvailableManagedRuleGroupVersions`
- CLI —
    - `aws wafv2 list-available-managed-rule-group-versions --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

透過主控台將受管規則群組新增至 Web ACL

本指引適用於所有 AWS 受管規則群組，以及您訂閱的規 AWS Marketplace 則群組。

> **⚠ 生產流量風險**
>
> 在 Web ACL 中針對生產流量部署變更之前，請先在測試或測試環境中對其進行測試和調整，直到您熟悉對流量的潛在影響為止。然後在啟用生產流量之前，在計數模式下測試和調整您更新的規則。如需準則，請參閱測試和調整您的 AWS WAF 保護。

> **Note**
>
> 在網頁 ACL 中使用超過 1,500 個 WCU 會產生超出基本網頁 ACL 價格的成本。如需詳細資訊，請參閱 AWS WAF 網路 ACL 容量單位 (WCU) 和 AWS WAF 定價。

透過主控台將受管規則群組新增至 Web ACL

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中選擇 [Web ACL]。
3. 在 [Web ACL] 頁面中，從 Web ACL 清單中選取要新增規則群組的目標。這會帶您前往單一 Web ACL 的頁面。
4. 在您的網頁 ACL 頁面中，選擇「規則」標籤。
5. 在「規則」窗格中，選擇「新增規則」，然後選擇「新增受管規則群組」。
6. 在 [新增受管規則群組] 頁面中，展開規則群組廠商的選取項目，以查看可用規則群組的清單。
7. 針對您要新增的每個規則群組，選擇「新增至 Web ACL」。如果您要變更規則群組的 Web ACL 組態，請選擇 [編輯]，進行變更，然後選擇 [儲存規則]。如需選項的相關資訊，請參閱的版本控制指引，以版本化的受管理規則群組及在 Web ACL 中使用受管規則群組的指引管理規則群組陳述式。
8. 在 [新增受管規則群組] 頁面底部，選擇 [新增規則]。
9. 在「設定規則優先順序」頁面中，視需要調整規則執行的順序，然後選擇「儲存」。如需詳細資訊，請參閱 Web ACL 中規則和規則群組的處理順序。

在 Web ACL 頁面中，您新增的受管規則群組會列在 [規則] 索引標籤下。

在將保護用於生產流量之前，請先測試和調整 AWS WAF 保護措施的任何變更。如需相關資訊，請參閱測試和調整您的 AWS WAF 保護。

更新期間暫時不一致

當您建立或變更 Web ACL 或其他 AWS WAF 資源時，變更需要少量時間才能傳播到儲存資源的所有區域。傳輸時間可以是幾秒鐘到分鐘數。

以下是您在變更傳播期間可能會注意到的暫時性不一致的範例：

- 建立 Web ACL 之後，如果您嘗試將其與資源建立關聯，可能會出現例外狀況，指出 Web ACL 無法使用。
- 將規則群組新增至 Web ACL 後，新規則群組規則可能會在使用 Web ACL 的某個區域中生效，而不會在另一個區域中生效。
- 變更規則動作設定後，您可能會在某些地方看到舊動作，而在其他地方看到新動作。
- 將 IP 位址新增至封鎖規則中使用的 IP 集後，該新位址可能會在某個區域遭到封鎖，而另一個區域仍允許使用該 IP 位址。

接收受管理規則群組的新版本和更新的通知

受管規則群組提供者會使用 SNS 通知來宣告規則群組變更，例如即將推出的新版本和緊急安全性更新。

如何訂閱 SNS 通知

若要訂閱規則群組的通知，您可以在美國東部 (維吉尼亞北部) 區域 us-east-1 國東部 (維吉尼亞北部) 區域中為規則群組的 Amazon SNS 主題 ARN 建立 Amazon SNS 訂閱。

如需有關如何訂閱的資訊，請參閱 Amazon 簡單通知服務開發人員指南。

> **Note**
>
> 僅在 us-east-1 區域建立 SNS 主題的訂閱。

版本控制的 AWS 受管規則規則群組都使用相同的 SNS 主題 Amazon 資源名稱 (ARN)。如需 AWS 受管規則規則群組通知的詳細資訊，請參閱部署通知。

哪裡可以找到受管規則群組的 Amazon SNS 主題 ARN

AWS 受管規則規則群組使用單一 SNS 主題 ARN，因此您可以從其中一個規則群組擷取主題 ARN，並加以訂閱，以取得提供 SNS 通知之所有 AWS 受管規則規則群組的通知。

- 主控台
  - (選項) 將受管規則群組新增至 Web ACL 時，請選擇編輯以查看規則群組的資訊，其中包括規則群組的 Amazon SNS 主題 ARN。
  - (選項) 將受管規則群組新增至 Web ACL 後，請在 Web ACL 上選擇「編輯」，然後選取並編輯規則群組規則，以查看規則群組的 Amazon SNS 主題 ARN。

- API — `DescribeManagedRuleGroup`
- CLI — `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

有關 Amazon SNS 通知格式以及如何篩選收到的通知的一般資訊，請參閱 Amazon 簡單通知服務開發人員指南中的剖析訊息格式和 Amazon SNS 訂閱篩選政策。

追蹤規則群組的版本到期

如果您使用特定版本的規則群組，請確定您不會繼續使用超過其到期日期的版本。

> **Tip**
>
> 為受管規則群組註冊 Amazon SNS 通知，並使用受管規則群組版本保持最新狀態。您將受益於規則群組的大多數 up-to-date 保護，並在到期前保持領先。如需相關資訊，請參閱取得新版本和更新的通知。

透過 Amazon 監控受管規則群組的到期排程 CloudWatch

1. 在中 CloudWatch，找出受管規則群組 AWS WAF 的到期量度。量度具有下列量度名稱和維度：
   - 指標名稱：DaysToExpiry
   - 公制維度：RegionManagedRuleGroup、Vendor、和 Version

   如果您的 Web ACL 中有評估流量的受管規則群組，您將會取得該群組的指標。您不使用的規則群組無法使用量度。
2. 針對您感興趣的指標設定警示，以便您及時收到切換至較新版本的規則群組的通知。

如需使用 Amazon 指 CloudWatch 標和設定警示的相關資訊，請參閱 Amazon 使用 CloudWatch 者指南。

JSON 和 YAML 中的受管規則群組設定範例

API 和 CLI 呼叫會傳回受管規則群組中所有規則的清單，您可以在 JSON 模型中或透過參照這些規則 AWS CloudFormation。

JSON

您可以使用 JSON 在規則陳述式中參考和修改受管規則群組。下列清單以 JSON 格式顯示「 AWS 受管規則」規則群組。AWSManagedRulesCommonRuleSetRuleActionOverrides規格會列出其作業已被覆寫為的規則Count。

```
{
    "Name": "AWS-AWSManagedRulesCommonRuleSet",
    "Priority": 0,
    "Statement": {
      "ManagedRuleGroupStatement": {
        "VendorName": "AWS",
        "Name": "AWSManagedRulesCommonRuleSet",
        "RuleActionOverrides": [

          {

            "ActionToUse": {

              "Count": {}

            },

            "Name": "NoUserAgent_HEADER"

          }

        ],
        "ExcludedRules": []
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesCommonRuleSet"
    }
}
```

YAML

您可以使用 AWS CloudFormation YAML 範本參照和修改規則陳述式中的受管規則群組。下列清單顯示 AWS CloudFormation 範本中的「 AWS 受管規則」規則群

組。AWSManagedRulesCommonRuleSetRuleActionOverrides規格會列出其作業已被覆寫為的規則Count。

```
Name: AWS-AWSManagedRulesCommonRuleSet
Priority: 0
Statement:
  ManagedRuleGroupStatement:
    VendorName: AWS
    Name: AWSManagedRulesCommonRuleSet
    RuleActionOverrides:
    - ActionToUse:
        Count: {}
      Name: NoUserAgent_HEADER
    ExcludedRules: []
OverrideAction:
  None: {}
VisibilityConfig:
  SampledRequestsEnabled: true
  CloudWatchMetricsEnabled: true
  MetricName: AWS-AWSManagedRulesCommonRuleSet
```

AWS 的受管規則 AWS WAF

AWS 託管規則 AWS WAF 是一種受管理的服務，可針對常見的應用程式弱點或其他不需要的流量提供保護 您可以選擇從每個 Web ACL 的 AWS 受管規則中選取一或多個規則群組，直到最大 Web ACL 容量單位 (WCU) 限制為止。

緩解誤判和測試規則群組變更

在生產環境中使用任何受管規則群組之前，請根據中的指導，在非生產環境中對其進行測試和調整您的 AWS WAF 保護測試。當您將規則群組新增至 Web ACL、測試規則群組的新版本，以及每當規則群組未根據需要處理您的網路流量時，請遵循測試和調整指引。

共同的安全責任

AWS 受管規則旨在保護您免受常見網頁威脅的侵害。根據文件使用時， AWS Managed Rules 規則群組會為您的應用程式新增另一層安全性。不過， AWS 受管規則群組並不是用來取代您的安全性責任，而這些責任是由您選取的 AWS 資源所決定。請參閱「共同責任模型」，以確保中的資源受到 AWS 適當的保護。

AWS 受管規則規則群組清單

我們針對 AWS Managed Rules 規則群組中的規則發佈的資訊旨在為您提供足夠的資訊來使用規則，同時不提供不良行為者可用來規避規則的資訊。如果您需要的資訊超過本文件中所找到的資訊，請聯絡本中AWS Support 心。

本節說明「 AWS 受管規則」規則群組的最新版本。當您將受管規則群組新增至 Web ACL 時，您會在主控台上看到這些項目。透過 API，您可以擷取此清單以及透過呼叫訂閱的 AWS Marketplace 受管規則群組`ListAvailableManagedRuleGroups`。

> **Note**
>
> 如需有關擷取 AWS 受管規則規則群組版本的資訊，請參閱擷取受管規則群組的可用版本。

所有 AWS 受管規則規則群組都支援標籤，而本節中列出的規則包括標籤規格。您可以透過呼叫 API 擷取受管規則群組的標籤`DescribeManagedRuleGroup`。標示會在回應中列示在AvailableLabels性質中。如需標示的資訊，請參閱AWS WAF 標籤, 上, 网, 請求。

在將保護用於生產流量之前，請先測試和調整 AWS WAF 保護措施的任何變更。如需相關資訊，請參閱測試和調整您的 AWS WAF 保護。

AWS 受管規則規則群組

- 基準規則群組
  - 核心規則集 (CRS) 受管規則群組
  - 管理員保護受管規則群組
  - 已知錯誤輸入受管規則群組
- 使用案例特定的規則群組
  - SQL 資料庫管理的規則群組
  - Linux 作業系統管理規則群組
  - POSIX 作業系統受管規則群組
  - Windows 作業系統受管理規則群組
  - PHP 應用程式管理規則群組
  - WordPress 應用程式管理規則群
- IP 評價規則群組
  - Amazon IP 信譽清單受管規則群組

- 匿名 IP 清單管理規則群組
- AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）規則組
  - 使用此規則群組的注意事項
  - 此規則群組新增的標籤
    - 令牌標籤
    - ACFP 標籤
  - 帳戶創建欺詐預防規則列表
- AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組
  - 使用此規則群組的注意事項
  - 此規則群組新增的標籤
    - 令牌標籤
    - 可承諾量標
  - 帳戶接管防止規則清單
- AWS WAF 機器人控制規則群組
  - 防護等級
  - 使用此規則群組的注意事項
  - 此規則群組新增的標籤
    - 令牌標籤
    - 機器人控制標籤
  - 機器人控制規則清單

基準規則群組

基準管理的規則群組可針對各種常見威脅提供一般防護。選擇這些規則群組中的一或多個，以建立資源的基準保護。

> **Note**
>
> 我們針對 AWS Managed Rules 規則群組中的規則發佈的資訊旨在為您提供足夠的資訊來使用規則，同時不提供不良行為者可用來規避規則的資訊。如果您需要的資訊超過本文件中所找到的資訊，請聯絡本中AWS Support 心。

核心規則集 (CRS) 受管規則群組

VendorName:AWS, 名稱:AWSManagedRulesCommonRuleSet, 中央大學:700

核心規則集 (CRS) 規則群組包含通常適用於 Web 應用程式的規則。這提供了防止利用各種漏洞的保護，包括 OWASP 出版物中描述的一些高風險和常見漏洞，例如 O WASP Top 10。請考慮針對任何使 AWS WAF 用案例使用此規則群組。

此受管規則群組會將標籤新增至其評估的 Web 要求，這些要求適用於在 Web ACL 中此規則群組之後執行的規則。 AWS WAF 還將標籤記錄到 Amazon CloudWatch 指標。如需有關標籤和標籤量度的一般資訊，請參閱網頁要求上的標籤和標示量度和維度。

> **Note**
>
> 此表格說明此規則群組的最新靜態版本。對於其他版本，請使用 API 命令DescribeManagedRuleGroup。

規則名稱	說明和標籤
NoUserAgent_HEADER	檢查是否有遺漏 HTTP User-Agent 標頭的要求。 規則動作：Block 標籤：awswaf:managed:aws:core-rule-set:NoUserAgent_Header
UserAgent_BadBots_HEADER	檢查是否有常見的User-Agent 標頭值，這些值表示要求是錯誤的機器人。範例模式包括 nessus 和 nmap。如需機器人管理，另請參閱AWS WAF 機器人控制規則群組。 規則動作：Block 標籤：awswaf:managed:aws:core-rule-set:BadBots_Header

規則名稱	說明和標籤
SizeRestrictions_QUERYSTRING	檢查超過 2,048 個位元組的 URI 查詢字串。 規則動作：Block 標籤：awswaf:managed:aws:core-rule-set:SizeRestrictions_QueryString
SizeRestrictions_Cookie_HEADER	檢查是否有超過 10,240 個位元組的 Cookie 標頭。 規則動作：Block 標籤：awswaf:managed:aws:core-rule-set:SizeRestrictions_Cookie_Header
SizeRestrictions_BODY	檢查超過 8 KB (8,192 位元組) 的要求主體。 規則動作：Block 標籤：awswaf:managed:aws:core-rule-set:SizeRestrictions_Body
SizeRestrictions_URIPATH	檢查超過 1,024 個位元組的 URI 路徑。 規則動作：Block 標籤：awswaf:managed:aws:core-rule-set:SizeRestrictions_URIPath

規則名稱	說明和標籤
EC2MetaDataSSRF_BODY	檢查是否嘗試從請求主體洩漏 Amazon EC2 中繼資料。 **Warning** 此規則只會檢查要求主體，最多可達到 Web ACL 和資源類型的主體大小限制。對於 Application Load Balancer AWS AppSync，限制固定為 8 KB。對於 CloudFront API Gateway、Amazon Cognito、應用程式執行器和驗證存取，預設限制為 16 KB，您可以在 Web ACL 組態中將限制增加到 64 KB。此規則會使用超大內容處理Continue選項。如需詳細資訊，請參閱 處理超大請求組件 AWS WAF。 規則動作：Block 標籤：awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Body
EC2MetaDataSSRF_COOKIE	檢查是否嘗試從請求 Cookie 洩漏 Amazon EC2 中繼資料。 規則動作：Block 標籤：awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Cookie

規則名稱	說明和標籤
EC2MetaDataSSRF_URIPATH	檢查是否嘗試從請求 URI 路徑洩漏 Amazon EC2 中繼資料。 規則動作：Block 標籤：awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_URIPath
EC2MetaDataSSRF_QUERYARGUMENTS	檢查是否嘗試從請求查詢引數洩漏 Amazon EC2 中繼資料。 規則動作：Block 標籤：awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_QueryArguments
GenericLFI_QUERYARGUMENTS	檢查查詢引數中是否存在本機檔案包含 (LFI) 漏洞。範例包括使用 ../../ 之類技術的路徑遍訪嘗試。 規則動作：Block 標籤：awswaf:managed:aws:core-rule-set:GenericLFI_QueryArguments
GenericLFI_URIPATH	檢查 URI 路徑中是否存在本機檔案包含 (LFI) 漏洞。範例包括使用 ../../ 之類技術的路徑遍訪嘗試。 規則動作：Block 標籤：awswaf:managed:aws:core-rule-set:GenericLFI_URIPath

規則名稱	說明和標籤
GenericLFI_BODY	檢查要求主體中是否存在本機檔案包含 (LFI) 漏洞。範例包括使用 ../../ 之類技術的路徑遍訪嘗試。 **Warning** 此規則只會檢查要求主體，最多可達到 Web ACL 和資源類型的主體大小限制。對於 Application Load Balancer AWS AppSync，限制固定為 8 KB。對於 CloudFront API Gateway、Amazon Cognito、應用程式執行器和驗證存取，預設限制為 16 KB，您可以在 Web ACL 組態中將限制增加到 64 KB。此規則會使用超大內容處理Continue選項。如需詳細資訊，請參閱 處理超大請求組件 AWS WAF。 規則動作：Block 標籤：awswaf:managed:aws:core-rule-set:GenericLFI_Body
RestrictedExtensions_URIPATH	檢查 URI 路徑包含不安全讀取或執行的系統檔案副檔名的要求。範例模式包括 .log 和 .ini 之類的副檔名。 規則動作：Block 標籤：awswaf:managed:aws:core-rule-set:RestrictedExtensions_URIPath

規則名稱	說明和標籤
RestrictedExtensions_QUERYARGUMENTS	檢查查詢引數包含不安全讀取或執行的系統副檔名的要求。範例模式包括 .log 和 .ini 之類的副檔名。 規則動作：Block 標籤：awswaf:managed:aws:core-rule-set:RestrictedExtensions_QueryArguments
GenericRFI_QUERYARGUMENTS	透過內嵌包含 IPv4 位址的 URL，檢查所有查詢參數的值是否嘗試在 Web 應用程式中利用 RFI (遠端檔案包含)。範例包括惡意利用嘗試中具有 IPv4 主機標頭的模式file://，例如http://、、、和。https:// ftp:// ftps:// 規則動作：Block 標籤：awswaf:managed:aws:core-rule-set:GenericRFI_QueryArguments

規則名稱	說明和標籤
GenericRFI_BODY	透過內嵌包含 IPv4 位址的 URL，檢查要求內文是否嘗試在 Web 應用程式中利用 RFI (遠端檔案包含)。範例包括惡意利用嘗試中具有 IPv4 主機標頭的模式`file://`，例如`http://`、、、和。`https://` `ftp://` `ftps://` **Warning** 此規則只會檢查要求主體，最多可達到 Web ACL 和資源類型的主體大小限制。對於 Application Load Balancer AWS AppSync，限制固定為 8 KB。對於 CloudFront API Gateway、Amazon Cognito、應用程式執行器和驗證存取，預設限制為 16 KB，您可以在 Web ACL 組態中將限制增加到 64 KB。此規則會使用超大內容處理`Continue`選項。如需詳細資訊，請參閱 處理超大請求組件 AWS WAF。 規則動作：Block 標籤：`awswaf:managed:aws:core-rule-set:GenericRFI_Body`

規則名稱	說明和標籤
GenericRFI_URIPATH	透過內嵌包含 IPv4 位址的 URL，檢查 URI 路徑是否嘗試在 Web 應用程式中利用 RFI (遠端檔案包含)。範例包括惡意利用嘗試中具有 IPv4 主機標頭的模式`file://`，例如`http://`、、、和。`https://` `ftp://` `ftps://` 規則動作：Block 標籤：`awswaf:managed:aws:core-rule-set:GenericRFI_URIPath`
CrossSiteScripting_COOKIE	使用內建功能檢查 Cookie 標頭的值是否有常見的跨網站指令碼 (XSS) 模式。 AWS WAF 跨網站指令碼攻擊規則陳述式範例模式包括 `<script>alert("hello")</script>` 之類的指令碼。 **Note** 此規則群組的 2.0 版不會填入 AWS WAF 記錄檔中的規則符合詳細資料。 規則動作：Block 標籤：`awswaf:managed:aws:core-rule-set:CrossSiteScripting_Cookie`

規則名稱	說明和標籤
`CrossSiteScripting_QUERYARGUMENTS`	檢查查詢引數的值是否有使用內建的常見跨網站指令碼 (XSS) 模式。 AWS WAF 跨網站指令碼攻擊規則陳述式範例模式包括 `<script>alert("hello")</script>` 之類的指令碼。 **Note** 此規則群組的 2.0 版不會填入 AWS WAF 記錄檔中的規則符合詳細資料。 規則動作：Block 標籤：`awswaf:managed:aws:core-rule-set:CrossSiteScripting_QueryArguments`

規則名稱	說明和標籤
`CrossSiteScripting_BODY`	使用內建的檢查要求主體是否有常見的跨網站指令碼 (XSS) 模式。 AWS WAF 跨網站指令碼攻擊規則陳述式範例模式包括 `<script>alert("hello")</script>` 之類的指令碼。 **Note** 此規則群組的 2.0 版不會填入 AWS WAF 記錄檔中的規則符合詳細資料。 **Warning** 此規則只會檢查要求主體，最多可達到 Web ACL 和資源類型的主體大小限制。對於 Application Load Balancer AWS AppSync，限制固定為 8 KB。對於 CloudFront API Gateway、Amazon Cognito、應用程式執行器和驗證存取，預設限制為 16 KB，您可以在 Web ACL 組態中將限制增加到 64 KB。此規則會使用超大內容處理`Continue`選項。如需詳細資訊，請參閱 處理超大請求組件 AWS WAF。 規則動作：Block 標籤：`awswaf:managed:aws:core-rule-set:CrossSiteScripting_Body`

規則名稱	說明和標籤
`CrossSiteScripting_URIPATH`	檢查 URI 路徑的值是否有使用內建的常見跨網站指令碼 (XSS) 模式。 AWS WAF 跨網站指令碼攻擊規則陳述式範例模式包括 `<script>alert("hello")</script>` 之類的指令碼。 **Note** 此規則群組的 2.0 版不會填入 AWS WAF 記錄檔中的規則符合詳細資料。 規則動作：Block 標籤：`awswaf:managed:aws:core-rule-set:CrossSiteScripting_URIPath`

管理員保護受管規則群組

VendorName:AWS, 名稱:AWSManagedRulesAdminProtectionRuleSet, 中央大學:100

管理員保護規則群組包含的規則可讓您封鎖對公開的管理頁面的外部存取。如果您執行第三方軟體，或想要降低惡意行為者取得應用程式系統管理存取權的風險，這可能會很有用。

此受管規則群組會將標籤新增至其評估的 Web 要求，這些要求適用於在 Web ACL 中此規則群組之後執行的規則。 AWS WAF 還將標籤記錄到 Amazon CloudWatch 指標。如需有關標籤和標籤量度的一般資訊，請參閱網頁要求上的標籤和標示量度和維度。

Note

此表格說明此規則群組的最新靜態版本。對於其他版本，請使用 API 命令DescribeManagedRuleGroup。

規則名稱	說明和標籤
AdminProtection_URIPATH	檢查通常保留用於管理 Web 伺服器或應用程式的 URI 路徑。範例模式包括 sqlmanager 。 規則動作：Block 標籤：awswaf:managed:aws:admin-protection:AdminProtection_URIPath

已知錯誤輸入受管規則群組

VendorName:AWS, 名稱:AWSManagedRulesKnownBadInputsRuleSet, 中央大學:200

已知錯誤輸入規則群組包含的規則可封鎖已知無效且與利用或發現的漏洞相關的請求模式。這有助於降低惡意行為者發現易受攻擊應用程式的風險。

此受管規則群組會將標籤新增至其評估的 Web 要求，這些要求適用於在 Web ACL 中此規則群組之後執行的規則。 AWS WAF 還將標籤記錄到 Amazon CloudWatch 指標。如需有關標籤和標籤量度的一般資訊，請參閱網頁要求上的標籤和標示量度和維度。

> **Note**
>
> 此表格說明此規則群組的最新靜態版本。對於其他版本，請使用 API 命令DescribeManagedRuleGroup。

規則名稱	說明和標籤
JavaDeserializationRCE_HEADER	檢查 HTTP 請求標頭的鍵和值是否有指示 Java 還原序列化遠程命令執行（RCE）嘗試的模式，例如彈簧核心和雲功能 RCE 漏洞（CVE-2022-22963，CVE-2022-22965）。範例模式包括 (java.lang.Runtime).getRuntime().exec("whoami") 。

規則名稱	說明和標籤
	Warning 此規則只會檢查要求標頭的前 8 KB 或前 200 個標頭 (以先達到限制為準)，並使用`Continue`選項處理超大內容。如需詳細資訊，請參閱 處理超大請求組件 AWS WAF。 規則動作：Block 標籤：`awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Header`

規則名稱	說明和標籤
`JavaDeserializationRCE_BODY`	檢查請求主體是否有指示 Java 還原序列化遠程命令執行（RCE）嘗試的模式，例如彈簧核心和雲功能 RCE 漏洞（CVE-2022-22963，CVE-2022-22965）。範例模式包括 `(java.lang.Runtime).getRuntime().exec("whoami")` 。 **Warning** 此規則只會檢查要求主體，最多可達到 Web ACL 和資源類型的主體大小限制。對於 Application Load Balancer AWS AppSync，限制固定為 8 KB。對於 CloudFront API Gateway、Amazon Cognito、應用程式執行器和驗證存取，預設限制為 16 KB，您可以在 Web ACL 組態中將限制增加到 64 KB。此規則會使用超大內容處理`Continue`選項。如需詳細資訊，請參閱 處理超大請求組件 AWS WAF。 規則動作：Block 標籤：`awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Body`

規則名稱	說明和標籤
JavaDeserializationRCE_URIPATH	檢查請求 URI 中是否有指示 Java 還原序列化遠程命令執行（RCE）嘗試的模式，例如彈簧核心和雲功能 RCE 漏洞（CVE-2022-22963，CVE-2022-22965）。範例模式包括 (java.lang.Runtime).getRuntime().exec("whoami") 。 規則動作：Block 標籤：awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_URIPath
JavaDeserializationRCE_QUERYSTRING	檢查請求查詢字串中是否有指示 Java 還原序列化遠端命令執行 (RCE) 嘗試的模式，例如彈簧核心和雲端功能 RCE 弱點 (CVE-2022-22963, CVE-2022-22965)。範例模式包括 (java.lang.Runtime).getRuntime().exec("whoami") 。 規則動作：Block 標籤：awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_QueryString
Host_localhost_HEADER	檢查要求中的主機標頭是否有模式指出 localhost。範例模式包括 localhost 。 規則動作：Block 標籤：awswaf:managed:aws:known-bad-inputs:Host_Localhost_Header

規則名稱	說明和標籤
PROPFIND_METHOD	檢查要求中的 HTTP 方法是否有 PROPFIND，這是類似 HEAD 的方法，但有滲透 XML 物件的額外意圖。 規則動作：Block 標籤：awswaf:managed:aws:known-bad-inputs:Propfind_Method
ExploitablePaths_URIPATH	檢查 URI 路徑是否有存取可利用 Web 應用程式路徑的嘗試。範例模式包括 web-inf 之類的路徑。 規則動作：Block 標籤：awswaf:managed:aws:known-bad-inputs:ExploitablePaths_URIPath

規則名稱	說明和標籤
Log4JRCE_HEADER	檢查要求標頭的索引鍵和值是否存在 Log4j 弱點 (CVE-2021-44228、CVE-2021-45046、CVE-2021-45105)，並防止遠端程式碼執行 (RCE) 嘗試。範例模式包括 `${jndi:ldap://example.com/}` 。 **Warning** 此規則只會檢查要求標頭的前 8 KB 或前 200 個標頭 (以先達到限制為準)，並使用`Continue`選項處理超大內容。如需詳細資訊，請參閱 處理超大請求組件 AWS WAF。 規則動作：Block 標籤：`awswaf:managed:aws:known-bad-inputs:Log4JRCE_Header`
Log4JRCE_QUERYSTRING	檢查查詢字串是否存在 Log4j 弱點 (CVE-2021-44228、CVE-2021-45046、CVE-2021-45105)，並防止遠端程式碼執行 (RCE) 嘗試。範例模式包括 `${jndi:ldap://example.com/}` 。 規則動作：Block 標籤：`awswaf:managed:aws:known-bad-inputs:Log4JRCE_QueryString`

規則名稱	說明和標籤
Log4JRCE_BODY	檢查主體是否存在 Log4j 弱點 (CVE-2021-44228、CVE-2021-45046、CVE-2021-45105)，並防止遠端程式碼執行 (RCE) 嘗試進行防護。範例模式包括 `${jndi:ldap://example.com/}` 。 **Warning** 此規則只會檢查要求主體，最多可達到 Web ACL 和資源類型的主體大小限制。對於 Application Load Balancer AWS AppSync，限制固定為 8 KB。對於 CloudFront API Gateway、Amazon Cognito、應用程式執行器和驗證存取，預設限制為 16 KB，您可以在 Web ACL 組態中將限制增加到 64 KB。此規則會使用超大內容處理`Continue`選項。如需詳細資訊，請參閱 處理超大請求組件 AWS WAF。 規則動作：Block 標籤：`awswaf:managed:aws:known-bad-inputs:Log4JRCE_Body`

規則名稱	說明和標籤
Log4JRCE_URIPATH	檢查 URI 路徑是否存在邏輯漏洞（CVE-2021-44228，CVE-2021-45046，CVE-2021-45105），並防止遠程代碼執行（RCE）嘗試。範例模式包括 ${jndi:ldap://example.com/} 。 規則動作：Block 標籤：awswaf:managed:aws:known-bad-inputs:Log4JRCE_URIPath

使用案例特定的規則群組

使用案例特定的規則群組可為許多不同的 AWS WAF 使用案例提供增量保護。選擇套用至應用程式的規則群組。

> **Note**
>
> 我們針對 AWS Managed Rules 規則群組中的規則發佈的資訊旨在為您提供足夠的資訊來使用規則，同時不提供不良行為者可用來規避規則的資訊。如果您需要的資訊超過本文件中所找到的資訊，請聯絡本中AWS Support 心。

SQL 資料庫管理的規則群組

VendorName:AWS, 名稱:AWSManagedRulesSQLiRuleSet, 中央大學:200

SQL 資料庫規則群組包含的規則，可封鎖與 SQL 資料庫利用相關的請求模式，例如 SQL Injection 攻擊。這有助於防止未經授權查詢的遠端注入。如果您的應用程式會與 SQL 資料庫互動，請評估此規則群組以供使用。

此受管規則群組會將標籤新增至其評估的 Web 要求，這些要求適用於在 Web ACL 中此規則群組之後執行的規則。 AWS WAF 還將標籤記錄到 Amazon CloudWatch 指標。如需有關標籤和標籤量度的一般資訊，請參閱網頁要求上的標籤和標示量度和維度。

> **Note**
>
> 此表格說明此規則群組的最新靜態版本。對於其他版本，請使用 API 命令DescribeManagedRuleGroup。

規則名稱	說明和標籤
SQLi_QUERYARGUMENTS	使用內建 AWS WAF SQL Injection 攻擊規則陳述式的敏感度層級設定為Low，檢查所有查詢參數的值是否符合惡意 SQL 程式碼的模式。 規則動作：Block 標籤：awswaf:managed:aws:sql-database:SQLi_QueryArguments
SQLiExtendedPatterns_QUERYARGUMENTS	檢查所有查詢參數的值是否有符合惡意 SQL 程式碼的模式。規則不涵蓋此規則檢查的模式。SQLi_QUERYARGUMENTS 規則動作：Block 標籤：awswaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments
SQLi_BODY	使用內建 AWS WAF SQL Injection 攻擊規則陳述式的敏感度層級設為Low，檢查要求主體是否符合惡意 SQL 程式碼的模式。 **Warning** 此規則只會檢查要求主體，最多可達到 Web ACL 和資源類型的主體大小限制。對於 Application Load Balancer AWS AppSync，限制固定為 8 KB。對

規則名稱	說明和標籤
	於 CloudFront API Gateway、Amazon Cognito、應用程式執行器和驗證存取，預設限制為 16 KB，您可以在 Web ACL 組態中將限制增加到 64 KB。此規則會使用超大內容處理`Continue`選項。如需詳細資訊，請參閱 處理超大請求組件 AWS WAF。 規則動作：Block 標籤：`awswaf:managed:aws:sql-database:SQLi_Body`

規則名稱	說明和標籤
SQLiExtendedPatterns_BODY	檢查要求主體是否有符合惡意 SQL 程式碼的模式。規則不涵蓋此規則檢查的模式。SQLi_BODY **Warning** 此規則只會檢查要求主體，最多可達到 Web ACL 和資源類型的主體大小限制。對於 Application Load Balancer AWS AppSync，限制固定為 8 KB。對於 CloudFront API Gateway、Amazon Cognito、應用程式執行器和驗證存取，預設限制為 16 KB，您可以在 Web ACL 組態中將限制增加到 64 KB。此規則會使用超大內容處理Continue選項。如需詳細資訊，請參閱 處理超大請求組件 AWS WAF。 規則動作：Block 標籤：awswaf:managed:aws:sql-database:SQLiExtendedPatterns_Body
SQLi_COOKIE	使用內建 AWS WAF SQL Injection 攻擊規則陳述式的敏感度層級設為Low，檢查要求 Cookie 標頭是否符合惡意 SQL 程式碼的病毒碼。 規則動作：Block 標籤：awswaf:managed:aws:sql-database:SQLi_Cookie

Linux 作業系統管理規則群組

VendorName:AWS, 名稱:AWSManagedRulesLinuxRuleSet, 中央大學:200

Linux 作業系統規則群組包含的規則會封鎖與利用 Linux 特定漏洞攻擊相關的請求模式，包括 Linux 特定本機檔案包含 (LFI) 攻擊。這有助於防止攻擊暴露檔案內容，或執行攻擊者不應具有存取權限的程式碼。如果應用程式的任何部分在 Linux 上執行，則應該評估此規則群組。您應該使用此規則群組結合作業系統 規則群組。

此受管規則群組會將標籤新增至其評估的 Web 要求，這些要求適用於在 Web ACL 中此規則群組之後執行的規則。 AWS WAF 還將標籤記錄到 Amazon CloudWatch 指標。如需有關標籤和標籤量度的一般資訊，請參閱網頁要求上的標籤和標示量度和維度。

> **Note**
>
> 此表格說明此規則群組的最新靜態版本。對於其他版本，請使用 API 命令DescribeManagedRuleGroup。

規則名稱	說明和標籤
LFI_URIPATH	檢查要求路徑是否有入侵 Web 應用程式中的本機檔案包含 (LFI) 弱點的嘗試。範例模式包括 /proc/version 之類的檔案，其可以對攻擊者提供作業系統訊息。 規則動作：Block 標籤：awswaf:managed:aws:linux-os:LFI_URIPath
LFI_QUERYSTRING	檢查查詢字串的值是否嘗試惡意利用 Web 應用程式中的本機檔案包含 (LFI) 弱點。範例模式包括 /proc/version 之類的檔案，其可以對攻擊者提供作業系統訊息。 規則動作：Block

規則名稱	說明和標籤
	標籤：awswaf:managed:aws:linux-os:LFI_QueryString
LFI_HEADER	檢查要求標頭是否嘗試惡意利用 Web 應用程式中的本機檔案包含 (LFI) 弱點。範例模式包括 /proc/version 之類的檔案，其可以對攻擊者提供作業系統訊息。 **Warning** 此規則只會檢查要求標頭的前 8 KB 或前 200 個標頭 (以先達到限制為準)，並使用Continue選項處理超大內容。如需詳細資訊，請參閱 處理超大請求組件 AWS WAF。 規則動作：Block 標籤：awswaf:managed:aws:linux-os:LFI_Header

POSIX 作業系統受管規則群組

VendorName:AWS, 名稱:AWSManagedRulesUnixRuleSet, 中央大學:100

POSIX 作業系統規則群組包含的規則會封鎖與利用 POSIX 和類似 POSIX 作業系統特定漏洞相關的請求模式，包括本機檔案包含 (LFI) 攻擊。這有助於防止攻擊暴露檔案內容，或執行攻擊者不應具有存取權限的程式碼。如果應用程式的任何部分在類似 POSIX 或類似 POSIX 的作業系統，包括 Linux、AIX、HP-UX、macOS、Solaris、FreeBSD 和 OpenBSD 上執行，則應該評估此規則群組。

此受管規則群組會將標籤新增至其評估的 Web 要求，這些要求適用於在 Web ACL 中此規則群組之後執行的規則。 AWS WAF 還將標籤記錄到 Amazon CloudWatch 指標。如需有關標籤和標籤量度的一般資訊，請參閱網頁要求上的標籤和標示量度和維度。

> **Note**
>
> 此表格說明此規則群組的最新靜態版本。對於其他版本，請使用 API 命令DescribeManagedRuleGroup。

規則名稱	說明和標籤
UNIXShellCommandsVariables_QUERYSTRING	檢查查詢字串的值是否嘗試利用 Unix 系統上執行的 Web 應用程式中的命令插入、LFI 和路徑遊走弱點。範例包括 echo $HOME 和 echo $PATH 之類的模式。 規則動作：Block 標籤：awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QueryString
UNIXShellCommandsVariables_BODY	檢查要求主體是否有入侵在 Unix 系統上執行之 Web 應用程式中的命令注入、LFI 和路徑遍訪弱點的嘗試。範例包括 echo $HOME 和 echo $PATH 之類的模式。 **Warning** 此規則只會檢查要求主體，最多可達到 Web ACL 和資源類型的主體大小限制。對於 Application Load Balancer AWS AppSync，限制固定為 8 KB。對於 CloudFront API Gateway、Amazon Cognito、應用程式執行器和驗證存取，預設限制為 16 KB，您可以在 Web ACL 組態中將限制增加到 64 KB。此規則會使用超大內容處理Continue選項。如

規則名稱	說明和標籤
	需詳細資訊，請參閱 處理超大請求組件 AWS WAF。 規則動作：Block 標籤：awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_Body
UNIXShellCommandsVariables_HEADER	檢查所有請求標頭是否嘗試利用在 Unix 系統上運行的 Web 應用程序中的命令注入，LFI 和路徑遍歷漏洞。範例包括 echo $HOME 和 echo $PATH 之類的模式。 ⚠ Warning 此規則只會檢查要求標頭的前 8 KB 或前 200 個標頭 (以先達到限制為準)，並使用Continue選項處理超大內容。如需詳細資訊，請參閱 處理超大請求組件 AWS WAF。 規則動作：Block 標籤：awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_Header

Windows 作業系統受管理規則群組

VendorName:AWS, 名稱:AWSManagedRulesWindowsRuleSet, 中央大學:200

Windows 作業系統規則群組包含的規則會封鎖與 Windows 特定弱點 (例如遠端執行 PowerShell 命令) 相關聯的要求模式。這有助於防止惡意利用漏洞，這些漏洞允許攻擊者執行未經授權的命令或執行惡意程式碼。如果應用程式的任何部分在 Windows 作業系統上執行，請評估此規則群組。

此受管規則群組會將標籤新增至其評估的 Web 要求，這些要求適用於在 Web ACL 中此規則群組之後執行的規則。 AWS WAF 還將標籤記錄到 Amazon CloudWatch 指標。如需有關標籤和標籤量度的一般資訊，請參閱網頁要求上的標籤和標示量度和維度。

> **Note**
>
> 此表格說明此規則群組的最新靜態版本。對於其他版本，請使用 API 命令DescribeManagedRuleGroup。

規則名稱	說明和標籤
`WindowsShellCommands_COOKIE`	檢查 Web 應用程序中的 WindowsShell 命令注入嘗試的請求 cookie 標頭。符合樣式代表 WindowsShell 指令。範例模式包括`||nslookup` 和`;cmd`。 規則動作：Block 標籤：`awswaf:managed:aws:windows-os:WindowsShellCommands_Cookie`
`WindowsShellCommands_QUERYARGUMENTS`	檢查 Web 應用程式中WindowsShell 指令插入嘗試的所有查詢參數值。符合樣式代表 WindowsShell 指令。範例模式包括`||nslookup` 和`;cmd`。 規則動作：Block 標籤：`awswaf:managed:aws:windows-os:WindowsShellCommands_QueryArguments`
`WindowsShellCommands_BODY`	

規則名稱	說明和標籤
	檢查 Web 應用程序中的 WindowsShell 命令注入嘗試的請求主體。符合樣式代表 WindowsShell 指令。範例模式包括`||nslookup` 和`;cmd`。 **Warning** 此規則只會檢查要求主體，最多可達到 Web ACL 和資源類型的主體大小限制。對於 Application Load Balancer AWS AppSync，限制固定為 8 KB。對於 CloudFront API Gateway、Amazon Cognito、應用程式執行器和驗證存取，預設限制為 16 KB，您可以在 Web ACL 組態中將限制增加到 64 KB。此規則會使用超大內容處理`Continue`選項。如需詳細資訊，請參閱 處理超大請求組件 AWS WAF。 規則動作：Block 標籤：`awswaf:managed:aws:windows-os:WindowsShellCommands_Body`
`PowerShellCommands_COOKIE`	檢查 Web 應用程序中的 PowerShell 命令注入嘗試的請求 cookie 標頭。符合樣式代表PowerShell 指令。例如 `Invoke-Expression` 。 規則動作：Block 標籤：`awswaf:managed:aws:windows-os:PowerShellCommands_Cookie`

規則名稱	說明和標籤
`PowerShellCommands_QUERYARGUMENTS`	檢查 Web 應用程式中PowerShell 指令插入嘗試的所有查詢參數值。符合樣式代表PowerShell 指令。例如 `Invoke-Expression` 。 規則動作：Block 標籤：`awswaf:managed:aws:windows-os:PowerShellCommands_QueryArguments`
`PowerShellCommands_BODY`	檢查 Web 應用程序中的 PowerShell 命令注入嘗試的請求主體。符合樣式代表 PowerShell 指令。例如 `Invoke-Expression` 。 **Warning** 此規則只會檢查要求主體，最多可達到 Web ACL 和資源類型的主體大小限制。對於 Application Load Balancer AWS AppSync，限制固定為 8 KB。對於 CloudFront API Gateway、Amazon Cognito、應用程式執行器和驗證存取，預設限制為 16 KB，您可以在 Web ACL 組態中將限制增加到 64 KB。此規則會使用超大內容處理`Continue`選項。如需詳細資訊，請參閱 處理超大請求組件 AWS WAF。 規則動作：Block 標籤：`awswaf:managed:aws:windows-os:PowerShellCommands_Body`

PHP 應用程式管理規則群組

VendorName:AWS, 名稱:AWSManagedRulesPHPRuleSet, 中央大學:100

PHP 應用程式規則群組包含的規則會封鎖與利用 PHP 程式設計語言特定漏洞相關的請求模式，包括注入不安全的 PHP 函數。這有助於防止惡意利用弱點，這些弱點允許攻擊者從遠端執行未獲授權的程式碼或命令。如果您的應用程式與其互動的任何伺服器上安裝 PHP，請評估此規則群組。

此受管規則群組會將標籤新增至其評估的 Web 要求，這些要求適用於在 Web ACL 中此規則群組之後執行的規則。 AWS WAF 還將標籤記錄到 Amazon CloudWatch 指標。如需有關標籤和標籤量度的一般資訊，請參閱網頁要求上的標籤和標示量度和維度。

> **Note**
>
> 此表格說明此規則群組的最新靜態版本。對於其他版本，請使用 API 命令DescribeManagedRuleGroup。

規則名稱	說明和標籤
PHPHighRiskMethodsVariables_HEADER	檢查 PHP 腳本代碼注入嘗試的所有頭文件。範例模式包括 fsockopen 之類的函數和 $_GET 超全域變數。 **Warning** 此規則只會檢查要求標頭的前 8 KB 或前 200 個標頭 (以先達到限制為準)，並使用Continue選項處理超大內容。如需詳細資訊，請參閱 處理超大請求組件 AWS WAF。 規則動作：Block 標籤：awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_Header

規則名稱	說明和標籤
PHPHighRiskMethodsVariables_QUERYSTRING	檢查請求 URL 中的第一個?之後的所有內容，尋找 PHP 腳本代碼注入嘗試。範例模式包括 fsockopen 之類的函數和 $_GET 超全域變數。 規則動作：Block 標籤：awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_QueryString

規則名稱	說明和標籤
PHPHighRiskMethodsVariables_BODY	檢查要求主體是否有 PHP 指令碼程式碼注入嘗試。範例模式包括 fsockopen 之類的函數和 $_GET 超全域變數。 **Warning** 此規則只會檢查要求主體，最多可達到 Web ACL 和資源類型的主體大小限制。對於 Application Load Balancer AWS AppSync，限制固定為 8 KB。對於 CloudFront API Gateway、Amazon Cognito、應用程式執行器和驗證存取，預設限制為 16 KB，您可以在 Web ACL 組態中將限制增加到 64 KB。此規則會使用超大內容處理Continue選項。如需詳細資訊，請參閱 處理超大請求組件 AWS WAF。 規則動作：Block 標籤：awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_Body

WordPress 應用程式管理規則群

VendorName:AWS, 名稱:AWSManagedRulesWordPressRuleSet, 中央大學:100

WordPress 應用程式規則群組包含的規則會封鎖與惡意利用網站特定弱WordPress 點相關聯的要求模式。如果您正在執行，則應評估此規則群組WordPress。此規則群組應結合 SQL 資料庫 和 PHP 應用程式 規則群組使用。

此受管規則群組會將標籤新增至其評估的 Web 要求，這些要求適用於在 Web ACL 中此規則群組之後執行的規則。 AWS WAF 還將標籤記錄到 Amazon CloudWatch 指標。如需有關標籤和標籤量度的一般資訊，請參閱網頁要求上的標籤和標示量度和維度。

> **Note**
>
> 此表格說明此規則群組的最新靜態版本。對於其他版本，請使用 API 命令DescribeManagedRuleGroup。

規則名稱	說明和標籤
`WordPressExploitableCommands_QUERYSTRING`	檢查請求查詢字串是否有可能在易受攻擊的安裝或外掛程式中利用的高風險WordPress 命令。範例模式包括 `do-reset-wordpress` 之類的命令。 規則動作：Block 標籤：`awswaf:managed:aws:wordpress-app:WordPressExploitableCommands_QUERYSTRING`
`WordPressExploitablePaths_URIPATH`	檢查請求 URI 路徑中的 WordPress 文件`xmlrpc.php` ，例如，這些文件已知具有易於利用的漏洞。 規則動作：Block 標籤：`awswaf:managed:aws:wordpress-app:WordPressExploitablePaths_URIPATH`

IP 評價規則群組

IP 信譽規則群組會根據其來源 IP 位址封鎖要求。

> **Note**
>
> 這些規則使用來自 Web 請求來源的來源 IP 位址。如果您有通過一個或多個 Proxy 或負載平衡器的流量，則 Web 請求來源將包含最後一個 Proxy 的位址，而不是用戶端的原始位址。

如果您要減少暴露於機器人流量、利用嘗試，或是對內容強制執行地理限制，請選擇一或多個這些規則群組。如需機器人管理，另請參閱AWS WAF 機器人控制規則群組。

此類別中的規則群組不提供版本控制或 SNS 更新通知。

> **Note**
>
> 我們針對 AWS Managed Rules 規則群組中的規則發佈的資訊旨在為您提供足夠的資訊來使用規則，同時不提供不良行為者可用來規避規則的資訊。如果您需要的資訊超過本文件中所找到的資訊，請聯絡中AWS Support 心。

Amazon IP 信譽清單受管規則群組

VendorName:AWS, 名稱:AWSManagedRulesAmazonIpReputationList, 中央大學:25

Amazon IP 評價清單規則群組包含以 Amazon 內部威脅情報為基礎的規則。如果您要封鎖通常與 Bot 或其他威脅相關聯的 IP 地址，這會很有用。封鎖這些 IP 地址有助於減輕 Bot，並降低惡意行為者發現易受攻擊應用程式的風險。

此受管規則群組會將標籤新增至其評估的 Web 要求，這些要求適用於在 Web ACL 中此規則群組之後執行的規則。 AWS WAF 還將標籤記錄到 Amazon CloudWatch 指標。如需有關標籤和標籤量度的一般資訊，請參閱網頁要求上的標籤和標示量度和維度。

規則名稱	說明和標籤
AWSManagedIPReputationList	檢查被識別為積極參與惡意活動的 IP 位址。 AWS WAF 從各種來源收集 IP 位址清單 MadPot，包括 Amazon 用來保護客戶免受網路犯罪攻擊的威脅情報工具。如需有關的更多資訊 MadPot，請參閱https://www.aboutamazon.com/news/aws/amazon-madpot-stops-cybersecurity-crime。

規則名稱	說明和標籤
	規則動作：Block 標籤：awswaf:managed:aws:amazon-ip-list:AWSManagedIPReputationList
AWSManagedReconnaissanceList	檢查來自對資源進行偵察的 IP 位址的連線。AWS 規則動作：Block 標籤：awswaf:managed:aws:amazon-ip-list:AWSManagedReconnaissanceList
AWSManagedIPDDoSList	檢查被識別為積極參與 DDoS 活動的 IP 地址。 規則動作：Count 標籤：awswaf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList

匿名 IP 清單管理規則群組

VendorName:AWS, 名稱:AWSManagedRulesAnonymousIpList, 中央大學:50

匿名 IP 清單規則群組包含封鎖允許模糊檢視者身分之服務的要求的規則。其中包括來自 VPN，代理，Tor 節點和網絡託管服務提供商的請求。如果您要篩除可能會嘗試從您應用程式隱藏自身身分的檢視器，則此規則群組相當有用。封鎖這些服務的 IP 地址能協助降低機器人，以及迴避地理區域限制的問題。

此受管規則群組會將標籤新增至其評估的 Web 要求，這些要求適用於在 Web ACL 中此規則群組之後執行的規則。 AWS WAF 還將標籤記錄到 Amazon CloudWatch 指標。如需有關標籤和標籤量度的一般資訊，請參閱網頁要求上的標籤和標示量度和維度。

規則名稱	說明和標籤
AnonymousIPList	檢查 IP 位址清單是否有已知會使用戶端資訊匿名化的來源，例如 TOR 節點、暫時代理伺服器和其他遮罩服務。 規則動作：Block 標籤：awswaf:managed:aws:anonymous-ip-list:AnonymousIPList
HostingProviderIPList	檢查來自 Web 託管和雲提供商的 IP 地址列表，這些 IP 地址不太可能獲取最終用戶流量。IP 清單不包含 AWS IP 位址。 規則動作：Block 標籤：awswaf:managed:aws:anonymous-ip-list:HostingProviderIPList

AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）規則組

VendorName:AWS, 名稱:AWSManagedRulesACFPRuleSet, 中央大學:50

AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 受管規則群組會標記並管理可能是詐騙帳戶建立嘗試的一部分的要求。規則群組會檢查用戶端傳送至應用程式註冊和帳號建立端點的帳號建立要求來達成此目的。

ACFP 規則群組會以各種方式檢查帳號建立嘗試，讓您能夠看見並控制潛在的惡意互動。規則群組使用要求 Token 來收集用戶端瀏覽器的相關資訊，以及建立帳戶建立要求時人工互動程度的相關資訊。規則群組會依據 IP 位址和用戶端工作階段彙總要求，並依據提供的帳戶資訊 (例如實體位址和電話號碼) 彙總，藉此偵測並管理大量帳戶建立嘗試。此外，規則群組會偵測並封鎖使用已遭入侵的認證建立新帳戶，這有助於保護應用程式和新使用者的安全狀態。

使用此規則群組的注意事項

此規則群組需要自訂組態，其中包括應用程式帳戶註冊和帳戶建立路徑的規格。除非另有說明，此規則群組中的規則會檢查用戶端傳送至這兩個端點的所有要求。若要設定和實作此規則群組，請參閱中的指引AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）。

> **Note**
>
> 使用此受管規則群組時，會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

此規則群組是中智慧型威脅緩和防護措施的一部分。 AWS WAF如需相關資訊，請參閱AWS WAF 智慧型威脅緩解。

為了降低成本並確保您正在管理您的網絡流量，請根據指導使用此規則組智慧型威脅緩解的最佳做法。

此規則群組無法與 Amazon Cognito 使用者集區搭配使用。您無法將使用此規則群組的 Web ACL 與使用者集區建立關聯，也無法將此規則群組新增至已與使用者集區關聯的 Web ACL。

此規則群組新增的標籤

此受管規則群組會將標籤新增至其評估的 Web 要求，這些要求適用於在 Web ACL 中此規則群組之後執行的規則。 AWS WAF 還將標籤記錄到 Amazon CloudWatch 指標。如需有關標籤和標籤量度的一般資訊，請參閱網頁要求上的標籤和標示量度和維度。

令牌標籤

此規則群組使用 AWS WAF 權杖管理，根據其權杖的狀態檢查和標 AWS WAF 記 Web 要求。 AWS WAF 使用令牌進行客戶端會話跟踪和驗證。

如需有關權杖和權杖管理的資訊，請參閱AWS WAF 網絡請求令牌。

如需此處所描述的標示元件的資訊，請參閱AWS WAF 標籤語法和命名需求。

客戶端會話標籤

標籤`awswaf:managed:token:id:`*`identifier`*包含 AWS WAF 權杖管理用來識別用戶端工作階段的唯一識別碼。如果客戶端獲取新令牌，則標識符可能會更改，例如在丟棄正在使用的令牌之後。

> **Note**
>
> AWS WAF 不報告此標籤的 Amazon CloudWatch 指標。

令牌狀態標籤：標籤命名空間前綴

令牌狀態標籤報告令牌的狀態，以及其包含的挑戰和 CAPTCHA 信息。

每個令牌狀態標籤都以下列命名空間前綴之一開始：

- awswaf:managed:token:— 用於報告令牌的一般狀態並報告令牌的挑戰信息的狀態。
- awswaf:managed:captcha:— 用於報告令牌的驗證碼信息的狀態。

權杖狀態標籤：標籤名稱

在前綴之後，標籤的其餘部分提供了詳細的令牌狀態信息：

- accepted-請求令牌存在並包含以下內容：
  - 有效的挑戰或驗證碼解決方案。
  - 未過期的挑戰或驗證碼時間戳記。
  - 對網頁 ACL 有效的網域規格。

  示例：該標籤awswaf:managed:token:accepted表示 Web 請求的令牌具有有效的挑戰解決方案，未過期的挑戰時間戳和有效的域。
- rejected— 請求令牌存在，但不符合驗收標準。

  隨著拒絕的標籤，令牌管理添加了一個自定義標籤命名空間和名稱來指示原因。
  - rejected:not_solved— 令牌缺少挑戰或驗證碼解決方案。
  - rejected:expired— 根據您的 Web ACL 配置的令牌免疫時間，令牌的挑戰或 CAPTCHA 時間戳已過期。
  - rejected:domain_mismatch— 令牌的域與 Web ACL 的令牌域配置不匹配。
  - rejected:invalid— AWS WAF 無法讀取指示的令牌。

  範例：標
  籤awswaf:managed:captcha:rejected並awswaf:managed:captcha:rejected:expired指出要求遭拒絕，因為權杖中的 CAPTCHA 時間戳記已超過 Web ACL 中設定的 CAPTCHA 權杖免疫時間。
- absent-請求沒有令牌或令牌管理器無法讀取它。

  示例：標籤awswaf:managed:captcha:absent表示請求沒有令牌。

ACFP 標籤

此規則群組會產生具有命名空間前置詞的標籤，awswaf:managed:aws:acfp:後面接著自訂命名空間和標籤名稱。規則群組可能會在要求中新增多個標籤。

您可以透過呼叫 API 擷取規則群組的所有標籤`DescribeManagedRuleGroup`。標示會在回應中列示在`AvailableLabels`性質中。

帳戶創建欺詐預防規則列表

本節列出中的 ACFP 規則以`AWSManagedRulesACFPRuleSet`及規則群組規則新增至 Web 要求的標籤。

> **Note**
>
> 我們針對 AWS Managed Rules 規則群組中的規則發佈的資訊旨在為您提供足夠的資訊來使用規則，同時不提供不良行為者可用來規避規則的資訊。如果您需要的資訊超過本文件中的資訊，請聯絡中AWS Support 心。

此規則群組中的所有規則都需要 Web 要求權杖，前兩個`UnsupportedCognitoIDP`和除外`AllRequests`。如需 Token 提供之資訊的說明，請參閱AWS WAF 令牌特徵。

除非另有說明，此規則群組中的規則會檢查用戶端傳送至您在規則群組設定中提供之帳戶註冊和帳戶建立頁面路徑的所有要求。如需有關配置此規則群組的資訊，請參閱AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）。

規則名稱	說明和標籤
`UnsupportedCognitoIDP`	檢查進入 Amazon Cognito 使用者集區的網路流量。ACFP 無法與 Amazon Cognito 使用者集區搭配使用，此規則有助於確保不使用其他 ACFP 規則群組規則來評估使用者集區流量。 規則動作：Block 標籤：`awswaf:managed:aws:acfp:unsupported:cognito_idp`
`AllRequests`	將規則動作套用至存取註冊頁面路徑的要求。您可以在設定規則群組時設定註冊頁面路徑。

規則名稱	說明和標籤
	依預設，此規則會套用Challenge至要求。透過套用此動作，規則可確保用戶端在規則群組中的其餘規則評估任何要求之前，先取得挑戰權杖。 請確定您的使用者在提交帳戶建立要求之前載入註冊頁面路徑。 憑證會由用戶端應用程式整合 SDK 以及規則動作CAPTCHA和Challenge新增至要求。為了獲得最有效的令牌獲取，我們強烈建議您使用應用程序集成 SDK。如需詳細資訊，請參閱 AWS WAF 用戶端應用整合。 規則動作：Challenge 標籤：無

規則名稱	說明和標籤
RiskScoreHigh	檢查具有 IP 地址或其他被認為是高度可疑因素的帳戶創建請求。此評估通常以多個促成因素為基礎，您可以在規則群組新增至要求的risk_score 標籤中看到這些因素。 規則動作：Block 標籤：awswaf:managed:aws:acfp:risk_score:high 該規則也可能對請求套用medium或low風險評分標籤。 如果 AWS WAF 無法成功評估 Web 要求的風險分數，則規則會新增標籤 awswaf:managed:aws:acfp:risk_score:evaluation_failed 此外，該規則還會新增包含命名空間的標籤awswaf:managed:aws:acfp:risk_score:contributor:　　，其中包括風險評分評估狀態，以及特定風險評分貢獻者的結果，例如 IP 信譽和失竊的認證評估。

規則名稱	說明和標籤
`SignalCredentialCompromised`	在失竊的認證資料庫中搜尋帳戶建立要求中提交的認證。 此規則可確保新用戶端以正面的安全狀況初始化其帳戶。 **Note** 您可以新增自訂封鎖回應，向使用者描述問題，並告訴他們如何繼續。如需相關資訊，請參閱ACFP 範例：對遭到入侵認證的自訂回應。 規則動作：Block 標籤：`awswaf:managed:aws:acfp:signal:credential_compromised` 規則群組會套用下列相關標籤，但不會對其採取任何動作，因為並非所有建立帳戶中的要求都會有認證：`awswaf:managed:aws:acfp:signal:missing_credential`

規則名稱	說明和標籤

`SignalClientHumanInteractivityAbsentLow`	檢查帳戶創建請求的令牌，以獲取指示與應用程序異常人為交互的數據。通過諸如鼠標移動和按鍵之類的交互來檢測人的交互性。如果頁面具有 HTML 表單，則人類互動性會包含與表單的互動。
	
	Note
	此規則只會檢查對帳戶建立路徑的要求，而且只有在您已實作應用程式整合 SDK 時才會進行評估。SDK 實作會被動擷取人類互動性，並將資訊儲存在要求 Token 中。如需詳細資訊，請參閱 AWS WAF 令牌特徵 及 AWS WAF 用戶端應用整合。
	
	規則動作：CAPTCHA
	
	標籤：無。規則會根據不同的因素決定相符項目，因此沒有適用於每個可能的比對案例的個別標籤。
	
	規則群組可將下列一或多個標籤套用至要求：
	
	`awswaf:managed:aws:acfp:signal:client:human_interactivity:low/medium/high`
	
	`awswaf:managed:aws:acfp:signal:client:human_interactivity:insufficient_data`
	
	`awswaf:managed:aws:acfp:signal:form_detected` .

規則名稱	說明和標籤
`SignalAutomatedBrowser`	檢查客戶端瀏覽器可能是自動化的指標的請求。 規則動作：Block 標籤：`awswaf:managed:aws:acfp:signal:automated_browser`
`SignalBrowserInconsistency`	檢查請求的令牌是否存在不一致的瀏覽器審訊數據。如需詳細資訊，請參閱 AWS WAF 令牌特徵。 規則動作：CAPTCHA 標籤：`awswaf:managed:aws:acfp:signal:browser_inconsistency`

規則名稱	說明和標籤
VolumetricIpHigh	檢查從個別 IP 位址傳送的大量帳戶建立要求。在 10 分鐘的視窗中，高容量超過 20 個請求。 **Note** 此規則套用的臨界值可能會因延遲而略有不同。對於大量，在套用規則動作之前，一些要求可能會超出限制。 規則動作：CAPTCHA 標籤：`awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:high` 此規則會將下列標籤套用至具有中等磁碟區 (每 10 分鐘視窗超過 15 個請求) 和低磁碟區 (每 10 分鐘時段超過 10 個請求) 的請求，但不會對這些請求採取任何動作：`awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:medium` 和`awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:low` 。

規則名稱	說明和標籤
VolumetricSessionHigh	檢查從單個客戶端會話發送的大量帳戶創建請求。在 30 分鐘的視窗中，高容量超過 10 個請求。 **Note** 此規則套用的臨界值可能會因延遲而略有不同。在套用規則動作之前，有些要求可能會超過限制。 規則動作：Block 標籤：`awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:high` 規則群組會將下列標籤套用至具有中等磁碟區 (每 30 分鐘視窗超過 5 個請求) 和低磁碟區 (每 30 分鐘時段超過 1 個請求) 的請求，但不對這些請求採取任何動作：`awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:medium` 和`awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:low` 。

規則名稱	說明和標籤
AttributeUsernameTraversalHigh	檢查使用不同使用者名稱的單一用戶端工作階段中，是否有高速的帳戶建立要求。高評估的臨界值在 30 分鐘內超過 10 個請求。 **Note** 此規則套用的臨界值可能會因延遲而略有不同。在套用規則動作之前，有些要求可能會超過限制。 規則動作：Block 標籤：`awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:high` 規則群組會將下列標籤套用至使用者名稱遊覽要求的中等磁碟區 (每 30 分鐘視窗超過 5 個請求) 和低磁碟區 (每 30 分鐘視窗超過 1 個請求) 的請求，但不會對這些請求採取任何動作：`awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:medium` 和。`awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:low`

規則名稱	說明和標籤
VolumetricPhoneNumberHigh	檢查使用相同電話號碼的大量帳戶建立要求。高評估的臨界值在 30 分鐘內超過 10 個請求。 **Note** 此規則套用的臨界值可能會因延遲而略有不同。在套用規則動作之前，有些要求可能會超過限制。 規則動作：Block 標籤：awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:high 規則群組會將下列標籤套用至具有中等磁碟區 (每 30 分鐘視窗超過 5 個請求) 和低磁碟區 (每 30 分鐘時段超過 1 個請求) 的請求，但不對這些請求採取任何動作：awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:medium 和awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:low 。

規則名稱	說明和標籤
`VolumetricAddressHigh`	檢查使用相同實體位址的大量帳戶建立要求。高評估的臨界值為每 30 分鐘視窗 100 個以上的要求。 **Note** 此規則套用的臨界值可能會因延遲而略有不同。在套用規則動作之前，有些要求可能會超過限制。 規則動作：Block 標籤：`awswaf:managed:aws:acfp:aggregate:volumetric:address:high`

規則名稱	說明和標籤
VolumetricAddressLow	檢查使用相同實體位址的中低量帳戶建立請求。中評估的臨界值為每 30 分鐘時段超過 50 個要求，而低評估的臨界值則為每 30 分鐘視窗 10 個以上的要求。 此規則會針對中或低磁碟區套用動作。 **Note** 此規則套用的臨界值可能會因延遲而略有不同。在套用規則動作之前，有些要求可能會超過限制。 規則動作：CAPTCHA 標籤：awswaf:managed:aws:acfp:aggregate:volumetric:address:low 或 awswaf:managed:aws:acfp:aggregate:volumetric:address:medium

規則名稱	說明和標籤
`VolumetricIPSuccessfulResponse`	檢查單一 IP 位址是否有大量成功建立帳戶的要求。此規則會將受保護資源的成功回應彙總至帳號建立請求。高評估的臨界值為每 10 分鐘視窗 10 個以上的要求。 此規則有助於防止批次處理帳號建立嘗試。它的閾值低於規則的閾值`VolumetricIpHigh` ，該規則僅計算請求。 如果您已將規則群組設定為檢查回應主體或 JSON 元件，則 AWS WAF 可以檢查這些元件類型的前 65,536 個位元組 (64 KB)，以取得成功或失敗指示器。 此規則會根據受保護資源對來自同一 IP 位址的最近登入嘗試的成功和失敗回應，將規則動作和標籤套用至來自 IP 位址的新 Web 請求。您可以定義設定規則群組時計算成功與失敗項目的方式。 **Note** AWS WAF 只會在保護 Amazon CloudFront 分發的網路 ACL 中評估此規則。 **Note** 此規則套用的臨界值可能會因延遲而略有不同。用戶端可能傳送的成功帳號建立嘗試次數超過規則在後續嘗試開始比對之前允許的要多。

規則名稱	說明和標籤
	規則動作：Block 標籤：awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:high 規則群組也會將下列相關標籤套用至要求，而不需要任何關聯的動作。所有計數均為 10 分鐘的窗口。 awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:medium 針對 5 個以上的成功要求、awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:low 1 個以上的成功要求、awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:high 超過 10 個失敗的要求、awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:medium 超過 5 個失敗的要求，以及 awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:low 1 個以上的失敗要求。

規則名稱	說明和標籤
`VolumetricSessionSuccessful Response`	檢查從受保護的資源到從單一用戶端工作階段傳送的帳號建立請求的少量成功回應。這有助於防止批次建立帳戶嘗試。低評估的臨界值為每 30 分鐘視窗 1 個以上的要求。 這有助於防止批次建立帳戶嘗試。此規則使用的臨界值低於規`VolumetricSessionHigh` 則 (僅追蹤要求)。 如果您已將規則群組設定為檢查回應主體或 JSON 元件，則 AWS WAF 可以檢查這些元件類型的前 65,536 個位元組 (64 KB)，以取得成功或失敗指示器。 此規則會根據受保護資源對來自相同用戶端工作階段最近登入嘗試的成功和失敗回應，將規則動作和標籤套用至來自用戶端工作階段的新 Web 要求。您可以定義設定規則群組時計算成功與失敗項目的方式。 **Note** AWS WAF 只會在保護 Amazon CloudFront 分發的網路 ACL 中評估此規則。 **Note** 此規則套用的臨界值可能會因延遲而略有不同。用戶端可能傳送的帳號建立失敗嘗試次數超過規則在後續嘗試開始比對之前允許的數量。

規則名稱	說明和標籤
	規則動作：Block 標籤：awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:low 規則群組也會將下列相關標籤套用至要求。所有計數均為 30 分鐘的窗口。 awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:high 針對 10 個以上的成功要awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:medium 求、超過 5 個成功要求、awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:high 超過 10 個失敗的要求、awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:medium 超過 5 個失敗的要求，以及 awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:low 1 個以上的失敗要求。

規則名稱	說明和標籤
`VolumetricSessionTokenReuseIp`	檢查帳戶創建請求是否在 5 個以上不同的 IP 地址中使用單個令牌。 **Note** 此規則套用的臨界值可能會因延遲而略有不同。在套用規則動作之前，有些要求可能會超過限制。 規則動作：Block 標籤：`awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:token_reuse:ip`

AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組

VendorName:`AWS`, 名稱:`AWSManagedRulesATPRuleSet`, 中央大學:50

AWS WAF 詐騙控制帳戶接管預防 (ATP) 受管規則群組會標記並管理可能是惡意帳戶接管嘗試一部分的要求。規則群組會檢查用戶端傳送到應用程式登入端點的登入嘗試來達成此目的。

- 請求檢查 — ATP 使您可以查看和控制異常登錄嘗試和使用被盜憑據的登錄嘗試，以防止可能導致欺詐活動的帳戶被盜。ATP 會根據其被盜的憑證資料庫檢查電子郵件和密碼組合，該資料庫會在黑暗的網路上發現新的洩漏憑證時定期更新。ATP 會依據 IP 位址和用戶端工作階段彙總資料，以偵測並封鎖傳送太多可疑要求的用戶端。
- 回應檢查 — 對於 CloudFront 分配，除了檢查內送登入請求之外，可承諾量規則群組還會檢查應用模組對登入嘗試的回應，以追蹤成功率與失敗率。使用此資訊，ATP 可以暫時封鎖發生過多登入失敗的用戶端工作階段或 IP 位址。 AWS WAF 異步執行響應檢查，因此這不會增加 Web 流量的延遲。

使用此規則群組的注意事項

此規則群組需要特定的組態。若要設定和實作此規則群組，請參閱中的指引AWS WAF 防止欺詐控制帳戶接管（ATP）。

此規則群組是中智慧型威脅緩和防護措施的一部分。 AWS WAF如需相關資訊，請參閱AWS WAF 智慧型威脅緩解。

> **Note**
>
> 使用此受管規則群組時，會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

為了降低成本並確保您正在管理您的網絡流量，請根據指導使用此規則組智慧型威脅緩解的最佳做法。

此規則群組無法與 Amazon Cognito 使用者集區搭配使用。您無法將使用此規則群組的 Web ACL 與使用者集區建立關聯，也無法將此規則群組新增至已與使用者集區關聯的 Web ACL。

此規則群組新增的標籤

此受管規則群組會將標籤新增至其評估的 Web 要求，這些要求適用於在 Web ACL 中此規則群組之後執行的規則。 AWS WAF 還將標籤記錄到 Amazon CloudWatch 指標。如需有關標籤和標籤量度的一般資訊，請參閱網頁要求上的標籤和標示量度和維度。

令牌標籤

此規則群組使用 AWS WAF 權杖管理，根據其權杖的狀態檢查和標 AWS WAF 記 Web 要求。 AWS WAF 使用令牌進行客戶端會話跟踪和驗證。

如需有關權杖和權杖管理的資訊，請參閱AWS WAF 網絡請求令牌。

如需此處所描述的標示元件的資訊，請參閱AWS WAF 標籤語法和命名需求。

客戶端會話標籤

標籤`awswaf:managed:token:id:`*`identifier`*包含 AWS WAF 權杖管理用來識別用戶端工作階段的唯一識別碼。如果客戶端獲取新令牌，則標識符可能會更改，例如在丟棄正在使用的令牌之後。

> **Note**
>
> AWS WAF 不報告此標籤的 Amazon CloudWatch 指標。

令牌狀態標籤：標籤命名空間前綴

令牌狀態標籤報告令牌的狀態，以及其包含的挑戰和 CAPTCHA 信息。

每個令牌狀態標籤都以下列命名空間前綴之一開始：

- awswaf:managed:token:— 用於報告令牌的一般狀態並報告令牌的挑戰信息的狀態。
- awswaf:managed:captcha:— 用於報告令牌的驗證碼信息的狀態。

權杖狀態標籤：標籤名稱

在前綴之後，標籤的其餘部分提供了詳細的令牌狀態信息：

- accepted-請求令牌存在並包含以下內容：
  - 有效的挑戰或驗證碼解決方案。
  - 未過期的挑戰或驗證碼時間戳記。
  - 對網頁 ACL 有效的網域規格。

  示例：該標籤awswaf:managed:token:accepted表示 Web 請求的令牌具有有效的挑戰解決方案，未過期的挑戰時間戳和有效的域。
- rejected— 請求令牌存在，但不符合驗收標準。

  隨著拒絕的標籤，令牌管理添加了一個自定義標籤命名空間和名稱來指示原因。
  - rejected:not_solved— 令牌缺少挑戰或驗證碼解決方案。
  - rejected:expired— 根據您的 Web ACL 配置的令牌免疫時間，令牌的挑戰或 CAPTCHA 時間戳已過期。
  - rejected:domain_mismatch— 令牌的域與 Web ACL 的令牌域配置不匹配。
  - rejected:invalid— AWS WAF 無法讀取指示的令牌。

  範例：標
  籤awswaf:managed:captcha:rejected並awswaf:managed:captcha:rejected:expired指出要求遭拒絕，因為權杖中的 CAPTCHA 時間戳記已超過 Web ACL 中設定的 CAPTCHA 權杖免疫時間。
- absent-請求沒有令牌或令牌管理器無法讀取它。

  示例：標籤awswaf:managed:captcha:absent表示請求沒有令牌。

可承諾量標

可承諾量管理規則群組會產生具有命名空間前置詞的標籤，awswaf:managed:aws:atp:後面接著自訂命名空間和標籤名稱

除了規則清單中註明的標籤之外，規則群組可能會新增下列任何標籤：

- awswaf:managed:aws:atp:signal:credential_compromised— 指出要求中提交的認證位於遭竊的認證資料庫中。
- awswaf:managed:aws:atp:aggregate:attribute:suspicious_tls_fingerprint— 僅適用於受保護的 Amazon CloudFront 分發。指出用戶端工作階段已傳送多個使用可疑 TLS 指紋的要求。
- awswaf:managed:aws:atp:aggregate:volumetric:session:token_reuse:ip— 指示在 5 個以上的不同 IP 位址中使用單一權杖。此規則套用的臨界值可能會因延遲而略有不同。在套用標籤之前，一些要求可能會使其超出限制。

您可以透過呼叫 API 擷取規則群組的所有標籤DescribeManagedRuleGroup。標示會在回應中列示在AvailableLabels性質中。

帳戶接管防止規則清單

本節列出中的可承諾量規則，以AWSManagedRulesATPRuleSet及規則群組規則新增至 Web 請求的標籤。

> **Note**
>
> 我們針對 AWS Managed Rules 規則群組中的規則發佈的資訊旨在為您提供足夠的資訊來使用規則，同時不提供不良行為者可用來規避規則的資訊。如果您需要的資訊超過本文件中的資訊，請聯絡中AWS Support 心。

規則名稱	說明和標籤
UnsupportedCognitoIDP	檢查進入 Amazon Cognito 使用者集區的網路流量。ATP 無法與 Amazon Cognito 使用者集區搭配使用，此規則有助於確保不使用其他 ATP 規則群組規則來評估使用者集區流量。

規則名稱	說明和標籤
	規則動作：Block 標籤：`awswaf:managed:aws:atp:unsupported:cognito_idp`
`VolumetricIpHigh`	檢查從個別 IP 位址傳送的大量要求。在 10 分鐘的視窗中，高容量超過 20 個請求。 **Note** 此規則套用的臨界值可能會因延遲而略有不同。對於大量，在套用規則動作之前，一些要求可能會超出限制。 規則動作：Block 標籤：`awswaf:managed:aws:atp:aggregate:volumetric:ip:high` 規則群組會將下列標籤套用至具有中等磁碟區 (每 10 分鐘時段超過 15 個請求) 和低磁碟區 (每 10 分鐘時段超過 10 個請求) 的請求，但不對這些請求採取任何動作：`awswaf:managed:aws:atp:aggregate:volumetric:ip:medium` 和`awswaf:managed:aws:atp:aggregate:volumetric:ip:low` 。

規則名稱	說明和標籤
`VolumetricSession`	檢查從個別用戶端工作階段傳送的大量要求。臨界值為每 30 分鐘視窗 20 個以上的請求。 此檢查僅適用於 Web 請求具有令牌時。Token 會由應用程式整合 SDK 和規則動作CAPTCHA與Challenge新增至要求。如需詳細資訊，請參閱 AWS WAF 網絡請求令牌。 **Note** 此規則套用的臨界值可能會因延遲而略有不同。在套用規則動作之前，有些要求可能會超過限制。 規則動作：Block 標籤：`awswaf:managed:aws:atp:aggregate:volumetric:session`
`AttributeCompromisedCredentials`	檢查來自使用失竊認證的相同用戶端工作階段的多個要求。 規則動作：Block 標籤：`awswaf:managed:aws:atp:aggregate:attribute:compromised_credentials`

規則名稱	說明和標籤
`AttributeUsernameTraversal`	檢查來自使用使用者名遍歷的相同用戶端工作階段的多個要求。 規則動作：Block 標籤：`awswaf:managed:aws:atp:aggregate:attribute:username_traversal`
`AttributePasswordTraversal`	檢查具有使用密碼遍歷的相同使用者名稱的多個請求。 規則動作：Block 標籤：`awswaf:managed:aws:atp:aggregate:attribute:password_traversal`
`AttributeLongSession`	檢查來自使用長期工作階段的相同用戶端工作階段的多個要求。臨界值是超過 6 小時的流量，每 30 分鐘至少有一個登入要求。 此檢查僅適用於 Web 請求具有令牌時。Token 會由應用程式整合 SDK 和規則動作CAPTCHA與Challenge新增至要求。如需詳細資訊，請參閱 AWS WAF 網絡請求令牌。 規則動作：Block 標籤：`awswaf:managed:aws:atp:aggregate:attribute:long_session`

規則名稱	說明和標籤
`TokenRejected`	檢查具有 AWS WAF 令牌管理拒絕的令牌的請求。 此檢查僅適用於 Web 請求具有令牌時。Token 會由應用程式整合 SDK 和規則動作CAPTCHA與Challenge新增至要求。如需詳細資訊，請參閱 AWS WAF 網絡請求令牌。 規則動作：Block 標籤：無。若要檢查拒絕的權杖，請使用標籤比對規則在標籤上進行比對：`awswaf:managed:token:rejected`
`SignalMissingCredential`	檢查缺少使用者名稱或密碼的認證的要求。 規則動作：Block 標籤：`awswaf:managed:aws:atp:signal:missing_credential`

規則名稱	說明和標籤
`VolumetricIpFailedLoginResponseHigh`	檢查最近成為登入嘗試失敗率過高的來源的 IP 位址。在 10 分鐘的時間內，高磁碟區是來自 IP 位址的 10 個以上失敗登入要求。 如果您已將規則群組設定為檢查回應主體或 JSON 元件，則 AWS WAF 可以檢查這些元件類型的前 65,536 個位元組 (64 KB)，以取得成功或失敗指示器。 此規則會根據受保護資源對來自同一 IP 位址的最近登入嘗試的成功和失敗回應，將規則動作和標籤套用至來自 IP 位址的新 Web 請求。您可以定義設定規則群組時計算成功與失敗項目的方式。 **Note** AWS WAF 只會在保護 Amazon CloudFront 分發的網路 ACL 中評估此規則。 **Note** 此規則套用的臨界值可能會因延遲而略有不同。用戶端可能傳送失敗的登入嘗試次數超過規則在後續嘗試開始比對之前允許的數量。 規則動作：Block

規則名稱	說明和標籤
	標籤：awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high 規則群組也會將下列相關標籤套用至要求，而不需要任何關聯的動作。所有計數均為 10 分鐘的窗口。 awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:medium 針對 5 個以上的失敗要awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:low 求、1 個以上的失敗要求、awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:high 10 個以上的成功要求、awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:medium 超過 5 個成功要求，以及 awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:low 1 個以上的成功要求。

規則名稱	說明和標籤
`VolumetricSessionFailedLoginResponseHigh`	檢查最近是否有登入嘗試失敗率過高的用戶端工作階段。在 30 分鐘的時間內，高磁碟區是來自用戶端工作階段的 10 個以上失敗登入要求。 如果您已將規則群組設定為檢查回應主體或 JSON 元件，則 AWS WAF 可以檢查這些元件類型的前 65,536 個位元組 (64 KB)，以取得成功或失敗指示器。 此規則會根據受保護資源對來自相同用戶端工作階段最近登入嘗試的成功和失敗回應，將規則動作和標籤套用至來自用戶端工作階段的新 Web 要求。您可以定義設定規則群組時計算成功與失敗項目的方式。 **Note** AWS WAF 只會在保護 Amazon CloudFront 分發的網路 ACL 中評估此規則。 **Note** 此規則套用的臨界值可能會因延遲而略有不同。用戶端可能傳送失敗的登入嘗試次數超過規則在後續嘗試開始比對之前允許的數量。 此檢查僅適用於 Web 請求具有令牌時。Token 會由應用程式整合 SDK 和規則動作CAPTCHA

規則名稱	說明和標籤
	與Challenge新增至要求。如需詳細資訊，請參閱 AWS WAF 網絡請求令牌。 規則動作：Block 標籤：awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:high 規則群組也會將下列相關標籤套用至要求，而不需要任何關聯的動作。所有計數均為 30 分鐘的窗口。 awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:medium 針對 5 個以上的失敗要awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:low 求、1 個以上的失敗要求、awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:high 10 個以上的成功要求、awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:medium 超過 5 個成功要求，以及 awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:low 1 個以上的成功要求。

AWS WAF 機器人控制規則群組

VendorName:AWS, 名稱:AWSManagedRulesBotControlRuleSet, 中央大學:50

機器人控制受管理規則群組會提供管理來自機器人要求的規則。機器人可能會消耗過多的資源，歪斜業務指標，導致停機時間並執行惡意活動。

防護等級

Bot Control 受管規則群組提供兩種保護層級，您可以從中選擇：

- 常見 — 檢測各種自我識別機器人，例如 Web 抓取框架，搜索引擎和自動瀏覽器。此層級的機器人控制保護可使用傳統機器人偵測技術 (例如靜態要求資料分析) 來識別常見的機器人。規則會標記來自這些機器人的流量，並封鎖他們無法驗證的機器人。
- 目標 — 包括共同層級保護，並針對無法自我識別的複雜機器人新增目標式偵測。有針對性的保護結合使用速率限制、CAPTCHA 以及背景瀏覽器挑戰來減輕機器人活動。
  - **TGT_**— 提供目標保護的規則名稱開頭為TGT_。所有目標保護都使用檢測技術（例如瀏覽器審訊，指紋識別和行為啟發式法）來識別不良的機器人流量。
  - **TGT_ML_**— 使用機器學習的目標保護規則的名稱開頭為TGT_ML_。這些規則使用網站流量統計資料的自動化機器學習分析，以偵測指示分散式協調機器人活動的異常行為。 AWS WAF 分析有關您網站流量的統計資料，例如時間戳記、瀏覽器特性和先前造訪的 URL，以改善 Bot Control 機器學習模型。機器學習功能預設為啟用，但您可以在規則群組設定中停用它們。停用機器學習時，AWS WAF 不會評估這些規則。

目標保護等級和以速 AWS WAF 率為基礎的規則陳述式都提供速率限制。如需兩個選項的比較，請參閱以速率為基礎的規則和目標機器人控制規則中的速率限制選項。

使用此規則群組的注意事項

此規則群組是中智慧型威脅緩和防護措施的一部分。 AWS WAF如需相關資訊，請參閱AWS WAF 智慧型威脅緩解。

> **Note**
>
> 使用此受管規則群組時，會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

為了降低成本並確保您正在管理您的網絡流量，請根據指導使用此規則組智慧型威脅緩解的最佳做法。

我們會定期更新我們的機器學習 (ML) 模型，以取得目標保護層級 ML 型規則，以改善機器人預測。以 ML 為基礎的規則的名稱開頭TGT_ML_為。如果您發現這些規則所做的機器人預測突然有重大變化，請通過您的客戶經理與我們聯繫或在AWS Support 中心提出案例。

此規則群組新增的標籤

此受管規則群組會將標籤新增至其評估的 Web 要求，這些要求適用於在 Web ACL 中此規則群組之後執行的規則。 AWS WAF 還將標籤記錄到 Amazon CloudWatch 指標。如需有關標籤和標籤量度的一般資訊，請參閱網頁要求上的標籤和標示量度和維度。

令牌標籤

此規則群組使用 AWS WAF 權杖管理，根據其權杖的狀態檢查和標 AWS WAF 記 Web 要求。 AWS WAF 使用令牌進行客戶端會話跟踪和驗證。

如需有關權杖和權杖管理的資訊，請參閱AWS WAF 網絡請求令牌。

如需此處所描述的標示元件的資訊，請參閱AWS WAF 標籤語法和命名需求。

客戶端會話標籤

標籤`awswaf:managed:token:id:`*`identifier`*包含 AWS WAF 權杖管理用來識別用戶端工作階段的唯一識別碼。如果客戶端獲取新令牌，則標識符可能會更改，例如在丟棄正在使用的令牌之後。

> **Note**
>
> AWS WAF 不報告此標籤的 Amazon CloudWatch 指標。

令牌狀態標籤：標籤命名空間前綴

令牌狀態標籤報告令牌的狀態，以及其包含的挑戰和 CAPTCHA 信息。

每個令牌狀態標籤都以下列命名空間前綴之一開始：

- `awswaf:managed:token:`— 用於報告令牌的一般狀態並報告令牌的挑戰信息的狀態。
- `awswaf:managed:captcha:`— 用於報告令牌的驗證碼信息的狀態。

權杖狀態標籤：標籤名稱

在前綴之後，標籤的其餘部分提供了詳細的令牌狀態信息：

- `accepted`-請求令牌存在並包含以下內容：
  - 有效的挑戰或驗證碼解決方案。
  - 未過期的挑戰或驗證碼時間戳記。

- 對網頁 ACL 有效的網域規格。

  示例：該標籤awswaf:managed:token:accepted表示 Web 請求的令牌具有有效的挑戰解決方案，未過期的挑戰時間戳和有效的域。

- rejected— 請求令牌存在，但不符合驗收標準。

  隨著拒絕的標籤，令牌管理添加了一個自定義標籤命名空間和名稱來指示原因。

  - rejected:not_solved— 令牌缺少挑戰或驗證碼解決方案。
  - rejected:expired— 根據您的 Web ACL 配置的令牌免疫時間，令牌的挑戰或 CAPTCHA 時間戳已過期。
  - rejected:domain_mismatch— 令牌的域與 Web ACL 的令牌域配置不匹配。
  - rejected:invalid— AWS WAF 無法讀取指示的令牌。

  範例：標籤awswaf:managed:captcha:rejected並awswaf:managed:captcha:rejected:expired指出要求遭拒絕，因為權杖中的 CAPTCHA 時間戳記已超過 Web ACL 中設定的 CAPTCHA 權杖免疫時間。

- absent-請求沒有令牌或令牌管理器無法讀取它。

  示例：標籤awswaf:managed:captcha:absent表示請求沒有令牌。

機器人控制標籤

Bot Control 受管規則群組會產生標籤，其中包含命名空間前置詞，awswaf:managed:aws:bot-control:後面接著自訂命名空間和標籤名稱 規則群組可能會在要求中新增多個標籤。

每個標籤都會反映機器人控制規則發現項目

- awswaf:managed:aws:bot-control:bot:— 與請求相關聯之機器人的相關資訊。
  - awswaf:managed:aws:bot-control:bot:name:*<name>*— 機器人名稱 (如果有的話)，例如，自訂命名空間bot:name:slurp和bot:name:pocket_parser。bot:name:googlebot
  - awswaf:managed:aws:bot-control:bot:category:*<category>*— 機器人的類別，由定義 AWS WAF，例如bot:category:search_engine和bot:category:content_fetcher。
  - awswaf:managed:aws:bot-control:bot:organization:*<organization>*— 機器人的發行者，例如，bot:organization:google.

- `awswaf:managed:aws:bot-control:bot:verified`— 用於表示可識別自身的機器人，並且機器人控制已經能夠驗證。這用於常見的理想漫遊器，並且在與類別標籤（如`bot:category:search_engine`或名稱標籤）結合使用時非常有用`bot:name:googlebot`。

  > **Note**
  >
  > 機器人控制會使用來自網頁要求來源的 IP 位址來協助判斷機器人是否已驗證。您無法將其設定為使用 AWS WAF 轉送的 IP 設定，以檢查不同的 IP 位址來源。如果您已驗證透過 Proxy 或負載平衡器路由的機器人，您可以新增在 Bot Control 規則群組之前執行的規則，以協助進行此操作。將您的新規則設定為使用轉送的 IP 位址，並明確允許來自已驗證機器人的要求。如需使用轉寄 IP 位址的相關資訊，請參閱轉送的 IP 位址。

  - `awswaf:managed:aws:bot-control:bot:user_triggered:verified`— 用於表示與經過驗證的機器人類似的機器人，但可能由最終用戶直接調用。這類機器人會被機器人控制規則視為未經驗證的機器人。
  - `awswaf:managed:aws:bot-control:bot:developer_platform:verified`— 用於表示與經過驗證的機器人相似的機器人，但開發人員平台用於腳本，例如 Google Apps 腳本。這類機器人會被機器人控制規則視為未經驗證的機器人。
  - `awswaf:managed:aws:bot-control:bot:unverified`— 用於指示可識別自身的機器人，因此可以對其進行命名和分類，但不會發布可用於獨立驗證其身份的信息。這些類型的機器人簽章可能會被偽造，因此會被視為未驗證。
- `awswaf:managed:aws:bot-control:targeted:<additional-details>` — 用於機器人控制目標保護的特定標籤。
- `awswaf:managed:aws:bot-control:signal:<signal-details>`和 `awswaf:managed:aws:bot-control:targeted:signal:<signal-details>` — 用於在某些情況下提供有關請求的其他資訊。

  以下是信號標籤的示例。這不是一個詳盡的列表：

  - `awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension`— 指示檢測有助於自動化的瀏覽器擴展，例如硒 IDE。

    每當使用者安裝此類擴充功能時，就會新增此標籤，即使他們沒有主動使用它。如果您為此實作標籤比對規則，請注意規則邏輯和動作設定中出現誤判的可能性。例如，您可以使用CAPTCHA動作

而不是使用動作，Block或者您可以將此標籤比對與其他標籤相符項目結合在一起，以提高您對自動化正在使用的信心。

- `awswaf:managed:aws:bot-control:signal:automated_browser`— 指出要求包含用戶端瀏覽器可能已自動化的指標。
- `awswaf:managed:aws:bot-control:targeted:signal:automated_browser`— 指出要求的 AWS WAF Token 包含用戶端瀏覽器可能已自動化的指標。

您可以透過呼叫 API 擷取規則群組的所有標籤`DescribeManagedRuleGroup`。標示會在回應中列示在`AvailableLabels`性質中。

Bot Control 受管規則群組會將標籤套用至一組通常允許的可驗證機器人。規則群組不會封鎖這些已驗證的機器人。如果需要，您可以透過撰寫使用 Bot Control 受管理規則群組套用之標籤的自訂規則來封鎖這些規則或其子集。如需此項目的詳細資訊和範例，請參閱AWS WAF 機器人控制。

機器人控制規則清單

本節列出機器人控制規則。

> **Note**
>
> 我們針對 AWS Managed Rules 規則群組中的規則發佈的資訊旨在為您提供足夠的資訊來使用規則，同時不提供不良行為者可用來規避規則的資訊。如果您需要的資訊超過本文件中的資訊，請聯絡中AWS Support 心。

規則名稱	描述
`CategoryAdvertising`	檢查用於廣告目的的機器人。例如，您可能會使用需要以程式設計方式存取網站的第三方廣告服務。 規則動作，僅套用至未驗證的機器人：Block 標籤：`awswaf:managed:aws:bot-control:bot:category:advertising` 對於已驗證的機器人，規則群組不會採取任何動作，但會新增規則標籤和標籤`awswaf:ma`

規則名稱	描述
	naged:aws:bot-control:bot:verified 。
CategoryArchiver	檢查用於封存目的的的機器人。這些漫遊器會抓取網頁並捕獲內容以創建存檔。 規則動作，僅套用至未驗證的機器人：Block 標籤：awswaf:managed:aws:bot-control:bot:category:archiver 對於已驗證的機器人，規則群組不會採取任何動作，但會新增規則標籤和標籤awswaf:managed:aws:bot-control:bot:verified 。
CategoryContentFetcher	檢查代表使用者造訪應用程式網站的機器人、擷取 RSS 摘要之類的內容，或驗證或驗證您的內容。 規則動作，僅套用至未驗證的機器人：Block 標籤：awswaf:managed:aws:bot-control:bot:category:content_fetcher 對於已驗證的機器人，規則群組不會採取任何動作，但會新增規則標籤和標籤awswaf:managed:aws:bot-control:bot:verified 。

規則名稱	描述
CategoryEmailClient	檢查檢查指向應用程序網站的電子郵件中的鏈接的漫遊器。這可能包括企業和電子郵件提供商運行的漫遊器，以驗證電子郵件中的鏈接並標記可疑電子郵件。 規則動作，僅套用至未驗證的機器人：Block 標籤：awswaf:managed:aws:bot-control:bot:category:email_client 對於已驗證的機器人，規則群組不會採取任何動作，但會新增規則標籤和標籤awswaf:managed:aws:bot-control:bot:verified 。
CategoryHttpLibrary	檢查是否有機器人從各種程式設計語言的 HTTP 程式庫產生的要求。這些可能包括您選擇允許或監視的 API 請求。 規則動作，僅套用至未驗證的機器人：Block 標籤：awswaf:managed:aws:bot-control:bot:category:http_library 對於已驗證的機器人，規則群組不會採取任何動作，但會新增規則標籤和標籤awswaf:managed:aws:bot-control:bot:verified 。

規則名稱	描述
CategoryLinkChecker	檢查檢查是否有損壞的連結的機器人。 規則動作，僅套用至未驗證的機器人：Block 標籤：awswaf:managed:aws:bot-control:bot:category:link_checker 對於已驗證的機器人，規則群組不會採取任何動作，但會新增規則標籤和標籤awswaf:managed:aws:bot-control:bot:verified 。
CategoryMiscellaneous	檢查與其他類別不匹配的雜項機器人。 規則動作，僅套用至未驗證的機器人：Block 標籤：awswaf:managed:aws:bot-control:bot:category:miscellaneous 對於已驗證的機器人，規則群組不會採取任何動作，但會新增規則標籤和標籤awswaf:managed:aws:bot-control:bot:verified 。

規則名稱	描述
CategoryMonitoring	檢查用於監視目的的的機器人。例如，您可以使用機器人監控服務來定期 ping 應用程式網站，以監控效能和正常運作時間等內容。 規則動作，僅套用至未驗證的機器人：Block 標籤：awswaf:managed:aws:bot-control:bot:category:monitoring 對於已驗證的機器人，規則群組不會採取任何動作，但會新增規則標籤和標籤awswaf:managed:aws:bot-control:bot:verified 。
CategoryScrapingFramework	從 Web 抓取框架中檢查漫遊器，該框架用於自動爬網和從網站中提取內容。 規則動作，僅套用至未驗證的機器人：Block 標籤：awswaf:managed:aws:bot-control:bot:category:scraping_framework 對於已驗證的機器人，規則群組不會採取任何動作，但會新增規則標籤和標籤awswaf:managed:aws:bot-control:bot:verified 。

規則名稱	描述
CategorySearchEngine	檢查搜索引擎機器人，它們會抓取網站以索引內容並使信息可用於搜索引擎結果。 規則動作，僅套用至未驗證的機器人：Block 標籤：awswaf:managed:aws:bot-control:bot:category:search_engine 對於已驗證的機器人，規則群組不會採取任何動作，但會新增規則標籤和標籤awswaf:managed:aws:bot-control:bot:verified 。
CategorySecurity	檢查可掃描 Web 應用程式中是否有漏洞或執行安全稽核的機器人。例如，您可能會使用協力廠商的安全性廠商來掃描、監控或稽核 Web 應用程式的安全性。 規則動作，僅套用至未驗證的機器人：Block 標籤：awswaf:managed:aws:bot-control:bot:category:security 對於已驗證的機器人，規則群組不會採取任何動作，但會新增規則標籤和標籤awswaf:managed:aws:bot-control:bot:verified 。

規則名稱	描述
CategorySeo	檢查用於搜索引擎優化的漫遊器。例如，您可以使用搜索引擎工具來抓取您的網站，以幫助您提高搜索引擎排名。 規則動作，僅套用至未驗證的機器人：Block 標籤：awswaf:managed:aws:bot-control:bot:category:seo 對於已驗證的機器人，規則群組不會採取任何動作，但會新增規則標籤和標籤awswaf:managed:aws:bot-control:bot:verified 。
CategorySocialMedia	檢查社交媒體平台使用的機器人，以便在用戶共享您的內容時提供內容摘要。 規則動作，僅套用至未驗證的機器人：Block 標籤：awswaf:managed:aws:bot-control:bot:category:social_media 對於已驗證的機器人，規則群組不會採取任何動作，但會新增規則標籤和標籤awswaf:managed:aws:bot-control:bot:verified 。
CategoryAI	檢查人工智慧 (AI) 機器人。 規則動作：Block 標籤：awswaf:managed:aws:bot-control:bot:category:ai

規則名稱	描述
SignalAutomatedBrowser	檢查客戶端瀏覽器可能是自動化的指標的請求。可以使用自動瀏覽器進行測試或抓取。例如，您可以使用這些類型的瀏覽器來監視或驗證您的應用程式網站。 規則動作：Block 標籤：awswaf:managed:aws:bot-control:signal:automated_browser
SignalKnownBotDataCenter	檢查機器人通常使用的資料中心指標。 規則動作：Block 標籤：awswaf:managed:aws:bot-control:signal:known_bot_data_center
SignalNonBrowserUserAgent	檢查似乎不是來自 Web 瀏覽器的用戶代理字符串。此類別可以包含 API 要求。 規則動作：Block 標籤：awswaf:managed:aws:bot-control:signal:non_browser_user_agent

規則名稱	描述
TGT_VolumetricIpTokenAbsent	在過去 5 分鐘內檢查來自客戶端的 5 個或更多請求，這些請求不包含有效的挑戰令牌。如需有關權杖的資訊，請參閱AWS WAF 網絡請求令牌。 **Note** 如果來自同一個客戶端的請求最近缺少令牌，則此規則可能會在具有令牌的請求上匹配。 此規則套用的臨界值可能會因延遲而略有不同。 此規則處理缺少的令牌與令牌標籤不同：awswaf:managed:token:absent 。令牌標記為沒有令牌的單個請求進行標籤。此規則會維護每個用戶端 IP 遺失其 Token 的要求計數，並符合超過限制的用戶端。 規則處理行動，僅套用至未通過驗證機器人的用戶端：Challenge 標籤：awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:ip:token_absent 對於已驗證的機器人，規則群組不會採取任何動作，但會新增規則標籤和標籤awswaf:managed:aws:bot-control:bot:verified 。

規則名稱	描述
TGT_VolumetricSession	在任何 5 分鐘的視窗中檢查來自用戶端工作階段的要求數量異常高。評估是基於與使用歷史流量模式 AWS WAF 維護的標準容積基準的比較。 此檢查僅適用於 Web 請求具有令牌時。Token 會由應用程式整合 SDK 和規則動作CAPTCHA與Challenge新增至要求。如需詳細資訊，請參閱 AWS WAF 網絡請求令牌。 **Note** 啟用此規則後，可能需要 5 分鐘才會生效。Bot Control 會比較目前的流量與 AWS WAF 計算的流量基準，藉此識別 Web 流量中的異常行為。 規則處理行動，僅套用至未通過驗證機器人的用戶端：CAPTCHA 標籤：`awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:high` 規則群組會將下列標籤套用至超過最小臨界值的中等數量和較低磁碟區要求。對於這些層級，無論用戶端是否已驗證，規則都不會採取任何處理行動：`awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:medium` 和`awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:low` 。

規則名稱	描述
	對於已驗證的機器人，規則群組不會採取任何動作，但會新增規則標籤和標籤awswaf:managed:aws:bot-control:bot:verified 。
TGT_SignalAutomatedBrowser	檢查請求的令牌，以獲取客戶端瀏覽器可能自動化的指標。如需詳細資訊，請參閱 AWS WAF 令牌特徵。 此檢查僅適用於 Web 請求具有令牌時。Token 會由應用程式整合 SDK 和規則動作CAPTCHA與Challenge新增至要求。如需詳細資訊，請參閱 AWS WAF 網絡請求令牌。 規則處理行動，僅套用至未通過驗證機器人的用戶端：CAPTCHA 標籤：awswaf:managed:aws:bot-control:targeted:signal:automated_browser 對於已驗證的機器人，規則群組不會採取任何動作，但會新增規則標籤和標籤awswaf:managed:aws:bot-control:bot:verified 。

規則名稱	描述
TGT_SignalBrowserInconsistency	檢查不一致的瀏覽器審訊資料。如需詳細資訊，請參閱 AWS WAF 令牌特徵。 此檢查僅適用於 Web 請求具有令牌時。Token 會由應用程式整合 SDK 和規則動作CAPTCHA與Challenge新增至要求。如需詳細資訊，請參閱 AWS WAF 網絡請求令牌。 規則處理行動，僅套用至未通過驗證機器人的用戶端：CAPTCHA 標籤：awswaf:managed:aws:bot-control:targeted:signal:browser_inconsistency 對於已驗證的機器人，規則群組不會採取任何動作，但會新增規則標籤和標籤awswaf:managed:aws:bot-control:bot:verified 。

規則名稱	描述
TGT_TokenReuseIp	檢查超過 5 個不同 IP 位址中是否使用單一權杖。 **Note** 此規則套用的臨界值可能會因延遲而略有不同。在套用規則動作之前，有些要求可能會超過限制。 規則動作：Count 標籤：awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:token_reuse:ip

規則名稱	描述
`TGT_ML_CoordinatedActivityMedium` 和 `TGT_ML_CoordinatedActivityHigh`	檢查與分散式協調機器人活動一致的異常行為。規則層級表示一組請求是協調攻擊參與者的信賴程度。 **Note** 只有在規則群組設定為使用機器學習 (ML) 時，才會執行這些規則。如需有關配置此選擇的資訊，請參閱將 AWS WAF 機器人控制受管規則群組新增至您的 Web ACL。 AWS WAF 通過對網站流量統計的機器學習分析執行此檢查。 AWS WAF 每隔幾分鐘分析一次網路流量，並最佳化分析，以偵測散佈在多個 IP 位址的低強度、長時間機器人。 在判斷協調攻擊未進行之前，這些規則可能會在少數要求上符合。所以，如果你只看到一兩個匹配，結果可能是誤報。但是，如果您看到很多符合這些規則的比賽，那麼您可能正在遭受協調的攻擊。 **Note** 使用 ML 選項啟用「機器人控制」目標規則後，這些規則最多可能需要 24 小時才會生效。Bot Control 會比較目前流量與 AWS WAF 已計算的流量基準，藉此識別 Web 流量中的異常行為。AWS WAF 只會在搭配 ML 選項使用 Bot Control 目標規則時，才會計算基

規則名稱	描述
	準，建立有意義的基準線最多可能需要 24 小時。 我們會定期更新這些規則的機器學習模型，以改善機器人預測。如果您發現這些規則所做的機器人預測發生突然且重大的變化，請聯繫您的客戶經理或在AWS Support 中心提出案例。 規則處理行動，僅套用至未經驗證機器人的用戶端： • 中型: Count • 高: Count 標籤：`awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:medium` 和 `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:high` 對於已驗證的機器人，規則群組不會採取任何動作，但會新增規則標籤和標籤`awswaf:managed:aws:bot-control:bot:verified` 。 規則群組也會新增標籤`awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low` 以指示低信賴等級，但不會套用任何規則或對這些要求採取任何動作。

版本控制的 AWS 受管規則規則群組的部署

AWS 在三個標準部署中，將變更部署至其版本控制的 AWS 受管規則規則群組：候選版本、靜態版本和預設版本。此外，有時 AWS 可能需要釋放例外部署或復原預設版本部署。

> **Note**
>
> 本節僅適用於已建立版本化的 AWS 受管規則規則群組。唯一未建立版本的規則群組是 IP 信譽規則群組。

主題

- AWS 受管規則規則群組部署的通知
- AWS 受管規則的標準部署概觀
- AWS 受管規則的典型版本狀態
- 針對 AWS 受管規則發行候選部署
- AWS 受管規則的靜態版本部署
- AWS 受管規則的預設版本部署
- AWS 受管規則的例外部署
- AWS 受管規則的預設部署復原

AWS 受管規則規則群組部署的通知

版本控制的 AWS 受管規則規則群組全部為部署提供 SNS 更新通知，而且它們都使用相同的 SNS 主題 Amazon 資源名稱 (ARN)。唯一未建立版本的規則群組是 IP 信譽規則群組。

對於影響保護的部署 (例如預設版本的變更) 會 AWS 提供 SNS 通知，以通知您計劃的部署，並在部署開始時通知您。對於不影響保護的部署，例如候選版本和靜態版本部署， AWS 可能會在部署開始後甚至在部署完成後通知您。部署完成新靜態版本後， AWS 更新本指南、文件歷史記錄頁面的AWS 受管規則變更記錄檔變更記錄檔中的文件歷史紀錄。

若要接收為 AWS 受管規則規則群組 AWS 提供的所有更新，請從本指南的任何 HTML 頁面訂閱 RSS 摘要，並訂閱 AWS 受管規則規則群組的 SNS 主題。如需訂閱 SNS 通知的相關資訊，請參閱接收受管理規則群組的新版本和更新的通知。

SNS 通知的內容

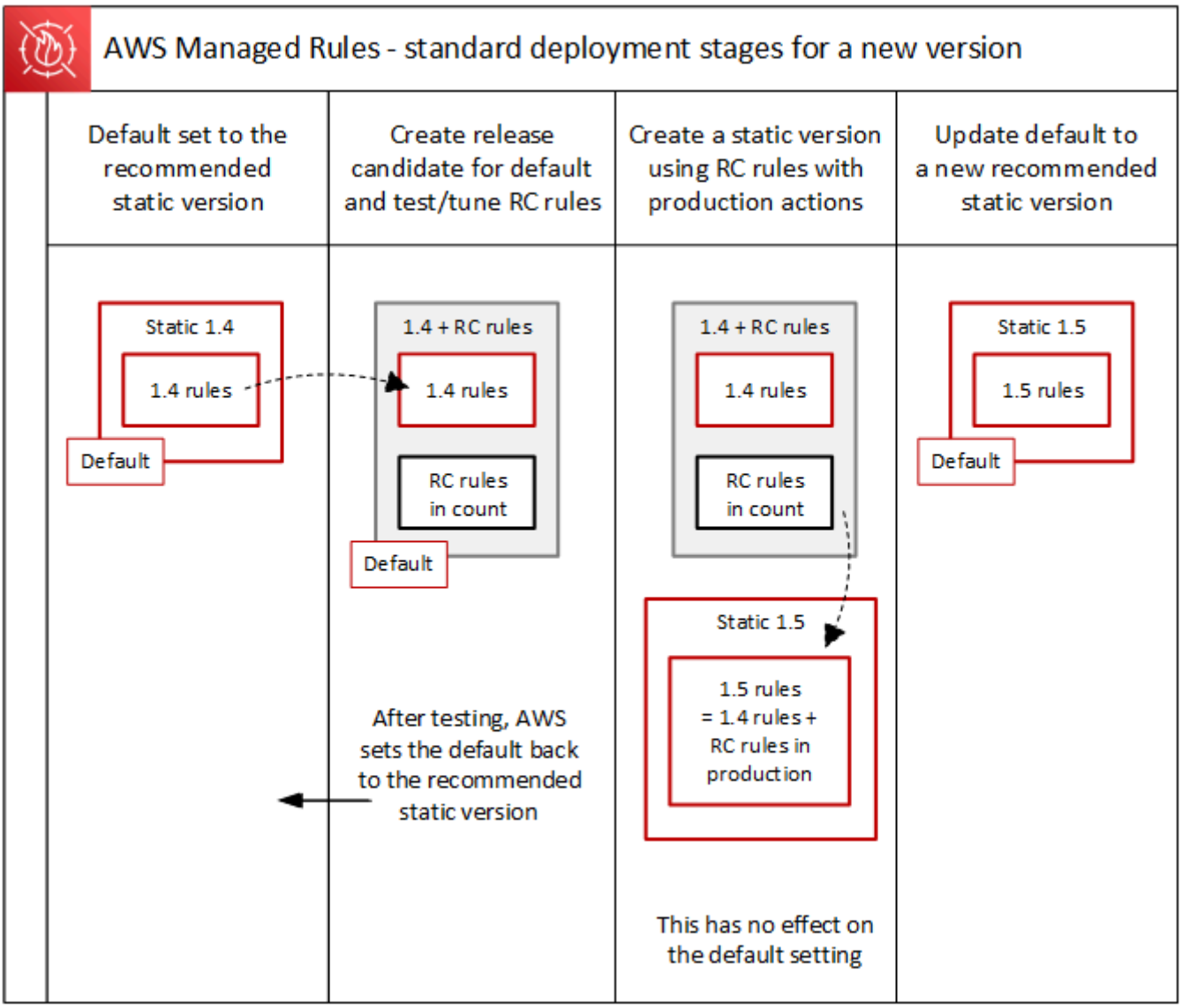
Amazon SNS 通知中的欄位一律包含主旨、訊息和 MessageAttributes。其他欄位取決於郵件類型以及通知所用的受管理規則群組。以下顯示的通知清單範例AWSManagedRulesCommonRuleSet。

```
{
    "Type": "Notification",
    "MessageId": "4286b830-a463-5e61-bd15-e1ae72303868",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:MyTopic",
    "Subject": "New version available for rule group AWSManagedRulesCommonRuleSet",
    "Message": "Welcome to AWSManagedRulesCommonRuleSet version 1.5! We've updated
 the regex specification in this version to improve protection coverage, adding
 protections against insecure deserialization. For details about this change, see
 http://updatedPublicDocs.html. Look for more exciting updates in the future! ",
    "Timestamp": "2021-08-24T11:12:19.810Z",
    "SignatureVersion": "1",
    "Signature": "EXAMPLEHXgJm...",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
f3ecfb7224c7233fe7bb5f59f96de52f.pem",
    "SubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=ConfirmSubscription&TopicArn=arn:aws:sns:us-
west-2:123456789012:MyTopic&Token=2336412f37...",
    "MessageAttributes": {
        "major_version": {
            "Type": "String",
            "Value": "v1"
        },
        "managed_rule_group": {
            "Type": "String",
            "Value": "AWSManagedRulesCommonRuleSet"
        }
    }
}
```

AWS 受管規則的標準部署概觀

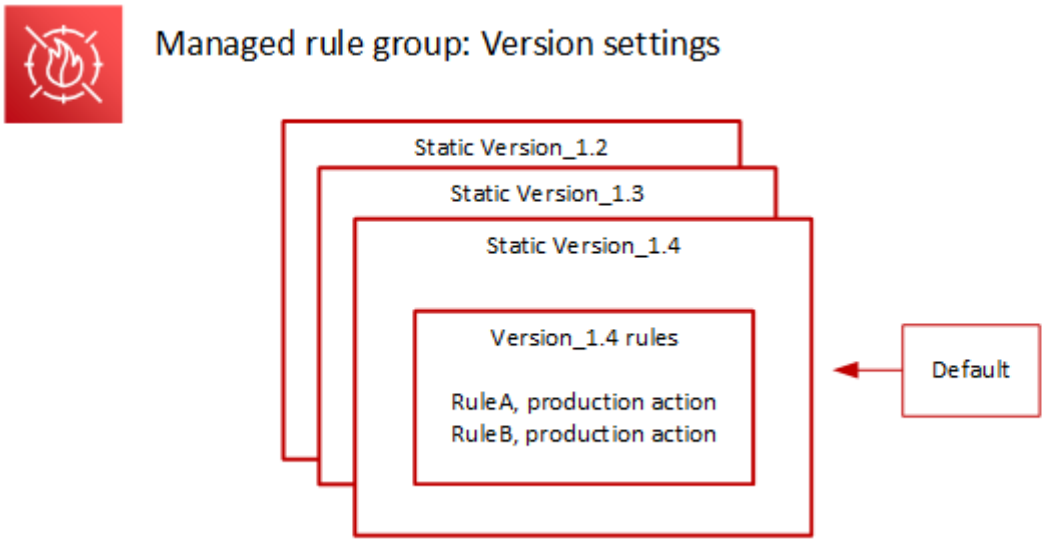
AWS 使用三個標準部署階段推出新的 AWS 受管規則功能：候選版本、靜態版本和預設版本。

下圖說明這些標準部署。以下各節將更詳細地描述每個項目。



AWS 受管規則的典型版本狀態

一般而言，已建立版本的受管理規則群組具有數個未過期的靜態版本，而預設版本會指向建議的靜態版本。 AWS 下圖顯示典型靜態版本集和預設版本設定的範例。



靜態版本中大多數規則的生產操作是Block，但它可能被設置為不同的東西。如需有關規則動作設定的詳細資訊，請參閱每個規則群組的規則清單AWS 受管規則規則群組清單。

針對 AWS 受管規則發行候選部署

當受管規則群組 AWS 有一組候選規則變更時，會在暫時候選發行版本部署中對其進行測試。 AWS 根據生產流量評估計數模式下的候選規則，並執行最終調整活動，包括緩解誤判。 AWS test 會針對使用預設規則群組預設版本的所有客戶，以這種方式發行候選規則。發行候選部署不適用於使用規則群組靜態版本的客戶。

如果您使用預設版本，候選版本部署將不會改變規則群組管理 Web 流量的方式。在測試候選規則時，您可能會注意到以下幾點：

- 預設版本名稱從變更`Default (using Version_X.Y)`為`Default (using Version_X.Y_PLUS_RC_COUNT)`。
- 在 Amazon CloudWatch 的其他計數指標與他們`RC_COUNT`的名字。這些是由發行候選規則產生的。

AWS 測試候選發行版本大約一週，然後將其移除，並將預設版本重設為目前建議的靜態版本。

AWS 針對候選版本部署執行下列步驟：

1. 建立候選版本 — 根據目前建議的靜態版本 (預設值指向的版本) AWS 新增候選發行版本。

   候選版本的名稱是附加的靜態版本名稱`_PLUS_RC_COUNT`。例如，如果目前建議的靜態版本為`Version_2.1`，則會命名候選發行版本`Version_2.1_PLUS_RC_COUNT`。

候選版本包含以下規則：

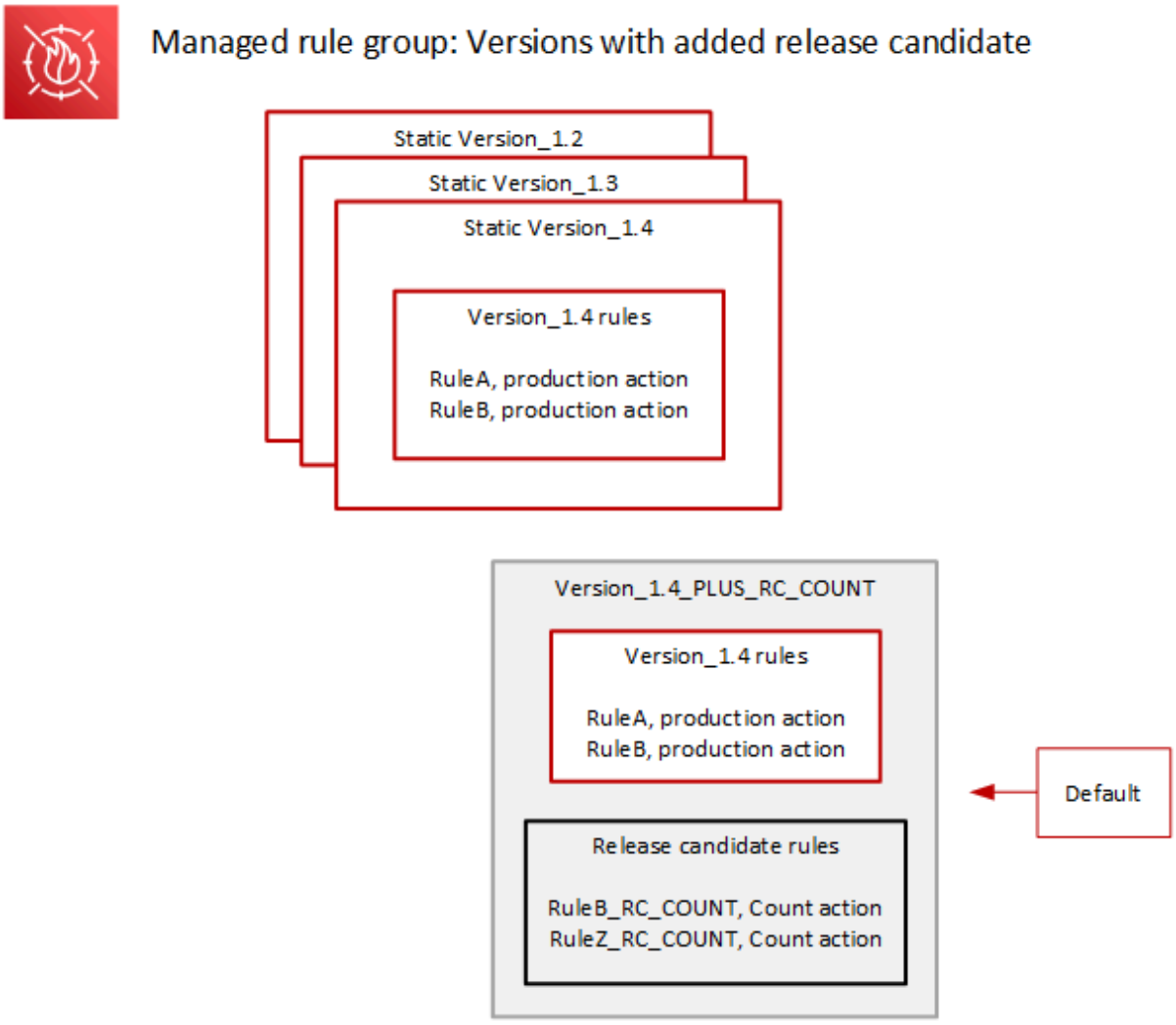
- 規則完全從目前建議的靜態版本複製而來，不會變更規則組態。
- 將規則動作設為Count且名稱結尾為的候選新規則_RC_COUNT。

  大多數候選規則會針對已存在於規則群組中的規則提供提議的改進。每個規則的名稱都是附加的現有規則名稱_RC_COUNT。

2. 將預設版本設 AWS 定為候選版本並測試 — 將預設版本設定為指向新候選發行版本，以針對您的生產流量執行測試。測試通常需要大約一周的時間。

   您會看到預設版本的名稱從僅指示靜態版本的名稱變更，例如，變更為`Default (using Version_1.4)`指示靜態版本加上候選版本規則的版本，例如`Default (using Version_1.4_PLUS_RC_COUNT)`。此命名方案可讓您識別用來管理網路流量的靜態版本。

   下圖顯示此時範例規則群組版本的狀態。



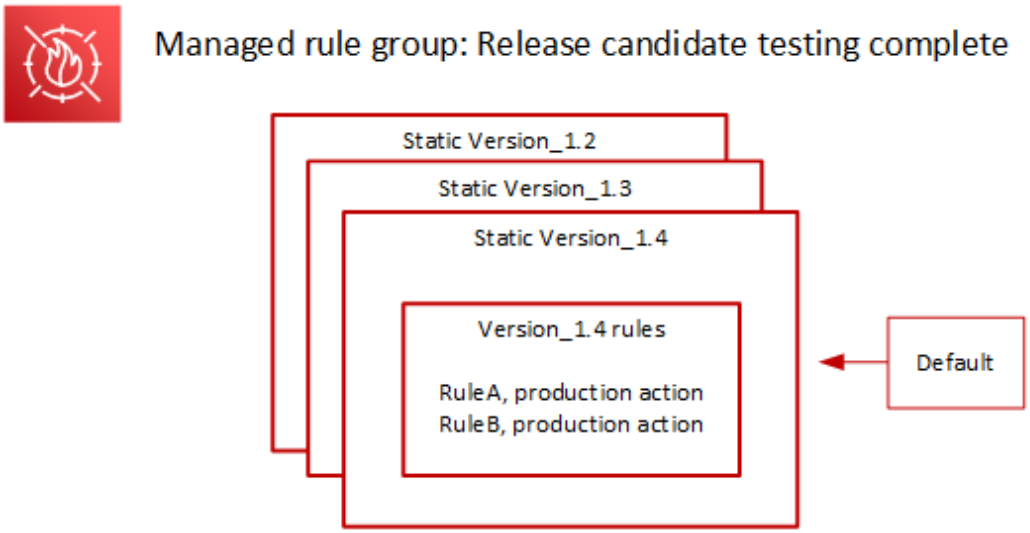
發行候選規則一律會設定Count動作，因此不會改變規則群組管理網路流量的方式。

發行候選規則會產生 Amazon CloudWatch 計數指標， AWS 用於驗證行為和識別誤判。 AWS 視需要進行調整，以調整發行候選計數規則的行為。

候選發行版本不是靜態版本，您無法從靜態規則群組版本清單中選擇。您只能在預設版本規格中查看候選版本的名稱。

3. 將預設版本恢復為建議的靜態版本 — 測試候選版本規則之後，將預設版本設 AWS 定回目前建議的靜態版本。預設版本名稱設定會刪除結_PLUS_RC_COUNT尾，而規則群組會停止產生發行候選規則的 CloudWatch 計數測量結果。這是無訊息變更，與預設版本復原的部署不同。

   下圖顯示範例規則群組版本在候選發行版本測試完成之後的狀態。



時間和通知

AWS 視需要部署發行候選版本，以測試對規則群組的改進。

- SNS — 在部署開始時 AWS 傳送 SNS 通知。該通知指出候選發行版本將接受測試的估計時間。測試完成時，無 AWS 訊息地將預設值返回靜態版本設定，而無需第二次通知。
- 變更記錄 — AWS 不會針對此類型部署更新變更記錄或本指南的其他部分。

AWS 受管規則的靜態版本部署

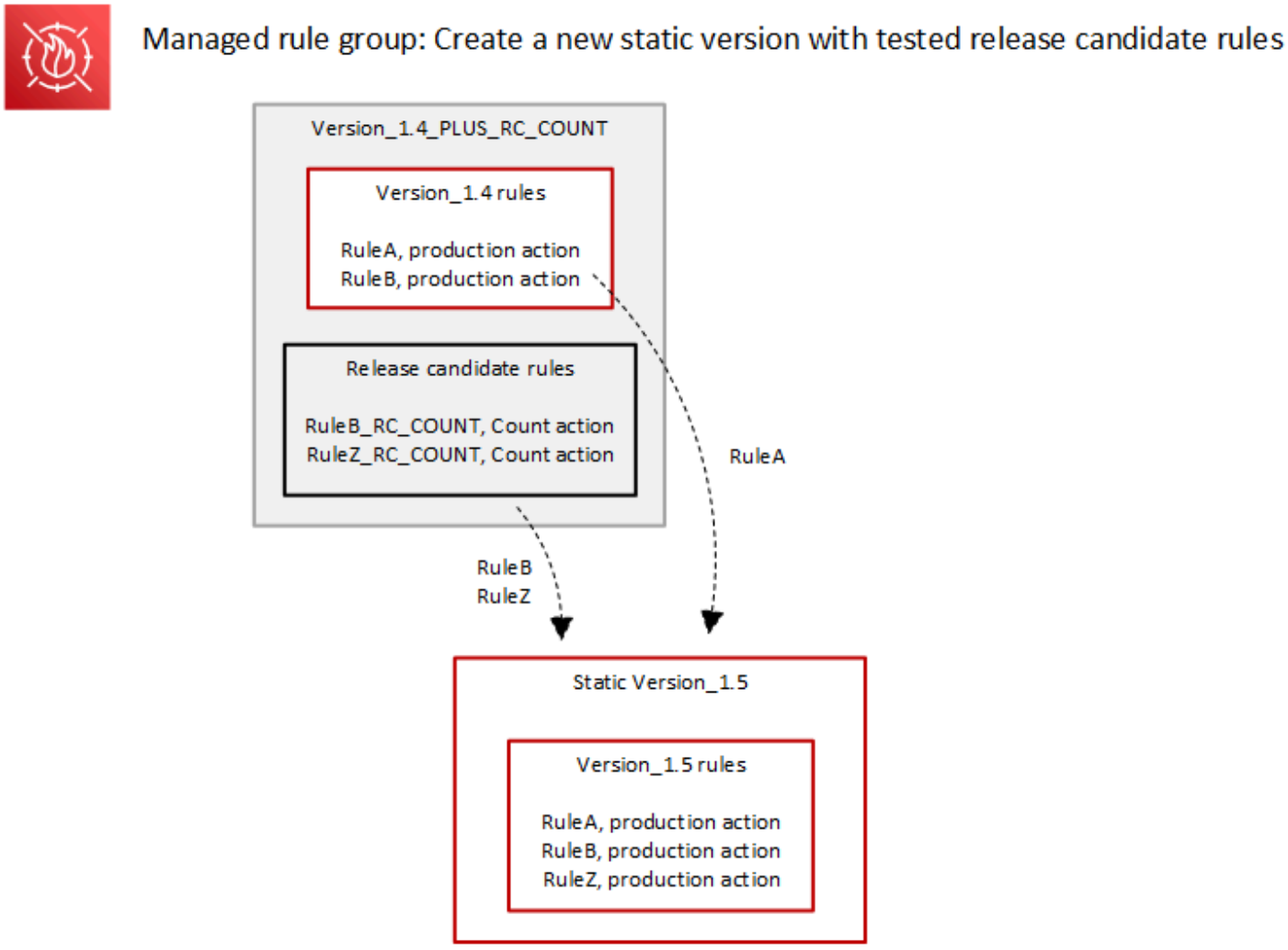
當 AWS 判斷候選版本對規則群組提供有價值的變更時，請根據候選發行版本為規則群組 AWS 部署新的靜態版本。此部署不會變更規則群組的預設版本。

新的靜態版本包含候選發行版本的以下規則：

- 先前靜態版本的規則，在發行候選規則中沒有替代候選條件。
- 發行候選規則，具有下列變更：
  - AWS 透過移除候選版本尾碼來變更規則名稱_RC_COUNT。
  - AWS 將規則動作從變更Count為其生產規則動作。

  對於取代先前現有規則的發行候選規則，這會取代新靜態版本中先前規則的功能。

下圖說明從候選發行版本建立新的靜態版本。



部署後，新的靜態版本可供您測試並在保護中使用，如果您想要的話。您可以在規則群組的規則清單中檢閱新增和更新的規則動作和說明AWS 受管規則規則群組清單。

靜態版本在部署後是不可變的，並且只有在 AWS 過期時才會更改。如需有關版本生命週期的資訊，請參閱版本化的受管理規則群組。

時間和通知

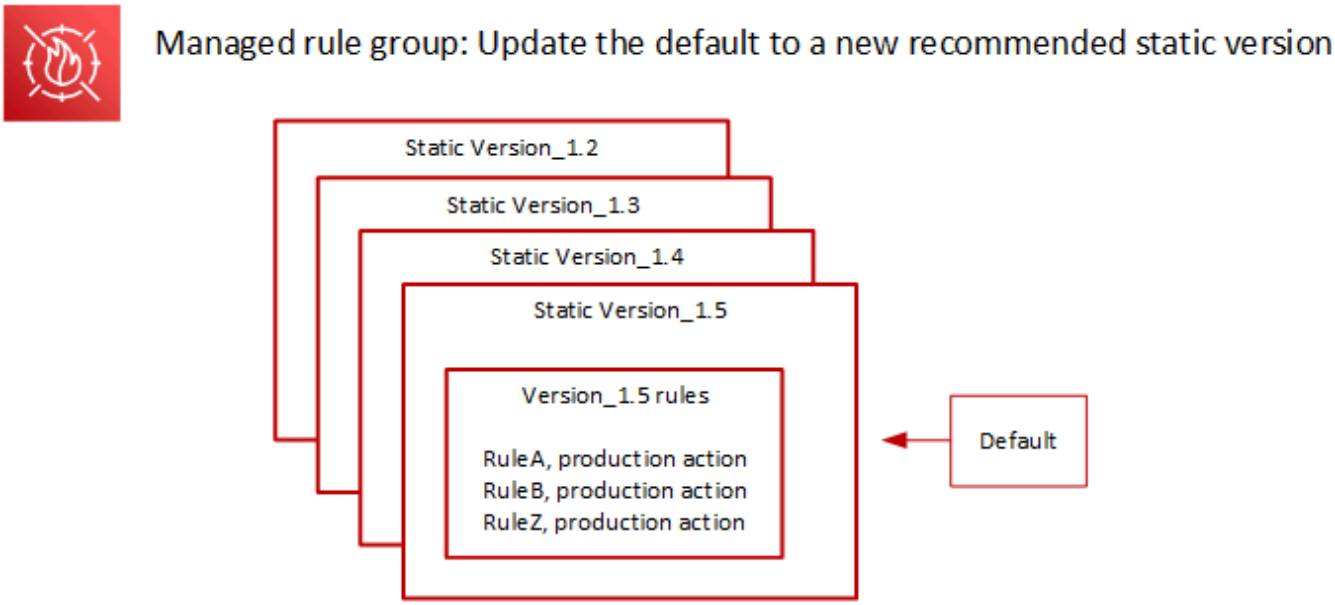
AWS 視需要部署新的靜態版本，以便部署對規則群組功能的改進。靜態版本的部署不會影響預設版本設定。

- SNS — 在部署完成時 AWS 傳送 SNS 通知。
- 變更記錄 — 部署完成所有可用 AWS WAF 位置之後，請視需要更 AWS 新本指南中的規則群組定義，然後在 AWS Managed Rules 規則群組變更記錄檔和文件記錄頁面中宣告發行。

AWS 受管規則的預設版本部署

當 AWS 判斷新的靜態版本是否為規則群組提供與目前預設值相較之下的改善保護時，會將預設版本 AWS 更新為新的靜態版本。 AWS 可能會先釋出多個靜態版本，再將一個靜態版本升級為規則群組的預設版本

下圖顯示將預設版本設定 AWS 移至新靜態版本之後，範例規則群組版本的狀態。



在將此變更部署到預設版本之前，會 AWS 提供通知，以便您可以測試並準備即將到來的變更。如果您使用預設版本，則無法採取任何動作，而且會在更新後繼續保留該版本。如果您想要延遲切換至新版本，則在預設版本部署的計劃開始之前，您可以明確地將規則群組設定為使用預設值設定為的靜態版本。

時間和通知

AWS 當規則群組建議使用與目前使用中的靜態版本不同的靜態版本時，會更新預設版本。

- SNS — 至少在目標部署日前一週 AWS 傳送 SNS 通知，然後在部署日傳送另一個訊息，在部署開始時傳送另一個通知。每個通知都包含規則群組名稱、預設版本更新目標的靜態版本、部署日期，以及執行更新的每個 AWS 區域的排程部署時間。
- 變更記錄 — AWS 不會針對此類型部署更新變更記錄或本指南的其他部分。

AWS 受管規則的例外部署

AWS 可能會略過標準部署階段，以便快速部署解決重大安全風險的更新。例外狀況部署可能涉及任何標準部署類型，而且可能會在各個 AWS 區域中快速推出。

AWS 為例外部署提供盡可能多的預先通知。

時間和通知

AWS 僅在需要時執行異常部署。

- SNS — 儘量在目標部署日期之前 AWS 傳送 SNS 通知，然後在部署開始時傳送另一個 SNS 通知。每個通知都包含規則群組名稱、正在進行的變更以及部署日期。
- 變更記錄 — 如果部署適用於靜態版本，則在部署完成所有可用 AWS WAF 位置之後，視需要更 AWS 新本指南中的規則群組定義，然後在 AWS Managed Rules 規則群組變更記錄檔和文件記錄頁面中宣告發行。

AWS 受管規則的預設部署復原

在某些情況下， AWS 可能會將預設版本回復為先前的設定。對於所有 AWS 區域，回復通常不到十分鐘。

AWS 執行復原只是為了緩解靜態版本中的重大問題，例如無法接受的高級誤判。

在復原預設版本設定之後，可 AWS 加速發生問題的靜態版本到期，以及發行新靜態版本以解決此問題。

時間和通知

AWS 僅在需要時執行預設版本復原。

- SNS — 在復原時 AWS 傳送單一 SNS 通知。通知包括規則群組名稱、預設版本設定的版本以及部署日期。此部署類型非常快速，因此通知不會提供「區域」的計時資訊。
- 變更記錄 — AWS 不會針對此類型部署更新變更記錄或本指南的其他部分。

AWS 管規則免責聲明

AWS 受管規則旨在保護您免受常見網頁威脅的侵害。根據文件使用時， AWS Managed Rules 規則群組會為您的應用程式新增另一層安全性。不過， AWS 受管規則群組並不是用來取代您的安全性責任，而這些責任是由您選取的 AWS 資源所決定。請參閱「共同責任模型」，以確保中的資源受到 AWS 適當的保護。

AWS 受管規則變更記錄檔

本節列出自 2019 年 11 月發行以 AWS WAF 來的 AWS 受管規則變更。

> **Note**
>
> 此變更記錄檔會報告的 AWS 受管規則中規則和規則群組的變更。 AWS WAF 對於IP 評價規則群組，此變更記錄檔會報告規則和規則群組的變更，並報告規則使用之 IP 位址清單來源的重大變更。由於這些清單的動態性質，它不會報告 IP 位址清單本身的變更。如果您對 IP 位址清單有任何疑問，請聯絡您的客戶經理或在AWS Support 中心提出案例。

規則群組和規則	描述	日期
WordPress 應用程式管理規則群 • `WordPressExploitableCommands_QUERYSTRING`	發行此規則群組的靜態版本 1.3。 已將 JS_ DECODE 文字轉換新增至列出的規則。	2024-07-15
Linux 作業系統管理規則群組 • `LFI_QUERYSTRING`	發布此規則組的靜態版本 2.4。 已將 JS_ DECODE 文字轉換新增至列出的規則。	2024-07-12

規則群組和規則	描述	日期
核心規則集 (CRS) 受管規則群組 • EC2MetaDataSSRF_BODY • EC2MetaDataSSRF_QUERYARGUMENTS • GenericLFI_QUERYARGUMENTS • GenericLFI_BODY • RestrictedExtensions_QUERYARGUMENTS • GenericRFI_QUERYARGUMENTS • GenericRFI_BODY • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_COOKIE • CrossSiteScripting_URIPATH	發行此規則群組的靜態 1.14 版。 已將 JS_ DECODE 文字轉換新增至列出的規則。	2024-07-09
PHP 應用程式管理規則群組 • PHPHighRiskMethodsVariables_BODY • PHPHighRiskMethodsVariables_QUERYSTRING	發行此規則群組的靜態 2.1 版。 已將 JS_ DECODE 文字轉換新增至列出的規則。	2024-07-03

規則群組和規則	描述	日期
Windows 作業系統受管理規則群組 • WindowsShellCommands_QUERYARGUMENTS • WindowsShellCommands_BODY • PowerShellCommands_QUERYARGUMENTS • PowerShellCommands_BODY	發行此規則群組的靜態 2.2 版。 已將 JS_ DECODE 文字轉換新增至列出的規則。	2024-07-03
Linux 作業系統管理規則群組 所有規則	發行此規則群組的靜態 2.3 版。 添加了簽名以改善檢測。	2024-06-06

規則群組和規則	描述	日期
AWS WAF 機器人控制規則群組 AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組 AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）規則組	機器人和詐騙規則群組現在已建立版本化。如果您使用這些規則群組中的任何一個，此更新不會變更它們處理您網路流量的方式。 此更新會將目前的規則群組版本設定為靜態 1.0 版，並將預設版本設定為指向該版本。 如需有關版本化管理規則的詳細資訊，請參閱下列內容： • 版本化的受管理規則群組 • 版本控制的 AWS 受管規則規則群組的部署 • 接收受管理規則群組的新版本和更新的通知	2024-05-29

規則群組和規則	描述	日期
POSIX 作業系統受管規則群組 • UNIXShellCommandsVariables_QUERYARGUMENTS • UNIXShellCommandsVariables_QUERYSTRING • UNIXShellCommandsVariables_HEADER • UNIXShellCommandsVariables_BODY	發行此規則群組的靜態 3.0 版。 刪除UNIXShellCommandsVariables_QUERYARGUMENTS 並替換它UNIXShellCommandsVariables_QUERYSTRING 。如果標籤上有符合的規則UNIXShellCommandsVariables_QUERYARGUMENTS ，當您使用此版本時，請將它們切換為符合的標籤UNIXShellCommandsVariables_QUERYSTRING 。新的標籤是awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QueryString 。 已新增符合所有標題的規則UNIXShellCommandsVariables_HEADER 。 使用改良的偵測邏輯更新受管規則群組中的所有規則。 已更正的標籤記錄的大小寫。UNIXShellCommandsVariables_BODY	2024-05-28

規則群組和規則	描述	日期
核心規則集 (CRS) 受管規則群組 • CrossSiteScripting*	發行此規則群組的靜態 1.12 版。 在所有跨網站指令碼規則中新增簽名，以改善偵測並減少誤判。	2024-05-21
SQL 資料庫管理的規則群組 • SQLi_BODY • SQLi_QUERYARGUMENTS • SQLiExtendedPatterns_QUERYARGUMENTS	發行此規則群組的靜態 1.2 版。 已將JS_DECODE 文字轉換新增至列出的規則。	2024-05-14
已知錯誤輸入受管規則群組 • JavaDeserializationRCE_BODY • JavaDeserializationRCE_QUERYSTRING • Log4JRCE_QUERYSTRING • Log4JRCE_BODY • Log4JRCE_HEADER	發行此規則群組的靜態版本 1.22。 已將JS_DECODE 文字轉換新增至列出的規則。	2024-05-08
POSIX 作業系統受管規則群組	發行此規則群組的靜態 2.2 版。 已將JS_DECODE 文字轉換新增至這兩個規則。	2024-05-08

規則群組和規則	描述	日期
Windows 作業系統受管理規則群組 • PowerShellCommands_BODY	發行此規則群組的靜態 2.1 版。 添加了簽名PowerShellCommands_BODY 以改善檢測。	2024-05-03
Amazon IP 信譽清單受管規則群組 • AWSManagedIPReputationList	更新 IP 信譽清單的來源，以改善主動參與惡意活動之位址的識別，並減少誤判。 此更新不涉及新版本，因為此規則群組未建立版本。	2024-03-13
已知錯誤輸入受管規則群組	發行此規則群組的靜態版本 1.21。 添加了簽名以改善檢測並減少誤判。	2023-12-16
已知錯誤輸入受管規則群組 • ExploitablePaths_URIPATH	發行此規則群組的靜態 1.20 版。 已更新ExploitablePaths_URIPATH 規則，以針對符合 Atlassian 聯合-2023-22518 不當授權弱點的要求新增偵測。CVE此弱點會影響匯流資料中心和伺服器的所有版本。如需詳細資訊，請參閱 NIST：國家弱點資料庫：CVE-2023-2 2518 詳細資訊。	2023-12-14

規則群組和規則	描述	日期
核心規則集 (CRS) 受管規則群組 • CrossSiteScripting*	發行此規則群組的靜態版本 1.11。 在所有跨網站指令碼規則中新增簽名，以改善偵測並減少誤判。	2023-12-06
AWS WAF 機器人控制規則群組 • 新標籤：awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low	在規則群組的目標防護等級標籤中新增協調活動低標籤。此標籤不與任何規則相關聯。此標籤是除了中級和高級規則和標籤之外的標籤。	2023-12-05
機器人控制標籤 • 標籤：awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension	已將訊號標籤新增至規則群組，指示偵測有助於自動化的瀏覽器擴充功能。此標籤不是個別規則的特定標籤。	2023-11-14
核心規則集 (CRS) 受管規則群組 • EC2MetaDataSSRF_QUERYARGUMENTS	發行此規則群組的靜態 1.10 版。 更新了一個規則以改善偵測並減少誤判。	2023-11-02

規則群組和規則	描述	日期
核心規則集 (CRS) 受管規則群組 • EC2MetaDataSSRF_BODY • EC2MetaDataSSRF_COOKIE • EC2MetaDataSSRF_URIPATH • EC2MetaDataSSRF_QUERYARGUMENTS	發行此規則群組的靜態 1.9 版。 更新規則以改善偵測並減少誤判。	2023-10-30
POSIX 作業系統受管規則群組 • UNIXShellCommandsVariables_QUERYARGUMENTS	發行此規則群組的靜態 2.1 版。 更新查詢引數規則以改善偵測。	2023-10-12
核心規則集 (CRS) 受管規則群組 • GenericLFI_QUERYARGUMENTS • GenericLFI_URIPATH • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS	發行此規則群組的靜態 1.8 版。 更新規則以改善偵測。	2023-10-11

規則群組和規則	描述	日期
已知錯誤輸入受管規則群組 • ExploitablePaths_URIPATH	例外部署：發行此規則群組的靜態 1.19 版。更新了默認版本以使用 1.19 版本。 已更新ExploitablePaths_URIPATH 規則，以針對符合 Atlassian 合併 -2023-22515 權限提升弱點的要求新增偵測。CVE此漏洞會影響阿特拉西亞匯合的某些版本。如需詳細資訊，請參閱 NIST：國家弱點資料庫：CVE-2023-22515 詳細資料和安全防護 Support：適用於 -2023-22515。FAQ CVE 如需有關此部署類型的資訊，請參閱AWS 受管規則的例外部署。	2023-10-04
已知錯誤輸入受管規則群組 • Host_localhost_HEADER • Log4J* • JavaDeserialization*	例外部署：發行此規則群組的靜態 1.18 版。這是此靜態版本的快速推出，以適應 1.19 版本的創建和推出。 更新了Host_localhost_HEADER 規則和所有 Log4j 和 Java 反序列化規則，以改進檢測。 如需有關此部署類型的資訊，請參閱AWS 受管規則的例外部署。	2023-10-04

規則群組和規則	描述	日期
AWS WAF 機器人控制規則群組 • TGT_TokenReuseIp • TGT_ML_CoordinatedActivityMedium • TGT_ML_CoordinatedActivityHigh	使用Count動作將規則新增至規則群組。 權杖重複使用 IP 規則會偵測並計算跨 IP 位址共用的權杖。 協調的活動規則使用網站流量的自動化機器學習（ML）分析來檢測機器人相關的活動。在規則群組設定中，您可以選擇不使用 ML。在此版本中，目前使用目標防護層級的客戶可選擇使用 ML。選擇退出會停用協調活動規則。	2023-09-06
AWS WAF 機器人控制規則群組 • CategoryAI	已將規則新增CategoryAI 至規則群組。	2023-08-30

規則群組和規則	描述	日期
核心規則集 (CRS) 受管規則群組 • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS • EC2MetaDataSSRF_COOKIE • EC2MetaDataSSRF_QUERYARGUMENTS • EC2MetaDataSSRF_BODY • EC2MetaDataSSRF_URIPATH	發行此規則群組的靜態 1.7 版。 已更新受限制的擴充功能和EC2中繼資料SSRF規則，以改善偵測並減少誤判。	2023-07-26
AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）規則組 新規則群組中的所有規則	已新增規則群組AWSManagedRulesACFPRuleSet 。	2023-06-13
Linux 作業系統管理規則群組 • LFI_HEADER • LFI_URIPATH • LFI_QUERYSTRING	發行此規則群組的靜態 2.2 版。 添加了簽名以改善檢測。	2023-05-22

規則群組和規則	描述	日期
核心規則集 (CRS) 受管規則群組 • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	發行此規則群組的靜態 1.6 版。 更新了跨網站指令碼 (XSS) 和受限延伸規則，以改善偵測並減少誤判。	2023-04-28

規則群組和規則	描述	日期
PHP 應用程式管理規則群組 • 已更新 PHPHighRiskMethodsVariables_BODY • 已移除 PHPHighRiskMethodsVariables_QUERYARGUMENTS • 已新增 PHPHighRiskMethodsVariables_QUERYSTRING • 已新增 PHPHighRiskMethodsVariables_HEADER	發行此規則群組的靜態 2.0 版。 添加了簽名以改善所有規則的檢測。 將規則PHPHighRiskMethodsVariables_QUERYARGUMENTS 取代為PHPHighRiskMethodsVariables_QUERYSTRING ，此規則會檢查整個查詢字串，而不只是查詢引數。 已新增規則PHPHighRiskMethodsVariables_HEADER ，以擴大涵蓋範圍以包含所有標題。 已更新下列標籤，以符合標準 AWS 受管規則標籤： • 舊名稱：PHPHighRiskMethodsVariables_BODY 新名稱：PHPHighRiskMethodsVariables_Body • 舊名稱：PHPHighRiskMethodsVariables_QUERYARGUMENTS 新名稱：PHPHighRiskMethodsVariables_QueryString	2023-02-27

規則群組和規則	描述	日期
AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組 • VolumetricIpFailedLoginResponseHigh • VolumetricSessionFailedLoginResponseHigh	新增登入回應檢查規則，以搭配受保護的 Amazon CloudFront 分發使用。這些規則可以封鎖來自 IP 位址和用戶端工作階段的新登入嘗試，這些嘗試最近是過多次登入嘗試失敗的來源。	2023-02-15
核心規則集 (CRS) 受管規則群組 • NoUserAgent_HEADER • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	發行此規則群組的靜態 1.5 版。 更新了跨網站指令碼 (XSS) 篩選器以改善偵測。	2023-01-25

規則群組和規則	描述	日期
Linux 作業系統管理規則群組 • LFI_COOKIE -刪除 • LFI_HEADER -添加 • LFI_URIPATH • LFI_QUERYSTRING	發行此規則群組的靜態 2.1 版。 移除規則LFI_COOKIE 及其標籤awswaf:managed:aws:linux-os:LFI_Cookie ，並將其取代為新規則LFI_HEADER 及其標籤awswaf:managed:aws:linux-os:LFI_Header 。此變更將檢查擴展到多個標題。 為所有規則添加了文本轉換和簽名以改善檢測。	2022-12-15
核心規則集 (CRS) 受管規則群組 • NoUserAgent_HEADER • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	發行此規則群組的靜態版本 1.4。 已新增文字轉換NoUserAgent_HEADER 以移除所有空位元組。更新跨網站指令碼規則中的篩選器，以改善偵測。	2022-12-05

規則群組和規則	描述	日期
已知錯誤輸入受管規則群組 • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URIPATH • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_QUERYSTRING • Host_localhost_HEADER	發行此規則群組的靜態 1.17 版。 已更新 Java 還原序列化規則，以針對符合 Apache CVE -2022-42889 的要求新增偵測，這是 Apache 共享資源文字版本 1.10.0 之前的遠端程式碼執行 (RCE) 漏洞。如需詳細資訊，請參閱 NIST：國家弱點資料庫:CVE-2022-42889 詳細資料與 CVE -2022-42889：1.10.0 之前的 Apache 共享資源文字，因為不安全的內插預設值，允許套用至不受信任的輸入。RCE 改善中的偵測功能Host_localhost_HEADER 。	2022-10-20
已知錯誤輸入受管規則群組 • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URIPATH • Log4JRCE_BODY	發行此規則群組的靜態 1.16 版。 移除了 1.15 版中 AWS 識別的誤報。	2022-10-05

規則群組和規則	描述	日期
POSIX 作業系統受管規則群組 PHP 應用程式管理規則群組 WordPress 應用程式管理規則群	更正記錄的標籤名稱。	2022-09-19
IP 評價規則群組 • AWSManagedIPDDoSList	此變更不會改變規則群組處理網路流量的方式。 根據 Amazon 威脅情報，新增了具有動Count作的新規則，以檢查主動參與DDoS活動的 IP 地址。	2022-08-30

規則群組和規則	描述	日期
已知錯誤輸入受管規則群組 • Log4JRCE • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URIPATH • Log4JRCE_BODY • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URIPATH • JavaDeserializationRCE_QUERYSTRING • Host_localhost_HEADER • PROPFIND_METHOD	發行此規則群組的靜態版本 1.15。 將其移除Log4JRCE並取代為Log4JRCE_HEADER Log4JRCE_QUERYSTRING 、Log4JRCE_URI 、和Log4JRCE_BODY ，以便更精細地監控和管理誤報。 添加了簽名，以改進對所有PROPFIND_METHOD 和Log4JRCE* 規則的檢測JavaDeserializationRCE* 和阻止。 更新標籤以更正所有JavaDeserializationRCE* 規則中Host_localhost_HEADER 和中的大寫。 已更正的描述JavaDeserializationRCE_HEADER 。	2022-08-22
AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組 • UnsupportedCognitoIDP	新增規則以防止針對 Amazon Cognito 使用者集區網路流量使用帳戶接管預防受管規則群組。	2022-08-11

規則群組和規則	描述	日期
核心規則集 (CRS) 受管規則群組	AWS 已排定版本Version_1.2 和規則群組Version_2.0 的到期日。這些版本將於 2022 年 9 月 9 日到期。如需有關版本到期的資訊，請參閱版本化的受管理規則群組。	2022-06-09
核心規則集 (CRS) 受管規則群組 • GenericLFI_URIPATH GenericRFI_URIPATH	此規則群組的 1.3 版發行。此版本會更新規則中的比對簽章GenericRFI_URIPATH ，GenericLFI_URIPATH 並改善偵測。	2022-05-24
AWS WAF 機器人控制規則群組 • CategoryEmailClient	已將規則新增CategoryEmailClient 至規則群組。	2022-04-06
已知錯誤輸入受管規則群組 • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URI • JavaDeserializationRCE_QUERYSTRING	已發行此規則群組 1.14 版。四個JavaDeserializiztionRCE 規則會移至Block模式。	2022-03-31

規則群組和規則	描述	日期
已知錯誤輸入受管規則群組 • JavaDeserializationRCE_HEADER_RC_COUNT • JavaDeserializationRCE_BODY_RC_COUNT • JavaDeserializationRCE_URI_RC_COUNT • JavaDeserializationRCE_QUERYSTRING_RC_COUNT	已發行此規則群組 1.13 版。更新了 Spring 核心和雲功能RCE漏洞的文本轉換。這些規則處於計數模式，以收集度量並評估相符的模式。標籤可用於封鎖自訂規則中的要求。後續版本將使用這些規則在封鎖模式中部署。	2022-03-31

規則群組和規則	描述	日期
已知錯誤輸入受管規則群組 • JavaDeserializationRCE_HEADER_RC_COUNT • JavaDeserializationRCE_BODY_RC_COUNT • JavaDeserializationRCE_URI_RC_COUNT • JavaDeserializationRCE_QUERYSTRING_RC_COUNT • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URI • Log4JRCE_BODY • Log4JRCE	此規則群組的 1.12 版發行。為 Spring 核心和雲功能RCE漏洞添加了簽名。這些規則處於計數模式，以收集度量並評估相符的模式。標籤可用於封鎖自訂規則中的要求。後續版本將使用這些規則在封鎖模式中部署。 已移除規則Log4JRCE_HEADER Log4JRCE_QUERYSTRING 、Log4JRCE_URI 、和，Log4JRCE_BODY 並將其取代為規則Log4JRCE。	2022-03-30
IP 評價規則群組 • AWSManagedReconnaissanceList	已更新AWSManagedReconnaissanceList 規則，將動作從計數變更為封鎖。	2022-02-15
AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組 新規則群組中的所有規則	已新增規則群組AWSManagedRulesATPRuleSet 。	2022-02-11

規則群組和規則	描述	日期
已知錯誤輸入受管規則群組 • Log4JRCE • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URI • Log4JRCE_BODY	此規則群組的 1.9 版發行。已移除規則，Log4JRCE並將其取代為規則Log4JRCE_HEADER 、Log4JRCE_QUERYSTRING Log4JRCE_URI 、和，Log4JRCE_BODY ，，，，，，，以便使用此功能。添加了簽名以改善檢測和阻止。	2022-01-28
核心規則集 (CRS) • CrossSiteScripting_URIPATH • CrossSiteScripting_BODY • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_COOKIE	此規則群組的 2.0 版發行。針對這些規則，請調整偵測簽章以減少誤判。將URL_DECODE 文字轉換取代為雙URL_DECODE_UNI 文字轉換。添加了HTML_ENTITY_DECODE 文本轉換。	2022-01-10
核心規則集 (CRS) • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS	作為此規則群組 2.0 版發行版本的一部分，新增了URL_DECODE_UNI 文字轉換。從中刪除了URL_DECODE 文本轉換RestrictedExtensions_URIPATH 。	2022-01-10

規則群組和規則	描述	日期
SQL 資料庫 • SQLi_BODY • SQLi_QUERYARGUMENTS • SQLi_COOKIE • SQLi_URIPATH • SQLiExtendedPatterns_BODY • SQLiExtendedPatterns_QUERYARGUMENTS	此規則群組的 2.0 版發行。將URL_DECODE 文字轉換取代為雙重URL_DECODE_UNI 文字轉換，並新增COMPRESS_WHITE_SPACE 文字轉換。 已將更多偵測簽名新增至SQLiExtendedPatterns_QUERYARGUMENTS . 已將JSON檢查新增至SQLi_BODY 。 已新增規則SQLiExtendedPatterns_BODY 。 已移除規則SQLi_URIPATH 。	2022-01-10
已知錯誤輸入 • Log4JRCE	發行規則 1.8 版，Log4JRCE以改善標頭檢查和匹配標準。	2021-12-17
已知錯誤輸入 • Log4JRCE	已發行規則 1.4 版，Log4JRCE以調整相符條件並檢查其他標頭。發布 1.5 版以調整匹配標準。	2021-12-11

規則群組和規則	描述	日期
已知錯誤輸入 • Log4JRCE • BadAuthToken_COOKIE_AUTHORIZATION	已新增規則 1.2 Log4JRCE 版，以回應 Log4j 中最近揭露的安全性問題。如需詳細資訊，請參閱 CVE-2021-44228。此規則會檢查通用URI路徑、查詢字串、要求主體的前 8KB 和一般標頭。規則使用雙重URL_DECODE_UNI 文字轉換。發行的 1.3 版Log4JRCE以調整匹配條件並檢查其他標題。 已移除規則BadAuthToken_COOKIE_AUTHORIZATION 。	2021-12-10

下表列出 2021 年 12 月之前的變更。

規則群組和規則	描述	日期	
Amazon IP 評價清單	AWSManagedReconnaissanceList	在監控/計數模式下新增AWSManagedReconnaissanceList 規則。此規則包含對資源執行偵察的 IP 位址。 AWS	2021-11-23
Windows 作業系統	WindowsShellCommands PowerShellCommands	已新增三個 WindowsShell 指令的新規則：WindowsShellCommands_COOKIE WindowsSh	2021-11-23

規則群組和規則	描述	日期	
		ellComman ds_QUERYA RGUMENTS 、和WindowsSh ellComman ds_BODY 。 已新增 PowerShell 規則：PowerShel lCommands _COOKIE 。 透過移除字串 _Set1 和 _Set2 來重新架構PowerShel lComands 規則命名。 已將更全面的偵測簽名新增至PowerShel lRules . 新增URL_DECOD E_UNI 文字轉換至所有 Windows 作業系統規則。	

規則群組和規則	描述	日期	
Linux 作業系統	LFI_URIPATH LFI_QUERYSTRING LFI_BODY LFI_COOKIE	用雙重URL_DECODE 文本替換雙文本轉換URL_DECODE_UNI 。 新增NORMALIZE_PATH_WIN 為第二個文字轉換。 將LFI_BODY規則取代為LFI_COOKIE 規則。 為所有LFI規則添加了更全面的檢測簽名。	2021-11-23
核心規則集 (CRS)	SizeRestrictions_BODY	減少封鎖內文承載大於 8 KB 的 Web 要求的大小限制。以前，限制為 10 KB。	2021-10-27
核心規則集 (CRS)	EC2MetaDataSSRF_BODY EC2MetaDataSSRF_COOKIE EC2MetaDataSSRF_URIPATH EC2MetaDataSSRF_QUERYARGUMENTS	添加了更多檢測簽名。添加了雙 Unicode URL 解碼以改善阻塞。	2021-10-27

規則群組和規則	描述	日期	
核心規則集 (CRS)	GenericLFI_QUERYARGUMENTS GenericLFI_URIPATH RestrictedExtensions_URIPATH RestrictedExtensions_QUERYARGUMENTS	添加了雙 Unicode URL 解碼以改善阻塞。	2021-10-27
核心規則集 (CRS)	GenericRFI_QUERYARGUMENTS GenericRFI_BODY GenericRFI_URIPATH	根據客戶意見反應，更新規則簽章以減少誤判。添加了雙 Unicode URL 解碼以改善阻塞。	2021-10-27
全部	所有規則	為所有尚未支援 AWS WAF 標籤的規則新增了對標籤的支援。	2021-10-25
Amazon IP 評價清單	AWSManagedIPReputationList_xxxx	重新架構 IP 信譽清單、從規則名稱移除尾碼，並新增對標籤的支援。 AWS WAF	2021-05-04

規則群組和規則	描述	日期	
匿名 IP 清單	AnonymousIPList HostingProviderList	增加了對 AWS WAF 標籤的支持。	2021-05-04
機器人控制	全部	新增機器人控制規則集。	2021-04-01
核心規則集 (CRS)	GenericRFI_QUERYARGUMENTS	添加了雙URL解碼。	2021-03-03
核心規則集 (CRS)	RestrictedExtensions_URIPATH	改進了規則的配置並添加了額外的URL解碼。	2021-03-03
管理員保護	AdminProtection_URIPATH	添加了雙URL解碼。	2021-03-03
已知錯誤輸入	ExploitablePaths_URIPATH	改進了規則的配置並添加了額外的URL解碼。	2021-03-03
Linux 作業系統	LFI_QUERYARGUMENTS	改進了規則的配置並添加了額外的URL解碼。	2021-03-03
Windows 作業系統	全部	改進了規則的配置。	2020-09-23

規則群組和規則	描述	日期	
PHP應用	PHPHighRiskMethodsVariables_QUERYARGUMENTS PHPHighRiskMethodsVariables_BODY	改變了從HTML解碼到URL解碼的文本轉換，以改善阻塞。	2020-09-16
POSIX作業系統	UNIXShellCommandsVariables_QUERYARGUMENTS UNIXShellCommandsVariables_BODY	改變了從HTML解碼到URL解碼的文本轉換，以改善阻塞。	2020-09-16
核心規則集	GenericLFI_QUERYARGUMENTS GenericLFI_URIPATH 通用 LFI _ BODY	改變了從HTML解碼到URL解碼的文本轉換，以改善阻塞。	2020-08-07
Linux 作業系統	LFI_URIPATH LFI_QUERYARGUMENTS LFI_BODY	改變了從HTML實體解碼到URL解碼的文本轉換，以改善檢測和阻止。	2020-05-19

規則群組和規則	描述	日期	
匿名 IP 清單	全部	新的規則群組可封鎖IP評價規則群組來自允許檢視者身分模糊化之服務的要求，以協助減輕機器人和逃避地理限制。	2020-03-06
WordPress 應用	`WordPressExploitableCommands_QUERYSTRING`	能檢查查詢字串中可入侵字串的新規則	2020-03-03

核心規則集 (CRS)	`SizeRestrictions_QUERYSTRING`
	
	`SizeRestrictions_Cookie_HEADER`
	
	`SizeRestrictions_BODY`
	
	`SizeRestrictions_URIPATH`
		調整大小值限制條件以改善準確性。	2020-03-03

SQL 資料庫	`SQLi_URIPATH`	規則現在會檢查訊息 URI。	2020-01-23

SQL 資料庫	`SQLi_BODY`
	
	`SQLi_QUERYARGUMENTS`
	
	`SQLi_COOKIE`
		更新的文字轉換。	2019-12-20

規則群組和規則	描述	日期	

核心規則集 (CRS)	`CrossSite Scripting _URIPATH`
	
	`CrossSite Scripting_BODY`
	
	`CrossSite Scripting _QUERYARG UMENTS`
	
	`CrossSite Scripting _COOKIE`
		更新的文字轉換。	2019-12-20

AWS Marketplace 受管規則群組

AWS Marketplace 訂閱可透過 AWS Marketplace 主控台使用的受管規則群組，網址為AWS Marketplace。訂閱 AWS Marketplace 受管規則群組後，即可在中使用該群組 AWS WAF。若要在 AWS Firewall Manager AWS WAF 策略中使用 AWS Marketplace 規則群組，組織中的每個帳戶都必須訂閱該群組。

在將保護用於生產流量之前，請先測試和調整 AWS WAF 保護措施的任何變更。如需相關資訊，請參閱測試和調整您的 AWS WAF 保護。

AWS Marketplace 規則群組定價

AWS Marketplace 規則群組可供使用，沒有長期合約，也沒有最低承諾。訂閱規則群組時，您必須按月支付費用 (依小時按比例分配)，以及基於用量的持續請求費用。如需詳細資訊，請參閱AWS WAF 定價和每個 AWS Marketplace 規則群組的說明AWS Marketplace。

對 AWS Marketplace 規則群組有疑問嗎？

如果您對 AWS Marketplace 賣家管理的規則群組有任何疑問，並要求變更功能，請聯絡供應商的客戶支援團隊。若要尋找聯絡資訊，請參閱供應商的清單，網址為AWS Marketplace。

AWS Marketplace 規則群組提供者決定如何管理規則群組，例如如何更新規則群組，以及規則群組是否已建立版本化。提供者也會決定規則群組的詳細資訊，包括規則、規則動作，以及規則新增至相符 Web 要求的任何標籤。

訂閱 AWS Marketplace 受管規則群組

您可以在 AWS WAF 主控台上訂閱和取消訂閱 AWS Marketplace 規則群組。

> **Important**
>
> 若要在 AWS Firewall Manager 策略中使用 AWS Marketplace 規則群組，組織中的每個帳戶都必須先訂閱該規則群組。

訂閱受 AWS Marketplace 管規則群組

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中，選擇 AWS Marketplace。
3. 在 Available marketplace products (提供市場產品)，選擇規則的名稱，檢視其詳細資訊和定價資訊。
4. 如果您想訂閱此規則群組，選擇繼續。

   > **Note**
   >
   > 如果您不想訂閱此規則群組，只需在您的瀏覽器關閉此頁面。

5. 選擇Set up your account (建立您的帳戶)。
6. 將規則群組新增至 Web ACL，類似於新增個別規則的方式。如需詳細資訊，請參閱 建立 Web ACL 或 編輯網路 ACL 。

   > **Note**
   >
   > 將規則群組新增至 Web ACL 時，您可以覆寫規則群組和規則群組結果中規則的動作。如需詳細資訊，請參閱 規則群組的動作覆寫選項。

訂閱 AWS Marketplace 規則群組後，您可以像在其他受管規則群組一樣在 Web ACL 中使用該群組。如需相關資訊，請參閱建立 Web ACL。

取消訂閱 AWS Marketplace 受管規則群組

您可以在 AWS WAF 主控台上取消訂閱 AWS Marketplace 規則群組。

> **Important**
>
> 若要停止受 AWS Marketplace 管規則群組的訂閱費用，除了取消訂閱之外，您還必須從任何 Firewall Manager 員 AWS WAF 原則中的所有 Web ACL 中移除該群組。 AWS WAF 如果您取消訂閱 AWS Marketplace 受管規則群組，但並未將其從 Web ACL 中移除，則會繼續向您收取訂閱費用。

取消訂閱受 AWS Marketplace 管規則群組

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 從所有 Web ACL 中移除規則群組。如需詳細資訊，請參閱 編輯網路 ACL。
3. 在導覽窗格中，選擇 AWS Marketplace。
4. 選擇Manage your subscriptions (管理我的訂閱)。
5. 在您想要取消訂閱的規則群組名稱旁，選擇取消訂閱。
6. 選擇是，取消訂閱。

排解 AWS Marketplace 規則群組

如果您發現 AWS Marketplace 規則群組封鎖了合法流量，您可以執行下列步驟來疑難排解問題。

AWS Marketplace 規則群組的故障診斷

1. 覆寫要針對封鎖合法流量之規則計數的動作。您可以使用 AWS WAF 取樣的要求或 AWS WAF 記錄來識別哪些規則會封鎖特定要求。您可以查看日誌中的 `ruleGroupId` 欄位或取樣請求中的 `RuleWithinRuleGroup` 來識別規則。您可以識別模式中的規則`<Seller Name>#<RuleGroup Name>#<Rule Name>`。
2. 如果將特定規則設定為僅計數請求無法解決問題，您可以覆寫所有規則動作，或將規 AWS Marketplace 則群組本身的動作從「無覆寫」變更為「覆寫」以計數。這允許 web 請求通過，無視規則群組內的個別規則動作。

3. 覆寫個別規則動作或整個規則群組動作之後，請連絡 AWS Marketplace 規則群組提供者的客戶支援團隊，以進一步疑難排解問題。如需聯絡資訊，請參閱 AWS Marketplace中產品列表頁面的規則群組清單。

聯絡 AWS 支援

如有問題 AWS WAF 或由管理的規則群組 AWS，請連絡 AWS Support。如果 AWS Marketplace 賣家管理的規則群組有問題，請聯絡供應商的客戶支援團隊。若要尋找聯絡資訊，請參閱上的供應商清單 AWS Marketplace。

管理您自己的規則群組

您可以建立自己的規則群組，以重複使用在受管規則群組提供項目中找不到或您偏好自行處理的規則集合。

您建立保留規則的規則群組就像網頁一ACL樣，而且您可以使用與對網頁相同的方式將規則新增至規則群組ACL。建立自己的規則群組時，必須為其設定不可變的容量上限。

主題

- 建立規則群組
- 編輯規則群組
- 在網頁 ACL 中使用規則群組
- 刪除規則群組
- 規則群組共用

建立規則群組

若要建立新的規則群組，請遵循此頁面上的程序。

建立規則群組

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中，選擇 Rule groups (規則群組)，然後選擇 Create rule group (建立規則群組)。
3. 輸入規則的名稱和描述。您將使用這些來識別規則集來管理和使用它。

   請勿使用以AWS、Shield、PreFM或開頭的名稱PostFM。這些字串是保留的，或者可能會與其他服務為您管理的規則群組造成混淆。請參閱由其他服務提供的規則群組。

> **Note**
>
> 建立規則群組後無法修改名稱。

4. 對於 Region (區域)，選擇您要儲存規則群組的區域。若要在保護 Amazon CloudFront 分發的 Web ACL 中使用規則群組，您必須使用全域設定。您也可以對區域應用程式使用全域設定。
5. 選擇下一步。
6. 使用 Rule builder (規則建置器) 精靈將規則新增至規則群組，與您在 Web ACL 管理中所做的相同。唯一的差異是您無法將規則群組新增到另一個規則群組。
7. 對於 Capacity (容量)，設定規則群組使用 Web ACL 容量單位 (WCU) 的上限。這是一個不可變的設定。如需 WCU 的相關資訊，請參閱 AWS WAF 網路 ACL 容量單位 (WCU)。

   當您將規則新增至規則群組時，Add rules and set capacity (新增規則和設定容量) 窗格會顯示所需的最小容量，這是根據您已新增的規則而定。您可以使用此項目和對於規則群組的未來計劃，協助評估規則群組將需要的容量。
8. 檢閱規則群組的設定，然後選擇 Create (建立)。

編輯規則群組

若要新增或移除規則群組中的規則，或變更組態設定，請使用此頁面上的程序存取規則群組。

> **生產流量風險**
>
> 如果您變更目前在網頁中使用的規則群組ACL，這些變更都會影響您在任何網頁使用中的ACL行為。請務必在測試或測試環境中測試和調整所有變更，直到您對流量的潛在影響感到滿意為止。然後在啟用生產流量之前，在計數模式下測試和調整您更新的規則。如需準則，請參閱測試和調整您的 AWS WAF 保護。

編輯規則群組

1. 登入 AWS Management Console 並開啟 AWS WAF 主控台，位於https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中，選擇 Rule groups (規則群組)。
3. 選擇您要編輯的規則群組名稱。主控台會帶您前往規則群組的頁面。

> **Note**
>
> 如果您沒有看到要編輯的規則群組，請勾選「規則群組」區段中的「區域」選項。對於用於保護 Amazon CloudFront 分發的規則群組，請使用全域 (CloudFront) 設定。

4. 視需要編輯規則群組。您可以編輯規則群組的可變屬性，類似於建立期間的操作方式。主控台會隨時儲存您的變更。

> **Note**
>
> 如果您變更規則的名稱，並希望規則的量度名稱反映變更，您也必須更新量度名稱。AWS WAF 變更規則名稱時，不會自動更新規則的度量名稱。您可以在主控台中編輯規則時，使用規則編輯JSON器來變更度量名稱。您也可以在任何用來定義網頁ACL或規則群組的JSON清單中變更名稱。APIs

更新期間暫時不一致

當您建立或變更 Web ACL 或其他 AWS WAF 資源時，變更需要少量時間才能傳播到儲存資源的所有區域。傳輸時間可以是幾秒鐘到分鐘數。

以下是您在變更傳播期間可能會注意到的暫時性不一致的範例：

- 建立 Web 之後ACL，如果您嘗試將其與資源建立關聯，可能會出現例外狀況，指出網頁無ACL法使用。
- 將規則群組新增至 Web 之後ACL，新規則群組規則可能會在使用 Web ACL 的某個區域中生效，而不會在另一個區域中生效。
- 變更規則動作設定後，您可能會在某些地方看到舊動作，而在其他地方看到新動作。
- 將 IP 位址新增至封鎖規則中使用的 IP 集後，該新位址可能會在某個區域遭到封鎖，而另一個區域仍允許使用該 IP 位址。

在網頁 ACL 中使用規則群組

若要在 Web ACL 中使用規則群組，請在規則群組參考陳述式中將其新增至 Web ACL。

生產流量風險

在 Web ACL 中針對生產流量部署變更之前，請先在測試或測試環境中對其進行測試和調整，直到您熟悉對流量的潛在影響為止。然後在啟用生產流量之前，在計數模式下測試和調整您更新的規則。如需準則，請參閱測試和調整您的 AWS WAF 保護。

Note

在網頁 ACL 中使用超過 1,500 個 WCU 會產生超出基本網頁 ACL 價格的成本。如需詳細資訊，請參閱 AWS WAF 網路 ACL 容量單位 (WCU) 和 AWS WAF 定價。

在主控台上，當您在 Web ACL 中新增或更新規則時，在 [新增規則和規則群組] 頁面上，選擇 [新增規則]，然後選擇 [新增我自己的規則和規則群組]。然後選擇 Rule group (規則群組)，並從清單中選取您的規則群組。

在 Web ACL 中，您可以將個別規則動作設定為Count或任何其他動作，來變更規則群組及其規則的行為。這可協助您執行諸如測試規則群組、從規則群組中的規則識別誤判，以及自訂受管規則群組如何處理您的要求。如需詳細資訊，請參閱 規則群組的動作覆寫選項。

如果您的規則群組包含以速率為基礎的陳述式，則您使用該規則群組的每個 Web ACL 都有自己獨立的費率追蹤和管理以比率為基礎的規則，與您使用規則群組的任何其他 Web ACL 無關。如需詳細資訊，請參閱 速率型規則陳述式。

更新期間暫時不一致

當您建立或變更 Web ACL 或其他 AWS WAF 資源時，變更需要少量時間才能傳播到儲存資源的所有區域。傳輸時間可以是幾秒鐘到分鐘數。

以下是您在變更傳播期間可能會注意到的暫時性不一致的範例：

- 建立 Web ACL 之後，如果您嘗試將其與資源建立關聯，可能會出現例外狀況，指出 Web ACL 無法使用。
- 將規則群組新增至 Web ACL 後，新規則群組規則可能會在使用 Web ACL 的某個區域中生效，而不會在另一個區域中生效。
- 變更規則動作設定後，您可能會在某些地方看到舊動作，而在其他地方看到新動作。
- 將 IP 位址新增至封鎖規則中使用的 IP 集後，該新位址可能會在某個區域遭到封鎖，而另一個區域仍允許使用該 IP 位址。

刪除規則群組

遵循本節中的指引來刪除規則群組。

刪除參照集和規則群組

當您刪除可在 Web ACL 中使用的實體 (例如 IP 集、regex 模式集或規則群組) 時，會 AWS WAF 檢查實體目前是否正在 Web 中使用ACL。如果發現它正在使用中， AWS WAF 會警告您。 AWS WAF 幾乎總是能夠確定一個實體是否被 Web 引用ACL。但是在極少數的情況下，它也可能無法判斷。如果您需要確保當前沒有任何實體正在使用該實體，請在刪除實體ACLs之前在 Web 中檢查它。如果實體是參照集，請同時檢查是否沒有規則群組正在使用它。

刪除規則群組

1. 登入 AWS Management Console 並開啟 AWS WAF 主控台，位於https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中，選擇 Rule groups (規則群組)。
3. 選擇您要刪除的規則群組，然後選擇 Delete (刪除)。

> **Note**
>
> 如果您沒有看到要刪除的規則群組，請勾選 [規則群組] 區段中的 [區域] 選項。對於用於保護 Amazon CloudFront 分發的規則群組，請使用全域 (CloudFront) 設定。

規則群組共用

您可以與其他帳戶共用規則群組，以供這些帳戶使用。

共用規則群組

您可以與一或多個特定帳戶共用，也可以與組織中的所有帳戶共用。

若要共用規則群組，您可 AWS WAF API以使用為您想要的規則群組共用建立原則。如需詳細資訊，請參閱〈AWS WAF API參考〉PutPermissionPolicy中的〈〉。

使用已與您共用的規則群組

如果已與您的帳戶共用規則群組，您可以透過存取該規則群組，API並在建立或更新網頁時ACLs透過API. 如需詳細資訊，請參閱〈〉GetRuleGroupCreateWebACL、〈〉和〈AWS WAF API參考〉UpdateWebACL中的〈〉。與您共享的規則群組不會顯示在 AWS WAF 主機規則群組清單中。

由其他服務提供的規則群組

如果您或組織中的系統管理員使用 AWS Firewall Manager 或 AWS Shield Advanced 管理資源保護 AWS WAF，您可能會在帳戶中看到新增至 Web ACL 的規則群組參考陳述式。

這些規則群組的名稱以下列字串開頭：

- **ShieldMitigationRuleGroup**— 這些規則群組由受保護的應用程式層 (第 7 層) 資源管理 AWS Shield Advanced 並用來提供自動應用程式層 DDoS 緩解功能。

  當您為受保護的資源啟用自動應用程式層 DDoS 緩解功能時，Shield Advanced 會將這些規則群組中的其中一個新增到您與資源關聯的 Web ACL 中。Shield Advanced 會將優先順序設定 10,000,000 指派給規則群組參照陳述式，以便在您在 Web ACL 中設定的規則之後執行。如需這些規則群組的詳細資訊，請參閱Shield 先進的自動應用層 DDoS 緩解。

  > **Warning**
  >
  > 請勿嘗試在 Web ACL 中手動管理此規則群組。特別是，請勿從 Web ACL 手動刪除`ShieldMitigationRuleGroup`規則群組參考陳述式。這樣做可能會對與 Web ACL 相關聯的所有資源產生意外後果。請改為使用「防 Shield 進階」來停用與 Web ACL 相關聯之資源的自動緩和措施。Shield Advanced 會在不需要自動緩解規則時為您移除規則群組。

- **PREFMManaged**和 **POSTFMManaged** — 這些規則群組由管理 AWS Firewall Manager。Firewall Manager 員會在 Firewall Manager 員建立和管理的 Web ACL 中提供這些選項。網路 ACL 的名稱開頭為。`FMManagedWebACLV2`如需有關這些 Web ACL 和規則群組的資訊，請參閱AWS WAF 政策。

AWS WAF 規則

AWS WAF 規則定義如何檢查 HTTP (S) Web 要求，以及符合檢查準則時要對要求採取的動作。您只能在規則群組或 Web ACL 的前後關聯中定義規則。

規則不存在 AWS WAF 於他們自己。他們不是 AWS 資源，他們沒有 Amazon 資源名稱（ARN）。您可以在定義規則的規則群組或 Web ACL 中依名稱存取規則。您可以使用規則群組的 JSON 檢視或包含規則的 Web ACL，來管理規則並將其複製到其他 Web ACL。您也可以透過可供 Web ACL 和規則群組使用的 AWS WAF 主控台規則產生器來管理這些規則產生器。

規則名稱

每個規則都需要一個名稱。避免使用以開頭的名稱AWS和用於其他服務為您管理的規則群組或規則的名稱。請參閱由其他服務提供的規則群組。

> **Note**
>
> 如果您變更規則的名稱，並希望規則的量度名稱反映變更，您也必須更新量度名稱。 AWS WAF 變更規則名稱時，不會自動更新規則的度量名稱。您可以在主控台中編輯規則時，使用規則 JSON 編輯器變更量度名稱。您也可以透過 API 和任何用來定義 Web ACL 或規則群組的 JSON 清單中變更名稱。

規則陳述式

每個規則還需要規則語句來定義規則檢查 Web 請求的方式。視規則和陳述式類型而定，規則陳述式可能包含任何深度的其他巢狀陳述式。有些規則陳述式會採用一組準則。例如，您可以為 IP 集比對規則指定最多 10,000 個 IP 位址或 IP 位址範圍。

您可以定義檢查條件的規則，如下所示：

- 指令碼可能為惡意。攻擊者可以利用 web 應用程式的漏洞內嵌指令碼。這稱為跨網站指令碼 (XSS)。
- 發出請求的 IP 地址或地址範圍。
- 發出請求的國家/地區或地理位置。
- 請求的指定部分的長度，例如查詢字符串。
- SQL 程式碼可能為惡意。攻擊者會藉由內嵌惡意 SQL 程式碼於 web 請求中，嘗試從您的資料庫碼擷取資料。此稱為 SQL Injection。
- 字串會出現在請求，例如出現在 `User-Agent` 標頭的值或出現在查詢字串的文字字串。您也可以使用規則運算式 (regex) 指定這些字串。
- Web ACL 中先前規則已新增至請求的標籤。

除了具有 Web 請求檢查條件的陳述式 (如前面清單中的陳述式) 之外，還 AWS WAF 支援AND、的邏輯陳述式OR，NOT以及您用來合併規則中的陳述式。

例如，根據您最近從攻擊者看到的要求，您可能會使用邏輯AND陳述式建立規則，並結合下列巢狀陳述式：

- 來自 192.0.2.44 的請求。

- 在 User-Agent 標頭中包含 BadBot 值。
- 它們好像有包含類似 SQL 程式碼的查詢字串。

在這種情況下，Web 請求需要匹配所有語句才能與頂層匹配AND。

主題

規則動作

當 Web 請求符合規則中定義的準則時，規則動作會告訴 AWS WAF 該如何處理 Web 請求。您可以選擇性地將自訂行為新增至每個規則動作。

> **Note**
>
> 規則動作可以是終止或非終止。終止動作會停止要求的 Web ACL 評估，並允許該要求繼續執行受保護的應用程式或封鎖該要求。

以下是規則動作選項：

- Allow- AWS WAF 允許將請求轉發到受保護的 AWS 資源以進行處理和響應。這是終止動作。在您定義的規則中，您可以在要求中插入自訂標頭，然後再將其轉寄至受保護的資源。
- Block- AWS WAF 阻止請求。這是終止動作。根據預設，受保護的 AWS 資源會以 HTTP 403 (Forbidden) 狀態碼回應。在您定義的規則中，您可以自訂回應。 AWS WAF 封鎖要求時，Block 處理行動設定會決定受保護資源傳送回用戶端的回應。
- Count- AWS WAF 計算請求，但不確定是否允許或阻止它。這是非終止動作。 AWS WAF 繼續處理網頁 ACL 中的其餘規則。在您定義的規則中，您可以將自訂標題插入要求中，也可以新增其他規則可以符合的標籤。

- CAPTCHA並且 Challenge — AWS WAF 使用 CAPTCHA 謎題和無聲挑戰來驗證請求是否來自機器人，並 AWS WAF 使用令牌來跟踪最近成功的客戶響應。

  驗證碼謎題和無聲挑戰只能在瀏覽器訪問 HTTPS 端點時運行。瀏覽器客戶端必須在安全上下文中運行才能獲取令牌。

  > **Note**
  >
  > 如果您在其中一項規則中使用CAPTCHA或規Challenge則動作，或是規則群組中的規則動作覆寫，系統會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

  這些規則動作可以終止或非終止，具體取決於請求中令牌的狀態：

  - 非終止有效，未過期的令牌-如果令牌根據配置的 CAPTCHA 或挑戰免疫時間有效且未過期，則 AWS WAF 處理類似於操作的請求。Count AWS WAF 繼續根據 Web ACL 中剩餘的規則檢查 Web 請求。與Count組態類似，在您定義的規則中，您可以選擇性地使用要插入要插入要求的自訂標頭來設定這些動作，也可以新增其他規則可符合的標籤。
  - 以無效或過期權杖的封鎖要求終止 — 如果 Token 無效或指定的時間戳記已過期， AWS WAF 會終止 Web 要求的檢查並封鎖要求，類似於動作。Block AWS WAF 然後使用自定義響應代碼響應客戶端。對於CAPTCHA，如果請求內容表明客戶端瀏覽器可以處理它，則以 JavaScript 插入式方式 AWS WAF 發送 CAPTCHA 難題，該謎題旨在區分人類客戶端和機器人。對於該Challenge動作， AWS WAF 發送帶有無聲挑戰的 JavaScript 插頁式挑戰，該挑戰旨在區分普通瀏覽器和由漫遊器運行的會話。

  如需其他資訊，請參閱 CAPTCHA並Challenge在 AWS WAF。

如需有關自訂請求和回應的資訊，請參閱定制的 Web 請求和響應 AWS WAF。

如需將標籤新增至相符請求的資訊，請參閱AWS WAF 標籤, 上, 网, 請求。

如需 Web ACL 和規則設定如何互動的資訊，請參閱Web ACL 規則和規則群組評估。

規則陳述式基礎

規則陳述式是指示 AWS WAF 如何檢查 Web 要求的規則的一部分。當在 Web 請求中 AWS WAF 找到檢查標準時，我們說 Web 請求與語句匹配。視陳述式類型而定，每個規則陳述式會指定要尋找什麼以及如何尋找。

中的每個規則都 AWS WAF 有單一頂層規則陳述式，其中可以包含其他陳述式。規則陳述式可以非常簡單。例如，您可以有一個陳述式，提供一組原始國家/地區來檢查您的 Web 要求，或者您可以在 Web ACL 中有一個只參照規則群組的規則陳述式。規則陳述式也可以非常複雜。例如，您可以擁有結合許多其他陳述式與邏輯AND、OR和陳述式的陳述式的NOT陳述式。

對於大多數規則，您可以將自訂 AWS WAF 標籤新增至相符請求。 AWS 受管規則規則群組中的規則會將標籤新增至相符要求。規則新增的標籤會提供有關規則要求的資訊，這些規則稍後會在 Web ACL 中評估，以及 AWS WAF 記錄檔和量度中評估。若要取得有關標示的資訊，請參閱AWS WAF 標籤, 上, 网, 請求和標籤比對規則陳述式。

巢狀規則陳述式

AWS WAF 支持許多規則語句的嵌套，但不適用於所有規則語句。例如，您無法將規則群組陳述式嵌套在另一個陳述式中。您需要在某些情況下使用巢狀，例如範圍向下陳述式和邏輯陳述式。規則陳述式會列出下列規則詳細資料，說明每個類別和規則的巢狀功能和需求。

主控台中規則的視覺化編輯器僅支援規則陳述式的一個巢狀層級。例如，您可以在邏輯AND或OR規則內嵌許多類型的陳述式，但您無法將其他AND或OR規則巢狀化，因為這需要第二層的巢狀結構。若要實作多個層級的巢狀，請透過主控台中的 JSON 規則編輯器或透過 API 提供 JSON 中的規則定義。

主題

- Web 請求組件規格和處理
- 範圍向下語句
- 參照集或規則群組的陳述式

Web 請求組件規格和處理

本節說明您可以在檢查 Web 要求元件的規則陳述式中指定的設定。如需使用方式的詳細資訊，請參閱中的個別規則陳述式比對規則陳述式。

這些 Web 要求元件的子集也可用於以速率為基礎的規則中，做為自訂要求彙總索引鍵。如需相關資訊，請參閱以速率為基礎的規則彙總選項和索。

對於請求組件設置，您可以指定組件類型本身，以及任何其他選項，具體取決於組件類型。例如，當您檢查包含文字的組件類型時，您可以在檢查之前對其套用文字轉換。

> **Note**
>
> 除非另有說明，否則如果 Web 要求沒有在規則陳述式中指定的 request 元件，則 AWS WAF 會將要求評估為不符合規則條件。

內容

要求元件選項

本節說明您可以指定用於檢查的 Web 要求元件。您可以為尋找 Web 請求中的模式的匹配規則語句指定請求組件。這些類型的語句包括字符串匹配，正則表達式匹配，大小約束和SQL注入攻擊語句。如需如何使用這些要求元件設定的詳細資訊，請參閱個別規則陳述式：比對規則陳述式

除非另有說明，否則如果 Web 要求沒有在規則陳述式中指定的 request 元件，則 AWS WAF 會將要求評估為不符合規則條件。

> **Note**
>
> 您可以為每個需要它的規則陳述式指定單一請求元件。若要檢查請求的多個元件，請為每個元件建立規則陳述式。

主 AWS WAF 控台和API說明文件會在下列位置提供要求元件設定的指引：

- 主控台上的規則產生器 — 在一般規則類型的陳述式設定中，在 [請求元件] 下的 [檢查] 對話方塊中選擇您要檢查的元件。
- API聲明內容 — `FieldToMatch`

本節的其餘部分描述了要檢查的 Web 請求部分的選項。

主題

- HTTP 方法
- 單一標頭
- 所有標題
- 表頭順序
- Cookie
- URI路徑
- JA3指紋
- 查詢字串
- 單一查詢參數
- 所有查詢參數
- Body
- JSON身體

HTTP 方法

檢查請求的HTTP方法。該HTTP方法指出 Web 請求要求受保護的資源執行的操作類型，例如`POST`或`GET`。

單一標頭

檢查請求中的單個命名標頭。

對於此選項，您可以指定標頭名稱，例如，`User-Agent`或`Referer`。名稱的字串比對不區分大小寫。

所有標題

檢查所有要求標頭，包括 Cookie。您可以套用篩選器來檢查所有標頭的子集。

對於此選項，您可以提供下列規格：

- 匹配模式 — 用於獲取標題子集以進行檢查的過濾器。 AWS WAF 在標題鍵中查找這些模式。

  比對模式設定可以是下列其中一種：

  - 全部 — 匹配所有鍵。評估所有標題的規則檢查條件。
  - 排除的標頭 — 僅檢查其金鑰不符合您在此處指定的任何字串的標頭。鍵的字符串匹配不區分大小寫。
  - 包含的標頭 — 僅檢查具有與您在此處指定的其中一個字串相符的索引鍵的標頭。鍵的字符串匹配不區分大小寫。
- 比對範圍 — AWS WAF 應使用規則檢查條件檢查的標頭部分。您可以指定 [索引鍵]、[值] 或 [全部] 來檢查相符項目的索引鍵和值。

  A@@ ll 並不需要在鍵中找到匹配項，並在值中找到匹配項。它需要在鍵或值或兩者中找到匹配。若要在索引鍵和值中要求相符項目，請使用邏輯AND陳述式來組合兩個比對規則，一個會檢查索引鍵，另一個會檢查這些值。
- 超大處理 — AWS WAF 如何處理標頭資料大於 AWS WAF 可檢查的要求。 AWS WAF 最多可以檢查請求標頭的前 8 KB（8,192 字節），最多可以檢查前 200 個標頭。內容可供檢查，最多可 AWS WAF 達到第一個限制。您可以選擇繼續檢驗，或跳過檢驗並將請求標示為符合或不符合規則。如需處理過大內容的詳細資訊，請參閱處理超大請求組件 AWS WAF。

表頭順序

檢查包含要求標頭名稱清單的字串，依照它們在 AWS WAF 接收檢查的 Web 要求中出現的順序排列。 AWS WAF 生成字符串，然後使用該字符串作為字段以匹配其檢查中的組件。 AWS WAF 例如，用冒號和不添加空格分隔字符串中的標題名稱。`host:user-agent:accept:authorization:referer`

對於此選項，您可以提供下列規格：

- 超大處理 — AWS WAF 如何處理具有大於或大於 AWS WAF 可檢查的標頭資料的要求。 AWS WAF 最多可以檢查請求標頭的前 8 KB（8,192 字節），最多可以檢查前 200 個標頭。內容可供檢查，最多可 AWS WAF 達到第一個限制。您可以選擇繼續檢查可用的標頭，或跳過檢查並將請求標示為符合或不符合規則。如需處理過大內容的詳細資訊，請參閱處理超大請求組件 AWS WAF。

Cookie

檢查所有的請求餅乾。您可以套用篩選器來檢查所有 Cookie 的子集。

對於此選項，您可以提供下列規格：

- 匹配模式 — 用於獲取 cookie 子集以進行檢查的過濾器。 AWS WAF 會在 Cookie 金鑰中尋找這些模式。

  比對模式設定可以是下列其中一種：

  - 全部 — 匹配所有鍵。評估所有 Cookie 的規則檢查標準。
  - 排除的 Cookie — 僅檢查其鍵不符合您在此處指定的任何字串的 Cookie。密鑰的字符串匹配區分大小寫，並且必須完全相符。
  - 包含的 Cookie — 僅檢查具有與您在此處指定的其中一個字串相符的金鑰的 Cookie。密鑰的字符串匹配區分大小寫，並且必須完全相符。
- 比對範圍 — Cookie AWS WAF 應使用規則檢查條件檢查的部分。您可以為鍵和值指定「鍵」、「值」或「全部」。

  A@@ ll 並不需要在鍵中找到匹配項，並在值中找到匹配項。它需要在鍵或值或兩者中找到匹配。若要在索引鍵和值中要求相符項目，請使用邏輯AND陳述式來組合兩個比對規則，一個會檢查索引鍵，另一個會檢查這些值。
- 超大處理 — AWS WAF 如何處理 Cookie 資料大於 AWS WAF 可檢查的要求。 AWS WAF 最多可以檢查請求餅乾的前 8 KB（8,192 字節），最多可以檢查前 200 個餅乾。內容可供檢查，最多可 AWS WAF 達到第一個限制。您可以選擇繼續檢驗，或跳過檢驗並將請求標示為符合或不符合規則。如需處理過大內容的詳細資訊，請參閱處理超大請求組件 AWS WAF。

URI路徑

檢查識別資源URL的部分，例如，`/images/daily-ad.jpg`。如需詳細資訊，請參閱統一資源識別元 (URI)：一般語法。

如果您未搭配此選項使用文字轉換，則 AWS WAF 不會將文字轉換正規化URI並完全依照從要求中從用戶端接收到的方式進行檢查。如需有關文字轉換的資訊，請參閱文字轉換選項。

JA3指紋

檢查請求的JA3指紋。

> **Note**
>
> JA3指紋檢測僅適用於 Amazon CloudFront 分發和應用程式負載平衡器。

指JA3紋是從傳入要求的TLS用戶端 Hello 衍生出來的 32 個字元的雜湊。此指紋可做為用戶端TLS組態的唯一識別碼。 AWS WAF 針對具有足夠TLS用於計算的 Client Hello 資訊的每個要求，計算並記錄此指紋。幾乎所有 Web 請求都包含此信息。

如何獲取客戶端的JA3指紋

您可以從 Web ACL 日誌中獲取客戶端請求的JA3指紋。如果能 AWS WAF 夠計算指紋，它將其包含在日誌中。如需有關記錄欄位的資訊，請參閱日誌欄位。

規則陳述式需求

您只能在字串 match 陳述式中檢查JA3指紋，該陳述式設定為完全符合您提供的字串。在字串 match 陳述式規格中提供記錄中的JA3指紋字串，以符合任何 future 具有相同TLS組態的要求。如需有關字串 match 陳述式的資訊，請參閱字串比對規則陳述式。

您必須為此規則陳述式提供後援行為。後援行為是您要在無法計算JA3指紋時指派 AWS WAF 給 Web 要求 AWS WAF 的符合狀態。如果您選擇比對，請 AWS WAF 將要求視為符合規則陳述式，並將規則動作套用至請求。如果您選擇不符合，請 AWS WAF 將要求視為不符合規則陳述式。

要使用此匹配選項，您必須記錄您的網絡ACL流量。如需相關資訊，請參閱記錄 AWS WAF 網頁 ACL 流量。

查詢字串

檢查?字元之後出現URL的部分 (如果有的話)。

> **Note**
>
> 對於跨網站指令碼比對陳述式，建議您選擇 [所有查詢參數]，而不是 [查詢字串]。選擇「所有查詢參數」會增加 10 WCUs 至基本成本。

單一查詢參數

檢查您已定義為查詢字串一部分的單一查詢參數。 AWS WAF 檢查您指定的參數值。

對於此選項，您也可以指定 Query 引數。例如，如果URL是www.xyz.com?UserName=abc&SalesRegion=seattle，則可以SalesRegion為查詢引數指定UserName或。引數名稱的最大長度為 30 個字元。名稱不區分大小寫，因此如果您指定UserName，會 AWS WAF 比對的所有變體UserName，包括username和UsERName。

如果查詢字串包含您所指定之查詢引數的多個執行個體，則會使用OR邏輯 AWS WAF 檢查相符項目的所有值。例如，在中 URLwww.xyz.com?SalesRegion=boston&SalesRegion=seattle， AWS WAF 評估您針對boston和指定的名稱seattle。如果其中一個相符，則檢查會是相符。

所有查詢參數

檢查請求中的所有查詢參數。這類似於單一查詢參數元件選擇，但 AWS WAF 會檢查查詢字串內所有引數的值。例如，如果URL是www.xyz.com?UserName=abc&SalesRegion=seattle，則在的值UserName或符合檢驗條件時 AWS WAF 觸發SalesRegion相符。

選擇此選項會增WCUs加 10 個基本成本。

Body

檢查請求主體，評估為純文本。您也可以使用JSON內容類型JSON來評估主體。

要求主體是緊接在要求標頭之後的要求的一部分。它包含 Web 請求所需的任何其他數據，例如，來自表單的數據。

- 在控制台中，您可以在「請求」選項選擇「主體」下選擇「內容類型」選擇「純文本」選擇。
- 在規則的FieldToMatch規格中API，您可Body以指定以純文字檢查要求主體。

對於 Application Load Balancer AWS AppSync， AWS WAF 可以檢查要求主體的前 8 KB。對於 CloudFront，默認情況下，網API關，Amazon Cognito，應用程序運行器和驗證訪問 AWS WAF 可以檢查前 16 KB，並且您可以在 Web ACL 配置中將限制增加到 64 KB。如需詳細資訊，請參閱 管理車身檢查尺寸限制。

您必須為此元件類型指定過大處理。超大處理定義如何 AWS WAF 處理具有大於 AWS WAF 可檢查的主體資料的要求。您可以選擇繼續檢驗，或跳過檢驗並將請求標示為符合或不符合規則。如需處理過大內容的詳細資訊，請參閱處理超大請求組件 AWS WAF。

您也可以將身體評估為已解析JSON。如需相關資訊，請參閱下一節。

JSON身體

檢查請求主體，評估為JSON。您也可以將本文評估為純文字。

要求主體是緊接在要求標頭之後的要求的一部分。它包含 Web 請求所需的任何其他數據，例如，來自表單的數據。

- 在主控台中，您可以在「請求」選項選擇「主體」下選取此選項，方法是選取「內容類型」選項JSON。
- 在規則的`FieldToMatch`規格中，您可以指定`JsonBody`。API

對於 Application Load Balancer AWS AppSync， AWS WAF 可以檢查要求主體的前 8 KB。對於 CloudFront，默認情況下，網API關，Amazon Cognito，應用程序運行器和驗證訪問 AWS WAF 可以檢查前 16 KB，並且您可以在 Web ACL 配置中將限制增加到 64 KB。如需詳細資訊，請參閱 管理車身檢查尺寸限制。

您必須為此元件類型指定過大處理。超大處理定義如何 AWS WAF 處理具有大於 AWS WAF 可檢查的主體資料的要求。您可以選擇繼續檢驗，或跳過檢驗並將請求標示為符合或不符合規則。如需處理過大內容的詳細資訊，請參閱處理超大請求組件 AWS WAF。

選擇此選項會使 match 陳述式的基本成本加倍WCUs。例如，如果 match 語句的基本成本是 5 WCUs而不進行JSON解析，則使用JSON解析將成本加倍為 10 WCUs。

對於此選項，您可以提供其他規格，如下一節所述。

如何 AWS WAF 處理JSON身體檢查

當 AWS WAF 檢查 Web 請求主體時JSON，它會執行分析主體的步驟，並提取要檢查的JSON元素。AWS WAF 根據您的組態選擇執行這些步驟。

以下列出 AWS WAF 執行的步驟。

1. 剖析主體內容 — AWS WAF 剖析 Web 要求主體的內容，以擷取要檢查的JSON元素。 AWS WAF 盡力解析主體的全部內容，但解析可能會因內容中的各種錯誤狀態而失敗。範例包括無效字元、重複索引鍵、截斷，以及根節點不是物件或陣列的內容。

   「主體剖析後援行為」選項會決定如果 AWS WAF 無法完全剖析JSON主體時會發生什麼作用：

   - 無 (預設行為)-只 AWS WAF 會評估內容，直到遇到剖析錯誤的時間點為止。
   - 評估為字符串-檢查正文為純文本。 AWS WAF 將為檢驗定義的文字轉換和檢JSON驗準則套用至本文字串。

- 匹配-將 Web 請求視為與規則語句匹配。 AWS WAF 將規則動作套用至請求。
- 不匹配-將 Web 請求視為與規則語句不匹配。

> **Note**
>
> 此後援行為只有在剖析JSON字串時 AWS WAF 遇到錯誤時才會觸發。

解析未完全驗證 JSON

AWS WAF 解析不會完全驗證輸入JSON字符串，因此即使無效，解析也可以成功JSON。

例如， AWS WAF 剖析下列無效JSON而不會發生錯誤：

- 缺失逗號：`{"key1":"value1""key2":"value2"}`
- 缺失冒號：`{"key1":"value1","key2""value2"}`
- 額外冒號：`{"key1"::"value1","key2""value2"}`

對於解析成功但結果不完全有效的情況下JSON，評估中後續步驟的結果可能會有所不同。擷取可能會遺漏某些元素，或規則評估可能會產生非預期的結果。我們建議您驗證您在JSON應用程式中收到的資訊，並視需JSON要處理無效。

2. 擷取JSON元素 — 根據您的設定 AWS WAF 識別要檢查的JSON元素子集：
   - 選項JSON匹配範圍指定的元素的類型 AWS WAF 應JSON該檢查。

     您可以為鍵和值指定「鍵」、「值」或「全部」。

     A@@ ll 並不需要在鍵中找到匹配項，並在值中找到匹配項。它需要在鍵或值或兩者中找到匹配。若要在索引鍵和值中要求相符項目，請使用邏輯AND陳述式來組合兩個比對規則，一個會檢查索引鍵，另一個會檢查這些值。
   - 要檢查的「內容」選項指定如何篩選元素集為您 AWS WAF 要檢查的子集。

     您必須指定下列其中一項：
     - 完整JSON內容-評估所有元素。
     - 僅包含的圖元-僅評估其路徑符合您提供的JSON指標條件的圖元。請勿使用此選項來指示中的所有路徑JSON。請改用「完整JSON內容」。

       如需有關JSON指標語法的資訊，請參閱網際網路工程工作小組 (IETF) 文JavaScript 件物件符號 (JSON) 指標。

例如，在控制台中，您可以提供以下內容：

```
/dogs/0/name
/dogs/1/name
```

在API或中CLI，您可以提供下列資訊：

```
"IncludedPaths": ["/dogs/0/name", "/dogs/1/name"]
```

例如，假設「要檢查的內容」設定為「僅包含的元素」，而包含的元素設定為/a/b。

對於以下示例JSON主體：

```
{
  "a":{
    "c":"d",
    "b":{
      "e":{
        "f":"g"
      }
    }
  }
}
```

下面列出了 AWS WAF 將檢查每個JSON匹配範圍設置的元素集。請注意b，密鑰（屬於包含元素路徑的一部分）不進行評估。

- 全部：e、f,和g。
- 按鍵：e和f。
- 價值觀：g。

3. 檢查JSON元素集 — 將您指定的任何文字轉換 AWS WAF 套用至擷取的元JSON素，然後將結果元素集與規則陳述式的符合條件進行比對。這與其他 Web 要求元件的轉換和評估行為相同。如果有任何擷取的JSON元素相符，則 Web 要求就會與規則相符。

轉送的 IP 位址

本節適用於使用 Web 要求之 IP 位址的規則陳述式。依預設， AWS WAF 會使用來自 Web 請求來源的 IP 位址。但是，如果 Web 請求通過一個或多個代理或負載平衡器，則 Web 請求源將包含最後一個

代理的地址，而不是客戶端的原始地址。在這種情況下，原始客戶端地址通常在另一個 HTTP 標頭轉發。這個標頭通常是X-Forwarded-For（XFF），但它可以是不同的。

使用 IP 位址的規則陳述式

使用 IP 位址的規則陳述式如下：

- IP 集合比對-檢查 IP 位址是否符合 IP 集中定義的位址。
- 地理比對-使用 IP 地址確定原產國家和地區，並與國家/地區列表匹配原產國。
- 速率型規則陳述式-可以透過 IP 位址彙總要求，以確保沒有任何個別 IP 位址以過高的速率傳送要求。您可以單獨使用 IP 位址彙總，也可以與其他彙總金鑰結合使用。

您可以指示 AWS WAF 針對任何這些規則陳述式 (從X-Forwarded-For標頭或其他 HTTP 標頭) 使用轉送的 IP 位址，而不是使用 Web 要求的來源。如需如何提供規格的詳細資訊，請參閱個別規則陳述式類型的指引。

> **Note**
>
> 如果您指定的標頭不存在於要求中，則完全 AWS WAF 不會將規則套用至 Web 要求。

後援行為

當您使用轉寄的 IP 位址時，如果要求在指定位置沒有有效的 IP 位址，則指定要指派給 Web 要求的符合狀態： AWS WAF

- 匹配-將 Web 請求視為與規則語句匹配。 AWS WAF 將規則動作套用至請求。
- 不匹配-將 Web 請求視為與規則語句不匹配。

AWS WAF 機器人控制中使用的 IP 位址

機器人控制受管規則群組會使用來自的 IP 位址來 AWS WAF驗證機器人。如果您使用 Bot Control，且已驗證透過 Proxy 或負載平衡器路由的機器人，則需要使用自訂規則明確允許這些機器人。例如，您可以設定自訂 IP 集比對規則，該規則使用轉寄的 IP 位址來偵測並允許已驗證的機器人。您可以透過多種方式使用此規則來自訂機器人管理。如需詳細資訊和範例，請參閱 AWS WAF 機器人控制。

使用轉送 IP 位址的一般考量

使用轉寄的 IP 位址之前，請注意下列一般警告：

- 頭可以通過沿途代理進行修改，並且代理可能以不同的方式處理頭。
- 攻擊者可能會改變標頭的內容以嘗試繞過 AWS WAF 檢查。
- 標頭內的 IP 位址可能格式錯誤或無效。
- 您指定的標頭可能根本不存在於請求中。

搭配使用轉送 IP 位址的注意事項 AWS WAF

下列清單說明在中使用轉寄 IP 位址的需求和注意事項： AWS WAF

- 對於任何單一規則，您可以為轉寄的 IP 位址指定一個標頭。標頭規格不區分大小寫。
- 對於以速率為基礎的規則陳述式，任何巢狀範圍陳述式都不會繼承轉送的 IP 設定。指定使用轉送 IP 位址之每個陳述式的組態。
- 對於地理比對和速率型規則，請 AWS WAF 使用標頭中的第一個位址。例如，如果一個標題包含 `10.1.1.1, 127.0.0.0, 10.10.10.10` AWS WAF use `10.1.1.1`
- 對於 IP 集匹配，您可以指出是否匹配標題中的第一個，最後一個還是任何地址。如果您指定任何位址，則會 AWS WAF 檢查標頭中的所有位址是否有相符項目，最多可檢查 10 個位址。如果標頭包含 10 個以上的位址，則 AWS WAF 會檢查最後 10 個位址。
- 包含多個地址的標頭必須在地址之間使用逗號分隔符號。如果要求使用逗號以外的分隔符號，請 AWS WAF 考慮標頭中格式錯誤的 IP 位址。
- 如果標頭內的 IP 位址格式錯誤或無效，請根據您在轉送的 IP 組態中 AWS WAF 指定的後援行為，將 Web 要求指定為符合規則或不相符。
- 如果您指定的標頭不存在於要求中，則完全 AWS WAF 不會將規則套用至要求。這表示 AWS WAF 不會套用規則動作，也不會套用後援行為。
- 使用轉寄 IP 標頭作為 IP 位址的規則陳述式不會使用 Web 要求來源報告的 IP 位址。

搭配使用轉寄 IP 位址的最佳做法 AWS WAF

當您使用轉寄的 IP 位址時，請遵循下列最佳作法：

- 在啟用轉送的 IP 配置之前，請仔細考慮請求標頭的所有可能狀態。您可能需要使用多個規則來取得您想要的行為。
- 若要檢查多個轉寄的 IP 標頭，或檢查 Web 要求來源和轉寄的 IP 標頭，請針對每個 IP 位址來源使用一個規則。
- 若要封鎖具有無效標頭的 Web 要求，請將規則動作設定為封鎖，並將轉送的 IP 組態的後援行為設定為符合。

轉寄 IP 位址的 JSON 範例

只有當X-Forwarded-For標頭包含原產國家/地區為的 IP 時，才會符合下列 geo match 陳述式US：

```
{
  "Name": "XFFTestGeo",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "XFFTestGeo"
  },
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ],
      "ForwardedIPConfig": {
        "HeaderName": "x-forwarded-for",
        "FallbackBehavior": "MATCH"
      }
    }
  }
}
```

下列以速率為基礎的規則會根據標頭中的第一個 IP 彙總要求。X-Forwarded-For此規則只會計算符合巢狀 geo match 陳述式的要求，而且只會封鎖符合 geo match 陳述式的要求。巢狀地理配對陳述式也會使用X-Forwarded-For標頭來判斷 IP 位址是否指出來自的國家/地區US。如果是這樣，或者如果標頭存在但格式錯誤，則 geo match 語句返回一個匹配。

```
{
  "Name": "XFFTestRateGeo",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
```

```
    "MetricName": "XFFTestRateGeo"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": "100",
      "AggregateKeyType": "FORWARDED_IP",
      "ScopeDownStatement": {
        "GeoMatchStatement": {
          "CountryCodes": [
            "US"
          ],
          "ForwardedIPConfig": {
            "HeaderName": "x-forwarded-for",
            "FallbackBehavior": "MATCH"
          }
        }
      },
      "ForwardedIPConfig": {
        "HeaderName": "x-forwarded-for",
        "FallbackBehavior": "MATCH"
      }
    }
  }
}
```

用於檢查 HTTP/2 偽標頭的選項

支援 HTTP/2 流量的受保護 AWS 資源不會將 HTTP/2 虛擬標頭轉寄至進行檢查，但它們會在檢查的 Web 要 AWS WAF 求元件中提供虛擬標頭的內容。 AWS WAF

您可以 AWS WAF 使用僅檢查下表中列出的虛擬標頭。

HTTP/2 映射到網絡請求組件的偽頭內容

HTTP/2 偽頭文件	要檢查的 Web 要求元件	文件
`:method`	HTTP 方法	HTTP 方法
`:authority`	`Host` 標頭	單一標頭 所有標題

HTTP/2 偽頭文件	要檢查的 Web 要求元件	文件
`:path`URI 路徑	URI 路徑	URI路徑
`:path` 查詢	查詢字串	查詢字串 單一查詢參數 所有查詢參數

文字轉換選項

在尋找模式或設定條件約束的陳述式中，您可以在檢查請求之前提供 AWS WAF 要套用的轉換。轉換會將 Web 請求重新格式化，以避免攻擊者用來試圖略過 AWS WAF的某些異常格式。

當您將此選項與 JSON 主體要求元件選取搭配使用時，會在剖析並擷取要從 JSON 檢查的元素之後 AWS WAF 套用您的轉換。如需詳細資訊，請參閱 JSON身體。

如果您提供多個轉換，您也可以設定讓 AWS WAF 套用它們的順序。

WCU — 每個文字轉換都是 10 個 WCU。

主 AWS WAF 控台和 API 文件也會在下列位置提供這些設定的指引：

- 主控台上的規則產生器 — 文字轉換。當您使用請求元件時，此選項可供使用。
- API 陳述式內容 — `TextTransformations`

文字轉換的選項

每個轉換清單都會顯示主控台和 API 規格，後面接著說明。

Base64 decode – `BASE64_DECODE`

AWS WAF 解碼一個以 BAS64 編碼的字符串。

Base64 decode extension – `BASE64_DECODE_EXT`

AWS WAF 解碼一個 Base64 編碼的字符串，但使用一個寬容的實現忽略無效的字符。

Command line – CMD_LINE

此選項可緩解攻擊者可能注入作業系統命令列命令，並使用不尋常的格式來掩飾部分或全部命令的情況。

使用此選項可執行下列轉換：

- 刪除以下字元：\ " ' ^
- 刪除以下字元前的空格：/ (
- 將以下字元取代為空格：, ;
- 將數個空格取代為一個空格
- 將大寫字母 A-Z 轉換成小寫字母 a-z

Compress whitespace – COMPRESS_WHITE_SPACE

AWS WAF 以一個空格取代多個空格，並以空格字元 (ASCII 32) 取代下列字元，以壓縮空格：

- 進紙 (12)
- 標籤頁 (ASCII 碼 9)
- 新行 (十字军)
- 回車符
- 「垂直」頁籤 (11)
- 非中斷空格

CSS decode – CSS_DECODE

AWS WAF 解碼使用 CSS 2.x 轉義規則編碼的字符。syndata.html#characters此函數在解碼過程中最多使用兩個位元組，因此它可以幫助您發現使用 CSS 編碼進行編碼的 ASCII 字元 (這些字元通常不會被編碼)。它在反擊逃脫方面也很有用，後者是反斜線和非十六進位字元的組合。例如，javascript 的 ja\vascript。

Escape sequences decode – ESCAPE_SEQ_DECODE

AWS WAF 解碼以下 ANSI C 轉義序列：\a,,\b,,\f,\n,,\r,\t,\v,,\\, \? \'\", \xHH (十六進制), \0000 (八進制)。無效的編碼會保留在輸出中。

Hex decode – HEX_DECODE

AWS WAF 將十六進制字符串解碼為二進制。

HTML entity decode – HTML_ENTITY_DECODE

AWS WAF 以相應的字元取代以十六進位格式&#xhhhh;或十進位格&#nnnn;式表示的字元。

AWS WAF 以未編碼的字元取代下列 HTML 編碼字元。此清單使用小寫 HTML 編碼，但處理方式不區分大小寫，例如&QuOt;，"處理方式相同。

HTML 編碼的字元	替換為...
"	"
&	&
<	<
>	>
或	非中斷空格，小數 160
\n，十進位數 10
	\t，十進位 9
{ 或 {	{
|、| 或		|
} 或 }	}
!	!
#	#
$	$
&percent; 或 %	%
'	\
(	(
)	)
* 或 *	*
+	+

HTML 編碼的字元	替換為...
,	,
.	.
/	/
:	:
;	;
=	=
?	?
˜ 或 ˜	~
−	-
[或 [	[
\	\\
] 或]	]
&hat;	^
_ 或 &underbar;	_
` 或 `	`

JS decode – JS_DECODE

AWS WAF 解碼 JavaScript 轉義序列。如果\uHHHH程式碼位於的全寬 ASCII 碼範圍內FF01-FF5E，則會使用較高的位元組來偵測並調整較低的位元組。如果不是，則只會使用較低的位元組，並將較高的位元組歸零，而這可能導致資訊遺失。

Lowercase – LOWERCASE

AWS WAF 將大寫字母 (A-Z) 轉換為小寫字母 (a-z)。

MD5 – MD5

AWS WAF 從輸入中的資料計算 MD5 雜湊值。計算出的雜湊是原始二進位形式。

None – NONE

AWS WAF 檢查接收到的 Web 請求，沒有任何文本轉換。

Normalize path – NORMALIZE_PATH

AWS WAF 通過刪除多個斜杠，目錄自引用和不在輸入開頭的目錄反向引用來標準化輸入字符串。

Normalize path Windows – NORMALIZE_PATH_WIN

AWS WAF 將反斜線字元轉換為正斜線，然後使用轉換處理產生的NORMALIZE_PATH字串。

Remove nulls – REMOVE_NULLS

AWS WAF 從輸入中刪除所有NULL字節。

Replace comments – REPLACE_COMMENTS

AWS WAF 用單個空格替換每次出現的 C 風格註釋（/*... */）。它不會壓縮多個連續出現的次數。它用空格（ASCII 0x20）替換未終止的註釋。它不會更改評論的獨立終止（*/）。

Replace nulls – REPLACE_NULLS

AWS WAF 以空格字NULL元 (ASCII 0x20) 取代輸入中的每個位元組。

SQL hex decode – SQL_HEX_DECODE

AWS WAF 解碼 SQL 十六進制數據。例如， AWS WAF 解碼 (0x414243) 到 (ABC)。

URL decode – URL_DECODE

AWS WAF 解碼 URL 編碼的值。

URL decode Unicode – URL_DECODE_UNI

像URL_DECODE，但支持特定於微軟%u的編碼。如果代碼是在 FF01-FF5E 的全形 ASCII 碼範圍內，則使用較高的位元組來偵測和調整較低的位元組。否則，只會使用較低的位元組，而較高的位元組會歸零。

UTF8 to Unicode – UTF8_TO_UNICODE

AWS WAF 將所有 UTF-8 字符序列轉換為統一碼。這有助於規範化輸入，並最大限度地減少非英語語言的誤報和誤報。

範圍向下語句

scope-down 陳述式是可嵌入的規則陳述式，您可以在受管規則群組陳述式或以速率為基礎的陳述式中加入，以縮小包含規則評估的要求集。包含規則只會評估第一個符合範圍向下陳述式的要求。

- 受管規則群組陳述式 — 如果您將範圍向下陳述式新增至受管規則群組陳述式，則會將任何不符合範圍下來陳述式的要求 AWS WAF 評估為不符合規則群組。只有符合範圍向下陳述式的要求才會根據規則群組進行評估。對於根據評估的請求數量定價的受管規則群組，向下範圍陳述式可協助控制成本。

  如需有關受管規則群組陳述式的詳細資訊，請參閱管理規則群組陳述式。
- 以速率為基礎的規則陳述式 — 不含計分陳述式費率的速率型規則陳述式，會限制規則評估的所有要求。如果您只想控制特定請求分類的費率，請將範圍向下陳述式新增至以費率為基準的規則。例如，若要僅追蹤和控制來自特定地理區域的要求速率，您可以在地理比對陳述式中指定該地理區域，並將其新增至以速率為基礎的規則中，做為範圍向下陳述式。

  如需以速率為基礎的規則陳述式的詳細資訊，請參閱 速率型規則陳述式

您可以在範圍語句中使用任何嵌套規則。如需可用陳述式，請參閱比對規則陳述式和邏輯規則陳述式。向下範圍陳述式的 WCU 是您在其中定義的規則陳述式所需的 WCU。使用範圍語句沒有額外的費用。

您可以使用與在一般規則中使用陳述式時相同的方式來設定範圍向下陳述式。例如，您可以將文字轉換套用至要檢查的 Web 要求元件，也可以指定轉寄的 IP 位址做為 IP 位址。這些組態僅適用於範圍式陳述式，不會由包含的受管規則群組或以速率為基礎的規則陳述式繼承。

例如，如果您將文字轉換套用至 scopeup 陳述式中的查詢字串，scope-down 陳述式會在套用轉換之後檢查查詢字串。如果要求符合範圍向下陳述式條件， AWS WAF 則會將 Web 要求以其原始狀態傳遞至包含規則，而不會進行範圍向下陳述式的轉換。包含 scope-down 陳述式的規則可能會套用其本身的文字轉換，但不會繼承任何來自範圍向下陳述式的文字轉換。

您不能使用範圍向下語句來為包含規則語句指定任何請求檢查配置。您不能將範圍語句用作包含規則語句的 Web 請求預處理器。範圍式陳述式的唯一角色是判斷哪些要求會傳送至包含的規則陳述式以進行檢查。

參照集或規則群組的陳述式

有些規則使用可重複使用且在 Web ACL 之外管理的實體，無論是由您或 AWS Marketplace 賣家。AWS更新可重複使用的實體時， AWS WAF 會將更新傳播至您的規則。例如，如果您在 Web ACL 中使用「 AWS 受管規則」規則群組，則在 AWS 更新規則群組時，會將變更 AWS 傳播至 Web ACL，

以更新其行為。如果您在規則中使用 IP set 陳述式，則當您更新集合時，會將變更 AWS WAF 傳播到參照它的所有規則，因此任何使用這些規則的 Web ACL 都會 up-to-date 與您的變更一起保留。

以下是您可以在規則陳述式中使用的可重複使用的實體。

- IP 集 — 您可以建立和管理自己的 IP 集。在主控台上，您可以從導覽窗格存取這些項目。如需管理 IP 集合的相關資訊，請參閱 IP 集和正則表達式模式集 AWS WAF。
- 正則表達式匹配集-您創建和管理自己的正則表達式匹配集。在主控台上，您可以從導覽窗格存取這些項目。如需管理規則運算式模式集的相關資訊，請參閱 IP 集和正則表達式模式集 AWS WAF。
- AWS 受管規則規則群組 — AWS 管理這些規則群組。在主控台上，當您將受管規則群組新增至 Web ACL 時，就可以使用這些設定。如需這些項目的詳細資訊，請參閱AWS 受管規則規則群組清單。
- AWS Marketplace 受管規則群組 — AWS Marketplace 賣家可以管理這些規則群組，您可以訂閱他們以使用這些規則群組。若要管理您的訂閱，請在主控台的導覽窗格中選擇 AWS Marketplace。當您將 AWS Marketplace 受管規則群組新增至 Web ACL 時，會列出受管規則群組。對於尚未訂閱的規則群組，您也可以 AWS Marketplace 在該頁面上找到指向的連結。如需 AWS Marketplace 賣家管理規則群組的詳細資料，請參閱AWS Marketplace 受管規則群組。
- 您自己的規則群組 — 您可以管理自己的規則群組，通常當您需要某些無法透過受管規則群組執行的行為時。在主控台上，您可以從導覽窗格存取這些項目。如需詳細資訊，請參閱 管理您自己的規則群組。

刪除參考集或規則群組

刪除參照的實體時，請 AWS WAF 檢查該實體目前是否正在 Web ACL 中使用。如果 AWS WAF 發現它正在使用中，它會警告您。 AWS WAF 幾乎總是能夠確定某個實體是否被 Web ACL 引用。但是在極少數的情況下，它也可能無法判斷。如果您需要確定要刪除的實體未在使用中，請在 Web ACL 中檢查它，然後再刪除它。

比對規則陳述式

比對陳述式會將 Web 要求或其來源與您提供的條件進行比較。對於此類型的許多陳述式， AWS WAF 比較要求的特定元件是否符合內容。

匹配語句是嵌套的。您可以在邏輯規則語句中嵌套任何這些語句，並且可以在 scope-down 語句中使用它們。如需邏輯規則陳述式的資訊，請參閱邏輯規則陳述式。如需有關向下範圍陳述式的資訊，請參閱。範圍向下語句

此表格說明您可以新增至規則的一般比對陳述式，並提供一些計算各項 Web ACL 容量單位 (WCU) 使用狀況的準則。如需 WCU 的相關資訊，請參閱 AWS WAF 網路 ACL 容量單位 (WCU)。

比對陳述式	描述	WCU
地理比對	檢查要求的原產國，並為原產國家和地區套用標籤。	1
IP 集合比對	根據一組 IP 位址和位址範圍檢查要求。	大多數情況下為 1。如果您將陳述式設定為使用具有轉寄 IP 位址的標頭，並在的標頭中指定位置Any，則將 WCU 增加 4。
標籤比對規則陳述式	檢查要求是否有已由相同 Web ACL 中其他規則新增的標籤。	1
正則表達式匹配規則	比較指定的請求組件的正則表達式模式。	3、作為基礎成本。 如果您使用要求元件所有查詢參數，請新增 10 個 WCU。如果您使用要求元件 JSON 主體，則將基本成本的 WCU 加倍。針對您套用的每個文字轉換，新增 10 個 WCU。
規則運算式模式集	將規則運算式模式與指定的請求元件比較。	每個模式集 25 個，作為基本成本。 如果您使用要求元件所有查詢參數，請新增 10 個 WCU。如果您使用要求元件 JSON 主體，則將基本成本的 WCU 加倍。針對您套用的每個文字轉換，新增 10 個 WCU。
大小約束	針對指定的請求元件檢查大小約束。	1、作為基礎成本。 如果您使用要求元件所有查詢參數，請新增 10 個 WCU。

比對陳述式	描述	WCU
		如果您使用要求元件 JSON 主體，則將基本成本的 WCU 加倍。針對您套用的每個文字轉換，新增 10 個 WCU。
SQLi 攻擊	檢查指定請求元件中的惡意 SQL 程式碼。	20、作為基礎成本。 如果您使用要求元件所有查詢參數，請新增 10 個 WCU。 如果您使用要求元件 JSON 主體，則將基本成本的 WCU 加倍。針對您套用的每個文字轉換，新增 10 個 WCU。
字串比對	比較字串與指定的請求元件。	基本成本取決於字符串匹配的類型，並且介於 1 和 10 之間。 如果您使用要求元件所有查詢參數，請新增 10 個 WCU。 如果您使用要求元件 JSON 主體，則將基本成本的 WCU 加倍。針對您套用的每個文字轉換，新增 10 個 WCU。
XSS 指令碼攻擊	檢查指定請求元件中的跨網站指令碼攻擊。	40、作為基礎成本。 如果您使用要求元件所有查詢參數，請新增 10 個 WCU。 如果您使用要求元件 JSON 主體，則將基本成本的 WCU 加倍。針對您套用的每個文字轉換，新增 10 個 WCU。

地理比對規則陳述式

使用地理位置或地理位置比對陳述式，根據來源國家和地區來管理 Web 請求。地理匹配聲明會在 Web 請求中添加標籤，以指示原產國和原產地區。無論陳述式條件是否與要求相符，它都會新增這些標籤。geo match 陳述式也會針對要求的原始國家/地區執行比對。

如何使用地理匹配語句

您可以使用 geo match 陳述式進行國家或地區比對，如下所示：

- 國家/地區 — 您可以單獨使用地理位置比對規則，僅根據其來源國來管理請求。規則陳述式會與國家/地區代碼相符。您也可以使用符合原產國標籤的標籤比對規則來遵循地理位置比對規則。
- 區域 — 使用地理比對規則後跟標籤比對規則，根據其來源地區管理請求。您無法單獨使用地理比對規則來比對地區代碼。

若要取得有關使用標示相符規則的資訊，請參閱標籤比對規則陳述式和AWS WAF 標籤, 上, 网, 請求。

地理匹配語句的工作原理

使用 geo match 語句， AWS WAF 管理每個網絡請求，如下所示：

1. 判斷請求的國家和地區代碼 — 根據要求的 IP 位址 AWS WAF 決定要求的國家和地區。依預設， AWS WAF 會使用 Web 要求來源的 IP 位址。您可以指示 AWS WAF 使用替代要求標頭的 IP 位址，例如`X-Forwarded-For`，在規則陳述式設定中啟用轉送的 IP 組態。

   AWS WAF 確定使用 MaxMind GeoIP 數據庫請求的位置。MaxMind 雖然準確性因國家/地區和 IP 類型等因素而異，但在國家/地區層面報告其數據的準確性非常高。如需有關的詳細資訊 MaxMind，請參閱 MaxMind IP 地理位置。如果您認為任何 GeoIP 數據不正確，可以通過「正確的 GeoIP2 數據」向 Maxmind 提交更MaxMind 正請求。

   AWS WAF 使用國際標準化組織 (ISO) 3166 標準中的英文字母 2 國家和地區代碼。您可以在以下位置找到代碼：

   - 在 ISO 網站上，您可以在 ISO 在線瀏覽平台（OBP）搜索國家代碼。
   - 在維基百科上，國家/地區代碼列在 ISO 316 6-2。

     某個國家/地區的地區代碼會列在 URL 中`https://en.wikipedia.org/wiki/ISO_3166-2:<ISO country code>`。例如，對於美國的區域是在 ISO 3166-2：美國，而對於烏克蘭，他們是在 ISO 3166-2: UA。

2. 確定要新增到要求的國家/地區標籤 — 這些標籤會指出 geo match 陳述式是使用原始 IP 還是轉送的 IP 設定。
   - 原產地 IP

     國家/地區標籤是awswaf:clientip:geo:country:*<ISO country code>*。美國的例子：awswaf:clientip:geo:country:US。

     區域標籤為awswaf:clientip:geo:region:*<ISO country code>*-*<ISO region code>*。美國奧勒岡州的範例：awswaf:clientip:geo:region:US-OR。
   - 已轉送的 IP

     國家/地區標籤是awswaf:forwardedip:geo:country:*<ISO country code>*。美國的例子：awswaf:forwardedip:geo:country:US。

     區域標籤為awswaf:forwardedip:geo:region:*<ISO country code>*-*<ISO region code>*。美國奧勒岡州的範例：awswaf:forwardedip:geo:region:US-OR。

   如果國家或地區碼不適用於請求的指定 IP 位址，請XX在標籤中 AWS WAF 使用，取代值。例如，以下標籤適用於國家/地區代碼無法使用的用戶端 IP：awswaf:clientip:geo:country:XX以下標籤適用於轉送的 IP，其國家是美國，但其區域代碼不可用：awswaf:forwardedip:geo:region:US-XX。
3. 根據規則評估請求的國家/地區代碼

geo match 陳述式會將國家/地區標籤新增至檢查的所有請求，無論是否找到相符項目。

> **Note**
>
> AWS WAF 在規則的 Web 要求評估結束時新增任何標籤。因此，您針對 geo match 陳述式中標籤使用的任何標籤比對，都必須在與包含 geo match 陳述式的規則不同的規則中定義。

如果您只想檢查地區值，則可以使用Count動作和單一國家/地區代碼比對來撰寫地理比對規則，然後再加上區域標籤的標籤比對規則。您需要提供國家/地區代碼，以便進行評估，即使是這種方法也是如此。您可以指定不太可能成為網站流量來源的國家/地區，以減少記錄和計算指標。

CloudFront 分佈和地 CloudFront 理限制功能

對於 CloudFront 分發，如果您使用 CloudFront 地理限制功能，請注意該功能不會將被阻止的請求轉發給 AWS WAF。它會將允許的要求轉寄給 AWS WAF。如果您想要根據地理位置加上您可以在中指定

的其他條件封鎖要求 AWS WAF，請使用 AWS WAF geo match 陳述式，而不要使用地理區域限制功能。 CloudFront

地理匹配語句特徵

嵌套-您可以嵌套此語句類型。

WCU — 1 WCU.

設定 — 此陳述式使用下列設定：

- 國家/地區代碼 — 要比較地理位置比對的國家/地區代碼陣列。這些代碼必須是兩個字元的國家/地區代碼，來自 ISO 3166 國際標準的 2 個國家/地區代碼，例如，。`["US","CN"]`
- (選擇性) 轉送的 IP 組態 — 依預設， AWS WAF 會使用 Web 請求來源中的 IP 位址來判斷來源國家/地區。或者，您可以將規則配置為在 HTTP 標頭中使用轉發的 IPX-Forwarded-For，例如。 AWS WAF 使用標頭中的第一個 IP 位址。透過此設定，您也可以指定後援行為，以套用至標頭中具有格式錯誤 IP 位址的 Web 要求。後援行為會設定要求的相符結果，以符合或不相符。如需詳細資訊，請參閱 轉送的 IP 位址。

在哪裡可以找到這個規則聲明

- 主控台上的規則產生器 — 對於「請求」選項，請選擇來自中的國家/地區。
- API — GeoMatchStatement

範例

您可以使用 geo match 聲明來管理來自特定國家或地區的請求。例如，如果您想要封鎖來自特定國家/地區的要求，但仍允許來自這些國家/地區的特定 IP 位址集的要求，您可以建立規則，將動作設為，Block並以虛擬程式碼顯示下列巢狀陳述式：

- AND 陳述式
  - 列出您要封鎖的國家/地區的地理比對陳述式
  - NOT 陳述式
    - IP 集合陳述式，指定您要允許通過的 IP 地址

或者，如果您想要封鎖某些國家/地區的某些地區，但仍允許來自這些國家/地區其他地區的要求，您可以先定義地理比對規則，並將動作設為Count。然後，定義與新增的地理匹配標籤匹配標籤匹配的標籤匹配規則，並根據需要處理請求。

下列虛擬程式碼說明此方法的範例：

1. Geo match 陳述式會列出您要封鎖地區的國家/地區，但動作設定為 [計數]。這會標記每個 Web 請求，而不論匹配狀態如何，它還為您提供了計算感興趣國家/地區的指標。
2. AND含封鎖動作的陳述式
   - Label match 語句，用於指定要阻止的國家/地區的標籤
   - NOT 陳述式
     - Label match 語句，用於指定您要允許通過的國家/地區中的地區的標籤

下列 JSON 清單顯示先前虛擬程式碼中描述的兩個規則的實作。這些規則會封鎖來自美國的所有流量，但來自俄勒岡州和華盛頓的流量除外。geo match 陳述式會在檢查的所有請求中新增國家和地區標籤。標籤比對規則會在地理比對規則之後執行，因此它可以與地理比對規則剛新增的國家和地區標籤進行比對。地理比對陳述式會使用轉送的 IP 位址，因此標籤比對也會指定轉寄的 IP 標籤。

```
{
   "Name": "geoMatchForLabels",
   "Priority": 10,
   "Statement": {
     "GeoMatchStatement": {
       "CountryCodes": [
         "US"
       ],
       "ForwardedIPConfig": {
           "HeaderName": "X-Forwarded-For",
           "FallbackBehavior": "MATCH"
       }
     }
   },
   "Action": {
     "Count": {}
   },
   "VisibilityConfig": {
     "SampledRequestsEnabled": true,
     "CloudWatchMetricsEnabled": true,
     "MetricName": "geoMatchForLabels"
   }
},
{
   "Name": "blockUSButNotOROrWA",
   "Priority": 11,
```

```
   "Statement": {
     "AndStatement": {
       "Statements": [
         {
           "LabelMatchStatement": {
             "Scope": "LABEL",
             "Key": "awswaf:forwardedip:geo:country:US"
           }
         },
         {
           "NotStatement": {
             "Statement": {
                "OrStatement": {
                  "Statements": [
                    {
                       "LabelMatchStatement": {
                         "Scope": "LABEL",
                         "Key": "awswaf:forwardedip:geo:region:US-OR"
                       }
                    },
                    {
                       "LabelMatchStatement": {
                         "Scope": "LABEL",
                         "Key": "awswaf:forwardedip:geo:region:US-WA"
                       }
                    }
                  ]
                }
             }
           }
         }
       ]
     }
   },
   "Action": {
     "Block": {}
   },
   "VisibilityConfig": {
     "SampledRequestsEnabled": true,
     "CloudWatchMetricsEnabled": true,
     "MetricName": "blockUSButNotOROrWA"
   }
}
```

另一個範例是，您可以將地理比對與以速率為基礎的規則結合起來，為特定國家或地區的使用者排定資源的優先順序 您可以針對用來區分使用者的每個地理位置比對或標籤比對陳述式，建立不同的以速率為基礎的陳述式。為偏好國家或地區的使用者設定較高的費率限制，並為其他使用者設定較低的費率限制。

下列 JSON 清單顯示地理區域比對規則，其後是以速率為基礎的規則，以限制來自美國的流量。該規則允許來自俄勒岡州的流量以比來自該國其他任何地方的流量進入的速度更高。

```
{
  "Name": "geoMatchForLabels",
  "Priority": 190,
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ]
    }
  },
  "Action": {
    "Count": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "geoMatchForLabels"
  }
},
{
  "Name": "rateLimitOregon",
  "Priority": 195,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 3000,
      "AggregateKeyType": "IP",
      "ScopeDownStatement": {
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "awswaf:clientip:geo:region:US-OR"
        }
      }
    }
  },
  "Action": {
```

```
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "rateLimitOregon"
  }
},
{
  "Name": "rateLimitUSNotOR",
  "Priority": 200,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "AggregateKeyType": "IP",
      "ScopeDownStatement": {
        "AndStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:clientip:geo:country:US"
              }
            },
            {
              "NotStatement": {
                "Statement": {
                  "LabelMatchStatement": {
                    "Scope": "LABEL",
                    "Key": "awswaf:clientip:geo:region:US-OR"
                  }
                }
              }
            }
          ]
        }
      }
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
```

```
    "CloudWatchMetricsEnabled": true,
    "MetricName": "rateLimitUSNotOR"
  }
}
```

IP 集合比對規則陳述式

IP 集比對陳述式會根據一組 IP 位址和位址範圍檢查 Web 要求的 IP 位址。使用此選項以根據請求源自的 IP 地址來允許或封鎖 Web 請求。根據預設， AWS WAF 會使用來自 Web 要求來源的 IP 位址，但您可以將規則設定為`X-Forwarded-For`改用 HTTP 標頭。

AWS WAF 支援所有 IPv4 和 IPv6 CIDR 範圍，除了. `/0` 如需 CIDR 符號表示法的詳細資訊，請參閱 Wikipedia 項目無類別域間路由。一個 IP 集合最多可容納 10,000 個 IP 地址或 IP 地址範圍進行檢查。

> **Note**
>
> 每個 IP 集合比對規則都會參考一個 IP 集合，您可以獨立於規則而建立和維護。您可以在多個規則中使用單一 IP 集，當您更新參照集時， AWS WAF 會自動更新所有參照該 IP 集的規則。如需建立和管理 IP 集的資訊，請參閱建立和管理 IP 集合。

當您新增或更新規則群組或 Web ACL 中的規則時，請選擇 IP set (IP 集合) 選項，並選取要使用的 IP 集合名稱。

嵌套-您可以嵌套此語句類型。

WCU — 大多數的 1 WCU。如果您將陳述式設定為使用轉送的 IP 位址並指定的位置ANY，請將 WCU 使用量增加 4。

這個陳述式會使用下列設定：

- IP 集規格 — 從清單中選擇您要使用的 IP 集，或建立新 IP 集。
- (選擇性) 已轉送 IP 組態 — 替代要用來取代要求來源的轉寄 IP 標頭名稱。您可以指定是否要比對標頭中的第一個、最後一個或任何位址。您也可以指定後援行為，以套用至指定標頭中具有格式錯誤 IP 位址的 Web 要求。後援行為會設定要求的相符結果，以符合或不相符。如需詳細資訊，請參閱轉送的 IP 位址。

在哪裡可以找到這個規則聲明

- 主控台上的規則產生器 — 對於「請求」選項，請在中選擇「源自 IP 位址」。
- 在主控台上新增我自己的規則和規則群組頁面 — 選擇 IP 集選項。
- API — IP SetReferenceStatement

標籤比對規則陳述式

標籤匹配語句檢查是針對字符串規範的 Web 請求的標籤。用於檢查的規則可用的標籤是已由相同 Web ACL 評估中其他規則新增至 Web 請求的標籤。

標籤不會在 Web ACL 評估之外持續存在，但您可以在中存取標籤指標， CloudWatch 並且可以在 AWS WAF 主控台中查看任何 Web ACL 的標籤資訊摘要。如需詳細資訊，請參閱 標示量度和維度 及 監控和調整。您也可以在記錄檔中看到標籤。如需相關資訊，請參閱日誌欄位。

> **Note**
>
> 標籤匹配語句只能看到 Web ACL 中先前評估的規則中的標籤。如需有關如何 AWS WAF 評估 Web ACL 中規則和規則群組的資訊，請參閱Web ACL 中規則和規則群組的處理順序。

若要取得有關加入和比對標示的更多資訊，請參閱AWS WAF 標籤, 上, 网, 請求。

嵌套-您可以嵌套此語句類型。

WCU — 1 WCU

此陳述式會使用下列設定：

- 比對範圍 — 將此選項設定為 Label 以符合標籤名稱，並選擇性地比對前面的命名空間和前置詞。將此項設定為「命名空間」，以符合部分或所有命名空間規格，並選擇性地比對前面的前置詞。
- Key — 您要比對的字串。如果您指定命名空間比對範圍，這應該只指定命名空間，並選擇性地指定前綴，並帶有結尾冒號。如果您指定標籤比對範圍，則必須包含標籤名稱，並且可以選擇性地包含前面的命名空間和前置詞。

如需這些設定的詳細資訊，請參閱 AWS WAF 符合標籤的規則 和 AWS WAF 標籤相符範例。

在哪裡可以找到這個規則聲明

- 主控台上的規則產生器 — 對於「請求」選項，請選擇「有標籤」。
- API — LabelMatchStatement

正則表達式匹配規則

正則表達式匹配語句指示 AWS WAF 將請求組件與單個正則表達式（正則表達式）匹配。如果 request 元件與您指定的正則表達式匹配，則 Web 請求匹配語句。

對於要使用數學邏輯合併匹配條件規則運算式模式集比對規則陳述式的情況，此語句類型是一個很好的替代方案。例如，如果您希望請求組件與某些正則表達式模式匹配，並且不匹配其他模式，則可以使用AND規則陳述式和來組合 regex 匹配語句NOT規則陳述式。

AWS WAF 支援 PCRE 程式庫所使用的模式語法，但`libpcre`有一些例外。該庫在 PCRE-Perl 兼容的正則表達式中記錄。如需有關 AWS WAF 支援的資訊，請參閱正則表達式模式匹配 AWS WAF。

嵌套-您可以嵌套此語句類型。

WCU — 3 個 WCU，作為基本成本。如果您使用要求元件所有查詢參數，請新增 10 個 WCU。如果您使用要求元件 JSON 主體，則將基本成本的 WCU 加倍。針對您套用的每個文字轉換，新增 10 個 WCU。

此陳述式類型會在 Web 要求元件上運作，而且需要下列要求元件設定：

- 要求元件 — 要檢查的 Web 要求部分，例如查詢字串或內文。

  > **Warning**
  >
  > 如果您檢查要求元件內文、JSON 內文、標頭或 Cookie，請參閱 AWS WAF 可以檢查多少內容的限制處理超大請求組件 AWS WAF。

  如需 Web 要求元件的詳細資訊，請參閱Web 請求組件規格和處理。
- 選擇性文字轉換 — 您要在檢查要求元件之前對 AWS WAF 要求元件執行的轉換。例如，您可以轉換為小寫或標準化空格。如果您指定多個轉換，則會依照列出的順 AWS WAF 序處理這些轉換。如需相關資訊，請參閱文字轉換選項。

在哪裡可以找到這個規則聲明

- 主控台上的規則產生器 — 對於比對類型，請選擇符合規則運算式。
- API — RegexMatchStatement

規則運算式模式集比對規則陳述式

規則表達式模式集比對會檢查您在規則表達式模式集內為規則表達式模式指定的 Web 請求部分。

AWS WAF 支援 PCRE 程式庫所使用的模式語法，但`libpcre`有一些例外。該庫在 PCRE-Perl 兼容的正則表達式中記錄。如需有關 AWS WAF 支援的資訊，請參閱正則表達式模式匹配 AWS WAF。

> **Note**
>
> 每個規則運算式模式集比對規則都會參考一個規則運算式模式集，您可以獨立於規則而建立和維護。您可以在多個規則中使用單個正則表達式模式集，並且當您更新引用的集合時， AWS WAF 會自動更新引用它的所有規則。
> 如需建立和管理規則運算式模式集的相關資訊，請參閱 建立和管理規則運算式模式集。

正則表達式模式集匹配語句指示 AWS WAF 搜索您選擇的請求組件內的任何模式集合。如果請求元件符合集合中的任何模式，則 Web 請求將比對模式集規則陳述式。

如果您想使用邏輯合併正則表達式模式匹配，例如匹配某些正則表達式而不匹配其他正則表達式，請考慮使用正則表達式匹配規則.

嵌套-您可以嵌套此語句類型。

WCU — 25 個 WCU，作為基本成本。如果您使用要求元件所有查詢參數，請新增 10 個 WCU。如果您使用要求元件 JSON 主體，則將基本成本的 WCU 加倍。針對您套用的每個文字轉換，新增 10 個 WCU。

此陳述式類型會在 Web 要求元件上運作，而且需要下列要求元件設定：

- 要求元件 — 要檢查的 Web 要求部分，例如查詢字串或內文。

> **Warning**
>
> 如果您檢查要求元件內文、JSON 內文、標頭或 Cookie，請參閱 AWS WAF 可以檢查多少內容的限制處理超大請求組件 AWS WAF。

如需 Web 要求元件的詳細資訊，請參閱Web 請求組件規格和處理。

- 選擇性文字轉換 — 您要在檢查要求元件之前對 AWS WAF 要求元件執行的轉換。例如，您可以轉換為小寫或標準化空格。如果您指定多個轉換，則會依照列出的順 AWS WAF 序處理這些轉換。如需相關資訊，請參閱文字轉換選項。

此陳述式需要下列設定：

- 正則表達式模式集規範-從列表中選擇要使用的正則表達式模式集或創建一個新的正則表達式模式集。

在哪裡可以找到這個規則聲明

- 主控台上的規則產生器 — 對於比對類型，請從規則運算式集中選擇字串比對條件 > 符合模式。
- API — RegexPatternSetReferenceStatement

大小約束規則陳述式

size 條件約束陳述式會比較 Web 要求元件中的位元組數目與您提供的數字，並根據您的比較準則進行比對。比較準則是一個運算子，例如大於 (>) 或小於 (<)。例如，您可以比對具有大小超過 100 個位元組的查詢字串的要求。

> **Note**
>
> 此聲明僅檢查 Web 請求組件的大小。它不會檢查組件的內容。

如果您檢查 URI 路徑，則路徑/中的任何一個都會計為一個字元。例如，URI 路徑長度/logo.jpg為九個字元。

嵌套-您可以嵌套此語句類型。

WCU — 1 WCU，作為基本成本。如果您使用要求元件所有查詢參數，請新增 10 個 WCU。如果您使用要求元件 JSON 主體，則將基本成本的 WCU 加倍。針對您套用的每個文字轉換，新增 10 個 WCU。

此陳述式類型會在 Web 要求元件上運作，而且需要下列要求元件設定：

- 要求元件 — 要檢查的 Web 要求部分，例如查詢字串或內文。如需 Web 要求元件的詳細資訊，請參閱Web 請求組件規格和處理。

  size 條件約束陳述式只會在套用任何變形之後檢查元件的大小。它不會檢查組件的內容。
- 選擇性文字轉換 — 您想 AWS WAF 要在檢查其大小之前對 request 元件執行的轉換。例如，您可以壓縮空格或解碼 HTML 實體。如果您指定多個轉換，則會依照列出的順 AWS WAF 序處理這些轉換。如需相關資訊，請參閱文字轉換選項。

此外，此陳述式需要下列設定：

- 大小匹配條件-這表示數字比較運算符用於比較您提供的請求組件與您選擇的請求組件的大小。從清單中選擇運算子。
- 大小 — 比較中要使用的大小設定 (以位元組為單位)。

在哪裡可以找到這個規則聲明

- 主控台上的規則產生器 — 對於 [比對類型]，在 [大小符合條件] 下，選擇您要使用的條件。
- API — SizeConstraintStatement

SQL Injection 攻擊規則陳述式

SQL 插入規則陳述式會檢查是否有惡意 SQL 程式碼。攻擊者將惡意 SQL 代碼插入 Web 請求中，以執行諸如修改數據庫或從中提取數據之類的操作。

嵌套-您可以嵌套此語句類型。

WCU — 基本成本取決於規則陳述式的敏感度層級設定：Low成本 20 和High成本 30。

如果您使用要求元件所有查詢參數，請新增 10 個 WCU。如果您使用要求元件 JSON 主體，則將基本成本的 WCU 加倍。針對您套用的每個文字轉換，新增 10 個 WCU。

此陳述式類型會在 Web 要求元件上運作，而且需要下列要求元件設定：

- 要求元件 — 要檢查的 Web 要求部分，例如查詢字串或內文。

  > **Warning**
  >
  > 如果您檢查要求元件內文、JSON 內文、標頭或 Cookie，請參閱 AWS WAF 可以檢查多少內容的限制處理超大請求組件 AWS WAF。

  如需 Web 要求元件的詳細資訊，請參閱Web 請求組件規格和處理。

- 選擇性文字轉換 — 您要在檢查要求元件之前對 AWS WAF 要求元件執行的轉換。例如，您可以轉換為小寫或標準化空格。如果您指定多個轉換，則會依照列出的順 AWS WAF 序處理這些轉換。如需相關資訊，請參閱文字轉換選項。

此外，此陳述式還需要下列設定：

- 敏感度層級 — 此設定會調整 SQL 插入符合條件的敏感度。選項包括 LOW 和 HIGH. 預設設定為 LOW。

  此HIGH設定會偵測到更多 SQL 插入攻擊，這是建議的設定。由於敏感度較高，此設定會產生更多誤報，尤其是當您的 Web 要求通常包含不尋常的字串時。在 Web ACL 測試和調整期間，您可能需要進行更多工作來減輕誤報。如需相關資訊，請參閱測試和調整您的 AWS WAF 保護。

  較低的設定提供較不嚴格的 SQL 插入偵測，這也會導致較少的誤判。 LOW對於具有其他 SQL 插入攻擊保護或誤判性較低的資源，可能是更好的選擇。

在哪裡可以找到這個規則聲明

- 主控台上的規則產生器 — 針對 [比對類型]，選擇 [攻擊符合條件] > [包含 SQL 插入攻擊]。
- API — SqliMatchStatement

字串比對規則陳述式

字符串 match 語句表示您 AWS WAF 要在請求中搜索的字符串，請求中搜索的位置以及如何搜索。例如，您可以在請求中任何查詢字串的開頭尋找特定字串，或是在請求的 `User-agent` 標頭中尋找完全相符項目。通常，字串包含可列印 ASCII 字元，但您可以使用十六進位 0x00 到 0xFF 的任何字元 (小數 0 到 255)。

嵌套-您可以嵌套此語句類型。

WCU — 基本成本取決於您使用的相符項目類型。

- 完全符合字串 — 2
- 從字符串開始-2
- 以字串結尾 — 2
- 包含字串 — 10 個
- 包含單字 — 10 個

如果您使用要求元件所有查詢參數，請新增 10 個 WCU。如果您使用要求元件 JSON 主體，則將基本成本的 WCU 加倍。針對您套用的每個文字轉換，新增 10 個 WCU。

此陳述式類型會在 Web 要求元件上運作，而且需要下列要求元件設定：

- 要求元件 — 要檢查的 Web 要求部分，例如查詢字串或內文。

  > **Warning**
  >
  > 如果您檢查要求元件內文、JSON 內文、標頭或 Cookie，請參閱 AWS WAF 可以檢查多少內容的限制處理超大請求組件 AWS WAF。

  如需 Web 要求元件的詳細資訊，請參閱Web 請求組件規格和處理。
- 選擇性文字轉換 — 您要在檢查要求元件之前對 AWS WAF 要求元件執行的轉換。例如，您可以轉換為小寫或標準化空格。如果您指定多個轉換，則會依列出的順 AWS WAF 序處理它們。如需相關資訊，請參閱文字轉換選項。

此外，此陳述式需要下列設定：

- 字符串匹配-這是要比較指定 AWS WAF 的請求組件的字符串。通常，字串包含可列印 ASCII 字元，但您可以使用十六進位 0x00 到 0xFF 的任何字元 (小數 0 到 255)。
- 字符串匹配條件-這表示您要 AWS WAF 執行的搜索類型。
  - 完全匹配字符串-請求組件的字符串和值是相同的。
  - 以字串開頭 — 字串會出現在要求元件的開頭。
  - 以字串結尾 — 字串會出現在要求元件的結尾。

- 包含字串 — 字串會出現在要求元件中的任何位置。
- 包含字詞 — 您指定的字串必須出現在要求元件中。

  對於此選項，您指定的字串必須只包含英數字元或底線 (A-Z、a-z、0-9 或 _)。

  下列其中一項必須為 true，才能比對請求：
  - 該字串與請求元件的數值 (如標頭值) 完全相符。
  - 該字串位於請求元件的開頭，後面加上非英數字元或底線 (_) 的字元，例如 `BadBot;`。
  - 該字串位於請求元件的尾端，前面加上非英數字元或底線 (_) 的字元，例如 `;BadBot`。
  - 該字串位於請求元件的中間，前後加上非英數字元或底線 (_) 的字元，例如 `-BadBot;`。

在哪裡可以找到這個規則聲明

- 主控台上的規則產生器 — 針對 [比對類型]，選擇 [字串比對條件]，然後填入您要比對的字串。
- API — ByteMatchStatement

跨網站指令碼攻擊規則陳述式

XSS (跨網站指令碼) 攻擊陳述式會檢查 Web 要求元件中是否有惡意指令碼。在 XSS 攻擊中，攻擊者會利用良性網站中的弱點做為工具，將惡意用戶端網站指令碼插入其他合法的網頁瀏覽器。

嵌套-您可以嵌套此語句類型。

WCU — 40 個 WCU，作為基本成本。如果您使用要求元件所有查詢參數，請新增 10 個 WCU。如果您使用要求元件 JSON 主體，則將基本成本的 WCU 加倍。針對您套用的每個文字轉換，新增 10 個 WCU。

此陳述式類型會在 Web 要求元件上運作，而且需要下列要求元件設定：

- 要求元件 — 要檢查的 Web 要求部分，例如查詢字串或內文。

> **Warning**
>
> 如果您檢查要求元件內文、JSON 內文、標頭或 Cookie，請參閱 AWS WAF 可以檢查多少內容的限制處理超大請求組件 AWS WAF。

如需 Web 要求元件的詳細資訊，請參閱Web 請求組件規格和處理。

- 選擇性文字轉換 — 您要在檢查要求元件之前對 AWS WAF 要求元件執行的轉換。例如，您可以轉換為小寫或標準化空格。如果您指定多個轉換，則會依照列出的順 AWS WAF 序處理這些轉換。如需相關資訊，請參閱文字轉換選項。

在哪裡可以找到這個規則聲明

- 主控台上的規則產生器 — 對於比對類型，請選擇 [攻擊符合條件] > [包含 XSS 插入攻擊]。
- API — XssMatchStatement

邏輯規則陳述式

使用邏輯規則陳述式結合其他陳述式或否定其結果。每個邏輯規則陳述式至少需要一個巢狀化的陳述式。

若要以邏輯方式合併或否定規則陳述式的結果，請將陳述式巢狀化在邏輯規則陳述式下。

邏輯規則語句是嵌套的。您可以將它們嵌套在其他邏輯規則語句中，並在範圍向下語句中使用它們。如需有關向下範圍陳述式的資訊，請參閱。範圍向下語句

> **Note**
>
> 主控台上的視覺化編輯器支援一個層級的規則陳述式巢狀，這適用於許多需求。若要巢狀化更多層級，請在主控台上編輯規則的 JSON 表示法，或使用 API。

此表格說明邏輯規則陳述式，並提供計算每個邏輯規則陳述式的 Web ACL 容量單位 (WCU) 使用情況的準則。如需 WCU 的相關資訊，請參閱 AWS WAF 網路 ACL 容量單位 (WCU)。

邏輯陳述式	描述	WCU
AND 邏輯	結合嵌套語句與AND邏輯。	以巢狀化陳述式為基礎
NOT 邏輯	否定巢狀化陳述式的結果。	以巢狀化陳述式為基礎
OR 邏輯	結合嵌套語句與OR邏輯。	以巢狀化陳述式為基礎

AND規則陳述式

ANDrule 陳述式會結合巢狀陳述式與邏輯AND運算，因此所有巢狀陳述式都必須相符，才能符合AND陳述式。這需要至少兩個嵌套語句。

嵌套-您可以嵌套此語句類型。

WCU — 取決於巢狀陳述式。

在哪裡可以找到這個規則聲明

- 主控台上的規則產生器 — 對於如果要求，請選擇符合所有陳述式 (AND)，然後填入巢狀陳述式。
- API — AndStatement

範例

下列清單顯示如何使用AND和NOT邏輯規則陳述式，從 SQL 插入攻擊陳述式的相符項目中消除誤判。在這個例子中，假設我們可以編寫一個字節 match 語句來匹配導致誤報的請求。

AND 陳述式會比對不符合位元組比對陳述式且符合 SQL 插入攻擊陳述式的要求。

```
{
      "Name": "SQLiExcludeFalsePositives",
      "Priority": 0,
      "Statement": {
        "AndStatement": {
          "Statements": [
            {
              "NotStatement": {
                "Statement": {
                  "ByteMatchStatement": {
                    "SearchString": "string identifying a false positive",
                    "FieldToMatch": {
                      "Body": {
                        "OversizeHandling": "MATCH"
                      }
                    },
                    "TextTransformations": [
                      {
                        "Priority": 0,
                        "Type": "NONE"
                      }
                    ],
```

```
                    "PositionalConstraint": "CONTAINS"
                  }
                }
              }
            },
            {
              "SqliMatchStatement": {
                "FieldToMatch": {
                  "Body": {
                    "OversizeHandling": "MATCH"
                  }
                },
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "SQLiExcludeFalsePositives"
      }
    }
```

使用主控台規則視覺化編輯器，您可以將非邏輯陳述式或陳述式嵌套在OR或NOTAND陳述式下。NOT陳述式的巢狀顯示在前面的範例中。

使用主控台規則視覺化編輯器，您可以將大多數 nestable 陳述式嵌套在邏輯規則陳述式下，例如先前範例中所示的陳述式。您不能使用可視化編輯器嵌套OR或AND語句。要配置這種類型的嵌套，您需要在 JSON 中提供規則語句。例如，下列 JSON 規則清單包含巢狀OR陳述式內的AND陳述式。

```
{
  "Name": "match_rule",
  "Priority": 0,
```

```
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
              }
            }
          }
        },
        {
          "OrStatement": {
            "Statements": [
              {
                "GeoMatchStatement": {
                  "CountryCodes": [
                    "JM",
                    "JP"
                  ]
                }
              },
              {
                "ByteMatchStatement": {
                  "SearchString": "JCountryString",
                  "FieldToMatch": {
                    "Body": {}
                  },
                  "TextTransformations": [
                    {
                      "Priority": 0,
                      "Type": "NONE"
                    }
                  ],
                  "PositionalConstraint": "CONTAINS"
                }
```

```
              }
            ]
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "match_rule"
  }
}
```

NOT規則陳述式

NOT規則陳述式會在邏輯上否定單一巢狀陳述式的結果，因此巢狀陳述式必須不符合要比對的NOT陳述式，反之亦然。這需要一個巢狀化陳述式。

例如，如果您想要封鎖不在特定國家/地區發出的要求，請建立動作設定為封鎖的NOT陳述式，然後巢狀化指定國家/地區的地理比對陳述式。

嵌套-您可以嵌套此語句類型。

WCU — 取決於巢狀陳述式。

在哪裡可以找到這個規則聲明

- 主控台上的規則產生器 — 對於如果要求，select 與陳述式 (NOT) 不符，然後填入巢狀陳述式。
- API — NotStatement

OR規則陳述式

ORrule 陳述式會結合巢狀陳述式與OR邏輯，因此其中一個巢狀陳述式必須相符，才能符合OR陳述式。這需要至少兩個嵌套語句。

例如，如果您想要封鎖來自特定國家/地區或包含特定查詢字串的要求，您可以建立OR陳述式並在其中巢狀化該國家/地區的 geo match 陳述式，以及查詢字串的字串 match 陳述式。

如果您想要封鎖不是來自特定國家/地區或包含特定查詢字串的要求，您可以修改先前的OR陳述式，將 geo match 陳述式巢狀化在陳NOT述式中低一層。此層級的巢狀需要您使用 JSON 格式，因為主控台僅支援一個巢狀層級。

嵌套-您可以嵌套此語句類型。

WCU — 取決於巢狀陳述式。

在哪裡可以找到這個規則聲明

- 主控台上的規則產生器 — 針對 [如果要求]，請選擇至少符合其中一個陳述式 (OR)，然後填入巢狀陳述式。
- API — OrStatement

範例

下列清單顯示結合其他兩個陳述式的OR使用方式。如果其中OR一個巢狀陳述式相符，陳述式就是相符項目。

```
{
  "Name": "neitherOfTwo",
  "Priority": 1,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "neitherOfTwo"
  },
  "Statement": {
    "OrStatement": {
      "Statements": [
        {
          "GeoMatchStatement": {
            "CountryCodes": [
              "CA"
            ]
          }
        },
        {
          "IPSetReferenceStatement": {
```

```
            "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/ipset/test-ip-
set-22222222/33333333-4444-5555-6666-777777777777"
          }
        }
      ]
    }
  }
}
```

使用主控台規則視覺化編輯器，您可以將大多數嵌套在邏輯規則陳述式下方，但不能使用視覺化編輯器來巢狀化OR或AND陳述式。要配置這種類型的嵌套，您需要在 JSON 中提供規則語句。例如，下列 JSON 規則清單包含巢狀OR陳述式內的AND陳述式。

```
{
  "Name": "match_rule",
  "Priority": 0,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
              }
            }
          }
        },
        {
          "OrStatement": {
            "Statements": [
              {
                "GeoMatchStatement": {
                  "CountryCodes": [
                    "JM",
                    "JP"
```

```
                ]
              }
            },
            {
              "ByteMatchStatement": {
                "SearchString": "JCountryString",
                "FieldToMatch": {
                  "Body": {}
                },
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ],
                "PositionalConstraint": "CONTAINS"
              }
            }
          ]
        }
      }
    ]
  }
},
"Action": {
  "Block": {}
},
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "match_rule"
}
}
```

速率型規則陳述式

以速率為基礎的規則會計算連入要求，並在速率過快時限制要求。此規則會根據您的條件彙總請求，並根據規則的評估時段、請求限制和作業設定來限制聚總群組。

> **Note**
>
> 您也可以使用「機器人控制 AWS 受管規則」規則群組的目標保護層級來分級限制 Web 要求。使用此受管規則群組會產生額外費用。如需詳細資訊，請參閱 以速率為基礎的規則和目標機器人控制規則中的速率限制選項。

AWS WAF 針對您使用的每個以速率為基礎的規則執行個體，個別追蹤和管理 Web 要求。例如，如果您在兩個 Web ACL 中提供相同的以速率為基礎的規則設定，則兩個規則陳述式中的每一個都代表以速率為基礎的規則的個別執行個體，而且每個都會依據自己的追蹤和管理。 AWS WAF如果您在規則群組中定義以比率為基準的規則，然後在多個位置使用該規則群組，則每次使用都會建立以比率為基準的規則的個別執行個體，以取得其自己的追蹤與管理。 AWS WAF

不嵌套-您不能在其他語句中嵌套此語句類型。您可以將其直接包含在 Web ACL 或規則群組中。

ScopeDown 陳述式 — 此規則類型可採用範圍向下陳述式，以縮小規則追蹤的要求範圍和速率限制。範圍下語句可以是可選的或必要的，具體取決於您的其他規則配置設置。詳細信息將在本節中介紹。如需有關向下範圍陳述式的一般資訊，請參閱。範圍向下語句

WCU — 2，作為基本成本。針對您指定的每個自訂彙總金鑰，新增 30 個 WCU。如果您在規則中使用向下範圍陳述式，請計算並新增 WCU。

在哪裡可以找到這個規則聲明

- Web ACL 中的規則產生器，在主控台上 — 在「規則」下，針對「類型」選擇以速率為基礎的規則。
- API — RateBasedStatement

主題

- 速率型規則高階設定
- 以速率為基礎的規則警告
- 以速率為基礎的規則彙總選項和索
- 速率型規則彙總執行個體和計數
- 速率型規則要求速率限制行為
- 速率型規則範例
- 列出受速率規則限制的 IP 位址

速率型規則高階設定

以速率為基礎的規則陳述式會使用下列高階設定：

- 評估期間 — 從目前時間回溯的要求計數中 AWS WAF 應包含的時間量 (以秒為單位)。例如，如果設定為 120，當 AWS WAF 檢查比率時，會計算緊接在目前時間之前 2 分鐘的要求。有效的設定為 60 (1 分鐘)、120 (兩分鐘)、300 (5 分鐘) 和 600 (10 分鐘)，而預設值為 300 (5 分鐘)。

  此設定不會決定 AWS WAF 檢查費率的頻率，而是每次檢查時看起來多遠。 AWS WAF 經常檢查速率，其時間與評估時段設定無關。
- 速率限制 — 符合您條件的請求數目上限， AWS WAF 應該只追蹤指定的評估時段。允許的最低限制設定為 100。違反此限制時，會將規則動作設定 AWS WAF 套用至符合條件的其他請求。

  AWS WAF 會在您設定的限制附近套用速率限制，但不保證限制完全符合。如需詳細資訊，請參閱 以速率為基礎的規則警告。
- 請求聚總 — 用於 Web 請求的聚總條件，以速率為基礎的規則計數和速率限制。您設定的速率限制會套用至每個彙總執行個體。如需詳細資訊，請參閱 彙總選項和索引鍵 和 彙總執行個體和計數。
- 動作 — 要對規則速率限制的請求採取的動作。您可以使用除以外的任何規則動作Allow。這會像往常一樣在規則層級設定，但有一些特定於速率型規則的限制和行為。如需有關規則動作的一般資訊，請參閱規則動作。如需速率限制的特定資訊，請參閱本節速率型規則要求速率限制行為中的〈〉。
- 檢驗範圍與費率限制 — 您可以新增範圍向下陳述式，來縮小以費率為基準的陳述式追蹤的請求範圍與費率限制。如果您指定了向下範圍陳述式，則規則只會彙總、計數和速率限制要求，且符合範圍向下陳述式。如果您選擇請求聚總選項「全部計數」，則需要向下範圍陳述式。如需有關向下範圍陳述式的詳細資訊，請參閱。範圍向下語句
- (選擇性) 轉送的 IP 組態 — 只有在您在要求彙總的標頭中指定 IP 位址時 (單獨指定或作為自訂金鑰設定的一部分) 時，才會使用此選項。 AWS WAF 檢索指定標頭中的第一個 IP 地址，並將其用作聚合值。用於此目的的一個共同的頭是`X-Forwarded-For`，但你可以指定任何頭。如需更多詳細資訊，請參閱 轉送的 IP 位址。

以速率為基礎的規則警告

AWS WAF 速率限制旨在控制高請求率，並以最有效率和最有效的方式保護應用程式的可用性。它不適用於精確的請求速率限制。

- AWS WAF 使用對較近期要求更重要的演算法來估算目前的要求率。因此， AWS WAF 將在您設定的限制附近套用速率限制，但不保證限制完全相符。

- 每次 AWS WAF 估計要求比率時，都會回 AWS WAF 顧設定的評估時段期間傳入的要求數目。由於這種情況和其他因素 (例如傳播延遲)，在 AWS WAF 偵測到要求並限制速率之前，可能會以過高的速率進入最多數分鐘。同樣。請求率可以在 AWS WAF 檢測到減少並中止速率限制操作之前一段時間低於限制。通常，此延遲低於 30 秒。
- 如果您變更正在使用的規則中的任何速率限制設定，變更會重設規則的速率限制計數。這可以將規則的速率限制活動暫停最多一分鐘。速率限制設定包括評估視窗、速率限制、要求彙總設定、轉送的 IP 組態以及檢查範圍。

以速率為基礎的規則彙總選項和索

根據預設，以速率為基礎的規則會根據請求 IP 位址彙總並限制要求。您可以將規則設定為使用各種其他彙總索引鍵和按鍵組合。例如，您可以根據轉送的 IP 位址、HTTP 方法或查詢引數進行彙總。您也可以指定彙總鍵組合，例如 IP 位址和 HTTP 方法，或兩個不同 Cookie 的值。

> **Note**
>
> 您在彙總索引鍵中指定的所有要求元件都必須出現在 Web 要求中，才能評估要求，或受規則限制比率。

您可以使用下列彙總選項來設定以速率為基礎的規則。

- 來源 IP 位址 — 僅使用來自 Web 請求來源的 IP 位址進行彙總。

  來源 IP 位址可能不包含原始用戶端的位址。如果 Web 請求通過一個或多個代理或負載平衡器，這將包含最後一個代理的地址。
- 標頭中的 IP 位址 — 僅使用 HTTP 標頭中的用戶端位址進行彙總。這也稱為轉送的 IP 位址。

  透過此設定，您也可以指定後援行為，以套用至標頭中具有格式錯誤 IP 位址的 Web 要求。後援行為會設定要求的相符結果，以符合或不相符。如果沒有比對，以速率為基礎的規則不會計算或費率限制請求。為了進行比對，以速率為基礎的規則會將要求與指定標頭中具有格式錯誤 IP 位址的其他要求分組在一起。

  請小心使用此選項，因為代理伺服器可能不一致地處理標頭，也可以修改它們以略過檢查。如需其他資訊和最佳作法，請參閱〈〉轉送的 IP 位址。
- 全部計數 — 計數和速率會限制符合規則範圍陳述式的所有請求。此選項需要向下範圍陳述式。這通常用於對特定請求集的限制進行分級，例如具有特定標籤的所有請求或來自特定地理區域的所有請求。

- 自訂索引鍵 — 使用一或多個自訂彙總索引鍵彙總。若要將其中一個 IP 位址選項與其他彙總金鑰結合使用，請在此處定義自訂金鑰。

  自訂彙總索引鍵是 Web 要求元件選項的子集，請參閱要求元件選項。

  關鍵選項如下。除非另有說明，您可以多次使用選項，例如，兩個標頭或三個標籤命名空間。

  - 標籤命名空間 — 使用標籤命名空間做為彙總索引鍵。每個具有指定標籤命名空間的不同完全限定標籤名稱都會貢獻給聚合實例。如果您只使用一個標籤命名空間作為自定義鍵，則每個標籤名稱都會完全定義一個聚合實例。

    以速率為基礎的規則只會使用已經由 Web ACL 中預先評估的規則新增至請求的標籤。

    如需有關標籤命名空間和名稱的資訊，請參閱AWS WAF 標籤語法和命名需求。
  - 標頭 — 使用具名的標頭做為彙總索引鍵。標頭中的每個不同值都有助於彙總執行個體。

    標題需要一個可選的文本轉換。請參閱文字轉換選項。
  - Cookie — 使用具名的 Cookie 做為彙總金鑰。Cookie 中的每個不同值都會貢獻給彙總執行個體。

    Cookie 需要一個可選的文本轉換。請參閱文字轉換選項。
  - Query 引數 — 使用請求中的單一查詢引數作為彙總索引鍵。具名查詢引數的每個不同值都會貢獻給彙總執行個體。

    查詢引數需要一個可選的文本轉換。請參閱文字轉換選項。
  - 查詢字串 — 使用請求中的整個查詢字串做為彙總索引鍵。每個不同的查詢字串都會貢獻給彙總執行個體。您可以使用此金鑰類型一次。

    查詢字串需要選擇性的文字轉換。請參閱文字轉換選項。
  - URI 路徑 — 使用請求中的 URI 路徑作為彙總索引鍵。每個不同的 URI 路徑都有助於聚合實例。您可以使用此金鑰類型一次。

    URI 路徑需要一個可選的文本轉換。請參閱文字轉換選項。
  - HTTP 方法 — 使用要求的 HTTP 方法做為彙總金鑰。每個不同的 HTTP 方法都有助於彙總執行個體。您可以使用此金鑰類型一次。
  - IP 位址 — 使用來自 Web 請求來源的 IP 位址與其他金鑰進行彙總。

    這可能不包含原始用戶端的位址。如果 Web 請求通過一個或多個代理或負載平衡器，這將包含最後一個代理的地址。

- 標頭中的 IP 位址 — 使用 HTTP 標頭中的用戶端位址與其他金鑰組合進行彙總。這也稱為轉送的 IP 位址。

  請小心使用此選項，因為代理伺服器可能會不一致地處理標頭，並且可以修改它們以略過檢查。如需其他資訊和最佳作法，請參閱〈〉轉送的 IP 位址。

速率型規則彙總執行個體和計數

當以速率為基礎的規則使用聚總條件評估 Web 請求時，規則針對指定的聚總索引鍵找到的每一組唯一值都會定義唯一的彙總執行處理。

- 多個索引鍵 — 如果您已定義多個自訂索引鍵，則每個索引鍵的值會貢獻彙總執行個體定義。每個唯一值組合都會定義彙總執行個體。
- 單一索引鍵 — 如果您選擇了單一金鑰 (無論是在自訂索引鍵中或選取其中一個單一 IP 位址選項)，則該金鑰的每個唯一值都會定義彙總執行個體。
- 全部計數-無索引鍵 — 如果您已選取彙總選項 [全部計數]，則規則評估的所有請求都屬於規則的單一彙總執行個體。此選擇需要一個向下範圍語句。

以速率為基礎的規則會針對其識別的每個彙總執行個體，個別計算 Web 要求。

例如，假設以速率為基礎的規則會使用下列 IP 位址和 HTTP 方法值來評估 Web 要求：

- IP 地址 10.1.1.1，HTTP 方法發布
- IP 地址：獲取方法
- IP 地址 127.0.0.0，HTTP 方法發布
- IP 地址：獲取方法

此規則會根據您的彙總準則建立不同的彙總執行個體。

- 如果彙總準則只是 IP 位址，則每個個別 IP 位址都是彙總執行個體，並分別 AWS WAF 計算每個 IP 位址的要求。我們範例的彙總執行個體和要求計數如下：
  - IP 位址 10.1.1.1：計數 3
  - IP 位址：計數 1
- 如果彙總準則是 HTTP 方法，則每個個別的 HTTP 方法都是彙總執行個體。我們範例的彙總執行個體和要求計數如下：

  - HTTP 方法發布：計數 2
  - HTTP 方法獲取：計數 2
- 如果彙總準則是 IP 位址和 HTTP 方法，則每個 IP 位址和每個 HTTP 方法都會有助於合併的彙總執行個體。我們範例的彙總執行個體和要求計數如下：
  - IP 地址 10.1.1.1，HTTP 方法發布：計數 1
  - IP 地址 10.1.1.1，HTTP 方法獲取：計數 2
  - IP 地址 127.0.0.0，HTTP 方法發布：計數 1

速率型規則要求速率限制行為

AWS WAF 用於對以速率為基準的規則進行限制請求評分的準則，與 AWS WAF 用於彙總規則請求的條件相同。如果您定義規則的向下範圍陳述式，則 AWS WAF 只會彙總、計數和速率限制要求，而且符合範圍向下陳述式。

導致以比率為基礎的規則將其規則作業設定套用至特定 Web 請求的比對條件如下：

- Web 要求符合規則的範圍向下陳述式 (如果已定義)。
- Web 要求屬於要求計數目前超過規則限制的彙總執行個體。

如何 AWS WAF 套用規則動作

當以費率為基礎的規則將費率限制套用至請求時，它會套用規則作業，而且，如果您已在作業規格中定義任何自訂處理或標籤，則規則會套用這些處理。此要求處理方式與比對規則將其動作設定套用至相符 Web 要求的方式相同。以速率為基礎的規則只會套用標籤或對其主動速率限制的請求執行其他動作。

您可以使用除以外的任何規則動作Allow。如需有關規則動作的一般資訊，請參閱規則動作。

下列清單說明速率限制對每個動作的運作方式。

- Block— AWS WAF 封鎖要求並套用您已定義的任何自訂封鎖行為。
- Count— AWS WAF 計算要求、套用您已定義的任何自訂標頭或標籤，並繼續要求的 Web ACL 評估。

  此動作不會限制要求的頻率。它只是計算超過限制的請求。
- CAPTCHA或 Challenge- AWS WAF 處理請求Block或類似的請求Count，具體取決於請求的令牌的狀態。

  此操作不會限制具有有效令牌的請求率。它限制了超過限制並且缺少有效令牌的請求的速率。

- 如果請求沒有有效的未過期令牌，則操作會阻止請求，並將 CAPTCHA 難題或瀏覽器挑戰發送回客戶端。

  如果最終用戶或客戶端瀏覽器響應成功，則客戶端會收到有效的令牌，並自動重新發送原始請求。如果彙總執行個體的速率限制仍然有效，這個具有有效、未過期權杖的新要求將會套用動作，如下一個 bullet 點所述。
- 如果請求具有有效的未過期令牌，則CAPTCHA或Challenge動作會驗證令牌，並且不對請求採取任何操作，類似於操作。Count以速率為基礎的規則會將要求評估傳回 Web ACL，而不採取任何終止動作，而 Web ACL 會繼續評估要求。

如需其他資訊，請參閱 CAPTCHA並Challenge在 AWS WAF。

如果您的速率限制只有 IP 地址或轉發的 IP 地址

當您將規則設定為僅限制轉寄 IP 位址的 IP 位址時，規則執行個體的速率最多可限制 10,000 個 IP 位址。如果規則執行個體識別出 10,000 個以上的 IP 位址以達到速率限制，則只會限制最高 10,000 個寄件者。

使用此組態，您可以擷取以速率為基礎的規則目前為速率限制的 IP 位址清單。如果您使用的是範圍向下陳述式，則速率限制的要求只是 IP 清單中符合範圍向下陳述式的要求。如需擷取 IP 位址清單的相關資訊，請參閱列出受速率規則限制的 IP 位址。

速率型規則範例

本節說明各種常見以速率為基礎的規則使用案例的範例組態。

每個範例都會提供使用案例的說明，然後在 JSON 清單中顯示自訂設定規則的解決方案。

> **Note**
>
> 這些範例中顯示的 JSON 清單是在主控台中設定規則，然後使用規則 JSON 編輯器進行編輯來建立。

主題

- 速率限制對登錄頁面的請求
- 速率限制從任何 IP 地址，用戶代理對登錄頁面的請求
- 速率限制缺少特定標頭的請求

- 速率限制帶有特定標籤的請求
- 速率限制對具有指定標籤命名空間的標籤的請求

速率限制對登錄頁面的請求

若要限制對您網站登入頁面的要求數目，而不影響到網站其他部分的流量，您可以建立以速率為基礎的規則，其中包含符合登入頁面的要求，並將要求彙總設為「全部計數」。

以速率為基礎的規則會計算單一聚總執行處理中登入頁面的所有要求，並在要求超出限制時套用規則動作。

下列 JSON 清單顯示此規則組態的範例。[計算所有彙總] 選項會列在 JSON 中做為設定CONSTANT。此範例與開頭為的登入頁面相符/login。

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 1000,
      "EvaluationWindowSec": 300,
      "AggregateKeyType": "CONSTANT",
      "ScopeDownStatement": {
        "ByteMatchStatement": {
          "FieldToMatch": {
            "UriPath": {}
          },
          "PositionalConstraint": "STARTS_WITH",
          "SearchString": "/login",
          "TextTransformations": [
            {
              "Type": "NONE",
              "Priority": 0
            }
```

```
          ]
        }
      }
    }
  }
}
```

速率限制從任何 IP 地址，用戶代理對登錄頁面的請求

若要限制對您網站上登入頁面的 IP 位址、使用者代理程式配對超出限制的要求數目，請將要求彙總設定為 [自訂索引鍵]，並提供彙總準則。

下列 JSON 清單顯示此規則組態的範例。在此範例中，我們將限制設定為每個 IP 位址 (使用者代理程式配對) 的任何五分鐘期間內 100 個要求。

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "EvaluationWindowSec": 300,
      "AggregateKeyType": "CUSTOM_KEYS",
      "CustomKeys": [
        {
          "Header": {
            "Name": "User-Agent",
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        },
```

```
        {
          "IP": {}
        }
      ],
      "ScopeDownStatement": {
        "ByteMatchStatement": {
          "FieldToMatch": {
            "UriPath": {}
          },
          "PositionalConstraint": "STARTS_WITH",
          "SearchString": "/login",
          "TextTransformations": [
            {
              "Type": "NONE",
              "Priority": 0
            }
          ]
        }
      }
    }
  }
}
```

速率限制缺少特定標頭的請求

若要限制缺少特定標頭的要求數目，您可以使用 [計算所有彙總] 選項搭配 scope-down 陳述式。使用邏輯NOT陳述式設定 scope-down 陳述式，其中包含只有在標頭存在且具有值時才會傳回 true 的陳述式。

下列 JSON 清單顯示此規則組態的範例。

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
```

```
    "RateBasedStatement": {
      "Limit": 1000,
      "AggregateKeyType": "CONSTANT",
      "EvaluationWindowSec": 300,
      "ScopeDownStatement": {
        "NotStatement": {
          "Statement": {
            "SizeConstraintStatement": {
              "FieldToMatch": {
                "SingleHeader": {
                  "Name": "user-agent"
                }
              },
              "ComparisonOperator": "GT",
              "Size": 0,
              "TextTransformations": [
                {
                  "Type": "NONE",
                  "Priority": 0
                }
              ]
            }
          }
        }
      }
    }
  }
}
```

速率限制帶有特定標籤的請求

您可以將速率限制與將標籤新增至要求的任何規則或規則群組結合使用，以限制不同類別的要求數目。若要執行這項操作，請依照下列方式設定 Web ACL：

- 新增新增標籤的規則或規則群組，並加以設定，使其不會封鎖或允許您要設定頻率限制的要求。如果您使用受管規則群組，您可能需要覆寫某些規則群組規則動作Count才能達成此行為。
- 使用高於標籤規則和規則群組的優先順序編號設定，將以速率為基礎的規則新增至 Web ACL。AWS WAF 以數字順序評估規則 (從最低值開始)，因此您的速率型規則會在標籤規則之後執行。使用規則向下範圍陳述式和標籤彙總中的標籤比對組合來設定標籤的速率限制。

下列範例使用 Amazon IP 信譽清單 AWS 受管規則規則群組。規則群組規則會`AWSManagedIPDDoSList`偵測並標記其 IP 已知會積極參與 DDoS 活動的要求。規則的動作在規則群組定義`Count`中設定為。如需規則群組的詳細資訊，請參閱the section called “Amazon IP 評價清單”。

下列 Web ACL JSON 清單使用 IP 信譽規則群組，後面接著以標籤比對速率為基礎的規則。以速率為基礎的規則會使用範圍向下陳述式來篩選已由規則群組規則標記的要求。以速率為基礎的規則陳述式會彙總並且速率會依據其 IP 位址來限制已篩選的要求。

```
{
  "Name": "test-web-acl",
  "Id": ...
  "ARN": ...
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesAmazonIpReputationList",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesAmazonIpReputationList"
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesAmazonIpReputationList"
      }
    },
    {
      "Name": "test-rbr",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 100,
          "EvaluationWindowSec": 300,
```

```
          "AggregateKeyType": "IP",
          "ScopeDownStatement": {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList"
            }
          }
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "test-rbr"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-web-acl"
  },
  "Capacity": 28,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:0000000000:webacl:test-web-acl:"
}
```

速率限制對具有指定標籤命名空間的標籤的請求

Bot Control 受管規則群組中的一般層級規則會為不同類別的機器人新增標籤，但它們只會封鎖來自未驗證機器人的要求。如需有關這些規則的資訊，請參閱機器人控制規則清單。

如果您使用 Bot Control 受管規則群組，則可以針對個別已驗證機器人的要求新增速率限制。若要這麼做，您可以新增在 Bot Control 規則群組之後執行的速率型規則，並依據機器人名稱標籤彙總請求。您可以指定 Label 命名空間彙總索引鍵，並將命名空間索引鍵設為`awswaf:managed:aws:bot-control:bot:name:`。每個具有指定命名空間的唯一標籤將定義一個聚合實例。例如，標籤`awswaf:managed:aws:bot-control:bot:name:axios`和`awswaf:managed:aws:bot-control:bot:name:curl`每個標籤都會定義彙總執行個體。

下列網頁 ACL JSON 清單會顯示此設定。此範例中的規則會在兩分鐘內將任何單一機器人彙總執行個體的要求限制為 1,000 個。

```
{
  "Name": "test-web-acl",
  "Id": ...
  "ARN": ...
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesBotControlRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesBotControlRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesBotControlRuleSet": {
                "InspectionLevel": "COMMON"
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesBotControlRuleSet"
      }
    },
    {
      "Name": "test-rbr",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 1000,
          "EvaluationWindowSec": 120,
          "AggregateKeyType": "CUSTOM_KEYS",
          "CustomKeys": [
```

```
            {
              "LabelNamespace": {
                "Namespace": "awswaf:managed:aws:bot-control:bot:name:"
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "test-rbr"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-web-acl"
  },
  "Capacity": 82,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:0000000000:webacl:test-web-acl:"
}
```

列出受速率規則限制的 IP 位址

如果以速率為基礎的規則僅彙總到 IP 位址或轉送的 IP 位址，您可以擷取規則目前受到速率限制的 IP 位址清單。 AWS WAF 將這些 IP 位址儲存在規則的受管理金鑰清單中。

> **Note**
>
> 只有當您僅彙總 IP 位址或標頭中的 IP 位址時，才能使用此選項。如果您使用自訂金鑰要求彙總，就無法擷取速率限制 IP 位址清單，即使您在自訂金鑰中使用其中一個 IP 位址規格也是如此。

以速率為基礎的規則會將其規則動作套用至符合規則範圍向下陳述式的規則受管理金鑰清單中的要求。當規則沒有範圍向下陳述式時，會將動作套用至來自清單中 IP 位址的所有要求。Block依預設，規則動

作可以是任何有效的規則動作，但可以是除了的任何有效規則動作Allow。使用以速率為基礎的規則執行個體， AWS WAF 可以進行頻率限制的 IP 位址數目上限為 10,000。如果超過 10,000 個位址超出速率限 AWS WAF 制，則會限制速率最高的位址。

您可以使用 CLI、API 或任何 SDK 存取以速率為基礎的規則的受管金鑰清單。本主題涵蓋使用 CLI 和 API 進行存取。控制台目前不提供對列表的訪問權限。

對於 AWS WAF API，命令是GetRateBasedStatementManagedKeys。

對於 AWS WAF CLI，該命令是受get-rate-based-statement管理的密鑰。

以下顯示針對 Amazon CloudFront 分發上 Web ACL 中使用的速率型規則擷取速率限制 IP 位址清單的語法。

```
aws wafv2 get-rate-based-statement-managed-keys --scope=CLOUDFRONT --region=us-east-1
 --web-acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

以下顯示區域應用程式、Amazon API 閘道 REST API、Application Load Balancer、 AWS AppSync GraphQL API、Amazon Cognito 使用者集區、 AWS App Runner 服務或 AWS 已驗證存取執行個體的語法。

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-
acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

AWS WAF 監控 Web 要求，並針對每個唯一的 Web ACL、選用規則群組和速率型規則組合獨立管理金鑰。例如，如果您在規則群組內定義以速率為基礎的規則，然後在 Web ACL 中使用規則群組，則會 AWS WAF 監視 Web 要求並管理該 Web ACL、規則群組參考陳述式和以速率為基礎的規則執行個體的索引鍵。如果您在第二個 Web ACL 中使用相同的規則群組，則會 AWS WAF 監控 Web 要求並管理第二次使用的金鑰，完全獨立於您的第一個使用方式。

對於您在規則群組中定義的以速率為基礎的規則，除了 Web ACL 名稱和規則群組內以速率為基礎的規則名稱之外，您還需要在請求中提供規則群組參考陳述式的名稱。以下顯示區域應用程式的語法，其中以速率為基礎的規則是在規則群組內定義的，而規則群組則用於 Web ACL。

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-
acl-name=WebACLName --web-acl-id=WebACLId --rule-group-rule-name=RuleGroupRuleName --
rule-name=RuleName
```

規則群組規則陳述式

規則群組規則陳述式不可嵌套。

本節說明您可以在 Web ACL 中使用的規則群組規則陳述式。規則群組 Web ACL 容量單位 (WCU) 是由規則群組擁有者在建立時設定的。如需 WCU 的相關資訊，請參閱 AWS WAF 網路 ACL 容量單位 (WCU)。

規則群組陳述式	描述	WCU
受管規則群組	執行指定的受管規則群組中定義的規則。 您可以透過新增範圍向下陳述式來縮小規則群組評估的要求範圍。 您無法在任何其他陳述式類型中巢狀化受管規則群組陳述式。	由規則群組定義，加上任何額外的 WCU，用於向下範圍陳述式。
規則群組	執行在您管理的規則群組中定義的規則。 您無法為自己的規則群組新增範圍陳述式至規則群組參考陳述式。 您無法在任何其他陳述式類型中巢狀化規則群組陳述式	您可以在建立規則群組時定義規則群組的 WCU 限制。

管理規則群組陳述式

受管規則群組規則陳述式會將 Web ACL 規則清單中的參考新增至受管規則群組。您在主控台上的規則陳述式下看不到此選項，但是當您使用 JSON 格式的 Web ACL 時，您新增的任何受管規則群組都會顯示為此類型。

受管規則群組可能是 AWS 受管規則群組，其中大部分對 AWS WAF 客戶免費使用，也可以是 AWS Marketplace 受管規則群組。當您將付費的 AWS 受管規則群組新增至 Web ACL 時，您會自動訂閱付費的受管規則群組。您可以透過訂閱 AWS Marketplace 受管規則群組 AWS Marketplace。如需詳細資訊，請參閱 受管規則群組。

將規則群組新增至 Web ACL 時，您可以將群組中規則的動作覆寫至另一個規則動作，Count或覆寫至另一個規則動作。如需詳細資訊，請參閱 規則群組的動作覆寫選項。

您可以縮小使用規則群組 AWS WAF 評估的要求範圍。若要這麼做，您可以在規則群組陳述式中加入範圍向下陳述式。如需有關向下範圍陳述式的資訊，請參閱。範圍向下語句這可協助您管理規則群組對流量的影響，並協助您控制使用規則群組時與流量相關的成本。如需將範圍向下陳述式與 AWS WAF 機器人控制管理規則群組搭配使用的資訊和範例，請參閱。AWS WAF 機器人控制

不可嵌套 — 您無法將此陳述式類型嵌套在其他陳述式中，也無法將其包含在規則群組中。您可以將它直接包含在 Web ACL 中。

(選擇性) ScopeUp 陳述式 — 此規則類型採用選用的範圍向下陳述式，以縮小規則群組評估的要求範圍。如需詳細資訊，請參閱 範圍向下語句。

WCU — 在建立時為規則群組設定。

在哪裡可以找到這個規則聲明

- 主控台 — 在建立 Web ACL 的過程中，在 [新增規則和規則群組] 頁面上，選擇 [新增受管規則群組]，然後尋找並選取您要使用的規則群組。
- API — ManagedRuleGroupStatement

規則群組陳述式

規則群組規則陳述式會將參考新增至您管理的規則群組的 Web ACL 規則清單中。您在主控台上的規則陳述式下看不到此選項，但是當您使用 JSON 格式的 Web ACL 時，您新增的自有規則群組都會顯示為此類型。如需有關使用您自己的規則群組的資訊，請參閱 管理您自己的規則群組。

將規則群組新增至 Web ACL 時，您可以將群組中規則的動作覆寫至另一個規則動作，Count或覆寫至另一個規則動作。如需詳細資訊，請參閱 規則群組的動作覆寫選項。

不可嵌套 — 您無法將此陳述式類型嵌套在其他陳述式中，也無法將其包含在規則群組中。您可以將它直接包含在 Web ACL 中。

WCU — 在建立時為規則群組設定。

在哪裡可以找到這個規則聲明

- 主控台 — 在建立 Web ACL 的過程中，在 [新增規則和規則群組] 頁面上，選擇 [新增我自己的規則和規則群組]、[規則群組]，然後新增您要使用的規則群組。
- API — RuleGroupReferenceStatement

處理超大請求組件 AWS WAF

AWS WAF 不支持檢查 Web 請求組件正文，標題或 cookie 的非常大的內容。基礎主機服務對轉寄至 AWS WAF 檢查的項目有計數和大小限制。例如，主機服務不會傳送超過 200 個標頭 AWS WAF，因此對於具有 205 個標頭的 Web 要求，則 AWS WAF 無法檢查最後 5 個標頭。

當 AWS WAF 允許 Web 要求繼續存取受保護的資源時，就會傳送整個 Web 要求，包括超出可檢查計數和大小限制 AWS WAF 的任何內容。

元件檢測尺寸限制

元件檢驗尺寸限制如下：

- **`Body`**和 **`JSON Body`** — 對於 Application Load Balancer AWS AppSync， AWS WAF 可以檢查要求主體的前 8 KB。對於 CloudFront API Gateway、Amazon Cognito、應用程式執行器和驗證存取，預設情況下 AWS WAF 可以檢查前 16 KB，而且您可以在 Web ACL 組態中將限制增加到 64 KB。如需詳細資訊，請參閱 管理車身檢查尺寸限制。
- **`Headers`**— 最多 AWS WAF 可以檢查要求標頭的前 8 KB (8,192 位元組)，以及最多前 200 個標頭。內容可供檢查，最多可 AWS WAF 達到第一個限制。
- **`Cookies`**— 最多 AWS WAF 可以檢查請求餅乾的前 8 KB（8,192 字節）和最多前 200 個餅乾。內容可供檢查，最多可 AWS WAF 達到第一個限制。

規則陳述式的超大處理選項

當您撰寫檢查其中一個要求元件類型的規則陳述式時，您可以指定如何處理過大的元件。當規則檢查的要求元件超過大小限制時，超大處理會告訴 AWS WAF 如何處理 Web 要求。

處理超大元件的選項如下：

- Continue— 根據規則檢查標準正常檢查請求元件。 AWS WAF 將檢查大小限制內的請求組件內容。
- Match— 將 Web 要求視為符合規則陳述式。 AWS WAF 將規則作業套用至請求，而不根據規則的檢驗條件評估它。

- No match— 將 Web 請求視為不符合規則陳述式，而不根據規則的檢查條件評估它。 AWS WAF 使用 Web ACL 中的其餘規則繼續檢查 Web 請求，就像對任何不相符的規則一樣。

在主 AWS WAF 控台中，您必須選擇其中一個處理選項。在主控台外部，預設選項為Continue。

如果您在將其動作設定為的規則中使用Match選項Block，則規則會封鎖檢查元件過大的要求。對於任何其他配置，請求的最終處理方式取決於各種因素，例如 Web ACL 中其他規則的配置以及 Web ACL 的預設動作設定。

您不擁有的規則群組中的超大處理

元件大小和計數限制適用於您在 Web ACL 中使用的所有規則。這包括您在受管規則群組和由其他帳戶與您共用的規則群組中使用但未管理的任何規則。

當您使用不管理的規則群組時，規則群組可能會有一個規則來檢查有限的要求元件，但不會按照您需要處理的方式來處理過大的內容。如需受管規則如何 AWS 管理過大元件的相關資訊，請參閱AWS 受管規則規則群組清單。如需其他規則群組的相關資訊，請洽詢您的規則群組提供者。

在 Web ACL 中管理過大元件的準則

您在 Web ACL 中處理過大元件的方式可能取決於許多因素，例如要求元件內容的預期大小、Web ACL 的預設要求處理，以及 Web ACL 中其他規則如何比對和處理要求。

管理過大型 Web 請求元件的一般準則如下：

- 如果您需要允許某些組件內容過大的請求，請盡可能添加規則以明確允許這些請求。排定這些規則的優先順序，使其在 Web ACL 中檢查相同元件類型的任何其他規則之前執行。使用這種方法，您將無法使用檢 AWS WAF 查允許傳遞給受保護資源的超大組件的全部內容。
- 對於所有其他請求，您可以阻止超過限制的請求來阻止任何其他字節傳遞：
  - 您的規則和規則群組 — 在使用大小限制檢查元件的規則中，設定超大處理，以便封鎖超過限制的要求。例如，如果您的規則封鎖具有特定標頭內容的要求，請將超大處理設定為符合標頭內容過大的要求。或者，如果您的 Web ACL 預設會封鎖要求，且您的規則允許特定的標頭內容，請將規則的超大處理設定為不符合任何具有超大標頭內容的要求。
  - 您不管理的規則群組 — 為了防止您不管理的規則群組允許過大的要求元件，您可以新增個別規則來檢查要求元件類型，並封鎖超過限制的要求。排定 Web ACL 中的規則優先順序，使其在規則群組之前執行。例如，在 Web ACL 中執行任何主體檢查規則之前，您可以封鎖具有超大主體內容的請求。下列程序說明如何新增此類型的規則。

阻止過大的 Web 請求組件

您可以在 Web ACL 中新增規則，以封鎖具有過大元件的請求。

新增封鎖過大內容的規則

1. 當您建立或編輯 Web ACL 時，請在規則設定中選擇 [新增規則]、[新增我自己的規則和規則群組]、[規則產生器]，然後選擇 [規則視覺化編輯器]。如需建立或編輯 Web ACL 的指導，請參閱使用 Web ACL。
2. 輸入規則的名稱，並將「類型」設定保留為「一般」規則。
3. 從預設值變更下列比對設定：
   a. 在「陳述式」中，針對「檢查」開啟下拉式清單，然後選擇您需要的 Web 要求元件 (「內文」、「標頭」或「Cookie」)。
   b. 對於「相符類型」，請選擇「大小大於」。
   c. 在「大小」中，輸入至少為組件類型最小大小的數字。對於標題和餅乾，請鍵入8192。在 Application Load Balancer 或 AWS AppSync Web ACL 中，針對主體，鍵8192入。對於 API Gateway CloudFront、Amazon Cognito、應用程式執行器或驗證存取網路 ACL 中的主體，如果您使用的是預設本體大小限制，請鍵入。16384否則，請輸入您為 Web ACL 定義的主體大小限制。
   d. 對於超大尺寸處理，請選取「符合」。
4. 選取「動作」做為「封鎖」。
5. 選擇新增規則。
6. 新增規則後，在 [設定規則優先順序] 頁面上，將其移至 Web ACL 中檢查相同元件類型的任何規則或規則群組上方。這會讓新規則具有較低的數值優先順序設定，因 AWS WAF 此會先評估該規則。如需更多詳細資訊，請參閱 Web ACL 中規則和規則群組的處理順序。

正則表達式模式匹配 AWS WAF

AWS WAF 支援 PCRE 程式庫`libpcre`所使用的樣式語法。該庫在 PCRE-Perl 兼容的正則表達式中記錄。

AWS WAF 不支持庫的所有構造。例如，它支持一些零寬度斷言，但不是全部。我們沒有支持的構造的完整列表。但是，如果您提供無效的正則表達式模式或使用不支持的構造，則 AWS WAF API 會報告失敗。

AWS WAF 不支援下列 PCRE 模式：

- Backreferences 和擷取子運算式
- 子程式參考和遞迴模式
- 條件式模式
- 恢復控制動詞
- \C 單一位元組指令
- \R 換行比對指令
- \K 開頭比對重設指令
- 圖說文字和內嵌的程式碼
- 原子分組和所佔有的量詞

IP 集和正則表達式模式集 AWS WAF

AWS WAF 透過在規則中參照這些資訊，將一些更複雜的資訊儲存在您使用的集合中。這些集合中的每一個都有一個名稱，並在建立時獲指派一個 Amazon Resource Name (ARN)。您可以從規則陳述式內管理這些集合，而且可以透過主控台導覽窗格存取和管理這些集合。

您可以在規則群組或 Web ACL 中使用受管理的集。

- 若要使用 IP 集，請參閱IP 集合比對規則陳述式。
- 要使用正則表達式模式集，請參閱規則運算式模式集比對規則陳述式。

更新期間暫時不一致

當您建立或變更 Web ACL 或其他 AWS WAF 資源時，變更需要少量時間才能傳播到儲存資源的所有區域。傳輸時間可以是幾秒鐘到分鐘數。

以下是您在變更傳播期間可能會注意到的暫時性不一致的範例：

- 建立 Web ACL 之後，如果您嘗試將其與資源建立關聯，可能會出現例外狀況，指出 Web ACL 無法使用。
- 將規則群組新增至 Web ACL 後，新規則群組規則可能會在使用 Web ACL 的某個區域中生效，而不會在另一個區域中生效。
- 變更規則動作設定後，您可能會在某些地方看到舊動作，而在其他地方看到新動作。
- 將 IP 位址新增至封鎖規則中使用的 IP 集後，該新位址可能會在某個區域遭到封鎖，而另一個區域仍允許使用該 IP 位址。

主題

建立和管理 IP 集合

IP 集合提供您要在規則陳述式中一起使用的 IP 地址和 IP 地址範圍的集合。IP 集是 AWS 資源。

若要在 Web ACL 或規則群組中使用 IP 集，請先建立`IPSet`具有位址規格的 AWS 資源。然後，當您將 IP 集合規則陳述式新增至 Web ACL 或規則群組時，您會參考該集合。

主題

建立 IP 集合

遵循本節中的程序來建立新的 IP 集合。

> **Note**
>
> 除了本節中的程序之外，您還可以在將 IP 比對規則新增至 Web ACL 或規則群組時選擇新增新的 IP 集合。選擇該選項需要您提供與此程序所需的相同設定。

建立 IP 集合

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中，選擇 IP sets (IP 集合)，然後選擇 Create IP set (建立 IP 集合)。
3. 輸入 IP 集合的名稱和描述。當您要使用它們時，您將使用它們來識別該集合。

   > **Note**
   >
   > 建立 IP 集合後無法修改名稱。

4. 在「地區」中，選擇「全域」(CloudFront) 或選擇您要儲存 IP 集的區域。您只能在保護區域資源的 Web ACL 中使用地區 IP 集。若要在保護 Amazon CloudFront 分發的 Web ACL 中使用 IP 集，您必須使用全域 (CloudFront)。
5. 針對 IP version (IP 版本)，選取您要使用的版本。
6. 在 IP 位址文字方塊中，以 CIDR 標記法輸入每行一個 IP 位址或 IP 位址範圍。 AWS WAF 支援所有 IPv4 和 IPv6 CIDR 範圍，除了 `/0` 如需 CIDR 符號表示法的詳細資訊，請參閱 Wikipedia 文章無類別網域間路由。

   以下是一些範例：

   - 若要指定 IPv4 地址 192.0.2.44，請輸入 192.0.2.44/32。
   - 若要指定 IPv6 位址，請輸入 2620：0：0：0：0：0
   - 若要指定 IPv4 地址的範圍，從 192.0.2.0 to 192.0.2.255，請輸入 192.0.2.0/24。
   - 若要指定 IPv6 地址的範圍，從 2620:0:2d0:200:0:0:0:0 to 2620:0:2d0:200:ffff:ffff:ffff:ffff，請輸入 2620:0:2d0:200::/64。
7. 檢閱 IP 集合的設定，然後選擇 Create IP set (建立 IP 集合)。

刪除 IP 集合

遵循本節中的指引來刪除參考集。

刪除參照集和規則群組

當您刪除可在 Web ACL 中使用的實體 (例如 IP 集、正則運算式模式集或規則群組) 時，會 AWS WAF 檢查實體目前是否正在 Web ACL 中使用。如果發現它正在使用中， AWS WAF 會警告您。 AWS WAF 幾乎總是能夠確定某個實體是否被 Web ACL 引用。但是在極少數的情況下，它也可能無法判斷。如果您需要確定目前沒有任何實體正在使用該實體，請在刪除實體之前在 Web ACL 中檢查它。如果實體是參照集，請同時檢查是否沒有規則群組正在使用它。

刪除 IP 集合

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中，選擇 IP sets (IP 集合)。
3. 選取您要刪除的 IP 集合，然後選擇 Delete (刪除)。

建立和管理規則運算式模式集

規則運算式模式集提供您要在規則陳述式中一起使用的規則運算式的集合。正則表達式模式集是 AWS 資源。

要在 Web ACL 或規則組中使用正則表達式模式集，首先使用正則表達式模式規格創建一個 AWS 資源。`RegexPatternSet`然後，當您將規則運算式模式集合規則陳述式新增至 Web ACL 或規則群組時，您會參考該集合。規則運算式模式集必須至少包含一個規則運算式模式。

如果您的正則表達式模式集包含多個正則表達式模式，則在規則中使用時，模式匹配將與`OR`邏輯相結合。也就是說，如果請求元件符合集合中的任何模式，則 Web 請求將比對模式集規則陳述式。

AWS WAF 支援 PCRE 程式庫所使用的模式語法，但`libpcre`有一些例外。該庫在 PCRE-Perl 兼容的正則表達式中記錄。如需有關 AWS WAF 支援的資訊，請參閱正則表達式模式匹配 AWS WAF。

主題

- 建立規則運算式模式集
- 刪除規則運算式模式集

建立規則運算式模式集

遵循本節中的程序來建立新的規則運算式模式集。

建立規則運算式模式集

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中，選擇 Regex pattern sets (規則運算式模式集)，然後選擇 Create regex pattern set (建立規則運算式模式集)。
3. 輸入規則運算式模式集的名稱和描述。當您要使用該集合時，您將使用這些項目來加以識別。

   > **Note**
   >
   > 建立規則運算式模式集後無法變更名稱。

4. 對於「區域」，請選擇「全域」(CloudFront) 或選擇您要儲存正則運算式模式集的區域。您只能在保護區域資源的 Web ACL 中使用區域正則表達式模式集。要使用在保護 Amazon CloudFront 分發的 Web ACL 中設置的正則表達式模式，您必須使用 Global (CloudFront)。

5. 在 Regular expressions (規則運算式) 文字方塊中，每行輸入一個規則運算式模式。

   例如，規則運算式 `I[a@]mAB[a@]dRequest` 符合下列字串：`IamABadRequest`、`IamAB@dRequest`、`I@mABadRequest` 和 `I@mAB@dRequest`。

   AWS WAF 支援 PCRE 程式庫所使用的模式語法，但`libpcre`有一些例外。該庫在 PCRE-Perl 兼容的正則表達式中記錄。如需有關 AWS WAF 支援的資訊，請參閱正則表達式模式匹配 AWS WAF。
6. 檢閱規則運算式模式集的設定，然後選擇 Create regex pattern set (建立規則運算式模式集)。

刪除規則運算式模式集

遵循本節中的指引來刪除參考集。

刪除參照集和規則群組

當您刪除可在 Web ACL 中使用的實體 (例如 IP 集、正則運算式模式集或規則群組) 時，會 AWS WAF 檢查實體目前是否正在 Web ACL 中使用。如果發現它正在使用中， AWS WAF 會警告您。 AWS WAF 幾乎總是能夠確定某個實體是否被 Web ACL 引用。但是在極少數的情況下，它也可能無法判斷。如果您需要確定目前沒有任何實體正在使用該實體，請在刪除實體之前在 Web ACL 中檢查它。如果實體是參照集，請同時檢查是否沒有規則群組正在使用它。

刪除規則運算式模式集

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中，選擇 Regex pattern sets (規則運算式模式集)。
3. 選取您要刪除的規則運算式模式集，然後選擇 Delete (刪除)。

定制的 Web 請求和響應 AWS WAF

您可以將自訂 Web 要求和回應處理行為新增至 AWS WAF 規則動作和預設 Web ACL 動作。每當附加的動作套用時，您的自訂設定便會套用。

您可以透過下列方式自訂 Web 要求和回應：

- 使用Allow、CountCAPTCHA、和Challenge動作，您可以在 Web 要求中插入自訂標頭。將 Web 請求 AWS WAF 轉發到受保護的資源時，請求包含整個原始請求以及您插入的自定義標頭。對於CAPTCHA和Challenge動作， AWS WAF 僅在請求通過 CAPTCHA 或挑戰權杖檢查時套用自訂。

- 透過Block動作，您可以使用回應碼、標頭和內文來定義完整的自訂回應。受保護的資源會使用提供的自訂回應來回應要求 AWS WAF。您的自訂回應會取代的預設Block動作回應403 (Forbidden)。

您可以自訂的動作設定

您可以在定義下列動作設定時指定自訂要求或回應：

- 規則動作。如需相關資訊，請參閱規則動作。
- Web ACL 的預設動作。如需相關資訊，請參閱網頁 ACL 預設動作。

您無法自訂的動作設定

您無法在 Web ACL 中使用的規則群組的覆寫動作中指定自訂要求處理。請參閱Web ACL 規則和規則群組評估。另請參閱管理規則群組陳述式和規則群組陳述式。

更新期間暫時不一致

當您建立或變更 Web ACL 或其他 AWS WAF 資源時，變更需要少量時間才能傳播到儲存資源的所有區域。傳輸時間可以是幾秒鐘到分鐘數。

以下是您在變更傳播期間可能會注意到的暫時性不一致的範例：

- 建立 Web ACL 之後，如果您嘗試將其與資源建立關聯，可能會出現例外狀況，指出 Web ACL 無法使用。
- 將規則群組新增至 Web ACL 後，新規則群組規則可能會在使用 Web ACL 的某個區域中生效，而不會在另一個區域中生效。
- 變更規則動作設定後，您可能會在某些地方看到舊動作，而在其他地方看到新動作。
- 將 IP 位址新增至封鎖規則中使用的 IP 集後，該新位址可能會在某個區域遭到封鎖，而另一個區域仍允許使用該 IP 位址。

限制您對自訂要求和回應的使用

AWS WAF 定義您使用自訂要求和回應的最大設定。例如，每個 Web ACL 或規則群組的要求標頭數目上限，以及單一自訂回應定義的自訂標頭數目上限。如需相關資訊，請參閱AWS WAF 配額。

主題

- 用於非阻塞操作的自定義請求標題插入

- Block動作的自訂回應
- 自訂回應的支援狀態碼

用於非阻塞操作的自定義請求標題插入

您可以指示 AWS WAF 在規則動作未封鎖要求時，將自訂標頭插入原始 HTTP 要求。使用此選項，您只會新增至要求。您無法修改或取代原始要求的任何部分。自訂標頭插入的使用案例包括向下游應用程式發出信號，以根據插入的標頭以不同的方式處理要求，以及標記要求以進行分析。

此選項適用於設定為的 Web ACL 預設動Allow作的規則動作CAPTCHA、Challenge和Allow。Count如需規則動作的詳細資訊，請參閱 規則動作。如需有關預設 Web ACL 動作的更多資訊，請參閱網頁 ACL 預設動作。

自訂要求標頭名稱

AWS WAF 前綴它插入的所有請求標頭`x-amzn-waf-`，以避免與請求中已經存在的標頭混淆。例如，如果您指定標頭名稱`sample`，則會 AWS WAF 插入標頭`x-amzn-waf-sample`。

具有相同名稱的標題

如果要求已具有與插入相同名稱的標頭， AWS WAF 則 AWS WAF 會覆寫標頭。因此，如果您在具有相同名稱的多個規則中定義標題，則檢查請求並找到匹配項的最後一條規則將添加其標題，並且以前的任何規則都不會添加。

具有非終止規則動作的自訂標頭

與Allow動作不同，Count動作不會停 AWS WAF 止使用 Web ACL 中其餘規則處理 Web 要求。同樣，當CAPTCHA並Challenge確定請求令牌有效時，這些操作不會停 AWS WAF 止處理 Web 請求。因此，如果您使用具有上述其中一個動作的規則插入自訂標題，後續規則也可能會插入自訂標題。如需規則動作行為的詳細資訊，請參閱規則動作。

例如，假設您有下列規則，並依照顯示的順序排列優先順序：

1. RULE 具有一個Count動作和名為`RuleAHeader`的自定義標題。
2. 具有Allow動作和名為的自訂標頭的 RuleB。`RuleBHeader`

如果要求同時符合 ruLeA 和 RuleB，請 AWS WAF 插入標頭`x-amzn-waf-RuleAHeader`和`x-amzn-waf-RuleBHeader`，然後將要求轉寄至受保護的資源。

AWS WAF 完成檢查請求後，將自定義標題插入 Web 請求中。因此，如果您將自訂要求處理與動作設定為的規則搭配使用Count，則後續規則不會檢查您新增的自訂標頭。

自訂要求處理範例

您可以為規則的動作或 Web ACL 的預設動作定義自訂要求處理。下列清單顯示新增至 Web ACL 預設動作的自訂處理的 JSON。

```
{
 "Name": "SampleWebACL",
 "Scope": "REGIONAL",
 "DefaultAction": {
  "Allow": {
   "CustomRequestHandling": {
    "InsertHeaders": [
     {
      "Name": "fruit",
      "Value": "watermelon"
     },
     {
      "Name": "pie",
      "Value": "apple"
     }
    ]
   }
  }
 },
 "Description": "Sample web ACL with custom request handling configured for default
 action.",
 "Rules": [],
 "VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "SampleWebACL"
 }
}
```

Block動作的自訂回應

您可以指示 AWS WAF 將規則動作或 Web ACL 預設處理行動設定為的自訂 HTTP 回應傳送回Block用戶端。如需規則動作的詳細資訊，請參閱 規則動作。如需有關預設 Web ACL 動作的更多資訊，請參閱網頁 ACL 預設動作。

當您定義Block動作的自訂回應處理時，您可以定義狀態碼、標頭和回應內文。如需可搭配使用的狀態碼清單 AWS WAF，請參閱下一節自訂回應的支援狀態碼。

使用案例

自訂回應的使用案例如下：

- 將非預設狀態碼傳送回用戶端。
- 將自定義響應頭發送回客戶端。您可以指定除外的任何標頭名稱`content-type`。
- 將靜態錯誤頁面發送回客戶端。
- 將用戶端重新導向至不同的 URL。若要這麼做，您可以指定其中一個重新`3xx`導向狀態碼 (例如`301 (Moved Permanently)`或)`302 (Found)`，然後指定以新 URL 命名`Location`的新標頭。

與您在受保護資源中定義的回應互動

您為 AWS WAF Block動作指定的自訂回應優先於您在受保護資源中定義的任何回應規格。

您所保護之 AWS 資源的主機服務 AWS WAF 可能允許處理 Web 要求的自訂回應。範例如下：

- 使用 Amazon CloudFront，您可以根據狀態碼自訂錯誤頁面。如需詳細資訊，請參閱 Amazon CloudFront 開發人員指南中的產生自訂錯誤回應。
- 使用 Amazon API Gateway，您可以定義閘道的回應和狀態碼。如需相關資訊，請參閱 Amazon API Gateway 開發人員指南中 API 閘道中的閘道回應。

您無法將 AWS WAF 自訂回應設定與受保護 AWS 資源中的自訂回應設定結合。任何個別 Web 請求的響應規範完全來自 AWS WAF 或完全來自受保護的資源。

對於 AWS WAF 封鎖的 Web 要求，下列項目顯示優先順序。

1. AWS WAF 自定義響應 — 如果 AWS WAF Block操作啟用了自定義響應，則受保護的資源將配置的自定義響應發送回客戶端。您可能已在受保護的資源本身中定義的任何回應設定都沒有作用。
2. 受保護資源中定義的自訂回應 — 否則，如果受保護的資源指定了自訂回應設定，則受保護的資源會使用這些設定來回應用戶端。
3. AWS WAF 預設Block回應 — 否則，受保護的資源會以 AWS WAF 預設回應來Block回應用戶端`403 (Forbidden)`。

對於 AWS WAF 允許的 Web 請求，受保護資源的配置將決定它發送回客戶端的響應。您無法在中 AWS WAF 針對允許的要求設定回應設定。您可以在中 AWS WAF 針對允許的要求設定的唯一自訂項

目是在將要求轉寄至受保護的資源之前，將自訂標頭插入原始要求。此選項在前面的章節中說明用於非阻塞操作的自定義請求標題插入。

自定義響應頭

您可以指定除外的任何標頭名稱content-type。

自訂回應主體

您可以在 Web ACL 或規則群組的前後關聯內容中定義自訂回應的主體。定義自訂回應主體之後，您可以在 Web ACL 或規則群組中的其他任何位置參照來使用它。在個別Block動作設定中，您會參考您要使用的自訂內文，並定義自訂回應的狀態碼和標頭。

當您在主控台中建立自訂回應時，您可以從已定義的回應主體中進行選擇，也可以建立新的主體。在主控台外部，您可以在 Web ACL 或規則群組層級定義自訂回應主體，然後從 Web ACL 或規則群組中的動作設定中參照這些回應本文。這會顯示在下一節的範例 JSON 中。

自定義響應示例

下列範例會列出具有自訂回應設定之規則群組的 JSON。自訂回應主體是針對整個規則群組定義的，然後在規則動作中按鍵參考。

```
{
 "ARN": "test_rulegroup_arn",
 "Capacity": 1,

 "CustomResponseBodies": {
  "CustomResponseBodyKey1": {
   "Content": "This is a plain text response body.",
   "ContentType": "TEXT_PLAIN"
  }
 },

 "Description": "This is a test rule group.",
 "Id": "test_rulegroup_id",
 "Name": "TestRuleGroup",

 "Rules": [
  {
   "Action": {
    "Block": {
     "CustomResponse": {
      "CustomResponseBodyKey": "CustomResponseBodyKey1",
```

```
      "ResponseCode": 404,
      "ResponseHeaders": [
       {
        "Name": "BlockActionHeader1Name",
        "Value": "BlockActionHeader1Value"
       }
      ]
     }
    }
   },
   "Name": "GeoMatchRule",
   "Priority": 1,
   "Statement": {
    "GeoMatchStatement": {
     "CountryCodes": [
      "US"
     ]
    }
   },
   "VisibilityConfig": {
    "CloudWatchMetricsEnabled": true,
    "MetricName": "TestRuleGroupReferenceMetric",
    "SampledRequestsEnabled": true
   }
  }
 ],
 "VisibilityConfig": {
  "CloudWatchMetricsEnabled": true,
  "MetricName": "TestRuleGroupMetric",
  "SampledRequestsEnabled": true
 }
}
```

自訂回應的支援狀態碼

有關 HTTP 狀態碼的詳細信息，請參閱互聯網工程任務組（IETF）的狀態代碼和維基百科上的 HTTP 狀態碼列表。

以下是 AWS WAF 支援自訂回應的 HTTP 狀態碼。

- 2xx Successful
  - 200 – OK

  - 201 – Created
  - 202 – Accepted
  - 204 – No Content
  - 206 – Partial Content
- 3xx Redirection
  - 300 – Multiple Choices
  - 301 – Moved Permanently
  - 302 – Found
  - 303 –See Other
  - 304 – Not Modified
  - 307 – Temporary Redirect
  - 308 – Permanent Redirect
- 4xx Client Error
  - 400 – Bad Request
  - 401 – Unauthorized
  - 403 – Forbidden
  - 404 – Not Found
  - 405 – Method Not Allowed
  - 408 – Request Timeout
  - 409 – Conflict
  - 411 – Length Required
  - 412 – Precondition Failed
  - 413 – Request Entity Too Large
  - 414 – Request-URI Too Long
  - 415 – Unsupported Media Type
  - 416 – Requested Range Not Satisfiable
  - 421 – Misdirected Request
  - 429 – Too Many Requests
- 5xx Server Error
  - 500 – Internal Server Error

- 501 – Not Implemented
- 502 – Bad Gateway
- 503 – Service Unavailable
- 504 – Gateway Timeout
- 505 – HTTP Version Not Supported

AWS WAF 標籤, 上, 网, 請求

標籤是當規則符合要求時，由規則新增至 Web 要求的中繼資料。新增之後，在 Web ACL 評估結束之前，標籤仍然可用於請求中。您可以使用 label match 陳述式存取稍後在 Web ACL 評估中執行的規則中的標籤。如需詳細資訊，請參閱 標籤比對規則陳述式。

Web 請求上的標籤會產生 Amazon CloudWatch 標籤指標。如需量度和維度的清單，請參閱標示量度和維度。如需透過主控台和透過 CloudWatch 主控台存取度量和測量結果摘要的相關資 AWS WAF 訊，請參閱監控和調整。

標籤使用案例

AWS WAF 標籤的常見使用案例如下：

- 在對請求採取動作之前，針對多個規則陳述式評估 Web 請求 — 在 Web ACL 中找到符合規則之後，如果規則動作未終止 Web ACL 評估，則 AWS WAF 繼續針對 Web ACL 評估評估請求。在決定允許或封鎖請求之前，您可以使用標籤來評估和收集來自多個規則的資訊。若要執行此操作，請將現有規則的動作變更為，Count並將其配置為將標籤新增至相符請求。然後，新增一或多個要在其他規則之後執行的新規則，並將其設定為評估標籤，並根據標籤比對組合管理請求。
- 依地理區域管理 Web 請求 — 您可以單獨使用地理比對規則，依來源國家/地區管理 Web 請求。若要微調至區域層級的位置，您可以使用地理比對規則搭配Count動作，然後再加上標籤比對規則。如需地理比對規則的相關資訊，請參閱地理比對規則陳述式。
- 跨多個規則重複使用邏輯 — 如果您需要跨多個規則重複使用相同的邏輯，您可以使用標籤來單一取得邏輯，然後只測試結果。當您有多個使用巢狀規則陳述式共同子集的複雜規則時，在複雜規則之間複製通用規則集可能會耗時且容易出錯。使用標籤，您可以建立包含通用規則子集的新規則，以計算相符請求並為其新增標籤。您可以將新規則新增至 Web ACL，使其在原始複雜規則之前執行。然後，在原始規則中，將共用規則子集取代為檢查標籤的單一規則。

  例如，假設您有多個只想套用至登入路徑的規則。您可以實作包含該邏輯的單一新規則，而不是讓每個規則都指定相同的邏輯以符合潛在的登入路徑。讓新規則為相符的要求新增標籤，以指出要求

位於登入路徑上。在 Web ACL 中，將此新規則指定為低於原始規則的數值優先順序設定，以便先執行。然後，在您的原始規則中，用檢查標籤是否存在替換共享邏輯。如需優先順序設定的資訊，請參閱Web ACL 中規則和規則群組的處理順序。

- 在規則群組中建立規則例外 — 此選項對於您無法檢視或變更的受管規則群組特別有用。許多受管規則群組規則會將標籤新增至相符的 Web 要求，以指出符合的規則，並可能提供相符項目的其他相關資訊。當您使用將標籤新增至要求的規則群組時，您可以覆寫規則群組規則來計算相符項目，然後在根據規則群組標籤處理 Web 要求的規則群組後執行規則。所有 AWS 受管規則都會將標籤新增至相符的 Web 要求。如需詳細資訊，請參閱中的規則說明AWS 受管規則規則群組清單。
- 使用標籤指標監控流量模式 — 您可以存取透過規則新增的標籤以及您在 Web ACL 中使用之任何受管規則群組新增的量度的指標。所有受 AWS 管規則群組都會將標籤新增至其評估的 Web 要求。如需標籤量度和維度的清單，請參閱標示量度和維度。您可以透過 AWS WAF 主控台中的 Web ACL 頁面存取測量結果 CloudWatch 和測量結果摘要。如需相關資訊，請參閱監控和調整。

AWS WAF 標籤的工作原理

當規則符合 Web 要求時，如果規則已定義標籤，則會在規則評估結束時將標籤 AWS WAF 新增至要求。在 Web ACL 中相符規則之後評估的規則可以與規則新增的標籤相符。

誰在請求中新增標籤

用於評估請求的 Web ACL 元件可以在請求中加入標籤。

- 任何不是規則群組參考陳述式的規則都可以在相符的 Web 要求中新增標籤。標籤準則是規則定義的一部分，當 Web 請求符合規則時，會將規則的標籤 AWS WAF 新增至請求。如需相關資訊，請參閱the section called “加入標示的規則”。
- geo 比對規則陳述式會將國家/地區標籤新增至其檢查的任何請求，而不論陳述式是否產生相符項目。如需相關資訊，請參閱the section called “地理比對”。
- AWS WAF 所有將標籤新增至其檢查請求的 AWS 受管規則。它們會根據規則群組中的規則相符項目新增一些標籤，並根據受管規則群組使用的 AWS 處理序新增一些標籤，例如當您使用智慧型威脅緩和規則群組時新增的 Token 標籤。如需每個受管規則群組新增之標籤的相關資訊，請參閱the section called “AWS 受管規則規則群組清單”。

如何 AWS WAF 管理標籤

AWS WAF 在規則檢查請求結束時，將規則的標籤新增至要求。標籤是規則比對活動的一部分，類似於動作。

Web ACL 評估結束後，標籤不會保留在 Web 要求中。為了讓其他規則與規則新增的標籤相符，您的規則動作不得終止 Web ACL 對 Web 要求的評估。規則動作必須設定為CountCAPTCHA、或Challenge。當 Web ACL 評估未終止時，Web ACL 中的後續規則可以針對請求執行其標籤比對準則。如需規則動作的詳細資訊，請參閱 規則動作。

在 Web ACL 評估期間存取標籤

新增之後，只要針對 Web ACL 評估請求，標籤仍可用於請求。 AWS WAF Web ACL 中的任何規則都可以存取已在相同 Web ACL 中執行的規則加入的標示。這包括直接在 Web ACL 內定義的規則，以及在 Web ACL 中使用的規則群組內定義的規則。

- 您可以使用 label match 陳述式來比對規則請求檢查條件中的標籤。您可以比對附加至要求的任何標籤。如需陳述式詳細資訊，請參閱 標籤比對規則陳述式
- 地理匹配語句添加了帶有或不匹配的標籤，但只有在語句的包含 Web ACL 規則完成請求評估後才可用。
  - 您不能使用單一規則 (例如邏輯AND陳述式) 來執行 geo match 陳述式，後面接著針對地理標籤的 label match 陳述式。您必須將 label match 陳述式置於在包含 geo match 陳述式的規則之後執行的個別規則中。
  - 如果您在以速率為基礎的規則陳述式或受管規則群組參考陳述式中使用 geo match 陳述式做為範圍向下陳述式，則 geo match 陳述式新增的標籤無法透過包含規則的陳述式進行檢查。如果您需要檢查以速率為基礎的規則陳述式或規則群組中的地理標籤，則必須在事先執行的個別規則中執行 geo match 陳述式。

在 Web ACL 評估之外存取標籤資訊

Web ACL 評估結束後，標籤不會保留在 Web 要求中，但會在 AWS WAF 記錄檔和指標中記錄標籤資訊。

- AWS WAF 在任何單一請求上存放前 100 個標籤的 Amazon CloudWatch 指標。如需有關存取標籤指標的資訊，請參閱使用 Amazon 監控 CloudWatch和標示量度和維度。
- AWS WAF 在 AWS WAF 主控台中摘要 Web ACL 流量概觀儀表板中的 CloudWatch 標籤度量。您可以存取任何 Web ACL 頁面上的儀表板。如需詳細資訊，請參閱 網頁 ACL 流量概觀儀表板。
- AWS WAF 在記錄檔中記錄要求前 100 個標籤的標籤。您可以使用標籤和規則動作來篩選記錄的記 AWS WAF 錄檔。如需相關資訊，請參閱記錄 AWS WAF 網頁 ACL 流量。

您的 Web ACL 評估可以將 100 多個標籤套用至 Web 請求，並與 100 多個標籤進行比對，但 AWS WAF 只會在記錄檔和指標中記錄前 100 個標籤。

AWS WAF 標籤語法和命名需求

標籤是由前綴，可選命名空間和名稱組成的字符串。標籤的組件用冒號分隔。標籤具有以下要求和特點：

- 標籤區分大小寫。
- 每個標籤命名空間或標籤名稱最多可包含 128 個字元。
- 您最多可以在標籤中指定五個命名空間。
- 標籤的組件由冒號（：）分隔。
- 您無法在為標籤指定的命名空間或名稱中使用下列保留字串：awswafawswaf、rulegroup、webacl、、regexpatternsetipset、和managed。

標籤語法

完整標籤具有前置詞、可選命名空間和標籤名稱。字首可識別新增標籤之規則的規則群組或 Web ACL 內容。命名空間可用於為標籤添加更多上下文。標示名稱提供標示的最低詳細等級。它通常指出將標籤添加到請求的特定規則。

標示字首會根據其原點而有所不同。

- 您的標籤 — 以下內容顯示您在 Web ACL 和規則群組規則中建立的標籤的完整標籤語法。實體類型為rulegroup和webacl。

```
awswaf:<entity owner account id>:<entity type>:<entity name>:<custom
 namespace>:...:<label name>
```

  - 標籤命名空間前綴：awswaf:<entity owner account id>:<entity type>:<entity name>:
  - 自訂命名空間新增：<custom namespace>:…:

  當您在規則群組或 Web ACL 中定義規則的標籤時，您可以控制自訂命名空間字串和標籤名稱。其餘的是由您生成的 AWS WAF。 AWS WAF 自動為所有標籤加上帳戶awswaf和 Web ACL 或規則群組實體設定的前置字元。
- 受管規則群組標籤 — 下列內容顯示由受管規則群組中規則所建立之標籤的完整標籤語法。

```
awswaf:managed:<vendor>:<rule group name>:<custom namespace>:...:<label name>
```

- 標籤命名空間前綴：awswaf:managed:<vendor>:<rule group name>:
- 自訂命名空間新增：<custom namespace>:…:

所有 AWS 受管規則規則群組都會新增標籤。如需受管規則群組的相關資訊，請參閱 受管規則群組。

- 來自其他 AWS 處理序的標籤 — 這些程序會由 AWS Managed Rules 規則群組使用，因此您可以看到這些程序新增至您使用受管規則群組評估的 Web 要求中。以下顯示由受管規則群組呼叫的處理程序所建立之標籤的完整標籤語法。

```
awswaf:managed:<process>:<custom namespace>:...:<label name>
```

- 標籤命名空間前綴：awswaf:managed:<process>:
- 自訂命名空間新增：<custom namespace>:…:

此類型的標籤會針對呼叫 AWS 程序的受管規則群組列出。如需受管規則群組的相關資訊，請參閱 受管規則群組。

標示規則的範例

下列範例標籤是由屬於帳戶 111122223333 testRules 的規則群組中的規則所定義。

```
awswaf:111122223333:rulegroup:testRules:testNS1:testNS2:LabelNameA
```

```
awswaf:111122223333:rulegroup:testRules:testNS1:LabelNameQ
```

```
awswaf:111122223333:rulegroup:testRules:LabelNameZ
```

下列清單顯示 JSON 中的範例標籤規格。這些標籤名稱在結尾標籤名稱之前包括自訂命名空間字串。

```
Rule: {
    Name: "label_rule",
    Statement: {...}
    RuleLabels: [
        Name: "header:encoding:utf8",
        Name: "header:user_agent:firefox"
    ],
    Action: { Count: {} }
```

```
}
```

> **Note**
>
> 您可以透過規則 JSON 編輯器在主控台中存取此類型的清單。

如果您在與上述標籤範例相同的規則群組和帳戶中執行前述規則，則產生的完全合格標籤將如下所示：

```
awswaf:111122223333:rulegroup:testRules:header:encoding:utf8
```

```
awswaf:111122223333:rulegroup:testRules:header:user_agent:firefox
```

受管規則群組的標籤範例

以下顯示來自 AWS 受管規則規則群組及其所呼叫之程序的範例標籤。

```
awswaf:managed:aws:core-rule-set:NoUserAgent_Header
```

```
awswaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments
```

```
awswaf:managed:aws:atp:aggregate:attribute:compromised_credentials
```

```
awswaf:managed:token:accepted
```

AWS WAF 加入標示的規則

在幾乎所有規則中，您都可以定義標籤，並 AWS WAF 將其應用於任何匹配的請求。

下列規則類型是唯一的例外：

- 速率型規則僅在速率限制時標籤 — 以速率為基礎的規則只會在特定彙總執行個體的 Web 要求中新增標籤，而該執行個體受速率限制。 AWS WAF如需以比率為基礎的規則的資訊，請參閱速率型規則陳述式。
- 規則群組參考陳述式中不允許標記 — 主控台不接受這些規則類型的標籤。透過 API，指定任一陳述式類型的標籤都會導致驗證例外狀況。如需有關這些陳述式類型的資訊，請參閱管理規則群組陳述式和規則群組陳述式。

WCU — 您在 Web ACL 或規則群組規則中每定義 5 個標籤的 1 個 WCU。

哪裡可以找到此項

- 主控台上的規則產生器 — 在規則的 [動作] 設定下的 [標籤] 下方。
- API 資料類型 — `Rule RuleLabels`

您可以透過指定要附加至標籤命名空間前置詞的自訂命名空間字串和名稱，在規則中定義標籤。 AWS WAF 從您在其中定義規則的前後關聯衍生字首。如需相關資訊，請參閱下的標籤語法資訊AWS WAF 標籤語法和命名需求。

AWS WAF 符合標籤的規則

您可以使用標籤比對陳述式來評估網頁要求標籤。您可以匹配需要標籤名稱的 Label，或與需要命名空間規格的命名空間進行匹配。對於 label 或命名空間，您可以選擇性地在規格中包含前面的命名空間和前置詞。如需有關此陳述式類型的一般資訊，請參閱標籤比對規則陳述式。

標籤的前置詞定義了規則群組或定義標籤規則的 Web ACL 的前後關聯。在規則的 label match 語句中，如果您的標籤或命名空間匹配字符串未指定前綴，則 AWS WAF 使用標籤匹配規則的前綴。

- 直接在 Web ACL 內定義的規則的標示具有指定 Web ACL 環境定義的字首。
- 規則群組內規則的標籤具有指定規則群組前後關聯的前置詞。這可能是您自己的規則群組或為您管理的規則群組。

如需相關資訊，請參閱下的標籤語法AWS WAF 標籤語法和命名需求。

> **Note**
>
> 某些受管規則群組會新增標籤。您可以通過調用 API 來檢索這些內容`DescribeManagedRuleGroup`。標示會在回應中列示在`AvailableLabels`性質中。

如果您想要比對位於與規則上下文不同的前後關聯中的規則，則必須在比對字串中提供前置詞。例如，如果您想要比對受管理規則群組中規則所新增的標籤，您可以在 Web ACL 中新增規則，其符合字串會指定規則群組的前置字元，後面接著您的其他符合條件。

在 label match 語句的匹配字符串中，您可以指定標籤或命名空間：

- 標籤 (Label) — 相符項目的標籤規格由標籤的結尾部分組成。您可以包含任意數量的連續命名空間，這些命名空間緊接在標籤名稱之前，後跟名稱。您也可以透過以字首開始規格來提供完全合格的標籤。

  規格範例：

  - `testNS1:testNS2:LabelNameA`
  - `awswaf:managed:aws:managed-rule-set:testNS1:testNS2:LabelNameA`
- 命名空間 — 相符項目的命名空間規格由不包括名稱之標籤規格的任何連續子集組成。您可以包含前置詞，並且可以包含一或多個命名空間字串。

  規格範例：

  - `testNS1:testNS2:`
  - `awswaf:managed:aws:managed-rule-set:testNS1:`

AWS WAF 標籤相符範例

本節提供標籤比對規則陳述式的比對規格範例。

> **Note**
>
> 這些 JSON 清單是在主控台中建立的，方法是在具有標籤比對規格的 Web ACL 中新增規則，然後編輯規則並切換至規則 JSON 編輯器。您也可以透過 API 或命令列介面取得規則群組或 Web ACL 的 JSON。

主題

- 符合本機標籤
- 匹配來自另一個上下文的標籤
- 比對受管規則群組標籤
- 匹配本地命名空間
- 符合受管規則群組命名空間

符合本機標籤

下列 JSON 清單會在與此規則相同的內容中，針對已在本機新增至 Web 要求的標籤顯示標籤比對陳述式。

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

如果您在帳戶 111122223333 中使用此比對陳述式，在您為網頁 ACL 定義的規則中testWebACL，它會符合下列標籤。

```
awswaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

```
awswaf:111122223333:webacl:testWebACL:testNS1:testNS2:header:encoding:utf8
```

它不匹配以下標籤，因為標籤字符串不是完全匹配。

```
awswaf:111122223333:webacl:testWebACL:header:encoding2:utf8
```

它不匹配以下標籤，因為上下文不相同，所以前綴不匹配。即使您已productionRules將規則群組新增至定義規則的 Web ACLtestWebACL，也是如此。

```
awswaf:111122223333:rulegroup:productionRules:header:encoding:utf8
```

匹配來自另一個上下文的標籤

下列 JSON 清單顯示標籤比對規則，該規則與使用者建立規則群組內的規則中的標籤相符。在 Web ACL 中執行且不屬於具名規則群組一部分的所有規則，規格中都需要前置字元。此範例標籤規格僅符合確切的標籤。

```
Rule: {
    Name: "match_rule",
    Statement: {
```

```
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "awswaf:111122223333:rulegroup:testRules:header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

比對受管規則群組標籤

這是比對來自另一個前後關聯而不是比對規則的標籤的特殊情況。下列 JSON 清單顯示受管規則群組標籤的標籤比對陳述式。這只匹配在 label match 語句的密鑰設置中指定的確切標籤。

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "awswaf:managed:aws:managed-rule-set:header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

匹配本地命名空間

下列 JSON 清單會顯示本機命名空間的標籤比對陳述式。

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "NAMESPACE",
            Key: "header:encoding:"
        }
    },
```

```
    Labels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

與本機相Label符項目類似，如果您在帳戶 111122223333 中使用此陳述式，在您為 Web ACL 定義的規則中testWebACL，它會符合下列標籤。

```
awswaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

它不匹配以下標籤，因為帳戶不相同，因此前綴不匹配。

```
awswaf:444455556666:webacl:testWebACL:header:encoding:utf8
```

前置詞也不符合受管規則群組套用的任何標籤，如下所示。

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

符合受管規則群組命名空間

下列 JSON 清單顯示受管規則群組命名空間的標籤比對陳述式。對於您擁有的規則群組，您也必須提供前置詞，才能符合規則內容之外的命名空間。

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "NAMESPACE",
            Key: "awswaf:managed:aws:managed-rule-set:header:"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

此規格與下列範例標籤相符。

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

```
awswaf:managed:aws:managed-rule-set:header:encoding:unicode
```

它不匹配以下標籤。

```
awswaf:managed:aws:managed-rule-set:query:badstring
```

AWS WAF 智慧型威脅緩解

本節涵蓋由提供的受管理智慧型威脅緩和功能 AWS WAF。這些是先進的專業保護，您可以實施這些保護措施，以防止惡意漫遊器和帳戶接管嘗試等威脅。

> **Note**
>
> 此處描述的功能會產生額外費用，而不是使用基本費用 AWS WAF。如需詳細資訊，請參閱 AWS WAF 定價。

本節提供的指引適用於一般知道如何建立和管理 AWS WAF Web ACL、規則和規則群組的使用者。這些主題涵蓋在本指南之前的章節中。

主題

- 智慧型威脅緩解選項
- 智慧型威脅緩解的最佳做法
- AWS WAF 網絡請求令牌
- AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）
- AWS WAF 防止欺詐控制帳戶接管（ATP）
- AWS WAF 機器人控制
- AWS WAF 用戶端應用整合
- CAPTCHA並Challenge在 AWS WAF

智慧型威脅緩解選項

本節提供實作智慧型威脅緩和措施的選項的詳細比較。

AWS WAF 針對智慧型威脅緩解提供下列類型的保護。

- AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）— 在應用程序的註冊頁面上檢測和管理惡意帳戶創建嘗試。核心功能由 ACFP 管理規則群組提供。如需詳細資訊，請參閱 AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP） 及 AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）規則組。
- AWS WAF 防止詐騙控制帳戶接管 (ATP) — 偵測並管理應用程式登入頁面上的惡意接管嘗試。核心功能由可承諾量管理規則群組提供。如需詳細資訊，請參閱 AWS WAF 防止欺詐控制帳戶接管（ATP） 及 AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組。
- AWS WAF 機器人控制 — 識別、標記和管理友善和惡意機器人。此功能可為具有跨應用程式唯一簽章的通用機器人提供管理功能，以及具有應用程式特定簽章的目標機器人。核心功能由機器人控制受管規則群組提供。如需詳細資訊，請參閱 AWS WAF 機器人控制 及 AWS WAF 機器人控制規則群組。
- 用戶端應用程式整合 SDK — 驗證網頁上的用戶端工作階段和最終使用者，並取得 AWS WAF 權杖供用戶端在其 Web 請求中使用。如果您使用 ACFP、ATP 或機器人控制，請在用戶端應用程式中實作應用程式整合 SDK，以充分利用所有規則群組功能。只有在需要快速保護關鍵資源且沒有足夠時間進行 SDK 整合時，我們才建議使用這些規則群組而不進行 SDK 整合作為臨時措施。如需實作 SDK 的相關資訊，請參閱AWS WAF 用戶端應用整合。
- Challenge和CAPTCHA規則動作 — 驗證用戶端工作階段和使用者，並取得 AWS WAF 權杖，以供用戶端在其 Web 請求中使用。您可以在您指定規則動作的任何位置、在規則中以及您使用的規則群組中的覆寫項目來實作這些功能。這些動作會使用 AWS WAF JavaScript 插入式物件來詢問用戶端或使用者，而且需要支援的用戶端應用程式。 JavaScript如需詳細資訊，請參閱 CAPTCHA並Challenge在 AWS WAF。

智慧型威脅緩解 AWS 受管規則會將 ACFP、ATP 和機器人控制使用 Token 進行進階偵測。如需有關權杖在規則群組中啟用之功能的資訊為什麼您應該將應用程式整合 SDK 與 ACFP 搭配使用，請參閱為什麼您應該將應用程式整合 SDK 與 ATP 搭配使用、和為什麼您應該使用應用程式整合 SDK 搭配機器人控制。

您可以選擇實作智慧型威脅緩和措施，包括執行挑戰和強制 Token 取得的基本規則動作，到智慧型威脅緩和 AWS Managed Rules 規則群組所提供的進階功能。

下表提供基本和進階功能之選項的詳細比較。

主題

- 挑戰和代幣獲取的選擇
- 智慧型威脅緩和受管規則群組的選項

- 以速率為基礎的規則和目標機器人控制規則中的速率限制選項

挑戰和代幣獲取的選擇

您可以使用應用 AWS WAF 程式整合 SDK 或規則動作Challenge和CAPTCHA. 從廣義上講，規則操作更易於實施，但會產生額外的成本，更多地侵入客戶體驗和需求。 JavaScriptSDK 需要在客戶端應用程序中進行編程，但它們可以提供更好的客戶體驗，可以免費使用，並且可以與 Android JavaScript 或 iOS 應用程序一起使用。您只能將應用程式整合 SDK 與 Web ACL 搭配使用其中一個付費智慧型威脅緩和管理規則群組 (如下節所述)。

挑戰和代幣獲取的選項比較

	Challenge 規則動作	CAPTCHA 規則動作	JavaScript SDK 的挑戰	移動 SDK 的挑戰
它是什麼	通過向瀏覽器客戶端顯示插頁式挑戰來強制獲取 AWS WAF 令牌的規則操作	通過向客戶端最終用戶插頁式提出視覺或音頻挑戰來強制獲取 AWS WAF 令牌的規則操作	應用程序集成層，用於客戶端瀏覽器和其他執行的設備JavaScript。呈現無聲挑戰並獲得令牌	應用程序集成層，適用於安卓和 iOS 應用程序。本地呈現了沉默的挑戰並獲得令牌
不錯的選擇...	針對機器人工作階段進行無訊息驗證，並為支援的用戶端強制執行 JavaScript	針對支援的用戶端，針對機器人工作階段進行最終使用者和靜默驗證，以及強制執行 JavaScript	針對機器人工作階段進行無訊息驗證，並為支援JavaScript的用戶端強制執行權杖 SDK 提供最低的延遲和最佳控制挑戰指令碼在應用程式中執行的位置。	針對 Android 和 iOS 上的原生移動應用程序對機器人會話進行靜默驗證，並強制執行令牌獲取。 SDK 提供最低的延遲和最佳控制挑戰指令碼在應用程式中執行的位置。
實作考量	實作為規則動作設定	實作為規則動作設定	需要 Web ACL 中的其中一個 ACFP、可承諾量	需要 Web ACL 中的其中一個 ACFP、可承諾量

	Challenge 規則動作	CAPTCHA 規則動作	JavaScript SDK 的挑戰	移動 SDK 的挑戰
			或機器人控制付費規則群組。 需要在客戶端應用程序編碼。	或機器人控制付費規則群組。 需要在客戶端應用程序編碼。
運行時考量	沒有有效令牌的請求的侵入性流程。用戶端會重新導向至插頁式 AWS WAF 挑戰。添加網絡往返，並需要對 Web 請求進行第二次評估。	沒有有效令牌的請求的侵入性流程。客戶端被重定向到插頁式 AWS WAF 驗證碼。添加網絡往返，並需要對 Web 請求進行第二次評估。	可以在幕後運行。讓您更好地控制挑戰體驗。	可以在幕後運行。讓您更好地控制挑戰體驗。
需要 JavaScript	是	是	是	否
支援的用戶端	執行指令碼的瀏覽器和裝置	執行指令碼的瀏覽器和裝置	執行指令碼的瀏覽器和裝置	安卓及 iOS 裝置
支援單一頁面應用程式 (SPA)	僅限執行。 您可以將此Challenge動作與 SDK 結合使用，以確保要求具有有效的挑戰權杖。您無法使用規則動作將挑戰指令碼傳送至頁面。	僅限執行。 您可以將該CAPTCHA操作與 SDK 一起使用，以確保請求具有有效的 CAPTCHA 令牌。您無法使用規則動作將 CAPTCHA 指令碼傳送至頁面。	是	N/A

	Challenge 規則動作	CAPTCHA 規則動作	JavaScript SDK 的挑戰	移動 SDK 的挑戰
額外費用	是，針對您在定義的規則中明確指定的動作設定，或在您使用的規則群組中作為規則動作覆寫。在所有其他情況下都沒有。	是，針對您在定義的規則中明確指定的動作設定，或在您使用的規則群組中作為規則動作覆寫。在所有其他情況下都沒有。	否，但需要其中一個付費規則群組 ACFP、ATP 或機器人控制。	否，但需要其中一個付費規則群組 ACFP、ATP 或機器人控制。

如需有關這些選項相關成本的詳細資訊，請參閱定AWS WAF 價中的智慧型威脅緩解資訊。

只需添加一個Challenge或操作的規則，就可以更簡單地運行挑戰並提供基本的令牌強制執CAPTCHA行。您可能需要使用規則動作，例如，如果您無法存取應用程式程式碼。

但是，如果您可以實施 SDK，則與使用以下Challenge操作相比，您可以節省成本並減少客戶端 Web 請求的 Web ACL 評估延遲：

- 您可以編寫 SDK 實施以在應用程序中的任何時候運行挑戰。您可以在執行將 Web 請求發送到受保護資源的任何客戶操作之前，在後台獲取令牌。這樣，令牌可以與客戶的第一個請求一起發送。
- 如果您透過使用Challenge動作實作規則來取得 Token，則在用戶端第一次傳送請求和 Token 到期時，規則和動作需要額外的 Web 要求評估和處理。該Challenge操作會阻止沒有有效，未過期令牌的請求，並將挑戰插頁式發送回客戶端。用戶端成功回應挑戰之後，插頁式會使用有效權杖重新傳送原始 Web 要求，然後由 Web ACL 第二次評估。

智慧型威脅緩和受管規則群組的選項

智慧型威脅緩和 AWS Managed Rules 規則群組可提供基本機器人的管理、複雜惡意機器人的偵測和緩解、帳戶接管嘗試的偵測和緩解，以及詐騙帳戶建立嘗試的偵測與緩解。這些規則群組結合上一節所述的應用程式整合 SDK，可提供最先進的保護，並與您的用戶端應用程式安全耦合。

受管規則群組選項的比較

	ACFP	ATP	機器人控制共同層級	機器人控制目標層級
它是什麼	管理可能是應用程式註冊和註冊頁面上詐騙帳戶建立嘗試的一部分的請求。 不管理機器人。 請參閱AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）規則組。	管理可能是應用程式登入頁面上惡意接管嘗試一部分的要求。 不管理機器人。 請參閱AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組。	使用跨應用程式唯一的簽章來管理可自我識別的常見機器人。 請參閱AWS WAF 機器人控制規則群組。	使用特定於應用程式的簽章來管理無法自我識別的目標機器人。 請參閱AWS WAF 機器人控制規則群組。
不錯的選擇...	檢查帳戶創建流量是否存在欺詐性帳戶創建攻擊，例如通過用戶名遍歷創建嘗試以及從單個 IP 地址創建許多新帳戶。	檢查登錄流量是否存在帳戶接管攻擊，例如使用密碼遍歷登錄嘗試以及來自同一 IP 地址的多次登錄嘗試。與 Token 搭配使用時，還會提供彙總保護，例如 IP 的速率限制和用戶端工作階段，以防大量失敗的登入嘗試。	基本的機器人保護和標記常見的自動化機器人流量。	針對複雜的漫遊器進行有針對性的保護，包括用戶端工作階段層級的速率限制，以及 Selenium 和 Puppeteer 等瀏覽器自動化工具的偵測和緩解。
加入指示評估結果的標籤	是	是	是	是
添加令牌標籤	是	是	是	是

	ACFP	ATP	機器人控制共同層級	機器人控制目標層級
阻止沒有有效令牌的請求	不包括在內。 請參閱阻止沒有有效 AWS WAF 令牌的請求。	不包括在內。 請參閱阻止沒有有效 AWS WAF 令牌的請求。	不包括在內。 請參閱阻止沒有有效 AWS WAF 令牌的請求。	封鎖傳送 5 個不使用權杖的要求的用戶端工作階段。
需要令 AWS WAF 牌 `aws-waf-token`	所有規則都需要。 請參閱為什麼您應該將應用程式整合 SDK 與 ACFP 搭配使用。	許多規則都需要。 請參閱為什麼您應該將應用程式整合 SDK 與 ATP 搭配使用。	否	是
獲取令牌 AWS WAF `aws-waf-token`	是，由規則強制執行 `AllRequests`	否	否	一些規則使用 Challenge或規 CAPTCHA則操作，它們獲取令牌。

如需與這些選項相關的成本詳細資訊，請參閱定AWS WAF 價中的智慧型威脅緩解資訊。

以速率為基礎的規則和目標機器人控制規則中的速率限制選項

AWS WAF Bot Control 規則群組的目標層級和以速 AWS WAF 率為基礎的規則陳述式都提供 Web 要求速率限制。下表比較兩個選項。

以速率為基礎的偵測和緩解措施的選項比較

	AWS WAF 以速率為基礎的	AWS WAF 機器人控制目標規則	
如何套用速率限制	對那些以太高的速率來的請求組的行為。	透過使用要求權杖，強制執行類似人類的	

	AWS WAF 以速率為基礎的	AWS WAF 機器人控制目標規則	
	您可以套用除以外的任何動作Allow。	存取模式，並套用動態速率限制。	
根據歷史流量基準？	否	是	
累積歷史流量基準所需的時間	N/A	五分鐘的動態閾值。不存在令牌的 N/A。	
緩解滯後	通常是 30 至 50 秒。最多可能需要幾分鐘。	通常不到 10 秒。最多可能需要幾分鐘。	
緩解目標	可配置。您可以使用範圍向下陳述式以及一或多個彙總索引鍵 (例如 IP 位址、HTTP 方法和查詢字串) 來分組請求。	IP 位址和用戶端工作階段	
觸發緩和措施所需的流量層級	中-在指定時間範圍內最低可達 100 個請求	低-用於檢測客戶端模式，例如慢速刮刀	
可自訂閾值	是	否	
預設緩解動作	主控台預設值為Block。API 中沒有預設設定；此設定為必要項目。 您可以將其設定為除外的任何規則動作Allow。	規則群組規則動作設定適用Challenge於不存在 Token 以及CAPTCHA來自單一用戶端工作階段的大量流量。 您可以將這些規則設定為任何有效的規則動作。	

	AWS WAF 以速率為基礎的	AWS WAF 機器人控制目標規則	
針對高度分散式攻擊的彈性	中-IP 位址本身限制的 IP 位址上限為 10,000 個	中-IP 地址和令牌之間的總數限制為 50,000	
AWS WAF 定價	已包含在的標準費用中 AWS WAF。	已包含在 Bot Control 智慧型威脅緩解目標層級的費用中。	
欲了解更多信息	速率型規則陳述式	AWS WAF 機器人控制規則群組	

智慧型威脅緩解的最佳做法

請遵循本節中的最佳做法，以最有效率且符合成本效益的智慧型威脅緩解功能實作。

- 實作 JavaScript 和行動應用程式整合 SDK — 實作應用程式整合，以最有效的方式啟用完整的 ACFP、ATP 或機器人控制功能。受管規則群組使用 SDK 提供的 Token，在工作階段層級將合法用戶端流量與不需要的流量分開。應用程序集成 SDK 可確保這些令牌始終可用。如需詳細資訊，請參閱以下：
  - 為什麼您應該將應用程式整合 SDK 與 ACFP 搭配使用
  - 為什麼您應該將應用程式整合 SDK 與 ATP 搭配使用
  - 為什麼您應該使用應用程式整合 SDK 搭配機器人控制

  使用這些集成來實現客戶端中的挑戰，並為 JavaScript自定義 CAPTCHA 難題向最終用戶呈現的方式。如需詳細資訊，請參閱 AWS WAF 用戶端應用整合。

  如果您使用 JavaScript API 自定義 CAPTCHA 難題，並在 Web ACL 中的任何位置使用CAPTCHA 規則操作，請按照在客戶端中處理 AWS WAF CAPTCHA 響應的指導處理來自的驗證碼響應 AWS WAF。本指引適用於任何使用此CAPTCHA動作的規則，包括 ACFP 受管規則群組中的規則，以及 Bot Control 受管規則群組的目標保護層級。
- 限制您傳送至 ACFP、ATP 和機器人控制規則群組的要求 — 使用智慧型威脅緩和 AWS 管理規則群組會產生額外費用。ACFP 規則群組會檢查對您指定之帳號註冊和建立端點的要求。可承諾量規則群組會向您指定的登入端點檢查請求。機器人控制規則群組會檢查在 Web ACL 評估中達到的每個要求。

請考慮下列方法來減少使用這些規則群組：

- 使用受管規則群組陳述式中的範圍向下陳述式，從檢查中排除要求。你可以用任何嵌套的語句來做到這一點。如需相關資訊，請參閱範圍向下語句。
- 在規則群組之前新增規則，從檢查中排除要求。對於無法在範圍下語句中使用的規則，以及對於更複雜的情況（例如標籤後跟標籤匹配），您可能需要添加在規則群組之前執行的規則。如需詳細資訊，請參閱 範圍向下語句 及 規則陳述式基礎。
- 在較便宜的規則之後執行規則群組。如果您有其他標準 AWS WAF 規則基於任何原因封鎖要求，請在這些付費規則群組之前執行這些規則。如需規則和規則管理的詳細資訊，請參閱規則陳述式基礎。
- 如果您使用其中一個以上的智慧型威脅緩和受管理規則群組，請依下列順序執行這些群組，以降低成本：機器人控制、ATP、ACFP。

如需更多定價的詳細資訊，請參閱 AWS WAF 定價。

- 在一般網路流量期間啟用 Bot Control 規則群組的目標防護層級 — 目標防護層級的某些規則需要時間為一般流量模式建立基準，才能辨識並回應不規則或惡意的流量模式。例如，`TGT_ML_*`規則最多需要 24 小時才能預熱。

  當您沒有遭受攻擊時，請新增這些保護，並讓他們有時間建立基準，然後再預期它們能夠適當地回應攻擊。如果您在攻擊期間新增這些規則，則在攻擊消退後，建立基準的時間通常是正常所需時間的兩倍到三倍，因為攻擊流量增加了偏斜。如需有關規則及其所需預熱時間的其他資訊，請參閱。上市規則

- 對於分佈式拒絕服務（DDoS）保護，請使用 Shield 高級自動應用程序層 DDoS 緩解-智能威脅緩解規則組不提供 DDoS 保護。ACFP 可防止對應用程序的註冊頁面進行欺詐性帳戶創建嘗試。ATP 可防止帳戶接管您的登入頁面。Bot Control 著重於使用權杖強制類似人類的存取模式，以及用戶端工作階段的動態速率限制。

  當您在啟用自動應用程式層 DDoS 緩解的情況下使用 Shield Advanced 時，Shield Advanced 會代表您建立、評估和部署自訂 AWS WAF 緩和措施，自動回應偵測到的 DDoS 攻擊。如需有關「Shield 進階」的更多資訊，請參閱AWS Shield Advanced 概述、和AWS Shield Advanced 應用程式層 (第 7 層) 保護。

- 調整和配置令牌處理 — 調整 Web ACL 的令牌處理以獲得最佳的用戶體驗。
  - 為了降低運營成本並改善最終用戶的體驗，請將令牌管理免疫時間調整為安全要求允許的最長時間。這使 CAPTCHA 難題和無聲挑戰的使用降至最低。如需相關資訊，請參閱時間戳記到期：AWS WAF 權杖豁免時間。

  - 若要在受保護的應用程式之間啟用權杖共用，請為您的 Web ACL 設定 Token 網域清單。如需相關資訊，請參閱AWS WAF 權杖網域和網域清單。
- 拒絕具有任意主機規格的請求 — 將受保護的資源配置為要求 Web 請求中的`Host`標頭與目標資源匹配。您可以接受一個值或一組特定的值，例如`myExampleHost.com`和`www.myExampleHost.com`，但不接受主機的任意值。
- 對於作為發佈起源的應用程式負載平衡器，請設定 CloudFront 並進 CloudFront 行 AWS WAF 適當的 Token 處理 — 如果您將 Web ACL 與 Application Load B alancer 產生關聯，並將 Application Load Balancer 部署為 CloudFront 發佈的來源，請參閱來源的應用程式負載平衡器所需的組態 CloudFront 。
- 在部署之前進行測試和調整 — 在您對 Web ACL 實作任何變更之前，請遵循本指南中的測試和調整程序，以確保您獲得預期的行為。這對於這些付費功能尤為重要。如需一般指引，請參閱測試和調整您的 AWS WAF 保護。如需付費受管規則群組的特定資訊測試和部署 ACFP，請參閱測試和部署可承諾量、和測試和部署 AWS WAF 機器人控制。

AWS WAF 網絡請求令牌

AWS WAF 代幣是 AWS WAF 智慧型威脅緩解所提供的增強型防護不可或缺的一部分。Token，有時稱為指紋，是用戶端儲存並提供每個 Web 要求傳送的單一用戶端工作階段的相關資訊集合。 AWS WAF 使用 Token 來識別惡意用戶端工作階段，並將其與合法工作階段分開，即使兩者都來自單一 IP 位址也是如此。對於合法用戶而言，令牌使用可以忽略不計的成本，但對於殭屍網絡來說，大規模昂貴。

AWS WAF 使用 Token 來支援其瀏覽器和終端使用者挑戰功能，這些功能由應用程式整合 SDK 和規則動作`Challenge`和`CAPTCHA`提供。此外，Token 還可啟用 AWS WAF Bot Control 和帳戶接管防止受管規則群組的功能。

AWS WAF 為成功響應無聲挑戰和 CAPTCHA 難題的客戶創建，更新和加密令牌。當具有令牌的客戶端發送 Web 請求時，它會包含加密令牌，並 AWS WAF 解密令牌並驗證其內容。

主題

- 如何 AWS WAF 使用令牌
- AWS WAF 令牌特徵
- 時間戳記到期： AWS WAF 權杖豁免時間
- AWS WAF 權杖網域和網域清單
- AWS WAF 機器人和欺詐管理規則群組的權杖標籤

- 阻止沒有有效 AWS WAF 令牌的請求
- 來源的應用程式負載平衡器所需的組態 CloudFront

如何 AWS WAF 使用令牌

AWS WAF 使用令牌記錄和驗證以下類型的客戶端會話驗證：

- 驗證碼 — 驗證碼拼圖有助於區分機器人與人類用戶。驗證碼只能由CAPTCHA規則動作執行。成功完成拼圖後，CAPTCHA 腳本將更新令牌的 CAPTCHA 時間戳。如需詳細資訊，請參閱 CAPTCHA並Challenge在 AWS WAF。
- 挑戰 — 挑戰會以無訊息方式執行，以協助區分常規用戶端工作階段與機器人工作階段，並使機器人的運作成本更高。當挑戰成功完成時，挑戰腳本會根據需要自動從中 AWS WAF 採購新令牌，然後更新令牌的挑戰時間戳記。

  AWS WAF 在下列情況下會遇到挑戰：

  - 應用程式整合 SDK — 應用程式整合 SDK 會在用戶端應用程式工作階段內執行，協助確保只有在用戶端成功回應挑戰後，才允許登入嘗試。如需詳細資訊，請參閱 AWS WAF 用戶端應用整合。
  - Challenge規則動作 — 如需詳細資訊，請參閱CAPTCHA並Challenge在 AWS WAF。
  - CAPTCHA— 當 CAPTCHA 插頁式運行時，如果客戶端還沒有令牌，則腳本會先自動運行一個挑戰，以驗證客戶端會話並初始化令牌。

智慧型威脅 AWS 受管規則群組中的許多規則都需要 Token。這些規則會使用 Token 來執行諸如區分工作階段層級的用戶端、判斷瀏覽器特性，以及瞭解應用程式網頁上人工互動的層級等。這些規則群組會叫用 AWS WAF 權杖管理，以套用規則群組接著檢查的權杖標籤。

- AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）— ACFP 規則要求具有有效令牌的 Web 請求。若要取得有關規則的更多資訊，請參閱AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）規則組。
- AWS WAF 防止欺詐控制帳戶接管（ATP）— 防止大量和長期持續用戶端會話的 ATP 規則需要具有有效令牌且具有未過期挑戰時間戳的 Web 請求。如需詳細資訊，請參閱 AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組。
- AWS WAF 機器人控制 — 此規則組中的目標規則對客戶端在沒有有效令牌的情況下可以發送的 Web 請求數進行限制，並使用令牌會話跟踪進行會話級監視和管理。根據需要，這些規則會套用Challenge和規CAPTCHA則動作，以強制執行權杖擷取和有效的用戶端行為。如需更多詳細資訊，請參閱 AWS WAF 機器人控制規則群組。

AWS WAF 令牌特徵

每個令牌具有以下特徵：

- 權杖會儲存在名為的 Cookie 中`aws-waf-token`。
- 令牌已加密。
- 該令牌使用包含以下信息的粘性粒度標識符為客戶端會話指紋：
  - 用戶端最新成功回應無訊息挑戰的時間戳記。
  - 終端使用者最近一次成功回應 CAPTCHA 的時間戳記。僅當您在保護中使用 CAPTCHA 時，此功能才存在。
  - 有關用戶端和用戶端行為的其他資訊，可協助您將合法用戶端與不必要的流量分開。這些資訊包括可用於偵測自動化活動的各種用戶端識別碼和用戶端訊號。收集的信息是非唯一的，不能映射到個人。
    - 所有令牌都包括來自客戶端瀏覽器審訊的數據，例如自動化指示和瀏覽器設置不一致。此資訊是由Challenge動作執行的指令碼以及用戶端應用程式 SDK 所擷取。腳本主動詢問瀏覽器並將結果放入令牌中。
    - 此外，當您實作用戶端應用程式整合 SDK 時，Token 會包含被動收集的有關使用者與應用程式頁面互動的資訊。互動性包括滑鼠移動、按鍵，以及與頁面上存在的任何 HTML 表單的互動。此資訊有助於 AWS WAF 偵測用戶端中的人類互動程度，以挑戰似乎不是人類的使用者。如需用戶端整合的相關資訊，請參閱AWS WAF 用戶端應用整合。

出於安全原因， AWS 不提供令牌內容的完整描述或有關令牌加密過程的 AWS WAF 詳細信息。

時間戳記到期： AWS WAF 權杖豁免時間

AWS WAF 使用挑戰和 CAPTCHA 免疫時間來控制單個客戶端會話可以呈現挑戰或 CAPTCHA 的頻率。最終用戶成功響應 CAPTCHA 後，CAPTCHA 免疫時間決定了最終用戶無法提供另一個 CAPTCHA 的時間。同樣，挑戰免疫時間決定了客戶端會話在成功響應挑戰後再次免受挑戰的時間。

AWS WAF 通過更新令牌內的相應時間戳記，記錄對挑戰或 CAPTCHA 的成功響應。當 AWS WAF 檢查令牌是否存在挑戰或 CAPTCHA 時，它會從當前時間中減去時間戳。如果結果大於設定的免疫時間，則時間戳記已過期。

您可以在 Web ACL 以及任何使用CAPTCHA或Challenge規則動作的規則中設定挑戰和 CAPTCHA 免疫時間。

- 兩個免疫時間的預設 Web ACL 設定都是 300 秒。

- 您可以為使用CAPTCHA或Challenge動作的任何規則指定豁免時間。如果您未指定規則的豁免時間，它會繼承 Web ACL 中的設定。
- 對於使用CAPTCHA或Challenge動作的規則群組內的規則，如果您未指定規則的豁免時間，則會從您使用該規則群組的每個 Web ACL 繼承設定。
- 應用程序集成 SDK 使用 Web ACL 的挑戰免疫時間。

挑戰免疫時間的最小值為 300 秒。驗證碼免疫時間的最小值為 60 秒。兩個免疫時間的最大值為 259,200 秒或三天。

您可以使用 Web ACL 和規則層級豁免時間設定來調整CAPTCHA動作或 SDK 挑戰管理行為。Challenge例如，您可以設定規則以低免疫力時間控制對高度敏感資料的存取，然後在 Web ACL 中為其他規則和要繼承的 SDK 設定較高的免疫力時間。

特別是對於 CAPTCHA，解決難題會降低客戶的網站體驗，因此調整 CAPTCHA 免疫時間可以幫助您減輕對客戶體驗的影響，同時仍然可以提供所需的保護。

如需調整免疫時間以使用Challenge和CAPTCHA規則動作的其他資訊，請參閱使用和動作的最佳CAPTCHAChallenge作法。

在哪裡設置令 AWS WAF 牌免疫時間

您可以在 Web ACL 中以及使用和規則動作的規則中設定Challenge豁免時間。CAPTCHA

如需有關管理 Web ACL 及其規則的一般資訊，請參閱使用 Web ACL。

在哪裡設置網頁 ACL 的免疫時間

- 主控台 — 當您編輯 Web ACL 時，請在 [規則] 索引標籤中編輯和變更 [Web ACL 驗證碼組態] 和 [Web ACL 挑戰] 組態窗格中的設定。在主控台中，您只能在建立 Web ACL 之後設定 Web ACL 驗證碼和挑戰免疫時間。
- 在主控台外部 — Web ACL 資料類型具有 CAPTCHA 和挑戰組態參數，您可以設定這些參數並提供給 Web ACL 上的建立和更新作業。

在何處設定規則的豁免時間

- 主控台 — 建立或編輯規則並指定CAPTCHA或Challenge動作時，您可以修改規則的免疫時間設定。
- 在主控台外部 — 規則資料類型具有 CAPTCHA 和挑戰配置參數，您可以在定義規則時進行配置。

AWS WAF 權杖網域和網域清單

為客戶端 AWS WAF 創建令牌時，它會使用令牌域對其進行配置。當 AWS WAF 檢查 Web 請求中的令牌時，如果其域不匹配任何被認為對 Web ACL 有效的域，它將拒絕令牌作為無效。

默認情況下， AWS WAF 僅接受其域設置與 Web ACL 關聯的資源的主機域完全匹配的令牌。這是 Web 請求中`Host`標頭的值。在瀏覽器中，您可以在 JavaScript `window.location.hostname`屬性和用戶在其地址欄中看到的地址中找到此域。

您也可以在 Web ACL 組態中指定可接受的權杖網域，如下節所述。在這種情況下， AWS WAF 接受與主機標頭完全匹配以及與令牌域列表中的域匹配。

您可以指定在設定網域時 AWS WAF 以及在 Web ACL 中評估權杖時使用的權杖網域。您指定的域不能是公共後綴，例如。`gov.au`如需您無法使用的網域，請參閱 https://publicsuffix.org/list/public_suffix_list.dat「公開尾碼」清單下的清單。

AWS WAF 網絡 ACL 令牌域列表配置

您可以將 Web ACL 設定為在多個受保護資源之間共用權杖，方法是提供包含您要 AWS WAF 接受的其他網域的權杖網域清單。對於令牌域列表， AWS WAF 仍然接受資源的主機域。此外，它接受權杖網域清單中的所有網域，包括其前置字元的子網域。

例如，權杖網域清單`example.com`中的網域規格符合 `example.com` (自`http://example.com/`) `api.example.com`、(自`http://api.example.com/`) 和 `www.example.com` (從`http://www.example.com/`)。它不匹配`example.api.com`，（從`http://example.api.com/`）或`apiexample.com`（從`http://apiexample.com/`）。

您可以在建立或編輯 Web ACL 時設定權杖網域清單。如需有關管理 Web ACL 的一般資訊，請參閱使用 Web ACL。

AWS WAF 權杖網域設定

AWS WAF 根據挑戰指令碼的要求建立權杖，這些指令碼由應用程式整合 SDK 和Challenge和CAPTCHA規則動作執行。

在 Token 中 AWS WAF 設定的網域取決於要求它的挑戰指令碼類型，以及您提供的任何其他 Token 網域組態。 AWS WAF 將權杖中的網域設定為可在組態中找到的最短、最一般的設定。

- JavaScript SDK — 您可以使用權杖網域規格來設定 JavaScript SDK，其中可包含一或多個網域。根據受保護的主機網域和 Web ACL 的 Token 網域清單，您設定的網域必須是 AWS WAF 將接受的網域。

當為用戶端 AWS WAF 發出 Token 時，它會將 Token 網域設定為符合主機網域的一個，並且是從主機網域和已設定清單中的網域中最短的網域。例如，如果主機域是`api.example.com`並且令牌域列表具有`example.com`，則在令牌`example.com`中 AWS WAF 使用，因為它與主機域匹配並且較短。如果您未在 JavaScript API 配置中提供令牌域列表，請將該域 AWS WAF 設置為受保護資源的主機域。

如需詳細資訊，請參閱 提供在權杖中使用的網域。

- 行動 SDK — 在您的應用程式程式碼中，您必須使用權杖網域屬性來設定行動 SDK。根據受保護的主機網域和 Web ACL 的 Token 網域清單，此屬性必須是 AWS WAF 將接受的網域。

  當為用戶端 AWS WAF 發出 Token 時，它會使用此屬性做為 Token 網域。 AWS WAF 不會在為行動 SDK 用戶端發出的權杖中使用主機網域。

  如需詳細資訊，請參閱中的`WAFConfigurationdomainName`設定行 AWS WAF 動 SDK 規格。
- Challenge動作 — 如果您在 Web ACL 中指定權杖網域清單，則會將權杖網域 AWS WAF 設定為與主機網域相符的權杖網域，並且從主機網域和清單中的網域中最短。例如，如果主機域是`api.example.com`並且令牌域列表具有`example.com`，則在令牌`example.com`中 AWS WAF 使用，因為它與主機域匹配並且較短。如果您未在 Web ACL 中提供 Token 網域清單，請將網域 AWS WAF 設定為受保護資源的主機網域。

AWS WAF 機器人和欺詐管理規則群組的權杖標籤

本節說明權 AWS WAF 杖管理新增至 Web 要求的標籤。如需有關標示的一般資訊，請參閱AWS WAF 標籤, 上, 网, 請求。

當您使用任何 AWS WAF 機器人或詐騙控制受管規則群組時，規則群組會使用 AWS WAF Token 管理來檢查 Web 要求 Token，並將 Token 標籤套用至要求。如需有關受管規則群組的資訊AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）規則組，請參閱AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組、和AWS WAF 機器人控制規則群組。

> **Note**
>
> AWS WAF 只有在您使用其中一個智慧型威脅緩和管理規則群組時，才會套用 Token 標籤。

令牌管理可以將以下標籤添加到 Web 請求中。

客戶端會話標籤

標籤`awswaf:managed:token:id:`*`identifier`*包含 AWS WAF 權杖管理用來識別用戶端工作階段的唯一識別碼。如果客戶端獲取新令牌，則標識符可能會更改，例如在丟棄正在使用的令牌之後。

> **Note**
>
> AWS WAF 不報告此標籤的 Amazon CloudWatch 指標。

令牌狀態標籤：標籤命名空間前綴

令牌狀態標籤報告令牌的狀態，以及其包含的挑戰和 CAPTCHA 信息。

每個令牌狀態標籤都以下列命名空間前綴之一開始：

- `awswaf:managed:token:`— 用於報告令牌的一般狀態並報告令牌的挑戰信息的狀態。
- `awswaf:managed:captcha:`— 用於報告令牌的驗證碼信息的狀態。

權杖狀態標籤：標籤名稱

在前綴之後，標籤的其餘部分提供了詳細的令牌狀態信息：

- `accepted`-請求令牌存在並包含以下內容：
  - 有效的挑戰或驗證碼解決方案。
  - 未過期的挑戰或驗證碼時間戳記。
  - 對網頁 ACL 有效的網域規格。

  示例：該標籤`awswaf:managed:token:accepted`表示 Web 請求的令牌具有有效的挑戰解決方案，未過期的挑戰時間戳和有效的域。
- `rejected`— 請求令牌存在，但不符合驗收標準。

  隨著拒絕的標籤，令牌管理添加了一個自定義標籤命名空間和名稱來指示原因。
  - `rejected:not_solved`— 令牌缺少挑戰或驗證碼解決方案。
  - `rejected:expired`— 根據您的 Web ACL 配置的令牌免疫時間，令牌的挑戰或 CAPTCHA 時間戳已過期。
  - `rejected:domain_mismatch`— 令牌的域與 Web ACL 的令牌域配置不匹配。
  - `rejected:invalid`— AWS WAF 無法讀取指示的令牌。

範例：標籤`awswaf:managed:captcha:rejected`並`awswaf:managed:captcha:rejected:expired`指出要求遭拒絕，因為權杖中的 CAPTCHA 時間戳記已超過 Web ACL 中設定的 CAPTCHA 權杖免疫時間。

- `absent`-請求沒有令牌或令牌管理器無法讀取它。

  示例：標籤`awswaf:managed:captcha:absent`表示請求沒有令牌。

阻止沒有有效 AWS WAF 令牌的請求

當您使用智慧型威脅 AWS 受管規則群組`AWSManagedRulesACFPRuleSet`、`AWSManagedRulesATPRuleSet`、和時`AWSManagedRulesBotControlRuleSet`，規則群組會叫用 AWS WAF Token 管理來評估 Web 要求 Token 的狀態，並據此標示要求。

> **Note**
>
> Token 標籤僅適用於您使用其中一個受管規則群組評估的 Web 要求。

如需有關權杖管理套用之標籤的資訊，請參閱前一節AWS WAF 機器人和欺詐管理規則群組的權杖標籤。

然後，智慧型威脅緩和受管理規則群組會如下處理 Token 需求：

- 該`AWSManagedRulesACFPRuleSetAllRequests`規則被配置為對所有請求運行該Challenge操作，有效地阻止任何沒有`accepted`令牌標籤的請求。
- `AWSManagedRulesATPRuleSet`阻止具有`rejected`令牌標籤的請求，但不會阻止帶有`absent`令牌標籤的請求。
- `AWSManagedRulesBotControlRuleSet`目標防護層級會在用戶端傳送五個沒有 `accepted` Token 標籤的要求後提出挑戰。它不會阻止沒有有效令牌的單個請求。規則群組的一般保護層級不會管理權杖需求。

如需智慧型安全威脅規則群組的其他詳細資訊AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）規則組，請參閱AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組和AWS WAF 機器人控制規則群組。

使用機器人控制或 ATP 管理規則群組時封鎖遺失 Token 的要求

透過「機器人控制」和「可承諾量」規則群組，沒有有效權杖的請求可能會結束規則群組評估，並繼續由 Web ACL 評估。

若要封鎖遺失其 Token 或其 Token 遭拒絕的所有要求，請新增規則以在受管規則群組之後立即執行，以擷取並封鎖規則群組未為您處理的要求。

以下是使用可承諾量管理規則群組之 Web ACL 的 JSON 清單範例。Web ACL 已新增規則來擷取標`awswaf:managed:token:absent`籤並加以處理。此規則會將評估範圍縮小為前往登入端點的 Web 要求，以符合可承諾量規則群組的範圍。新增的規則以粗體列示。

```
{
  "Name": "exampleWebACL",
  "Id": "55555555-6666-7777-8888-999999999999",
  "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/webacl/
exampleWebACL/55555555-4444-3333-2222-111111111111",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesATPRuleSet",
      "Priority": 1,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesATPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesATPRuleSet": {
                "LoginPath": "/web/login",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  }
                },
                "ResponseInspection": {
                  "StatusCode": {
                    "SuccessCodes": [
```

```
                    200
                  ],
                  "FailureCodes": [
                    401,
                    403,
                    500
                  ]
                }
              }
            }
          }
        ]
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesATPRuleSet"
    }
  },
  {
    "Name": "RequireTokenForLogins",
    "Priority": 2,
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:token:absent"
              }
            }
          },
          {
            "ByteMatchStatement": {
              "SearchString": "/web/login",
              "FieldToMatch": {
                "UriPath": {}
              },
              "TextTransformations": [
```

```
                {
                  "Priority": 0,
                  "Type": "NONE"
                }
              ],
              "PositionalConstraint": "STARTS_WITH"
            }
          },
          {
            "ByteMatchStatement": {
              "SearchString": "POST",
              "FieldToMatch": {
                "Method": {}
              },
              "TextTransformations": [
                {
                  "Priority": 0,
                  "Type": "NONE"
                }
              ],
              "PositionalConstraint": "EXACTLY"
            }
          }
        ]
      }
    },
    "Action": {
      "Block": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "RequireTokenForLogins"
    }
  }
],
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "exampleWebACL"
},
"Capacity": 51,
"ManagedByFirewallManager": false,
"LabelNamespace": "awswaf:111111111111:webacl:exampleWebACL:"
```

```
}
```

來源的應用程式負載平衡器所需的組態 CloudFront

如果您將 Web ACL 與應用程式負載平衡器建立關聯，並將應用程 Application Load Balancer 部署為 CloudFront 發佈的來源，請閱讀本節。

使用此架構，您需要提供以下附加配置，以便正確處理令牌信息。

- 進行設 CloudFront 定以將 `aws-waf-token` Cookie 轉寄至 Application Load Balancer。預設情況下， CloudFront 會先從網頁要求中移除 Cookie，然後再將其轉寄至來源。要使用 Web 請求保留令牌 cookie，請配置 CloudFront 緩存行為以僅包含令牌 cookie 或所有 cookie。有關如何執行此操作的詳細資訊，請參閱 Amazon CloudFront 開發人員指南中的根據 Cookie 快取內容。
- 進行配置， AWS WAF 以便它將 CloudFront分發的域識別為有效的令牌域。依預設，會將標`Host`頭設 CloudFront 定為應用程式負載平衡器原點，並將其 AWS WAF 用作受保護資源的網域。不過，用戶端瀏覽器會將 CloudFront散佈視為主機網域，而針對用戶端產生的 Token 則會使用該 CloudFront 網域做為 Token 網域。如果沒有任何其他配置，當根據令牌域 AWS WAF 檢查受保護的資源域時，它將得到不匹配。若要修正此問題，請將 CloudFront 分發網域名稱新增至 Web ACL 組態中的權杖網域清單。如需如何進行該服務的詳細資訊，請參閱AWS WAF 網絡 ACL 令牌域列表配置。

AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）

帳戶創建欺詐是一種在線非法活動，攻擊者嘗試創建一個或多個虛假帳戶。攻擊者使用虛假帳戶進行欺詐活動，例如濫用促銷和註冊獎金，冒充某人以及網絡釣魚等網絡攻擊。虛假帳戶的存在可能會損害您與客戶的聲譽並暴露於金融欺詐行為，對您的業務產生負面影響。

您可以通過實施欺詐控制帳戶創建欺詐預防（ACFP）功能來監控和控制帳戶創建欺詐嘗試。 AWS WAF AWS WAF 在 AWS 受管規則規則群組中提供此功能，以及`AWSManagedRulesACFPRuleSet`隨附的應用程式整合 SDK。

ACFP 受管規則群組會標示並管理可能是惡意帳戶建立嘗試一部分的要求。規則群組透過檢查用戶端傳送到應用程式帳戶註冊端點的帳號建立嘗試來達成此目的。

ACFP 會監控帳戶註冊異常活動的要求，並自動封鎖可疑要求，藉此保護您的帳戶註冊頁面。規則群組會使用要求識別碼、行為分析和機器學習來偵測詐騙要求。

- 請求檢查 — ACFP 使您可以查看和控制異常帳戶創建嘗試和使用被盜憑據的嘗試，以防止創建欺詐帳戶。ACFP 會根據其被盜的憑據數據庫檢查電子郵件和密碼組合，該數據庫會在黑暗的網絡上發現新的洩露憑據時定期更新。ACFP 會評估電子郵件地址中使用的網域，並監控電話號碼和地址欄位的

使用情況，以驗證輸入項目並偵測詐騙行為。ACFP 會依據 IP 位址和用戶端工作階段彙總資料，以偵測並封鎖傳送太多可疑要求的用戶端。

- 回應檢查 — 對於 CloudFront 分發，除了檢查傳入的帳戶建立請求之外，ACFP 規則群組還會檢查應用程式對帳戶建立嘗試的回應，以追蹤成功率和失敗率。使用此資訊，ACFP 可以暫時封鎖嘗試失敗次數過多的用戶端工作階段或 IP 位址。 AWS WAF 異步執行響應檢查，因此這不會增加 Web 流量的延遲。

> **Note**
>
> 使用此受管規則群組時，會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

> **Note**
>
> ACFP 功能不適用於亞馬遜認可使用者集區。

主題

AWS WAF ACFP 零組件

AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）的主要組成部分如下：

- **`AWSManagedRulesACFPRuleSet`**— 此 AWS 受管規則規則群組中的規則會偵測、標記和處理各種類型的詐騙帳戶建立活動。規則群組會檢查用戶端傳送至指定帳戶註冊端點的 HTTP GET 文字 /html 要求，以及用戶端傳送至指定帳號註冊端點的 POST Web 要求。對於受保護的 CloudFront 分配，規則群組也會檢查分發傳回帳戶建立請求的回應。如需此規則群組規則的清單，請參閱AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）規則組。您可以使用受管規則群組參考陳述式將此規則群組包含在 Web ACL 中。如需有關使用此規則群組的資訊，請參閱將 ACFP 管理規則群組新增至您的網路 ACL。

> **Note**
>
> 使用此受管規則群組時，會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

- 有關應用程式帳戶註冊和建立頁面的詳細資訊 — 當您將AWSManagedRulesACFPRuleSet規則群組新增至 Web ACL 時，您必須提供有關帳戶註冊和建立頁面的資訊。這可讓規則群組縮小其檢查要求的範圍，並正確驗證帳戶建立 Web 要求。註冊頁面必須接受GET文本/HTML 請求。帳號建立路徑必須接受POST要求。ACFP 規則群組會使用電子郵件格式的使用者名稱。如需詳細資訊，請參閱 將 ACFP 管理規則群組新增至您的網路 ACL。
- 對於受保護的 CloudFront 發行版，有關您的應用程式如何回應帳戶建立嘗試的詳細資訊 — 您提供應用程式對帳戶建立嘗試回應的詳細資訊，而 ACFP 規則群組會追蹤並管理來自單一 IP 位址或單一用戶端工作階段的批次建立帳戶嘗試。如需有關配置此選項的資訊，請參閱將 ACFP 管理規則群組新增至您的網路 ACL。
- JavaScript 和行動應用程式整合 SDK — 透過 ACFP 實作來實作 AWS WAF JavaScript 和行動 SDK，以啟用規則群組提供的完整功能集。許多 ACFP 規則會使用 SDK 提供的資訊來進行工作階段層級用戶端驗證和行為彙總，這些資訊需要將合法的用戶端流量與機器人流量分開。如需 SDK 的詳細資訊，請參閱「AWS WAF 用戶端應用整合」。

您可以將 ACFP 實施與以下內容結合使用，以幫助您監控、調整和自訂您的保護。

- 記錄和指標 — 透過設定和啟用 Web ACL 的日誌、Amazon Security Lake 資料收集和 Amazon 指標，您可以監控流 CloudWatch 量，並瞭解 ACFP 受管規則群組對其有何影響。AWSManagedRulesACFPRuleSet添加到 Web 請求的標籤包含在數據中。如需有關選項的資訊記錄 AWS WAF 網頁 ACL 流量，請參閱使用 Amazon 監控 CloudWatch、和什麼是 Amazon 安全湖？ 。

  根據您的需求和看到的流量，您可能需要自訂AWSManagedRulesACFPRuleSet實作。例如，您可能想要從 ACFP 評估中排除某些流量，或者您可能想要使用範圍向下陳述式或標籤比對規則等 AWS WAF 功能來更改其處理某些帳戶建立詐騙嘗試的方式。
- 標籤和標籤相符規則 — 對於中的任何規則AWSManagedRulesACFPRuleSet，您可以將封鎖行為切換為計數，然後與規則新增的標籤進行比對。使用此方法可自訂處理 ACFP 受管規則群組所識別之 Web 要求的方式。若要取得有關標示和使用標籤比對陳述式的詳細資訊，請參閱標籤比對規則陳述式和AWS WAF 標籤, 上, 网, 請求。

- 自訂請求和回應 — 您可以將自訂標頭新增至您允許的請求，也可以針對您封鎖的請求傳送自訂回應。要做到這一點，您可以將匹配的標籤與 AWS WAF 自定義請求和響應功能配對。如需自訂請求和回應的詳細資訊，請參閱定制的 Web 請求和響應 AWS WAF。

為什麼您應該將應用程式整合 SDK 與 ACFP 搭配使用

我們強烈建議您實作應用程式整合 SDK，以便最有效地使用 ACFP 規則群組。

- 完整規則群組功能 — ACFP 規則`SignalClientHumanInteractivityAbsentLow`僅適用於應用程式整合所填入的權杖。此規則會偵測並管理與應用程式頁面的異常人類互動。應用程序集成 SDK 可以通過鼠標移動，按鍵和其他測量來檢測正常的人類交互性。由規則動作傳送且無法提供此類資料CAPTCHA的Challenge插入式廣告。
- 降低延遲 — 規則群組規則會將Challenge規則動作`AllRequests`套用至任何尚未擁有挑戰權杖的要求。發生這種情況時，規則組評估請求兩次：一次沒有令牌，然後在通過插頁式Challenge操作獲取令牌後第二次。只使用該`AllRequests`規則不會向您收取任何額外費用，但這種方法會增加 Web 流量的開銷，並增加最終使用者體驗的延遲。如果您使用應用程式整合取得 Token 用戶端，則在傳送帳戶建立要求之前，ACFP 規則群組會評估要求一次。

如需規則群組權能的詳細資訊，請參閱AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）規則組。

如需 SDK 的相關資訊，請參閱AWS WAF 用戶端應用整合。如需有關 AWS WAF 權杖的資訊，請參閱AWS WAF 網絡請求令牌。如需有關規則動作的資訊，請參閱CAPTCHA並Challenge在 AWS WAF。

將 ACFP 管理規則群組新增至您的網路 ACL

若要設定 ACFP 受管規則群組以辨識 Web 流量中的帳戶建立詐騙活動，您需要提供有關用戶端如何存取註冊頁面的資訊，並將帳戶建立要求傳送至您的應用程式。對於受保護的 Amazon CloudFront 分發，您還提供應用程式如何回應帳戶建立請求的相關資訊。此組態是受管理規則群組的一般組態以外的配置。

如需規則群組說明與規則清單，請參閱AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）規則組。

> **Note**
>
> ACFP 失竊的認證資料庫僅包含電子郵件格式的使用者名稱。

本指引適用於一般知道如何建立和管理 AWS WAF Web ACL、規則和規則群組的使用者。這些主題涵蓋在本指南之前的章節中。如需如何將受管規則群組新增至 Web ACL 的基本資訊，請參閱透過主控台將受管規則群組新增至 Web ACL。

遵循最佳做法

請依照上智慧型威脅緩解的最佳做法的最佳作法使用 ACFP 規則群組。

若要在 Web ACL 中使用**AWSManagedRulesACFPRuleSet**規則群組

1. 將受 AWS 管規則群組新增AWSManagedRulesACFPRuleSet至 Web ACL，然後在儲存前編輯規則群組設定。

   > **Note**
   >
   > 使用此受管規則群組時，會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

2. 在規則群組組態窗格中，提供 ACFP 規則群組用來檢查帳戶建立要求的資訊。

   a. 對於在路徑中使用規則運算式，如果您要針對註冊和帳戶建立頁面路徑規格執行規則運算式比對，請 AWS WAF 將此選項切換為開啟。

      AWS WAF 支援 PCRE 程式庫所使用的模式語法，但libpcre有一些例外。該庫在 PCRE-Perl 兼容的正則表達式中記錄。如需有關 AWS WAF 支援的資訊，請參閱正則表達式模式匹配 AWS WAF。

   b. 對於「註冊」頁面路徑，請提供應用程式註冊頁面端點的路徑。此頁面必須接受GET文字 / html 要求。規則群組只會檢查指定註冊頁面端點的 HTTP GET 文字 /html 要求。

      > **Note**
      >
      > 端點的比對不區分大小寫。正則表達式規範不能包含標誌(?-i)，這會禁用不區分大小寫的匹配。字串規格必須以正斜線開頭/。

      例如，對於 URLhttps://example.com/web/registration，您可以提供字串路徑規格/web/registration。以您提供的路徑開頭的註冊頁面路徑會被視為相符項目。例如，/web/registration符合註冊路徑/web/registration/web/registration//web/registrationPage、/web/registration/thisPage、和，但不符合路徑/home/web/registration或/website/registration。

> **Note**
>
> 請確定您的使用者在提交帳戶建立要求之前載入註冊頁面。這有助於確保來自客戶端的帳戶創建請求包含有效令牌。

c. 對於帳戶創建路徑，請在您的網站中提供接受完成的新用戶詳細信息的 URI。此 URI 必須接受POST請求。

> **Note**
>
> 端點的比對不區分大小寫。正則表達式規範不能包含標誌(?-i)，這會禁用不區分大小寫的匹配。字串規格必須以正斜線開頭/。

例如，對於 URLhttps://example.com/web/newaccount，您可以提供字串路徑規格/web/newaccount。以您提供的路徑開頭的帳戶建立路徑會被視為相符項目。例如，/web/newaccount符合帳戶建立路徑/web/newaccount/web/newaccount//web/newaccountPage、/web/newaccount/thisPage、和，但不符合路徑/home/web/newaccount或/website/newaccount。

d. 針對要求檢查，請指定應用程式接受帳戶建立嘗試的方式，方法是提供要求承載類型，以及要求內文中提供使用者名稱、密碼和其他帳戶建立詳細資訊的欄位名稱。

> **Note**
>
> 對於主要地址和電話號碼欄位，請依照欄位出現在要求承載中的順序提供欄位。

欄位名稱的指定取決於裝載類型。

- JSON 裝載類型 — 以 JSON 指標語法指定欄位名稱。如需 JSON 指標語法的相關資訊，請參閱網際網路工程工作小組 (IETF) 文JavaScript件物件標記法 (JSON) 指標。

  例如，對於下列範例 JSON 承載，使用者名稱欄位規格為/signupform/username，主要位址欄位規格為/signupform/addrp1/signupform/addrp2、和/signupform/addrp3。

```
{
```

```
    "signupform": {
        "username": "THE_USERNAME",
        "password": "THE_PASSWORD",
        "addrp1": "PRIMARY_ADDRESS_LINE_1",
        "addrp2": "PRIMARY_ADDRESS_LINE_2",
        "addrp3": "PRIMARY_ADDRESS_LINE_3",
        "phonepcode": "PRIMARY_PHONE_CODE",
        "phonepnumber": "PRIMARY_PHONE_NUMBER"
    }
}
```

- 表單編碼有效負載類型 — 使用 HTML 表單名稱。

  例如，對於名為 AND 的使用者和密碼輸入元素的 HTML 表單 `username1password1`，使用者名稱欄位規格為`username1`且密碼欄位規格為`password1`。

e. 如果您要保護 Amazon CloudFront 分發，請在「回應檢查」下，指定應用程式如何在帳戶建立嘗試的回應中表示成功或失敗。

> **Note**
>
> ACFP 回應檢測僅適用於保護 CloudFront 散佈的網路 ACL。

在帳號建立回應中指定您要 ACFP 檢查的單一元件。對於主體和 JSON 組件類型， AWS WAF 可以檢查組件的前 65,536 個字節（64 KB）。

提供元件類型的檢驗標準，如介面所示。您必須同時提供成功和失敗準則，才能在元件中進行檢查。

例如，假設您的應用程序在響應的狀態代碼中指出帳戶創建嘗試的狀態，並用`200 OK`於成功和`/401 Unauthorized`或`403 Forbidden`失敗。您可以將回應檢查元件類型設定為狀態碼，然後在成功文字方塊中輸入，`200`並在失敗文字方塊中輸入`401`第一行，`403`在第二行輸入。

ACFP 規則群組只會計算符合成功或失敗檢查準則的回應。規則群組規則會在用戶端上運作，而這些規則群組規則在計數的回應中的成功率過高，以減輕批次處理帳號建立嘗試。為了確保規則群組規則的正確行為，請務必提供完整的資訊以供成功和失敗的帳號建立嘗試。

若要查看檢查帳號建立回應的規則，請`VolumetricSessionSuccessfulResponse`在列出的規則中尋找`VolumetricIPSuccessfulResponse`和AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）規則組。

3. 為規則群組提供任何您想要的其他組態。

   您可以在受管規則群組陳述式中新增範圍向下陳述式，進一步限制規則群組檢查的要求範圍。例如，您只能檢查具有特定查詢引數或 Cookie 的請求。規則群組只會檢查符合範圍陳述式中條件的要求，以及傳送至您在規則群組組態中指定的帳戶註冊和帳戶建立路徑的要求。如需有關向下範圍陳述式的資訊，請參閱。範圍向下語句

4. 將您的變更儲存至網路 ACL。

在為生產流量部署 ACFP 實施之前，請在測試或測試環境中對其進行測試和調整，直到您熟悉對流量的潛在影響為止。然後在啟用規則之前，使用生產流量在計數模式下測試和調整規則。如需指引，請參閱下一節。

測試和部署 ACFP

本節提供設定和測試網站 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 實作的一般指引。您選擇遵循的特定步驟將取決於您收到的需求、資源和 Web 要求。

此資訊是除了有關測試和調整的一般資訊之外，請參閱測試和調整您的 AWS WAF 保護。

> **Note**
>
> AWS 受管規則旨在保護您免受常見網頁威脅的侵害。根據文件使用時， AWS Managed Rules 規則群組會為您的應用程式新增另一層安全性。不過， AWS 受管規則群組並不是用來取代您的安全性責任，而這些責任是由您選取的 AWS 資源所決定。請參閱「共同責任模型」，以確保中的資源受到 AWS 適當的保護。

> **生產流量風險**
>
> 在為生產流量部署 ACFP 實施之前，請在測試或測試環境中對其進行測試和調整，直到您熟悉對流量的潛在影響為止。然後在啟用規則之前，使用生產流量在計數模式下測試和調整規則。

AWS WAF 提供測試認證，您可以用來驗證您的 ACFP 組態。在下列程序中，您將設定測試 Web ACL 以使用 ACFP 受管規則群組、設定規則以擷取規則群組新增的標籤，然後使用這些測試認證執行帳戶建立嘗試。您可以檢查帳戶建立嘗試的 Amazon CloudWatch 指標，以確認您的 Web ACL 是否已妥善管理嘗試。

本指引適用於一般知道如何建立和管理 AWS WAF Web ACL、規則和規則群組的使用者。這些主題涵蓋在本指南之前的章節中。

設定和測試 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 實作

請先在測試環境中執行這些步驟，然後在生產環境中執行。

1. 在計數模式中 AWS WAF 新增詐騙控制帳戶建立詐騙預防 (ACFP) 受管規則群組

   > **Note**
   >
   > 使用此受管規則群組時，會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

   將受 AWS 管規則規則群組新增`AWSManagedRulesACFPRuleSet`至新的或現有的 Web ACL，並對其進行設定，使其不會改變目前的 Web ACL 行為。如需有關此規則群組之規則和標籤的詳細資訊，請參閱AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）規則組。

   - 新增受管規則群組時，請加以編輯並執行下列動作：
     - 在規則群組設定窗格中，提供應用程式帳戶註冊和建立頁面的詳細資料。ACFP 規則群組會使用此資訊來監視登入活動。如需詳細資訊，請參閱 將 ACFP 管理規則群組新增至您的網路 ACL。
     - 在「規則」窗格中，開啟「覆寫所有規則動作」下拉式清單並選擇Count。使用此設定時，AWS WAF 會根據規則群組中的所有規則評估要求，並僅計算結果的相符項目，同時仍將標籤新增至要求。如需詳細資訊，請參閱 覆寫規則群組中的規則動作。

       透過此覆寫，您可以監視 ACFP 管理規則的潛在影響，以判斷是否要新增例外狀況，例如內部使用案例的例外狀況。
   - 定位規則群組，使其在 Web ACL 中的現有規則之後進行評估，其優先順序設定的數值高於您已經使用的任何規則或規則群組。如需詳細資訊，請參閱 Web ACL 中規則和規則群組的處理順序。

     這樣，您當前的流量處理不會中斷。例如，如果您有偵測惡意流量的規則，例如 SQL 插入或跨網站指令碼，他們將繼續偵測並記錄該流量。或者，如果您有允許已知非惡意流量的規則，它們

可以繼續允許該流量，而不會讓 ACFP 受管規則群組封鎖該流量。您可能會決定在測試和調整活動期間調整處理順序。

2. 實作應用程式整合 SDK

   將 AWS WAF JavaScript SDK 整合到瀏覽器的帳戶註冊和帳戶建立路徑中。 AWS WAF 還提供移動軟件開發套件，以集成 iOS 和安卓設備。如需整合 SDK 的詳細資訊，請參閱AWS WAF 用戶端應用整合。如需有關此建議的資訊，請參閱為什麼您應該將應用程式整合 SDK 與 ACFP 搭配使用。

   > **Note**
   >
   > 如果您無法使用應用程式整合 SDK，可以透過在 Web ACL 中編輯 ACFP 規則群組並移除您置於規則上的覆寫來測試 ACFP 規則群組。`AllRequests`這會啟用規則的Challenge動作設定，以確保要求包含有效的挑戰 Token。
   >
   > 首先在測試環境中執行此操作，然後在生產環境中小心執行此操作。這種方法有可能阻止用戶。例如，如果您的註冊頁面路徑不接受 GET text/html 請求，則此規則配置可以有效地阻止註冊頁面上的所有請求。

3. 啟用 Web ACL 的記錄和指標

   視需要設定網路 ACL 的記錄、Amazon 安全湖資料收集、請求取樣和 Amazon CloudWatch 指標。您可以使用這些可見度工具來監視 ACFP 受管規則群組與流量的互動。

   - 如需日誌記錄的相關資訊，請參閱記錄 AWS WAF 網頁 ACL 流量。
   - 有關 Amazon 安全湖的信息，請參閱什麼是 Amazon 安全湖？ 以及從 Amazon 安全湖使用者指南中的 AWS 服務收集資料。
   - 如需 Amazon CloudWatch 指標的相關資訊，請參閱使用 Amazon 監控 CloudWatch。
   - 如需 Web 請求取樣的詳細資訊，請參閱檢視 Web 請求的範例。

4. 將網路 ACL 與資源建立關聯

   如果 Web ACL 尚未與測試資源相關聯，請將其關聯。如需相關資訊，請參閱建立 Web ACL 與資源的關聯或取消關聯 AWS。

5. 監控流量和 ACFP 規則符合

   請確定您的一般流量正在流動，而且 ACFP 受管規則群組規則正在新增標籤至相符的 Web 要求。您可以在日誌中看到標籤，並在 Amazon 指標中查看 ACFP 和標籤 CloudWatch 指標。在記錄檔

中，您覆寫規則群組中要計數的規則會顯示在action設定為 count ruleGroupList 的規則中，並overriddenAction指示您覆寫的已設定規則動作。

6. 測試規則群組的認證檢查功能

   使用測試遭到入侵的認證執行帳戶建立嘗試，並檢查規則群組是否符合預期。

   a. 存取受保護資源的帳號註冊頁面，並嘗試新增帳號。使用以下 AWS WAF 測試憑證對並輸入任何測試

      - 使用者：WAF_TEST_CREDENTIAL@wafexample.com
      - 密碼：WAF_TEST_CREDENTIAL_PASSWORD

      這些測試認證會歸類為遭到入侵的認證，而 ACFP 管理規則群組會將awswaf:managed:aws:acfp:signal:credential_compromised標籤新增至帳戶建立要求，您可以在記錄檔中看到這些要求。

   b. 在您的 Web ACL 日誌中，在測試帳戶創建請求的日誌條目的labels字段中查找awswaf:managed:aws:acfp:signal:credential_compromised標籤。如需日誌記錄的相關資訊，請參閱記錄 AWS WAF 網頁 ACL 流量。

   驗證規則群組如預期擷取遭到入侵的認證之後，您可以根據受保護的資源所需採取步驟來設定其實作。

7. 對於 CloudFront 分發，請測試規則群組對批次建立帳號嘗試的管理

   針對您為 ACFP 規則群組設定的每個成功回應條件執行此測試。測試之間至少等待 30 分鐘。

   a. 對於每個成功條件，請確定帳戶創建嘗試，該嘗試將在響應中成功使用該成功條件。然後，在單個客戶端會話中，在 30 分鐘內執行至少 5 次成功創建帳戶嘗試。使用者通常只會在您的網站上建立一個帳戶。

      第一次成功建立帳戶之後，VolumetricSessionSuccessfulResponse規則應該會根據您的規則動作覆寫規則，開始與帳戶建立回應的其餘部分進行比對，並加上標籤並計算這些回應。由於延遲，規則可能會錯過前一個或兩個規則。

   b. 在您的 Web ACL 記錄中，在測試帳戶建立 Web 請求的記錄項目labels欄位中尋找awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation標籤。如需日誌記錄的相關資訊，請參閱記錄 AWS WAF 網頁 ACL 流量。

這些測試會檢查規則彙總的成功計數是否超過規則的臨界值，以驗證您的成功條件是否符合您的回應。達到臨界值之後，如果您繼續從相同的工作階段傳送帳戶建立要求，規則將繼續符合，直到成功率降至閾值以下為止。當超過臨界值時，規則會符合從工作階段位址建立成功或失敗的帳號建立嘗試。

8. 自訂 ACFP 網頁要求處理

   視需要新增明確允許或封鎖要求的自己規則，以變更 ACFP 規則處理要求的方式。

   例如，您可以使用 ACFP 標籤來允許或封鎖要求或自訂要求處理。您可以在 ACFP 管理規則群組之後新增標籤比對規則，以篩選要套用之處理的標籤要求。測試之後，請將相關的 ACFP 規則保持在計數模式中，並在自訂規則中維護要求處理決策。如需範例，請參閱ACFP 範例：對遭到入侵認證的自訂回應。

9. 移除測試規則並啟用 ACFP 受管規則群組設定

   根據您的情況，您可能已決定要將某些 ACFP 規則保留為計數模式。針對您要在規則群組內設定執行的規則，請停用 Web ACL 規則群組組態中的計數模式。完成測試後，您也可以移除測試標籤比對規則。

10. 監控和調整

    為了確保網頁要求能夠依照您的需求處理，請在啟用想要使用的 ACFP 功能之後，密切監視您的流量。使用規則群組上的規則計數覆寫，並使用您自己的規則，視需要調整行為。

完成測試 ACFP 規則群組實作之後，如果您尚未將 AWS WAF JavaScript SDK 整合到瀏覽器的帳戶註冊和帳戶建立頁面中，我們強烈建議您這麼做。 AWS WAF 還提供移動軟件開發套件，以集成 iOS 和安卓設備。如需整合 SDK 的詳細資訊，請參閱AWS WAF 用戶端應用整合。如需有關此建議的資訊，請參閱為什麼您應該將應用程式整合 SDK 與 ACFP 搭配使用。

AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）示例

本節顯示符合 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 實作的常見使用案例的範例組態。

每個範例都會提供使用案例的說明，然後在 JSON 清單中顯示自訂設定規則的解決方案。

> **Note**
>
> 您可以透過主控台 Web ACL JSON 下載或規則 JSON 編輯器，或透過 API 和命令列介面中的`getWebACL`作業擷取 JSON 清單，如這些範例所示。

主題

ACFP 範例：簡單的設定

下列 JSON 清單顯示具有 AWS WAF 詐騙控制帳戶建立詐騙預防 (ACFP) 管理規則群組的網路 ACL 範例。請記下其他`CreationPath`和`RegistrationPagePath`組態，以及承載類型，以及在承載中尋找新帳戶資訊所需的資訊，以便進行驗證。規則群組會使用此資訊來監控和管理您的帳戶建立要求。此 JSON 包含 Web ACL 自動產生的設定，例如標籤命名空間和 Web ACL 的應用程式整合 URL。

```
{
  "Name": "simpleACFP",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/simpleACFP/... ",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  },
```

```
                "EmailField": {
                  "Identifier": "/form/email"
                },
                "PhoneNumberFields": [
                  {
                    "Identifier": "/form/country-code"
                  },
                  {
                    "Identifier": "/form/region-code"
                  },
                  {
                    "Identifier": "/form/phonenumber"
                  }
                ],
                "AddressFields": [
                  {
                    "Identifier": "/form/name"
                  },
                  {
                    "Identifier": "/form/street-address"
                  },
                  {
                    "Identifier": "/form/city"
                  },
                  {
                    "Identifier": "/form/state"
                  },
                  {
                    "Identifier": "/form/zipcode"
                  }
                ]
              },
              "EnableRegexInPath": false
            }
          }
        ]
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
```

```
        "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "simpleACFP"
  },
  "Capacity": 50,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:simpleACFP:"
}
```

ACFP 範例：對遭到入侵認證的自訂回應

根據預設，規則群組執行的認證檢查會透過標記要求並封鎖要求來`AWSManagedRulesACFPRuleSet`處理遭到入侵的認證。如需有關規則群組和規則行為的詳細資訊，請參閱AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）規則組。

要通知用戶他們提供的帳戶憑據已被洩露，您可以執行以下操作：

- 將**`SignalCredentialCompromised`**規則覆寫為 Count — 這會導致規則僅計算相符請求並加上標籤。
- 使用自訂處理新增標籤比對規則 — 設定此規則以符合 ACFP 標籤並執行您的自訂處理。

下列 Web ACL 清單顯示先前範例中的 ACFP 管理規則群組，而`SignalCredentialCompromised`規則動作會覆寫為計數。使用此配置時，當此規則組評估任何使用受損憑據的 Web 請求時，它將標記該請求，但不會阻止它。

此外，Web ACL 現在具有名為的自訂回應`aws-waf-credential-compromised`和名為的新規則`AccountSignupCompromisedCredentialsHandling`。規則優先順序的數值設定高於規則群組，因此它會在 Web ACL 評估中的規則群組之後執行。新規則會符合具有規則群組遭入侵認證標籤的任何要求。當規則找到相符項目時，會將`Block`動作套用至具有自訂回應主體的要求。自訂回應主體會向使用者提供其認證已遭入侵的資訊，並提出要採取的動作。

```
{
  "Name": "compromisedCreds",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/compromisedCreds/...",
  "DefaultAction": {
```

```
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  },
                  "EmailField": {
                    "Identifier": "/form/email"
                  },
                  "PhoneNumberFields": [
                    {
                      "Identifier": "/form/country-code"
                    },
                    {
                      "Identifier": "/form/region-code"
                    },
                    {
                      "Identifier": "/form/phonenumber"
                    }
                  ],
                  "AddressFields": [
                    {
                      "Identifier": "/form/name"
                    },
                    {
                      "Identifier": "/form/street-address"
```

```
                    },
                    {
                      "Identifier": "/form/city"
                    },
                    {
                      "Identifier": "/form/state"
                    },
                    {
                      "Identifier": "/form/zipcode"
                    }
                  ]
                },
                "EnableRegexInPath": false
              }
            }
          ],
          "RuleActionOverrides": [
            {
              "Name": "SignalCredentialCompromised",
              "ActionToUse": {
                "Count": {}
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
      }
    },
    {
      "Name": "AccountSignupCompromisedCredentialsHandling",
      "Priority": 1,
      "Statement": {
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "awswaf:managed:aws:acfp:signal:credential_compromised"
        }
      },
```

```
      "Action": {
        "Block": {
          "CustomResponse": {
            "ResponseCode": 406,
            "CustomResponseBodyKey": "aws-waf-credential-compromised",
            "ResponseHeaders": [
              {
                "Name": "aws-waf-credential-compromised",
                "Value": "true"
              }
            ]
          }
        }
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AccountSignupCompromisedCredentialsHandling"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "compromisedCreds"
  },
  "Capacity": 51,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:compromisedCreds:",
  "CustomResponseBodies": {
    "aws-waf-credential-compromised": {
      "ContentType": "APPLICATION_JSON",
      "Content": "{\n  \"credentials-compromised\": \"The credentials you provided have
 been found in a compromised credentials database.\\n\\nTry again with a different
 username, password pair.\"\n}"
    }
  }
}
```

ACFP 範例：回應檢查組態

下列 JSON 清單顯示範例 Web ACL，其中包含設定為 AWS WAF 檢查來源回應的詐騙控制帳戶建立詐騙預防 (ACFP) 受管規則群組。請注意響應檢查配置，該配置指定成功和響應狀態代碼。您也可以根

據標題、內文和內文 JSON 相符項目來設定成功和回應設定。此 JSON 包含 Web ACL 自動產生的設定，例如標籤命名空間和 Web ACL 的應用程式整合 URL。

> **Note**
>
> 可承諾量回應檢查僅適用於保護 CloudFront 分配的 Web ACL。

```
{
  "Name": "simpleACFP",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/simpleACFP/... ",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  },
                  "EmailField": {
                    "Identifier": "/form/email"
                  },
                  "PhoneNumberFields": [
                    {
```

```
                    "Identifier": "/form/country-code"
                  },
                  {
                    "Identifier": "/form/region-code"
                  },
                  {
                    "Identifier": "/form/phonenumber"
                  }
                ],
                "AddressFields": [
                  {
                    "Identifier": "/form/name"
                  },
                  {
                    "Identifier": "/form/street-address"
                  },
                  {
                    "Identifier": "/form/city"
                  },
                  {
                    "Identifier": "/form/state"
                  },
                  {
                    "Identifier": "/form/zipcode"
                  }
                ]
              },
              "ResponseInspection": {
                "StatusCode": {
                  "SuccessCodes": [
                    200
                  ],
                  "FailureCodes": [
                    401
                  ]
                }
              },
              "EnableRegexInPath": false
            }
          }
        ]
      }
    },
    "OverrideAction": {
```

```
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "simpleACFP"
  },
  "Capacity": 50,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:simpleACFP:"
  }
```

AWS WAF 防止欺詐控制帳戶接管（ATP）

帳戶接管是一種在線非法活動，攻擊者可以在未經授權的情況下訪問某個人的帳戶。攻擊者可能會通過多種方式執行此操作，例如使用被盜的憑據或通過一系列嘗試來猜測受害者的密碼。當攻擊者獲得訪問權限時，他們可能會從受害者那裡竊取金錢，信息或服務。攻擊者可能冒充受害者，以取得受害者擁有的其他帳戶的存取權，或取得其他人員或組織帳戶的存取權。此外，他們可能會嘗試更改用戶的密碼，以阻止受害者進入他們自己的帳戶。

您可以透過實作 AWS WAF 詐騙控制帳戶接管預防 (ATP) 功能來監控帳戶接管嘗試。 AWS WAF 在 AWS 受管規則規則群組`AWSManagedRulesATPRuleSet`和隨附應用程式整合 SDK 中提供此功能。

ATP 受管規則群組會標示並管理可能是惡意帳戶接管嘗試一部分的要求。規則群組會檢查用戶端傳送到應用程式登入端點的登入嘗試來達成此目的。

- 請求檢查 — ATP 使您可以查看和控制異常登錄嘗試和使用被盜憑據的登錄嘗試，以防止可能導致欺詐活動的帳戶被盜。ATP 會根據其被盜的憑證資料庫檢查電子郵件和密碼組合，該資料庫會在黑暗的網路上發現新的洩漏憑證時定期更新。ATP 會依據 IP 位址和用戶端工作階段彙總資料，以偵測並封鎖傳送太多可疑要求的用戶端。
- 回應檢查 — 對於 CloudFront 分配，除了檢查內送登入請求之外，可承諾量規則群組還會檢查應用模組對登入嘗試的回應，以追蹤成功率與失敗率。使用此資訊，ATP 可以暫時封鎖發生過多登入失敗的用戶端工作階段或 IP 位址。 AWS WAF 異步執行響應檢查，因此這不會增加 Web 流量的延遲。

> **Note**
>
> 使用此受管規則群組時，會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

> **Note**
>
> 可承諾量功能不適用於 Amazon Cognito 用者集區。

主題

AWS WAF 可承諾量元

防止 AWS WAF 詐騙控制帳戶接管 (ATP) 的主要元件如下：

- **`AWSManagedRulesATPRuleSet`**— 此 AWS 受管規則規則群組中的規則會偵測、標記和處理各種類型的帳戶接管活動。規則群組會檢查用戶端傳送至指定登入端點的 HTTP POST Web 要求。對於受保護的散 CloudFront 佈，規則群組也會檢查散發傳回這些要求的回應。如需規則群組規則的清單，請參閱AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組。您可以使用受管規則群組參考陳述式將此規則群組包含在 Web ACL 中。如需有關使用此規則群組的資訊，請參閱將可承諾量管理規則群組新增至您的 Web ACL。

  > **Note**
  >
  > 使用此受管規則群組時，會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

- 應用程式登入頁面的詳細資訊 — 將`AWSManagedRulesATPRuleSet`規則群組新增至 Web ACL 時，必須提供有關登入頁面的資訊。這可讓規則群組縮小其檢查要求的範圍，並正確驗證 Web 要求中的認證使用情況。可承諾量規則群組會使用電子郵件格式的使用者名稱。如需詳細資訊，請參閱將可承諾量管理規則群組新增至您的 Web ACL。

- 對於受保護的 CloudFront 發行版，有關應用程式如何回應登入嘗試的詳細資訊 — 您提供應用程式對登入嘗試回應的詳細資訊，規則群組會追蹤和管理傳送太多登入嘗試失敗的用戶端。如需有關配置此選項的資訊，請參閱將可承諾量管理規則群組新增至您的 Web ACL。
- JavaScript 和行動應用程式整合 SDK — 透過 ATP 實作來實作 AWS WAF JavaScript 和行動 SDK，以啟用規則群組提供的完整功能集。許多可承諾量規則會使用 SDK 提供的資訊來進行工作階段層級用戶端驗證和行為彙總，這些資訊需要將合法的用戶端流量與機器人流量分開。如需 SDK 的詳細資訊，請參閱「AWS WAF 用戶端應用整合」。

您可以將 ATP 導入與下列項目結合使用，以協助您監視、調整及自訂保護。

- 記錄和指標 — 透過設定和啟用 Web ACL 的日誌、Amazon Security Lake 資料收集和 Amazon 指標，您可以監控流 CloudWatch 量，並瞭解 ACFP 受管規則群組對其有何影響。`AWSManagedRulesATPRuleSet`添加到 Web 請求的標籤包含在數據中。如需有關選項的資訊記錄 AWS WAF 網頁 ACL 流量，請參閱使用 Amazon 監控 CloudWatch、和什麼是 Amazon 安全湖？。

  根據您的需求和看到的流量，您可能需要自訂`AWSManagedRulesATPRuleSet`實作。例如，您可能想要從 ATP 評估中排除某些流量，或者您可能想要使用範圍向下陳述式或標籤比對規則等 AWS WAF 功能來改變其處理某些帳戶接管嘗試的方式。
- 標籤和標籤相符規則 — 對於中的任何規則`AWSManagedRulesATPRuleSet`，您可以將封鎖行為切換為計數，然後與規則新增的標籤進行比對。使用此方法可自訂處理可承諾量管理規則群組所識別之 Web 要求的方式。若要取得有關標示和使用標籤比對陳述式的詳細資訊，請參閱標籤比對規則陳述式和AWS WAF 標籤, 上, 网, 請求。
- 自訂請求和回應 — 您可以將自訂標頭新增至您允許的請求，也可以針對您封鎖的請求傳送自訂回應。要做到這一點，您可以將匹配的標籤與 AWS WAF 自定義請求和響應功能配對。如需自訂請求和回應的詳細資訊，請參閱定制的 Web 請求和響應 AWS WAF。

為什麼您應該將應用程式整合 SDK 與 ATP 搭配使用

ATP 受管規則群組需要應用程式整合 SDK 所產生的挑戰權杖。權杖會啟用規則群組提供的全套保護。

我們強烈建議您實作應用程式整合 SDK，以便最有效地使用可承諾量規則群組。挑戰命令檔必須在可承諾量規則群組之前執行，規則群組才能從指令集取得的權杖中獲益。這會透過應用程式整合 SDK 自動發生。如果您無法使用 SDK，您可以交替地設定 Web ACL，使其針對可承諾量CAPTCHA規則群組將檢查的所有請求執行Challenge或規則動作。使用Challenge或CAPTCHA規則動作可能會產生額外費用。如需定價詳細資訊，請參閱 AWS WAF 定價。

不需要權杖之可承諾量規則群組的功能

當 Web 請求沒有 Token 時，可承諾量管理規則群組能夠封鎖下列類型的流量：

- 發出大量登錄請求的單個 IP 地址。
- 單一 IP 位址會在短時間內發出大量失敗的登入要求。
- 嘗試使用相同的用戶名，但更改密碼的密碼進行密碼遍歷登錄。

需要權杖之可承諾量規則群組的功能

挑戰 Token 中提供的資訊可擴充規則群組和整體用戶端應用程式安全性的功能。

Token 會針對每個 Web 要求提供用戶端資訊，這些要求可讓 ATP 規則群組將合法的用戶端工作階段與行為不良的用戶端工作階段分隔開來，即使兩者都來自單一 IP 位址也是如此。規則群組會使用 Token 中的資訊來彙總用戶端工作階段要求行為，以進行微調的偵測和緩和措施。

當 Token 在 Web 請求中可用時，可承諾量規則群組可偵測並封鎖階段作業層級的下列其他用戶端類別：

- SDK 管理的無訊息挑戰失敗的用戶端工作階段。
- 遍歷使用者名稱或密碼的用戶端工作階段。這也稱為認證填充。
- 重複使用失竊認證登入的用戶端工作階段。
- 花費很長時間嘗試登入的用戶端工作階段。
- 發出大量登入要求的用戶端工作階段。與 AWS WAF 速率型規則相比，可承諾量規則群組可提供更好的用戶端隔離，該規則可依據 IP 位址封鎖用戶端。可承諾量規則群組也會使用較低的臨界值。
- 在短時間內發出許多失敗登入要求的用戶端工作階段。此功能適用於受保護的 Amazon CloudFront 發行版。

如需規則群組權能的詳細資訊，請參閱AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組。

如需 SDK 的相關資訊，請參閱AWS WAF 用戶端應用整合。如需有關 AWS WAF 權杖的資訊，請參閱AWS WAF 網絡請求令牌。如需有關規則動作的資訊，請參閱CAPTCHA並Challenge在 AWS WAF。

將可承諾量管理規則群組新增至您的 Web ACL

若要將 ATP 受管規則群組設定為辨識 Web 流量中的帳戶接管活動，您需要提供用戶端如何傳送登入要求至您的應用程式的相關資訊。對於受保護的 Amazon CloudFront 分發，您還提供有關應用程式如何回應登入請求的資訊。此組態是受管理規則群組的一般組態以外的配置。

如需規則群組說明與規則清單，請參閱AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組。

> **Note**
>
> ATP 失竊的認證資料庫僅包含電子郵件格式的使用者名稱。

本指引適用於一般知道如何建立和管理 AWS WAF Web ACL、規則和規則群組的使用者。這些主題涵蓋在本指南之前的章節中。如需如何將受管規則群組新增至 Web ACL 的基本資訊，請參閱透過主控台將受管規則群組新增至 Web ACL。

遵循最佳做法

請根據的最佳作法來使用可承諾量規則群組智慧型威脅緩解的最佳做法。

若要在 Web ACL 中使用**`AWSManagedRulesATPRuleSet`**規則群組

1. 將受 AWS 管規則群組新增`AWSManagedRulesATPRuleSet`至 Web ACL，然後在儲存前編輯規則群組設定。

   > **Note**
   >
   > 使用此受管規則群組時，會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

2. 在「規則群組組態」窗格中，提供可承諾量規則群組用來檢查登入要求的資訊。

   a. 對於在路徑中使用規則運算式，如果您要針對登入頁面路徑規格執行規則運算式比對，請 AWS WAF 將此選項切換為開啟。

      AWS WAF 支援 PCRE 程式庫所使用的模式語法，但`libpcre`有一些例外。該庫在 PCRE-Perl 兼容的正則表達式中記錄。如需有關 AWS WAF 支援的資訊，請參閱正則表達式模式匹配 AWS WAF。

   b. 針對登入路徑，請提供應用程式登入端點的路徑。規則群組只會檢查對您指定之登入端點的 HTTP POST 要求。

> **Note**
>
> 端點的比對不區分大小寫。正則表達式規範不能包含標誌(?-i)，這會禁用不區分大小寫的匹配。字串規格必須以正斜線開頭/。

例如，對於 URLhttps://example.com/web/login，您可以提供字串路徑規格/web/login。以您提供的路徑開頭的登入路徑會被視為相符項目。例如，/web/login符合登入路徑/web/login/web/login//web/loginPage、、和/web/login/thisPage，但不符合登入路徑/home/web/login或/website/login。

c. 針對要求檢查，請指定應用程式接受登入嘗試的方式，方法是提供要求承載類型，以及要求主體中提供使用者名稱和密碼的欄位名稱。欄位名稱的指定取決於有效負載類型。

- JSON 裝載類型 — 以 JSON 指標語法指定欄位名稱。如需 JSON 指標語法的相關資訊，請參閱網際網路工程工作小組 (IETF) 文JavaScript件物件標記法 (JSON) 指標。

  例如，對於下列範例 JSON 承載，使用者名稱欄位規格為/login/username，密碼欄位規格為/login/password。

  ```
  {
      "login": {
          "username": "THE_USERNAME",
          "password": "THE_PASSWORD"
      }
  }
  ```

- 表單編碼有效負載類型 — 使用 HTML 表單名稱。

  例如，對於具有名為username1和輸入元素的 HTML 表單password1，使用者名稱欄位規格為username1且密碼欄位規格為password1。

d. 如果您要保護 Amazon CloudFront 分發，請在「回應檢查」下，指定應用程式如何在回應登入嘗試時表示成功或失敗。

> **Note**
>
> 可承諾量回應檢查僅適用於保護 CloudFront 分配的 Web ACL。

在登入回應中指定您要可承諾量檢查的單一元件。對於主體和 JSON 元件類型， AWS WAF 可以檢查元件的前 65,536 個位元組 (64 KB)。

提供元件類型的檢驗標準，如介面所示。您必須同時提供成功和失敗準則，才能在元件中進行檢查。

例如，假設您的應用程序在響應的狀態代碼中指示登錄嘗試的狀態，並用`200 OK`於成功和`/401 Unauthorized`或`403 Forbidden`失敗。您可以將回應檢查元件類型設定為狀態碼，然後在成功文字方塊中輸入，`200`並在失敗文字方塊中輸入`401`第一行，`403`在第二行輸入。

可承諾量規則群組只會計算符合成功或失敗檢驗條件的回應。規則群組規則會對用戶端採取行動，而這些規則群組規則在計數的回應中失敗率過高。為了確保規則群組規則的正確行為，請務必提供成功和失敗登入嘗試的完整資訊。

若要查看檢查登入回應的規則，請`VolumetricSessionFailedLoginResponseHigh`在列出的規則中尋找`VolumetricIpFailedLoginResponseHigh`和AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組。

3. 為規則群組提供任何您想要的其他組態。

   您可以在受管規則群組陳述式中新增範圍向下陳述式，進一步限制規則群組檢查的要求範圍。例如，您只能檢查具有特定查詢引數或 Cookie 的請求。規則群組只會檢查傳送至您指定登入端點的 HTTP POST 要求，而這些要求符合範圍向下陳述式中的準則。如需有關向下範圍陳述式的資訊，請參閱。範圍向下語句

4. 將您的變更儲存至網路 ACL。

在針對生產流量部署 ATP 實施之前，請先在測試或測試環境中對其進行測試和調整，直到您熟悉對流量的潛在影響為止。然後在啟用規則之前，使用生產流量在計數模式下測試和調整規則。如需指引，請參閱下一節。

測試和部署可承諾量

本節提供設定和測試網站 AWS WAF 詐騙控制帳戶接管預防 (ATP) 實作的一般指引。您選擇遵循的特定步驟將取決於您收到的需求、資源和 Web 要求。

此資訊是除了有關測試和調整的一般資訊之外，請參閱測試和調整您的 AWS WAF 保護。

> **Note**
>
> AWS 受管規則旨在保護您免受常見網頁威脅的侵害。根據文件使用時， AWS Managed Rules 規則群組會為您的應用程式新增另一層安全性。不過， AWS 受管規則群組並不是用來取代您的安全性責任，而這些責任是由您選取的 AWS 資源所決定。請參閱「共同責任模型」，以確保中的資源受到 AWS 適當的保護。

> **⚠ 生產流量風險**
>
> 在針對生產流量部署 ATP 實施之前，請先在測試或測試環境中對其進行測試和調整，直到您熟悉對流量的潛在影響為止。然後在啟用規則之前，使用生產流量在計數模式下測試和調整規則。

AWS WAF 提供測試證明資料，您可以用來驗證可承諾量組態。在下列程序中，您將設定測試 Web ACL 以使用可承諾量管理規則群組、設定規則以擷取規則群組新增的標籤，然後使用這些測試認證執行登入嘗試。您將通過檢查登錄嘗試的 Amazon CloudWatch 指標來驗證您的 Web ACL 已正確管理嘗試。

本指引適用於一般知道如何建立和管理 AWS WAF Web ACL、規則和規則群組的使用者。這些主題涵蓋在本指南之前的章節中。

設定與測試 AWS WAF 詐騙控制帳戶接管預防 (ATP) 實作

請先在測試環境中執行這些步驟，然後在生產環境中執行。

1. 在計數模式中新增 AWS WAF 詐騙控制帳戶接管預防 (ATP) 管理規則群組

   > **Note**
   >
   > 使用此受管規則群組時，會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

   將受 AWS 管規則規則群組新增`AWSManagedRulesATPRuleSet`至新的或現有的 Web ACL，並對其進行設定，使其不會改變目前的 Web ACL 行為。如需有關此規則群組之規則和標籤的詳細資訊，請參閱AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組。

   - 新增受管規則群組時，請加以編輯並執行下列動作：

- 在規則群組設定窗格中，提供應用程式登入頁面的詳細資料。可承諾量規則群組會使用此資訊來監視登入活動。如需詳細資訊，請參閱 將可承諾量管理規則群組新增至您的 Web ACL。
- 在「規則」窗格中，開啟「覆寫所有規則動作」下拉式清單並選擇Count。使用此設定時，AWS WAF 會根據規則群組中的所有規則評估要求，並僅計算結果的相符項目，同時仍將標籤新增至要求。如需詳細資訊，請參閱 覆寫規則群組中的規則動作。

  透過此覆寫，您可以監視可承諾量管理規則的潛在影響，以決定是否要新增例外，例如內部使用案例的例外。

- 定位規則群組，使其在 Web ACL 中的現有規則之後進行評估，其優先順序設定的數值高於您已經使用的任何規則或規則群組。如需詳細資訊，請參閱 Web ACL 中規則和規則群組的處理順序。

  如此一來，您目前的流量處理就不會中斷。例如，如果您有偵測惡意流量的規則，例如 SQL 插入或跨網站指令碼，他們將繼續偵測並記錄該流量。或者，如果您有允許已知非惡意流量的規則，它們可以繼續允許該流量，而不會讓 ATP 受管規則群組封鎖該流量。您可能會決定在測試和調整活動期間調整處理順序。

2. 啟用 Web ACL 的記錄和指標

   視需要設定網路 ACL 的記錄、Amazon 安全湖資料收集、請求取樣和 Amazon CloudWatch 指標。您可以使用這些可見度工具來監視可承諾量管理規則群組與流量的互動。

   - 如需有關配置和使用記錄的資訊，請參閱記錄 AWS WAF 網頁 ACL 流量。
   - 有關 Amazon 安全湖的信息，請參閱什麼是 Amazon 安全湖？ 以及從 Amazon 安全湖使用者指南中的 AWS 服務收集資料。
   - 如需 Amazon CloudWatch 指標的相關資訊，請參閱使用 Amazon 監控 CloudWatch。
   - 如需 Web 請求取樣的詳細資訊，請參閱檢視 Web 請求的範例。

3. 將網路 ACL 與資源建立關聯

   如果 Web ACL 尚未與測試資源相關聯，請將其關聯。如需相關資訊，請參閱建立 Web ACL 與資源的關聯或取消關聯 AWS。

4. 監控流量和 ATP 規則符合

   請確定正常流量正在流動，且可承諾量受管規則群組規則正在新增標籤至相符的 Web 請求。您可以在日誌中看到標籤，並在 Amazon 指標中查看 ATP 和標籤 CloudWatch 指標。在記錄檔中，您覆寫規則群組中要計數的規則會顯示在`action`設定為 count `ruleGroupList` 的規則中，並`overriddenAction`指示您覆寫的已設定規則動作。

5. 測試規則群組的認證檢查功能

   使用測試遭到入侵的認證執行登入嘗試，並檢查規則群組是否符合預期。

   a. 使用下列 AWS WAF 測試憑證組登入受保護資源的登入頁面：

      - 使用者：`WAF_TEST_CREDENTIAL@wafexample.com`
      - 密碼：`WAF_TEST_CREDENTIAL_PASSWORD`

      這些測試認證會歸類為遭到入侵的認證，而且可承諾量管理規則群組會將`awswaf:managed:aws:atp:signal:credential_compromised`標籤新增至登入要求，您可以在記錄檔中看到這些標籤。

   b. 在您的 Web ACL 日誌中，在測試登錄 Web 請求的日誌條目的`labels`字段中查找`awswaf:managed:aws:atp:signal:credential_compromised`標籤。如需日誌記錄的相關資訊，請參閱記錄 AWS WAF 網頁 ACL 流量。

   確認規則群組如預期擷取遭到入侵的認證之後，您可以根據受保護的資源所需採取步驟來設定其實作。

6. 對於 CloudFront 發行版，請測試規則群組的登入失敗管理

   a. 針對您為可承諾量規則群組設定的每個失敗回應條件，執行測試。測試之間至少等待 10 分鐘。

      若要測試單一失敗條件，請在回應中識別將以該條件失敗的登入嘗試。然後，從單一用戶端 IP 位址，在 10 分鐘內執行至少 10 次失敗的登入嘗試。

      在前 6 次失敗之後，容積失敗的登入規則應該會開始對其餘嘗試進行比對，並加上標籤和計數。由於延遲，規則可能會錯過前一個或兩個規則。

   b. 在您的 Web ACL 日誌中，在測試登錄 Web 請求的日誌條目的`labels`字段中查找`awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:hig`標籤。如需日誌記錄的相關資訊，請參閱記錄 AWS WAF 網頁 ACL 流量。

   這些測試會檢查失敗的登入計數是否超過規則的閾值，以驗證失敗準則`VolumetricIpFailedLoginResponseHigh`是否符合您的回應。達到閾值之後，如果您繼續從相同的 IP 位址傳送登入要求，規則將會繼續符合，直到失敗率降至閾值以下為止。當超過臨界值時，規則會同時符合從 IP 位址登入成功或失敗的登入。

7. 自訂可承諾量 Web 請求處理

   視需要新增明確允許或封鎖請求的自己規則，以變更可承諾量規則處理這些請求的方式。

   例如，您可以使用可承諾量標籤來允許或封鎖請求，或自訂請求處理。您可以在可承諾量管理規則群組之後新增標籤比對規則，以篩選您要套用之處理的標籤請求。測試之後，請將相關的可承諾量規則保持為盤點模式，並在自訂規則中維護請求處理決策。如需範例，請參閱可承諾量範例：遺失與遭到入侵之認證的自訂處。

8. 移除測試規則並啟用可承諾量管理規則群組設定

   視您的情況而定，您可能已決定要將某些可承諾量規則保留為盤點模式。針對您要在規則群組內設定執行的規則，請停用 Web ACL 規則群組組態中的計數模式。完成測試後，您也可以移除測試標籤比對規則。

9. 監控和調整

   若要確定 Web 請求能夠依照您的需求處理，請在啟用要使用的可承諾量功能之後，密切監視您的流量。使用規則群組上的規則計數覆寫，並使用您自己的規則，視需要調整行為。

在您完成測試 ATP 規則群組實作之後，如果您尚未這麼做，我們強烈建議您將 AWS WAF JavaScript SDK 整合至瀏覽器登入頁面，以增強偵測功能。 AWS WAF 還提供移動軟件開發套件，以集成 iOS 和安卓設備。如需整合 SDK 的詳細資訊，請參閱AWS WAF 用戶端應用整合。如需有關此建議的資訊，請參閱為什麼您應該將應用程式整合 SDK 與 ATP 搭配使用。

AWS WAF 防止詐騙控制帳戶接管 (ATP) 範例

本節顯示符合 AWS WAF 詐騙控制帳戶接管預防 (ATP) 實作之常見使用案例的範例組態。

每個範例都會提供使用案例的說明，然後在 JSON 清單中顯示自訂設定規則的解決方案。

> **Note**
>
> 您可以透過主控台 Web ACL JSON 下載或規則 JSON 編輯器，或透過 API 和命令列介面中的`getWebACL`作業擷取 JSON 清單，如這些範例所示。

主題

- 可承諾量範例：簡單組態
- 可承諾量範例：遺失與遭到入侵之認證的自訂處

- 可承諾量範例：回應檢驗組態

可承諾量範例：簡單組態

下列 JSON 清單顯示具有 AWS WAF 詐騙控制帳戶接管預防 (ATP) 受管規則群組的 Web ACL 範例。請注意其他登入頁面設定，這會提供規則群組監視和管理登入要求所需的資訊。此 JSON 包含 Web ACL 自動產生的設定，例如標籤命名空間和 Web ACL 的應用程式整合 URL。

```
{
    "WebACL": {
        "LabelNamespace": "awswaf:111122223333:webacl:ATPModuleACL:",
        "Capacity": 50,
        "Description": "This is a test web ACL for ATP.",
        "Rules": [
            {
                "Priority": 1,
                "OverrideAction": {
                    "None": {}
                },
                "VisibilityConfig": {
                    "SampledRequestsEnabled": true,
                    "CloudWatchMetricsEnabled": true,
                    "MetricName": "AccountTakeOverValidationRule"
                },
                "Name": "DetectCompromisedUserCredentials",
                "Statement": {
                    "ManagedRuleGroupStatement": {
                        "VendorName": "AWS",
                        "Name": "AWSManagedRulesATPRuleSet",
                        "ManagedRuleGroupConfigs": [
                          {
                            "AWSManagedRulesATPRuleSet": {
                              "LoginPath": "/web/login",
                              "RequestInspection": {
                                "PayloadType": "JSON",
                                "UsernameField": {
                                  "Identifier": "/form/username"
                                },
                                "PasswordField": {
                                  "Identifier": "/form/password"
                                }
                              },
```

```
                            "EnableRegexInPath": false
                        }
                    }
                ]
            }
        }
    ],
    "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "ATPValidationAcl"
    },
    "DefaultAction": {
        "Allow": {}
    },
    "ManagedByFirewallManager": false,
    "Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
    "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
    "Name": "ATPModuleACL"
},
"ApplicationIntegrationURL": "https://9z87abce34ea.us-
east-1.sdk.awswaf.com/9z87abce34ea/1234567a1b10/",
"LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}
```

可承諾量範例：遺失與遭到入侵之認證的自訂處

根據預設，規則群組執行的認證檢查AWSManagedRulesATPRuleSet處理 Web 要求，如下所示：

- 遺失認證 — 標籤和封鎖要求。
- 受損的憑據 — 標籤請求，但不要阻止或計算它。

如需有關規則群組和規則行為的詳細資訊，請參閱AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組。

您可以執行下列動作，針對遺失或遭到入侵認證的 Web 要求新增自訂處理：

- 將**MissingCredential**規則覆寫為 Count — 此規則動作覆寫會導致規則僅計數和標籤相符請求。
- 使用自訂處理新增標籤比對規則 — 設定此規則以符合兩個可承諾量標籤，並執行您的自訂處理。例如，您可以將客戶重新導向至您的註冊頁面。

下列規則顯示先前範例中的可承諾量管理規則群組，其中MissingCredential規則作業已覆寫為計數。這會導致規則將其標籤應用於匹配的請求，然後僅計算請求，而不是阻止它們。

```
"Rules": [
    {
        "Priority": 1,
        "OverrideAction": {
            "None": {}
        },
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "AccountTakeOverValidationRule"
        },
        "Name": "DetectCompromisedUserCredentials",
        "Statement": {
            "ManagedRuleGroupStatement": {
                "ManagedRuleGroupConfigs": [
                  {
                    "AWSManagedRulesATPRuleSet": {
                      "LoginPath": "/web/login",
                      "RequestInspection": {
                        "PayloadType": "JSON",
                        "UsernameField": {
                          "Identifier": "/form/username"
                        },
                        "PasswordField": {
                          "Identifier": "/form/password"
                        }
                      },
                      "EnableRegexInPath": false
                    }
                  }
                ]
                "VendorName": "AWS",
                "Name": "AWSManagedRulesATPRuleSet",
                "RuleActionOverrides": [
                  {
                    "ActionToUse": {
                      "Count": {}
                    },
                    "Name": "MissingCredential"
                  }
```

```
                ],
                "ExcludedRules": []
            }
        }
    }
],
```

使用此配置時，當此規則組評估任何缺少或洩露憑據的 Web 請求時，它將標記該請求，但不會阻止它。

下列規則的優先順序設定高於前一個規則群組的數值。 AWS WAF 以數字順序評估規則 (從最低值開始)，因此會在規則群組評估之後評估此規則。此規則設定為符合任一認證標籤，並傳送相符要求的自訂回應。

```
"Name": "redirectToSignup",
      "Priority": 10,
      "Statement": {
        "OrStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:atp:signal:missing_credential"
              }
            },
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:atp:signal:credential_compromised"
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {
          "CustomResponse": {
             your custom response settings
          }
        }
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
```

```
        "CloudWatchMetricsEnabled": true,
        "MetricName": "redirectToSignup"
      }
```

可承諾量範例：回應檢驗組態

下列 JSON 清單顯示範例 Web ACL，其中包含設定為檢查原始回應的 AWS WAF 詐騙控制帳戶接管 (ATP) 受管理規則群組。請注意響應檢查配置，該配置指定成功和響應狀態代碼。您也可以根據標題、內文和內文 JSON 相符項目來設定成功和回應設定。此 JSON 包含 Web ACL 自動產生的設定，例如標籤命名空間和 Web ACL 的應用程式整合 URL。

> **Note**
>
> 可承諾量回應檢查僅適用於保護 CloudFront 分配的 Web ACL。

```
{
    "WebACL": {
        "LabelNamespace": "awswaf:111122223333:webacl:ATPModuleACL:",
        "Capacity": 50,
        "Description": "This is a test web ACL for ATP.",
        "Rules": [
            {
                "Priority": 1,
                "OverrideAction": {
                    "None": {}
                },
                "VisibilityConfig": {
                    "SampledRequestsEnabled": true,
                    "CloudWatchMetricsEnabled": true,
                    "MetricName": "AccountTakeOverValidationRule"
                },
                "Name": "DetectCompromisedUserCredentials",
                "Statement": {
                    "ManagedRuleGroupStatement": {
                        "VendorName": "AWS",
                        "Name": "AWSManagedRulesATPRuleSet",
                        "ManagedRuleGroupConfigs": [
                          {
                            "AWSManagedRulesATPRuleSet": {
                              "LoginPath": "/web/login",
```

```
                            "RequestInspection": {
                              "PayloadType": "JSON",
                              "UsernameField": {
                                "Identifier": "/form/username"
                              },
                              "PasswordField": {
                                "Identifier": "/form/password"
                              }
                            },
                            "ResponseInspection": {
                              "StatusCode": {
                                "SuccessCodes": [
                                  200
                                ],
                                "FailureCodes": [
                                  401
                                ]
                              }
                            },
                            "EnableRegexInPath": false
                          }
                        }
                    ]
                }
            }
        ],
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "ATPValidationAcl"
        },
        "DefaultAction": {
            "Allow": {}
        },
        "ManagedByFirewallManager": false,
        "Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
        "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
        "Name": "ATPModuleACL"
    },
    "ApplicationIntegrationURL": "https://9z87abce34ea.us-
east-1.sdk.awswaf.com/9z87abce34ea/1234567a1b10/",
    "LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
```

```
}
```

AWS WAF 機器人控制

借助 Bot Control，您可以輕鬆監控，阻止或速率限制機器人，例如抓取器，掃描器，爬蟲程序，狀態監視器和搜索引擎。如果您使用規則組的目標檢查級別，則還可以挑戰無法自我識別的機器人，從而使惡意漫遊器對您的網站進行操作變得更加困難和更昂貴。您可以單獨使用 Bot Control 受管規則群組，或與其他受 AWS 管規則群組和您自己的自訂 AWS WAF 規則結合使用來保護您的應用程式。

Bot Control 包含一個主控台儀表板，根據請求取樣顯示您目前來自機器人的流量量。將 Bot Control 受管規則群組新增至 Web ACL 後，您就可以針對機器人流量採取行動，並接收有關進入應用程式的常見機器人流量的詳細即時資訊。

> **Note**
>
> 使用此受管規則群組時，會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

Bot Control 受管規則群組提供基本的通用保護層級，可將標籤新增至自我識別機器人、驗證一般需要的機器人，以及偵測高信賴度的機器人簽章。這使您能夠監控和控制常見類別的機器人流量。

機器人控制規則群組也提供目標保護層級，可針對無法自我識別的複雜機器人新增偵測功能。目標式保護會使用瀏覽器詢問、指紋識別和行為啟發式等偵測技術來識別不良的機器人流量。此外，有針對性的保護功能可針對網站流量統計資料提供選用的自動機器學習分析，以偵測機器人相關活動 啟用機器學習時， AWS WAF 會使用有關網站流量的統計資料 (例如時間戳記、瀏覽器特性和先前造訪的 URL) 來改善 Bot Control 機器學習模型。

如需機器人控制受管規則群組的詳細資訊，請參閱AWS WAF 機器人控制規則群組。

針對 Bot Control 受管理規則群組 AWS WAF 評估 Web 要求時，規則群組會將標籤新增至偵測為機器人相關的請求，例如機器人類別和機器人名稱。您可以在自己的 AWS WAF 規則中匹配這些標籤以自定義處理。由機器人控制受管規則群組產生的標籤會包含在 Amazon CloudWatch 指標和 Web ACL 日誌中。

您也可以使用 AWS Firewall Manager AWS WAF 原則，將 Bot Control 受管規則群組部署到您組織中的多個帳戶中的應用程式 AWS Organizations。

AWS WAF 機器人控制元件

Bot Control 實作的主要元件如下：

- **AWSManagedRulesBotControlRuleSet**— 機器人控制受管理規則群組，其規則會偵測並處理不同類別的機器人。此規則群組會將標籤新增至偵測為機器人流量的 Web 要求。

  > **Note**
  >
  > 使用此受管規則群組時，會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

  Bot Control 受管規則群組提供兩種保護層級，您可以從中選擇：

  - 常見 — 檢測各種自我識別機器人，例如 Web 抓取框架，搜索引擎和自動瀏覽器。此層級的機器人控制保護可使用傳統機器人偵測技術 (例如靜態要求資料分析) 來識別常見的機器人。規則會標記來自這些機器人的流量，並封鎖他們無法驗證的機器人。
  - 目標 — 包括共同層級保護，並針對無法自我識別的複雜機器人新增目標式偵測。有針對性的保護結合使用速率限制、CAPTCHA 以及背景瀏覽器挑戰來減輕機器人活動。
    - **TGT_**— 提供目標保護的規則名稱開頭為TGT_。所有目標保護都使用檢測技術（例如瀏覽器審訊，指紋識別和行為啟發式法）來識別不良的機器人流量。
    - **TGT_ML_**— 使用機器學習的目標保護規則的名稱開頭為TGT_ML_。這些規則使用網站流量統計資料的自動化機器學習分析，以偵測指示分散式協調機器人活動的異常行為。 AWS WAF 分析有關您網站流量的統計資料，例如時間戳記、瀏覽器特性和先前造訪的 URL，以改善 Bot Control 機器學習模型。機器學習功能預設為啟用，但您可以在規則群組設定中停用它們。停用機器學習時， AWS WAF 不會評估這些規則。

  如需包括規則群組規則的詳細資訊，請參閱AWS WAF 機器人控制規則群組。

  您可以使用受管規則群組參考陳述式，並指出您要使用的檢查層級，將此規則群組包含在 Web ACL 中。針對目標層級，您也會指出是否要啟用機器學習。如需有關將此受管規則群組新增至 Web ACL 的詳細資訊，請參閱將 AWS WAF 機器人控制受管規則群組新增至您的 Web ACL。

- 機器人控制儀表板 — Web ACL 的機器人監控儀表板，可透過 Web ACL 機器人控制索引標籤取得。使用此儀表板監控您的流量，並了解其中有多少來自各種類型的漫遊器。這可以是自訂機器人管理的起點，如本主題所述。您還可以使用它來驗證您的更改並監視各種漫遊器和機器人類別的活動。
- JavaScript 和行動應用程式整合 SDK — 如果您使用 Bot Control 規則群組的目標保護層級，則應該實作 AWS WAF JavaScript 和行動 SDK。目標規則使用客戶端令牌中 SDK 提供的信息，以增強對惡意漫遊器的檢測。如需 SDK 的詳細資訊，請參閱「AWS WAF 用戶端應用整合」。
- 記錄和指標 — 透過研究 AWS WAF 日誌、Amazon Security Lake 和 Amazon 為 Web ACL 收集的資料，您可以監控機器人流量並了解機器人控制受管規則群組如何評估和處理您的流量 CloudWatch。Bot Control 新增至您的網頁要求的標籤會包含在資料中。如需有關這些選項的資訊記

錄 AWS WAF 網頁 ACL 流量，請參閱使用 Amazon 監控 CloudWatch、和什麼是 Amazon 安全湖？。

根據您的需求和看到的流量，您可能想要自訂 Bot Control 實作。以下是一些最常用的選項。

- ScopeDlow 陳述式 — 您可以在 Bot Control 受管理規則群組參考陳述式中新增一個範圍向下陳述式，從 Bot Control 受管理規則群組評估的 Web 要求中排除部分流量。範圍向下語句可以是任何嵌套的規則語句。當要求與 scopelow 陳述式不符時， AWS WAF 會將其評估為不符合規則群組參考陳述式，而不會針對規則群組進行評估。如需有關向下範圍陳述式的詳細資訊，請參閱。範圍向下語句

  Bot Control 受管規則群組的定價會隨著使用該群組進行 AWS WAF 評估的 Web 請求數量而增加。您可以使用範圍向下陳述式來限制規則群組評估的要求，協助降低這些成本。例如，您可能想要允許每個人 (包括機器人) 載入首頁，然後將規則群組規則套用至要傳送至應用程式 API 或包含特定內容類型的要求。

- 標籤和標籤比對規則 — 您可以自訂機器人控制規則群組如何處理使用 AWS WAF 標籤比對規則陳述式識別的某些機器人流量。機器人控制規則群組會將標籤新增至您的 Web 請求。您可以在「機器人控制」標籤上符合的「機器人控制」規則群組後新增標籤比對規則，並套用您需要的處理方式。若要取得有關標示和使用標籤比對陳述式的詳細資訊，請參閱標籤比對規則陳述式和AWS WAF 標籤, 上, 网, 請求。
- 自訂請求和回應 — 您可以將自訂標頭新增至您允許的請求，也可以透過將標籤符合與自訂請求和回應功能配對，針對您封鎖的請求傳送 AWS WAF 自訂回應。如需自訂請求和回應的詳細資訊，請參閱定制的 Web 請求和響應 AWS WAF。

為什麼您應該使用應用程式整合 SDK 搭配機器人控制

Bot Control 受管規則群組的大多數目標保護都需要應用程式整合 SDK 所產生的挑戰權杖。請求中不需要挑戰權杖的規則為 Bot Control 共同層級保護和目標層級機器學習規則。如需規則群組中保護層級和規則的說明，請參閱AWS WAF 機器人控制規則群組。

我們強烈建議您實作應用程式整合 SDK，以便最有效地使用機器人控制規則群組。挑戰指令碼必須在 Bot Control 規則群組之前執行，規則群組才能從指令碼取得的權杖中受益。

- 透過應用程式整合 SDK，指令碼會自動執行。
- 如果您無法使用 SDK，您可以設定 Web ACL，使其針對將由 Bot Control CAPTCHA 規則群組檢查的所有要求執行Challenge或規則動作。使用Challenge或CAPTCHA規則動作可能會產生額外費用。如需定價詳細資訊，請參閱 AWS WAF 定價。

當您在用戶端中實作應用程式整合 SDK 或使用其中一個執行挑戰指令碼的規則動作時，您可以擴充規則群組和整體用戶端應用程式安全性的功能。

令牌為每個 Web 請求提供客戶端信息。此額外資訊可讓 Bot Control 規則群組將合法的用戶端工作階段與行為不良的用戶端工作階段分開，即使兩者都來自單一 IP 位址也是如此。規則群組會使用 Token 中的資訊來彙總用戶端工作階段要求行為，以進行目標防護層級所提供的微調偵測和緩和措施。

如需 SDK 的相關資訊，請參閱AWS WAF 用戶端應用整合。如需有關 AWS WAF 權杖的資訊，請參閱AWS WAF 網絡請求令牌。如需有關規則動作的資訊，請參閱CAPTCHA並Challenge在 AWS WAF。

將 AWS WAF 機器人控制受管規則群組新增至您的 Web ACL

Bot Control 受管理規則群組`AWSManagedRulesBotControlRuleSet`需要其他設定，才能識別您要實作的保護層級。

如需規則群組說明與規則清單，請參閱AWS WAF 機器人控制規則群組。

本指引適用於一般知道如何建立和管理 AWS WAF Web ACL、規則和規則群組的使用者。這些主題涵蓋在本指南之前的章節中。如需如何將受管規則群組新增至 Web ACL 的基本資訊，請參閱透過主控台將受管規則群組新增至 Web ACL。

遵循最佳做法

請依照上的最佳做法使用機器人控制規則群組智慧型威脅緩解的最佳做法。

若要在 Web ACL 中使用**`AWSManagedRulesBotControlRuleSet`**規則群組

1. 將受 AWS 管規則群組新增`AWSManagedRulesBotControlRuleSet`至您的 Web ACL。如需完整規則群組描述，請參閱the section called “機器人控制規則群組”。

   > **Note**
   >
   > 使用此受管規則群組時，會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

   新增規則群組時，請對其進行編輯，以開啟規則群組的配置頁面。
2. 在規則群組的組態頁面的 [檢驗層級] 窗格中，選取您要使用的檢驗層級。

- 常見 — 檢測各種自我識別機器人，例如 Web 抓取框架，搜索引擎和自動瀏覽器。此層級的機器人控制保護可使用傳統機器人偵測技術 (例如靜態要求資料分析) 來識別常見的機器人。規則會標記來自這些機器人的流量，並封鎖他們無法驗證的機器人。
- 目標 — 包括共同層級保護，並針對無法自我識別的複雜機器人新增目標式偵測。有針對性的保護結合使用速率限制、CAPTCHA 以及背景瀏覽器挑戰來減輕機器人活動。
  - **TGT_**— 提供目標保護的規則名稱開頭為TGT_。所有目標保護都使用檢測技術（例如瀏覽器審訊，指紋識別和行為啟發式法）來識別不良的機器人流量。
  - **TGT_ML_**— 使用機器學習的目標保護規則的名稱開頭為TGT_ML_。這些規則使用網站流量統計資料的自動化機器學習分析，以偵測指示分散式協調機器人活動的異常行為。 AWS WAF 分析有關您網站流量的統計資料，例如時間戳記、瀏覽器特性和先前造訪的 URL，以改善 Bot Control 機器學習模型。機器學習功能預設為啟用，但您可以在規則群組設定中停用它們。停用機器學習時， AWS WAF 不會評估這些規則。

3. 如果您使用的是目標防護層級，而且不想 AWS WAF 使用機器學習 (ML) 來分析網路流量以進行分散式協調的機器人活動，請停用機器學習選項。名稱以開頭的機器人控制規則需要機器學習TGT_ML_。如需這些規則的詳細資訊，請參閱機器人控制規則清單。
4. 新增規則群組的向下範圍陳述式，以包含使用該規則群組的成本。範圍向下陳述式會縮小規則群組檢查的要求集。例如使用案例，請以機器人控制範例：僅針對登入頁面使用機器人控制和開頭機器人控制範例：僅針對動態內容使用機器人控制。
5. 提供規則群組所需的任何其他組態。
6. 將您的變更儲存至網路 ACL。

在針對生產流量部署 Bot Control 實作之前，請先在測試或測試環境中對其進行測試和調整，直到您熟悉對流量的潛在影響為止。然後在啟用規則之前，使用生產流量在計數模式下測試和調整規則。如需指引，請參閱下列各節。

利用 AWS WAF 機器人控制誤報

我們已仔細選取「 AWS WAF 機器人控制」管理規則群組中的規則，以盡量減少誤判。我們針對全球流量測試規則，並監控其對測試 Web ACL 的影響。但是，由於流量模式的變化，仍然有可能獲得誤報。此外，已知某些使用案例會導致誤報，並且需要針對您的 Web 流量進行自訂。

您可能會遇到誤報的情況包括：

- 行動應用程式通常具有非瀏覽器使用者代理程式，依預設會封鎖SignalNonBrowserUserAgent規則。如果您預期來自行動應用程式的流量，或任何其他非瀏覽器使用者代理程式的合法流量，則需要新增例外狀況才能允許。

- 您可能依賴某些特定的機器人流量來執行正常運行時間監控，集成測試或營銷工具。如果 Bot Control 識別並封鎖您要允許的機器人流量，您需要透過新增自己的規則來變更處理方式。雖然這不是所有客戶的誤報情況，但如果適合您，則需要處理與誤報相同的方式。
- 機器人控制受管規則群組會使用來自的 IP 位址來 AWS WAF驗證機器人。如果您使用 Bot Control，且已驗證透過 Proxy 或負載平衡器路由的機器人，則可能需要使用自訂規則明確允許這些機器人。如需如何建立此類型自訂規則的相關資訊，請參閱轉送的 IP 位址。
- 具有低全域誤判率的機器人控制規則可能會嚴重影響特定裝置或應用程式。例如，在測試和驗證中，我們可能沒有觀察到來自低流量的應用程序或來自不常見的瀏覽器或設備的請求。
- 歷史上誤判率較低的機器人控制規則可能會增加有效流量的誤判率。這可能是由於新的流量模式或請求屬性隨有效流量出現，導致其與以前沒有的規則相符。這些變更可能是由於下列情況所造成：
  - 流量詳細資料會隨著流量透過網路應用裝置 (例如負載平衡器或內容分發網路 (CDN) 而變更。
  - 流量數據的新變化，例如新瀏覽器或現有瀏覽器的新版本。

如需如何處理您可能從 AWS WAF Bot Control 受管理規則群組取得的誤判情形的詳細資訊，請參閱下一節中的指引。測試和部署 AWS WAF 機器人控制

測試和部署 AWS WAF 機器人控制

本節提供設定和測試網站的 AWS WAF Bot Control 實作的一般指引。您選擇遵循的特定步驟將取決於您的需求、資源和您收到的 Web 要求。

此資訊是除了有關測試和調整的一般資訊之外，請參閱測試和調整您的 AWS WAF 保護。

> **Note**
>
> AWS 受管規則旨在保護您免受常見網頁威脅的侵害。根據文件使用時， AWS Managed Rules 規則群組會為您的應用程式新增另一層安全性。不過， AWS 受管規則群組並不是用來取代您的安全性責任，而這些責任是由您選取的 AWS 資源所決定。請參閱「共同責任模型」，以確保中的資源受到 AWS 適當的保護。

> **生產流量風險**
>
> 在針對生產流量部署 Bot Control 實作之前，請先在測試或測試環境中對其進行測試和調整，直到您熟悉對流量的潛在影響為止。然後在啟用規則之前，使用生產流量在計數模式下測試和調整規則。

本指引適用於一般知道如何建立和管理 AWS WAF Web ACL、規則和規則群組的使用者。這些主題涵蓋在本指南之前的章節中。

設定和測試機器人控制實作

請先在測試環境中執行這些步驟，然後在生產環境中執行。

1. 新增機器人控制受管規則群組

> **Note**
>
> 使用此受管規則群組時，會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

將受管 AWS 規則群組新增`AWSManagedRulesBotControlRuleSet`至新的或現有的 Web ACL，並對其進行設定，使其不會改變目前的 Web ACL 行為。

- 新增受管規則群組時，請加以編輯並執行下列動作：
  - 在「檢驗層次」窗格中，選取您要使用的檢驗層次。
    - 常見 — 檢測各種自我識別機器人，例如 Web 抓取框架，搜索引擎和自動瀏覽器。此層級的機器人控制保護可使用傳統機器人偵測技術 (例如靜態要求資料分析) 來識別常見的機器人。規則會標記來自這些機器人的流量，並封鎖他們無法驗證的機器人。
    - 目標 — 包括共同層級保護，並針對無法自我識別的複雜機器人新增目標式偵測。有針對性的保護結合使用速率限制、CAPTCHA 以及背景瀏覽器挑戰來減輕機器人活動。
      - **`TGT_`**— 提供目標保護的規則名稱開頭為`TGT_`。所有目標保護都使用檢測技術（例如瀏覽器審訊，指紋識別和行為啟發式法）來識別不良的機器人流量。
      - **`TGT_ML_`**— 使用機器學習的目標保護規則的名稱開頭為`TGT_ML_`。這些規則使用網站流量統計資料的自動化機器學習分析，以偵測指示分散式協調機器人活動的異常行為。AWS WAF 分析有關您網站流量的統計資料，例如時間戳記、瀏覽器特性和先前造訪的 URL，以改善 Bot Control 機器學習模型。機器學習功能預設為啟用，但您可以在規則群組設定中停用它們。停用機器學習時， AWS WAF 不會評估這些規則。

    如需有關此選擇的詳細資訊，請參閱AWS WAF 機器人控制規則群組。
  - 在「規則」窗格中，開啟「覆寫所有規則動作」下拉式清單並選擇Count。使用此設定時，AWS WAF 會根據規則群組中的所有規則評估要求，並僅計算結果的相符項目，同時仍將標籤新增至要求。如需詳細資訊，請參閱 覆寫規則群組中的規則動作。

透過此覆寫，您可以監控機器人控制規則對流量的潛在影響，以判斷是否要為內部使用案例或所需機器人等新增例外狀況。

- 定位規則群組，使其在 Web ACL 中最後評估，其優先順序設定的數值高於您正在使用的任何其他規則或規則群組。如需詳細資訊，請參閱 Web ACL 中規則和規則群組的處理順序。

  如此一來，您目前的流量處理就不會中斷。例如，如果您有可偵測惡意流量的規則，例如 SQL 插入或跨網站指令碼，它們將繼續偵測並記錄這些要求。或者，如果您有允許已知非惡意流量的規則，它們可以繼續允許該流量，而不會讓 Bot Control 受管理規則群組封鎖該流量。您可能會決定在測試和調整活動期間調整處理順序，但這是一個很好的開始方法。

2. 啟用 Web ACL 的記錄和指標

   視需要設定網路 ACL 的記錄、Amazon 安全湖資料收集、請求取樣和 Amazon CloudWatch 指標。您可以使用這些可見度工具來監控 Bot Control 受管理規則群組與流量的互動情況。

   - 如需日誌記錄的相關資訊，請參閱記錄 AWS WAF 網頁 ACL 流量。
   - 有關 Amazon 安全湖的信息，請參閱什麼是 Amazon 安全湖？ 以及從 Amazon 安全湖使用者指南中的 AWS 服務收集資料。
   - 如需 Amazon CloudWatch 指標的相關資訊，請參閱使用 Amazon 監控 CloudWatch。
   - 如需 Web 請求取樣的詳細資訊，請參閱檢視 Web 請求的範例。

3. 將網路 ACL 與資源建立關聯

   如果 Web ACL 尚未與資源相關聯，請將其關聯。如需相關資訊，請參閱建立 Web ACL 與資源的關聯或取消關聯 AWS。

4. 監控流量和機器人控制規則符合

   請確定流量正在流動，且 Bot Control 受管理規則群組規則正在新增標籤至相符的 Web 要求。您可以在日誌中看到標籤，並在 Amazon 指標中查看機器人和標籤 CloudWatch 指標。在記錄檔中，您覆寫規則群組中要計數的規則會顯示在`action`設定為 count `ruleGroupList` 的規則中，並`overriddenAction`指示您覆寫的已設定規則動作。

   > **Note**
   >
   > 機器人控制受管規則群組會使用來自的 IP 位址來 AWS WAF驗證機器人。如果您使用 Bot Control，且已驗證透過 Proxy 或負載平衡器路由的機器人，則可能需要使用自訂規則明確允許這些機器人。若要取得有關如何建立自訂規則的資訊，請參閱〈轉送的 IP 位址。如需如何使用規則自訂 Bot Control Web 要求處理的相關資訊，請參閱下一個步驟。

請仔細檢閱 Web 要求處理，找出您可能需要透過自訂處理來緩解的任何誤報。如需誤報的範例，請參閱利用 AWS WAF 機器人控制誤報。

5. 自訂機器人控制網頁要求處理

   視需要新增明確允許或封鎖要求的自己規則，以變更 Bot Control 規則處理這些要求的方式。

   您如何執行此操作取決於您的使用案例，但以下是常見的解決方案：

   - 明確允許包含您在 Bot Control 受管理規則群組之前新增之規則的要求。如此一來，允許的要求永遠不會送達規則群組進行評估。這有助於控制使用機器人控制受管規則群組的成本。
   - 透過在 Bot Control 受管規則群組陳述式中新增範圍陳述式，以排除 Bot Control 評估的要求。此功能與前面的選項相同。它有助於控制使用 Bot Control 受管規則群組的成本，因為與範圍向下陳述式不符的要求永遠不會達到規則群組評估。如需有關向下範圍陳述式的資訊，請參閱。範圍向下語句

     如需 範例，請參閱下方：

     - 從機器人管理中排除 IP 範圍
     - 允許來自您控制的機器人的流量
   - 在要求處理中使用機器人控制標籤來允許或封鎖要求。在 Bot Control 受管理規則群組之後新增標籤比對規則，以篩選出您要允許來自您要封鎖的請求的標籤請求。

     測試之後，請將相關的機器人控制規則保持在計數模式中，並在自訂規則中維護要求處理決策。如需標籤比對陳述式的資訊，請參閱標籤比對規則陳述式。

     如需此類型自訂的範例，請參閱下列內容：

     - 為封鎖的使用者代理程式建立例外
     - 允許特定的封鎖機器人
     - 封鎖驗證機器人

   如需額外的範例，請參閱AWS WAF 機器人控制範例。

6. 視需要啟用機器人控制受管規則群組設定

   根據您的情況，您可能已決定要將某些機器人控制規則保留在計數模式或使用不同的動作覆寫。對於您希望在規則群組中設定時執行的規則，請啟用一般規則組態。若要這麼做，請在 Web ACL 中編輯規則群組陳述式，並在「規則」窗格中進行變更。

AWS WAF 機器人控制範例

本節顯示符合 AWS WAF Bot Control 實作之各種常見使用案例的範例組態。

每個範例都會提供使用案例的說明，然後在 JSON 清單中顯示自訂設定規則的解決方案。

> **Note**
>
> 這些範例中顯示的 JSON 清單是在主控台中設定規則，然後使用規則 JSON 編輯器進行編輯來建立。

主題

機器人控制範例：簡單的設定

下列 JSON 清單顯示具有 AWS WAF 機器人控制受管規則群組的網頁 ACL 範例。請注意可見性組態，這會導致儲存 AWS WAF 要求範例和量度以供監視用途。

```
{
  "Name": "Bot-WebACL",
  "Id": "...",
  "ARN": "...",
  "DefaultAction": {
    "Allow": {}
```

```
  },
  "Description": "Bot-WebACL",
  "Rules": [
      {
        ...
      },
      {
         "Name": "AWS-AWSBotControl-Example",
         "Priority": 5,
         "Statement": {
            "ManagedRuleGroupStatement": {
               "VendorName": "AWS",
               "Name": "AWSManagedRulesBotControlRuleSet",
               "ManagedRuleGroupConfigs": [
                 {
                   "AWSManagedRulesBotControlRuleSet": {
                     "InspectionLevel": "COMMON"
                   }
                 }
               ],
               "RuleActionOverrides": [],
               "ExcludedRules": []
            },
            "VisibilityConfig": {
               "SampledRequestsEnabled": true,
               "CloudWatchMetricsEnabled": true,
               "MetricName": "AWS-AWSBotControl-Example"
             }
          }
      }
    ],
    "VisibilityConfig": {
      ...
    },
    "Capacity": 1496,
    "ManagedByFirewallManager": false
}
```

機器人控制範例：明確允許經過驗證的

AWS WAF 機器人控制不會阻止已知為常見且可驗證的機器人。 AWS 當機器人控制將 Web 請求識別為來自經過驗證的機器人時，它會添加一個標籤，用於命名該機器人和一個標籤，表示它是經過驗證的機器人。Bot Control 不會添加任何其他標籤，例如信號標籤，以防止已知的良好機器人被阻止。

您可能有其他阻止驗證機器人的 AWS WAF 規則。如果您想確保允許經過驗證的機器人，請新增自訂規則，以根據機器人控制標籤允許這些機器人。您的新規則必須在 Bot Control 受管理規則群組之後執行，以便標籤可供比對。

下列規則明確允許已驗證的機器人。

```
{
    "Name": "match_rule",
    "Statement": {
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:bot-control:bot:verified"
      }
    },
    "RuleLabels": [],
    "Action": {
      "Allow": {}
    }
}
```

機器人控制範例：封鎖驗證機器人

若要封鎖已驗證的機器人，您必須新增規則來封鎖在 AWS WAF Bot Control 受管理規則群組之後執行的規則。為此，請識別要阻止的機器人名稱，然後使用標籤匹配語句來識別和阻止它們。如果您只想阻止所有經過驗證的漫遊器，則可以省略與`bot:name:`標籤相匹配的匹配項。

下列規則只會封鎖`bingbot`已驗證的機器人。此規則必須在「機器人控制」受管理規則群組之後執行。

```
{
    "Name": "match_rule",
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:bot:name:bingbot"
            }
          },
          {
            "LabelMatchStatement": {
```

```
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:bot:verified"
            }
          }
        ]
      }
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    }
  }
```

以下規則會封鎖所有已驗證的機器人。

```
{
    "Name": "match_rule",
    "Statement": {
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:bot-control:bot:verified"
      }
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    }
}
```

機器人控制範例：允許特定的封鎖機器人

機器人可能會被一個以上的機器人控制規則封鎖。針對每個封鎖規則執行下列程序。

如果 AWS WAF 機器人控制規則封鎖了您不想封鎖的機器人，請執行下列動作：

1. 透過檢查記錄來識別封鎖機器人的機器人控制規則。封鎖規則會在名稱開頭為的欄位中指定記錄檔`terminatingRule`。如需有關網路 ACL 記錄的資訊，請參閱記錄 AWS WAF 網頁 ACL 流量。請注意規則新增至要求的標籤。
2. 在 Web ACL 中，覆寫要計數之封鎖規則的動作。若要在主控台中執行此操作，請在 Web ACL 中編輯規則群組規則，並為規則選擇Count的規則動作覆寫。這可確保機器人不會被規則封鎖，但規則仍會將其標籤套用至相符的要求。

3. 在「機器人控制」受管規則群組之後，將標籤比對規則新增至 Web ACL。設定規則以符合覆寫規則的標籤，並封鎖除您不想封鎖的機器人以外的所有相符要求。

   您的 Web ACL 現在已設定好，因此您要允許的機器人不再遭到您透過記錄檔識別的封鎖規則所封鎖。

再次檢查流量和您的日誌，以確保機器人被允許通過。如果沒有，請再次執行上述過程。

例如，假設您想要封鎖所有監視機器人，除了pingdom. 在此情況下，您會覆寫要計數的CategoryMonitoring規則，然後撰寫規則來封鎖所有監視機器人，但具有機器人名稱標籤的機器人除外pingdom。

下列規則使用 Bot Control 受管理規則群組，但會覆寫CategoryMonitoring要計數的規則動作。類別監控規則會像往常一樣將其標籤套用至相符的要求，但只會計算它們，而不是執行其一般的封鎖動作。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
   "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "CategoryMonitoring"
        }
      ],
      "ExcludedRules": []
    }
  },
  "VisibilityConfig": {
```

```
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Example"
  }
}
```

下列規則會比對先前規CategoryMonitoring則新增至相符 Web 要求的類別監控標籤。在類別監控要求中，此規則會封鎖除機器人名稱標籤的所有要求以外的所有要求pingdom。

下列規則必須在 Web ACL 處理順序中的前一個「機器人控制」受管理規則群組之後執行。

```
{
      "Name": "match_rule",
      "Priority": 10,
      "Statement": {
        "AndStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
              }
            },
            {
              "NotStatement": {
                "Statement": {
                  "LabelMatchStatement": {
                    "Scope": "LABEL",
                    "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
                  }
                }
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "match_rule"
```

```
      }
}
```

機器人控制範例：為封鎖的使用者代理程式建立例外

如果錯誤地封鎖來自某些非瀏覽器使用者代理程式的流量，您可以將違規的 AWS WAF Bot Control 規則設定為「計數」，然後將規則SignalNonBrowserUserAgent的標籤與例外條件合併，以建立例外。

> **Note**
>
> 行動應用程式通常具有非瀏覽器使用者代理程式，依預設會封鎖SignalNonBrowserUserAgent規則。

下列規則使用「機器人控制」受管理規則群組，但會覆寫「SignalNonBrowserUserAgent要計數」的規則動作。信號規則像往常一樣將其標籤應用於匹配請求，但只對它們進行計數，而不是執行其通常的塊操作。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
   "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "SignalNonBrowserUserAgent"
        }
      ],
      "ExcludedRules": []
```

```
    }
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Example"
  }
}
```

下列規則會比對機器人控制SignalNonBrowserUserAgent規則新增至其相符 Web 要求的訊號標籤。在信號請求中，此規則會阻止所有，但具有我們要允許的用戶代理的用戶代理。

下列規則必須在 Web ACL 處理順序中的前一個「機器人控制」受管理規則群組之後執行。

```
{
    "Name": "match_rule",
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:signal:non_browser_user_agent"
            }
          },
          {
            "NotStatement": {
              "Statement": {
                "ByteMatchStatement": {
                  "FieldToMatch": {
                    "SingleHeader": {
                      "Name": "user-agent"
                    }
                  },
                  "PositionalConstraint": "EXACTLY",
                  "SearchString": "PostmanRuntime/7.29.2",
                  "TextTransformations": [
                    {
                      "Priority": 0,
                      "Type": "NONE"
                    }
                  ]
                }
```

```
              }
            }
          }
        ]
      }
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "match_rule"
    }
}
```

機器人控制範例：僅針對登入頁面使用機器人控制

下列範例會使用範圍向下陳述式，將 AWS WAF Bot Control 套用至網站登入頁面 (由 URI 路徑識別) 的流量。login根據您的應用程式和環境而定，登入頁面的 URI 路徑可能與範例不同。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
   "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
```

```
    },
    "ScopeDownStatement": {
      "ByteMatchStatement": {
        "SearchString": "login",
        "FieldToMatch": {
          "UriPath": {}
        },
        "TextTransformations": [
          {
            "Priority": 0,
            "Type": "NONE"
          }
        ],
        "PositionalConstraint": "CONTAINS"
      }
    }
  }
}
```

機器人控制範例：僅針對動態內容使用機器人控制

此範例使用範圍向下陳述式，僅將 AWS WAF 機器人控制套用至動態內容。

scope-down 語句通過否定正則表達式模式集的匹配結果來排除靜態內容：

- 正則表達式模式集被配置為匹配靜態內容的擴展。例如，正則表達式模式集規範可能是`(?i)\.(jpe?g|gif|png|svg|ico|css|js|woff2?)$`。如需有關 regex 模式集和陳述式的資訊，請參閱規則運算式模式集比對規則陳述式。
- 在範圍向下語句中，我們通過在語句中嵌套正則表達式模式 set 語句來排除匹配的靜態內容。NOT如需有關NOT陳述式的資訊，請參閱NOT規則陳述式。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
   "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
```

```
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "RegexPatternSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:123456789:regional/regexpatternset/
excludeset/00000000-0000-0000-0000-000000000000",
            "FieldToMatch": {
              "UriPath": {}
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        }
      }
    }
  }
}
```

機器人控制範例：從機器人管理中排除 IP 範圍

如果您想要從 AWS WAF Bot Control 管理中排除網路流量子集，並且可以使用規則陳述式來識別該子集，請在 Bot Control 管理規則群組陳述式中新增範圍向下陳述式來排除該子集。

下列規則會對所有網路流量執行一般的 Bot Control 機器人管理，但來自特定 IP 位址範圍的網頁要求除外。

```
{
  "Name": "AWS-AWSBotControl-Example",
```

```
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "IPSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:123456789:regional/ipset/
friendlyips/00000000-0000-0000-0000-000000000000"
          }
        }
      }
    }
  }
}
```

機器人控制範例：允許來自您控制的機器人的流量

您可以配置一些站點監控漫遊器和自定義漫遊器以發送自定義標題。如果您想要允許來自這些類型機器人的流量，您可以將其設定為在標頭中新增共用密碼。然後，您可以在 AWS WAF Bot Control 受管理規則群組陳述式中新增範圍向下陳述式，以排除具有標頭的郵件。

下列範例規則會從機器人控制檢查中排除含有秘密標頭的流量。

```
{
  "Name": "AWS-AWSBotControl-Example",
```

```
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "ByteMatchStatement": {
            "SearchString": "YSBzZWNyZXQ=",
            "FieldToMatch": {
              "SingleHeader": {
                "Name": "x-bypass-secret"
              }
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ],
            "PositionalConstraint": "EXACTLY"
          }
        }
      }
    }
  }
}
```

機器人控制範例：目標檢驗層級

若要增強保護層級，您可以在 AWS WAF Bot Control 受管理規則群組中啟用目標檢查層級。

在下列範例中，已啟用機器學習功能。您可以將設定為來選擇退出此行`EnableMachineLearning`為`false`。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "TARGETED",
            "EnableMachineLearning": true
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    }
  }
}
```

機器人控制範例：使用兩個陳述式來限制目標檢驗層級的使用

作為成本最佳化，您可以在 Web ACL 中使用兩個 AWS WAF Bot Control 受管規則群組陳述式，其中包含不同的檢查層級和範圍。例如，您可以將目標檢查層級陳述式的範圍限定為較敏感的應用程式端點。

下列範例中的兩個陳述式具有互斥的範圍設定。如果沒有此配置，請求可能會導致兩次計費評估。

> **Note**
>
> 主控台的視覺化編輯器不支援參考AWSManagedRulesBotControlRuleSet多個陳述式。而是使用 JSON 編輯器。

```
{
  "Name": "Bot-WebACL",
  "Id": "...",
  "ARN": "...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "Bot-WebACL",
  "Rules": [
      {
        ...
      },
      {
       "Name": "AWS-AWSBotControl-Common",
       "Priority": 5,
       "Statement": {
          "ManagedRuleGroupStatement": {
             "VendorName": "AWS",
             "Name": "AWSManagedRulesBotControlRuleSet",
             "ManagedRuleGroupConfigs": [
               {
                 "AWSManagedRulesBotControlRuleSet": {
                   "InspectionLevel": "COMMON"
                 }
               }
             ],
             "RuleActionOverrides": [],
             "ExcludedRules": []
          },
          "VisibilityConfig": {
             "SampledRequestsEnabled": true,
             "CloudWatchMetricsEnabled": true,
             "MetricName": "AWS-AWSBotControl-Common"
           },
           "ScopeDownStatement": {
              "NotStatement": {
```

```
            "Statement": {
              "ByteMatchStatement": {
                "FieldToMatch": {
                  "UriPath": {}
                },
                "PositionalConstraint": "STARTS_WITH",
                "SearchString": "/sensitive-endpoint",
                "TextTransformations": [
                  {
                    "Type": "NONE",
                    "Priority": 0
                  }
                ]
              }
            }
          }
        }
      }
    },
    {
     "Name": "AWS-AWSBotControl-Targeted",
     "Priority": 6,
     "Statement": {
        "ManagedRuleGroupStatement": {
           "VendorName": "AWS",
           "Name": "AWSManagedRulesBotControlRuleSet",
           "ManagedRuleGroupConfigs": [
             {
               "AWSManagedRulesBotControlRuleSet": {
                 "InspectionLevel": "TARGETED",
                 "EnableMachineLearning": true
               }
             }
           ],
           "RuleActionOverrides": [],
           "ExcludedRules": []
        },
        "VisibilityConfig": {
           "SampledRequestsEnabled": true,
           "CloudWatchMetricsEnabled": true,
           "MetricName": "AWS-AWSBotControl-Targeted"
         },
         "ScopeDownStatement": {
            "Statement": {
```

```
                "ByteMatchStatement": {
                  "FieldToMatch": {
                    "UriPath": {}
                  },
                  "PositionalConstraint": "STARTS_WITH",
                  "SearchString": "/sensitive-endpoint",
                  "TextTransformations": [
                    {
                      "Type": "NONE",
                      "Priority": 0
                    }
                  ]
                }
              }
            }
          }
        }
    ],
    "VisibilityConfig": {
      ...
    },
    "Capacity": 1496,
    "ManagedByFirewallManager": false
}
```

AWS WAF 用戶端應用整合

使用用戶 AWS WAF 端應用程式整合 API，將用戶端保護與 AWS 伺服器端 Web ACL 保護結合在一起，以協助驗證傳送 Web 要求至受保護資源的用戶端應用程式是否為預定用戶端，而且您的使用者是人類。

使用客戶端集成來管理無聲瀏覽器挑戰和 CAPTCHA 難題，獲取帶有成功瀏覽器和最終用戶響應證明的令牌，並將這些令牌包含在向受保護端點的請求中。如需有關 AWS WAF 權杖的一般資訊，請參閱AWS WAF 網絡請求令牌。

將您的用戶端整合與需要有效權杖才能存取資源的 Web ACL 保護相結合。您可以使用規則群組來檢查和監控挑戰權杖 (如下一節所列的項目)智慧型威脅整合與 AWS 受管規則，位於，您可以使用CAPTCHA和Challenge規則動作來檢查，如中所述CAPTCHA並Challenge在 AWS WAF。

AWS WAF 為 JavaScript 應用程式提供兩種整合層級，另一個適用於行動應用程式：

- 智慧型威脅整合 — 驗證用戶端應用程式，並提供 AWS 權杖取得與管理。這與 AWS WAF Challenge規則動作提供的功能類似。此功能將您的用戶端應用程式與AWSManagedRulesACFPRuleSet受管規則群組、受AWSManagedRulesATPRuleSet管規則群組和受AWSManagedRulesBotControlRuleSet管規則群組的目標保護層級完全整合。

  智慧型威脅整合 API 使用 AWS WAF 無訊息瀏覽器挑戰來協助確保只有在用戶端取得有效權杖之後，才允許登入嘗試和對受保護資源進行其他呼叫。該 API 管理客戶端應用程序會話的令牌授權，並收集有關客戶端的信息，以幫助確定它是由機器人還是由人操作。

  > **Note**
  >
  > 這適用於安卓 JavaScript 和 iOS 移動應用程序。

- CAPTCHA 集成 — 使用您在應用程序中管理的自定義驗證碼拼圖驗證最終用戶。這與 AWS WAF CAPTCHA規則動作提供的功能類似，但增加了對拼圖放置和行為的控制權。

  此整合利用 JavaScript 智慧型威脅整合來執行無訊息挑戰，並為客戶的頁面提供 AWS WAF 權杖。

  > **Note**
  >
  > 這適 JavaScript 用於應用程序。

主題

- 智慧型威脅整合與 AWS 受管規則
- 存取用 AWS WAF 戶端應用程式整合 API
- AWS WAF JavaScript 整合
- AWS WAF 移動應用集成

智慧型威脅整合與 AWS 受管規則

智慧型威脅整合 API 可與使用智慧型威脅規則群組的 Web ACL 搭配使用，以啟用這些進階受管規則群組的完整功能。

- AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）託管規則組AWSManagedRulesACFPRuleSet。

  帳戶創建欺詐是一種在線非法活動，攻擊者在您的應用程序中創建無效的帳戶，例如接收註冊獎金或冒充某人。ACFP 受管規則群組提供規則，以封鎖、標記和管理可能是詐騙帳戶建立嘗試的一部分的

要求。這些 API 可提供微調的用戶端瀏覽器驗證和人工互動資訊，ACFP 規則用來區隔有效的用戶端流量與惡意流量。

如需詳細資訊，請參閱 AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）規則組 及 AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）。

- AWS WAF 詐騙控制帳戶接管預防 (ATP) 管理規則群組`AWSManagedRulesATPRuleSet`。

  帳戶接管是一種在線非法活動，攻擊者可以在未經授權的情況下訪問某個人的帳戶。可承諾量管理規則群組提供規則，以封鎖、標記和管理可能是惡意帳戶接管嘗試一部分的要求。這些 API 可讓 ATP 規則用來將有效的用戶端流量與惡意流量分隔開來的用戶端驗證和行為彙總。

  如需詳細資訊，請參閱 AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組 及 AWS WAF 防止欺詐控制帳戶接管（ATP）。

- AWS WAF 機器人控制受管規則群組的目標保護層級`AWSManagedRulesBotControlRuleSet`。

  機器人從自我識別和有用的機器人（例如大多數搜索引擎和爬蟲）運行到針對您的網站運行且不會自我識別的惡意漫遊器。Bot Control 受管規則群組提供規則，以監控、標記及管理網路流量中的機器人活動。當您使用此規則群組的目標防護層級時，目標規則會使用 API 提供的用戶端工作階段資訊來更好地偵測惡意機器人。

  如需詳細資訊，請參閱 AWS WAF 機器人控制規則群組 及 AWS WAF 機器人控制。

若要將其中一個受管規則群組新增至 Web ACL，請參閱程序將 ACFP 管理規則群組新增至您的網路 ACL將可承諾量管理規則群組新增至您的 Web ACL、和將 AWS WAF 機器人控制受管規則群組新增至您的 Web ACL。

> **Note**
>
> 受管規則群組目前不會封鎖遺失 Token 的要求。若要封鎖遺失 Token 的要求，在您實作應用程式整合 API 之後，請遵循的指引阻止沒有有效 AWS WAF 令牌的請求。

存取用 AWS WAF 戶端應用程式整合 API

JavaScript 集成 API 通常可用，您可以將它們用於瀏覽器和其他執行的設備 JavaScript。

AWS WAF 為 Android 和 iOS 行動應用程式提供客製化的智慧型威脅整合 SDK。

- 對於安卓移動應用程序， AWS WAF SDK 適用於安卓 API 版本 23（安卓版本 6）及更高版本。如需 Android 版本的相關資訊，請參閱 SDK 平台版本說明。
- 針對 iOS 行動應用程式， AWS WAF SDK 適用於 iOS 13 版及更新版本。如需 iOS 版本的相關資訊，請參閱 iOS 和 iPadOS 版本說明。

透過主控台存取整合 API

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中選擇 [應用程式整合]，然後選擇您感興趣的索引標籤。

   - 智慧型威脅整合功能適用於 JavaScript 行動應用程式。

     該標籤包含以下內容：

     - 已啟用智慧型安全威脅應用程式整合的 Web ACL 清單。此清單包括使用`AWSManagedRulesACFPRuleSet`受管規則群組、受管規則群組或`AWSManagedRulesATPRuleSet`受管規則群組的目標保護層級的`AWSManagedRulesBotControlRuleSet`每個 Web ACL。當您實作智慧型威脅 API 時，您可以使用要整合之 Web ACL 的整合 URL。
     - 您有權存取的 API。這些 JavaScript API 始終可用。如需存取行動 SDK，請至「聯絡」連絡支援人 AWS員。
   - 驗證碼集成可用於 JavaScript 應用程序。

     該標籤包含以下內容：

     - 整合中使用的整合 URL。
     - 您為用戶端應用程式網域建立的 API 金鑰。您使用 CAPTCHA API 需要一個加密的 API 密鑰，該密鑰使客戶有權從他們的域訪問 AWS WAF 驗證碼。對於與之整合的每個用戶端，請使用包含用戶端網域的 API 金鑰。如需這些需求與管理這些金鑰的詳細資訊，請參閱〈〉管理 JS 驗證碼 API 的 API 密鑰。

AWS WAF JavaScript 整合

您可以使用 JavaScript 整合 API 在瀏覽器和其他執行的裝置中實作 AWS WAF 應用程式整合 JavaScript。

驗證碼謎題和無聲挑戰只能在瀏覽器訪問 HTTPS 端點時運行。瀏覽器客戶端必須在安全上下文中運行才能獲取令牌。

- 智慧型威脅 API 可讓您透過無訊息的用戶端瀏覽器挑戰來管理 Token 授權，並將權杖包含在傳送至受保護資源的要求中。
- CAPTCHA 整合 API 可新增至智慧型威脅 API，讓您自訂用戶端應用程式中 CAPTCHA 難題的位置和特性。該 API 利用智能威脅 API 獲取 AWS WAF 令牌，以便在最終用戶成功完成 CAPTCHA 難題後在頁面中使用。

通過使用這些集成，您可以確保客戶端的遠程過程調用包含有效的令牌。當這些整合 API 位於應用程式的頁面上時，您可以在 Web ACL 中實作緩和規則，例如封鎖不包含有效權杖的要求。您也可以透過在規則中使用Challenge或CAPTCHA動作來實作規則，以強制使用用戶端應用程式取得的權杖。

下列清單顯示 Web 應用程式頁面中一般實作智慧型威脅 API 的基本元件。

```
<head>
<script type="text/javascript" src="Web ACL integration URL/challenge.js" defer></
script>
</head>
<script>
const login_response = await AwsWafIntegration.fetch(login_url, {
    method: 'POST',
    headers: {
      'Content-Type': 'application/json'
    },
    body: login_body
  });
</script>
```

驗證碼整合 API 可讓您自訂最終使用者的驗證碼拼圖體驗。CAPTCHA 集成利用 JavaScript 智能威脅集成，用於瀏覽器驗證和令牌管理，並添加了用於配置和渲染 CAPTCHA 難題的功能。

以下列表顯示了在 Web 應用程序頁面中驗證碼 JavaScript API 的典型實現的基本組成部分。

```
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>

<script type="text/javascript">
    function showMyCaptcha() {
        var container = document.querySelector("#my-captcha-container");
```

```
        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            ...other configuration parameters as needed...
        });
    }

    function captchaExampleSuccessFunction(wafToken) {
        // Use WAF token to access protected resources
        AwsWafIntegration.fetch("...WAF-protected URL...", {
            method: "POST",
            ...
        });
    }

    function captchaExampleErrorFunction(error) {
        /* Do something with the error */
    }
</script>

<div id="my-captcha-container">
    <!-- The contents of this container will be replaced by the captcha widget -->
</div>
```

主題

- 提供在權杖中使用的網域
- 搭配內容安全性原則使用 JavaScript API
- 使用智慧型威脅 JavaScript API
- 使用驗證碼 JavaScript API

提供在權杖中使用的網域

根據預設， AWS WAF 建立權杖時，它會使用與 Web ACL 相關聯之資源的主機網域。您可以為為 JavaScript API AWS WAF 建立的權杖提供其他網域。若要這麼做，請使用一或多個 Token 網域來設定全域變數`window.awsWafCookieDomainList`。

AWS WAF 建立權杖時，它會使用中的網域組合中最適當、最短的網域，
以`window.awsWafCookieDomainList`及與 Web ACL 相關聯之資源的主機網域。

範例設定：

```
window.awsWafCookieDomainList = ['.aws.amazon.com']
```

```
window.awsWafCookieDomainList = ['.aws.amazon.com', 'abc.aws.amazon.com']
```

您不能在此列表中使用公共後綴。例如，您無法在清單中使用gov.au或co.uk做為權杖網域。

您在此清單中指定的網域必須與您的其他網域和網域組態相容：

- 根據受保護的主機網域和針對 Web ACL 設定的權杖網域清單，這些網域必須是 AWS WAF 將接受的網域。如需詳細資訊，請參閱 AWS WAF 網絡 ACL 令牌域列表配置。
- 如果您使用 JavaScript CAPTCHA API，則 CAPTCHA API 密鑰中至少有一個域必須與其中一個令牌域完全匹配，window.awsWafCookieDomainList否則必須是其中一個令牌域的頂點域。

  例如，對於令牌域mySubdomain.myApex.com，API 密鑰mySubdomain.myApex.com是完全匹配的，API 密鑰myApex.com是頂點域。任一個密鑰都匹配令牌域。

  如需 API 金鑰的詳細資訊，請參閱管理 JS 驗證碼 API 的 API 密鑰。

如果您使用受AWSManagedRulesACFPRuleSet管規則群組，則可能會設定與您提供給規則群組組態之帳戶建立路徑中的網域相符。如需此組態的詳細資訊，請參閱「將 ACFP 管理規則群組新增至您的網路 ACL」。

如果您使用AWSManagedRulesATPRuleSet受管規則群組，則可以設定與您提供給規則群組配置之登入路徑中的網域相符。如需此組態的詳細資訊，請參閱「將可承諾量管理規則群組新增至您的 Web ACL」。

搭配內容安全性原則使用 JavaScript API

如果您將內容安全策略 (CSP) 套用至資源，您必須允許列出 AWS WAF Apex 網域，才能讓JavaScript實作正常運作。awswaf.com JavaScript SDK 會對不同 AWS WAF 端點進行呼叫，因此允許列出此網域可提供 SDK 操作所需的權限。

以下顯示允許列出 AWS WAF Apex 網域的範例組態：

```
connect-src 'self' https://*.awswaf.com;
script-src 'self' https://*.awswaf.com;
script-src-elem 'self' https://*.awswaf.com;
```

如果您嘗試將 JavaScript SDK 與使用 CSP 的資源搭配使用，但尚未允許列出 AWS WAF 網域，您會收到類似下列的錯誤訊息：

```
Refused to load the script ...awswaf.com/<> because it violates the following Content
 Security Policy directive: “script-src ‘self’
```

使用智慧型威脅 JavaScript API

智慧型威脅 API 可提供針對使用者瀏覽器執行無訊息挑戰的作業，以及處理可提供成功挑戰證明和 CAPTCHA 回應的 AWS WAF 權杖。

先在測試環境中實作 JavaScript 整合，然後在生產環境中實作整合。如需其他程式碼撰寫指引，請參閱下列各節。

使用智慧型威脅 API

1. 安裝 API

   如果您使用驗證碼 API，則可以跳過此步驟。當您安裝驗證碼 API 時，指令碼會自動安裝智慧型威脅 API。

   a. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
   b. 在導覽窗格中，選擇 Application integration (應用程式整合)。在「應用程式整合」頁面上，您可以看到標籤式選項。
   c. 選擇智慧型威脅整合
   d. 在「」頁籤中，選取您要整合的 Web ACL。Web ACL 清單僅包含使用`AWSManagedRulesACFPRuleSet`受管規則群組、受管規則群組或`AWSManagedRulesATPRuleSet`受管規則群組的目標保護層級的`AWSManagedRulesBotControlRuleSet` Web ACL。
   e. 開啟 JavaScript SDK 窗格，然後複製要在整合中使用的指令碼標記。
   f. 在應用程式頁面程式碼的<head>區段中，插入您為 Web ACL 複製的指令碼標記。此包含會導致您的客戶端應用程序在頁面加載時在後台自動檢索令牌。

      ```
      <head>
          <script type="text/javascript" src="Web ACL integration URL/challenge.js”
       defer></script>
      <head>
      ```

此<script>清單已使用defer屬性進行設定，但async如果您希望頁面採用不同的行為，則可以將設定變更為。

2. (選擇性) 新增用戶端權杖的網域組態 — 依預設， AWS WAF 建立權杖時，它會使用與 Web ACL 相關聯之資源的主機網域。若要為 JavaScript API 提供其他網域，請遵循的指引提供在權杖中使用的網域。
3. 編寫智慧型威脅整合的程式碼 — 撰寫程式碼，以確保在用戶端將其請求傳送到受保護的端點之前完成 Token 擷取。如果您已經使用 fetch API 進行調用，則可以替換 AWS WAF 集成fetch包裝器。如果您不使用 fetch API，則可以改用 AWS WAF 整合getToken作業。如需程式碼撰寫指引，請參閱下列各節。
4. 在 Web ACL 中新增權杖驗證 — 在 Web ACL 中新增至少一個規則，以檢查用戶端傳送的 Web 要求中是否有效的挑戰權杖。您可以使用規則群組來檢查和監控挑戰權杖 (例如 Bot Control 受管理規則群組的目標層級)，也可以使用Challenge規則動作進行檢查，如中所述CAPTCHA並Challenge在 AWS WAF。

   Web ACL 新增功能會驗證對受保護端點的要求是否包含您在用戶端整合中取得的權杖。包含有效、未過期權杖的要求會通過Challenge檢查，並且不會向您的用戶端傳送另一個無訊息的挑戰。
5. (選擇性) 封鎖遺失 Token 的要求 — 如果您將 API 與 ACFP 管理規則群組、ATP 管理規則群組或機器人控制規則群組的目標規則搭配使用，則這些規則不會封鎖遺失 Token 的要求。要阻止缺少令牌的請求，請按照中的指導進行操作阻止沒有有效 AWS WAF 令牌的請求。

主題

- 智慧型威脅 API 規格
- 如何使用整合fetch包裝
- 如何使用整合 getToken

智慧型威脅 API 規格

本節列出智慧型威脅緩和 JavaScript API 的方法和特性的規格。使用這些 API 進行智慧威脅和驗證碼整合。

`AwsWafIntegration.fetch()`

使用 AWS WAF 整合實作將 HTTP fetch 要求傳送至伺服器。

AwsWafIntegration.getToken()

檢索存儲的 AWS WAF 令牌並將其存儲在具有名稱的當前頁面上的 cookie 中aws-waf-token，並將值設置為令牌值。

AwsWafIntegration.hasToken()

返回一個布爾值，指示 aws-waf-token cookie 當前是否持有未過期的令牌。

如果您還使用 CAPTCHA 集成，請參閱該集成的規範驗證碼 JavaScript API 規格。

如何使用整合**fetch**包裝

您可以通過更改AwsWafIntegration命名空間下的 fetch API 的常規fetch調用來使用 AWS WAF fetch包裝器。 AWS WAF 包裝器支援與標準 JavaScript fetch API 呼叫相同的所有選項，並為整合新增權杖處理。這種方法通常是整合應用程式的最簡單方法。

在包裝實現之前

下列範例清單會顯示實作AwsWafIntegrationfetch包裝函式之前的標準程式碼。

```
const login_response = await fetch(login_url, {
     method: 'POST',
     headers: {
       'Content-Type': 'application/json'
     },
     body: login_body
   });
```

包裝實現之後

下列清單顯示了AwsWafIntegrationfetch包裝函式實作的相同程式碼。

```
const login_response = await AwsWafIntegration.fetch(login_url, {
     method: 'POST',
     headers: {
       'Content-Type': 'application/json'
     },
     body: login_body
   });
```

如何使用整合 **getToken**

AWS WAF 要求您對受保護端點的請求包含以當前令牌值命名aws-waf-token的 cookie。

該getToken操作是一個異步 API 調用，它檢索 AWS WAF 令牌並將其存儲在具有名稱的當前頁面上的 cookie 中aws-waf-token，並將值設置為令牌值。您可以根據需要在頁面中使用此令牌 cookie。

當你打電話時getToken，它會執行以下操作：

- 如果一個未過期的令牌已經可用，調用立即返回它。
- 否則，呼叫會從權杖提供者擷取新的權杖，等待最多 2 秒鐘，讓權杖擷取工作流程在逾時之前完成。如果操作超時，它會拋出一個錯誤，您的調用代碼必須處理。

該getToken操作具有隨附的hasToken操作，指示 aws-waf-token cookie 當前是否持有未過期的令牌。

AwsWafIntegration.getToken()檢索一個有效的令牌並將其存儲為 cookie。大多數客戶端調用會自動附加此 cookie，但有些則不會。例如，跨主機網域進行的呼叫不會附加 Cookie。在接下來的實作詳細資訊中，我們會示範如何處理這兩種類型的用戶端呼叫。

基本**getToken**實作，適用於附加 **aws-waf-token** Cookie 的呼叫

下列範例清單顯示使用登入要求實作getToken作業的標準程式碼。

```
const login_response = await AwsWafIntegration.getToken()
     .catch(e => {
         // Implement error handling logic for your use case
     })
     // The getToken call returns the token, and doesn't typically require special
 handling
     .then(token => {
         return loginToMyPage()
     })

 async function loginToMyPage() {
     // Your existing login code
 }
```

僅在令牌可用後才提交表單 **getToken**

下列清單顯示如何註冊事件偵聽程式以攔截表單提交，直到有效的 Token 可供使用為止。

```
<body>
   <h1>Login</h1>
   <p></p>
   <form id="login-form" action="/web/login" method="POST" enctype="application/x-www-
form-urlencoded">
     <label for="input_username">USERNAME</label>
     <input type="text" name="input_username" id="input_username"><br>
     <label for="input_password">PASSWORD</label>
     <input type="password" name="input_password" id="input_password"><br>
     <button type="submit">Submit<button>
   </form>

 <script>
   const form = document.querySelector("#login-form");

   // Register an event listener to intercept form submissions
   form.addEventListener("submit", (e) => {
       // Submit the form only after a token is available
       if (!AwsWafIntegration.hasToken()) {
           e.preventDefault();
           AwsWafIntegration.getToken().then(() => {
               e.target.submit();
           }, (reason) => { console.log("Error:"+reason) });
         }
     });
 </script>
 </body>
```

在您的客戶端默認情況下未附加 **aws-waf-token** cookie 時附加令牌

AwsWafIntegration.getToken()檢索有效的令牌並將其存儲為 cookie，但並非所有客戶端調用默認附加此 cookie。例如，跨主機網域進行的呼叫不會附加 Cookie。

fetch包裝器會自動處理這些情況，但是如果您無法使用fetch包裝器，則可以使用自定義x-aws-waf-token標題來處理此問題。 AWS WAF 除了從 aws-waf-token cookie 中讀取它們之外，還可以從此標頭讀取令牌。下列程式碼顯示設定標頭的範例。

```
const token = await AwsWafIntegration.getToken();
const result = await fetch('/url', {
    headers: {
        'x-aws-waf-token': token,
    },
```

```
});
```

默認情況下， AWS WAF 僅接受包含與請求的主機域相同的域的令牌。任何跨網域權杖都需要 Web ACL 權杖網域清單中的對應項目。如需詳細資訊，請參閱 AWS WAF 網絡 ACL 令牌域列表配置。

如需有關跨網域權杖使用的其他資訊，請參閱 aws-aws-waf-bot-control 範例/-。api-protection-with-captcha

使用驗證碼 JavaScript API

CAPTCHA JavaScript API 允許您配置 CAPTCHA 拼圖並將其放置在客戶端應用程序中所需的位置。該 API 利用智能威脅 JavaScript API 的功能在最終用戶成功完成 CAPTCHA 難題後獲取和使用 AWS WAF 令牌。

先在測試環境中實作 JavaScript 整合，然後在生產環境中實作整合。如需其他程式碼撰寫指引，請參閱下列各節。

若要使用驗證碼整合 API

1. 安裝應用程式碼

   a. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   b. 在導覽窗格中，選擇 Application integration (應用程式整合)。在「應用程式整合」頁面上，您可以看到標籤式選項。

   c. 選擇驗證碼整合。

   d. 複製列出的 JavaScript 整合指令碼標記，以便在整合中使用。

   e. 在應用程式頁面程式碼的<head>區段中，插入您複製的指令碼標記。這種包含使 CAPTCHA 難題可用於配置和使用。

   ```
   <head>
       <script type="text/javascript" src="integrationURL/jsapi.js" defer></
   script>
   </head>
   ```

   此<script>清單已使用defer屬性進行設定，但async如果您希望頁面採用不同的行為，則可以將設定變更為。

如果智慧型威脅整合指令碼尚未存在，CAPTCHA 指令碼也會自動載入。智慧型威脅整合指令碼可讓您的用戶端應用程式在頁面載入時在背景自動擷取權杖，並提供您使用 CAPTCHA API 所需的其他權杖管理功能。

2. (選擇性) 新增用戶端權杖的網域組態 — 依預設， AWS WAF 建立權杖時，它會使用與 Web ACL 相關聯之資源的主機網域。若要為 JavaScript API 提供其他網域，請遵循的指引提供在權杖中使用的網域。
3. 取得用戶端的加密 API 金鑰 — CAPTCHA API 需要加密的 API 金鑰，其中包含有效的用戶端網域清單。 AWS WAF 使用此金鑰驗證您在整合中使用的用戶端網域是否已獲准使用 AWS WAF CAPTCHA。若要產生您的 API 金鑰，請遵循的指引管理 JS 驗證碼 API 的 API 密鑰。
4. 編碼您的 CAPTCHA 小部件實現-在您要使用它的位置在您的頁面中實現 `renderCaptcha()` API 調用。如需有關配置和使用此函數的資訊，請參閱下列各節驗證碼 JavaScript API 規格和如何渲染驗證碼拼圖。

   CAPTCHA 實現與智能威脅集成 API 集成在一起，用於令牌管理和運行使用令 AWS WAF 牌的獲取調用。如需有關使用這些 API 的指導，請參閱使用智慧型威脅 JavaScript API。
5. 在 Web ACL 中添加令牌驗證 — 在 Web ACL 中添加至少一個規則，以檢查客戶端發送的 Web 請求中是否存在有效的 CAPTCHA 令牌。您可以使用CAPTCHA規則動作來檢查，如中所述CAPTCHA並Challenge在 AWS WAF。

   Web ACL 新增功能會驗證傳送至受保護端點的要求是否包含您在用戶端整合中取得的權杖。包含有效、未過期的 CAPTCHA Token 的要求會通過CAPTCHA規則動作檢查，而且不會向您的使用者顯示其他 CAPTCHA 謎題。

主題

- 驗證碼 JavaScript API 規格
- 如何渲染驗證碼拼圖
- 處理來自的驗證碼響應 AWS WAF
- 管理 JS 驗證碼 API 的 API 密鑰

驗證碼 JavaScript API 規格

本節列出了驗證碼 JavaScript API 的方法和屬性的規範。使用驗證碼 JavaScript API 在您的客戶端應用程序中運行自定義驗證碼難題。

此 API 以智慧型威脅 API 為基礎，您可以使用這些 API 來設定和管理 AWS WAF 權杖擷取和使用。請參閱智慧型威脅 API 規格。

`AwsWafCaptcha.renderCaptcha(container, configuration)`

向最終用戶提供 AWS WAF CAPTCHA 難題，成功後，使用 CAPTCHA 驗證更新客戶端令牌。這僅適用於與驗證碼集成。將此呼叫與智慧威脅 API 搭配使用，以管理權杖擷取，並在`fetch`呼叫中提供 Token。請參閱智慧型威脅 API，請參閱智慧型威脅 API 規格。

與 AWS WAF 發送的 CAPTCHA 插頁式不同，通過此方法呈現的 CAPTCHA 拼圖立即顯示拼圖，而無需初始標題屏幕。

`container`

頁面上`Element`目標容器元素的物件。這通常是透過呼叫`document.getElementById()`或來擷取`document.querySelector()`。

必要：是

類型：`Element`

配置

包含驗證碼配置設置的對象，如下所示：

`apiKey`

啟用用戶端網域權限的加密 API 金鑰。使用主 AWS WAF 控台為您的用戶端網域產生 API 金鑰。您最多可以將一個金鑰用於五個網域。如需相關資訊，請參閱管理 JS 驗證碼 API 的 API 密鑰。

必要：是

類型：`string`

`onSuccess: (wafToken: string) => void;`

當最終用戶成功完成 CAPTCHA 難題時，使用有效 AWS WAF 令牌調用。在您傳送至使用 AWS WAF Web ACL 保護之端點的要求中使用 Token。令牌提供證明和最近成功拼圖完成的時間戳。

必要：是

`onError?: (error: CaptchaError) => void;`

當驗證碼操作過程中發生錯誤時，使用錯誤對象調用。

必要：否

CaptchaError類別定義 — onError 處理常式會提供具有下列類別定義的錯誤類型。

```
CaptchaError extends Error {
    kind: "internal_error" | "network_error" | "token_error" | "client_error";
    statusCode?: number;
}
```

- kind— 傳回的錯誤類型。
- statusCode— HTTP 狀態碼 (如果有的話)。network_error如果錯誤是由 HTTP 錯誤引起的，則使用此選項。

onLoad?: () => void;

當一個新的驗證碼拼圖加載時調用。

必要：否

onPuzzleTimeout?: () => void;

當驗證碼難題在到期前未完成時調用。

必要：否

onPuzzleCorrect?: () => void;

當提供正確答案給驗證碼難題時調用。

必要：否

onPuzzleIncorrect?: () => void;

當提供錯誤的答案給驗證碼難題時調用。

必要：否

defaultLocale

用於驗證碼難題的預設語言環境。驗證碼拼圖的書面說明有阿拉伯文 (AR-SA)、簡體中文 (zh-CN)、荷蘭文 (NL-NL)、英文 (en-US)、法文 (FR-FR)、德文 (DE-DE)、義大利文 (IT-IT)、日文 (JA-JP)、巴西葡萄牙文 (PT-BR)、西班牙文 (ES-ES) 和土耳其文 (TR-TR)。音訊指示適用於所有書面語言，中文和日文除外，預設為英文。若要變更預設語言，請提供國際語言和地區設定代碼，例如，ar-SA。

預設值：使用者瀏覽器中目前使用的語言

必要：否

類型：string

disableLanguageSelector

如果設定為true，驗證碼謎題會隱藏語言選擇器。

預設：false

必要：否

類型：boolean

dynamicWidth

如果設定為true，CAPTCHA 難題會變更寬度，以便與瀏覽器視窗寬度相容。

預設：false

必要：否

類型：boolean

skipTitle

如果設定為true，CAPTCHA 拼圖不會顯示拼圖標題標題解決難題。

預設：false

必要：否

類型：boolean

如何渲染驗證碼拼圖

您可以在客戶端界面中使用所需的 AWS WAF renderCaptcha呼叫。該呼叫從中檢索 CAPTCHA 難題 AWS WAF，進行渲染，然後將結果發送到以 AWS WAF 進行驗證。當您進行呼叫時，您會提供拼圖轉譯配置和您想要在最終使用者完成謎題時執行的回呼。如需有關選項的詳細資訊，請參閱前一節驗證碼 JavaScript API 規格。

將此呼叫搭配智慧型威脅整合 API 的權杖管理功能搭配使用。這個調用為您的客戶提供了一個令牌，用於驗證 CAPTCHA 難題的成功完成。使用智慧型威脅整合 API 來管理 Token，並將用戶端呼叫中的權杖提供給受 AWS WAF Web ACL 保護的端點。如需智慧型威脅 API 的相關資訊，請參閱使用智慧型威脅 JavaScript API。

實施示例

下列清單範例顯示標準 CAPTCHA 實作，包括<head>區段中 AWS WAF 整合 URL 的位置。

此清單會使用使用智慧型威脅整合 API AwsWafIntegration.fetch 包裝renderCaptcha函式的成功回呼來設定函數。如需有關此函數的資訊，請參閱如何使用整合fetch包裝。

```
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>

<script type="text/javascript">
    function showMyCaptcha() {
        var container = document.querySelector("#my-captcha-container");

        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            ...other configuration parameters as needed...
        });
    }

    function captchaExampleSuccessFunction(wafToken) {
        // Captcha completed. wafToken contains a valid WAF token. Store it for
        // use later or call AwsWafIntegration.fetch() to use it easily.
        // It will expire after a time, so calling AwsWafIntegration.getToken()
        // again is advised if the token is needed later on, outside of using the
        // fetch wrapper.

        // Use WAF token to access protected resources
        AwsWafIntegration.fetch("...WAF-protected URL...", {
            method: "POST",
            headers: {
                "Content-Type": "application/json",
            },
            body: "{ ... }" /* body content */
        });
    }

    function captchaExampleErrorFunction(error) {
        /* Do something with the error */
    }
</script>
```

```
<div id="my-captcha-container">
    <!-- The contents of this container will be replaced by the captcha widget -->
</div>
```

範例組態設定

下列範例列出了`renderCaptcha`寬度和標題選項的非預設設定。

```
        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            dynamicWidth: true,
            skipTitle: true
        });
```

如需組態選項的完整資訊，請參閱驗證碼 JavaScript API 規格。

處理來自的驗證碼響應 AWS WAF

如果請求沒有具有有效 CAPTCHA 時間戳記的令牌， AWS WAF 則具有CAPTCHA操作的規則將終止對匹配 Web 請求的評估。如果請求是GET文本/HTML 調用，則該CAPTCHA操作然後為客戶提供帶有 CAPTCHA 難題的插頁式信息。當您未整合 CAPTCHA JavaScript API 時，插頁式會執行謎題，如果最終使用者成功解決問題，則會自動重新提交要求。

當您集成 CAPTCHA JavaScript API 並自定義 CAPTCHA 處理時，您需要檢測終止的 CAPTCHA 響應，為您的自定義 CAPTCHA 提供服務，然後如果最終用戶成功解決了難題，請重新提交客戶端的 Web 請求。

下列程式碼範例示範其做法：

> **Note**
>
> AWS WAF CAPTCHA動作響應具有 HTTP 405 的狀態碼，我們用它來識別此代碼中的 CAPTCHA響應。如果您的受保護端點使用 HTTP 405 狀態碼來通訊相同呼叫的任何其他類型的回應，則此範例程式碼也會為這些回應呈現 CAPTCHA 難題。

```
<!DOCTYPE html>
```

```
<html>
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>
<body>
    <div id="my-captcha-box"></div>
    <div id="my-output-box"></div>

    <script type="text/javascript">
    async function loadData() {
        // Attempt to fetch a resource that's configured to trigger a CAPTCHA
        // action if the rule matches. The CAPTCHA response has status=HTTP 405.
        const result = await AwsWafIntegration.fetch("/protected-resource");

        // If the action was CAPTCHA, render the CAPTCHA and return

        // NOTE: If the endpoint you're calling in the fetch call responds with HTTP
 405
        // as an expected response status code, then this check won't be able to tell
 the
        // difference between that and the CAPTCHA rule action response.

        if (result.status === 405) {
            const container = document.querySelector("#my-captcha-box");
            AwsWafCaptcha.renderCaptcha(container, {
                apiKey: "...API key goes here...",
                onSuccess() {
                    // Try loading again, now that there is a valid CAPTCHA token
                    loadData();
                },
            });
            return;
        }

        const container = document.querySelector("#my-output-box");
        const response = await result.text();
        container.innerHTML = response;
    }

    window.addEventListener("load", () => {
        loadData();
    });
    </script>
</body>
```

```
</html>
```

管理 JS 驗證碼 API 的 API 密鑰

要將 AWS WAF CAPTCHA 集成到帶有 JavaScript API 的客戶端應用程序中，您需要 JavaScript API 集成標籤和要運行驗證碼難題的客戶端域的加密 API 密鑰。

的 CAPTCHA 應用程式整合 JavaScript 會使用加密的 API 金鑰來驗證用戶端應用程式網域是否具有使用 AWS WAF CAPTCHA API 的權限。當您從 JavaScript 用戶端呼叫 CAPTCHA API 時，您會提供一個包含目前用戶端網域的網域清單的 API 金鑰。您最多可以在一個加密金鑰中列出 5 個網域。

API 金鑰需求

您在 CAPTCHA 整合中使用的 API 金鑰必須包含適用於您使用金鑰的用戶端的網域。

- 如果您`window.awsWafCookieDomainList`在用戶端的智慧型威脅整合中指定，則 API 金鑰中至少有一個網域必須與其中一個 Token 網域完全相符，`window.awsWafCookieDomainList`或者必須是其中一個 Token 網域的頂點網域。

  例如，對於令牌域`mySubdomain.myApex.com`，API 密鑰`mySubdomain.myApex.com`是完全匹配的，API 密鑰`myApex.com`是頂點域。其中一個金鑰都符合權杖網域。

  如需設定權杖網域清單的相關資訊，請參閱提供在權杖中使用的網域。
- 否則，當前域必須包含在 API 密鑰中。目前的網域是您可以在瀏覽器網址列中看到的網域。

根據受保護的主機網域和針對 AWS WAF Web ACL 設定的權杖網域清單，您使用的網域必須是接受的網域。如需詳細資訊，請參閱 AWS WAF 網絡 ACL 令牌域列表配置。

如何為您的 API 密鑰選擇區域

AWS WAF 可以在任何可用的區域生成驗證碼 API 密鑰。 AWS WAF

一般而言，您應該使用與用於網頁 ACL 相同的區域作為驗證碼 API 金鑰。但是，如果您希望地區性 Web ACL 擁有全球受眾，則可以獲得範圍為的 CAPTCHA JavaScript 整合標記 CloudFront 和範圍為的 API 密鑰 CloudFront，並將其與地區 Web ACL 一起使用。這種方法允許客戶從最接近的區域加載 CAPTCHA 難題，從而減少延遲。

範圍為非區域的 CAPTCHA API 金鑰不支援跨多個區域使用。 CloudFront 它們只能在其範圍範圍內使用。

若要為您的用戶端網域產生 API 金鑰

取得整合 URL，並透過主控台產生和擷取 API 金鑰。

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中，選擇 Application integration (應用程式整合)。
3. 在窗格中已啟用應用程式整合的 Web ACL，選取您要用於 API 金鑰的區域。您也可以在「驗證碼」整合標籤的「API 金鑰」面板中選取「區域」。
4. 選擇標籤驗證碼集成。此選項卡提供了 CAPTCHA JavaScript 集成標籤，您可以在集成中使用該標籤以及 API 密鑰列表。兩者都設定為所選「區域」的範圍。
5. 在「API 金鑰」窗格中，選擇「產生金鑰」。金鑰產生對話方塊隨即出現。
6. 輸入您要包含在金鑰中的用戶端網域。您最多可以輸入 5。完成後，選擇 [產生金鑰]。該界面返回到 CAPTCHA 集成選項卡，其中列出了您的新密鑰。

   一旦創建，API 密鑰是不可變的。如果您需要對密鑰進行更改，請生成一個新密鑰並使用該密鑰。
7. (選擇性) 複製新產生的金鑰，以便在整合中使用。

您也可以使用 REST API 或其中一個特定於語言的 AWS SDK 進行這項工作。其餘 API 調用是創建密鑰和列表應用密鑰。

若要刪除 API 金鑰

若要刪除 API 金鑰，您必須使用 REST API 或其中一個特定語言的 AWS SDK。其餘 API 調用是刪除密鑰。您無法使用主控台刪除金鑰。

刪除金鑰後，最多可能需要 24 小時 AWS WAF 才能禁止在所有區域使用該金鑰。

AWS WAF 移動應用集成

您可以使用行 AWS WAF 動 SDK 實作適用於 Android 和 iOS 行動應用程式的 AWS WAF 智慧型威脅整合 SDK。

- 對於安卓移動應用程序， AWS WAF SDK 適用於安卓 API 版本 23（安卓版本 6）及更高版本。如需 Android 版本的相關資訊，請參閱 SDK 平台版本說明。
- 針對 iOS 行動應用程式， AWS WAF SDK 適用於 iOS 13 版及更新版本。如需 iOS 版本的相關資訊，請參閱 iOS 與 iPadOS 版本說明。

使用移動 SDK，您可以管理令牌授權，並在發送到受保護資源的請求中包含令牌。通過使用 SDK，您可以確保客戶端的這些遠程過程調用包含有效的令牌。此外，在應用程式頁面上進行此整合時，您可以在 Web ACL 中實作緩和規則，例如封鎖不包含有效權杖的要求。

如需存取行動 SDK，請至「聯絡」連絡支援人 AWS員。

> **Note**
>
> 行 AWS WAF 動 SDK 不適用於驗證碼自訂。

使用 SDK 的基本方法是使用配置對象創建令牌提供程序，然後使用令牌提供程序從中檢索令牌 AWS WAF。默認情況下，令牌提供程序在您的 Web 請求中包含檢索到的令牌到受保護的資源。

以下是 SDK 實現的部分列表，其中顯示了主要組件。如需更詳細的範例，請參閱撰寫行 AWS WAF 動 SDK 的程式碼。

iOS

```
let url: URL = URL(string: "Web ACL integration URL")!
 let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
 "Domain name")
 let tokenProvider = WAFTokenProvider(configuration)
 let token = tokenProvider.getToken()
```

Android

```
URL applicationIntegrationURL = new URL("Web ACL integration URL");
 String domainName = "Domain name";
 WAFConfiguration configuration =
 WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(
 WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,
 configuration);
 WAFToken token = tokenProvider.getToken();
```

安裝行 AWS WAF 動 SDK

如需存取行動 SDK，請至「聯絡」連絡支援人 AWS員。

先在測試環境中實作行動 SDK，然後在生產環境中實作。

若要安裝 AWS WAF 行動 SDK

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中，選擇 Application integration (應用程式整合)。
3. 在智慧型威脅整合標籤中，執行下列動作：
   a. 在窗格中已啟用應用程式整合的 Web ACL，找出您要整合的 Web ACL。複製並儲存 Web ACL 整合 URL，以便在實作中使用。您也可以透過 API 呼叫取得此 URL `GetWebACL`。
   b. 選擇行動裝置類型和版本，然後選擇 [下載]。您可以選擇任何您喜歡的版本，但我們建議您使用最新版本。 AWS WAF 將裝置的`zip`檔案下載到您的標準下載位置。
4. 在您的應用程式開發環境中，將檔案解壓縮至您選擇的工作位置。在 zip 檔案的頂層目錄中，找出並開啟`README`. 依照`README`檔案中的指示安裝行 AWS WAF 動 SDK，以便在行動應用程式程式碼中使用。
5. 根據以下各節中的指導對您的應用程式進行程式設計。

行 AWS WAF 動 SDK 規格

本節列出最新可用版 AWS WAF 行動 SDK 的 SDK 物件、作業和組態設定。如需有關權杖提供者和作業如何在各種組態設定組合中運作的詳細資訊，請參閱AWS WAF 行動 SDK 的運作方式。

`WAFToken`

持有一個 AWS WAF 令牌。

`getValue()`

擷取的`String`表示`WAFToken`。

`WAFTokenProvider`

在您的行動應用程式中管理權杖。使用`WAFConfiguration`對象實現此操作。

`getToken()`

如果啟用後台刷新，這將返回緩存令牌。如果禁用後台刷新，則會進行同步，阻止調用 AWS WAF 以檢索新令牌。

onTokenReady(WAFTokenResultCallback)

指示令牌提供者刷新令牌，並在活動令牌準備就緒時調用提供的回調。令牌提供者將在令牌緩存並準備就緒時在後台線程中調用您的回調。當您的應用程序首次加載以及返回活動狀態時調用此選項。如需返回使用中狀態的詳細資訊，請參閱the section called “在應用程序不活動後檢索令牌”。

對於 Android 或 iOS 應用程序，您可以設置`WAFTokenResultCallback`為在請求的令牌準備就緒時希望令牌提供者調用的操作。您的實現`WAFTokenResultCallback`必須採用參數`WAFToken`，`SdkError`. 對於 iOS 應用程序，您可以交替創建一個內聯函數。

storeTokenInCookieStorage(WAFToken)

指示將指定的 AWS WAF 權杖儲存到 SDK 的 Cookie 管理員中。`WAFTokenProvider`默認情況下，令牌僅在首次獲取和刷新時才添加到 cookie 存儲中。如果應用程序出於任何原因清除共享 cookie 存儲，則 SDK 在下次刷新之前不會自動添加 AWS WAF 令牌。

WAFConfiguration

保留實作的組態`WAFTokenProvider`。實作此功能時，您需要提供 Web ACL 的整合 URL、要在 Token 中使用的網域名稱，以及您希望權杖提供者使用的任何非預設設定。

下列清單指定您可以在`WAFConfiguration`物件中管理的組態設定。

applicationIntegrationUrl

應用程式整合 URL。從 AWS WAF 控制台或通過 `getWebACL` API 調用獲取此信息。

必要：是

類型：特定於應用程序的 URL。對於 iOS，請參閱 iOS 網址。如需安卓系統，請參閱 Java 網址。

backgroundRefreshEnabled

指出您是否希望權杖提供者在背景中重新整理權杖。如果您設定此項，權杖提供者會根據管理自動權杖重新整理活動的組態設定，在背景重新整理您的權杖。

必要：否

類型：`Boolean`

預設值：`TRUE`

domainName

要在權杖中使用的網域，用於權杖擷取和 Cookie 儲存。例如 example.com 或 aws.amazon.com。這通常是與 Web ACL 相關聯的資源的主機域，您將在其中發送 Web 請求。對於 ACFP 管理規則群組AWSManagedRulesACFPRuleSet，這通常是與您在規則群組組態中提供之帳號建立路徑中的網域相符的單一網域。對於可承諾量管理規則群組AWSManagedRulesATPRuleSet，這通常是與您在規則群組組態中提供之登入路徑中的網域相符的單一網域。

不允許使用公共後綴。例如，您無法使用gov.au或co.uk做為權杖網域。

根據受保護的主機域和 Web ACL 的令牌域列表，該域必須是 AWS WAF 將接受的域。如需詳細資訊，請參閱 AWS WAF 網絡 ACL 令牌域列表配置。

必要：是

類型：String

maxErrorTokenRefreshDelayMsec

嘗試失敗後重複權杖重新整理之前等待的最長時間 (以毫秒為單位)。這個值會在權杖擷取失敗並重試maxRetryCount次數之後使用。

必要：否

類型：Integer

預設值：5000(5 秒)

允許的最小值：1（1 毫秒）

允許的最大值：30000（30 秒）

maxRetryCount

要求權杖時，使用指數輪詢執行的重試次數上限。

必要：否

類型：Integer

預設值：如果啟用了背景重新整理，5. 否則為 3。

允許的最小值：0

允許的最大值：10

setTokenCookie

指出您是否希望 SDK 的 Cookie 管理器在您的請求中添加令牌 cookie。默認情況下，這會向所有請求添加一個令牌 cookie。Cookie 管理器將一個令牌 cookie 添加到其路徑位於中指定的路徑下的任何請求tokenCookiePath。

必要：否

類型：Boolean

預設值：TRUE

tokenCookiePath

當setTokenCookie是時使用TRUE。表示您希望 SDK 的 cookie 管理器添加令牌 cookie 的頂級路徑。管理器將令牌 cookie 添加到您發送到此路徑和所有子路徑的所有請求。

例如，如果您將其設置為/web/login，則管理器包含發送到的所有內容/web/login及其任何子路徑的令牌 cookie，例如/web/login/help。它不包括發送到其他路徑的請求的令牌/，例如/web，或/web/order。

必要：否

類型：String

預設值：/

tokenRefreshDelaySec

用於後台刷新。背景權杖重新整理之間的時間上限 (以秒為單位)。

必要：否

類型：Integer

預設值：88

允許的最小值：88

允許的最大值：300（5 分鐘）

AWS WAF 行動 SDK 的運作方式

移動 SDK 為您提供了可配置的令牌提供程序，您可以用於令牌檢索和使用。權杖提供者會驗證您允許的要求來自合法客戶。當您向使用保護的 AWS 資源發送請求時 AWS WAF，您將令牌包含在 cookie 中以驗證請求。您可以手動處理令牌 cookie，也可以讓令牌提供者為您執行此操作。

本節介紹了包含在移動 SDK 中的類，屬性和方法之間的交互。如需 SDK 規格的資訊，請參閱行 AWS WAF 動 SDK 規格。

令牌檢索和緩存

在移動應用程序中創建令牌提供程序實例時，您可以配置希望它如何管理令牌和令牌檢索。您的主要選擇是如何維護有效的，未過期的令牌以在應用程序的 Web 請求中使用：

- [啟用背景重新整理] — 這是預設值。令牌提供程序會在後台自動刷新令牌並對其進行緩存。啟用背景重新整理後，當您呼叫時`getToken()`，作業會擷取快取的權杖。

  令牌提供程序以可配置的間隔執行令牌刷新，以便在應用程序處於活動狀態時始終在緩存中可用未過期的令牌。當您的應用程式處於非作用中狀態時，背景重新整理會暫停。如需相關資訊，請參閱在應用程序不活動後檢索令牌。
- 背景重新整理停用 — 您可以停用背景權杖重新整理，然後僅在需要時擷取權杖。按需檢索的令牌不會被緩存，如果需要，您可以檢索多個令牌。每個令牌都獨立於您檢索的任何其他令牌，並且每個令牌都有自己的時間戳記用於計算到期時間。

  停用背景重新整理時，您可以選擇以下權杖擷取：

  - **`getToken()`**— 在停用背景重新整理`getToken()`的情況下呼叫時，呼叫會同步從中 AWS WAF 擷取新的權杖。這是一個可能的阻塞調用，如果您在主線程上調用它，可能會影響應用程序響應。
  - **`onTokenReady(WAFTokenResultCallback)`**— 此呼叫以非同步方式擷取新的權杖，然後在 Token 就緒時，在背景執行緒中叫用提供的結果回呼。

令牌提供者如何重試失敗的令牌檢索

當擷取失敗時，權杖提供者會自動重試權杖擷取。重試一開始是使用指數輪詢來執行，開始重試等待時間為 100 ms。如需指數重試的相關資訊，請參閱. AWS

當重試次數達到設定後`maxRetryCount`，權杖提供者會停止嘗試或切換至每`maxErrorTokenRefreshDelayMsec`毫秒嘗試一次，視記號擷取的類型而定：

- **`onTokenReady()`**— 權杖提供者在嘗試之間切換到等待`maxErrorTokenRefreshDelayMsec`毫秒數，並繼續嘗試擷取權杖。

- 背景重新整理 — 權杖提供者會在嘗試之間切換到等待maxErrorTokenRefreshDelayMsec毫秒數，並繼續嘗試擷取權杖。
- 禁用後台刷新時的按需**getToken()**調用 — 令牌提供者停止嘗試檢索令牌並返回先前的令牌值，如果沒有先前的令牌，則返回 null 值。

在應用程序不活動後檢索令牌

背景重新整理只會在您的應用程式類型視為作用中時執行：

- iOS — 當應用程式位於前景時，會執行背景重新整理。
- Android — 背景重新整理會在應用程式未關閉時執行，無論是在前景還是背景。

如果您的應用程序處於不支持後台刷新的任何狀態超過配置的tokenRefreshDelaySec秒數，則令牌提供程序將暫停後台刷新。例如，對於 iOS 應用程序，如果tokenRefreshDelaySec是 300 並且應用程序關閉或進入後台超過 300 秒，則令牌提供程序將停止刷新令牌。當應用程序返回到活動狀態時，令牌提供程序會自動重新啟動後台刷新。

當您的應用返回到活動狀態時，請調用以onTokenReady()便在令牌提供程序檢索並緩存新令牌時收到通知。不要只是調用getToken()，因為緩存可能還不包含當前的有效令牌。

撰寫行 AWS WAF 動 SDK 的程式碼

本節提供使用行動 SDK 的程式碼範例。

初始化令牌提供者並獲取令牌

您可以使用配置對象啟動令牌提供者實例。然後，您可以使用可用的操作檢索令牌。下面顯示了所需代碼的基本組件。

iOS

```
let url: URL = URL(string: "Web ACL integration URL")!
let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
 "Domain name")
let tokenProvider = WAFTokenProvider(configuration)

//onTokenReady can be add as an observer for
 UIApplication.willEnterForegroundNotification
self.tokenProvider.onTokenReady() { token, error in
 if let token = token {
```

```
 //token available
 }

 if let error = error {
 //error occurred after exhausting all retries
 }
}

//getToken()
let token = tokenProvider.getToken()
```

Android

Java 的例子：

```
String applicationIntegrationURL = "Web ACL integration URL";
//Or
URL applicationIntegrationURL = new URL("Web ACL integration URL");

String domainName = "Domain name";

WAFConfiguration configuration =
 WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(
WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,
 configuration);

// implement a token result callback
WAFTokenResultCallback callback = (wafToken, error) -> {
 if (wafToken != null) {
 // token available
 } else {
 // error occurred in token refresh
 }
};

// Add this callback to application creation or activity creation where token will
 be used
tokenProvider.onTokenReady(callback);

// Once you have token in token result callback
// if background refresh is enabled you can call getToken() from same tokenprovider
 object
// if background refresh is disabled you can directly call getToken()(blocking call)
 for new token
```

```
WAFToken token = tokenProvider.getToken();
```

Kotlin 範例：

```
import com.amazonaws.waf.mobilesdk.token.WAFConfiguration
import com.amazonaws.waf.mobilesdk.token.WAFTokenProvider

private lateinit var wafConfiguration: WAFConfiguration
private lateinit var wafTokenProvider: WAFTokenProvider

private val WAF_INTEGRATION_URL = "Web ACL integration URL"
private val WAF_DOMAIN_NAME = "Domain name"

fun initWaf() {
 // Initialize the tokenprovider instance
 val applicationIntegrationURL = URL(WAF_INTEGRATION_URL)
 wafConfiguration =
  WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL)
   .domainName(WAF_DOMAIN_NAME).backgroundRefreshEnabled(true).build()
 wafTokenProvider = WAFTokenProvider(getApplication(), wafConfiguration)

  // getToken from tokenprovider object
  println("WAF: "+ wafTokenProvider.token.value)

  // implement callback for where token will be used
  wafTokenProvider.onTokenReady {
   wafToken, sdkError ->
  run {
   println("WAF Token:" + wafToken.value)
  }
 }
}
```

允許 SDK 在您的 HTTP 請求中提供令牌 cookie

如果setTokenCookie是TRUE，則令牌提供程序會在您的 Web 請求中為您包含令牌 cookie，以發送到在中指定的路徑下的所有位置tokenCookiePath。默認情況下，setTokenCookietokenCookiePath是TRUE和/。

您可以透過指定權杖 Cookie 路徑來縮小包含權杖 Cookie 的要求範圍，例如，/web/login。如果這樣做，請檢查您的 AWS WAF 規則是否不檢查發送到其他路徑的請求中的令牌。使

用AWSManagedRulesACFPRuleSet規則群組時，您需要設定帳戶註冊和建立路徑，規則群組會檢查傳送至這些路徑的要求中是否有 Token。如需詳細資訊，請參閱 將 ACFP 管理規則群組新增至您的網路 ACL。同樣地，當您使用AWSManagedRulesATPRuleSet規則群組時，您會設定登入路徑，規則群組會檢查傳送至該路徑之要求中的 Token。如需詳細資訊，請參閱 將可承諾量管理規則群組新增至您的 Web ACL。

iOS

如果setTokenCookie是TRUE，令牌提供程序將 AWS WAF 令牌存儲在一個中，HTTPCookieStorage.shared並在對您在中指定的域的請求中自動包含 cookie WAFConfiguration。

```
let request = URLRequest(url: URL(string: domainEndpointUrl)!)
//The token cookie is set automatically as cookie header
let task = URLSession.shared.dataTask(with: request) { data, urlResponse, error  in
}.resume()
```

Android

如果setTokenCookie是TRUE，令牌提供程序將 AWS WAF 令牌存儲在共享應用程序範圍內的CookieHandler實例中。權杖提供者會自動將 Cookie 包含在對您在中指定的網域的要求中WAFConfiguration。

Java 的例子：

```
URL url = new URL("Domain name");
//The token cookie is set automatically as cookie header
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
connection.getResponseCode();
```

Kotlin 範例：

```
val url = URL("Domain name")
//The token cookie is set automatically as cookie header
val connection = (url.openConnection() as HttpsURLConnection)
connection.responseCode
```

如果您已經初始化了CookieHandler默認實例，令牌提供商將使用它來管理 cookie。如果沒有，權杖提供者將使用權 AWS WAF 杖初始化新CookieManager執行個

體，CookiePolicy.ACCEPT_ORIGINAL_SERVER然後將此新執行個體設定為中的預設執行個體CookieHandler。

下面的代碼顯示了 SDK 如何初始化 cookie 管理器和 cookie 處理程序時，它們在您的應用程序中不可用。

Java 的例子：

```
CookieManager cookieManager = (CookieManager) CookieHandler.getDefault();
if (cookieManager == null) {
 // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
 cookieManager = new CookieManager();
 CookieHandler.setDefault(cookieManager);
}
```

Kotlin 範例：

```
var cookieManager = CookieHandler.getDefault() as? CookieManager
if (cookieManager == null) {
 // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
 cookieManager = CookieManager()
 CookieHandler.setDefault(cookieManager)
}
```

在您的 HTTP 請求中手動提供令牌 cookie

如果設置setTokenCookie為FALSE，則需要在向受保護端點的請求中手動提供令牌 cookie 作為 Cookie HTTP 請求標頭。下面的代碼演示了如何做到這一點。

iOS

```
var request = URLRequest(url: wafProtectedEndpoint)
request.setValue("aws-waf-token=token from token provider", forHTTPHeaderField:
 "Cookie")
request.httpShouldHandleCookies = true
URLSession.shared.dataTask(with: request) { data, response, error in }
```

Android

Java 的例子：

```
URL url = new URL("Domain name");
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
String wafTokenCookie = "aws-waf-token=token from token provider";
connection.setRequestProperty("Cookie", wafTokenCookie);
connection.getInputStream();
```

Kotlin 範例：

```
val url = URL("Domain name")
val connection = (url.openConnection() as HttpsURLConnection)
val wafTokenCookie = "aws-waf-token=token from token provider"
connection.setRequestProperty("Cookie", wafTokenCookie)
connection.inputStream
```

CAPTCHA並Challenge在 AWS WAF

您可以將 AWS WAF 規則設定為針對符合規則檢查準則的 Web 要求執行CAPTCHA或Challenge動作。您還可以編程 JavaScript 客戶端應用程序以在本地運行 CAPTCHA 難題和瀏覽器挑戰。

驗證碼謎題和無聲挑戰只能在瀏覽器訪問 HTTPS 端點時運行。瀏覽器客戶端必須在安全上下文中運行才能獲取令牌。

- CAPTCHA— 要求最終用戶解決 CAPTCHA 難題，以證明一個人正在發送請求。CAPTCHA 拼圖的目的是相當容易和快速地為人類成功完成，並且很難讓計算機成功完成或隨機完成任何有意義的成功率。

  在 Web ACL 規則中，CAPTCHA 通常會在Block動作停止太多合法請求時使用，但讓所有流量通過會導致難以接受的高層次不需要的請求，例如來自漫遊器。如需有關規則動作行為的資訊，請參閱AWS WAFCAPTCHA和Challenge規則動作的運作方式。

  您還可以在客戶端應用程序集成 API 中編程驗證碼難題實現。執行此操作時，您可以在用戶端應用程式中自訂拼圖的行為和位置。如需詳細資訊，請參閱 AWS WAF 用戶端應用整合。
- Challenge— 執行無訊息挑戰，需要用戶端工作階段驗證它是瀏覽器，而不是機器人。驗證會在背景執行，而不會涉及使用者。對於驗證您懷疑無效的客戶端而不會對 CAPTCHA 難題產生負面影響，這是一個很好的選擇。如需有關規則動作行為的資訊，請參閱AWS WAFCAPTCHA和Challenge規則動作的運作方式。

  Challenge規則處理行動類似於用戶端智慧型安全威脅整合 API 所執行的挑戰，如中所述AWS WAF用戶端應用整合。

> **Note**
>
> 如果您在其中一項規則中使用CAPTCHA或規Challenge則動作，或是規則群組中的規則動作覆寫，系統會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

如需所有規則動作選項的說明，請參閱規則動作。

主題

- AWS WAF 驗證碼謎題
- AWS WAFCAPTCHA和Challenge規則動作的運作方式
- 使用和動作的最佳CAPTCHAChallenge作法

AWS WAF 驗證碼謎題

AWS WAF 提供標準的 CAPTCHA 功能，挑戰用戶確認他們是人類。CAPTCHA 代表完全自動化的公共圖靈測試告訴計算機和人類分開。CAPTCHA 謎題旨在驗證人是否正在發送請求，並防止諸如網絡抓取，憑據填充和垃圾郵件之類的活動。驗證碼拼圖無法清除所有不需要的請求。使用機器學習和人工智能解決了許多難題。為了規避 CAPTCHA，一些組織通過人工干預補充自動化技術。儘管如此，CAPTCHA 仍然是一個有用的工具，可以防止不太複雜的機器人流量並增加大規模操作所需的資源。

AWS WAF 隨機生成其 CAPTCHA 難題並通過它們進行旋轉，以確保用戶面臨獨特的挑戰。 AWS WAF 定期添加新類型和風格的謎題，以保持對自動化技術的有效性。除了謎題之外， AWS WAF CAPTCHA 腳本還收集有關客戶端的數據，以確保任務由人類完成並防止重播攻擊。

每個 CAPTCHA 拼圖都包括一組標準控件，供最終用戶請求新拼圖，在音頻和視覺拼圖之間切換，訪問其他說明以及提交拼圖解決方案。所有拼圖都包括對屏幕閱讀器，鍵盤控件和對比色的支持。

AWS WAF 驗證碼謎題符合《網頁內容無障礙指南》（WCAG）的要求。有關資訊，請參閱萬維網聯盟（W3C）網站上的《無障礙網頁內容指引》（WCAG）概述。

主題

- 驗證碼拼圖語言支持
- 驗證碼拼圖示例

驗證碼拼圖語言支持

CAPTCHA 難題從用戶端瀏覽器語言的書面指示開始，或者，如果瀏覽器語言不支援，則使用英文。拼圖通過下拉菜單提供了替代語言選項。

用戶可以通過選擇頁面底部的耳機圖標切換到音頻說明。拼圖的音頻版本提供了有關用戶應在文本框中鍵入的文本的說明，並覆蓋背景噪音。

下表列出您可以為 CAPTCHA 拼圖中的書面指示選擇的語言，以及每個選項的音訊支援。

AWS WAF 驗證碼拼圖支持語言

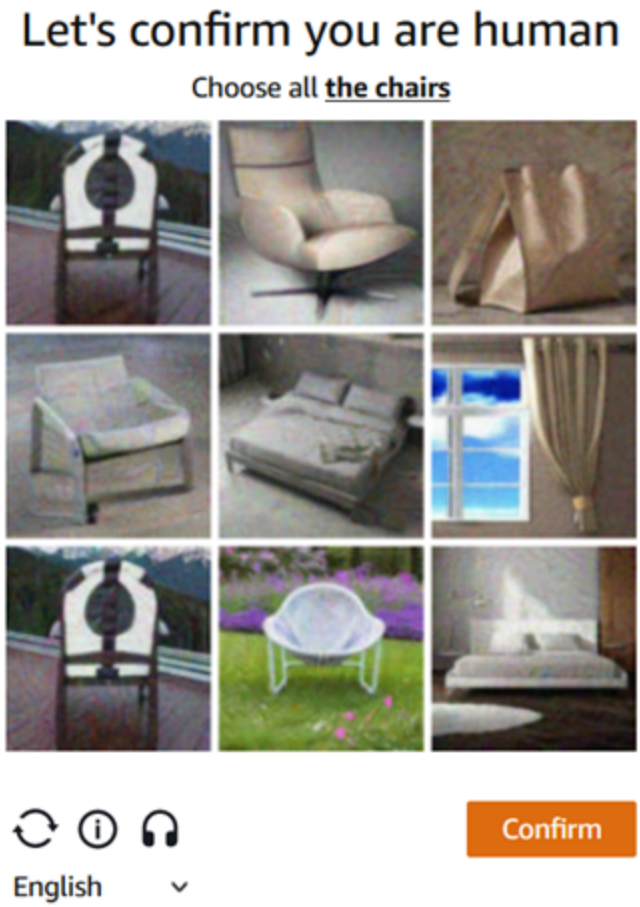
書面說明支持	地區設定碼	音頻指令支持
Arabic	AR-SA	Arabic
簡體中文	zh-CN	英語語音
荷蘭文	nl-NL	荷蘭文
英文	zh-TW	英文
法文	fr-FR	法文
德文	de-DE	德文
義大利文	it-IT	義大利文
日文	ja-JP	英語語音
巴西葡萄牙	pt-BR	巴西葡萄牙
西班牙文	es-ES	西班牙文

書面說明支持	地區設定碼	音頻指令支持
Turkish	tr-TR	Turkish

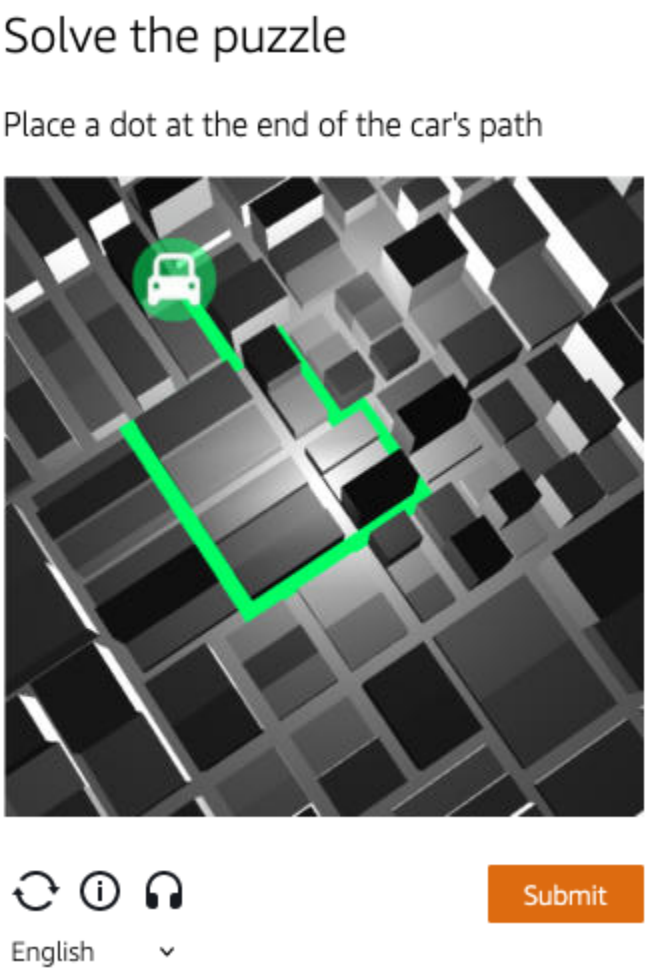
驗證碼拼圖示例

典型的視覺 CAPTCHA 拼圖需要互動，以表明用戶可以理解一個或多個圖像並與之進行交互。

下列螢幕擷取畫面顯示圖片網格拼圖的範例。這個難題需要您選擇網格中包含特定類型對象的所有圖片。

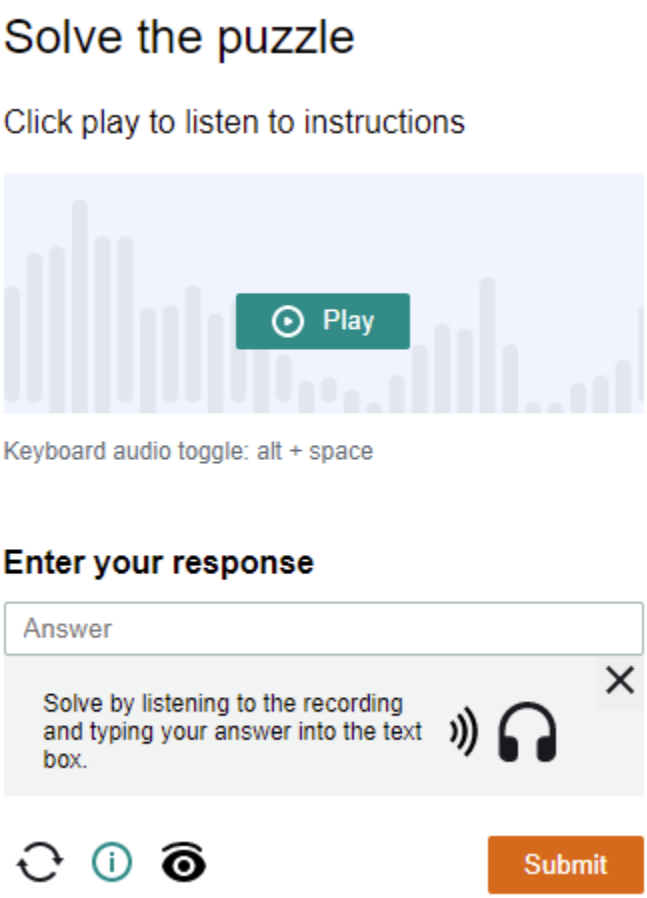


下列螢幕擷取畫面顯示了一個謎題範例，需要您識別圖面中汽車路徑的端點。



音頻拼圖提供背景噪聲覆蓋有關用戶應在文本框中鍵入的文本的口語說明。

下面的屏幕截圖顯示了音頻拼圖選擇的顯示。



AWS WAFCAPTCHA和Challenge規則動作的運作方式

AWS WAF CAPTCHA並且Challenge是標準的規則操作，因此它們相對容易實現。若要使用其中任何一個，請為您的規則建立檢驗條件，以識別您要檢查的請求，然後指定兩個規則動作的其中一個。如需有關規則動作選項的一般資訊，請參閱規則動作。

除了從服務器端實施沉默的挑戰和 CAPTCHA 難題外，您還可以在您的 iOS JavaScript 和 Android 客戶端應用程序中集成沉默的挑戰，並且可以在 JavaScript 客戶端中渲染 CAPTCHA 難題。這些整合可讓您為終端使用者提供更好的效能和 CAPTCHA 謎題體驗，並且可以降低與使用規則動作和智慧型威脅緩解規則群組相關的成本。如需關於這些選項的詳細資訊，請參閱 AWS WAF 用戶端應用整合。如需定價資訊，請參閱 AWS WAF 定價。

主題

- CAPTCHA和行Challenge動行為
- CAPTCHA和日誌和指標中的Challenge操作

CAPTCHA和行Challenge動行為

當 Web 請求符合具有CAPTCHA或Challenge動作的規則的檢查條件時，會根據其 Token 的狀態和免疫時間配置來 AWS WAF 決定如何處理請求。 AWS WAF 還考慮請求是否可以處理 CAPTCHA 難題或挑戰腳本插頁式。這些指令碼的設計是以 HTML 內容的形式處理，而且只能由預期 HTML 內容的用戶端正確處理。

> **Note**
>
> 如果您在其中一項規則中使用CAPTCHA或規Challenge則動作，或是規則群組中的規則動作覆寫，系統會向您收取額外費用。如需詳細資訊，請參閱 AWS WAF 定價。

動作如何處理 Web 請求

AWS WAF 將CAPTCHA或動Challenge作套用至 Web 要求，如下所示：

- 有效權杖 — AWS WAF 處理類似於Count動作的權杖。 AWS WAF 套用您為規則動作設定的任何標籤和要求自訂，然後使用 Web ACL 中的其餘規則繼續評估要求。
- 遺失、無效或已過期的 Token — AWS WAF 停止要求的 Web ACL 評估，並阻止它前往預定的目的地。

  AWS WAF 根據規則動作類型，產生回應並傳回給用戶端：

  - Challenge— 在回應中 AWS WAF 包含下列項目：
    - 具有 `challenge` 值的標頭 `x-amzn-waf-action`。

      > **Note**
      >
      > 在用戶端瀏覽器中執行的 JavaScript 應用程式無法使用此標頭。如需詳細資訊，請參閱下一節。

    - HTTP 狀態碼 `202 Request Accepted`。
    - 如果要求包含值為的`Accept`標頭`text/html`，則回應會包含插JavaScript 頁式頁面與挑戰指令碼。
  - CAPTCHA— 在回應中 AWS WAF 包含下列項目：
    - 具有 `captcha` 值的標頭 `x-amzn-waf-action`。

> **Note**
>
> 在用戶端瀏覽器中執行的 JavaScript 應用程式無法使用此標頭。如需詳細資訊，請參閱下一節。

- HTTP 狀態碼 `405 Method Not Allowed`。
- 如果要求包含值為的`Accept`標頭`text/html`，則回應會包含帶有 CAPTCHA 指令碼的插 JavaScript 頁式頁面。

若要在 Web ACL 或規則層級設定權杖到期的時間，請參閱時間戳記到期： AWS WAF 權杖豁免時間。

在用戶端瀏覽器中執行的 JavaScript 應用程式無法使用標頭

使用 CAPTCHA 或挑戰 AWS WAF 回應回應來回應用戶端要求時，不包含跨來源資源共用 (CORS) 標頭。CORS 標頭是一組訪問控制標頭，它告訴客戶端 Web 瀏覽器哪些域，HTTP 方法和 HTTP 標頭可以由 JavaScript應用程序使用。如果沒有 CORS 標頭，在 JavaScript 用戶端瀏覽器中執行的應用程式就不會被授與 HTTP 標`x-amzn-waf-action`頭的存取權，因此無法讀取CAPTCHA和Challenge回應中提供的標頭。

什麼挑戰和驗證碼插頁式的作用

當挑戰插頁式運行時，在客戶端成功響應之後，如果它還沒有令牌，則插頁式初始化一個令牌。然後它使用挑戰解決時間戳更新令牌。

當 CAPTCHA 插頁式運行時，如果客戶端還沒有令牌，CAPTCHA 插頁式首先調用挑戰腳本以挑戰瀏覽器並初始化令牌。然後插頁式運行其驗證碼拼圖。當最終用戶成功完成難題時，插頁式更新帶有 CAPTCHA 解決時間戳的令牌。

在任何一種情況下，在用戶端成功回應且指令碼更新權杖之後，指令碼會使用更新的 Token 重新提交原始 Web 要求。

您可以配置如何 AWS WAF 處理令牌。如需相關資訊，請參閱AWS WAF 網絡請求令牌。

CAPTCHA和日誌和指標中的Challenge操作

CAPTCHA和動Challenge作可以是非終止、類似或終止的Count，例如。Block結果取決於請求是否具有具有動作類型未過期時間戳的有效令牌。

- 有效令牌 — 當操作找到有效的令牌並且未阻止請求時，請按如下方式 AWS WAF 捕獲指標和日誌：

- 遞增 AND RequestsWithValidCaptchaToken 或CaptchaRequests和的量ChallengeRequests度RequestsWithValidChallengeToken。
- 使用CAPTCHA或的動作將相符nonTerminatingMatchingRules項目記錄為項目Challenge。下列清單顯示此類型與CAPTCHA動作相符項目的記錄區段。

```
  "nonTerminatingMatchingRules": [
  {
    "ruleId": "captcha-rule",
    "action": "CAPTCHA",
    "ruleMatchDetails": [],
    "captchaResponse": {
      "responseCode": 0,
      "solveTimestamp": 1632420429
    }
  }
]
```

- 遺失、無效或過期的 Token — 當動作因為遺失或無效的 Token 而封鎖要求時，會 AWS WAF 擷取指標和記錄，如下所示：
  - 遞增CaptchaRequests或的量度ChallengeRequests。
  - 將相符CaptchaResponse項目記錄為含有 HTTP 405 狀態碼的ChallengeResponse項目或含有 HTTP 202 狀態碼的項目。日誌指出請求是否缺少令牌或具有過期的時間戳。該日誌還指出是否向客戶端 AWS WAF 發送 CAPTCHA 插頁式頁面，還是向客戶端瀏覽器發送無聲挑戰。下列清單顯示此類型與CAPTCHA動作相符項目的記錄區段。

```
  "terminatingRuleId": "captcha-rule",
  "terminatingRuleType": "REGULAR",
  "action": "CAPTCHA",
  "terminatingRuleMatchDetails": [],
  ...
  "responseCodeSent": 405,
  ...
  "captchaResponse": {
    "responseCode": 405,
    "solveTimestamp": 0,
    "failureReason": "TOKEN_MISSING"
  }
```

如需有關 AWS WAF 記錄檔的資訊，請參閱記錄 AWS WAF 網頁 ACL 流量。

如需 AWS WAF 測量結果的資訊，請參閱AWS WAF 量度和維度。

如需有關規則動作選項的資訊，請參閱規則動作。

使用和動作的最佳CAPTCHAChallenge作法

請遵循本節中的指導來規劃和實施 AWS WAF 驗證碼或挑戰。

規劃您的驗證碼並挑戰實施

根據您的網站使用情況，要保護的數據的敏感性以及請求類型，確定要在哪裡放置 CAPTCHA 難題或無聲挑戰。選擇您要應用 CAPTCHA 的請求，以便根據需要提出拼圖，但請避免在沒有用處的地方提出它們，並且可能會降低用戶體驗。使用此Challenge動作可執行對使用者影響較小的無訊息挑戰，但仍有助於確認要求來自 JavaScript 已啟用的瀏覽器。

驗證碼謎題和無聲挑戰只能在瀏覽器訪問 HTTPS 端點時運行。瀏覽器客戶端必須在安全上下文中運行才能獲取令牌。

決定在哪裡運行 CAPTCHA 難題和沉默的挑戰你的客戶

識別您不希望受到 CAPTCHA 影響的請求，例如對 CSS 或圖像的請求。僅在必要時使用驗證碼。例如，如果您打算在登錄時進行 CAPTCHA 檢查，並且始終直接從登錄到另一個屏幕將用戶帶到另一個屏幕，則可能不需要在第二個屏幕上進行 CAPTCHA 檢查，並且可能會降低您的最終用戶體驗。

配置您的Challenge並CAPTCHA使用，以便 AWS WAF 僅發送 CAPTCHA 難題和響應`GET`text/html請求的無聲挑戰。您無法運行難題或挑戰來響應`POST`請求，跨源資源共享（CORS）預檢`OPTIONS`請求或任何其他非請求類型`GET`。其他要求類型的瀏覽器行為可能會有所不同，而且可能無法正確處理插頁式廣告。

客戶端可能接受 HTML，但仍無法處理驗證碼或挑戰插頁式。例如，網頁上含有小型 iFrame 的小工具可能接受 HTML，但無法顯示驗證碼或處理它。請避免針對這些類型的要求設置規則動作，與不接受 HTML 的要求相同。

使用CAPTCHA或驗證先前Challenge的令牌獲取

在合法使用者應始終擁有一個有效權杖的位置，您只能使用規則動作來驗證是否存在。在這些情況下，請求是否可以處理插入式項目並不重要。

例如，如果您實施 JavaScript 客戶端應用程序 CAPTCHA API，並在將第一個請求發送到受保護的端點之前立即在客戶端上運行 CAPTCHA 難題，則您的第一個請求應始終包含對挑戰和 CAPTCHA 都有效的令牌。如需用 JavaScript 戶端應用程式整合的資訊，請參閱AWS WAF JavaScript 整合。

在此情況下，您可以在 Web ACL 中新增符合此第一個呼叫的規則，並使用Challenge或CAPTCHA規則動作來設定。當規則與合法的終端使用者和瀏覽器相符時，動作會找到有效的 Token，因此不會封鎖要求，也不會傳送挑戰或 CAPTCHA 拼圖作為回應。如需規則動作如何運作的詳細資訊，請參閱CAPTCHA和行Challenge動行為。

使用和保護您的敏感非 HTML 資料 CAPTCHAChallenge

您可以通過以下方法對敏感的非 HTML 數據（例如 API）使用驗證碼和Challenge保護。

1. 識別接受 HTML 回應的要求，並且在接近您敏感、非 HTML 資料要求的要求時執行的要求。
2. 撰寫CAPTCHA或符合 HTML 要求並符合您敏感資料要求的Challenge規則。
3. 調整您的CAPTCHA和Challenge免疫時間設置，以便對於一般用戶互動，客戶端從 HTML 請求中獲得的令牌可用，並且在對您敏感數據的請求中未過期。如需調整資訊，請參閱時間戳記到期： AWS WAF 權杖豁免時間。

當您的敏感數據的請求匹配CAPTCHA或Challenge規則時，如果客戶端仍然具有來自先前難題或挑戰的有效令牌，則不會阻止它。如果令牌不可用或時間戳記已過期，則訪問敏感數據的請求將失敗。如需規則動作如何運作的詳細資訊，請參閱CAPTCHA和行Challenge動行為。

使用驗證碼並Challenge調整您現有的規則

檢閱您現有的規則，查看是否要變更或新增規則。以下是一些需要考慮的常見情況。

- 如果您有封鎖流量的速率型規則，但是您將速率限制保持相對較高以避免封鎖合法使用者，請考慮在封鎖規則之後新增第二個以速率為基礎的規則。指定第二個規則比封鎖規則下限，並將規則動作設定為CAPTCHA或Challenge。封鎖規則仍會封鎖速率過高的要求，而新規則會以更低的速率封鎖大部分自動化流量。如需以比率為基礎的規則的資訊，請參閱速率型規則陳述式。
- 如果您有封鎖要求的受管規則群組，您可以將部分或所有規則的行為從切換Block至CAPTCHA或Challenge。若要這麼做，請在受管規則群組組態中覆寫規則動作設定。如需有關覆寫規則動作的資訊，請參閱規則群組規則動作覆寫。

在部署驗證碼之前對其進行測試並提出挑戰

至於所有新功能，請遵循的指導the section called “測試和調整您的保護”。

在測試過程中，請查看令牌時間戳記到期要求，並設置 Web ACL 和規則級別免疫時間配置，以便在控制對網站的訪問和為客戶提供良好體驗之間取得良好的平衡。如需相關資訊，請參閱時間戳記到期： AWS WAF 權杖豁免時間。

記錄 AWS WAF 網頁 ACL 流量

您可以啟用日誌記錄取得您 Web ACL 分析流量的詳細資訊。記錄的資訊包括從您的 AWS 資源 AWS WAF 接收 Web 要求的時間、有關請求的詳細資訊，以及有關要求符合之規則的詳細資訊。您可以將 Web ACL 日誌傳送到 Amazon CloudWatch 日誌日誌群組、Amazon 簡單儲存服務 (Amazon S3) 儲存貯體或亞馬遜資料 Firehose 交付串流。

其他數據收集和分析選項

除了記錄之外，您還可以啟用下列資料收集和分析選項：

- Amazon 安全湖 — 您可以設定安全湖來收集 Web ACL 資料。Security Lake 會從各種來源收集記錄和事件資料，以進行標準化、分析和管理。如需此選項的相關資訊，請參閱什麼是 Amazon 安全湖？ 以及從 Amazon 安全湖使用者指南中的 AWS 服務收集資料。

  AWS WAF 使用此選項不會向您收取費用。如需定價資訊，請參閱 Amazon Security Lake 使用者指南中的安全湖定價以及安全湖定價的決定方式。
- 請求抽樣 — 您可以配置 Web ACL 來對其評估的 Web 請求進行採樣，以了解應用程序接收的流量類型。如需此選項的詳細資訊，請參閱檢視 Web 請求的範例。

> **Note**
>
> Web ACL 記錄設定只會影響記 AWS WAF 錄檔。特別是，用於記錄的編輯欄位設定對請求取樣或 Security Lake 資料收集沒有影響。安全湖資料收集完全透過安全湖服務進行設定。從取樣請求中排除欄位的唯一方法是停用 Web ACL 的取樣。

主題

記錄網頁 ACL 流量資訊的定價

系統會根據與每個記錄目標類型相關聯的成本，向您收取記錄 Web ACL 流量資訊的費用。這些費用是除了使用費用之外的費用 AWS WAF。您的費用可能會因為因素而有所不同，例如您選擇的目的地類型和記錄的資料量。

下列提供每個記錄目的地型態之訂價資訊的連結：

- CloudWatch 防護記錄 — 費用是針對付費記錄傳送。請參閱 Amazon CloudWatch 日誌定價。在 [付費層] 下，選擇 [記錄] 索引標籤，然後在 [付費記錄檔] 下方，查看傳送至 CloudWatch 記錄檔的資訊。
- Amazon S3 儲存貯體 — Amazon S3 費用是將日誌付費 CloudWatch 日誌交付到 Amazon S3 儲存貯體和使用 Amazon S3 的合併費用。
  - 對於 Amazon S3，請參閱 Amazon S3 定價。
  - 如需將 CloudWatch 日誌付費日誌交付至 Amazon S3 的相關資訊，請參閱 Amazon CloudWatch 日誌定價。在 [付費方案] 下，選擇 [記錄] 索引標籤，然後在 [付費記錄] 下方，查看交付至 S3 的資訊
- Firehose — 查看 Amazon 數據 Firehose 定價。

如需 AWS WAF 定價的相關資訊，請參閱AWS WAF 定價。

AWS WAF 記錄目的地

本節說明您可以為記錄選擇的記 AWS WAF 錄選項。每個區段都提供設定記錄的指引，包括目的地類型特定之任何行為的相關資訊。設定記錄目的地之後，您可以將其規格提供給您的 Web ACL 記錄設定，以開始記錄到它。

主題

- Amazon CloudWatch 日誌日誌組
- Amazon 簡單存儲服務桶
- Amazon 數據 Firehose 交付流

Amazon CloudWatch 日誌日誌組

本主題提供將 Web ACL 流量記錄檔傳送至記錄檔記 CloudWatch 錄群組的相關資訊。

> **Note**
>
> 除了使用費外，您還需要支付登錄費用 AWS WAF。如需相關資訊，請參閱記錄網頁 ACL 流量資訊的定價。

若要將日誌傳送到 Amazon CloudWatch 日誌，請建立 CloudWatch 日誌日誌群組。啟用登入時 AWS WAF，請提供記錄群組 ARN。啟用 Web ACL 的記錄之後，會將記錄 AWS WAF 傳送到記錄串流中的記錄 CloudWatch 檔記錄群組。

使用 CloudWatch 記錄檔時，您可以在 AWS WAF 主控台中瀏覽 Web ACL 的記錄。在您的 Web ACL 頁面中，選取 [記錄見解] 索引標籤。此選項是透過 CloudWatch 主控台為 Lo CloudWatch gs 提供的記錄深入解析之外的其他選項。

在與 AWS WAF Web ACL 相同的區域中設定 Web ACL 記錄的記錄群組，並使用與管理 Web ACL 相同的帳戶。如需設定記 CloudWatch 錄檔記錄群組的詳細資訊，請參閱使用記錄群組和記錄串流。

CloudWatch 記錄檔記錄群組的配額

CloudWatch 記錄具有輸送量的預設最大配額，可供區域內的所有記錄群組共用，您可以要求增加。如果您的記錄需求對於目前的輸送量設定而言太高，您會看到帳戶的`PutLogEvents`節流指標。若要在「Service Quotas」主控台中檢視限制並要求增加，請參閱CloudWatch 記錄配 PutLogEvents 額。

記錄群組命名

您的記錄群組名稱必須以您喜歡的任何尾碼開頭，`aws-waf-logs-`並且可以結尾，例如`aws-waf-logs-testLogGroup2`。

產生的 ARN 格式如下：

```
arn:aws:logs:Region:account-id:log-group:aws-waf-logs-log-group-suffix
```

記錄串流具有下列命名格式：

```
Region_web-acl-name_log-stream-number
```

以下顯示區域`TestWebACL`中 Web ACL 的記錄資料流範例`us-east-1`。

```
us-east-1_TestWebACL_0
```

將記錄檔發佈至記錄檔所需的 CloudWatch 權限

為記錄 CloudWatch 檔記錄群組設定 Web ACL 流量記錄需要本節所述的權限設定。當您使用其中一個 AWS WAF 完整存取受管理的原則時，會為您設定權限，`AWSWAFConsoleFullAccess`或`AWSWAFFullAccess`。如果您想要管理更精細的記錄和 AWS WAF 資源存取權限，您可以自行設定權限。如需管理許可的相關資訊，請參閱 IAM 使用者指南中的 AWS 資源存取管理。如需有關 AWS WAF 受管理策略的資訊，請參閱AWS 受管理的政策 AWS WAF。

這些權限可讓您變更 Web ACL 記錄設定、設定記錄 CloudWatch 檔的記錄傳遞，以及擷取記錄群組的相關資訊。這些權限必須附加至您用來管理的使用者 AWS WAF。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[

            "wafv2:PutLoggingConfiguration",
            "wafv2:DeleteLoggingConfiguration"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow",
         "Sid":"LoggingConfigurationAPI"
      }
      {
         "Sid":"WebACLLoggingCWL",
         "Action":[
            "logs:CreateLogDelivery",
            "logs:DeleteLogDelivery",
            "logs:PutResourcePolicy",
            "logs:DescribeResourcePolicies",
            "logs:DescribeLogGroups"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow"
      }
   ]
```

```
}
```

當允許對所有 AWS 資源執行動作時，會在策略中以"Resource"設定表示"*"。這表示每個動作支援的所有 AWS 資源都允許執行這些動作。例如，只有wafv2記錄組態資源才支援動作wafv2:PutLoggingConfiguration。

Amazon 簡單存儲服務桶

本主題提供將網頁ACL流量日誌傳送到 Amazon S3 儲存貯體的相關資訊。

> **Note**
>
> 除了使用費外，您還需要支付登錄費用 AWS WAF。如需相關資訊，請參閱 記錄網頁 ACL 流量資訊的定價。

若要將您的網路ACL流量日誌傳送到 Amazon S3，請使用與管理網路相同的帳戶設定 Amazon S3 儲存貯體ACL，並以開頭命名該儲存貯體aws-waf-logs-。啟用登入功能時 AWS WAF，您需要提供值區名稱。如需建立記錄值區的詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的建立儲存貯體。

您可以使用亞馬遜雅典娜互動式查詢服務存取和分析 Amazon S3 日誌。Athena 可讓您輕鬆地使用標準直接在 Amazon S3 中分析資料SQL。只SQL要在中執行一些動作 AWS Management Console，您就可以將 Athena 指向存放在 Amazon S3 中的資料，然後快速開始使用標準執行臨機操作查詢並取得結果。如需詳細資訊，請參閱 Amazon Athena 使用者指南中的查詢 AWS WAF 記錄。如需其他 Amazon Athena 查詢範例，請參閱網站上的 AWS 範例/waf-log-sample-athena-查詢。 GitHub

> **Note**
>
> AWS WAF 針對金鑰類型 Amazon S3 金鑰 (SSE-S3) 和 AWS Key Management Service (SSE-KMS) AWS KMS keys，支援使用 Amazon S3 儲存貯體加密。 AWS WAF 不支援由管理的 AWS Key Management Service 金鑰加密 AWS。

您的ACLs網路每隔 5 分鐘將其日誌檔發佈到 Amazon S3 儲存貯體。每個記錄檔都包含前 5 分鐘內記錄之流量的記錄檔記錄。

日誌檔的大小上限為 75 MB。如果日誌檔在 5 分鐘內達到檔案大小限制，則日誌會停止向其新增記錄，將其發佈到 Amazon S3 儲存貯體，然後建立新的日誌檔。

日誌檔案已壓縮。如果您使用 Amazon S3 主控台開啟檔案，Amazon S3 會將日誌記錄解壓縮並顯示。如果您下載記錄檔，則必須將它們解壓縮才能檢視記錄。

單一記錄檔包含具有多筆記錄的交錯項目。若要查看網路的所有記錄檔ACL，請尋找依網路ACL名稱、地區和您的帳戶 ID 彙總的項目。

命名需求和語法

用於 AWS WAF 記錄的值區名稱必須以您想要的任何尾碼開頭，`aws-waf-logs-`並且可以結尾。例如：`aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX`。

鏟斗位置

值區位置使用下列語法：

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/
```

水桶 ARN

存儲桶 Amazon 資源名稱（ARN）的格式如下：

```
arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX
```

含有前置字元的值區位置

如果您在物件金鑰名稱中使用字首來組織儲存在值區中的資料，您可以在記錄值區名稱中提供前置字元。

> **Note**
>
> 此選項無法透過主控台使用。使用 AWS WAF APIsCLI、或 AWS CloudFormation。

如需在 Amazon S3 中使用前置字元的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用前置詞組織物件。

含前置字元的值區位置使用下列語法：

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/DOC-EXAMPLE-KEY-NAME-PREFIX/
```

值區資料夾和檔案名稱

在值區內，並遵循您提供的任何前置字元後，您的 AWS WAF 記錄會寫入資料夾結構之下，該資料夾結構取決於您的帳戶 ID、地區、網頁ACL名稱以及日期和時間。

```
AWSLogs/account-id/WAFLogs/Region/web-acl-name/YYYY/MM/dd/HH/mm
```

在資料夾內，記錄檔名稱的格式類似：

```
account-id_waflogs_Region_web-acl-name_timestamp_hash.log.gz
```

資料夾結構和記錄檔名稱中使用的時間規格會遵循時間戳記格式規格YYYYMMddTHHmmZ。

以下顯示 Amazon S3 儲存貯體中名為的儲存貯體的日誌檔範例DOC-EXAMPLE-BUCKET。是 AWS 帳戶 的11111111111。網絡ACL是TEST-WEBACL，地區是us-east-1。

```
s3://DOC-EXAMPLE-BUCKET/AWSLogs/11111111111/WAFLogs/us-east-1/
TEST-WEBACL/2021/10/28/19/50/11111111111_waflogs_us-east-1_TEST-
WEBACL_20211028T1950Z_e0ca43b5.log.gz
```

> **Note**
>
> 用於 AWS WAF 記錄的值區名稱必須以您想要的任何尾碼開頭，aws-waf-logs-並且可以結尾。

將日誌發佈到 Amazon S3 所需的許可

為 Amazon S3 儲存貯體設定 Web ACL 流量記錄需要下列許可設定。當您使用其中一個 AWS WAF 完整存取受管理的原則時，會為您設定這些權限，AWSWAFConsoleFullAccess或AWSWAFFullAccess。如果您想要管理更精細的記錄和 AWS WAF 資源存取權限，您可以自行設定這些權限。如需有關管理權限的資訊，請參閱《IAM使用指南》中的 AWS 資源存取管理。如需有關 AWS WAF 受管理策略的資訊，請參閱AWS 受管理的政策 AWS WAF。

下列權限可讓您變更 Web 記ACL錄組態，以及設定 Amazon S3 儲存貯體的日誌傳遞。這些權限必須附加至您用來管理的使用者 AWS WAF。

> **Note**
>
> 當您設定下列權限時，您可能會在記錄 AWS CloudTrail 檔中看到錯誤，表示存取遭拒，但權限對於 AWS WAF 記錄而言是正確的。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "wafv2:PutLoggingConfiguration",
            "wafv2:DeleteLoggingConfiguration"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow",
         "Sid":"LoggingConfigurationAPI"
      },
    {

       "Sid":"WebACLLogDelivery",

       "Action":[

          "logs:CreateLogDelivery",

          "logs:DeleteLogDelivery"

       ],

       "Resource": "*",

       "Effect":"Allow"

    },
      {
         "Sid":"WebACLLoggingS3",
         "Action":[
            "s3:PutBucketPolicy",
            "s3:GetBucketPolicy"
```

```
         ],
         "Resource": [
                "arn:aws:s3:::aws-waf-logs-amzn-s3-demo-bucket"
         ],
         "Effect":"Allow"
      }
   ]
}
```

當允許對所有 AWS 資源執行動作時，會在策略中以"Resource"設定為指示"*"。這表示每個動作支援的所有 AWS 資源都允許執行這些動作。例如，只有wafv2記錄組態資源才支援動作wafv2:PutLoggingConfiguration。

根據預設，Amazon S3 儲存貯體及其包含的物件都是私有的。只有儲存貯體擁有者可存取儲存貯體及存放於其中的物件。但是，值區擁有者可以透過撰寫存取原則來授與其他資源和使用者的存取權。

如果建立記錄檔的使用者擁有該值區，服務會自動將下列原則附加至值區，以授予記錄檔發佈至該值區的記錄權限：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::aws-waf-logs-amzn-s3-demo-bucket/AWSLogs/account-id/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceAccount": ["account-id"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
        }
      }
    },
    {
      "Sid": "AWSLogDeliveryAclCheck",
      "Effect": "Allow",
```

```
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::aws-waf-logs-amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": ["account-id"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
        }
      }
    }
  ]
}
```

> **Note**
>
> 用於 AWS WAF 記錄的值區名稱必須以您想要的任何尾碼開頭，aws-waf-logs-並且可以結尾。

如果建立記錄的使用者不擁有值區，或者沒有值區的GetBucketPolicy和PutBucketPolicy權限，則記錄建立會失敗。在此情況下，值區擁有者必須手動將上述政策新增至值區，並指定記錄建立者的 AWS 帳戶 ID。如需詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南中的我該如何新增 S3 儲存貯體政策？。如果值區收到來自多個帳戶的記錄，請在每個帳戶的AWSLogDeliveryWrite政策聲明中新增Resource元素項目。

例如，下列值區政策允許 AWS 帳戶 111122223333將記錄發佈到名為的值區aws-waf-logs-*amzn-s3-demo-bucket*：

```
{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryWrite20150319",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
```

```
            },
            "Action": "s3:PutObject",
                "Resource": "arn:aws:s3:::aws-waf-logs-amzn-s3-demo-bucket/
AWSLogs/111122223333/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": ["111122223333"]
                },
                "ArnLike": {
                    "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::aws-waf-logs-amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                "aws:SourceAccount": ["111122223333"]
                },
                "ArnLike": {
                "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
                }
            }
        }
    ]
}
```

搭配KMS金鑰使 AWS Key Management Service 用的權限

如果您的記錄目的地使用伺服器端加密與儲存在 AWS Key Management Service (SSE-KMS) 中的金鑰，而您使用客戶管理的金KMS鑰 (金鑰)，則必須 AWS WAF 授予使用金KMS鑰的權限。若要這麼做，請將金鑰原則新增至所選目的地的KMS金鑰。這允許 AWS WAF 記錄將日誌文件寫入目的地。

將下列金鑰政策新增至您的KMS金鑰， AWS WAF 以便登入 Amazon S3 儲存貯體。

```
{
```

```
    "Sid": "Allow AWS WAF to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*"
}
```

存取 Amazon S3 日誌檔所需的許可

Amazon S3 使用存取控制清單 (ACLs) 來管理對日誌建立的日誌檔的存取。 AWS WAF 根據預設，儲存貯體擁有者擁有各個日誌檔案的 FULL_CONTROL 許可。日誌交付擁有者與儲存貯體擁有者不同時，就沒有任何許可。日誌交付帳戶擁有 READ 與 WRITE 許可。如需詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的存取控制清單 (ACL) 概觀。

Amazon 數據 Firehose 交付流

本節提供將網頁 ACL 流量日誌傳送至 Amazon 資料 Firehose 交付串流的相關資訊。

> **Note**
>
> 除了使用費外，您還需要支付登錄費用 AWS WAF。如需相關資訊，請參閱記錄網頁 ACL 流量資訊的定價。

若要將日誌傳送到 Amazon 資料 Firehose，您可以將日誌從您的網路 ACL 傳送到 Amazon 資料 Firehose 交付串流，您可以在 Firehose 中設定該串流。啟用記錄後，會透過 Firehose 的 HTTPS 端點將記錄 AWS WAF 傳送至儲存目的地。

一個 AWS WAF 日誌相當於一個 Firehose 記錄。如果您通常每秒收到 10,000 個請求，而且啟用了完整記錄，則 Firehose 中的每秒應該有 10,000 筆記錄設定。如果您未正確設定 Firehose， AWS WAF 將不會記錄所有記錄檔。如需詳細資訊，請參閱 Amazon Kinesis Data Firehose 配額。

如需如何建立 Amazon 資料 Firehose 交付串流和檢閱儲存的日誌的相關資訊，請參閱什麼是 Amazon 資料 Fire hose？

如需建立交付串流的相關資訊，請參閱建立 Amazon 資料 Firehose 交付串流。

為您的網頁 ACL 設定 Amazon 資料 Firehose 交付串流

為您的網路 ACL 設定 Amazon 資料 Firehose 交付串流，如下所示。

- 使用與管理 Web ACL 相同的帳戶建立它。
- 在與 Web ACL 相同的區域中建立它。如果您要擷取 Amazon 的日誌 CloudFront，請在美國東部 (維吉尼亞北部) 區域建立 Firehose。`us-east-1`
- 為資料提供以前綴`aws-waf-logs-`開頭的名稱。例如 `aws-waf-logs-us-east-2-analytics`。
- 將其設定為直接 put，這可讓應用程式直接存取交付串流。在 Amazon 資料 Firehose 主控台中，對於交付串流來源設定，請選擇直接 PUT 或其他來源。透過 API，將交付串流屬性設定`DeliveryStreamType`為`DirectPut`。

> **Note**
>
> 請勿使用 a `Kinesis stream` 作為來源。

將日誌發佈到 Amazon 資料 Firehose 交付串流所需的許可

若要瞭解 Kinesis Data Firehose 組態所需的許可，請參閱使用 Amazon Kinesis Data Firehose 控制存取。

您必須具備下列許可，才能透過 Amazon 資料 Firehose 交付串流成功啟用 Web ACL 記錄。

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

如需服務連結角色和`iam:CreateServiceLinkedRole`權限的相關資訊，請參閱使用服務連結角色 AWS WAF。

網頁 ACL 記錄設定

您可以隨時啟用和停用 Web ACL 的記錄。

> **Note**
>
> 除了使用費外，您還需要支付登錄費用 AWS WAF。如需相關資訊，請參閱記錄網頁 ACL 流量資訊的定價。

如果您在日誌中找不到日誌記錄

在極少數情況下，記 AWS WAF 錄傳送可能會降至 100% 以下，並以最佳方式傳送記錄。與所有其他考量相比，該 AWS WAF 架構會優先考慮應用程式的安全性。在某些情況下，例如當記錄流程遇到流量限制時，這可能會導致記錄被丟棄。這應該不會影響超過幾條記錄。如果您發現許多記錄項目遺失，請聯絡中AWS Support 心。

在 Web ACL 的記錄設定中，您可以自訂 AWS WAF 傳送至記錄的內容。

- 欄位密文 — 您可以從使用對應比對設定之規則的記錄記錄中編輯下列欄位：URI 路徑、查詢字串、單一標題和 HTTP 方法。已編輯的欄位在記錄檔REDACTED中顯示為。例如，如果您編輯了 [查詢字串] 欄位，則記錄檔中的 [查詢字串] 欄位會列REDACTED為使用 [查詢字串比對] 元件設定的所有規則。密文只會套用至您在規則中指定要比對的要求元件，因此 S ingle 標頭元件的密文不會套用至符合標頭的規則。如需記錄欄位的清單，請參閱日誌欄位。

  > **Note**
  >
  > 此設定對請求取樣沒有影響。使用請求取樣時，排除欄位的唯一方法是停用 Web ACL 的取樣。

- 防護記錄篩選 — 您可以新增篩選，以指定哪些 Web 要求會保留在防護記錄中，哪些要求會被捨棄。您可以篩選 Web 要求評估期間 AWS WAF 套用的設定。您可以篩選下列設定：
  - 完全限定標籤 — 完全限定的標籤具有前置詞、可選命名空間和標籤名稱。字首可識別新增標籤之規則的規則群組或 Web ACL 內容。如需有關標示的資訊，請參閱AWS WAF 標籤, 上, 网, 請求。
  - 規則動作 — 您可以篩選任何一般規則動作設定，也可以篩選規則群組規則的舊版EXCLUDED_AS_COUNT覆寫選項。如需有關規則動作設定的資訊，請參閱規則動作。如需有關規則群組規則之目前和舊版規則動作覆寫的資訊，請參閱規則群組的動作覆寫選項。
    - 一般規則動作篩選器會套用至規則中設定的動作，以及使用目前選項來覆寫規則群組規則動作所配置的動作。
    - EXCLUDED_AS_COUNT防護記錄篩選器會與Count動作記錄篩選器重疊。EXCLUDED_AS_COUNT篩選目前和舊版選項，以Count將規則群組規則動作覆寫為。

啟用網頁 ACL 的記錄功能

若要啟用 Web ACL 的記錄功能，您必須已設定記錄目的地。如需目的地選項及每個選項需求的相關資訊，請參閱AWS WAF 記錄目的地。

啟用 Web ACL 記錄

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中，選擇 Web ACL。
3. 選擇您要啟用記錄功能的 Web ACL 名稱。主控台會將您帶到 Web ACL 的描述，您可以在其中編輯它。
4. 在記錄標籤中，選擇啟用記錄。
5. 選擇記錄目的地類型，然後選擇您設定的記錄目的地。您必須選擇名稱開頭的記錄目的地`aws-waf-logs-`。
6. (選擇性) 如果您不希望記錄中包含某些欄位，請將其編輯為其編輯。選擇要編寫的欄位，然後選擇新增。重複其他需要編寫的欄位。

   > **Note**
   >
   > 此設定對請求取樣沒有影響。使用請求取樣時，排除欄位的唯一方法是停用 Web ACL 的取樣。

7. (選擇性) 如果您不想將所有要求傳送至記錄檔，請新增篩選條件和行為。在「篩選記錄檔」下方，針對您要套用的每個篩選器，選擇「新增篩選器」，然後選擇您的篩選條件，並指定要保留或刪除符合條件的要求。完成新增篩選器後，如有需要，請修改預設記錄行為。
8. 選擇 Enable Logging (啟用記錄日誌)。

   > **Note**
   >
   > 當您成功啟用記錄時， AWS WAF 將建立具有必要權限的服務連結角色，以將記錄檔寫入記錄目的地。如需更多詳細資訊，請參閱 使用服務連結角色 AWS WAF。

日誌欄位

下列清單說明可能的記錄檔欄位。

動作

AWS WAF 套用至要求的終止動作。這表示允許，阻止，驗證碼或挑戰。當 Web 請求不包含有效令牌時，CAPTCHA和Challenge操作將終止。

args

查詢字串。

驗證碼

請求的 CAPTCHA 操作狀態，當一個CAPTCHA動作被應用到請求填充。此欄位會針對任何CAPTCHA動作填入，無論是終止還是非終止動作。如果要求多次套用CAPTCHA動作，則會從上次套用動作開始填入此欄位。

當請求不包含令牌或令牌無效或過期時，該CAPTCHA操作終止 Web 請求檢查。如果CAPTCHA動作正在終止，此欄位會包含回應代碼和失敗原因。如果動作未終止，則此欄位會包含解決時間戳記。若要區分終止動作與非終止動作，您可以篩選此欄位中的非空白`failureReason`屬性。

挑戰回應

要求的挑戰動作狀態，會在將Challenge動作套用至要求時填入。此欄位會針對任何Challenge動作填入，無論是終止還是非終止動作。如果要求多次套用Challenge動作，則會從上次套用動作開始填入此欄位。

當請求不包含令牌或令牌無效或過期時，該Challenge操作終止 Web 請求檢查。如果Challenge動作正在終止，此欄位會包含回應代碼和失敗原因。如果動作未終止，則此欄位會包含解決時間戳記。若要區分終止動作與非終止動作，您可以篩選此欄位中的非空白`failureReason`屬性。

clientIp

傳送請求的用戶端 IP 地址。

國家/地區

請求來源的國家/地區。如果 AWS WAF 無法確定原產國，則會將此欄位設定為`-`。

excludedRules

僅用於規則群組規則。規則群組中已排除的規則清單。這些規則的動作設定為Count。

如果您使用覆寫規則動作選項覆寫要計數的規則，則此處不會列出相符項目。它們被列為動作配對`action`和`overriddenAction`。

exclusionType

表示排除的規則具有動作的類型Count。

ruleId

在規則群組中被排除的規則 ID。

formatVersion

日誌的格式版本。

標頭

標題清單。

httpMethod

請求的 HTTP 方法。

httpRequest

請求的中繼資料。

httpSourceId

關聯資源的 ID：

- 對於 Amazon CloudFront 分發，ID 是 ARN 語法*distribution-id*中的 ID：

  arn:*partition*cloudfront::*account-id*:distribution/*distribution-id*
- 對於 Application Load Balancer，ID 是 ARN 語法*load-balancer-id*中的：

  arn:*partition*:elasticloadbalancing:*region*:*account-id*:loadbalancer/app/*load-balancer-name/load-balancer-id*
- 對於 Amazon API Gateway REST API，該識別碼是 ARN 語法*api-id*中的標識：

  arn:*partition*:apigateway:*region*::/restapis/*api-id*/stages/*stage-name*
- 對於一個 AWS AppSync GraphQL API，識別碼是 ARN 語法*GraphQLApiId*中的：

  arn:*partition*:appsync:*region*:*account-id*:apis/*GraphQLApiId*
- 對於 Amazon Cognito 使用者集區而言，識別碼是 ARN 語法*user-pool-id*中的識別碼：

  arn:*partition*:cognito-idp:*region*:*account-id*:userpool/*user-pool-id*
- 對於 AWS App Runner 服務，識別碼是 ARN 語法*apprunner-service-id*中的：

`arn:partition:apprunner:region:account-id:service/apprunner-service-name/apprunner-service-id`

httpSourceName

請求的來源。可能的值：CF適用於 Amazon CloudFront、APIGW Amazon API Gateway、應ALB用程式負載平衡器、用APPSYNCCOGNITOIDP於 AWS AppSync Amazon Cognito、應APPRUNNER用程式執行器，以及VERIFIED_ACCESS已驗證存取。

httpVersion

HTTP 版本。

指紋

要求的 JA3 指紋。

> **Note**
>
> JA3 指紋檢測僅適用於 Amazon CloudFront 分發和應用程式負載平衡器。

JA3 指紋是一個 32 個字元的雜湊，衍生自傳入要求的 TLS 用戶端 Hello。此指紋可做為用戶端 TLS 組態的唯一識別碼。 AWS WAF 針對具有足夠 TLS 用戶端 Hello 資訊進行計算的每個要求，計算並記錄此指紋。

當您在 Web ACL 規則中設定 JA3 指紋比對時，請提供此值。如需有關建立與 JA3 指紋相符項目的詳細資訊，請參閱JA3指紋中的 要求元件選項 for 規則陳述式。

labels

網頁要求上的標籤。這些標籤是由用來評估請求的規則所套用。 AWS WAF 記錄前 100 個標籤。

nonTerminatingMatching規則

符合要求的非終止規則清單。清單中的每個項目都包含下列資訊。

動作

AWS WAF 套用至要求的動作。這表示計數，驗證碼或挑戰。當 Web 要求包含有效權杖時，CAPTCHA和Challenge不會終止。

ruleId

符合要求且未終止的規則識別碼。

ruleMatchDetails

有關符合要求之規則的詳細資訊。只有 SQL 插入和跨網站指令碼 (XSS) 比對規則陳述式才會填入此欄位。相符規則可能需要符合多個檢驗準則，因此這些比對詳細資訊會以符合條件陣列的形式提供。

為每個規則提供的任何其他資訊會因規則組態、規則比對類型和比對詳細資訊等因素而有所不同。例如，對於具有CAPTCHA或Challenge動作的規則，challengeResponse將會列出captchaResponse或。如果比對規則位於規則群組中，且您已覆寫其設定的規則動作，則會在中提供已設定的動作overriddenAction。

超大字段

Web 請求中由 Web ACL 檢查且超過 AWS WAF 檢驗限制的欄位清單。如果欄位過大，但 Web ACL 未檢查，則此處將不會列出該欄位。

此清單可以包含零個或多個下列
值：REQUEST_BODYREQUEST_JSON_BODY、REQUEST_HEADERS、和REQUEST_COOKIES。若要取得有關過大欄位的更多資訊，請參閱處理超大請求組件 AWS WAF。

rateBasedRule清單

處理請求的以速率為基礎的規則名單。如需以比率為基礎的規則的資訊，請參閱速率型規則陳述式。

rateBasedRule識別碼

處理請求的速率規則 ID。若此項目已終止請求，則 rateBasedRuleId 的 ID 將與 terminatingRuleId 的 ID 相同。

rateBasedRule姓名

根據請求採取行動的以費率為基準的規則名稱。

limitKey

規則正在使用的彙總類型。可能的值是IP針對 Web 請求來源，FORWARDED_IP對於在請求標題中轉發的 IP，用CUSTOMKEYS於自定義彙總密鑰設置。並用CONSTANT於將所有請求一起計數，而不進行聚合。

極限值

僅在以單一 IP 位址類型限制速率時使用。如果要求包含無效的 IP 位址，則limitvalue為INVALID.

maxRateAllowed

特定聚總執行處理在指定時間範圍內允許的要求數目上限。彙總執行個體由limitKey加上您在以速率為基礎的規則組態中提供的任何其他索引鍵規格所定義。

evaluationWindowSec

AWS WAF 包含在其請求中的時間計數，以秒為單位。

自訂值

請求中以比率為基準的規則所識別的唯一值。對於字串值，記錄會列印字串值的前 32 個字元。視金鑰類型而定，這些值可能只適用於索引鍵，例如 HTTP 方法或查詢字串，也可能用於索引鍵和名稱，例如用於標頭和標頭名稱。

requestHeadersInserted

插入用於自訂要求處理的標頭清單。

requestId

請求的 ID，由基礎主機服務產生。對於 Application Load Balancer，這是追蹤識別碼。對於所有其他人，這是請求 ID。

responseCodeSent

隨自訂回應一起傳送的回應碼。

ruleGroupId

規則群組的 ID。若規則封鎖請求，則 `ruleGroupID` 的 ID 將與 `terminatingRuleId` 的 ID 相同。

ruleGroupList

針對此要求採取動作的規則群組清單，以及比對資訊。

terminatingRule

終止要求的規則。如果存在，則它包含以下信息。

動作

AWS WAF 套用至要求的終止動作。這表示允許，阻止，驗證碼或挑戰。當 Web 請求不包含有效令牌時，CAPTCHA和Challenge操作將終止。

ruleId

符合要求的規則識別碼。

ruleMatchDetails

有關符合要求之規則的詳細資訊。只有 SQL 插入和跨網站指令碼 (XSS) 比對規則陳述式才會填入此欄位。相符規則可能需要符合多個檢驗準則，因此這些比對詳細資訊會以符合條件陣列的形式提供。

為每個規則提供的任何其他資訊會因規則組態、規則比對類型和比對詳細資訊等因素而有所不同。例如，對於具有CAPTCHA或Challenge動作的規則，`challengeResponse`將會列出`captchaResponse`或。如果比對規則位於規則群組中，且您已覆寫其設定的規則動作，則會在中提供已設定的動作`overriddenAction`。

terminatingRuleId

終止請求的規則 ID。如果無法終止請求，則值為 `Default_Action`。

terminatingRuleMatch詳情

符合請求之終止規則的詳細資訊。終止規則對 Web 請求具有結束檢查程序的動作。終止規則的可能動作包括AllowBlock、CAPTCHA、和Challenge。在檢查 Web 要求期間，在符合要求且具有終止動作的第一個規則中， AWS WAF 會停止檢查並套用動作。除了記錄檔中針對相符終止規則報告的安全威脅外，Web 要求可能還包含其他安全威脅。

這只會為 SQL Injection 和跨網站指令碼 (XSS) 符合規則陳述式填入。相符規則可能需要符合多個檢驗準則，因此這些比對詳細資訊會以符合條件陣列的形式提供。

terminatingRuleType

終止請求的規則類型。可能的值：RATE_BASED、REGULAR、GROUP 和 MANAGED_RULE_GROUP。

timestamp

時間戳記，以毫秒為單位。

uri

URI 請求。

webaclId

Web ACL 的 GUID。

記錄範例

Example 以速率為基礎的規則 1：具有一個索引鍵的規則組態，設定為 **Header:dogname**

```
    {
      "Name": "RateBasedRule",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 100,
          "AggregateKeyType": "CUSTOM_KEYS",
          "CustomKeys": [
            {
              "Header": {
                "Name": "dogname",
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "RateBasedRule"
      }
    }
```

Example 速率型規則 1：以速率為基礎的規則封鎖之要求的記錄項目

```
{
   "timestamp":1683355579981,
   "formatVersion":1,
   "webaclId": ...,
   "terminatingRuleId":"RateBasedRule",
```

```
    "terminatingRuleType":"RATE_BASED",
    "action":"BLOCK",
    "terminatingRuleMatchDetails":[

    ],
    "httpSourceName":"APIGW",
    "httpSourceId":"EXAMPLE11:rjvegx5guh:CanaryTest",
    "ruleGroupList":[

    ],
    "rateBasedRuleList":[
       {
          "rateBasedRuleId": ...,
          "rateBasedRuleName":"RateBasedRule",
          "limitKey":"CUSTOMKEYS",
          "maxRateAllowed":100,
          "evaluationWindowSec":"120",
          "customValues":[
             {
                "key":"HEADER",
                "name":"dogname",
                "value":"ella"
             }
          ]
       }
    ],
    "nonTerminatingMatchingRules":[

    ],
    "requestHeadersInserted":null,
    "responseCodeSent":null,
    "httpRequest":{
       "clientIp":"52.46.82.45",
       "country":"FR",
       "headers":[
          {
             "name":"X-Forwarded-For",
             "value":"52.46.82.45"
          },
          {
             "name":"X-Forwarded-Proto",
             "value":"https"
          },
          {
```

```
            "name":"X-Forwarded-Port",
            "value":"443"
         },
         {
            "name":"Host",
            "value":"rjvegx5guh.execute-api.eu-west-3.amazonaws.com"
         },
         {
            "name":"X-Amzn-Trace-Id",
            "value":"Root=1-645566cf-7cb058b04d9bb3ee01dc4036"
         },
         {
            "name":"dogname",
            "value":"ella"
         },
         {
            "name":"User-Agent",
            "value":"RateBasedRuleTestKoipOneKeyModulePV2"
         },
         {
            "name":"Accept-Encoding",
            "value":"gzip,deflate"
         }
      ],
      "uri":"/CanaryTest",
      "args":"",
      "httpVersion":"HTTP/1.1",
      "httpMethod":"GET",
      "requestId":"Ed0AiHF_CGYF-DA="
   }
}
```

Example 以速率為基礎的規則 2：具有兩個索引鍵的規則組態，設定為**Header:dogname**和**Header:catname**

```
    {
      "Name": "RateBasedRule",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 100,
          "AggregateKeyType": "CUSTOM_KEYS",
          "CustomKeys": [
```

```
            {
              "Header": {
                "Name": "dogname",
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            },
            {
              "Header": {
                "Name": "catname",
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "RateBasedRule"
      }
    }
```

Example 速率型規則 2：以速率為基礎的規則封鎖之要求的記錄項目

```
{
   "timestamp":1633322211194,
   "formatVersion":1,
   "webaclId":...,
   "terminatingRuleId":"RateBasedRule",
   "terminatingRuleType":"RATE_BASED",
```

```
    "action":"BLOCK",
    "terminatingRuleMatchDetails":[

    ],
    "httpSourceName":"APIGW",
    "httpSourceId":"EXAMPLE11:rjvegx5guh:CanaryTest",
    "ruleGroupList":[

    ],
    "rateBasedRuleList":[
       {
          "rateBasedRuleId":...,
          "rateBasedRuleName":"RateBasedRule",
          "limitKey":"CUSTOMKEYS",
          "maxRateAllowed":100,
          "evaluationWindowSec":"120",
          "customValues":[
             {
                "key":"HEADER",
                "name":"dogname",
                "value":"ella"
             },
             {
                "key":"HEADER",
                "name":"catname",
                "value":"goofie"
             }
          ]
       }
    ],
    "nonTerminatingMatchingRules":[

    ],
    "requestHeadersInserted":null,
    "responseCodeSent":null,
    "httpRequest":{
       "clientIp":"52.46.82.35",
       "country":"FR",
       "headers":[
          {
             "name":"X-Forwarded-For",
             "value":"52.46.82.35"
          },
          {
```

```
            "name":"X-Forwarded-Proto",
            "value":"https"
         },
         {
            "name":"X-Forwarded-Port",
            "value":"443"
         },
         {
            "name":"Host",
            "value":"23llbyn8v3.execute-api.eu-west-3.amazonaws.com"
         },
         {
            "name":"X-Amzn-Trace-Id",
            "value":"Root=1-64556629-17ac754c2ed9f0620e0f2a0c"
         },
         {
            "name":"catname",
            "value":"goofie"
         },
         {
            "name":"dogname",
            "value":"ella"
         },
         {
            "name":"User-Agent",
            "value":"Apache-HttpClient/UNAVAILABLE (Java/11.0.19)"
         },
         {
            "name":"Accept-Encoding",
            "value":"gzip,deflate"
         }
      ],
      "uri":"/CanaryTest",
      "args":"",
      "httpVersion":"HTTP/1.1",
      "httpMethod":"GET",
      "requestId":"EdzmlH5OCGYF1vQ="
   }
}
```

Example SQLi 偵測 (終止) 時觸發之規則的記錄輸出

```
{
```

```
    "timestamp": 1576280412771,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/
STMTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
    "terminatingRuleId": "STMTest_SQLi_XSS",
    "terminatingRuleType": "REGULAR",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "HIGH",
            "location": "HEADER",
            "matchedData": [
                "10",
                "AND",
                "1"
            ]
        }
    ],
    "httpSourceName": "-",
    "httpSourceId": "-",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [],
    "httpRequest": {
        "clientIp": "1.1.1.1",
        "country": "AU",
        "headers": [
            {
                "name": "Host",
                "value": "localhost:1989"
            },
            {
                "name": "User-Agent",
                "value": "curl/7.61.1"
            },
            {
                "name": "Accept",
                "value": "*/*"
            },
            {
                "name": "x-stm-test",
                "value": "10 AND 1=1"
            }
```

```
        ],
        "uri": "/myUri",
        "args": "",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "GET",
        "requestId": "rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example SQLi 偵測 (非終止) 時觸發之規則的記錄輸出

```
{
    "timestamp":1592357192516
    ,"formatVersion":1
    ,"webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-
world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
    ,"terminatingRuleId":"Default_Action"
    ,"terminatingRuleType":"REGULAR"
    ,"action":"ALLOW"
    ,"terminatingRuleMatchDetails":[]
    ,"httpSourceName":"-"
    ,"httpSourceId":"-"
    ,"ruleGroupList":[]
    ,"rateBasedRuleList":[]
    ,"nonTerminatingMatchingRules":
    [{
        "ruleId":"TestRule"
        ,"action":"COUNT"
        ,"ruleMatchDetails":
        [{
            "conditionType":"SQL_INJECTION"
            ,"sensitivityLevel": "HIGH"
            ,"location":"HEADER"
            ,"matchedData":[
                "10"
                ,"and"
                ,"1"]
            }]
```

```
    }]
    ,"httpRequest":{
        "clientIp":"3.3.3.3"
        ,"country":"US"
        ,"headers":[
            {"name":"Host","value":"localhost:1989"}
            ,{"name":"User-Agent","value":"curl/7.61.1"}
            ,{"name":"Accept","value":"*/*"}
            ,{"name":"myHeader","myValue":"10 AND 1=1"}
            ]
            ,"uri":"/myUri","args":""
            ,"httpVersion":"HTTP/1.1"
            ,"httpMethod":"GET"
            ,"requestId":"rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example 在規則群組內觸發的多個規則的記錄輸出 (規則-XSS 正在終止，而規則 B 不會終止)

```
{
    "timestamp":1592361810888,
    "formatVersion":1,
    "webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-
world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
    ,"terminatingRuleId":"RG-Reference"
    ,"terminatingRuleType":"GROUP"
    ,"action":"BLOCK",
    "terminatingRuleMatchDetails":
    [{
        "conditionType":"XSS"
        ,"location":"HEADER"
        ,"matchedData":["<","frameset"]
    }]
    ,"httpSourceName":"-"
    ,"httpSourceId":"-"
    ,"ruleGroupList":
    [{
```

```
        "ruleGroupId":"arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/hello-
world/c05lb698-1f11-4m41-aef4-99a506d53f4b"
        ,"terminatingRule":{
            "ruleId":"RuleA-XSS"
            ,"action":"BLOCK"
            ,"ruleMatchDetails":null
            }
        ,"nonTerminatingMatchingRules":
        [{
            "ruleId":"RuleB-SQLi"
            ,"action":"COUNT"
            ,"ruleMatchDetails":
            [{
                "conditionType":"SQL_INJECTION"
                ,"sensitivityLevel": "LOW"
                ,"location":"HEADER"
                ,"matchedData":[
                    "10"
                    ,"and"
                    ,"1"]
            }]
        }]
        ,"excludedRules":null
    }]
    ,"rateBasedRuleList":[]
    ,"nonTerminatingMatchingRules":[]
    ,"httpRequest":{
        "clientIp":"3.3.3.3"
        ,"country":"US"
        ,"headers":
        [
            {"name":"Host","value":"localhost:1989"}
            ,{"name":"User-Agent","value":"curl/7.61.1"}
            ,{"name":"Accept","value":"*/*"}
            ,{"name":"myHeader1","value":"<frameset onload=alert(1)>"}
            ,{"name":"myHeader2","value":"10 AND 1=1"}
            ]
        ,"uri":"/myUri"
        ,"args":""
        ,"httpVersion":"HTTP/1.1"
        ,"httpMethod":"GET"
        ,"requestId":"rid"
    },
    "labels": [
```

```
        {
            "name": "value"
        }
    ]
}
```

Example 針對使用內容類型 JSON 檢查要求主體而觸發之規則的記錄輸出

AWS WAF 目前將 JSON 主體檢查的位置報告為UNKNOWN。

```
{
    "timestamp": 1576280412771,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:123456789012:regional/webacl/test/111",
    "terminatingRuleId": "STMTest_SQLi_XSS",
    "terminatingRuleType": "REGULAR",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "LOW",
            "location": "UNKNOWN",
            "matchedData": [
                "10",
                "AND",
                "1"
            ]
        }
    ],
    "httpSourceName": "ALB",
    "httpSourceId": "alb",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [],
    "requestHeadersInserted":null,
    "responseCodeSent":null,
    "httpRequest": {
        "clientIp": "1.1.1.1",
        "country": "AU",
        "headers": [],
        "uri": "",
        "args": "",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "POST",
```

```
        "requestId": "null"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example 針對具有有效、未過期的 CAPTCHA 權杖的網頁要求，記錄驗證碼規則的輸出

下列記錄清單適用於符合規則與CAPTCHA動作的 Web 要求。Web 請求具有有效且未過期的 CAPTCHA 令牌，並且僅通過驗證碼匹配來標記 AWS WAF，類似於Count操作的行為。此驗證碼匹配在下註明nonTerminatingMatchingRules。

```
{
  "timestamp": 1632420429309,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-
acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "Default_Action",
  "terminatingRuleType": "REGULAR",
  "action": "ALLOW",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "123456789012:b34myvfw0b:pen-test",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [
    {
      "ruleId": "captcha-rule",
      "action": "CAPTCHA",
      "ruleMatchDetails": [],
      "captchaResponse": {
        "responseCode": 0,
        "solveTimestamp": 1632420429
      }
    }
  ],
  "requestHeadersInserted": [
    {
      "name": "x-amzn-waf-test-header-name",
      "value": "test-header-value"
```

```
    }
  ],
  "responseCodeSent": null,
  "httpRequest": {
    "clientIp": "72.21.198.65",
    "country": "US",
    "headers": [
      {
        "name": "X-Forwarded-For",
        "value": "72.21.198.65"
      },
      {
        "name": "X-Forwarded-Proto",
        "value": "https"
      },
      {
        "name": "X-Forwarded-Port",
        "value": "443"
      },
      {
        "name": "Host",
        "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
      },
      {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-614cc24d-5ad89a09181910c43917a888"
      },
      {
        "name": "cache-control",
        "value": "max-age=0"
      },
      {
        "name": "sec-ch-ua",
        "value": "\"Chromium\";v=\"94\", \"Google Chrome\";v=\"94\", \";Not A Brand
\";v=\"99\""
      },
      {
        "name": "sec-ch-ua-mobile",
        "value": "?0"
      },
      {
        "name": "sec-ch-ua-platform",
        "value": "\"Windows\""
      },
```

```
      {
        "name": "upgrade-insecure-requests",
        "value": "1"
      },
      {
        "name": "user-agent",
        "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/94.0.4606.54 Safari/537.36"
      },
      {
        "name": "accept",
        "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
      },
      {
        "name": "sec-fetch-site",
        "value": "same-origin"
      },
      {
        "name": "sec-fetch-mode",
        "value": "navigate"
      },
      {
        "name": "sec-fetch-user",
        "value": "?1"
      },
      {
        "name": "sec-fetch-dest",
        "value": "document"
      },
      {
        "name": "referer",
        "value": "https://b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com/pen-
test/pets"
      },
      {
        "name": "accept-encoding",
        "value": "gzip, deflate, br"
      },
      {
        "name": "accept-language",
        "value": "en-US,en;q=0.9"
      },
      {
```

```
        "name": "cookie",
        "value": "aws-waf-token=51c71352-41f5-4f6d-b676-c24907bdf819:EQoAZ/J
+AAQAAAAA:t9wvxbw042wva7E2Y6lgud/
bS6YG0CJKVAJqaRqDZ140ythKW0Zj9wKB2O8lSkYDRqf1yONcVBFo5u0eYi0tvT4rtQCXsu
+KanAardW8go4QSLw4yoED59lgV7oAhGyCalAzE7ra29j+RvvZPsQyoQuDCrtoY/TvQyMTXIXzGPDC/rKBbg=="
      }
    ],
    "uri": "/pen-test/pets",
    "args": "",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "GINMHHUgoAMFxug="
  }
}
```

Example 針對沒有驗證碼令牌的網絡請求記錄驗證碼規則的輸出

下列記錄清單適用於符合規則與CAPTCHA動作的 Web 要求。網絡請求沒有 CAPTCHA 令牌，並被阻止 AWS WAF。

```
{
  "timestamp": 1632420416512,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-
acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "captcha-rule",
  "terminatingRuleType": "REGULAR",
  "action": "CAPTCHA",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "123456789012:b34myvfw0b:pen-test",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [],
  "requestHeadersInserted": null,
  "responseCodeSent": 405,
  "httpRequest": {
    "clientIp": "72.21.198.65",
    "country": "US",
    "headers": [
      {
        "name": "X-Forwarded-For",
        "value": "72.21.198.65"
```

```
      },
      {
        "name": "X-Forwarded-Proto",
        "value": "https"
      },
      {
        "name": "X-Forwarded-Port",
        "value": "443"
      },
      {
        "name": "Host",
        "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
      },
      {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-614cc240-18b57ff33c10e5c016b508c5"
      },
      {
        "name": "sec-ch-ua",
        "value": "\"Chromium\";v=\"94\", \"Google Chrome\";v=\"94\", \";Not A Brand
\";v=\"99\""
      },
      {
        "name": "sec-ch-ua-mobile",
        "value": "?0"
      },
      {
        "name": "sec-ch-ua-platform",
        "value": "\"Windows\""
      },
      {
        "name": "upgrade-insecure-requests",
        "value": "1"
      },
      {
        "name": "user-agent",
        "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/94.0.4606.54 Safari/537.36"
      },
      {
        "name": "accept",
        "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
      },
```

```
      {
        "name": "sec-fetch-site",
        "value": "cross-site"
      },
      {
        "name": "sec-fetch-mode",
        "value": "navigate"
      },
      {
        "name": "sec-fetch-user",
        "value": "?1"
      },
      {
        "name": "sec-fetch-dest",
        "value": "document"
      },
      {
        "name": "accept-encoding",
        "value": "gzip, deflate, br"
      },
      {
        "name": "accept-language",
        "value": "en-US,en;q=0.9"
      }
    ],
    "uri": "/pen-test/pets",
    "args": "",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "GINKHEssoAMFsrg="
  },
  "captchaResponse": {
    "responseCode": 405,
    "solveTimestamp": 0,
    "failureReason": "TOKEN_MISSING"
  }
}
```

測試和調整您的 AWS WAF 保護

建議您先測試並調整 AWS WAF Web ACL 的任何變更，然後再將變更套用至您的網站或 Web 應用程式流量。

> **⚠ 生產流量風險**
>
> 在針對生產流量部署 Web ACL 實作之前，請先在測試或測試環境中對其進行測試和調整，直到您熟悉流量的潛在影響為止。然後在啟用規則之前，使用生產流量在計數模式下測試和調整規則。

本節提供測試和調整 AWS WAF Web ACL、規則、規則群組、IP 集和規則運算式模式集的指引。

本節也提供一般指導，以測試您使用由其他人管理的規則群組。其中包括 AWS 受管規則規則群組、AWS Marketplace 受管規則群組，以及由其他帳戶與您共用的規則群組。對於這些規則群組，也請遵循從規則群組提供者取得的任何指引。

- 如需機器人控制 AWS 受管規則規則群組的資訊，另請參閱測試和部署 AWS WAF 機器人控制。
- 如需帳戶接 AWS 管預防受管規則規則群組的相關資訊，另請參閱測試和部署可承諾量。
- 如需帳號建立詐騙預防 AWS 受管規則規則群組的相關資訊，另請參閱測試和部署 ACFP。

更新期間暫時不一致

當您建立或變更 Web ACL 或其他 AWS WAF 資源時，變更需要少量時間才能傳播到儲存資源的所有區域。傳輸時間可以是幾秒鐘到分鐘數。

以下是您在變更傳播期間可能會注意到的暫時性不一致的範例：

- 建立 Web ACL 之後，如果您嘗試將其與資源建立關聯，可能會出現例外狀況，指出 Web ACL 無法使用。
- 將規則群組新增至 Web ACL 後，新規則群組規則可能會在使用 Web ACL 的某個區域中生效，而不會在另一個區域中生效。
- 變更規則動作設定後，您可能會在某些地方看到舊動作，而在其他地方看到新動作。
- 將 IP 位址新增至封鎖規則中使用的 IP 集後，該新位址可能會在某個區域遭到封鎖，而另一個區域仍允許使用該 IP 位址。

測試和調整高階步驟

本節提供測試 Web ACL 變更的步驟檢查清單，包括其使用的任何規則或規則群組。

> **Note**
>
> 若要遵循本節中的指引，您需要瞭解如何建立和管理 Web ACL、規則和規則群組等 AWS WAF 保護。本指南前面的章節涵蓋了該資訊。

若要測試和調整您的網路 ACL

請先在測試環境中執行這些步驟，然後在生產環境中執行。

1. 準備測試

   準備監控環境，將新的 AWS WAF 保護切換為計數模式以進行測試，並創建所需的任何資源關聯。

   請參閱準備測試。

2. 在測試和生產環境中進行監控和調整

   首先在測試或測試環境中監控和調整您的 AWS WAF 保護，然後在生產環境中，直到您滿意他們可以根據需要處理流量為止。

   請參閱監控和調整。

3. 在生產環境中啟用您的保護

   如果您對測試保護感到滿意，請將其切換到生產模式，清理所有不必要的測試成品，然後繼續監視。

   請參閱在生產環境中啟用您的保護。

完成變更實作之後，請繼續監視網路流量和生產環境中的保護，以確保它們正常運作，如您所願。Web 流量模式可能會隨著時間而改變，因此您可能需要偶爾調整保護措施。

準備測試

本節說明如何設定以測試和調整您的 AWS WAF 保護。

> **Note**
>
> 若要遵循本節中的指引，您需要一般了解如何建立和管理 Web ACL、規則和規則群組等 AWS WAF 保護。本指南前面的章節涵蓋了該資訊。

為了準備測試

1. 啟用網路 ACL 的網頁 ACL 記錄、Amazon CloudWatch 指標和網路請求取樣

   使用日誌記錄、指標和抽樣來監視 Web ACL 規則與 Web 流量的互動。

   - 記錄 — 您可 AWS WAF 以配置為記錄 Web ACL 評估的 Web 請求。您可以將日誌傳送到 CloudWatch 日誌、Amazon S3 儲存貯體或 Amazon 資料 Firehose 交付串流。您可以標記字段并應用過濾。如需詳細資訊，請參閱 記錄 AWS WAF 網頁 ACL 流量。
   - Amazon 安全湖 — 您可以設定安全湖來收集 Web ACL 資料。Security Lake 會從各種來源收集記錄和事件資料，以進行標準化、分析和管理。如需此選項的相關資訊，請參閱什麼是 Amazon 安全湖？ 以及從 Amazon 安全湖使用者指南中的 AWS 服務收集資料。
   - Amazon CloudWatch 指標 — 在您的 Web ACL 組態中，為您要監控的所有項目提供指標規格。您可以透過 AWS WAF 和 CloudWatch主控台檢視指標。如需詳細資訊，請參閱 使用 Amazon 監控 CloudWatch。
   - Web 請求抽樣 — 您可以檢視 Web ACL 評估的所有 Web 請求範例。如需 Web 請求取樣的詳細資訊，請參閱檢視 Web 請求的範例。
2. 將Count您的保護設定為模式

   在 Web ACL 配置中，將要測試的任何內容切換到計數模式。這會導致測試保護記錄對 Web 請求的匹配，而不會改變請求的處理方式。您將能夠在指標，日誌和採樣請求中查看匹配項，以驗證匹配條件並了解可能對您的網絡流量產生什麼影響。無論規則動作為何，新增標籤至相符請求的規則都會新增標籤。

   - 在 Web ACL 中定義的規則 — 編輯 Web ACL 中的規則，並將其動作設定為Count。
   - 規則群組 — 在 Web ACL 配置中，編輯規則群組的規則陳述式，然後在「規則」窗格中開啟「覆寫所有規則動作」下拉式清單並選擇Count。如果您以 JSON 管理 Web ACL，請將規則新增至規則群組參考陳述式中的`RuleActionOverrides`設定，並將設`ActionToUse`定為 Count。下列範例清單顯示「`AWSManagedRulesAnonymousIpList` AWS 受管規則」規則群組中兩個規則的覆寫。

```
"ManagedRuleGroupStatement": {
  "VendorName": "AWS",
  "Name": "AWSManagedRulesAnonymousIpList",
    "RuleActionOverrides": [
      {
        "ActionToUse": {
          "Count": {}
        },
        "Name": "AnonymousIPList"
      },
      {
        "ActionToUse": {
          "Count": {}
        },
        "Name": "HostingProviderIPList"
      }
    ],
    "ExcludedRules": []
  }
},
```

如需有關規則動作覆寫的詳細資訊，請參閱覆寫規則群組中的規則動作。

針對您自己的規則群組，請勿修改規則群組本身中的規則動作。具有Count動作的規則群組規則不會產生測試所需的量度或其他成品。此外，變更規則群組會影響使用該群組的所有 Web ACL，而 Web ACL 組態內的變更只會影響單一 Web ACL。

- Web ACL — 如果您正在測試新的 Web ACL，請將 Web ACL 的預設動作設定為允許請求。這可讓您試用 Web ACL，而不會以任何方式影響流量。

一般而言，計數模式會產生比生產更多的相符項目。這是因為計算要求的規則不會停止 Web ACL 對要求的評估，因此稍後在 Web ACL 中執行的規則也可能符合要求。當您將規則動作變更為其生產設定時，允許或封鎖要求的規則將會終止符合要求的評估。因此，在 Web ACL 中，通常會使用較少的規則來檢查相符的要求。如需規則動作對 Web 要求整體評估之影響的詳細資訊，請參閱規則動作。

透過這些設定，您的新保護不會改變網路流量，而是會在指標、Web ACL 記錄和要求範例中產生比對資訊。

3. 將網路 ACL 與資源建立關聯

   如果 Web ACL 尚未與資源相關聯，請將其關聯。

   請參閱建立 Web ACL 與資源的關聯或取消關聯 AWS。

現在，您已準備好監控和調整您的 Web ACL。

監控和調整

本節說明如何監控和調整您的 AWS WAF 保護。

> **Note**
>
> 若要遵循本節中的指引，您需要一般了解如何建立和管理 Web ACL、規則和規則群組等 AWS WAF 保護。本指南前面的章節涵蓋了該資訊。

監控網路流量和規則相符項目，以驗證 Web ACL 的行為。如果發現問題，請調整規則以更正，然後進行監視以驗證調整。

重複以下程序，直到 Web ACL 視需要管理您的網路流量為止。

若要監視和調整

1. 監控流量和規則符合

   確保流量正在流動，並且您的測試規則正在找到匹配的請求。

   請尋找下列資訊，瞭解您正在測試的保護措施：

   - 防護記錄 — 存取符合 Web 要求之規則的相關資訊：
     - 您的規則-Web ACL 中具有Count動作的規則會列在下nonTerminatingMatchingRules。具有Allow或的規則Block會列為terminatingRule。具有CAPTCHA或Challenge可以是終止或非終止的規則，因此會根據規則相符的結果列在兩個類別中的其中一個。
     - 規則群組-規則群組會在ruleGroupId欄位中識別，其規則相符項目的分類與獨立規則相同。
     - 標籤-已套用至請求的規則標籤會列在Labels欄位中。

     如需詳細資訊，請參閱 日誌欄位。
   - Amazon CloudWatch 指標 — 您可以存取以下網頁 ACL 請求評估的指標。

- 您的規則 — 量度依規則動作分組。例如，當您在Count模式中測試規則時，其相符項目會列為 Web ACL 的Count度量。
- 您的規則群組 — 規則群組的量度會列在規則群組量度下。
- 另一個帳戶擁有的規則群組 — 規則群組量度通常只有規則群組擁有者才能看到。不過，如果您覆寫規則的規則動作，則該規則的度量會列在您的 Web ACL 量度下。此外，任何規則群組新增的標籤都會列在 Web ACL 量度中

  此類別中的規則群組是AWS 的受管規則 AWS WAF另一個帳戶與您共用的由其他服務提供的規則群組、、和規則群組。AWS Marketplace 受管規則群組
- 標籤-在評估期間新增至 Web 要求的標籤會列在 Web ACL 標籤度量中。您可以存取所有標籤的量度，無論這些標籤是由您的規則和規則群組新增，還是由其他帳戶擁有的規則群組中的規則新增。

如需詳細資訊，請參閱 檢視網路 ACL 的量度。

- Web ACL 流量概觀儀表板 — 前往 AWS WAF 主控台中的 Web ACL 頁面並開啟「流量概觀」索引標籤，即可存取 Web ACL 評估的 Web 流量摘要。

  流量概觀儀表板提供近乎即時的 Amazon CloudWatch 指標摘要，這些指標會在評估應用程式 Web 流量時 AWS WAF 收集到。

  如需詳細資訊，請參閱 網頁 ACL 流量概觀儀表板。
- 已取樣的 Web 請求 — 存取符合 Web 請求取樣之規則的資訊。範例資訊會依 Web ACL 中規則的測量結果名稱來識別相符規則。針對規則群組，測量結果會識別規則群組參照陳述式。對於規則群組內的規則，範例會在中列出相符的規則名稱RuleWithinRuleGroup。

  如需詳細資訊，請參閱 檢視 Web 請求的範例。

2. 設定緩和措施以解決誤判

   如果您判斷規則會產生誤判，則在不應該的情況下比對 Web 要求，下列選項可協助您調整 Web ACL 保護以減輕。

   更正規則檢查條件

   對於您自己的規則，您通常只需要調整用於檢查 Web 請求的設置即可。範例包括變更 regex 模式集中的規格、在檢查前調整您套用至要求元件的文字轉換，或切換至使用轉送的 IP 位址。請參閱下導致問題的規則類型指引規則陳述式基礎。

   修正更複雜的問題

對於您無法控制的檢查準則以及某些複雜規則，您可能需要進行其他變更，例如新增明確允許或封鎖要求的規則，或是排除有問題規則的評估要求的規則。受管規則群組通常需要這種類型的緩和措施，但其他規則也可以。範例包括以速率為基礎的規則陳述式和 SQL 插入攻擊規則陳述式。

你做什麼來減輕誤報取決於你的用例。以下是常見的方法：

- [新增緩解規則] — 新增在新規則之前執行的規則，並明確允許造成誤判的要求。如需有關 Web ACL 中規則評估順序的資訊，請參閱Web ACL 中規則和規則群組的處理順序。

  使用這種方法，允許的請求會發送到受保護的資源，因此它們永遠不會達到評估的新規則。如果新規則是付費受管規則群組，此方法也有助於控制使用規則群組的成本。

- 新增具有緩解規則的邏輯規則 — 使用邏輯規則陳述式將新規則與排除誤判的規則結合在一起。如需相關資訊，請參閱邏輯規則陳述式。

  例如，假設您正在添加 SQL 注入攻擊 match 語句，該語句會為請求類別生成誤報。建立符合這些要求的規則，然後使用邏輯規則陳述式合併規則，讓您只比對兩者都不符合誤判準則且符合 SQL 插入攻擊準則的要求。

- 新增範圍向下陳述式 — 對於以速率為基礎的陳述式和受管規則群組參考陳述式，請在 main 陳述式中新增範圍向下陳述式，從評估中排除產生誤報的要求。

  與範圍向下陳述式不符的要求永遠不會到達規則群組或以速率為基礎的評估。如需有關向下範圍陳述式的資訊，請參閱。範圍向下語句如需範例，請參閱從機器人管理中排除 IP 範圍。

- 新增標籤比對規則 — 對於使用標籤的規則群組，識別有問題的規則套用至請求的標籤。您可能需要先在計數模式中設定規則群組規則 (如果尚未設定)。新增標籤比對規則，定位為在規則群組之後執行，該規則與有問題的規則所新增的標籤相符。在標籤比對規則中，您可以從要封鎖的要求中篩選要允許的要求。

  如果您使用這種方法，當您完成測試時，請將有問題的規則保持在規則群組中的計數模式，並保持自訂標籤比對規則。如需標籤比對陳述式的資訊，請參閱標籤比對規則陳述式。如需範例，請參閱 允許特定的封鎖機器人 和 可承諾量範例：遺失與遭到入侵之認證的自訂處。

- 變更受管規則群組的版本 — 對於版本控制的受管規則群組，變更您正在使用的版本。例如，您可以切換回上次成功使用的靜態版本。

  這通常是暫時的修正程式。您可以在測試或測試環境中繼續測試最新版本，或等待提供者提供更相容的版本時，變更生產流量的版本。如需受管規則群組版本的相關資訊，請參閱受管規則群組。

如果您滿意新規則符合您需要的要求，請移至下一個測試階段，然後重複此程序。在生產環境中執行測試和調整的最後階段。

檢視網路 ACL 的量度

將 Web ACL 與一或多個 AWS 資源建立關聯之後，您可以在 Amazon CloudWatch 圖形中檢視關聯產生的指標。

如需 AWS WAF 測量結果的資訊，請參閱AWS WAF 量度和維度。如需有關指 CloudWatch 標的資訊，請參閱 Amazon CloudWatch 使用者指南。

對於 Web ACL 中的每個規則，以及關聯資源針對 Web ACL 轉發到 AWS WAF 的所有請求，CloudWatch 可讓您執行以下操作：

- 檢視前一小時或三小時前的資料。
- 變更資料點之間的間隔。
- 變更對資料 CloudWatch 執行的計算，例如最大值、最小值、平均值或總和。

> **Note**
>
> AWS WAF the CloudFront 是全域服務和量度只有當您在中選擇美國東部 (維吉尼亞北部) 區域時才可用 AWS Management Console。如果您選擇其他區域， CloudWatch控制台中將不會顯示任何 AWS WAF 指標。

若要在 Web ACL 查看規則資料

1. 請登入 AWS Management Console 並開啟 CloudWatch 主控台，網址為 https://console.aws.amazon.com/cloudwatch/。
2. 如有必要，請將「地區」變更為資 AWS 源所在的地區。對於 CloudFront，選擇美國東部 (維吉尼亞北部) 區域。
3. 在導覽窗格的「量度」下，選擇「所有量度」，然後在「瀏覽」索引標籤下搜尋`AWS::WAFV2`。
4. 選取要檢視資料的 Web ACL 的核取方塊。
5. 變更適用的設定：

   統計數字

   選擇對資料 CloudWatch 執行的計算。

時間範圍

選擇您想要檢視前一小時或前三個小時的資料。

期間

選擇圖形中資料點之間的間隔。

規則

選擇您要檢視資料的規則。

> **Note**
>
> 如果您變更規則的名稱，並希望規則的量度名稱反映變更，您也必須更新量度名稱。AWS WAF 變更規則名稱時，不會自動更新規則的度量名稱。您可以在主控台中編輯規則時，使用規則 JSON 編輯器變更量度名稱。您也可以透過 API 和任何用來定義 Web ACL 或規則群組的 JSON 清單中變更名稱。

注意下列事項：

- 如果您最近將 Web ACL 與 AWS 資源產生關聯，您可能需要等待幾分鐘，資料才會顯示在圖形中，以及 Web ACL 的量度才會顯示在可用量度清單中。
- 如果您將多個資源與 Web ACL 相關聯，資 CloudWatch料將包含對所有這些資源的請求。
- 您可以將游標停留在資料點上以取得更多資訊。
- 圖形不會自動自我重新整理。若要更新顯示，請選擇重新整理 () 圖示。

如需 CloudWatch 測量結果的詳細資訊，請參閱使用 Amazon 監控 CloudWatch。

網頁 ACL 流量概觀儀表板

本節說明主 AWS WAF 控台中的 Web ACL 流量概觀儀表板。將 Web ACL 與一或多個 AWS 資源建立關聯並啟用 Web ACL 的指標後，您可以前往 AWS WAF 主控台中的 Web ACL 的「流量概觀」標籤，存取 Web ACL 評估的 Web 流量摘要。儀表板包括近乎即時的 Amazon CloudWatch 指標摘要，這些指標會在評估應用程式 Web 流量時 AWS WAF 收集到。

> **Note**
>
> 如果您在儀表板上沒有看到任何內容，請確定您已啟用 Web ACL 的指標。

Web ACL 的「流量概觀」標籤包含具有下列資訊類別的標籤式儀表板：

- 所有流量 — Web ACL 評估的所有 Web 請求。

  儀表板焦點是終止動作，但您可以在下列位置檢視計數規則的相符項目：

  - 此儀表板的前 10 個規則窗格。切換切換至計數動作以顯示符合計數規則。
  - 網頁 ACL 頁面的取樣請求索引標籤。這個新標籤包含所有符合規則的圖表。如需相關資訊，請參閱檢視 Web 請求的範例。
- 機器人控制 — Web ACL 使用「機器人控制」管理規則群組評估的 Web 要求。

  如果您沒有在 Web ACL 中使用此規則群組，此標籤會顯示根據機器人控制規則評估 Web 流量取樣的結果。這使您可以了解應用程序接收的機器人流量，並且它是免費的。

  此規則群組是 AWS WAF 提供的智慧型威脅緩和選項的一部分。如需詳細資訊，請參閱 AWS WAF 機器人控制 及 AWS WAF 機器人控制規則群組。
- 帳戶接管預防 — Web ACL 使用 AWS WAF 詐騙控制帳戶接管預防 (ATP) 受管規則群組評估的 Web 要求。只有當您在 Web ACL 中使用此規則群組時，才能使用此索引標籤。

  ATP 規則群組是 AWS WAF 智慧型威脅緩和產品的一部分。如需詳細資訊，請參閱 AWS WAF 防止欺詐控制帳戶接管（ATP） 及 AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組。
- 帳戶建立詐騙預防 — Web ACL 使用詐 AWS WAF 騙控制帳戶建立詐騙預防 (ACFP) 受管規則群組評估的 Web 要求。只有當您在 Web ACL 中使用此規則群組時，才能使用此索引標籤。

  ACFP 規則群組是 AWS WAF 智慧型威脅緩和產品的一部分。如需詳細資訊，請參閱 AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP） 及 AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）規則組。

儀表板以 Web ACL 的 CloudWatch 指標為基礎，圖形可讓您存取中對應量度 CloudWatch。對於智慧型威脅緩解儀表板 (例如 Bot Control)，使用的指標主要是標籤指標。

- 如需提 AWS WAF 供的測量結果清單，請參閱AWS WAF 量度和維度。
- 如需有關指 CloudWatch 標的資訊，請參閱 Amazon CloudWatch 使用者指南。

儀表板會針對您選取的終止動作和日期範圍提供流量模式摘要。智慧型威脅緩和儀表板包含對應的受管規則群組評估的要求，無論受管規則群組本身是否已套用終止動作。例如，如果選取此選項，Block則「帳戶接管預防控制面板」會包含所有 Web 請求的資訊，這些請求均由可承諾量管理規則群組評估，以及在 Web ACL 評估期間某個時間點封鎖的所有 Web 請求。可承諾量管理規則群組、在 Web ACL 中規則群組之後執行的規則，或 Web ACL 預設動作，可封鎖請求。

檢視網頁 ACL 的儀表板

請遵循本節中的程序來存取 Web ACL 儀表板並設定資料篩選準則。如果您最近將 Web ACL 與 AWS 資源相關聯，則可能需要等待幾分鐘，才能在儀表板中使用資料。

儀表板包括您與 Web ACL 相關聯的所有資源的請求。

若要檢視 Web ACL 的流量概觀儀表板

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 在瀏覽窗格中，選擇 [Web ACL]，然後搜尋您感興趣的網頁 ACL。
3. 選取腹板 ACL。主控台會帶您前往網頁 ACL 的頁面。預設會選取 [流量概觀] 索引標籤。
4. 視需要變更資料篩選器設定。

    - 終止規則動作 — 選取要包含在儀表板中的終止動作。儀表板概述了 Web 請求的指標，這些要求具有 Web ACL 評估所套用的其中一個所選動作。如果您選取所有可用的動作，則儀表板會包含所有評估的 Web 請求。如需有關動作的資訊，請參閱如何 AWS WAF 處理 Web ACL 中的規則和規則群組動作。
    - 時間範圍 — 選取要在儀表板中檢視的時間間隔。您可以選擇檢視相對於現在的時間範圍，例如最近 3 小時或上週，也可以從行事曆中選取絕對時間範圍。
    - 時區 — 當您指定絕對時間範圍時，會套用此設定。您可以使用瀏覽器的當地時區或 UTC（國際標準時間）。

檢閱您感興趣的索引標籤中的資訊。資料篩選選項會套用至所有儀表板。在圖形窗格中，您可以將游標停留在資料點或區域上，以查看任何其他詳細資訊。

Count動作規則

您可以在兩個位置之一檢視計數動作相符項目的資訊。

- 在此流量概觀索引標籤的 [所有流量] 儀表板上，找到 [前 10 名規則] 窗格，然後切換 [切換至計數動作]。開啟此切換後，窗格會顯示符合計數規則，而不是終止符合規則。

- 在 Web ACL 的 [抽樣要求] 索引標籤中，查看您在 [流量概觀] 索引標籤上設定的時間範圍內所有符合規則和動作的圖表。如需 [抽樣請求] 索引標籤的詳細資訊，請參閱。檢視 Web 請求的範例

Amazon CloudWatch 指標

在儀表板圖形窗格中，您可以存取圖形資料的 CloudWatch 量度。選擇圖表窗格頂端的選項，或從窗格內的 (垂直省略號) 下拉式功能表中選擇選項。

重新整理儀表板

儀表板不會自動重新整理。若要更新顯示，請選擇重新整理

圖示。

Web ACL 的流量概觀儀表板範例

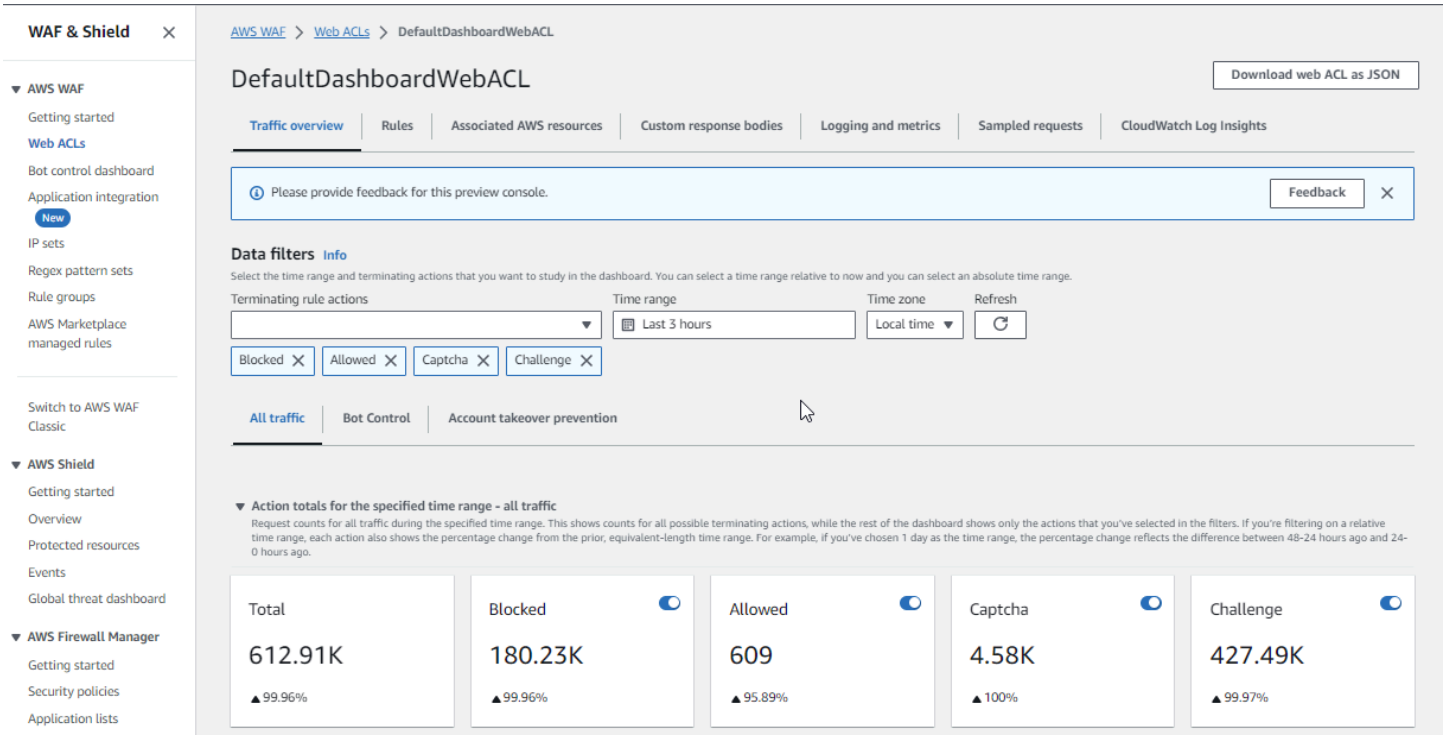
本節顯示 Web ACL 流量概觀儀表板的範例畫面。

> **Note**
>
> 如果您已經在使用 AWS WAF 來保護應用程式資源，您可以在 AWS WAF 主控台的網頁上看到任何 Web ACL 的儀表板。如需相關資訊，請參閱檢視網頁 ACL 的儀表板。

範例畫面：資料篩選器和所有流量儀表板動作計數

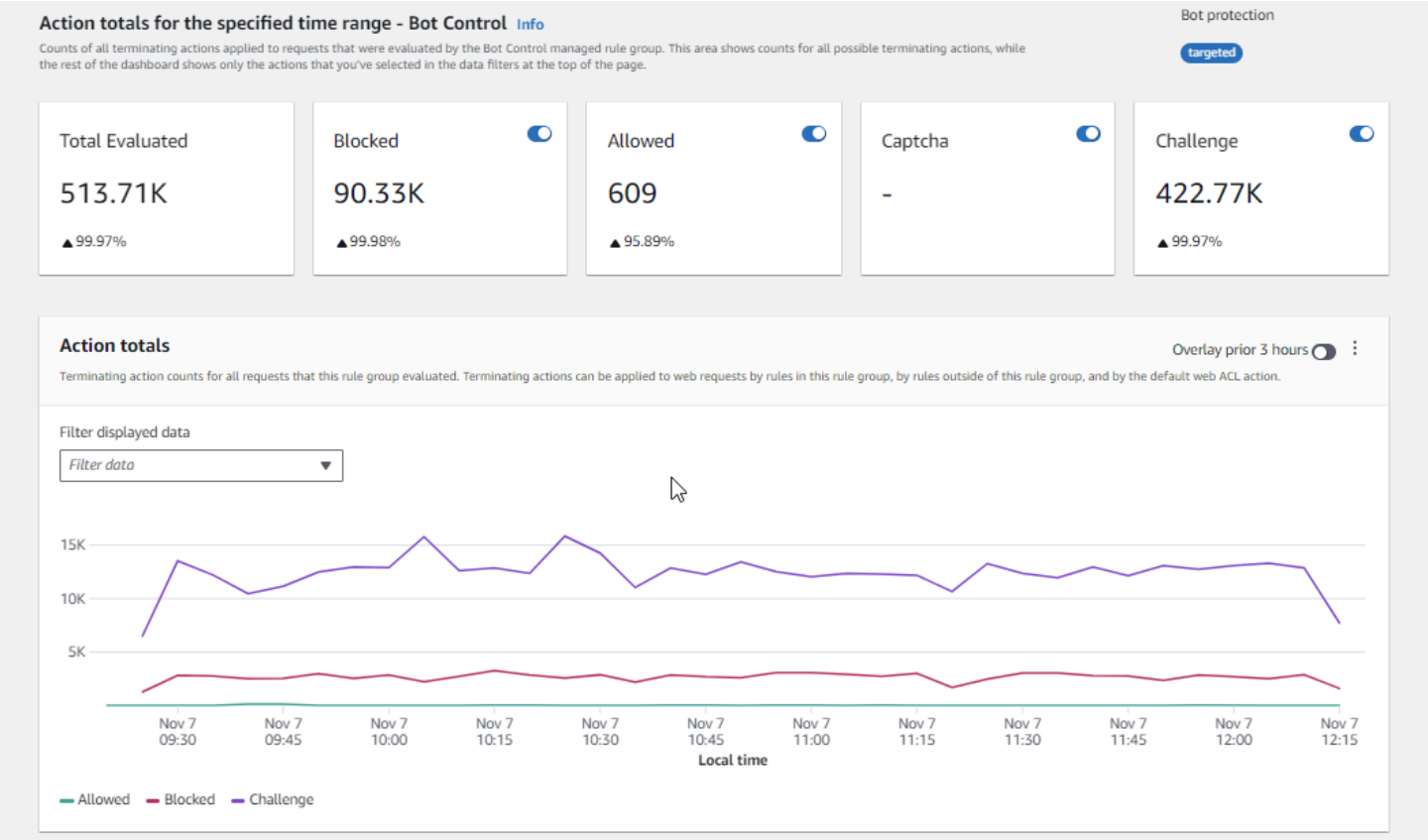
下列螢幕擷取畫面說明已選取 [所有流量] 索引標籤的 Web ACL 流量概觀。資料篩選器會設定為預設值：過去三小時的所有終止動作。

在所有流量儀表板內部是各種終止動作的動作總計。每個窗格都會列出請求計數，並顯示一個向上/向下箭頭，指示自前三小時時間範圍以來的變更。



範例畫面：機器人控制儀表板動作計數

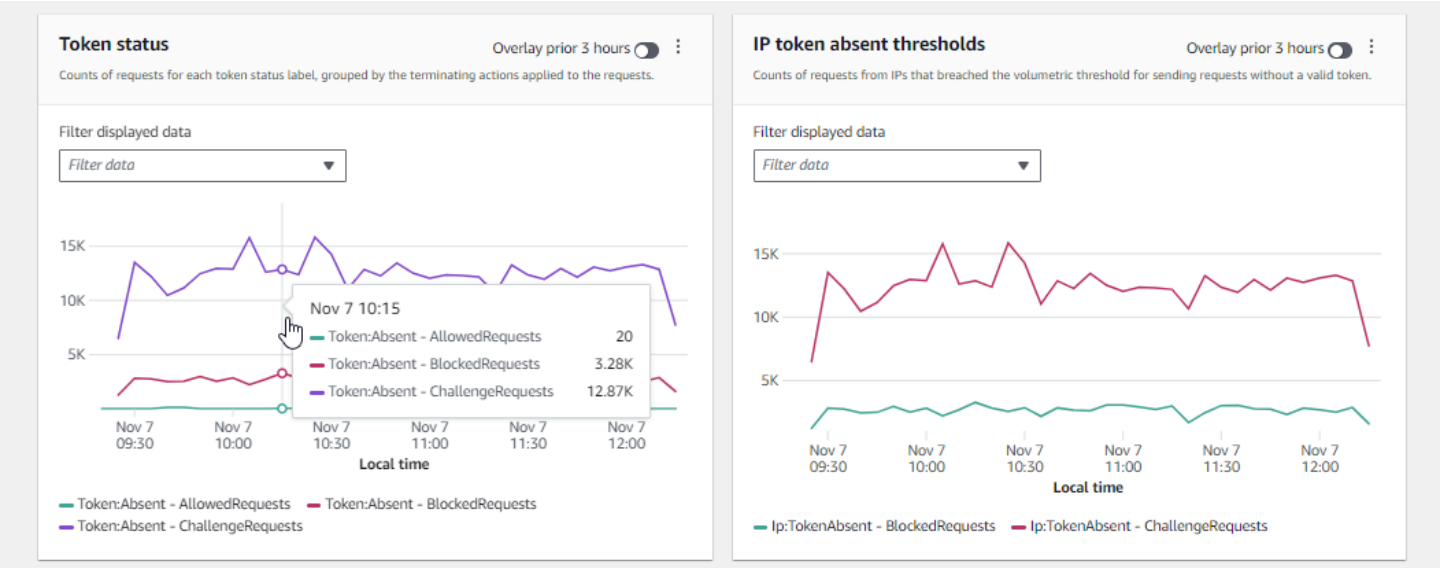
下列螢幕擷取畫面說明「機器人控制」儀表板的動作計數。這會顯示時間範圍的相同總窗格，但計數僅適用於機器人控制規則群組評估的請求。再往下，在 [動作總計] 窗格中，您可以查看指定三小時時間範圍內的動作計數。在此時間範圍內，CAPTCHA動作不會套用至規則群組評估的任何要求。



畫面範例：機器人控制儀表板權杖狀態摘要圖表

下列螢幕擷取畫面說明機器人控制儀表板中可用的兩個摘要圖形。Token 狀態窗格會顯示各種 Token 狀態標籤的計數，並與套用至要求的規則動作配對。IP Token 不存在閾值窗格顯示來自 IP 的請求的數據，這些請求在沒有令牌的情況下發送太多請求。

將游標暫留在圖形中的任何區域上，會顯示可用的資訊詳細資訊。在此屏幕截圖的「令牌狀態」窗格中，鼠標懸停在某個時間點上，而不在任何圖形線上，因此控制台顯示該時間點的所有行的數據。



本節僅顯示 Web ACL 流量概觀儀表板中提供的一些流量摘要。若要查看任何 Web ACL 的儀表板，請在主控台中開啟 Web ACL 頁面。有關如何執行此操作的詳細資訊，請參閱的指引檢視網頁 ACL 的儀表板。

檢視 Web 請求的範例

本節說明主控台中的 Web ACL 抽樣請求索引標籤。 AWS WAF 在此索引標籤中，您可以檢視 AWS WAF 已檢查之 Web 要求的所有符合規則的圖形。此外，如果您已啟用 Web ACL 的請求取樣，您可以看到 AWS WAF 已檢查的 Web 請求範例的表格檢視。您也可以透過 API 呼叫擷取已取樣的要求資訊。`GetSampledRequests`

請求範例包含最多 100 個要求，符合 Web ACL 中規則的準則，以及另外 100 個請求 (不符合任何規則且已套用 Web ACL 預設動作)。範例中的要求來自前三個小時內收到您內容要求的所有受保護資源。

當 Web 要求符合規則中的準則且該規則的動作未終止要求評估時，會 AWS WAF 繼續使用 Web ACL 中的後續規則檢查 Web 要求。因此，Web 請求可能會出現多次。如需有關規則動作行為的資訊，請參閱規則動作。

若要檢視所有規則圖表和取樣請求

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中，選擇 Web ACL。
3. 選擇您要檢視其要求的 Web ACL 名稱。主控台會將您帶到 Web ACL 的描述，您可以在其中編輯它。

4. 在「抽樣請求」標籤中，您可以看到以下內容：

   - 所有規則圖形 — 此圖表顯示在指定時間範圍內執行的所有 Web 請求評估的相符規則和規則動作。

     > **Note**
     >
     > 此圖形的時間範圍是在 Web ACL 的「流量概觀」標籤的「資料篩選」區段中設定。如需相關資訊，請參閱檢視網頁 ACL 的儀表板。

   - 抽樣請求表格 — 此表格顯示過去 3 小時的抽樣請求資料。表格會針對每個項目顯示下列資料：

     指標名稱

     Web ACL 中符合要求之規則的 CloudWatch 測量結果名稱。如果 Web 請求與 Web ACL 中的任何規則不相符，則此值為「預設」。

     > **Note**
     >
     > 如果您變更規則的名稱，並希望規則的量度名稱反映變更，您也必須更新量度名稱。AWS WAF 變更規則名稱時，不會自動更新規則的度量名稱。您可以在主控台中編輯規則時，使用規則 JSON 編輯器變更量度名稱。您也可以透過 API 和任何用來定義 Web ACL 或規則群組的 JSON 清單中變更名稱。

     來源 IP

     要求來源的 IP 位址，或者 (如果檢視者使用 HTTP Proxy 或 Application Load Balancer 器傳送要求) Proxy 或 Application Load Balancer 器的 IP 位址。

     URI

     URL 識別資源的一部分，例如 `/images/daily-ad.jpg`。

     規則群組內的規則

     如果測量結果名稱識別規則群組參照陳述式，就會識別符合要求的規則群組內的規則。

     動作

     指出對應規則的處理行動。如需有關可能規則動作的資訊，請參閱規則動作。

時間

從受保護的資源 AWS WAF 接收請求的時間。

若要顯示有關 Web 要求元件的其他資訊，請在要求列中選擇 URI 的名稱。

在生產環境中啟用您的保護

當您在生產環境中完成測試和調整的最後階段後，請在生產模式下啟用保護。

> **生產流量風險**
>
> 在針對生產流量部署 Web ACL 實作之前，請先在測試環境中對其進行測試和調整，直到您熟悉流量的潛在影響為止。在啟用生產流量保護之前，還可以在生產流量的計數模式下對其進行測試和調整。

> **Note**
>
> 若要遵循本節中的指引，您需要一般了解如何建立和管理 Web ACL、規則和規則群組等 AWS WAF 保護。本指南前面的章節涵蓋了該資訊。

請先在測試環境中執行這些步驟，然後在生產環境中執行。

在生產環境中啟用您的 AWS WAF 保護

1. 切換到您的生產保護

   更新您的 Web ACL 並切換生產環境的設定。

   a. 移除您不需要的任何測試規則

      如果您新增了在生產環境中不需要的測試規則，請將其移除。如果您使用任何標籤比對規則來篩選受管規則群組規則的結果，請務必將這些規則保留在適當位置。

   b. 切換到生產動作

      將新規則的動作設定變更為預期的生產設定。

- 在 Web ACL 中定義的規則 — 編輯 Web ACL 中的規則，並將其動作從變更Count為其生產動作。
- 規則群組 — 在規則群組的 Web ACL 配置中，根據測試和調整活動的結果，切換規則以使用自己的Count動作，或將其保留為動作覆寫。如果您正在使用標籤比對規則來篩選規則群組規則的結果，請務必保留該規則的覆寫。

  若要切換至使用規則的動作，請在 Web ACL 組態中編輯規則群組的規則陳述式，並移除規則的Count覆寫。如果您以 JSON 管理 Web ACL，請在規則群組參考陳述式中，從`RuleActionOverrides`清單中移除規則的項目。
- Web ACL — 如果您變更了測試的 Web ACL 預設動作，請將其切換至其生產設定。

使用這些設置，您的新保護將按照您的意圖管理 Web 流量。

當您儲存 Web ACL 時，與其關聯的資源將會使用您的生產設定。

2. 監控和調整

   為了確保網頁要求能夠依照您的需求處理，請在啟用新功能之後密切監控您的流量。您將監控生產規則動作的指標和記錄，而不是您在調整工作中監視的計數動作。持續監控並根據需要調整行為，以適應網絡流量的變化。

如何 AWS WAF 使用 Amazon CloudFront 功能

建立 Web ACL 時，您可以指定一個或多個 AWS WAF 要檢查的 CloudFront 分佈。 AWS WAF 根據您在 Web ACL 中識別的條件，開始檢查和管理這些分發的 Web 請求。 CloudFront 提供了一些增強 AWS WAF 功能的功能。本章介紹了一些您可以配置CloudFront 以使一起更好地 AWS WAF 工作 CloudFront 和工作的方法。

主題

使 AWS WAF 用 CloudFront 自定義錯誤頁面

根據預設，當根據您指定的準則 AWS WAF 封鎖 Web 要求時，會將 HTTP 狀態碼傳回403 (Forbidden)給檢視器 CloudFront，並將該狀態碼 CloudFront 傳回給檢視器。檢視器接著會顯示類似下列內容的簡短且格式稀疏的預設訊息：

```
Forbidden: You don't have permission to access /myfilename.html on this server.
```

您可以定義自訂回應，在 AWS WAF Web ACL 規則中覆寫此行為。如需有關使用 AWS WAF 規則自訂回應行為的詳細資訊，請參閱Block動作的自訂回應。

> **Note**
>
> 您使用 AWS WAF 規則自訂的回應優先順序高於您在 CloudFront 自訂錯誤頁面中定義的任何回應規格。

如果您希望透過 CloudFront顯示自訂錯誤訊息 (可能使用與網站其他部分相同的格式)，您可 CloudFront 以設定將包含您自訂錯誤訊息的物件 (例如 HTML 檔案) 傳回給檢視者。

> **Note**
>
> CloudFront 無法區分來源傳回的 HTTP 狀態碼 403，以及封鎖要求 AWS WAF 時傳回的 HTTP 狀態碼 403。這表示您無法根據不同原因導致 HTTP 狀態碼 403 而傳回不同的自訂錯誤頁面。

如需有關 CloudFront 自訂錯誤頁面的詳細資訊，請參閱 Amazon CloudFront 開發人員指南中的產生自訂錯誤回應。

AWS WAF 搭配 CloudFront使用在您自己的 HTTP 伺服器上執行的應用程式

AWS WAF 搭配使用時 CloudFront，您可以保護在任何 HTTP 網路伺服器上執行的應用程式，無論是在 Amazon 彈性運算雲端 (Amazon EC2) 中執行的網路伺服器，還是您私下管理的網路伺服器。您還可以配置 CloudFront 為在 CloudFront和您自己的網絡服務器之間以及查看者和 CloudFront.

在 CloudFront 和您自己的網絡服務器之間需要 HTTPS

要在 CloudFront 和您自己的網絡服務器之間要求 HTTPS，您可以使用自定 CloudFront 義來源功能並為特定來源配置原始協議策略和原始域名設置。在您的 CloudFront 配置中，您可以指定服務器的 DNS

名稱以及端口和從源獲取對象時 CloudFront 要使用的協議。您也應確保您自訂原始伺服器上的 SSL/TLS 憑證符合您已設定的原始伺服器的網域名稱。當您在以外的地方使用自己的 HTTP Web 伺服器時 AWS，您必須使用由受信任的第三方憑證授權單位 (CA) 簽署的憑證，例如 Comodo 或賽門鐵克。DigiCert如需需要 HTTPS 才能 CloudFront與您自己的網路伺服器之間進行通訊的詳細資訊，請參閱 Amazon CloudFront 開發人員指南中的〈需要 HTTPS 進行通訊〉主題。 CloudFront

在檢視器和檢視器之間需要 HTTPS CloudFront

若要在檢視器和之間要求 HTTPS CloudFront，您可以針對 CloudFront發行版中的一或多個快取行為變更檢視器通訊協定原則。如需有關 CloudFront在檢視者之間使用 HTTPS 的詳細資訊 CloudFront，請參閱 < 在檢視者之間需要 HTTPS 進行通訊 > 主題和 Amazon CloudFront 開發人員指南。您還可以攜帶自己的 SSL 證書，以便觀眾可以使用您自己的域名 CloudFront 通過 HTTPS 連接到您的分發，例如 https://www.mysite.com。如需詳細資訊，請參閱 Amazon CloudFront 開發人員指南中的設定替代網域名稱和 HTTPS 主題。

選擇可 CloudFront回應的 HTTP 方法

當您建立 Amazon CloudFront 網路分發時，您可 CloudFront 以選擇要處理的 HTTP 方法並轉寄到原始伺服器。您可以從下列選項來選擇：

- **GET**，**HEAD**— 您 CloudFront 只能使用來從來源取得物件或取得物件標頭。
- **GETHEAD**、**OPTIONS** — 您 CloudFront 只能使用來從原始伺服器取得物件、取得物件標頭，或擷取原始伺服器支援的選項清單。
- **GET**、**HEAD**、、**OPTIONS**、**PUTPOSTPATCH**、**DELETE** — 您可以使用 CloudFront 來取得、新增、更新和刪除物件，以及取得物件標頭。此外，您還可以執行其他POST操作，例如從 Web 表單提交數據。

您也可以使用 AWS WAF 位元組比對規則陳述式，根據 HTTP 方法允許或封鎖要求，如中所述字串比對規則陳述式。如果您想要使用 CloudFront 支援的方法組合 (例如GET和)HEAD，則不需 AWS WAF 要設定為封鎖使用其他方法的要求。如果您想要允許 CloudFront 不支援的方法組合，例如、和 GET HEADPOST，您可以設定為 CloudFront 回應所有方法，然後使用封鎖使用其他方法的 AWS WAF 要求。

如需有關選擇可 CloudFront 回應之方法的詳細資訊，請參閱 Amazon CloudFront 開發人員指南中建立或更新 Web 分發時指定的值主題中的允許的 HTTP 方法。

您使用 AWS WAF 服務時的安全

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

> **Note**
>
> 本節針對您使用 AWS WAF 服務及其 AWS 資源 (例如 AWS WAF Web ACL 和規則群組) 提供標準 AWS 安全性指引。
> 如需有關使用保護資 AWS 源的詳細資訊 AWS WAF，請參閱 AWS WAF 指南的其餘部分。

安全是 AWS 與您之間共同承擔的責任。共同責任模型 將此描述為雲端的安全和雲端內的安全：

- 雲端安全性 — AWS 負責保護中執行 AWS 服務的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。第三方稽核人員定期檢測及驗證安全的效率也是我們 AWS 合規計劃的一部分。若要深入瞭解適用於的規範遵循計劃 AWS WAF，請參閱合規方案的AWS 服務範圍。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對資料敏感度、組織要求，以及適用法律和法規等其他因素負責。

本文件可協助您瞭解如何在使用時套用共同責任模型 AWS WAF。下列主題說明如何設定 AWS WAF 以符合安全性與合規性目標。您還將學習如何使用其他 AWS 服務來幫助您監控和保護您的 AWS WAF 資源。

主題

- 資料保護 AWS WAF
- 的身分識別與存取管理 AWS WAF
- 登錄和監控 AWS WAF
- 符合性驗證 AWS WAF
- 韌性在 AWS WAF
- AWS WAF中的基礎設施安全

資料保護 AWS WAF

AWS 共用責任模型適用於中的資料保護 AWS WAF。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管

理任務。如需有關資料隱私權的詳細資訊，請參閱資料隱私權FAQ。 如需歐洲資料保護的相關資訊，請參閱AWS 安全性GDPR部落格上的AWS 共同責任模型和部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 認證並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 對每個帳戶使用多重要素驗證 (MFA)。
- 使用SSL/TLS與 AWS 資源溝通。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 使用設定API和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果 AWS 透過命令列介面或存取時需要 FIPS 140-3 驗證的密碼編譯模組API，請使用端點。FIPS 如需有關可用FIPS端點的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您與控制台、API、 AWS WAF 或一起 AWS 服務 使用或使用其他控制台時 AWS SDKs。 AWS CLI您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供URL給外部伺服器，我們強烈建議您不要在中包含認證資訊，URL以驗證您對該伺服器的要求。

AWS WAF 實體 (例如 Web ACLs、規則群組和 IP 集) 會在靜態時加密，但在某些無法使用加密的區域除外，包括中國 (北京) 和中國 (寧夏)。每個區域都會採用唯一的加密金鑰。

刪除 AWS WAF 資源

您可以刪除在中建立的資源 AWS WAF。請參閱以下各節中每種資源類型的指引。

- 刪除網頁 ACL
- 刪除規則群組
- 刪除 IP 集合
- 刪除規則運算式模式集

的身分識別與存取管理 AWS WAF

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM管理員控制誰可以驗證（登錄）和授權（有權限）使用 AWS WAF 資源。IAM是一種您 AWS 服務 可以使用，無需額外費用。

主題

物件

你如何使用 AWS Identity and Access Management （IAM）不同，具體取決於你在做的工作 AWS WAF。

服務使用者 — 如果您使用 AWS WAF 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 AWS WAF 功能來完成工作時，您可能需要其他權限。了解存取的管理方式可協助您向管理員請求正確的許可。若您無法存取 AWS WAF中的某項功能，請參閱 疑難排解 AWS WAF 身分和存取。

服務管理員 — 如果您負責公司的 AWS WAF 資源，您可能擁有完整的存取權 AWS WAF。決定您的服務使用者應該存取哪些 AWS WAF 功能和資源是您的工作。然後，您必須向IAM管理員提交請求，才能變更服務使用者的權限。檢閱此頁面上的資訊，以瞭解的基本概念IAM。若要深入瞭解貴公司如何IAM搭配使用 AWS WAF，請參閱如何 AWS WAF 使用 IAM。

IAM系統管理員 — 如果您是IAM系統管理員，您可能想要瞭解如何撰寫原則來管理存取權的詳細資訊 AWS WAF。若要檢視可在中使用 AWS WAF 的識別型原則範例IAM，請參閱。AWS WAF的身分型政策範例

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以IAM使用者身分或假設IAM角色來驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM身分識別中心) 使用者、貴公司的單一登入驗證，以及您的 Google 或 Facebook 認證都是聯合身分識別的範例。當您以同盟身分登入時，您的管理員先前會使用IAM角色設定聯合身分識別。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以密碼編譯方式簽署您的要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署要求的詳細資訊，請參閱使用IAM者指南中的簽署 AWS API要求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。若要深入瞭解，請參閱使用AWS IAM Identity Center 者指南中的多重要素驗證和使用多重要素驗證 (MFA) AWS的使用IAM者指南。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以 root 使用者身分登入的完整工作清單，請參閱《使用指南》中的〈需要 root 使用者認證的IAM工作〉。

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時登入資料進行存取 AWS 服務 。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步至您自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需IAM身分識別中心的相關資訊，請參閱IAM識別中心是什麼？在《AWS IAM Identity Center 使用者指南》中。

IAM 使用者和群組

IAM使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定權限。在可能的情況下，我們建議您仰賴臨時登入資料，而不要建立具有長期認證 (例如密碼和存取金鑰) 的IAM使用者。不過，如果

您的特定使用案例需要使用IAM者的長期認證，建議您輪換存取金鑰。如需詳細資訊，請參閱《使用指南》中的「IAM定期輪換存取金鑰」以瞭解需要長期認證的使用案例。

IAM群組是指定IAM使用者集合的身分識別。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為的群組，IAMAdmins並授與該群組管理IAM資源的權限。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。要了解更多信息，請參閱《IAM用戶指南》中的創建用戶（而不是角色）的IAM時間。

IAM角色

IAM角色是您 AWS 帳戶 中具有特定權限的身份。它類似於用IAM戶，但不與特定人員相關聯。您可以 AWS Management Console 透過切換角色來暫時擔任中的角色。IAM您可以透過呼叫 AWS CLI 或 AWS API作業或使用自訂來擔任角色URL。如需有關使用角色方法的詳細資訊，請參閱《使用指南》中的IAM〈使用IAM角色〉。

IAM具有臨時認證的角色在下列情況下很有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱《使用指南》中的〈建立第三方身分識別提供IAM者的角色〉。如果您使用IAM身分識別中心，則需要設定權限集。為了控制身分驗證後可以存取的內IAM容，IAMIdentity Center 會將權限集與中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時IAM使用者權限 — IAM 使用者或角色可以假定某個IAM角色，暫時取得特定工作的不同權限。
- 跨帳戶存取 — 您可以使用IAM角色允許不同帳戶中的某個人 (受信任的主體) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要瞭解跨帳戶存取角色與以資源為基礎的政策之間的差異，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或將物件存放在 Amazon S3 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用使用IAM者或角色執行中的動作時 AWS，您會被視為主參與者。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到

需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。

- 服務角色 — 服務角色是指服務代表您執行動作所代表的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給
- 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。

- 在 Amazon 上執行的應用程式 EC2 — 您可以使用IAM角色來管理在執行個體上EC2執行的應用程式以及發出 AWS CLI 或 AWS API請求的臨時登入資料。這比在EC2執行個體中儲存存取金鑰更可取。若要將 AWS 角色指派給EC2執行個體並讓其所有應用程式都能使用，請建立附加至執行個體的執行個體設定檔。執行個體設定檔包含角色，可讓執行個體上EC2執行的程式取得臨時登入資料。如需詳細資訊，請參閱使用者指南中的使用IAM角色將許可授與在 Amazon EC2 執行個體上執行的應IAM用程式。

要了解是否使用IAM角色還是用IAM戶，請參閱《用戶指南》中的「IAM創建IAM角色的時機（而不是用戶）」。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以JSON文件的形式儲存在中。如需有關JSON原則文件結構和內容的詳細資訊，請參閱《IAM使用指南》中的策略概觀。JSON

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

IAM原則會定義動作的權限，不論您用來執行作業的方法為何。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或取得角色資訊 AWS API。

身分型政策

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管策略或內嵌策略之間進行選擇，請參閱《IAM使用手冊》中的「在受管策略和內嵌策略之間進行選擇」。

資源型政策

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的策略IAM中使用 AWS 受管政策。

存取控制清單 (ACLs)

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

Amazon S3 和 Amazon VPC 是支持服務的示例ACLs。 AWS WAF若要進一步了解ACLs，請參閱 Amazon 簡單儲存服務開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 權限界限 — 權限界限是一項進階功能，您可以在其中設定以身分識別為基礎的原則可授與給IAM實體 (IAM使用者或角色) 的最大權限。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需有關權限界限的詳細資訊，請參閱《IAM使用指南》中的IAM實體的權限界限。
- 服務控制策略 (SCPs) — SCPs 是指定中組織或組織單位 (OU) 最大權限的JSON策略 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個

服務。如果您啟用組織中的所有功能，則可以將服務控制策略 (SCPs) 套用至您的任何或所有帳戶。SCP限制成員帳戶中實體的權限，包括每個帳戶 AWS 帳戶根使用者。如需有關 Organizations 的詳細資訊SCPs，請參閱AWS Organizations 使用指南中的服務控制原則。

- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱《IAM使用指南》中的工作階段原則。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要瞭解如何在涉及多個原則類型時 AWS 決定是否允許要求，請參閱IAM使用指南中的原則評估邏輯。

如何 AWS WAF 使用 IAM

在您用IAM來管理存取權之前 AWS WAF，請先瞭解哪些IAM功能可搭配使用 AWS WAF。

IAM您可以搭配使用的功能 AWS WAF

IAM特徵	AWS WAF 支持
身分型政策	是
資源型政策	是
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	是
ACLs	否
ABAC(策略中的標籤)	部分
臨時憑證	是
轉寄存取工作階段 (FAS)	是

IAM特徵	AWS WAF 支持
服務角色	是
服務連結角色	是

若要深入瞭解其他 AWS 服務如何 AWS WAF 與大部分IAM功能搭配使用，請參閱IAM使用者指南IAM中的使用AWS 服務。

以身分識別為基礎的原則 AWS WAF

支援身分型政策：是

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

使用以IAM身分識別為基礎的策略，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。若要瞭解可在JSON策略中使用的所有元素，請參閱《使用IAM者指南》中的IAMJSON策略元素參考資料。

若要檢視以 AWS WAF 身分為基礎的原則範例，請參閱。AWS WAF的身分型政策範例

以資源為基礎的政策 AWS WAF

支援以資源為基礎的政策：是

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

若要啟用跨帳戶存取，您可以在以資源為基礎的策略中指定一個或多個帳戶中的一個或多個帳戶中的IAM實體作為主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主參與者和資源位於不同時 AWS 帳戶，受信任帳戶中的IAM管理員也必須授與主參與者實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。

AWS WAF 使用以資源為基礎的策略來支援跨帳號共用規則群組。您可以透過將資源型原則設定提供給呼叫或對等PutPermissionPolicy或 AWS WAF API呼叫，以便與其他 AWS 帳戶共用您擁有的規CLI則SDK群組。如需其他資訊，包括其他可用語言的範例和說明文件連結，請參閱《 AWS WAF API參考》PutPermissionPolicy中的。此功能無法透過其他方式使用，例如主控台或 AWS CloudFormation.

的政策動作 AWS WAF

支援政策動作：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON策略Action元素描述了您可以用來允許或拒絕策略中存取的動作。策略動作通常與關聯 AWS API操作具有相同的名稱。有一些例外情況，例如沒有匹配API操作的僅限權限的操作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看每個 AWS WAF 動作和權限的清單，請參閱服務授權參考中 AWS WAF V2 定義的動作。

中的策略動作在動作之前 AWS WAF 使用下列前置詞：

```
wafv2
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "wafv2:action1",
      "wafv2:action2"
         ]
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭為的 AWS WAF 所有動作List，請包括下列動作：

```
"Action": "wafv2:List*"
```

若要檢視以 AWS WAF 身分為基礎的原則範例，請參閱。AWS WAF的身分型政策範例

需要其他權限設定的動作

某些動作需要的權限無法在服務授權參考中 AWS WAF V2 定義的動作中完整描述。本節提供其他權限資訊。

主題

- AssociateWebACL 的許可
- DisassociateWebACL 的許可
- GetWebACLForResource 的許可
- ListResourcesForWebACL 的許可

AssociateWebACL 的許可

本節列出使用 AWS WAF 動作將 Web 與資源ACL相關聯所需的權限`AssociateWebACL`。

對於 Amazon CloudFront 發行版，請使用動作而非此 CloudFront 動作`UpdateDistribution`。如需相關資訊，請參閱 Amazon 參 CloudFront API考資料UpdateDistribution中的。

Amazon API 网关 REST API

需要權限才能在RESTAPI資源類型`SetWebACL`上調用 API Gateway 並在 Web AWS WAF `AssociateWebACL` 上調用ACL。

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apigateway:SetWebACL"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/restapis/*/stages/*"
```

```
    ]
}
```

Application Load Balancer

需要對 Application Load Balancer 資源類型呼叫`elasticloadbalancing:SetWebACL`動作以及在 Web AWS WAF `AssociateWebACL` 上呼叫的權限ACL。

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:SetWebACL"
    ],
    "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
    ]
}
```

AWS AppSync GraphQL API

需要有權限才能呼叫 AWS AppSync `SetWebACL` GraphQL API 資源類型並在網頁 AWS WAF `AssociateWebACL`ACL上呼叫。

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
```

```
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "appsync:SetWebACL"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

Amazon Cognito 使用者集區

需要對使用者集區資源類型呼叫 Amazon Cognito `AssociateWebACL` 動作以及在網路 AWS WAF `AssociateWebACL`ACL上呼叫的權限。

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner 服務

需要權限才能在 App Runner 服務資源類型上調用應用程序運行器`AssociateWebACL`操作並在 Web AWS WAF `AssociateWebACL` 上調用ACL。

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:AssociateWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS 驗證存取實例

需要權限才能在「已驗證存取」執ec2:AssociateVerifiedAccessInstanceWebAcl行個體資源類型 AWS WAF AssociateWebACL上呼叫動作，以及在 Web 上呼叫ACL。

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:AssociateVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
```

```
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

`DisassociateWebACL` 的許可

本節列出使用 AWS WAF 動`DisassociateWebACL`作取消 Web ACL 與資源關聯所需的權限。

對於 Amazon CloudFront 分發，而不是此動作，請使用`UpdateDistribution`帶有空 Web ACL ID 的 CloudFront 動作。如需相關資訊，請參閱 Amazon 參 CloudFront API考資料UpdateDistribution中的。

Amazon API 网关 REST API

需要`SetWebACL`對RESTAPI資源類型呼叫API閘道的權限。不需要許可即可通話 AWS WAF `DisassociateWebACL`。

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "apigateway:SetWebACL"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/restapis/*/stages/*"
    ]
}
```

Application Load Balancer

需要對 Application Load Balancer 資源類型呼叫`elasticloadbalancing:SetWebACL`動作的權限。不需要許可即可通話 AWS WAF `DisassociateWebACL`。

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:SetWebACL"
    ],
    "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
```

```
    ]
}
```

AWS AppSync GraphQL API

需要呼叫 AWS AppSync `SetWebACL` GraphQL API 資源類型的權限。不需要許可即可通話 AWS WAF `DisassociateWebACL`。

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "appsync:SetWebACL"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

Amazon Cognito 使用者集區

需要對使用者集區資源類型呼叫 Amazon Cognito `DisassociateWebACL` 動作並進行呼叫 AWS WAF `DisassociateWebACL`的權限。

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:DisassociateWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner 服務

需要在 App Runner 服務資源類型上呼叫應用程式執行器DisassociateWebACL動作並呼叫的權限 AWS WAF DisassociateWebACL。

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:DisassociateWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS 驗證存取實例

需要對「已驗證存取」執ec2:DisassociateVerifiedAccessInstanceWebAcl行個體資源類型呼叫動作並呼叫的權限 AWS WAF DisassociateWebACL。

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:DisassociateVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

`GetWebACLForResource` 的許可

本節列出使用 AWS WAF 動作取得受保護資源之 Web ACL 所需的權限`GetWebACLForResource`。

對於 Amazon CloudFront 發行版，請使用動作而非此 CloudFront 動作`GetDistributionConfig`。如需相關資訊，請參閱 Amazon 參 CloudFront API考資料GetDistributionConfig中的。

> **Note**
>
> `GetWebACLForResource`需要呼叫的權限`GetWebACL`。在此情況下，`GetWebACL`僅 AWS WAF 用於驗證您的帳戶是否具有訪問`GetWebACLForResource`返回的 Web 所需ACL的權限。當您呼叫時`GetWebACLForResource`，您可能會收到錯誤訊息，指出您的帳戶未獲授權`wafv2:GetWebACL`對資源執行。 AWS WAF 不會將這種類型的錯誤添加到 AWS CloudTrail 事件歷史記錄中。

Amazon API 閘道RESTAPI、Application Load Balancer 和 AWS AppSync GraphQL API

需要通話 AWS WAF `GetWebACLForResource`和網絡`GetWebACL`的權限ACL。

```
{
    "Sid": "GetWebACLForResource",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}
```

Amazon Cognito 使用者集區

需要對使用者集區資源類型呼叫 Amazon Cognito `GetWebACLForResource` 動作以及呼叫 AWS WAF `GetWebACLForResource`和`GetWebACL`的權限。

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
```

```
            "wafv2:GetWebACLForResource",
            "wafv2:GetWebACL"
        ],
        "Resource": [
            "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
        ]
    },
    {
        "Sid": "GetWebACLForResource2",
        "Effect": "Allow",
        "Action": [
            "cognito-idp:GetWebACLForResource"
        ],
        "Resource": [
            "arn:aws:cognito-idp:*:account-id:userpool/*"
        ]
    }
```

AWS App Runner 服務

需要權限才能在 App Runner 服務資源類型上呼叫應用程式執行器`DescribeWebAclForService`動作，以及呼叫 AWS WAF `GetWebACLForResource`和`GetWebACL`。

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "apprunner:DescribeWebAclForService"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
```

```
}
```

AWS 驗證存取實例

需要權限才能對「已驗證存取」執ec2:GetVerifiedAccessInstanceWebAcl行個體資源類型呼叫動作，以及呼叫 AWS WAF GetWebACLForResource和GetWebACL。

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "ec2:GetVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

ListResourcesForWebACL 的許可

本節列出ACL使用 AWS WAF 動作擷取 Web 受保護資源清單所需的權限ListResourcesForWebACL。

對於 Amazon CloudFront 發行版，請使用動作而非此 CloudFront 動作ListDistributionsByWebACLId。如需相關資訊，請參閱 Amazon 參 CloudFront API考資料ListDistributionsByWebACLId中的。

Amazon API 閘道RESTAPI、Application Load Balancer 和 AWS AppSync GraphQL API

需要權限才能 AWS WAF ListResourcesForWebACL呼叫網頁ACL。

```
{
```

```
    "Sid": "ListResourcesForWebACL",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}
```

Amazon Cognito 使用者集區

需要對使用者集區資源類型呼叫 Amazon Cognito `ListResourcesForWebACL` 動作並進行呼叫 AWS WAF `ListResourcesForWebACL`的權限。

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner 服務

需要在 App Runner 服務資源類型上呼叫應用程式執行器`ListAssociatedServicesForWebAcl`動作並呼叫的權限 AWS WAF `ListResourcesForWebACL`。

```
{
```

```
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:ListAssociatedServicesForWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS 驗證存取實例

需要對「已驗證存取」執ec2:DescribeVerifiedAccessInstanceWebAclAssociations行個體資源類型呼叫動作並呼叫的權限 AWS WAF ListResourcesForWebACL。

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
```

```
    ]
}
```

的政策資源 AWS WAF

支援政策資源：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

ResourceJSON原則元素會指定要套用動作的一或多個物件。陳述式必須包含 Resource 或 NotResource 元素。最佳做法是使用其 Amazon 資源名稱 (ARN) 指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看資 AWS WAF 源類型及其清單ARNs，請參閱服務授權參考中 AWS WAF V2 定義的資源。若要瞭解您可以針對每個資源指定ARN哪些動作，請參閱 AWS WAF V2 定義的動作。若要允許或拒絕 AWS WAF 資源子集的存取，請在策略ARN的resource元素中包含資源的資源。

ARNs的 AWS WAF wafv2資源具有以下格式：

```
arn:partition:wafv2:region:account-id:scope/resource-type/resource-name/resource-id
```

如需有關ARN規格的一 Amazon 資訊，請參閱 Amazon Web Services 一般參考. ARNs

以下列出資wafv2源ARNs的特定需求：

- *region*：對於您用來保護 Amazon CloudFront 分發的 AWS WAF 資源，請將其設定為us-east-1。否則，請將其設定為您正在使用受保護區域資源的區域。
- *scope*：將範圍設定global為與 Amazon CloudFront 分發搭配使用，或regional與任何 AWS WAF 支援的區域資源搭配使用。區域資源包括 Amazon API 閘道RESTAPI、應用程式負載平衡器、AWS AppSync GraphQL API、Amazon Cognito 使用者集區、 AWS App Runner 服務和 AWS 驗證存取執行個體。
- *resource-type*：指定下列其中一個值：webaclrulegroup、ipset、regexpatternset、或managedruleset。

- *resource-name*：指定您為 AWS WAF 資源提供的名稱，或指定萬用字元 (*) 以指示符合中其他規格的所有資源ARN。您必須指定資源名稱和資源 ID，或為兩者指定萬用字元。
- *resource-id*：指定 AWS WAF 資源的 ID，或指定萬用字元 (*) 以指示符合中其他規格的所有資源ARN。您必須指定資源名稱和資源 ID，或為兩者指定萬用字元。

例如，以下ARN指定所有ACLs具有區域範圍的 Web 區域111122223333中的帳戶us-west-1：

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

下列內容ARN指定區域111122223333中帳戶MyIPManagementRuleGroup的全域範圍命名的規則群組us-east-1：

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

若要檢視以 AWS WAF 身分為基礎的原則範例，請參閱。AWS WAF的身分型政策範例

的政策條件索引鍵 AWS WAF

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，只有在IAM使用者名稱標記資源時，您才可以授與IAM使用者存取資源的權限。如需詳細資訊，請參閱IAM使用指南中的IAM政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《使用指南》中的AWS 全域條件內IAM容索引鍵。

此外，還 AWS WAF 支援下列條件金鑰，您可以用來為IAM原則提供精細篩選：

- 波夫 2：LogDestinationResource

  此條件金鑰為記錄目的地採用 Amazon 資源名稱 (ARN) 規格。這是您在ARN使用RESTAPI呼叫時為記錄目標提供的`PutLoggingConfiguration`。

  您可以明確指定，ARN而且您可以為ARN. 下列範例會針對具有特定位置和前置詞的 Amazon S3 儲存貯ARNs體指定篩選。

  ```
  "Condition": { "ArnLike": { "wafv2:LogDestinationResource": "arn:aws:s3:::aws-waf-logs-suffix/custom-prefix/*" } }
  ```

- 波夫 2：LogScope

  此條件索引鍵會以字串定義記錄組態的來源。目前，這一律設定為的預設值`Customer`，表示記錄目的地為您擁有及管理。

若要查看 AWS WAF 條件金鑰清單，請參閱服務授權參考中 AWS WAF V2 的條件金鑰。若要瞭解您可以使用條件索引鍵的動作和資源，請參閱 AWS WAF V2 定義的動作。

若要檢視以 AWS WAF 身分為基礎的原則範例，請參閱。AWS WAF的身分型政策範例

ACLs在 AWS WAF

支持ACLs：無

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

ABAC與 AWS WAF

支援 ABAC (策略中的標籤): 部分

以屬性為基礎的存取控制 (ABAC) 是一種授權策略，可根據屬性定義權限。在中 AWS，這些屬性稱為標籤。您可以將標籤附加至IAM實體 (使用者或角色) 和許多 AWS 資源。標記實體和資源是的第一步ABAC。然後，您可以設計ABAC策略，以便在主參與者的標籤與他們嘗試存取的資源上的標籤相符時允許作業。

ABAC在快速成長的環境中很有幫助，並且有助於原則管理變得繁瑣的情況。

如需根據標籤控制存取，請使用 `aws:ResourceTag/`*`key-name`*、`aws:RequestTag/`*`key-name`* 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需有關的詳細資訊ABAC，請參閱什麼是ABAC？ 在《IAM使用者指南》中。若要檢視包含設定步驟的自學課程ABAC，請參閱《使用指南》中的〈使用以屬性為基礎的存取控制 (ABAC) IAM 〉。

使用臨時登入資料 AWS WAF

支援臨時憑證：是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配使用 AWS 服務 ，請參閱《IAM使用指南》IAM中的使用方式。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立臨時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需有關切換角色的詳細資訊，請參閱《IAM使用者指南》中的〈切換到角色 (主控台)〉。

您可以使用 AWS CLI 或手動建立臨時認證 AWS API。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而非使用長期存取金鑰。如需詳細資訊，請參閱IAM。

轉寄服務的存取工作階段 AWS WAF

支援轉寄存取工作階段 (FAS)：是

當您使用使用IAM者或角色在中執行動作時 AWS，您會被視為主參與者。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。

AWS WAF的服務角色

支援服務角色：是

服務角色是服務假定代表您執行動作的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給

> **Warning**
>
> 變更服務角色的權限可能會中斷 AWS WAF 功能。只有在 AWS WAF 提供指引時才編輯服務角色。

服務連結角色 AWS WAF

支援服務連結角色：是

服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。

如需有關建立或管理 AWS WAF 服務連結角色的詳細資訊，請參閱使用服務連結角色 AWS WAF。

AWS WAF的身分型政策範例

根據預設，使用者和角色不具備建立或修改 AWS WAF 資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

如需有關由定義的動作和資源類型的詳細資訊 AWS WAF，包括每個資源類型的 ARN 格式，請參閱服務授權參考中 AWS WAF V2 的動作、資源和條件索引鍵。

主題

- 政策最佳實務
- 使用 AWS WAF 主控台
- 允許使用者檢視他們自己的許可
- 授與 AWS WAF、 CloudFront和的唯讀存取權 CloudWatch
- 授予 AWS WAF、 CloudFront和的完整存取權 CloudWatch
- 授予單一存取權 AWS 帳戶
- 授與單一 Web ACL 的存取權
- 將 CLI 存取權授與 Web ACL 和規則群組

政策最佳實務

以身分識別為基礎的政策會決定某人是否可以建立、存取或刪除您帳戶中的 AWS WAF 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定

於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。

- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需更多資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

使用 AWS WAF 主控台

若要存取 AWS WAF 主控台，您必須擁有最少一組權限。這些權限必須允許您列出和檢視有關 AWS 帳戶. AWS WAF 如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

為了確保使用者和角色可以使用 AWS WAF 主控台，請至少將 AWS WAF `AWSWAFConsoleReadOnlyAccess` AWS 受管理的原則附加至實體。如需有關此受管理原則的資訊，請參閱AWS 受管理策略： AWSWAFConsoleReadOnlyAccess。如需有關將受管政策附加到使用者的詳細資訊，請參閱 IAM 使用者指南中的向使用者新增許可。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

授與 AWS WAF、 CloudFront和的唯讀存取權 CloudWatch

下列政策授予使用者對資 AWS WAF 源、Amazon CloudFront 網路分發和 Amazon CloudWatch 指標的唯讀存取權。對於需要檢視 AWS WAF 條件、規則和 Web ACL 中設定的權限的使用者來說，以查看哪個分發與 Web ACL 相關聯，以及監視中 CloudWatch的指標和要求範例，這非常有用。這些使用者無法建立、更新或刪除 AWS WAF 資源。

```
{
   "Version":"2012-10-17",
```

```
   "Statement": [
      {
         "Action": [
            "wafv2:Get*",
            "wafv2:List*",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Effect": "Allow",
         "Resource": "*"
      }
   ]
}
```

授予 AWS WAF、 CloudFront和的完整存取權 CloudWatch

下列原則可讓使用者執行任何 AWS WAF 作業、對 CloudFront Web 發佈執行任何作業，以及監視中的指標和要求範例 CloudWatch。它對身為 AWS WAF 管理員的使用者很有用。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": [
            "wafv2:*",
            "cloudfront:CreateDistribution",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:UpdateDistribution",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudfront:DeleteDistribution",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Effect": "Allow",
         "Resource": "*"
```

```
      }
   ]
}
```

我們強烈建議您為具有管理權限的使用者設定多重驗證 (MFA)。如需詳細資訊，請參閱 IAM 使用指南 AWS中的搭配使用 Multi-Factor Authentication (MFA) 裝置。

授予單一存取權 AWS 帳戶

此原則會將下列權限授與帳戶 444455556666：

- 完全存取所有 AWS WAF 作業和資源。
- 讀取和更新對所有 CloudFront 發行版的訪問權限，這使您可以將 Web ACL 和 CloudFront 發行版關聯起來。
- 所有測量結 CloudWatch 果和測量結果統計資料的讀取存取權，以便您可以在 AWS WAF 主控台中檢視 CloudWatch 資料和要求範例。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "wafv2:*"
         ],
         "Resource": [
            "arn:aws:wafv2:us-east-1:444455556666:*"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudfront:UpdateDistribution",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
```

```
         "Resource": [
            "*"
         ]
      }
   ]
}
```

授與單一 Web ACL 的存取權

下列策略可讓使用者透過帳戶中特定 Web ACL 上的主控台執行任何 AWS WAF 作業444455556666。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wafv2:*"
            ],
            "Resource": [
                "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
            ]
        },
        {
            "Sid": "consoleAccess",
            "Effect": "Allow",
            "Action": [
                "wafv2:ListWebACLs",
                "ec2:DescribeRegions"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

將 CLI 存取權授與 Web ACL 和規則群組

下列原則可讓使用者透過 CLI 在特定 Web ACL 和帳戶中的特定規則群組上執行任何 AWS WAF 作業444455556666。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "wafv2:*"
         ],
         "Resource": [
        "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
        "arn:aws:wafv2:us-east-1:444455556666:regional/rulegroup/
test123rulegroup/555555555-6666-1234-abcd-00d11example"
         ]
      }
   ]
}
```

下列策略可讓使用者透過帳戶中特定 Web ACL 上的主控台執行任何 AWS WAF 作業444455556666。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wafv2:*"
            ],
            "Resource": [
                "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
            ]
        },
        {
            "Sid": "consoleAccess",
            "Effect": "Allow",
            "Action": [
                "wafv2:ListWebACLs",
                "ec2:DescribeRegions"
            ],
            "Resource": [
                "*"
```

```
            ]
        }
    ]
}
```

AWS 受管理的政策 AWS WAF

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新 AWS 服務 的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 受管理策略： AWSWAFReadOnlyAccess

此政策授予唯讀許可，允許使用者存取整合式服務的資 AWS WAF 源和資源，例如 Amazon CloudFront、Amazon API Gateway、Application Load Balancer AWS AppSync、Amazon Cognito 和 AWS 已驗證存取。 AWS App Runner您可以將此政策附加到 IAM 身分。 AWS WAF 也會將此原則附加至允許代表您執 AWS WAF 行動作的服務角色。

如需有關此政策的詳細資訊，請參閱 IAM 主控台AWSWAFReadOnlyAccess中的。

AWS 受管理策略： AWSWAFFullAccess

此政策授予對整合式服務 (例如 Amazon、Amazon API 閘道、Application Load Balancer CloudFront、 AWS AppSync Amazon Cognito 和 AWS 驗證存取) 的資源和資源的完整存取權。 AWS WAF AWS App Runner您可以將此政策附加到 IAM 身分。 AWS WAF 也會將此原則附加至允許代表您執 AWS WAF 行動作的服務角色。

如需有關此政策的詳細資訊，請參閱 IAM 主控台AWSWAFFullAccess中的。

AWS 受管理策略： AWSWAFConsoleReadOnlyAccess

此政策將唯讀許可授予 AWS WAF 主控台，其中包括整合式服務的資源，例如 Amazon CloudFront、Amazon API Gateway、Application Load Balancer AWS AppSync、Amazon Cognito 和 AWS 已驗證存取權限。 AWS WAF AWS App Runner您可以將此政策附加到 IAM 身分。 AWS

WAF 還將此策略附加到 aiam/home # / 策略 /arn: aw:iam:: aws: 策略/$ 服務角色，允許代表您執行操作。AWSWAFConsoleFullAccess serviceLevelSummary AWS WAF

如需有關此政策的詳細資訊，請參閱 IAM 主控台AWSWAFConsoleReadOnlyAccess中的。

AWS 受管理策略： AWSWAFConsoleFullAccess

此政策授予對 AWS WAF AWS WAF 主控台的完整存取權，其中包括整合式服務的資源，例如 Amazon CloudFront、Amazon API Gateway、Application Load Balancer AWS AppSync、Amazon Cognito 和 AWS 驗證存取。 AWS App Runner您可以將此政策附加到 IAM 身分。 AWS WAF 也會將此原則附加至允許代表您執 AWS WAF 行動作的服務角色。

如需有關此政策的詳細資訊，請參閱 IAM 主控台AWSWAFConsoleFullAccess中的。

AWS 受管理的策略：WAFV2 LoggingServiceRolePolicy

此政策允許 AWS WAF 將日誌寫入 Amazon 數據 Firehose。只有當您啟用登入時，才會使用此原則 AWS WAF。此政策連接至 `AWSServiceRoleForWAFV2Logging` 服務連結角色。如需服務連結角色的詳細資訊，請參閱使用服務連結角色 AWS WAF。

如需有關此政策的詳細資訊，請參閱 IAM 主控台LoggingServiceRolePolicy中的 WAFV2。

AWS WAFAWS 受管理策略的更新

檢視 AWS WAF 自此服務開始追蹤這些變更以來的 AWS 受管理策略更新詳細資料。如需有關此頁面變更的自動警示，請訂閱 AWS WAF 文件記錄頁面上的 RSS 摘要，網址為文件歷史紀錄。

政策	變更說明	日期
`WAFV2LoggingServiceRolePolicy` 此政策允許 AWS WAF 將日誌寫入 Amazon 數據 Firehose。它僅在啟用日誌記錄時使用。 IAM 主控台中的詳細資料：WAFV2 LoggingServiceRolePolicy。	已將陳述式 ID (Sid) 新增至此原則所附加之服務連結角色中的權限設定。	2024-06-03

政策	變更說明	日期
AWSServiceRoleForWAFV2Logging 此服務連結角色提供允許 AWS WAF 將日誌寫入 Amazon 資料 Firehose 的許可政策。 IAM 主控台中的詳細資訊：AWSServiceRoleForWAFV2Logging。	在權限設定中新增陳述式識別碼 (Sid)。	2024-06-03
AWS WAF 新增至變更追蹤	AWS WAF 開始追蹤受管理策略WAFV2LoggingServiceRolePolicy 和服務連結角色AWSServiceRoleForWAFV2Logging 的變更。	2024-06-03
AWSWAFFullAccess 此原則 AWS WAF 允許代表您在整合式服務中管理 AWS 資源。 AWS WAF IAM 主控台中的詳細資訊：AWSWAFFullAccess。	擴充權限，可將 AWS 已驗證存取執行個體新增至您可以使用保護的資源類型 AWS WAF。	2023-06-17
AWSWAFReadOnlyAccess 此原則 AWS WAF 允許代表您在整合式服務中管理 AWS 資源。 AWS WAF IAM 主控台中的詳細資訊：AWSWAFReadOnlyAccess。	擴充權限，可將 AWS 已驗證存取執行個體新增至您可以使用保護的資源類型 AWS WAF。	2023-06-17

政策	變更說明	日期
`AWSWAFConsoleFullAccess` 此原則可 AWS WAF 讓您在整合式服務中代表您管理 AWS 主控台 AWS 資源 AWS WAF 和其他資源。 IAM 主控台中的詳細資訊：AWSWAFConsoleFullAccess。	擴充權限，可將 AWS 已驗證存取執行個體新增至您可以使用保護的資源類型 AWS WAF。	2023-06-17
`AWSWAFConsoleReadOnlyAccess` 此原則可 AWS WAF 讓您在整合式服務中代表您管理 AWS 主控台 AWS 資源 AWS WAF 和其他資源。 IAM 主控台中的詳細資訊：AWSWAFConsoleReadOnlyAccess。	擴充權限，可將 AWS 已驗證存取執行個體新增至您可以使用保護的資源類型 AWS WAF。	2023-06-17
`AWSWAFFullAccess` 此原則 AWS WAF 允許代表您在整合式服務中管理 AWS 資源。 AWS WAF IAM 主控台中的詳細資訊：AWSWAFFullAccess。	擴充權限以更正 AWS App Runner 服務的存取設定。	2023-06-06

政策	變更說明	日期
AWSWAFReadOnlyAccess 此原則 AWS WAF 允許代表您在整合式服務中管理 AWS 資源。 AWS WAF IAM 主控台中的詳細資訊：AWSWAFReadOnlyAccess。	擴充權限以更正 AWS App Runner 服務的存取設定。	2023-06-06
AWSWAFConsoleFullAccess 此原則可 AWS WAF 讓您在整合式服務中代表您管理 AWS 主控台 AWS 資源 AWS WAF 和其他資源。 IAM 主控台中的詳細資訊：AWSWAFConsoleFullAccess。	擴充權限以更正 AWS App Runner 服務的存取設定。	2023-06-06
AWSWAFConsoleReadOnlyAccess 此原則可 AWS WAF 讓您在整合式服務中代表您管理 AWS 主控台 AWS 資源 AWS WAF 和其他資源。 IAM 主控台中的詳細資訊：AWSWAFConsoleReadOnlyAccess。	擴充權限以更正 AWS App Runner 服務的存取設定。	2023-06-06

政策	變更說明	日期
AWSWAFFullAccess 此原則 AWS WAF 允許代表您在整合式服務中管理 AWS 資源。 AWS WAF IAM 主控台中的詳細資訊：AWSWAFFullAccess。	擴充權限，可將 AWS App Runner 服務新增至您可以使用保護的資源類型 AWS WAF。	2023-03-30
AWSWAFReadOnlyAccess 此原則 AWS WAF 允許代表您在整合式服務中管理 AWS 資源。 AWS WAF IAM 主控台中的詳細資訊：AWSWAFReadOnlyAccess。	擴充權限，可將 AWS App Runner 服務新增至您可以使用保護的資源類型 AWS WAF。	2023-03-30
AWSWAFConsoleFullAccess 此原則可 AWS WAF 讓您在整合式服務中代表您管理 AWS 主控台 AWS 資源 AWS WAF 和其他資源。 IAM 主控台中的詳細資訊：AWSWAFConsoleFullAccess。	擴充權限，可將 AWS App Runner 服務新增至您可以使用保護的資源類型 AWS WAF。	2023-03-30

政策	變更說明	日期
`AWSWAFConsoleReadOnlyAccess` 此原則可 AWS WAF 讓您在整合式服務中代表您管理 AWS 主控台 AWS 資源 AWS WAF 和其他資源。 IAM 主控台中的詳細資訊：AWSWAFConsoleReadOnlyAccess。	擴充權限，可將 AWS App Runner 服務新增至您可以使用保護的資源類型 AWS WAF。	2023-03-30
`AWSWAFFullAccess` 此原則 AWS WAF 允許代表您在整合式服務中管理 AWS 資源。 AWS WAF IAM 主控台中的詳細資訊：AWSWAFFullAccess。	擴充許可，可將 Amazon Cognito 使用者集區新增至您可以使用保護的資源類型。 AWS WAF	2022-08-25
`AWSWAFReadOnlyAccess` 此原則 AWS WAF 允許代表您在整合式服務中管理 AWS 資源。 AWS WAF IAM 控制台中的詳細信息：AWSWAFReadOnlyAccess。	擴充許可，可將 Amazon Cognito 使用者集區新增至您可以使用保護的資源類型。 AWS WAF	2022-08-25

政策	變更說明	日期
`AWSWAFConsoleFullAccess` 此原則可 AWS WAF 讓您在整合式服務中代表您管理 AWS 主控台 AWS 資源 AWS WAF 和其他資源。 IAM 控制台中的詳細信息：AWSWAFConsoleFullAccess。	擴充許可，可將 Amazon Cognito 使用者集區新增至您可以使用保護的資源類型。AWS WAF	2022-08-25
`AWSWAFConsoleReadOnlyAccess` 此原則可 AWS WAF 讓您在整合式服務中代表您管理 AWS 主控台 AWS 資源 AWS WAF 和其他資源。 IAM 控制台中的詳細信息：AWSWAFConsoleReadOnlyAccess。	擴充許可，可將 Amazon Cognito 使用者集區新增至您可以使用保護的資源類型。AWS WAF	2022-08-25
`AWSWAFFullAccess` 此原則 AWS WAF 允許代表您在整合式服務中管理 AWS 資源。 AWS WAF IAM 控制台中的詳細信息：AWSWAFFullAccess。	更正 Amazon 簡單儲存服務 (Amazon S3) 和亞馬遜日誌的 CloudWatch 日誌交付許可設定。此變更可解決記錄組態期間發生的拒絕存取錯誤。如需有關記錄 Web ACL 流量的資訊，請參閱記錄 AWS WAF 網頁 ACL 流量。	2022-01-11

政策	變更說明	日期
AWSWAFConsoleFullAccess 此原則可 AWS WAF 讓您在整合式服務中代表您管理 AWS 主控台 AWS 資源 AWS WAF 和其他資源。 IAM 控制台中的詳細信息：AWSWAFConsoleFullAccess。	更正 Amazon 簡單儲存服務 (Amazon S3) 和亞馬遜日誌的 CloudWatch 日誌交付許可設定。此變更可解決記錄組態期間發生的存取錯誤。如需有關記錄 Web ACL 流量的資訊，請參閱記錄 AWS WAF 網頁 ACL 流量。	2022-01-11
AWSWAFFullAccess 此原則 AWS WAF 允許代表您在整合式服務中管理 AWS 資源。 AWS WAF IAM 控制台中的詳細信息：AWSWAFFullAccess。	為擴展的日誌選項添加了新的權限。 這項變更可讓您 AWS WAF 存取其他日誌記錄目的地亞馬遜簡單儲存服務 (Amazon S3) 和 Amazon CloudWatch 日誌。如需有關記錄 Web ACL 流量的資訊，請參閱記錄 AWS WAF 網頁 ACL 流量。	2021-11-15
AWSWAFConsoleFullAccess 此原則可 AWS WAF 讓您在整合式服務中代表您管理 AWS 主控台 AWS 資源 AWS WAF 和其他資源。 IAM 控制台中的詳細信息：AWSWAFConsoleFullAccess。	為擴展的日誌選項添加了新的權限。 這項變更可讓您 AWS WAF 存取其他日誌記錄目的地亞馬遜簡單儲存服務 (Amazon S3) 和 Amazon CloudWatch 日誌。如需有關記錄 Web ACL 流量的資訊，請參閱記錄 AWS WAF 網頁 ACL 流量。	2021-11-15
AWS WAF 開始追蹤變更	AWS WAF 開始追蹤其 AWS 受管理策略的變更。	2021-3-01

疑難排解 AWS WAF 身分和存取

使用下列資訊可協助您診斷和修正使用和 IAM 時可能會遇到的 AWS WAF 常見問題。

主題

我沒有執行操作的授權 AWS WAF

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 wafv2:*GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 wafv2:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 wafv2:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我沒有授權執行 iam：PassRole

如果您收到錯誤，告知您未獲授權執行 iam:PassRole 動作，您的政策必須更新，允許您將角色傳遞給 AWS WAF。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

名為 marymajor 的 IAM 使用者嘗試使用主控台在 AWS WAF中執行動作時，發生下列範例錯誤。但是，動作要求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我想允許我以外的人訪 AWS 帳戶 問我的 AWS WAF 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要瞭解是否 AWS WAF 支援這些功能，請參閱如何 AWS WAF 使用 IAM。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM 使用者指南》中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何向第三方提供對資源的存取權 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 若要了解跨帳戶存取使用角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。

使用服務連結角色 AWS WAF

AWS WAF 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結到 AWS WAF的唯一 IAM 角色類型。服務連結角色由預先定義， AWS WAF 並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

服務連結角色可讓您 AWS WAF 更輕鬆地設定，因為您不需要手動新增必要的權限。 AWS WAF 定義其服務連結角色的權限，除非另有定義，否則只 AWS WAF 能擔任其角色。已定義的許可包括信任政策和許可政策。該許可政策無法連接至其他任何 IAM 實體。

您必須先刪除角色的相關資源，才能刪除服務連結角色。這樣可以保護您的 AWS WAF 資源，因為您無法不小心移除存取資源的權限。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

服務連結角色權限 AWS WAF

AWS WAF 使用服務連結角色AWSServiceRoleForWAFV2Logging將日誌寫入 Amazon 資料 Firehose。只有在您啟用登入時，才會使用此角色 AWS WAF。如需日誌記錄的相關資訊，請參閱記錄 AWS WAF 網頁 ACL 流量。

此服務連結角色會附加至 AWS 受管理的策略WAFV2LoggingServiceRolePolicy。如需受管政策的更多相關資訊，請參閱AWS 受管理的策略：WAFV2 LoggingServiceRolePolicy。

AWSServiceRoleForWAFV2Logging 服務連結角色信任 wafv2.amazonaws.com 服務來擔任該角色。

角色的權限原則允許 AWS WAF 對指定的資源完成下列動作：

- Amazon 數據防火管動作：以PutRecord及PutRecordBatch在 Firehose 上的數據流資源，名稱開頭為。aws-waf-logs-例如 aws-waf-logs-us-east-2-analytics。
- AWS Organizations 作業：針DescribeOrganization對「Organizations」組織資源。

請參閱 IAM 主控台中的完整服務連結角色：AWSServiceRoleForWAFV2Logging

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

為 AWS WAF建立服務連結角色

您不需要手動建立一個服務連結角色。當您在上啟用 AWS WAF 記錄 AWS Management Console，或在 AWS WAF CLI 或 AWS WAF API 中PutLoggingConfiguration提出要求時， AWS WAF 會為您建立服務連結角色。

您必須擁有 iam:CreateServiceLinkedRole 許可才能啟用記錄。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。啟用 AWS WAF 記錄時，請再次為您 AWS WAF 建立服務連結角色。

為 AWS WAF編輯服務連結角色

AWS WAF 不允許您編輯AWSServiceRoleForWAFV2Logging服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

為 AWS WAF刪除服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 當您嘗試刪除資源時，如果 AWS WAF 服務正在使用此角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

若要刪除使用的 AWS WAF 資源 **AWSServiceRoleForWAFV2Logging**

1. 在主 AWS WAF 控台上，移除每個 Web ACL 的記錄。如需詳細資訊，請參閱 記錄 AWS WAF 網頁 ACL 流量。
2. 使用 API 或 CLI，為每個 Web ACL 提交 `DeleteLoggingConfiguration` 請求啟用記錄功能。如需詳細資訊，請參閱 AWS WAF API 參考。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台、IAM CLI 或 IAM API 刪除 `AWSServiceRoleForWAFV2Logging` 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

AWS WAF 服務連結角色的支援區域

AWS WAF 支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱 AWS WAF 端點和配額。

登錄和監控 AWS WAF

監控是維持 AWS 解決方案的可靠性、可用性和效能的 AWS WAF 重要組成部分。您應該從 AWS 解決方案的所有部分收集監視資料，以便在發生多點失敗時更輕鬆地偵錯。 AWS 提供數種工具來監控您的 AWS WAF 資源並回應潛在事件：

Amazon CloudWatch 警報

您可以使用 CloudWatch 警示來監視指定期間內的單一量度。如果指標超過指定臨界值，則 CloudWatch 會傳送通知給 Amazon SNS 主題或 AWS Auto Scaling 政策。如需詳細資訊，請參閱使用 Amazon 監控 CloudWatch。

AWS CloudTrail 日誌

CloudTrail 提供使用者、角色或 AWS 服務所採取之動作的記錄 AWS WAF。使用收集的資訊 CloudTrail，您可以判斷提出的要求 AWS WAF、提出要求的 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。如需詳細資訊，請參閱 使用 AWS CloudTrail記錄 API 呼叫。

AWS WAF 網絡 ACL 流量記錄

AWS WAF 為您的 Web ACL 分析的流量提供記錄。記錄檔包含資訊，例如從受保護的 AWS 資源 AWS WAF 接收要求的時間、有關要求的詳細資訊，以及要求符合之規則的動作設定。如需更多詳細資訊，請參閱 記錄 AWS WAF 網頁 ACL 流量。

符合性驗證 AWS WAF

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於您資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上進行HIPAA安全與合規架構 — 本白皮書說明公司如何使用建立符合資格的應 AWS 用程HIPAA式。

> **Note**
>
> 並非所有 AWS 服務 人都HIPAA符合資格。如需詳細資訊，請參閱合HIPAA格服務參考資料。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準 AWS 服務 與技術研究所 (NIST)、支付卡產業安全標準委員會 () 和國際標準化組織 ()PCI) 中保護安全控制指引的最佳做法，並將其對應至安全性控制。ISO
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您因應各種合規性需求 PCIDSS，例如符合特定合規性架構所要求的入侵偵測需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

韌性在 AWS WAF

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分離和隔離的可用區域，這些區域與低延遲、高輸送量和高冗餘網路相連。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠在可用區域之間自動容錯移轉，而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱AWS 全域基礎結構。

AWS WAF中的基礎設施安全

作為託管服務， AWS WAF 受到 AWS 全球網絡安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的API呼叫透 AWS WAF 過網路存取。使用者端必須支援下列專案：

- 傳輸層安全性 (TLS)。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 具有完美前向保密（ ）的密碼套件，例如（短暫的迪菲-赫爾曼PFS）或DHE（橢圓曲線短暫迪菲-赫爾曼）。ECDHE現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與IAM主體相關聯的秘密存取金鑰來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 以產生暫時安全憑證以簽署請求。

AWS WAF 配額

> **Note**
>
> 這是最新版本的 AWS WAF. 對於「 AWS WAF 經典」，請參閱AWS WAF 經典。

AWS WAF 受以下配額約束 (先前稱為限制)。所有可用區域的配額都相同。 AWS WAF 每個區域分別受制於這些配額。配額不會跨區域累計。

AWS WAF 對每個帳戶可擁有的最大實體數量具有預設配額。您可以請求提高這些配額。

資源	每個區域每個帳戶的預設配額
最大網絡數量 ACLs	100
規則群組數目上限	100
IP 集合的最大數量	100
每個 Web 每秒的要求數目上限 ACL	25,000
每個 Web ACL 或規則群組的自訂要求標頭數目上限	100
每個 Web ACL 或規則群組的自訂回應標頭數目上限	100
每個 Web ACL 或規則群組的自訂回應主體數目上限	50
Web Token 網域清單中的ACL權杖網域數目上限	10

開啟允許的每秒要求數 AWS WAF 上 CloudFront 限 (RPS) 由CloudFront 開發人員指南設定 CloudFront 並加以說明。

AWS WAF 針對每個區域的每個帳戶，具有下列實體設定的固定配額。這些配額無法變更。

資源	每個區域每個帳戶的配額
每個網頁的最大 Web ACL 容量單位 (WCUs) ACL *	5,000
WCUs每個規則群組的上限	5,000
每個規則群組的參照陳述式數目上限。在規則群組中，參考陳述式可以參考 IP 集或正則運算式模式集。	50
每個 Web 的參考語句的最大數量ACL。在 Web 中ACL，引用語句可以引用規則組，IP 集或正則表達式模式集。	50
每個 IP 集的最大 IP 位址數目 (以CIDR符號表示)	10,000

資源	每個區域每個帳戶的配額
每個網頁的最大速率規則數目 ACL	10
每個規則群組的最大速率規則數目	4
可針對速率型規則定義的最小請求速率	100
每個以速率為基礎的規則可限制速率的唯一 IP 位址數目上限	10,000
字符串 match 語句中的最大字符數	200
每個正則表達式模式中的最大字符數	200
每個正則表達式設置的唯一正則表達式模式	10
正則表達式集的最大數量	10
可檢查 Application Load Balancer 和 AWS AppSync 防護的 Web 要求主體大小上限	8 KB
可檢查的 Web 請求主體的最大大小 CloudFront、API閘道、Amazon Cognito、應用程式執行器和驗證存取保護 **	64 KB
每個規則陳述式的文字轉換數目上限	10
單一自訂回應定義的自訂回應主體內容大小上限	4 KB
單一自訂回應定義的自訂標頭數目上限	10
單一自訂要求定義的自訂標頭數目上限	10
單一規則群組或單一 Web 之所有回應主體內容的組合大小上限 ACL	50 KB

* 在網絡中使用 1,500 多WCUs個ACL會產生超出基本網絡價格的成本。ACL如需詳細資訊，請參閱 AWS WAF 網路 ACL 容量單位 (WCU) 和 AWS WAF 定價。

** 根據預設，API閘道、Amazon Cognito CloudFront、應用程式執行器和已驗證存取資源的主體檢查限制設定為 16 KB，但是您可以將 Web ACL 組態中任何這些資源的此限制增加到列出的上限。如需詳細資訊，請參閱 管理車身檢查尺寸限制。

AWS WAF 每個區域的每個帳戶的通話具有以下固定配額。這些配額適用於透過任何可用方式 (包括主控台、、CLI AWS CloudFormation RESTAPI、和) 對服務的呼叫總數SDKs。這些配額無法變更。

呼叫類型	每個區域每個帳戶的配額
`AssociateWebACL` 呼叫次數上限	每 2 秒一個請求
`DisassociateWebACL` 呼叫次數上限	每 2 秒一個請求
`GetWebACLForResource` 呼叫次數上限	每秒一個請求
`ListResourcesForWebACL` 呼叫次數上限	每秒一個請求
任何個別 `Get` 或 `List` 動作的呼叫次數上限 (若未定義其他配額)	每秒五個請求
任何個別 `Create`、`Put` 或 `Update` 動作的呼叫次數上限 (若未定義其他配額)	每秒一個請求

AWS WAF 中單一組織中所有帳戶的通話具有下列固定配額 AWS Organizations。這些配額適用於透過任何可用方式 (包括主控台、、CLI AWS CloudFormation RESTAPI、和) 對服務的呼叫總數SDKs。這些配額無法變更。

呼叫類型	單一區域內每個組織的配額
在美國東部 (維吉尼亞北部) (us-east-1) `ListResourcesForWebACL` 、美國西部 (奧勒岡州) (US-西部 -2) 或歐洲 (愛爾蘭) (歐洲-西部-1) 或歐洲 (愛爾蘭) (歐洲-西部 -1)，組織中所有帳戶撥打的最大電話數目。	每秒 12 個要求
組織中所有帳戶在任何單一區域中未列出不同配額的通話次數上限。`ListResourcesForWebACL`	每秒 6 個要求

將您的 AWS WAF 傳統資源遷移到 AWS WAF

本節提供將規則和 Web ACL 從 AWS WAF 傳統版移轉至 AWS WAF的指引。 AWS WAF 於二零一九年十一月發布。如果您使用 C AWS WAF lassic 建立規則和 Web ACL 等資源，則需要使用傳統版本來使 AWS WAF 用這些資源，或將它們遷移到最新版本。

在開始移轉工作之前，請先閱讀以熟 AWS WAF 悉。AWS WAF

主題

為什麼要移轉到 AWS WAF？

最新版本的 AWS WAF 提供了許多比先前版本的改進，同時保留了您習慣的大多數概念和術語。

下列清單說明最新版 AWS WAF中的主要變更。在繼續移轉之前，請花一些時間檢閱此清單，並熟悉本指南的其餘部分。 AWS WAF

- AWS 的受管規則 AWS WAF— 現在可透過受 AWS 管規則取得的規則群組可提供防護，以防止常見的網頁威脅。這些規則群組中的大部分都是免費隨附的 AWS WAF。如需詳細資訊，請參閱AWS 受管規則規則群組清單和部落格文章宣布 AWSAWS WAF.
- 新 AWS WAF API — 新的 API 允許您使用一組 API 配置所有 AWS WAF 資源。為了區分區域和全域應用程式，全新的 API 包含一個 `scope` 設定。如需 API 的詳細資訊，請參閱 AWS WAFV2 動作和 AWS WAFV2 資料類型。

  在 API、SDK、CLI 和 C AWS WAF lassic 中，會保留其命名配置 AWS CloudFormation，而且這個最新版本的 AWS WAF 參考與新增的V2或 v2 (視上下文而定)。
- 簡化的服務配額（限制）— AWS WAF 現在允許每個 Web ACL 更多規則，並允許您表達更長的正則表達式模式。如需詳細資訊，請參閱 AWS WAF 配額。
- Web ACL 限制現在以運算需求為基礎 — Web ACL 限制現在以 Web ACL 容量單位 (WCU) 為基礎。 AWS WAF 根據執行規則所需的作業產能，計算規則的 WCU。網路 ACL 的 WCU 是網路 ACL 中所有規則和規則群組的 WCU 總和。

如需 WCU 的一般資訊，請參閱如何 AWS WAF 工作。如需有關每個規則之 WCU 用法的資訊，請參閱規則陳述式基礎。

- 以文件為基礎的規則撰寫 — 您現在可以使用 JSON 格式撰寫和表示規則、規則群組和 Web ACL。您不再需要使用個別 API 呼叫來建立不同的條件，然後將條件與規則產生關聯。這大幅簡化了編寫和維護程式碼的方式。檢視 Web ACL 時，您可以透過主控台選擇 Download web ACL as JSON (將 Web ACL 下載為 JSON)，來存取 JSON 格式的 Web ACL。當您建立自己的規則時，可以選擇 Rule JSON editor (規則 JSON 編輯器) 來存取其 JSON 表示。
- 規則巢狀與完整邏輯作業支援 — 您可以使用邏輯規則陳述式和巢狀來撰寫複雜的組合規則。您可以建立如 `[A AND NOT(B OR C)]` 的陳述式。如需詳細資訊，請參閱 邏輯規則陳述式。
- 改善以速率為基礎的規則 — 在的最新版本中 AWS WAF，您可以自訂規則評估的時間範圍，以及規則如何彙總請求。您可以使用多種 Web 要求特性的組合來自訂彙總。此外，最新的以速率為基礎的規則會對流量變化做出更快的反應。如需詳細資訊，請參閱 速率型規則陳述式。
- IP 集的可變 CIDR 範圍支援 — IP 集規格現在在 IP 範圍內具有更大的彈性。對於 IPv4， AWS WAF 支援/1. /32 對於 IPv6， AWS WAF 支援/1到/128。如需 IP 集合的詳細資訊，請參閱 IP 集合比對規則陳述式。
- 可鏈接文本轉換 — AWS WAF 可以在檢查 Web 請求內容之前對其執行多個文本轉換。如需詳細資訊，請參閱 文字轉換選項。
- 改良的主控台體驗 — 新 AWS WAF 主控台具有視覺化規則產生器，以及使用者更直覺的主控台設計。
- Firewall Manager 員 AWS WAF 策略的擴充選項 — 在 AWS WAF Web ACL 的「Firewall Manager 員」管理中，您現在可以建立一組先 AWS WAF 處理的規則群組，以及一組最後 AWS WAF 處理的規則群組。套用 AWS WAF 原則後，本機帳戶擁有者可以新增自己的規則群組，以便在這兩個集合之間進行 AWS WAF 處理。如需 Firewall Manager 員 AWS WAF 策略的詳細資訊，請參閱AWS WAF 政策。
- AWS CloudFormation 支援所有規則陳述式類型 — AWS WAF 中 AWS CloudFormation 支援 AWS WAF 主控台和 API 支援的所有規則陳述式類型。此外，您可以輕鬆地將以 JSON 格式撰寫的規則轉換為 YAML 格式。

遷移的運作方式

自動化遷移會承載大部分的 C AWS WAF lassic Web ACL 配置，留下一些您需要手動處理的事情。

以下列出遷移 Web ACL 的高階步驟。

1. 自動遷移可讀取與現有 Web ACL 相關的所有內容，而無需修改或刪除 C AWS WAF lassic 中的任何內容。它會建立 Web ACL 及其相關資源的表現法，與之相容 AWS WAF。它會為新的 Web ACL 產生一個 AWS CloudFormation 範本，並將其存放在 Amazon S3 儲存貯體中。
2. 您可以將範本部署到 AWS CloudFormation，以便在中重新建立 Web ACL 和相關資源 AWS WAF。
3. 您可以檢閱 Web ACL，然後手動完成遷移，確保您的新 Web ACL 充分利用最新版 AWS WAF的功能。
4. 您手動將受保護的資源切換到新的 Web ACL。

遷移警告與限制

遷移作業不會繼承您的所有設定，就像您在 C AWS WAF lassic 中的設定一樣。有些項目 (例如受管規則) 不會在兩個版本之間完全映射。其他設定 (例如 Web ACL 與受保護 AWS 資源的關聯) 最初會在新版本中停用，因此您可以在準備就緒時新增這些設定。

下列清單說明遷移的注意事項，並說明您可能想要採取的任何回應步驟。請使用此概觀來規劃遷移。稍後詳細的遷移步驟會帶您演練建議的緩解步驟。

- 單一帳戶 — 您只能將任何帳號的 AWS WAF 傳統資 AWS WAF 源移轉至相同帳戶的資源。
- 託管規則 — 遷移不會從 AWS Marketplace 賣方帶來任何託管規則。有些 AWS Marketplace 賣家有同等的管理規則 AWS WAF ，你可以再次訂閱。執行此操作之前，請先檢閱隨最新版本的提供的 AWS 受管規則 AWS WAF。其中大多數對 AWS WAF 用戶都是免費的。如需受管規則的相關資訊，請參閱受管規則群組。
- Web ACL 關聯 — 遷移不會引入 Web ACL 和受保護資源之間的任何關聯。這是經過設計的，以避免影響您的生產工作負載。確認所有項目都已正確遷移之後，請將新的 Web ACL 與您的資源產生關聯。
- 記錄 — 已移轉 Web ACL 的記錄預設為停用。這是設計本身所致。當您準備好從 AWS WAF 傳統切換到時啟用記錄 AWS WAF。
- AWS Firewall Manager 規則群組 — 遷移不會處理由 Firewall Manager 員管理的規則群組。您可以移轉由 Firewall Manager 員管理的 Web ACL，但遷移作業不會超過規則群組。請不要將遷移工具用於這些 Web ACL，而是 AWS WAF 在 Firewall Manager 員中重新建立新策略。

> **Note**
>
> Firewall Manager 員為 AWS WAF 典型管理的規則群組為「Firewall Manager 員」規則群組。使用的新版本時 AWS WAF，規則群組是 AWS WAF 規則群組。它們在功能上是一樣的。

- AWS WAF 安全自動化 — 不要嘗試遷移任何AWS WAF 安全自動化。遷移並不會轉換 Lambda 函數，這些函數可能正由自動化使用中。當新的 AWS WAF 安全自動化解決方案可用且與最新版本相容時 AWS WAF，請重新部署該解決方案。

將網頁 ACL 從 AWS WAF 傳統版移轉至 AWS WAF

若要遷移 Web ACL 並切換至該 ACL，請執行自動遷移，然後完成一系列手動步驟。

主題

移轉 Web ACL：自動遷移

若要將 Web ACL 組態從「 AWS WAF 典型」自動移轉至 AWS WAF

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 選擇「切換到 AWS WAF 典型」，然後檢閱 Web ACL 的組態設定。請記下設定，並考慮前一節遷移警告與限制中所述的警告和限制。
3. 在頂端的資訊對話方塊中，找出以 Migrate Web ACL 開頭的句子，然後選擇移轉精靈的連結。這會啟動遷移精靈。

   如果您沒有看到資訊性對話方塊，可能是因為您啟動 C AWS WAF lassic 主控台以來已關閉它。在導覽列中，選擇 [切換至新的]， AWS WAF然後選擇 [切換至 AWS WAF 傳統]，資訊對話方塊應該會重新出現。
4. 選取您要遷移的 Web ACL。

5. 對於遷移組態，請提供用於範本的 Amazon S3 儲存貯體。您需要針對遷移 API 正確設定的 Amazon S3 儲存貯體，才能存放其產生的 AWS CloudFormation 範本。

   - 如果儲存貯體已加密，則加密必須使用 Amazon S3 (SSE-S3) 金鑰。遷移作業不支援使用 AWS Key Management Service (SSE-KMS) 金鑰加密。
   - 儲存貯體名稱必須以 `aws-waf-migration-` 開頭。例如 `aws-waf-migration-my-web-acl`。
   - 儲存貯體必須位於您要部署範本的區域中。例如，對於中的 Web ACL`us-west-2`，您必須在中使用 Amazon S3 儲存貯體，`us-west-2`而且必須將範本堆疊部署到`us-west-2`。

6. 對於 S3 bucket policy (S3 儲存貯體政策)，建議您選擇 Auto apply the bucket policy required for migration (自動套用遷移所需的儲存貯體政策)。如果您選擇自行管理儲存貯體，則必須手動套用下列儲存貯體政策：

   - 對於全球 Amazon CloudFront 應用程序（`waf`）：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "apiv2migration.waf.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/<CUSTOMER_ACCOUNT_ID>/
*"
        }
    ]
}
```

   - 對於區域性 Amazon API Gateway 或應用 Application Load Balancer 應用程式 (`waf-regional`)：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Principal": {
                "Service": "apiv2migration.waf-regional.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/<CUSTOMER_ACCOUNT_ID>/
*"
        }
    ]
}
```

7. 針對 Choose how to handle rules that cannot be migrated (選擇如何處理無法遷移的規則)，選擇排除無法遷移的規則，或停止遷移。如需無法遷移之規則的相關資訊，請參閱遷移警告與限制。
8. 選擇下一步。
9. 在 [建立 AWS CloudFormation 範本] 中，確認您的設定，然後選擇 [開始建立 AWS CloudFormation 範本] 以開始移轉程序。這可能需要幾分鐘的時間，視您的 Web ACL 複雜度而定。
10. 在 [建立並執行 AWS CloudFormation 堆疊以完成移轉] 中，您可以選擇移至 AWS CloudFormation 主控台以從範本建立堆疊，以建立新的 Web ACL 及其資源。若要這麼做，請選擇 [建立 AWS CloudFormation 堆疊]。

自動遷移程序完成後，您就可以繼續進行手動後續步驟。請參閱遷移 Web ACL：手動後續步驟。

遷移 Web ACL：手動後續步驟

完成自動遷移之後，請檢閱新建立的 Web ACL，並填入遷移沒有為您轉變過來的元件。下列程序涵蓋遷移無法處理的 Web ACL 管理層面。如需清單，請參閱遷移警告與限制。

完成基本遷移 - 手動步驟

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。
2. 主控台應該會自動使用最新版本的 AWS WAF. 要驗證這一點，請在導航窗格中，檢查您是否可以看到「切換到 AWS WAF 經典」選項。如果您看到「切換到新版本」 AWS WAF，請選擇該選項以切換到最新版本。
3. 在導覽窗格中，選擇 Web ACL。
4. 在 Web ACL 頁面，在您建立新的 Web ACL 的區域清單中找出您的新 Web ACL。選擇 Web ACL 的名稱，以顯示 Web ACL 的設定。

5. 針對先前的 AWS WAF 傳統網頁 ACL 檢閱新 Web ACL 的所有設定。根據預設，會停用記錄日誌和受保護的資源關聯。您可以在準備好切換時啟用這些功能。
6. 如果您的 AWS WAF 傳統 Web ACL 具有以速率為基礎的規則，且條件不會在移轉過程中移轉。您可以將條件新增至新 Web ACL 中的規則。

   a. 在您的 Web ACL 設定頁面中，選擇 Rules (規則) 索引標籤。

   b. 在清單中找到以速率為基礎的規則，選取該規則，然後選擇 Edit (編輯)。

   c. 對於 Criteria to count request towards rate limit (將請求計入費率限制的條件)，選取 Only consider requests that match the criteria in a rule statement (僅考慮符合規則陳述式中條件的請求)，然後提供您的其他條件。您可以使用任何可巢狀處理的規則陳述式 (包括邏輯陳述式) 來新增準則。如需您的選擇的相關資訊，請參閱速率型規則陳述式。
7. 如果您的 C AWS WAF lassic Web ACL 具有受管規則群組，則移轉時不會帶入規則群組包含項目。您可以將受管規則群組新增至新的 Web ACL。檢閱有關受管規則群組的資訊，包括新版本的可用的 AWS AWS WAF受管規則清單受管規則群組。若要新增受管規則群組，請執行下列動作：

   a. 在您的 Web ACL 設定頁面中，選擇 Web ACL Rules (規則) 索引標籤。

   b. 選擇 Add rules (新增規則)，然後選擇 Add managed rule groups (新增受管規則群組)。

   c. 展開您所選廠商的清單，然後選取您要新增的規則群組。 AWS Marketplace 賣家可能需要訂閱規則群組。如需在 Web ACL 中使用受管規則群組的詳細資訊，請參閱受管規則群組和 Web ACL 規則和規則群組評估。

完成基本遷移程序之後，我們建議您檢閱您的需求並考慮其他選項，以確保新的組態盡可能有效率，並且使用最新可用的安全選項。請參閱遷移 Web ACL：其他考量。

遷移 Web ACL：其他考量

檢閱新的 Web ACL，並考慮新版本中可用的選項， AWS WAF 以確定組態盡可能有效率，而且使用的是最新的可用安全性選項。

其他 AWS 受管規則

請考慮在 Web ACL 中實作其他 AWS 受管規則，以增加應用程式的安全狀態。這些都包含 AWS WAF 在內，無需額外費用。 AWS 受管規則包含下列類型的規則群組：

- 基準規則群組可針對各種常見威脅提供一般保護，例如停止已知的錯誤輸入進入您的應用程式，以及防止管理頁面存取。
- 使用案例特定的規則群組可為眾多不同的使用案例和環境提供增量式保護。

- IP 評價清單會根據用戶端的來源 IP 提供安全威脅情報。

如需詳細資訊，請參閱 AWS 的受管規則 AWS WAF。

規則最佳化與清理

重新查看您的舊規則，並考慮進行重寫或刪除過時的規則將它們最佳化。例如，如果您過去部署了 OWASP 十大 Web 應用程式弱點技術 paper 中的範 AWS CloudFormation 本，準備 OWASP 前 10 大 Web 應用程式弱點使用 AWS WAF 和我們的新白皮書，您應該考慮將其取代為受管規則。 AWS 雖然在文件中找到的概念仍然適用，而且可協助您撰寫自己的規則，但範本建立的規則已大部分被 AWS Managed Rules 取代。

Amazon CloudWatch 指標和警報

重新訪問您的 Amazon CloudWatch 指標並根據需要設置警報。遷移不會超過CloudWatch 警報，您的指標名稱可能不是您想要的。

與您的應用程式團隊一起審核

與您的應用程式團隊合作，並檢查您的安全狀態。找出應用程式經常剖析的欄位，並相應地新增規則來清理輸入。檢查是否有任何邊緣案例，如果應用程式的商業邏輯無法處理，新增規則以找出這些案例。

規劃切換

與您的應用程式團隊一起規劃切換的時機。從舊 Web ACL 關聯切換到新的 ACL 關聯可能需要很少的時間才能傳播到儲存資源的所有區域。傳輸時間可以是幾秒鐘到分鐘數。在此期間，某些請求將由舊的 Web ACL 處理，其他請求將由新的 Web ACL 處理。您的資源將在整個切換過程中受到保護，但您可能會注意到切換進行中的請求處理不一致。

當您準備好切換時，請按照遷移 Web ACL：切換中的程序進行操作。

遷移 Web ACL：切換

驗證新的 Web ACL 設定之後，您就可以開始使用它來取代 AWS WAF 傳統網頁 ACL。

開始使用新 AWS WAF 網頁 ACL 的步驟

1. 依照中的指引，將 AWS WAF Web ACL 與您要保護的資源相關聯建立 Web ACL 與資源的關聯或取消關聯 AWS。這會自動解除資源與舊 Web ACL 的關聯。

交換器可能需要幾秒鐘到幾分鐘的時間才能傳播。在此期間，舊的 Web ACL 可能會處理某些要求，而新的 Web ACL 可能會處理其他要求。您的資源將在整個切換過程中受到保護，但在請求處理完成之前，您可能會注意到處理請求不一致。

2. 請遵循記錄 AWS WAF 網頁 ACL 流量的指引設定新 Web ACL 的記錄日誌。
3. (選擇性) 如果您的 AWS WAF 傳統 Web ACL 不再與任何資源相關聯，請考慮將其完全從 AWS WAF 傳統版移除。如需相關資訊，請參閱刪除網頁 ACL。

AWS WAF 經典

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

AWS WAF 典型是一種 Web 應用程式防火牆，可讓您監控轉寄至 Amazon API 閘道 API、亞馬遜 CloudFront 或 Application Load Balancer 的 HTTP 和 HTTPS 請求。 AWS WAF 經典版也可讓您控制內容的存取權。根據您指定的條件，例如要求來源的 IP 位址或查詢字串的值、API Gateway CloudFront 或應 Application Load Balancer 會以要求的內容或 HTTP 403 狀態碼 (禁止) 回應要求。您還可以配置 CloudFront 為在請求被阻止時返回自定義錯誤頁面。

主題

設定 AWS WAF 經典

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

本主題說明初步步驟，例如建立使用者帳戶，以便準備使用「 AWS WAF 傳統」。您不需要支付這些費用。我們只會針對您使用的 AWS 服務向您收費。

> **Note**
>
> 如果您是新使用者 AWS WAF，請勿遵循 AWS WAF 經典版的下列設定步驟。請改為遵循最新版本的步驟 AWS WAF，位於設定您的帳戶以使用服務。

完成這些步驟之後，請參閱開始使用經 AWS WAF 典版繼續開始使用 AWS WAF 經典版。

> **Note**
>
> AWS Shield Standard 包含在 AWS WAF 經典中，不需要額外的設置。如需詳細資訊，請參閱 如何 AWS Shield 和 Shield 高級工作。

使用「 AWS WAF 典型」或第一 AWS Shield Advanced 次使用之前，請完成本節中的步驟。

主題

- 註冊一個 AWS 帳戶
- 建立具有管理權限的使用者
- 下載工具

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊一個時 AWS 帳戶，將創建AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理權限的使用者

註冊後，請保護您的 AWS 帳戶 AWS 帳戶根使用者 AWS IAM Identity Center、啟用和建立系統管理使用者，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

1. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。AWS Management Console在下一頁中，輸入您的密碼。

   如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。
2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

   如需指示，請參閱《IAM 使用者指南》中的為 AWS 帳戶 根使用者啟用虛擬 MFA 裝置 (主控台)。

建立具有管理權限的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。
2. 在 IAM 身分中心中，將管理存取權授予使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。

以具有管理權限的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

  如需使用 IAM 身分中心使用者登入的說明，請參閱使用AWS 登入 者指南中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「建立權限集」。
2. 將使用者指派給群組，然後將單一登入存取權指派給群組。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「新增群組」。

下載工具

AWS Management Console 包含 C AWS WAF lassic 的主控台，但如果您想要以程式設計方式存取 C AWS WAF lassic，請參閱下列內容：

- 如果您想要呼叫 AWS WAF 傳統 API，而不必處理組裝原始 HTTP 要求等低層級詳細資料，則可以使用 AWS SDK。 AWS SDK 提供封裝 AWS WAF 經典和其 AWS 他服務功能的函數和資料類型。若要下載 AWS SDK，請參閱適用的頁面，其中也包含必要條件和安裝說明：
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

  如需開 AWS 發套件的完整清單，請參閱 Amazon Web Services 的工具。
- 如果您使用的程式設計語言 AWS 不提供 SDK，AWS WAF API 參考會記錄 AWS WAF 傳統支援的作業。

- AWS Command Line Interface （AWS CLI）支持 AWS WAF 經典。 AWS CLI 可讓您從命令列控制多個 AWS 服務，並透過指令碼將它們自動化。如需詳細資訊，請參閱 AWS Command Line Interface。
- AWS Tools for Windows PowerShell 支持 AWS WAF 經典。如需詳細資訊，請參閱 AWS Tools for PowerShell Cmdlet 參考。

AWS WAF 經典如何運作

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

您可以使用 AWS WAF 典型來控制 API Gateway、Amazon CloudFront 或應用 Application Load Balancer 如何回應 Web 請求。首先，建立條件、規則和 web 存取控制清單 (Web ACL)。定義您的條件，並將您的條件組合成規則，再組合這些規則到 Web ACL 中。

> **Note**
>
> 您也可以使用 AWS WAF 傳統版來保護在 Amazon Elastic Container Service (Amazon ECS) 容器中託管的應用程式。Amazon ECS 是可高度擴展、快速的容器管理服務，可讓您輕鬆執行、停止和管理叢集上的 Docker 容器。若要使用此選項，您可以將 Amazon ECS 設定為使用啟用 AWS WAF 典型的 Application Load Balancer，在服務中的任務中路由和保護 HTTP/HTTPS (第 7 層) 流量。如需詳細資訊，請參閱 Amazon 彈性容器服務開發人員指南中的主題服務負載平衡。

條件

條件定義了您希望 C AWS WAF lassic 在 Web 請求中監視的基本特徵：

- 指令碼可能為惡意。攻擊者可以利用 web 應用程式的漏洞內嵌指令碼。此為跨網站指令碼。
- 發出請求的 IP 地址或地址範圍。
- 發出請求的國家/地區或地理位置。

- 指定請求的部分長度，例如：查詢字串。
- SQL 程式碼可能為惡意。攻擊者會藉由內嵌惡意 SQL 程式碼於 web 請求中，嘗試從您的資料庫碼擷取資料。此為 SQL injection。
- 字串會出現在請求，例如出現在 User-Agent 標頭的值或出現在查詢字串的文字字串。您也可以使用規則運算式 (regex) 指定這些字串。

某些條件採用多種數值 例如，您可以指定(最多) 10,000 個 IP 地址或在此 IP 條件下的 IP 地址範圍。

規則

您可以將條件合併到規則中，以精確定位要允許、封鎖或計數的要求。 AWS WAF 經典提供了兩種類型的規則：

一般規則

一般規則只使用條件針對特定請求。例如，根據最近已知攻擊者的請求，您可建立包括以下條件的規則：

- 來自 192.0.2.44 的請求。
- 在 User-Agent 標頭中包含 BadBot 值。
- 它們好像有包含類似 SQL 程式碼的查詢字串。

當規則包含多個條件時 (如本範例所示)，C AWS WAF lassic 會尋找符合所有條件的要求，也就是說，它是一起的AND條件。

請至少新增一項條件至一般規則。沒有條件的一般規則無法符合任何請求，因此永遠不會觸發規則的動作 (允許、計數或封鎖)。

以速率為基礎的規則

以速率為基礎的規則就像一般規則，但增加了速率限制。以速率為基礎的規則會計算從滿足規則條件的 IP 地址抵達的請求數。如果在五分鐘期間內，來自 IP 地址的請求超過速率限制，規則就會觸發動作。動作可能需要一兩分鐘才會觸發。

條件對以速率為基礎的規則來說是選用的。如果您未在以速率為基礎的規則中新增任何條件，速率限制會套用到所有 IP 地址。如果您結合條件與速率限制，速率限制會套用到符合條件的 IP 地址。

例如，根據最近已知攻擊者的請求，您可建立包括以下條件的以速率為基礎的規則：

- 來自 192.0.2.44 的請求。
- 在 User-Agent 標頭中包含 BadBot 值。

在這以速率為基礎的規則中，您還可以定義的速率限制。在這個範例中，假設您建立的速率限制為 1,000。同時符合這兩種條件且每五分鐘超過 1,000 的請求，會觸發此規則在 Web ACL 定義的動作 (封鎖或計數)。

未同時符合這兩個條件的請求不會計入速率限制，也不會受到此規則影響。

在第二個範例中，假設您想要限制對您網站的特定頁面所發出的請求。若要這麼做，您可以新增以下字串比對條件至以速率為基礎的規則中：

- 要篩選的請求部分是 URI。
- 請求類型是 Starts with。
- 符合值是 login。

更進一步，您需要指定 RateLimit 為 1,000。

將這個以速率為基礎的規則新增到 Web ACL，您就可以限制對您登入頁面的請求數量，但不影響網站的其他部分。

Web ACL

將您的條件組合成規則後，再組合這些規則到 Web ACL 中。您可以在這裡為每個規則 (允許、封鎖或計數) 定義動作以及預設動作：

每個規則的動作

當 Web 請求符合規則中的所有條件時，C AWS WAF lassic 可以阻止請求或允許將請求轉發到 API Gateway API， CloudFront 分發或 Application Load Balancer。您可以指定要 AWS WAF 傳統針對每個規則執行的動作。

AWS WAF 典型會依照您列出規則的順序，將請求與 Web ACL 中的規則進行比較。 AWS WAF Classic 接著會採取與要求相符之第一個規則相關聯的動作。例如，如果 Web 要求符合一個允許要求的規則，而另一個封鎖要求的規則相符，則 AWS WAF 傳統會根據最先列出的規則來允許或封鎖要求。

如果您想在開始使用新規則之前測試新規則，也可以設定 C AWS WAF lassic 來計算符合規則中所有條件的要求。與允許或封鎖請求的規則一樣，計數請求的規則受其自身在 web ACL 清單上所列的順序影響。例如，如果 web 請求符合兩個規則，一個為允許請求，另一個為計數請求，如果該允許請求的規則先列於清單，則不會對此請求進行計數。

預設動作

預設動作會決定 AWS WAF 傳統是否允許或封鎖不符合 Web ACL 中任何規則中所有條件的要求。例如，假設您建立 Web ACL，僅新增您之前定義過的規則：

- 來自 192.0.2.44 的請求。
- 在 `User-Agent` 標頭中包含 `BadBot` 值。
- 它們好像有包含惡意 SQL 的查詢字串。

如果要求不符合規則中的全部三個條件，且預設動作為`ALLOW`，C AWS WAF lassic 會將要求轉送至 API Gateway CloudFront 或 Application Load Balancer，而服務會以要求的物件回應。

如果您將兩個或多個規則新增至 Web ACL，則只有在要求不符合任何規則中的所有條件時，C AWS WAF lassic 才會執行預設動作。例如，假設您新增第二個規則，其中含有一項條件：

- 請求在 `User-Agent` 標頭有 `BIGBadBot` 值。

AWS WAF 只有當請求不符合第一個規則中的所有三個條件，且不符合第二個規則中的一個條件時，Classic 才會執行預設動作。

在某些情況下， AWS WAF 可能會遇到內部錯誤，延遲對 Amazon API 閘道、Amazon CloudFront 或應 Application Load Balancer 的回應，說明是否允許還是封鎖請求。在這些情況下，通常 CloudFront會允許請求或提供內容。API Gateway 和應用程式負載平衡器通常則會拒絕請求，而且不會處理內容。

AWS WAF 經典定價

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

使用 AWS WAF 傳統版時，您只需支付您建立的網頁 ACL 和規則，以及 AWS WAF 傳統檢查的 HTTP 要求數量付費。如需詳細資訊，請參閱AWS WAF 傳統定價。

開始使用經 AWS WAF 典版

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

本教學課程顯示如何使用「 AWS WAF 傳統」來執行下列工作：

- 設定「 AWS WAF 經典」。
- 使用 AWS WAF 典型主控台建立 Web 存取控制清單 (Web ACL)，並指定要用來篩選 Web 要求的條件。例如，您可以指定請求源於的 IP 地址和僅由攻擊者使用的請求數值。
- 新增條件至規則。規則可讓您定位要封鎖或允許的 web 請求。Web 要求必須符合規則中的所有條件，C AWS WAF lassic 才能根據您指定的條件封鎖或允許要求。
- 新增規則至您的 Web ACL。可以在此處指定您是否想要根據所新增至每個規則的條件來允許或封鎖 web 請求。
- 指定預設動作 (封鎖或允許)。這是 C AWS WAF lassic 在 Web 請求不符合您的任何規則時採取的操作。
- 選擇您希望 AWS WAF 經典 CloudFront 版檢查 Web 請求的 Amazon 分發。本教學僅涵蓋應用 CloudFront程 Application Load Balancer 和 Amazon API Gateway 的程序基本上是相同的。 AWS WAF 經典版 CloudFront 適用於所有人 AWS 區域。 AWS WAF AWS 服務端點上列出的區域提供可搭配 API Gateway 或應用程式負載平衡器使用的典型版。

> **Note**
>
> AWS 一般而言，對於您在本教學課程中建立的資源，每天收取的費用不到 USD $0.25。當您完成此教學課程，我們建議您刪除資源以免產生不必要的費用。

主題

步驟 1：設定 AWS WAF 傳統版

如果您尚未遵循中的一般設定步驟設定 AWS WAF 經典，請立即執行。

步驟二：建立 Web ACL

C AWS WAF lassic 主控台會引導您完成設定 AWS WAF 典型的程序，以根據您指定的條件封鎖或允許 Web 要求，例如要求來源的 IP 位址或要求中的值。在此步驟中，建立Web ACL。

建立 Web ACL

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 如果這是您第一次使用「 AWS WAF 典型」，請選擇「移至 AWS WAF 典型」，然後選擇「設定 Web ACL」。

   如果您之前使用過 AWS WAF 傳統版，請在導覽窗格中選擇 [Web ACL]，然後選擇 [建立 Web ACL]。
3. 在 Name web ACL (命名 Web ACL) 頁面的 Web ACL name (Web ACL 名稱) 中輸入名稱。

> **Note**
>
> 建立 Web ACL 後無法修改名稱。

4. 對於CloudWatch 測量結果名稱，請輸入名稱。名稱只能包含英數字元 (A-Z、a-z、0-9)。不能含有空格。

   > **Note**
   >
   > 建立 Web ACL 後無法修改名稱。

5. 對於 區域，選擇一個區域。如果您要將此 Web ACL 與 CloudFront 分佈產生關聯，請選擇「全域」(CloudFront)。
6. 對於要關聯的AWS 資源，選擇您想要將此 Web ACL 關聯的資源，然後選擇下一步。

步驟 3：建立 IP 比對條件

IP 比對條件可指定發出請求的 IP 地址或 IP 地址範圍。在此步驟中，建立 IP 比對條件。在後續步驟中，您指定是否要允許或封鎖來自指定 IP 地址的請求。

> **Note**
>
> 如需 IP 比對條件的詳細資訊，請參閱使用 IP 比對條件。

建立 IP 比對條件

1. 在建立條件頁面，於IP 符合條件，選擇建立條件。
2. 在 Create IP match condition (建立 IP 比對條件) 對話方塊中，於 Name (名稱)，輸入名稱。名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_-!"#`+*},./。
3. 針對 Address (地址)，輸入 192.0.2.0/24。指定於 CIDR 符號的此 IP 地址範圍，包含 IP 地址，從 192.0.2.0 192.0.2.255。(例如，預留 192.0.2.0/24 IP 地址範圍，則沒有任何 web 請求會來自這些 IP 地址)。

   AWS WAF 傳統版支援 IPv4 位址範圍：/8 以及 /16 到 /32 之間的任何範圍。 AWS WAF 傳統版支援 IPv6 位址範圍：/24、/32、48、/56、64 和 /128。(若要指定單一 IP 地址，例如 192.0.2.44，請輸入 192.0.2.44/32)。不支援其他範圍。

   如需 CIDR 符號表示法的詳細資訊，請參閱 Wikipedia 文章 無類別網域間路由。
4. 選擇建立。

步驟 4：建立地理比對條件

地理比對條件指定國家/地區為請求的發源地。在此步驟中，建立地理比對條件。在後續步驟中，您指定是否要允許或封鎖來自指定國家/地區的請求。

> **Note**
>
> 如需地理比對條件的詳細資訊，請參閱使用地理比對條件。

建立地理比對條件

1. 在建立條件頁面，於地理符合條件，選擇建立條件。
2. 在 Create geo match condition (建立地理比對條件) 對話方塊中，於 Name (名稱)，輸入名稱。名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_-!"#`+*},./。
3. 選擇位置類型和國家/地區。目前， Location type (位置類型) 只能是 Country (國家/地區)。
4. 選擇新增位置。
5. 選擇建立。

步驟 5：建立字串比對條件

字串比對條件會識別要 C AWS WAF lassic 在要求中搜尋的字串，例如標頭或查詢字串中的指定值。通常，字串包含可列印 ASCII 字元，但您可以指定十六字元範圍 0x00 到 0xFF 的任何字元 (小數點 0 到 255)。在此步驟中，建立字串比對條件。在後續步驟中，您指定是否要允許或封鎖含有指定字串的請求。

> **Note**
>
> 如需字串比對條件的詳細資訊，請參閱使用字串比對條件。

建立字串比對條件

1. 在 Create conditions (建立條件) 頁面，於 String and regex match conditions (字串和 regex 符合條件) 選擇 Create condition (建立條件)。
2. 在 Create string match condition (建立字串比對條件) 對話方塊中，輸入以下的值：

名稱

輸入名稱。名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_-!"#`+*},./。

Type

選擇 String match (字串比對)。

要篩選的請求部分是

選擇您希望 C AWS WAF lassic 檢查指定字符串的 Web 請求部分。

在此範例中，請選擇 Header (標頭)。

> **Note**
>
> 如果您選擇 [內文] 做為要篩選的要求的部分值， AWS WAF 典型只會檢查前 8192 個位元組 (8 KB)，因為只會 CloudFront 轉寄前 8192 個位元組以進行檢查。若要允許或封鎖主體超過 8192 個位元組的要求，您可以建立大小限制條件。（ AWS WAF 經典從請求頭獲取主體的長度。）如需詳細資訊，請參閱 使用容量限制條件。

標頭 (必要，如果「部分請求的篩選條件」為「標頭」時)

因為您選擇了要篩選的要求部分的標頭，因此您必須指定要 C AWS WAF lassic 檢查的標頭。輸入 User-Agent (使用者代理程式)。(此值不區分大小寫)。

符合類型

選擇指定字串必須顯示在 User-Agent (使用者代理程式) 標頭中的位置，例如，在開始時或在字串中。

在此範例中，選擇「完全相符」，表示 C AWS WAF lassic 會檢查網頁要求的標頭值與您指定的值相同。

轉換

為了繞過 C AWS WAF lassic，攻擊者在 Web 請求中使用不尋常的格式化，例如通過添加空格或 URL 編碼部分或全部請求。轉換藉由移除空格、URL 解碼、或執行其他操作可以降低攻擊常使用的不常見格式，將 web 請求轉換成更標準的格式。

您只能指定一種文字轉換類型。

在此範例中，請選擇 None (無)。

base64 編碼值

如果您於 Value to match (符合值) 輸入的值是 base64 編碼，請選取此核取方塊。

在此範例中，不需選取核取方塊。

符合值

指定您希望 C AWS WAF lassic 在您在篩選要求的部分中指定的 Web 要求部分中搜尋的值。

在此範例中，輸入BadBot。 AWS WAF 經典將檢查 Web 請求中的值的`User-Agent`標題BadBot。

符合值 的長度上限為 50 個字元。如果您想要指定 base64 編碼值，可在編碼前提供最多 50 個字元。

3. 如果您希望 C AWS WAF lassic 檢查多個值的 Web 請求，例如包含的`User-Agent`標頭`BadBot`和包含的查詢字符串`BadParameter`，則有兩種選擇：

   - 如果您想要當它們含有兩者得的值時 (AND) 才允許或封鎖 web 請求，您可以為每個值建立一個字串比對條件。
   - 如果您想要當它們含有其中一個值或兩者的值時 (OR) 才允許或封鎖 web 請求，您可以新增兩者的值至相同的字串比對條件中。

   在本範例中，請選擇 Create (建立)。

步驟 5A：建立 Regex 條件 (選用)

規則運算式條件是一種字串比對條件類型，類似的是，它會識別您希望 C AWS WAF lassic 在要求中搜尋的字串，例如標頭或查詢字串中的指定值。主要區別在於您使用正則表達式（regex）來指定要 C AWS WAF lassic 搜索的字符串模式。在此步驟中，建立 regex 比對條件。在後續步驟中，您指定是否要允許或封鎖含有指定字串的請求。

> **Note**
>
> 如需規則運算式比對條件的詳細資訊，請參閱使用 Regex 比對條件。

建立 regex 比對條件

1. 在 Create conditions (建立條件) 頁面，於 String match and regex conditions (字串符合和 regex 條件) 選擇 Create condition (建立條件)。
2. 在 Create string match condition (建立字串比對條件) 對話方塊中，輸入以下的值：

   名稱

   輸入名稱。名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_-!"#`+*},./。

   Type

   選擇 Regex match (Regex 比對)。

   要篩選的請求部分是

   選擇您希望 C AWS WAF lassic 檢查指定字符串的 Web 請求部分。

   在此範例中，請選擇 Body (內容主體)。

   > **Note**
   >
   > 如果您選擇 [內文] 做為要篩選的要求的部分值， AWS WAF 典型只會檢查前 8192 個位元組 (8 KB)，因為只會 CloudFront 轉寄前 8192 個位元組以進行檢查。若要允許或封鎖主體超過 8192 個位元組的要求，您可以建立大小限制條件。（ AWS WAF 經典從請求頭獲取主體的長度。）如需詳細資訊，請參閱 使用容量限制條件。

   轉換

   為了繞過 C AWS WAF lassic，攻擊者在 Web 請求中使用不尋常的格式化，例如通過添加空格或 URL 編碼部分或全部請求。轉換藉由移除空格、URL 解碼、或執行其他操作可以降低攻擊常使用的不常見格式，將 web 請求轉換成更標準的格式。

   您只能指定一種文字轉換類型。

   在此範例中，請選擇 None (無)。

   比對請求的 Regex 模式

   選擇 Create regex pattern set (建立 Regex 模式集)。

新模式集的名稱

輸入名稱，然後指定要 C AWS WAF lassic 搜尋的正則運算式模式。

接下來，輸入正則表達式 I [a@] MAB [a@] d 請求。 AWS WAF 經典將檢查 Web 請求中的值的`User-Agent`標題：

- 艾馬 BadRequest
- IamAB@dRequest
- I @mA BadRequest
- I@mAB@dRequest

3. 選擇 Create pattern set and add filter (建立模式集並新增篩選條件)。
4. 選擇建立。

步驟 6：建立 SQL Injection 比對條件

SQL 插入比對條件可識別您希望 C AWS WAF lassic 檢查是否有惡意 SQL 程式碼的 Web 要求部分，例如標頭或查詢字串。攻擊者使用 SQL 查詢來擷取您資料庫的資料。在此步驟中，建立 SQL injection 比對條件。在後續步驟中，您指定是否要允許或封鎖貌似含有惡意 SQL 程式碼的請求。

> **Note**
>
> 如需字串比對條件的詳細資訊，請參閱使用 SQL Injection 比對條件。

建立 SQL Injection 比對條件

1. 在 Create conditions (建立條件) 頁面，於 SQL injection match conditions (SQL injection 符合條件)，選擇 Create condition (建立條件)。
2. 在 Create SQL injection match condition (建立 SQL injection 比對條件) 對話方塊中，輸入以下的值：

名稱

輸入名稱。

要篩選的請求部分是

選擇您希望 AWS WAF 傳統版檢查是否有惡意 SQL 程式碼的 Web 要求部分。

在此範例中，選擇 Query string (查詢字串)。

> **Note**
>
> 如果您選擇 [內文] 做為要篩選的要求的部分值， AWS WAF 典型只會檢查前 8192 個位元組 (8 KB)，因為只會 CloudFront 轉寄前 8192 個位元組以進行檢查。若要允許或封鎖主體超過 8192 個位元組的要求，您可以建立大小限制條件。（ AWS WAF 經典從請求頭獲取主體的長度。）如需詳細資訊，請參閱 使用容量限制條件。

轉換

在此範例中，請選擇 URL decode (URL 解碼)。

攻擊者會使用不尋常的格式，例如 URL 編碼，以繞過 AWS WAF 傳統版。URL 解碼選項可在 AWS WAF 傳統檢查請求之前消除 Web 請求中的某些格式。

您只能指定一種文字轉換類型。

3. 選擇建立。
4. 選擇下一步。

步驟 7：(選用) 建立其他條件

AWS WAF 經典包括其他條件，包括以下條件：

- 大小限制條件 — 識別您希望 C AWS WAF lassic 檢查長度的 Web 請求部分，例如標頭或查詢字串。如需詳細資訊，請參閱 使用容量限制條件。
- 跨網站指令碼比對條件 — 識別您要檢查是否有惡意指令碼的 Web 要 AWS WAF 求部分，例如標頭或查詢字串。如需詳細資訊，請參閱 使用跨網站指令碼比對條件。

您可以現在選擇性地建立這些條件，或者您可以略過此步驟，前往 步驟 8：建立規則並新增條件。

步驟 8：建立規則並新增條件

您可以建立規則來指定要 AWS WAF 傳統在 Web 請求中搜尋的條件。如果您在規則中新增多個條件，Web 要求必須符合 C AWS WAF lassic 規則中的所有條件，才能根據該規則允許或封鎖要求。

> **Note**
>
> 如需規則的詳細資訊，請參閱使用規則。

建立規則並新增條件

1. 在 Create rules (建立規則) 頁面上，選擇 Create rules (建立規則)。
2. 在 Create rules (建立規則) 對話方塊中，輸入以下的值：

   名稱

   輸入名稱。

   CloudWatch 量度名稱

   輸入「 AWS WAF 典型」將建立並與規則產生關聯的 CloudWatch 測量結果名稱。名稱只能包含英數字元 (A-Z、a-z、0-9)。不能含有空格。

   規則類型

   選擇 Regular rule (一般規則) 或 Rate-based rule (以速率為基礎的規則)。以速率為基礎的規則與一般規則相同，但還會考慮每五分鐘，從已識別的 IP 地址所發出的請求數量。如需這些規則類型的詳細資訊，請參閱AWS WAF 經典如何運作。在此範例中，選擇 `Regular rule`。

   速率限制

   對於以速率為基礎的規則，輸入五分鐘期間內允許來自符合規則條件之 IP 地址的最大請求數量。
3. 對於您希望新增到規則的第一個條件，請指定以下設定：

   - 根據 Web 要求是否符合條件中的設定，選擇您要 C AWS WAF lassic 允許或封鎖要求。

     在此範例中，請選擇 does (有符合)。
   - 選擇您想新增至規則的條件類型：IP 比對設定條件、字串比對設定條件、或是 SQL injection 比對設定條件。

     在此範例中，選擇 originate from IP addresses in (源於的 IP 地址)。
   - 選擇要新增到規則的條件。

     在此範例中，選擇您在前一任務中所建立的 IP 比對條件。

4. 選擇新增條件。
5. 新增您之前建立的地理比對條件。指定下列值：
   - When a request does (當請求有)
   - 源於的地理位置
   - 選擇您的地裡比對條件。
6. 選擇新增其他條件。
7. 新增您之前建立的字串比對條件。指定下列值：
   - When a request does (當請求有)
   - 至少符合字串比對條件裡的一項篩選條件
   - 選擇您的字串比對條件。
8. 選擇新增條件。
9. 新增您之前建立的 SQL injection 比對條件。指定下列值：
   - When a request does (當請求有)
   - 至少符合 SQL injection 比對條件裡的一項篩選條件
   - 選擇您的 SQL injection 比對條件。
10. 選擇新增條件。
11. 新增您之前建立的容量限制條件。指定下列值：
    - When a request does (當請求有)
    - 至少符合容量限制條件裡的一項篩選條件
    - 選擇您的容量限制條件。
12. 如果您建立任何其他的條件，例如 regex 條件，以相同方式新增。
13. 選擇建立。
14. 對於 Default action (預設動作)，選擇 Allow all requests that don't match any rules (允許不符合任何規則的請求)。
15. 選擇 Review and create (檢閱和建立)。

步驟 9：新增規則至 Web ACL

當您新增規則至 Web ACL，您可以指定以下設定：

- 您希望 C AWS WAF lassic 對符合規則中所有條件的 Web 請求採取的動作：允許、封鎖或計數要求。
- Web ACL 的預設動作。這是您希望 C AWS WAF lassic 對不符合規則中所有條件的 Web 請求採取的操作：允許或阻止請求。

AWS WAF 傳統版開始封鎖符合下列所有條件的 CloudFront 網頁要求 (以及您可能已新增的任何其他條件)：

- `User-Agent` 標頭的值為 `BadBot`
- (如果您建立並新增 regex 條件) `Body` 的值為任何符合 `I[a@]mAB[a@]dRequest` 模式的四個字串 (four strings)。
- 發出請求的 IP 地址範圍為 192.0.2.0-192.0.2.255
- 您在地理比對條件中選取發出請求的國家/地區
- 請求貌似有包含惡意 SQL 的查詢字串。

AWS WAF 經典 CloudFront 允許響應不滿足所有這三個條件的任何請求。

步驟 10：清理您的資源

現在，您已成功完成教學課程。為了防止您的帳戶累積額外的 AWS WAF 經典費用，您應該清理您建立的 AWS WAF 傳統物件。或者，您可以變更設定，以確實比對要允許、封鎖和計數的 web 請求。

> **Note**
>
> AWS 一般而言，對於您在本教學課程中建立的資源，每天收取的費用不到 USD $0.25。當您完成時，我們建議您刪除資源以免產生不必要的費用。

若要刪除 AWS WAF 傳統收費的物件

1. 取消 Web ACL 與 CloudFront 發行版的關聯：

   a. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

      如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。

   b. 選擇您要刪除的網頁 ACL 名稱。這會開啟右窗格中包含 Web ACL 詳細資訊的頁面。

c. 在右窗格的 [規則] 索引標籤上，移至使用此 Web ACL 的AWS 資源區段。對於與 Web ACL 相關聯的 CloudFront 分佈，請在「類型」欄中選擇 x。

2. 從您的規則移除條件：

   a. 在導覽窗格中，選擇規則。
   b. 選擇在本教學課程中建立的規則。
   c. 選擇編輯規則。
   d. 選擇每個條件標題右邊的 x。
   e. 選擇更新。

3. 從您的 Web ACL 移除規則，以及刪除 Web ACL：

   a. 在導覽窗格中，選擇 Web ACL。
   b. 選擇您在教學課程中建立的 Web ACL 的名稱。這會開啟右窗格中包含 Web ACL 詳細資訊的頁面。
   c. 在規則標籤上，選擇 Edit web ACL (編輯 Web ACL)。
   d. 選擇每個規則標題右邊的 x。
   e. 選擇 Actions (動作)，然後選擇 Delete web ACL (刪除 Web ACL)。

4. 刪除您的規則：

   a. 在導覽窗格中，選擇規則。
   b. 選擇在本教學課程中建立的規則。
   c. 選擇刪除。
   d. 在刪除對話方塊中，再次選擇刪除確認。

AWS WAF Classic 不會收取條件費用，但如果您想要完成清除作業，請執行下列程序，從條件中移除篩選條件並刪除條件。

刪除篩選條件和條件

1. 刪除您的 IP 比對條件的 IP 地址範圍，以及刪除 IP 比對條件：

   a. 在「 AWS WAF 典型」主控台的導覽窗格中，選擇「IP 位址」。
   b. 選擇在本教學課程中建立的 IP 比對條件。
   c. 選取您新增的 IP 地址範圍的核取方塊。
   d. 選擇刪除 IP 地址或範圍。

e. 在 IP match conditions (IP 比對條件) 窗格中，選擇刪除。

f. 在刪除對話方塊中，再次選擇刪除確認。

2. 刪除您的 SQL injection 比對條件的篩選條件，以及刪除 SQL injection 比對條件：

a. 在導覽窗格中，選擇 SQL injection。

b. 選擇在本教學課程中建立的 SQL injection 比對條件。

c. 選取您新增篩的選條件的核取方塊。

d. 選擇刪除篩選條件。

e. 在 SQL injection match conditions (SQL injection 比對條件) 窗格中，選擇刪除。

f. 在刪除對話方塊中，再次選擇刪除確認。

3. 刪除您的字串比對條件的篩選條件，以及刪除字串比對條件：

a. 在導覽窗格中選擇字串和 regex 比對。

b. 選擇在本教學課程中建立的字串比對條件。

c. 選取您新增篩的選條件的核取方塊。

d. 選擇刪除篩選條件。

e. 在 String match conditions (字串比對條件) 窗格中，選擇刪除。

f. 在刪除對話方塊中，再次選擇刪除確認。

4. 如果您有建立的話，請刪除您的 regex 比對條件的篩選條件，以及刪除 regex 比對條件：

a. 在導覽窗格中選擇字串和 regex 比對。

b. 選擇在本教學課程中建立的 regex 比對條件。

c. 選取您新增篩的選條件的核取方塊。

d. 選擇刪除篩選條件。

e. 在 Regex match conditions (Regex 比對條件)窗格中，選擇刪除。

f. 在刪除對話方塊中，再次選擇刪除確認。

5. 刪除您的容量限制條件的篩選條件，以及刪除容量限制條件：

a. 在導覽窗格中，選擇容量限制。

b. 選擇在本教學課程中建立的容量限制條件。

c. 選取您新增篩的選條件的核取方塊。

d. 選擇刪除篩選條件。

e. 在 Size constraint conditions (容量限制條件) 窗格中，選擇刪除。

f. 在刪除對話方塊中，再次選擇刪除確認。

建立和設定 Web 存取控制清單 (Web ACL)

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

Web 存取控制清單 (Web ACL) 可讓您對 Amazon API 閘道 API、Amazon CloudFront 分發或應 Application Load Balancer 回應的 Web 請求進行更精確的控制。您可以允許或封鎖以下類型的請求：

- 源自於 IP 地址或 IP 地址的範圍
- 源自於特定國家/地區
- 包含指定的字串或符合特定請求中的規則運算式 (regex) 模式
- 超過指定的長度
- 似乎含有惡意 SQL 程式碼 (稱為 SQL injection)
- 似乎含有惡意指令碼 (稱為跨網站指令碼)

您葛已操是這些條件的任意組合，封鎖或計數不僅只符合指定條件的 web 請求，還有在任五分鐘內超過指定數量的請求。

若要選擇您想允許的請求，以存取您的內容，或您想要封鎖的內容，請執行以下：

1. 選擇預設的動作，允許或封鎖不符合任何您所指定條件的 web 請求。如需詳細資訊，請參閱 決定 Web ACL 的預設動作。
2. 指定您想要允許或封鎖請求的條件：
   - 若要根據請求是否有含有惡意指令碼，允許或封鎖請求，請建立跨網站指令碼比對條件。如需詳細資訊，請參閱 使用跨網站指令碼比對條件。
   - 若要根據他們源於的 IP 地址，允許或封鎖請求，請建立 IP 比對條件。如需詳細資訊，請參閱 使用 IP 比對條件。

- 若要根據他們源於的國家/地區執行，允許或封鎖請求，請建立地理比對條件。如需詳細資訊，請參閱 使用地理比對條件。
- 若要根據請求是否超過指定的長度，允許或封鎖請求，請建立容量的限制條件。如需詳細資訊，請參閱 使用容量限制條件。
- 若要據請求是否有含有惡意 SQL 碼，允許或封鎖請求，請建立 SQL injection 比對條件。如需詳細資訊，請參閱 使用 SQL Injection 比對條件。
- 若要根據在請求中出現的字串，允許或封鎖請求，請建立字串比對條件。如需詳細資訊，請參閱使用字串比對條件。
- 若要根據在請求中出現的 regex 模式，允許或封鎖請求，請建立 regex 比對條件。如需詳細資訊，請參閱 使用 Regex 比對條件。

3. 將此條件新增至一個或多個規則。如果您在相同規則中新增多個條件，Web 要求必須符合 C AWS WAF lassic 的所有條件，才能根據規則允許或封鎖要求。如需詳細資訊，請參閱 使用規則。或者，您可以使用以速率為基礎的規則來取代一般規則，限制來自任何 IP 地址且符合條件的請求數量。
4. 新增規則至 Web ACL。針對每個規則，指定要讓 C AWS WAF lassic 根據您新增至規則的條件來允許或封鎖要求。如果您將多個規則新增至 Web ACL， AWS WAF 典型會依照規則在 Web ACL 中列出的順序來評估規則。如需詳細資訊，請參閱 使用 Web ACL。

   當您新增新的規則或更新現有的規則，可能需要一分鐘左右讓所做的變更完成，才會出現在您的 Web ACL 和資源。

主題

使用條件

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

指定何時您想要允許或封鎖請求的條件。

- 若要根據請求是否有含有惡意指令碼，允許或封鎖請求，請建立跨網站指令碼比對條件。如需詳細資訊，請參閱 使用跨網站指令碼比對條件。
- 若要根據他們源於的 IP 地址，允許或封鎖請求，請建立 IP 比對條件。如需詳細資訊，請參閱 使用 IP 比對條件。
- 若要根據他們源於的國家/地區執行，允許或封鎖請求，請建立地理比對條件。如需詳細資訊，請參閱 使用地理比對條件。
- 若要根據請求是否超過指定的長度，允許或封鎖請求，請建立容量的限制條件。如需詳細資訊，請參閱 使用容量限制條件。
- 若要據請求是否有含有惡意 SQL 碼，允許或封鎖請求，請建立 SQL injection 比對條件。如需詳細資訊，請參閱 使用 SQL Injection 比對條件。
- 若要根據在請求中出現的字串，允許或封鎖請求，請建立字串比對條件。如需詳細資訊，請參閱 使用字串比對條件。
- 若要根據在請求中出現的 regex 模式，允許或封鎖請求，請建立 regex 比對條件。如需更多詳細資訊，請參閱 使用 Regex 比對條件。

主題

使用跨網站指令碼比對條件

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。

如需的最新版本 AWS WAF，請參閱AWS WAF。

攻擊者有時會將指令碼插入到 web 請求中，利用 web 應用程式的漏洞。您可以建立一或多個跨網站指令碼比對條件，以識別 Web 要求的部分，例如 URI 或查詢字串，您希望 C AWS WAF lassic 檢查可能的惡意指令碼。稍後，當您建立 Web ACL，您需要指定是否要允許或封鎖貌似含有惡意指令碼的請求。

主題

建立跨網站指令碼比對條件

當您建立跨網站指令碼比對條件時，請您指定篩選條件。篩選器會指出您希望 C AWS WAF lassic 檢查惡意指令碼的 Web 要求部分，例如 URI 或查詢字串。您可以將多個篩選條件增至跨網站指令碼比對條件，或您可以為每個篩選條件建立獨立的條件。以下是每個配置如何影響 AWS WAF 傳統行為：

- 每個跨網站指令碼相符條件有多個篩選器 (建議使用) — 當您新增包含多個篩選條件的跨網站指令碼比對條件至規則，並將規則新增至 Web ACL 時，Web 要求必須僅符合 C AWS WAF lassic 跨網站指令碼比對條件中的一個篩選器，才能根據該條件允許或封鎖要求。

  例如，假設您建立一個跨網站指令碼比對條件，此條件含有兩個篩選條件。一個過濾器指示 C AWS WAF lassic 檢查 URI 是否存在惡意腳本，另一個則指示 C AWS WAF lassic 檢查查詢字符串。AWS WAF 如果要求似乎包含在 URI 或查詢字串中的惡意指令碼，Classic 會允許或封鎖要求。
- 每個跨網站指令碼相符條件一個篩選器 — 當您將個別的跨網站指令碼比對條件新增至規則，並將規則新增至 Web ACL 時，Web 要求必須符合 C AWS WAF lassic 的所有條件，才能根據條件允許或封鎖要求。

  假設您建立兩個條件，每個條件含有前述範例中兩個篩選條件中的一個。當您將這兩個條件新增至相同的規則，並將規則新增至 Web ACL 時，只有當 URI 和查詢字串看起來都包含惡意指令碼時，C AWS WAF lassic 才會允許或封鎖要求。

> **Note**
>
> 當您將跨網站指令碼比對條件新增至規則時，您也可以將 C AWS WAF lassic 設定為允許或封鎖看似不包含惡意指令碼的 Web 要求。

建立跨網站指令碼比對條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中，選擇 Cross-site scripting (跨網站訂閱)。
3. 選擇 Create condition (建立條件)。
4. 指定適用的篩選條件設定。如需詳細資訊，請參閱 當您建立或編輯跨網站指令碼比對條件時所指定的值。
5. 選擇 Add another filter (新增其他篩選條件)。
6. 如果您希望新增另一個篩選，重複步驟四和五。
7. 完成新增篩選條件，請選擇建立。

當您建立或編輯跨網站指令碼比對條件時所指定的值

當您建立或更新跨網站指令碼比對條件時，您需指定的以下的值：

名稱

跨網站指令碼比對條件的篩選條件的名稱。

名稱僅能由 A-Z、a-z、0-9 和特殊字元：_-!"#`+*},./ 組成。條件的名稱在建立後無法變更。

要篩選的請求部分是

選擇您希望 C AWS WAF lassic 檢查惡意腳本的每個 Web 請求的部分：

標頭

指定的請求標頭，例如，`User-Agent` 或 `Referer` 標頭。如果您選擇標頭，請在標頭欄位裡指定標頭的名稱。

HTTP 方法

HTTP 方法，指出要求來源執行的作業類型。CloudFront 支援下列方法：DELETEGET、HEAD、OPTIONS、PATCH、POST、和PUT。

查詢字串

出現在？字元後的 URL 部分 (如果有)。

> **Note**
>
> 針對跨網站指令碼比對條件，建議您選擇 [所有查詢參數 (僅限值)]，而不是 [查詢字串] 做為要篩選的部分要求。

URI

請求的 URI 路徑，用於識別資源，例如/images/daily-ad.jpg。這不包括 URI 的查詢字串或片段元件。如需詳細資訊，請參閱統一資源識別元 (URI)：一般語法。

除非指定了轉換，否則 URI 不會被標準化，並且會像從客戶端 AWS 接收它作為請求的一部分一樣進行檢查。Transformation (轉換) 將如指定重新格式化 URI。

Body

部分的請求內容含有您想傳送至您的 web 伺服器做為 HTTP 請求內文的額外資料，您要傳送到您的 Web 伺服器的 HTTP 請求的內文，例如資料表單。

> **Note**
>
> 如果您選擇 [內文] 做為要篩選之要求的部分值， AWS WAF 典型只會檢查前 8192 個位元組 (8 KB)。若要允許或封鎖主體超過 8192 個位元組的要求，您可以建立大小限制條件。（ AWS WAF 經典從請求頭獲取主體的長度。）如需詳細資訊，請參閱 使用容量限制條件。

單一查詢參數 (僅數值)

任何您已定義做為部分查詢字串的參數。例如，如果網址是「www.xyz.com」UserName = ABC& SalesRegion = 西雅圖」，您可以將過濾器添加到或參數中。UserNameSalesRegion

如果您選擇單一查詢參數 (僅數值)，您也可以指定查詢參數名稱。這是您要檢查的查詢字串中的參數，例如UserName或SalesRegion。查詢參數名稱的長度上限為 30 個字元。查詢參數名稱不區分大小寫。例如，您指定UserName為查詢參數名稱，這將匹配的所有變體 UserName，例如用戶名和用戶名。

所有的查詢參數 (僅數值)

類似於單一查詢參數 (僅限值)，而不是檢查單一參數的值，C AWS WAF lassic 會檢查查詢字串中的所有參數值是否存在可能的惡意指令碼。例如，如果網址是「www.xyz.com? UserName =abc& = 西雅圖/ SalesRegion 西雅圖」，並且您選擇「所有查詢參數」(僅限值)，如果其中一個值為或包含可能的惡意指令碼， AWS WAF 傳統就會觸發相符項目。UserNameSalesRegion

標頭

如果您選擇要篩選的部分要求的標頭，請從通用標頭清單中選擇標頭，或輸入您希望 C AWS WAF lassic 檢查是否有惡意指令碼的標頭名稱。

轉換

轉換會在 AWS WAF 傳統檢查要求之前重新格式化 Web 要求。這消除了攻擊者在 Web 請求中使用的一些不尋常的格式，以便繞過 C AWS WAF lassic。

您只能指定一種文字轉換類型。

轉換可執行下列操作：

無

AWS WAF Classic 在檢查 Val ue 中是否有要匹配的字符串之前，不會對 Web 請求執行任何文本轉換。

轉換成小寫

AWS WAF 經典將大寫字母（A-Z）轉換為小寫（a-z）。

HTML 解碼

AWS WAF 經典用未編碼字符替換 HTML 編碼的字符：

- 將 " 換成 &
- 以非中斷空格取代
- 將 < 換成 <
- 將 > 換成 >
- 將表示為十六進位格式的字元 &#xhhhh; 以對應字元取代
- 將表示為十進位格式的字元 &#nnnn; 以對應字元取代

標準化空格

AWS WAF 經典用空格字符（十進制 32）替換以下字符：

- \f、跳頁、小數 12
- \t、標籤、小數 9
- \n、換行，小數 10
- \r、換行、小數 13
- \v、垂直標籤，小數 11
- 非中斷空格，小數 160

此外，此選項將數個空格取代為一個空格。

簡化命令列

對於包含作業系統命令列命令的請求，請使用此選項以執行以下轉換：

- 刪除以下字元：\ " ' ^
- 刪除以下字元前的空格：/ (
- 將以下字元取代為空格：, ;
- 將數個空格取代為一個空格
- 將所有大寫字母 (A-Z) 轉換成小寫 (a-z)

URL 解碼

解碼 URL 編碼請求。

新增和刪除跨網站指令碼比對條件的篩選條件

您可以新增和刪除跨網站指令碼比對條件的篩選條件。若要變更篩選條件、新增新的篩選條件、和刪除舊的篩選條件。

若要新增和刪除跨網站指令碼比對條件的篩選條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中，選擇 Cross-site scripting (跨網站訂閱)。
3. 選擇您想要在條件裡新增或刪除的篩選條件。

4. 若要新增篩選條件，請執行以下步驟：

   a. 選擇新增篩選條件。

   b. 指定適用的篩選條件設定。如需詳細資訊，請參閱 當您建立或編輯跨網站指令碼比對條件時所指定的值。

   c. 選擇新增。

5. 若要刪除篩選條件，請執行以下步驟：

   a. 選取您要刪除的篩選條件。

   b. 選擇刪除篩選條件。

刪除跨網站指令碼比對條件

如果您想要刪除跨網站指令碼比對條件，您必須先刪除該條件內的所有篩選條件，以及從所有使用它的規則中移除，請參閱下列程序。

刪除跨網站指令碼比對條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。

2. 在導覽窗格中，選擇 Cross-site scripting (跨網站訂閱)。

3. 在跨網站指令碼比對條件窗格中，選擇您要刪除的跨網站指令碼比對條件。

4. 在右窗格中，選擇 Associated rules (關聯的規則) 標籤。

   如果使用此跨網站指令碼比對條件規則的名單為空白，請移至步驟六。如果清單有包含任何規則，請記下該規則並繼續步驟五。

5. 若要從使用該跨網站指令碼比對條件的規則中移除該條件，請執行以下步驟：

   a. 在導覽窗格中，選擇規則。

   b. 選擇要刪除使用該跨網站指令碼比對條件的規則名稱。

   c. 在右窗格中，選擇要刪除使用該跨網站指令碼比對條件的規則，然後選擇移除選取的條件。

   d. 對所有剩下要刪除使用該跨網站指令碼比對條件的規則，重複步驟 b 和 c。

   e. 在導覽窗格中，選擇 Cross-site scripting (跨網站訂閱)。

   f. 在跨網站指令碼比對條件窗格中，選擇您要刪除的跨網站指令碼比對條件。

6. 選擇刪除以刪除選取的條件。

使用 IP 比對條件

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

如果您想根據請求源於的 IP 地址，允許或封鎖 web 請求，請建立一個或多個 IP 比對條件。IP 比對條件可列出 10,000 個您的請求源於的 IP 地址或 IP 地址範圍。稍後，當您建立 Web ACL，您需要指定是否要允許或封鎖自這些 IP 地址的請求。

主題

- 建立 IP 比對條件
- 編輯 IP 比對條件
- 刪除 IP 比對條件

建立 IP 比對條件

如果您想根據請求源於的 IP 地址執行允許某些請求、封鎖某些請求的話，請建立您想允許請求 IP 地址的 IP 比對條件，和您想封鎖請求 IP 地址的 IP 比對條件。

> **Note**
>
> 當您將 IP 比對條件新增至規則時，您也可以將「 AWS WAF 典型」設定為允許或封鎖非來自您在條件中指定之 IP 位址的 Web 要求。

建立 IP 比對條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。

2. 在導覽窗格中，選擇 IP 地址。
3. 選擇 Create condition (建立條件)。
4. 在 Name (名稱) 欄位中輸入名稱。

   名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_-!"#`+*},./。條件的名稱在建立後無法變更。
5. 選擇正確的 IP 版本，並使用 CIDR 符號指定 IP 地址或 IP 地址範圍。以下是一些範例：

   - 若要指定 IPv4 地址 192.0.2.44，請輸入 192.0.2.44/32。
   - 若要指定 IPv6 地址 0:0:0:0:0:ffff:c000:22c，請輸入 0:0:0:0:0:ffff:c000:22c/128。
   - 若要指定 IPv4 地址的範圍，從 192.0.2.0 to 192.0.2.255，請輸入 192.0.2.0/24。
   - 若要指定 IPv6 地址的範圍，從 2620:0:2d0:200:0:0:0:0 to 2620:0:2d0:200:ffff:ffff:ffff:ffff，請輸入 2620:0:2d0:200::/64。

   AWS WAF 傳統版支援 IPv4 位址範圍：/8 以及 /16 到 /32 之間的任何範圍。 AWS WAF 傳統版支援 IPv6 位址範圍：/24、/32、48、/56、64 和 如需 CIDR 符號表示法的詳細資訊，請參閱 Wikipedia 項目無類別域間路由。
6. 選擇新增另一個 IP 地址或範圍。
7. 如果您希望新增另一個 IP 地址或範圍，重複步驟五和六。
8. 當您完成新增後，請選擇建立 IP 比對條件。

編輯 IP 比對條件

您可以將 IP 地址範圍新增至 IP 比對條件中，也可刪除範圍。若要變更範圍、新增新的範圍、和刪除舊的範圍。

編輯 IP 比對條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中，選擇 IP 地址。
3. 在 IP 比對條件窗格中，選擇您要編輯的 IP 比對條件。
4. 若要新增 IP 地址或範圍：

a. 在右窗格中，選擇新增 IP 地址或範圍。

b. 選擇正確的 IP 版本，並使用 CIDR 符號輸入 IP 地址。以下是一些範例：

- 若要指定 IPv4 地址 192.0.2.44，請輸入 192.0.2.44/32。
- 若要指定 IPv6 地址 0:0:0:0:0:ffff:c000:22c，請輸入 0:0:0:0:0:ffff:c000:22c/128。
- 若要指定 IPv4 地址的範圍，從 192.0.2.0 to 192.0.2.255，請輸入 192.0.2.0/24。
- 若要指定 IPv6 地址的範圍，從 2620:0:2d0:200:0:0:0:0 to 2620:0:2d0:200:ffff:ffff:ffff:ffff，請輸入 2620:0:2d0:200::/64。

AWS WAF 傳統版支援 IPv4 位址範圍：/8 以及 /16 到 /32 之間的任何範圍。 AWS WAF 傳統版支援 IPv6 位址範圍：/24、/32、48、/56、64 和 如需 CIDR 符號表示法的詳細資訊，請參閱 Wikipedia 項目無類別域間路由。

c. 若要新增更多 IP 地址，請選擇 Add another IP address (新增另一個 IP 地址) 並輸入值。

d. 選擇新增。

5. 若要刪除 IP 地址或範圍：

a. 在右窗格中，選取要刪除的數值。

b. 選擇刪除 IP 地址或範圍。

刪除 IP 比對條件

如果您想要刪除 IP 比對條件，您必須先刪除該條件內的所有 IP 地址和範圍，以及從所有使用它的規則中移除，請參閱下列程序。

刪除 IP 比對條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。

2. 在導覽窗格中，選擇 IP 地址。
3. 在 IP 比對條件窗格中，選擇您要刪除的 IP 比對條件。
4. 在右窗格中，選擇規則標籤。

如果使用此 IP 比對條件規則的名單為空白，請移至步驟六。如果清單有包含任何規則，請記下該規則並繼續步驟五。

5. 若要從使用該 IP 比對條件的規則中移除該條件，請執行以下步驟：

   a. 在導覽窗格中，選擇規則。

   b. 選擇要刪除使用該 IP 比對條件的規則名稱。

   c. 在右窗格中，選擇要刪除 IP 比對條件的規則，然後選擇移除選取的條件。

   d. 對所有剩下要刪除使用該 IP 比對條件的規則，重複步驟 b 和 c。

   e. 在導覽窗格中，選擇 IP 比對條件。

   f. 在 IP 比對條件窗格中，選擇您要刪除的 IP 比對條件。

6. 選擇刪除以刪除選取的條件。

使用地理比對條件

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

如果您想根據請求源於的國家/地區，允許或封鎖 web 請求，請建立一個或多個地理比對條件。地理比對條件列出的國家/地區為您請求的發源地。稍後，當您建立 Web ACL，您需要指定是否要允許或封來自這些國家/地區的請求。

您可以將地理比對條件與其他 AWS WAF 傳統條件或規則搭配使用，以建立複雜的篩選。例如，如果您想要封鎖特定國家/地區，但仍想允許該國家/地區的特定 IP 地址，您可以建立地理比對條件和 IP 比對條件，將這兩個一起增至一項規則中。設定規則以封鎖來自該國家/地區的請求，和未受核准的 IP 地址。舉另一個例子，如果您想未特定國家/地區的使用者劃分資源優先使用順序，您可以在兩個不同以速率為基礎的規則中，放入相同的地理比對條件。為慣用的國家/地區的使用者這定高速率限制，對其他國家/地區的使用者設定低的速率限制。

> **Note**
>
> 如果您使用 CloudFront 地理位置限制功能來阻止某個國家/地區訪問您的內容，則該國家/地區的任何請求都會被阻止，並且不會轉發到 C AWS WAF lassic。因此，如果您想要根據地理位置和其他 AWS WAF 傳統條件來允許或封鎖要求，則不應使用地 CloudFront 理位置限制功能。相反，您應該使用 AWS WAF 傳統地理匹配條件。

主題

建立地理比對條件

如果您想根據請求源於的國家/地區執行允許某些請求、封鎖某些請求的話，請建立您想允許請求國家/地區的地理比對條件，和您想封鎖請求國家/地區的地理比對條件。

> **Note**
>
> 當您將地理區域比對條件新增至規則時，也可以將「 AWS WAF 典型」設定為允許或封鎖非來自您在條件中指定的國家/地區的 Web 要求。

建立地理比對條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中，選擇地理比對。
3. 選擇 Create condition (建立條件)。
4. 在 Name (名稱) 欄位中輸入名稱。

   名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_-!"#`+*},./。條件的名稱在建立後無法變更。
5. 選擇一個區域。

6. 選擇位置類型和國家/地區。Location type (位置類型) 目前只能是 Country (國家/地區)。
7. 選擇新增位置。
8. 選擇建立。

編輯地理比對條件

您可以從地理比對條件新增或刪除國家/地區。

編輯地理比對條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中，選擇地理比對。
3. 在地理比對條件窗格中，選擇您要編輯的地理比對條件。
4. 新增國家/地區：
   a. 在右窗格中選擇新增篩選條件。
   b. 選擇位置類型和國家/地區。Location type (位置類型) 目前只能是 Country (國家/地區)。
   c. 選擇新增。
5. 若要刪除國家/地區：
   a. 在右窗格中，選取要刪除的數值。
   b. 選擇刪除篩選條件。

刪除地理比對條件

如果您想要刪除地理比對條件，您必須先移除該條件內的所有國家/地區，以及從所有使用它的規則中移除，請參閱下列程序。

刪除地理比對條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。

2. 從使用該地理比對條件的規則中移除該條件：

   a. 在導覽窗格中，選擇規則。

   b. 選擇要刪除使用該地理比對條件的規則名稱。

   c. 在右窗格中選擇編輯規則。

   d. 在您要刪除的條件旁，選擇 X。

   e. 選擇更新。

   f. 對所有剩下要刪除使用該地理比對條件的規則，重複步驟。

3. 從您想刪除的條件移除篩選條件：

   a. 在導覽窗格中，選擇地理比對。

   b. 選擇您要刪除的地理比對條件名稱。

   c. 在右窗格中，選擇篩選條件旁的核取方塊，以選取所有篩選條件。

   d. 選擇刪除篩選條件。

4. 在導覽窗格中，選擇地理比對。

5. 在地理比對條件窗格中，選擇您要刪除的地理比對條件。

6. 選擇刪除以刪除選取的條件。

使用容量限制條件

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

如果您想根據指定部分請求的長度，允許或封鎖 web 請求，請建立容量限制條件。大小限制條件可識別您希望 C AWS WAF lassic 查看的 Web 請求的部分，您希望 C AWS WAF lassic 查找的字節數以及運算符，例如大於（>）或小於（<）。例如，您可以使用容量限制條件，以尋找超過 100 位元組的查詢字串。稍後，當您建立 Web ACL，您需要指定是否要根據這些設定允許或封鎖請求。

請注意，如果您將 C AWS WAF lassic 設定為檢查要求主體，例如透過搜尋指定字串的內文，C AWS WAF lassic 只會檢查前 8192 個位元組 (8 KB)。如果您的 Web 請求的請求主體永遠不會超過 8192 個位元組，您可以建立容量限制條件，封鎖大於 8192 位元組的請求。

主題

建立容量限制條件

當您建立大小限制條件時，您可以指定篩選器，以識別您希望 C AWS WAF lassic 評估長度的 Web 請求部分。您可以將多個篩選條件增至容量限制條件，或您可以為每個篩選條件建立獨立的條件。以下是每個配置如何影響 AWS WAF 傳統行為：

- 每個大小限制條件一個篩選器 — 當您將個別的大小限制條件新增至規則，並將規則新增至 Web ACL 時，Web 請求必須符合 C AWS WAF lassic 的所有條件，才能根據條件允許或封鎖請求。

  例如，假設您建立兩個條件。一個符合 web 請求查詢字串大於 100 位元組。另一個符合 web 請求內文大於 1024 位元組。當您將這兩個條件新增至相同的規則，並將規則新增至 Web ACL 時，只有在兩個條件都成立時， AWS WAF 傳統才會允許或封鎖要求。
- 每個大小限制條件有多個篩選器 — 當您將包含多個篩選條件的大小限制條件新增至規則，並將規則新增至 Web ACL 時，Web 請求只需要符合 C AWS WAF lassic 大小限制條件中的其中一個篩選器，即可根據該條件允許或封鎖要求。

  假設您建立一個條件而不是兩個條件，而一個條件包含與前面範例中相同的兩個篩選器。 AWS WAF 如果查詢字串大於 100 個位元組或要求主體大於 1024 個位元組，則傳統會允許或封鎖要求。

> **Note**
>
> 當您將大小限制條件新增至規則時，您也可以將「 AWS WAF 典型」設定為允許或封鎖與條件中值不符的 Web 要求。

建立容量限制條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中，選擇容量限制。
3. 選擇 Create condition (建立條件)。
4. 指定適用的篩選條件設定。如需詳細資訊，請參閱 在您建立或編輯容量限制條件時所指定的值。
5. 選擇 Add another filter (新增其他篩選條件)。
6. 如果您希望新增另一個篩選，重複步驟四和五。
7. 當您完成新增篩選條件後，請選擇建立容量限制條件。

在您建立或編輯容量限制條件時所指定的值

在建立或更新容量限制條件時，請指定以下的值：

名稱

輸入容量限制條件的名稱。

名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_-!"#`+*},./。條件的名稱在建立後無法變更。

要篩選的請求部分是

選擇您希望 C AWS WAF lassic 評估長度的每個 Web 請求的部分：

標頭

指定的請求標頭，例如，`User-Agent` 或 `Referer` 標頭。如果您選擇標頭，請在標頭欄位裡指定標頭的名稱。

HTTP 方法

HTTP 方法，指出要求來源執行的作業類型。CloudFront 支援下列方法：`DELETEGET`、`HEAD`、`OPTIONS`、`PATCH`、`POST`、和`PUT`。

查詢字串

出現在 ? 字元後的 URL 部分 (如果有)。

URI

請求的 URI 路徑，用於識別資源，例如/images/daily-ad.jpg。這不包括 URI 的查詢字串或片段元件。如需詳細資訊，請參閱統一資源識別元 (URI)：一般語法。

除非指定了轉換，否則 URI 不會被標準化，並且會像從客戶端 AWS 接收它作為請求的一部分一樣進行檢查。Transformation (轉換) 將如指定重新格式化 URI。

Body

部分的請求內容含有您想傳送至您的 web 伺服器做為 HTTP 請求內文的額外資料，您要傳送到您的 Web 伺服器的 HTTP 請求的內文，例如資料表單。

單一查詢參數 (僅數值)

任何您已定義做為部分查詢字串的參數。例如，如果網址是「www.xyz.com」UserName = ABC& SalesRegion = 西雅圖」，您可以將過濾器添加到或參數中。UserNameSalesRegion

如果您選擇單一查詢參數 (僅數值)，您也可以指定查詢參數名稱。這是您要檢查的查詢字串中的參數，例如UserName。查詢參數名稱的長度上限為 30 個字元。查詢參數名稱 不區分大小寫。例如，您指定UserName為查詢參數名稱，這將匹配的所有變體 UserName，例如用戶名和用戶名。

所有的查詢參數 (僅數值)

類似於 S ingle 查詢參數 (僅限值)，而不是檢查單一參數的值，C AWS WAF lassic 會檢查查詢字串中所有參數的值是否有大小限制。例如，如果網址是「www.xyz.com? UserName =abc& = SalesRegion 西雅圖」，並且您選擇「所有查詢參數」(僅限值)，「 AWS WAF 傳統」會在任一或超過指定大小時觸發符合的值。UserNameSalesRegion

標頭 (只有當「部分請求的篩選條件」為「標頭」時)

如果您選擇要篩選之要求部分的標頭，請從通用標頭清單中選擇標頭，或輸入您希望 C AWS WAF lassic 評估長度的標頭名稱。

比較運算子

選擇您希望 C AWS WAF lassic 如何根據您為 Size 指定的值，評估 Web 請求中查詢字串的長度。

例如，如果您針對「比較」運算子選擇「大於」，並在「大小」中輸入 100，則 C AWS WAF lassic 會針對長度超過 100 個位元組的查詢字串評估 Web 要求。

大小

輸入您希望 C AWS WAF lassic 在查詢字串中監視的長度 (以位元組為單位)。

> **Note**
>
> 如果您選擇 URI 為 部分請求的值來篩選，則會視 URI 的 / 為一個字元。例如，URI 路徑長度/logo.jpg為九個字元。

轉換

轉換會在 C AWS WAF lassic 評估請求的指定部分長度之前重新格式化 Web 請求。這消除了攻擊者在 Web 請求中使用的一些不尋常的格式，以便繞過 C AWS WAF lassic。

> **Note**
>
> 如果您選擇 [本文] 做為要篩選的要求的部分，則無法設定 [傳 AWS WAF 統] 執行轉換，因為只會轉送前 8192 個位元組進行檢查。不過，您仍然可以根據 HTTP 要求主體的大小篩選流量，並指定「無」 轉換。（AWS WAF 經典從請求頭獲取主體的長度。）

您只能指定一種文字轉換類型。

轉換可執行下列操作：

無

AWS WAF 在檢查長度之前，Classic 不會對 Web 請求執行任何文本轉換。

轉換成小寫

AWS WAF 經典將大寫字母（A-Z）轉換為小寫（a-z）。

HTML 解碼

AWS WAF 經典用未編碼字符替換 HTML 編碼的字符：

- 將 " 換成 &
- 以非中斷空格取代
- 將 < 換成 <
- 將 > 換成 >
- 將表示為十六進位格式的字元 &#xhhhh; 以對應字元取代
- 將表示為十進位格式的字元 &#nnnn; 以對應字元取代

標準化空格

AWS WAF 經典用空格字符（十進制 32）替換以下字符：

- \f、跳頁、小數 12
- \t、標籤、小數 9
- \n、換行，小數 10
- \r、換行、小數 13
- \v、垂直標籤，小數 11
- 非中斷空格，小數 160

此外，此選項將數個空格取代為一個空格。

簡化命令列

對於包含作業系統命令列命令的請求，請使用此選項以執行以下轉換：

- 刪除以下字元：\ " ' ^
- 刪除以下字元前的空格：/ (
- 將以下字元取代為空格：, ;
- 將數個空格取代為一個空格
- 將所有大寫字母 (A-Z) 轉換成小寫 (a-z)

URL 解碼

解碼 URL 編碼請求。

新增和刪除容量限制條件的篩選條件

您可以新增和刪除容量限制條件的篩選條件。若要變更篩選條件、新增新的篩選條件、和刪除舊的篩選條件。

新增和刪除容量限制條件的篩選條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中，選擇容量限制。
3. 選擇您想要在條件裡新增或刪除的篩選條件。

4. 若要新增篩選條件，請執行以下步驟：

   a. 選擇新增篩選條件。

   b. 指定適用的篩選條件設定。如需詳細資訊，請參閱 在您建立或編輯容量限制條件時所指定的值。

   c. 選擇新增。

5. 若要刪除篩選條件，請執行以下步驟：

   a. 選取您要刪除的篩選條件。

   b. 選擇刪除篩選條件。

刪除容量限制條件

如果您想要刪除容量限制條件，您需要先刪除該條件內的所有篩選條件，以及從所有使用它的規則中移除，請參閱下列程序。

刪除容量限制條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。

2. 在導覽窗格中，選擇容量限制。

3. 在容量限制條件窗格中，選擇您要刪除的容量限制條件。

4. 在右窗格中，選擇 Associated rules (關聯的規則) 標籤。

   如果使用此容量限制條件規則的名單為空白，請移至步驟六。如果清單有包含任何規則，請記下該規則並繼續步驟五。

5. 若要從使用該容量限制條件的規則中移除該條件，請執行以下步驟：

   a. 在導覽窗格中，選擇規則。

   b. 選擇要刪除使用該容量限制條件的規則名稱。

   c. 在右窗格中，選擇要刪除使用該容量限制條件的規則，然後選擇移除選取的條件。

   d. 對所有剩下要刪除使用該容量限制條件的規則，重複步驟 b 和 c。

   e. 在導覽窗格中，選擇容量限制。

   f. 在容量限制條件窗格中，選擇您要刪除的容量限制條件。

6. 選擇刪除以刪除選取的條件。

使用 SQL Injection 比對條件

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

攻擊者有時插入惡意 SQL 程式碼到 web 請求中，以從您的資料庫擷取資料。若要根據請求是否有含有惡意 SQL 碼，允許或封鎖 web 請求，請建立一個或多個 SQL injection 比對條件。SQL 注入匹配條件標識 Web 請求的部分，例如 URI 路徑或查詢字符串，您希望 AWS WAF 經典檢查。稍後，當您建立 Web ACL，您需要指定是否要允許或封鎖貌似含有惡意 SQL 程式碼的請求。

主題

- 使用 SQL Injection 比對條件
- 在您建立或編輯 SQL Injection 比對條件時所指定的值
- 新增和刪除 SQL Injection 比對條件的篩選條件
- 刪除 SQL Injection 比對條件

使用 SQL Injection 比對條件

當您建立 SQL 插入相符條件時，您可以指定篩選器，這些篩選器會指出您希望 C AWS WAF lassic 檢查是否有惡意 SQL 程式碼的 Web 要求部分，例如 URI 或查詢字串。您可以將多個篩選條件增至 SQL injection 比對條件，或您可以為每個篩選條件建立獨立的條件。以下是每個配置如何影響 AWS WAF 傳統行為：

- 每個 SQL 插入相符條件有多個篩選器 (建議使用) — 當您將包含多個篩選的 SQL 插入相符條件新增至規則，並將規則新增至 Web ACL 時，Web 要求只需要符合 AWS WAF 傳統 SQL 插入比對條件中的其中一個篩選器，即可根據該條件允許或封鎖要求。

  例如，假設您建立一個SQL injection 比對條件，此條件含有兩個篩選條件。一個過濾器指示 AWS WAF 經典檢查 URI 是否存在惡意 SQL 代碼，另一個則指示 AWS WAF 經典檢查查詢字符串。AWS WAF 如果要求似乎包含在 URI 或查詢字串中的惡意 SQL 程式碼，則傳統會允許或封鎖要求。

- 每個 SQL 插入相符條件都有一個篩選器 — 當您將個別的 SQL 插入相符條件新增至規則，並將規則新增至 Web ACL 時，Web 要求必須符合「 AWS WAF 典型」的所有條件，才能根據條件允許或封鎖要求。

  假設您建立兩個條件，每個條件含有前述範例中兩個篩選條件中的一個。當您將這兩個條件新增至相同的規則，並將規則新增至 Web ACL 時，只有當 URI 和查詢字串看起來都包含惡意 SQL 程式碼時， AWS WAF 傳統才會允許或封鎖要求。

> **Note**
>
> 當您將 SQL 插入相符條件新增至規則時，您也可以將「 AWS WAF 典型」設定為允許或封鎖看似不包含惡意 SQL 程式碼的 Web 要求。

建立 SQL Injection 比對條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中，選擇 SQL injection。
3. 選擇 Create condition (建立條件)。
4. 指定適用的篩選條件設定。如需詳細資訊，請參閱 在您建立或編輯 SQL Injection 比對條件時所指定的值。
5. 選擇 Add another filter (新增其他篩選條件)。
6. 如果您希望新增另一個篩選，重複步驟四和五。
7. 完成篩選條件，請選擇建立。

在您建立或編輯 SQL Injection 比對條件時所指定的值

在建立或更新 SQL Injection 比對條件時，請指定以下的值：

名稱

SQL Injection 比對條件的名稱。

名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_-!"#`+*},./。條件的名稱在建立後無法變更。

要篩選的請求部分是

選擇您希望 C AWS WAF lassic 檢查惡意 SQL 代碼的每個 Web 請求的部分：

標頭

指定的請求標頭，例如，`User-Agent` 或 `Referer` 標頭。如果您選擇標頭，請在標頭欄位裡指定標頭的名稱。

HTTP 方法

HTTP 方法，指出要求來源執行的作業類型。CloudFront 支援下列方法：`DELETEGET`、`HEAD`、`OPTIONS`、`PATCH`、`POST`、和`PUT`。

查詢字串

出現在 ? 字元後的 URL 部分 (如果有)。

> **Note**
>
> 對於 SQL 注入匹配條件，我們建議您選擇所有查詢參數（僅限值），而不是查詢字符串為部分請求進行篩選。

URI

請求的 URI 路徑，用於識別資源，例如`/images/daily-ad.jpg`。這不包括 URI 的查詢字串或片段元件。如需詳細資訊，請參閱統一資源識別元 (URI)：一般語法。

除非指定了轉換，否則 URI 不會被標準化，並且會像從客戶端 AWS 接收它作為請求的一部分一樣進行檢查。Transformation (轉換) 將如指定重新格式化 URI。

Body

部分的請求內容含有您想傳送至您的 web 伺服器做為 HTTP 請求內文的額外資料，您要傳送到您的 Web 伺服器的 HTTP 請求的內文，例如資料表單。

> **Note**
>
> 如果您選擇 [內文] 做為要篩選之要求的部分值， AWS WAF 典型只會檢查前 8192 個位元組 (8 KB)。若要允許或封鎖主體超過 8192 個位元組的要求，您可以建立大小限制條

件。（AWS WAF 經典從請求頭獲取主體的長度。）如需詳細資訊，請參閱 使用容量限制條件。

單一查詢參數 (僅數值)

任何您已定義做為部分查詢字串的參數。例如，如果網址是「www.xyz.com」UserName = ABC& SalesRegion = 西雅圖」，您可以將過濾器添加到或參數中。UserNameSalesRegion

如果您選擇單一查詢參數 (僅數值)，您也可以指定查詢參數名稱。這是您要檢查的查詢字串中的參數，例如UserName或SalesRegion。查詢參數名稱的長度上限為 30 個字元。查詢參數名稱不區分大小寫。例如，您指定UserName為查詢參數名稱，這將匹配的所有變體 UserName，例如用戶名和用戶名。

所有的查詢參數 (僅數值)

類似於單一查詢參數 (僅限值)，但不是檢查單一參數的值，C AWS WAF lassic 會檢查查詢字串中所有參數的值，找出可能的惡意 SQL 程式碼。例如，如果網址是「www.xyz.com? UserName =abc& = SalesRegion 西雅圖」，而您選擇「所有查詢參數 (僅限值)」，如果其中一個值或UserName包含可能的惡意 SQL 程式碼， AWS WAF 傳統就會觸發相符項目。SalesRegion

標頭

如果您選擇要篩選的部分要求的標頭，請從通用標頭清單中選擇標頭，或輸入您希望 C AWS WAF lassic 檢查惡意 SQL 程式碼的標頭名稱。

轉換

轉換會在 AWS WAF 傳統檢查要求之前重新格式化 Web 要求。這消除了攻擊者在 Web 請求中使用的一些不尋常的格式，以便繞過 C AWS WAF lassic。

您只能指定一種文字轉換類型。

轉換可執行下列操作：

無

AWS WAF Classic 在檢查 Val ue 中是否有要匹配的字符串之前，不會對 Web 請求執行任何文本轉換。

轉換成小寫

AWS WAF 經典將大寫字母（A-Z）轉換為小寫（a-z）。

HTML 解碼

AWS WAF 經典用未編碼字符替換 HTML 編碼的字符：

- 將 " 換成 &
- 以非中斷空格取代
- 將 < 換成 <
- 將 > 換成 >
- 將表示為十六進位格式的字元 &#xhhhh; 以對應字元取代
- 將表示為十進位格式的字元 &#nnnn; 以對應字元取代

標準化空格

AWS WAF 經典用空格字符（十進制 32）替換以下字符：

- \f、跳頁、小數 12
- \t、標籤、小數 9
- \n、換行，小數 10
- \r、換行、小數 13
- \v、垂直標籤，小數 11
- 非中斷空格，小數 160

此外，此選項將數個空格取代為一個空格。

簡化命令列

對於包含作業系統命令列命令的請求，請使用此選項以執行以下轉換：

- 刪除以下字元：\ " ' ^
- 刪除以下字元前的空格：/ (
- 將以下字元取代為空格：, ;
- 將數個空格取代為一個空格
- 將所有大寫字母 (A-Z) 轉換成小寫 (a-z)

URL 解碼

解碼 URL 編碼請求。

新增和刪除 SQL Injection 比對條件的篩選條件

您可以新增和刪除 SQL Injection 比對條件的篩選條件。若要變更篩選條件、新增新的篩選條件、和刪除舊的篩選條件。

新增和刪除 SQL Injection 比對條件的篩選條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中，選擇 SQL injection。
3. 選擇您想要在條件裡新增或刪除的篩選條件。
4. 若要新增篩選條件，請執行以下步驟：

   a. 選擇新增篩選條件。
   b. 指定適用的篩選條件設定。如需詳細資訊，請參閱 在您建立或編輯 SQL Injection 比對條件時所指定的值。
   c. 選擇新增。
5. 若要刪除篩選條件，請執行以下步驟：

   a. 選取您要刪除的篩選條件。
   b. 選擇刪除篩選條件。

刪除 SQL Injection 比對條件

如果您想要刪除 SQL Injection 比對條件，您需要先刪除該條件內的所有篩選條件，以及從所有使用它的規則中移除，請參閱下列程序。

刪除 SQL Injection 比對條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中，選擇 SQL injection。
3. 在 SQL Injection 比對條件窗格中，選擇您要刪除的 SQL Injection 比對條件。
4. 在右窗格中，選擇 Associated rules (關聯的規則) 標籤。

如果使用此 SQL Injection 比對條件規則的名單為空白，請移至步驟六。如果清單有包含任何規則，請記下該規則並繼續步驟五。

5. 若要從使用該 SQL Injection 比對條件的規則中移除該條件，請執行以下步驟：

   a. 在導覽窗格中，選擇規則。

   b. 選擇要刪除使用該 SQL Injection 比對條件的規則名稱。

   c. 在右窗格中，選擇要刪除 SQL Injection 比對條件的規則，然後選擇移除選取的條件。

   d. 對所有剩下要刪除使用該 SQL Injection 比對條件的規則，重複步驟 b 和 c。

   e. 在導覽窗格中，選擇 SQL injection。

   f. 在 SQL Injection 比對條件窗格中，選擇您要刪除的 SQL Injection 比對條件。

6. 選擇刪除以刪除選取的條件。

使用字串比對條件

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

如果您想根據請求裡出現的字串，允許或封鎖 web 請求，請建立一個或多個字串比對條件。字串比對條件會識別您要搜尋的字串，以及您希望 C AWS WAF lassic 檢查字串的 Web 要求部分，例如指定的標頭或查詢字串。稍後，當您建立 Web ACL，您需要指定是否要允許或封鎖含有這些字串的請求。

主題

- 建立字串比對條件
- 在您建立或編輯字串比對條件時所指定的值
- 新增和刪除字串比對條件的篩選條件
- 刪除字串比對條件

建立字串比對條件

當您建立字串比對條件時，您可以指定篩選器，以識別您要搜尋的字串，以及您希望 C AWS WAF lassic 檢查該字串的 Web 要求部分，例如 URI 或查詢字串。您可以將多個篩選條件增至字串比對條件，或您可以為每個篩選條件建立獨立的條件。以下是每個配置如何影響 AWS WAF 傳統行為：

- 每個字串符合條件一個篩選器 — 當您將個別字串符合條件新增至規則，並將規則新增至 Web ACL 時，Web 要求必須符合 C AWS WAF lassic 的所有條件，才能根據條件允許或封鎖要求。

  例如，假設您建立兩個條件。一個符合 web 請求，還有 `User-Agent` 標頭的 `BadBot` 值。另一個符合 web 請求，含有查詢字串的 `BadParameter` 值。當您將這兩個條件新增至相同的規則，並將規則新增至 Web ACL 時， AWS WAF 傳統只會在這兩個條件包含兩個值時才允許或封鎖要求。
- 每個字串符合條件有多個篩選器 — 當您將包含多個篩選的字串比對條件新增至規則，並將規則新增至 Web ACL 時，Web 請求只需要符合 C AWS WAF lassic 字串比對條件中的其中一個篩選器，即可根據一個條件允許或封鎖要求。

  假設您建立一個條件而不是兩個條件，而一個條件包含與前面範例中相同的兩個篩選器。AWS WAF 傳統允許或阻止請求，如果它們包含*`BadBot`*在*`User-Agent`*標題或查詢字符串*`BadParameter`*中。

> **Note**
>
> 當您將字串比對條件新增至規則時，您也可以將「 AWS WAF 典型」設定為允許或封鎖與條件中值不符的 Web 要求。

建立字串比對條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中選擇字串和 regex 比對。
3. 選擇 Create condition (建立條件)。
4. 指定適用的篩選條件設定。如需詳細資訊，請參閱 在您建立或編輯字串比對條件時所指定的值。
5. 選擇新增篩選條件。
6. 如果您希望新增另一個篩選，重複步驟四和五。

7. 完成篩選條件，請選擇建立。

在您建立或編輯字串比對條件時所指定的值

在建立或更新字串比對條件時，請指定以下的值：

名稱

輸入字串比對條件的名稱。名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_-!"#`+*},./。條件的名稱在建立後無法變更。

Type

選擇 String match (字串比對)。

要篩選的請求部分是

選擇您希望 C AWS WAF lassic 檢查您在值中指定要匹配的字符串的每個 Web 請求的部分：

標頭

指定的請求標頭，例如，`User-Agent` 或 `Referer` 標頭。如果您選擇標頭，請在標頭欄位裡指定標頭的名稱。

HTTP 方法

HTTP 方法，指出要求來源執行的作業類型。CloudFront 支援下列方法：`DELETEGET`、`HEAD`、`OPTIONS`、`PATCH`、`POST`、和`PUT`。

查詢字串

出現在 ? 字元後的 URL 部分 (如果有)。

URI

請求的 URI 路徑，用於識別資源，例如`/images/daily-ad.jpg`。這不包括 URI 的查詢字串或片段元件。如需詳細資訊，請參閱統一資源識別元 (URI)：一般語法。

除非指定了轉換，否則 URI 不會被標準化，並且會像從客戶端 AWS 接收它作為請求的一部分一樣進行檢查。Transformation (轉換) 將如指定重新格式化 URI。

Body

部分的請求內容含有您想傳送至您的 web 伺服器做為 HTTP 請求內文的額外資料，您要傳送到您的 Web 伺服器的 HTTP 請求的內文，例如資料表單。

> **Note**
>
> 如果您選擇 [內文] 做為要篩選之要求的部分值， AWS WAF 典型只會檢查前 8192 個位元組 (8 KB)。若要允許或封鎖主體超過 8192 個位元組的要求，您可以建立大小限制條件。（ AWS WAF 經典從請求頭獲取主體的長度。）如需詳細資訊，請參閱 使用容量限制條件。

單一查詢參數 (僅數值)

任何您已定義做為部分查詢字串的參數。例如，如果網址是「www.xyz.com」UserName = ABC& SalesRegion = 西雅圖」，您可以將過濾器添加到或參數中。UserNameSalesRegion

如果重複的參數顯示在查詢字串上，則數值評估則為「OR」。也就是說，將會觸發符合的值。例如，在網址「www.xyz.com? SalesRegion =boston& = SalesRegion 西雅圖」中，「要匹配的值」中的「波士頓」或「西雅圖」都會觸發匹配。

如果您選擇單一查詢參數 (僅數值)，您也可以指定查詢參數名稱。這是您要檢查的查詢字串中的參數，例如UserName或SalesRegion。查詢參數名稱的長度上限為 30 個字元。查詢參數名稱不區分大小寫。例如，您指定UserName為查詢參數名稱，這將匹配的所有變體 UserName，例如用戶名和用戶名。

所有的查詢參數 (僅數值)

類似於單一查詢參數 (僅限值)，而不是檢查單一參數的值，C AWS WAF lassic 會檢查查詢字串中所有參數的值是否符合「值」。例如，如果網址是「www.xyz.com? UserName =abc& = 西雅圖/ SalesRegion 西雅圖」，而您選擇「所有查詢參數」(僅限值)，如果將UserName或的值指定為要比對的值，則 AWS WAF 傳統將觸發相符項SalesRegion目。

標頭 (只有當「部分請求的篩選條件」為「標頭」時)

如果您從要篩選清單的要求部分中選擇 [標頭]，請從通用標頭清單中選擇標頭，或輸入您希望 C AWS WAF lassic 檢查的標頭名稱。

符合類型

在您希望 C AWS WAF lassic 檢查的請求部分中，選擇要匹配的值中的字符串必須顯示以匹配此過濾器的位置：

包含

該字串出現在指定請求部分中的任何位置。

包含的字

指定的請求部分必須包含符合值，且符合值必須只能含有字母數字字元或底線 (A-Z, a-z, 0-9, or _)。此外，符合值必須為字，表示以下其中一項：

- 符合值完全符合指定的值，例如 web 請求部分的標頭的值。
- 符合值為指定的 Web 請求部分的開始，後面接的字元為一個字母數字字元或底線 (_)，例如 BadBot;。
- 符合值為指定的 Web 請求部分的結尾，前面接的字元為一個字母數字字元或底線 (_)，例如;BadBot。
- 符合值為指定的 Web 請求部分的中間，前後面接的字元為字母數字字元或底線 (_)，例如-BadBot;。

完全符合

字串和指定的請求部分，值為相同的。

開頭為

該字串出現在指定請求部分中的起始位置。

結尾為

該字串出現在指定請求部分中的結束位置。

轉換

轉換會在 AWS WAF 傳統檢查要求之前重新格式化 Web 要求。這消除了攻擊者在 Web 請求中使用的一些不尋常的格式，以便繞過 C AWS WAF lassic。

您只能指定一種文字轉換類型。

轉換可執行下列操作：

無

AWS WAF Classic 在檢查 Val ue 中是否有要匹配的字符串之前，不會對 Web 請求執行任何文本轉換。

轉換成小寫

AWS WAF 經典將大寫字母（A-Z）轉換為小寫（a-z）。

HTML 解碼

AWS WAF 經典用未編碼字符替換 HTML 編碼的字符：

- 將 " 換成 &
- 以非中斷空格取代
- 將 < 換成 <
- 將 > 換成 >
- 將表示為十六進位格式的字元 &#xhhhh; 以對應字元取代
- 將表示為十進位格式的字元 &#nnnn; 以對應字元取代

標準化空格

AWS WAF 經典用空格字符（十進制 32）替換以下字符：

- \f、跳頁、小數 12
- \t、標籤、小數 9
- \n、換行，小數 10
- \r、換行、小數 13
- \v、垂直標籤，小數 11
- 非中斷空格，小數 160

此外，此選項將數個空格取代為一個空格。

簡化命令列

若您將擔心攻擊者插入作業命令列命令，或使用不尋常的格式偽裝某些或所有命令，請使用此選項執行下列轉換：

- 刪除以下字元：\ " ' ^
- 刪除以下字元前的空格：/ (
- 將以下字元取代為空格：, ;
- 將數個空格取代為一個空格
- 將所有大寫字母 (A-Z) 轉換成小寫 (a-z)

URL 解碼

解碼 URL 編碼請求。

base64 編碼值

如果符合值的值是 base64 編碼，請選取此核取方塊。使用 base64 編碼指定攻擊者在其請求中使用的無法列印字元，例如標籤和換行。

符合值

指定您希望 AWS WAF 傳統版在 Web 請求中搜尋的值。長度上限為 50 個位元組。如果您使用 base64 編碼此數值，50 個位元組的長度上限適用於之前編碼的值。

新增和刪除字串比對條件的篩選條件

您可以新增和刪除字串比對條件的篩選條件。若要變更篩選條件、新增新的篩選條件、和刪除舊的篩選條件。

新增和刪除字串比對條件的篩選條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中選擇字串和 regex 比對。
3. 選擇您想要在條件裡新增或刪除的篩選條件。
4. 若要新增篩選條件，請執行以下步驟：

   a. 選擇新增篩選條件。
   b. 指定適用的篩選條件設定。如需詳細資訊，請參閱 在您建立或編輯字串比對條件時所指定的值。
   c. 選擇新增。
5. 若要刪除篩選條件，請執行以下步驟：

   a. 選取您要刪除的篩選條件。
   b. 選擇刪除篩選條件。

刪除字串比對條件

如果您想要刪除字串條件，您需要先刪除該條件內的所有篩選條件，以及從所有使用它的規則中移除，請參閱下列程序。

刪除字串比對條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。

2. 從使用該字串比對條件的規則中移除該條件：

   a. 在導覽窗格中，選擇規則。

   b. 選擇要刪除使用該字串比對條件的規則名稱。

   c. 在右窗格中選擇編輯規則。

   d. 在您要刪除的條件旁，選擇 X。

   e. 選擇更新。

   f. 對所有剩下要刪除使用該字串比對條件的規則，重複步驟。

3. 從您想刪除的條件移除篩選條件：

   a. 在導覽窗格中選擇字串和 regex 比對。

   b. 選擇您要刪除的字串比對條件名稱。

   c. 在右窗格中，選擇篩選條件旁的核取方塊，以選取所有篩選條件。

   d. 選擇刪除篩選條件。

4. 在導覽窗格中選擇字串和 regex 比對。

5. 在字串比對條件窗格中，選擇您要刪除的字串比對條件。

6. 選擇刪除以刪除選取的條件。

使用 Regex 比對條件

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

如果您想根據請求裡出現符合規則運算式 (regex) 模式的字串，允許或封鎖 web 請求，請建立一個或多個 Regex 比對條件。正則表達式匹配條件是一種字符串匹配條件的類型，用於標識要搜索的模式以及您希望 C AWS WAF lassic 檢查模式的 Web 請求的一部分，例如指定的標頭或查詢字符串。稍後，當您建立 Web ACL，您需要指定是否要允許或封鎖含有這些模式的請求。

主題

建立 Regex 比對條件

當您建立 Regex 比對條件，您需指定模式集以識別您想搜尋的字串 (使用規則運算式)。然後，您可以將這些模式集添加到過濾器中，該過濾器指定您希望 C AWS WAF lassic 檢查該模式集的 Web 請求部分，例如 URI 或查詢字符串。

您可以將多個規則運算式增至單一模式集中。若您這麼做，這些運算式會與 OR 結合。如此，如果請求符合清單中的任一個運算式，web 請求將比對模式集。

當您將正則表達式匹配條件添加到規則時，也可以配置 C AWS WAF lassic 以允許或阻止與條件中的值不匹配的 Web 請求。

AWS WAF 經典支持大多數標準的 Perl 兼容正則表達式（PCRE）。然而，目前不支援下列各項：

- Backreferences 和擷取子運算式
- 任意零寬度宣告
- 子程式參考和遞迴模式
- 條件式模式
- 恢復控制動詞
- \C 單一位元組指令
- \R 換行比對指令
- \K 開頭比對重設指令
- 圖說文字和內嵌的程式碼
- 原子分組和所佔有的量詞

建立 regex 比對條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。

2. 在導覽窗格中選擇字串和 regex 比對。
3. 選擇 Create condition (建立條件)。
4. 指定適用的篩選條件設定。如需詳細資訊，請參閱 您在建立或編輯 RegEx 符合條件時指定的值。
5. 選擇建立模式集和新增篩選條件 (如果您建立了新的模式集) 或新增篩選條件，如果您是使用現有的模式。
6. 選擇建立。

您在建立或編輯 RegEx 符合條件時指定的值

在建立或更新 Regex 比對條件時，請指定以下的值：

名稱

輸入 Regex 比對條件的名稱。名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_-!"#`+*},./。條件的名稱在建立後無法變更。

Type

選擇 Regex match (Regex 比對)。

要篩選的請求部分是

選擇您希望 C AWS WAF lassic 檢查您在值中指定的模式以匹配的每個 Web 請求的部分：

標頭

指定的請求標頭，例如，`User-Agent` 或 `Referer` 標頭。如果您選擇標頭，請在標頭欄位裡指定標頭的名稱。

HTTP 方法

HTTP 方法，指出要求來源執行的作業類型。CloudFront 支援下列方法：`DELETEGET`、`HEAD`、`OPTIONS`、`PATCH`、`POST`、和`PUT`。

查詢字串

出現在 ? 字元後的 URL 部分 (如果有)。

URI

要求的 URI 路徑，可識別資源，例如`/images/daily-ad.jpg`。這不包括 URI 的查詢字串或片段元件。如需詳細資訊，請參閱統一資源識別元 (URI)：一般語法。

除非指定了轉換，否則 URI 不會被標準化，並且會像從客戶端 AWS 接收它作為請求的一部分一樣進行檢查。Transformation (轉換) 將如指定重新格式化 URI。

Body

部分的請求內容含有您想傳送至您的 web 伺服器做為 HTTP 請求內文的額外資料，您要傳送到您的 Web 伺服器的 HTTP 請求的內文，例如資料表單。

> **Note**
>
> 如果您選擇 [內文] 做為要篩選之要求的部分值， AWS WAF 典型只會檢查前 8192 個位元組 (8 KB)。若要允許或封鎖主體超過 8192 個位元組的要求，您可以建立大小限制條件。（ AWS WAF 經典從請求頭獲取主體的長度。）如需詳細資訊，請參閱 使用容量限制條件。

單一查詢參數 (僅數值)

任何您已定義做為部分查詢字串的參數。例如，如果網址是「www.xyz.com」UserName = ABC& SalesRegion = 西雅圖」，您可以將過濾器添加到或參數中。UserNameSalesRegion

如果重複的參數顯示在查詢字串上，則數值評估則為「OR」。也就是說，將會觸發符合的值。例如，在網址「www.xyz.com? SalesRegion =boston& = SalesRegion 西雅圖」中，匹配「要匹配的值」中的「波士頓」或「西雅圖」模式將觸發匹配。

如果您選擇單一查詢參數 (僅數值)，您也可以指定查詢參數名稱。這是您要檢查的查詢字串中的參數，例如UserName或SalesRegion。查詢參數名稱的長度上限為 30 個字元。查詢參數名稱不區分大小寫。例如，您指定UserName為查詢參數名稱，這將匹配的所有變體 UserName，例如用戶名和用戶名。

所有的查詢參數 (僅數值)

類似於 S ingle 查詢參數 (僅限值)，而不是檢查單一參數的值，C AWS WAF lassic 會檢查查詢字串內所有參數的值，以找出要比對的「值」中指定的模式。例如，在網址「www.xyz.com? UserName =abc& = SalesRegion 西雅圖」中，要比對的值中的一個模式，該模式符合或中的值將觸發匹配。UserNameSalesRegion

標頭 (只有當「部分請求的篩選條件」為「標頭」時)

如果您從要篩選清單的要求部分中選擇 [標頭]，請從通用標頭清單中選擇標頭，或輸入您希望 C AWS WAF lassic 檢查的標頭名稱。

轉換

轉換會在 AWS WAF 傳統檢查要求之前重新格式化 Web 要求。這消除了攻擊者在 Web 請求中使用的一些不尋常的格式，以便繞過 C AWS WAF lassic。

您只能指定一種文字轉換類型。

轉換可執行下列操作：

無

AWS WAF Classic 在檢查 Val ue 中是否有要匹配的字符串之前，不會對 Web 請求執行任何文本轉換。

轉換成小寫

AWS WAF 經典將大寫字母（A-Z）轉換為小寫（a-z）。

HTML 解碼

AWS WAF 經典用未編碼字符替換 HTML 編碼的字符：

- 將 " 換成 &
- 以非中斷空格取代
- 將 < 換成 <
- 將 > 換成 >
- 將表示為十六進位格式的字元 &#xhhhh; 以對應字元取代
- 將表示為十進位格式的字元 &#nnnn; 以對應字元取代

標準化空格

AWS WAF 經典用空格字符（十進制 32）替換以下字符：

- \f、跳頁、小數 12
- \t、標籤、小數 9
- \n、換行，小數 10
- \r、換行、小數 13
- \v、垂直標籤，小數 11
- 非中斷空格，小數 160

此外，此選項將數個空格取代為一個空格。

簡化命令列

若您將擔心攻擊者插入作業命令列命令，或使用不尋常的格式偽裝某些或所有命令，請使用此選項執行下列轉換：

- 刪除以下字元：\ " ' ^
- 刪除以下字元前的空格：/ (
- 將以下字元取代為空格：, ;
- 將數個空格取代為一個空格
- 將所有大寫字母 (A-Z) 轉換成小寫 (a-z)

URL 解碼

解碼 URL 編碼請求。

比對請求的 Regex 模式

您可以選擇現有的模式集，或建立新的。如果您建立新的模式集指定以下：

新模式集的名稱

輸入名稱，然後指定要 C AWS WAF lassic 搜尋的正則運算式模式。

如果您新增多個規則運算式至模式集，這些運算式會與 OR 結合。如此，如果請求符合清單中的任一個運算式，web 請求將比對模式集。

符合值 的長度上限為 70 個字元。

編輯 Regex 比對條件

您可以使用下列變更現有的 regex 比對條件：

- 刪除現有模式集裡的模式
- 新增模式至現有的模式集
- 從現有的 Regex 比對條件刪除篩選條件
- 將過濾器添加到現有的正則表達式匹配條件（在正則表達式匹配條件中只能有一個過濾器。 因此，若要新增篩選器，您必須先刪除現有的篩選器。）
- 刪除現有的 Regex 比對條件

> **Note**
>
> 您不能從現有篩選條件新增或刪除模式集。您必須編輯模式集、或刪除篩選條件並建立新的篩選條件與其新的模式集。

刪除現有模式集裡的模式

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中選擇字串和 regex 比對。
3. 選擇檢視 Regex 模式集。
4. 選擇您要編輯的模式集名稱。
5. 選擇編輯。
6. 在您要刪除的模式旁，選擇 X。
7. 選擇儲存。

新增模式至現有的模式集

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中選擇字串和 regex 比對。
3. 選擇檢視 Regex 模式集。
4. 選擇要編輯的模式集名稱。
5. 選擇編輯。
6. 輸入新的 Regex 模式。
7. 選擇新的模式旁的 +。
8. 選擇儲存。

從現有的 Regex 比對條件刪除篩選條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中選擇字串和 regex 比對。
3. 選擇您要刪除的篩選條件的比對條件名稱。

4. 選擇您要刪除篩選條件旁的方塊。
5. 選擇刪除篩選條件。

刪除 Regex 比對條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 從 Regex 比對條件刪除篩選條件。請參閱 從現有的 Regex 比對條件刪除篩選條件 以取得執行此動作的指示。)
3. 從使用該 Regex 比對條件的規則中移除該條件：
   a. 在導覽窗格中，選擇規則。
   b. 選擇要刪除使用該 Regex 比對條件的規則名稱。
   c. 在右窗格中選擇編輯規則。
   d. 在您要刪除的條件旁，選擇 X。
   e. 選擇更新。
   f. 對所有剩下要刪除使用該 Regex 比對條件的規則，重複步驟。
4. 在導覽窗格中選擇字串和 regex 比對。
5. 選擇您要刪除條件旁的按鈕。
6. 選擇刪除。

從現有的 Regex 比對條件新增或變更篩選條件

Regex 比對條件只能擁有一個篩選條件。如果您想新增或變更篩選條件，您必須先刪除現有的篩選條件。

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 從您想變更的 Regex 條件刪除篩選條件：請參閱 從現有的 Regex 比對條件刪除篩選條件 以取得執行此動作的指示。)
3. 在導覽窗格中選擇字串和 regex 比對。

4. 選擇您要變更的條件名稱。
5. 選擇新增篩選條件。
6. 為新的篩選條件輸入適當的值，然後選擇新增。

使用規則

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

規則可讓您指定 C AWS WAF lassic 要監視的確切條件，以精確鎖定您希望 C AWS WAF lassic 允許或封鎖的 Web 請求。例如，C AWS WAF lassic 可以監視要求來源的 IP 位址、要求包含的字串以及字串出現的位置，以及要求是否包含惡意 SQL 程式碼。

主題

- 建立規則和新增條件
- 建立和移除規則的條件
- 刪除規則
- AWS Marketplace 規則群組

建立規則和新增條件

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

如果您在規則中新增多個條件，Web 要求必須符合 C AWS WAF lassic 的所有條件，才能根據該規則允許或封鎖要求。

建立規則並新增條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。

2. 在導覽窗格中，選擇規則。
3. 選擇建立規則。
4. 輸入下列值：

   名稱

   輸入名稱。

   CloudWatch 量度名稱

   輸入「 AWS WAF 典型」將建立並與規則產生關聯的 CloudWatch 測量結果名稱。名稱只能包含英數字元 (A-Z、a-z、0-9)，最大長度為 128 且最短長度為 1。它不能包含為 AWS WAF 傳統保留的空白字元或量度名稱，包括「全部」和「Default_Action」。

   規則類型

   選擇 `Regular rule` 或 `Rate-based rule`。以速率為基礎的規則與一般規則相同，但也會考慮五分鐘內從 IP 位址到達的要求數目。如需這些規則類型的詳細資訊，請參閱AWS WAF 經典如何運作。

   速率限制

   對於以速率為基礎的規則，輸入五分鐘期間內允許來自符合規則條件之 IP 地址的最大請求數量。速率限制必須至少為 100。

   您可以單獨指定速率限制，也可以同時指定速率限制和條件。如果您僅指定速率限制， AWS WAF 則會在所有 IP 位址上設定限制。如果您指定速率限制和條件，請 AWS WAF 在符合條件的 IP 位址上設定限制。

   當 IP 位址達到速率限制閾值時，會盡快 AWS WAF 套用指派的動作 (封鎖或計數)，通常會在 30 秒內套用。一旦動作到位，如果五分鐘過去，沒有來自 IP 位址的要求， AWS WAF 將計數器重設為零。

5. 若要新增條件至規則，請指定以下值：

請求為有 (does)/沒有 (does not) 的時機

如果您希望 C AWS WAF lassic 根據條件中的篩選器允許或封鎖要求，請選擇 [執行]。例如，如果 IP 比對條件包含 IP 位址範圍 192.0.2.0/24，而您希望 AWS WAF 傳統版允許或封鎖來自這些 IP 位址的要求，請選擇 [執行]。

如果您希望 C AWS WAF lassic 根據條件中的反向篩選條件允許或封鎖要求，請選擇「不」。例如，如果 IP 比對條件包含 IP 位址範圍 192.0.2.0/24，而您希望「 AWS WAF 典型」允許或封鎖不來自這些 IP 位址的要求，請選擇「不」。

符合/來自

選擇要新增到規則的條件類型。

- 跨網站指令碼比對條件 — 在跨網站指令碼比對條件中，選擇至少符合其中一個篩選器
- IP 匹配條件 — 從中選擇來自 IP 地址
- 地理匹配條件 — 選擇源自地理位置
- 大小限制條件 — 在大小限制條件下選擇至少匹配一個過濾器
- SQL 注入相符條件 — 選擇符合 SQL 注入相符條件中至少一個篩選條件
- 字串比對條件 — 選擇符合字串符合條件中至少一個篩選條件
- 正則表達式匹配條件 — 在正則表達式匹配條件中選擇至少匹配一個過濾器

條件名稱

選擇要新增到規則的條件。指清單只顯示您在前述步驟中所選擇的條件類型。

6. 若要新增其他條件至規則，請選擇新增另一個條件，並重複步驟四和五。注意下列事項：
   - 如果您新增多個條件，Web 要求必須符合每個條件中的至少一個篩選器，C AWS WAF lassic 才能根據該規則允許或封鎖要求
   - 如果您在同一規則中新增兩個 IP 比對條件，C AWS WAF lassic 將只允許或封鎖來自兩個 IP 相符條件中出現的 IP 位址的要求
7. 完成新增條件，請選擇建立。

建立和移除規則的條件

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

您可以新增或移除條件來變更規則。

新增或移除規則裡的條件

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中，選擇規則。
3. 選擇要新增或移除條件的規則名稱。
4. 選擇新增規則。
5. 若要新增一個條件，請選擇新增條件 並指定以下值：

   請求為有 (does)/沒有 (does not) 的時機

   如果您希望 AWS WAF 傳統版根據條件的篩選器允許或封鎖要求，例如，來自 192.0.2.0/24 IP 位址範圍的網頁要求，請選擇 [do]。

   如果您希望 C AWS WAF lassic 根據條件中的反向篩選條件允許或封鎖要求，請選擇「不」。例如，如果 IP 比對條件包含 IP 位址範圍 192.0.2.0/24，而您希望「 AWS WAF 典型」允許或封鎖不來自這些 IP 位址的要求，請選擇「不」。

   符合/來自

   選擇要新增到規則的條件類型。

   - 跨網站指令碼比對條件 — 在跨網站指令碼比對條件中，選擇至少符合其中一個篩選器
   - IP 匹配條件 — 從中選擇來自 IP 地址
   - 地理匹配條件 — 選擇源自地理位置

- 大小限制條件 — 在大小限制條件下選擇至少匹配一個過濾器
- SQL 插入相符條件 — 選擇符合 SQL 注入相符條件中至少一個篩選條件
- 字串比對條件 — 選擇符合字串符合條件中至少一個篩選條件
- 正則表達式匹配條件 — 在正則表達式匹配條件中選擇至少匹配一個過濾器

條件名稱

選擇要新增到規則的條件。指清單只顯示您在前述步驟中所選擇的條件類型。

6. 若要移除條件，選擇條件名稱右邊的 X。
7. 選擇更新。

刪除規則

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和網頁等 AWS WAF 資源ACLs，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

如果要刪除規則，您必須先從正在使用該規則的 Web 中移除ACLs該規則，然後移除規則中包含的條件。

刪除規則

1. 登入 AWS Management Console 並開啟 AWS WAF 主控台，位於https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 若要從正在使用規則ACLs的 Web 移除規則，請針對每個 Web 執行下列步驟ACLs：

   a. 在導覽窗格中，選擇 [Web] ACLs。

   b. 選擇正在使用您要刪除之規則的網頁ACL名稱。

> **Note**
>
> 如果沒有看到網頁ACL，請確認「地區」選項正確無誤。ACLs保護 Amazon CloudFront 分佈的網絡位於全球（CloudFront）。

c. 選擇規則標籤。

d. 選擇 「編輯網頁」ACL。

e. 選擇您要刪除的規則右側的 X，然後選擇 [更新]。

3. 在導覽窗格中，選擇規則。

4. 選擇您要刪除的規則名稱。

> **Note**
>
> 如果看不到規則，請確定 [地區] 選項正確無誤。保護 Amazon CloudFront 分發的規則在全球（CloudFront）。

5. 選擇 Delete (刪除)。

AWS Marketplace 規則群組

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

AWS WAF 傳AWS Marketplace 統提供規則群組來協助您保護資源。 AWS Marketplace 規則群組是由 AWS 以及 AWS 合作夥伴公司撰寫和更新的預先定義 ready-to-use 規則的集合。

有些 AWS Marketplace 規則群組旨在協助保護特定類型的 Web 應用程式 WordPress，例如 Joomla 或 PHP。其他 AWS Marketplace 規則群組提供廣泛的保護，防範已知的安全威脅或常見 Web 應用程式弱點，例如 OWASP 前 10 名所列的弱點。

您可以從偏好的 AWS 合作夥伴處安裝單一 AWS Marketplace 規則群組，也可以新增自己的自訂 C AWS WAF lassic 規則，以增強保護。如果您需遵守 PCI 或 HIPAA 等法規遵循，您可能可以使用 AWS Marketplace 規則群組來滿足 Web 應用程式防火牆的需求。

AWS Marketplace 規則群組可供使用，沒有長期合約，也沒有最低承諾。訂閱規則群組時，您必須按月支付費用 (依小時按比例分配)，以及基於用量的持續請求費用。如需詳細資訊，請參閱AWS WAF 傳統定價和上每個 AWS Marketplace 規則群組的說明 AWS Marketplace。

自動更新

掌握不斷變化的威脅環境的最新資訊可能既耗時又昂貴。 AWS Marketplace 規則群組可以在您實作和使用「 AWS WAF 傳統」時節省您的時間。另一個好處是，當出現新的漏洞 AWS 和威脅時，我們的 AWS 合作夥伴會自動更新 AWS Marketplace 規則群組。

許多公開這些漏洞前，我們的合作夥伴會先收到相關通知。他們可以更新規則群組並將它們部署給您，即使在新的威脅已廣泛為人熟知之前。很多合作夥伴也有威脅研究團隊調查和分析最新的威脅，以便寫入最相關的規則。

存取規則群組中的 AWS Marketplace 規則

每個 AWS Marketplace 規則群組都會針對其設計用來防範的攻擊類型和弱點提供完整描述。為了保護規則群組供應商的智慧財產權，所以您無法在規則群組裡逐一查看規則。此限制也有助於防止惡意使用者利用規避發佈的規則設計攻擊威脅。

因為您無法檢視規則群組中的個別規則，因此也無法編輯規則群組中的任何規 AWS Marketplace 則。AWS Marketplace 然而，您可將特定規則自規則群組排除。這稱為「規則群組例外」。排除規則不會移除這些規則，而是會將規則的動作變更為 COUNT。因此，符合排除規則的請求會納入計算，但不會被封鎖。您將接收每個已排除規則的 COUNT 指標。

針對意外封鎖流量 (誤報) 的規則群組進行故障排除時，排除規則十分實用。一個故障排除技巧就是去辨識規則群組內封鎖所需流量的特定規則，然後停用 (排除) 該條規則。

除了排除特定規則，您可啟用或停用整個規則群組，並選擇欲執行的規則群組動作，藉此強化保護。如需詳細資訊，請參閱 使用 AWS Marketplace 規則群組。

配額

您只能啟用一個 AWS Marketplace 規則群組。您也可以啟用使用建立的一個自訂規則群組 AWS Firewall Manager。這些規則群組會計入每 Web ACL 的 10 個規則限額。因此，單一 Web ACL 中可以有一個 AWS Marketplace 規則群組、一個自訂規則群組以及最多八個自訂規則。

定價

如需 AWS Marketplace 規則群組定價的相關資訊，請參閱AWS WAF 傳統定價和上每個 AWS Marketplace 規則群組的說明 AWS Marketplace。

使用 AWS Marketplace 規則群組

您可以在 AWS WAF 傳統主控台上訂閱和取消訂閱 AWS Marketplace 規則群組。您亦可將特定規則自規則群組排除。

若要訂閱和使用 AWS Marketplace 規則群組

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中，選擇市集。
3. 在 Available marketplace products (提供市場產品)，選擇規則的名稱，檢視其詳細資訊和定價資訊。
4. 如果您想訂閱此規則群組，選擇繼續。

   > **Note**
   >
   > 如果您不想訂閱此規則群組，只需在您的瀏覽器關閉此頁面。

5. 選擇Set up your account (建立您的帳戶)。
6. 新增規則群組至 Web ACL，就像您新增個別規則一樣。如需詳細資訊，請參閱 建立 Web ACL 或編輯 Web ACL 。

   > **Note**
   >
   > 新增一個規則群組至 Web ACL 時，您為規則群組設定的動作 (No override (不覆寫) 或 Override to count (覆寫計數)) 稱為規則群組覆寫動作。如需詳細資訊，請參閱 規則群組覆寫。

若要取消訂閱 AWS Marketplace 規則群組

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 從所有 Web ACL 中移除規則群組。如需詳細資訊，請參閱 編輯 Web ACL。
3. 在導覽窗格中，選擇市集。
4. 選擇Manage your subscriptions (管理我的訂閱)。
5. 在您想要取消訂閱的規則群組名稱旁，選擇取消訂閱。
6. 選擇是，取消訂閱。

自規則群組排除規則 (規則群組例外)

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 如果尚未啟用，請啟用 AWS WAF 傳統記錄。如需詳細資訊，請參閱 記錄 Web ACL 流量資訊。使用 AWS WAF 傳統記錄檔來識別您要排除的規則 ID。這些通常是封鎖正當請求的規則。
3. 在導覽窗格中，選擇 Web ACL。
4. 選擇您要編輯的 Web ACL 名稱。這會開啟右窗格中包含 Web ACL 詳細資訊的頁面。

   > **Note**
   >
   > 您希望編輯的規則群組必須與 Web ACL 建立關聯，之後您才能自該規則群組排除規則。

5. 在規則標籤上，右側窗格中，選擇編輯 Web ACL。
6. 在 Rule group exceptions (規則群組例外) 的部分，請展開您想要編輯的規則群組。
7. 選擇欲排除規則旁的 X。您可以使用 AWS WAF 傳統記錄檔來識別正確的規則識別碼。
8. 選擇更新。

   排除規則不會將這些規則自規則群組中移除，而是會將規則的動作變更為 COUNT。因此，符合排除規則的請求會納入計算，但不會被封鎖。您將接收每個已排除規則的 COUNT 指標。

> **Note**
>
> 您可使用相同程序從 AWS Firewall Manager中所建立的自訂規則群組中排除規則。然而，若不想使用這些步驟來將規則從自訂規則群組中排除，您只要編輯自訂規則群組即可，步驟詳見從 AWS WAF 傳統規則群組新增和刪除規則。

規則群組覆寫

AWS Marketplace 規則群組有兩種可能的動作：「不覆寫」和「覆寫要計數」。如果您想要測試規則群組，設定動作為覆寫計數。這個規則群組動作會覆寫任何群組內個別規則所指定的封鎖動作。也就是說，如果規則群組的動作是設定為覆寫計數，部會封鎖這些符合群組規則的請求，而是將這些請求計數在內。反之，如果您設定規則群組的動作為2不覆寫，則會使用該群組裡規則的動作。

針對 AWS Marketplace 規則群組進行故障診斷

如果您發現 AWS Marketplace 規則群組封鎖了合法流量，請執行下列步驟。

AWS Marketplace 規則群組的故障診斷

1. 排除會封鎖正當流量的特定規則。您可以使用 AWS WAF 傳統記錄來識別哪些規則會封鎖哪些要求。如需排除規則的詳細資訊，請參閱自規則群組排除規則 (規則群組例外)。
2. 如果排除特定規則無法解決問題，您可以將規 AWS Marketplace 則群組的動作從 「無覆寫」 變更為「覆寫」以計數。這允許 web 請求通過，無視規則群組內的個別規則動作。這也為您提供規則群組的 Amazon CloudWatch 指標。
3. 將 AWS Marketplace 規則群組動作設定為 [覆寫以計數] 後，請連絡規則群組提供者的客戶支援團隊，以進一步疑難排解問題。如需聯絡資訊，請參閱 AWS Marketplace中產品列表頁面的規則群組清單。

聯絡客戶支援

對於 AWS WAF 傳統或由管理的規則群組的問題 AWS，請連絡 AWS Support。對於由 AWS 合作夥伴管理的規則群組發生問題，請聯絡該合作夥伴的客戶支援團隊。若要尋找合作夥伴聯絡資訊，請參閱上的合作夥伴清單 AWS Marketplace。

建立和銷售 AWS Marketplace 規則群組

如果您想要出售 AWS Marketplace 規則群組 AWS Marketplace，請參閱如何銷售您的軟體 AWS Marketplace。

使用 Web ACL

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

當您將規則新增至 Web ACL 時，您可以指定是否希望 C AWS WAF lassic 根據規則中的條件允許或封鎖請求。如果您將多個規則新增至 Web ACL， AWS WAF 典型會依照您在 Web ACL 中列出規則的順序來評估每個請求。當 Web 要求符合規則中的所有條件時，C AWS WAF lassic 會立即採取對應的動作 (允許或封鎖)，並且不會根據 Web ACL 中剩餘的規則 (如果有的話) 評估要求。

如果 Web 請求不符合 Web ACL 中的任何規則， AWS WAF 典型會採用您為 Web ACL 指定的預設動作。如需詳細資訊，請參閱 決定 Web ACL 的預設動作。

如果您想在開始使用規則來允許或封鎖要求之前先測試規則，您可以設定 C AWS WAF lassic 來計算符合規則中條件的 Web 要求。如需更多詳細資訊，請參閱 測試 Web ACL。

主題

決定 Web ACL 的預設動作

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。

如需的最新版本 AWS WAF，請參閱AWS WAF。

當您建立並設定 Web ACL 時，您必須做出的第一個也是最重要的決定，就是預設動作是否應該讓 AWS WAF 傳統版允許 Web 要求或封鎖 Web 要求。預設動作會指出 C AWS WAF lassic 在檢查您指定的所有條件的 Web 要求之後執行的動作，且 Web 要求不符合下列任何條件：

- 允許 — 如果您想要允許大多數使用者存取您的網站，但想要封鎖對要求來自指定 IP 位址的攻擊者的存取，或其要求似乎包含惡意 SQL 程式碼或指定值的攻擊者，請針對預設動作選擇 [允許]。
- 封鎖 — 如果您想要防止大多數潛在使用者存取您的網站，但想要允許存取來自指定 IP 位址的請求，或其請求包含指定值的使用者，請選擇 [封鎖] 做為預設動作。

在決定預設動作後，您做的許多決定會取決於您是要允許還是封鎖大多數 Web 請求。例如，如果您想要允許大多數的請求，您建立的比對條件通常應指定您想要封鎖 的 web 請求，如下所示：

- 來自發出異常數量 IP 地址的請求
- 來自您不常交涉、或時常受到攻擊國家/地區的請求
- 請求包含仿造使用者代理程式標頭中的值
- 似乎含有惡意 SQL 程式碼的請求

建立 Web ACL

Note

這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
如需的最新版本 AWS WAF，請參閱AWS WAF。

建立 Web ACL

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。

2. 如果這是您第一次使用「 AWS WAF 典型」，請選擇「移至 AWS WAF 典型」，然後選擇「設定 Web ACL」。如果您之前使用過 AWS WAF 傳統版，請在導覽窗格中選擇 [Web ACL]，然後選擇 [建立 Web ACL]。
3. 在「網頁 ACL 名稱」中，輸入名稱。

   > **Note**
   >
   > 建立 Web ACL 後無法修改名稱。

4. 若為CloudWatch 量度名稱，請變更預設名稱 (如果適用)。名稱只能包含英數字元 (A-Z、a-z、0-9)，最大長度為 128 且最短長度為 1。它不能包含為 AWS WAF 傳統保留的空白字元或量度名稱，包括「全部」和「Default_Action」。

   > **Note**
   >
   > 建立 Web ACL 後無法修改名稱。

5. 對於 區域，選擇一個區域。
6. 對於AWS 資源，請選擇您想要將此 Web ACL 關聯的資源，然後選擇下一步。
7. 如果您已經建立了希望 C AWS WAF lassic 用來檢查 Web 請求的條件，請選擇 [下一步]，然後繼續進行下一個步驟。

   若您尚未建立條件，請立即執行。如需詳細資訊，請參閱下列主題：

   - 使用跨網站指令碼比對條件
   - 使用 IP 比對條件
   - 使用地理比對條件
   - 使用容量限制條件
   - 使用 SQL Injection 比對條件
   - 使用字串比對條件
   - 使用 Regex 比對條件
8. 如果您已經建立要新增至此 Web ACL 的規 AWS Marketplace 則或規則群組 (或訂閱規則群組)，請將規則新增至 Web ACL：

   a. 在規則清單中選擇規則。

   b. 選擇 Add rule to web ACL (新增規則至 Web ACL)。

c. 重複步驟 a 和 b，直到您已新增所有想要新增至 Web ACL 的規則。

d. 前往步驟 10。

9. 如果您尚未建立規則，您可以現在新增規則：

a. 選擇建立規則。

b. 輸入下列值：

名稱

輸入名稱。

CloudWatch 量度名稱

輸入「 AWS WAF 典型」將建立並與規則產生關聯的 CloudWatch 測量結果名稱。名稱只能包含英數字元 (A-Z、a-z、0-9)，最大長度為 128 且最短長度為 1。它不能包含為 AWS WAF 傳統保留的空白字元或量度名稱，包括「全部」和「Default_Action」。

> **Note**
>
> 建立規則後無法修改指標名稱。

c. 若要新增條件至規則，請指定以下值：

請求為有 (does)/沒有 (does not) 的時機

如果您希望 AWS WAF 傳統版根據條件的篩選器允許或封鎖要求，例如，來自 IP 位址 192.0.2.0/24 範圍的網頁要求，請選擇 [do]。

如果您希望 C AWS WAF lassic 根據條件中的反向篩選條件允許或封鎖要求，請選擇「不」。例如，如果 IP 比對條件包含 IP 位址範圍 192.0.2.0/24，而您希望「 AWS WAF 典型」允許或封鎖不來自這些 IP 位址的要求，請選擇「不」。

符合/來自

選擇要新增到規則的條件類型。

- 跨網站指令碼比對條件 — 在跨網站指令碼比對條件中選擇至少符合其中一個篩選器
- IP 匹配條件 — 從中選擇來自 IP 地址
- 地理匹配條件 — 選擇源自地理位置
- 大小限制條件 — 在大小限制條件下選擇至少匹配一個過濾器

- SQL 注入相符條件 — 選擇符合 SQL 注入相符條件中至少一個篩選條件
- 字串比對條件 — 選擇符合字串符合條件中至少一個篩選條件
- 正則表達式匹配條件-在正則表達式匹配條件中選擇至少匹配一個過濾器

條件名稱

選擇要新增到規則的條件。指清單只顯示您在前述名單中所選擇的條件類型。

d. 若要新增其他條件至規則，請選擇 Add another condition (新增另一個條件)，並重複步驟 b 和 c。注意下列事項：

- 如果您新增多個條件，Web 要求必須符合每個條件中的至少一個篩選器，C AWS WAF lassic 才能根據該規則允許或封鎖要求。
- 如果您在同一個規則中新增兩個 IP 比對條件，C AWS WAF lassic 將只允許或封鎖來自兩個 IP 比對條件中出現的 IP 位址的要求。

e. 重複步驟九，直到您已建立所有想要新增至 Web ACL 的規則。

f. 選擇建立。

g. 繼續執行步驟 10。

10. 針對 Web ACL 中的每個規則或規則群組，選擇要 AWS WAF 傳統提供的管理類型，如下所示：

- 針對每個規則，選擇您是否希望 AWS WAF 傳統根據規則中的條件允許、封鎖或計算 Web 要求：
  - 允許 — API Gateway CloudFront 或應用程式負載平衡器會回應要求的物件。在的情況下 CloudFront，如果物件不在邊緣快取中，請將要求 CloudFront 轉寄至原始位置。
  - 封鎖 — API Gateway CloudFront 或應用 Application Load Balancer 會使用 HTTP 403 (禁止) 狀態碼回應要求。CloudFront 也可以使用自定義錯誤頁面響應。如需詳細資訊，請參閱 使用 AWS WAF 經典與 CloudFront 自定義錯誤頁面。
  - 計數 — AWS WAF 傳統會遞增符合規則中條件的要求計數器，然後繼續根據 Web ACL 中的其餘規則檢查 Web 要求。

    如需先使用 Count (計數) 來測試 Web ACL，再開始用於允許或封鎖 Web 請求的詳細資訊，請參閱計數在 Web ACL 中符合規則的 web 請求。
- 對於每個規則群組，設定規則群組的覆寫動作：
  - 不覆寫 — 使規則群組中個別規則的動作被使用。
  - 覆寫計數 — 覆寫群組中個別規則指定的任何區塊動作，以便僅計算所有相符的請求。

    如需詳細資訊，請參閱 規則群組覆寫。

11. 如果您要變更 Web ACL 中規則的順序，請使用「順序」欄中的箭頭。 AWS WAF 典型會根據規則在 Web ACL 中出現的順序來檢查 Web 請求。
12. 如果您想要移除新增到 Web ACL 的規則，在該規則列選擇 x。
13. 選擇 Web ACL 的預設動作。當 Web 請求與此 Web ACL 中任何規則中的條件不匹配時， AWS WAF 經典採取的操作。如需詳細資訊，請參閱 決定 Web ACL 的預設動作。
14. 選擇 Review and create (檢閱和建立)。
15. 檢視 Web ACL 的設定，然後選擇確認並建立。

將 Web ACL 與 Amazon API Gateway、 CloudFront 分發或 Application Load Balancer 建立關聯或取消關聯

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

若要關聯或取消關聯 Web ACL，請執行適用的程序。請注意，您也可以在建立或更新發 CloudFront 佈時將 Web ACL 與分佈相關聯。如需詳細資訊，請參閱 Amazon CloudFront 開發人員指南中的使用 AWS WAF 傳統版控制內容的存取。

當與 Web ACL 關聯時，套用以下限制：

- 每個 API Gateway API、Application Load Balancer 和 CloudFront 發佈只能與一個 Web ACL 產生關聯。
- 與 CloudFront 發佈相關聯的 Web ACL 無法與 Application Load Balancer 或 API Gateway API 產生關聯。但是，Web ACL 可以與其他 CloudFront 分佈相關聯。

將 Web ACL 與 API Gateway API、 CloudFront 散發或 Application Load Balancer 產生關聯

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。

2. 在導覽窗格中，選擇 Web ACL。
3. 選擇您要與 API Gateway API、 CloudFront 分發或 Application Load Balancer 產生關聯的 Web ACL 名稱。這會開啟右窗格中包含 Web ACL 詳細資訊的頁面。
4. 在 [規則] 索引標籤的 [使用此 Web ACL 的AWS 資源] 下，選擇 [新增關聯]。
5. 出現提示時，請使用 [資源] 清單來選擇要與此 Web ACL 建立關聯的 API Gateway API、CloudFront散發或應用程式負載平衡器。如果您選擇「應用程式負載平衡器」，則還必須指定「區域」。
6. 選擇新增。
7. 若要將此 Web ACL 與其他 API Gateway API、 CloudFront 分發或其他 Application Load Balancer 產生關聯，請重複步驟 4 到 6。

取消 Web ACL 與 API Gateway API、散 CloudFront 發或 Application Load Balancer 的關聯

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中，選擇 Web ACL。
3. 選擇您要取消與 API Gateway API、散 CloudFront 發或 Application Load Balancer 關聯的 Web ACL 名稱。這會開啟右窗格中包含 Web ACL 詳細資訊的頁面。
4. 在 [規則] 索引標籤的使用此 Web ACL 的AWS 資源下，針對您要取消此 Web ACL 關聯的每個 API Gateway API、散 CloudFront 佈或應用程式負載平衡器選擇 x。

編輯 Web ACL

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

若要從 Web ACL 移除規則或變更預設動作，請執行下列程序。

編輯 Web ACL

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中，選擇 Web ACL。
3. 選擇您要編輯的 Web ACL 名稱。這會開啟右窗格中包含 Web ACL 詳細資訊的頁面。
4. 在規則標籤上，右側窗格中，選擇編輯 Web ACL。
5. 若要新增規則至 Web ACL，請執行以下步驟：

   a. 在規則名單中，選擇您要新增的規則。

   b. 選擇 Add rule to web ACL (新增規則至 Web ACL)。

   c. 重複步驟 a 和 b，直到您已加入所有想新增的規則。
6. 如果您要變更 Web ACL 中規則的順序，請使用「順序」欄中的箭頭。 AWS WAF 典型會根據規則在 Web ACL 中出現的順序來檢查 Web 要求。
7. 若要從 Web ACL 移除規則，在該規則行的右邊選擇 x。這不會從 AWS WAF 經典中刪除規則，它只是從此 Web ACL 中刪除規則。
8. 若要變更規則的動作或 Web ACL 的預設動作，選擇慣用的選項。

   > **Note**
   >
   > 為規則群組或規則群組設定動作時 (相對於單一規則)，您為規則群組設定的動作 (「不覆寫」或「覆寫至計數」) 稱為覆寫動作。 AWS Marketplace 如需詳細資訊，請參閱 規則群組覆寫
9. 選擇儲存變更。

刪除網頁 ACL

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和網頁等 AWS WAF 資源ACLs，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。

如需的最新版本 AWS WAF，請參閱AWS WAF。

若要刪除 WebACL，您必須移除包含在 Web 中的規則，並取消所有 CloudFront 分發ACL和應用程式負載平衡器與 Web 的關聯。ACL請執行以下程序。

刪除網頁的步驟 ACL

1. 登入 AWS Management Console 並開啟 AWS WAF 主控台，位於https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中，選擇 [Web] ACLs。
3. 選擇您要刪除ACL的網頁名稱。這會在右窗格中開啟網頁詳細資料ACL的頁面。

   > **Note**
   >
   > 如果沒有看到網頁ACL，請確認「地區」選項正確無誤。ACLs保護 Amazon CloudFront 分佈的網絡位於全球（CloudFront）。
4. 在右窗格的 [規則] 索引標籤上，選擇 [編輯網頁] ACL。
5. 若要從 Web 移除所有規則ACL，請為每個規則選擇列右側的 x。這不會從 AWS WAF 經典中刪除規則，它只是從此網絡中刪除規則ACL。
6. 選擇更新。
7. 取消 Web 與所有ACL CloudFront 發行版和應用程式負載平衡器的關聯。在 [規則] 索引標籤的 [使用此 Web 的AWS 資源] 下ACL，選擇每個API閘道API、 CloudFront 散發或 Application Load Balancer 的 x。
8. 在網ACLs頁上，確認已選取ACL要刪除的網頁，然後選擇 [刪除]。

測試 Web ACL

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。

如需的最新版本 AWS WAF，請參閱AWS WAF。

為了確保您不會意外地將 C AWS WAF lassic 設定為封鎖要允許或允許要封鎖要求的 Web 要求，建議您在開始在網站或 Web 應用程式上使用 Web ACL 之前，先徹底測試 Web ACL。

主題

- 計數在 Web ACL 中符合規則的 web 請求
- 檢視 API Gateway CloudFront 或 Application Load Balancer 已轉寄至 AWS WAF 典型的 Web 請求範例

計數在 Web ACL 中符合規則的 web 請求

當您將規則新增至 Web ACL 時，您可以指定是否要讓 C AWS WAF lassic 允許、封鎖或計算符合該規則中所有條件的 Web 要求。建議您以下列組態開始動作：

- 設定 Web ACL 的所有規則，以計數 Web 請求
- 設定 Web ACL 的預設動作，以允許請求

在此組態中，C AWS WAF lassic 會根據第一個規則中的條件檢查每個 Web 要求。如果 Web 要求符合該規則中的所有條件，C AWS WAF lassic 會增加該規則的計數器。然後，「AWS WAF 典型」會根據下一個規則中的條件檢查 Web 要求。如果要求符合該規則中的所有條件，C AWS WAF lassic 會增加規則的計數器。這會持續到 C AWS WAF lassic 根據您所有規則中的條件檢查請求為止。

在 Web ACL 中設定所有規則來計算請求，並將 Web ACL 與 Amazon API Gateway、 CloudFront 分發或 Application Load Balancer 產生關聯後，您可以在 Amazon CloudWatch 圖形中檢視產生的計數。針對 Web ACL 中的每個規則，以及 API Gateway CloudFront 或 Application Load Balancer 針對 Web ACL 轉寄至 AWS WAF 典型的所有要求， CloudWatch 可讓您：

- 檢視前一小時或前三小時的資料，
- 變更資料點之間的間隔。
- 變更對資料 CloudWatch 執行的計算，例如最大值、最小值、平均值或總和

> **Note**
>
> AWS WAF 傳統服務 CloudFront 是全域服務，而量度只有在您選擇美國東部 (維吉尼亞北部) 區域時才可用 AWS Management Console。如果您選擇其他地區， CloudWatch 主控台中將不會顯示任何 AWS WAF 傳統量度。

若要在 Web ACL 查看規則資料

1. 請登入 AWS Management Console 並開啟 CloudWatch 主控台，網址為 https://console.aws.amazon.com/cloudwatch/。
2. 在導覽窗格中，於 Metrics (指標) 下選擇 WAF。
3. 選取要檢視資料的 Web ACL 的核取方塊。
4. 變更適用的設定：

   統計數字

   選擇對資料 CloudWatch 執行的計算。

   時間範圍

   選擇您想要檢視前一小時或前三個小時的資料。

   期間

   選擇圖形中資料點之間的間隔。

   規則

   選擇您要檢視資料的規則。

   注意下列事項：

   - 如果您只是將 Web ACL 與 API Gateway API、 CloudFront 分發或 Application Load Balancer 產生關聯，則可能需要等待幾分鐘，資料才會顯示在圖形中，以及 Web ACL 顯示在可用度量清單中的指標。
   - 如果您將多個 API Gateway API、 CloudFront 散發或 Application Load Balancer 與 Web ACL 產生關聯， CloudWatch 資料將包含與 Web ACL 相關聯的所有分發的所有要求。
   - 您可以將滑鼠指標移至資料點以取得更多資訊。

- 圖形不會自動自我重新整理。若要更新顯示，請選擇重新整理
  ()
  圖示。

5. (選擇性) 檢視 API Gateway CloudFront 或 Application Load Balancer 已轉寄至 AWS WAF 典型之個別要求的詳細資訊。如需詳細資訊，請參閱 檢視 API Gateway CloudFront 或 Application Load Balancer 已轉寄至 AWS WAF 典型的 Web 請求範例。
6. 如果您認為規則正在攔截您不希望攔截的請求，請變更設定。如需詳細資訊，請參閱 建立和設定 Web 存取控制清單 (Web ACL)。

   當您對所有規則都能攔截到正確請求感到滿意時，請將每個規則的操作更改為允許或封鎖。如需詳細資訊，請參閱 編輯 Web ACL。

檢視 API Gateway CloudFront 或 Application Load Balancer 已轉寄至 AWS WAF 典型的 Web 請求範例

在 AWS WAF 典型主控台中，您可以檢視 API Gateway CloudFront 或 Application Load Balancer 已轉寄至 AWS WAF 典型進行檢查的要求範例。對於每個抽樣請求，您可以查看請求的詳細資料，例如源於的 IP 地址和包含在請求中的標頭。您也可以檢視請求符合的規則、規則是否有正確設定以用於允許或封鎖請求。

請求樣本最多含有 100 個請求符合所有條件中的每個規則中，以及另外 100 個預設動作的請求，這些請求適用於不符合所有條件中的任何規則。範例中的要求來自過去 15 分鐘內收到內容要求的所有 API Gateway API、 CloudFront 節點或應用程式負載平衡器。

檢視 API Gateway 的 Web 要求範例； CloudFront 或 Application Load Balancer 已轉寄至 AWS WAF 傳統版

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中，選擇您要檢視的 Web ACL 請求。
3. 在右窗格中，選擇請求標籤。

   抽樣請求 表為每個請求顯示以下的值：

來源 IP

要求來源的 IP 位址，或者 (如果檢視者使用 HTTP Proxy 或 Application Load Balancer 器傳送要求) Proxy 或 Application Load Balancer 器的 IP 位址。

URI

請求的 URI 路徑，用於識別資源，例如`/images/daily-ad.jpg`。這不包括 URI 的查詢字串或片段元件。如需詳細資訊，請參閱統一資源識別元 (URI)：一般語法。

比對規則

識別 web 請求中符合所有 Web ACL 條件的中第一個規則。如果 web 請求不符合和所有 Web ACL 條件的規則，則 Matches rule (比對規則) 為預設。

請注意，當 Web 要求符合規則中的所有條件，且該規則的動作為「計數」時，C AWS WAF lassic 會繼續根據 Web ACL 中的後續規則檢查 Web 要求。在這種情況下，web 請求可能會在抽樣請求名單上出現兩次：一次因為規則操作 Count (計數) 的動作，並再次在後續規則或預設動作操作。

動作

指出動作對應的規則為允許、封鎖 或 Count (計數)。

時間

AWS WAF 典型從 API Gateway CloudFront 或 Application Load Balancer 接收要求的時間。

4. 若要顯示有關要求的其他資訊，請選擇該要求之 IP 位址左側的箭頭。 AWS WAF 「典型」會顯示下列資訊：

來源 IP

相同的 IP 地址做為表格中來源 IP欄的值。

Country

請求源自國家的雙字母國家/地區代碼。如果檢視器使用 HTTP Proxy 或 Application Load Balancer 器傳送要求，則這是 HTTP Proxy 或 Application Load Balancer 器所在國家/地區的兩個字母國碼。

如需雙字母國家/地區代碼對應的國家/地區名稱，請參閱 Wikipedia 項目 ISO 3166-1 alpha-2。

方法

HTTP 請求方法的請求：GET、HEAD、OPTIONS、PUT、POST、PATCH 或 DELETE。

URI

相同的 URI 做為表格中來源 IP欄的值。

請求標頭

請求的標頭和請求的標頭值。

5. 若要重新整理範例清單，選擇Get new samples (取得新的範例)。

使用 AWS WAF 傳統規則群組以搭配使用 AWS Firewall Manager

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

AWS WAF 傳統規則群組是您新增至 AWS WAF 傳統原則的一組規 AWS Firewall Manager 則。您可以建立自己的規則群組，也可以從中購買受管規則群組 AWS Marketplace。

> **Important**
>
> 如果您想要將 AWS Marketplace 規則群組新增至您的 Firewall Manager 策略，組織中的每個帳戶都必須先訂閱該規則群組。所有帳戶都已完成訂閱後，您就可以將規則群組新增至政策。如需更多詳細資訊，請參閱 AWS Marketplace 規則群組。

主題

- 建立 AWS WAF 傳統規則群組
- 從 AWS WAF 傳統規則群組新增和刪除規則

建立 AWS WAF 傳統規則群組

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

當您建立要搭配使用的 AWS WAF 傳統規則群組時 AWS Firewall Manager，您可以指定要新增至群組的規則。

建立規則群組 (主控台)

1. AWS Management Console 使用您在必要條件中設定的 AWS Firewall Manager 系統管理員帳戶登入，然後在開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fms。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 步驟 2：建立 AWS Firewall Manager 預設的管理員帳戶。

2. 在導覽窗格中，選擇 [切換至 AWS WAF 典型]。
3. 在 [AWS WAF 傳統] 功能窗格中，選擇 [規則群組]。
4. 選擇 建立規則群組。

   > **Note**
   >
   > 您不能將以速率為基礎的規則新增至規則群組中。

5. 如果您已建立了希望新增至規則群組的規則，選擇 Use existing rules for this rule group (對此規則群組使用現有的規則)。如果您要建立新規則以新增到群組中，選擇 Create rules and conditions for this rule group (為此規則群組建立規則和條件)。
6. 選擇下一步。
7. 如果您選擇建立規則，請遵循 建立規則和新增條件 的步驟來建立規則。

> **Note**
>
> 使用「 AWS WAF 典型」主控台建立規則。

建立所有需要的規則後，請移至下一個步驟。

8. 輸入規群組則名稱。
9. 若要新增規則至規則群組，請選取規則，然後選擇 Add rule (新增規則)。選擇是否允許、封鎖或計數符合規則條件的請求。如需選項的詳細資訊，請參閱AWS WAF 經典如何運作。
10. 完成規則新增作業時，選擇 Create (建立)。

您可以測試規則群組，方法是將規則群組新增至 AWS WAF WebACL，並將 WebACL 動作設定為「覆寫為計數」。此動作會覆寫您為群組中規則選擇的任何動作，且只會計數符合的請求。如需更多詳細資訊，請參閱 建立 Web ACL。

從 AWS WAF 傳統規則群組新增和刪除規則

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和網頁等 AWS WAF 資源ACLs，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

您可以在「 AWS WAF 典型」規則群組中新增或刪除規則。

刪除規則群組裡的規則，並不刪除規則本身。它只會移除規則群組裡的規則。

新增或刪除規則群組裡的規則 (主控台)。

1. AWS Management Console 使用您在必要條件中設定的 AWS Firewall Manager 系統管理員帳戶登入，然後在開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fms。

> **Note**
>
> 如需建立防火牆管理員帳戶的詳細資訊，請參閱 步驟 2：建立 AWS Firewall Manager 預設的管理員帳戶。

2. 在導覽窗格中，選擇 [切換至 AWS WAF 典型]。
3. 在 [AWS WAF 傳統] 功能窗格中，選擇 [規則群組]。
4. 選擇您要編輯的規則群組。

> **Note**
>
> 如果您沒有看到要編輯的規則群組，請確定已選取正確的區域。對於用於保護 Amazon CloudFront 分發的規則群組，請使用全域 (CloudFront) 設定。

5. 選擇編輯規則群組。
6. 若要新增規則，請執行以下步驟：

   a. 選取一個規則，然後選擇Add rule to rule group (新增規則至規則群組)。選擇是否允許、封鎖或計數符合規則條件的請求。如需選項的詳細資訊，請參閱AWS WAF 經典如何運作。重複，以新增更多規則至規則群組。

   > **Note**
   >
   > 您不能將以速率為基礎的規則新增至規則群組中。

   b. 選擇更新。
7. 若要刪除規則，請執行以下步驟：

   a. 在您要刪除的規則旁，選擇 X。重複，以刪除更多規則群組裡的規則。

   b. 選擇更新。

開始啟 AWS Firewall Manager 用 AWS WAF 傳統規則

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

您可以使用 AWS Firewall Manager 來啟用 AWS WAF 規則、 AWS WAF 傳統規則、 AWS Shield Advanced 保護和 Amazon VPC 安全群組。每個開始設定的步驟稍微不同。

- 如果要使用 Firewall Manager 員啟用使用最新版本的規則 AWS WAF，請勿使用此主題。反之，請依照開始使用 AWS Firewall ManagerAWS WAF 政策中的步驟進行。
- 如果要使用 Firewall Manager 員啟用防 AWS Shield Advanced 護，請遵循中開始使用 AWS Firewall ManagerAWS Shield Advanced 政策的步驟。
- 若要使用 Firewall Manager 員啟用 Amazon VPC 安全群組，請遵循中開始使用 AWS Firewall Manager Amazon VPC 安全群組政策的步驟。

若要使用 Firewall Manager 員啟用 AWS WAF 典型規則，請依序執行下列步驟。

主題

步驟 1：完成先決條件

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。

如需的最新版本 AWS WAF，請參閱AWS WAF。

為 AWS Firewall Manager準備您的帳戶有幾個必要的步驟。AWS Firewall Manager 前提 說明這些步驟。先完成所有的先決條件，再進行 步驟 2：建立規則。

步驟 2：建立規則

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

在此步驟中，您可以使用「 AWS WAF 傳統」建立規則。如果您已有要搭配使用的 AWS WAF 傳統規則 AWS Firewall Manager，請略過此步驟並移至步驟 3：建立規則群組。

> **Note**
>
> 使用「 AWS WAF 典型」主控台建立規則。

若要建立 AWS WAF 傳統規則 (主控台)

- 建立您的規則，然後將您的條件新增至您的規則。如需詳細資訊，請參閱 建立規則和新增條件。

您現在可以前往步驟 3：建立規則群組。

步驟 3：建立規則群組

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。

如需的最新版本 AWS WAF，請參閱AWS WAF。

規則群組是一組規則的集合，定義當滿足特定條件時該採取的動作。您可以從中使用受管規則群組 AWS Marketplace，也可以建立自己的規則群組。如需受管規則群組的相關資訊，請參閱 AWS Marketplace 規則群組。

若要建立自己的安全群組，請執行下列程序。

建立規則群組 (主控台)

1. AWS Management Console 使用您在必要條件中設定的 AWS Firewall Manager 系統管理員帳戶登入，然後在開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fms。
2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 如果您不符合先決條件，主控台會顯示修復問題的相關說明。遵循指示，然後再度開始此步驟 (建立規則群組)。如果您已滿足先決條件，選擇關閉。
4. 選擇建立政策。

   針對 Policy type (政策類型)，選擇 AWS WAF Classic。
5. 選擇 [建立 AWS Firewall Manager 原則] 並新增規則群組。
6. 選擇一個 AWS 區域，然後選擇 [下一步]。
7. 由於您已建立的規則，所以您無需建立條件。選擇下一步。
8. 由於您已建立的規則，所以您無需建立規則。選擇下一步。
9. 選擇 建立規則群組。
10. 在 Name (名稱) 中，輸入易記的名稱。
11. 輸入「 AWS WAF 典型」將建立並與規則群組產生關聯的 CloudWatch 測量結果名稱。名稱僅能含有英數字元 (A-Z、a-z、0-9) 或以下特殊字元：_-!"#`+*},./。不能含有空格。
12. 選取一個規則，然後選擇新增規則。規則有動作設定，可讓您選擇是否允許、封鎖或計數符合規則條件的請求。在此教學課程，請選擇計數。重複新增規則，直到您已新增完所有想要新贈至規則群組的規則。
13. 選擇建立。

您現在可以前往步驟 4：建立並套用 AWS Firewall ManagerAWS WAF 傳統原則。

步驟 4：建立並套用 AWS Firewall ManagerAWS WAF 傳統原則

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

建立規則群組之後，即可建立 AWS Firewall Manager AWS WAF 原則。Firewall Manager 員 AWS WAF 策略包含您要套用至資源的規則群組。

建立 Firewall Manager 員 AWS WAF 策略（主控台）

1. 在您建立規則群組後 (上一個程序的最後一個步驟，步驟 3：建立規則群組) 主控台會顯示 Rule group summary (規則群組摘要) 頁面。選擇下一步。
2. 在 Name (名稱) 中，輸入易記的名稱。
3. 針對政策類型，選擇 WAF。
4. 在「區域」中，選擇一個 AWS 區域。若要保護 Amazon CloudFront 資源，請選擇「全球」。

   若要保護多個區域 (資源除外) 中的 CloudFront 資源，您必須為每個區域建立個別的 Firewall Manager 員政策。
5. 選取要新增得規則群組，然後選擇新增規則群組。
6. 政策有兩種動作：規則群組這定的動作和計數。如果您想要測試政策和規則群組，設定動作為計數。這個動作覆寫任何由政策裡規則群組所指定的封鎖動作。也就是說，如果政策的動作是設定為計數，只會計算請求，而不會封鎖請求。反之，如果您設定政策的動作為規則群組這定的動作，則會使用該政策裡規則群組的動作。在此教學課程，請選擇計數。
7. 選擇下一步。
8. 如果您想要在政策中只包含特定帳戶、或在政策中排除特定帳戶，請選取 Select accounts to include/exclude from this policy (optional) (選擇此政策要包含/排除的帳戶選用)。選擇在此政策中只包含這些帳戶或在此政策中排除這些帳戶。您只可以選擇一個選項。選擇新增。選取要包含或排除的帳戶號碼，然後選擇 OK。

> **Note**
>
> 如果您未選取此選項，則 Firewall Manager 員會將策略套用至組織中的所有帳號 AWS Organizations。如果您將新帳號新增至組織，Firewall Manager 員會自動將策略套用至該帳號。

9. 選擇您要保護的資源類型。
10. 如果您只想保護具有特定標籤的資源，或排除具有特定標籤的資源，請選擇 Use tags to include/exclude resources (使用標籤包含/排除資源)，輸入標籤的類型，然後選擇包含或排除。您只可以選擇一個選項。

    如果您輸入多個標籤 (以逗號分隔)，且如果資源擁有其中任一的標籤，都會被視為符合條件。

    如需標籤的詳細資訊，請參閱使用標籤編輯器。
11. 選擇建立和套用此政策到現有的和新的資源。

    此選項會在組織中的每個適用帳戶中建立 Web ACL AWS Organizations，並將 Web ACL 與帳號中的指定資源相關聯。此選項還會將政策套用到與前述條件 (資源類型和標籤) 符合的所有新的資源。或者，如果您選擇 [建立] 但不將此策略套用至現有或新資源，則 Firewall Manager 會在組織內的每個適用帳戶中建立 Web ACL，但不會將 Web ACL 套用至任何資源。之後，您必須將政策套用到資源。
12. 在預設設定中保留 [取代現有關聯的 Web ACL] 的選擇。

    選取此選項時，Firewall Manager 員會先從範圍內的資源移除所有現有的 Web ACL 關聯，然後再將新原則的 Web ACL 關聯與它們建立關聯。
13. 選擇下一步。
14. 檢視新政策。若要修改，選擇編輯。當您滿意時，選擇 建立政策。

教學課程：使用階層規則建立 AWS Firewall Manager政策

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。

如需的最新版本 AWS WAF，請參閱AWS WAF。

使用 AWS Firewall Manager，您可以建立並套用包含階層式規則的 AWS WAF 傳統保護原則。也就是，您可以集中建立並強制執行特定規則，但將帳戶專屬規則的建立和維護作業委派給其他個人。您可以監控集中套用 (通用) 的任何意外刪除或錯誤處理規則，因此可確保一致地套用這些規則。帳戶專屬規則可新增針對個別團隊需求自訂的進一步防護。

> **Note**
>
> 在的最新版本中 AWS WAF，此功能是內建的，不需要任何特殊處理。如果您尚未使用 AWS WAF 經典版，請改用最新版本。請參閱建立 AWS Firewall Manager 政策 AWS WAF。

下列教學課程說明如何建立防護規則的階層組。

主題

步驟 1：指定 Firewall Manager 員帳戶

若要使用 AWS Firewall Manager，您必須將組織中的帳戶指定為 Firewall Manager 員帳戶。此帳戶可以是組織中的管理帳戶或成員帳戶。

您可以使用 Firewall Manager 員管理員帳戶來建立一組套用至組織中其他帳戶的一般規則。組織中的其他帳戶無法變更集中套用的規則。

若要將帳戶指定為 Firewall Manager 員帳戶，並完成使用 Firewall Manager 員的其他必要條件，請參閱中的指示AWS Firewall Manager 前提。如果您已完成先決條件，則可以跳至此教學課程中的步驟 2。

在本教學課程中，我們將管理員帳戶稱為 **`Firewall-Administrator-Account`**。

步驟 2：使用 Firewall Manager 員管理員帳戶建立規則群組

接著，使用 **Firewall-Administrator-Account** 建立一個規則群組。此規則群組包含您將套用至所有成員帳戶的通用規則。這些成員帳戶是以您在下一步中建立的政策管理。僅 **Firewall-Administrator-Account** 可以變更這些規則和容器規則群組。

在本教學課程中，我們將此容器規則群組稱為 **Common-Rule-Group**。

若要建立規則群組，請參閱建立 AWS WAF 傳統規則群組中的說明。請記得在遵循這些指示時，使用您的 Firewall Manager 員管理員帳戶 (**Firewall-Administrator-Account**) 登入主控台。

步驟 3：建立 Firewall Manager 員原則並附加通用規則群組

使用**Firewall-Administrator-Account**，建立 Firewall Manager 員策略。建立此政策時，您必須執行下列作業：

- 新增 **Common-Rule-Group** 至新政策。
- 將組織內您想要套用 **Common-Rule-Group** 的所有帳戶納入。
- 新增您想要套用 **Common-Rule-Group** 的所有資源。

如需建立政策的說明，請參閱建立 AWS Firewall Manager 策略。

此會在各指定的帳戶中建立 web ACL，並將 **Common-Rule-Group** 新增至各 web ACL。建立政策後，此 web ACL 和通用規則便會部署至所有指定的帳戶。

在本教學課程中，我們將此 web ACL 稱為 **Administrator-Created-ACL**。唯一的 **Administrator-Created-ACL** 現在存在於組織中各個指定成員帳戶內。

步驟 4：新增帳戶專屬規則

組織中的各成員帳戶現在可以將自己的帳戶專屬規則新增至存在於其帳戶中的 **Administrator-Created-ACL**。已存在的一般規則會**Administrator-Created-ACL**繼續套用，以及新的帳戶特定規則。 AWS WAF 根據規則在 Web ACL 中出現的順序來檢查 Web 請求。這適用於 **Administrator-Created-ACL** 和帳戶專屬規則。

若要將規則新增至**Administrator-Created-ACL**，請參閱編輯網路 ACL。

結論

您現在有一個 Web ACL，其中包含由 Firewall Manager 員管理員帳戶管理的一般規則，以及每個成員帳戶所維護的帳戶特定規則。

各帳戶中的 **Administrator-Created-ACL** 參照單一 **Common-Rule-Group**。因此，Firewall Manager 員管理員帳戶 future 的變更**Common-Rule-Group**將立即在每個成員帳戶中生效。

會員帳戶無法變更或移除 **Common-Rule-Group** 中的通用規則。

帳戶專屬規則不會影響其他帳戶。

記錄 Web ACL 流量資訊

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

> **Note**
>
> 您無法使用 Amazon 安全湖來收集 AWS WAF 傳統資料。

您可以啟用日誌記錄取得您 Web ACL 分析流量的詳細資訊。記錄檔中包含的資訊包括 C AWS WAF lassic 從您的 AWS 資源接收要求的時間、有關請求的詳細資訊，以及每個要求相符之規則的動作。

開始請您先建立 Amazon Kinesis Data Firehose。您可以選擇存放日誌的目的地。然後，可以選擇要啟用記錄的 Web ACL。啟用記錄後，會透過 Firehose 將記錄 AWS WAF 傳送至您的儲存目的地。

如需如何建立 Amazon Kinesis 資料 Firehose 和檢閱儲存的日誌的相關資訊，請參閱什麼是亞馬遜資料防火管？ 若要瞭解 Kinesis Data Firehose 組態所需的許可，請參閱使用 Amazon Kinesis Data Firehose 控制存取。

您必須擁有以下權限，才能順利啟用記錄：

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `waf:PutLoggingConfiguration`

如需服務連結角色和 `iam:CreateServiceLinkedRole` 許可的詳細資訊，請參閱針 AWS WAF 對傳統使用服務連結角色。

啟用 Web ACL 記錄

1. 使用以字首為「aws-waf-logs-」開頭的名稱建立 Amazon Kinesis 資料防火管。例如，`aws-waf-logs-us-east-2-analytics`使用 PUT 來源以及您正在操作的區域建立資料 firehose。如果您要擷取 Amazon 的日誌 CloudFront，請在美國東部 (維吉尼亞北部) 建立 Firehose。如需詳細資訊，請參閱建立 Amazon 資料 Firehose 交付串流。

   > **Important**
   >
   > 請勿選擇 `Kinesis stream` 做為您的來源。
   > 一個 AWS WAF 經典日誌相當於一個 Firehose 記錄。如果您通常每秒收到 10,000 個請求，而且啟用了完整記錄，則 Firehose 中的每秒應該有 10,000 筆記錄設定。如果您沒有正確配置 Firehose， AWS WAF 經典版將不會記錄所有日誌。如需詳細資訊，請參閱 Amazon Kinesis Data Firehose 配額。

2. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。

3. 在導覽窗格中，選擇 Web ACL。
4. 選擇您要啟用記錄功能的 Web ACL 名稱。這會開啟右窗格中包含 Web ACL 詳細資訊的頁面。
5. 在記錄標籤中，選擇啟用記錄。
6. 選擇您在第一步驟建立的 Kinesis Data Firehose。您必須選擇以「aws-waf-logs-」開頭的防火喉。
7. (選用) 如果您不想要特定欄位及其值包含在日誌中，請編寫這些欄位。選擇要編寫的欄位，然後選擇新增。重複其他需要編寫的欄位。在日誌中編寫的欄位顯示為 `REDACTED`。例如，如果您編寫 Cookie 欄位，在日誌的 Cookie 欄位則會為 `REDACTED`。
8. 選擇 Enable Logging (啟用記錄日誌)。

> **Note**
>
> 當您成功啟用記錄時， AWS WAF 傳統會建立具有必要權限的服務連結角色，以便將日誌寫入 Amazon Kinesis Data Firehose。如需詳細資訊，請參閱 針 AWS WAF 對傳統使用服務連結角色。

停用 Web ACL 記錄

1. 在導覽窗格中，選擇 Web ACL。
2. 選擇您要停用記錄的 Web ACL 名稱。這會開啟右窗格中包含 Web ACL 詳細資訊的頁面。
3. 在記錄標籤中，選擇停用記錄。
4. 在對話方塊中，選擇停用記錄。

Example 範例日誌

```
{

 "timestamp":1533689070589,
 "formatVersion":1,
 "webaclId":"385cb038-3a6f-4f2f-ac64-09ab912af590",
 "terminatingRuleId":"Default_Action",
 "terminatingRuleType":"REGULAR",
 "action":"ALLOW",
 "httpSourceName":"CF",
 "httpSourceId":"i-123",
 "ruleGroupList":[
                         {
                          "ruleGroupId":"41f4eb08-4e1b-2985-92b5-e8abf434fad3",
                          "terminatingRule":null,
                          "nonTerminatingMatchingRules":[
                                                          {"action" : "COUNT",
                                                          "ruleId" :
 "4659b169-2083-4a91-bbd4-08851a9aaf74"}
                                                         ],
                          "excludedRules":               [
                                                          {"exclusionType" :
 "EXCLUDED_AS_COUNT",
```

```
                                                                  "ruleId" :
 "5432a230-0113-5b83-bbb2-89375c5bfa98"}
                                                               ]
                         }
                        ],

 "rateBasedRuleList":[
                             {
                              "rateBasedRuleId":"7c968ef6-32ec-4fee-96cc-51198e412e7f",

                              "limitKey":"IP",
                              "maxRateAllowed":100

                             },
                             {
                              "rateBasedRuleId":"462b169-2083-4a93-bbd4-08851a9aaf30",
                              "limitKey":"IP",
                              "maxRateAllowed":100
                              }
                              ],

 "nonTerminatingMatchingRules":[
                                       {"action" : "COUNT",

                                       "ruleId" : "4659b181-2011-4a91-
bbd4-08851a9aaf52"}
                                      ],

 "httpRequest":{
                      "clientIp":"192.10.23.23",

                      "country":"US",

                      "headers":[

                                 {
                                  "name":"Host",
                                  "value":"127.0.0.1:1989"
                                 },
                                 {
                                  "name":"User-Agent",
                                  "value":"curl/7.51.2"
                                 },
                                 {
```

```
                                    "name":"Accept",
                                    "value":"*/*"
                                  }
                                ],
                        "uri":"REDACTED",
                        "args":"usernam=abc",
                        "httpVersion":"HTTP/1.1",
                        "httpMethod":"GET",
                        "requestId":"cloud front Request id"
                        }
}
```

以下是這些日誌中所列項目的說明：

timestamp

時間戳記，以毫秒為單位。

formatVersion

日誌的格式版本。

webaclId

Web ACL 的 GUID。

terminatingRuleId

終止請求的規則 ID。如果無法終止請求，則值為 `Default_Action`。

terminatingRuleType

終止請求的規則類型。可能的值：RATE_BASED、REGULAR 及 GROUP。

動作

動作。終止規則可能的值：ALLOW 及 BLOCK。COUNT 並非終止規則的有效值。

terminatingRuleMatch詳情

符合請求之終止規則的詳細資訊。終止規則對 Web 請求具有結束檢查程序的動作。終止規則可能的動作是「允許」和「封鎖」。這只會為 SQL Injection 和跨網站指令碼 (XSS) 符合規則陳述式填入。與所有檢查多個項目的規則陳述式一樣， AWS WAF 會在第一個符合項目上套用動作，並停止檢查 Web 請求。具有終止動作的 Web 請求除了包含記錄中報告的威脅之外，還可能包含其他威脅。

httpSourceName

請求的來源。可能的值：CF (如果來源是亞馬遜 CloudFront)、APIGW (如果來源是 Amazon API 閘道) 和 ALB (如果來源是 Application Load Balancer)。

httpSourceId

來源 ID。此欄位顯示相關聯 Amazon CloudFront 分發的識別碼、API Gateway 的 REST API，或 Application Load Balancer 的名稱。

ruleGroupList

處理此請求的規則群組名單。前述程式碼範例僅有一個規則群組。

ruleGroupId

規則群組的 ID。若規則封鎖請求，則 `ruleGroupID` 的 ID 將與 `terminatingRuleId` 的 ID 相同。

terminatingRule

在規則群組中終止請求的規則。若此不是 null 值，則也包含 ruleid (ruleid) 和 action (動作)。在這種情況下，動作一律是 BLOCK。

nonTerminatingMatching規則

規則群組中符合請求的規則名單。這些一律是 COUNT 規則 (符合的非終止規則)。

動作 (nonTerminatingMatching規則群組)

這一律是 COUNT (符合的非終止規則)。

ruleId (nonTerminatingMatching規則群組)

在規則群組符合請求的規則 ID 為非終止的。也就是 COUNT (計數) 規則。

excludedRules

規則群組中已排除的規則清單。這些規則的動作設定為 COUNT。

exclusionType (excludedRules 群組)

此類型表示已排除的規則均具備動作 COUNT。

ruleId (excludedRules 群組)

在規則群組中被排除的規則 ID。

rateBasedRule清單

處理請求的以速率為基礎的規則名單。

rateBasedRule識別碼

處理請求的速率規則 ID。若此項目已終止請求，則 `rateBasedRuleId` 的 ID 將與 `terminatingRuleId` 的 ID 相同。

limitKey

AWS WAF 用來判斷要求是否可能來自單一來源，因此受到速率監控的欄位。可能的值：IP。

maxRateAllowed

五分鐘內允許的請求數量上限，此值與 `limitKey` 指定之欄位中的值相同。如果要求數目超過，`maxRateAllowed`而且也符合規則中指定的其他述詞，則會 AWS WAF 觸發針對此規則指定的動作。

httpRequest

請求的中繼資料。

clientIp

傳送請求的用戶端 IP 地址。

國家/地區

請求來源的國家/地區。如果 AWS WAF 無法確定原產國，則會將此欄位設定為-。

標頭

標題清單。

uri

URI 請求。前述程式碼範例說明此欄位經修訂後可能的值。

args

查詢字串。

httpVersion

HTTP 版本。

httpMethod

請求的 HTTP 方法。

requestId

請求的 ID。

以速度為基礎的規則列出封鎖的 IP 地址

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

AWS WAF 傳統會提供以速率為基礎的規則封鎖的 IP 位址清單。

檢視以速度為基礎的規則的地址

1. 請登入 AWS Management Console 並開啟 AWS WAF 主控台，網址為 https://console.aws.amazon.com/wafv2/。

   如果您在導覽窗格中看到 [切換到 AWS WAF 傳統]，請選取它。
2. 在導覽窗格中，選擇規則。
3. 在名稱 欄，選擇以速率為基礎的規則。

   此名單顯示規則目前封鎖的 IP 地址。

AWS WAF 經典版如何與 Amazon CloudFront 功能搭配

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

建立 Web ACL 時，您可以指定一個或多個要 AWS WAF 傳統檢查的 CloudFront 分佈。 AWS WAF 傳統版會根據您在 Web ACL 中識別的條件，開始允許、封鎖或計數這些散佈的 Web 要求。 CloudFront 提供了一些增強經 AWS WAF 典功能的功能。本章介紹了幾種可以配置CloudFront 為使 CloudFront 和 C AWS WAF lassic 一起更好地工作的方法。

主題

使用 AWS WAF 經典與 CloudFront 自定義錯誤頁面

當 AWS WAF 經典根據您指定的條件阻止 Web 請求時，它會將 HTTP 狀態碼 403（禁止）返回到 CloudFront。接下來，將該狀態碼 CloudFront 傳回給檢視器。檢視器然後會顯示與此相似的簡短且稀疏格式化的預設訊息：

```
Forbidden: You don't have permission to access /myfilename.html on this
server.
```

如果您想要顯示自訂錯誤訊息 (可能使用與網站其他部分相同的格式)，您可 CloudFront 以設定將包含您自訂錯誤訊息的物件 (例如 HTML 檔案) 傳回給檢視者。

> **Note**
>
> CloudFront 無法區分您的來源返回的 HTTP 狀態碼 403 和 C AWS WAF lassic 在請求被阻止時返回的 HTTP 狀態碼 403。這表示您無法根據不同原因導致 HTTP 狀態碼 403 而傳回不同的自訂錯誤頁面。

如需有關自 CloudFront 訂錯誤頁面的詳細資訊，請參閱 Amazon CloudFront 開發人員指南中的自訂錯誤回應。

CloudFront針對在您自己的 HTTP 伺服器上執行的應用程式使用 AWS WAF 典型

搭配使用 C AWS WAF lassic 時 CloudFront，您可以保護在任何 HTTP 網路伺服器上執行的應用程式，無論是在 Amazon 彈性運算雲端 (Amazon EC2) 中執行的網路伺服器，還是您私下管理的網路伺服器。您還可以配置 CloudFront 為在 CloudFront和您自己的網絡服務器之間以及查看者和 CloudFront.

在 CloudFront 與您自己的網絡服務器之間需要 HTTPS

要在 CloudFront 和您自己的網絡服務器之間要求 HTTPS，您可以使用自定 CloudFront 義來源功能並為特定來源配置原始協議策略和原始域名設置。在您的 CloudFront 配置中，您可以指定服務器的 DNS 名稱以及端口和從源獲取對象時 CloudFront 要使用的協議。您也應確保您自訂原始伺服器上的 SSL/TLS 憑證符合您已設定的原始伺服器的網域名稱。當您在以外的地方使用自己的 HTTP Web 伺服器時 AWS，您必須使用由受信任的第三方憑證授權單位 (CA) 簽署的憑證，例如 Comodo 或賽門鐵克。DigiCert如需需要 HTTPS 才能 CloudFront與您自己的網路伺服器之間進行通訊的詳細資訊，請參閱 Amazon CloudFront 開發人員指南中的〈需要 HTTPS 進行通訊〉主題。 CloudFront

在檢視器和檢視器之間需要 HTTPS CloudFront

若要在檢視器和之間要求 HTTPS CloudFront，您可以針對 CloudFront發行版中的一或多個快取行為變更檢視器通訊協定原則。如需有關 CloudFront在檢視者之間使用 HTTPS 的詳細資訊 CloudFront，請參閱 < 在檢視者之間需要 HTTPS 進行通訊 > 主題和 Amazon CloudFront 開發人員指南。您還可以攜帶自己的 SSL 證書，以便觀眾可以使用您自己的域名 CloudFront 通過 HTTPS 連接到您的分發，例如 https://www.mysite.com。如需詳細資訊，請參閱 Amazon CloudFront 開發人員指南中的設定替代網域名稱和 HTTPS 主題。

選擇可 CloudFront回應的 HTTP 方法

當您建立 Amazon CloudFront 網路分發時，您可 CloudFront 以選擇要處理的 HTTP 方法並轉寄到原始伺服器。您可以從下列選項來選擇：

- GET，HEAD — 您 CloudFront 只能使用來從您的來源獲取對象或獲取對象標題。
- GET、HEAD、OPTI ONS — 您 CloudFront 只能使用從原始伺服器取得物件、取得物件標頭，或擷取原始伺服器支援的選項清單。
- 取得、標頭、選項、PUT、POST、修補程式、刪除 — 您可以使用 CloudFront 來取得、新增、更新和刪除物件，以及取得物件標頭。此外，您可以執行其他 POST 操作，例如從 Web 表單提交資料。

您也可以使用 AWS WAF 傳統字串比對條件，根據 HTTP 方法允許或封鎖要求，如中所述使用字串比對條件。如果您想要使用 CloudFront 支援的方法組合，例如GET和HEAD，則不需要將 C AWS WAF lassic 設定為封鎖使用其他方法的要求。如果您想要允許 CloudFront 不支援的方法組合，例如、和 GET HEADPOST，您可以設定 CloudFront 為回應所有方法，然後使用 C AWS WAF lassic 封鎖使用其他方法的要求。

如需有關選擇可 CloudFront 回應之方法的詳細資訊，請參閱 Amazon CloudFront 開發人員指南中建立或更新 Web 分發時指定的值主題中的允許的 HTTP 方法。

AWS WAF 經典中的安全性

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同承擔的責任。共同責任模型 將此描述為雲端的安全和雲端內的安全：

- 雲端安全性 — AWS 負責保護中執行 AWS 服務的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。第三方稽核人員定期檢測及驗證安全的效率也是我們 AWS 合規計劃的一部分。若要瞭解適用於「 AWS WAF 典型」的規範遵循計劃，請參閱合規計劃範圍內的AWS 服務。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對資料敏感度、組織要求，以及適用法律和法規等其他因素負責。

本文件可協助您瞭解如何在使用 AWS WAF 傳統版時套用共同的責任模型。下列主題說明如何設定「 AWS WAF 典型」，以符合您的安全性與合規性目標。您也會學到如何使用其他可 AWS 協助您監控和保護 AWS WAF 經典資源的服務。

主題

AWS WAF 傳統版中的資料保護

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和網頁等 AWS WAF 資源ACLs，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

AWS 共同責任模型適用於 AWS WAF 傳統中的資料保護。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需有關資料隱私權的詳細資訊，請參閱資料隱私權FAQ。 如需歐洲資料保護的相關資訊，請參閱AWS 安全性GDPR部落格上的AWS 共同責任模型和部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 認證並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 對每個帳戶使用多重要素驗證 (MFA)。
- 使用SSL/TLS與 AWS 資源溝通。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 使用設定API和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果 AWS 透過命令列介面或存取時需要 FIPS 140-3 驗證的密碼編譯模組API，請使用端點。FIPS 如需有關可用FIPS端點的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用主控台、、API或 AWS 服務 使用「 AWS WAF 經典」或其他工作時 AWS SDKs。 AWS CLI您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供URL給外部伺服器，我們強烈建議您不要在中包含認證資訊，URL以驗證您對該伺服器的要求。

AWS WAF 傳統實體 (例如網頁ACLs、規則和條件) 會在靜態時加密，但在某些無法使用加密的區域，包括中國 (北京) 和中國 (寧夏)。每個區域都會採用唯一的加密金鑰。

刪除 AWS WAF 典型資源

您可以刪除在「 AWS WAF 傳統」中建立的資源。請參閱以下各節中每種資源類型的指引。

- 刪除網頁 ACL
- 從 AWS WAF 傳統規則群組新增和刪除規則
- 刪除規則

AWS WAF 傳統版的身分識別與存取管理

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和網頁等 AWS WAF 資源ACLs，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM系統管理員控制誰可以驗證 (登入) 和授權 (有權限) 使用 AWS WAF 傳統資源。IAM是一種您 AWS 服務 可以使用，無需額外費用。

主題

- 物件
- 使用身分驗證
- 使用政策管理存取權
- AWS WAF 經典如何搭配使用 IAM
- 傳統版的身分識別型原則範例 AWS WAF
- 疑難排解 AWS WAF 傳統身分和存取
- 針 AWS WAF 對傳統使用服務連結角色

物件

根據您在 C AWS WAF lassic 中執行的工作，使用方式 AWS Identity and Access Management (IAM) 會有所不同。

服務使用者 — 如果您使用 C AWS WAF lassic 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 AWS WAF 經典功能來完成工作時，您可能需要額外的權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取「 AWS WAF 典型」中的功能，請參閱疑難排解 AWS WAF 傳統身分和存取。

服務管理員 — 如果您負責公司的 C AWS WAF lassic 資源，您可能擁有完整的 AWS WAF 經典存取權。決定您的服務使用者應該存取哪些 C AWS WAF lassic 功能和資源是您的工作。然後，您必須向IAM管理員提交請求，才能變更服務使用者的權限。檢閱此頁面上的資訊，以瞭解的基本概念IAM。若要深入瞭解貴公司如何IAM搭配 C AWS WAF lassic 使用，請參閱AWS WAF 經典如何搭配使用 IAM。

IAM系統管理員 — 如果您是IAM系統管理員，您可能想要瞭解如何撰寫原則來管理 C AWS WAF lassic 存取權的詳細資訊。若要檢視可在中使用的 AWS WAF 傳統身分型原則範例IAM，請參閱。傳統版的身分識別型原則範例 AWS WAF

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以IAM使用者身分或假設IAM角色來驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM身分識別中心) 使用者、貴公司的單一登入驗證，以及您的 Google 或 Facebook 認證都是聯合身分識別的範例。當您以同盟身分登入時，您的管理員先前會使用IAM角色設定聯合身分識別。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以密碼編譯方式簽署您的要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署要求的詳細資訊，請參閱使用IAM者指南中的簽署 AWS API要求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。若要深入瞭解，請參閱使用AWS IAM Identity Center 者指南中的多重要素驗證和使用多重要素驗證 (MFA) AWS的使用IAM者指南。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由

根使用者執行的任務。如需需要您以 root 使用者身分登入的完整工作清單，請參閱《使用指南》中的〈需要 root 使用者認證的IAM工作〉。

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步處理至您自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需IAM身分識別中心的相關資訊，請參閱IAM識別中心是什麼？ 在《AWS IAM Identity Center 使用者指南》中。

IAM 使用者和群組

IAM使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定權限。在可能的情況下，我們建議您仰賴臨時登入資料，而不要建立具有長期認證 (例如密碼和存取金鑰) 的IAM使用者。不過，如果您的特定使用案例需要使用IAM者的長期認證，建議您輪換存取金鑰。如需詳細資訊，請參閱《使用指南》中的「IAM定期輪換存取金鑰」以瞭解需要長期認證的使用案例。

IAM群組是指定IAM使用者集合的身分識別。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為的群組，IAMAdmins並授與該群組管理IAM資源的權限。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。要了解更多信息，請參閱《IAM用戶指南》中的創建用戶（而不是角色）的IAM時間。

IAM角色

IAM角色是您 AWS 帳戶 中具有特定權限的身份。它類似於用IAM戶，但不與特定人員相關聯。您可以 AWS Management Console 透過切換角色來暫時擔任中的角色。IAM您可以透過呼叫 AWS CLI 或 AWS API作業或使用自訂來擔任角色URL。如需有關使用角色方法的詳細資訊，請參閱《使用指南》中的IAM〈使用IAM角色〉。

IAM具有臨時認證的角色在下列情況下很有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱《使用指南》中的〈建立第三方身分識別提供IAM者的角色〉。如果您使用IAM身分識別中心，則需要設定權限集。為了控制身分驗證後可以存取的內IAM容，IAMIdentity Center 會將權限集與中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時IAM使用者權限 — IAM 使用者或角色可以假定某個IAM角色，暫時取得特定工作的不同權限。
- 跨帳戶存取 — 您可以使用IAM角色允許不同帳戶中的某個人 (受信任的主體) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要瞭解跨帳戶存取角色與以資源為基礎的政策之間的差異，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或將物件存放在 Amazon S3 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用使用IAM者或角色執行中的動作時 AWS，您會被視為主參與者。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。
  - 服務角色 — 服務角色是指服務代表您執行動作所代表的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。
- 在 Amazon 上執行的應用程式 EC2 — 您可以使用IAM角色來管理在執行個體上EC2執行的應用程式以及發出 AWS CLI 或 AWS API請求的臨時登入資料。這比在EC2執行個體中儲存存取金鑰更可取。若要將 AWS 角色指派給EC2執行個體並讓其所有應用程式都能使用，請建立附加至執行個體的執行個體設定檔。執行個體設定檔包含角色，可讓執行個體上EC2執行的程式取得臨時登入資料。如需詳細資訊，請參閱使用者指南中的使用IAM角色將許可授與在 Amazon EC2 執行個體上執行的應IAM用程式。

要了解是否使用IAM角色還是用IAM戶，請參閱《用戶指南》中的「IAM創建IAM角色的時機（而不是用戶）」。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以JSON文件的形式儲存在中。如需有關JSON原則文件結構和內容的詳細資訊，請參閱《IAM使用指南》中的策略概觀。JSON

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

IAM原則會定義動作的權限，不論您用來執行作業的方法為何。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或取得角色資訊 AWS API。

身分型政策

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管策略或內嵌策略之間進行選擇，請參閱《IAM使用手冊》中的「在受管策略和內嵌策略之間進行選擇」。

資源型政策

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的策略IAM中使用 AWS 受管政策。

存取控制清單 (ACLs)

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

Amazon S3 和 Amazon VPC 是支持服務的示例ACLs。 AWS WAF若要進一步了解ACLs，請參閱 Amazon 簡單儲存服務開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 權限界限 — 權限界限是一項進階功能，您可以在其中設定以身分識別為基礎的原則可授與給IAM實體 (IAM使用者或角色) 的最大權限。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需有關權限界限的詳細資訊，請參閱《IAM使用指南》中的IAM實體的權限界限。
- 服務控制策略 (SCPs) — SCPs 是指定中組織或組織單位 (OU) 最大權限的JSON策略 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。如果您啟用組織中的所有功能，則可以將服務控制策略 (SCPs) 套用至您的任何或所有帳戶。SCP限制成員帳戶中實體的權限，包括每個帳戶 AWS 帳戶根使用者。如需有關 Organizations 的詳細資訊SCPs，請參閱AWS Organizations 使用指南中的服務控制原則。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱《IAM使用指南》中的工作階段原則。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要瞭解如何在涉及多個原則類型時 AWS 決定是否允許要求，請參閱IAM使用指南中的原則評估邏輯。

AWS WAF 經典如何搭配使用 IAM

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和網頁等 AWS WAF 資源ACLs，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。

如需的最新版本 AWS WAF，請參閱AWS WAF。

在您用IAM來管理 AWS WAF 經典版的存取權限之前，請先瞭解哪些IAM功能可與 AWS WAF 傳統搭配使用。

IAM您可以與 AWS WAF 經典搭配使用的功能

IAM特徵	AWS WAF 經典支持
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	是
ACLs	否
ABAC(策略中的標籤)	部分
暫時性憑證	是
轉寄存取工作階段 (FAS)	是
服務角色	是
服務連結角色	是

若要取得 C AWS WAF lassic 和其他 AWS 服務如何搭配大部分IAM功能運作的高階檢視，請參閱IAM使用者指南IAM中的使用AWS 服務。

傳統版的身分識別型原則 AWS WAF

支援身分型政策：是

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

使用以IAM身分識別為基礎的策略，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。若要瞭解可在JSON策略中使用的所有元素，請參閱《使用IAM者指南》中的IAMJSON策略元素參考資料。

若要檢視 AWS WAF 傳統身分型原則的範例，請參閱。傳統版的身分識別型原則範例 AWS WAF

傳統內 AWS WAF 的資源型政策

支援資源型政策：否

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

若要啟用跨帳戶存取，您可以在以資源為基礎的策略中指定一個或多個帳戶中的一個或多個帳戶中的IAM實體作為主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主參與者和資源不同時 AWS 帳戶，受信任帳戶中的IAM管理員也必須授與主參與者實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。

AWS WAF 傳統版的政策動作

支援政策動作：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON策略`Action`元素描述了您可以用來允許或拒絕策略中存取的動作。策略動作通常與關聯 AWS API操作具有相同的名稱。有一些例外情況，例如沒有匹配API操作的僅限權限的操作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 AWS WAF 傳統動作清單，請參閱服務授權參考中由區域定義的動作 AWS WAF和 AWS WAF 區域定義的動作。

「 AWS WAF 傳統」中的原則動作會在動作之前使用下列前置詞：

```
waf
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "waf:action1",
      "waf:action2"
         ]
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定「 AWS WAF 傳統」中以開頭的所有動作List，請包含下列動作：

```
"Action": "waf:List*"
```

若要檢視 AWS WAF 傳統身分型原則的範例，請參閱。傳統版的身分識別型原則範例 AWS WAF

AWS WAF 傳統版的政策資源

支援政策資源：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

ResourceJSON原則元素會指定要套用動作的一個或多個物件。陳述式必須包含 Resource 或 NotResource 元素。最佳做法是使用其 Amazon 資源名稱 (ARN) 指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看 AWS WAF 傳統資源類型及其清單ARNs，請參閱服務授權參考中由定義的資源 AWS WAF與 AWS WAF 區域定義的資源。若要瞭解您可以針對每個資源指定哪些動作，請參閱由定義ARN的動作

AWS WAF與 AWS WAF 區域定義的動作。若要允許或拒絕存取 C AWS WAF lassic 資源子集，請在策略ARN的`resource`元素中包含資源的資源。

在 AWS WAF 經典中，資源是 Web ACLs 和規則。 AWS WAF 典型還支持諸如字節匹配，IP 匹配和大小約束之類的條件。

這些資源和條件具有與其關聯的唯一 Amazon 資源名稱 (ARNs)，如下表所示。

AWS WAF 主控台中的名稱	姓名 AWS WAF SDK/CLI	ARN格式
網頁 ACL	`WebACL`	`arn:aws:waf:: account:webacl/ID`
規則	`Rule`	`arn:aws:waf:: account:rule/ID`
字串比對條件	`ByteMatchSet`	`arn:aws:waf:: account:bytematchset /ID`
SQL注射匹配條件	`SqlInjectionMatchSet`	`arn:aws:waf:: account:sqlinjectionset /ID`
容量限制條件	`SizeConstraintSet`	`arn:aws:waf:: account:sizeconstraintset /ID`
IP 符合條件	`IPSet`	`arn:aws:waf:: account:ipset/ID`
跨網站指令碼比對條件	`XssMatchSet`	`arn:aws:waf:: account:xssmatchset /ID`

若要允許或拒絕存取 C AWS WAF lassic 資源子集，請在策略ARN的`resource`元素中包含資源的資源。對ARNs於 AWS WAF 經典具有以下格式：

```
arn:aws:waf::account:resource/ID
```

更換 *account*, *resource* 和 *ID* 具有有效值的變量。有效值如下：

- *account*：您的識別碼 AWS 帳戶。您必須指定一個數值。
- *resource*： AWS WAF 傳統資源的類型。

- *ID*： AWS WAF 傳統資源的 ID，或萬用字元 (*)，表示與指定之相關聯之指定類型的所有資源 AWS 帳戶。

例如，下列ARN指定帳戶ACLs的所有網頁111122223333：

```
arn:aws:waf::111122223333:webacl/*
```

AWS WAF 傳統版的政策條件索引鍵

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，只有在IAM使用者名稱標記資源時，您才可以授與IAM使用者存取資源的權限。如需詳細資訊，請參閱《IAM使用指南》中的IAM政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《使用指南》中的AWS 全域條件內IAM容索引鍵。

若要查看 AWS WAF 傳統條件金鑰清單，請參閱服務授權參考資料中的 [區域] 的條件索引鍵 AWS WAF和由 [AWS WAF 區域定義的資源]。若要瞭解您可以使用條件索引鍵的動作和資源，請參閱區域定義的動作 AWS WAF與由 AWS WAF區域定義的動作。

若要檢視 AWS WAF 傳統身分型原則的範例，請參閱。傳統版的身分識別型原則範例 AWS WAF

ACLs在 AWS WAF 經典

支持ACLs：無

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

ABAC與 AWS WAF 經典

支援 ABAC (策略中的標籤): 部分

以屬性為基礎的存取控制 (ABAC) 是一種授權策略，可根據屬性定義權限。在中 AWS，這些屬性稱為標籤。您可以將標籤附加至IAM實體 (使用者或角色) 和許多 AWS 資源。標記實體和資源是的第一步ABAC。然後，您可以設計ABAC策略，以便在主參與者的標籤與他們嘗試存取的資源上的標籤相符時允許作業。

ABAC在快速成長的環境中很有幫助，並且有助於原則管理變得繁瑣的情況。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需有關的詳細資訊ABAC，請參閱什麼是ABAC？ 在《IAM使用者指南》中。若要檢視包含設定步驟的自學課程ABAC，請參閱《使用指南》中的〈使用以屬性為基礎的存取控制 (ABAC) IAM 〉。

搭配 AWS WAF 典型使用臨時認證

支援臨時憑證：是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配使用 AWS 服務 ，請參閱《IAM使用指南》IAM中的使用方式。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立臨時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需有關切換角色的詳細資訊，請參閱《IAM使用者指南》中的〈切換到角色 (主控台)〉。

您可以使用 AWS CLI 或手動建立臨時認證 AWS API。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱IAM。

AWS WAF 傳統的轉寄存取工作階段

支援轉寄存取工作階段 (FAS)：是

當您使用使用IAM者或角色在中執行動作時 AWS，您會被視為主參與者。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS會使用主參與者呼叫的權限 AWS 服務，並結

合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。

AWS WAF 傳統版的服務角色

支援服務角色：是

服務角色是服務假定代表您執行動作的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給

> **Warning**
>
> 變更服務角色的權限可能會中斷 AWS WAF 傳統功能。只有在 AWS WAF 傳統提供指引時，才編輯服務角色。

傳統版的 AWS WAF 服務連結角色

支援服務連結角色：是

服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。

如需有關建立或管理 AWS WAF 傳統服務連結角色的詳細資訊，請參閱針 AWS WAF 對傳統使用服務連結角色。

傳統版的身分識別型原則範例 AWS WAF

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

依預設，使用者和角色沒有建立或修改 AWS WAF 傳統資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授

予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

如需 C AWS WAF lassic 定義的動作和資源類型的詳細資訊，包括每個資源類型的 ARN 格式，請參閱服務授權參考中地區的動作、資源 AWS WAF和條件索引鍵以及 AWS WAF 地區的動作、資源和條件索引鍵。

主題

- 政策最佳實務
- 使用傳 AWS WAF 統主控台
- 允許使用者檢視他們自己的許可

政策最佳實務

以身分識別為基礎的政策會決定某人是否可以建立、存取或刪除您帳戶中的 AWS WAF 傳統資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需更多資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。

- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

使用傳 AWS WAF 統主控台

若要存取 AWS WAF 典型主控台，您必須擁有最少一組權限。這些權限必須允許您列出和檢視有關 AWS 帳戶. AWS WAF 如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

可以存取和使用 AWS 主控台的使用者也可以存取 AWS WAF 典型主控台。不需要額外許可。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
```

```
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

疑難排解 AWS WAF 傳統身分和存取

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

使用下列資訊可協助您診斷並修正使用 AWS WAF 典型和 IAM 時可能會遇到的常見問題。

主題

- 我沒有在 AWS WAF 經典版中執行動作的授權
- 我沒有授權執行 iam：PassRole
- 我想允許我以外的人訪問我 AWS 帳戶 的 AWS WAF 經典資源

我沒有在 AWS WAF 經典版中執行動作的授權

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在`mateojackson` IAM 使用者嘗試使用主控台檢視一個虛構 *`my-example-widget`* 資源的詳細資訊，但卻無虛構 `waf:`*`GetWidget`* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 waf:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 waf:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我沒有授權執行 iam：PassRole

如果您收到未獲授權執行iam:PassRole動作的錯誤訊息，則必須更新您的原則，才能將角色傳遞給「傳 AWS WAF 統」。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為的 IAM 使用者marymajor嘗試使用主控台在 C AWS WAF lassic 中執行動作時，就會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我想允許我以外的人訪問我 AWS 帳戶 的 AWS WAF 經典資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要瞭解「 AWS WAF 經典」是否支援這些功能，請參閱AWS WAF 經典如何搭配使用 IAM。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM 使用者指南》中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。

- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 角色與資源型政策的差異。

針 AWS WAF 對傳統使用服務連結角色

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

AWS WAF 傳統使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 AWS WAF 傳統型的唯一 IAM 角色類型。服務連結角色由 C AWS WAF lassic 預先定義，並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

服務連結角色可讓您更輕鬆地設定「 AWS WAF 典型」，因為您不需要手動新增必要的權限。 AWS WAF 傳統會定義其服務連結角色的權限，除非另有定義，否則只有 AWS WAF 傳統可以擔任其角色。已定義的許可包括信任政策和許可政策。該許可政策無法連接至其他任何 IAM 實體。

您必須先刪除角色的相關資源，才能刪除服務連結角色。這樣可以保護您的 C AWS WAF lassic 資源，因為您無法不小心移除存取資源的權限。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

傳統版的 AWS WAF 服務連結角色權限

AWS WAF 典型使用下列服務連結角色：

- `AWSServiceRoleForWAFLogging`
- `AWSServiceRoleForWAFRegionalLogging`

AWS WAF 經典版會使用這些服務連結角色，將日誌寫入 Amazon 資料 Firehose。只有當您啟用登入時，才會使用這些角色 AWS WAF。如需詳細資訊，請參閱 記錄 Web ACL 流量資訊。

AWSServiceRoleForWAFLogging和服AWSServiceRoleForWAFRegionalLogging務連結角色會信任下列服務 (分別) 擔任該角色：

- waf.amazonaws.com

  waf-regional.amazonaws.com

角色的權限原則可讓 C AWS WAF lassic 對指定的資源完成下列動作：

- 動作：firehose:PutRecord並firehose:PutRecordBatch在 Amazon 數據 Firehose 上以「aws-waf-logs-」開頭的名稱數據流資源。例如 aws-waf-logs-us-east-2-analytics。

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

建立傳統版的 AWS WAF 服務連結角色

您不需要手動建立一個服務連結角色。當您在上啟用 AWS WAF 傳統記錄 AWS Management Console，或在 AWS WAF 傳統 CLI 或傳統 API 中發出PutLoggingConfiguration要求時， AWS WAF AWS WAF 傳統會為您建立服務連結角色。

您必須擁有 iam:CreateServiceLinkedRole 許可才能啟用記錄。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您啟用 AWS WAF 傳統記錄時， AWS WAF 傳統會再次為您建立服務連結角色。

編輯傳統版的 AWS WAF 服務連結角色

AWS WAF 傳統版不允許您編輯AWSServiceRoleForWAFLogging和AWSServiceRoleForWAFRegionalLogging服務連結的角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需更多資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除傳統的服務連結角色 AWS WAF

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 當您嘗試刪除資源時，如果 AWS WAF 傳統服務正在使用此角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

若要刪除**AWSServiceRoleForWAFLogging**和使用的 AWS WAF 傳統資源**AWSServiceRoleForWAFRegionalLogging**

1. 在 AWS WAF 典型主控台上，移除每個 Web ACL 的記錄。如需詳細資訊，請參閱 記錄 Web ACL 流量資訊。
2. 使用 API 或 CLI，為每個 Web ACL 提交 `DeleteLoggingConfiguration` 請求啟用記錄功能。如需詳細資訊，請參閱AWS WAF 傳統 API 參考。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台、IAM CLI 或 IAM API 刪除AWSServiceRoleForWAFLogging和AWSServiceRoleForWAFRegionalLogging服務連結的角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

AWS WAF 傳統服務連結角色的支援區域

AWS WAF 傳統支援在下 AWS 區域列項目中使用服務連結角色。

區域名稱	區域身分	Support 經 AWS WAF 典
美國東部 (維吉尼亞北部)	us-east-1	是
美國東部 (俄亥俄)	us-east-2	是
美國西部 (加利佛尼亞北部)	us-west-1	是
美國西部 (奧勒岡)	us-west-2	是
亞太區域 (孟買)	ap-south-1	是
亞太區域 (大阪)	ap-northeast-3	是
亞太區域 (首爾)	ap-northeast-2	是

區域名稱	區域身分	Support 經 AWS WAF 典
亞太區域 (新加坡)	ap-southeast-1	是
亞太區域 (悉尼)	ap-southeast-2	是
亞太區域 (東京)	ap-northeast-1	是
加拿大 (中部)	ca-central-1	是
歐洲 (法蘭克福)	eu-central-1	是
歐洲 (愛爾蘭)	eu-west-1	是
歐洲 (倫敦)	eu-west-2	是
Europe (Paris)	eu-west-3	是
南美洲 (聖保羅)	sa-east-1	是

在 AWS WAF 傳統版中記錄和監視

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

監控是維持 C AWS WAF lassic 和您 AWS 解決方案的可靠性、可用性和效能的重要組成部分。您應該從 AWS 解決方案的所有部分收集監視資料，以便在發生多點失敗時更輕鬆地偵錯。 AWS 提供數種工具來監視您的 C AWS WAF lassic 資源並回應潛在事件：

Amazon CloudWatch 警報

您可以使用 CloudWatch 警示來監視指定期間內的單一量度。如果指標超過指定閾值，則 CloudWatch 會傳送通知給 Amazon SNS 主題或 AWS Auto Scaling 政策。如需詳細資訊，請參閱 使用 Amazon 監控 CloudWatch。

AWS CloudTrail 日誌

CloudTrail 提供「 AWS WAF 傳統」中使用者、角色或 AWS 服務所採取之動作的記錄。使用收集的資訊 CloudTrail，您可以判斷傳送給 C AWS WAF lassic 的要求、提出要求的 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。如需更多詳細資訊，請參閱 使用 AWS CloudTrail 記錄 API 呼叫。

AWS WAF 傳統的合規性驗證

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和網頁等 AWS WAF 資源ACLs，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於您資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上進行HIPAA安全與合規架構 — 本白皮書說明公司如何使用建立符合資格的應 AWS 用程HIPAA式。

  > **Note**
  >
  > 並非所有 AWS 服務 人都HIPAA符合資格。如需詳細資訊，請參閱合HIPAA格服務參考資料。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準 AWS 服務 與技術研究所 (NIST)、支付卡產業安全標準委員會 () 和國際標準化組織 ()PCI) 中保護安全控制指引的最佳做法，並將其對應至安全性控制。ISO
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。

- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您因應各種合規性需求 PCIDSS，例如符合特定合規性架構所要求的入侵偵測需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

AWS WAF 經典的韌性

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠在可用區域之間自動容錯移轉，而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱AWS 全域基礎結構。

AWS WAF 傳統版中的基礎結構

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和網頁等 AWS WAF 資源ACLs，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

作為託管服務，C AWS WAF lassic 受到 AWS 全球網路安全性的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的API呼叫透過網路存取 AWS WAF 典型。使用者端必須支援下列專案：

- 傳輸層安全性 (TLS)。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 具有完美前向保密（ ）的密碼套件，例如（短暫的迪菲-赫爾曼PFS）或DHE（橢圓曲線短暫迪菲-赫爾曼）。ECDHE現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與IAM主體相關聯的秘密存取金鑰來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 以產生暫時安全憑證以簽署請求。

AWS WAF 傳統配額

> **Note**
>
> 這是AWS WAF 經典文檔。只有在您在 2019 年 11 月 AWS WAF 之前建立了規則和 Web ACL 等 AWS WAF 資源，但尚未將資源移轉至最新版本時，才應使用此版本。若要移轉資源，請參閱 將您的 AWS WAF 傳統資源遷移到 AWS WAF。
> 如需的最新版本 AWS WAF，請參閱AWS WAF。

AWS WAF 傳統配額必須遵守下列配額 (先前稱為限制)。

AWS WAF 傳統對每個區域每個帳戶的實體數量有預設配額。您可以請求增加這些配額。

資源	每個區域每個帳戶的預設配額
Web ACL	50
規則	100
R ate-based-rules	5
每個區域每個 帳戶的條件數量	對於除正則表達式匹配和地理匹配以外的所有條件，每種條件類型有 100 個。例如，100 個大小限制條件和 100 個 IP 相符條件。有關正則表達式和地理匹配條件，請參閱下表。

資源	每個區域每個帳戶的預設配額
每秒請求數	每個 Web ACL* 25,000 個

* 此配額僅適用於應用 Application Load Balancer 上的 AWS WAF 典型。 AWS WAF 傳統版的每秒要求數 (RPS) 配額與CloudFront 開發人員指南中所述的 CloudFront RPS 配額支援相同。CloudFront

AWS WAF 傳統實體的下列配額無法變更。

資源	每個區域每個帳戶的配額
每個 web ACL 的規則群組	2：1 個客戶建立的規則群組和 1 個 AWS Marketplace 規則群組
每個 Web ACL 的規則數	10
每個規則的條件數	10
每個 IP 比對條件的 IP 地址範圍 (採用 CIDR 表示法)	10,000 您一次最多可以更新 1,000 個地址。API 呼叫最多可在單一要求中`UpdateIPSet` 接受 1,000 個位址。
每個以速度為基礎的規則，受封鎖的 IP 地址	10,000
每 5 分鐘速率限制的最低以速率為基礎的規則	100

資源	每個區域每個帳戶的配額
每個跨網站指令碼比對條件的篩選條件數	10
每個大小限制條件的篩選條件數	10
每個 SQL injection 比對條件的篩選條件數	10
每個字串比對條件的篩選條件數	10
在字符串匹配條件中，HTTP 標頭名稱中的字符數，當您將 C AWS WAF lassic 配置為檢查 Web 請求中的指定值的標頭時	40
在字符串匹配條件中，您希望 C AWS WAF lassic 搜索的值中的字符數	50
正則表達式匹配	10
在正則表達式匹配條件中，您希望 AWS WAF 經典搜索的模式中的字符數	70
在 regex 符合條件的模式，每個模式設定的數量	10
在 regex 符合條件的模式，每個模式設定 regex 條件的數量	1
模式集	5
地理匹配條件	50
每個地理匹配條件的位置	50

AWS WAF 傳統對每個區域的每個帳戶的通話具有以下固定配額。這些配額適用於透過任何可用方式 (包括主控台、CLI AWS CloudFormation、REST API 和 SDK) 對服務的呼叫總數。這些配額無法變更。

呼叫類型	每個區域每個帳戶的配額
`AssociateWebACL` 呼叫次數上限	每 2 秒 1 個請求
`DisassociateWebACL` 呼叫次數上限	每 2 秒 1 個請求

呼叫類型	每個區域每個帳戶的配額
GetWebACLForResource 呼叫次數上限	每秒 1 個請求
ListResourcesForWebACL 呼叫次數上限	每秒 1 個請求
CreateWebACLMigrationStack 呼叫次數上限	每秒 1 個請求
GetChangeToken 呼叫次數上限	每秒 10 個請求
GetChangeTokenStatus 呼叫次數上限	每秒 1 個請求
任何個別 List 動作的呼叫數上限 (若未定義其他配額)	每秒 5 個請求
任何個別 Create、Put、Get 或 Update 動作的呼叫次數上限 (若未定義其他配額)	每秒 1 個請求

AWS Shield

對於面向網際網路的應用程式來說，防範分散式拒絕服務 (DDoS) 攻擊至關重要。當您建置應用程式時 AWS，您可以利用 AWS 提供的保護，而不需要額外費用。此外，您還可以使用 AWS Shield Advanced 託管威脅防護服務，透過其他 DDoS 偵測、緩解和回應功能來改善您的安全狀態。

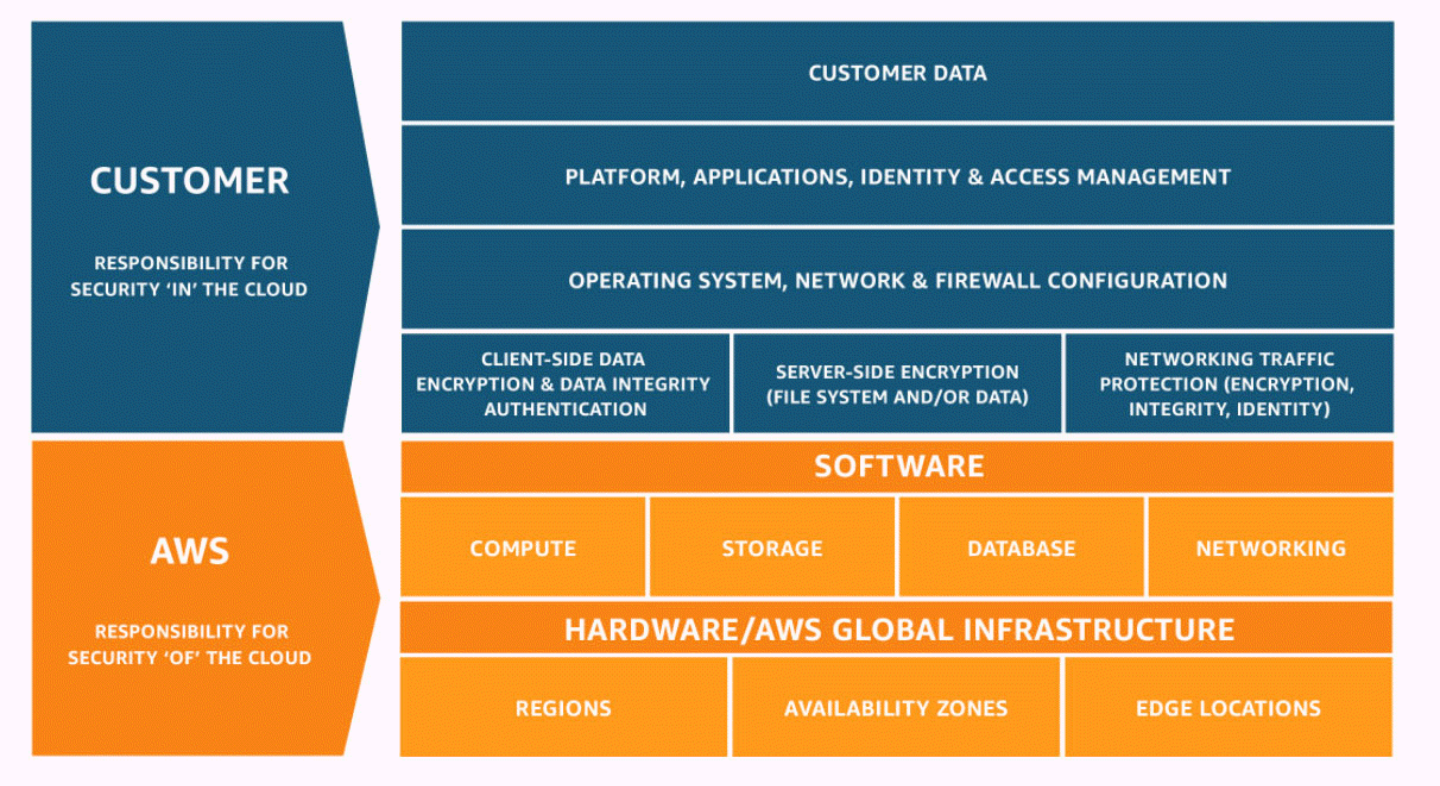
AWS 致力於為您提供工具、最佳實務和服務，以協助確保高可用性、安全性和彈性，以防禦網際網路上的不良行為者。本指南旨在幫助 IT 決策者和安全工程師了解如何使用 Shield and Shield Advanced 來更好地保護其應用程式免受 DDoS 攻擊和其他外部威脅的侵害。

當您在上建置應用程式時 AWS，您會透過 AWS 對抗常見的容積 DDoS 攻擊媒介 (例如 UDP 反射攻擊和 TCP SYN 洪水) 來獲得自動保護。您可以透 AWS 過設計和設定 DDoS 彈性的架構，利用這些保護來確保執行應用程式的可用性。

本指南提供的建議可協助您設計、建立和設定 DDoS 彈性的應用程式架構。如果應用程式受到更大型 DDoS 攻擊和更廣泛的 DDoS 攻擊媒介的目標，則遵循本指南中提供的最佳實踐方式可以從提高可用性連續性中受益。此外，本指南還向您展示如何使用 Shield Advanced 為您的關鍵應用程式實作最佳化的 DDoS 防護狀態。這些應用程式包括您保證為客戶提供一定程度可用性的應用程式，以及在 DDoS 事件 AWS 期間需要作業支援的應用程式。

安全是 AWS 與您之間共同承擔的責任。共同責任模型 將此描述為雲端的安全和雲端內的安全：

- 雲端安全性 — AWS 負責保護中執行 AWS 服務的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。第三方稽核人員定期檢測及驗證安全的效率也是我們 AWS 合規計劃的一部分。若要瞭解適用於 Shield Advanced 的法規遵循計劃，請參閱合規計劃的AWS 服務範圍。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對資料敏感度、組織要求，以及適用法律和法規等其他因素負責。



如何 AWS Shield 和 Shield 高級工作

AWS Shield Standard 並 AWS Shield Advanced 針對網路和傳輸層 (第 3 層和第 4 層) 和應用程式層 (第 7 層) 的 AWS 資源提供分散式拒絕服務 (DDoS) 攻擊的保護。DDoS 攻擊是一種攻擊，其中多個受感染的系統試圖用流量淹沒目標。DDoS 攻擊可以防止合法的最終用戶訪問目標服務，並可能導致目標由於流量過大而崩潰。

AWS Shield 針對各種已知的 DDoS 攻擊媒介和零時差攻擊媒介提供保護。防 Shield 偵測與緩解功能的設計目的是提供涵蓋範圍，即使服務在偵測時並未明確知道威脅。Shield 標準是自動提供的，在您使用時不收取額外費用 AWS。

Shield 牌偵測到的攻擊類別包括：

- 網路容量攻擊 (第 3 層) — 這是基礎架構層攻擊媒介的子類別。這些媒介試圖飽和目標網絡或資源的能力，以拒絕向合法用戶提供服務。
- 網路通訊協定攻擊 (第 4 層) — 這是基礎架構層攻擊媒介的子類別。這些媒介濫用協議以拒絕對目標資源的服務。網路通訊協定攻擊的常見範例是 TCP SYN 洪水，可能會耗盡伺服器、負載平衡器或防火牆等資源上的連線狀態。網絡協議攻擊也可以是容量的。例如，較大的 TCP SYN 洪水可能會打算飽和網路的容量，同時也會耗盡目標資源或中繼資源的狀態。

- 應用程式層攻擊 (第 7 層) — 這類攻擊媒介會嘗試使用對目標有效的查詢充滿應用程式 (例如 Web 要求洪水)，藉此拒絕向合法使用者提供服務。

內容

AWS Shield Standard 概述

AWS Shield 是一項受管理的威脅防護服務，可保護您的應用程式周邊。周邊是來自 AWS 網路外部的應用程式流量的第一個進入點。

若要判斷應用程式周邊的位置，請考慮使用者如何從網際網路存取您的應用程式。如果第一個進入點位於某個 AWS 區域，則應用程式周邊就是您的 Amazon Virtual Private Cloud (VPC)。如果 Amazon Route 53 將使用者導向至您的應用程式，並首先使用 Amazon CloudFront 或存取應用程式 AWS Global Accelerator，則應用程式周邊會從 AWS 網路邊緣開始。

Shield 可為執行的所有應用程式提供 DDoS 偵測和緩解優勢 AWS，但是您在設計應用程式架構時所做的決策將會影響您的 DDoS 彈性等級。DDoS 彈性是您的應用程式在攻擊期間能夠在預期參數內繼續運作的能力。

所有 AWS 客戶都可以享受 Shield 標準的自動保護，無需額外付費。Shield Standard 可防禦針對您網站或應用程式的最常見、經常發生的網路和傳輸層 DDoS 攻擊。雖然 Shield 牌標準有助於保護所有 AWS 客戶，但 Amazon Route 53 託管區域、Amazon CloudFront 分發和 AWS Global Accelerator 標準加速器，您將獲得特別的好處。這些資源會針對所有已知的網路和傳輸層攻擊獲得全面的可用性保護。

AWS Shield Advanced 概述

AWS Shield Advanced 這是一項託管服務，可協助您保護您的應用程式免受外部威脅，例如 DDoS 攻擊、容量傀儡程式和漏洞利用嘗試。如需更高層級的攻擊防護，您可以訂閱 AWS Shield Advanced。

當您訂閱 Shield Advanced 並為您的資源增加保護時，Shield 牌進階可為這些資源提供擴充的 DDoS 攻擊防護。您從 Shield Advanced 獲得的保護可能會因您的架構和組態選擇而有所不同。使用本指南中的資訊，使用 Shield Advanced 建置和保護彈性應用程式，並在需要專家協助時進行升級。

Shield 高級訂閱和 AWS WAF 成本

您的 Shield 進階訂閱可涵蓋使用標準 AWS WAF 功能來保護您使用 Shield 進階保護的資源所需的費用。Shield Advanced 保護所涵蓋的標準 AWS WAF 費用包括每個 Web ACL 的成本、每個規則的成本，以及每百萬個 Web 請求檢查請求的基本價格，最高可達 1,500 個 WCU，最高可達到預設主體大小。

啟用防 Shield 進階自動應用程式層 DDoS 緩解功能會將規則群組新增至使用 150 個 Web ACL 容量單位 (WCU) 的網路 ACL。這些 WCU 會計入您網路 ACL 中的 WCU 使用量。如需詳細資訊，請參閱Shield 先進的自動應用層 DDoS 緩解、Shield 牌進階規則群組及AWS WAF 網路 ACL 容量單位 (WCU)。

您 AWS WAF 對 Shield 進階版的訂閱並不涵蓋您未使用神 Shield 進階保護的資源使用。它也不包括受保護資源的任何額外非標準 AWS WAF 成本。非標準 AWS WAF 成本的範例包括機器人控制、CAPTCHA規則動作、使用超過 1,500 個 WCU 的 Web ACL，以及檢查超出預設主體大小的要求主體。完整列表在 AWS WAF 定價頁面上提供。

如需完整資訊和定價範例，請參閱 Shield 定價和AWS WAF 定價。

Shield 牌進階訂閱計費

如果您是 AWS 通路經銷商，請洽詢您的帳戶團隊以取得相關資訊和指引。此帳單資訊適用於非 AWS 通路經銷商的客戶。

對於所有其他人，以下訂閱和計費準則適用：

- 對於屬於 AWS Organizations 組織成員的帳戶，無論付款人 AWS 帳戶本身是否已訂閱，都會針對組織的付款人帳戶收取 Shield Advanced 訂閱費用。
- 當您訂閱同一個AWS Organizations 合併帳單帳戶系列中的多個帳戶時，一個訂閱價格涵蓋該家庭中所有訂閱的帳戶。組織必須擁有所有 AWS 帳戶 及其所有資源。
- 當您為多個組織訂閱多個帳戶時，您仍然可以在所有組織、帳戶和資源中支付一筆訂閱費用，以便您擁有所有這些帳戶。請聯絡您的客戶經理或 AWS 支援人員，並要求豁免其中一個組織的 AWS Shield Advanced 訂閱費用。

如需詳細的定價資訊和範例，請參閱AWS Shield 定價。

主題

AWS Shield Advanced 受保護資源

> **Note**
>
> 護 Shield 進階保護功能只會針對您在「Shield 牌進階」中明確指定的資源，或您透過「Shield 牌進階」政策進行保護的資源啟用。 AWS Firewall Manager 防 Shield 進階版不會自動保護您的資源。

您可以使用「Shield 牌進階」，透過下列資源類型進行進階監控和防護：

- Amazon CloudFront 分佈。針對 CloudFront 持續部署，Shield Advanced 會保護任何與受保護主要發行版相關聯的暫存散發。
- Amazon 路線 53 託管區域。
- AWS Global Accelerator 標準加速器。
- Amazon EC2 彈性 IP 地址。Shield 進階保護與受保護的彈性 IP 位址相關聯的資源。

- Amazon EC2 執行個體，透過與 Amazon EC2 彈性 IP 地址的關聯。
- 下列 Elastic Load Balancing (ELB) 負載平衡器：
  - 應用程式負載平衡器。
  - Classic Load Balancer。
  - 網路負載平衡器，透過與 Amazon EC2 彈性 IP 地址的關聯。

如需有關這些資源類型保護的其他資訊，請參閱AWS Shield Advanced 依資源類型分類的保護。

AWS Shield Advanced 功能和選項

AWS Shield Advanced 訂閱包括下列功能和選項。這些補充了您已經收到的 DDoS 偵測和緩解功能 AWS。

- AWS WAF 整合 — Shield Advanced 使用 AWS WAF Web ACL、規則和規則群組作為其應用程式層保護的一部分。如需有關的更多資訊 AWS WAF，請參閱如何 AWS WAF 工作。

> **Note**
>
> 您的 Shield 進階訂閱可涵蓋使用標準 AWS WAF 功能來保護您使用 Shield 進階保護的資源所需的費用。Shield Advanced 保護所涵蓋的標準 AWS WAF 費用包括每個 Web ACL 的成本、每個規則的成本，以及每百萬個 Web 請求檢查請求的基本價格，最高可達 1,500 個 WCU，最高可達到預設的主體大小。
>
> 啟用防 Shield 進階自動應用程式層 DDoS 緩解功能會將規則群組新增至使用 150 個 Web ACL 容量單位 (WCU) 的網路 ACL。這些 WCU 會計入您網路 ACL 中的 WCU 使用量。如需詳細資訊，請參閱Shield 先進的自動應用層 DDoS 緩解、Shield 牌進階規則群組及AWS WAF 網路 ACL 容量單位 (WCU)。
>
> 您 AWS WAF 對 Shield 進階版的訂閱並不涵蓋您未使用神 Shield 進階保護的資源使用。它也不包括受保護資源的任何額外非標準 AWS WAF 成本。非標準 AWS WAF 成本的範例包括機器人控制、CAPTCHA規則動作、使用超過 1,500 個 WCU 的 Web ACL，以及檢查超出預設主體大小的要求主體。完整列表在 AWS WAF 定價頁面上提供。
>
> 如需完整資訊和定價範例，請參閱 Shield 定價和AWS WAF 定價。

- 自動應用程式層 DDoS 防護 — 您可以將 Shield Advanced 設定為自動回應，以減輕受保護資源的應用程式層 (第 7 層) 攻擊。透過自動緩解 AWS WAF 功能，Shield Advanced 會對來自已知 DDoS 來源的要求執行 AWS WAF 速率限制，並自動新增和管理自訂保護，以回應偵測到的 DDoS 攻擊。您可以設定自動緩和措施，以計算或封鎖屬於攻擊一部分的 Web 要求。

如需詳細資訊，請參閱 Shield 先進的自動應用層 DDoS 緩解。

- Health 狀況偵測 — 您可以搭配防 Shield 進階使用 Amazon Route 53 運作狀態檢查，以通知事件偵測和緩解措施。運作狀態檢查會根據您的規格來監控您的應用程式，並在符合規格時回報狀況良好，且不 Health 狀況。搭配 Shield Advanced 使用健康狀態檢查有助於防止誤判，並在受保護的資源不健康時提供更快的偵測和緩解措施。您可以針對任何資源類型使用健全狀況型偵測 (Route 53 託管區域除外)。Shield 進階主動互動僅適用於已啟用健康狀態偵測的資源。

  如需詳細資訊，請參閱 以 Health 狀態檢查為基礎的偵測。

- 保護群組 — 您可以使用保護群組建立受保護資源的邏輯群組，以增強整個群組的偵測和緩和措施。您可以定義保護群組中的成員資格準則，以便自動包含新受保護的資源。受保護的資源可以屬於多個保護群組。

  如需詳細資訊，請參閱 AWS Shield Advanced 保護群組。

- 增強對 DDoS 事件和攻擊的可見性 — Shield Advanced 使您可以訪問高級的實時指標和報告，以便廣泛地了解受保護 AWS 資源的事件和攻擊。您可以透過 Shield 牌進階 API 和主控台，以及透過 Amazon CloudWatch 指標存取此資訊。

  如需詳細資訊，請參閱 DDoS 事件的可見性。

- Shield 進階防護的集中管理方式： AWS Firewall Manager— 您可以使用 Firewall Manager 員將 Shield 進階防護自動套用至您的新帳戶和資源，並將 AWS WAF 規則部署到 Web ACL。對於 Shield 進階客戶，Firewall Manager 員防護進階防護政策不收取額外費用。您也可以使用 Firewall Manager 員搭配 Amazon Simple Notification Service (SNS) 主題或 AWS Security Hub，集中管理您帳戶的 Shield 進階監控活動。

  如需有關使用 Firewall Manager 員管理防護進階防護的詳細資訊，請參閱AWS Firewall Manager和AWS Shield Advanced 政策。如需有關 Firewall Manager 員定價的資訊，請參閱AWS Firewall Manager 定價

- AWS Shield 牌應變團隊（ SRT ）— SRT 在保護 AWS亞馬遜及其子公司方面擁有豐富的經驗。身為 AWS Shield Advanced 客戶，您可以在 DDoS 攻擊期間隨時聯絡 SRT 以取得協助，這會影響應用程式的可用性。您也可以使用 SRT 來建立和管理資源的自訂緩和措施。若要使用 SRT 的服務，您也必須訂閱商務 Support 方案或企業 Support 方案。

  如需詳細資訊，請參閱 Shield 牌回應小組 (SRT) 支援。

- 主動參與 — 如果您與受保護的資源相關聯的 Amazon Route 53 運作狀態檢查在由 Shield Advanced 偵測到的事件期間變得不健康，Shield 牌回應團隊 (SRT) 會直接與您聯絡。當應用程式的可用性可能受到可疑攻擊的影響時，這可讓您更快速地與專家互動。

如需詳細資訊，請參閱 設定主動參與。

- 成本保護機會 — Shield Advanced 提供一些成本保護，以防止帳 AWS 單中可能因 DDoS 攻擊對受保護的資源而造成的高峰。這可能包括 Shield 進階資料傳出 (DTO) 使用費中峰值的涵蓋範圍。Shield 牌進階以 Shield 牌進階服務積分的形式提供任何費用保護。

  如需更多詳細資訊，請參閱 申請信用 AWS Shield Advanced。

決定是否訂閱 AWS Shield Advanced 及套用其他保護

檢閱本節中的案例，以協助決定要訂閱哪些帳戶，以 AWS Shield Advanced 及在何處套用其他保護。使用 Shield Advanced，您可以為在合併帳單帳戶下建立的所有帳戶支付一個月的訂閱費用，再加上根據傳出的 GB 資料量計算的使用費。如需有關 Shield 進階定價的資訊，請參閱AWS Shield Advanced 定價。

若要使用 Shield Advanced 保護應用程式及其資源，您可以向 Shield Advanced 訂閱管理應用程式的帳戶，然後為應用程式的資源新增保護。如需訂閱帳號和保護資源的相關資訊，請參閱開始使用 AWS Shield Advanced。

Shield 高級訂閱和 AWS WAF 成本

您的 Shield 進階訂閱可涵蓋使用標準 AWS WAF 功能來保護您使用 Shield 進階保護的資源所需的費用。Shield Advanced 保護所涵蓋的標準 AWS WAF 費用包括每個 Web ACL 的成本、每個規則的成本，以及每百萬個 Web 請求檢查請求的基本價格，最高可達 1,500 個 WCU，最高可達到預設主體大小。

啟用防 Shield 進階自動應用程式層 DDoS 緩解功能會將規則群組新增至使用 150 個 Web ACL 容量單位 (WCU) 的網路 ACL。這些 WCU 會計入您網路 ACL 中的 WCU 使用量。如需詳細資訊，請參閱Shield 先進的自動應用層 DDoS 緩解、Shield 牌進階規則群組及AWS WAF 網路 ACL 容量單位 (WCU)。

您 AWS WAF 對 Shield 進階版的訂閱並不涵蓋您未使用神 Shield 進階保護的資源使用。它也不包括受保護資源的任何額外非標準 AWS WAF 成本。非標準 AWS WAF 成本的範例包括機器人控制、CAPTCHA規則動作、使用超過 1,500 個 WCU 的 Web ACL，以及檢查超出預設主體大小的要求主體。完整列表在 AWS WAF 定價頁面上提供。

如需完整資訊和定價範例，請參閱 Shield 定價和AWS WAF 定價。

Shield 牌進階訂閱計費

如果您是 AWS 通路經銷商，請洽詢您的帳戶團隊以取得相關資訊和指引。此帳單資訊適用於非 AWS 通路經銷商的客戶。

對於所有其他人，以下訂閱和計費準則適用：

- 對於屬於 AWS Organizations 組織成員的帳戶，無論付款人 AWS 帳戶本身是否已訂閱，都會針對組織的付款人帳戶收取 Shield Advanced 訂閱費用。
- 當您訂閱同一個AWS Organizations 合併帳單帳戶系列中的多個帳戶時，一個訂閱價格涵蓋該家庭中所有訂閱的帳戶。組織必須擁有所有 AWS 帳戶 及其所有資源。
- 當您為多個組織訂閱多個帳戶時，您仍然可以在所有組織、帳戶和資源中支付一筆訂閱費用，以便您擁有所有這些帳戶。請聯絡您的客戶經理或 AWS 支援人員，並要求豁免其中一個組織的 AWS Shield Advanced 訂閱費用。

如需詳細的定價資訊和範例，請參閱AWS Shield 定價。

識別要保護的應用程式

請考慮針對您需要下列任何一項的應用程式實作 Shield 進階保護：

- 保證應用程式使用者的可用性。
- 如果應用程式受到 DDoS 攻擊的影響，可快速聯絡 DDoS 緩解專家。
- 意識到 AWS 應用程式可能會受到 DDoS 攻擊以及來自安全或營運團隊的攻擊通知 AWS 和升級的影響。
- 雲端成本的可預測性，包括 DDoS 攻擊何時影響您對 AWS 服務的使用。

如果應用程式或其資源需要上述任何一項，請考慮建立相關帳戶的訂閱。

確定要保護的資源

對於每個訂閱的帳號，請考慮為每個具有下列特性的資源新增 Shield Advanced 防護：

- 該資源為互聯網上的外部用戶提供服務。
- 該資源暴露在互聯網上，也是關鍵應用程序的一部分。考慮每個暴露的資源，無論您是否打算由 Internet 上的用戶訪問它。
- 該資源受到 AWS WAF 網絡 ACL 的保護。

若要深入瞭解如何為資源建立和管理保護，請參閱資源保護 AWS Shield Advanced。

此外，請遵循本指南中的建議，以協助確保您架構應用程式的 DDoS 復原能力，並且已正確設定 Shield Advanced 的功能，以獲得最佳保護。

DDoS 攻擊的例子

AWS Shield Advanced 針對多種類型的攻擊提供擴充保護。

下列清單說明一些常見的攻擊類型：

使用者資料包通訊協定 (UDP) 反射攻擊

在 UDP 反射攻擊中，攻擊者可偽造請求的源並使用 UDP 從服務器引起大量響應。導向詐騙性、受攻擊 IP 位址的額外網路流量可能會降低目標伺服器的速度，並防止合法使用者存取所需的資源。

同步洪水

TCP SYN 洪水攻擊的目的是讓連線處於半開啟狀態，藉此耗盡系統的可用資源。當用戶連接到 TCP 服務，如 Web 服務器，客戶端發送一個 TCP SYN 數據包。伺服器會傳回確認，而用戶端會傳回自己的確認，完成三向交握。在 TCP SYN 洪水中，永遠不會返回第三個確認，並且服務器等待響應。這可防止其他使用者連線到該伺服器上。

DNS 查詢泛洪

在 DNS 查詢氾濫中，攻擊者會使用多個 DNS 查詢來耗盡 DNS 伺服器的資源。 AWS Shield Advanced 可協助針對 Route 53 DNS 伺服器上的 DNS 查詢洪水攻擊提供保護。

HTTP 洪水/cache-busting (layer 7) 攻擊

使用 HTTP 洪水 (包括GET和POST洪水) 時，攻擊者會傳送多個看似來自 Web 應用程式真實使用者的 HTTP 要求。Cache-busting 攻擊也是一種 HTTP 洪水的類型，使用 HTTP 請求的查詢字串的變體防止使用位置快取內容，和強制從原始 web 伺服器提供內容，導致其他及潛在損壞原始 web 伺服器的壓力。

如何 AWS Shield 偵測事件

AWS 為 AWS 網絡和個人 AWS 服務運行服務級別檢測系統，以確保它們在 DDoS 攻擊期間仍然可用。此外，資源層級偵測系統會監控每個個別 AWS 資源，以確保流向資源的流量保持在預期的參數內。此組合可套用降低已知錯誤封包、反白顯示潛在惡意流量，並排定來自使用者流量的優先順序，藉此同時保護目標 AWS 資源和 AWS 服務。

偵測到的事件會顯示在您的 Shield Advanced 事件摘要、攻擊詳細資料和 Amazon CloudWatch 指標中，做為 DDoS 攻擊媒介的名稱，或者`Volumetric`就像評估是根據流量而非簽章一樣。如需量度內可用攻擊向量維度的詳細資`DDoSDetected` CloudWatch訊，請參閱 AWS Shield Advanced 度量

主題

- 基礎架構層威脅的偵測邏輯
- 應用程式層威脅的偵測邏輯
- 應用程式中多個資源的偵測邏輯

基礎架構層威脅的偵測邏輯

用於保護目標 AWS 資源免受基礎架構層（第 3 層和第 4 層）中的 DDoS 攻擊的檢測邏輯取決於資源類型以及資源是否受到保護 AWS Shield Advanced。

檢測 Amazon CloudFront 和 Amazon 路線 53

當您使用 CloudFront 和 Route 53 為 Web 應用程式提供服務時，所有到應用程式的封包都會由完全內嵌 DDoS 緩解系統進行檢查，該系統不會產生任何可觀察到的延遲。對 CloudFront 分佈和 Route 53 託管區域的 DDoS 攻擊可實時緩解。無論您是否使用，這些保護都適用 AWS Shield Advanced。

盡可能遵循使用 CloudFront 和 Route 53 作為 Web 應用程式進入點的最佳做法，以便最快速地偵測和緩解 DDoS 事件。

檢測 AWS Global Accelerator 和區域服務

資源層級偵測可保護 AWS 區域中啟動的 AWS Global Accelerator 標準加速器和資源，例如傳統負載平衡器、應用程式負載平衡器和彈性 IP 位址 (EIP)。系統會監控這些資源類型的流量高度，這些資源可能表示存在需要緩解的 DDoS 攻擊。每分鐘都會評估每個 AWS 資源的流量。如果對資源的流量提高，則會執行額外的檢查以測量資源的容量。

「Shield」會執行下列標準檢查：

- 亞馬遜彈性運算雲端 (Amazon EC2) 執行個體、連接到 Amazon EC2 執行個體的 EIP — Shield 會從受保護的資源擷取容量。容量取決於目標的執行個體類型、執行個體大小和其他因素，例如執行個體是否使用增強型聯網。
- 傳統負載平衡器和應用程式負載平衡器 — Shield 會從目標負載平衡器節點擷取容量。
- 連接至網路負載平衡器的 EIP — Shield 會從目標負載平衡器擷取容量。容量獨立於目標負載平衡器的群組組態。

- AWS Global Accelerator 標準加速器 — Shield 會擷取容量，此容量是以端點組態為基礎。

這些評估會跨多個網路流量維度進行，例如連接埠和通訊協定。如果超過目標資源的容量，Shield 牌會放置 DDoS 緩解措施。Shield 放置的緩和措施將減少 DDoS 流量，但可能無法消除它。如果在與已知 DDoS 攻擊媒介一致的流量維度上超過一小部分資源容量，Shield 也可能會放置緩解措施。Shield 牌在有限的存留時間內放置此緩解措施（TTL），只要攻擊持續進行，它就會擴展。

> **Note**
>
> Shield 放置的緩解措施將減少 DDoS 流量，但可能無法消除它。您可以使用類似的解決方案 AWS Network Firewall 或主機上的防火牆iptables來增強 Shield，例如防止應用程式處理對您的應用程式無效或非合法使用者產生的流量。

「Shield 牌進階防護」可將下列項目新增至現有的 Shield 偵測活動：

- 較低的偵測閾值 —「Shield 牌進階」會將緩和措施放在計算容量的一半。這可以為緩慢加速的攻擊提供更快的緩解措施，並減輕具有更模糊容量特徵的攻擊。
- 間歇性攻擊防護 — Shield Advanced 會根據攻擊的頻率和持續時間，以指數級增加的存留時間 (TTL) 設置緩和措施。當資源經常被鎖定目標，以及在短時間內發生攻擊時，這樣可以延長緩和措施的時間。
- 健全狀況偵測 — 當您將 Route 53 He alth 狀態檢查與 Shield Advanced 受保護的資源建立關聯時，偵測邏輯中會使用健康狀態檢查的狀態。在偵測到的事件期間，如果健全狀況檢查狀況良好，Shield Advanced 會在放置緩和措施之前，需要更有信心確定該事件是攻擊。如果運作狀態檢查不健康，Shield Advanced 可能會在建立信心之前放置緩解措施。此功能有助於避免誤報，並對影響應用程式的攻擊提供更快的反應。如需使用「Shield 進階」進階進行狀態檢查的相關資以 Health 狀態檢查為基礎的偵測訊

應用程式層威脅的偵測邏輯

AWS Shield Advanced 為受保護的 Amazon CloudFront 分發和應用程式負載平衡器提供 Web 應用程式層偵測。當您使用 Shield Advanced 保護這些資源類型時，您可以將 AWS WAF Web ACL 與您的保護建立關聯，以啟用 Web 應用程式層偵測。Shield Advanced 會耗用關聯網頁 ACL 的要求資料，並為您的應用程式建立流量基準。Web 應用程式層偵測仰賴 Shield 牌進階和 AWS WAF. 若要深入瞭解應用程式層保護，包括將 AWS WAF Web ACL 與 Shield Advanced 受保護的資源建立關聯，請參閱。AWS Shield Advanced 應用程式層 (第 7 層) 保護

對於 Web 應用程式層偵測，Shield Advanced 會監控應用程式流量，並將其與尋找異常的歷史基準進行比較。這項監測涵蓋總體積和流量組成。在 DDoS 攻擊期間，我們預計流量和組成都會發生變化，而 Shield Advanced 需要在統計上顯著偏差來宣告事件。

「Shield 牌進階」會針對歷史時間範圍執行測量。這種方法可以減少因流量合法變化或符合預期模式的流量變化而產生的誤報通知，例如每天同一時間提供的銷售。

> **Note**
>
> 給予 Shield Advanced 時間來建立代表正常、合法流量模式的基準，以避免 Shield 進階保護中的誤判。當您將 Web ACL 與受保護的資源建立關聯時，Shield Advanced 會開始收集其基準線的資訊。在任何可能導致 Web 流量異常模式的計劃事件之前至少 24 小時，將 Web ACL 與受保護的資源建立關聯。Shield 高級 Web 應用程序層檢測是最準確的，當它已經觀察到 30 天的正常流量。

Shield Advanced 偵測事件所花費的時間會受到它在流量中觀察到的變化程度的影響。對於較低的數量變化，Shield Advanced 會更長時間觀察流量，以建立事件發生的信心。對於更高的音量變化，Shield Advanced 可以更快地檢測並報告事件。

Web ACL 中的速率型規則 (無論是由您或由 Shield Advanced 自動應用程式層緩和功能新增) 都可以在攻擊達到可偵測等級之前緩解攻擊。如需有關自動應用程式層 DDoS 緩解的詳細資訊，請參閱Shield 先進的自動應用層 DDoS 緩解。

> **Note**
>
> 您可以架構應用程式以回應提升的流量或負載，以確保應用程式不受較小的要求洪水影響。使用 Shield 進階版，您受保護的資源將受到成本保護。這有助於保護您免受 DDoS 攻擊可能發生的雲端帳單意外增加。若要深入瞭解 Shield 進階成本保護，請參閱申請信用 AWS Shield Advanced。

應用程式中多個資源的偵測邏輯

您可以使用 AWS Shield Advanced 保護群組來建立屬於相同應用程式一部分的受保護資源集合。您可以選擇要放置在群組中的受保護資源，或指示應將相同類型的所有資源視為一個群組。例如，您可以建立所有應用程式負載平衡器的群組。建立保護群組時，Shield Advanced 偵測會彙總群組內受保護資源的所有流量。如果您有許多資源，而且每個資源都有少量流量，但彙總量較大，則此功能非常有用。對於在受保護資源之間傳輸流量的藍綠色部署，您也可以使用保護群組來保留應用程式基準。

您可以選擇以下列其中一種方式彙總保護群組中的流量：

- 總和 — 此彙總會結合保護群組中資源的所有流量。您可以使用此彙總來確保新建立的資源具有現有的基準線，並降低偵測敏感度，這有助於防止誤判。
- 平均值 — 此彙總會使用保護群組中所有流量的平均值。您可以將此彙總用於跨資源流量一致的應用程式，例如負載平衡器。
- Max — 此彙總會使用保護群組中任何資源的最高流量。當保護群組中的應用程式有多個層級時，您可以使用此彙總。例如，您可能有一個保護群組，其中包括 CloudFront 分發、其 Application Load Balancer 來源，以及應用程式負載平衡器的 Amazon EC2 執行個體目標。

針對針對多個面向網際網路的 Elastic IP 或 AWS Global Accelerator 標準加速器的攻擊，您也可以使用保護群組來改善 Shield Advanced 放置緩和措施的速度。當保護群組中的一個資源成為目標時，Shield Advanced 會為群組中的其他資源建立信賴度。這會將「Shield 牌進階偵測」置於警示上，並可縮短建立其他緩和措施所需的時間。

若要深入了解保護群組，請參閱AWS Shield Advanced 保護群組。

AWS Shield 緩解事件的方式

保護應用程式的緩解邏輯可能會因應您的應用程式架構而有所不同。當您使用 Amazon CloudFront 和 Amazon Route 53 來保護 Web 應用程式時，您將受益於 Web 和 DNS 使用案例專屬的緩和措施，以及保護服務的所有流量。如果應用程式的進入點是在 AWS 區域中執行的資源，緩和邏輯會根據服務、資源類型和您的使用情況而有所不同 AWS Shield Advanced。

AWS DDoS 緩解系統由 Shield 工程師開發，並與 AWS 服務緊密整合。工程師會考慮您架構的各個層面，例如目標資源的容量和健康狀態。Shield 工程師會持續監控 DDoS 緩解系統的有效性和效能，並在發現或預期新威脅時迅速做出回應。

您可以架構應用程式以因應升高的流量或負載而進行擴充，以協助確保應用程式不受較小的要求洪水影響。如果您使用 Shield Advanced 來保護您的資源，您將獲得涵蓋範圍，以防止因 DDoS 攻擊而發生的雲帳單意外增加。

基礎架構緩和措

對於基礎架構層攻擊， AWS Shield DDoS 緩解系統存在於 AWS 網路邊界和 AWS 邊緣位置。在整個 AWS 基礎架構中放置多個層級的安全控制可 defense-in-depth 為您的雲端應用程式提供服務。

Shield 在來自互聯網的所有入口點維護 DDoS 緩解系統。當 Shield 偵測到 DDoS 攻擊時，會針對每個輸入點重新路由流量，透過同一位置的 DDoS 緩解系統。這不會產生任何可觀察到的額外延遲，而且

在所有 AWS 區域和所有節點提供超過 100 TeraBits 每秒 (Tbps) 的緩解容量。Shield 可保護您的資源可用性，而無需將流量重新路由到外部或遠端清洗中心，進而增加延遲。

- 在 AWS 網路邊界，對於任何 AWS 服務或資源，DDoS 緩解系統可減輕來自網際網路的基礎架構層攻擊。當 Shield 牌偵測或 Shield 牌回應小組 (SRT) 的工程師發出訊號時，系統會執行緩解措施。
- 在節 AWS 點，DDoS 緩解系統會持續檢查轉發到 Amazon CloudFront 分發和 Amazon Route 53 託管區域的每個封包，而不論其來源為何。必要時，系統會套用專為 Web 和 DNS 流量設計的緩和措施。使用 Amazon CloudFront 和 Amazon Route 53 來保護您的 Web 應用程式的另一個好處是，即可立即緩解 DDoS 攻擊，而不需要 Shield 偵測訊號。

應用程式層緩和措施

Shield Advanced 為您已啟用 Shield 進階保護的 Amazon CloudFront 分發和應用程式負載平衡器提供 Web 應用程式層緩解措施。啟用防護時，您可以將 AWS WAF Web ACL 與資源建立關聯，以啟用 Web 應用程式層偵測。此外，您還可以選擇啟用自動應用程式層緩解功能，這會指示 Shield Advanced 在 DDoS 攻擊期間為您管理保護。

Shield 僅針對已啟用 Shield 進階和自動應用程式層緩解的資源，提供應用程式層攻擊的自訂緩和措施。透過自動緩解 AWS WAF 功能，Shield Advanced 會對來自已知 DDoS 來源的要求執行 AWS WAF 速率限制，並自動新增和管理自訂保護，以回應偵測到的 DDoS 攻擊。如需此類型緩和措施的詳細資訊，請參閱防 Shield 進階如何管理自動緩解。

Web ACL 中以速率為基礎的規則 (無論是由您新增還是由 Shield Advanced 自動應用程式層緩和功能新增) 都可以在攻擊達到可偵測等級之前緩解攻擊。如需偵測的詳細資訊，請參閱應用程式層威脅的偵測邏輯。

緩解功能

AWS Shield DDoS 緩解的主要功能如下：

- 封包驗證 — 這可確保每個檢查封包都符合預期的結構，且對其通訊協定有效。支援的通訊協定驗證包括 IP、TCP (包括標頭和選項)、UDP、ICMP、DNS 和 NTP。
- 存取控制清單 (ACL) 和塑形器 — ACL 會根據特定屬性評估流量，並捨棄相符的流量或將其對應至塑形器。Shaper 會限制相符流量的封包速率，捨棄多餘的封包以包含到達目的地的磁碟區。 AWS Shield 偵測與防 Shield 回應小組 (SRT) 工程師可以針對預期流量提供專屬的費率分配，並為具有符合已知 DDoS 攻擊媒介的屬性的流量提供更嚴格的速率分配。ACL 可以比對的屬性包括連接埠、通訊協定、TCP 旗標、目的地位址、來源國家/地區，以及封包裝載中的任意模式。

- 可疑評分 — 這會使用 Shield 預期流量的知識，將分數套用至每個封包。較接近已知良好流量模式的封包會指派較低的可疑分數。觀察已知不良流量屬性可能會增加封包的可疑分數。當需要對限制封包進行分級時，Shield 會先丟棄可疑分數較高的封包。這有助於 Shield 減輕已知和零時差 DDoS 攻擊，同時避免誤判。
- TCP SYN 代理 — 這通過發送 TCP SYN Cookie 來挑戰新的連接，然後允許它們傳遞給受保護的服務，以提供針對 TCP SYN 洪水的保護。Shield DDoS 緩解提供的 TCP SYN 代理是無狀態的，這使得它可以緩解最大的已知 TCP SYN 洪水攻擊，而不會達到狀態耗盡。這是通過與 AWS 服務集成來分發連接狀態，而不是在客戶端和受保護的服務之間維護連續的代理來實現的。TCP SYN 代理目前在 Amazon CloudFront 和 Amazon 路線 53 上可用。
- 速率分配 — 這會根據流量向受保護資源的輸入模式持續調整每個位置整形器值。這樣可以防止可能無法平均進入 AWS 網絡的客戶流量的速率限制。

AWS Shield 53 號公路 CloudFront 和緩解邏輯

防 Shield DDoS 緩解功能會持續檢查 53 號路線 CloudFront 的流量。這些服務透過遍佈全球的 AWS 邊緣位置網路運作，為您提供對 Shield DDoS 緩解功能的廣泛存取權，並從更接近最終使用者的基礎架構交付應用程式。

- CloudFront— Shield DDoS 緩解措施僅允許對 Web 應用程序有效的流量傳遞到服務。這提供了對許多常見的 DDoS 媒介的自動保護，例如 UDP 反射攻擊。

  CloudFront 維護與應用程式來源的持續性連線，透過與 Shield TCP SYN 代理功能整合而自動緩解 TCP SYN 洪水，並在邊緣終止傳輸層安全性 (TLS)。這些組合功能可確保您的應用程式來源僅接收格式良好的 Web 請求，並且可以防止低層 DDoS 攻擊、連線洪水和 TLS 濫用。

  CloudFront 使用 DNS 流量方向和任意廣播路由的組合。這些技術可減輕接近來源的攻擊、提供故障隔離，並確保容量存取以減輕最大的已知攻擊，藉此改善應用程式的彈性。
- 路由 53 — Shield 牌緩和措施僅允許有效的 DNS 請求連接到服務。Shield 使用可疑評分來緩解 DNS 查詢洪水，該評分會優先處理已知的良好查詢，並排除包含可疑或已知 DDoS 攻擊屬性的查詢的優先順序。

  Route 53 使用隨機分片，為 IPv4 和 IPv6 的每個託管區域提供一組唯一的四個解析器 IP 位址。每個 IP 地址對應於 Route 53 位置的不同子集。每個位置子集都包含授權 DNS 伺服器，這些 DNS 伺服器僅與任何其他子集中的基礎結構部分重疊。這樣可以確保如果用戶查詢因任何原因失敗，它將在重試時成功提供。

  Route 53 會根據網路接近度，使用任意傳送路由將 DNS 查詢導向至最近的節點位置。Anycast 還將 DDoS 流量散佈到許多邊緣位置，從而防止攻擊專注於單個位置。

除了緩解速度之外，Route 53 CloudFront 還提供了對全球分佈式 Shield 容量的廣泛訪問權限。若要利用這些功能，請使用這些服務做為動態或靜態 Web 應用程式的進入點。

若要進一步了解如何使用 CloudFront 和 Route 53 來保護 Web 應用程式，請參閱如何使用 Amazon CloudFront 和 Amazon Route 53 協助保護動態 Web 應用程式免受 DDoS 攻擊。若要深入了解 Route 53 上的故障隔離，請參閱全域故障隔離中的案例研究。

AWS ShieldAWS 區域的緩解邏輯

在 AWS 區域中啟動的資源受到 Shield 資源級檢測所放置的 AWS Shield DDoS 緩解系統的保護。區域資源包括彈性 IP (EIP)、傳統負載平衡器和應用程式負載平衡器。

在放置緩解措施之前，Shield 會識別目標資源及其容量。Shield 會使用容量來判斷其緩和措施應允許轉送至資源的最大總流量。緩解措施中的存取控制清單 (ACL) 和其他塑造程式可能會減少某些流量允許的磁碟區，例如與已知 DDoS 攻擊媒介相符的流量，或者預期不會大量出現的流量。這進一步限制緩和措施允許 UDP 反射攻擊或具有 TCP SYN 或 FIN 旗標的 TCP 流量的流量。

Shield 會針對每種資源類型決定容量並以不同方式放置緩和措施

- 對於 Amazon EC2 執行個體或連接到 Amazon EC2 執行個體的 EIP，Shield 會根據執行個體類型和其他執行個體屬性 (例如執行個體是否已啟用增強型聯網) 來計算容量。
- 對於「應用程式負載平衡器」或「Classic Load Balancer」，Shield 會個別計算負載平衡器每個目標節點的容量。這些資源的 DDoS 攻擊緩解措施是由 Shield DDoS 緩解措施和負載平衡器自動擴展的組合提供的。當 Shield 牌回應小組 (SRT) 參與對應用程式負載平衡器或 Classic Load Balancer 資源的攻擊時，他們可能會加速擴展作為額外的保護措施。
- Shield 會根據基 AWS 礎結構的可用容量來計算某些 AWS 資源的容量。這些資源類型包括網路負載平衡器 (NLB) 和透過閘道負載平衡器或路由流量的資源。 AWS Network Firewall

> **Note**
>
> 透過附加受防護進階保護的 EIP 來保護您的網路負載平衡器。您可以使用 SRT，根據基礎應用程式的預期流量和容量來建置自訂的緩和措施。

當 Shield 進行緩解時，Shield 在緩解邏輯中定義的初始速率限制會同樣套用到每個 Shield 牌 DDoS 緩解系統。例如，如果 Shield 放置了每秒 100,000 個封包 (pps) 限制的緩和措施，則每個位置一開始會允許 100,000 pps。然後，Shield 會持續彙總緩和指標以確定實際的流量比率，並使用該比率調整每個位置的速率限制。這樣可以防止誤判，並確保緩和措施不會過於寬鬆。

AWS ShieldAWS Global Accelerator 標準加速器的緩解邏輯

Shield 緩和措施只允許有效流量到達全域加速器標準加速器的接聽程式端點。標準加速器是全球部署的，它們為您提供 IP 地址，您可以使用這些 IP 地址將流量路由到任何 AWS 區域的 AWS 資源。Shield 針對全域加速器緩解措施所強制執行的速率限制，是以標準加速器路由流量的資源容量為基礎。當總流量超過確定的速率時，以及已知 DDoS 向量超過該速率的一小部分時，Shield 會放置緩解措施。

設定標準加速器時，您會為每個 AWS 區域定義端點群組，以便為應用程式路由傳送流量。Shield 放置緩解措施時，它會計算每個端點群組的容量，並相應地更新每個 Shield DDoS 緩解系統的速率限制。每個位置的費率都會有所不同，基於 Shield 對流量如何從網際網路路由到您的 AWS 資源所做的假設。端點群組的容量計算方式為群組中的資源數目乘以群組中任何資源的最低容量。Shield 會定期重新計算應用程式的容量，並視需要更新速率限制。

> **Note**
>
> 使用流量撥號變更導向端點群組的流量百分比並不會改變 Shield 計算或分配速率限制給其 DDoS 緩解系統的方式。如果您使用流量撥號，請將端點群組設定為根據資源類型和數量彼此鏡像。這有助於確保 Shield 計算的容量代表為您的應用程式提供流量的資源。

如需有關全域加速器中端點群組和流量撥號的詳細資訊，請參閱AWS Global Accelerator 標準加速器中的端點群組。

AWS Shield Advanced 彈性 IP 的緩解邏輯

當您使用防護彈性 IP (EIP) 來保護彈性 IP (EIP) 時 AWS Shield Advanced，防 Shield 進階可增強防 Shield 在 DDoS 事件期間放置的緩和措施。Shield 進階 DDoS 防護系統會針對 EIP 相關聯的公用子網路複寫網路 ACL (NACL) 組態。例如，如果您的 NACL 設定為封鎖所有 UDP 流量，則「Shield 牌進階」會將該規則合併到「Shield 牌」放置的緩和措施中。

這項額外功能可協助您避免因應用程式無效的流量而導致可用性風險。您也可以使用 NACL 封鎖個別來源 IP 位址或來源 IP 位址 CIDR 範圍。對於未分佈的 DDoS 攻擊，這可能是有用的緩解工具。它也可讓您輕鬆管理自己的允許清單，或封鎖不應與應用程式通訊的 IP 位址，而無需依賴 AWS 工程師的介入。

AWS Shield Advanced Web 應用程式的緩解邏輯

AWS Shield Advanced 用 AWS WAF 於緩解 Web 應用程序層攻擊。 AWS WAF 隨附於護 Shield 進階版中，無需額外費用。

標準應用層保護

當您使用 Shield Advanced 保護 Amazon CloudFront 分發或應用程式負載平衡器時，您可以使用 Shield Advanced 將 AWS WAF Web ACL 與受保護的資源建立關聯 (如果您尚未建立關聯的資源)。如果您尚未設定 Web ACL，則可以使用 Shield 進階主控台精靈建立一個 ACL，並在其中新增以速率為基礎的規則。以速率為基礎的規則會限制每個 IP 位址每五分鐘時段的要求數目，提供針對 Web 應用程式層要求洪水的基本保護。您可以配置速率，最低至 100。如需詳細資訊，請參閱 Shield 進階應用程式層 AWS WAF Web ACLs 和速率型規則。

您也可以使用該 AWS WAF 服務來管理 Web ACL。透過 AWS WAF，您可以展開 Web ACL 組態以執行諸如檢查特定 Web 要求元件的字串相符項目或模式、新增自訂要求和回應處理，以及比對要求來源的地理位置。如需 AWS WAF 規則的詳細資訊，請參閱AWS WAF 規則。

自動緩解應用程式層

若要增強保護，請啟用 Shield 進階自動應用程式層緩解功能 使用此選項，Shield Advanced 會針對來自已知 DDoS 來源的要求維護 AWS WAF 速率限制規則，並針對偵測到的 DDoS 攻擊提供自訂緩和措施。

當 Shield Advanced 偵測到受保護資源的攻擊時，它會嘗試識別攻擊特徵，將攻擊流量與應用程式的正常流量隔離。Shield Advanced 會根據受到攻擊的資源以及與相同 Web ACL 相關聯的任何其他資源的歷史流量模式來評估已識別的攻擊特徵。

如果 Shield Advanced 判斷攻擊特徵僅隔離了 DDoS 攻擊涉及的流量，則會在關聯的 Web ACL 內的 AWS WAF 規則中實作簽章。您可以指示 Shield Advanced 放置只計算符合的流量或封鎖的緩和措施，而且您可以隨時變更設定。當「Shield 牌進階」判斷不再需要其緩和規則時，會將它們從 Web ACL 中移除。如需應用程式層事件緩和措施的詳細資訊，請參閱Shield 先進的自動應用層 DDoS 緩解。

如需 Shield 進階應用程式層緩和措施的詳細資訊，請參閱AWS Shield Advanced 應用程式層 (第 7 層) 保護。

基本 DDoS 彈性架構的例子

DDoS 彈性是您的應用程式架構能夠抵禦分散式拒絕服務 (DDoS) 攻擊，同時繼續為合法的終端使用者提供服務。具有高彈性的應用程式可在攻擊期間保持可用狀態，而對效能指標 (例如錯誤或延遲) 的影響最小。本節介紹一些常見的示例架構，並說明如何使用和 Shield Advanced 提供的 DDoS 偵測 AWS 和緩解功能來提高其 DDoS 彈性。

本節中的範例架構強調了為您部署的應用程式提供最大 DDoS 彈性優勢的 AWS 服務。突出顯示的服務的好處包括以下內容：

- 存取全球分散式網路容量 — Amazon 和 Amazon CloudFront Route 53 的服務可讓您在 AWS 全球邊緣網路上存取網際網路和 DDoS 緩解容量。 AWS Global Accelerator這對於緩解更大的體積攻擊很有用，這可以達到規模達到百萬比特。您可以在任何 AWS 區域執行應用程式，並使用這些服務來保護可用性並最佳化合法使用者的效能。
- 防範 Web 應用程式層 DDoS 攻擊媒介 — 結合應用程式規模和 Web 應用程式防火牆 (WAF)，最好緩解 Web 應用程式層 DDoS 攻擊。Shield Advanced 使用 Web 請求檢查記錄檔 AWS WAF 來偵測可自動或透過與 AWS Shield 牌回應團隊 (SRT) 協助緩解的異常情況。透過部署的 AWS WAF 速率型規則，也可透過 Shield 進階自動應用程式層 DDoS 緩解提供自動緩解功能。

除了檢閱這些範例之外，還可以檢閱並遵循 DDoS 彈性最佳實務中適用的AWS 最佳做法。

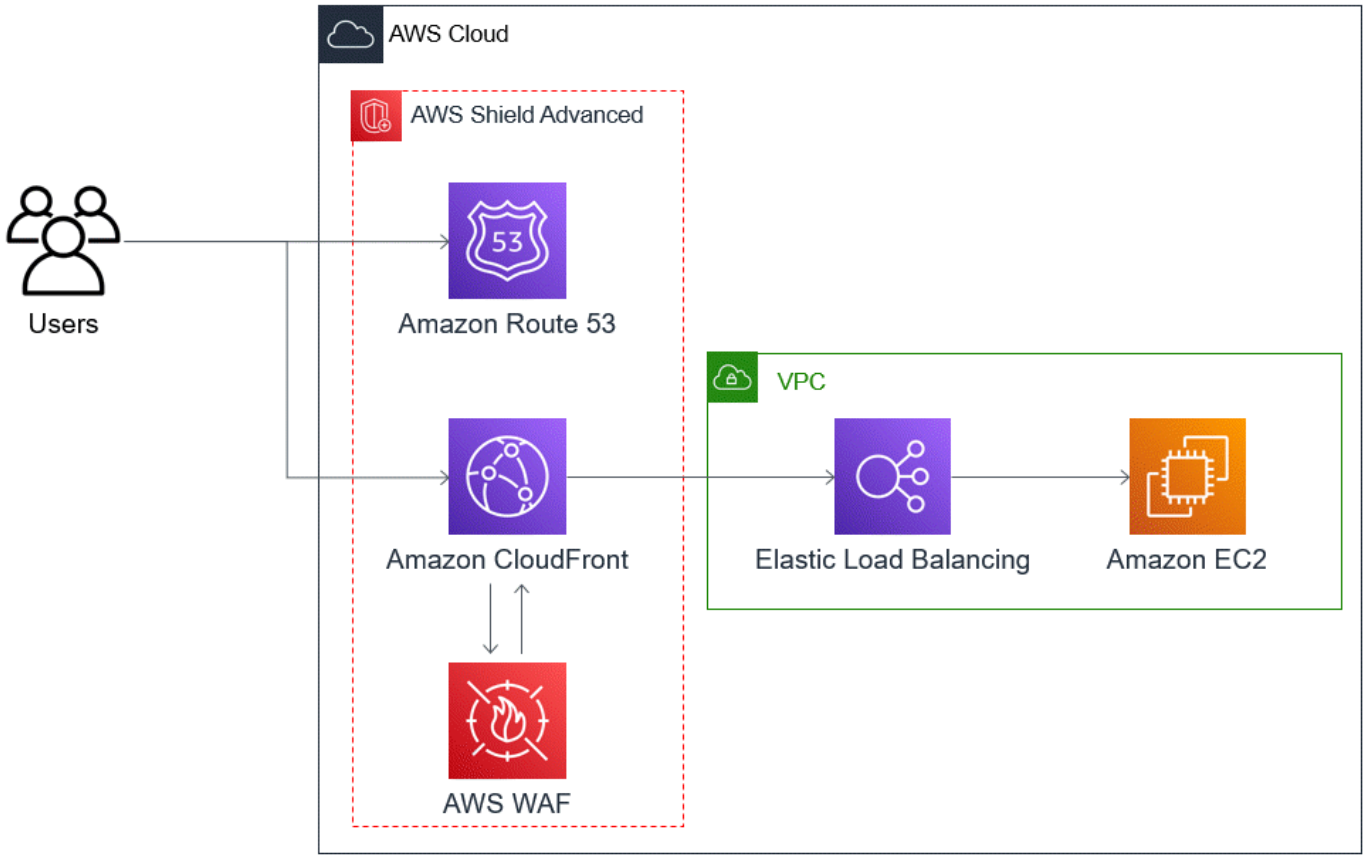
常見 Web 應用程式的 DDoS 彈性範例

您可以在任何 AWS 區域建置 Web 應用程式，並從該地區 AWS 提供的偵測和緩解功能獲得自動 DDoS 保護。

此範例適用於使用傳統負載平衡器、應用程式負載平衡器、網路負載平衡器、 AWS Marketplace 解決方案或您自己的 Proxy 層等資源，將使用者路由至 Web 應用程式的架構。您可以在這些 Web 應用程式資源和使用者之間插入 Amazon Route 53 託管區域、Amazon CloudFront 分發和 AWS WAF Web ACL，以提高 DDoS 彈性。這些插入可以混淆應用程式來源、提供更接近使用者的要求，以及偵測和緩解應用程式層要求洪水。使用 CloudFront 和 Route 53 為使用者提供靜態或動態內容的應用程式受到整合式、完全內嵌 DDoS 緩解系統的保護，該系統可即時緩解基礎架構層攻擊。

有了這些架構改良，您就可以使用 Shield 進階來保護您的 Route 53 託管區域和 CloudFront 分佈。當您保護 CloudFront 發行版時，Shield Advanced 會提示您關聯 AWS WAF Web ACL 並為其建立速率型規則，並提供啟用自動應用程式層 DDoS 緩解或主動參與的選項。主動參與和自動應用程式層 DDoS 緩解功能會使用您與資源相關聯的 Route 53 運作狀態檢查。若要進一步了解這些選項，請參閱資源保護 AWS Shield Advanced。

下面的參考圖描述了 Web 應用程序的此 DDoS 彈性架構。



這種方法為您的 Web 應用程序提供的好處包括以下內容：

- 防範常用的基礎架構層 (第 3 層和第 4 層) DDoS 攻擊，不會延遲偵測。此外，如果資源經常成為目標，Shield Advanced 會將緩解措施放置較長的時間。Shield 進階也會使用從網路 ACL (NACL) 推斷出的應用程式內容，以封鎖進一步上游的不必要流量。這會將故障隔離到更接近其來源的位置，將對合法使用者的影響降到最低。
- 防止 TCP SYN 洪水。與 Route 53 集成的 DDoS 緩解系統CloudFront，並 AWS Global Accelerator 提供 TCP SYN 代理功能，該功能會挑戰新的連接嘗試並僅為合法用戶提供服務。
- 保護 DNS 應用程式層攻擊，因為 Route 53 負責提供權威性 DNS 回應。
- 防止 Web 應用程序層請求洪水。您在 AWS WAF Web ACL 中設定的以速率為基礎的規則會在來源 IP 傳送的要求數量超過規則允許時封鎖這些 IP。
- 如果您選擇啟用此選項，則為您的 CloudFront 發行版自動應用程式層 DDoS 緩解。借助自動 DDoS 緩解功能，Shield Advanced 在分發的相關 AWS WAF Web ACL 中維護基於速率的規則，以限制來自已知 DDoS 來源的請求量。此外，當 Shield Advanced 偵測到會影響應用程式健康狀態的事件時，它會自動建立、測試和管理 Web ACL 中的緩和規則。

- 如果您選擇啟用此選項，請主動與 Shield 牌回應團隊 (SRT) 互動。當 Shield Advanced 偵測到會影響應用程式健康狀態的事件時，SRT 會使用您提供的聯絡資訊回應並主動與您的安全或營運團隊互動。SRT 會分析流量中的模式，並可以更新 AWS WAF 規則以阻止攻擊。

適用於 TCP 和 UDP 應用程式的 DDoS 彈性範例

此範例顯示在使用 Amazon 彈性運算雲端 (Amazon EC2) 執行個體或彈性 IP (EIP) 地址的 AWS 區域中，TCP 和 UDP 應用程式適用的 DDoS 彈性架構。

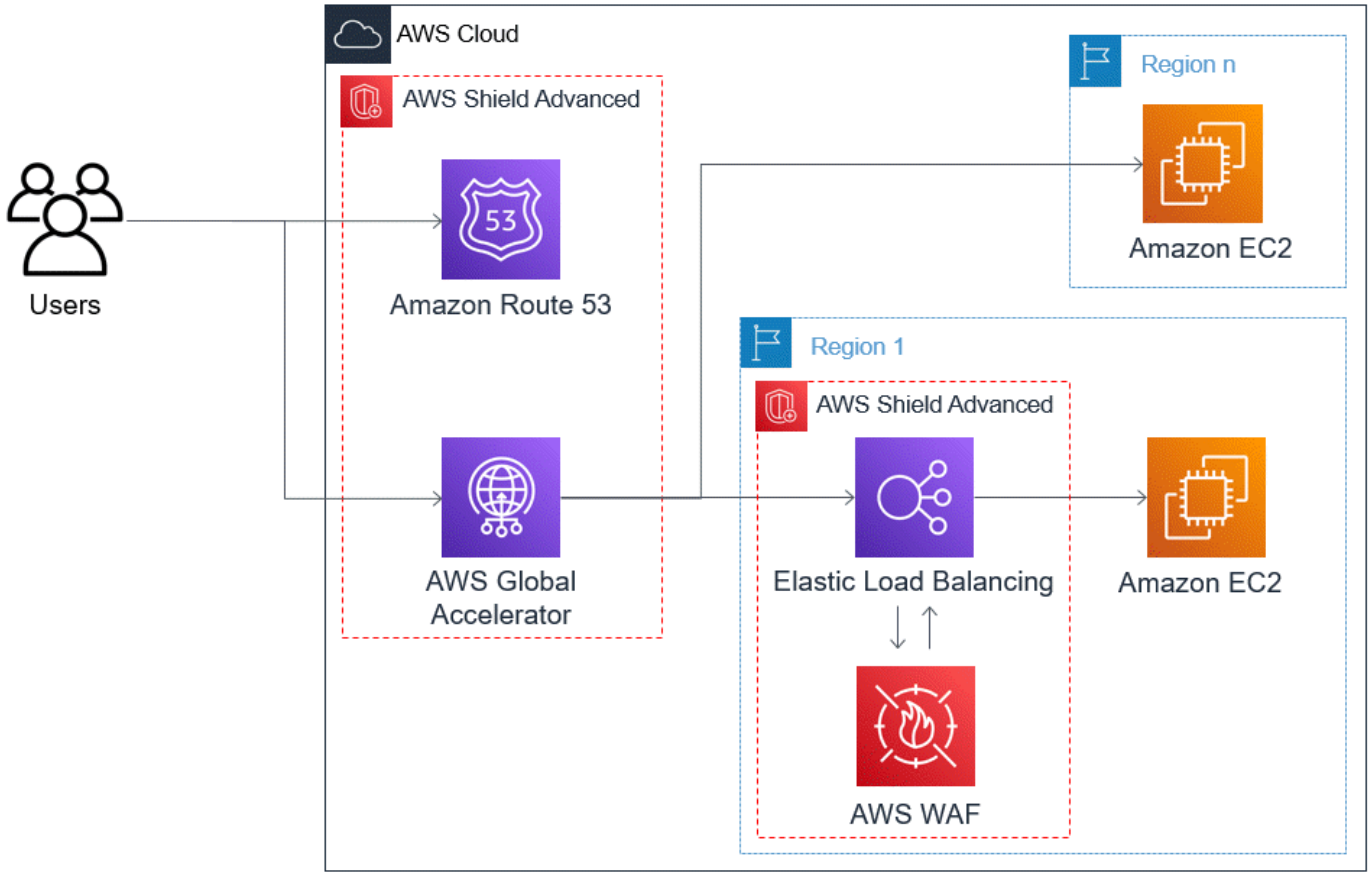
您可以依照此一般範例來改善下列應用程式類型的 DDoS 彈性：

- TCP 或 UDP 應用程式。例如，用於遊戲、IoT 和 IP 語音的應用程式。
- 需要靜態 IP 位址或使用 Amazon CloudFront 不支援之通訊協定的 Web 應用程式。例如，您的應用程式可能需要使用者可以新增至防火牆允許清單的 IP 位址，而且其他任何 AWS 客戶都不會使用這些 IP 位址。

您可以透過引入 Amazon Route 53 和 AWS Global Accelerator. 來改善這些應用程式類型的 DDoS 彈性。這些服務可以將使用者路由到您的應用程式，而且他們可以為您的應用程式提供靜態 IP 位址，這些 IP 位址是透過 AWS 全球邊緣網路傳送的任 全域加速器標準加速器可將使用者延遲提升高達 60%。如果您有 Web 應用程式，則可以在應用程式負載平衡器上執行應用程式，然後使用 Web ACL 保護 Application Load Balancer，藉此偵測並緩解 AWS WAF Web Application Load Balancer 層要求洪水。

建置應用程式之後，請使用 Shield Advanced 保護 Route 53 託管區域、全域加速器標準加速器，以及任何應用程式負載平衡器。當您保護應用程式負載平衡器時，您可以建立 AWS WAF Web ACL 的關聯，並為它們建立速率型規則。您可以透過關聯新的或現有的 Route 53 運作狀態檢查，為 Global Accelerator 標準加速器和應用程式負載平衡器設定 SRT 的主動互動。若要進一步瞭解這些選項，請參閱資源保護 AWS Shield Advanced。

下面的參考圖描述了 TCP 和 UDP 應用程序的 DDoS 彈性架構示例。



這種方法為您的應用程序提供的好處包括以下內容：

- 防止最大的已知基礎架構層（第 3 層和第 4 層）DDoS 攻擊。如果攻擊的數量從上游導致阻塞 AWS，則該故障將被隔離在更靠近其來源的位置，並將對您的合法使用者產生最小的影響。
- 保護 DNS 應用程式層攻擊，因為 Route 53 負責提供權威性 DNS 回應。
- 如果您有 Web 應用程序，則此方法可提供防止 Web 應用程序層請求洪水的保護。您在 AWS WAF Web ACL 中設定的以速率為基礎的規則會在來源 IP 傳送的要求數量超過規則允許的情況下封鎖這些 IP。
- 如果您選擇針對符合資格的資源啟用此選項，請與護 Shield 回應團隊 (SRT) 主動互動。當 Shield Advanced 偵測到會影響應用程式健康狀態的事件時，SRT 會使用您提供的聯絡資訊回應並主動與您的安全或營運團隊互動。

Shield 牌進階使用案例範例

您可以在多種情況下使用 Shield 進階來保護您的資源。但是，在某些情況下，您應該使用其他服務或將其他服務與 Shield Advanced 結合使用，以提供最佳保護。以下是如何使用 Shield 進階或其他 AWS 服務來協助保護您的資源的範例。

目標	建議的服務	相關的服務文件
保護 web 應用程式和 RESTful API 對抗 DDoS 攻擊	Shield 進階保護 Amazon CloudFront 分發和應用程式負載平衡器	Elastic Load Balancing 文件、Amazon CloudFront 文件
保護 TCP 為基礎的應用程式對抗 DDoS 攻擊	Shield 高級保護 AWS Global Accelerator 標準加速器; 連接到彈性 IP 地址	AWS Global Accelerator 文件, E lastic Load Balancing 說明文件
保護 UDP 為基礎的遊戲伺服器對抗 DDoS 攻擊	Shield 進階保護連接到彈性 IP 地址的 Amazon EC2 執行個體	Amazon Elastic Compute Cloud 文件

例如，如果您使用防 Shield 進階來保護彈性 IP 位址，則防 Shield 進階會保護任何與其相關聯的資源。在攻擊期間，Shield 牌進階會自動將您的網路 ACL 部署到網路邊界 AWS 。當您的網路 ACL 位於網路邊界時，防 Shield 進階可提供針對較大型 DDoS 事件的保護。一般而言，網路 ACL 會套用在 Amazon VPC 內的 Amazon EC2 執行個體附近。網路 ACL 只能緩解 Amazon VPC 和執行個體所能處理的攻擊大小。如果連接到 Amazon EC2 執行個體的網路界面最多可處理 10 Gbps，則 10 Gbps 以上的磁碟區會減慢速度，並且可能會封鎖傳送至該執行個體的流量。在攻擊期間，Shield Advanced 會將您的網路 ACL 提升到 AWS 邊界，這可以處理多 TB 的流量。您的網路 ACL 能夠提供您的資源遠超過網路典型容量的保護。如需網路 ACL 的詳細資訊，請參閱 網路 ACL。

開始使用 AWS Shield Advanced

本教學將逐步引導您如何開始 AWS Shield Advanced 使用 Shield 進階主控台。

> **Note**
>
> Shield 牌進階需要訂閱，但 AWS Shield Standard 不需要。Shield 標準版所提供的保護是免費提供給所有 AWS 客戶。

Shield Advanced 為網路層（第 3 層）、傳輸層（第 4 層）和應用程式層（第 7 層）攻擊提供進階 DDoS 偵測和緩解保護。如需有關 Shield 進階的更多資訊，請參閱AWS Shield Advanced 概述。

AWS 技術社區已經發布了一個自動化過程的示例，用於使用基礎結構作為代碼（IaC）工具 AWS CloudFormation 和 Terraform 配置 Shield 高級。如果您的帳戶屬於組織的一部分，而 AWS Organizations 且您要保護 Amazon Route 53 或以外的任何資源類型，則可以 AWS Firewall Manager 搭配此解決方案使用 AWS Global Accelerator。若要探索這個選項，請參閱 aws-sample/ aws-shield-advanced-one-按一下部署的程式碼儲存庫，以及 Shield 進階的一鍵部署中的教學課程。

> **Note**
>
> 在發生分散式拒絕服務 (DDoS) 事件之前，請務必先完整設定 Shield 進階。完成設定以協助確保您的應用程式受到保護，並且在您的應用程式受到 DDoS 攻擊的影響時，您可以做出回應。

依序執行下列步驟，以開始使用「Shield 牌進階」。

內容

订阅 AWS Shield Advanced

您必須為每個 AWS 帳戶 想要保護的項目訂閱護 Shield 進階版。您不需要訂閱 Shield 牌標準版。

Shield 牌進階訂閱計費

如果您是 AWS 通路經銷商，請洽詢您的帳戶團隊以取得相關資訊和指引。此帳單資訊適用於非 AWS 通路經銷商的客戶。

對於所有其他人，以下訂閱和計費準則適用：

- 對於屬於 AWS Organizations 組織成員的帳戶，無論付款人 AWS 帳戶本身是否已訂閱，都會針對組織的付款人帳戶收取 Shield Advanced 訂閱費用。
- 當您訂閱同一個AWS Organizations 合併帳單帳戶系列中的多個帳戶時，一個訂閱價格涵蓋該家庭中所有訂閱的帳戶。組織必須擁有所有 AWS 帳戶 及其所有資源。
- 當您為多個組織訂閱多個帳戶時，您仍然可以在所有組織、帳戶和資源中支付一筆訂閱費用，以便您擁有所有這些帳戶。請聯絡您的客戶經理或 AWS 支援人員，並要求豁免其中一個組織的 AWS Shield Advanced 訂閱費用。

如需詳細的定價資訊和範例，請參閱AWS Shield 定價。

使用簡化訂閱 AWS Firewall Manager

如果您的帳戶是組織的一部分，建議您盡可能 AWS Firewall Manager 使用，以自動化組織的訂閱和保護。Firewall Manager 員支援所有受保護的資源類型，Amazon Route 53 和 AWS Global Accelerator. 若要使用 Firewall Manager 員，請參閱AWS Firewall Manager和開始使用 AWS Firewall ManagerAWS Shield Advanced 政策。

如果您不使用 Firewall Manager，請針對每個具有保護資源的帳戶，使用下列程序訂閱並新增保護。

若要訂閱帳戶 AWS Shield Advanced

1. 登入 AWS Management Console 並開啟 Shield 牌主控台 AWS WAF (S)，網址為 https://console.aws.amazon.com/wafv2/。
2. 在AWS Shield導覽列中，選擇 [開始使用]。選擇訂閱 Shield 牌進階。
3. 在「訂閱 Shield 牌進階」頁面中，閱讀合約的每個條款，然後選取所有核取方塊，表示您接受這些條款。對於合併帳單系列中的帳戶，您必須同意每個帳戶的條款。

   > **Important**
   >
   > 訂閱後，若要取消訂閱，您必須聯絡AWS Support。
   > 若要停用訂閱的自動續訂，您必須使用 Shield API 作業UpdateSubscription或 CLI 命令更新訂閱。

   選擇訂閱 Shield 牌進階。這會將您的帳戶訂閱到神 Shield 進階版並啟用服務。

您的帳戶已訂閱。繼續執行以下步驟，使用神 Shield 進階保護您帳號的資源。

> **Note**
>
> 在您訂閱後，神 Shield 進階版不會自動保護您的資源。您必須指定希望「防 Shield 進階」來保護設定防護的資源。

新增資源以保護和設定保護

Shield Advanced 僅保護您透過「Shield 牌進階」或「Firewall Manager 員防護進階」策略中指定的資源。它不會自動保護訂閱帳戶的資源。

如果您使用 AWS Firewall Manager Shield 進階政策進行保護，則不需要執行此步驟。您可以使用要保護的資源類型設定策略，而 Firewall Manager 會自動將保護新增至策略範圍內的資源。

如果您不使用 Firewall Manager 員，請針對每個具有保護資源的帳戶執行下列程序。

使用防護進階選擇要保 Shield 的資源

1. 從先前程序的訂閱確認頁面，或從 [受保護的資源] 或 [概觀] 頁面選擇 [新增資源] 以保護資源。
2. 在 「選擇要使用 Shield 進階保護的資源」頁面的「指定區域」與「資源類型」中，針對您要保護的資源提供「區域」與「資源類型」規格。您可以選取「所有區域」來保護多個區域中的資源，也可以選取「全域」，將選取範圍縮小為全域資源。您可以取消選取任何不想保護的資源類型。如需有關資源類型保護的資訊，請參閱AWS Shield Advanced 依資源類型分類的保護。
3. 選擇「載入資源」。「Shield 牌進階」會將符合您條件的資源填入「選取 AWS 資源」區段。
4. 在 「選取資源」 區段中，您可以輸入要在資源清單中搜尋的字串，以篩選資源清單。

   選取您要保護的資源。
5. 在「標籤」區段中，如果您要將標籤新增至您正在建立的防 Shield 進階保護，請指定這些標籤。若要取得有關標籤 AWS 資源的資訊，請參閱〈使用標籤編輯器
6. 選擇使用 Shield 進階保護。這樣可以為資源增加護 Shield 進階保護。

繼續執行主控台精靈畫面，以完成資源保護的設定。

主題

- 設定應用程式層 (第 7 層) DDoS 防護 AWS WAF
- 針對您的保護設定健康型偵測

- 設定警報和通知
- 檢閱並完成您的防護組態

設定應用程式層 (第 7 層) DDoS 防護 AWS WAF

為了保護應用程式層資源，Shield Advanced 會使用具有速率規則的 AWS WAF Web ACL 作為起點。AWS WAF 是一種 Web 應用程式防火牆，可讓您監視轉寄至應用程式層資源的 HTTP 和 HTTPS 要求，並可讓您根據要求的特性控制內容的存取。以速率為基礎的規則會根據您的要求彙總準則限制流量，為您的應用程式提供基本的 DDoS 保護。如需詳細資訊，請參閱 如何 AWS WAF 工作 及 速率型規則陳述式。

您也可以選擇性地啟用 Shield Advanced 自動應用程式層 DDoS 緩解功能，讓 Shield 來自已知 DDoS 來源的進階速率限制要求，並自動為您提供特定於事件的保護。

> **Important**
>
> 如果您透過 AWS Firewall Manager 使用 Shield 進階政策來管理您的 Shield 進階防護，則無法在此管理應用程式層防護。您必須在 Firewall Manager 員防 Shield 進階政策中管理它們。

Shield 高級訂閱和 AWS WAF 成本

您的 Shield 進階訂閱可涵蓋使用標準 AWS WAF 功能來保護您使用 Shield 進階保護的資源所需的費用。Shield Advanced 保護所涵蓋的標準 AWS WAF 費用包括每個 Web ACL 的成本、每個規則的成本，以及每百萬個 Web 請求檢查請求的基本價格，最高可達 1,500 個 WCU，最高可達到預設主體大小。

啟用防 Shield 進階自動應用程式層 DDoS 緩解功能會將規則群組新增至使用 150 個 Web ACL 容量單位 (WCU) 的網路 ACL。這些 WCU 會計入您網路 ACL 中的 WCU 使用量。如需詳細資訊，請參閱Shield 先進的自動應用層 DDoS 緩解、Shield 牌進階規則群組及AWS WAF 網路 ACL 容量單位 (WCU)。

您 AWS WAF 對 Shield 進階版的訂閱並不涵蓋您未使用神 Shield 進階保護的資源使用。它也不包括受保護資源的任何額外非標準 AWS WAF 成本。非標準 AWS WAF 成本的範例包括機器人控制、CAPTCHA規則動作、使用超過 1,500 個 WCU 的 Web ACL，以及檢查超出預設主體大小的要求主體。完整列表在 AWS WAF 定價頁面上提供。

如需完整資訊和定價範例，請參閱 Shield 定價和AWS WAF 定價。

設定區域的第 7 層 DDoS 保護

Shield 牌進階讓您可以選擇為所選資源所在的每個區域設定第 7 層 DDoS 緩解措施。如果您要在多個地區新增保護，精靈會引導您完成每個區域的下列程序。

1. [設定第 7 層 DDoS 防護] 頁面會列出尚未與 Web ACL 相關聯的每個資源。對於這些 ACL，請選擇現有的 Web ACL 或建立新的 Web ACL。對於任何已經有關聯 Web ACL 的資源，您可以先取消目前 ACL 的關聯，以變更 Web ACL。 AWS WAF如需詳細資訊，請參閱 建立 Web ACL 與資源的關聯或取消關聯 AWS。

   對於尚未具有以速率為基礎的規則的 Web ACL，設定精靈會提示您新增一個。以速率為基礎的規則會在傳送大量要求時限制來自 IP 位址的流量。速率型規則有助於保護您的應用程式免受 Web 要求洪水的影響，並提供有關流量突然峰值的警示，這些警示可能表示潛在的 DDoS 攻擊。選擇新增費率限制規則，然後提供費率限制和規則動作，將以速率為基礎的規則新增至 Web ACL。您可以透過 AWS WAF在 Web ACL 中設定其他保護。

   如需在 Shield 進階保護中使用 Web ACL 和速率型規則的相關資訊，包括以速率為基礎的規則的其他組態選項，請參閱。Shield 進階應用程式層 AWS WAF Web ACLs 和速率型規則

2. 對於自動應用程式層 DDoS 緩解，如果您想讓 Shield Advanced 自動緩解對應用程式層資源的 DDoS 攻擊，請選擇 [啟用]，然後選取 AWS WAF 您希望 Shield Advanced 在其自訂規則中使用的規則動作。此設定會套用至您在此精靈階段作業中管理之資源的所有 Web ACL。

   借助自動應用層 DDoS 緩解功能，Shield Advanced 在資源的 AWS WAF Web ACL 中維護基於速率的規則，以限制來自已知 DDoS 來源的請求量。此外，Shield Advanced 會將目前的流量模式與歷史流量基準進行比較，以偵測可能表示 DDoS 攻擊的偏差。當 Shield Advanced 偵測到 DDoS 攻擊時，會透過建立、評估和部署自訂 AWS WAF 規則來回應。您可以指定自訂規則是代表您計數還是封鎖攻擊。

   > **Note**
   >
   > 自動應用程式層 DDoS 防護功能僅適用於使用最新版本的 AWS WAF (v2) 建立的 Web ACL。

   有關 Shield 高級自動應用程序層 DDoS 緩解的更多信息，包括使用此功能的警告和最佳實踐，請參閱。Shield 先進的自動應用層 DDoS 緩解

3. 選擇下一步。主控台精靈會前進至健全狀況型偵測頁面。

針對您的保護設定健康型偵測

設定 Shield Advanced 以使用健康狀況型偵測來改善攻擊偵測和緩解的回應速度和準確性。配置良好的健康狀態檢查對於準確偵測事件至關重要。您可以針對任何資源類型 (Route 53 託管區域除外) 設定健全狀況型偵測。

若要使用健康狀態偵測，請在 Route 53 中為您的資源定義健康狀態檢查，然後將健康狀態檢查與您的 Shield 進階防護建立關聯。您設定的健康狀態檢查必須準確反映資源的健全狀況。如需設定健康狀態檢查以搭配 Shield Advanced 搭配使用的資訊和範例，請參閱以 Health 狀態檢查為基礎的偵測。

Shield 牌應變團隊 (SRT) 主動參與支援需要運作 Health 態檢查。如需主動參與的相關資訊，請參閱設定主動參與。

> **Note**
>
> 當您將 Health 狀態檢查與 Shield 進階保護建立關聯時，健康狀態檢查必須正常報告。

若要設定健全狀況型偵測

1. 在 Associate Health Check (關聯運作狀態檢查) 下，選擇您要與保護產生關聯的運作狀態檢查 ID。

   > **Note**
   >
   > 如果您沒有看到所需的健康狀態檢查，請移至 Route 53 主控台並驗證健康狀態檢查及其 ID。如需相關資訊，請參閱建立和更新運作狀態檢查。

2. 選擇下一步。主控台精靈會前進到 [警示和通知] 頁面。

設定警報和通知

您可以選擇針對偵測到的 Amazon CloudWatch 警示和以速率為基礎的規則活動設定 Amazon 簡單通知服務通知。當 Shield 偵測到受保護資源上的事件，或者超過以速率為基礎的規則中設定的速率限制時，您可以使用這些功能來接收通知。

如需「Shield 進階 CloudWatch 」度量的資訊，請參閱AWS Shield Advanced 度量。如需 Amazon SNS 的相關資訊，請參閱 Amazon 簡易通知服務開發人員指南。

若要設定警示與通知

1. 選取您要通知的 Amazon SNS 主題。您可以針對所有受保護的資源和速率型規則使用單一 Amazon SNS 主題，也可以選擇針對組織自訂的不同主題。例如，您可以為負責特定資源集事件回應的每個團隊建立 SNS 主題。
2. 選擇下一步。主控台精靈會前進至資源保護檢閱頁面。

檢閱並完成您的防護組態

檢閱和設定您的設定

1. 在 [檢閱和設定 DDoS 緩和能見度] 頁面中，檢閱您的設定。若要進行修改，請在您要修改的區域中選擇「編輯」。這會帶您回到主控台精靈中的相關頁面。進行變更，然後在後續頁面中選擇 [下一步]，直到您返回 [檢閱並設定 DDoS 緩和能見度] 頁面為止。
2. 選擇 [完成組態]。受保護的資源頁面會列出您新受保護的資源。

設定 AWS SRT 支援

Shield 牌應變團隊（SRT）是專門從事 DDoS 事件響應的安全工程師。您可以選擇性地新增權限，讓 SRT 在 DDoS 事件期間代表您管理資源。此外，如果與受保護資源相關聯的 Route 53 健康狀態檢查在偵測到的事件期間不健康，您可以設定 SRT 主動與您互動。這兩種新增的保護功能都可以更快地回應 DDoS 事件。

> **Note**
>
> 若要使用 Shield 牌回應團隊 (SRT) 的服務，您必須訂閱商業 Support 計劃或企業 Support 計劃。

SRT 可以在應用程式層事件期間監控 AWS WAF 要求資料和記錄，以識別異常流量。他們可以幫助制定自定義 AWS WAF 規則以減輕違規流量來源。SRT 可能會視需要提出架構建議，協助您將資源與建 AWS 議更有效地調整。

如需 SRT 的詳細資訊，請參閱Shield 牌回應小組 (SRT) 支援。

若要授與 SRT 權限

1. 在 AWS Shield 主控台 [概觀] 頁面的 [設定 AWS SRT 支援] 下，選擇 [編輯 SRT 存取權]。編輯 AWS Shield 牌回應小組 (SRT) 存取頁面隨即開啟。
2. 對於 SRT 存取設定，請選取下列其中一個選項：
   - 請勿將 SRT 存取權授予我的帳戶 — Shield 會移除您先前授予 SRT 的任何權限，以存取您的帳戶和資源。
   - 為 SRT 建立新角色以存取我的帳戶 — Shield 會建立信任代表 SRT 的服務主體的角色`drt.shield.amazonaws.com`，並將受管理的原則附加`AWSShieldDRTAccessPolicy`至該角色。受管政策允許 SRT 代表您進行呼叫 AWS Shield Advanced 和 AWS WAF API 呼叫，並存取您的 AWS WAF 記錄。如需受管政策的更多相關資訊，請參閱AWS 受管理的策略：AWSShieldDRTAccessPolicy。
   - 選擇 SRT 的現有角色以存取我的帳戶 — 對於此選項，您必須在 AWS Identity and Access Management (IAM) 中修改角色的組態，如下所示：
     - 將受管政策 `AWSShieldDRTAccessPolicy` 連接至角色。此受管政策允許 SRT 代表您進行呼叫 AWS Shield Advanced 和 AWS WAF API 呼叫，並存取您的 AWS WAF 記錄。如需受管政策的更多相關資訊，請參閱AWS 受管理的策略： AWSShieldDRTAccessPolicy。如需將受管政策附加到角色的相關資訊，請參閱附加和卸離 IAM 政策。
     - 修改角色以信任服務委託人 `drt.shield.amazonaws.com`。這是代表 SRT 的服務主體。如需詳細資訊，請參閱 IAM JSON 政策元素：委託人。
3. 選擇儲存，以儲存變更。

如需有關讓 SRT 存取您的保護和資料的詳細資訊，請參閱。設定護 Shield 回應群組 (SRT) 的存取權限

啟用 SRT 主動參與

1. 在主 AWS Shield 控台 [概觀] 頁面的 [主動互動和連絡人] 底下，選擇 [連絡人] 區域中的 [編輯]。

   在 [編輯連絡人] 頁面中，提供您希望 SRT 連絡人以進行主動參與的人員的聯絡資訊。

   如果您提供多個聯絡人，請在「備註」中指明應使用每個聯絡人的情況。包括主要和次要聯絡人指定，並提供每個聯絡人的可用時間和時區。

   範例連絡人備註：

   - 這是一個全天候工作人員的熱線。請與響應分析師合作，他們將在通話中獲得合適的人員。

- 如果熱線在 5 分鐘內沒有回復，請與我聯繫。

2. 選擇儲存。

   「概觀」頁面會反映更新的聯絡資訊。

3. 選擇 [編輯主動互動] 功能，選擇 [啟用]，然後選擇 [儲存] 以啟用主動式互動。

如需主動參與的詳細資訊，請參閱設定主動參與。

在中創建 DDoS 儀表板 CloudWatch 並設置 CloudWatch 警報

您可以使用 Amazon 監控潛在的 DDoS 活動 CloudWatch，Amazon 會從 Shield Advanced 收集原始資料，並將其處理為可讀且近乎即時的指標。您可以在中使用統計資料 CloudWatch 來瞭解 Web 應用程式或服務的執行方式。如需有關使用的詳細資訊 CloudWatch，請參閱 Amazon 使用 CloudWatch 者指南 CloudWatch中的內容。

- 如需建立 CloudWatch 管控面板的指示，請參閱使用 Amazon 監控 CloudWatch。
- 如需可新增至儀表板的「Shield 牌進階」指標的說明，請參閱AWS Shield Advanced 度量。

Shield Advanced 在 DDoS 事件期間回 CloudWatch 報資源指標的頻率高於沒有事件正在進行的情況下。「Shield 牌進階」會在活動期間每分鐘報告一次指標，然後在活動結束後立即報告一次。雖然沒有任何事件正在進行中，Shield Advanced 會在指派給資源的時間每天報告一次度量。此定期報告會保持指標處於作用中狀態，並可用於您的自訂 CloudWatch 警示。

這樣就完成了開始使用「Shield 牌進階」的教學課程。若要充分利用您選擇的保護功能，請繼續探索 Shield 進階的功能和選項。首先，請熟悉在DDoS 事件的可見性和中檢視和回應事件的選項。回應 DDoS 事件

Shield 牌回應小組 (SRT) 支援

Shield 牌應變團隊 (SRT) 為 Shield 牌進階客戶提供額外的支援。SRT 是專門從事 DDoS 事件響應的安全工程師。作為 AWS Support 計劃的另一層支持，您可以直接與 SRT 合作，利用他們的專業知識作為事件響應工作流程的一部分。如需選項的相關資訊以及設定指引，請參閱下列主題。

> **Note**
>
> 若要使用 Shield 牌回應團隊 (SRT) 的服務，您必須訂閱商業 Support 計劃或企業 Support 計劃。

SRT 支援活動

與 SRT 互動的主要目標是保護應用程式的可用性和效能。根據 DDoS 事件的類型和應用程式的架構，SRT 可能會採取下列一或多個動作：

- AWS WAF 日誌分析和規則 — 對於使用 AWS WAF Web ACL 的資源，SRT 可以分析您的 AWS WAF 日誌，以識別應用程序 Web 請求中的攻擊特徵。在您參與過程中的批准後，SRT 可以將更改應用於您的 Web ACL，以阻止他們所識別的攻擊。
- 建置自訂網路緩和措施 — SRT 可為您撰寫自訂的緩和措施，以進行基礎架構層攻擊。SRT 可與您合作，瞭解應用程式預期的流量、封鎖非預期的流量，以及最佳化每秒封包速率限制。如需詳細資訊，請參閱 使用 Shield 牌回應小組 (SRT) 設定自訂緩和措施。
- 網路流量工程 — SRT 與網 AWS 路團隊密切合作，保護 Shield 進階客戶。必要時， AWS 可以變更網際網路流量到達 AWS 網路的方式，以便為您的應用程式配置更多緩解容量。
- 架構建議 — SRT 可能會判斷攻擊的最佳緩解措施是否需要架構變更才能與 AWS 最佳實務保持一致，而且它們將有助於支援您實作這些做法。如需詳細資訊，請參閱 DDoS 彈性的AWS 最佳做法。

主題

設定護 Shield 回應群組 (SRT) 的存取權限

您可以授予 Shield 回應團隊 (SRT) 的權限，以代表您採取行動、存取您的 AWS WAF 記錄以及呼叫 AWS Shield Advanced 和 AWS WAF API 以管理保護。在應用程式層 DDoS 事件期間，SRT 可監控 AWS WAF 要求以識別異常流量，並協助制定自訂 AWS WAF 規則以減輕違規流量來源。

此外，您可以將 SRT 存取權授與存放在 Amazon S3 儲存貯體中的其他資料，例如來自 Application Load Balancer CloudFront、Amazon 或第三方來源的封包擷取或日誌。

> **Note**
>
> 若要使用 Shield 牌回應團隊 (SRT) 的服務，您必須訂閱商業 Support 計劃或企業 Support 計劃。

若要管理 SRT 的權限

1. 在 AWS Shield 主控台 [概觀] 頁面的 [設定 AWS SRT 支援] 下，選擇 [編輯 SRT 存取權]。編輯 AWS Shield 牌回應小組 (SRT) 存取頁面隨即開啟。
2. 對於 SRT 存取設定，請選取下列其中一個選項：
   - 請勿將 SRT 存取權授予我的帳戶 — Shield 會移除您先前授予 SRT 存取帳號和資源的任何權限。
   - 為 SRT 建立新角色以存取我的帳戶 — Shield 會建立信任代表 SRT 的服務主體的角色`drt.shield.amazonaws.com`，並將受管理的原則附加`AWSShieldDRTAccessPolicy`至該角色。受管政策允許 SRT 代表您進行呼叫 AWS Shield Advanced 和 AWS WAF API 呼叫，並存取您的 AWS WAF 記錄。如需受管政策的更多相關資訊，請參閱AWS 受管理的策略：AWSShieldDRTAccessPolicy。
   - 選擇 SRT 的現有角色以存取我的帳戶 — 對於此選項，您必須在 AWS Identity and Access Management (IAM) 中修改角色的組態，如下所示：
     - 將受管政策 `AWSShieldDRTAccessPolicy` 連接至角色。此受管政策允許 SRT 代表您進行呼叫 AWS Shield Advanced 和 AWS WAF API 呼叫，並存取您的 AWS WAF 記錄。如需受管政策的更多相關資訊，請參閱AWS 受管理的策略： AWSShieldDRTAccessPolicy。如需將受管政策附加到角色的相關資訊，請參閱附加和卸離 IAM 政策。
     - 修改角色以信任服務委託人 `drt.shield.amazonaws.com`。這是代表 SRT 的服務主體。如需詳細資訊，請參閱 IAM JSON 政策元素：委託人。
3. 對於（可選）：如果您需要共用 AWS WAF Web ACL 日誌中不存在的資料，請對 Amazon S3 儲存貯體授予 SRT 存取權，請進行設定。例如，Application Load Balancer 存取日誌、Amazon CloudFront 日誌或來自第三方來源的日誌。

   > **Note**
   >
   > 您不需要為您的 AWS WAF Web ACL 日誌執行此操作。當您授予帳戶存取權時，SRT 可以存取這些資訊。

   a. 根據下列準則設定 Amazon S3 儲存貯體：
      - 值區位置必須與您授予 SRT 一般存取權限的位置相同 AWS 帳戶 ，在先前的步驟「AWS Shield 牌回應小組」(SRT) 存取權限中。

- 存儲桶可以是純文本或 SSE-S3 加密。如需有關 Amazon S3 SSE-S3 加密的詳細資訊，請參閱 Amazon S3 使用者指南中的使用伺服器端加密搭配 Amazon S3 受管加密金鑰 (SSE-S3) 來保護資料。

  SRT 無法檢視或處理儲存在值區中的記錄，而這些記錄是使用儲存在 AWS Key Management Service (AWS KMS) 中的金鑰加密的。

b. 在 Shield 牌進階 (選用)：授予對 Amazon S3 儲存貯體的 SRT 存取權限區段，針對存放資料或日誌的每個 Amazon S3 儲存貯體，輸入儲存貯體的名稱，然後選擇新增儲存貯體。您最多可以新增 10 個儲存貯體。

   這會授與 SRT 對每個儲存貯體的下列權限：`s3:GetBucketLocations3:GetObject`、和`s3:ListBucket`。

   如果您想要授與 SRT 存取超過 10 個值區的權限，您可以透過編輯其他值區政策並手動授與此處列出的 SRT 權限來執行此操作。

   以下顯示原則清單的範例。

```
{
    "Sid": "AWSDDoSResponseTeamAccessS3Bucket",
    "Effect": "Allow",
    "Principal": {
        "Service": "drt.shield.amazonaws.com"
    },
    "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource": [
        "arn:aws:s3:::bucket-name",
        "arn:aws:s3:::bucket-name/*"
    ]
}
```

4. 選擇儲存，以儲存變更。

您也可以透過 API 授權 SRT，方法是建立 IAM 角色，將政策附加 AWSShieldDRTAccessPolicy 至該角色，然後將角色傳遞給作業 AtRtRole。

設定主動參與

透過主動互動，Shield 回應團隊 (SRT) 會在應用程式的可用性或效能因可能遭受攻擊而受到影響時，直接與您聯絡。我們建議使用此參與模型，因為它提供了最快的 SRT 回應，並允許 SRT 在與您建立聯繫之前就開始進行疑難排解。

主動參與適用於彈性 IP 地址和 AWS Global Accelerator 標準加速器上的網路層和傳輸層事件，以及 Amazon CloudFront 分發和應用程式負載平衡器上的 Web 請求洪水。主動參與僅適用於具有相關聯 Amazon Route 53 運作狀態檢查的 Shield 牌進階資源保護。如需有關管理和使用健康狀態檢查的資訊，請參閱以 Health 狀態檢查為基礎的偵測。

在 Shield Advanced 偵測到的事件期間，SRT 會使用您的健康狀態檢查狀態來判斷該活動是否符合主動參與的資格。如果是這樣，SRT 會根據您在主動互動組態中提供的聯絡指引與您連絡。

您最多可以配置十個聯繫人以進行主動互動，並且可以提供說明以指導 SRT 與您聯繫。您的主動互動聯繫人應該可以在活動期間與 SRT 互動。如果您沒有全年無休的營運中心，您可以提供呼叫器連絡人，並在您的聯絡備註中指明此聯絡偏好設定。

主動參與需要您執行以下操作：

- 您必須訂閱商務 Support 方案或企業 Support 方案。
- 您必須將 Amazon Route 53 運作狀態檢查與任何想要透過主動互動保護的資源建立關聯。SRT 會使用健康狀態檢查的狀態來協助判斷事件是否需要主動參與，因此您的健康狀態檢查必須準確反映受保護資源的狀態。如需詳細資訊和指引，請參閱以 Health 狀態檢查為基礎的偵測。
- 對於與 AWS WAF Web ACL 相關聯的資源，您必須使用 AWS WAF (v2) 建立 Web ACL，這是的最新版本 AWS WAF。
- 您必須提供至少一個聯絡人，SRT 才能在活動期間用於主動參與。保持您的聯繫信息完整和最新。

啟用 SRT 主動參與

1. 在主 AWS Shield 控台 [概觀] 頁面的 [主動互動和連絡人] 底下的 [連絡人] 區域中，選擇 [編輯]。

   在 [編輯連絡人] 頁面中，提供您希望 SRT 連絡人以進行主動參與的人員的聯絡資訊。

   如果您提供多個聯絡人，請在「備註」中指明應使用每個聯絡人的情況。包括主要和次要聯絡人指定，並提供每個聯絡人的可用時間和時區。

   範例連絡人備註：

   - 這是一個全年無休的人員熱線。請與響應分析師合作，他們將在通話中獲得合適的人員。

- 如果熱線在 5 分鐘內沒有回復，請與我聯繫。

2. 選擇儲存。

   「概觀」頁面會反映更新的聯絡資訊。

3. 選擇編輯主動參與功能，選擇啟用，然後選擇儲存以啟用主動互動。

聯繫 Shield 牌響應小組（SRT）

您可以透過下列其中一種方式聯絡護 Shield 回應小組 (SRT)：

支援案例

您可以AWS Shield在 Sup AWS port 中心主控台中開啟案例。

如需建立支援案例的指引，請參閱AWS Support 中心。

選擇適合您情況的嚴重性，並提供您的聯繫方式。在說明中，盡可能提供詳細資訊。提供您認為可能受到影響的任何受保護資源的相關資訊，以及使用者體驗的目前狀態。例如，如果您的使用者體驗降級或部分應用程式目前無法使用，請提供該資訊。

- 對於可疑的 DDoS 攻擊 — 如果您的應用程式的可用性或效能目前受到可能的 DDoS 攻擊影響，請選擇下列嚴重性和聯絡選項：
  - 針對嚴重性，請選擇支援方案可用的最高嚴重性：
    - 對於業務支持，這是生產系統關閉：<1 小時。
    - 對於企業支持，這是關鍵業務系統故障：<15 分鐘。
  - 對於聯繫選項，請選擇電話或聊天並提供您的詳細信息。使用實時聯繫方式提供最快的響應。

主動參與

透過 AWS Shield Advanced 主動互動，如果與受保護資源相關聯的 Amazon Route 53 運作狀態檢查在偵測到的事件期間變得不健康，SRT 會直接與您聯絡。如需有關此選項的詳細資訊，請參閱 設定主動參與。

使用 Shield 牌回應小組 (SRT) 設定自訂緩和措施

針對彈性 IP (EIP) 和 AWS Global Accelerator 標準加速器，您可以與護 Shield 回應小組 (SRT) 合作，設定自訂緩和措施。如果您知道放置緩和措施時應強制執行的特定邏輯，這很有用。例如，您可能希望

只允許來自特定國家/地區的流量、強制執行特定速率限制、設定選擇性驗證、不允許片段，或只允許符合封包裝載中特定模式的流量。

常見的自訂緩和措施範例包括：

- 模式比對 — 如果您操作的服務與用戶端應用程式互動，您可以選擇比對這些應用程式特有的已知模式。例如，您可能需要使用者安裝您散發的特定軟體的遊戲或通訊服務。您可以在應用程序發送到服務的每個數據包中包含一個幻數。您最多可以匹配 128 個字節（單獨或連續）的非碎片 TCP 或 UDP 數據包有效負載和標頭。相符項目可以用十六進位標記法表示為封包裝載開始的特定偏移量，或是在已知值之後的動態偏移量。例如，緩和措施可以尋找位元組，`0x01`然後預期`0x12345678`為接下來的四個位元組。
- DNS 專屬 — 如果您使用全球加速器或 Amazon 彈性運算雲端 (Amazon EC2) 等服務來操作自己的授權 DNS 服務，您可以請求自訂緩解措施來驗證封包，以確保封包是有效的 DNS 查詢，並套用可評估 DNS 流量特定屬性的懷疑評分。

若要詢問如何使用 SRT 來建置自訂緩和措施，請在下建立支援案例。 AWS Shield若要深入瞭解如何建立 AWS Support 案例，請參閱開始使用 AWS Support。

資源保護 AWS Shield Advanced

您可以新增和設定資源的 AWS Shield Advanced 保護。您可以管理單一資源的保護，也可以將受保護的資源分組到邏輯集合中，以便更好地管理事件。您也可以使 AWS Config用追蹤 Shield 牌進階防護的變更。

主題

- AWS Shield Advanced 依資源類型分類的保護
- AWS Shield Advanced 應用程式層 (第 7 層) 保護
- 以 Health 狀態檢查為基礎的偵測
- 管理資源保護 AWS Shield Advanced
- AWS Shield Advanced 保護群組
- 追蹤資源保護變更 AWS Config

AWS Shield Advanced 依資源類型分類的保護

Shield 高級保護在網絡和傳輸層（第 3 層和 4 層）和應用層（第 7 層）的 AWS 資源。您可以直接保護某些資源，也可以透過與受保護的資源建立關聯，Shield 高級支持 IPv4，並且不支持 IPv6。

本節提供有關每種資源類型的「Shield 進階保護」的資訊。

> **Note**
>
> 護 Shield 進階僅保護您在 Shield 牌進階或透過護 Shield 進階策略指定的資源。 AWS Firewall Manager 它不會自動保護您的資源。

您可以使用「Shield 牌進階」，透過下列資源類型進行進階監控和防護：

- Amazon CloudFront 分佈。針對 CloudFront 持續部署，Shield Advanced 會保護任何與受保護主要發行版相關聯的暫存散發。
- Amazon 路線 53 託管區域。
- AWS Global Accelerator 標準加速器。
- Amazon EC2 彈性 IP 地址。Shield 進階保護與受保護的彈性 IP 位址相關聯的資源。
- Amazon EC2 執行個體，透過與 Amazon EC2 彈性 IP 地址的關聯。
- 下列 Elastic Load Balancing (ELB) 負載平衡器：
  - 應用程式負載平衡器。
  - Classic Load Balancer。
  - 網路負載平衡器，透過與 Amazon EC2 彈性 IP 地址的關聯。

您無法使用「Shield 牌進階」來保護任何其他資源類型。例如，您無法保護 AWS Global Accelerator 自訂路由加速器或閘道負載平衡器。

每種資源類型最多可監控和保護 1,000 個資源 AWS 帳戶。例如，在單一帳戶中，您可以保護 1,000 個 Amazon EC2 彈性 IP 地址、1,000 個 CloudFront 分發和 1,000 個應用程式負載平衡器。您可以透過 Service Quotas 主控台 https://console.aws.amazon.com/servicequotas/ 申請增加使用 Shield 牌進階保護的資源數量。

使用 Shield 護進階保護 Amazon EC2 執行個體和網路負載平衡器

您可以先將這些資源附加到彈性 IP 地址，然後在 Shield 進階中保護彈性 IP 地址，以保護 Amazon EC2 執行個體和網路負載平衡器。

當您保護彈性 IP 位址時，防 Shield 進階會識別並保護它們所附加的資源。Shield Advanced 會自動識別附加至彈性 IP 位址的資源類型，並針對該資源套用適當的偵測和緩和措施。這包括設定彈性 IP 位址

專屬的網路 ACL。如需將彈性 IP 地址與 AWS 資源搭配使用的詳細資訊，請參閱下列指南：Amazon 彈性運算雲端文件或 E lastic Load Balancing 說明文件。

在攻擊期間，Shield 牌進階會自動將您的網路 ACL 部署到網路邊界 AWS 。當您的網路 ACL 位於網路邊界時，防 Shield 進階可提供針對較大型 DDoS 事件的保護。一般而言，網路 ACL 會套用在 Amazon VPC 內的 Amazon EC2 執行個體附近。網路 ACL 只能緩解 Amazon VPC 和執行個體所能處理的攻擊大小。例如，如果連接到 Amazon EC2 執行個體的網路界面最多可處理 10 Gbps，則超過 10 Gbps 的磁碟區會減慢速度，並可能封鎖傳送至該執行個體的流量。在攻擊期間，Shield Advanced 會將您的網路 ACL 提升到 AWS 邊界，這可以處理多 TB 的流量。您的網路 ACL 能夠提供您的資源遠超過網路典型容量的保護。如需網路 ACL 的詳細資訊，請參閱 網路 ACL。

某些擴展工具，例如 AWS Elastic Beanstalk，不允許您將彈性 IP 地址自動附加到 Network Load Balancer。對於這些情況，您需要手動附加彈性 IP 地址。

AWS Shield Advanced 應用程式層 (第 7 層) 保護

若要使用 Shield Advanced 保護您的應用程式層資源，請先將 AWS WAF Web ACL 與資源建立關聯，然後在其中新增一或多個以速率為基礎的規則。您還可以啟用自動應用程式層 DDoS 緩解功能，這會使 Shield Advanced 代表您自動建立和管理 Web ACL 規則，以回應 DDoS 攻擊。

當您使用 Shield Advanced 保護應用程式層資源時，Shield Advanced 會分析一段時間內的流量，以建立和維護基準。Shield 牌進階使用這些基準來偵測流量模式中可能表示 DDoS 攻擊的異常情況。Shield Advanced 偵測到攻擊的時間點取決於 Shield Advanced 在攻擊前能夠觀察到的流量，以及您用於 Web 應用程式的架構。可能會影響 Shield Advanced 行為的架構差異包括您使用的執行個體類型、執行個體大小，以及執行個體類型是否支援增強型聯網。您也可以將 Shield Advanced 設定為針對應用程式層攻擊自動放置緩和措施。

Shield 高級訂閱和 AWS WAF 成本

您的 Shield 進階訂閱可涵蓋使用標準 AWS WAF 功能來保護您使用 Shield 進階保護的資源所需的費用。Shield Advanced 保護所涵蓋的標準 AWS WAF 費用包括每個 Web ACL 的成本、每個規則的成本，以及每百萬個 Web 請求檢查請求的基本價格，最高可達 1,500 個 WCU，最高可達到預設主體大小。

啟用防 Shield 進階自動應用程式層 DDoS 緩解功能會將規則群組新增至使用 150 個 Web ACL 容量單位 (WCU) 的網路 ACL。這些 WCU 會計入您網路 ACL 中的 WCU 使用量。如需詳細資訊，請參閱Shield 先進的自動應用層 DDoS 緩解、Shield 牌進階規則群組及AWS WAF 網路 ACL 容量單位 (WCU)。

您 AWS WAF 對 Shield 進階版的訂閱並不涵蓋您未使用神 Shield 進階保護的資源使用。它也不包括受保護資源的任何額外非標準 AWS WAF 成本。非標準 AWS WAF 成本的範例包括機器人控制、CAPTCHA規則動作、使用超過 1,500 個 WCU 的 Web ACL，以及檢查超出預設主體大小的要求主體。完整列表在 AWS WAF 定價頁面上提供。

如需完整資訊和定價範例，請參閱 Shield 定價和AWS WAF 定價。

主題

- 偵測和緩解
- Shield 進階應用程式層 AWS WAF Web ACLs 和速率型規則
- Shield 先進的自動應用層 DDoS 緩解

偵測和緩解

本節說明 Shield Advanced 影響偵測和緩解應用程式層事件的因素。

運作狀態檢查

運作狀態檢查可準確報告應用程式的整體 Health 狀態，為 Shield Advanced 提供應用程式所遇到之流量狀況的相關資訊。當您的應用程式回報不健康狀態時，Shield Advanced 需要較少的資訊指向潛在攻擊，而且如果您的應用程式回報狀況良好，則需要更多攻擊證據。

請務必設定健康狀態檢查，以便準確地報告應用程式健康狀態。如需詳細資訊和指引，請參閱以 Health 狀態檢查為基礎的偵測。

流量基準

流量基準會為您的應用程式提供 Shield 進階資訊，以瞭解正常流量的特性。Shield Advanced 會使用這些基準來辨識您的應用程式何時未接收正常流量。因此它可以通知您，並在設定後開始設計和測試緩解選項以應對潛在攻擊。如需 Shield Advanced 如何使用流量基準偵測潛在事件的詳細資訊，請參閱概觀一節應用程式層威脅的偵測邏輯。

「Shield 牌進階」會根據與受保護資源相關聯的 Web ACL 所提供的資訊建立其基準線。Web ACL 必須與資源建立關聯至少 24 小時，最多 30 天，讓 Shield 進階才能可靠地判斷應用程式的基準。所需的時間會從您透過防護進階或透過防護 ACL 建立關聯時開始 AWS WAF。

如需使用 Web ACL 搭配防護進階應用程式層保護的詳細資訊，請參閱Shield 進階應用程式層 AWS WAF Web ACLs 和速率型規則。

速率為基礎的規則

以速率為基礎的規則有助於緩解攻擊。他們還可以掩蓋攻擊，方法是在攻擊成為足夠大的問題以顯示在正常流量基準或健康狀態檢查狀態報告中之前緩解攻擊。

當您使用 Shield Advanced 保護應用程式資源時，建議您在 Web ACL 中使用以速率為基礎的規則。儘管他們的緩和措施可能會掩蓋潛在的攻擊，但它們仍然是寶貴的第一道防線，可協助確保您的應用程式可供合法客戶使用。您以速率為基礎的規則偵測到的流量和速率限制會顯示在您的 AWS WAF 指標中。

除了您自己以速率為基礎的規則之外，如果您啟用自動應用程式層 DDoS 緩解功能，Shield Advanced 會在您的 Web ACL 中新增一個規則群組，以緩解攻擊。在此規則群組中，Shield Advanced 始終具有以速率為基礎的規則，以限制來自已知為 DDoS 攻擊來源之 IP 位址的請求數量。您無法檢視 Shield 進階規則緩解的流量量度。

如需以比率為基礎的規則的詳細資訊，請參閱速率型規則陳述式。如需 Shield Advanced 用於自動應用程式層 DDoS 緩解的速率型規則的相關資訊，請參閱Shield 牌進階規則群組。

如需有關「Shield 進階 AWS WAF 」和指標的詳細資訊，請參閱使用 Amazon 監控 CloudWatch。

Shield 進階應用程式層 AWS WAF Web ACLs 和速率型規則

若要使用 Shield Advanced 保護應用程式層資源，請先將 AWS WAF 網頁ACL與資源建立關聯。 AWS WAF 這是一種 Web 應用程式防火牆，可讓您監控轉寄至應用程式層資源的和HTTPS要求，並可讓您根據要求的特性控制內容的存取。HTTP您可以設定 WebACL，以根據要求的來源位置、查詢字串和 Cookie 的內容，以及來自單一 IP 位址的要求速率等因素來監視和管理要求。您的 Shield 進階防護至少要求您將網路ACL與速率型規則建立關聯，以限制每個 IP 位址的要求速率。

如果關聯的網站ACL沒有定義以速率為基礎的規則，「Shield 牌進階」會提示您至少定義一個規則。速率型規則會在來源超過您定義的閾值IPs時，自動封鎖來自來源的流量。它們有助於保護您的應用程式免受 Web 請求洪水的影響，並提供有關流量突然峰值的警示，這些警示可能表示潛在DDoS攻擊。

> **Note**
>
> 以速率為基礎的規則對規則監視的流量尖峰作出非常快速的回應。因此，以速率為基礎的規則不僅可以防止攻擊，還可以防止 Shield Advanced 偵測偵測潛在攻擊。這種權衡有利於防止攻擊模式的完全可見性。我們建議您使用以速率為基礎的規則作為抵禦攻擊的第一道防線。

如果發生DDoS攻擊，您可以透過ACL在 Web 中新增和管理規則來套用緩和措施。ACL您可以在 Shield 響應小組（SRT）的幫助下直接執行此操作，也可以通過自動應用程序層DDoS緩解自動執行此操作。

> **Important**
>
> 如果您也使用自動應用程式層DDoS緩和措施，請參閱管理 Web ACL 的最佳做法，請參閱使用自動緩解措施的最佳做法。

預設速率型規則行為

當您將以速率為基礎的規則與其預設組態搭配使用時，會 AWS WAF 定期評估前 5 分鐘時間範圍的流量。 AWS WAF 封鎖來自任何超過規則臨界值之 IP 位址的要求，直到要求率降至可接受的層級為止。當您透過 Shield Advanced 設定以速率為基礎的規則時，請將其速率閾值設定為大於您在任何五分鐘時間範圍內從任何一個來源 IP 預期的一般流量速率的值。

您可能想要在 Web ACL 中使用多個以速率為基礎的規則。例如，對於所有具有高臨界值的流量，您可以擁有一個以速率為基礎的規則，以及一或多個其他規則，這些規則設定為符合 Web 應用程式的特定部分且具有較低閾值。例如，您可能會在較低的URI/login.html閾值上進行匹配，以減輕對登錄頁面的濫用行為。

您可以設定以比率為基礎的規則，使其使用不同的評估時間範圍，並依據許多請求元件 (例如標頭值、標籤及查詢引數) 聚總請求。如需詳細資訊，請參閱速率型規則陳述式。

如需其他資訊和指引，請參閱安全性部落格文章三個最重要的 AWS WAF 速率規則。

透過擴充組態選項 AWS WAF

Shield 進階主控台可讓您新增以速率為基礎的規則，並使用基本的預設設定進行設定。您可以透過AWS WAF管理以費率為基礎的規則，以定義其他組態選項。例如，您可以將規則設定為根據轉寄的 IP 位址、查詢字串和標籤等金鑰彙總要求。您也可以在規則中新增範圍陳述式，以篩選出來自評估和速率限制的某些要求。如需詳細資訊，請參閱速率型規則陳述式。如需使用 AWS WAF 來管理 Web 要求監視和管理規則的相關資訊，請參閱建立 Web ACL。

Shield 先進的自動應用層 DDoS 緩解

您可以將 Shield Advanced 設定為自動回應，藉由計算或封鎖屬於攻擊一部分的 Web 要求，以減輕受保護應用程式層資源的應用程式層 (第 7 層) 攻擊。此選項是您透過 Shield Advanced 新增的應用程式層保護功能的新增功能，搭配 AWS WAF Web ACL 和您自己的速率規則。

為資源啟用自動緩和措施時，Shield Advanced 會在資源關聯的 Web ACL 中維護一個規則群組，該群組會代表資源管理緩和規則。規則群組包含以速率為基礎的規則，可追蹤來自已知為 DDoS 攻擊來源之 IP 位址的要求量。

此外，Shield Advanced 會將目前的流量模式與歷史流量基準進行比較，以偵測可能表示 DDoS 攻擊的偏差。Shield Advanced 透過在規則群組中建立、評估和部署其他自訂 AWS WAF 規則來回應偵測到的 DDoS 攻擊。

內容

使用自動緩解的注意事項

下列清單說明 Shield 進階自動應用程式層 DDoS 緩解的警告，並說明您可能想要採取的步驟來回應。

- 自動應用程式層 DDoS 防護功能僅適用於使用最新版本 AWS WAF (v2) 建立的 Web ACL。
- Shield Advanced 需要時間來建立應用程式的正常歷史流量基準，並利用此基準來偵測攻擊流量與正常流量並將其隔離，以減輕攻擊流量。建立基準線的時間是從您將 Web ACL 與受保護的應用程式資源建立關聯起來的 24 小時到 30 天之間。如需流量基準的其他資訊，請參閱偵測和緩解。
- 啟用自動應用程式層 DDoS 緩解功能會將規則群組新增至使用 150 個 Web ACL 容量單位 (WCU) 的網路 ACL。這些 WCU 會計入您網路 ACL 中的 WCU 使用量。如需詳細資訊，請參閱 Shield 牌進階規則群組 和 AWS WAF 網路 ACL 容量單位 (WCU)。
- 「Shield 牌進階」規則群組會產生 AWS WAF 量度，但無法檢視這些量度。這與您在 Web ACL 中使用但不擁有的任何其他規則群組 (例如 AWS 受管規則群組) 的規則群組相同。如需 AWS WAF

測量結果的詳細資訊，請參閱AWS WAF 量度和維度。如需此防護進階防護選項的相關資訊，請參閱Shield 先進的自動應用層 DDoS 緩解。

- 對於保護多個資源的 Web ACL，自動緩和措施只會部署不會對任何受保護資源造成負面影響的自訂緩和措施。
- DDoS 攻擊開始到 Shield Advanced 放置自訂自動緩解規則之間的時間會因每個事件而異。部分 DDoS 攻擊可能會在部署自訂規則之前結束。其他攻擊可能在緩解措施已經到位時發生，因此這些規則可能會從事件開始緩解。此外，Web ACL 和 Shield 進階規則群組中的速率型規則可能會在偵測到可能的事件之前減輕攻擊流量。
- 對於透過內容交付網路 (CDN) (例如 Amazon CloudFront) 接收任何流量的應用程式負載平衡器，這些應用程式負載平衡器資源的 Shield Advanced 應用程式層自動緩解功能將會降低。Shield Advanced 會使用用戶端流量屬性來識別和隔離攻擊流量與應用程式的正常流量，而 CDN 可能無法保留或轉寄原始用戶端流量屬性。如果您使用 CloudFront，建議您在 CloudFront 發行版上啟用自動緩和措施。
- 自動應用程式層 DDoS 防護功能不會與保護群組互動。您可以為保護群組中的資源啟用自動緩和措施，但 Shield Advanced 不會根據保護群組發現的項目自動套用攻擊緩和措施。Shield 牌進階對個別資源套用自動攻擊緩和措施。

使用自動緩解措施的最佳做法

使用自動緩和措施時，請遵守本節中提供的指導。

一般保護管理

請遵循以下準則，以規劃和實施自動緩解保護。

- 您可以透過 Shield Advanced 管理所有自動緩解保護，或者如果您使用 AWS Firewall Manager Firewall Manager 員管理您的 Shield 牌進階自動緩解設定。請勿混合使用 Shield 進階和 Firewall Manager 員來管理這些保護。
- 使用相同的 Web ACL 和保護設定來管理類似的資源，並使用不同的 Web ACL 管理不同的資源。當 Shield Advanced 緩解受保護資源上的 DDoS 攻擊時，它會定義與資源相關聯的 Web ACL 的規則，然後針對與 Web ACL 相關聯的所有資源的流量測試規則。護 Shield 進階版只有在沒有對任何相關資源造成負面影響的情況下才會套用這些規則。如需詳細資訊，請參閱 防 Shield 進階如何管理自動緩解。
- 對於透過 Amazon CloudFront 分發代理所有網際網路流量的應用程式負載平衡器，請僅在分發上啟用自動緩解功能。 CloudFront該 CloudFront 分配將始終具有最多數量的原始流量屬性，Shield Advanced 利用這些屬性來緩解攻擊。

偵測和緩解最佳化

請遵循這些準則，將自動緩和措施提供給受保護資源的保護最佳化。如需應用程式層偵測和緩和措施的概觀，請參閱偵測和緩解。

- 為受保護的資源設定健康狀態檢查，並使用它們在 Shield Advanced 防護中啟用健康狀態偵測。如需準則，請參閱以 Health 狀態檢查為基礎的偵測。
- 在Count模式中啟用自動緩解功能，直到 Shield Advanced 建立正常歷史流量的基準為止。Shield 進階需要 24 小時到 30 天才能建立基準。

  建立一般流量模式的基準需要下列條件：

  - Web ACL 與受保護資源的關聯。您可以 AWS WAF 直接使用來關聯您的 Web ACL，或者當您啟用「防 Shield 進階」應用程式層保護並指定要使用的 Web ACL 時，可以讓「防護進階」建立關聯。
  - 正常流量流向受保護的應用程式。如果您的應用程式未遇到正常流量 (例如在應用程式啟動之前)，或長時間缺少生產流量，則無法收集歷史資料。

網路 ACL 管理

請遵循下列準則，以管理您搭配自動緩和措施使用的 Web ACL。

- 如果您需要取代與受保護資源關聯的 Web ACL，請依序進行下列變更：

  1. 在 Shield 牌進階中，停用自動緩解功能。
  2. 在中 AWS WAF，取消舊網頁 ACL 的關聯，並關聯新 Web ACL。
  3. 在 Shield 牌進階中，啟用自動緩解功能。

  防 Shield 進階版不會自動將舊版 Web ACL 的自動緩和措施傳輸到新的 ACL。
- 請勿從 Web ACL 中刪除名稱開頭為的任何規則群組規則。`ShieldMitigationRuleGroup`如果您確實刪除此規則群組，則會針對與 Web ACL 相關聯的每個資源停用 Shield Advanced 自動緩和措施提供的保護。此外，Shield Advanced 可能需要一些時間才能收到變更通知並更新其設定。在此期間，Shield 進階主控台頁面會提供不正確的資訊。

  如需規則群組的詳細資訊，請參閱Shield 牌進階規則群組。
- 請勿修改名稱開頭為的規則群組規則名稱`ShieldMitigationRuleGroup`。這樣做可能會干擾 Shield 牌進階自動緩解透過 Web ACL 提供的保護。
- 建立規則和規則群組時，請勿使用開頭為的名稱`ShieldMitigationRuleGroup`。Shield 進階使用此字串來管理您的自動緩和措施。

- 在管理網頁 ACL 規則時，請勿指派 10,000,000 的優先順序設定。Shield Advanced 在新增時，會將此優先順序設定指派給其自動緩和規則群組規則。
- 將`ShieldMitigationRuleGroup`規則保持優先順序，以便在您希望規則與 Web ACL 中的其他規則相關時執行。「Shield 牌進階」會將規則群組規則新增至具有優先順序為 10,000,000 的網頁 ACL，以便在您的其他規則之後執行。如果您使用 AWS WAF 主控台精靈管理 Web ACL，請在將規則加入至 Web ACL 後，依需要調整優先順序設定。
- 如果您使用 AWS CloudFormation 來管理 Web ACL，則不需要管理`ShieldMitigationRuleGroup`規則群組規則。請遵循的指導AWS CloudFormation 搭配自動應用程式層 DDoS 緩解使用。

啟用自動緩和措施所需的組態

您可以啟用 Shield 進階自動緩解作為資源的應用程式層 DDoS 保護的一部分。如需透過主控台執行此作業的詳細資訊，請參閱設定應用程式層 DDoS 保護。

自動緩和功能需要您執行以下操作：

- 將 Web ACL 與資源建立關聯 — 任何「Shield 牌進階應用程式層保護」都需要此功能。您可以針對多個資源使用相同的 Web ACL。我們建議僅針對具有類似流量的資源執行此操作。如需 Web ACL 的詳細資訊，包括將它們與多個資源搭配使用的需求，請參閱如何 AWS WAF 工作。
- 啟用和設定 Shield 進階自動應用程式層 DDoS 緩解 — 啟用此功能時，您可以指定是否希望 Shield Advanced 自動封鎖或計算其判定為 DDoS 攻擊一部分的 Web 要求。Shield Advanced 將規則群組新增至關聯的 Web ACL，並使用它來動態管理其對資源 DDoS 攻擊的回應。如需有關規則動作選項的資訊，請參閱規則動作。
- (選擇性，但建議使用) 將速率規則新增至 Web ACL — 依預設，以速率為基礎的規則會防止任何個別 IP 位址在短時間內傳送過多要求，為您的資源提供基本的 DDoS 攻擊防護。如需以速率為基礎的規則 (包括自訂要求彙總選項和範例) 的資訊，請參閱速率型規則陳述式。

防 Shield 進階如何管理自動緩解

本節中的主題說明 Shield Advanced 如何處理自動應用程式層 DDoS 緩解的組態變更，以及在啟用自動緩解功能時如何處理 DDoS 攻擊。

主題

- 啟用自動緩解時會發生什麼情況
- Shield 牌進階如何透過自動緩解來回應 DDoS 攻擊

- 「Shield 牌進階」如何管理規則動作設定
- 當攻擊消退時，Shield 牌進階如何管理緩和措施
- 停用自動緩解時會發生什麼情況

啟用自動緩解時會發生什麼情況

當您啟用自動緩解時，Shield 牌進階會執行下列動作：

- 視需要新增 Shield Advanced 使用的規則群組 — 如果您與資源關聯的 AWS WAF Web ACL 還沒有專用於自動應用程式層 DDoS 緩解的規則群組規則，Shield Advanced 會新增一個規則群組規則。AWS WAF

  規則群組規則的名稱開頭為`ShieldMitigationRuleGroup`。規則群組一律包含名為以速率為基礎的規則`ShieldKnownOffenderIPRateBasedRule`，該規則會限制來自已知為 DDoS 攻擊來源之 IP 位址的要求數量。如需有關「Shield 進階」規則群組及其參考之 Web ACL 規則的其他詳細資訊，請參閱Shield 牌進階規則群組。
- 開始回應針對資源的 DDoS 攻擊 — Shield Advanced 會自動回應受保護資源的 DDoS 攻擊。除了以速率為基礎的規則 (始終存在) 之外，Shield Advanced 還使用其規則群組來部署 DDoS 攻擊緩解的自訂 AWS WAF 規則。Shield Advanced 會根據您的應用程式和應用程式所遭受的攻擊量身打造這些規則，並在部署前對資源的歷史流量進行測試。

Shield 牌進階會在您用於自動緩和措施的任何 Web ACL 中使用單一規則群組規則。如果 Shield Advanced 已經為另一個受保護的資源新增了規則群組，則不會將其他規則群組新增至 Web ACL。

自動應用程式層 DDoS 緩解功能取決於規則群組的存在，以減輕攻擊。如果由於任何原因從 AWS WAF Web ACL 中移除規則群組，則移除會停用與 Web ACL 相關聯的所有資源的自動緩和措施。

Shield 牌進階如何透過自動緩解來回應 DDoS 攻擊

當您在受保護的資源上啟用自動緩和措施時，Shield Advanced 規則群組`ShieldKnownOffenderIPRateBasedRule`中的速率型規則會自動回應來自已知 DDoS 來源的升高流量。這種速率限制可快速套用，並可作為抵禦攻擊的前線防禦。

當護 Shield 進階偵測到攻擊時，它會執行下列動作：

1. 嘗試識別攻擊特徵，以隔離攻擊流量與應用程式的正常流量。我們的目標是產生高品質的 DDoS 緩解規則，這些規則放置時僅會影響攻擊流量，而不會影響應用程式的正常流量。

2. 根據遭受攻擊的資源以及與相同 Web ACL 相關聯的任何其他資源的歷史流量模式來評估已識別的攻擊特徵。Shield Advanced 會在部署任何規則以回應事件之前執行此動作。

   根據評估結果，「Shield 牌進階」會執行下列其中一項作業：

   - 如果 Shield Advanced 判斷攻擊特徵僅隔離了 DDoS 攻擊涉及的流量，則會在 Web ACL 的 Shield 進階緩解 AWS WAF 規則群組中的規則中實作簽章。Shield Advanced 為這些規則提供您為資源自動緩解設定的動作設定-Count 或Block。
   - 否則，護 Shield 進階不會放置緩解措施。

在攻擊期間，Shield Advanced 會傳送相同的通知，並提供與基本 Shield 進階應用程式層保護相同的事件資訊。您可以在 Shield 進階事件主控台中查看有關事件和 DDoS 攻擊的資訊，以及任何針對攻擊的 Shield 進階緩和措施的資訊。如需相關資訊，請參閱DDoS 事件的可見性。

如果您已將自動緩和措施設定為使用規Block則動作，並且在 Shield Advanced 部署的緩和規則中遇到Count誤判，則可以將規則動作變更為。如需有關如何執行此操作的資訊，請參閱變更用於自動應用程式層 DDoS 緩解的動作。

「Shield 牌進階」如何管理規則動作設定

您可以將自動緩和措施的規則動作設為Block或Count。

當您變更受保護資源的自動緩和規則動作設定時，Shield Advanced 會更新資源的所有規則設定。它會更新 Shield Advanced 規則群組中目前針對資源設定的任何規則，並在建立新規則時使用新的動作設定。

對於使用相同 Web ACL 的資源，如果您指定不同的動作，「Shield 牌進階」會使用規則群組以速率為基礎的規則的Block動作設定。`ShieldKnownOffenderIPRateBasedRule`Shield Advanced 代表特定受保護的資源在規則群組中建立和管理其他規則，並使用您為資源指定的動作設定。Web ACL 中「Shield 進階」規則群組中的所有規則都會套用至所有關聯資源的 Web 流量。

變更動作設定可能需要幾秒鐘的時間來傳播。在此期間，您可能會在使用規則群組的某些地方看到舊設定，而在其他位置會看到新設定。

您可以在主控台的事件頁面中，以及透過應用程式層組態頁面變更自動緩和措施組態的規則動作設定。如需有關事件頁面的資訊，請參閱回應 DDoS 事件。如需有關組態頁面的資訊，請參閱設定應用程式層 DDoS 保護。

當攻擊消退時，Shield 牌進階如何管理緩和措施

當 Shield Advanced 判定不再需要針對特定攻擊部署的緩和規則時，會將其從 Shield Advanced 緩和規則群組中移除。

刪除緩解規則不一定與攻擊結束一致。「Shield 牌進階」會監控在受保護資源上偵測到的攻擊模式。它可能會主動防禦使用特定簽名的攻擊再次發生，方法是將其部署的規則保持在適當的位置以防止該攻擊的初始發生。必要時，護 Shield 進階版會增加規則的時間範圍。如此一來，Shield Advanced 可以減輕具有特定簽章的重複攻擊，避免它們影響您受保護的資源。

Shield Advanced 絕不會移除以速率為基礎的規則`ShieldKnownOffenderIPRateBasedRule`，這會限制來自已知為 DDoS 攻擊來源之 IP 位址的要求量。

停用自動緩解時會發生什麼情況

當您停用資源的自動緩和措施時，Shield Advanced 會執行下列動作：

- 停止自動回應 DDoS 攻擊 — Shield Advanced 停止其資源的自動回應活動。
- 從 Shield Advanced 規則群組中移除不需要的規則 — 如果 Shield Advanced 代表受保護的資源維護其受管規則群組中的任何規則，則會移除這些規則。
- 移除 Shield 進階規則群組 (如果不再使用) — 如果您與資源相關聯的 Web ACL 未與任何其他已啟用自動緩和措施的資源相關聯，Shield Advanced 會從 Web ACL 中移除其規則群組規則。

Shield 牌進階規則群組

Shield Advanced 會使用它為您擁有並管理的規則群組中的規則來管理自動緩解活動。Shield Advanced 會參照規則群組，其中包含您與受保護資源相關聯的 Web ACL 中的規則。

網頁 ACL 中的規則群組規則

Web ACL 中的「Shield 進階規則群組規則」具有下列屬性：

- 名稱 – `ShieldMitigationRuleGroup_`*`account-id`*`_`*`web-acl-id`*`_`*`unique-identifier`*
- 網頁 ACL 容量單位 (WCU) — 150。這些 WCU 會計入您網路 ACL 中的 WCU 使用量。

「Shield 牌進階」會在您的網頁 ACL 中建立此規則，其優先順序設定為 10,000,000，以便在 Web ACL 中的其他規則和規則群組之後執行。 AWS WAF 從上的數值優先順序最低的設定執行 Web ACL 中的規則。在管理 Web ACL 期間，此優先順序設定可能會變更。

自動緩和功能不會消耗您帳戶中的任何其他 AWS WAF 資源，除了 Web ACL 中規則群組所使用的 WCU 之外。例如，Shield 進階規則群組不會計為您帳戶的其中一個規則群組。如需中帳戶限制的相關資訊 AWS WAF，請參閱AWS WAF 配額。

規則群組中的規則

在參照的 Shield 進階規則群組中，Shield Advanced 會維護以速率為基礎的規則`ShieldKnownOffenderIPRateBasedRule`，該規則會限制來自已知為 DDoS 攻擊來源之 IP 位址的要求數量。此規則是抵禦任何攻擊的第一道防線，因為它始終存在於規則群組中，並且不依賴於流量模式的分析來遏制攻擊。此規則的動作會設定為您為自動緩和措施選擇的動作，就像規則群組中的其他規則一樣。如需以速率為基礎的規則的資訊，請參閱速率型規則陳述式。

> **Note**
>
> 以速率為基礎的規則`ShieldKnownOffenderIPRateBasedRule`運作與 Shield 進階事件偵測無關。啟用自動緩解功能時，此規則速率會限制已知為 DDoS 攻擊來源的 IP 位址。對於這些 IP 位址，規則的速率限制可以防止攻擊，並防止攻擊出現在 Shield 牌進階偵測資訊中。這種權衡有利於防止攻擊模式的完全可見性。

除了上述以速率為基礎的永久規則之外，規則群組還包含 Shield Advanced 目前用於緩解 DDoS 攻擊的任何規則。Shield 牌進階版視需要新增、修改和移除這些規則。如需相關資訊，請參閱防 Shield 進階如何管理自動緩解。

指標

規則群組會產生 AWS WAF 量度，但由於此規則群組由 Shield Advanced 擁有，因此無法檢視這些量度。如需更多詳細資訊，請參閱 AWS WAF 量度和維度。

管理自動應用程式層 DDoS 防護

使用本節中的指導來管理您的自動應用程式層 DDoS 緩解設定。如需自動緩和措施如何運作的相關資訊，請參閱上述主題。

> **Note**
>
> 請遵循中所述的最佳作法使用自動緩解措施的最佳做法。

主題

檢視資源的自動應用程式層 DDoS 緩解設定

您可以在受保護的資源頁面和個別保護頁面中檢視資源的自動應用程式層 DDoS 緩解設定。

檢視自動應用程式層 DDoS 安全防護設定

1. 登入 AWS Management Console 並開啟 Shield 牌主控台 AWS WAF (S)，網址為 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 導覽窗格中，選擇 [受保護的資源]。在受保護的資源清單中，[自動應用程式層 DDoS 緩解] 欄會指出是否啟用自動緩和措施，以及 Shield Advanced 要在其緩和措施中使用的動作 (若已啟用)。

   您也可以選取任何應用程式層資源，以查看資源的保護頁面上列出的相同資訊。

啟用和停用自動應用程式層 DDoS 緩解

下列程序顯示如何啟用或停用受保護資源的自動回應。

啟用或停用單一資源的自動應用程式層 DDoS 緩解

1. 登入 AWS Management Console 並開啟 Shield 牌主控台 AWS WAF (S)，網址為 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 導覽窗格中，選擇 [受保護的資源]。
3. 在 [保護] 索引標籤中，選取您要啟用自動緩和措施的應用程式層資源。資源的保護頁面隨即開啟。
4. 在資源的保護頁面中，選擇 [編輯]。
5. 在頁面中為全域資源設定第 7 層 DDoS 緩解-選用，對於自動應用程式層 DDoS 緩解，請選擇您要用於自動緩解的選項。控制台中的選項如下：

   - 保留目前設定 — 不變更受保護資源的自動緩和措施設定。
   - 啟用 — 為受保護的資源啟用自動緩和措施。當您選擇此選項時，也請選取您希望自動緩和措施在 Web ACL 規則中使用的規則動作。如需有關規則動作設定的資訊，請參閱規則動作。

如果受保護的資源還沒有正常應用程式流量的歷史記錄，請在Count模式中啟用自動緩解功能，直到 Shield Advanced 可以建立基準為止。當您將 Web ACL 與受保護的資源建立關聯時，Shield Advanced 會開始收集其基準的資訊，而且可能需要 24 小時到 30 天才能建立正常流量的良好基準線。

- 停用 — 停用受保護資源的自動緩和措施。

6. 逐步瀏覽其餘頁面，直到完成並儲存設定。

在 [保護] 頁面中，會更新資源的自動緩和措施設定。

變更用於自動應用程式層 DDoS 緩解的動作

您可以在主控台的多個位置變更 Shield Advanced 用於應用程式層自動回應的動作：

- 自動緩和設定 — 變更為資源設定自動緩和措施時的動作。如需程序的相關資訊，請參閱前一節啟用和停用自動應用程式層 DDoS 緩解。
- 事件詳細資訊頁面 — 在主控台中檢視事件資訊時，變更事件詳細資訊頁面中的動作。如需相關資訊，請參閱AWS Shield Advanced 活動詳情。

如果您有兩個共用 Web ACL 的受保護資源，並且將其中一個 ACL 設定Count為另一個 ACL，則 Shield Advanced 會將規則群組以速率為基礎的規則的處理行動設定`ShieldKnownOffenderIPRateBasedRule`為Block。Block

AWS CloudFormation 搭配自動應用程式層 DDoS 緩解使用

瞭解如何使用 AWS CloudFormation 來管理您的防護和 AWS WAF 網路 ACL。

啟用或停用自動應用程式層 DDoS 緩解

您可以通 AWS CloudFormation過使用`AWS::Shield::Protection`資源啟用和禁用自動應用程序層 DDoS 緩解。效果與透過主控台或任何其他介面啟用或停用功能時相同。若要取得有關資 AWS CloudFormation 源的資訊，請參閱AWS CloudFormation 使用指南AWS::Shield::Protection中的〈〉。

管理搭配自動緩解功能使用的 Web ACL

Shield Advanced 會使用受保護資源的 AWS WAF Web ACL 中的規則群組規則來管理受保護資源的自動緩和措施。透過 AWS WAF 主控台和 API，您會看到 Web ACL 規則中列出的規則，名稱開頭為`ShieldMitigationRuleGroup`。此規則專用於您的自動應用程式層 DDoS 緩解，並由 Shield 進階和 AWS WAF. 如需詳細資訊，請參閱 Shield 牌進階規則群組 及 防 Shield 進階如何管理自動緩解。

如果您使用 AWS CloudFormation 來管理 Web ACL，請勿將「Shield 牌進階」規則群組規則新增至您的 Web ACL 範本。當您更新與自動緩和保護搭配使用的 Web ACL 時， AWS WAF 會自動管理 Web ACL 中的規則群組規則。

與您管理的其他 Web ACL 相比，您會看到以下差異： AWS CloudFormation

- AWS CloudFormation 在沒有規則的情況下，不會報告 Web ACL 實際配置之間的堆棧漂移狀態，使用 Shield 高級規則組規則和 Web ACL 模板之間的任何漂移。護 Shield 進階規則不會出現在漂移詳細資料中資源的實際清單中。

  您可以在從 AWS WAF中擷取的 Web ACL 清單 (例如透過 AWS WAF 主控台或 AWS WAF API) 查看「Shield 牌進階」規則群組規則。
- 如果您修改堆疊中的 Web ACL 範本， AWS WAF 且「Shield 牌進階」會自動在更新的 Web ACL 中維護防 Shield 進階自動緩和規則。防護進階提供的自動緩解保 Shield 功能不會因您對網路 ACL 的更新而中斷。

請勿在您的 AWS CloudFormation 網頁 ACL 範本中管理護 Shield 進階規則。網頁 ACL 範本不應該列出「Shield 牌進階」規則。請遵循網頁 ACL 管理的最佳作法，請參閱使用自動緩解措施的最佳做法。

以 Health 狀態檢查為基礎的偵測

您可以將 Shield Advanced 設定為使用健康狀況型偵測來改善攻擊偵測和緩解的反應速度和準確性。您可以將此選項用於任何資源類型，但 Route 53 託管區域除外。

若要設定健康狀態偵測，請在 Route 53 中為資源定義健康狀態檢查，確認資源報告狀況良好，然後將其與您的 Shield 進階防護建立關聯。如需有關 Route 53 運作狀態檢查的詳細資訊，請參閱 Amazon Route 53 如何檢查資源的運作狀態以及建立、更新和刪除運作狀態檢查 (詳見 Amazon Route 53 開發人員指南)。

> **Note**
>
> Shield 牌應變團隊 (SRT) 主動參與支援需要運作 Health 態檢查。如需主動參與的相關資訊，請參閱設定主動參與。

運作 Health 態檢查會根據您定義的需求來衡量資源的健全狀況。健康狀態檢查狀態為 Shield Advanced 偵測機制提供重要的輸入，讓它們對特定應用程式的目前狀態有更大的敏感度。

您可以針對任何資源類型 (Route 53 託管區域除外) 啟用健全狀況型偵測。

- 網路和傳輸層 (第 3 層/第 4 層) 資源 — Health 狀況型偵測可改善網路層和傳輸層事件偵測和緩解的準確性，適用於網路負載平衡器、彈性 IP 位址和全域加速器標準加速器。當您使用 Shield Advanced 保護這些資源類型時，Shield Advanced 可以為較小的攻擊提供緩和措施，並加快緩解攻擊的速度，即使流量在應用程式容量範圍內也是如此。

  當您新增健康狀況型偵測時，在關聯的健康狀態檢查狀態不良的期間，Shield Advanced 可以更快速地進行緩和措施，甚至更低的臨界值。

- 應用程式層 (第 7 層) 資源 — Health 狀況型偵測可改善 CloudFront散佈和應用程式負載平衡器的 Web 要求洪水偵測的準確性。當您使用 Shield Advanced 保護這些資源類型時，當流量存在統計上顯著的偏差，並且結合了流量模式的重大變化 (根據請求特性)，您會收到 Web 請求洪水偵測警示。

  透過健康狀態偵測，當相關的 Route 53 健康狀態檢查狀況不佳時，Shield Advanced 需要較小的偏差來警示，並且可以更快速地報告事件。相反地，當相關的 Route 53 健康狀態檢查狀況良好時，護 Shield 進階需要較大的偏差才能發出警示。

內容

使用「Shield 牌進階」運作狀態檢查的最佳做法

當您使用「Shield 牌進階」建立並使用健康狀態檢查時，請遵循本節中的最佳作法。

- 識別您要監視的基礎結構元件，以規劃健康狀態檢查。運作狀態檢查請考慮下列資源類型：

  - 關鍵資源。
  - 任何您想要在 Shield 進階偵測和緩解中獲得更高靈敏度的資源。
  - 您希望讓 Shield 進階主動接觸到您的資源。您的健康檢查狀態會通知主動參與。

  您可能想要監控的資源範例包括 Amazon CloudFront 分發、面向網際網路的負載平衡器和 Amazon EC2 執行個體。
- 定義運作狀態檢查，以盡可能少的通知準確反映應用程式來源的健康狀態。
  - 撰寫健康狀態檢查，以便只有當您的應用程式無法使用或未在可接受的參數範圍內執行時，才會不健康。您有責任根據應用程式的特定需求來定義和維護運作狀態檢查。
  - 儘可能少地使用健康狀態檢查，同時仍可準確報告應用程式的健康狀態。例如，來自應用程式多個區域的多個警示，這些警示都會報告相同問題，可能會增加回應活動的額外負荷，而不會增加資訊值。
  - 使用計算的運作狀態檢查，結合使用 Amazon CloudWatch 指標來監控應用程式運作狀態。例如，您可以根據應用程式伺服器的延遲及其 5xx 錯誤率來計算合併的健全狀況，這表示原始伺服器未滿足要求。
  - 視需要建立您自己的應用程式健康狀態指標，並將其發佈至自 CloudWatch 訂指標，並在計算的健康狀態檢查中使用
- 實施和管理您的運行狀態檢查，以改善檢測並減少不必要的維護活動。
  - 在您將健康狀態檢查與 Shield 進階防護建立關聯之前，請確定其處於健康狀態。建立報告狀態不良的健康狀態檢查關聯可能會扭曲受保護資源的 Shield Advanced 偵測機制。
  - 保持您的健康檢查可供 Shield 牌進階使用。請勿在 Route 53 中刪除您用於 Shield 牌進階防護的健康狀態檢查。
  - 僅使用測試和測試環境來測試健康狀態檢查。僅針對需要生產層級效能和可用性的環境維護健全狀況檢查關聯。請勿在「Shield Advanced」中針對測試和測試環境維護健康狀態檢查關聯。

常用於健康狀態檢查的指標

本節列出運作狀態檢查中常用的 Amazon CloudWatch 指標，以在分散式拒絕服務 (DDoS) 事件期間測量應用程式運作狀態。如需每個資源類型 CloudWatch 測量結果的完整資訊，請參閱表格後面的清單。

主題

- 用來監視應用程式健全狀況的
- 每種資源類型的 Amazon CloudWatch 指標

用來監視應用程式健全狀況的

資源	指標	描述
Route 53	HealthCheckStatus	健全狀況檢查端點的狀態。
CloudFront	5xxErrorRate	HTTP 狀態碼為 5xx 之所有要求的百分比。這表示正在影響應用程式的攻擊。
Application Load Balancer	HTTPCode_ELB_5XX_Count	負載平衡器所產生的 HTTP 5xx 用戶端錯誤碼數目。
Application Load Balancer	RejectedConnectionCount	因為負載平衡器達到其連線數目上限而遭拒絕的連線數目。
Application Load Balancer	TargetConnectionErrorCount	在負載平衡器與目標之間未成功建立的連線數目。
Application Load Balancer	TargetResponseTime	要求離開負載平衡器以及收到目標回應之後所經過的時間 (以秒為單位)。
Application Load Balancer	UnHealthyHostCount	視為不健康的目標數目。
Amazon EC2	CPUUtilization	目前使用中的已配置 EC2 運算單元的百分比。

每種資源類型的 Amazon CloudWatch 指標

如需有關受保護資源可用指標的其他資訊，請參閱資源指南中的下列各節：

- Amazon 路線 53 — CloudWatch 在 Amazon Route 53 開發人員指南中使用 Amazon 路線 53 運行狀況檢查和 Amazon 監控您的資源。
- Amazon CloudFront — 在 Amazon CloudFront 開發人員指南 CloudWatch中 CloudFront 與 Amazon 進行監控
- Application Load Balancer — 應用程式負載平衡器使用者指南中的應用程式負載平衡器指 CloudWatch 標。

- Network Load Balancer — Network Load Balancer 使用者指南中的網路負載平衡器指CloudWatch 標。
- AWS Global Accelerator — 在 AWS Global Accelerator 開發人員指南 AWS Global Accelerator中使用 Amazon CloudWatch 。
- Amazon 彈性運算雲端 — 在 https://docs.aws.amazon.com/ AWSEC中列出適用於您執行個體的可用 CloudWatch 指標。UserGuide
- Amazon EC2 Auto Scaling — 在 Amazon EC2 Auto Scaling 使用者指南中監控自 Auto Scaling 群組和執行個體的指 CloudWatch 標。

管理健康檢查關聯

如果健康狀態檢查僅在您的應用程式在可接受的參數範圍內執行時報告健康狀態，並且僅在不健康狀態的情況下報告狀況不良時，您將獲益最大。使用本節中的指南來管理您在 Shield 牌進階中的健康狀態檢查關聯。

> **Note**
>
> 「Shield 牌進階」不會自動管理您的健康狀態檢查。

若要透過護 Shield 進階使用健康狀態檢查，必須具備以下條件：

- 當您將健康狀態檢查與您的 Shield 進階防護建立關聯時，必須報告健康狀況檢
- 健康狀態檢查必須與受保護資源的健全狀況相關。您有責任定義和維護運作狀態檢查，以根據應用程式的特定需求，準確報告應用程式的健康狀態。
- 健康狀態檢查必須保持可供 Shield 進階防護使用。請勿在 Route 53 中刪除您用於 Shield 牌進階防護的健康狀態檢查。

主題

- 建立健康狀態檢查與資源的關聯
- 取消健康狀態檢查與資源的關聯
- 健康狀態檢查關聯狀態

建立健康狀態檢查與資源的關聯

下列程序顯示如何將 Amazon Route 53 運作狀態檢查與受保護的資源建立關聯。

> **Note**
>
> 在您將健康狀態檢查與 Shield 進階防護建立關聯之前，請確定其處於健康狀態。如需相關資訊，請參閱 Amazon Route 53 開發人員指南中的監控運作狀態檢查狀態和取得通知。

建立健康狀態檢查的關聯

1. 登入 AWS Management Console 並開啟 Shield 牌主控台 AWS WAF (S)，網址為 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 導覽窗格中，選擇 [受保護的資源]。
3. 在 [保護] 索引標籤上，選取您要與健全狀況檢查相關聯的資源。
4. 選擇 [設定保護]。
5. 選擇 [下一步]，直到您進入頁面設定運作狀態檢查型 DDoS 偵測-選用。
6. 在 Associate Health Check (關聯運作狀態檢查) 下，選擇您要與保護產生關聯的運作狀態檢查 ID。

   > **Note**
   >
   > 如果您沒有看到所需的健康狀態檢查，請移至 Route 53 主控台並驗證健康狀態檢查及其 ID。如需相關資訊，請參閱建立和更新運作狀態檢查。

7. 逐步瀏覽其餘頁面，直到完成設定為止。在 [保護] 頁面上，會針對資源列出您更新的健全狀況檢查關聯。
8. 在 [保護] 頁面上，檢查您新關聯的健康狀態檢查報告狀況良好。

   當健康狀態檢查報告不健康狀況時，您無法在 Shield Advanced 中成功開始使用健康狀態檢查。這樣做會導致 Shield Advanced 在極低的閾值下偵測誤報，並且也會對 Shield 牌回應小組 (SRT) 提供資源主動參與的能力產生負面影響。

   如果新關聯的健全狀況檢查報告狀況不良，請執行下列動作：

   a. 在「Shield 牌進階」中取消健康狀態檢查與防護的關聯。
   b. 重新瀏覽 Amazon Route 53 中的運作狀態檢查規格，並驗證您的整體應用程式效能和可用性。
   c. 當您的應用程式在您的參數內執行以保持健康狀態，且您的健康狀態檢查報告正常狀況時，請再試一次在 Shield Advanced 中建立關聯狀態檢查。

當您建立新的健康檢查關聯並在 Shield Advanced 中報告健康狀況時，健康狀態檢查關聯程序即完成。

取消健康狀態檢查與資源的關聯

下列程序說明如何取消 Amazon Route 53 運作狀態檢查與受保護資源的關聯。

取消健康狀態檢查的關聯

1. 登入 AWS Management Console 並開啟 Shield 牌主控台 AWS WAF (S)，網址為 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 導覽窗格中，選擇 [受保護的資源]。
3. 在 [保護] 索引標籤上，選取您要取消與健康狀態檢查關聯的資源。
4. 選擇 [設定保護]。
5. 選擇 [下一步]，直到您進入頁面設定運作狀態檢查型 DDoS 偵測-選用。
6. 在「關聯的 Health 狀態檢查」下，選擇列為 - 的空白選項。
7. 逐步瀏覽其餘頁面，直到完成設定為止。

在 [保護] 頁面上，資源的健全狀況檢查欄位設定為 -，表示沒有健康狀態檢查關聯。

健康狀態檢查關聯狀態

您可以在與 Shield 控制台受保護的資源頁面以 AWS WAF 及每個資源的詳細資料頁面上查看與保護相關聯的健康狀態檢查狀態。

- 健康 — 健康狀況檢查可用且報告狀況良好。
- 不健康 — 健康狀況檢查可用且報告不健康狀況。
- 無法使用 — 健康狀態檢查無法供 Shield 牌進階使用。

解決無法使用的健全狀況檢查

建立並使用新的健康狀態檢查。在 Shield 牌進階中的狀態為無法使用之後，不要再嘗試重新建立健康檢查的關聯。

如需遵循這些步驟的詳細指引，請參閱上述主題。

1. 在 Shield 牌進階中，取消健全狀況檢查與資源的關聯。

2. 在 Route 53 中，為資源建立新的健康狀態檢查並記下其 ID。如需詳細資訊，請參閱 Amazon Route 53 開發人員指南中的建立和更新運作 Health 態檢查。
3. 在 Shield 牌進階中，將新的健康狀態檢查與資源建立關聯。

Health 檢查範例

本節顯示您可以在計算的健全狀況檢查中使用的健全狀況檢查範例。計算的健康狀態檢查會使用一些個別的健康狀態檢查來決定合併的狀態。每個個別運作狀態檢查的狀態是根據端點的運作狀態或 Amazon CloudWatch 指標的狀態而定。您可以將健全狀況檢查合併到計算的健康狀態檢查中，然後設定計算的健全狀況檢查，以根據個別健全狀況檢查的合併健康狀態報告健全狀況。根據您對應用程式效能和可用性的需求，調整計算運作狀態檢查的敏感度。

有關計算運作狀態檢查的資訊，請參閱 Amazon Route 53 開發人員指南中的監控其他運作狀態檢查 (計算的運作狀態檢查) 如需其他資訊，請參閱 Route 53 改進 — 計算運作 Health 態檢查和延遲檢查的部落格文章。

主題

- Amazon CloudFront 分佈
- 負載平衡器
- Amazon EC2 彈性 IP 地址 (EIP)

Amazon CloudFront 分佈

下列範例說明可以合併為 CloudFront 分配的已計算健康狀態檢查的運作狀態檢查：

- 透過在提供動態內容的發佈上指定路徑的網域名稱來監視端點。一個健康的響應將包括 HTTP 響應代碼 2xx 和 3xx。
- 監控正在測量 CloudFront 原點健康狀態的 CloudWatch 警報狀態。例如，您可以在「Application Load Balancer」度量上維護 CloudWatch 警示`TargetResponseTime`，並建立反映警示狀態的健全狀況檢查。當要求離開負載平衡器到負載平衡器接收到來自目標的回應之間的回應時間超過警示中設定的臨界值時，健全狀況檢查可能會不健康。
- 監視 CloudWatch 警報的狀態，該警報可測量響應的 HTTP 狀態碼為 5xx 的請求百分比。如果 CloudFront 分配的 5xx 錯誤率高於 CloudWatch 警示中定義的臨界值，則此健康狀態檢查的狀態將切換為狀態不良。

負載平衡器

下列範例說明可用於針對「應用程式負載平衡器」、「Network Load Balancer」或「全域加速器」標準加速器計算的健全狀況檢查的運作狀態檢查

- 監視警示的狀態，該 CloudWatch 警示會測量用戶端與負載平衡器建立的新連線數目。您可以為新連線的平均數量設定警示閾值，其程度高於每天的平均值。每種資源類型的指標如下：
  - Application Load Balancer `NewConnectionCount`
  - Network Load Balancer：`ActiveFlowCount`
  - 全球加速器：`NewFlowCount`
- 對於「Application Load Balancer 器」和「Network Load Balancer」，監視 CloudWatch 警示的狀態，該警示會測量被視為良好的負載平衡器數目。您可以在可用區域或負載平衡器需要的運作狀態良好的主機數目下限上設定警示臨界值。負載平衡器資源的可用度量如下：
  - Application Load Balancer `HealthyHostCount`
  - Network Load Balancer：`HealthyHostCount`
- 針對「Application Load Balancer」，監視警示的狀態，該 CloudWatch 警示會測量負載平衡器目標所產生的 HTTP 5xx 回應代碼數目。對於「應用程式負載平衡器」，您可以使用指標，`HTTPCode_Target_5XX_Count`並以負載平衡器的所有 5xx 錯誤總和為基礎，並根據警示臨界值。

Amazon EC2 彈性 IP 地址 (EIP)

下列範例運作狀態檢查可以合併為 Amazon EC2 彈性 IP 地址的計算運作狀態檢查：

- 透過指定彈性 IP 位址的 IP 位址來監視端點。只要可以使用 IP 位址後面的資源建立 TCP 連線，健康狀態檢查就會保持健康狀態。
- 監控 CloudWatch 警示狀態，以測量執行個體目前正在使用的已配置 Amazon EC2 運算單元的百分比。您可以使用 Amazon EC2 指標，`CPUUtilization`並根據您認為應用程式的高 CPU 使用率 (例如 90%) 來設定警示閾值。

管理資源保護 AWS Shield Advanced

使用本節中的指南來管理資源的 Shield 進階防護。

> **Note**
>
> 護 Shield 進階僅保護您在 Shield 牌進階或透過護 Shield 進階策略指定的資源。 AWS Firewall Manager 它不會自動保護您的資源。

如果您使用的是 AWS Firewall Manager Shield 進階政策，則不需要針對原則範圍內的資源管理保護。Firewall Manager 員會根據策略組態，自動管理策略範圍內之帳號和資源的保護。如需詳細資訊，請參閱 AWS Shield Advanced 政策。

主題

- 為 AWS 資源添加 AWS Shield Advanced 保護
- 設定 AWS Shield Advanced 保護
- 從 AWS 資源移除 AWS Shield Advanced 保護

為 AWS 資源添加 AWS Shield Advanced 保護

請遵循本節中的指引，將 Shield 進階防護新增至一或多個資源。

若要新增 AWS 資源的保護

1. 登入 AWS Management Console 並開啟 Shield 牌主控台 AWS WAF (S)，網址為 https://console.aws.amazon.com/wafv2/。
2. 在導覽窗格中， AWS Shield 選擇 [受保護的資源] 下方。
3. 選擇 [新增要保護的資源]。
4. 在 「選擇要使用 Shield 進階保護的資源」頁面的「指定區域」與「資源類型」中，針對您要保護的資源提供「區域」與「資源類型」規格。您可以選取「所有區域」來保護多個區域中的資源，也可以選取「全域」，將選取範圍縮小為全域資源。您可以取消選取任何不想保護的資源類型。如需有關資源類型保護的資訊，請參閱AWS Shield Advanced 依資源類型分類的保護。
5. 選擇「載入資源」。「Shield 牌進階」會將符合您條件的資源填入「選取 AWS 資源」區段。
6. 在 「選取資源」 區段中，您可以輸入要在資源清單中搜尋的字串，以篩選資源清單。

   選取您要保護的資源。
7. 在「標籤」區段中，如果您要將標籤新增至您正在建立的防 Shield 進階保護，請指定這些標籤。若要取得有關標籤 AWS 資源的資訊，請參閱〈使用標籤編輯器
8. 選擇使用 Shield 進階保護。這樣可以為資源增加護 Shield 進階保護。

設定 AWS Shield Advanced 保護

您可以隨時變更 AWS Shield Advanced 防護的設定。若要這麼做，請逐步瀏覽所選保護的選項，並修改您需要變更的設定。

管理受保護的資源

1. 登入 AWS Management Console 並開啟 Shield 牌主控台 AWS WAF (S)，網址為 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 導覽窗格中，選擇 [受保護的資源]。
3. 在 [保護] 索引標籤中，選取您要保護的資源。
4. 選擇 [設定保護] 和您想要的資源規格選項。
5. 逐步瀏覽每個資源保護選項，並視需要進行變更。

設定應用程式層 DDoS 保護

為了防止對 Amazon CloudFront 和 Application Load Balancer 資源的攻擊，您可以新增 AWS WAF Web ACL 並新增以速率為基礎的規則。如需相關資訊，請參閱Shield 進階應用程式層 AWS WAF Web ACLs 和速率型規則。

您也可以啟用防 Shield 進階自動應用程式層 DDoS 緩解功能。如需有關 AWS WAF 運作方式的資訊，請參閱AWS WAF。如需有關自動緩和功能的資訊，請參閱Shield 先進的自動應用層 DDoS 緩解。

> **Important**
>
> 如果您透過 AWS Firewall Manager 使用 Shield 進階政策來管理 Shield 進階防護，則無法在此管理應用程式層防護。對於所有其他資源，我們建議您至少將 Web ACL 附加到每個資源，即使 Web ACL 不包含任何規則也是如此。

> **Note**
>
> 當您為資源啟用自動應用程式層 DDoS 緩解時，該作業會自動將服務連結角色新增至您的帳戶，以便為 Shield Advanced 授予管理 Web ACL 保護所需的權限。如需相關資訊，請參閱使用服務連結角色進階 Shield。

若要設定應用程式層 DDoS 保護

1. 在 [設定第 7 層 DDoS 防護] 頁面中，如果資源尚未與 Web ACL 相關聯，您可以選擇現有的 Web ACL 或建立自己的 ACL。

   若要建立 Web ACL，請執行下列步驟：

   a. 選擇 建立 Web ACL。

   b. 輸入名稱。建立 Web ACL 後無法修改名稱。

   c. 選擇建立。

   > **Note**
   >
   > 如果資源已與 Web ACL 關聯，您無法變更為不同的 Web ACL。如果您想要變更 Web ACL，您必須先從資源移除關聯的 Web ACL。如需詳細資訊，請參閱 建立 Web ACL 與資源的關聯或取消關聯 AWS。

2. 如果 Web ACL 未定義以速率為基礎的規則，您可以選擇新增速率限制規則，然後執行下列步驟來新增規則：

   a. 輸入名稱。

   b. 輸入速率限制。這是在將以速率為基礎的規則動作套用至 IP 位址之前，任何單一 IP 位址在任何五分鐘內允許的要求數目上限。當來自 IP 位址的要求低於限制時，動作便會中止。

   c. 設定規則動作，以在 IP 位址的要求計數超過限制時計數或封鎖來自 IP 位址的要求。應用程式和移除規則動作可能會在 IP 位址要求率變更後一兩分鐘生效。

   d. 選擇新增規則。

3. 對於自動應用程式層 DDoS 緩解，請選擇您是否希望 Shield Advanced 代表您自動緩解 DDoS 攻擊，如下所示：

   - 若要啟用自動緩和措施，請選擇 [啟用]，然後選取您希望 Shield Advanced 在其自訂規則中使用的規則動作。 AWS WAF 您的選擇是Count和Block。如需有關這些 AWS WAF 規則動作的資訊，請參閱規則動作。如需 Shield 進階如何管理此動作設定的相關資訊，請參閱「Shield 牌進階」如何管理規則動作設定。
   - 若要停用自動緩和措施，請選擇停用。
   - 若要讓您正在管理的資源的自動緩和措施設定保持不變，請保留預設選項 [保留目前設定]。

如需有關防 Shield 進階自動應用程式層 DDoS 緩解的資訊，請參閱Shield 先進的自動應用層 DDoS 緩解。

4. 選擇下一步。

建立鬧鐘和通知

下列程序顯示如何管理受保護資源的 CloudWatch 警示。

> **Note**
>
> CloudWatch 會產生額外費用。有關 CloudWatch 定價，請參閱 Amazon CloudWatch 定價。

若要建立鬧鐘和通知

1. 在 [保護] 頁面 [建立警示和通知-選用] 中，針對您要接收的警示和通知設定 SNS 主題。對於您不想收到通知的資源，請選擇 No topic (無主題)。您可以新增 Amazon SNS 主題或建立新主題。
2. 若要建立 Amazon SNS 主題，請依照下列步驟執行：
   a. 在下拉式清單中，選擇 [建立 SNS 主題]。
   b. 輸入主題名稱。
   c. 選擇性地輸入將傳送 Amazon SNS 訊息的電子郵件地址，然後選擇 [新增電子郵件]。您可以輸入多個。
   d. 選擇建立。
3. 選擇下一步。

從 AWS 資源移除 AWS Shield Advanced 保護

您可以隨時從任何資 AWS 源中移除 AWS Shield Advanced 保護。

> **Important**
>
> 刪除資 AWS 源並不會從中移除資源 AWS Shield Advanced。您也必須從中移除資源的保護 AWS Shield Advanced，如本程序所述。

移除 AWS Shield Advanced 資 AWS 源的保護

1. 登入 AWS Management Console 並開啟 Shield 牌主控台 AWS WAF (S)，網址為 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 導覽窗格中，選擇 [受保護的資源]。
3. 在 [保護] 索引標籤中，選取您要移除其保護的資源。
4. 選擇 [刪除保護]。
   - 如果您設定了 Amazon CloudWatch 警報以進行保護，則可以選擇刪除警報以及保護。如果您此時選擇不刪除鬧鐘，您可以稍後使用 CloudWatch 主控台將其刪除。

> **Note**
>
> 對於已設定 Amazon Route 53 運作狀態檢查的保護，如果稍後再次新增保護，保護仍會包含運作狀態檢查。

上述步驟會移除特定資 AWS 源的 AWS Shield Advanced 保護。他們不會取消您的 AWS Shield Advanced 訂閱。您將繼續支付該服務的費用。如需有關您的 AWS Shield Advanced 訂閱的資訊，請聯絡中AWS Support 心。

從防護 Shield 進階保護移除 CloudWatch 警報

若要移除 Shield 進階防護的 CloudWatch 警示，請執行下列其中一項操作：

- 刪除 從 AWS 資源移除 AWS Shield Advanced 保護 所述的保護。請確實選取 Also delete related DDoSDetection alarm (同時刪除相關 DDoSDetection 警示) 旁的核取方塊。
- 使用 CloudWatch 控制台刪除警報。要刪除的警示名稱以 DDoS 開頭DetectedAlarmForProtection。

AWS Shield Advanced 保護群組

使用保護群組建立受保護資源的邏輯集合，並以群組形式管理其保護。如需有關管理資源保護的資訊，請參閱設定 AWS Shield Advanced 保護。

> **Note**
>
> 自動應用程式層 DDoS 防護功能不會與保護群組互動。您可以為保護群組中的資源啟用自動緩和措施，但 Shield Advanced 不會根據保護群組發現的項目自動套用攻擊緩和措施。Shield 牌進階對個別資源套用自動攻擊緩和措施。

AWS Shield Advanced 保護群組可讓您以自助方式，將多個受保護的資源視為單一單元來自訂偵測和緩解範圍。資源分組可提供許多好處。

- 提高檢測的準確性。
- 減少無法執行的事件通知。
- 增加緩解措施的涵蓋範圍，以包含在事件期間也可能受到影響的受保護資源。
- 加速緩解具有多個類似目標的攻擊的時間。
- 促進新創建的受保護資源的自動保護。

在藍色/綠色交換等情況下，保護群組可協助減少誤判，其中資源在接近零負載和完全載入之間交替。另一個範例是，當您經常建立和刪除資源，同時維護群組成員之間共用的負載層級。對於這種情況，監視個別資源可能會導致誤判，而監視資源群組的健全狀況則不會。

您可以將保護群組設定為包含所有受保護的資源、特定資源類型的所有資源，或個別指定的資源。符合保護群組條件的新受保護資源會自動包含在您的保護群組中。受保護的資源可以屬於多個保護群組。

管理 AWS Shield Advanced 保護群組

請使用本節中的指導來管理您的保護群組組態。

建立 Shield 牌進階保護群組

若要建立保護群組

1. 登入 AWS Management Console 並開啟 Shield 牌主控台 AWS WAF (S)，網址為 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 導覽窗格中，選擇 [受保護的資源]。
3. 選擇保護群組索引標籤，然後選擇 [建立保護群組]。
4. 在 [建立保護群組] 頁面中，提供群組的名稱。您將使用此名稱來識別受保護資源清單中的群組。您無法在建立保護群組之後變更它的名稱。

5. 在「保護」分組條件中，選取您希望 Shield Advanced 用來識別要包含在群組中的受保護資源的條件。根據您選擇的條件進行其他選擇。
6. 在「彙總」中，選取您希望 Shield Advanced 如何結合群組的資源資料，以便偵測、緩解和報告事件。

   - 總和 — 使用整個群組的總流量。對於大多數情況下，這是一個不錯的選擇。範例包括可手動或自動擴展的 Amazon EC2 執行個體的彈性 IP 地址。
   - 平均值 — 使用整個群組的平均流量。對於統一共享流量的資源來說，這是一個不錯的選擇。範例包括加速器和負載平衡器。
   - 最大 — 使用來自每個資源的最高流量。這對於不共享流量的資源以及以非統一方式共享流量的資源非常有用。範例包括用於 CloudFront 分發的 Amazon 分 CloudFront 發和來源資源。
7. 選擇 [儲存] 以儲存您的保護群組，並返回 [受保護的資源] 頁面。

在「Shield 牌事件」頁面中，您可以檢視保護群組的事件，並向下展開以查看群組中受保護資源的其他資訊。

更新 Shield 牌進階保護群組

更新保護群組

1. 登入 AWS Management Console 並開啟 Shield 牌主控台 AWS WAF (S)，網址為 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 導覽窗格中，選擇 [受保護的資源]。
3. 在 [保護群組] 索引標籤中，選取您要修改之保護群組旁邊的核取方塊。
4. 在保護群組的頁面中，選擇 [編輯]。對保護群組設定進行變更。
5. 選擇儲存，以儲存變更。

刪除 Shield 進階保護群組

若要刪除保護群組

1. 登入 AWS Management Console 並開啟 Shield 牌主控台 AWS WAF (S)，網址為 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 導覽窗格中，選擇 [受保護的資源]。
3. 在 [保護群組] 索引標籤中，選取您要移除之保護群組旁邊的核取方塊。
4. 在保護群組的頁面中，選擇 [刪除] 並確認動作。

追蹤資源保護變更 AWS Config

您可以使用記錄對資源 AWS Shield Advanced 保護的變更 AWS Config。然後，您可以使用這些資訊來維護組態變更歷史記錄，稽核和排除故障問題。

若要記錄保護變更， AWS Config 請為您要追蹤的每個資源啟用。如需詳細資訊，請參閱《AWS Config 開發人員指南》中的開始使用 AWS Config。

您必須針 AWS Config 對每個包 AWS 區域 含追蹤資源的項目啟用。您可以 AWS Config 手動啟用，也可以使用《使用 AWS CloudFormation 指南 AWS Config》中的範AWS CloudFormation StackSets 例範本中的「啟AWS CloudFormation 用」範本。

如果您啟用 AWS Config，系統會依AWS Config 定價頁面上的詳細資訊向您收費。

> **Note**
>
> 如果您已 AWS Config 啟用必要的區域和資源，則無需執行任何動作。 AWS Config 有關資源保護變更的記錄會開始自動填入。

啟用之後 AWS Config，請使用 AWS Config 主控台中的美國東部 (維吉尼亞北部) 區域來檢視 AWS Shield Advanced 全域資源的組態變更歷史記錄。

透過美國東部 (維吉尼亞北部)、美國東部 (俄亥俄)、美國西部 (奧勒岡)、美國西部 (加利佛尼亞北部)、歐洲 (愛爾蘭)、歐洲 (法蘭克福)、亞太區 AWS Shield Advanced 域 (東京) 和亞太區域 (雪梨) 區域的 AWS Config 主控台，檢視區域資源的變更記錄。

DDoS 事件的可見性

AWS Shield 提供下列類別的事件和事件活動的可見度：

- 全域 — 所有客戶都可以存取過去兩週內全域威脅活動的彙總檢視。您可以在主控台的 [入門] 和 [全域威脅] 儀表板頁面下看到此資 AWS Shield 訊。如需詳細資訊，請參閱 AWS Shield 全域和帳戶活動。
- 帳戶 — 所有客戶都可以存取其帳戶前一年的事件摘要。您可以在主控台的 [開始使用] 頁面下看到此資 AWS Shield 訊。如需詳細資訊，請參閱 AWS Shield 全域和帳戶活動。

當您訂閱 Shield Advanced 並為資源添加保護時，您可以訪問有關受保護資源的事件和 DDoS 攻擊的其他信息：

- 受保護資源上的事件 — Shield Advanced 透過 AWS Shield 主控台的「事件」頁面提供每個事件的詳細資訊。如需詳細資訊，請參閱 AWS Shield Advanced 事件。
- 受保護資源的事件指標 — Shield Advanced 針對其保護的所有資源發佈偵測、緩解措施和主要貢獻者 Amazon CloudWatch 指標。您可以使用這些指標來設定 CloudWatch 儀表板和警示。如需詳細資訊，請參閱 AWS Shield Advanced 度量。
- 受保護資源的跨帳戶事件可見性 — 如果您用 AWS Firewall Manager 來管理 Shield Advanced 防護，您可以透過結合使用 Firewall Manager 員來啟用多個帳戶的防護能見度。 AWS Security Hub如需詳細資訊，請參閱 跨帳戶的事件可見性。

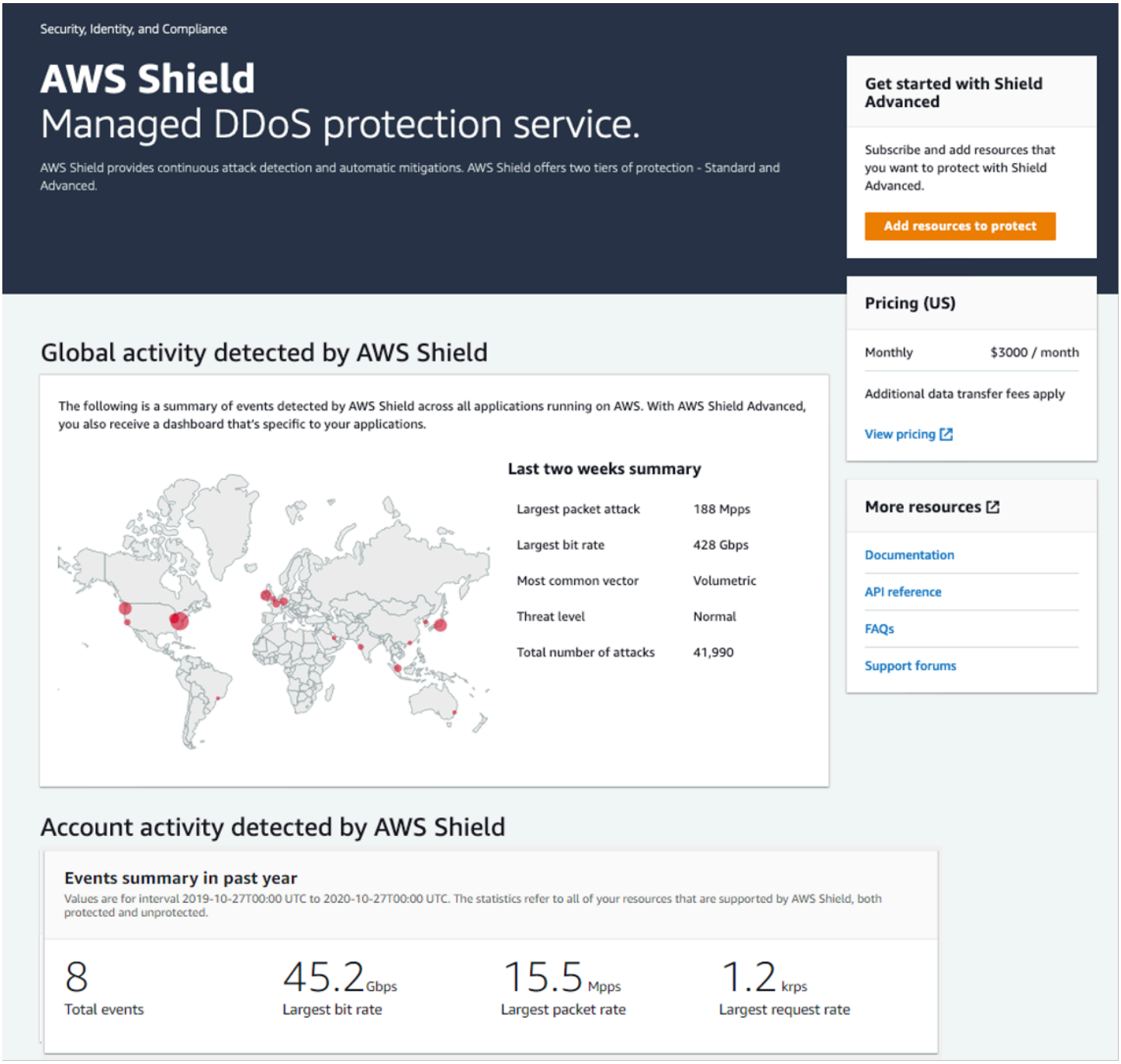
如果您為應用程式層保護啟用自動應用程式層 DDoS 緩解功能，

主題

AWS Shield 全域和帳戶活動

您可以在 AWS Shield 主控台開始使用和全域威脅儀表板頁面中，存取全域威脅活動的彙總檢視和每個帳戶事件摘要。

下列螢幕擷取畫面顯示 [入門] 頁面的範例。



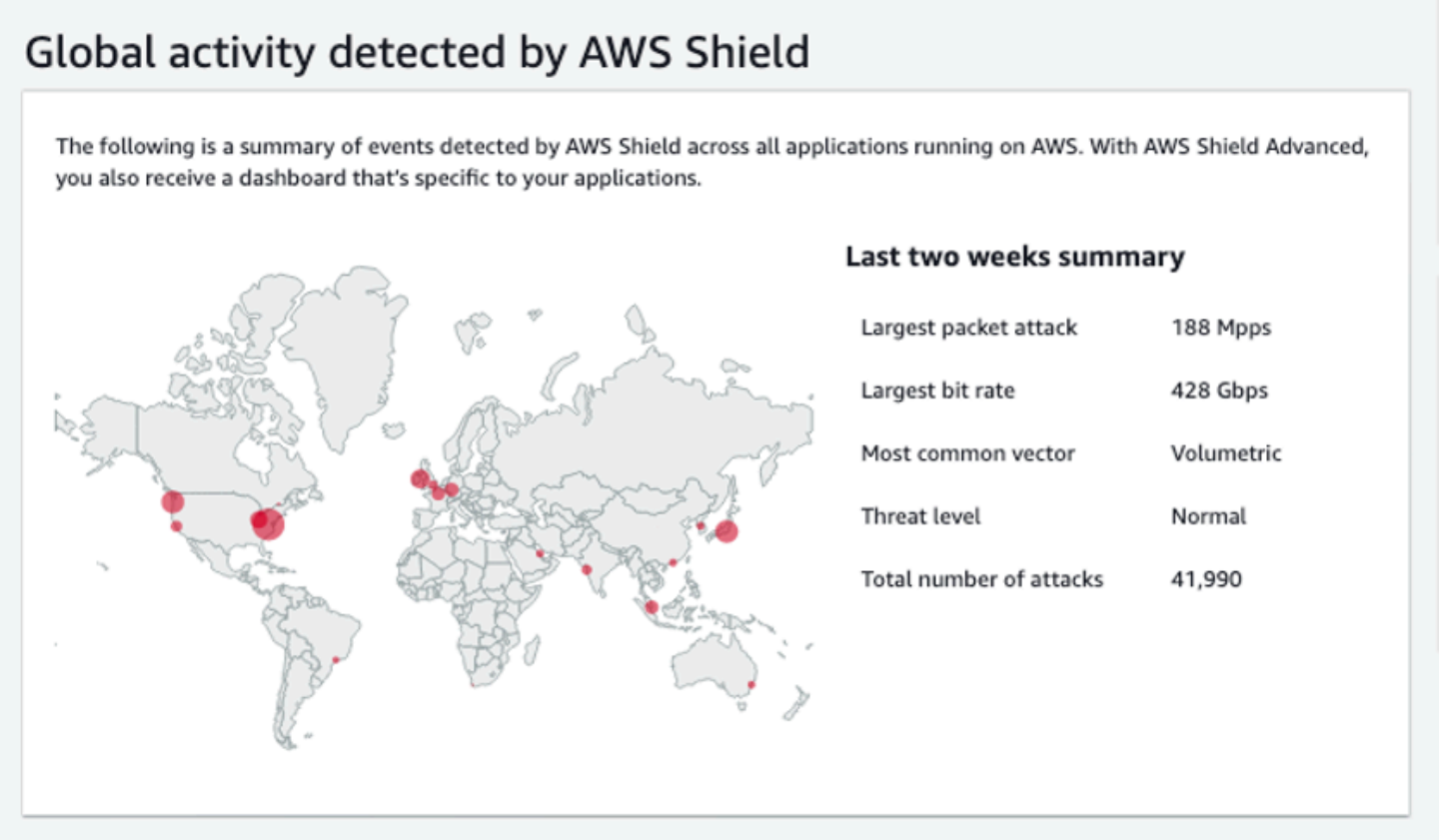
存取 AWS Shield 主控台

- 登入 AWS Management Console 並開啟 Shield 牌主控台 AWS WAF (S)，網址為 https://console.aws.amazon.com/wafv2/。

您不需要訂閱 Shield Advanced 即可存取全球活動和帳戶事件摘要資訊。

全球活動

此資訊可透過 AWS Shield 主控台的「全域威脅儀表板」和「入門」頁面取得。下列螢幕擷取畫面顯示全域活動窗格的範例。



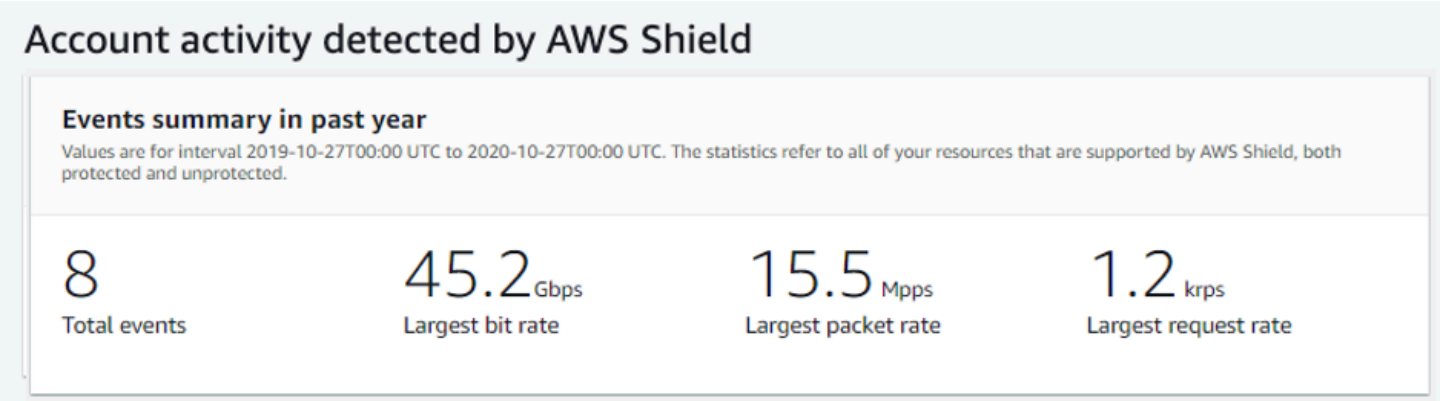
全球活動描述了在所有 AWS 客戶中觀察到的 DDoS 事件。每小時一次， AWS 更新前兩週的資訊。在控制台窗格中，您可以看到按 AWS 區域劃分並顯示在世界熱圖上的結果。在地圖旁邊，Shield 會顯示摘要資訊，例如最大封包攻擊、最大位元速率、最常見的向量、攻擊總數和威脅等級。威脅等級是對目前全球活動的評估，與 AWS 通常觀察到的活動相比。預設威脅等級值為「正常」。 AWS 自動將值更新為高，以提高 DDoS 活動。

全球威脅儀表板還提供時間序列指標，讓您能夠在時間持續時間之間進行變更。要查看重大 DDoS 攻擊的歷史記錄，您可以自定義從最後一天到過去兩週的視圖儀表板。時間序列度量可針對您選取的時間範圍 AWS 內執行的應用程式偵測到的所有事件，提 AWS Shield 供最大位元速率、封包速率或要求率的檢視。

帳戶活動

此資訊可在 AWS Shield 主控台 [開始使用] 頁面中取得。

下列螢幕擷取畫面顯示範例帳戶活動窗格。



帳戶活動描述 Shield 針對您的資源偵測到符合 Shield 進階保護資格的 DDoS 事件。Shield 每天都會為前一天 00:00 UTC 結束的年度建立摘要指標，然後顯示事件總數、最大位元速率、最大封包速率和最大請求率。

- 事件總計量度會反映每次 Shield 在傳送至您應用程式的流量中觀察到可疑屬性時。可疑屬性可能包括高於正常磁碟區的流量、與應用程式歷史設定檔不符的流量，或與 Shield 針對有效應用程式流量定義的啟發式法不相符的流量。
- 每個資源都可以使用最大的位元速率和最大封包速率統計資料。
- 最大的請求率統計資料僅適用於具有關聯 AWS WAF Web ACL 的 Amazon CloudFront 分發和應用程式負載平衡器。

> **Note**
>
> 您還可以通過 AWS Shield API 操作訪問帳戶級別的事件摘要DescribeAttackStatistics。

AWS Shield Advanced 事件

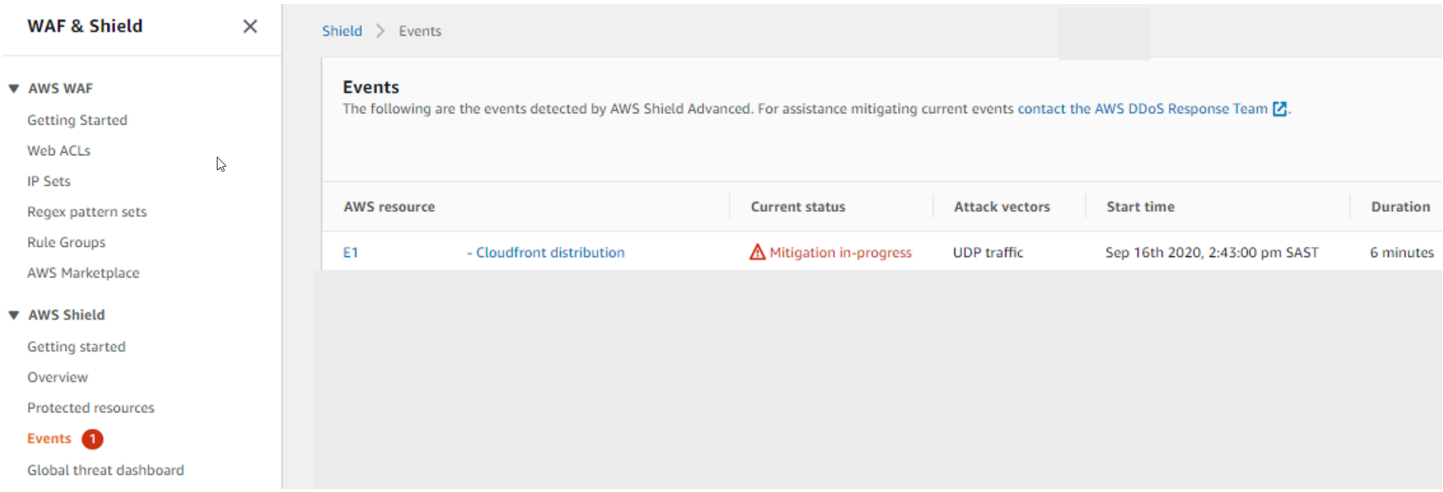
當您訂閱 Shield Advanced 並保護您的資源時，您可以存取資源的其他可見性功能。其中包括 Shield Advanced 偵測到的事件的近乎即時通知，以及有關偵測到的事件和緩和措施的其他資訊。

> **Note**
>
> 您在 Shield 進階主控台中的賽事資訊是以 Shield 牌進階指標為基礎。如需「Shield 進階」度量的相關資訊，請 AWS Shield Advanced 度量

AWS Shield 沿著多個維度評估受保護資源的流量。偵測到異常時，護 Shield 進階會為每個受影響的資源建立個別的事件。

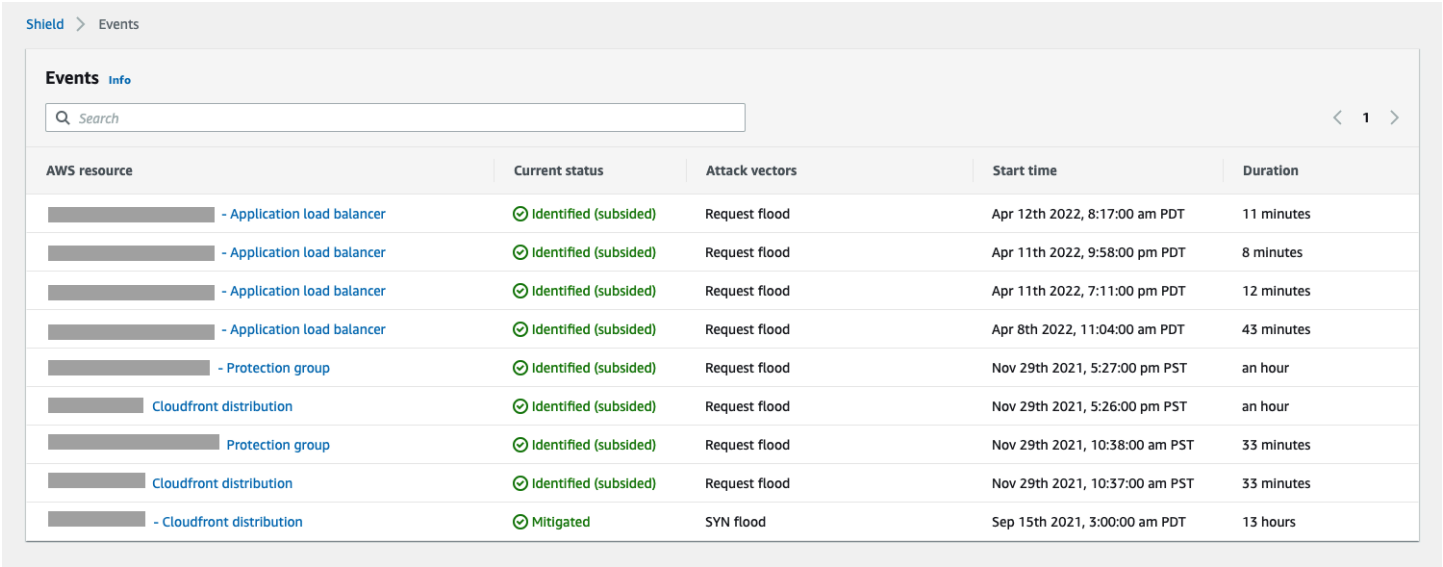
您可以透過 Shield 主控台的「事件」頁面存取事件摘要和詳細資訊。最上層「事件」頁面提供目前和過去事件的總覽。

下面的屏幕截圖顯示了一個單一正在進行的事件的例子事件頁面。此活動事件也會在左側導覽窗格中加上旗標。



Shield Advanced 也可能會根據流量類型和您設定的保護，自動針對攻擊放置緩和措施。這些緩和措施可以保護您的資源，避免接收符合已知 DDoS 攻擊特徵的過量流量或流量。

下列螢幕擷取畫面顯示一個範例事件，其中所有事件都已由 Shield Advanced 緩解或已自行消退的事件。



在活動開始前保護您的資源

在受到 DDoS 攻擊之前，使用 Shield Advanced 在接收正常預期流量時使用 Shield Advanced 保護資源來提高事件偵測的準確性。

為了準確地報告受保護資源的事件，Shield Advanced 必須先為其建立預期流量模式的基準。

- Shield Advanced 會在資源受到保護至少 15 分鐘後報告基礎結構層事件。
- 「Shield 牌進階」會在資源受到保護至少 24 小時後報告 Web 應用程式層事件。在 Shield Advanced 觀察 30 天的預期流量之後，應用層事件的偵測準確度最高。

若要存取 AWS Shield 主控台中的事件資訊

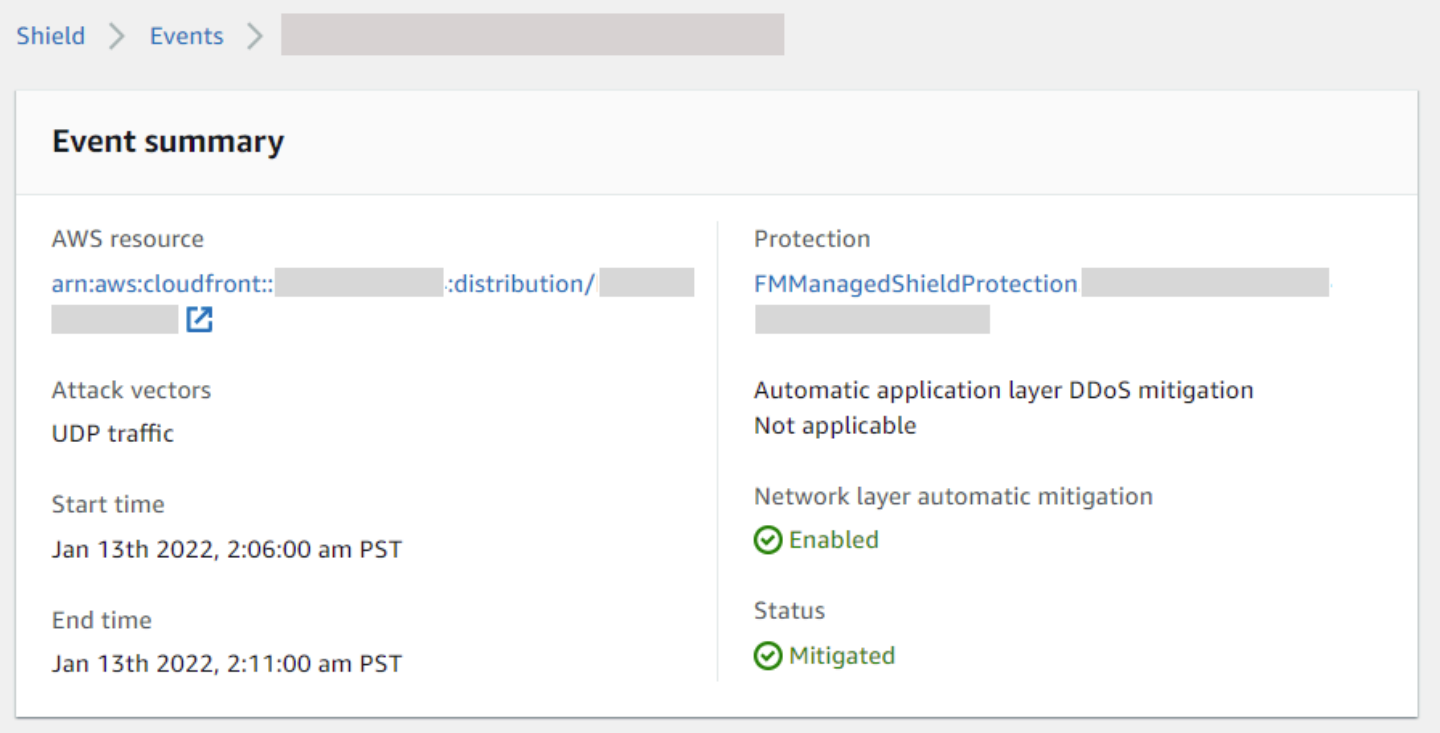
1. 登入 AWS Management Console 並開啟 Shield 牌主控台 AWS WAF (S)，網址為 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 導覽窗格中，選擇 [事件]。主控台會顯示 [事件] 頁面。
3. 在「事件」(E ven ts) 頁面中，您可以選取清單中的任何事件，以查看事件的其他摘要資訊和詳細資訊。

主題

AWS Shield Advanced 事件摘要

您可以在事件的主控台頁面中檢視事件的摘要和詳細資訊。若要開啟事件的頁面，請從「事件」(E vents) 頁面清單中選取其 AWS 資源名稱。

下列螢幕擷取畫面顯示網路層事件的範例事件摘要。



事件頁面摘要資訊包括下列項目。

- 目前狀態 — 指出事件狀態以及「Shield 牌進階」對事件所採取之動作的值。狀態值會套用至基礎結構層 (第 3 層或第 4 層) 和應用程式層 (第 7 層) 事件。
  - 已識別（進行中）和已識別（消退）— 這些表示 Shield Advanced 偵測到事件，但到目前為止尚未對其採取任何行動。已識別 (已停止) 表示 Shield 偵測到的可疑流量已停止，而未經介入。
  - 緩解進行中和已緩解 — 這些表示 Shield Advanced 偵測到事件並已對其採取行動。當目標資源是 Amazon CloudFront 分發或 Amazon Route 53 託管區域 (具有自己的自動內嵌緩解措施) 時，也會使用降低功能。
- 攻擊媒介 — DDoS 攻擊媒介，例如 TCP SYN 洪水和 Shield 牌高級檢測啟發式方法，例如請求洪水。這些可能是 DDoS 攻擊的指標。
- 開始時間 — 偵測到第一個異常流量資料點的日期和時間。
- 持續時間或結束時間 — 表示 Shield Advanced 觀察到的事件開始時間和上次觀察到的異常資料點之間經過的時間。雖然事件正在進行中，這些值將繼續增加。
- 保護 — 命名與資源相關聯的 Shield 進階防護，並提供其防護頁面的連結。這可以在個別活動的頁面中找到。
- 自動應用程式層 DDoS 緩解 — 用於應用程式層保護，用於指示資源是否已啟用 Shield 進階自動應用程式層 DDoS 緩解。如果已啟用，則會提供存取和管理組態的連結。這可以在個別活動的頁面中找到。

- 網路層自動緩解 — 指出資源是否在網路層具有自動緩解功能。如果資源具有網路層元件，則會啟用此功能。此信息可在個別活動的頁面中找到。

對於經常以目標為目標的資源，Shield 可能會在超量流量消退後將緩和措施留在適當位置，以防止進一步的重複發生事件。

> **Note**
>
> 您也可以透過 AWS Shield API 作ListAttacks業存取受保護資源的事件摘要。

AWS Shield Advanced 活動詳情

您可以在事件的主控台頁面底部查看有關事件偵測、緩解措施和主要貢獻者的詳細資訊。本節可能包括合法和可能不需要的流量混合，並且可能代表傳遞到受保護資源的流量和 Shield 緩和措施阻止的流量。

- 偵測和緩解措施 — 提供有關觀察到的事件及任何套用的緩和措施的資訊。如需事件緩和的相關資訊，請參閱回應 DDoS 事件。
- 頂級貢獻者 — 對活動中涉及的流量進行分類，並列出 Shield 為每個類別識別的主要流量來源。如果是應用程式層事件，請使用主要貢獻者資訊來取得事件性質的一般概念，但請使用這些 AWS WAF 記錄檔做為安全性決策。如需詳細資訊，請參閱以下各節。

您在 Shield 進階主控台中的賽事資訊是以 Shield 牌進階指標為基礎。如需「Shield 進階」度量的相關資訊，請 AWS Shield Advanced 度量

Amazon CloudFront 或 Amazon Route 53 資源不包含緩解指標，因為這些服務受到始終啟用且不需要緩解措施的緩解系統保護。

詳細資料區段會根據資訊是針對基礎結構層還是應用程式層事件而有所不同。

應用層事件詳細信息

您可以在事件的主控台頁面底部查看應用程式層事件偵測、緩解措施和主要貢獻者的詳細資料。本節可能包括合法和可能不需要的流量混合，並且可能代表傳遞至受保護資源的流量和 Shield Advanced 緩和措施封鎖的流量。

緩和措施詳細資料適用於 Web ACL 中與資源相關聯的任何規則，包括針對回應攻擊而特別部署的規則，以及 Web ACL 中定義的以速率為基礎的規則。如果您為應用程式啟用自動應用程式層 DDoS 緩

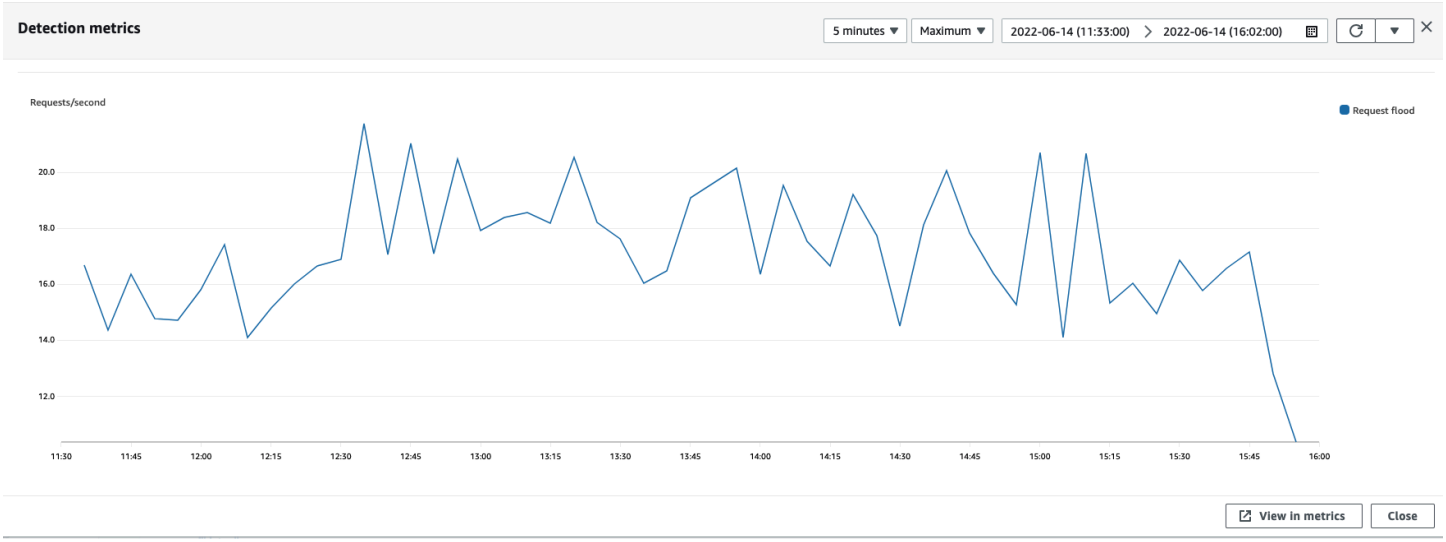
解措施，緩解指標會包含這些額外規則的指標。如需有關這些應用程式層保護的資訊，請參閱AWS Shield Advanced 應用程式層 (第 7 層) 保護。

偵測和緩解

對於應用程式層 (第 7 層) 事件，[偵測和緩和措施] 索引標籤會根據 AWS WAF 記錄檔取得的資訊顯示偵測指標。緩解指標是以關聯 Web ACL 中設定為封鎖不需要流量的 AWS WAF 規則為基礎。

對於 Amazon CloudFront 分發，您可以設定 Shield 進階為您套用自動緩和措施。使用任何應用程式層資源，您可以選擇在 Web ACL 中定義自己的緩和規則，也可以向 Shield 牌回應小組 (SRT) 請求協助。如需這些選項的資訊，請參閱 回應 DDoS 事件。

下列螢幕擷取畫面顯示在數小時後消退之應用程式層事件的偵測指標範例。



緩解規則生效前消退的事件流量不會顯示在緩解指標中。這可能會導致偵測圖表中顯示的 Web 要求流量與緩和圖表中顯示的允許和封鎖量度之間產生差異。

頂尖貢獻者

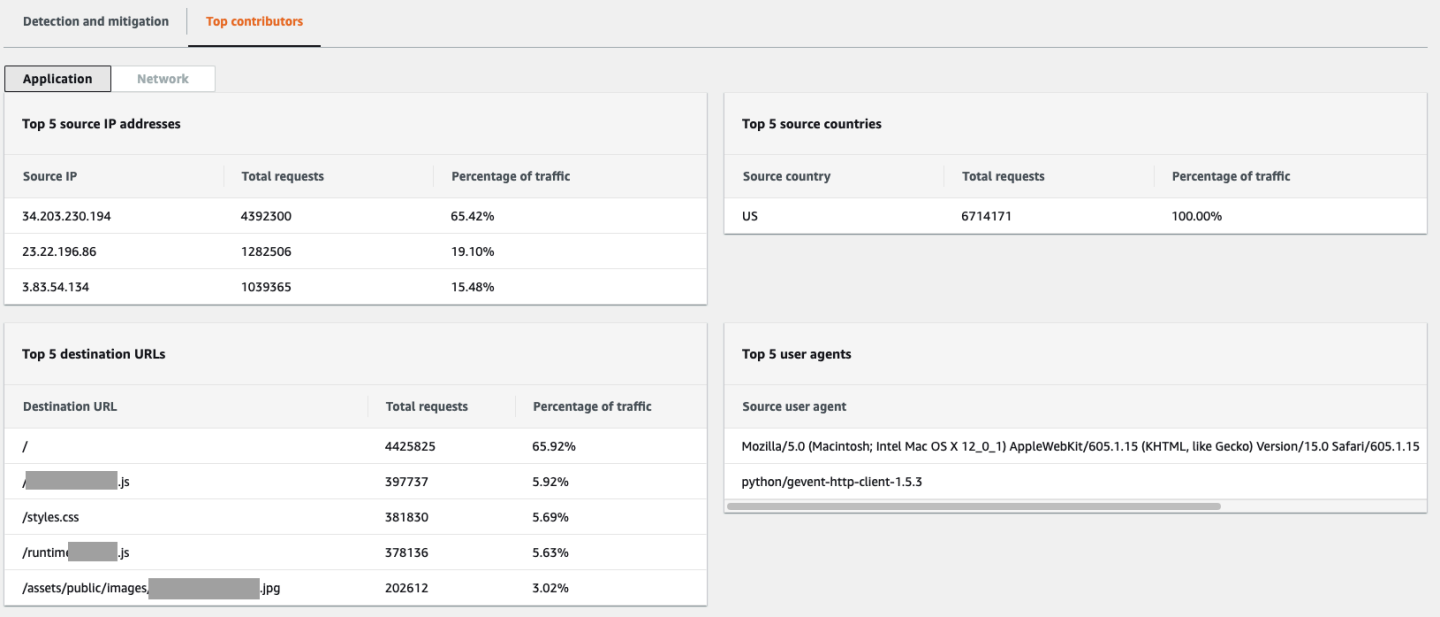
應用程式層事件的頂尖貢獻者索引標籤會根據 Shield 擷取的 AWS WAF 記錄檔，顯示 Shield 為該事件識別的前 5 名貢獻者。Shield 會依來源 IP、來源國家/地區和目的地 URL 等維度來分類最熱門的貢獻者資訊。

> **Note**
>
> 如需有關導致應用程式層事件之流量的最準確資訊，請使用記 AWS WAF 錄檔。

使用 Shield 應用程式層的主要貢獻者資訊，只能大致瞭解攻擊的性質，而不是以安全決策為基礎。對於應用程式層事件， AWS WAF 記錄檔是瞭解攻擊貢獻者和設計緩解策略的最佳資訊來源。

Shield 主要貢獻者資訊並不總是完全反映 AWS WAF 記錄中的資料。當它擷取記錄檔時，Shield 會優先考慮降低對系統效能的影響，而不是從記錄擷取完整的資料集。這可能會導致 Shield 可用於分析的資料粒度遺失。在大多數情況下，大多數資訊都是可用的，但是對於任何攻擊，頂部貢獻者資料都可能在某種程度上傾斜。

下列螢幕擷取畫面顯示應用程式層事件的前幾個貢獻者索引標籤範例。



貢獻者信息基於對合法和潛在不需要流量的請求。較大的數量事件和請求來源未高度分佈的事件更有可能具有可識別的頂級貢獻者。大幅分散式攻擊可能有任意數量的來源，因此很難識別攻擊的主要貢獻者。如果 Shield Advanced 無法識別特定類別的重要貢獻者，就會將資料顯示為無法使用。

基礎結構層事件詳情

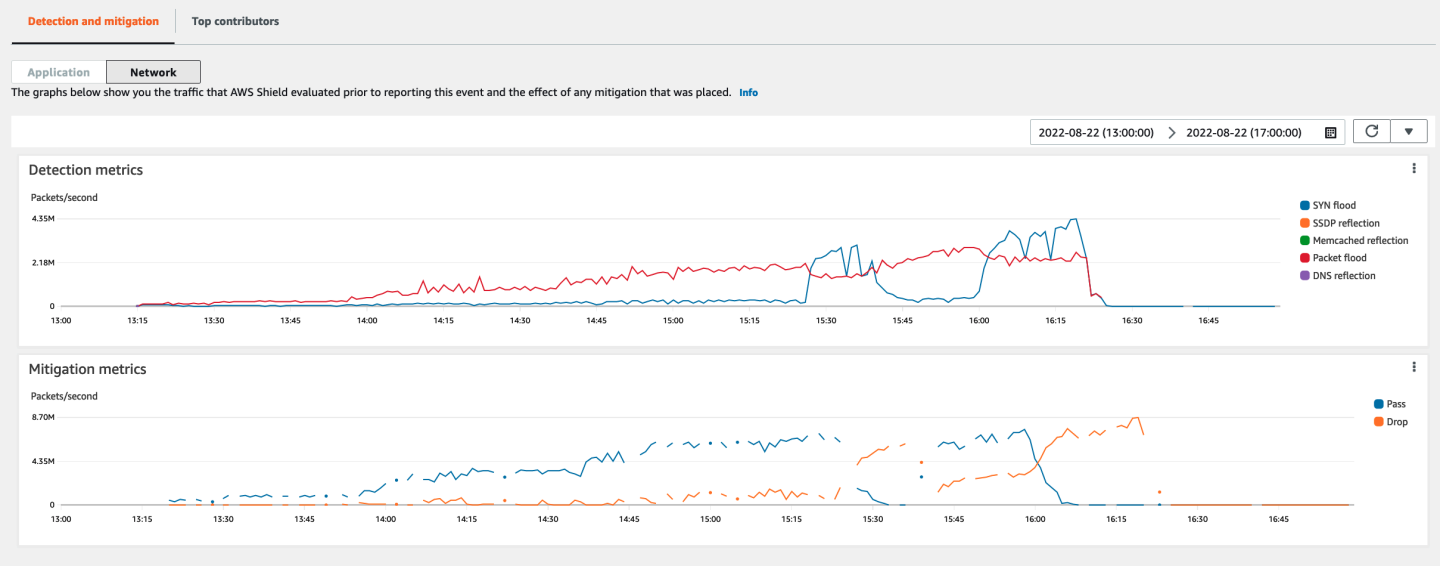
您可以在事件的主控台頁面底部查看有關基礎結構層事件偵測、緩解措施和主要貢獻者的詳細資料。本節可能包括合法和可能不需要的流量混合，並且可能代表傳遞到受保護資源的流量和 Shield 緩和措施阻止的流量。

偵測和緩解

對於基礎結構層（第 3 層或第 4 層）事件，[偵測和緩和措施] 索引標籤會顯示以取樣的網路流量和緩和措施指標為基礎的偵測指標，這些指標是根據緩和系統觀察到的流量。緩解指標是對資源流量進入的更精確的衡量。

Shield 會自動為受保護的資源類型彈性 IP (EIP)、Classic Load Balancer (CLB)、Application Load Balancer 器 (ALB) 和標準加速器建立緩和 AWS Global Accelerator 措施。EIP 位址和 AWS Global Accelerator 標準加速器的緩和指標指出傳遞和丟棄的封包數目。

下列螢幕擷取畫面顯示基礎結構層事件的 [偵測和緩和] 索引標籤範例。

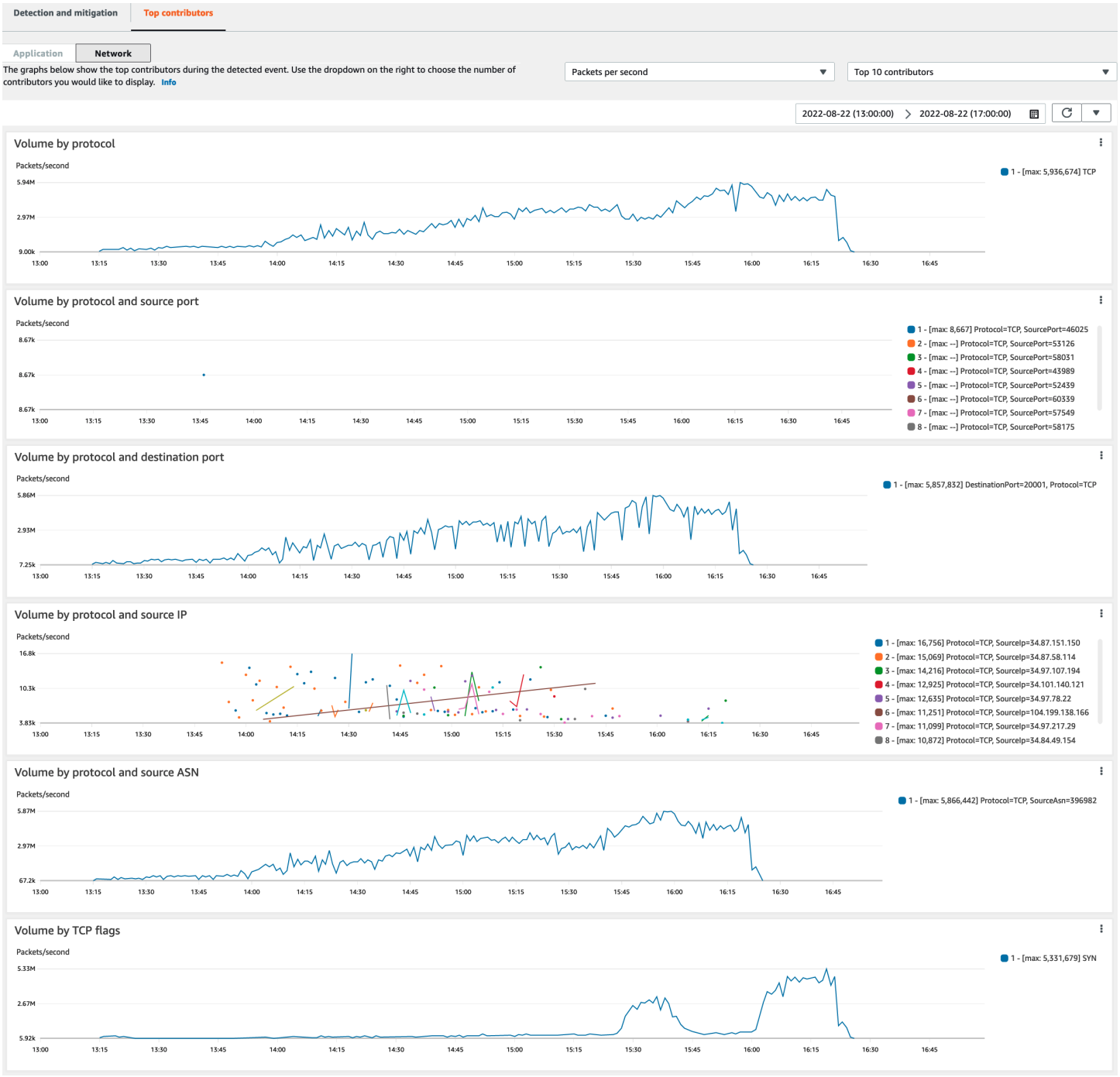


在 Shield 放置緩解之前消退的事件流量不會顯示在緩解指標中。這可能會導致偵測圖表中顯示的流量與緩和圖表中顯示的通過和捨棄量度之間產生差異。

頂尖貢獻者

基礎結構層事件的「熱門貢獻者」索引標籤會列出多個流量維度上最多 100 位頂尖貢獻者的量度。詳細資料包括任何可識別至少五個重要流量來源的維度的網路層屬性。流量來源的範例為來源 IP 和來源 ASN。

下列螢幕擷取畫面顯示基礎結構層事件的「前幾名貢獻者」索引標籤。



參與者指標是以針對合法和潛在不需要流量的取樣網路流量為基礎。流量來源未高度分佈的大量事件和事件更有可能具有可識別的頂級貢獻者。大幅分散式攻擊可能有任意數量的來源，因此很難識別攻擊的主要貢獻者。如果 Shield 無法識別特定量度或類別的任何重要貢獻者，則會將資料顯示為無法使用。

在基礎架構層 DDoS 攻擊中，流量來源可能會被欺騙或反映出來。攻擊者故意偽造了偽造的來源。反射來源是檢測到的流量的真正來源，但它不是攻擊的願意參與者。例如，攻擊者可能會透過反映網際網

路上通常合法服務的攻擊，對目標產生大量、擴大的流量。在這種情況下，源信息可能是有效的，而它不是攻擊的實際來源。這些因素可能會限制根據封包標頭封鎖來源的緩和技術的可行性。

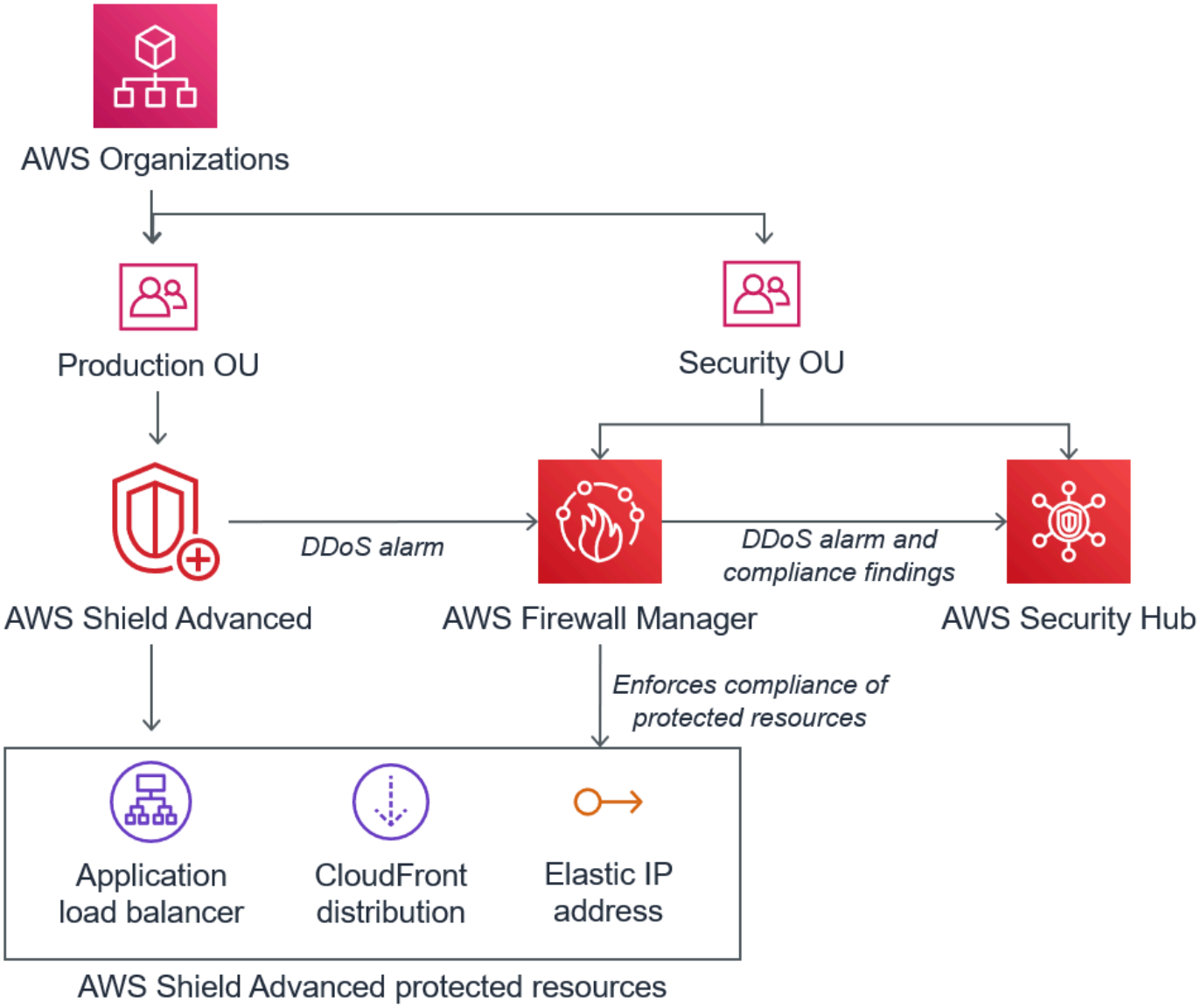
跨帳戶的事件可見性

您可以使用 AWS Firewall Manager 和 AWS Security Hub 管理和監控多個帳戶中 AWS Shield Advanced 受保護的資源。

使用 Firewall Manager 員，您可以建立 Shield 進階安全性原則，報告並強制執行所有帳戶的 DDoS 防護合規性。Firewall Manager 員會監控受保護的資源，包括為進入 Shield 進階策略範圍的新資源新增保護。

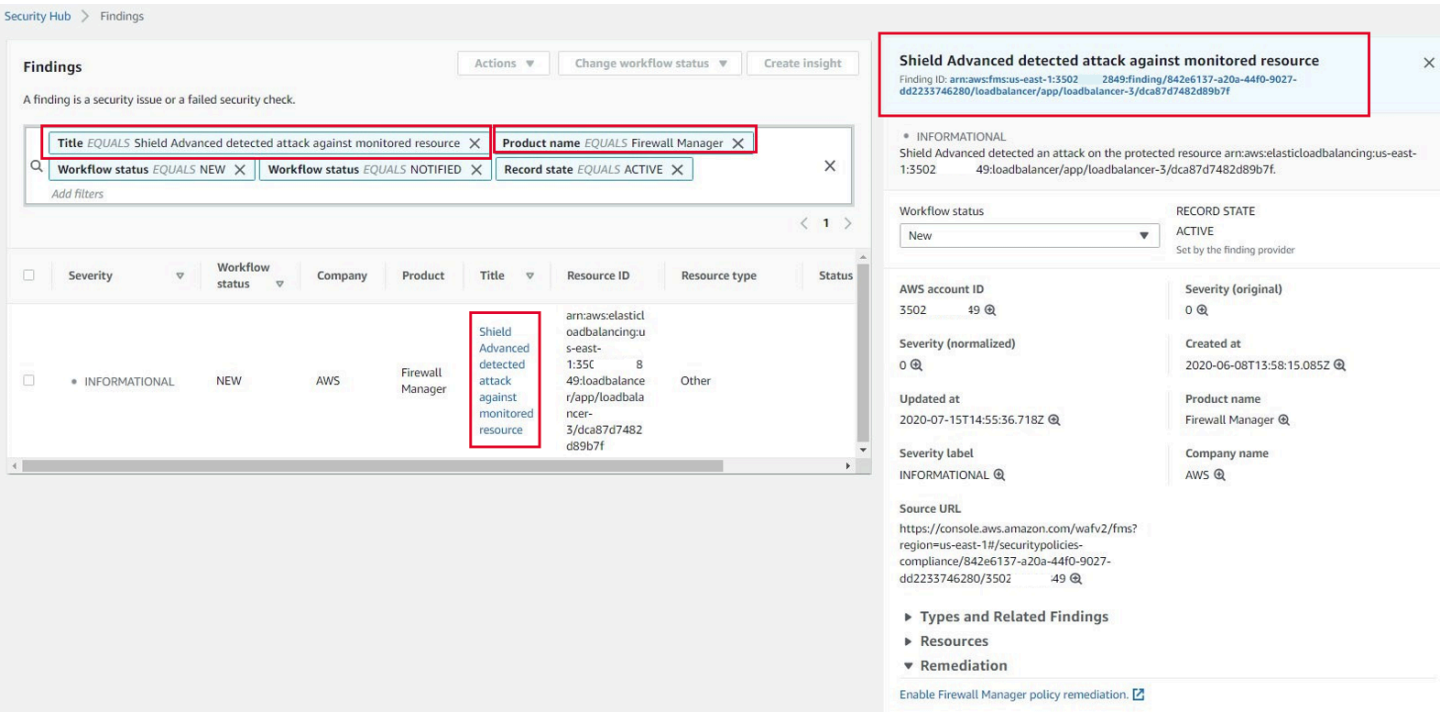
當 Firewall Manager 員識別出與 AWS Security Hub 您的 Shield Advanced 安全策略不合規的資源時，您可以將 Firewall Manager 員與以獲得報告由 Shield Advanced 和 Firewall Manager 器合規性發現偵測到的 DDoS 事件的單一儀表板。

下圖說明使用 Firewall Manager 員和 Security Hub 監視 Shield 進階受保護資源的典型架構。



將 Firewall Manager 與 Security Hub 整合時，您可以在單一位置檢視安全性發現項目，以及您執行之應用程式的其他警示和符合性狀態資訊 AWS。

下列螢幕擷取畫面反白顯示當您整合此類型時，Security Hub 主控台內的 Shield 進階事件可以看到的資訊。



若要瞭解如何將 Firewall Manager 員和安全中心與 Shield Advanced 整合，以集中監控受保護帳戶的事件和合規性，請參閱 AWS 安全性部落格設定 DDoS 事件集中監控，並自動修復不合規資源。

回應 DDoS 事件

AWS 自動緩解網路和傳輸層 (第 3 層和第 4 層) 分散式拒絕服務 (DDoS) 攻擊。如果您使用防 Shield 進階來保護您的 Amazon EC2 執行個體，則進行攻擊防 Shield 進階時，會自動將您的 Amazon VPC 網路 ACL 部署到網路邊界。 AWS 這使得 Shield 牌進階能夠針對較大的 DDoS 事件提供保護。如需網路 ACL 的詳細資訊，請參閱 網路 ACL。

對於應用程序層（第 7 層）DDoS 攻擊， AWS 嘗試通過 CloudWatch 警報檢測並通知 AWS Shield Advanced 客戶。依預設，它不會自動套用緩和措施，以避免意外封鎖有效的使用者流量。

對於應用程式層 (第 7 層) 資源，您可以使用下列選項來回應攻擊。

- 提供您自己的緩和措施 — 您可以自行調查和減輕攻擊。如需相關資訊，請參閱手動緩解應用程式層 DDoS 攻擊。
- 聯絡支援 — 如果您是 Shield Advanced 客戶，您可以聯絡AWS Support 中心以取得有關緩解措施的協助。重大和緊急案例會直接路由發送給 DDoS 專家。如需相關資訊，請參閱在應用程式層 DDoS 攻擊期間聯絡支援中心。

此外，在攻擊發生之前，您可以主動啟用下列緩和措施選項：

- Amazon CloudFront 分發上的自動緩解措施 — 使用此選項，Shield Advanced 在您的 Web ACL 中為您定義和管理緩解規則。如需自動應用程式層緩和措施的資訊，請參閱Shield 先進的自動應用層 DDoS 緩解。
- 主動參與 — 當 AWS Shield Advanced 偵測到針對其中一個應用程式的大型應用程式層攻擊時，SRT 可以主動與您聯絡。SRT 會對 DDoS 事件進行分類，並建立 AWS WAF 緩和措施。SRT 與您聯繫，並且在您同意的情況下，可以應用 AWS WAF 規則。如需有關此選項的詳細資訊，請參閱 設定主動參與。

在應用程式層 DDoS 攻擊期間聯絡支援中心

如果您是 AWS Shield Advanced 客戶，可以聯絡AWS Support 中心以取得有關緩解措施的協助。重大和緊急案例會直接路由發送給 DDoS 專家。通過 AWS Shield Advanced，複雜的案例可以升級到 AWS Shield 牌響應團隊（SRT），該團隊在保護方面擁有豐富的經驗 AWS，Amazon.com 及其子公司。如需 SRT 的詳細資訊，請參閱Shield 牌回應小組 (SRT) 支援。

若要取得 Shield 牌回應小組 (SRT) 支援，請聯絡中AWS Support 心。您的案例的回應時間取決於您選取的嚴重性和回應時間，這些時間會記錄在 [AWS Support 方案] 頁面上。

選取下列選項：

- 案例類型：技術支援
- 服務：分散式阻斷服務 (DDoS)
- 類別:入境至 AWS
- 嚴重等級：選擇適當選項

與我們的代表討論時，請說明您是遭受 DDoS 攻擊的 AWS Shield Advanced 客戶。我們的代表會引導您呼叫適當的 DDoS 專家。如果您使用分散式拒絕服務 (DDoS) 服務類型向AWS Support 中心提出案例，您可以透過聊天或電話直接與 DDoS 專家交談。DDoS 支援工程師可協助您識別攻擊、建議您的 AWS 架構改進，並提供 DDoS 攻擊緩解 AWS 服務的使用指引。

針對應用程式層攻擊，SRT 可協助您分析可疑活動。如果您已為資源啟用自動緩解措施，SRT 可以檢閱 Shield Advanced 自動針對攻擊進行的緩和措施。在任何情況下，SRT 都可以幫助您審查和緩解問題。SRT 建議的緩解措施通常需要 SRT 在您的帳戶中建立或更新 AWS WAF Web 存取控制清單 (Web ACL)。SRT 將需要您的許可才能執行此工作。

> **Important**
>
> 我們建議您按照中的步驟主動設定護 Shield 回應群組 (SRT) 的存取權限向 SRT 提供攻擊期間協助您所需的權限 AWS Shield Advanced，以便在啟用過程中進行操作。提前提供許可有助於防止在發生實際攻擊時所造成的事件延遲。

SRT 可協助您分類 DDoS 攻擊，以識別攻擊特徵和模式。在您的同意下，SRT 會建立並部署 AWS WAF 規則以減輕攻擊。

您也可以在可能發生攻擊之前或期間聯絡 SRT，以檢閱緩和措施，並開發和部署自訂的緩和措施。例如，如果您正在執行 Web 應用程式，而且只需要開啟連接埠 80 和 443，您可以使用 SRT 將 Web ACL 預先設定為「允許」連接埠 80 和 443。

您在帳戶層級授權並連絡 SRT。也就是說，如果您在 Firewall Manager 員防護進階策略中使用 Shield Advanced，帳戶擁有者 (而非 Firewall Manager 員管理員) 必須連絡 SRT 以取得支援。Firewall Manager 員管理員只能針對他們擁有的帳戶連絡 SRT。

手動緩解應用程式層 DDoS 攻擊

如果您確定資源的事件頁面中的活動代表 DDoS 攻擊，則可以在 Web ACL 中創建自己的 AWS WAF 規則以減輕攻擊。如果您不是 Shield 牌進階客戶，這是唯一可用的選項。 AWS WAF 包含 AWS Shield Advanced 在內，無需額外費用。若要取得有關在 Web ACL 中建立規則的資訊，請參閱〈〉AWS WAF 網頁存取控制清單 (網路 ACL)。

如果您使用 AWS Firewall Manager，則可以將 AWS WAF 規則新增至 Firewall Manager 員 AWS WAF 策略。

手動緩解潛在的應用程式層 DDoS 攻擊

1. 使用符合異常行為的準則，在 Web ACL 中建立規則陳述式。首先，將它們配置為計數匹配請求。如需有關設定 Web ACL 和規則陳述式的資訊，請參閱Web ACL 規則和規則群組評估和測試和調整您的 AWS WAF 保護。

   > **Note**
   >
   > 請務必先使用規則動作Count而非使用規則動作來測試您的規則Block。在您認為新規則正在識別正確的請求之後，您可以修改它們以阻止請求。

2. 監視要求計數，以判斷您是否要封鎖相符的要求。如果要求數量持續異常高，而且您確信規則正在擷取造成大量的要求，請變更 Web ACL 中的規則以封鎖要求。
3. 繼續監視事件頁面，以確保您的流量正在按照您的需求進行處理。

AWS 提供預先設定的範本，讓您快速開始使用。範本包含一組 AWS WAF 規則，您可以自訂並使用這些規則來封鎖常見的 Web 型攻擊。如需詳細資訊，請參閱 AWS WAF 安全自動化。

申請信用 AWS Shield Advanced

如果您已訂閱 AWS Shield Advanced 並且遭遇 DDoS 攻擊，會增加 Shield Advanced 受保護資源的使用率，您可以申請 Shield Advanced 服務抵免與使用率增加相關的費用，但在 Shield Advanced 未減輕使用率的範圍內。

> **Note**
>
> 您只能將透過此程序獲得的任何積分套用至 Shield 牌進階用量。Shield 牌進階積分無法與其他服務搭配使用。

抵免額僅適用於下列類型的費用：

- Shield 進階資料傳出
- Amazon CloudFront HTTP/HTTP請求
- CloudFront 資料傳出
- Amazon 路線 53 查詢
- AWS Global Accelerator 標準加速器資料傳輸
- Application Load Balancer 的負載平衡器容量單位
- 受保護 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的執行個體成本，這些執行個體是由 auto-scaling 政策建立以回應攻擊

申請信用額度的先決條件

要有資格獲得抵免，在攻擊開始之前，您必須完成以下操作：

- 您必須已為您要申請信用額度的資源新增 Shield 進階保護。攻擊期間新增的受保護資源不符合成本保護的資格。

> **Note**
>
> 在您的上啟用防 Shield 進階功能 AWS 帳戶 並不會自動為個別資源啟用防 Shield 進階防護。

如需如何使用「防護進階」保護 AWS 資源的詳細資訊，請參閱為 AWS 資源添加 AWS Shield Advanced 保護。

- 對於適用 CloudFront 且受 Application Load Balancer 保護的資源，您必須關聯 AWS WAF Web ACL，並以Block模式在 Web ACL 中實作以速率為基礎的規則。如需 AWS WAF 以速率為基礎的規則的資訊，請參閱速率型規則陳述式。如需有關如何將 Web ACL 與 AWS 資源建立關聯的資訊，請參閱AWS WAF 網頁存取控制清單 (網路 ACL)。
- 您必須在 DDoS 彈性的最佳實踐中實施了適當的AWS 最佳實踐，以最大程度地降低 DDoS 攻擊期間成本的方式配置應用程序。

如何申請信用

若要符合信用額度的資格，您必須在發生攻擊的帳單月份後的 15 天內提交您的信用申請。

要申請信用額度，請透過AWS Support 中心提交帳單個案。在您的請求中包含以下內容：

- 主旨行中的「DDoS 優惠」
- 您要求抵免的每個事件或可用性中斷的日期和時間
- 受影響的 AWS 服務和特定資源

提交請求後， AWS Shield 牌響應小組（ SRT ）將驗證是否發生 DDoS 攻擊，如果是，則是否有任何受保護的資源擴展以吸收 DDoS 攻擊。如果 AWS 確定受保護的資源擴展以吸收 DDoS 攻擊，則 AWS 將為確 AWS 定由 DDoS 攻擊引起的該部分流量發出評分。積分有效期限為 12 個月。

您使用 AWS Shield 服務時的安全性

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

> **Note**
>
> 本節為您使用 AWS Shield 服務及其 AWS 資源提供標準 AWS 安全性指引，例如 Shield 進階保護。
> 如需使用「護 Shield 與護 Shield 進階」保護 AWS 資源的相關資訊，請參閱本 AWS Shield 指南的其餘部分。

安全是 AWS 與您之間共同承擔的責任。共同責任模型 將此描述為雲端的安全和雲端內的安全：

- 雲端安全性 — AWS 負責保護中執行 AWS 服務的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。第三方稽核人員定期檢測及驗證安全的效率也是我們 AWS 合規計劃的一部分。若要瞭解適用於 Shield 的法規遵循計劃，請參閱合規計劃的AWS 服務範圍。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對資料敏感度、組織要求，以及適用法律和法規等其他因素負責。

本文件可協助您瞭解如何在使用 Shield 時套用共同責任模型。下列主題說明如何設定 Shield 以符合您的安全性和合規性目標。您也會學到如何使用其他可 AWS 協助您監控和保護 Shield 資源的服務。

主題

- Shield 牌中的資料保護
- 的身分識別與存取管理 AWS Shield
- 在 Shield 牌中進行記錄和監控
- Shield 牌的合規性驗證
- Shield 牌中的韌性
- AWS Shield中的基礎設施安全

Shield 牌中的資料保護

AWS 共用責任模型適用於中的資料保護 AWS Shield。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需有關資料隱私權的詳細資訊，請參閱資料隱私權FAQ。 如需歐洲資料保護的相關資訊，請參閱AWS 安全性GDPR部落格上的AWS 共同責任模型和部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 認證並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 對每個帳戶使用多重要素驗證 (MFA)。
- 使用SSL/TLS與 AWS 資源溝通。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 使用設定API和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果 AWS 透過命令列介面或存取時需要 FIPS 140-3 驗證的密碼編譯模組API，請使用端點。FIPS 如需有關可用FIPS端點的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用主控台、、API或 AWS 服務 使用 Shield 或其他使用時 AWS SDKs。 AWS CLI您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供URL給外部伺服器，我們強烈建議您不要在中包含認證資訊，URL以驗證您對該伺服器的要求。

除了某些無法使用加密的區域，包括中國（北京）和中國（寧夏），否則 Shield 實體（例如保護）會被靜態加密。每個區域都會採用唯一的加密金鑰。

的身分識別與存取管理 AWS Shield

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM管理員控制誰可以驗證（登錄）和授權（有權限）使用 Shield 資源。IAM是您 AWS 服務 可以免費使用的。

主題

- 物件
- 使用身分驗證
- 使用政策管理存取權
- 如何 AWS Shield 使用 IAM
- AWS Shield的身分型政策範例
- AWS 受管理的政策 AWS Shield
- 疑難排解 AWS Shield 身分和存取

- 使用服務連結角色進階 Shield

物件

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，具體取決於您在 Shield 中所做的工作。

服務使用者 — 如果您使用 Shield 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 Shield 功能來完成工作時，您可能需要額外的權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取「Shield」中的特徵，請參閱疑難排解 AWS Shield 身分和存取。

服務管理員 — 如果您負責公司的 Shield 資源，您可能擁有完整的 Shield 存取權。您的工作就是決定您的服務使用者應該存取哪些 Shield 功能和資源。然後，您必須向IAM管理員提交請求，才能變更服務使用者的權限。檢閱此頁面上的資訊，以瞭解的基本概念IAM。若要深入瞭解貴公司如何IAM搭配 Shield 使用，請參閱如何 AWS Shield 使用 IAM。

IAM系統管理員 — 如果您是IAM系統管理員，您可能想要瞭解如何撰寫原則以管理 Shield 存取權限的詳細資訊。若要檢視您可以在中使用的 Shield 身分型原則範例IAM，請參閱。AWS Shield的身分型政策範例

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以IAM使用者身分或假設IAM角色來驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM身分識別中心) 使用者、貴公司的單一登入驗證，以及您的 Google 或 Facebook 認證都是聯合身分識別的範例。當您以同盟身分登入時，您的管理員先前會使用IAM角色設定聯合身分識別。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以密碼編譯方式簽署您的要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署要求的詳細資訊，請參閱使用IAM者指南中的簽署 AWS API要求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。若要深入瞭解，請參閱使用AWS IAM Identity Center 者指南中的多重要素驗證和使用多重要素驗證 (MFA) AWS的使用IAM者指南。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以 root 使用者身分登入的完整工作清單，請參閱《使用指南》中的〈需要 root 使用者認證的IAM工作〉。

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步至您自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需IAM身分識別中心的相關資訊，請參閱IAM識別中心是什麼？在《AWS IAM Identity Center 使用者指南》中。

IAM 使用者和群組

IAM使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定權限。在可能的情況下，我們建議您仰賴臨時登入資料，而不要建立具有長期認證 (例如密碼和存取金鑰) 的IAM使用者。不過，如果您的特定使用案例需要使用IAM者的長期認證，建議您輪換存取金鑰。如需詳細資訊，請參閱《使用指南》中的「IAM定期輪換存取金鑰」以瞭解需要長期認證的使用案例。

IAM群組是指定IAM使用者集合的身分識別。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為的群組，IAMAdmins並授與該群組管理IAM資源的權限。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。要了解更多信息，請參閱《IAM用戶指南》中的創建用戶（而不是角色）的IAM時間。

IAM角色

IAM角色是您 AWS 帳戶 中具有特定權限的身份。它類似於用IAM戶，但不與特定人員相關聯。您可以切換角色來暫時擔任中 AWS Management Console 的角色。IAM您可以呼叫 AWS CLI 或 AWS

API作業或使用自訂來擔任角色URL。如需有關使用角色方法的詳細資訊，請參閱《使用指南》中的IAM〈使用IAM角色〉。

IAM具有臨時認證的角色在下列情況下很有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱《使用指南》中的〈建立第三方身分識別提供IAM者的角色〉。如果您使用IAM身分識別中心，則需要設定權限集。為了控制身分驗證後可以存取的內IAM容，IAMIdentity Center 會將權限集與中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時IAM使用者權限 — IAM 使用者或角色可以假定某個IAM角色，暫時取得特定工作的不同權限。
- 跨帳戶存取 — 您可以使用IAM角色允許不同帳戶中的某個人 (受信任的主體) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要瞭解跨帳戶存取角色與以資源為基礎的政策之間的差異，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或將物件存放在 Amazon S3 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用使用IAM者或角色執行中的動作時 AWS，您會被視為主參與者。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。
  - 服務角色 — 服務角IAM色是服務代表您執行動作的角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。
- 在 Amazon 上執行的應用程式 EC2 — 您可以使用IAM角色來管理在執行個體上EC2執行的應用程式以及發出 AWS CLI 或 AWS API請求的臨時登入資料。這比在EC2實例中存儲訪問密鑰更好。若要將 AWS 角色指派給EC2執行個體並讓其所有應用程式都能使用，請建立附加至執行個體的執行個體設定檔。執行個體設定檔包含角色，可讓執行個體上EC2執行的程式取得臨時登入資料。如需詳細資訊，請參閱使用者指南中的使用IAM角色將許可授與在 Amazon EC2 執行個體上執行的應IAM用程式。

要了解是否使用IAM角色還是用IAM戶，請參閱《用戶指南》中的「IAM創建IAM角色的時機（而不是用戶）」。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以JSON文件的形式儲存在中。如需有關JSON原則文件結構和內容的詳細資訊，請參閱《IAM使用指南》中的策略概觀。JSON

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

IAM原則會定義動作的權限，不論您用來執行作業的方法為何。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或取得角色資訊 AWS API。

身分型政策

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管策略或內嵌策略之間進行選擇，請參閱《IAM使用手冊》中的「在受管策略和內嵌策略之間進行選擇」。

資源型政策

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的策略IAM中使用 AWS 受管政策。

存取控制清單 (ACLs)

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

Amazon S3 和 Amazon VPC 是支持服務的示例ACLs。 AWS WAF若要進一步了解ACLs，請參閱 Amazon 簡單儲存服務開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 權限界限 — 權限界限是一項進階功能，您可以在其中設定以身分識別為基礎的原則可授與給IAM實體 (IAM使用者或角色) 的最大權限。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需有關權限界限的詳細資訊，請參閱《IAM使用指南》中的IAM實體的權限界限。
- 服務控制策略 (SCPs) — SCPs 是指定中組織或組織單位 (OU) 最大權限的JSON策略 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。如果您啟用組織中的所有功能，則可以將服務控制策略 (SCPs) 套用至您的任何或所有帳戶。SCP限制成員帳戶中實體的權限，包括每個帳戶 AWS 帳戶根使用者。如需有關 Organizations 的詳細資訊SCPs，請參閱AWS Organizations 使用指南中的服務控制原則。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱IAM使用指南中的工作階段原則。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要瞭解如何在涉及多個原則類型時 AWS 決定是否允許要求，請參閱IAM使用指南中的原則評估邏輯。

如何 AWS Shield 使用 IAM

在您用IAM來管理 Shield 存取權限之前，請先瞭解哪些IAM功能可搭配 Shield 使用。

IAM您可以搭配使用的功能 AWS Shield

IAM特徵	護 Shield 支撐
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	是
ACLs	否
ABAC(策略中的標籤)	部分
暫時性憑證	是
轉寄存取工作階段 (FAS)	是
服務角色	是
服務連結角色	是

若要深入瞭解 Shield 和其他 AWS 服務如何與大部分IAM功能搭配使用，請參閱IAM使用者指南IAM中的可使用AWS 服務。

以身分識別為基礎的 Shield 政策

支援身分型政策：是

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

使用以IAM身分識別為基礎的策略，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。若要瞭解可在JSON策略中使用的所有元素，請參閱《使用IAM者指南》中的IAMJSON策略元素參考資料。

若要檢視 Shield 身分型原則的範例，請參閱。AWS Shield的身分型政策範例

Shield 內以資源為基礎的政策

支援資源型政策：否

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

若要啟用跨帳戶存取，您可以在以資源為基礎的策略中指定一個或多個帳戶中的一個或多個帳戶中的IAM實體作為主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主參與者和資源不同時 AWS 帳戶，受信任帳戶中的IAM管理員也必須授與主參與者實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。

Shield 牌的政策行動

支援政策動作：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON策略`Action`元素描述了您可以用來允許或拒絕策略中存取的動作。策略動作通常與關聯 AWS API操作具有相同的名稱。有一些例外情況，例如沒有匹配API操作的僅限權限的操作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 Shield 動作清單，請參閱服務授權參考 AWS Shield中定義的動作。

Shield 中的政策動作會在動作之前使用下列前置詞：

```
shield
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "shield:action1",
      "shield:action2"
```

```
        ]
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定 Shield 中以開頭的所有動作`List`，請包含下列動作：

```
"Action": "shield:List*"
```

若要檢視 Shield 身分型原則的範例，請參閱。AWS Shield的身分型政策範例

Shield 牌政策資源

支援政策資源：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Resource`JSON原則元素會指定要套用動作的一或多個物件。陳述式必須包含 `Resource` 或 `NotResource` 元素。最佳做法是使用其 Amazon 資源名稱 (ARN) 指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看 Shield 資源類型及其清單ARNs，請參閱服務授權參考 AWS Shield中的定義資源。若要瞭解您可以針對每個資源指定哪些動作，請參閱由定義ARN的動作 AWS Shield。若要允許或拒絕存取 Shield 資源子集，請在策略ARN的`resource`元素中包含資源。

在 AWS Shield, 資源是保護和攻擊. 這些資源具有與其關聯的唯一 Amazon 資源名稱 (ARNs)，如下表所示。

AWS Shield 主控台中的名稱	姓名 AWS Shield SDK/ CLI	ARN格式	
事件或攻擊	`AttackDetail`	`arn:aws:shield:: account:attack/ID`	
保護	`Protection`	`arn:aws:shield:: account:protection/ ID`	

若要允許或拒絕存取 Shield 資源子集，請在策略ARN的`resource`元素中包含資源。Shield 牌的格式ARNs如下：

```
arn:partition:shield::account:resource/ID
```

更換 *account*, *resource* 和 *ID* 具有有效值的變量。有效值如下：

- *account*：您的識別碼 AWS 帳戶。您必須指定一個數值。
- *resource*：護 Shield 資源的類型，`attack`或者`protection`。
- *ID*：Shield 資源的 ID 或萬用字元 (*)，表示與指定之相關聯之指定類型的所有資源 AWS 帳戶。

例如，以下內容ARN指定了帳戶`111122223333`的所有保護：

```
arn:aws:shield::111122223333:protection/*
```

Shield 牌資源的格式如下：ARNs

```
arn:partition:shield:region:account-id:scope/resource-type/resource-name/resource-id
```

如需有關ARN規格的一 Amazon 資訊，請參閱 Amazon Web Services 一般參考. ARNs

以下列出資`wafv2`源ARNs的特定需求：

- *region*：對於您用來保護 Amazon CloudFront 分發的 Shield 牌資源，請將其設定為`us-east-1`。否則，請將其設定為您正在使用受保護區域資源的區域。
- *scope*：將範圍設定`global`為與 Amazon CloudFront 分發搭配使用，或`regional`與任何 AWS WAF 支援的區域資源搭配使用。區域資源包括 Amazon API 閘道RESTAPI、應用程式負載平衡器、AWS AppSync GraphQL API、Amazon Cognito 使用者集區、 AWS App Runner 服務和 AWS 驗證存取執行個體。
- *resource-type*: 指定下列其中一個值：`attack`針對事件或攻擊、`protection`保護。
- *resource-name*：指定您為 Shield 資源提供的名稱，或指定萬用字元 (*) 以指示滿足中其他規格的所有資源ARN。您必須指定資源名稱和資源 ID，或為兩者指定萬用字元。
- *resource-id*：指定 Shield 資源的 ID，或指定萬用字元 (*) 以指示滿足中其他規格的所有資源ARN。您必須指定資源名稱和資源 ID，或為兩者指定萬用字元。

例如，以下ARN指定所有ACLs具有區域範圍的 Web 區域`111122223333`中的帳戶`us-west-1`：

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

下列內容ARN指定區域111122223333中帳戶MyIPManagementRuleGroup的全域範圍命名的規則群組us-east-1：

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

若要檢視 Shield 身分型原則的範例，請參閱。AWS Shield的身分型政策範例

護 Shield 的政策條件金鑰

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，只有在IAM使用者名稱標記資源時，您才可以授與IAM使用者存取資源的權限。如需詳細資訊，請參閱《IAM使用指南》中的IAM政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《使用指南》中的AWS 全域條件內IAM容索引鍵。

若要查看 Shield 條件金鑰清單，請參閱服務授權參考 AWS Shield中的條件金鑰。若要瞭解您可以使用條件索引鍵的動作和資源，請參閱定義的動作 AWS Shield。

若要檢視 Shield 身分型原則的範例，請參閱。AWS Shield的身分型政策範例

ACLs在 Shield

支持ACLs：無

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

ABAC有 Shield 牌

支援 ABAC (策略中的標籤): 部分

以屬性為基礎的存取控制 (ABAC) 是一種授權策略，可根據屬性定義權限。在中 AWS，這些屬性稱為標籤。您可以將標籤附加至IAM實體 (使用者或角色) 和許多 AWS 資源。標記實體和資源是的第一步ABAC。然後，您可以設計ABAC策略，以便在主參與者的標籤與他們嘗試存取的資源上的標籤相符時允許作業。

ABAC在快速成長的環境中很有幫助，並且有助於原則管理變得繁瑣的情況。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需有關的詳細資訊ABAC，請參閱什麼是ABAC？ 在《IAM使用者指南》中。若要檢視包含設定步驟的自學課程ABAC，請參閱《使用指南》中的〈使用以屬性為基礎的存取控制 (ABAC) IAM 〉。

使用臨時登入資料搭配 Shield

支援臨時憑證：是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配使用 AWS 服務 ，請參閱《IAM使用指南》IAM中的使用方式。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立臨時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需有關切換角色的詳細資訊，請參閱《IAM使用者指南》中的〈切換到角色 (主控台)〉。

您可以使用 AWS CLI 或手動建立臨時認證 AWS API。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而非使用長期存取金鑰。如需詳細資訊，請參閱IAM。

Shield 牌的轉寄存取工作階段

支援轉寄存取工作階段 (FAS)：是

當您使用使用IAM者或角色在中執行動作時 AWS，您會被視為主參與者。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完

成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。

Shield 的服務角色

支援服務角色：是

服務角色是服務假定代表您執行動作的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給

> ⚠ Warning
>
> 變更服務角色的權限可能會中斷 Shield 功能。只有在 Shield 提供指引時才編輯服務角色。

Shield 牌的服務連結角色

支援服務連結角色：是

服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。

如需有關建立或管理 Shield 服務連結角色的詳細資訊，請參閱使用服務連結角色進階 Shield。

AWS Shield的身分型政策範例

根據預設，使用者和角色沒有建立或修改 Shield 資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

如需 Shield 定義的動作和資源類型的詳細資訊，包括每個資源類型的 ARN 格式，請參閱服務授權參考AWS Shield中的動作、資源和條件索引鍵。

主題

- 政策最佳實務
- 使用 Shield 牌主控台

- 允許使用者檢視他們自己的許可
- 授予您的 Shield 牌進階保護的讀取權限
- 授與「Shield」、 CloudFront和「唯讀」存取權 CloudWatch
- 授予護 Shield 的完整存取權限 CloudFront，以及 CloudWatch

政策最佳實務

以身分識別為基礎的政策決定是否有人可以在您的帳戶中建立、存取或刪除 Shield 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與服務動作的存取權 (如透過特 AWS 服務定的方式使用) AWS CloudFormation。如需更多資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

使用 Shield 牌主控台

若要存取 AWS Shield 主控台，您必須擁有最少一組權限。這些權限必須允許您列出並檢視您的 AWS 帳戶. 如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

可以存取和使用 AWS 主控台的使用者也可以存取 AWS Shield 主控台。不需要額外許可。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

授予您的 Shield 牌進階保護的讀取權限

AWS Shield 允許跨帳號資源存取，但不允許您建立跨帳號資源保護。您只能從擁有這些資源的帳戶內建立資源保護。

以下為一個範例政策，該政策授與對所有資源進行 shield:ListProtections 動作的許可。Shield 不支援針對某些 API 動作使用資源 ARN (也稱為資源層級權限) 來識別特定資源，因此您可以指定萬用字元 (*)。這只允許存取您可以透過動作擷取的資源ListProtections。

```
{
    "Version": "2016-06-02",
    "Statement": [
        {
            "Sid": "ListProtections",
            "Effect": "Allow",
            "Action": [
                "shield:ListProtections"
            ],
            "Resource": "*"
        }
    ]
}
```

授與「Shield」、 CloudFront和「唯讀」存取權 CloudWatch

以下政策授予使用者對 Shield 和相關資源 (包括 Amazon 資 CloudFront 源和 Amazon CloudWatch 指標) 的唯讀存取權。對於需要查看 Shield 保護和攻擊中的設置以及監視指標的權限的用戶而言，此功能非常有用。 CloudWatch這些使用者無法建立、更新或刪除 Shield 資源。

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "ProtectedResourcesReadAccess",
                "Effect": "Allow",
                "Action": [
                    "cloudfront:List*",
                    "elasticloadbalancing:List*",
                    "route53:List*",
                    "cloudfront:Describe*",
                    "elasticloadbalancing:Describe*",
                    "route53:Describe*",
                    "cloudwatch:Describe*",
```

```
                    "cloudwatch:Get*",
                    "cloudwatch:List*",
                    "cloudfront:GetDistribution*",
                    "globalaccelerator:ListAccelerators",
                    "globalaccelerator:DescribeAccelerator"
                ],
                "Resource": [
                    "arn:aws:elasticloadbalancing:*:*:*",
                    "arn:aws:cloudfront::*:*",
                    "arn:aws:route53:::hostedzone/*",
                    "arn:aws:cloudwatch:*:*:*:*",
                    "arn:aws:globalaccelerator::*:*"
                ]
            },
            {
                "Sid": "ShieldReadOnly",
                "Effect": "Allow",
                "Action": [
                    "shield:List*",
                    "shield:Describe*",
                    "shield:Get*"
                ],
                "Resource": "*"
            }
    ]
}
```

授予護 Shield 的完整存取權限 CloudFront，以及 CloudWatch

下列原則可讓使用者執行任何 Shield 作業、對 CloudFront Web 發佈執行任何作業，以及監控中的指標和要求範例 CloudWatch。這對身為 Shield 系統管理員的使用者很有用。

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "ProtectedResourcesReadAccess",
                "Effect": "Allow",
                "Action": [
                    "cloudfront:List*",
                    "elasticloadbalancing:List*",
                    "route53:List*",
                    "cloudfront:Describe*",
```

```
                    "elasticloadbalancing:Describe*",
                    "route53:Describe*",
                    "cloudwatch:Describe*",
                    "cloudwatch:Get*",
                    "cloudwatch:List*",
                    "cloudfront:GetDistribution*",
                    "globalaccelerator:ListAccelerators",
                    "globalaccelerator:DescribeAccelerator"
                ],
                "Resource": [
                    "arn:aws:elasticloadbalancing:*:*:*",
                    "arn:aws:cloudfront::*:*",
                    "arn:aws:route53:::hostedzone/*",
                    "arn:aws:cloudwatch:*:*:*:*",
                    "arn:aws:globalaccelerator::*:*"
                ]
            },
            {
                "Sid": "ShieldFullAccess",
                "Effect": "Allow",
                "Action": [
                    "shield:*"
                ],
                "Resource": "*"
            }
        ]
}
```

我們強烈建議您為具有管理權限的使用者設定多重驗證 (MFA)。如需詳細資訊，請參閱 IAM 使用指南 AWS中的搭配使用 Multi-Factor Authentication (MFA) 裝置。

AWS 受管理的政策 AWS Shield

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新 AWS 服務 的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 受管理的策略： AWSShieldDRTAccessPolicy

AWS Shield 當您授予 Shield 牌回應團隊 (SRT) 代表您採取行動的權限時，會使用此受管理政策。此政策提供 SRT 對您 AWS 帳戶的有限存取權，以協助在高嚴重性事件期間緩解 DDoS 攻擊。此政策允許 SRT 管理您的 AWS WAF 規則和防 Shield 進階保護，以及存取您 AWS WAF 的記錄。

如需授與 SRT 代表您操作之權限的相關資訊，請參閱設定護 Shield 回應群組 (SRT) 的存取權限。

如需有關此政策的詳細資訊，請參閱 IAM 主控台AWSShieldDRTAccessPolicy中的。

AWS 受管理的策略： AWSShieldServiceRolePolicy

Shield Advanced 會在您啟用自動應用程式層 DDoS 緩解功能時，使用此受管理策略來設定管理帳戶資源所需的權限。此政策允許 Shield Advanced 在您與受保護資源相關聯的 Web ACL 中建立和套用 AWS WAF 規則和規則群組，以自動回應 DDoS 攻擊。

您無法附加 AWSShieldServiceRolePolicy 到 IAM 實體。Shield 將此政策附加到服務連結的角色上，`AWSServiceRoleForAWSShield`以允許 Shield 代表您執行動作。

當您啟用自動應用程式層 DDoS 緩解功能時，Shield 牌進階會啟用此原則。如需有關此原則之用法的詳細資訊，請參閱Shield 先進的自動應用層 DDoS 緩解。

如需使用此原則之服務連結角色 AWSServiceRoleForAWSShield 的相關資訊，請參閱 使用服務連結角色進階 Shield

如需有關此政策的詳細資訊，請參閱 IAM 主控台AWSShieldServiceRolePolicy中的。

Shield AWS 受管理策略的更新

檢視有關 Shield AWS 受管政策的更新詳細資訊，因為此服務開始追蹤這些變更。如需有關此頁面變更的自動警示，請在 Shield 文件歷史記錄頁面上訂閱 RSS 摘要，網址為文件歷史紀錄。

政策	變更說明	日期
`AWSShieldServiceRolePolicy`	新增此原則，為 Shield Advanced 提供自動應用程式	2021 年 12 月 1 日

政策	變更說明	日期
此政策允許 Shield 存取和管理 AWS 資源，以便代表您自動回應應用程式層 DDoS 攻擊。 IAM 主控台中的詳細資訊：AWSShieldServiceRolePolicy 服務連結角色AWSServiceRoleForAWSShield 會使用此原則。如需相關資訊，請參閱使用服務連結角色進階 Shield。	層 DDoS 緩解功能所需的權限。如需有關此功能的資訊，請參閱Shield 先進的自動應用層 DDoS 緩解。	
Shield 牌開始追蹤變更	Shield 開始追蹤其 AWS 受管理政策的變更。	2021 年 3 月 3 日

疑難排解 AWS Shield 身分和存取

使用下列資訊可協助您診斷並修正使用 Shield 和 IAM 時可能會遇到的常見問題。

主題

- 我沒有在 Shield 牌中執行動作的權限
- 我沒有授權執行 iam：PassRole
- 我想讓我以外的人存取我 AWS 帳戶 的 Shield 牌資源

我沒有在 Shield 牌中執行動作的權限

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 shield:*GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 shield:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 shield:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我沒有授權執行 iam：PassRole

如果您收到未獲授權執行iam:PassRole動作的錯誤訊息，則必須更新您的政策以允許您將角色傳遞給 Shield。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為的 IAM 使用者marymajor嘗試使用主控台在 Shield 中執行動作時，就會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我想讓我以外的人存取我 AWS 帳戶 的 Shield 牌資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要瞭解 Shield 是否支援這些功能，請參閱如何 AWS Shield 使用 IAM。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM 使用者指南》中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 角色與資源型政策的差異。

使用服務連結角色進階 Shield

AWS Shield Advanced 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是一種獨特的 IAM 角色類型，可直接連結至 Shield 牌進階。服務連結角色由 Shield Advanced 預先定義，並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

服務連結角色讓設定 Shield Advanced 變得更容易，因為您不需要手動新增必要的權限。Shield 進階定義其服務連結角色的權限，除非另有定義，否則只有 Shield Advanced 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。這樣可以保護您的 Shield Advanced 資源，因為您無法不小心移除存取資源的權限。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

Shield 進階的服務連結角色權限

Shield 牌進階使用名為AWSServiceRoleForAWSShield的服務連結角色。此角色允許 Shield Advanced 存取和管理 AWS 資源，以便代表您自動回應應用程式層 DDoS 攻擊。如需此功能的詳細資訊，請參閱Shield 先進的自動應用層 DDoS 緩解。

服 AWSServiceRoleForAWSShield 務連結角色會信任下列服務擔任該角色：

- `shield.amazonaws.com`

名為的角色權限原則 AWSShieldServiceRolePolicy 允許 Shield Advanced 對所有 AWS 資源完成下列動作：

- `wafv2:GetWebACL`
- `wafv2:UpdateWebACL`
- `wafv2:GetWebACLForResource`
- `wafv2:ListResourcesForWebACL`
- `cloudfront:ListDistributions`
- `cloudfront:GetDistribution`

當允許對所有 AWS 資源執行動作時，這會在策略中表示為"Resource": "*"。這只表示服務連結角色可以對動作支援的所有 AWS 資源採取每個指定的動作。例如，wafv2:GetWebACL此動作僅支援 wafv2 Web ACL 資源。

Shield Advanced 只會針對已啟用應用程式層保護功能的受保護資源，以及與這些受保護資源相關聯的 Web ACL 進行資源層級 API 呼叫。

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

建立 Shield 進階的服務連結角色

您不需要手動建立一個服務連結角色。當您為 AWS Management Console、或 AWS API 中的資源啟用自動應用程式層 DDoS 緩解時 AWS CLI，Shield Advanced 會為您建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您為資源啟用自動應用程式層 DDoS 緩解時，Shield Advanced 會再次為您建立服務連結角色。

編輯 Shield 進階的服務連結角色

Shield 牌進階不允許您編輯 AWSServiceRoleForAWSShield 服務連結的角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需更多資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除 Shield 進階的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 如果 Shield Advanced 在您嘗試刪除資源時正在使用此角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

若要刪除「護 Shield 進階」資源 AWSServiceRoleForAWSShield

對於已設定應用程式層 DDoS 保護的所有資源，請停用自動應用程式層 DDoS 緩解功能。如需主控台指示，請參閱設定應用程式層 DDoS 保護。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台或 AWS API 刪除 AWSServiceRoleForAWSShield服務連結角色。 AWS CLI如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

Shield 進階服務連結角色的支援區域

Shield 進階支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱 Shield 進階端點和配額。

在 Shield 牌中進行記錄和監控

監控是保持 Shield 和您的 AWS 解決方案的可靠性、可用性和效能的重要組成部分。您應該從 AWS 解決方案的所有部分收集監視資料，以便在發生多點失敗時更輕鬆地偵錯。 AWS 提供數種工具來監控您的 Shield 資源並回應潛在事件：

Amazon CloudWatch 警報

您可以使用 CloudWatch 警示來監視指定期間內的單一量度。如果指標超過指定臨界值，則 CloudWatch 會傳送通知給 Amazon SNS 主題或 AWS Auto Scaling 政策。如需詳細資訊，請參閱使用 Amazon 監控 CloudWatch。

AWS CloudTrail 日誌

CloudTrail 提供使用者、角色或 AWS 服務在 Shield 中採取的動作記錄。使用收集的資訊 CloudTrail，您可以判斷向 Shield 提出的要求、提出要求的 IP 位址、提出要求的人員、提出要求的時間以及其他詳細資訊。如需更多詳細資訊，請參閱 使用 AWS CloudTrail記錄 API 呼叫。

Shield 牌的合規性驗證

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上進行HIPAA安全與合規架構 — 本白皮書說明公司如何使用建立符合資格的應 AWS 用程HIPAA式。

> **Note**
>
> 並非所有 AWS 服務 人都HIPAA符合資格。如需詳細資訊，請參閱合HIPAA格服務參考資料。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準 AWS 服務 與技術研究所 (NIST)、支付卡產業安全標準委員會 () 和國際標準化組織 ()PCI) 中保護安全控制指引的最佳做法，並將其對應至安全性控制。ISO
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您因應各種合規性需求 PCIDSS，例如符合特定合規性架構所要求的入侵偵測需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

Shield 牌中的韌性

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠在可用區域之間自動容錯移轉，而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱AWS 全域基礎結構。

AWS Shield中的基礎設施安全

作為託管服務， AWS Shield 受到 AWS 全球網絡安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的API呼叫透過網路存取 Shield。使用者端必須支援下列專案：

- 傳輸層安全性 (TLS)。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 具有完美前向保密（ ）的密碼套件，例如（短暫的迪菲-赫爾曼PFS）或DHE（橢圓曲線短暫迪菲-赫爾曼）。ECDHE現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與IAM主體相關聯的秘密存取金鑰來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 以產生暫時安全憑證以簽署請求。

AWS Shield Advanced 配額

AWS Shield Advanced 每個區域的實體數量都有預設配額。您可以請求提高這些配額。

資源	預設配額
針對每個帳號 AWS Shield Advanced 提供保護的每個資源類型的受保護資源數目上限。	1,000
每個帳戶的保護群組數目上限。	100
您可以特別包含在保護群組中的個別受保護資源數目上限。在 API 中，這適用於您`Members`在設定保護群組時指定`Pattern`的`ARBITRARY` 。在主控台中，這適用於您為保護群組選取的資源 [從受保護的資源中選擇]。	1,000

AWS Firewall Manager

AWS Firewall Manager 簡化您跨多個帳戶和資源的管理和維護任務，以提供各種保護 AWS WAF AWS Shield Advanced，包括 Amazon VPC 安全群組和網路 ACL AWS Network Firewall，以及 Amazon Route 53 解析器 DNS 防火牆。有了 Firewall Manager，您只需設定一次保護，服務就會自動將其套用至您的帳戶和資源，即使您新增了新的帳戶和資源也一樣。

防火牆管理員有這些優點：

- 協助保護跨帳戶的資源
- 有助於保護特定類型的所有資源，例如所有 Amazon CloudFront 分佈
- 協助保護有特定標籤的資源
- 自動新增保護到新增至帳戶中的資源
- 可讓您訂閱 AWS Organizations 組織中的所有成員帳戶 AWS Shield Advanced，並自動訂閱加入組織的新範圍內帳戶
- 允許您將安全群組規則套用至所有會員帳戶或 AWS Organizations 組織中特定帳戶子集，並自動將規則套用至加入組織的範圍內新帳戶
- 可讓您使用自己的規則，或從中購買受管規則 AWS Marketplace

當您想要保護整個組織而非少數特定帳戶和資源，或者您經常新增要保護的新資源時，Firewall Manager 特別有用。Firewall Manager 員還可以集中監控整個組織中的 DDoS 攻擊。

主題

AWS Firewall Manager 定價

所產生的費用 AWS Firewall Manager 是基礎服務，例如 AWS WAF 和 AWS Config。如需詳細資訊，請參閱 AWS Firewall Manager 定價。

AWS Firewall Manager 前提

本主題說明如何準備好進行管理 AWS Firewall Manager。您可以使用一個 Firewall Manager 員管理員帳戶來管理中組織的所有 Firewall Manager 員安全策略 AWS Organizations。除非另有說明，請使用您作為「Firewall Manager 員」系統管理員的帳戶執行先決條件步驟。

第一次使用 Firewall Manager 員之前，請依序執行下列步驟。

主題

步驟 1：加入並設定 AWS Organizations

若要使用 Firewall Manager 員，您的帳戶必須是 AWS Organizations 服務中要使用 Firewall Manager 員策略的組織成員。

> **Note**
>
> 如需有關 Organizations 的資訊，請參閱AWS Organizations 使用指南。

若要建立所需的 AWS Organizations 成員資格和組態

1. 選擇一個帳號，作為組織中組織的 Firewall Manager 員管理員。
2. 如果您選擇的帳戶還不是組織的成員，請加入該帳戶。請按照邀請加入您的組織中 AWS 帳戶的指導進行操作。

3. AWS Organizations 有兩個可用的功能集：合併帳單功能和所有功能。若要使用 Firewall Manager 員，您的組織必須啟用所有功能。如果您的組織只設定為合併帳單，請遵循啟用組織中的所有功能中的指引。

步驟 2：建立 AWS Firewall Manager 預設的管理員帳戶

此程序會使用您在上一個步驟中選擇並配置的帳戶與組織。

只有組織的管理帳戶可以建立 Firewall Manager 員預設管理員帳戶。您建立的第一個系統管理員帳戶是預設的系統管理員帳戶。預設管理員帳戶可以管理協力廠商防火牆，並具有完整的管理範圍 當您設定預設管理員帳戶時，Firewall Manager 員會自動將其設定為「Firewall Manager 員」的 AWS Organizations 委派管理員。這可讓 Firewall Manager 員存取組織中組織單位 (OU) 的相關資訊。您可以使用 OU 來指定 Firewall Manager 員策略的範圍。如需有關設定原則範圍的詳細資訊，請參閱下個別原則類型的指引建立 AWS Firewall Manager 策略。如需有關組 Organizations 和管理帳戶的詳細資訊，請參閱管理組織中的 AWS 帳戶。

組織管理帳戶的必要設定

組織的管理帳戶必須具有下列設定，才能將組織加入 Firewall Manager 員並建立預設管理員：

- 它必須是您要套用 Firewall Manager 員策略的組織成員。 AWS Organizations

設定預設管理員帳戶

1. AWS Management Console 使用現有的 AWS Organizations 管理帳戶登入 Firewall Manager 員。
2. 開啟位於 https://console.aws.amazon.com/wafv2/fmsv2 的 Firewall Manager 主控台。
3. 在導覽窗格中，選擇設定。
4. 輸 AWS 入您選擇作為 Firewall Manager 員使用的帳戶 ID。

> **Note**
>
> 預設管理員具有完整的管理範圍。完整的系統管理範圍表示此帳戶可以將原則套用至組織內的所有帳戶和組織單位 (OU)、在所有區域採取動作，以及管理所有 Firewall Manager 員原則類型。

5. 選擇 [建立管理員帳戶] 以建立帳戶。

如需管理 Firewall Manager 員管理員帳戶的詳細資訊，請參閱使用 AWS Firewall Manager 管理員。

步驟 3：啟用 AWS Config

若要使用 Firewall Manager 員，您必須啟用 AWS Config。

> **Note**
>
> 根據定 AWS Config 價，您的 AWS Config 設定會產生費用。如需詳細資訊，請參閱入門 AWS Config。

> **Note**
>
> 若要讓「Firewall Manager 員」監控策略符合性， AWS Config 必須持續記錄受保護資源的組態變更。在您的 AWS Config 配置中，錄製頻率必須設置為連續，這是默認設置。

啟用 AWS Config Firewall Manager 員

1. AWS Config 為您的每個成 AWS Organizations 員帳戶啟用，包括 Firewall Manager 員管理員帳戶。如需詳細資訊，請參閱入門 AWS Config。
2. 針 AWS Config 對包含要保護之資源的每個 AWS 區域 項目啟用。您可以 AWS Config 手動啟用，也可以在範例 AWS CloudFormation 範本中使用 AWS Config「啟用」AWS CloudFormation StackSets 範本。

   如果您不想 AWS Config 為所有資源啟用，則必須根據您使用的 Firewall Manager 員策略類型啟用下列項目：

   - WAF 策略 — 為資源類型 CloudFront 分 Config、應用程式負載平衡器 (從清單中選擇 ElasticLoadBalancingV2)、API Gateway、WAF WebACL、WAF 地區 WebACL 和 WAFv2 WebACL 啟用組態。若 AWS Config 要啟用保護發 CloudFront 佈，您必須位於美國東部 (維吉尼亞北部) 區域。「其他地區」沒有 CloudFront 作為選項。
   - 屏蔽政策 — 為資源類型啟用 Config Shield 保護、 ShieldRegional 保護、Application Load Balancer、EC2 EIP、WAF WebACL、WAF 區域 WebACL 和 WAFv2 WebACL。
   - 安全群組原則 — 為資源類型 EC2 SecurityGroup、EC2 執行個體和 EC2 啟用 Config NetworkInterface。
   - 網路 ACL 政策 — 為 Amazon EC2 子網路和 Amazon EC2 網路 ACL 的資源類型啟用 Config。

- Network Firewall 政策 — 為資源類型 NetworkFirewall FirewallPolicy、EC2 VPC NetworkFirewall RuleGroup、EC2 InternetGateway、EC2 和 EC2 子網路啟用 Config。RouteTable
- DNS 防火牆政策 — 為 EC2 VPC 資源類型啟用 Config。
- 第三方防火牆政策 — 為資源類型啟用 Config：Amazon EC2 VPC InternetGateway、Amazon EC2、Amazon EC2 RouteTable 子網路和 Amazon EC2 vpcendPoint。

> **Note**
>
> 如果您將 AWS Config 錄製程式設定為使用自訂 IAM 角色，則需要確保 IAM 政策具有適當的許可，以記錄 Firewall Manager 員政策的必要資源類型。如果沒有適當的權限，則可能無法記錄所需的資源，以防止 Firewall Manager 員正確保護您的資源。Firewall Manager 員無法檢視這些權限錯誤設定。如需搭配使用 IAM 的詳細資訊 AWS Config，請參閱 AWS Config.

步驟 4：對於第三方政策，請在 AWS Marketplace 中訂閱並配置第三方設置

完成下列必要條件，以開始使用 Firewall Manager 員協力廠商防火牆策略

將雲端原生防火牆 (CNF) 作為服務政策的先決條件

若要使用 Firewall Manager 員的 CNF

1. 在 Marketplace 上訂閱 Fortigate 雲端原生防火牆 (CNF) 即服務。 AWS
2. 首先，在 Fortigate CNF 產品門戶網站上註冊租戶。然後，在 Fortigate CNF 產品入口網站上，將您的 Firewall Manager 員系統管理員帳戶新增到租用戶下。如需詳細資訊，請參閱《重要 CNF》文件。

有關如何使用 Fortigate CNF 策略的更多內容，敬請參閱。強制雲端原生防火牆 (CNF) 即服務政策

帕洛阿爾托網路雲端次世代防火牆政策先決條件

若要使用帕洛阿爾托網路雲端 NGFW 進行 Firewall Manager 員

1. 在 Marketplace 上訂閱帕洛阿爾托網絡雲端次世代防火牆按用量付費服務。 AWS

2. AWS 使用帕洛奧圖網路雲端下一代防火牆部署指南中的 AWS Firewall Manager主題，完成部署帕洛阿爾托網路雲端 NGFW 中所列出的部署步驟。 AWS

如需使用帕洛阿爾托網路雲端 NGFW 原則的相關資訊，請參閱。帕洛奧圖網路雲端新世代防火牆政策

步驟 5：針對 Network Firewall 和 DNS 防火牆策略，啟用資源共用

若要管理 Firewall Manager 員 Network Firewall 和 DNS 防火牆策略，您必須啟用與 AWS Organizations 中的共用 AWS Resource Access Manager。這可讓 Firewall Manager 員在您建立這些策略類型時，在您的帳戶中部署防護。

若要啟用與 AWS Organizations 中的共用功能 AWS Resource Access Manager

- 請遵循「使用者指南」中「啟用 AWS Organizations共AWS Resource Access Manager用方式」中的指引。

如果您在使用資源共用時遇到問題，請參閱的指引Network Firewall 和 DNS 防火牆策略的資源共用。

步驟 6： AWS Firewall Manager 在預設停用的區域中使用

若要在預設停用的區域中使用 Firewall Manager 員，您必須為 AWS 組織的管理帳戶和 Firewall Manager 員預設管理員帳戶啟用「地區」。如需有關預設停用的區域以及如何啟用它們的資訊，請參閱AWS 一般參考 AWS 區域中的管理。

啟用已停用的區域

- 對於 Organizations 管理帳戶和 Firewall Manager 員預設管理員帳戶，請遵循AWS 一般參考中啟用區域中的指引。

執行這些步驟之後，您可以將 Firewall Manager 員設定為開始保護您的資源。如需更多詳細資訊，請參閱 開始使用 AWS Firewall ManagerAWS WAF 政策。

使用 AWS Firewall Manager 管理員

AWS Firewall Manager 您可以使用一個或多個管理員來管理組織的防火牆資源。如果您想要在組織中使用多個 Firewall Manager 管理員，可以將系統管理範圍條件套用至每個管理員，以定義他們可以管理的資源。這可讓您彈性在組織中擁有不同的管理員角色，並協助您維護最低權限存取的主體。例如，您可以讓一位系統管理員為您的組織管理一組組織單位 (OU)，同時委派其他管理員只管理特定的

Firewall Manager 原則類型。如需有關組 Organizations 和管理帳戶的詳細資訊，請參閱管理組織中的 AWS 帳戶。

如需每個組織可擁有的管理員數目上限，請參閱 AWS Firewall Manager 配額

開始使用 Firewall Manager 員管理員

開始使用 Firewall Manager 員管理員之前，您必須完成中列出的先決條件AWS Firewall Manager 前提。在先決條件中，您會將 AWS Organizations 組織上線至 Firewall Manager 員，並為 Firewall Manager 員建立預設的系統管理員帳戶。預設管理員帳戶可以管理協力廠商防火牆，並具有完整的系統管理範圍。

行政範圍

系統管理範圍定義 Firewall Manager 員管理員可以管理的資源。 AWS Organizations 管理帳戶將組織登入 Firewall Manager 後，管理帳戶可以建立具有不同系統管理範圍的其他 Firewall Manager 員管理員。 AWS Organizations 管理帳戶可以授與系統管理員完整或受限的系統管理範圍。「完整範圍」可讓管理員完整存取先前所有資源類型。受限範圍是指僅將管理權限授與先前資源的子集。我們建議您僅授與管理員執行其角色職責所需的權限。您可以將下列管理範圍條件的任意組合套用至系統管理員：

- 管理員可以套用原則的組織中的帳戶或 OU。
- 管理員可以在其中執行動作的區域。
- 系統管理員可以管理的 Firewall Manager 員原則類型。

管理員角色

Firewall Manager 員中有兩種類型的管理員角色：預設管理員和 Firewall Manager 員管理員。

- 預設管理員-組織的管理帳戶會建立 Firewall Manager 員預設的管理員帳戶，當他們將組織上線至 Firewall Manager 員，同時完成AWS Firewall Manager 前提。預設管理員可以管理協力廠商防火牆並具有完整的管理範圍，但如果您選擇擁有多個管理員，則預設管理員可以與其他管理員處於相同的對等層級。
- Firewall Manager 系統管理員-Firewall Manager 員可以在管理範圍設定中 AWS Organizations 管理管理帳戶為他們指定的資源。如需每個組織可擁有的管理員數目上限，請參閱AWS Firewall Manager 配額。建立 Firewall Manager 系統管理員帳戶後，服務會檢查該帳戶是否已經是組織內 Firewall Manager 的委派系統管理員。 AWS Organizations 如果沒有，則「Firewall Manager 員」會呼叫 Organizations，將帳戶設定為「Firewall Manager 員」的委派管理員。如需有關「Organizations 委派管理員」的資訊，請參閱AWS Organizations 使用指南中的AWS Organizations 術語和概念。

現有管理員

如果您是現有的「Firewall Manager 員」客戶，且已設定管理員，則此現有管理員將是「Firewall Manager 員」的預設管理員。不應該對現有流程造成任何影響。如果您想要新增更多管理員，可以遵循本章中的程序來執行此操作。

建立、更新和撤銷 Firewall Manager 員管理員帳戶

下列主題中的程序說明如何建立、更新和撤銷 Firewall Manager 員管理員帳戶。只有組織的管理帳戶可以建立和更新 Firewall Manager 員管理員帳戶。只有個別的 Firewall Manager 員管理員可以撤銷自己的管理員帳戶。

建立 Firewall Manager 員管理員帳戶

下列程序說明如何使用 Firewall Manager 員主控台建立 Firewall Manager 員管理員帳戶。

建立 Firewall Manager 員管理員帳戶

1. AWS Management Console 使用現有的 AWS Organizations 管理帳戶登入 Firewall Manager 員。
2. 開啟位於 https://console.aws.amazon.com/wafv2/fmsv2 的 Firewall Manager 主控台。
3. 在導覽窗格中，選擇設定。
4. 選擇建立管理員帳戶。
5. 在 [詳細資料] 窗格中，針對AWS 帳戶 AWS ID，輸入您要新增為 Firewall Manager 員的成員帳戶 ID。
6. 針對「管理」範圍，選擇下列其中一個選項：

   - 完整 — 這可讓系統管理員將策略套用至組織內的所有帳戶和組織單位 (OU)、在所有區域中採取動作，以及套用所有 Firewall Manager 原則類型 (第三方防火牆除外)。只有預設管理員可以建立和管理協力廠商防火牆。如果將此層級的權限授與系統管理員，請特別小心。本著最少權限的精神，我們建議您僅授與管理員執行其角色職責所需的權限。
   - 受限制 — 如果套用 [受限制] 範圍，則在 [設定] 系統管理範圍中設定帳戶可管理的帳戶和組織單位、區域和原則類型。

     對於 [帳戶] 和 [組織單位]，請依下列方式選擇選項：

     - 如果您要將策略套用至組織中的所有帳戶或組織單位，請選擇 [包含組 AWS 織下的所有帳戶]。

- 如果您只想將策略套用至特定 AWS Organizations 組織單位 (OU) 中的特定帳戶或帳戶，請選擇 [僅包含指定的帳戶和組織單位]，然後新增您要包含的帳戶和 OU。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。
- 如果您要將原則套用至特定帳戶或 AWS Organizations 組織單位 (OU) 以外的所有帳戶或組織單位，請選擇 [排除指定的帳戶和組織單位]，並包含所有其他帳戶，然後新增您要排除的帳戶和 OU。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

對於「區域」，請依下列方式選擇選項：

- 如果您要允許管理員在所有可用區域中執行動作，請選擇「包含所有區域」。
- 如果您希望管理員只在特定區域中執行動作，請選擇「僅包含指定的區域」，然後指定要包含的「區域」。

> **Note**
>
> 若要包含預設為停用的「區域」，您必須同時針對 AWS Organizations 組織管理帳戶和預設管理帳戶啟用「區域」。如需為帳戶啟用區域的相關資訊，請參閱在 Amazon Web Services 一般參考.

針對策略類型，選擇如下選項：。

- 如果您想要允許管理員管理所有策略類型，請選擇 [包括所有策略類型]。
- 如果您希望管理員只管理特定的原則類型，請選擇 [僅包含指定的原則類型]，然後指定您要包含的原則類型。

7. 選擇 [建立管理員帳戶] 以建立管理員帳戶。建立時，Firewall Manager 會呼叫 AWS Organizations 以查看管理員是否已經是組織的委派系統管理員。否則，「Firewall Manager 員」會將該帳戶指定為委派的管理員。如需有關「Organizations」中委派管理員的資訊，請參閱《AWS Organizations 使用指南》中的AWS Organizations 術語和概

如果您套用限制的系統管理範圍，Firewall Manager 員會根據您的設定自動評估任何新資源 例如，如果您只包含特定帳戶，則 Firewall Manager 員不會將策略套用至任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子系 OU 時，Firewall Manager 會自動將帳戶納入系統管理範圍內。

更新 Firewall Manager 員管理員帳戶

下列程序說明如何使用 Firewall Manager 員主控台更新 Firewall Manager 員管理員帳戶。

> **Note**
>
> 若要將管理員的範圍更新為包含預設為停用的「區域」，您必須同時針對 AWS Organizations 組織管理帳戶與預設管理帳戶啟用「區域」。如需為帳戶啟用區域的相關資訊，請參閱在 Amazon Web Services 一般參考.

更新管理員帳戶（控制台）

1. AWS Management Console 使用現有的 AWS Organizations 管理帳戶登入 Firewall Manager 員。
2. 開啟位於 https://console.aws.amazon.com/wafv2/fmsv2 的 Firewall Manager 主控台。
3. 在導覽窗格中，選擇設定。
4. 在「Firewall Manager 員管理員」表格中，選擇您要更新的帳戶。
5. 選取 [編輯] 以變更管理員帳戶的詳細資料。您無法變更帳號 ID。
6. 選擇儲存，以儲存變更。

撤銷管理員帳戶

下列程序說明如何撤銷 Firewall Manager 員管理員帳戶。如果您是預設管理員，您組織中的所有 Firewall Manager 管理員帳戶必須先撤銷自己的帳戶，才能撤銷帳戶。要撤銷管理員帳戶，請按照以下步驟操作

撤銷管理員帳戶（控制台）

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。
2. 在導覽窗格中，選擇設定。
3. 在「管理員帳戶」窗格中，選取「撤銷管理員帳戶」以撤銷您的帳戶。

> **Important**
>
> 當您從管理員帳戶撤銷管理員權限時，該帳戶建立的所有 Firewall Manager 策略都會遭到刪除。

變更預設管理員帳戶

您只能將組織中的一個帳戶指定為預設的 Firewall Manager 員帳戶。預設的管理員帳戶遵循先進後出的原則。若要指定不同的預設管理員帳戶，每個個別管理員帳戶都必須先撤銷自己的帳戶。然後，現有的預設管理員可以撤銷自己的帳戶，這也會從 Firewall Manager 員離開組織。當系統管理員撤銷其帳戶時，該帳戶所建立的所有 Firewall Manager 員策略都會遭到刪除。若要指定新的預設系統管理員帳戶，您必須使用 AWS Organizations 管理帳戶登入 Firewall Manager，以指定新的系統管理員帳戶。若要變更組織的預設管理員帳戶，請執行下列步驟。

變更預設管理員帳戶

1. AWS Management Console 使用現有的 AWS Organizations 管理帳戶登入 Firewall Manager 員。
2. 開啟位於 https://console.aws.amazon.com/wafv2/fmsv2 的 Firewall Manager 主控台。
3. 在導覽窗格中，選擇設定。
4. 輸入您選擇作為 Firewall Manager 員使用的帳戶 ID。

> **Note**
>
> 這個帳戶被授予跨組織內所有帳戶建立和管理 Firewall Manager 員策略的權限。

5. 選擇建立管理員帳戶。
6. 輸 AWS 入您選擇作為 Firewall Manager 員使用的帳戶 ID。

> **Note**
>
> 此帳戶具有完整的管理範圍。完整的系統管理範圍表示此帳戶可以將原則套用至組織內的所有帳戶和組織單位 (OU)、在所有區域採取動作，以及管理所有 Firewall Manager 員原則類型。

7. 選擇 [建立管理員帳戶] 以建立預設的管理員帳戶。

取消對管理員帳戶的變更資格

對管理員帳戶進行的某些變更可能會使其無法保留系統管理員帳戶。

本節說明可能會取消系統管理員帳戶資格的變更，以 AWS 及 Firewall Manager 員如何處理這些變更。

從中的組織移除的帳號 AWS Organizations

如果管理 AWS Firewall Manager 員帳號已從中的組織中移除 AWS Organizations，則無法再管理組織的策略。Firewall Manager 員會執行下列其中一個處理行動

- 沒有策略的帳號 — 如果 Firewall Manager 員管理員帳戶沒有 Firewall Manager 員策略，則 Firewall Manager 員會撤銷管理員帳戶。
- 具有 Firewall Manager 員策略的帳號 — 如果 Firewall Manager 員管理員帳戶具有 Firewall Manager 員策略，Firewall Manager 會在 AWS 銷售帳戶代表的協助下傳送電子郵件通知您情況，並提供您可以採取的選項。

帳戶已關閉

如果您關閉系統管理員所使用的帳戶， AWS 而 Firewall Manager AWS Firewall Manager 員會按照下列方式處理關閉：

- AWS 從 Firewall Manager 員撤銷帳戶的管理員存取權，而 Firewall Manager 員會停用由管理員帳戶管理的所有策略。這些原則所提供的保護會在整個組織中停止。
- AWS 自管理員帳戶關閉生效日起，保留帳戶的 Firewall Manager 員策略資料 90 天。在 90 天期間，您可以重新打開已關閉的帳戶。
  - 如果您在 90 天期間重新開啟已關閉的帳戶，請將該帳戶 AWS 重新指派為 Firewall Manager 員管理員，並復原該帳戶的 Firewall Manager 員策略資料。
  - 否則，在 90 天期限結束時，會 AWS 永久刪除該帳戶的所有 Firewall Manager 員策略資料。

開始使用 AWS Firewall Manager 政策

您可以使用 AWS Firewall Manager 來啟用許多不同類型的安全性原則。每個開始設定的步驟稍微不同。

主題

- 開始使用 AWS Firewall ManagerAWS WAF 政策
- 開始使用 AWS Firewall ManagerAWS Shield Advanced 政策
- 開始使用 AWS Firewall Manager Amazon VPC 安全群組政策
- 開始使用 AWS Firewall Manager Amazon VPC 網路 ACL 政策
- 開始使用 AWS Firewall ManagerAWS Network Firewall 政策

- 開始使用 AWS Firewall Manager DNS 防火牆政策
- 開始使用 AWS Firewall Manager帕洛阿爾托網路雲端次世代防火牆政策
- 開始使用 AWS Firewall Manager富泰蓋特 CNF 政策

開始使用 AWS Firewall ManagerAWS WAF 政策

若要用 AWS Firewall Manager 來在整個組織中啟用 AWS WAF 規則，請依序執行下列步驟。

主題

- 步驟 1：完成先決條件
- 步驟 2：建立並套用 AWS WAF 原則
- 步驟 3：清除

步驟 1：完成先決條件

為 AWS Firewall Manager準備您的帳戶有幾個必要的步驟。AWS Firewall Manager 前提 說明這些步驟。先完成所有的先決條件，再進行步驟 2：建立並套用 AWS WAF 原則。

步驟 2：建立並套用 AWS WAF 原則

Firewall Manager 員 AWS WAF 策略包含您要套用至資源的規則群組。Firewall Manager 員會在您套用策略的每個帳戶中建立 Firewall Manager 員 Web ACL。除了您已定義的規則群組之外，個別帳戶管理員還可以將規則和規則群組新增至產生的 Web ACL。如需有關 Firewall Manager 員 AWS WAF 策略的資訊，請參閱 AWS WAF 政策

建立 Firewall Manager 員 AWS WAF 策略（主控台）

AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

1. 在導覽窗格中，選擇 Security policies (安全群組政策)。
2. 選擇建立政策。
3. 針對政策類型，選擇 AWS WAF。
4. 在「區域」中，選擇一個 AWS 區域。要保護 Amazon CloudFront 分佈，請選擇全球。

若要保護多個區域中的資源 (CloudFront 散佈除外)，您必須為每個區域建立個別的 Firewall Manager 員政策。

5. 選擇下一步。
6. 在策略名稱中，輸入描述性名稱。Firewall Manager 員會在其管理的 Web ACL 名稱中包含策略名稱。Web ACL 名稱`FMManagedWebACLV2-`後面接著您在此處輸入的策略名稱`-`，以及 Web ACL 建立時間戳記 (以 UTC 毫秒為單位)。例如 `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`。

   > **Important**
   >
   > 網頁 ACL 名稱在建立之後就無法變更。如果您更新策略的名稱，Firewall Manager 員將不會更新關聯的 Web ACL 名稱。若要讓 Firewall Manager 員使用不同名稱建立 Web ACL，您必須建立新策略。

7. 在 Policy rules (政策規則) 下，針對 First rule groups (第一個規則群組)，選擇 Add rule groups (新增規則群組)。展開受AWS 管規則群組。對於 Core rule set (核心規則集)，請切換 Add to web ACL (新增至 Web ACL)。對於AWS 已知錯誤的輸入，切換「新增至 Web ACL」。選擇 Add rules (新增規則)。

   對於 Last rule groups (最後一個規則群組)，選擇 Add rule groups (新增規則群組)。展開受AWS 管規則群組，並針對 Amazon IP 信譽清單切換「新增至網頁 ACL」。選擇 Add rules (新增規則)。

   在第一個規則群組下，選取核心規則集，然後選擇下移。 AWS WAF 在評估核心規則集之前，針對AWS 已知的錯誤輸入規則群組評估 Web 要求。

   您也可以視需要使用 AWS WAF 主控台建立自己的 AWS WAF 規則群組。您建立的任何規則群組都會顯示在 [描述原則：新增規則群組] 頁面中的規則群組下方。

   您透過 Firewall Manager 管理的第一個和最後一個 AWS WAF 規則群組的名稱分別以`PREFMManaged-`或開頭`POSTFMManaged-`，後跟 Firewall Manager 員原則名稱，以及規則群組建立時間戳記 (以 UTC 毫秒為單位)。例如 `PREFMManaged-MyWAFPolicyName-1621880555123`。
8. 保留 Web ACL 的預設動作為 Allow (允許)。
9. 將 Policy action (政策動作) 保留為預設狀態，即不自動修補不合規的資源。您可於稍後變更此選項。
10. 選擇下一步。

11. 針對 Policy scope (政策範圍)，您可以提供帳戶的設定、資源類型和用以識別您要套用政策之資源的標記。對於本教學課程，請保留AWS 帳戶和資源設定，然後選擇一或多個資源類型。
12. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

    如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

    資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。
13. 選擇下一步。
14. 對於策略標記，請新增任何您要新增至 Firewall Manager 員策略資源的識別標籤。如需標籤的詳細資訊，請參閱使用標籤編輯器。
15. 選擇下一步。
16. 檢閱新的原則設定，並返回需要進行任何調整的頁面。

    請務必確定 Policy action (政策動作) 已設為 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)。這可讓您在啟用政策之前檢閱原則所做的變更。
17. 當您滿意時，選擇 建立政策。

    在 [原AWS Firewall Manager 則] 窗格中，應該會列出您的原則。它可能會在帳戶標題下指示「待處理」，並指示「自動補救」設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱檢視 AWS Firewall Manager 原則的符合性資訊。

步驟 3：清除

若要避免額外費用，請刪除任何不必要的政策和資源。

刪除政策 (主控台)

1. 在AWS Firewall Manager 策略頁面上，選擇策略名稱旁邊的圓鈕，然後選擇刪除。
2. 在 Delete (刪除) 確認方塊中，選取 Delete all policy resources (刪除所有政策資源)，然後再次選擇 Delete (刪除)。

   AWS WAF 會移除策略及其在您帳戶中建立的任何相關資源 (例如 Web ACL)。這些變更可能需要幾分鐘的時間才能傳播到所有帳戶。

開始使用 AWS Firewall ManagerAWS Shield Advanced 政策

您可以使用 AWS Firewall Manager 來啟用整個組織的 AWS Shield Advanced 保護。

> **Important**
>
> Firewall Manager 員不支援 Amazon 路由 53 或 AWS Global Accelerator. 如果您需要使用 Shield Advanced 來保護這些資源，就無法使用 Firewall Manager 員政策。或者，請遵循為 AWS 資源添加 AWS Shield Advanced 保護中的說明進行。

若要使用 Firewall Manager 員啟用 Shield 進階防護，請依序執行下列步驟。

主題

步驟 1：完成先決條件

為 AWS Firewall Manager準備您的帳戶有幾個必要的步驟。AWS Firewall Manager 前提 說明這些步驟。先完成所有的先決條件，再進行 步驟 2：建立並套用 Shield 牌進階政策。

步驟 2：建立並套用 Shield 牌進階政策

完成先決條件之後，您可以建立 AWS Firewall Manager Shield 進階策略。Firewall Manager 員防護進階策略包含您要使用 Shield 進階保護的帳號和資源。

> **Important**
>
> Firewall Manager 員不支援 Amazon 路由 53 或 AWS Global Accelerator. 如果您需要使用 Shield Advanced 來保護這些資源，就無法使用 Firewall Manager 員政策。或者，請遵循為 AWS 資源添加 AWS Shield Advanced 保護中的說明進行。

建立 Firewall Manager 員防 Shield 進階策略（主控台）

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對策略類型，選擇 Shield 進階。

   若要建立 Shield 牌進階策略，您的 Firewall Manager 員管理員帳戶必須訂閱 Shield 牌進階。如果您未訂閱，系統會提示您訂閱。如需訂閱費用的相關資訊，請參閱AWS Shield Advanced 定價。

   > **Note**
   >
   > 您不需要手動訂閱每個會員帳戶到 Shield 牌進階版。Firewall Manager 員會在建立策略時為您執行此動作。每個帳號都必須維持「Firewall Manager 員」和「防 Shield 進階」的訂閱，才能繼續保護帳號中的資源。

5. 在「區域」中，選擇一個 AWS 區域。若要保護 Amazon CloudFront 資源，請選擇「全球」。

   若要保護多個區域 (資源除外) 中的 CloudFront 資源，您必須為每個區域建立個別的 Firewall Manager 員政策。
6. 選擇下一步。
7. 在「名稱」中，輸入描述性名稱。
8. (僅限全球區域) 對於全球區域政策，您可以選擇是否要管理 Shield 進階自動應用程式層 DDoS 緩解。對於此自學課程，請將此選項保留為「忽略」的預設設定。
9. 針對「原則」動作，請選擇不會自動修復的選項。
10. 選擇下一步。
11. AWS 帳戶 此政策適用於允許您指定要包含或排除的帳戶來縮小策略範圍。在本教學課程中，請選擇 Include all accounts under my organization. (納入我組織下的所有帳戶。)。
12. 選擇您要保護的資源類型。

Firewall Manager 員不支援 Amazon 路由 53 或 AWS Global Accelerator. 如果您需要使用 Shield Advanced 來保護這些資源，就無法使用 Firewall Manager 員政策。相反，請遵循的「Shield 牌進階」指引為 AWS 資源添加 AWS Shield Advanced 保護。

13. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

    如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

    資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。

14. 選擇下一步。
15. 對於策略標記，請新增任何您要新增至 Firewall Manager 員策略資源的識別標籤。如需標籤的詳細資訊，請參閱使用標籤編輯器。
16. 選擇下一步。
17. 檢閱新的原則設定，並返回需要進行任何調整的頁面。

    請務必確定 Policy action (政策動作) 已設為 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)。這可讓您在啟用政策之前檢閱原則所做的變更。

18. 當您滿意時，選擇 建立政策。

    在 [原AWS Firewall Manager 則] 窗格中，應該會列出您的原則。它可能會在帳戶標題下指示「待處理」，並指示「自動補救」設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱檢視 AWS Firewall Manager 原則的符合性資訊。

繼續進行步驟 3：（可選）授權 Shield 牌響應小組（SRT）。

步驟 3：（可選）授權 Shield 牌響應小組（SRT）

其中一個好處 AWS Shield Advanced 是 Shield 牌響應小組（SRT）的支持。當您遇到潛在的 DDoS 攻擊時，可以聯繫中AWS Support 心。如有必要，Support 中心會將您的問題呈報至 SRT。SRT 可協助您分析可疑活動，並協助您緩解問題。這種緩解措施通常涉及在您的帳戶中建立或更新 AWS WAF 規則和 Web ACL。SRT 可以檢查您的 AWS WAF 配置，並為您創建或更新 AWS WAF 規則和 Web ACL，但團隊需要您的授權才能這樣做。我們建議您在設定過程 AWS Shield Advanced中主動向 SRT 提供必要的授權。提前提供授權有助於防止在發生實際攻擊時所造成的問題緩解延遲。

您在帳戶層級授權並連絡 SRT。也就是說，帳戶擁有者 (而非 Firewall Manager 員管理員) 必須執行下列步驟來授權 SRT 以減輕潛在攻擊。Firewall Manager 員管理員只能針對他們擁有的帳戶授權 SRT。同樣地，只有帳戶擁有者可以聯絡 SRT 以取得支援。

> **Note**
>
> 若要使用 SRT 的服務，您必須訂閱商務 Support 方案或企業 Support 方案。

若要授權 SRT 以代表您緩解潛在攻擊，請遵循中Shield 牌回應小組 (SRT) 支援的指示。您可以使用相同的步驟隨時變更 SRT 存取和權限。

繼續進行步驟 4：設定 Amazon SNS 通知和 Amazon CloudWatch 警示。

步驟 4：設定 Amazon SNS 通知和 Amazon CloudWatch 警示

您可以繼續執行此步驟，而不需設定 Amazon SNS 通知或 CloudWatch 警示。但是，配置這些警報和通知會顯著提高您對可能的 DDoS 事件的可見性。

您可以使用 Amazon SNS 監控受保護的資源，瞭解潛在的 DDoS 活動。若要接收可能攻擊的通知，請為每個區域建立 Amazon SNS 主題。

在 Firewall Manager 員 (主控台) 中建立 Amazon SNS 主題

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在功能窗格的 AWS FMS 下，選擇 [設定]。
3. 請選擇 Create new topic (建立新主題)。
4. 輸入主題名稱。
5. 輸入將傳送 Amazon SNS 訊息的電子郵件地址，然後選擇 [新增電子郵件地址]。
6. 選擇更新 SNS 組態。

配置 Amazon CloudWatch 警報

Shield 進階記錄偵測、緩和措施，以及您可以監控的主 CloudWatch 要貢獻者指標。如需詳細資訊，請參閱AWS Shield Advanced 度量。 CloudWatch 會產生額外費用。有關 CloudWatch 定價，請參閱Amazon CloudWatch 定價。

若要建立 CloudWatch 警示，請依照使用 Amazon CloudWatch 鬧鐘中的指示操作。預設情況下，Shield 牌進階設定 CloudWatch 為在潛在 DDoS 事件的一個指示器之後提醒您。如有需要，您可以使用CloudWatch 主控台變更此設定，以便僅在偵測到多個指示器之後提醒您。

> **Note**
>
> 除了警報之外，您還可以使用 CloudWatch 儀表板監控潛在的 DDoS 活動。儀表板會收集 Shield Advanced 的原始資料，並將其處理為可讀且接近即時的指標。您可以使用 Amazon 中的統計信息 CloudWatch 來了解 Web 應用程序或服務的執行情況。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南 CloudWatch中的內容。
> 如需有關建立 CloudWatch 管控面板的指示，請參閱使用 Amazon 監控 CloudWatch。如需可新增至儀表板之特定 Shield Advanced 量度的相關資訊，請參閱AWS Shield Advanced 度量。

當您完成 Shield 進階設定後，請熟悉您在檢視事件的選項。DDoS 事件的可見性

開始使用 AWS Firewall Manager Amazon VPC 安全群組政策

若要在整個組織中啟用 AWS Firewall Manager Amazon VPC 安全群組，請依序執行下列步驟。

主題

- 步驟 1：完成先決條件
- 步驟 2：建立要在您的政策中使用的安全群組
- 步驟 3：建立並套用通用安全性群組原則

步驟 1：完成先決條件

為 AWS Firewall Manager準備您的帳戶有幾個必要的步驟。AWS Firewall Manager 前提 說明這些步驟。先完成所有的先決條件，再進行 步驟 2：建立要在您的政策中使用的安全群組。

步驟 2：建立要在您的政策中使用的安全群組

在此步驟中，您會建立可以使用 Firewall Manager 員在整個組織中套用的安全性群組。

> **Note**
>
> 在本教學課程，您不會將自己的安全群組政策套用至組織中的資源。您只會建立政策，然後查看如果將政策的安全群組套用至資源，會發生什麼事？ 您可以停用政策上的自動修補，來執行此作業。

如果您已定義一般的安全群組，請略過此步驟並移至 步驟 3：建立並套用通用安全性群組原則。

建立要在 Firewall Manager 員一般安全性群組原則中使用的安全性群組

- 遵循 Amazon VPC 使用者指南中 VPC 安全群組下的指引，建立可套用至組織中所有帳戶和資源的安全群組。

  如需安全群組規則選項的資訊，請參閱安全群組規則參考。

您現在可以前往步驟 3：建立並套用通用安全性群組原則。

步驟 3：建立並套用通用安全性群組原則

完成必要條件之後，您可以建立一 AWS Firewall Manager 般安全性群組原則。通用安全性群組原則可為整個組織提供集中控制的安全性群 AWS 組。它也會定義安全性群組套用的 AWS 帳戶 和資源。除了一般安全性群組原則之外，Firewall Manager 還支援內容稽核安全性群組原則、管理組織中使用的安全性群組規則，以及使用狀況稽核安全性群組原則，以管理未使用的和冗餘的安全性群組。如需詳細資訊，請參閱 安全性群組原則。

在本教學課程，您會建立常見安全群組政策，並將其動作設為不要自動修補。這可讓您在不變更 AWS 組織的情況下查看原則會產生什麼影響。

建立 Firewall Manager 員一般安全性群組原則 (主控台)

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。

3. 如果您不符合先決條件，主控台會顯示修復問題的相關說明。遵循說明進行，然後回到此步驟，以建立常見安全群組政策。
4. 選擇建立政策。
5. 對於 Policy type (政策類型)，選擇 Security group (安全群組)。
6. 對於 Security group policy type (安全群組類型)，選擇 Common security groups (常見安全群組)。
7. 在「區域」中，選擇一個 AWS 區域。
8. 選擇下一步。
9. 在策略名稱中，輸入描述性名稱。
10. Policy rules (政策規則)可讓您選擇如何套用和維護此政策中的安全群組。在此自學課程中，不勾選選項。
11. 選擇 Add primary security group (新增主要安全群組)、選取您在本教學課程中建立的安全群組，然後選擇 Add security group (新增安全群組)。
12. 對於 Policy action (政策動作)，選擇 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)。
13. 選擇下一步。
14. AWS 帳戶 受此策略影響可讓您指定要包含或排除的帳戶，以縮小策略的範圍。在本教學課程中，請選擇 Include all accounts under my organization. (納入我組織下的所有帳戶。)。
15. 針對「資源」類型，請根據您為 AWS 組織定義的資源，選擇一或多個型態。
16. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

    如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

    資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。
17. 選擇下一步。
18. 對於策略標記，請新增任何您要新增至 Firewall Manager 員策略資源的識別標籤。如需標籤的詳細資訊，請參閱使用標籤編輯器。
19. 選擇下一步。
20. 檢閱新的原則設定，並返回需要進行任何調整的頁面。

    請務必確定 Policy action (政策動作) 已設為 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)。這可讓您在啟用政策之前檢閱原則所做的變更。

21. 當您滿意時，選擇 建立政策。

    在 [原AWS Firewall Manager 則] 窗格中，應該會列出您的原則。它可能會在帳戶標題下指示「待處理」，並指示「自動補救」設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱檢視 AWS Firewall Manager 原則的符合性資訊。

22. 完成探索後，如果不想要保留本教學課程建立的政策，請選擇政策名稱、選擇 Delete (刪除)、選擇 Clean up resources created by this policy. (清理此政策建立的資源。)，最後選擇 Delete (刪除)。

如需 Firewall Manager 員安全性群組原則的詳細資訊，請參閱安全性群組原則。

開始使用 AWS Firewall Manager Amazon VPC 網路 ACL 政策

若要用 AWS Firewall Manager 來啟用組織中的網路 ACL，請依序執行本節中的步驟。

如需有關網路 ACL 的資訊，請參閱 Amazon V PC 使用者指南中的使用網路 ACL 控制到子網路的流量。

主題

- 步驟 1：完成先決條件
- 步驟 2：建立網路 ACL 原則

步驟 1：完成先決條件

為 AWS Firewall Manager準備您的帳戶有幾個必要的步驟。AWS Firewall Manager 前提 說明這些步驟。先完成所有的先決條件，再進行 步驟 2：建立網路 ACL 原則。

步驟 2：建立網路 ACL 原則

完成必要條件之後，您可以建立 Firewall Manager 員網路 ACL 原則。網路 ACL 原則可為您的整個 AWS 組織提供集中控制的網路 ACL 定義。它也會定義網路 ACL 套用至的 AWS 帳戶 和子網路。

如需有關 Firewall Manager 員網路 ACL 策略的資訊，請參閱網路 ACL 政策。

如需有關 Firewall Manager 員網路 ACL 策略的一般資訊，請參閱網路 ACL 政策。

> **Note**
>
> 在本教學課程中，您不會將網路 ACL 原則套用至組織中的子網路。您只需建立原則，然後查看將原則的網路 ACL 套用至子網路時會發生什麼情況。您可以停用政策上的自動修補，來執行此作業。

建立 Firewall Manager 員網路 ACL 策略（主控台）

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 如果您不符合先決條件，主控台會顯示修復問題的相關說明。遵循指示，然後返回此步驟，以建立網路 ACL 原則。
4. 選擇建立政策。
5. 在「區域」中，選擇一個 AWS 區域。
6. 針對「原則類型」，選擇「網路 ACL」。
7. 選擇下一步。
8. 在策略名稱中，輸入描述性名稱。
9. 針對網路 ACL 原則規則，定義輸入和輸出流量的第一個和最後一個規則。

   您可以在 Firewall Manager 員中定義網路 ACL 規則，與透過 Amazon VPC 定義這些規則的方式類似。唯一的不同之處在於，您不需要自行指派規則編號，而是指派執行每組規則的順序，然後 Firewall Manager 會在您儲存原則時為您指派編號。您最多可以定義 5 個輸入規則，在第一個和最後一個之間以任何方式劃分，最多可以定義 5 個輸出規則。

   如需指定網路 ACL 規則的指引，請參閱 Amazon VPC 使用者指南中的新增和刪除網路 ACL 規則。

您在 Firewall Manager 員策略中定義的規則會指定網路 ACL 必須符合網路 ACL 策略的最低規則組態。例如，網路 ACL 的輸入規則無法與原則相容，除非它們以原則的輸入第一個規則開頭 (與原則中指定的順序相同)。如需詳細資訊，請參閱 網路 ACL 政策。

10. 對於 Policy action (政策動作)，選擇 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)。
11. 選擇下一步。
12. AWS 帳戶 受此策略影響可讓您指定要包含或排除的帳戶，以縮小策略的範圍。在本教學課程中，請選擇 Include all accounts under my organization. (納入我組織下的所有帳戶。)。

    網路 ACL 原則的資源類型一律為子網路。
13. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

    如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

    資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。
14. 選擇下一步。
15. 對於策略標記，請新增任何您要新增至 Firewall Manager 員策略資源的識別標籤。如需標籤的詳細資訊，請參閱使用標籤編輯器。
16. 選擇下一步。
17. 檢閱新的原則設定，並返回需要進行任何調整的頁面。

    請務必確定 Policy action (政策動作) 已設為 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)。這可讓您在啟用政策之前檢閱原則所做的變更。
18. 當您滿意時，選擇 建立政策。

    在 [原AWS Firewall Manager 則] 窗格中，應該會列出您的原則。它可能會在帳戶標題下指示「待處理」，並指示「自動補救」設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱檢視 AWS Firewall Manager 原則的符合性資訊。
19. 完成探索後，如果您不想保留為此教學課程建立的原則，請選擇原則名稱，選擇 [刪除]，然後選擇 [清除此原則建立的資源]。 ，最後選擇刪除。

如需有關 Firewall Manager 員網路 ACL 策略的詳細資訊，請參閱網路 ACL 政策。

開始使用 AWS Firewall ManagerAWS Network Firewall 政策

若要用 AWS Firewall Manager 來啟用組織內的 AWS Network Firewall 防火牆，請依序執行下列步驟。如需 Firewall Manager 員 Network Firewall 策略的資訊，請參閱AWS Network Firewall 政策。

主題

步驟 1：完成一般先決條件

為 AWS Firewall Manager準備您的帳戶有幾個必要的步驟。AWS Firewall Manager 前提 說明這些步驟。繼續進行下一個步驟之前，請先完成所有先決條件。

步驟 2：建立要在策略中使用的 Network Firewall 規則群組

若要遵循本教學課程，您應該熟悉 AWS Network Firewall 並瞭解如何設定其規則群組和防火牆策略。

您必須在 Network Firewall 中至少有一個規則群組，這些群組將用於您的 AWS Firewall Manager 原則。如果您尚未在 Network Firewall 中建立規則群組，請立即執行。如需有關使用 Network Firewall 的資訊，請參閱開AWS Network Firewall 發人員指南。

步驟 3：建立並套用 Network Firewall 政策

完成必要條件之後，您可以建立 AWS Firewall Manager Network Firewall 策略。Network Firewall 原則可為整個 AWS 組織提供集中控制的 AWS Network Firewall 防火牆。它也會定義防火牆套用的 AWS 帳戶 和資源。

如需 Firewall Manager 員如何管理 Network Firewall 策略的相關資訊，請參閱AWS Network Firewall 政策。

建立 Firewall Manager 員 Network Firewall 策略（主控台）

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

> **Note**
>
> 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 如果您尚未符合先決條件，主控台會顯示如何修正任何問題的指示。遵循指示，然後返回此步驟，建立 Network Firewall 策略。
4. 選擇建立安全性原則。
5. 針對政策類型，選擇 AWS Network Firewall。
6. 在「區域」中，選擇一個 AWS 區域。
7. 選擇下一步。
8. 在策略名稱中，輸入描述性名稱。
9. 策略配置可讓您定義防火牆策略。這與您在 AWS Network Firewall 控制台中使用的過程相同。您可以新增要在原則中使用的規則群組，並提供預設的無狀態動作。在本教學課程中，請像設定 Network Firewall 中的防火牆策略一樣設定此原則。

> **Note**
>
> AWS Firewall Manager Network Firewall 策略會自動進行自動修復，因此您不會在此處看到選擇不 auto 動修復的選項。

10. 選擇下一步。
11. 對於防火牆端點，請選擇「多個防火牆端點 此選項可為您的防火牆提供高可用性。當您建立原則時，Firewall Manager 會在每個可用區域中建立防火牆子網路，您可以在其中保護公用子網路。
12. 對於AWS Network Firewall 路由組態，請選擇監控讓 Firewall Manager 監控您的 VPC 是否存在路由組態違規，並提供修正建議警示您，以協助您使路由符合規範。或者，如果您不想讓「Firewall Manager 員」監控路由設定並接收這些警示，請選擇「關閉」。

> **Note**
>
> 監控可為您提供由於錯誤的路由設定而導致不合規資源的詳細資訊，並從 Firewall Manager 員 `GetViolationDetails` API 建議修復動作。例如，如果流量未經由您的策略所建立的防火牆端點路由傳送，則 Network Firewall 會警示您。

> **Warning**
>
> 如果您選擇 [監控]，您將來無法針對相同原則 future 其變更為 [關閉]。您必須建立新策略。

13. 對於流量類型，請選取新增至防火牆策略以透過網際網路閘道路由傳送流量。
14. AWS 帳戶 受此策略影響可讓您指定要包含或排除的帳戶，以縮小策略的範圍。在本教學課程中，請選擇 Include all accounts under my organization. (納入我組織下的所有帳戶。)。

    Network Firewall 策略的資源類型一律為 VPC。
15. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

    如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

    資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。
16. 選擇下一步。
17. 對於策略標記，請新增任何您要新增至 Firewall Manager 員策略資源的識別標籤。如需標籤的詳細資訊，請參閱使用標籤編輯器。
18. 選擇下一步。
19. 檢閱新的原則設定，並返回需要進行任何調整的頁面。

    請務必確定 Policy action (政策動作) 已設為 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)。這可讓您檢閱原則在啟用前所做的變更。
20. 當您滿意時，選擇 建立政策。

    在 [原AWS Firewall Manager 則] 窗格中，應該會列出您的原則。它可能會在帳戶標題下指示「待處理」，並指示「自動補救」設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱檢視 AWS Firewall Manager 原則的符合性資訊。
21. 完成探索後，如果您不想保留為此教學課程建立的原則，請選擇原則名稱，選擇 [刪除]，然後選擇 [清除此原則建立的資源]。 ，最後選擇刪除。

如需 Firewall Manager 員 Network Firewall 策略的詳細資訊，請參閱AWS Network Firewall 政策。

開始使用 AWS Firewall Manager DNS 防火牆政策

若 AWS Firewall Manager 要使用在您的組織中啟用 Amazon Route 53 解析器 DNS 防火牆，請依序執行下列步驟。如需有關 Firewall Manager 員 DNS 防火牆策略的資訊，請參閱 Amazon 路線 53 解析器 DNS 防火牆政策

主題

- 步驟 1：完成一般先決條件
- 步驟 2：建立要在策略中使用的 DNS 防火牆規則群組
- 步驟 3：建立並套用 DNS 防火牆政策

步驟 1：完成一般先決條件

為 AWS Firewall Manager準備您的帳戶有幾個必要的步驟。AWS Firewall Manager 前提 說明這些步驟。繼續進行下一個步驟之前，請先完成所有先決條件。

步驟 2：建立要在策略中使用的 DNS 防火牆規則群組

若要遵循本教學課程，您應該熟悉 Amazon Route 53 解析器 DNS 防火牆，並且知道如何設定其規則群組。

您必須在 DNS 防火牆中至少有一個將用於您的 AWS Firewall Manager 策略的規則群組。如果您尚未在 DNS 防火牆中建立規則群組，請立即執行。如需有關使用 DNS 防火牆的資訊，請參閱 Amazon 路線 53 開發人員指南中的 Amazon 路由 53 解析器 DNS 防火牆。

步驟 3：建立並套用 DNS 防火牆政策

完成必要條件之後，您可以建立 AWS Firewall Manager DNS 防火牆政策。DNS 防火牆原則為您的整個 AWS 組織提供一組集中控制的 DNS 防火牆規則群組關聯。它也會定義防火牆套用的 AWS 帳戶 和資源。

如需有關 Firewall Manager 員如何管理 DNS 防火牆規則群組關聯的詳細資訊，請參閱Amazon 路線 53 解析器 DNS 防火牆政策。

建立 Firewall Manager 員 DNS 防火牆政策（主控台）

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。
2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 如果您尚未符合先決條件，主控台會顯示如何修正任何問題的指示。遵循指示，然後返回此步驟，建立 DNS 防火牆政策。
4. 選擇建立安全性原則。
5. 對於政策類型，請選擇 Amazon 路由 53 解析器 DNS 防火牆。
6. 在「區域」中，選擇一個 AWS 區域。
7. 選擇下一步。
8. 在策略名稱中，輸入描述性名稱。
9. 原則組態可讓您定義要從 Firewall Manager 員管理的 DNS 防火牆規則群組關聯。您可以新增要在原則中使用的規則群組。您可以定義要先評估 VPC 的關聯，然後定義一個最後評估的關聯。在本教學課程中，請根據您的需求新增一或兩個規則群組關聯。
10. 選擇下一步。
11. AWS 帳戶 受此策略影響可讓您指定要包含或排除的帳戶，以縮小策略的範圍。在本教學課程中，請選擇 Include all accounts under my organization. (納入我組織下的所有帳戶。)。

    DNS 防火牆策略的資源類型一律為 VPC。
12. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

    如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

    資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。
13. 選擇下一步。
14. 對於策略標記，請新增任何您要新增至 Firewall Manager 員策略資源的識別標籤。如需標籤的詳細資訊，請參閱使用標籤編輯器。
15. 選擇下一步。
16. 檢閱新的原則設定，並返回需要進行任何調整的頁面。

請務必確定 Policy action (政策動作) 已設為 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)。這可讓您檢閱原則在啟用前所做的變更。

17. 當您滿意時，選擇 建立政策。

    在 [原AWS Firewall Manager 則] 窗格中，應該會列出您的原則。它可能會在帳戶標題下指示「待處理」，並指示「自動補救」設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱檢視 AWS Firewall Manager 原則的符合性資訊。

18. 完成探索後，如果您不想保留為此教學課程建立的原則，請選擇原則名稱，選擇 [刪除]，然後選擇 [清除此原則建立的資源]。 ，最後選擇刪除。

如需 Firewall Manager 員 DNS 防火牆策略的相關資訊，請參閱Amazon 路線 53 解析器 DNS 防火牆政策。

開始使用 AWS Firewall Manager帕洛阿爾托網路雲端次世代防火牆政策

若要用 AWS Firewall Manager 來啟用帕洛阿爾托網路雲端次世代防火牆 (NGFW) 原則，請依序執行下列步驟。如需帕洛阿爾托網路雲端 NGFW 原則的相關資訊，請參閱。帕洛奧圖網路雲端新世代防火牆政策

主題

- 步驟 1：完成一般先決條件
- 步驟 2：完成帕洛阿爾托網路雲端 NGFW 政策先決條件
- 步驟 3：建立並套用帕洛阿爾托網路雲端 NGFW 政策

步驟 1：完成一般先決條件

為 AWS Firewall Manager準備您的帳戶有幾個必要的步驟。AWS Firewall Manager 前提 說明這些步驟。繼續進行下一個步驟之前，請先完成所有先決條件。

步驟 2：完成帕洛阿爾托網路雲端 NGFW 政策先決條件

您必須完成幾個額外的必要步驟，才能使用帕洛阿爾托網路雲端 NGFW 政策。帕洛阿爾托網路雲端次世代防火牆政策先決條件 說明這些步驟。繼續進行下一個步驟之前，請先完成所有先決條件。

步驟 3：建立並套用帕洛阿爾托網路雲端 NGFW 政策

完成必要條件後，您可以建立 AWS Firewall Manager 帕洛阿爾托網路雲端 NGFW 政策。

如需帕洛阿爾托網路雲端 NGFW 的 Firewall Manager 員原則的詳細資訊，請參閱。帕洛奧圖網路雲端新世代防火牆政策

建立帕洛阿爾托網路雲端 NGFW (主控台) 的 Firewall Manager 員政策

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對「原則類型」，選擇「帕洛奧圖網路雲端 NGFW」。如果您尚未在 AWS Marketplace 上訂閱帕洛阿爾托網絡雲 NGFW 服務，則需要先這樣做。若要在 AWS Marketplace 中訂閱，請選擇 [檢視 AWS Marketplace 詳細資料]。
5. 對於部署模型，請選擇分散式模型或集中式模型。部署模式會決定 Firewall Manager 員如何管理策略的端點。使用分散式模型時，Firewall Manager 員會在策略範圍內的每個 VPC 中維護防火牆端點。使用集中式模型，Firewall Manager 員會在檢查 VPC 中維護單一端點。
6. 在「區域」中，選擇一個 AWS 區域。若要保護多個區域中的資源，您必須為每個區域建立個別的政策。
7. 選擇下一步。
8. 在策略名稱中，輸入描述性名稱。
9. 在原則組態中，選擇要與此原則建立關聯的 Palo Alto 網路雲端 NGFW 防火牆原則。帕洛阿爾托網路雲端 NGFW 防火牆政策清單包含與帕洛阿爾托網路雲端 NGFW 租用戶相關聯的所有帕洛阿爾托網路雲端 NGFW 防火牆政策。如需建立和管理帕洛阿爾托網路雲端 NGFW 防火牆原則的相關資訊，請參閱部署帕洛阿爾托網路雲端 NGFW 部署指南中的 AWS Firewall Manager主題中的 AWS部署帕洛阿爾托網路雲端新世代防火牆。 AWS
10. 對於帕洛奧圖網路雲端 NGFW 記錄-選用，選擇性地選擇要記錄原則的帕羅奧圖網路雲端 NGFW 記錄類型。如需有關帕洛阿爾托網路雲端 NGFW 記錄檔類型的資訊，請參閱在帕羅奧圖網路雲端 NGFW 的部署指南 AWS中設定帕洛阿爾托網路雲端 NGFW 的記錄。 AWS

若為記錄目的地，請指定 Firewall Manager 員應將記錄檔寫入的時間

11. 選擇下一步。
12. 在 [設定協力廠商防火牆端點] 底下，執行下列其中一項動作，視您使用的是分散式或集中式部署模型來建立防火牆端點而定：

    - 如果您針對此原則使用分散式部署模型，請在可用區域下選取要在其中建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 來選取可用區域。
    - 如果您使用此原則的集中式部署模型，請在 [檢查 VPC 組態] 下的AWS Firewall Manager 端點設定中，輸入檢查 VPC 擁有者的 AWS 帳戶識別碼，以及檢查 VPC 的 VPC ID。
      - 在可用區域下，選取要在其中建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 來選取可用區域。
13. 選擇下一步。
14. 針對策略範圍，在AWS 帳戶 此原則適用於下方，選擇如下選項：

    - 如果您要將策略套用至組織中的所有帳戶，請保留預設選項「包含我的 AWS 組織下的所有帳戶」。
    - 如果您只想將策略套用至特定 AWS Organizations 組織單位 (OU) 中的特定帳戶或帳戶，請選擇 [僅包含指定的帳戶和組織單位]，然後新增您要包含的帳戶和 OU。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。
    - 如果您要將策略套用至特定帳戶或 AWS Organizations 組織單位 (OU) 以外的所有帳戶或組織單位，請選擇 [排除指定的帳戶和組織單位]，並包含所有其他帳戶，然後新增您要排除的帳戶和 OU。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

    您只能選擇一個選項。

    套用策略後，Firewall Manager 員會根據您的設定自動評估任何新帳號。例如，如果您只包含特定帳戶，則 Firewall Manager 員不會將策略套用至任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子系 OU 時，Firewall Manager 員會自動將原則套用至新帳戶。

    Network Firewall 策略的資源類型為 VPC。
15. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

    如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。

16. 對於授予跨帳戶存取權，請選擇 [下載 AWS CloudFormation 範本]。這會下載可用來建立 AWS CloudFormation 堆疊的 AWS CloudFormation 範本。該堆棧創建一個 AWS Identity and Access Management 角色，授予 Firewall Manager 器跨帳戶權限來管理帕洛阿爾托網絡雲 NGFW 資源。如需有關堆疊的資訊，請參閱使用指南中的AWS CloudFormation 使用堆疊。
17. 選擇下一步。
18. 對於策略標記，請新增任何您要新增至 Firewall Manager 員策略資源的識別標籤。如需標籤的詳細資訊，請參閱使用標籤編輯器。
19. 選擇下一步。
20. 檢閱新的原則設定，並返回需要進行任何調整的頁面。

    請務必確定 Policy action (政策動作) 已設為 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)。這可讓您在啟用政策之前檢閱原則所做的變更。
21. 當您滿意時，選擇 建立政策。

    在 [原AWS Firewall Manager 則] 窗格中，應該會列出您的原則。它可能會在帳戶標題下指示「待處理」，並指示「自動補救」設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱檢視 AWS Firewall Manager 原則的符合性資訊。

如需 Firewall Manager 員帕洛阿爾托網路雲端 NGFW 原則的詳細資訊，請參閱。帕洛奧圖網路雲端新世代防火牆政策

開始使用 AWS Firewall Manager富泰蓋特 CNF 政策

Fortigate 雲端原生防火牆 (CNF) 即服務是一項協力廠商防火牆服務，可用於您的政策。 AWS Firewall Manager 使用 Fortigate CNF 的 Firewall Manager 員，您可以在所有帳戶中創建和集中部署 Fortigate CNF 資源和策略集。 AWS 若要用 AWS Firewall Manager 來啟用 Fortigate CNF 策略，請依序執行下列步驟。如需有關 Fortigate CNF 政策的詳細資訊，請參閱。強制雲端原生防火牆 (CNF) 即服務政策

主題

- 步驟 1：完成一般先決條件
- 步驟 2：完成強制 CNF 政策先決條件

步驟 1：完成一般先決條件

為 AWS Firewall Manager準備您的帳戶有幾個必要的步驟。AWS Firewall Manager 前提 說明這些步驟。繼續進行下一個步驟之前，請先完成所有先決條件。

步驟 2：完成強制 CNF 政策先決條件

您必須完成其他強制步驟才能使用 Fortigate CNF 政策。將雲端原生防火牆 (CNF) 作為服務政策的先決條件 說明這些步驟。繼續進行下一個步驟之前，請先完成所有先決條件。

步驟 3：建立並套用強制 CNF 政策

完成必要條件之後，您可以建立一個 AWS Firewall Manager 強制 CNF 策略。

如需有關 Fortigate CNF Firewall Manager 員原則的詳細資訊，請參閱。強制雲端原生防火牆 (CNF) 即服務政策

建立 Firewall Manager 員策略

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對「策略類型」，選擇「強制 CNF」。如果您尚未在 AWS Marketplace 中訂閱 Fortigate CNF 服務，則需要先這樣做。若要在 AWS Marketplace 中訂閱，請選擇 [檢視 AWS Marketplace 詳細資料]。
5. 對於部署模型，請選擇分散式模型或集中式模型。部署模型會決定 Firewall Manager 員如何管理策略的端點。使用分散式模型時，Firewall Manager 員會在策略範圍內的每個 VPC 中維護防火牆端點。使用集中式模型，Firewall Manager 員會在檢查 VPC 中維護單一端點。
6. 在「區域」中，選擇一個 AWS 區域。若要保護多個區域中的資源，您必須為每個區域建立個別的政策。

7. 選擇下一步。
8.
9. 在策略配置中，選擇要與此策略關聯的 Fortigate CNF 防火牆策略。Fortigate CNF 防火牆策略列表包含與您的 Fortigate CNF 租戶相關聯的所有 Fortigate CNF 防火牆策略。如需有關建立和管理 Fortigate CNF 防火牆策略的詳細資訊，請參閱更多 CNF 文件。
10. 選擇下一步。
11. 在 [設定協力廠商防火牆端點] 底下，執行下列其中一項動作，視您使用的是分散式或集中式部署模型來建立防火牆端點而定：

    - 如果您針對此原則使用分散式部署模型，請在可用區域下選取要在其中建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 來選取可用區域。
    - 如果您使用此原則的集中式部署模型，請在 [檢查 VPC 組態] 下的AWS Firewall Manager 端點設定中，輸入檢查 VPC 擁有者的 AWS 帳戶識別碼，以及檢查 VPC 的 VPC ID。
      - 在可用區域下，選取要在其中建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 來選取可用區域。
12. 選擇下一步。
13. 針對策略範圍，在AWS 帳戶 此原則適用於下方，選擇如下選項：

    - 如果您要將策略套用至組織中的所有帳戶，請保留預設選項「包含我的 AWS 組織下的所有帳戶」。
    - 如果您只想將策略套用至特定 AWS Organizations 組織單位 (OU) 中的特定帳戶或帳戶，請選擇 [僅包含指定的帳戶和組織單位]，然後新增您要包含的帳戶和 OU。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。
    - 如果您要將策略套用至特定帳戶或 AWS Organizations 組織單位 (OU) 以外的所有帳戶或組織單位，請選擇 [排除指定的帳戶和組織單位]，並包含所有其他帳戶，然後新增您要排除的帳戶和 OU。指定 OU 等同於指定 OU 及其任何子 OU 中的所有帳戶，包括稍後新增的任何子 OU 和帳戶。

    您只能選擇一個選項。

    套用策略後，Firewall Manager 員會根據您的設定自動評估任何新帳號。例如，如果您只包含特定帳戶，則 Firewall Manager 員不會將策略套用至任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子系 OU 時，Firewall Manager 員會自動將原則套用至新帳戶。

    強制 CNF 策略的資源類型為 VPC。

14. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

    如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

    資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。
15. 對於授予跨帳戶存取權，請選擇 [下載 AWS CloudFormation 範本]。這會下載可用來建立 AWS CloudFormation 堆疊的 AWS CloudFormation 範本。此堆棧創建一個 AWS Identity and Access Management 角色，該角色授予 Firewall Manager 器跨帳戶管理 Fortigate CNF 資源的權限。如需有關堆疊的資訊，請參閱使用指南中的AWS CloudFormation 使用堆疊。要創建一個堆棧，您需要來自 Fortigate CNF 門戶的帳戶 ID。
16. 選擇下一步。
17. 對於策略標記，請新增任何您要新增至 Firewall Manager 員策略資源的識別標籤。如需標籤的詳細資訊，請參閱使用標籤編輯器。
18. 選擇下一步。
19. 檢閱新的原則設定，並返回需要進行任何調整的頁面。

    請務必確定 Policy action (政策動作) 已設為 Identify resources that don't comply with the policy rules, but don't auto remediate. (識別不符合政策規則的資源，但不要自動修補。)。這可讓您檢閱原則在啟用前所做的變更。
20. 當您滿意時，選擇 建立政策。

    在 [原AWS Firewall Manager 則] 窗格中，應該會列出您的原則。它可能會在帳戶標題下指示「待處理」，並指示「自動補救」設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱檢視 AWS Firewall Manager 原則的符合性資訊。

如需有關 Firewall Manager 員強制 CNF 策略的詳細資訊，請參閱。強制雲端原生防火牆 (CNF) 即服務政策

使用 AWS Firewall Manager 原則

AWS Firewall Manager 提供下列類型的原則。您可以針對每個原則類型定義下列項目：

- AWS WAF原則 — Firewall Manager 員支援 AWS WAF 和 AWS WAF 傳統策略。對於這兩個版本，您可以定義哪些資源受到政策保護。

  - AWS WAF 原則類型會在 Web ACL 中先執行和最後一組規則群組。然後，在您套用 Web ACL 的帳戶中，帳戶擁有者可以新增要在兩個集合之間執行的規則和規則群組。
  - 「AWS WAF 典型」原則類型會在 Web ACL 中執行單一規則群組。
- 屏蔽進階策略 — 此策略類型會針對您指定的資源類型，在整個組織中套用 Shield 進階保護。
- Amazon VPC 安全群組原則 — 此政策類型可讓您控制整個組織中使用的安全群組，並可讓您在整個組織中強制執行基準規則集。
- Amazon VPC 網路存取控制清單 (ACL) 政策 — 此政策類型可讓您控制整個組織中使用的網路 ACL，並可讓您在組織中強制執行一組基準網路 ACL。
- Network Firewall 原則 — 此原則類型會將 AWS Network Firewall 保護套用至組織的 VPC。
- Amazon 路由 53 解析器 DNS 防火牆政策 — 此政策將 DNS 防火牆保護套用到您組織的 VPC。
- 第三方防火牆策略 — 此策略類型會套用協力廠商防火牆保護。協力廠商防火牆可透過 AWS Marketplace 主控台的訂閱方式取得。AWS
  - 帕洛奧圖網路雲端新世代防火牆原則 — 此原則類型將帕洛奧圖網路雲端次世代防火牆 (NGFW) 保護和帕洛阿爾托網路雲端 NGFW 規則堆疊套用至您組織的 VPC。
  - Fortigate 雲端原生防火牆 (CNF) 即服務政策 — 此原則類型適用 Fortigate 雲端原生防火牆 (CNF) 即服務保護。Fortigate CNF 是以雲端為中心的解決方案，透過業界領先的進階威脅防護、智慧型 Web 應用程式防火牆 (WAF) 和 API 保護，封鎖零時差威脅並保護雲端基礎架構。

Firewall Manager 員策略特定於個別策略類型。如果您想要跨帳戶強制執行多種政策類型，您可以建立多項政策。您可以為各種類型建立一個以上的政策。

如果您將新帳戶新增至使用建立的組織 AWS Organizations，Firewall Manager 會自動將策略套用至該帳戶中位於策略範圍內的資源。

原則的一 AWS Firewall Manager 般設定

AWS Firewall Manager 受管理的策略有一些常見的設定和行為。對於所有人，您可以指定名稱並定義策略的範圍，並且可以使用資源標記來控制策略範圍。您可以選擇檢視不合規的帳戶和資源，但不採取修正動作或自動修補不合規的資源。

如需有關策略範圍的資訊，請參閱AWS Firewall Manager 政策範圍。

建立 AWS Firewall Manager 策略

不同政策類型的政策建立步驟有所不同。務必根據您所需的政策類型使用程序。

> **Important**
>
> AWS Firewall Manager 不支持 Amazon 路線 53 或 AWS Global Accelerator. 如果您想要使用 Shield Advanced 來保護這些資源，就無法使用 Firewall Manager 員原則。或者，請遵循為 AWS 資源添加 AWS Shield Advanced 保護中的說明進行。

主題

建立 AWS Firewall Manager 政策 AWS WAF

在 Firewall Manager 員 AWS WAF 政策中，您可以使用受管規則群組，這些群組 AWS 和 AWS Marketplace 賣家會為您建立和維護。您也可以建立和使用自己的規則群組。如需規則群組的詳細資訊，請參閱AWS WAF 規則群組。

如果您想要使用自己的規則群組，請在建立 Firewall Manager 員 AWS WAF 政策之前先建立這些規則群組。如需準則，請參閱管理您自己的規則群組。若要使用個別的自訂規則，您必須定義自己的規則群組、在該群組中定義規則，然後在政策中使用規則群組。

如需有關 Firewall Manager 員 AWS WAF 策略的資訊，請參閱 AWS WAF 政策

若要建立 AWS WAF (主控台) 的 Firewall Manager 員策略

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對政策類型，選擇 AWS WAF。
5. 在「區域」中，選擇一個 AWS 區域。要保護 Amazon CloudFront 分佈，請選擇全球。

   若要保護多個區域中的資源 (CloudFront 散佈除外)，您必須為每個區域建立個別的 Firewall Manager 員政策。
6. 選擇下一步。
7. 在策略名稱中，輸入描述性名稱。Firewall Manager 員會在其管理的 Web ACLs 名稱中包含策略名稱。網頁ACL名稱`FMManagedWebACLV2-`後面接著您在此處輸入的策略名稱`-`，以及 Web ACL 建立時間戳記 (以UTC毫秒為單位)。例如 `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`。
8. 對於 Web 要求主體檢查，選擇性地變更主體大小限制。如需有關本體檢查大小限制的資訊，包括定價考量，請參閱AWS WAF 開發人員指南管理車身檢查尺寸限制中的。
9. 在 [原則規則] 底下，新增您要在 Web 中評估 AWS WAF 的第一個和最後一個規則群組ACL。若要使用 AWS WAF 受管規則群組版本控制，請切換 [啟用版本 個別帳戶管理員可以在第一個規則群組和最後一個規則群組之間新增規則和規則群組。如需有關在的 Firewall Manager 員策略中使用 AWS WAF 規則群組的詳細資訊 AWS WAF，請參閱AWS WAF 政策。

   (選擇性) 若要自訂 Web ACL 使用規則群組的方式，請選擇 「編輯」。以下是常見的自訂設定：

   - 針對受管規則群組，覆寫部分或所有規則的規則動作。如果您未定義規則的覆寫動作，則評估會使用規則群組內定義的規則動作。如需有關此選項的資訊，請參閱規則群組的動作覆寫選項開AWS WAF 發人員指南中的。
   - 某些受管規則群組會要求您提供其他組態。請參閱受管規則群組提供者的說明文件。如需「 AWS 受管規則」規則群組的特定資訊，請參閱AWS WAF 開發人員指南AWS 的受管規則 AWS WAF中的。

完成設定後，請選擇 [儲存規則]。

10. 設定 Web 的預設動作ACL。這是當 Web 請求與 Web 中的任何規則不匹配時所 AWS WAF採取的操作ACL。您可以使用「允許」動作新增自訂標頭，或針對「封鎖」動作新增自訂回應。如需有關預設 Web ACL 動作的詳細資訊，請參閱網頁 ACL 預設動作。如需有關設定自訂 Web 要求和回應的資訊，請參閱定制的 Web 請求和響應 AWS WAF。
11. 對於記錄組態，請選擇啟用記錄以開啟記錄。記錄可提供有關 Web 分析流量的詳細資訊ACL。選擇記錄目的地，然後選擇您設定的記錄目的地。您必須選擇名稱開頭的記錄目的地`aws-waf-logs-`。如需有關設定 AWS WAF 記錄目的地的資訊，請參閱設定 AWS WAF 原則的記錄。
12. (選用) 如果您不想要特定欄位及其值包含在日誌中，請編寫這些欄位。選擇要編寫的欄位，然後選擇新增。重複其他需要編寫的欄位。在日誌中編寫的欄位顯示為 `REDACTED`。例如，如果您編輯URI欄位，記錄中的URI欄位將會是`REDACTED`。
13. (選擇性) 如果您不想將所有要求傳送至記錄檔，請新增篩選條件和行為。在「篩選記錄檔」下方，針對您要套用的每個篩選器，選擇「新增篩選器」，然後選擇您的篩選條件，並指定要保留或刪除符合條件的要求。完成新增篩選器後，如有需要，請修改預設記錄行為。如需詳細資訊，請參閱《AWS WAF 開發人員指南》中的 網頁 ACL 記錄設定。
14. 您可以定義 Token 網域清單，以啟用受保護應用程式之間的權杖共用。當您使用「受管規則」規則群組進Challenge行 AWS WAF 詐騙控制帳戶接 AWS 管預防 (ATP) 和 AWS WAF 機器人控制時，您實作的應用程式整合SDKs會使用 Token 和動作以及應用程式整合。CAPTCHA

    不允許使用公共後綴。例如，您無法使用`gov.au`或`co.uk`做為權杖網域。

    默認情況下，僅 AWS WAF 接受保護資源的域令牌。如果您在此清單中新增 Token 網域，請 AWS WAF 接受清單中所有網域和相關資源網域的權杖。如需詳細資訊，請參閱《AWS WAF 開發人員指南》中的 AWS WAF 網絡 ACL 令牌域列表配置。

    您只能在編輯現有網頁ACL時變更網頁CAPTCHA和挑戰免疫時間ACL。您可以在 Firewall Manager 員策略詳細資料頁面下找到這些設定。如需這些設定的資訊，請參閱 時間戳記到期：AWS WAF 權杖豁免時間。如果您更新現有策略中的關聯設定CAPTCHA、挑戰或權杖網域清單設定，Firewall Manager 將會以新值覆寫您ACLs的本機 Web。不過，如果您未更新原則的「關聯設定」CAPTCHA、「挑戰」或「權杖網域清單」設定，則本機 Web 中的值ACLs將保持不變。如需有關此選項的資訊，請參閱CAPTCHA並Challenge在 AWS WAF開AWS WAF 發人員指南中的。
15. 在「Web ACL 管理」下，如果您希望「Firewall Manager 員」管理未關聯的 WebACLs，請啟用「管理未關聯的網頁」。ACLs使用此選項時，Firewall Manager 員只會ACLs在至少一個資源使用 Web 時，才ACLs會在策略範圍內的帳號中建立 Web。如果任何時候有帳戶進入策略範圍，如果至少有一個資源將使用 Web，則 Firewall Manager 員會ACL在帳戶中自動建立網頁ACL。啟用此

選項後，Firewall Manager 員會執行一次性清除帳戶中未關聯ACLs的網頁。清理過程可能需要幾個小時。如果資源在 Firewall Manager 建立網頁之後離開策略範圍ACL，則 Firewall Manager 員會取消資源與網路的關聯ACL，但不會清除未關聯的網頁。ACLFirewall Manager 員只會在您第一次啟用策略中未關聯網頁的管理ACLs時，才會清除未關聯ACLs的網頁。

16. 對於「策略」動作，如果您要ACL在組織內的每個適用帳號中建立 Web，但尚未ACL將 Web 套用至任何資源，請選擇 [識別不符合策略規則，但不 auto 動修復的資源]，且不要選擇 [管理未關聯的 Web]。ACLs您可以稍後變更這些選項。

    如果您要改為自動將政策套用至現有的範圍內資源，請選擇 Auto remediate any noncompliant resources (自動修補任何不合規的資源)。如果停用「管理未關聯的 Web ACLs」，則「自動修復任何不符合標準的資源」選項會ACL在組織內的每個適用帳號中建立 Web，並將 Web ACL 與帳號中的資源相關聯。如果啟用了「管理未關聯的 Web ACLs」，則「自動修復任何不符合標準的資源」選項僅會建立並關聯具有資源可與 Web 關聯的帳號ACL中的 Web 帳號。ACL

    當您選擇自動修復任何不符合標準的資源時，您也可以選擇從範圍內的資源中移除現有的 Web ACL 關聯，針對不受其他作用中 Firewall Manager 員策略管理的 Web ACLs。如果您選擇此選項，則 Firewall Manager 員會先將策略的網頁ACL與資源建立關聯，然後移除先前的關聯。如果資源與另一個由不同作用中 Firewall Manager 員策略管理的 Web ACL 有關聯，則此選項不會影響該關聯。

17. 選擇下一步。

18. 針對AWS 帳戶 此原則適用於，請依下列方式選擇選項：

    - 如果您要將策略套用至組織中的所有帳戶，請保留預設選項「包含我的 AWS 組織下的所有帳戶」。
    - 如果您只想將策略套用至特定 AWS Organizations 組織單位中的特定帳戶或帳號 (OUs)，請選擇 [僅包含指定的帳戶和組織單位]，然後新增您OUs要包含的帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。
    - 如果您要將策略套用至特定帳戶或組織單位 () 以外的所有帳戶或 AWS Organizations 組織單位 (OUs)，請選擇 [排除指定的帳戶和組織單位]，並包含所有其他帳戶，然後新增您OUs要排除的帳號和帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。

    您只能選擇一個選項。

套用策略後，Firewall Manager 員會根據您的設定自動評估任何新帳號。例如，如果您只包含特定帳戶，則 Firewall Manager 員不會將策略套用至任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子系時OUs，Firewall Manager 會自動將策略套用至新帳戶。

19. 針對 Resource type (資源類型)，請選擇您要保護的資源類型。
20. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

    如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

    資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。
21. 選擇下一步。
22. 對於策略標記，請新增任何您要新增至 Firewall Manager 員策略資源的識別標籤。如需標籤的詳細資訊，請參閱使用標籤編輯器。
23. 選擇下一步。
24. 檢閱新的原則設定，並返回需要進行任何調整的頁面。

    當您滿意時，選擇 建立政策。在 [原AWS Firewall Manager 則] 窗格中，應該會列出您的原則。它可能會在帳戶標題下指示「待處理」，並指示「自動補救」設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱檢視 AWS Firewall Manager 原則的符合性資訊。

建立 AWS WAF 傳統的 AWS Firewall Manager 原則

建立 AWS WAF 典型（主控台）的 Firewall Manager 員策略

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。

4. 針對 Policy type (政策類型)，選擇 AWS WAF Classic。
5. 如果您已 AWS WAF 經建立要新增至原則的傳統規則群組，請選擇 [建立 AWS Firewall Manager 原則] 並新增現有規則群組。如果您要建立新的規則群組，請選擇 [建立 Firewall Manager 員原則]，然後新增規則群組。
6. 在「區域」中，選擇一個 AWS 區域。若要保護 Amazon CloudFront 資源，請選擇「全球」。

   若要保護多個區域 (資源除外) 中的 CloudFront 資源，您必須為每個區域建立個別的 Firewall Manager 員政策。
7. 選擇下一步。
8. 如果您要建立一個規則群組，則遵循建立 AWS WAF 傳統規則群組的指示。在您建立規則群組，請繼續執行以下步驟。
9. 輸入政策名稱。
10. 如果您要新增現有的規則群組，請使用下拉式功能表選取要新增的規則群組，然後選擇 [新增規則群組]。
11. 政策有兩種動作：規則群組這定的動作和計數。如果您想要測試政策和規則群組，設定動作為計數。這個動作覆寫任何由規則群組中的規則所指定的封鎖動作。也就是說，如果政策的動作是設定為計數，只會計算請求，而不會封鎖請求。反之，如果您設定政策的動作為規則群組設定的動作，則會使用該規則群組規則的動作。選擇適當動作。
12. 選擇下一步。
13. 針對AWS 帳戶 此原則適用於，請依下列方式選擇選項：

    - 如果您要將策略套用至組織中的所有帳戶，請保留預設選項「包含我的 AWS 組織下的所有帳戶」。
    - 如果您只想將策略套用至特定 AWS Organizations 組織單位中的特定帳戶或帳號 (OUs)，請選擇 [僅包含指定的帳戶和組織單位]，然後新增您OUs要包含的帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。
    - 如果您要將策略套用至特定帳戶或組織單位 () 以外的所有帳戶或 AWS Organizations 組織單位 (OUs)，請選擇 [排除指定的帳戶和組織單位]，並包含所有其他帳戶，然後新增您OUs要排除的帳號和帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。

    您只能選擇一個選項。

套用策略後，Firewall Manager 員會根據您的設定自動評估任何新帳號。例如，如果您只包含特定帳戶，則 Firewall Manager 員不會將策略套用至任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子系時OUs，Firewall Manager 會自動將策略套用至新帳戶。

14. 選擇您要保護的資源類型。
15. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

    如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

    資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。
16. 如果您想自動套用政策到現有的資源，請選擇建立和套用此政策到現有的和新的資源。

    此選項會ACL在 AWS 組織內的每個適用帳戶中建立 Web，並將 Web ACL 與帳戶中的資源相關聯。此選項還會將政策套用到與前述條件 (資源類型和標籤) 符合的所有新的資源。或者，如果您選擇 [建立策略] 但未將策略套用至現有或新資源，則 Firewall Manager 會ACL在組織內的每個適用帳戶中建立網頁，但不會ACL將 Web 套用至任何資源。之後，您必須將政策套用到資源。選擇適當選項。
17. 對於 [取代現有的關ACL聯網頁]ACLs，您可以選擇移除目前針對範圍內資源定義的任何 Web 關聯，然後將它們取代為您正在使用此原則建立之 Web ACLs 的關聯。默認情況下，Firewall Manager 器不會刪除現有的 Web ACL 關聯之前，它添加新的。如果您要移除現有的 Web ACL 關聯，請選擇此選項。
18. 選擇下一步。
19. 檢視新政策。若要修改，選擇編輯。當您滿意政策時，選擇 Create and apply policy (建立和套用政策)。

建立 AWS Firewall Manager 政策 AWS Shield Advanced

建立 Firewall Manager 員策略 Shield 火牆進階（主控台）

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

> **Note**
>
> 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對策略類型，選擇 Shield 進階。

   若要建立 Shield 牌進階政策，您必須訂閱 Shield 牌進階。如果您未訂閱，系統會提示您訂閱。如需訂閱費用的相關資訊，請參閱AWS Shield Advanced 定價。
5. 在「區域」中，選擇一個 AWS 區域。要保護 Amazon CloudFront 分佈，請選擇全球。

   對於「全域」以外的「區域」選項，若要保護多個區域中的資源，您必須為每個區域建立個別的 Firewall Manager 員政策。
6. 選擇下一步。
7. 在「名稱」中，輸入描述性名稱。
8. 僅適用於全球區域政策，您可以選擇是否要管理 Shield Advanced 自動應用程式層DDoS緩和措施。如需有關此 Shield 進階功能的資訊，請參閱Shield 先進的自動應用層 DDoS 緩解。

   您可以選擇啟用或停用自動緩和措施，也可以選擇忽略它。如果您選擇忽略它，Firewall Manager 員根本不會管理 Shield 進階防護的自動緩和措施。如需這些原則選項的詳細資訊，請參閱自動化應用程式層 DDoS 防護。
9. 在「Web ACL 管理」下，如果您希望「Firewall Manager 員」管理未關聯的 WebACLs，請啟用「管理未關聯的網頁」。ACLs使用此選項時，Firewall Manager 員只會ACLs在至少一個資源使用 Web 時，才ACLs會在策略範圍內的帳號中建立 Web。如果任何時候有帳戶進入策略範圍，如果至少有一個資源將使用 Web，則 Firewall Manager 員會ACL在帳戶中自動建立網頁ACL。啟用此選項後，Firewall Manager 員會執行一次性清除帳戶中未關聯ACLs的網頁。清理過程可能需要幾個小時。如果資源在 Firewall Manager 員建立 Web 之後離開策略範圍ACL，則 Firewall Manager 員將不會取消資源與 Web ACL 的關聯。若要在一次性清除ACL中包含網頁，您必須先手動取消資源與網路的關聯，ACL然後啟用「管理未關聯的網頁」。ACLs
10. 對於「策略」動作，建議您使用不自動修復不符合資源的選項來建立策略。停用自動補救時，您可以先評估新原則的效果，然後再套用它。如果您滿意變更是您想要的，請編輯原則並變更原則動作以啟用自動修復。

如果您要改為自動將政策套用至現有的範圍內資源，請選擇 Auto remediate any noncompliant resources (自動修補任何不合規的資源)。此選項會針對 AWS 組織內的每個適用帳號及帳號中的每個適用資源套用「Shield 牌進階」保護。

僅針對「全域區域」策略，如果您選擇自動修復任何不符合標準的資源，您也可以選擇讓「Firewall Manager 員」自動將任何現有的「 AWS WAF 典型」Web 關聯取代ACLs為使用最新版 AWS WAF (v2) 建立的 Web 關聯。ACL如果您選擇這個選項，Firewall Manager 會移除與舊版網頁的關聯，ACLs並建立與最新版 Web 的新關聯ACLs，ACLs在任何尚未包含原則的範圍內帳戶中建立新的空白網頁之後。如需有關此選項的詳細資訊，請參閱 以最新版本的網頁 ACL 取代 AWS WAF 傳統網頁 ACL。

11. 選擇下一步。
12. 針對AWS 帳戶 此原則適用於，請依下列方式選擇選項：

    - 如果您要將策略套用至組織中的所有帳戶，請保留預設選項「包含我的 AWS 組織下的所有帳戶」。
    - 如果您只想將策略套用至特定 AWS Organizations 組織單位中的特定帳戶或帳號 (OUs)，請選擇 [僅包含指定的帳戶和組織單位]，然後新增您OUs要包含的帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。
    - 如果您要將策略套用至特定帳戶或組織單位 () 以外的所有帳戶或 AWS Organizations 組織單位 (OUs)，請選擇 [排除指定的帳戶和組織單位]，並包含所有其他帳戶，然後新增您OUs要排除的帳號和帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。

    您只能選擇一個選項。

    套用策略後，Firewall Manager 員會根據您的設定自動評估任何新帳號。例如，如果您只包含特定帳戶，則 Firewall Manager 員不會將策略套用至任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子系時OUs，Firewall Manager 會自動將策略套用至新帳戶。
13. 選擇您要保護的資源類型。

    Firewall Manager 員不支援 Amazon 路由 53 或 AWS Global Accelerator. 如果您需要使用 Shield Advanced 來保護資源不受這些服務攻擊，則無法使用 Firewall Manager 員策略。相反，請遵循的「Shield 牌進階」指引為 AWS 資源添加 AWS Shield Advanced 保護。
14. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。

15. 選擇下一步。
16. 對於策略標記，請新增任何您要新增至 Firewall Manager 員策略資源的識別標籤。如需標籤的詳細資訊，請參閱使用標籤編輯器。
17. 選擇下一步。
18. 檢閱新的原則設定，並返回需要進行任何調整的頁面。

    當您滿意時，選擇 建立政策。在 [原AWS Firewall Manager 則] 窗格中，應該會列出您的原則。它可能會在帳戶標題下指示「待處理」，並指示「自動補救」設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱檢視 AWS Firewall Manager 原則的符合性資訊。

建立 AWS Firewall Manager 常見安全群組政策

如需常見安全群組政策如何運作的資訊，請參閱 常見安全群組政策。

若要建立一般安全性群組原則，您必須在您的 Firewall Manager 系統管理員帳戶中已建立一個安全性群組，您想要做為原則的主要使用。您可以通過 Amazon Virtual Private Cloud（AmazonVPC）或 Amazon 彈性計算雲（AmazonEC2）管理安全組。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用安全群組。

若要建立常見安全群組政策 (主控台)

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 對於 Policy type (政策類型)，選擇 Security group (安全群組)。

5. 對於 Security group policy type (安全群組類型)，選擇 Common security groups (常見安全群組)。
6. 在「區域」中，選擇一個 AWS 區域。
7. 選擇下一步。
8. 對於 Policy name (政策名稱)，輸入易記的名稱。
9. 對於 Policy rules (政策規則)，執行下列操作：

   a. 從 rules 選項中，選擇您要套用至安全性群組規則和原則範圍內的資源的限制。如果您選擇將標籤從主要安全性群組分發到由此原則建立的安全性群組，則您也必須選取 [識別並報告] 當此原則建立的安全性群組變成不符合標準時。

   > **Important**
   >
   > Firewall Manager 員不會將 AWS 服務新增的系統標記散佈到複本安全性群組中。系統標籤以 `aws:` 字首開頭。此外，如果策略的標記與組織的標籤策略衝突，Firewall Manager 將不會更新現有安全群組的標記或建立新的安全群組。如需有關標籤策略的資訊，請參閱 AWS Organizations 使用指南中的標籤策略。

   如果您選擇將安全群組參考從主要安全群組分發到此政策建立的安全群組，則 Firewall Manager 只會在安全群組參考在 Amazon 中具有作用中的對等連線時，才會分發安全群組參考。VPC如需有關此選項的詳細資訊，請參閱策略規則設定。

   b. 對於 [主要安全性群組]，請選擇 [新增安全性群組]，然後選擇您要使用的安全性群組。Firewall Manager 員會填入 Firewall Manager 員帳戶中所有 Amazon VPC 執行個體的安全群組清單。

   根據預設，每個原則的主要安全性群組數目上限為 3。如需有關此設定的詳細資訊，請參閱 AWS Firewall Manager 配額。

   c. 對於 Policy action (政策動作)，我們建議建立包含不自動修補選項的政策。這可讓您在套用新政策之前評估其效用。當您確認這些變更正是您所需的時，請編輯政策並變更政策動作，以啟用不合規資源的自動修補。

10. 選擇下一步。
11. 針對AWS 帳戶 此原則適用於，請依下列方式選擇選項：

    - 如果您要將策略套用至組織中的所有帳戶，請保留預設選項「包含我的 AWS 組織下的所有帳戶」。

- 如果您只想將策略套用至特定 AWS Organizations 組織單位中的特定帳戶或帳號 (OUs)，請選擇 [僅包含指定的帳戶和組織單位]，然後新增您OUs要包含的帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。
- 如果您要將策略套用至特定帳戶或組織單位 () 以外的所有帳戶或 AWS Organizations 組織單位 (OUs)，請選擇 [排除指定的帳戶和組織單位]，並包含所有其他帳戶，然後新增您OUs要排除的帳號和帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。

  您只能選擇一個選項。

  套用策略後，Firewall Manager 員會根據您的設定自動評估任何新帳號。例如，如果您只包含特定帳戶，則 Firewall Manager 員不會將策略套用至任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子系時OUs，Firewall Manager 會自動將策略套用至新帳戶。

12. 針對 Resource type (資源類型)，請選擇您要保護的資源類型。

    對於資源類型EC2執行個體，您可以選擇修復所有 Amazon EC2 執行個體，或僅修復僅具有預設主 elastic network interface () ENI 的執行個體。對於後一個選項，Firewall Manager 員不會修復具有其他ENI附件的執行個體。而是啟用自動修復時，Firewall Manager 只會標記這些EC2執行個體的符合性狀態，而不會套用任何補救動作。請參閱 Amazon EC2 資源類型的其他警告和限制，網址為。安全性群組原則警告和限制

13. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

    如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

    資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。

14. 對於共用VPC資源，如果您想要將策略套用至共用的資源VPCs，除了帳號擁有的資源VPCs之外，請選取「包含共用的資源」VPCs。
15. 選擇下一步。
16. 檢閱政策設定，以確保其為您所需的設定，然後選擇 Create policy (建立政策)。

Firewall Manager 員會在範圍內帳戶中包含的每個 Amazon VPC 執行個體中建立主要安全群組的複本，最多可達到每個帳戶支援的 Amazon VPC 最大配額。Firewall Manager 員會將複本安全性群組與每個範圍內帳戶原則範圍內的資源相關聯。如需此政策如何運作的詳細資訊，請參閱 常見安全群組政策。

建立 AWS Firewall Manager 內容稽核安全群組政策

如需內容稽核安全群組政策如何運作的資訊，請參閱 內容稽核安全群組政策。

對於某些內容稽核策略設定，您必須提供稽核安全性群組，Firewall Manager 員才能做為範本使用。例如，您可能有一個稽核安全性群組，其中包含您在任何安全性群組中不允許的所有規則。您必須先使用 Firewall Manager 員管理員帳戶建立這些稽核安全性群組，才能在策略中使用這些群組。您可以通過 Amazon Virtual Private Cloud（AmazonVPC）或 Amazon 彈性計算雲（AmazonEC2）管理安全組。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用安全群組。

若要建立內容稽核安全群組政策 (主控台)

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 對於 Policy type (政策類型)，選擇 Security group (安全群組)。
5. 對於 Security group policy type (安全群組政策類型)，選擇 Auditing and enforcement of security group rules (稽核和強制執行安全群組規則)。
6. 在「區域」中，選擇一個 AWS 區域。
7. 選擇下一步。
8. 對於 Policy name (政策名稱)，輸入易記的名稱。
9. 對於策略規則，請選擇您要使用的受管理或自訂策略規則選項。

   a. 對於設定受管理的稽核策略規則，請執行下列動作：

      i. 對於 [設定要稽核的安全性群組規則]，選取您希望稽核策略套用的安全性群組規則類型。

      ii. 如果您想要根據安全性群組中的通訊協定、通訊埠和CIDR範圍設定執行稽核規則之類的作業，請選擇 [稽核過於寬鬆的安全性群組規則]，然後選取您想要的選項。

對於選取 [規則允許所有流量]，您可以提供自訂應用程式清單來指定要稽核的應用程式。如需有關自訂應用程式清單以及如何在原則中使用這些清單的資訊，請參閱受管理清單和使用受管理清單。

對於使用通訊協定清單的選取項目，您可以使用現有的清單，也可以建立新清單。如需有關通訊協定清單以及如何在原則中使用通訊協定清單的資訊，請參閱受管理清單和使用受管理清單。

iii. 如果您要根據對預留或非保留CIDR範圍的存取權來稽核高風險，請選擇「稽核高風險應用模組」，然後選取您要的選項。

下列選項是互斥的：只能存取保留CIDR範圍的應用程式，以及允許存取非保留CIDR範圍的應用程式。您最多可以在任何策略中選取其中一個。

對於使用應用程式清單的選取項目，您可以使用現有清單，也可以建立新清單。如需有關應用程式清單以及如何在原則中使用這些清單的資訊，請參閱受管理清單和使用受管理清單。

iv. 使用覆寫設定可明確覆寫原則中的其他設定。您可以選擇永遠允許或永遠拒絕特定的安全性群組規則，不論這些規則是否符合您為原則設定的其他選項。

對於此選項，您可以提供稽核安全性群組作為允許的規則或拒絕的規則範本。針對 [稽核安全性群組]，選擇 [新增稽核安全性群組]，然後選擇您要使用的安全性群組。Firewall Manager 員會填入 Firewall Manager 員帳戶中所有 Amazon VPC 執行個體的稽核安全群組清單。政策的稽核安全群組數目的預設限額為一個。如需增加配額的詳細資訊，請參閱AWS Firewall Manager 配額。

b. 對於 [設定自訂原則規則]，請執行下列動作：

i. 從規則選項中，選擇是否只允許在稽核安全群組中定義的規則，或拒絕所有規則。如需此選項的詳細資訊，請參閱內容稽核安全群組政策。

ii. 針對 [稽核安全性群組]，選擇 [新增稽核安全性群組]，然後選擇您要使用的安全性群組。Firewall Manager 員會填入 Firewall Manager 員帳戶中所有 Amazon VPC 執行個體的稽核安全群組清單。政策的稽核安全群組數目的預設限額為一個。如需增加配額的詳細資訊，請參閱AWS Firewall Manager 配額。

iii. 對於 Policy action (政策動作)，您必須建立包含不自動修補選項的政策。這可讓您在套用新政策之前評估其效用。當您確認這些變更正是您所需的時，請編輯政策並變更政策動作，以啟用不合規資源的自動修補。

10. 選擇下一步。

11. 針對AWS 帳戶 此原則適用於，請依下列方式選擇選項：

    - 如果您要將策略套用至組織中的所有帳戶，請保留預設選項「包含我的 AWS 組織下的所有帳戶」。
    - 如果您只想將策略套用至特定 AWS Organizations 組織單位中的特定帳戶或帳號 (OUs)，請選擇 [僅包含指定的帳戶和組織單位]，然後新增您OUs要包含的帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。
    - 如果您要將策略套用至特定帳戶或組織單位 () 以外的所有帳戶或 AWS Organizations 組織單位 (OUs)，請選擇 [排除指定的帳戶和組織單位]，並包含所有其他帳戶，然後新增您OUs要排除的帳號和帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。

    您只能選擇一個選項。

    套用策略後，Firewall Manager 員會根據您的設定自動評估任何新帳號。例如，如果您只包含特定帳戶，則 Firewall Manager 員不會將策略套用至任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子系時OUs，Firewall Manager 會自動將策略套用至新帳戶。
12. 對於 Resource type (資源類型)，請選擇您要保護的資源類型。
13. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

    如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

    資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。
14. 選擇下一步。
15. 檢閱政策設定，以確保其為您所需的設定，然後選擇 Create policy (建立政策)。

Firewall Manager 會根據您的策略規則設定，將稽核安全性群組與組 AWS 織中的範圍內安全群組進行比較。您可以在策略主控台中檢閱 AWS Firewall Manager 策略狀態。建立政策後，您可以編輯該政策，並啟用自動修補，以使您的稽核安全群組政策生效。如需此政策如何運作的詳細資訊，請參閱 內容稽核安全群組政策。

建立 AWS Firewall Manager 用途稽核安全群組政策

如需用途稽核安全群組政策如何運作的資訊，請參閱 用途稽核安全群組政策。

建立用途稽核安全群組政策 (主控台)

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 對於 Policy type (政策類型)，選擇 Security group (安全群組)。
5. 針對 [安全性群組原則類型]，選擇 [稽核和清除未關聯及備援的安全性群組]。
6. 在「區域」中，選擇一個 AWS 區域。
7. 選擇下一步。
8. 對於 Policy name (政策名稱)，輸入易記的名稱。
9. 對於 Policy rules (政策規則)，選擇一個可用的選項或兩者都選擇。

   - 如果您選擇此策略範圍內的安全性群組至少必須由一個資源使用，則 Firewall Manager 會移除其判斷為未使用的任何安全性群組。啟用此規則時，Firewall Manager 員會在您儲存策略時執行最後一次。

     如需有關 Firewall Manager 員如何判斷使用情況和修復時間的詳細資訊，請參閱用途稽核安全群組政策。

     > **Note**
     >
     > 當您使用此用法稽核安全性群組原則類型時，請避免在短時間內對範圍內安全性群組的關聯狀態進行多次變更。這樣做可能會導致 Firewall Manager 員遺漏對應的事件。

     根據預設，Firewall Manager 只要安全性群組未使用，就會立即將其視為不相容於此原則規則。您可以選擇性地指定安全性群組在被視為不相容之前可使用的分鐘數，最多可達 525,600 分鐘 (365 天)。您可以使用此設定，讓自己有時間將新的安全性群組與資源建立關聯。

> **Important**
>
> 如果您指定的預設值為零以外的分鐘數，則必須在中啟用間接關係 AWS Config。否則，您的使用稽核安全性群組原則將無法如預期般運作。如需有關中間接關係的資訊 AWS Config，請參閱AWS Config 開發人員指南 AWS Config中的間接關係。

- 如果您選擇此策略範圍內的安全性群組必須是唯一的，Firewall Manager 會合併多餘的安全性群組，以便只有一個與任何資源相關聯。如果您選擇此選項，Firewall Manager 員會在您儲存策略時先執行它。

10. 對於 Policy action (政策動作)，我們建議建立包含不自動修補選項的政策。這可讓您在套用新政策之前評估其效用。當您確認這些變更正是您所需的時，請編輯政策並變更政策動作，以啟用不合規資源的自動修補。
11. 選擇下一步。
12. 針對AWS 帳戶 此原則適用於，請依下列方式選擇選項：

    - 如果您要將策略套用至組織中的所有帳戶，請保留預設選項「包含我的 AWS 組織下的所有帳戶」。
    - 如果您只想將策略套用至特定 AWS Organizations 組織單位中的特定帳戶或帳號 (OUs)，請選擇 [僅包含指定的帳戶和組織單位]，然後新增您OUs要包含的帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。
    - 如果您要將策略套用至特定帳戶或組織單位 () 以外的所有帳戶或 AWS Organizations 組織單位 (OUs)，請選擇 [排除指定的帳戶和組織單位]，並包含所有其他帳戶，然後新增您OUs要排除的帳號和帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。

    您只能選擇一個選項。

    套用策略後，Firewall Manager 員會根據您的設定自動評估任何新帳號。例如，如果您只包含特定帳戶，則 Firewall Manager 員不會將策略套用至任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子系時OUs，Firewall Manager 會自動將策略套用至新帳戶。
13. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

    如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。

14. 選擇下一步。
15. 如果您尚未從策略範圍中排除 Firewall Manager 員管理員帳戶，則 Firewall Manager 員會提示您執行此操作。這樣做會讓 Firewall Manager 員管理員帳戶中的安全性群組受您手動控制的一般和稽核安全性群組原則所使用。在此對話方塊中選擇您想要的選項。
16. 檢閱政策設定，以確保其為您所需的設定，然後選擇 Create policy (建立政策)。

如果您選擇需要唯一的安全群組，Firewall Manager 員會掃描每個範圍內 Amazon VPC 執行個體中的冗餘安全群組。然後，如果您選擇要求至少一個資源使用每個安全性群組，Firewall Manager 會掃描規則中指定分鐘內未使用的安全性群組。您可以在策略主控台中檢閱 AWS Firewall Manager 策略狀態。如需此政策如何運作的詳細資訊，請參閱 用途稽核安全群組政策。

建立 AWS Firewall Manager 網路ACL原則

如需有關網路ACL原則如何運作的資訊，請參閱網路 ACL 政策。

若要建立網路ACL政策，您必須知道如何定義網路ACL以搭配 Amazon VPC 子網路使用。如需詳細資訊，請參閱 Amazon 使用VPC者指南中的使用網路控制到子網路ACLs的流量ACLs和使用網路。

若要建立網路ACL原則 (主控台)

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對 [原則類型] 選擇 [網路] ACL。
5. 在「區域」中，選擇一個 AWS 區域。
6. 選擇下一步。
7. 在策略名稱中，輸入描述性名稱。

8. 針對策略規則，請定義您要一律在 Firewall Manager 員為您管理ACLs的網路中執行的規則。網路ACLs監控和處理入站和出站流量，因此在您的政策中，您可以定義兩個方向的規則。

   對於任何一個方向，您都可以定義要始終首先執行的規則，以及您希望永遠最後執行的規則。在 Firewall Manager 管理ACLs的網路中，帳戶擁有者可以定義要在這些第一個和最後一個規則之間執行的自訂規則。

9. 針對策略動作，如果您要識別不符合標準的子網路和網路ACLs，但尚未採取任何更正動作，請選擇 [識別不符合策略規則，但不 auto 動修復的資源]。您可以稍後變更這些選項。

   如果您想要將原則自動套用至現有範圍內的子網路，請選擇 [自動修復任何不符合標準的資源]。使用此選項，您也可以指定當原則規則的流量處理行為與網路中的自訂規則衝突時，是否強制修復ACL。無論您是否強制修復，Firewall Manager 都會在其規範遵循違規中報告衝突的規則。

10. 選擇下一步。

11. 針對AWS 帳戶 此原則適用於，請依下列方式選擇選項：

    - 如果您要將策略套用至組織中的所有帳戶，請保留預設選項「包含我的 AWS 組織下的所有帳戶」。
    - 如果您只想將策略套用至特定 AWS Organizations 組織單位中的特定帳戶或帳號 (OUs)，請選擇 [僅包含指定的帳戶和組織單位]，然後新增您OUs要包含的帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。
    - 如果您要將策略套用至特定帳戶或組織單位 () 以外的所有帳戶或 AWS Organizations 組織單位 (OUs)，請選擇 [排除指定的帳戶和組織單位]，並包含所有其他帳戶，然後新增您OUs要排除的帳號和帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。

    您只能選擇一個選項。

    套用策略後，Firewall Manager 員會根據您的設定自動評估任何新帳號。例如，如果您只包含特定帳戶，則 Firewall Manager 員不會將策略套用至任何不同的新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子系時OUs，Firewall Manager 會自動將策略套用至新帳戶。

12. 對於資源類型，此設定固定在「子網路」中。

13. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

    如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。

14. 選擇下一步。
15. 檢閱政策設定，以確保其為您所需的設定，然後選擇 Create policy (建立政策)。

Firewall Manager 員會建立策略，並ACLs根據您的設定開始監視和管理範圍內的網路。如需此政策如何運作的詳細資訊，請參閱 網路 ACL 政策。

建立 AWS Firewall Manager 政策 AWS Network Firewall

在 Firewall Manager 員 Network Firewall 策略中，您可以使用您在中管理的規則群組 AWS Network Firewall。如需管理規則群組的詳細資訊，請參閱《Network Firewall 開發人員指南》中的AWS Network Firewall 規則群組。

如需 Firewall Manager 員 Network Firewall 策略的資訊，請參閱AWS Network Firewall 政策。

若要建立 AWS Network Firewall (主控台) 的 Firewall Manager 員策略

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對政策類型，選擇 AWS Network Firewall。
5. 在 [Firewall Manager 類型] 下，選擇您希望防火牆管理員如何管理原則的防火牆。您可以從以下選項中選擇：

   - 分散式-Firewall Manager 員會在策略範圍內的每個VPC端點中建立並維護防火牆端點。
   - 集中式-Firewall Manager 員會在單次檢查中建立和維護端點VPC。
   - 匯入現有防火牆-Firewall Manager 員使用資源集從 Network Firewall 匯入現有的防火牆 如需有關資源集的資訊，請參閱在 Firewall Manager 員中使用資源集。

6. 在「區域」中，選擇一個 AWS 區域。若要保護多個區域中的資源，您必須為每個區域建立個別的政策。
7. 選擇下一步。
8. 在策略名稱中，輸入描述性名稱。Firewall Manager 員會在其建立的 Network Firewall 防火牆和防火牆策略的名稱中包含策略名稱。
9. 在AWS Network Firewall 策略配置中，像在 Network Firewall 中一樣設定防火牆策略。新增無狀態和可設定狀態的規則群組，並指定原則的預設動作。您可以選擇性地設定原則的可設定狀態規則評估順序和預設動作，以及記錄組態。如需有關 Network Firewall 防火牆策略管理的詳細資訊，請參閱AWS Network Firewall《AWS Network Firewall 開發人員指南》中的

   當您建立 Firewall Manager 員 Network Firewall 策略時，Firewall Manager 員會為範圍內的帳戶建立防火牆策略。個別帳戶管理員可以將規則群組新增至防火牆策略，但無法變更您在此處提供的設定。
10. 選擇下一步。
11. 根據您在上一個步驟中選取的防火牆管理類型，執行下列其中一項作業：

    - 如果您使用的是分散式防火牆管理類型，請在「防火牆AWS Firewall Manager 端點位置」下的端點設定中，選擇下列其中一個選項：
      - 自訂端點組態-Firewall Manager 會在您指定的可用區域中，為原則範圍VPC內的每個防火牆建立防火牆。每個防火牆至少包含一個防火牆端點。
        - 在可用區域下，選取要在其中建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 來選取可用區域。
        - 如果您想要提供 Firewall Manager 員在您的防火牆子網路中使用的CIDR封鎖VPCs，它們都必須是 /28 CIDR 個區塊。每行輸入一個圖塊。如果您省略這些項目，Firewall Manager 員會從中提供的 IP 位址為您選擇 IP 位址VPCs。

          > **Note**
          >
          > AWS Firewall Manager Network Firewall 策略會自動進行自動修復，因此您不會在此處看到選擇不 auto 動修復的選項。

      - 自動端點配置-Firewall Manager 員會在可用區域中自動建立防火牆端點，其中包含. VPC
        - 對於「防火牆」端點組態設定，指定 Firewall Manager 員如何管理防火牆端點。我們建議使用多個端點以獲得高可用性。
    - 如果您使用的是集中式防火牆管理類型，請在 [檢查VPC設定] 下的AWS Firewall Manager 端點設定中，輸入檢查VPC擁有者的 AWS 帳戶 VPC ID 以及檢查的識別碼VPC。

- 在可用區域下，選取要在其中建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 來選取可用區域。
- 如果您想要提供 Firewall Manager 員在您的防火牆子網路中使用的CIDR封鎖VPCs，它們都必須是 /28 CIDR 個區塊。每行輸入一個圖塊。如果您省略這些項目，Firewall Manager 員會從中提供的 IP 位址為您選擇 IP 位址VPCs。

> **Note**
>
> AWS Firewall Manager Network Firewall 策略會自動進行自動修復，因此您不會在此處看到選擇不 auto 動修復的選項。

- 如果您使用匯入現有的防火牆防火牆管理類型，請在資源集中新增一或多個資源集。資源集定義您要在此策略中集中管理的組織帳戶所擁有的現有 Network Firewall 防火牆。若要將資源集新增至策略，您必須先使用主控台或建立資源集PutResourceSetAPI。如需有關資源集的資訊，請參閱在 Firewall Manager 員中使用資源集。如需從 Network Firewall 匯入現有防火牆的詳細資訊，請參閱匯入現有防火牆。

12. 選擇下一步。
13. 如果您的策略使用分散式防火牆管理類型，請在「路由管理」下，選擇「Firewall Manager」是否會監控和警示必須透過個別防火牆端點路由傳送的流量。

> **Note**
>
> 如果您選擇「監視」，日後無法將設定變更為「關閉」。監視會繼續進行，直到您刪除原則為止

14. 對於流量類型，選擇性地新增要路由傳送流量的流量端點，以進行防火牆檢查。
15. 針對 [允許必要的跨可用區域流量]，如果您啟用此選項，則 Firewall Manager 會將流量從可用區域傳送流量以進行檢查的合規路由，針對沒有自己防火牆端點的可用區域視為合規路由。具有端點的可用區域必須一律檢查其自己的流量。
16. 選擇下一步。
17. 針對策略範圍，在AWS 帳戶 此原則適用於下方，選擇如下選項：

- 如果您要將策略套用至組織中的所有帳戶，請保留預設選項「包含我的 AWS 組織下的所有帳戶」。

- 如果您只想將策略套用至特定 AWS Organizations 組織單位中的特定帳戶或帳號 (OUs)，請選擇 [僅包含指定的帳戶和組織單位]，然後新增您OUs要包含的帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。
- 如果您要將策略套用至特定帳戶或組織單位 () 以外的所有帳戶或 AWS Organizations 組織單位 (OUs)，請選擇 [排除指定的帳戶和組織單位]，並包含所有其他帳戶，然後新增您OUs要排除的帳號和帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。

您只能選擇一個選項。

套用策略後，Firewall Manager 員會根據您的設定自動評估任何新帳號。例如，如果您只包含特定帳戶，則 Firewall Manager 員不會將策略套用至任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子系時OUs，Firewall Manager 會自動將策略套用至新帳戶。

18. Network Firewall 策略的資源類型為VPC。
19. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

    如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

    資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。
20. 選擇下一步。
21. 對於策略標記，請新增任何您要新增至 Firewall Manager 員策略資源的識別標籤。如需標籤的詳細資訊，請參閱使用標籤編輯器。
22. 選擇下一步。
23. 檢閱新的原則設定，並返回需要進行任何調整的頁面。

    當您滿意時，選擇 建立政策。在 [原AWS Firewall Manager 則] 窗格中，應該會列出您的原則。它可能會在帳戶標題下指示「待處理」，並指示「自動補救」設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱檢視 AWS Firewall Manager 原則的符合性資訊。

為 Amazon 路線 53 解析器DNS防火牆創建 AWS Firewall Manager 策略

在 Firewall Manager 員防火DNS牆政策中，您可以使用在 Amazon Route 53 解析器DNS防火牆中管理的規則群組。如需管理規則群組的相關資訊，請參閱 Amazon Route 53 開發人員指南中的「在DNS防火牆中管理規則群組和規則」。

如需 Firewall Manager 員防火DNS牆策略的資訊，請參閱Amazon 路線 53 解析器 DNS 防火牆政策。

為 Amazon Route 53 解析器防火牆 (主控台) 建立 DNS Firewall Manager 員政策

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對策略類型，選擇Amazon Route 53 Resolver DNS防火牆。
5. 在「區域」中，選擇一個 AWS 區域。若要保護多個區域中的資源，您必須為每個區域建立個別的政策。
6. 選擇下一步。
7. 在策略名稱中，輸入描述性名稱。
8. 在原則組態中，新增您希望DNS防火牆在您的規則群組關聯中首先和最後評估VPCs的規則群組。您最多可以將兩個規則群組新增至策略。

   當您建立 Firewall Manager 員DNS防火牆策略時，Firewall Manager 會為範圍內的VPCs和帳戶建立規則群組關聯，以及您所提供的關聯優先順序。個別帳戶管理員可以在您的第一個和最後一個關聯之間新增規則群組關聯，但無法變更您在此處定義的關聯。如需詳細資訊，請參閱 Amazon 路線 53 解析器 DNS 防火牆政策。
9. 選擇下一步。
10. 針對AWS 帳戶 此原則適用於，請依下列方式選擇選項：

    - 如果您要將策略套用至組織中的所有帳戶，請保留預設選項「包含我的 AWS 組織下的所有帳戶」。

- 如果您只想將策略套用至特定 AWS Organizations 組織單位中的特定帳戶或帳號 (OUs)，請選擇 [僅包含指定的帳戶和組織單位]，然後新增您OUs要包含的帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。
- 如果您要將策略套用至特定帳戶或組織單位 () 以外的所有帳戶或 AWS Organizations 組織單位 (OUs)，請選擇 [排除指定的帳戶和組織單位]，並包含所有其他帳戶，然後新增您OUs要排除的帳號和帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。

您只能選擇一個選項。

套用策略後，Firewall Manager 員會根據您的設定自動評估任何新帳號。例如，如果您只包含特定帳戶，則 Firewall Manager 員不會將策略套用至任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子系時OUs，Firewall Manager 會自動將策略套用至新帳戶。

11. DNS防火牆策略的資源類型為VPC。
12. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

    如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

    資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。
13. 選擇下一步。
14. 對於策略標記，請新增任何您要新增至 Firewall Manager 員策略資源的識別標籤。如需標籤的詳細資訊，請參閱使用標籤編輯器。
15. 選擇下一步。
16. 檢閱新的原則設定，並返回需要進行任何調整的頁面。

    當您滿意時，選擇 建立政策。在 [原AWS Firewall Manager 則] 窗格中，應該會列出您的原則。它可能會在帳戶標題下指示「待處理」，並指示「自動補救」設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱檢視 AWS Firewall Manager 原則的符合性資訊。

建立帕洛阿爾托網路雲端 AWS Firewall Manager 原則 NGFW

使用帕洛阿爾托網絡雲下一代防火牆（帕洛阿爾托網絡雲NGFW）的 Firewall Manager 器策略，您可以使用 Firewall Manager 器部署帕洛阿爾托網絡雲NGFW資源，並在所有帳戶中集中管理NGFW規則堆棧。 AWS

如需有關 Firewall Manager 員帕洛阿爾托網路雲端NGFW政策的資訊，請參閱帕洛奧圖網路雲端新世代防火牆政策。有關如何配置和管理帕洛阿爾托網絡雲 Firewall Manager 器NGFW的信息，請參閱帕洛阿爾托網絡帕洛阿爾托網絡雲NGFW的文檔。 AWS

必要條件

為 AWS Firewall Manager準備您的帳戶有幾個必要的步驟。AWS Firewall Manager 前提 說明這些步驟。繼續進行下一個步驟之前，請先完成所有先決條件。

建立帕洛阿爾托網路雲端的 Firewall Manager 員政策 NGFW (主控台)

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對「原則類型」，選擇「帕洛奧圖網路雲端 NGFW」。如果您尚未在 AWS Marketplace 上訂閱帕洛阿爾托網絡雲NGFW服務，則需要先這樣做。若要在 AWS Marketplace 中訂閱，請選擇 [檢視 AWS Marketplace 詳細資料]。
5. 對於部署模型，請選擇分散式模型或集中式模型。部署模型會決定 Firewall Manager 員如何管理策略的端點。使用分散式模型時，Firewall Manager 員會在策略範圍內的每VPC個端點中維護防火牆端點。使用集中式模型，Firewall Manager 員會在檢查中維護單一端點VPC。
6. 在「區域」中，選擇一個 AWS 區域。若要保護多個區域中的資源，您必須為每個區域建立個別的政策。
7. 選擇下一步。
8. 在策略名稱中，輸入描述性名稱。

9. 在原則組態中，選擇要與此原則建立關聯的 Palo Alto 網路雲端NGFW防火牆原則。帕洛阿爾托網路雲端NGFW防火牆政策清單包含與您的帕洛阿爾托網路雲端租用戶相關聯的所有帕洛阿爾托網路雲端NGFW防火牆政策。NGFW如需有關建立和管理帕洛阿爾托網路雲端NGFW防火牆原則的資訊，請參閱部署帕洛阿爾托網路雲端NGFW部署指南中的 AWS Firewall Manager主題 AWS與部署指南中NGFW的 AWS 主題。
10. 對於帕洛奧圖網路雲端NGFW記錄-選用，選擇性地選擇要為您的政策記NGFW錄的帕羅奧圖網路雲端記錄類型。如需帕洛阿爾托網路雲端記錄NGFW檔類型的相關資訊，請參閱在帕洛阿爾托網路雲端NGFW部署指南 AWS中設定帕洛阿爾托網路雲端NGFW的 AWS 記錄。

    若為記錄目的地，請指定 Firewall Manager 員應將記錄檔寫入的時間
11. 選擇下一步。
12. 在 [設定協力廠商防火牆端點] 底下，執行下列其中一項動作，視您使用的是分散式或集中式部署模型來建立防火牆端點而定：

    - 如果您針對此原則使用分散式部署模型，請在可用區域下選取要在其中建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 來選取可用區域。
    - 如果您要針對此原則使用集中式部署模型，請在 [檢查設VPC定] 下的AWS Firewall Manager 端點設定中，輸入檢VPC查擁有者的 AWS 帳戶識別碼以及檢查的VPC識別碼VPC。
        - 在可用區域下，選取要在其中建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 來選取可用區域。
13. 如果您想要提供 Firewall Manager 員在您的防火牆子網路中使用的CIDR封鎖VPCs，它們都必須是 /28 CIDR 個區塊。每行輸入一個圖塊。如果您省略這些項目，Firewall Manager 員會從中提供的 IP 位址為您選擇 IP 位址VPCs。

    > **Note**
    >
    > AWS Firewall Manager Network Firewall 策略會自動進行自動修復，因此您不會在此處看到選擇不 auto 動修復的選項。
14. 選擇下一步。
15. 針對策略範圍，在AWS 帳戶 此原則適用於下方，選擇如下選項：

    - 如果您要將策略套用至組織中的所有帳戶，請保留預設選項「包含我的 AWS 組織下的所有帳戶」。

- 如果您只想將策略套用至特定 AWS Organizations 組織單位中的特定帳戶或帳號 (OUs)，請選擇 [僅包含指定的帳戶和組織單位]，然後新增您OUs要包含的帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。
- 如果您要將策略套用至特定帳戶或組織單位 () 以外的所有帳戶或 AWS Organizations 組織單位 (OUs)，請選擇 [排除指定的帳戶和組織單位]，並包含所有其他帳戶，然後新增您OUs要排除的帳號和帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。

您只能選擇一個選項。

套用策略後，Firewall Manager 員會根據您的設定自動評估任何新帳號。例如，如果您只包含特定帳戶，則 Firewall Manager 員不會將策略套用至任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子系時OUs，Firewall Manager 會自動將策略套用至新帳戶。

16. Network Firewall 策略的資源類型為VPC。
17. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

    如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

    資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。
18. 對於授予跨帳戶存取權，請選擇 [下載 AWS CloudFormation 範本]。這會下載可用來建立 AWS CloudFormation 堆疊的 AWS CloudFormation 範本。該堆棧創建一個 AWS Identity and Access Management 角色，授予 Firewall Manager 器跨帳戶權限來管理帕洛阿爾托網絡雲NGFW資源。如需有關堆疊的資訊，請參閱使用指南中的AWS CloudFormation 使用堆疊。
19. 選擇下一步。
20. 對於策略標記，請新增任何您要新增至 Firewall Manager 員策略資源的識別標籤。如需標籤的詳細資訊，請參閱使用標籤編輯器。
21. 選擇下一步。
22. 檢閱新的原則設定，並返回需要進行任何調整的頁面。

    當您滿意時，選擇 建立政策。在 [原AWS Firewall Manager 則] 窗格中，應該會列出您的原則。它可能會在帳戶標題下指示「待處理」，並指示「自動補救」設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱檢視 AWS Firewall Manager 原則的符合性資訊。

建立 Fortigate 雲端原生防火牆 (CNF) 即服務的原 AWS Firewall Manager 則

使用 Fortigate 的 Firewall Manager 員策略CNF，您可以使用 Firewall Manager 器在所有帳戶中部署和管理 Fortigate CNF 資源。 AWS

如需 Firewall Manager 員 Fortigate CNF 策略的相關資訊，請參閱。強制雲端原生防火牆 (CNF) 即服務政策如需如何設定 Fortigate 以搭配 Firewall Manager 員使用的CNF詳細資訊，請參閱 For tinet 文件。

必要條件

為 AWS Firewall Manager準備您的帳戶有幾個必要的步驟。AWS Firewall Manager 前提 說明這些步驟。繼續進行下一個步驟之前，請先完成所有先決條件。

建立 FortigateCNF（主控台）的 Firewall Manager 員策略

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇建立政策。
4. 針對策略類型，選擇 Fortigate 雲端原生防火牆 (CNF) 即服務。如果您尚未在 AWS Marketplace 中訂閱 Fortigate CNF 服務，則需要先進行訂閱。若要在 AWS Marketplace 中訂閱，請選擇 [檢視 AWS Marketplace 詳細資料]。
5. 對於部署模型，請選擇分散式模型或集中式模型。部署模型會決定 Firewall Manager 員如何管理策略的端點。使用分散式模型時，Firewall Manager 員會在策略範圍內的每VPC個端點中維護防火牆端點。使用集中式模型，Firewall Manager 員會在檢查中維護單一端點VPC。
6. 在「區域」中，選擇一個 AWS 區域。若要保護多個區域中的資源，您必須為每個區域建立個別的政策。
7. 選擇下一步。
8. 在策略名稱中，輸入描述性名稱。

9. 在策略配置中，選擇要與此策略關聯的 Fortigate CNF 防火牆策略。Fortigate CNF 防火牆策略的清單包含與 Fortigate 租用戶相關聯的所有 Fortigate CNF 防火牆策略。CNF如需建立和管理 Fortigate CNF 租用戶的相關資訊，請參閱 For tinet 說明文件。
10. 選擇下一步。
11. 在 [設定協力廠商防火牆端點] 底下，執行下列其中一項動作，視您使用的是分散式或集中式部署模型來建立防火牆端點而定：

    - 如果您針對此原則使用分散式部署模型，請在可用區域下選取要在其中建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 來選取可用區域。
    - 如果您要針對此原則使用集中式部署模型，請在 [檢查設VPC定] 下的AWS Firewall Manager 端點設定中，輸入檢VPC查擁有者的 AWS 帳戶識別碼以及檢查的VPC識別碼VPC。
      - 在可用區域下，選取要在其中建立防火牆端點的可用區域。您可以依可用區域名稱或可用區域 ID 來選取可用區域。
12. 如果您想要提供 Firewall Manager 員在您的防火牆子網路中使用的CIDR封鎖VPCs，它們都必須是 /28 CIDR 個區塊。每行輸入一個圖塊。如果您省略這些項目，Firewall Manager 員會從中提供的 IP 位址為您選擇 IP 位址VPCs。

    > **Note**
    >
    > AWS Firewall Manager Network Firewall 策略會自動進行自動修復，因此您不會在此處看到選擇不 auto 動修復的選項。

13. 選擇下一步。
14. 針對策略範圍，在AWS 帳戶 此原則適用於下方，選擇如下選項：

    - 如果您要將策略套用至組織中的所有帳戶，請保留預設選項「包含我的 AWS 組織下的所有帳戶」。
    - 如果您只想將策略套用至特定 AWS Organizations 組織單位中的特定帳戶或帳號 (OUs)，請選擇 [僅包含指定的帳戶和組織單位]，然後新增您OUs要包含的帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。
    - 如果您要將策略套用至特定帳戶或組織單位 () 以外的所有帳戶或 AWS Organizations 組織單位 (OUs)，請選擇 [排除指定的帳戶和組織單位]，並包含所有其他帳戶，然後新增您OUs要排除的帳號和帳號。指定 OU 等同於指定 OU 及其任何子系中的所有帳戶OUs，包括稍後新增的任何子系帳戶OUs和帳戶。

    您只能選擇一個選項。

套用策略後，Firewall Manager 員會根據您的設定自動評估任何新帳號。例如，如果您只包含特定帳戶，則 Firewall Manager 員不會將策略套用至任何新帳戶。另一個範例是，如果您包含 OU，當您將帳戶新增至 OU 或其任何子系時OUs，Firewall Manager 會自動將策略套用至新帳戶。

15. Network Firewall 策略的資源類型為VPC。
16. 對於 Resources，您可以使用標記來縮小策略的範圍，方法是包含或排除具有指定標籤的資源。您可以使用包含或排除，而不能同時使用兩者。如需標籤的詳細資訊，請參閱使用標籤編輯器。

    如果您輸入多個標籤，資源必須具有所有標籤才會被包含或排除。

    資源標籤只能有非空值。如果您省略標籤的值，「Firewall Manager 員」會以空白字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。
17. 對於授予跨帳戶存取權，請選擇 [下載 AWS CloudFormation 範本]。這會下載可用來建立 AWS CloudFormation 堆疊的 AWS CloudFormation 範本。此堆棧創建一個 AWS Identity and Access Management 角色，該角色授予 Firewall Manager 器跨帳戶管理 Forti CNF gate 資源的權限。如需有關堆疊的資訊，請參閱使用指南中的AWS CloudFormation 使用堆疊。若要建立堆疊，您需要 Fortigate CNF 入口網站提供的帳號 ID。
18. 選擇下一步。
19. 對於策略標記，請新增任何您要新增至 Firewall Manager 員策略資源的識別標籤。如需標籤的詳細資訊，請參閱使用標籤編輯器。
20. 選擇下一步。
21. 檢閱新的原則設定，並返回需要進行任何調整的頁面。

    當您滿意時，選擇 建立政策。在 [原AWS Firewall Manager 則] 窗格中，應該會列出您的原則。它可能會在帳戶標題下指示「待處理」，並指示「自動補救」設定的狀態。原則可能需要幾分鐘的時間建立。在 Pending (待定) 狀態被帳戶計數取代後，您可以選擇政策名稱，以探索帳戶和資源的合規狀態。如需相關資訊，請參閱檢視 AWS Firewall Manager 原則的符合性資訊。

刪除 AWS Firewall Manager 策略

您可以執行以下步驟刪除防火牆管理員政策。

刪除政策 (主控台)

1. 在導覽窗格中，選擇 Security policies (安全群組政策)。
2. 選擇您要刪除的政策旁邊的選項。

3. 選擇刪除。

> **Note**
>
> 當您刪除 Firewall Manager 一般安全性群組原則時，若要移除原則的複本安全性群組，請選擇清除原則所建立之資源的選項。否則，刪除主要執行個體後，複本會保留，並且需要在每個 Amazon VPC 執行個體中進行手動管理。

> **Important**
>
> 當您刪除 Firewall Manager 員防護進階策略時，該策略會被刪除，但您的帳號仍然訂閱了 Shield Advanced。

AWS Firewall Manager 政策範圍

原則範圍會定義原則的套用位置。您可以將集中控制的政策套用至組織內的所有帳戶和資源 AWS Organizations，或套用至帳戶和資源的子集。如需有關如何設定原則範圍的指示，請參閱建立 AWS Firewall Manager 策略。

政策範圍選項 AWS Firewall Manager

當您將新的帳號或資源新增至組織時，Firewall Manager 會根據每個策略的設定自動評估該帳號或資源，並根據這些設定套用策略。例如，您可以選擇將策略套用至指定清單中的帳號以外的所有帳號；您也可以選擇僅將策略套用至清單中包含所有標籤的資源。

AWS 帳戶 在範圍內

您提供用來定義受策略 AWS 帳戶 影響的設定會決定組 AWS 織中要套用策略的哪些帳號。您可以透過下列方式之一套用政策：

- 套用至您組織中的所有帳戶
- 僅套用至特定包含帳戶號碼與 AWS Organizations 組織單位 (OU) 的清單
- 套用至特定排除帳戶號碼和 AWS Organizations 組織單位 (OU) 之外所有項目的清單

若要取得有關資訊 AWS Organizations，請參閱AWS Organizations 使用指南。

範圍內的資源

與範圍中帳號的設定類似，您為資源提供的設定會決定要套用策略的範圍內資源類型。您可以選擇下列其中之一：

- 所有 資源
- 具有您指定之所有標籤的資源
- 除了具有您指定之所有標籤的資源以外的所有資源

您只能指定具有非空值的資源標籤。如果您未提供任何值，「Firewall Manager 員」會以空字串值儲存標籤：「」。資源標籤僅與具有相同鍵和相同值的標籤匹配。

如需標記資源的詳細資訊，請參閱使用標籤編輯器。

政策範圍管理 AWS Firewall Manager

策略到位時，Firewall Manager 會根據策略範圍持續管理這些策略， AWS 帳戶 並在新增時將它們套用至新增的資源和資源。

Firewall Manager 員如何管理 AWS 帳戶 和資源

如果帳號或資源因任何原因超出範圍，則 AWS Firewall Manager 不會自動移除保護或刪除防火牆管理員管理的資源，除非您選取 [從離開策略範圍的資源自動移除保護] 核取方塊。

> **Note**
>
> [從離開策略範圍的資源自動移除保護] 選項不適用於 AWS Shield Advanced 或 AWS WAF 傳統策略。

選取此核取方塊會指示 AWS Firewall Manager 當這些帳號離開策略範圍時，自動清除 Firewall Manager 為帳號管理的資源。例如，當客戶資源離開策略範圍時，Firewall Manager 將取消 Firewall Manager 員管理的 Web ACL 與受保護的客戶資源的關聯。

若要判斷當客戶資源離開策略範圍時，應從保護中移除哪些資源，Firewall Manager 會遵循下列準則：

- 預設行為：
  - 相關聯的 AWS Config 受管理規則即會刪除。此行為與核取方塊無關。
  - 任何不包含任何資源的相關 AWS WAF Web 存取控制清單 (Web ACL) 都會遭到刪除。此行為與核取方塊無關。

  - 任何超出範圍的受保護資源都會保持關聯並受到保護。例如，與 Web ACL 相關聯的 API Gateway 中的 Application Load Balancer 或 API 會保持與 Web ACL 相關聯，而且保護會保持原位。
- 選取 [從離開策略範圍的資源自動移除保護] 核取方塊時：
  - 相關聯的 AWS Config 受管理規則即會刪除。此行為與核取方塊無關。
  - 任何不包含任何資源的相關 AWS WAF Web 存取控制清單 (Web ACL) 都會遭到刪除。此行為與核取方塊無關。
  - 任何超出範圍的受保護資源在離開策略範圍時，都會自動取消關聯並從 Firewall Manager 員保護中移除。例如，對於安全群組政策，Elastic Inference 加速器或 Amazon EC2 執行個體離開原則範圍時，會自動與複寫的安全群組取消關聯。複製的安全性群組及其資源會自動從保護中移除。

受管理清單

受管理的應用程式和通訊協定清單可簡化 AWS Firewall Manager 內容稽核安全性群組原則的設定與管理 您可以使用受管理的清單來定義原則允許和不允許的通訊協定和應用程式。如需有關內容稽核安全性群組原則的資訊，請參閱內容稽核安全群組政策。

您可以在內容稽核安全性群組原則中使用下列類型的受管理清單：

- Firewall Manager 員應用程式清單和通訊協定清單 — Firewall Manager 員會管理
  - 應用程序列表包括`FMS-Default-Public-Access-Apps-Allowed`和`FMS-Default-Public-Access-Apps-Denied`，它描述了應該允許或拒絕給普通大眾的常用應用程序。
  - 通訊協定清單包括`FMS-Default-Protocols-Allowed`應允許公眾使用的常用通訊協定清單。您可以使用「Firewall Manager 員」管理的任何清單，但無法編輯或刪除它。
- 自訂應用程式清單和通訊協定清單 — 您管理這些清單。您可以使用所需的設置創建任何類型的列表。您可以完全控制自己的自訂受管清單，並且可以視需要建立、編輯和刪除這些清單。

> **Note**
>
> 目前，當您刪除自訂受管理清單時，Firewall Manager 員不會檢查其參考。這表示您可以刪除自訂受管理的應用程式清單或通訊協定清單，即使該清單正由作用中的原則使用中。這可能會造成原則停止運作。只有在確認應用程式清單或通訊協定清單未被任何使用中原則參照之後，才刪除該清單。

受管理的清單是 AWS 資源。您可以標記自訂受管清單。您無法標記 Firewall Manager 員管理清單。

受管理清單版本

自訂受管清單沒有版本。當您編輯自訂清單時，參照該清單的策略會自動使用更新的清單。

Firewall Manager 員管理清單已建立版本化。Firewall Manager 員服務團隊會視需要發佈新版本，以便將最佳安全性做法套用至清單。

當您在策略中使用 Firewall Manager 員受管理的清單時，您可以按如下方式選擇版本控制策略：

- 最新可用版本 — 如果您未為清單指定明確的版本設定，則您的原則會自動使用最新版本。這是通過控制台可用的唯一選項。
- 明確版本 — 如果您為清單指定版本，則您的策略會使用該版本。您的原則會保持鎖定至您指定的版本，直到您修改版本設定為止。若要指定版本，您必須在主控台外部定義原則，例如透過 CLI 或其中一個 SDK。

如需有關為清單選擇版本設定的更多資訊，請參閱在內容稽核安全性群組原則中使用受管理的清單。

在內容稽核安全性群組原則中使用受管理的清單

當您建立內容稽核安全性群組原則時，您可以選擇使用受管理的稽核策略規則。此選項的某些設定需要受管理的應用程式清單或通訊協定清單。這些設定的範例包括安全性群組規則中允許的通訊協定，而應用程式可以存取網際網路。

下列限制適用於使用受管理清單的每個原則設定：

- 您最多可以為任何設定指定一個「Firewall Manager 員」管理清單。依預設，您最多可以指定一個自訂清單。自訂清單限制是軟配額，因此您可以要求增加配額。如需詳細資訊，請參閱 AWS Firewall Manager 配額。
- 在主控台中，如果您選取「Firewall Manager 員」受管理清單，則無法指定版本。政策將永遠使用最新版本的清單。若要指定版本，您必須在主控台外部定義原則，例如透過 CLI 或其中一個 SDK。如需有關「Firewall Manager 員管理清單」之版本控制的資訊受管理清單版本，

如需透過主控台建立內容稽核安全性群組原則的詳細資訊，請參閱建立內容稽核安全群組政策。

建立自訂受管理應用程式清單

建立自訂受管理的應用程式清單

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 [應用程式清單]。
3. 在應用程式清單頁面中，選擇建立應用程式清單。
4. 在 [建立應用程式清單] 頁面中，為您的清單命名。請勿使用前置詞，`fms-`因為這是為 Firewall Manager 員保留的。
5. 提供通訊協定和連接埠號碼，或從類型下拉式清單中選取應用程式，以指定應用程式。為您的應用程式規格命名。
6. 視需要選擇 [新增其他]，然後填寫申請資訊，直到您完成清單為止。
7. (選擇性) 將標籤套用至清單。
8. 選擇 [儲存] 以儲存清單並返回 [應用程式清單] 頁面。

建立自訂受管通訊協定清單

建立自訂受管理的通訊協定清單

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在瀏覽窗格中，選擇 [通訊協定清單]。
3. 在 [協定清單] 頁面中，選擇 [建立通訊協定清單]

4. 在通訊協定清單建立頁面中，為您的清單命名。請勿使用前置詞，fms-因為這是為 Firewall Manager 員保留的。
5. 指定通訊協定。
6. 視需要選擇 [新增其他通訊協定]，然後填入通訊協定資訊，直到您完成清單為止。
7. (選擇性) 將標籤套用至清單。
8. 選擇 [儲存] 以儲存清單並返回 [通訊協定清單] 頁面。

檢視受管理清單

若要檢視應用程式清單或通訊協定清單

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在瀏覽窗格中，選擇 [應用程式清單] 或 [通訊協定清單

   此頁面會顯示可供您使用的所選類型的所有清單。「Firewall Manager 員」管理的清單ManagedList欄中有一個 Y。
3. 若要查看清單的詳細資訊，請選擇其名稱。詳細資訊頁面會顯示清單的內容和任何標籤。

   對於「Firewall Manager 員」管理清單，您也可以選取「版本」下拉式清單來查看可用的版本。

刪除自訂受管清單

您可以刪除自訂受管清單。您無法編輯或刪除 Firewall Manager 員管理的清單。

> **Note**
>
> 目前，當您刪除自訂受管理清單時，Firewall Manager 員不會檢查其參考。這表示您可以刪除自訂受管理的應用程式清單或通訊協定清單，即使該清單正由作用中的原則使用中。這可能會造成原則停止運作。只有在確認應用程式清單或通訊協定清單未被任何使用中原則參考之後，才刪除該清單。

刪除自訂受管理的應用程式或通訊協定清單

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 請執行下列動作，確定您要刪除的清單未在任何稽核安全性群組原則中使用：

   a. 在導覽窗格中，選擇 Security policies (安全群組政策)。

   b. 在AWS Firewall Manager 策略頁面中，選取並編輯您的稽核安全性群組，然後移除您要刪除之自訂清單的任何參考。

      如果您刪除稽核安全性群組原則中正在使用的自訂受管理清單，則使用該清單的原則可能會停止運作。

3. 在導覽窗格中，選擇 [應用程式清單] 或 [通訊協定清單]，視您要刪除的清單類型而定。

4. 在清單頁面中，選取您要刪除的自訂清單，然後選擇 [刪除]。

AWS WAF 政策

在 Firewall Manager 員 AWS WAF 策略中，您可以指定要在資源中使用的 AWS WAF 規則群組。當您套用策略時，Firewall Manager 員會根據您ACLs在策略中設定 Web 管理的方式，ACLs在策略範圍內建立網頁帳戶。在策略ACLs建立的 Web 中，除了透過 Firewall Manager 員定義的規則群組外，個別帳戶管理員還可以新增規則和規則群組。

Firewall Manager 員如何管理 Web ACLs

Firewall Manager 員會ACLs根據您在策略中設定「管理未關聯的 Web」ACLs 設定的方式，或中的SecurityServicePolicyData資料類型中的`optimizeUnassociatedWebACL`設定來建立 Web。API

如果您啟用非關聯網路的管理ACLs，則 Firewall Manager 員只會ACLs在至少一個資源使用 Web 時，才ACLs會在策略範圍內的帳號中建立 Web。如果任何時候有帳戶進入策略範圍，如果至少有一個資源將使用 Web，則 Firewall Manager 員會ACL在帳戶中自動建立網頁ACL。當您啟用非關聯網頁的管理時ACLs，Firewall Manager 會執行一次性清除帳戶ACLs中未關聯的網頁。在清除期間，Firewall Manager 會略過您在建立後修改過的任何網頁ACLs，例如，如果您將規則群組新增至

網頁ACL或修改了其設定。清理過程可能需要幾個小時。如果資源在 Firewall Manager 建立網頁之後離開策略範圍ACL，則 Firewall Manager 員會取消資源與網路的關聯ACL，但不會清除未關聯的網頁。ACL「Firewall Manager 員」只會在您第一次啟用策略中未關聯網頁的管理ACLs時，才會清除未關聯ACLs的網頁。

如果您未啟用此選項，則 Firewall Manager 員不會管理未關聯的網頁ACLs，而且 Firewall Manager 員會ACL在每個位於策略範圍內的帳戶中自動建立網頁。

抽樣和 CloudWatch 指標

AWS Firewall Manager 為其為 AWS WAF 政策建立的 Web ACLs 和規則群組啟用取樣和 Amazon CloudWatch 指標。

網頁ACL命名結構

當「Firewall Manager 員」ACL 為策略建立網頁時，它會為網頁命名 ACL`FMManagedWebACLV2-`*`policy name`*`-`*`timestamp`*。時間戳記以UTC毫秒為單位。例如：`FMManagedWebACLV2-MyWAFPolicyName-1621880374078`。

> **Note**
>
> 如果設定了進階自動應用程式層DDoS緩和措施的資源進入 AWS WAF 策略的範圍，Firewall Manager 將無法將 AWS WAF 原則ACL建立的 Web 與資源建立關聯。

策略中的規 AWS WAF 則群組

由 Firewall Manager 員 AWS WAF 策略管理的 Web ACLs 包含三組規則。這些集合為 Web ACL 中的規則和規則群組提供更高層級的優先順序排定：

- 由您在 Firewall Manager 員 AWS WAF 策略中定義的第一個規則群組。 AWS WAF 首先評估這些規則群組。
- 由 Web 中客戶管理員定義的規則和規則群組ACLs。 AWS WAF 接下來會評估任何帳戶管理的規則或規則群組。
- 您在「Firewall Manager 員」 AWS WAF 策略中定義的最後一個規則群組。 AWS WAF 最後評估這些規則群組。

在這些規則集中，根據規則集中的優先順序設定，如常一樣 AWS WAF 評估規則和規則群組。

在政策的第一個和最後一個規則群組集中，您只能新增規則群組。您可以使用受管規則群組，這些群組 AWS 受管規則和 AWS Marketplace 銷售者會為您建立和維護。您也可以管理和使用自己的規則群組。如需所有這些選項的詳細資訊，請參閱AWS WAF 規則群組。

如果您想要使用自己的規則群組，請先建立這些規則群組，然後再建立 Firewall Manager 員 AWS WAF 原則。如需準則，請參閱管理您自己的規則群組。若要使用個別的自訂規則，您必須定義自己的規則群組、在該群組中定義規則，然後在政策中使用規則群組。

您透過 Firewall Manager 管理的第一個和最後一個 AWS WAF 規則群組的名稱分別以`PREFMManaged-`或開頭`POSTFMManaged-`，後跟 Firewall Manager 員原則名稱，以及規則群組建立時間戳記 (以UTC毫秒為單位)。例如：`PREFMManaged-MyWAFPolicyName-1621880555123`。

如需有關如何 AWS WAF 評估 Web 請求的資訊，請參閱Web ACL 規則和規則群組評估。

如需建立 Firewall Manager 員 AWS WAF 策略的程序，請參閱建立 AWS Firewall Manager 政策 AWS WAF。

Firewall Manager 員會為您為 AWS WAF 政策定義的規則群組啟用取樣和 Amazon CloudWatch 指標。

個別帳戶擁有者可以完全控制他們新增至原則受管理 Web 的任何規則或規則群組的指標和取樣組態 ACLs。

設定 AWS WAF 原則的記錄

您可以為 AWS WAF 原則啟用集中式記錄功能，以取得組織ACL內網路所分析流量的詳細資訊。記錄檔中的資訊包括從您的 AWS 資源 AWS WAF 接收要求的時間、請求的詳細資訊，以及每個要求與所有範圍內帳戶相符之規則的動作。您可以將日誌傳送到 Amazon 資料 Firehose 資料串流或 Amazon Simple Storage Service (S3) 儲存貯體。如需有關 AWS WAF 記錄的資訊，請參閱記錄 AWS WAF 網頁 ACL 流量開AWS WAF 發人員指南中的。

> **Note**
>
> AWS Firewall Manager 支援此選項 AWS WAFV2，而不適用於「 AWS WAF 經典」。

主題

記錄目的地

本節說明您可以選擇傳送 AWS WAF 原則記錄檔的記錄目的地。每節都會提供為目的地類型設定記錄的指引，以及目的地類型專屬行為的相關資訊。設定記錄目的地之後，您可以將其規格提供給您的 Firewall Manager 員 AWS WAF 原則，以開始記錄到該目的地。

建立記錄設定之後，Firewall Manager 員無法看到記錄檔失敗。您有責任確認記錄傳送是否正常運作。

> **Note**
>
> Firewall Manager 員不會修改組織成員帳戶中任何現有的記錄設定。

主題

- Amazon 數據 Firehose 數據流
- Amazon Simple Storage Service 儲存貯體

Amazon 數據 Firehose 數據流

本主題提供將網路ACL流量日誌傳送至 Amazon 資料 Firehose 資料串流的相關資訊。

啟用 Amazon Data Firehose 日誌記錄時，Firewall Manager 員會將日誌從政策的網頁傳送ACLs到您已設定儲存目的地的 Amazon Data Firehose。啟用記錄後，會透過 Kinesis Data Firehose 的HTTPS端點ACL，將每個已設定網路的記錄傳 AWS WAF 送至設定的儲存目的地。在使用之前，請先測試您的交付串流，以確定其輸送量足以容納組織的記錄。如需有關如何建立 Amazon Kinesis Data Firehose 和檢閱儲存的日誌的詳細資訊，請參閱什麼是 Amazon 資料防火管？

您必須具備下列權限，才能成功啟用 Kinesis 的記錄功能：

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

當您在 AWS WAF 政策上設定 Amazon Data Firehose 記錄目的地時，Firewall Manager 員會在 Firewall Manager 員管理員帳戶中ACL為該政策建立網頁，如下所示：

- 無論帳戶是否ACL在策略範圍內，Firewall Manager 員都會在 Firewall Manager 員管理員帳戶中建立 Web。

- Web ACL 已啟用日誌記錄，並帶有日誌名稱FMManagedWebACLV2-Logging*policy name*-*timestamp*，其中UTC時間戳記是為 Web 啟用日誌的時間ACL，以毫秒為單位。例如：FMManagedWebACLV2-LoggingMyWAFPolicyName-1621880565180。Web 沒ACL有規則群組，也沒有關聯的資源。
- 我們會ACL根據 AWS WAF 定價準則向您收取網路費用。如需詳細資訊，請參閱 AWS WAF 定價。
- 當您刪除策略ACL時，Firewall Manager 員會刪除 Web。

如需服務連結角色和iam:CreateServiceLinkedRole權限的相關資訊，請參閱使用服務連結角色 AWS WAF。

如需有關建立交付串流的詳細資訊，請參閱建立 Amazon 資料 Firehose 交付串流。

Amazon Simple Storage Service 儲存貯體

本主題提供將網頁ACL流量日誌傳送到 Amazon S3 儲存貯體的相關資訊。

您選擇作為記錄目的地的值區必須由 Firewall Manager 員管理員帳戶擁有。如需針對日誌記錄和儲存貯體命名要求建立 Amazon S3 儲存貯體的相關要求的詳細資訊，請參閱AWS WAF 開發人員指南中的Amazon 簡單儲存體服務。

最終一致性

當您變更使用 Amazon S3 記錄目標設定的政 AWS WAF 策時，Firewall Manager 員會更新儲存貯體政策以新增記錄所需的許可。這樣做時，Firewall Manager 員會遵循 Amazon 簡單儲存服務遵循的 last-writer-wins 語意和資料一致性模型。如果您在 Firewall Manager 員主控台或透過同時對 Amazon S3 目的地進行多個政策更新 PutPolicyAPI，則可能無法儲存某些許可。如需 Amazon S3 資料一致性模型的詳細資訊，請參閱 Amazon S3 資料一致性模型，其中的 Amazon 簡單儲存服務使用者指南。

將日誌發佈到 Amazon S3 儲存貯體的許可

在 AWS WAF 政策中設定 Amazon S3 儲存貯體的 Web ACL 流量記錄需要以下許可設定。當您將 Amazon S3 設定為記錄目的地時，Firewall Manager 員會自動將這些許可附加到 Amazon S3 儲存貯體，以授予將日誌發佈到儲存貯體的服務權限。如果您想要管理更精細的記錄和 Firewall Manager 員資源存取權限，您可以自行設定這些權限。如需有關管理權限的資訊，請參閱《IAM使用指南》中的 AWS 資源存取管理。如需有關 AWS WAF 受管理策略的資訊，請參閱AWS 受管理的政策 AWS WAF。

```
{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryForFirewallManager",
```

```
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheckFMS",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::aws-waf-amzn-s3-demo-bucket"
        },
        {
            "Sid": "AWSLogDeliveryWriteFMS",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::aws-waf-logs-amzn-s3-demo-bucket/policy-id/
AWSLogs/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

為了防止跨服務混淆的副問題，您可以將aws:SourceArn和aws:SourceAccount全局條件上下文鍵添加到存儲桶的策略中。若要新增這些金鑰，您可以在設定記錄目的地時修改 Firewall Manager 為您建立的原則，或者如果您想要精細控制，您可以建立自己的原則。如果您將這些條件新增至記錄目的地原則，Firewall Manager 將不會驗證或監視混淆的副保護。有關混淆副問題的一般信息，請參閱混淆的副問題 在《IAM使用者指南》中。

當您添加sourceAccount添加sourceArn屬性時，它將增加存儲桶策略大小。如果您要新增一長串sourceAccount新增sourceArn屬性，請注意不要超過 Amazon S3 儲存貯體政策大小配額。

下列範例說明如何在值區政策中使用aws:SourceArn和aws:SourceAccount全域條件內容索引鍵，以避免混淆的副問題。Replace (取代) *member-account-id* 與您組織中IDs的成員帳戶。

```
{
   "Version":"2012-10-17",
```

```
   "Id":"AWSLogDeliveryForFirewallManager",
   "Statement":[
      {
         "Sid":"AWSLogDeliveryAclCheckFMS",
         "Effect":"Allow",
         "Principal":{
            "Service":"delivery.logs.amazonaws.com"
         },
         "Action":"s3:GetBucketAcl",
         "Resource":"arn:aws:s3:::aws-waf-logs-amzn-s3-demo-bucket",
         "Condition":{
            "StringEquals":{
               "aws:SourceAccount":[
                  "member-account-id",
                  "member-account-id"
               ]
            },
            "ArnLike":{
               "aws:SourceArn":[
                  "arn:aws:logs:*:member-account-id:*",
                  "arn:aws:logs:*:member-account-id:*"
               ]
            }
         }
      },
      {
         "Sid":"AWSLogDeliveryWriteFMS",
         "Effect":"Allow",
         "Principal":{
            "Service":"delivery.logs.amazonaws.com"
         },
         "Action":"s3:PutObject",
         "Resource":"arn:aws:s3:::aws-waf-logs-amzn-s3-demo-bucket/policy-id/AWSLogs/
*",
         "Condition":{
            "StringEquals":{
               "s3:x-amz-acl":"bucket-owner-full-control",
               "aws:SourceAccount":[
                    "member-account-id",
                  "member-account-id"
               ]
            },
            "ArnLike":{
               "aws:SourceArn":[
```

```
                "arn:aws:logs:*:member-account-id-1:*",
                "arn:aws:logs:*:member-account-id-2:*"
            ]
        }
    }
  }
]
}
```

Amazon S3 儲存貯體的伺服器端加密

您可以啟用 Amazon S3 伺服器端加密，或在 S3 儲存貯體上使用 AWS Key Management Service 客戶受管金鑰。如果您選擇在 Amazon S3 儲存貯體上對 AWS WAF 日誌使用預設的 Amazon S3 加密，則不需要採取任何特殊動作。但是，如果您選擇使用客戶提供的加密金鑰來加密 Amazon S3 靜態資料，則必須在 AWS Key Management Service 金鑰政策中新增以下許可聲明：

```
{
            "Sid": "Allow Logs Delivery to use the key",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
}
```

如需將客戶提供的加密金鑰與 Amazon S3 搭配使用的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用伺服器端加密搭配客戶提供的金鑰 (SSE-C)。

啟用記錄

下列程序說明如何在 Firewall Manager 員主控台中啟用 AWS WAF 策略的記錄功能。

若要啟用 AWS WAF 原則的記錄功能

1. 啟用記錄之前，您必須設定記錄目的地資源，如下所示：

- Amazon Kinesis Data Streams-使用您的防 Firehose 理員帳戶建立 Amazon 資料防火軟管。使用以前綴開頭的名稱`aws-waf-logs-`。例如：`aws-waf-logs-firewall-manager-central`。使用PUT源和您正在運營的區域中創建數據防火軟管。如果您要擷取 Amazon 的日誌 CloudFront，請在美國東部 (維吉尼亞北部) 建立 Firehose。在使用之前，請先測試您的交付串流，以確定其輸送量足以容納組織的記錄。如需詳細資訊，請參閱建立 Amazon 資料 Firehose 交付串流。
- Amazon 簡單儲存服務儲存貯體-根據AWS WAF 開發人員指南中 Amazon 簡單儲存服務主題中的準則建立 Amazon S3 儲存貯體。您還必須使用中列出的許可設定 Amazon S3 儲存貯體將日誌發佈到 Amazon S3 儲存貯體的許可 。

2. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

> **Note**
>
> 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

3. 在瀏覽窗格中，選擇 [安全性原則]。
4. 選擇您要啟用記錄的 AWS WAF 原則。如需有關 AWS WAF 記錄的詳細資訊，請參閱 記錄 AWS WAF 網頁 ACL 流量。
5. 在 [原則詳細資料] 索引標籤的 [原則規則] 區段中，選擇 [編輯]。
6. 對於記錄組態，請選擇啟用記錄以開啟記錄。記錄可提供有關 Web 分析流量的詳細資訊ACL。選擇記錄目的地，然後選擇您設定的記錄目的地。您必須選擇名稱開頭的記錄目的地`aws-waf-logs-`。如需有關設定 AWS WAF 記錄目的地的資訊，請參閱設定 AWS WAF 原則的記錄。
7. (選用) 如果您不想要特定欄位及其值包含在日誌中，請編寫這些欄位。選擇要編寫的欄位，然後選擇新增。重複其他需要編寫的欄位。在日誌中編寫的欄位顯示為 REDACTED。例如，如果您編輯URI欄位，記錄中的URI欄位將會是REDACTED。
8. (選擇性) 如果您不想將所有要求傳送至記錄檔，請新增篩選條件和行為。在「篩選記錄檔」下方，針對您要套用的每個篩選器，選擇「新增篩選器」，然後選擇您的篩選條件，並指定要保留或刪除符合條件的要求。完成新增篩選器後，如有需要，請修改預設記錄行為。如需詳細資訊，請參閱《AWS WAF 開發人員指南》中的 網頁 ACL 記錄設定。
9. 選擇 Next (下一步)。
10. 檢閱您的設定，然後選擇 [儲存] 以儲存對策略的變更。

停用記錄

下列程序說明如何在 Firewall Manager 員主控台中停用 AWS WAF 策略的記錄。

若要停用 AWS WAF 原則的記錄

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在瀏覽窗格中，選擇 [安全性原則]。
3. 選擇您要停用記錄的 AWS WAF 原則。
4. 在 [原則詳細資料] 索引標籤的 [原則規則] 區段中，選擇 [編輯]。
5. 在「記錄」組態狀態中，選擇「停用」
6. 選擇 Next (下一步)。
7. 檢閱您的設定，然後選擇 [儲存] 以儲存對策略的變更。

AWS Shield Advanced 政策

在 Firewall Manager 員 AWS Shield 策略中，您可以選擇要保護的資源。當您套用原則並啟用 auto 修復時，Firewall Manager 員會為每個尚未與 AWS WAF Web ACL 關聯的範圍內資源建立關聯。 AWS WAF 空的腹板 ACL 用於 Shield 監視目的。如果您接著將任何其他 Web ACL 與資源建立關聯，則 Firewall Manager 員會移除空的 Web ACL 關聯。

> **Note**
>
> 當 AWS WAF 策略範圍內的資源進入使用自動應用程式層 DDoS 緩解設定的 Shield Advanced 策略的範圍時，Firewall Manager 員只會在與原 AWS WAF 則建立的 Web ACL 產生關聯之後才套用 Shield 牌進階防護。

如何在 Shield 牌政策中 AWS Firewall Manager 管理非關聯的網頁 ACL

您可以透過原則中的 [管理未關聯的 Web ACL] 設定，設定 Firewall Manager 員是否為您管理非關聯的 Web ACL，或是 API 中SecurityServicePolicyData資料類型中的`optimizeUnassociatedWebACLs`設定。如果您在策略中啟用管理未關聯的 Web ACL，則 Firewall Manager 員只會在至少一個資源使用 Web ACL 時，才會在策略範圍內的帳號中建立 Web ACL。如果任何時候有帳號進入策略範圍，如果至少有一個資源將使用 Web ACL，則 Firewall Manager 員會在帳號中自動建立 Web ACL。

當您啟用非關聯 Web ACL 的管理時，Firewall Manager 員會執行一次性清除帳戶中未關聯的 Web ACL。清理過程可能需要幾個小時。如果資源在 Firewall Manager 員建立 Web ACL 之後離開策略範圍，則 Firewall Manager 員不會取消資源與 Web ACL 的關聯。如果您希望 Firewall Manager 員清除 Web ACL，您必須先手動取消資源與 Web ACL 的關聯，然後在策略中啟用管理未關聯的 Web ACL 選項。

如果您未啟用此選項，則 Firewall Manager 員不會管理未關聯的 Web ACL，而且 Firewall Manager 員會在策略範圍內的每個帳戶中自動建立 Web ACL。

如何 AWS Firewall Manager 管理護 Shield 政策中的範圍變更

帳號和資源可能會超出 AWS Firewall Manager Shield Advanced 策略的範圍，這是因為許多變更，例如政策範圍設定變更、資源上的標籤變更，以及從組織移除帳號。如需有關策略範圍設定的一般資訊，請參閱AWS Firewall Manager 政策範圍。

使用 AWS Firewall Manager Shield 進階策略時，如果帳號或資源超出範圍，Firewall Manager 員就會停止監視帳號或資源。

如果帳號因從組織中移除而超出範圍，該帳號將會繼續訂閱 Shield 牌進階版。由於該帳戶不再是合併帳單系列的一部分，因此該帳戶將產生按比例分配的 Shield Advanced 訂閱費用。另一方面，超出範圍但仍在組織中的帳戶不會產生額外費用。

如果資源超出範圍，則會繼續受到「Shield 牌進階」的保護，並繼續產生「Shield 牌進階」資料傳輸費用。

自動化應用程式層 DDoS 防護

將 Shield 進階政策套用至 Amazon CloudFront 分發或應用程式負載平衡器時，您可以選擇在政策中設定 Shield 進階自動應用程式層 DDoS 緩解措施。

如需有關防 Shield 進階自動緩和的資訊，請參閱Shield 先進的自動應用層 DDoS 緩解。

Shield 高級自動應用層 DDoS 緩解具有以下要求：

- 自動應用程式層 DDoS 緩解功能僅適用於 Amazon CloudFront 分發和應用程式負載平衡器。

  如果將您的 Shield 進階政策套用至 Amazon CloudFront 分發，您可以針對為全球區域建立的 Shield 進階政策選擇此選項。如果將保護套用至應用程式負載平衡器，您可以將原則套用至 Firewall Manager 員支援的任何區域。

- 自動應用程式層 DDoS 防護功能僅適用於使用最新版本的 AWS WAF (v2) 建立的 Web ACL。

  因此，如果您有使用 AWS WAF 傳統 Web ACL 的原則，您必須使用新原則來取代原則，這會自動使用最新版本的原則 AWS WAF，或讓 Firewall Manager 員為您現有的原則建立新版 Web ACL，然後切換至使用這些原則。如需選項的詳細資訊，請參閱 以最新版本的網頁 ACL 取代 AWS WAF 傳統網頁 ACL。

自動緩解組態

Firewall Manager 員 Shield 進階政策的自動應用程式層 DDoS 緩解選項可將 Shield 進階自動緩解功能套用至您政策範圍內的帳戶和資源。如需此 Shield 進階功能的詳細資訊，請參閱Shield 先進的自動應用層 DDoS 緩解。

您可以選擇讓 Firewall Manager 針對原則範圍內的 CloudFront散佈或應用程式負載平衡器啟用或停用自動緩和措施，也可以選擇讓原則忽略 Shield Advanced 自動緩和措施設定：

- 啟用 — 如果您選擇啟用自動緩和措施，您也可以指定緩和 Shield Advanced 規則是否應該計數或封鎖相符的 Web 請求。如果範圍內的資源未啟用自動緩解措施，或者使用的規則動作與您為策略指定的動作不符，Firewall Manager 會將其標記為不符合標準。如果您設定自動修復的策略，則 Firewall Manager 員會視需要更新不符合標準的資源。
- 停用 — 如果您選擇停用自動緩和措施，Firewall Manager 會在範圍內的資源標示為不相容 (如果已啟用自動緩和措施)。如果您設定自動修復的策略，則 Firewall Manager 員會視需要更新不符合標準的資源。
- 略過 — 如果您選擇忽略自動緩和措施，則 Firewall Manager 在為策略執行修復活動時，不會考慮 Shield 策略中的任何自動緩和措施設定。此設定可讓您透過 Shield Advanced 控制自動緩和措施，而不會讓 Firewall Manager 員覆寫這些設定。此設定不適用於透過 Shield Advanced 管理的任何傳統負載平衡器或彈性 IP 資源，因為 Shield Advanced 目前不支援這些資源的 L7 自動緩解功能。

以最新版本的網頁 ACL 取代 AWS WAF 傳統網頁 ACL

自動應用程式層 DDoS 防護功能僅適用於使用最新版本的 AWS WAF (v2) 建立的 Web ACL。

若要判斷 Shield 進階政策的網頁 ACL 版本，請參閱判斷 Shield 牌進階政策所使用的 AWS WAF 版本。

如果您想要在 Shield Advanced 原則中使用自動緩和措施，而您的原則目前使用 AWS WAF 傳統 Web ACL，您可以建立新的 Shield 牌進階政策來取代您目前的防護進階政策，或者您可以使用本節所述的選項，將舊版 Web ACL 取代為目前的防 Shield 進階政策中的新 (v2) Web ACL。新原則一律使用最新版本的 AWS WAF建立 Web ACL。如果您取代整個原則，當您刪除它時，您也可以讓 Firewall Manager 員刪除所有舊版 Web ACL。本節的其餘部分說明您在現有政策中取代 Web ACL 的選項。

當您修改 Amazon CloudFront 資源的現有防 Shield 進階政策時，Firewall Manager 員可以在任何尚未具有 v2 Web ACL 的範圍內帳戶中，為該政策自動建立新的空白 AWS WAF (v2) Web ACL。當 Firewall Manager 員建立新的 Web ACL 時，如果策略在相同帳戶中已經有 AWS WAF 典型 Web ACL，則 Firewall Manager 員會使用與現有 Web ACL 相同的預設處理行動設定來設定新版 Web ACL。如果沒有現有的 AWS WAF 傳統 Web ACL，「Firewall Manager 員」會在新的 Web ACL Allow 中將預設處理行動設定為。Firewall Manager 員建立新的 Web ACL 之後，您可以視需要透過 AWS WAF 主控台自訂它。

當您選擇下列任一原則組態選項時，Firewall Manager 員會為尚未擁有的範圍內帳戶建立新的 (v2) Web ACL：

- 啟用或停用自動應用程式層 DDoS 緩解時。僅此選項只會導致 Firewall Manager 員建立新的 Web ACL，而不會取代原則範圍內資源上任何現有的 AWS WAF 傳統 Web ACL 關聯。
- 當您選擇自動修復的原則動作，並選擇以 AWS WAF (v2) Web ACL 取代 AWS WAF 傳統 Web ACL 的選項時。無論自動應用程式層 DDoS 緩解的組態選項為何，您都可以選擇取代舊版 Web ACL。

  當您選擇取代選項時，Firewall Manager 員會視需要建立新版本的 Web ACL，然後針對原則的範圍內資源執行下列動作：

  - 如果資源與任何其他作用中的 Firewall Manager 員策略中的 Web ACL 相關聯，則「Firewall Manager 員」會保留該關聯。
  - 對於任何其他情況，Firewall Manager 員會移除與 AWS WAF 傳統 Web ACL 的任何關聯，並將資源與策略的 AWS WAF (v2) Web ACL 產生關聯。

您可以選擇讓 Firewall Manager 員視需要將舊版網頁 ACL 取代為新版 Web ACL。如果您先前已自訂原則的 AWS WAF 傳統 Web ACL，您可以先將新版 Web ACL 更新為可比較的設定，然後再選擇讓 Firewall Manager 員執行取代步驟。

您可以透過相同版本的主控台 AWS WAF 或 AWS WAF 傳統，存取原則的任一版本 Web ACL。

在您刪除策略本身之前，Firewall Manager 員不會刪除任何已取代的 AWS WAF 傳統 Web ACL。原則不再使用 AWS WAF 傳統 Web ACL 之後，您可以視需要將其刪除。

判斷 Shield 牌進階政策所使用的 AWS WAF 版本

您可以透過查看策略 AWS WAF 的 AWS Config 服務連結規則中的參數鍵，判斷 Firewall Manager 員 Shield 進階策略使用的版本。如果使用中的 AWS WAF 版本是最新版本，則參數鍵會包含`policyId`和`webAclArn`。如果它是較早的版本「 AWS WAF 經典」，則參數鍵包括`webAclId`和`resourceTypes`。

此 AWS Config 規則只會列出原則目前與範圍內資源搭配使用的 Web ACL 金鑰。

判斷 Firewall Manager 員防 Shield 進階策略使用哪個版本 AWS WAF

1. 擷取「Shield 進階」策略的策略 ID：

   a. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   b. 在瀏覽窗格中，選擇 [安全性原則]。

   c. 選擇策略的「地區」。對於 CloudFront 發行版，這是`Global`。

   d. 找到您想要的策略，然後複製其策略 ID 的值。

      策略識別碼範例：`1111111-2222-3333-4444-a55aa5aaa555`。

2. 將原 AWS Config 則 ID 附加至字串`FMManagedShieldConfigRule`，以建立原則的規則名稱。

   AWS Config 規則名稱範例：`FMManagedShieldConfigRule1111111-2222-3333-4444-a55aa5aaa555`。

3. 在相關 AWS Config 規則中搜尋名為`policyId`和的索引鍵的參數`webAclArn`：

   a. 請在以下位置開啟 AWS Config 主控台。 https://console.aws.amazon.com/config/

   b. 在導覽窗格中，選擇規則。

   c. 在清單中找到您的 Firewall Manager 員策略的 AWS Config 規則名稱，然後加以選取。規則的頁面隨即開啟。

   d. 在「規則詳細資料」下的「參數」區段中，查看機碼。如果您找到名為`policyId`和的金鑰`webAclArn`，則原則會使用使用最新版本的建立的 AWS WAF Web ACL。如果您找到名為`webAclId`和的金鑰`resourceTypes`，則原則會使用使用舊版「 AWS WAF 傳統」建立的 Web ACL。

安全性群組原則

您可以使用 AWS Firewall Manager 安全群組政策來管理中組織的 Amazon Virtual Private Cloud 安全群組 AWS Organizations。您可以將集中控制的安全群組政策套用至整間組織，或選取您的帳戶和資源子集。您也可以監控並管理在您組織中使用的安全群組政策，以及監控稽核和用途安全群組政策。

Firewall Manager 會持續維護您的策略，並在整個組織中新增或更新帳號和資源時，將其套用至帳號和資源。若要取得有關資訊 AWS Organizations，請參閱AWS Organizations 使用指南。

如需 Amazon Virtual Private Cloud 安全群組的相關資訊，請參閱 Amazon VPC 使用者指南VPC中的適用於您的安全群組。

您可以使用 Firewall Manager 員安全性群組原則，在整個 AWS 組織中執行下列作業：

- 將常見安全群組套用至指定的帳戶和資源。
- 稽核安全群組規則，以尋找和修補不合規規則。
- 稽核安全群組的用途，以清理未使用的與備援安全群組。

本節說明 Firewall Manager 員安全群組原則的運作方式，並提供使用這些原則的指引。如需建立安全性群組原則的程序，請參閱建立 AWS Firewall Manager 策略。

常見安全群組政策

透過一般安全性群組原則，Firewall Manager 可提供集中控制的安全性群組與組織中帳戶和資源的關聯。您可以指定要在您組織中要套用政策的項目與如何套用。

您可以將一般安全性群組原則套用至下列資源類型：

- Amazon 彈性運算雲（AmazonEC2）實例
- 彈性網路介面
- Application Load Balancer
- Classic Load Balancer

如需使用主控台建立通用安全性群組原則的指引，請參閱建立常見安全群組政策。

共享 VPCs

在一般安全性群組原則的原則範圍設定中，您可以選擇包含共用VPCs。此選項包括VPCs由其他帳戶擁有並與範圍內帳戶共用的選項。VPCs範圍內的帳戶擁有始終包括在內。如需共用的相關資訊VPCs，請參閱 Amazon VPC 使用者指南VPCs中的使用共用。

下列警告適用於包含共用。VPCs這些是安全性群組原則的一般注意事項之外，位於. 安全性群組原則警告和限制

- Firewall Manager 員會將主要安全性群組複寫到每個範圍內帳VPCs戶的。對於共用VPC，Firewall Manager 員會針對與共用的每個範圍內帳戶複寫主要安全性群組一次。VPC這可能會導致在單一共用VPC中產生多個複本。
- 當您建立新的共用時VPC，除非您在原則範圍內建立至少一個資源之後，才會在 Firewall Manager 安全性群組原則詳細資料中看到VPC該資源。
- 當您在VPCs已啟用VPCs共用的原則中停用共用時VPCs，Firewall Manager 會在共用中刪除未與任何資源關聯的複本安全性群組。Firewall Manager 員會保留剩餘的複本安全性群組，但會停止管理它們。移除剩餘的安全性群組需要在每個共用VPC執行個體中進行手動管理。

主要安全群組

針對每個一般安全性群組原則，您會提 AWS Firewall Manager 供一或多個主要安全性群組：

- 主要安全群組必須由 Firewall Manager 員管理員帳戶建立，且可以位於帳戶中的任何 Amazon VPC 執行個體中。
- 您可以透過 Amazon Virtual Private Cloud (AmazonVPC) 或 Amazon 彈性運算雲 (AmazonEC2) 管理您的主要安全群組。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用安全群組。
- 您可以將一或多個安全群組命名為「Firewall Manager 員」安全性群組原則的主要群組。政策中允許的安全群組數量預設為一個，但您可以提交增加數量的請求。如需相關資訊，請參閱AWS Firewall Manager 配額。

政策規則設定

您可以針對通用安全性群組原則的安全性群組和資源，選擇下列一或多個變更控制行為：

- 識別並報告本機使用者對複本安全性群組所做的任何變更。
- 取消任何其他安全性群組與原則範圍內 AWS 資源的關聯。
- 將標籤從主要群組分配到複本安全性群組。

> **Important**
>
> Firewall Manager 員不會將 AWS 服務新增的系統標記散佈到複本安全性群組中。系統標籤以 aws: 字首開頭。此外，如果策略具有與組織的標籤策略衝突的標記，Firewall Manager 將不會更新現有安全群組的標記或建立新的安全群組。如需有關標籤策略的詳細資訊，請參閱 AWS Organizations 使用指南中的標籤策略。

- 將安全性群組參照從主要群組散佈至複本安全性群組。

  這可讓您輕鬆地在所有範圍內資源建立參照規則的通用安全性群組，以及與指定安全性群組相關聯的VPC執行個體。啟用此選項時，Firewall Manager 員僅在安全群組參考 Amazon Virtual Private Cloud 中的對等安全群組時，才會傳播安全群組參考。如果複本安全性群組未正確參考對等安全性群組，則 Firewall Manager 會將這些複寫的安全性群組標示為不相容。如需如何在 Amazon 中參考對等安全群組的詳細資訊VPC，請參閱 Amazon 對等互VPC連指南中的更新安全群組以參考對等安全群組。

  如果您未啟用此選項，則 Firewall Manager 員不會將安全性群組參照傳播至複本安全性群組。如需 Amazon 中VPC對等互連的相關資訊VPC，請參閱 Amazon VPC 對等互連指南。

政策建立與管理

建立通用安全群組政策時，Firewall Manager 會將主要安全群組複寫到政策範圍內的每個 Amazon VPC 執行個體，並將複製的安全群組與政策範圍內的帳戶和資源建立關聯。當您修改主要安全性群組時，「Firewall Manager 員」會將變更傳播至複本。

刪除常見安全群組政策時，您可以選擇是否要清理依此政策建立的資源。對於「Firewall Manager 員」一般安全性群組，這些資源是複本安全性群組。除非您想要在刪除政策後手動管理每個個別複本，否則請選擇清理選項。在大多數情況下，選擇清理是最簡單的方法。

如何管理複本

Amazon 執行個體中的複本安全群組與其他 VPC Amazon VPC 安全群組一樣進行管理。如需詳細資訊，請參閱 Amazon VPC 使用者指南VPC中的適用於您的安全群組。

內容稽核安全群組政策

使用 AWS Firewall Manager 內容稽核安全性群組策略來稽核原則動作，並將其套用至組織安全性群組中使用的規則。內容稽核安全性群組原則會根據您在原則中定義的範圍，套用至 AWS 組織中使用中的所有客戶建立的安全性群組。

如需使用主控台建立內容稽核安全性群組原則的指引，請參閱建立內容稽核安全群組政策。

政策範圍資源類型

您可以將內容稽核安全性群組策略套用至下列資源類型：

- Amazon 彈性運算雲（AmazonEC2）實例
- 彈性網路介面
- Amazon VPC 安全集團

如果安全群組明確位於範圍內，或與範圍內的資源相關聯，則會將該安全群組視為在政策範圍內。

策略規則選項

您可以針對每個內容稽核策略使用受管策略規則或自訂策略規則，但不能同時使用這兩種規則。

- 受管策略規則 — 在具有受管規則的策略中，您可以使用應用程式和通訊協定清單來控制 Firewall Manager 稽核的規則，以及標記為合規或不合規。您可以使用由 Firewall Manager 員管理的清單。您也可以建立和使用自己的應用程式和通訊協定清單。如需這些清單類型以及自訂清單的管理選項的相關資訊，請參閱受管理清單。
- 自訂策略規則 — 在具有自訂策略規則的策略中，您可以指定現有的安全性群組作為策略的稽核安全性群組。您可以使用稽核安全性群組規則做為範本，該範本可定義 Firewall Manager 稽核的規則，並將其標記為符合或不合規。

稽核安全性群組

您必須先使用 Firewall Manager 員管理員帳戶建立稽核安全性群組，才能在策略中使用這些群組。您可以通過 Amazon Virtual Private Cloud（AmazonVPC）或 Amazon 彈性計算雲（AmazonEC2）管理安全組。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用安全群組。

Firewall Manager 只會使用您用於內容稽核安全性群組原則的安全性群組，作為原則範圍內之安全性群組的比較參考。Firewall Manager 員不會將其與組織中的任何資源建立關聯。

您在稽核安全性群組中定義規則的方式取決於您在原則規則設定中的選擇：

- 受管策略規則 — 對於受管策略規則設定，您可以使用稽核安全性群組覆寫策略中的其他設定，以明確允許或拒絕可能有其他符合性結果的規則。
  - 如果您選擇永遠允許稽核安全性群組中定義的規則，則不論其他原則設定為何，符合稽核安全性群組中定義之規則的任何規則都會被視為符合該策略。

- 如果您選擇一律拒絕稽核安全性群組中定義的規則，則不論其他原則設定為何，符合稽核安全性群組中定義之規則的任何規則都會被視為不符合該策略。
- 自訂原則規則 — 對於自訂原則規則設定，稽核安全性群組提供範圍內安全性群組規則中可接受或不可接受的範例：
  - 如果您選擇允許使用規則，則所有範圍內的安全性群組都必須只有位於策略稽核安全性群組規則允許範圍內的規則。在此情況下，原則的安全性群組規則會提供範例說明可接受的動作。
  - 如果您選擇拒絕使用規則，則所有範圍內的安全性群組只能擁有不在策略稽核安全性群組規則允許範圍內的規則。在此情況下，原則的安全性群組會提供不可接受的範例。

政策建立與管理

建立稽核安全群組政策時，您必須停用自動修補。建議的實務為在啟用自動修補前檢閱政策建立的效用。檢閱預期的效用後，您可以編輯政策，並啟用自動修補。啟用自動補救時，Firewall Manager 會更新或移除範圍內安全性群組中不相容的規則。

受稽核安全群組政策影響的安全群組

您組織中由客戶建立的所有安全群組均有資格位於稽核安全群組政策中。

複本安全群組不是由客戶建立，因此沒有直接位於稽核安全群組政策範圍中的資格。不過它們可以隨著政策的自動修補活動而更新。常見安全群組政策的主要安全群組是由客戶建立，因此可以在稽核安全群組政策的範圍內。如果稽核安全性群組原則對主要安全性群組進行變更，Firewall Manager 會自動將這些變更傳播到複本。

用途稽核安全群組政策

使用使 AWS Firewall Manager 用狀況稽核安全性群組原則來監控您的組織是否有未使用和冗餘的安全群組，並選擇性地執 當您啟用此原則的自動修復時，Firewall Manager 員會執行下列動作：

1. 整合多餘的安全群組 (如果您已選擇該選項)。
2. 移除未使用的安全群組 (如果您已選擇該選項)。

您可以將使用情況稽核安全性群組策略套用至下列資源類型：

- Amazon VPC 安全集團

如需使用主控台建立使用情況稽核安全性群組原則的指引，請參閱建立用途稽核安全群組政策。

Firewall Manager 員如何偵測並修復冗餘安全性群組

若要將安全群組視為多餘群組，它們必須設定完全相同的規則，且位於相同的 Amazon VPC 執行個體中。

若要修復多餘的安全性群組集，Firewall Manager 會選取集合中要保留的其中一個安全性群組，然後將其與集中其他安全性群組關聯的所有資源關聯。然後，「Firewall Manager 員」會將其他安全性群組與其相關聯的資源取消關聯，使其未使用。

> **Note**
>
> 如果您也選擇移除未使用的安全性群組，則「Firewall Manager 員」會在下一步執行。此動作會移除備援組中的安全群組。

Firewall Manager 員如何偵測並修復未使用的安全群組

如果下列兩項都成立，則 Firewall Manager 員會將安全性群組視為未使用：

- 任何 Amazon EC2 執行個體或 Amazon EC2 elastic network interface 都不會使用安全群組。
- 在策略規則期間指定的分鐘數內，「Firewall Manager 員」尚未收到該項目的組態項目。

原則規則期間的預設設定為零分鐘，但您可以將時間增加到 365 天 (525,600 分鐘)，讓自己有時間將新的安全性群組與資源建立關聯。

> **Important**
>
> 如果您指定的預設值為零以外的分鐘數，則必須在中啟用間接關係 AWS Config。否則，您的使用稽核安全性群組原則將無法如預期般運作。如需有關中間接關係的資訊 AWS Config，請參閱AWS Config 開發人員指南 AWS Config中的「間接關係」。

如果可能，Firewall Manager 會根據您的規則設定從您的帳戶中刪除未使用的安全性群組來修復這些群組。如果「Firewall Manager 員」無法刪除安全性群組，則會將其標示為不符合策略。Firewall Manager 員無法刪除其他安全性群組所參考的安全性群組。

修復的時間會根據您使用的是預設時間週期設定還是自訂設定而有所不同：

- 時間週期設為零 (預設值) — 使用此設定時，一旦 Amazon EC2 執行個體或 elastic network interface 未使用安全群組，就會被視為未使用。

針對此零時間週期設定，「Firewall Manager 員」會立即修復安全性群組。

- 大於零的期間 — 使用此設定時，如果 Amazon EC2 執行個體或 elastic network interface 未使用安全群組，且 Firewall Manager 在指定的分鐘數內未收到該群組的組態項目，則會將其視為未使用。

  對於非零時間週期設定，Firewall Manager 會在安全性群組維持未使用狀態 24 小時之後修復安全性群組。

預設帳戶規格

當您透過主控台建立使用情況稽核安全性群組原則時，Firewall Manager 會自動選擇 [排除指定的帳戶] 並包含所有其他帳戶。然後，服務會將 Firewall Manager 員管理員帳戶放在清單中以排除。這是建議的方法，可讓您手動管理屬於 Firewall Manager 員管理員帳戶的安全性群組。

安全群組政策的最佳實務

本節列出使用 AWS Firewall Manager管理安全群組的建議。

排除 Firewall Manager 員管理員帳戶

當您設定策略範圍時，請排除 Firewall Manager 員管理員帳戶。當您透過主控台建立用途稽核安全群組政策時，這是預設選項。

從停用自動修補開始

對於內容或用途稽核安全群組政策，請先從停用自動修補開始。檢閱政策詳細資訊，以判定自動修補可能有的效用。當您確認這些變更正是您所需的時，請編輯政策，以啟用自動修補。

如果您也使用外部來源管理安全群組，請避免衝突

如果您使用「Firewall Manager 員」以外的工具或服務來管理安全性群組，請注意避免「Firewall Manager 員」中的設定與外部來源的設定之間發生衝突。如果您使用自動修補且設定有衝突，您可以建立消耗雙方資源的衝突修補循環。

例如，假設您將另一個服務設定為維護一組 AWS 資源的安全性群組，並設定 Firewall Manager 原則，以維護部分或所有相同資源的不同安全性群組。如果您設定任何其他安全群組與範圍內資源相關聯的任何一方，該方將會移除由另一方維護的安全群組關聯。如果雙方都以這種方式進行配置，則最終可能會產生衝突的分離和關聯循環。

此外，假設您建立了 Firewall Manager 稽核原則，以強制執行與其他服務之安全性群組組態衝突的安全性群組組態設定。Firewall Manager 稽核策略套用的補救可以更新或刪除該安全性群組，使其不符合

其他服務的規範。如果其他服務設定為監視並自動修復發現的任何問題，則會重新建立或更新安全性群組，使其再次不符合 Firewall Manager 稽核策略。如果 Firewall Manager 稽核策略設定了自動補救，它將再次更新或刪除外部安全性群組，依此類推。

若要避免這類衝突，請在 Firewall Manager 員與任何外部來源之間建立互斥的組態。

您可以使用標記，將外部安全群組排除在 Firewall Manager 員原則的自動修復之外。若要這樣做，請將一或多個標記新增至由外部來源管理的安全群組或其他資源。然後，當您定義 Firewall Manager 員策略範圍時，請在資源規格中排除具有已新增標籤的資源。

同樣地，在您的外部工具或服務中，將 Firewall Manager 管理的安全性群組排除在任何管理或稽核活動之外。請勿匯入 Firewall Manager 員資源，或使用 Firewall Manager 員特定的標記將其排除在外部管理之外。

使用稽核安全性群組原則的最佳作法

當您使用使用稽核安全性群組原則時，請遵循下列準則。

- 避免在短時間內對安全性群組的關聯狀態進行多次變更，例如在 15 分鐘內變更。這樣做可能會導致 Firewall Manager 員遺漏部分或所有對應的事件。例如，請勿快速將安全群組與 elastic network interface 建立關聯或取消關聯。

安全性群組原則警告和限制

本節列出使用 Firewall Manager 員安全性群組原則的注意事項和限制。

資源類型:Amazon EC2 實例

本節列出使用 Firewall Manager 員安全群組政策保護 Amazon EC2 執行個體的注意事項和限制。

- 使用保護 Amazon EC2 彈性網路界面 (ENIs) 的安全群組，Firewall Manager 員不會立即看到對安全群組的變更。Firewall Manager 員通常會在數小時內偵測到變更，但偵測最多可能會延遲六個小時。
- Firewall Manager 員不支援 Amazon EC2 ENIs 關聯式資料庫服務所建立的 Amazon 安全群組。
- Firewall Manager 員不支援更新使用 Fargate 服務類型建立的 Amazon EC2 ENIs 安全群組。但是，您可以使用 Amazon EC2 服務類型更新 Amazon ECS ENIs 的安全組。
- 對於一般安全性群組原則，這些警告與連接至執行個體的彈性網路介面 (ENIs) 數目與原則選項之間的互動，該選項指定是否只修復沒有新增附件的EC2執行個體，還是修復所有執行個體。EC2每個EC2例證都有一個默認的主實例ENI，您可以附加更多實例ENIs。在中API，此選擇的原則選項設定為`ApplyToAllEC2InstanceENIs`。

如果範圍內的EC2執行個體已ENIs附加其他執行個體，且原則設定為僅包含主EC2執行個體的執行個體ENI，則 Firewall Manager 將不會嘗試對該EC2執行個體進行任何修復。此外，如果執行個體超出原則範圍，Firewall Manager 就不會嘗試取消其可能為執行個體建立的任何安全性群組關聯性的關聯性。

對於下列邊緣情況，無論原則的資源清除規格為何，Firewall Manager 都可以保持複製的安全群組關聯不變：

- 當具有其他執行個體的執行個體先前ENIs已由設定為包含所有EC2執行個體的策略修復，然後執行個體超出原則範圍，或原則設定變更為僅包含不含其他ENIs執行個體的執行個體。
- 當設定為只包含沒有其ENIs他執行個體的原則修復時ENIs，另一個執行個體ENI已附加至執行個體，然後執行個體就會超出原則範圍。

其他警告和限制

以下是 Firewall Manager 員安全性群組原則的其他警告和限制。

- 只有使用滾動更新 (AmazonECS) 部署控制器的 Amazon ECS 服務才能更新 Amazon。ECS ENIs對於其他 Amazon ECS 部署控制器 (例如 CODE _ DEPLOY 或外部控制器)，Firewall Manager 員目前無法更新ENIs.
- Firewall Manager 員不支援更新網路負載平衡器中ENIs的安全群組。
- 在一般安全性群組原則中，如果稍後與帳戶取消共用的共用 Firewall Manager 員將不會刪除帳戶中的複本安全性群組。VPC
- 使用狀況稽核安全性群組原則時，如果您使用自訂延遲時間設定建立多個策略，且所有策略都具有相同範圍，則第一個具有符合性發現項目的原則將是報告發現項目的策略。

安全群組政策使用案例

您可以使用一 AWS Firewall Manager 般安全群組政策自動化主機防火牆組態，以便在 Amazon VPC 執行個體之間進行通訊。本節列出標準 Amazon VPC 架構，並說明如何使用 Firewall Manager 員一般安全群組政策保護每個架構。這些安全群組原則可協助您套用一組統一的規則來選取不同帳戶中的資源，並避免 Amazon 彈性運算雲端和 Amazon VPC 中的每個帳戶進行設定。

使用 Firewall Manager 員一般安全群組政策，您可以只標記與其他 Amazon 中執行個體通訊所需的EC2彈性網路界面VPC。然後，同一 Amazon VPC 中的其他實例更加安全和孤立。

使用案例：監視和控制對應用程式負載平衡器和傳統負載平衡器的要求

您可以使用 Firewall Manager 一般安全性群組原則來定義範圍內負載平衡器應提供哪些要求。您可以透過 Firewall Manager 員主控台進行設定。只有符合安全群組輸入規則的要求才能連線到負載平衡器，而且負載平衡器只會分發符合輸出規則的要求。

使用案例：可存取網際網路的公用 Amazon VPC

您可以使用 Firewall Manager 員一般安全群組原則來保護公用 AmazonVPC，例如，僅允許輸入連接埠 443。這與僅允許公用入站HTTPS流量相同VPC。您可以在中標記公用資源 VPC (例如，為 VPC「Public」)，然後將 Firewall Manager 員策略範圍設定為只有具有該標籤的資源。Firewall Manager 員會自動將策略套用至這些資源。

使用案例：公有和私有 Amazon VPC 執行個體

您可以對公有資源使用相同的通用安全群組原則，如先前使用案例中建議的公用 Amazon VPC 執行個體使用相同的通用安全群組原則。您可以使用第二個常見安全群組政策，限制公有資源與私有資源之間的通訊。使用類似「PublicPrivate」的標記公有和私有 Amazon VPC 執行個體中的資源，以便將第二個政策套用至這些執行個體。您可以使用第三個政策來定義私有資源與其他公司或私有 Amazon VPC 執行個體之間允許的通訊。對於此政策，您可以在私有資源上使用另一個識別標籤。

使用案例：集線器和支點 Amazon VPC 執行個體

您可以使用通用的安全群組政策來定義中樞 Amazon 執行個體和交談 Amazon VPC VPC 執行個體之間的通訊。您可以使用第二個政策定義從每個分支 Amazon 執行個VPC體到中樞 Amazon VPC 執行個體的通訊。

使用案例：Amazon EC2 執行個體的預設網路界面

您可以使用一般安全性群組原則，僅允許標準通訊，例如內部SSH和 Patch /OS 更新服務，並禁止其他不安全的通訊。

使用案例：識別具有開放權限的資源

您可以使用稽核安全群組政策，來識別您組織內擁有可與公有 IP 地址進行通訊之許可，或擁有屬於第三方廠商之 IP 地址的所有資源。

Amazon VPC 網路存取控制清單 (ACL) 政策

本節介紹 AWS Firewall Manager 網路 ACL 原則的運作方式，並提供使用這些原則的指引。如需使用主控台建立網路 ACL 原則的指引，請參閱建立網路ACL原則。

如需 Amazon VPC 網路存取控制清單 (ACL) 的相關資訊，請參閱 Amazon VPC 使用者指南中的使用網路 ACL 控制到子網路的流量。

您可以使用 Firewall Manager 員網路 ACL 政策來管理您在中組織的 Amazon Virtual Private Cloud (Amazon VPC) 網路存取控制清單 (ACL)。 AWS Organizations您可以定義策略的網路 ACL 規則設定，以及要在其中強制執行設定的帳戶和子網路。當帳戶和子網路在整個組織中新增或更新時，Firewall Manager 會持續將您的策略設定套用至帳戶和子網路。如需有關策略範圍和的資訊 AWS Organizations，請參閱AWS Firewall Manager 政策範圍和《AWS Organizations 使用指南》。

當您定義 Firewall Manager 員網路 ACL 原則時，除了標準 Firewall Manager 員原則設定 (例如名稱和範圍) 之外，還提供下列資訊：

- 入站和出站流量處理的第一個和最後一個規則。Firewall Manager 員會強制執行在策略範圍內的網路 ACL 中存在和排序，或報告不符合規範圍。您的個人帳戶可以建立自訂規則，以便在策略的第一個和最後一個規則之間執行。
- 當修復會導致網路 ACL 中規則之間的流量管理衝突時，是否強制進行修復。這僅在為策略啟用修復時適用。

Firewall Manager 員網路 ACL 規則和標記

本節說明網路 ACL 原則規則規格，以及由 Firewall Manager 員管理的網路 ACL。

在受管理的網路 ACL 上進行標記

Firewall Manager 員使用值為的`FMManaged`標籤來標記受管理的網路 ACL `true`。Firewall Manager 員只會對具有此標記設定的網路 ACL 執行修復。

您在策略中定義的規則

在您的網路 ACL 原則規格中，您可以定義要針對輸入流量最先和最後執行的規則，以及您想要針對輸出流量執行的第一個和最後一個規則。

依預設，您最多可以定義 5 個輸入規則，以用於原則中第一個和最後一個規則的任意組合。同樣地，您最多可以定義 5 個輸出規則。如需這些限制的詳細資訊，請參閱軟配額。如需有關網路 ACL 一般限制的資訊，請參閱 Amazon VPC 使用者指南中的 Amazon 網路 ACL 配額。

您不會將規則編號指派給原則規則。相反地，您可以依照要評估規則的順序來指定規則，而「Firewall Manager 員」會使用該順序在其管理的網路 ACL 中指派規則編號。

除此之外，您可以管理政策的網路 ACL 規則規格，就像透過 Amazon VPC 管理網路 ACL 中的規則一樣。如需 Amazon VPC 中網路 ACL 管理的相關資訊，請參閱 Amazon VPC 使用者指南中的使用網路 ACL 控制到子網路的流量和使用網路 ACL。

受管網路 ACL 中的規則

Firewall Manager 會在其管理的網路 ACL 中設定規則，方法是將策略的第一個和最後一個規則置於個別帳戶管理員定義的任何自訂規則之前和之後。Firewall Manager 員會保留自訂規則的順序。網路 ACL 會從編號最低的規則開始評估。

當 Firewall Manager 員第一次建立網路 ACL 時，會使用下列編號來定義規則：

- 第一條規則：1，2，... — 由您在 Firewall Manager 員網路 ACL 原則中定義。

  「Firewall Manager 員」會指派規則編號，從 1 開始遞增為 1，並依照您在原則規格中的排序順序來指派規則編號。
- 自定義規則：5，5，100，... — 由個別客戶經理透過 Amazon VPC 管理。

  「Firewall Manager 員」會為這些規則指派數字，從 5,000 開始，並針對每個後續規則遞增 100。
- 最後規則：... 32,765, 32,766 — 由您在 Firewall Manager 員網路 ACL 原則中定義。

  「Firewall Manager 員」會指派以最高可能數字結尾的規則編號，32766 以遞增 1，並依照您在原則規格中的排序順序排列規則。

網路 ACL 初始化之後，Firewall Manager 員不會控制個別帳戶在其受管理網路 ACL 中所做的變更。個別帳戶可以變更網路 ACL 而不會超出合規性，前提是任何自訂規則在策略的第一個和最後一個規則之間保持編號，而第一個和最後一個規則會維持其指定的順序。最佳作法是，在管理自訂規則時，請遵循本節所述的編號。

Firewall Manager 員如何啟動子網路的網路 ACL 管理

當子網路與 Firewall Manager 員建立並標記為的網路 ACL 建立關聯時，Firewall Manager 員會開始管理子網路 ACL `true`。`FMManaged`

符合網路 ACL 原則時，子網路的網路 ACL 必須將原則的第一個規則依照原則中指定的順序放在首位、最後一個規則排在最後、依序排列，以及任何其他自訂規則放在中間。這些需求可以由子網路已與子網路建立關聯的未受管理網路 ACL 或受管理的網路 ACL 來滿足。

當 Firewall Manager 員將網路 ACL 原則套用至與未受管理網路 ACL 相關聯的子網路時，Firewall Manager 員會依序檢查下列項目，並在識別出可行選項時停止：

1. 相關聯的網路 ACL 已經相容 — 如果目前與子網路相關聯的網路 ACL 符合規範，則 Firewall Manager 員會保留該關聯，並且不會啟動子網路的網路 ACL 管理。

Firewall Manager 員不會變更或以其他方式管理它不擁有的網路 ACL，但只要它符合規範，Firewall Manager 員就會將其保留在適當的位置，只是監視它是否符合原則。

2. 可使用符合規範的受管理網路 ACL — 如果 Firewall Manager 員已經在管理符合所需組態的網路 ACL，則這是一個選項。如果已啟用修復，則 Firewall Manager 員會將子網路與其關聯。如果修復已停用，則 Firewall Manager 員會將子網路標示為不相容，並提供取代網路 ACL 關聯作為補救選項。
3. 建立新的合規受管理網路 ACL — 如果啟用修復，則 Firewall Manager 員會建立新的網路 ACL，並將其與子網路產生關聯。否則，Firewall Manager 員會將子網路標示為不相容，並提供建立新網路 ACL 和取代網路 ACL 關聯的補救選項。

如果這些步驟失敗，Firewall Manager 員會報告子網路的不符合規範。

當子網路第一次進入範圍，以及子網路的非受管理網路 ACL 不符合規範時，Firewall Manager 員會遵循下列步驟。

Firewall Manager 員如何修復不符合標準的受管理網路 ACL

本節說明當受管理的網路 ACL 不符合原則時，Firewall Manager 員如何修復其受管理的網路 ACL。Firewall Manager 員只會修復受管理的網路 ACL — 標籤設為`FMManaged`。`true`如需非由 Firewall Manager 員管理的網路 ACL，請參閱初始網路 ACL 管理。

修復會還原第一個規則、自訂規則和最後一個規則的相對位置，並還原第一個和最後一個規則的順序。在修復期間，Firewall Manager 員不一定會將規則移至其在網路 ACL 初始化中使用的規則編號。如需這些規則品類的初始編號設定和描述，請參閱初始網路 ACL 管理。

為了建立相容的規則和規則順序，Firewall Manager 員可能需要在網路 ACL 內移動規則。Firewall Manager 員會盡可能保留網路 ACL 的保護，方法是維持現有的相容規則順序，就像這樣做。例如，它可能會暫時將規則複製到新位置，然後執行原始規則的順序移除，以便在程序期間保留相對位置。

此方法可保護您的設定，但也需要網路 ACL 中的空間，以供暫時規則使用。如果 Firewall Manager 員達到網路 ACL 中規則的限制，則會中止修復。發生這種情況時，網路 ACL 會維持不符合規範，而且 Firewall Manager 員會報告原因。

如果帳戶將自訂規則新增至由 Firewall Manager 員管理的網路 ACL，而這些規則會干擾 Firewall Manager 員修復，則 Firewall Manager 員會停止網路 ACL 上的任何補救活動並報告衝突。

強制補救

如果您為策略選擇 auto 修復，您還可以指定是強制對第一個規則還是最後一個規則強制修復。

當 Firewall Manager 在自訂規則與策略規則之間的流量處理發生衝突時，它會參照對應的強制修復設定。如果啟用強制修復，則儘管發生衝突，Firewall Manager 員仍會套用補救。如果未啟用此選項，「Firewall Manager 員」會停止修復。在任何一種情況下，Firewall Manager 員都會報告規則衝突並提供補救選項。

規則計數需求和限制

在修復期間，Firewall Manager 可能會暫時複製規則，以便在不變更規則提供的防護的情況下移動規則。

對於輸入或輸出規則，「Firewall Manager 員」可能需要執行修復的最多規則數目如下：

```
2 * (the number of rules defined in the policy for the traffic direction)
+
the number of custom rules defined in the network ACL for the traffic direction
```

網路 ACL 和網路 ACL 原則受到可變規則限制的約束。如果 Firewall Manager 員在修復工作中達到限制，它就會停止嘗試修復並報告不符合規範。

若要騰出空間讓 Firewall Manager 員執行其補救活動，您可以要求提高限制。或者，您可以變更原則或網路 ACL 中的組態，以減少使用的規則數目。

如需有關網路 ACL 限制的資訊，請參閱 Amazon VPC 使用者指南中的 Amazon 網路 ACL 配額。

修復失敗時

更新網路 ACL 時，如果 Firewall Manager 員因任何原因需要停止，它不會復原變更，而是讓網路 ACL 保持暫時狀態。如果您在`FMManaged`標籤設定為的網路 ACL 中看到重複的規則`true`，則 Firewall Manager 員可能正在進行修復。變更可能會在一段時間內完成部分，但是由於 Firewall Manager 採取的修復方法，因此不會中斷流量或減少相關子網路的保護。

當 Firewall Manager 員未完全修復不符合規範的網路 ACL 時，它會報告相關子網路的不符合性，並建議可能的補救選項。

修復失敗後重試

在大多數情況下，如果 Firewall Manager 員無法完成網路 ACL 的修復變更，它最終會重試變更。

例外情況是修復達到網路 ACL 規則計數限制或 VPC 網路 ACL 計數限制時。Firewall Manager 員無法執行會佔用 AWS 資源超過其限制設定的補救活動。在這些情況下，您需要減少計數或增加限制才能繼續。如需有關限制的資訊，請參閱 Amazon VPC 使用者指南中的網路 ACL 上的 Amazon VPC 配額。

Firewall Manager 員網路 ACL 符合報告

Firewall Manager 員會監控並報告附加至範圍內子網路之所有網路 ACL 的符合性。

一般而言，如果原則規則與自訂規則之間的規則順序不正確或流量處理行為發生衝突等情況，就會發生不符合性。不符合性報告包括規範遵循違規和修正選項。

「Firewall Manager 員」會以與其他策略類型相同的方式回報網路 ACL 策略的符合性違規。如需符合性報告的相關資訊，請參閱檢視 AWS Firewall Manager 原則的符合性資訊。

策略更新期間不符合

修改網路 ACL 原則之後，直到 Firewall Manager 員更新原則範圍內的網路 ACL 之前，Firewall Manager 員會將這些網路 ACL 標示為不符合標準。即使嚴格來說，即使網路 ACL 可能符合規定，Firewall Manager 員也會執行此操作。

例如，如果您從原則規格中移除規則，而範圍內的網路 ACL 仍有額外的規則，則其規則定義仍可能符合原則。但是，由於額外的規則是「Firewall Manager 員」所管理規則的一部分，因此「Firewall Manager 員」會將其視為違反目前策略設定的規則。這與「Firewall Manager 員」檢視您新增至「Firewall Manager 員」管理網路 ACL 的自訂規則的方式不同。

使用 Firewall Manager 員網路 ACL 原則的最佳作法

本節列出使用 Firewall Manager 員網路 ACL 原則和受管理網路 ACL 的建議。

請參閱標**FMManaged**籤以識別由 Firewall Manager 員管理的網路 ACL

Firewall Manager 員管理的網路 ACL 會將標`FMManaged`籤設定為`true`。使用此標記可協助區分您自己的自訂網路 ACL 和透過 Firewall Manager 員管理的 ACL。

請勿修改網路 ACL 上**FMManaged**標籤的值

Firewall Manager 員會使用此標記，透過網路 ACL 來設定及判斷其管理狀態。

請勿修改具有 Firewall Manager 員管理網路 ACL 之子網路的關聯

請勿手動變更子網路與由 Firewall Manager 員管理的任何網路 ACL 之間的關聯。這樣做可能會停用 Firewall Manager 員管理這些子網路的保護功能。您可以尋找的`FMManaged`標籤設定，識別由 Firewall Manager 員管理的`true`網路 ACL。

若要從 Firewall Manager 員原則管理中移除子網路，請使用 Firewall Manager 員原則範圍設定來排除子網路。例如，您可以標記子網路，然後從原則範圍中排除該標記。如需詳細資訊，請參閱 AWS Firewall Manager 政策範圍。

當您更新受管理的網路 ACL 時，請勿修改由 Firewall Manager 員管理的規則

在由 Firewall Manager 管理的網路 ACL 中，遵循中所述的編號配置，讓您的自訂規則與原則規則分開。Firewall Manager 員網路 ACL 規則和標記僅新增或修改數字介於 5,000 到 32,000 之間的規則。

避免為帳戶限制新增太多規則

在修復網路 ACL 期間，Firewall Manager 員通常會暫時增加網路 ACL 規則計數。為了避免不合規問題，請確定您有足夠的空間容納您正在使用的規則。如需詳細資訊，請參閱 Firewall Manager 員如何修復不符合標準的受管理網路 ACL。

從停用自動修補開始

從停用自動修復開始，然後檢閱原則詳細資料資訊，以判斷自動修復會產生的影響。當您確認這些變更正是您所需的時，請編輯政策，以啟用自動修補。

Firewall Manager 員網路 ACL 原則警告

本節列出使用 Firewall Manager 員網路 ACL 原則的注意事項和限制。

- 更新時間比其他政策慢 — 由於 Amazon EC2 網路 ACL API 處理請求的速率有限，因此 Firewall Manager 員套用網路 ACL 政策和政策變更的速度通常會比其他 Firewall Manager 員政策慢。您可能會注意到，策略變更所花費的時間超過與其他 Firewall Manager 策略相似的變更，尤其是當您第一次新增策略時。
- 對於初始子網路保護，Firewall Manager 偏好較舊的原則 — 這僅適用於尚未受 Firewall Manager 員網路 ACL 原則保護的子網路。如果子網路同時進入多個網路 ACL 原則的範圍，則 Firewall Manager 員會使用最舊的原則來保護子網路。
- 原則停止保護子網路的原因 — 管理子網路之網路 ACL 的原則會保留管理，直到發生下列其中一種情況為止：
  - 子網路超出原則的範圍。
  - 即會刪除策略。
  - 您可以手動將子網路的關聯變更為由不同 Firewall Manager 員原則管理且子網路在範圍內的網路 ACL。

刪除 Firewall Manager 員網路 ACL 策略

當您刪除 Firewall Manager 員網路 ACL 策略時，Firewall Manager 員會將它為策略管理的所有網路 ACL `false` 上的`FMManaged`標籤值變更為。

此外，您可以選擇是否清除策略所建立的資源。如果您選擇「清除」，「Firewall Manager 員」會依序嘗試下列步驟：

1. 將關聯設回原始狀態 —「Firewall Manager 員」會在 Firewall Manager 員開始管理子網路之前，嘗試將子網路與其關聯的網路 ACL 相關聯。
2. 從網路 ACL 移除第一個和最後一個規則 — 如果無法變更關聯性，Firewall Manager 會嘗試移除原則的第一個和最後一個規則，只在與子網路關聯的網路 ACL 中保留自訂規則。
3. 對規則或關聯不執行任何動作 — 如果無法執行上述任一項作業，則 Firewall Manager 員會保留網路 ACL 及其關聯原樣。

如果您未選擇清除選項，則必須在刪除原則後手動管理每個網路 ACL。在大多數情況下，選擇清理是最簡單的方法。

AWS Network Firewall 政策

您可以使用 AWS Firewall Manager Network Firewall 政策來管理整個組織中 AWS Organizations Amazon Virtual Pri vate Cloud VPC 的 AWS Network Firewall 防火牆。您可以將集中控制的防火牆套用至整個組織，或套用至特定的帳戶和 VPC 子集。

Network Firewall 為 VPC 中的公用子網路提供網路流量篩選保護。Firewall Manager 員會根據您的策略定義的防火牆管理類型來建立和管理防火牆。Firewall Manager 員提供下列防火牆管理模式：

- 分散式-對於策略範圍內的每個帳戶和 VPC，Firewall Manager 會建立 Network Firewall 防火牆防火牆，並將防火牆端點部署到 VPC 私人雲端子網路，以過濾網路流量。
- 集中式-Firewall Manager 員會在單一 Amazon VPC 中建立單一 Network Firewall 防火牆。
- 匯入現有的防火牆-「Firewall Manager 員」會在單一 Firewall Manager 員原則中匯入現有防火牆 您可以將其他規則套用至由原則管理的匯入防火牆，以確保防火牆符合您的安全標準。

> **Note**
>
> Firewall Manager 員 Network Firewall 策略是 Firewall Manager 員策略，可用來管理整個組織中 VPC 的 Network Firewall 保護。
> Network Firewall 防護是在稱為防火牆策略的「Network Firewall」服務的資源中指定。

如需有關使用 Network Firewall 的資訊，請參閱開AWS Network Firewall 發人員指南。

下列各節涵蓋使用 Firewall Manager 員 Network Firewall 策略的需求，並說明這些策略的運作方式。如需建立策略的程序，請參閱建立 AWS Firewall Manager 政策 AWS Network Firewall。

您必須啟用資源共用

「Network Firewall」策略會跨組織中的帳號共用「Network Firewall」規則群組。若要使用此功能，您必須啟用的資源共用 AWS Organizations。若要取得有關如何啟用資源共用的資訊，請參閱Network Firewall 和 DNS 防火牆策略的資源共用。

您必須已定義 Network Firewall 規則群組

當您指定新的 Network Firewall 策略時，防火牆策略的定義與 AWS Network Firewall 直接使用時的方式相同。您可以指定要新增的無狀態規則群組、預設無狀態動作，以及可設定狀態的規則群組。您的規則群組必須已存在於 Firewall Manager 員管理員帳戶中，您才能將它們包含在策略中。如需建立 Network Firewall 規則群組的詳細資訊，請參閱AWS Network Firewall 規則群組。

Firewall Manager 員建立防火牆端點

策略中的 Firewall Manager 類型決定了防火牆管理員如何建立防火牆。您的原則可以建立分散式防火牆、集中式防火牆，或匯入現有的防火牆：

- 分散式-使用分散式部署模式，Firewall Manager 員會為策略範圍內的每個 VPC 建立端點。您可以指定要在其中建立防火牆端點的可用區域來自訂端點位置，或 Firewall Manager 可以在具有公用子網路的可用區域中自動建立端點。如果您手動選擇可用區域，則可以選擇限制每個可用區域允許的 CIDR 集。如果您決定讓 Firewall Manager 自動建立端點，您也必須指定服務要在您的 VPC 中建立單一端點還是多個防火牆端點。
  - 對於多個防火牆端點，Firewall Manager 會在每個可用區域中部署防火牆端點，其中您擁有具有網際網路閘道的子網路，或路由表格中有 Firewall Manager 員建立的防火牆端點路由。這是 Network Firewall 策略的預設選項。
  - 對於單一防火牆端點，Firewall Manager 會在具有網際網路閘道路由的任何子網路中的單一可用區域中部署防火牆端點。使用此選項時，其他區域中的流量需要跨越區域邊界，才能由防火牆過濾。

    > **Note**
    >
    > 對於這兩個選項，必須有一個與路由表相關聯的子網路，其中包含 IPv4/Prefix List 路由。Firewall Manager 員不會檢查任何其他資源。

- 集中式-使用集中式部署模式，Firewall Manager 員會在檢查 VPC 內建立一或多個防火牆端點。檢查 VPC 是 Firewall Manager 員啟動端點的中央 VPC。使用集中式部署模型時，您也可以指定要在其中

建立防火牆端點的可用區域。建立原則之後，您無法變更檢查 VPC。若要使用不同的檢查 VPC，您必須建立新原則。

- 匯入現有的防火牆-匯入現有防火牆時，您可以在策略中新增一或多個資源集，以選擇要在策略中管理的防火牆。資源集是資源的集合，在此情況下，Network Firewall 中的現有防火牆是由您組織中的帳號所管理。在策略中使用資源集之前，必須先建立資源集。如需有關 Firewall Manager 員資源集的資訊，請參閱在 Firewall Manager 員中使用資源集。

  使用匯入的防火牆時，請記住下列考量事項：

  - 如果匯入的防火牆變成不相容，Firewall Manager 會嘗試自動解決違規，但下列情況除外：
    - 如果「Firewall Manager 員」和「Network Firewall」策略的狀態或無狀態預設處理行動之間發生不相符。
    - 如果匯入的防火牆防火牆策略中的規則群組的優先順序與「Firewall Manager 員」策略中的規則群組具有相同的優先順序。
    - 如果匯入的防火牆使用與不屬於策略資源集一部分的防火牆相關聯的防火牆策略。這可能是因為防火牆只能有一個防火牆策略，但單一防火牆策略可以與多個防火牆關聯。
    - 如果屬於已匯入之防火牆防火牆策略 (也在 Firewall Manager 策略中指定) 的預先存在規則群組具有不同的優先順序。
  - 如果您在策略中啟用資源清理，Firewall Manager 會從資源集範圍內的防火牆中移除已在 FMS 匯入策略中的規則群組。
  - 由「防火牆管理員」(Firewall Manager) 所管理的防火牆匯入現有防火牆管理類型，一次只能由一個原則來管理。如果將相同資源集新增至多個匯入網路防火牆策略，則資源集中的防火牆將由新增資源集的第一個策略來管理，而第二個策略將忽略該資源集中的防火牆。
  - Firewall Manager 員目前不會串流例外狀況策略設定。如需串流例外狀況政策的詳細資訊，請參閱AWS Network Firewall 開發人員指南中的串流例外狀況

如果您使用分散式或集中式防火牆管理變更原則的可用區域清單，Firewall Manager 會嘗試清除過去建立但目前不在策略範圍內的任何端點。只有在沒有參考超出範圍端點的路由表路由時，Firewall Manager 員才會移除端點。如果 Firewall Manager 發現無法刪除這些端點，它會將防火牆子網路標示為不相容，並會繼續嘗試移除端點，直到可以安全刪除為止。

Firewall Manager 員如何管理防火牆子網路

防火牆子網路是 Firewall Manager 員為防火牆端點建立的虛擬私人雲端子網路，以過濾您的網路流量。每個防火牆端點都必須部署在專用的 VPC 子網路中。Firewall Manager 員會在策略範圍內的每個 VPC 中至少建立一個防火牆子網路。

對於使用具有自動端點組態設定的分散式部署模型的策略，Firewall Manager 只會在具有具有網際網路閘道路由之子網路的可用區域中建立防火牆子網路，或建立路由到 Firewall Manager 為其策略建立之防火牆端點的子網路。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 VPC 和子網路。

對於使用您指定可用區域 Firewall Manager 在其中建立防火牆端點的分散式或集中式模型的策略，Firewall Manager 會在這些特定的可用區域中建立端點，而不論可用區域中是否有其他資源。

當您第一次定義 Network Firewall 策略時，您可以指定 Firewall Manager 如何管理範圍內的每個 VPC 中的防火牆子網路。您之後無法變更此選擇。

對於使用具有自動端點設定的分散式部署模型的策略，您可以選擇下列選項：

- 為每個具有公用子網路的可用區域部署防火牆子網路。這是預設行為。這可為您的流量過濾保護提供高可用性。
- 在一個可用區域中部署單一防火牆子網路。透過此選項，Firewall Manager 員可識別 VPC 中具有最多公用子網路的區域，並在該處建立防火牆子網路。單一防火牆端點會過濾 VPC 的所有網路流量。這樣可以降低防火牆成本，但它不具備高可用性，而且需要來自其他區域的流量才能跨越區域邊界才能進行篩選。

對於使用具有自訂端點組態或集中式部署模型的分散式部署模型的原則，Firewall Manager 會在原則範圍內的指定可用區域中建立子網路。

您可以為 Firewall Manager 員提供 VPC CIDR 封鎖以供防火牆子網路使用，或者您可以將防火牆端點位址的選擇保留給 Firewall Manager 員來決定。

- 如果您未提供 CIDR 封鎖，Firewall Manager 員會查詢您的 VPC 是否有可用的 IP 位址可供使用。
- 如果您提供 CIDR 封鎖清單，則「Firewall Manager 員」只會在您提供的 CIDR 區塊中搜尋新的子網路。您必須使用 /28 CIDR 區塊。對於 Firewall Manager 建立的每個防火牆子網路，它會逐步引導您的 CIDR 封鎖清單，並使用發現適用於可用區域和 VPC 且具有可用位址的第一個防火牆子網路。如果 Firewall Manager 員無法在 VPC 中找到開放空間（有無限制），則該服務將不會在 VPC 中創建防火牆。

如果 Firewall Manager 無法在可用區域中建立必要的防火牆子網路，則會將子網路標示為不符合原則。當區域處於此狀態時，區域的流量必須跨越區域邊界，才能由另一個區域中的端點進行篩選。這類似於單一防火牆子網路案例。

Firewall Manager 員如何管理 Network Firewall 資源

當您在 Firewall Manager 員中定義策略時，您會提供標準防 AWS Network Firewall 火牆策略的網路流量過濾行為。您可以新增無狀態和可設定狀態的 Network Firewall 規則群組，並為不符合任何無狀態規則的封包指定預設動作。如需有關使用中的防火牆策略的資訊 AWS Network Firewall，請參閱AWS Network Firewall 防火牆策略。

對於分散式和集中式策略，當您儲存 Network Firewall 策略時，Firewall Manager 會在策略範圍內的每個 VPC 中建立防火牆和防火牆策略。Firewall Manager 員藉由串連下列值來命名這些 Network Firewall 資源：

- 固定字串 (FMManagedNetworkFirewall或)FMManagedNetworkFirewallPolicy，視資源類型而定。
- Firewall Manager 員策略名稱。這是您在建立策略時指派的名稱。
- Firewall Manager 員策略 ID。這是 Firewall Manager 員策略的 AWS 資源 ID。
- Amazon VPC 識別碼。這是 Firewall Manager 員在其中建立防火牆和防火牆策略的 VPC 的 AWS 資源 ID。

以下顯示由「Firewall Manager 員」管理之防火牆的範例名稱：

```
FMManagedNetworkFirewallEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

以下顯示防火牆策略名稱的範例：

```
FMManagedNetworkFirewallPolicyEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

建立原則之後，VPC 中的成員帳戶無法覆寫您的防火牆原則設定或規則群組，但可以將規則群組新增至 Firewall Manager 所建立的防火牆策略。

Firewall Manager 員如何針對您的政策管理和監控 VPC 路由表

> **Note**
>
> 使用集中式部署模型的原則目前不支援路由表管理。

當 Firewall Manager 員建立防火牆端點時，也會為其建立 VPC 路由表。但是，Firewall Manager 員不會管理您的 VPC 路由表。您必須設定 VPC 路由表，以將網路流量導向至 Firewall Manager 員建立的

防火牆端點。使用 Amazon VPC 輸入路由增強功能，變更路由表以透過新的防火牆端點路由流量。您的變更必須將防火牆端點插入您要保護的子網路之間以及位置之外。您需要執行的確切路由取決於您的架構及其元件。

目前，Firewall Manager 員允許監控您的 VPC 路由表路由，以查看目的地到 Internet 閘道（即繞過防火牆）的任何流量。Firewall Manager 員不支援 NAT 閘道等其他目標閘道。

有關管理 VPC 路由表的詳細資訊，請參閱 Amazon Virtual Private Cloud 使用者指南中的管理 VPC 的路由表。如需管理「Network Firewall」路由表的詳細資訊，請參閱AWS Network Firewall 開發人員指南 AWS Network Firewall中的「路由表組態」。

當您啟用對策略的監控時，Firewall Manager 會持續監控 VPC 路由配置，並警告您有關繞過該 VPC 防火牆檢查的流量。如果子網路具有防火牆端點路由，「Firewall Manager 員」會尋找下列路由：

- 路由傳送流量至 Network Firewall 端點。
- 路由以將流量從 Network Firewall 端點轉送至網際網路閘道。
- 從網際網路閘道到 Network Firewall 端點的輸入路由。
- 從防火牆子網路路由。

如果子網路具有 Network Firewall 路由，但 Network Firewall 和您的網際網路閘道路由表中有非對稱路由，則 Firewall Manager 員會將子網路報告為不相容。Firewall Manager 也會在 Firewall Manager 員建立的防火牆路由表中偵測到網際網路閘道的路由，以及子網路的路由表，並將其報告為不相容。Network Firewall 子網路路由表和您的網際網路閘道路由表中的其他路由也會報告為不相容。根據違規類型，Firewall Manager 員會建議修復動作，以使路由組態符合性。Firewall Manager 員不會在所有情況下提供建議。例如，如果您的客戶子網路具有在 Firewall Manager 員之外建立的防火牆端點，則 Firewall Manager 員不會建議修復動作。

根據預設，Firewall Manager 員會將任何跨越可用區域界限的流量標記為不相容。不過，如果您選擇在 VPC 中自動建立單一端點，Firewall Manager 就不會將跨越可用區域界限的流量標記為不合規。

對於使用具有自訂端點組態的分散式部署模型的策略，您可以選擇是否將跨越可用區域界限的流量從沒有防火牆端點的可用區域界限標記為合規還是不合規。

> **Note**
>
> - Firewall Manager 員不會針對非 IPv4 路由 (例如 IPv6 和首碼清單路由) 建議修復動作。
> - 使用 `DisassociateRouteTable` API 呼叫進行的呼叫最多可能需要 12 小時才能偵測到。

- Firewall Manager 員會為包含防火牆端點的子網路建立「Network Firewall」路由表。Firewall Manager 員假設此路由表只包含有效的網際網路閘道和 VPC 預設路由。此路由表中的任何額外或無效的路由都被認為是不合規的。

設定 Firewall Manager 員策略時，如果您選擇監控模式，則 Firewall Manager 員會提供有關資源的資源違規和修復詳細資訊。您可以使用這些建議的修正動作來修正路由表中的路由問題。如果您選擇「關閉」模式，「Firewall Manager 員」不會為您監控路由表內容。使用此選項，您可以自行管理 VPC 路由表。如需這些資源違規的詳細資訊，請參閱檢視 AWS Firewall Manager 原則的符合性資訊。

> **Warning**
>
> 如果您在建立原則時選擇 [AWS Network Firewall 路由設定] 底下的 [監視器]，則無法針對該原則將其關閉。但是，如果您選擇關閉，您可以稍後啟用它。

設定 AWS Network Firewall 原則的記錄

您可以為 Network Firewall 原則啟用集中式記錄，以取得組織內流量的詳細資訊。您可以選取流程記錄來擷取網路流量，或選取警示記錄來報告符合規則且規則動作設為DROP或的流量ALERT。如需有關 AWS Network Firewall 記錄的詳細資訊，請參閱AWS Network Firewall 開發人員指南 AWS Network Firewall中的記錄網路流量。

您可以從政策的 Network Firewall 防火牆將日誌傳送到 Amazon S3 儲存貯體。啟用日誌記錄後，AWS Network Firewall 透過更新防火牆設定來為每個設定的 Network Firewall 交付日誌，以便使用保留 AWS Firewall Manager 前綴將日誌傳遞到選取的 Amazon S3 儲存貯體`<policy-name>-<policy-id>`。

> **Note**
>
> Firewall Manager 員會使用此前置詞來判斷 Firewall Manager 員是否已新增記錄組態，或是帳戶擁有者是否已新增記錄組態。如果帳戶擁有者嘗試將保留的前置詞用於自己的自訂記錄，則 Firewall Manager 員策略中的記錄設定會覆寫該前置詞。

如需如何建立 Amazon S3 儲存貯體和檢閱存放日誌的詳細資訊，請參閱什麼是 Amazon S3？ 在 Amazon 簡單存儲服務用戶指南。

若要啟用記錄，您必須符合下列需求：

- 您在 Firewall Manager 員政策中指定的 Amazon S3 必須存在。
- 您必須具備下列許可：
  - `logs:CreateLogDelivery`
  - `s3:GetBucketPolicy`
  - `s3:PutBucketPolicy`
- 如果作為記錄目的地的 Amazon S3 儲存貯體使用伺服器端加密和存放在其中的金鑰 AWS Key Management Service，您必須將下列政策新增至 AWS KMS 客戶管理的金鑰，以允許 Firewall Manager 員記錄到您的 CloudWatch 日誌記錄群組：

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt*",
        "kms:Decrypt*",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:Describe*"
    ],
    "Resource": "*"
}
```

請注意，只有 Firewall Manager 員管理員帳戶中的值區才能用於 AWS Network Firewall 集中記錄。

當您在 Network Firewall 策略上啟用集中式記錄時，Firewall Manager 員會對您的帳戶採取下列動作：

- Firewall Manager 員會更新所選 S3 儲存貯體上的許可，以允許日誌傳遞。
- Firewall Manager 員會為策略範圍內的每個成員帳戶在 S3 儲存貯體中建立目錄。您可以在以下位置找到每個帳戶的記錄`<bucket-name>/<policy-name>-<policy-id>/AWSLogs/<account-id>`。

啟用 Network Firewall 策略的記錄

1. 使用 Firewall Manager 員管理員帳戶建立 Amazon S3 儲存貯體。如需詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的建立儲存貯體。

2. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

> **Note**
>
> 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

3. 在瀏覽窗格中，選擇 [安全性原則]。
4. 選擇您要啟用記錄的 Network Firewall 策略。如需有關 AWS Network Firewall 記錄的詳細資訊，請參閱AWS Network Firewall 開發人員指南 AWS Network Firewall中的記錄網路流量。
5. 在 [原則詳細資料] 索引標籤的 [原則規則] 區段中，選擇 [編輯]。
6. 若要啟用和彙總記錄，請在記錄設定下選擇一或多個選項：
   - 啟用和彙總流程記錄
   - 啟用和彙總警示記錄
7. 選擇您要在其中交付日誌的 Amazon S3 儲存貯體。您必須為啟用的每個記錄類型選擇一個值區。兩種記錄類型都可以使用相同的值區。
8. (選擇性) 如果要將自訂成員帳戶建立的記錄檔取代為原則的記錄組態，請選擇 [覆寫現有的記錄組態]。
9. 選擇下一步。
10. 檢閱您的設定，然後選擇 [儲存] 以儲存對策略的變更。

停用 Network Firewall 策略的記錄

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

> **Note**
>
> 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在瀏覽窗格中，選擇 [安全性原則]。
3. 選擇您要停用記錄的 Network Firewall 策略。
4. 在 [原則詳細資料] 索引標籤的 [原則規則] 區段中，選擇 [編輯]。

5. 在 [記錄組態狀態] 下，取消選取 [啟用和彙總流程記錄] 和 [啟用和彙總警示記錄 (如果已選取警示
6. 選擇下一步。
7. 檢閱您的設定，然後選擇 [儲存] 以儲存對策略的變更。

Amazon 路線 53 解析器 DNS 防火牆政策

您可以使用 AWS Firewall Manager DNS 防火牆政策來管理 Amazon Route 53 解析器 DNS 防火牆規則群組與您在中組織中的 Amazon Virtual Private Cloud VPC 之間的關聯。 AWS Organizations您可以將集中控制的規則群組套用至整個組織，或套用至特定的帳戶和 VPC 子集。

DNS 防火牆可為您的 VPC 提供對輸出 DNS 流量的篩選和規範。您可以在 DNS 防火牆規則群組中建立可重複使用的篩選規則集合，並將規則群組與 VPC 建立關聯。當您套用 Firewall Manager 員策略時，對於策略範圍內的每個帳戶和 VPC，Firewall Manager 會使用您在 Firewall Manager 員策略中指定的關聯優先順序設定，在策略中的每個 DNS 防火牆規則群組與策略範圍內的每個 VPC 之間建立關聯。

如需有關使用 DNS 防火牆的資訊，請參閱 Amazon 路線 53 開發人員指南中的 Amazon 路由 53 解析器 DNS 防火牆。

以下各節涵蓋使用 Firewall Manager 員 DNS 防火牆策略的需求，並說明策略的運作方式。如需建立策略的程序，請參閱為 Amazon 路線 53 解析器DNS防火牆創建 AWS Firewall Manager 策略。

您必須啟用資源共用

DNS 防火牆政策會在組織中的帳戶之間共用 DNS 防火牆規則群組。若要使用此功能，您必須啟用資源共用 AWS Organizations。若要取得有關如何啟用資源共用的資訊，請參閱Network Firewall 和 DNS 防火牆策略的資源共用。

您必須已定義 DNS 防火牆規則群組

當您指定新的 DNS 防火牆政策時，定義規則群組的方式與直接使用 Amazon Route 53 解析器 DNS 防火牆時的方式相同。您的規則群組必須已存在於 Firewall Manager 員管理員帳戶中，您才能將它們包含在策略中。如需建立 DNS 防火牆規則群組的詳細資訊，請參閱 DNS 防火牆規則群組和規則。

您定義最低與最高優先順序的規則群組關聯

您透過 Firewall Manager 員 DNS 防火牆策略管理的 DNS 防火牆規則群組關聯包含最低優先順序的關聯，以及 VPC 的最高優先順序關聯。在您的原則組態中，這些會顯示為第一個和最後一個規則群組。

DNS 防火牆會依下列順序篩選 VPC 的 DNS 流量：

1. 您在 Firewall Manager 員 DNS 防火牆策略中定義的第一個規則群組。有效值介於 1 到 99 之間。
2. 個別帳戶管理員透過 DNS 防火牆關聯的 DNS 防火牆規則群組。
3. 您在 Firewall Manager 員 DNS 防火牆策略中定義的最後一個規則群組。有效值介於 9,901 到 1 萬之間。

刪除規則群組

若要從 Firewall Manager 員 DNS 防火牆政策刪除規則群組，您必須執行下列步驟：

1. 從 Firewall Manager 員 DNS 防火牆策略中移除規則群組。
2. 在 AWS Resource Access Manager中取消共用規則群組。若要取消共用您擁有的規則群組，您必須將其從資源共用中移除。您可以使用 AWS RAM 控制台或 AWS CLI 執行此操作。若要取消共用資源的相關資訊，請參閱《使用指南》 AWS RAM中的〈更新資源共AWS RAM用〉。
3. 使用 DNS 防火牆主控台或 AWS CLI 刪除規則群組。

Firewall Manager 員如何命名其建立的規則群組關聯

當您儲存 DNS 防火牆原則時，如果您啟用自動補救，Firewall Manager 會在您在原則中提供的規則群組與原則範圍內的 VPC 之間建立 DNS 防火牆關聯。Firewall Manager 員藉由串連下列值來命名這些關聯：

- 固定字串，`FMManaged_`。
- Firewall Manager 員策略識別碼。這是 Firewall Manager 員策略的 AWS 資源 ID。

以下顯示由「Firewall Manager 員」管理之防火牆的範例名稱：

```
FMManaged_EXAMPLEDNSFirewallPolicyId
```

建立原則後，如果 VPC 中的帳戶擁有者覆寫您的防火牆原則設定或規則群組關聯，則 Firewall Manager 會將該策略標示為不符合標準，並嘗試提出補救動作。帳戶擁有者可以將其他 DNS 防火牆規則群組與 DNS 防火牆策略範圍內的 VPC 建立關聯。個別帳戶擁有者所建立的任何關聯必須在您的第一個和最後一個規則群組關聯之間具有優先順序設定。

帕洛奧圖網路雲端新世代防火牆政策

帕洛阿爾托網路雲端次世代防火牆 (NGFW) 是一項協力廠商防火牆服務，可用於您的政策。 AWS Firewall Manager 使用 Palo Alto Networks 適用於 Firewall Manager 員的雲端新世代防火牆，您可以在所有帳戶中建立並集中部署帕洛阿爾托網路雲端 NGFW 資源和規則堆疊。 AWS

若要將帕洛阿爾托網路雲端 NGFW 與 Firewall Manager 員搭配使用，您首先在 Marketplace 上訂閱帕洛阿爾托網路雲端 NGFW 隨付服務。 AWS 訂閱後，您可以在帕洛阿爾托網絡雲端 NGFW 服務中執行一系列步驟，以配置您的帳戶和雲端 NGFW 設定。然後，您可以建立 Firewall Manager 員雲端 FMS 政策，以集中部署和管理帕洛阿爾托網路雲端 NGFW 資源和規則，跨 Organizations 中的所有帳戶。 AWS

如需建立 Firewall Manager 員策略的程序，請參閱建立帕洛阿爾托網路雲端 AWS Firewall Manager 原則 NGFW。如需有關如何設定和管理 Palo Alto 網路 Firewall Manager 員的雲端 NGFW 的詳細資訊，請參閱帕洛阿爾托網路帕洛阿爾托網路雲端 NGFW 的說明文件。 AWS

強制雲端原生防火牆 (CNF) 即服務政策

Fortigate 雲端原生防火牆 (CNF) 即服務是一項協力廠商防火牆服務，可用於您的政策。 AWS Firewall Manager Fortigate CNF 是下一代防火牆服務，可讓您輕鬆保護雲網絡並管理安全策略。使用 Fortigate CNF 的 Firewall Manager 員，您可以在所有帳戶中創建和集中部署 Fortigate CNF 資源和策略集。 AWS

要將 Fortigate CNF 與 Firewall Manager 器一起使用，您首先在 Marketplace 上訂閱 Fortigate 雲端原生防火牆（CNF）作為服務。 AWS 訂閱之後，您可以在 Fortigate CNF 服務中執行一系列步驟，以設定全域原則集和其他設定。然後，您可以建立 Firewall Manager 員政策，以集中部署和管理 Fortigate CNF 資源到 Organizations 中的所有帳戶。 AWS

如需建立 Fortigate CNF Firewall Manager 員策略的程序，請參閱。建立 Fortigate 雲端原生防火牆 (CNF) 即服務的原 AWS Firewall Manager 則如需如何設定和管理 Fortigate CNF 以搭配 Firewall Manager 員使用的詳細資訊，請參閱 For tigate CNF 文件。

Network Firewall 和 DNS 防火牆策略的資源共用

若要管理 Firewall Manager 員 Network Firewall 和 DNS 防火牆策略，您必須 AWS Organizations 在中啟用資源共用 AWS Resource Access Manager。這可讓 Firewall Manager 員在您建立這些策略類型時，在您的帳戶中部署防護。

若要啟用資源共用，請遵循使用指南中「啟用共AWS Resource Access Manager 用方式」 AWS Organizations中的指示。

資源共享問題

您可能會在使用資源共用時遇到問題，或當您使用 AWS RAM 需要資源共用的 Firewall Manager 員原則時。

這些問題的範例包括：

- 當您依照指示啟用共用時，在 AWS RAM 主控台中，[啟用共用 AWS Organizations方式] 選項會呈現灰色且無法選取。
- 當您在 Firewall Manager 中處理需要資源共用的策略時，該策略會標記為不相容，而且您會看到指出資源共用或 AWS RAM 未啟用的訊息。

如果您在資源共用時遇到問題，請使用下列程序嘗試啟用它。

再試一次以啟用資源共用

- 再試一次，使用下列其中一個選項啟用共用功能：
  - (選項) 透過 AWS RAM 主控台，按照使用指南中「啟用共AWS Resource Access Manager用方式」 AWS Organizations中的指示進行。
  - （選項）使用 AWS RAM API，調用`EnableSharingWithAwsOrganization`。請參閱文件，網址為EnableSharingWithAwsOrganization。

在 Firewall Manager 員中使用資源集

AWS Firewall Manager 資源集是資源 (例如防火牆) 的集合，您可以在 Firewall Manager 員策略中將它們分組在一起並進行管理。資源集可讓組織中的成員精細控制要在策略中管理的資源。若要使用資源集，請在主控台中建立資源集或使用 PutResourceSetAPI，然後將資源集新增至 Firewall Manager 員策略。

您可以建立和管理下列資源和安全性原則類型的資源集：

資源類型	Firewall Manager 員安全性原則
AWS Network Firewall -防火牆	Network Firewall 策略-使用資源集從 Network Firewall 匯入現有防火牆。如需有關在 Network Firewall 策略中使用資源集的詳細資訊，請參閱程序中的匯入現有防火牆步建立 AWS Firewall Manager 政策 AWS Network Firewall驟。

下列各節涵蓋建立與刪除資源集的需求。

主題

- 在 Firewall Manager 員中使用資源集時的考量
- 建立資源集
- 刪除資源集

在 Firewall Manager 員中使用資源集時的考量

使用資源集時請注意下列考量

對不存在資源的引用

將資源新增至資源集時，您可以使用 Amazon 資源名稱 (ARN) 建立資源的參考。Firewall Manager 員會驗證 Amazon 資源名稱 (ARN) 是否正確的格式，但 Firewall Manager 員不會檢查參考的資源是否存在。如果資源尚未通過ARN驗證，則 Firewall Manager 員會在資源集中包含資源參照。如果稍後建立了具有相同ARN資源的新資源，Firewall Manager 會將規則群組從資源集的關聯策略套用至新資源。

已刪除資源

刪除資源集中的資源時，對資源的參照會保留在資源集中，直到 Firewall Manager 管理員將其移除為止。

離開組織的成員帳戶所擁有的 AWS Organizations 資源

如果成員帳號離開組織，該成員帳號所擁有之資源的任何參照都會保留在資源集中，但不會再由與資源集相關聯的任何策略管理。

關聯到多個策略

資源集可以與多個策略相關聯，但並非所有策略類型都支援管理相同資源的多個策略。如需有關不支援案例的資訊，請參閱特定原則類型的文件。

建立資源集

若要建立資源集 (主控台)

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 [資源集]。
3. 選擇「建立資源集」。
4. 針對資源集名稱，輸入描述性名稱。
5. (選擇性) 輸入資源集的「說明」。
6. 選擇下一步。
7. 對於 [選擇資源]，選取AWS 帳號 ID，然後選取 [選擇資源]，將此帳號擁有和管理的資源新增至資源集。選取資源後，選取新增以將資源新增至資源集。
8. 選擇下一步。
9. 針對資源集標籤，新增任何您想要用於資源集的識別標籤。如需標籤的詳細資訊，請參閱使用標籤編輯器。
10. 選擇下一步。
11. 檢閱新資源集。若要進行任何變更，請在您要變更的區域中選擇 Edit (編輯)。這會讓您返回建立精靈中的對應步驟。如果您滿意資源集，請選擇建立資源集。

刪除資源集

刪除資源集之前，必須先取消資源集與使用該資源集的所有策略的關聯。您可以使用主控台或使用策略詳細資訊頁面中取消資源群組的關聯。PutPolicyAPI

刪除資源集 (控制台)

1. 在導覽窗格中，選擇 [資源集]。
2. 選擇您要刪除的資源集旁邊的選項。
3. 選擇 Delete (刪除)。

檢視 AWS Firewall Manager 原則的符合性資訊

本節提供檢視 AWS Firewall Manager 策略範圍內帳號和資源之符合性狀態的指引。如需維護雲端安全性與合規性之控制項的相關資訊，請參閱Firewall Manager 員的合規驗證。 AWS

> **Note**
>
> 若要讓「Firewall Manager 員」監控策略符合性， AWS Config 必須持續記錄受保護資源的組態變更。在您的 AWS Config 配置中，錄製頻率必須設置為連續，這是默認設置。

> **Note**
>
> 若要在受保護的資源中維持適當的符合性狀態，請避免自動或手動重複變更 Firewall Manager 防護的狀態。Firewall Manager 員會使用的資訊 AWS Config 來偵測資源組態的變更。如果套用變更的速度不夠快， AWS Config 可能會遺失其中一些變更，這可能會導致 Firewall Manager 員中的符合性或修復狀態相關資訊遺失。
> 如果您發現使用 Firewall Manager 保護的資源具有不正確的合規性或修復狀態，請先確定您沒有執行任何會變更或重設 Firewall Manager 保護的程序，然後重新評估中的相關組態規則來重新整理資源的 AWS Config 追蹤。 AWS Config

對於所有 AWS Firewall Manager 策略，您可以檢視策略範圍內之帳號和資源的符合性狀態。如果策略中的設定反映在帳號或資源的設定中，則帳號或資源符合 Firewall Manager 員策略。每個原則類型都有自己的符合性需求，您可以在定義原則時對其進行調整。對於某些策略，您也可以檢視範圍內資源的詳細違規資訊，以協助您進一步瞭解和管理安全風險。

若要檢視原則的符合性資訊

1. AWS Management Console 使用您的 Firewall Manager 員管理員帳戶登入，然後在中開啟 Firewall Manager 員主控台https://console.aws.amazon.com/wafv2/fmsv2。如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

   > **Note**
   >
   > 如需建立防火牆管理員帳戶的詳細資訊，請參閱 AWS Firewall Manager 前提。

2. 在導覽窗格中，選擇 Security policies (安全群組政策)。
3. 選擇政策。在策略頁面的 [帳號和資源] 索引標籤中，Firewall Manager 會列出組織中的帳號，依策略範圍內的帳號和超出範圍的帳號進行分組。

   策略範圍內的帳號」窗格會列出每個帳號的合規性狀態。[符合標準] 狀態表示策略已成功套用至帳號的所有範圍內資源。「不符合標準」狀態表示該策略尚未套用至帳號的一或多個範圍內資源。
4. 選擇不符合規定的帳戶。在帳號頁面中，Firewall Manager 會列出每個不相容資源的 ID 和類型，以及資源違反策略的原因。

   > **Note**
   >
   > 對於資源類型 `AWS::EC2::NetworkInterface` (ENI) 和 `AWS::EC2::Instance` Firewall Manager 員可能會顯示有限數量的不相容資源。若要列出其他不符合標準的資源，請修正帳號最初顯示的資源。

5. 如果 Firewall Manager 員策略類型是內容稽核安全性群組策略，您可以存取資源的詳細違規資訊。

   若要檢視違規詳細資訊，請選擇資源。

   > **Note**
   >
   > Firewall Manager 在新增詳細資源違規頁面之前發現不相容的資源可能沒有違規詳細資料。

   在資源頁面中，Firewall Manager 員會根據資源類型列出有關違規的特定詳細資料。

- **AWS::EC2::NetworkInterface**(ENI) — Firewall Manager 員會顯示資源不符合之安全群組的相關資訊。選擇安全性群組以查看更多詳細資訊。
- **AWS::EC2::Instance**— Firewall Manager 器顯示連接到不合規 EC2 實例的 ENI。它也會顯示資源不符合之安全性群組的相關資訊。選擇安全性群組以查看更多詳細資訊。
- **AWS::EC2::SecurityGroup**— Firewall Manager 員會顯示下列違規詳細資訊：
  - 不相容的安全性群組規則 — 違反的規則，包括其通訊協定、連接埠範圍、IP CIDR 範圍和說明。
  - 參照的規則 — 不符合安全性群組規則違反的稽核安全性群組規則及其詳細資訊。
  - 違規原因 — 不符合性發現項目的說明。
  - 修正動作 — 建議採取的動作。如果 Firewall Manager 員無法判斷安全修復動作，此欄位為空白。
- **AWS::EC2::Subnet**— 這是用於網路 ACL 和 Network Firewall 策略。

  「Firewall Manager 員」會顯示子網路識別碼、VPC ID 和可用區域。如果適用，Firewall Manager 員會包含有關違規的其他資訊。違規描述元件包含資源的預期狀態、目前不符合標準狀態的描述，以及造成差異之原因的描述 (如果有的話)。

  Network Firewall 違規

  - 路由管理違規 — 對於使用監控模式的 Network Firewall 策略，Firewall Manager 會顯示基本子網路資訊，以及子網路、網際網路閘道和 Network Firewall 子網路路由表中的預期和實際路由。如果實際路由與路由表中的預期路由不符，則 Firewall Manager 員會警告您發生違規。
  - 路由管理違規的補救動作 — 對於使用監控模式的 Network Firewall 策略，Firewall Manager 會針對具有違規的路由組態建議可能的補救動作。

  例如，假設子網路預期會透過防火牆端點傳送流量，但目前的子網路會將流量直接傳送至網際網路閘道。這是路由管理違規。在此情況下，建議的補救措施可能是已排序動作的清單。第一個建議是將必要的路由新增至「Network Firewall」子網路的路由表，以將外送流量導向至網際網路閘道，並將 VPC 內目的地的傳入流量導向至`local`。第二個建議是取代網際網路閘道路由或子網路路由表中無效的 Network Firewall 路由，以將外送流量導向防火牆端點。第三個建議是將必要的路由新增至網際網路閘道的路由表，以將內送流量導向到防火牆端點。
- **AWS::EC2:InternetGateway**— 這用於已啟用監視模式的 Network Firewall 策略。
  - 路由管理違規 — 如果網際網路閘道與路由表沒有關聯，或網際網路閘道路由表中有無效的路由，則網際網路閘道不相容。

- 路由管理違規的修正動作 — Firewall Manager 員會建議可能的補救動作，以補救路由管理違規。

  Example 1 — 路由管理違規和補救建議

  網際網路閘道與路由表沒有關聯。建議的補救動作可能是已排序動作的清單。第一個動作是建立路由表。第二個動作是將路由表與網際網路閘道相關聯。第三個動作是將必要的路由新增至網際網路閘道路由表。

  Example 2 — 路由管理違規和補救建議

  網際網路閘道與有效的路由表相關聯，但路由設定不正確。建議的補救可能是已排序動作的清單。第一個建議是刪除無效的路由。第二種方法是將所需的路由添加到互聯網網關路由表中。

- **`AWS::NetworkFirewall::FirewallPolicy`**— 這是用於 Network Firewall 策略。「Firewall Manager 員」會顯示 Network Firewall 防火牆策略的相關資訊，這些策略已修改過的方式使其不相容。這些資訊提供預期的防火牆策略及其在客戶帳戶中找到的策略，因此您可以比較無狀態和可設定狀態的規則群組名稱和優先順序設定、自訂動作名稱以及預設無狀態動作設定。違規描述元件包含資源的預期狀態、目前不符合標準狀態的描述，以及造成差異之原因的描述 (如果有的話)。
- **`AWS::EC2::VPC`**— 這是用於 DNS 防火牆策略。「Firewall Manager 員」會顯示位於 Firewall Manager 員 DNS 防火牆原則範圍內且不符合原則之 VPC 的相關資訊。提供的資訊包括預期與 VPC 和實際規則群組相關聯的預期規則群組。違規描述元件包含資源的預期狀態、目前不符合標準狀態的描述，以及造成差異之原因的描述 (如果有的話)。

AWS Firewall Manager 發現

AWS Firewall Manager 會針對不合規的資源和偵測到的攻擊建立發現項目，然後將它們傳送至 AWS Security Hub。如需有關安全中樞發現項目的資訊，請參閱 AWS Security Hub.

當您使用 Security Hub 和 Firewall Manager 員時，Firewall Manager 員會自動將您的發現項目傳送到 Security Hub。如需有關開始使用 Security Hub 的資訊，請參閱AWS Security Hub 使用者指南 AWS Security Hub中的設定。

> **Note**
>
> 「Firewall Manager 員」只會更新其管理下之策略及其監控資源的發現項目。
> Firewall Manager 員不會解決下列項目的發現項目：

- 已刪除的策略。
- 已刪除的資源。
- 已超出 Firewall Manager 員策略範圍的資源，例如由於標籤變更或策略定義變更。

如何檢視我的 Firewall Manager 員發現項目？

若要檢視 Security Hub 中的 Firewall Manager 員發現項目，請遵循在 Security Hub 中使用發現項目的指引，並使用下列設定建立篩選器：

- 屬性設定為 Product Name (產品名稱)。
- 運算子設定為 EQUALS (等於)。
- 數值設定為 `Firewall Manager`。此設定會區分大小寫。

我可以停用此項目嗎？

您可以透過 Security Hub 主控台停用 AWS Firewall Manager 發現項目與 Security Hub 的整合。選擇導覽列中的「整合」，然後在「Firewall Manager 員」窗格中選擇「停用整合」。如需詳細資訊，請參閱 AWS Security Hub 使用者指南。

AWS Firewall Manager 尋找類型

- AWS WAF 政策發現
- AWS Shield Advanced 政策發現
- 安全群組通用政策問題清單
- 安全性群組內容稽核政策問題清單
- 安全群組使用狀況稽核政策問題清單
- Amazon 路線 53 解析器 DNS 防火牆政策調查結果

AWS WAF 政策發現

您可以使用 Firewall Manager 員 AWS WAF 策略將 AWS WAF 規則群組套用至中的資源 AWS Organizations。如需詳細資訊，請參閱 使用 AWS Firewall Manager 原則。

資源缺少 Firewall Manager 員管理 Web ACL。

根據 Firewall Manager 員策略， AWS 資源沒有 AWS Firewall Manager 受管理的 Web ACL 關聯。您可以在策略上啟用 Firewall Manager 員修復以更正此問題。

- 嚴重性 — 80
- 狀態設定 — 通過/失敗
- 更新 — 如果 Firewall Manager 員執行修復動作，它會更新發現項目，且嚴重性會從降低`HIGH`到`INFORMATIONAL`。如果您執行修復，「Firewall Manager 員」將不會更新發現項目。

Firewall Manager 員受管理的 Web ACL 設定錯誤的規則群組。

根據 Firewall Manager 員策略，Web ACL 中由 Firewall Manager 員管理的規則群組未正確設定。這表示 Web ACL 缺少政策所需的規則群組。您可以在策略上啟用 Firewall Manager 員修復以更正此問題。

- 嚴重性 — 80
- 狀態設定 — 通過/失敗
- 更新 — 如果 Firewall Manager 員執行修復動作，它會更新發現項目，且嚴重性會從降低`HIGH`到`INFORMATIONAL`。如果您執行修復，「Firewall Manager 員」將不會更新發現項目。

AWS Shield Advanced 政策發現

如需有關 AWS Shield Advanced 策略的資訊，請參閱安全性群組原則。

資源缺乏 Shield 牌高級保護。

根據 Firewall Manager 員策略，應具有 Shield 高級防護的 AWS 資源沒有它。您可以在策略上啟用 Firewall Manager 員修復，以啟用資源的保護。

- 嚴重性 — 60
- 狀態設定 — 通過/失敗
- 更新 — 如果 Firewall Manager 員執行修復動作，它會更新發現項目，且嚴重性會從降低`HIGH`到`INFORMATIONAL`。如果您執行修復，「Firewall Manager 員」將不會更新發現項目。

防 Shield 進階偵測到對受監控資源的攻擊。

Shield 牌進階偵測到受保護資 AWS 源的攻擊。您可以在策略上啟用 Firewall Manager 員修復。

- 嚴重性 — 70
- 狀態設定 — 無
- 更新 — Firewall Manager 員不會更新此發現項目。

安全群組通用政策問題清單

如需安全群組通用政策的資訊，請參閱安全性群組原則。

資源具有設定錯誤的安全群組。

根據 Firewall Manager 員策略，「Firewall Manager 員」已識別出缺少「Firewall Manager 員」管理的安全性群組關聯的資源。您可以在策略上啟用 Firewall Manager 員修復，這樣就會根據策略設定建立關聯。

- 嚴重性 — 70
- 狀態設定 — 通過/失敗
- 更新 — Firewall Manager 員更新此發現項目。

Firewall Manager 員複本安全性群組與主要安全性群組不同步。

根據其通用安全性群組原則，Firewall Manager 員複本安全性群組與其主要安全性群組不同步。您可以在原則上啟用 Firewall Manager 員修復，以便將複本安全性群組與主要群組同步。

- 嚴重性 — 80
- 狀態設定 — 通過/失敗
- 更新 — Firewall Manager 員更新此發現項目。

安全性群組內容稽核政策問題清單

如需安全群組內容稽核政策的相關資訊，請參閱安全性群組原則。

安全群組不符合內容稽核安全群組。

「Firewall Manager 員」安全性群組內容稽核策略已識別出不相容的安全性群組。這是客戶建立的安全群組，位於內容稽核政策的範圍內，且不符合政策及其稽核安全群組所定義的設定。您可以在原則上啟用 Firewall Manager 員修復，如此可修改不相容的安全性群組，使其符合規範。

- 嚴重性 — 70

- 狀態設定 — 通過/失敗
- 更新 — Firewall Manager 員更新此發現項目。

安全群組使用狀況稽核政策問題清單

如需安全群組使用狀況稽核政策的相關資訊，請參閱安全性群組原則。

Firewall Manager 員找到冗餘安全群組。

「Firewall Manager 員」安全群組使用狀況稽核已識別冗餘安全性群組。這是一個安全群組，其規則設定為相同 Amazon 虛擬私有雲執行個體中的另一個安全群組。您可以在使用情況稽核策略上啟用 Firewall Manager 自動補救，以取代多餘的安全群組和單一安全性群組。

- 嚴重性 — 30
- 狀態設定 — 無
- 更新 — Firewall Manager 員不會更新此發現項目。

Firewall Manager 員找到未使用的安全組

Firewall Manager 員安全群組使用稽核已識別未使用的安全性群組。這是任何 Firewall Manager 員一般安全性群組原則未參考的安全性群組。您可以在使用情況稽核策略上啟用 Firewall Manager 自動補救，以移除未使用的安全群組。

- 嚴重性 — 30
- 狀態設定 — 無
- 更新 — Firewall Manager 員不會更新此發現項目。

Amazon 路線 53 解析器 DNS 防火牆政策調查結果

如需 DNS 防火牆策略的詳細資訊，請參閱Amazon 路線 53 解析器 DNS 防火牆政策。

資源缺少 DNS 防火牆保護

VPC 缺少 Firewall Manager 員 DNS 防火牆策略中定義的 DNS 防火牆規則群組關聯。發現項目會列出原則所指定的規則群組。

- 嚴重性 — 80

您使用 AWS Firewall Manager 服務時的安全性

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

> **Note**
>
> 本節為您使用 AWS Firewall Manager 服務及其 AWS 資源提供標準 AWS 安全性指引，例如 Firewall Manager 員 Network Firewall 原則和安全性群組原則。
> 如需有關使用 Firewall Manager 員保護 AWS 資源的資訊，請參閱《Firewall Manager 員》指南的其餘部分。

安全是 AWS 與您之間共同承擔的責任。共同責任模型 將此描述為雲端的安全和雲端內的安全：

- 雲端安全性 — AWS 負責保護中執行 AWS 服務的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。第三方稽核人員定期檢測及驗證安全的效率也是我們 AWS 合規計劃的一部分。若要瞭解適用於 Firewall Manager 員的符合性計劃，請參閱符合性計劃範圍內的AWS 服務。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對資料敏感度、組織要求，以及適用法律和法規等其他因素負責。

本文件可協助您瞭解如何在使用「Firewall Manager 員」時套用共同的責任模型。下列主題說明如何設定 Firewall Manager 員，以符合您的安全性和合規性目標。您也會學到如何使用其他可 AWS 協助您監控和保護 Firewall Manager 員資源的服務。

主題

Firewall Manager 員的資料保護

AWS 共用責任模型適用於中的資料保護 AWS Firewall Manager。如此模型所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需有關資料隱私權的詳細資訊，請參閱資料隱私權FAQ。 如需歐洲資料保護的相關資訊，請參閱AWS 安全性GDPR部落格上的AWS 共同責任模型和部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 認證並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 對每個帳戶使用多重要素驗證 (MFA)。
- 使用SSL/TLS與 AWS 資源溝通。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 使用設定API和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果 AWS 透過命令列介面或存取時需要 FIPS 140-3 驗證的密碼編譯模組API，請使用端點。FIPS 如需有關可用FIPS端點的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 Firewall Manager 員或其他 AWS 服務 使用主控台API、 AWS CLI、或時 AWS SDKs。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供URL給外部伺服器，我們強烈建議您不要在中包含認證資訊，URL以驗證您對該伺服器的要求。

Firewall Manager 員實體 (例如原則) 會被靜態加密，但在某些無法使用加密的區域，包括中國 (北京) 和中國 (寧夏)。每個區域都會採用唯一的加密金鑰。

的 Identity and Access Management AWS Firewall Manager

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM系統管理員控制誰可以驗證 (登入) 和授權 (有權限) 使用 Firewall Manager 員資源。IAM是您 AWS 服務 可以免費使用的。

主題

- 物件

- 使用身分驗證
- 使用政策管理存取權
- 如何 AWS Firewall Manager 使用 IAM
- 以身分識別為基礎的原則範例 AWS Firewall Manager
- AWS 受管理的政策 AWS Firewall Manager
- 疑難排解 AWS Firewall Manager 身分和存取
- 使用 Firewall Manager 員的服務連結角色
- 預防跨服務混淆代理人

物件

根據您在 Firewall Manager 員中執行的工作， AWS Identity and Access Management (IAM) 的使用方式會有所不同。

服務使用者 — 如果您使用 Firewall Manager 員服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 Firewall Manager 員功能來完成工作時，您可能需要其他權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 Firewall Manager 員中的功能，請參閱疑難排解 AWS Shield 身分和存取。

服務管理員 — 如果您負責公司的 Firewall Manager 員資源，您可能擁有 Firewall Manager 員的完整存取權。決定您的服務使用者應該存取哪些 Firewall Manager 員功能和資源是您的工作。然後，您必須向IAM管理員提交請求，才能變更服務使用者的權限。檢閱此頁面上的資訊，以瞭解的基本概念IAM。若要深入瞭解貴公司如何IAM搭配 Firewall Manager 員使用，請參閱如何 AWS Shield 使用 IAM。

IAM系統管理員 — 如果您是IAM系統管理員，您可能想要瞭解如何撰寫原則來管理 Firewall Manager 員存取權的詳細資訊。若要檢視可在中使用的 Firewall Manager 員身分型策略範例IAM，請參閱。AWS Shield的身分型政策範例

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以IAM使用者身分或假設IAM角色來驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM身分識別中心) 使用者、貴公司的單一登入驗證，以及您的 Google 或 Facebook 認證都是聯合身分識別的範例。當您以同盟身分登入時，您的管理員先前會使用IAM角色設定聯合身分識別。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以密碼編譯方式簽署您的要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署要求的詳細資訊，請參閱使用IAM者指南中的簽署 AWS API要求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。若要深入瞭解，請參閱使用AWS IAM Identity Center 者指南中的多重要素驗證和使用多重要素驗證 (MFA) AWS的使用IAM者指南。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以 root 使用者身分登入的完整工作清單，請參閱《使用指南》中的〈需要 root 使用者認證的IAM工作〉。

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步處理至您自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需IAM身分識別中心的相關資訊，請參閱IAM識別中心是什麼？ 在《AWS IAM Identity Center 使用者指南》中。

IAM 使用者和群組

IAM使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定權限。在可能的情況下，我們建議您仰賴臨時登入資料，而不要建立具有長期認證 (例如密碼和存取金鑰) 的IAM使用者。不過，如果您的特定使用案例需要使用IAM者的長期認證，建議您輪換存取金鑰。如需詳細資訊，請參閱《使用指南》中的「IAM定期輪換存取金鑰」以瞭解需要長期認證的使用案例。

IAM群組是指定IAM使用者集合的身分識別。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為的群組，IAMAdmins並授與該群組管理IAM資源的權限。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。要了解更多信息，請參閱《IAM用戶指南》中的創建用戶（而不是角色）的IAM時間。

IAM角色

IAM角色是您 AWS 帳戶 中具有特定權限的身份。它類似於用IAM戶，但不與特定人員相關聯。您可以 AWS Management Console 透過切換角色來暫時擔任中的角色。IAM您可以呼叫 AWS CLI 或 AWS API作業或使用自訂來擔任角色URL。如需有關使用角色方法的詳細資訊，請參閱《使用指南》中的IAM〈使用IAM角色〉。

IAM具有臨時認證的角色在下列情況下很有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱《使用指南》中的〈建立第三方身分識別提供IAM者的角色〉。如果您使用IAM身分識別中心，則需要設定權限集。為了控制身分驗證後可以存取的內IAM容，IAMIdentity Center 會將權限集與中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時IAM使用者權限 — IAM 使用者或角色可以假定某個IAM角色，暫時取得特定工作的不同權限。
- 跨帳戶存取 — 您可以使用IAM角色允許不同帳戶中的某個人 (受信任的主體) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要瞭解跨帳戶存取角色與以資源為基礎的政策之間的差異，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或將物件存放在 Amazon S3 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用使用IAM者或角色執行中的動作時 AWS，您會被視為主參與者。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。

- 服務角色 — 服務角色是指服務代表您執行動作所代表的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給
- 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。

- 在 Amazon 上執行的應用程式 EC2 — 您可以使用IAM角色來管理在執行個體上EC2執行的應用程式以及發出 AWS CLI 或 AWS API請求的臨時登入資料。這比在EC2實例中存儲訪問密鑰更好。若要將 AWS 角色指派給EC2執行個體並讓其所有應用程式都能使用，請建立附加至執行個體的執行個體設定檔。執行個體設定檔包含角色，可讓執行個體上EC2執行的程式取得臨時登入資料。如需詳細資訊，請參閱使用者指南中的使用IAM角色將許可授與在 Amazon EC2 執行個體上執行的應IAM用程式。

要了解是否使用IAM角色還是用IAM戶，請參閱《用戶指南》中的「IAM創建IAM角色的時機（而不是用戶）」。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以JSON文件的形式儲存在中。如需有關JSON原則文件結構和內容的詳細資訊，請參閱《IAM使用指南》中的策略概觀。JSON

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

IAM原則會定義動作的權限，不論您用來執行作業的方法為何。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或取得角色資訊 AWS API。

身分型政策

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管策略或內嵌策略之間進行選擇，請參閱《IAM使用手冊》中的「在受管策略和內嵌策略之間進行選擇」。

資源型政策

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的策略IAM中使用 AWS 受管政策。

存取控制清單 (ACLs)

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

Amazon S3 和 Amazon VPC 是支持服務的示例ACLs。 AWS WAF若要進一步了解ACLs，請參閱 Amazon 簡單儲存服務開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 權限界限 — 權限界限是一項進階功能，您可以在其中設定以身分識別為基礎的原則可授與給IAM實體 (IAM使用者或角色) 的最大權限。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需有關權限界限的詳細資訊，請參閱《IAM使用指南》中的IAM實體的權限界限。
- 服務控制策略 (SCPs) — SCPs 是指定中組織或組織單位 (OU) 最大權限的JSON策略 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。如果您啟用組織中的所有功能，則可以將服務控制策略 (SCPs) 套用至您的任何或所有帳戶。SCP限制成員帳戶中實體的權限，包括每個帳戶 AWS 帳戶根使用者。如需有關 Organizations 的詳細資訊SCPs，請參閱AWS Organizations 使用指南中的服務控制原則。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作

階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱《IAM使用指南》中的工作階段原則。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要瞭解如何在涉及多個原則類型時 AWS 決定是否允許要求，請參閱IAM使用指南中的原則評估邏輯。

如何 AWS Firewall Manager 使用 IAM

在您用IAM來管理 Firewall Manager 員的存取權之前，請先了解哪些IAM功能可搭配 Firewall Manager 員使用。

IAM您可以搭配使用的功能 AWS Firewall Manager

IAM特徵	Firewall Manager 支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	否
ACLs	否
ABAC(策略中的標籤)	是
暫時性憑證	是
轉寄存取工作階段 (FAS)	是
服務角色	部分
服務連結角色	是

若要取得 Firewall Manager 員和其他 AWS 服務如何與大部分IAM功能搭配運作的高階檢視，請參閱《IAM使用者指南》IAM中的適用AWS 服務。

Firewall Manager 員的身分識別型策略

支援身分型政策：是

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱IAM使用指南中的建立IAM策略。

使用以IAM身分識別為基礎的策略，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。若要瞭解可在JSON策略中使用的所有元素，請參閱《使用IAM者指南》中的IAMJSON策略元素參考資料。

若要檢視 Firewall Manager 員身分型策略的範例，請參閱。以身分識別為基礎的原則範例 AWS Firewall Manager

Firewall Manager 員的身分識別原則範例

若要檢視 Firewall Manager 員身分型策略的範例，請參閱。以身分識別為基礎的原則範例 AWS Firewall Manager

Firewall Manager 員中的資源型策略

支援資源型政策：否

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

若要啟用跨帳戶存取，您可以在以資源為基礎的策略中指定一個或多個帳戶中的一個或多個帳戶中的IAM實體作為主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主參與者和資源不同時 AWS 帳戶，受信任帳戶中的IAM管理員也必須授與主參與者實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。

Firewall Manager 員的政策處理

支援政策動作：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON策略Action元素描述了您可以用來允許或拒絕策略中存取的動作。策略動作通常與關聯的 AWS API操作具有相同的名稱。有一些例外情況，例如沒有匹配API操作的僅限權限的操作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 Firewall Manager 員動作清單，請參閱服務授權參考 AWS Firewall Manager中所定義的處理行動。

Firewall Manager 員中的策略處理行動會在處理行動前使用下列前置

```
fms
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "fms:action1",
      "fms:action2"
         ]
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 Describe 文字的所有動作，請包含以下動作：

```
"Action": "fms:Describe*"
```

若要檢視 Firewall Manager 員身分型策略的範例，請參閱。以身分識別為基礎的原則範例 AWS Firewall Manager

Firewall Manager 員的策略資源

支援政策資源：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

ResourceJSON原則元素會指定要套用動作的一個或多個物件。陳述式必須包含 Resource 或 NotResource 元素。最佳做法是使用其 Amazon 資源名稱 (ARN) 指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看 Firewall Manager 員資源類型及其清單ARNs，請參閱服務授權參考 AWS Firewall Manager中由定義的資源。若要瞭解您可以針對每個資源指定哪些動作，請參閱由定義ARN的動作 AWS Firewall Manager。

若要檢視 Firewall Manager 員身分型策略的範例，請參閱。以身分識別為基礎的原則範例 AWS Firewall Manager

Firewall Manager 員的政策條件金鑰

支援服務特定政策條件金鑰：否

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，只有在IAM使用者名稱標記資源時，您才可以授與IAM使用者存取資源的權限。如需詳細資訊，請參閱IAM使用指南中的IAM政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《使用指南》中的AWS 全域條件內IAM容索引鍵。

若要查看 Firewall Manager 員條件金鑰清單，請參閱服務授權參考 AWS Firewall Manager中的條件金鑰。若要瞭解您可以使用條件索引鍵的動作和資源，請參閱定義的動作 AWS Firewall Manager。

若要檢視 Firewall Manager 員身分型策略的範例，請參閱。以身分識別為基礎的原則範例 AWS Firewall Manager

ACLs在 Firewall Manager 器

支持ACLs：無

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

ABAC與 Firewall Manager 器

支援 ABAC (策略中的標籤): 是

以屬性為基礎的存取控制 (ABAC) 是一種授權策略，可根據屬性定義權限。在中 AWS，這些屬性稱為標籤。您可以將標籤附加至IAM實體 (使用者或角色) 和許多 AWS 資源。標記實體和資源是的第一步ABAC。然後，您可以設計ABAC策略，以便在主參與者的標籤符合他們嘗試存取的資源上的標籤時允許作業。

ABAC在快速成長的環境中很有幫助，並且有助於原則管理變得繁瑣的情況。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需有關的詳細資訊ABAC，請參閱什麼是ABAC？ 在《IAM使用者指南》中。若要檢視包含設定步驟的自學課程ABAC，請參閱《使用指南》中的〈使用以屬性為基礎的存取控制 (ABAC) IAM 〉。

搭配 Firewall Manager 員使用臨時憑

支援臨時憑證：是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配使用 AWS 服務 ，請參閱《IAM使用指南》IAM中的使用方式。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立臨時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需有關切換角色的詳細資訊，請參閱《IAM使用者指南》中的〈切換到角色 (主控台)〉。

您可以使用 AWS CLI 或手動建立臨時認證 AWS API。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱IAM。

「Firewall Manager 員」的轉寄存取

支援轉寄存取工作階段 (FAS)：是

當您使用使用IAM者或角色在中執行動作時 AWS，您會被視為主參與者。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。

Firewall Manager 員的服務角色

支援服務角色：部分

服務角色是服務假定代表您執行動作的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色 IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給

> **Warning**
>
> 變更服務角色的權限可能會中斷 Firewall Manager 員功能。只有在 Firewall Manager 員提供指引時，才編輯服務角色。

在 Firewall Manager 員中選擇IAM角色

若要使用 *PutNotificationChannel* API在 Firewall Manager 員中執行動作時，您必須選擇允許 Firewall Manager 員存取 Amazon 的角色，以SNS便服務可以代表您發佈 Amazon SNS 訊息。如需詳細資訊，請參閱〈AWS Firewall Manager API參考〉PutNotificationChannel中的〈〉。

以下顯示SNS主題權限設定的範例。若要將此政策與您自己的自訂角色搭配使用，請將 AWSServiceRoleForFMS Amazon 資源名稱 (ARN) 取代為 SnsRoleNameARN.

```
{
  "Sid": "AWSFirewallManagerSNSPolicy",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account ID:role/aws-service-role/
fms.amazonaws.com/AWSServiceRoleForFMS"
```

```
  },
  "Action": "sns:Publish",
  "Resource": "SNS topic ARN"
}
```

如需有關 Firewall Manager 員動作和資源的詳細資訊，請參閱 AWS Identity and Access Management 指南主題定義的動作 AWS Firewall Manager

Firewall Manager 員的服務連結角色

支援服務連結角色：是

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。

如需有關建立或管理服務連結角色的詳細資訊，請參閱使用IAM的AWS 服務。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

以身分識別為基礎的原則範例 AWS Firewall Manager

根據預設，使用者和角色沒有建立或修改 Firewall Manager 員資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

如需有關 Firewall Manager 定義的動作和資源類型的詳細資訊，包括每個資源類型的 ARN 格式，請參閱服務授權參考 AWS Firewall Manager中的動作、資源和條件索引鍵。

主題

- 政策最佳實務
- 使用 Firewall Manager 員主控台
- 允許使用者檢視他們自己的許可
- 授與 Firewall Manager 員安全性群組的讀取存取權

政策最佳實務

以身分識別為基礎的策略會決定某人是否可以建立、存取或刪除您帳戶中的 Firewall Manager 員資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您的使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需更多資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

使用 Firewall Manager 員主控台

若要存取 AWS Firewall Manager 主控台，您必須擁有最少一組權限。這些權限必須允許您列出並檢視有關 AWS 帳戶. 如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

若要確保使用者和角色仍可使用 Firewall Manager 主控台，請同時將 Firewall Manager 員*ConsoleAccess*或*ReadOnly* AWS 受管理的策略附加至實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

授與 Firewall Manager 員安全性群組的讀取存取權

Firewall Manager 員允許跨帳號資源存取，但不允許您建立跨帳號資源保護。您只能從擁有這些資源的帳戶內建立資源保護。

以下是授與所有資源`fms:Get`、`fms:List`和`ec2:DescribeSecurityGroups`動作權限的範例原則。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "fms:Get*",
                "fms:List*",
                "ec2:DescribeSecurityGroups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS 受管理的政策 AWS Firewall Manager

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新API作業可供現有服務使 AWS 服務 用時，最有可能更新 AWS 受管理的策略。

如需詳細資訊，請參閱IAM使用指南中的AWS 受管理策略。

AWS 受管理的策略：**AWSFMAdminFullAccess**

使用受AWSFMAdminFullAccess AWS 管理策略可讓您的系統管理員存取 AWS Firewall Manager 資源，包括所有 Firewall Manager 員策略類型。此政策不包括在中設定 Amazon 簡單通知服務通知的許可 AWS Firewall Manager。如需如何設定 Amazon 簡單通知服務存取權限的相關資訊，請參閱設定 Amazon 簡單通知服務的存取權限。

如需政策清單和詳細資訊，請參閱主IAM控台，位於AWSFMAdminFullAccess。本節的其餘部分提供原則設定的概觀。

權限聲明

根據權限集，此原則會分組為陳述式。

- AWS Firewall Manager 策略資源-允許中資源的完整管理權限 AWS Firewall Manager，包括所有 Firewall Manager 員策略類型。
- 將 AWS WAF 日誌寫入 Amazon 簡單儲存服務-允許 Firewall Manager 員在 Amazon S3 中寫入和讀取 AWS WAF 日誌。
- 建立服務連結角色 — 允許管理員建立服務連結角色，讓 Firewall Manager 代表您存取其他服務中的資源。此權限允許建立僅供 Firewall Manager 員使用的服務連結角色。如需 Firewall Manager 員如何使用服務連結角色的相關資訊，請參閱 使用 Firewall Manager 員的服務連結角色
- AWS Organizations— 可讓系統管理員針對中的組織使用 Firewall Manager 員 AWS Organizations。在中啟用 Firewall Manager 員的信任存取權之後 AWS Organizations，管理員帳戶的成員可以檢視其組織中的發現項目。若要取得有關 AWS Organizations 搭配使用的資訊 AWS Firewall Manager，請參閱《使 AWS OrganizationsAWS Organizations 用指南》中的「與其他 AWS 服務搭配

權限類別

以下列出策略中的權限類型及其提供的權限。

- `fms`— 使用 AWS Firewall Manager 資源.
- `waf`和 `waf-regional` — 使用 AWS WAF 傳統策略。
- `elasticloadbalancing`— 關聯 AWS WAF web ACLsto 彈性負載平衡器.
- `firehose`— 檢視有關 AWS WAF 防護記錄的資訊。
- `organizations`— 使用 Organ AWS izations 資源。
- `shield`— 檢視原 AWS Shield 則的訂閱狀態。

- `route53resolver`— 使用路由 53 私有DNS的路線 53 私人原VPCs則中的規則群組DNS的VPCs私人。
- `wafv2`— 使用 AWS WAFV2 原則。
- `network-firewall`— 使用 AWS Network Firewall 原則。
- `ec2`— 查看政策可用區域和區域。
- `s3`— 檢視有關 AWS WAF 防護記錄的資訊。

AWS 受管理的策略：**`FMSServiceRolePolicy`**

此原則可 AWS Firewall Manager 讓您在 Firewall Manager 員和整合式服務中代表您管理 AWS 資源。此政策連接至 `AWSServiceRoleForFMS` 服務連結角色。如需服務連結角色的詳細資訊，請參閱使用 Firewall Manager 員的服務連結角色。

如需策略詳細資訊，請參閱主IAM控台，位於FMSServiceRolePolicy。

AWS 受管理的策略： AWSFMAdminReadOnlyAccess

授予所有 AWS Firewall Manager 員資源的唯讀存取權。

如需政策清單和詳細資訊，請參閱主IAM控台，位於AWSFMAdminReadOnlyAccess。本節的其餘部分提供原則設定的概觀。

權限類別

以下列出策略中的權限類型，以及權限允許唯讀存取的資訊。

- `fms`— AWS Firewall Manager 資源.
- `waf`和 `waf-regional` — AWS WAF 經典政策。
- `firehose`— AWS WAF 日誌.
- `organizations`— Or AWS ganizations 資源。
- `shield`— AWS Shield 政策。
- `route53resolver`— 路由 53 私DNS人路由中的VPCs規則群組 53 私DNS人VPCs原則。
- `wafv2`— 中提供的 AWS WAFV2 規則群組和 AWS 受管規則群組 AWS WAFV2。
- `network-firewall`— AWS Network Firewall 規則群組和規則群組中繼資料。
- `ec2`— AWS Network Firewall 原則可用區域和區域。
- `s3`— AWS WAF 日誌.

AWS 受管理的策略： AWSFMMemberReadOnlyAccess

授與 AWS Firewall Manager 成員資源的唯讀存取權。如需政策清單和詳細資訊，請參閱主IAM控台，位於AWSFMMemberReadOnlyAccess。

Firewall Manager 員更新受 AWS 管理策略

檢視有關 Firewall Manager 員 AWS 受管理策略的詳細資料，因為此服務開始追蹤這些變更。如需有關此頁面變更的自動警示，請在「Firewall Manager 員」文件記錄頁面上訂閱RSS摘要，網址為文件歷史紀錄。

變更	描述	日期
FMSServiceRolePolicy-更新的政策	已新增 Firewall Manager 員服務角色原則的權限。 添加了讀取 Network Firewall TLS 配置信息的功能。請參閱IAM控制台中的更新策略：FMSServiceRolePolicy。	2024-07-22
FMSServiceRolePolicy-更新的政策	新增管理網路的權限ACLs。 請參閱IAM控制台中的更新策略：FMSServiceRolePolicy。	2024-04-22
FMSServiceRolePolicy-更新的政策	已新增允許「Firewall Manager 員」描述指定 AWS Config 規則是否符合規則的權限。 請參閱IAM控制台中的更新策略：FMSServiceRolePolicy。	2023-04-21
FMSServiceRolePolicy-更新的政策	新增允許 Firewall Manager 員描述 Amazon EC2 執行個體和網路界面屬性的許可。	2022-11-15

變更	描述	日期
	請參閱IAM控制台中的更新策略：FMSServiceRolePolicy。	
AWSFMAdminReadOnlyAccess-更新的政策	添加了支持 AWS WAFV2，Shield，Network Firewall，防火DNS牆，Amazon VPC 安全組，政策的許可。 請參閱IAM控制台中的更新策略：AWSFMAdminReadOnlyAccess。	2022-11-02
AWSFMAdminFullAccess-更新的政策	添加了支持 AWS WAFV2，Shield，Network Firewall，防火DNS牆，Amazon VPC 安全組，政策的許可。刪除了 Amazon SNS 許可。 請參閱IAM控制台中的更新策略：AWSFMAdminFullAccess。	2022-10-21
FMSServiceRolePolicy — AWS Firewall Manager 第三方防火牆策略的新權限	此變更可讓 Firewall Manager 員建立和刪除與第三方防火牆政策關聯的 Amazon EC2 VPC 端點。	2022-03-30
FMSServiceRolePolicy — AWS Network Firewall 政策的新權限	已新增新權限，以支援 Network Firewall 策略的防火牆部署。新權限允許針對原則範圍內的帳戶擷取有關可用區域的資訊。	2022-02-16

變更	描述	日期
FMSServiceRolePolicy — AWS Shield 政策的新權限	添加了新的權限，以檢索 AWS WAF 地區和 AWS WAF 全球資源的標籤。添加了使用資源檢索 Web ACLs 的 AWS WAF 地區權限ARN。新增支援 Shield 自動應用程式層DDoS緩解功能的權限。	2022-01-07
FMSServiceRolePolicy — AWS Shield 政策的新權限	已新增可擷取 Elastic Load Balancing 資源標籤的新權限。	2021-11-18
FMSServiceRolePolicy — 安全組和 AWS Network Firewall 策略的新權限	已新增新權限以啟用 AWS Network Firewall 原則的集中式記錄功能。此外，還新增了唯讀 Amazon EC2 許可以支援 Config 服務的變更，這些變更會影響 AWS Firewall Manager 查詢安全群組政策的資源方式。	2021-09-29
FMSServiceRolePolicy — AWS WAF 資源ARN格式	更新了FMSServiceRolePolicy 標準化 AWS WAF 資源的ARN格式。更新的ARN格式為arn:aws:waf:*:*:* 和arn:aws:waf-regional:*:*:* 。	2021-08-12
FMSServiceRolePolicy — 中國其他地區	AWS Firewall Manager 已FMSServiceRolePolicy 針對中國的BJS和ZHY地區啟用。	2021-08-12

變更	描述	日期
FMSServiceRolePolicy — 更新至現有政策	添加了允許管理 Amazon Route 53 Resolver DNS防火牆 AWS Firewall Manager 的新權限。 此變更可讓 Firewall Manager 員設定 Amazon Route 53 Resolver DNS防火牆關聯。這可讓您使用 Firewall Manager 員為您的VPCs整個組織提供DNS防火牆保護。 AWS Organizations	2021-03-17
Firewall Manager 員已開始追蹤	Firewall Manager 員開始追蹤其 AWS 受管理策略的變更。	2021-03-02

疑難排解 AWS Firewall Manager 身分和存取

使用下列資訊可協助您診斷並修正使用 Firewall Manager 員和 IAM 時可能會遇到的常見問題。

主題

- 我沒有在 Firewall Manager 器中執行操作的權限
- 我沒有授權執行 iam：PassRole
- 我想允許我以外的人訪問我 AWS 帳戶 的 Firewall Manager 器資源

我沒有在 Firewall Manager 器中執行操作的權限

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 fms:*GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fms:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 fms:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我沒有授權執行 iam：PassRole

如果您收到未授權執行iam:PassRole動作的錯誤訊息，您必須更新原則，才能讓您將角色傳遞給 Firewall Manager 員。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為的 IAM 使用者marymajor嘗試使用主控台在 Firewall Manager 員中執行動作時，會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我想允許我以外的人訪問我 AWS 帳戶 的 Firewall Manager 器資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要瞭解 Firewall Manager 員是否支援這些功能，請參閱如何 AWS Shield 使用 IAM。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM 使用者指南》中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 角色與資源型政策的差異。

使用 Firewall Manager 員的服務連結角色

AWS Firewall Manager 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 Firewall Manager 員的唯一 IAM 角色類型。服務連結角色由 Firewall Manager 預先定義，並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

服務連結角色可讓您更輕鬆地設定 Firewall Manager 員，因為您不需要手動新增必要的權限。Firewall Manager 員會定義其服務連結角色的權限，除非另有定義，否則只有 Firewall Manager 員可以擔任其角色。已定義的許可包括信任政策和許可政策。該許可政策無法連接至其他任何 IAM 實體。

您必須先刪除角色的相關資源，才能刪除服務連結角色。這樣可以保護您的 Firewall Manager 員資源，因為您無法意外移除存取資源的權限。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

Firewall Manager 員的服務連結角色權限

AWS Firewall Manager 使用服務連結的角色名稱， AWSServiceRoleForFMS 允許 Firewall Manager 代表您呼叫 AWS 服務，以管理防火牆策略和 AWS Organizations 帳號資源。此原則會附加至 AWS 受管理的角色AWSServiceRoleForFMS。如需有關受管理角色的詳細資訊，請參閱AWS 受管理的策略：FMSServiceRolePolicy。

服 AWSServiceRoleForFMS 務連結角色會信任服務擔任該角色fms.amazonaws.com。

角色權限策略允許 Firewall Manager 員對指定的資源完成下列動作：

- waf-管理您帳戶中的 AWS WAF 傳統 Web ACL，規則組權限以及 Web ACL 關聯。
- ec2-管理彈性網路界面和 Amazon EC2 執行個體上的安全群組。在 Amazon VPC 子網路上管理網路 ACL。
- vpc-在 Amazon VPC 中管理子網路、路由表、標籤和端點。
- wafv2-管理您帳戶中的 AWS WAF Web ACL，規則組權限和 Web ACL 關聯。
- cloudfront-創建 Web ACL 以保護發 CloudFront 行版。
- config-在您的帳戶中管理防火牆管理員擁有的 AWS Config 規則。
- iam-管理此服務連結角色，並在為 AWS WAF 和 Shield 策略配置記錄時建立必要的 AWS WAF 和 Shield 服務連結角色。
- organization-建立 Firewall Manager 員所擁有的服務連結角色，以管理 Firewall Manager 員使用的 AWS Organizations 資源。

- `shield`-管理您帳戶中資源的 AWS Shield 保護和 L7 緩解配置。
- `ram`-管理 AWS RAM DNS 防火牆規則群組和 Network Firewall 規則群組的資源共用。
- `network-firewall`-管理您帳戶中的防火牆管理員擁有的 AWS Network Firewall 資源和相依的 Amazon VPC 資源。
- `route53resolver`-在您的帳戶中管理防火牆管理器擁有的 DNS 防火牆關聯。

請參閱 IAM 主控台中的完整政策：FMS ServiceRolePolicy。

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

建立 Firewall Manager 員的服務連結角色

您不需要手動建立一個服務連結角色。當您在上啟用 Firewall Manager 員記錄 AWS Management Console，或在 Firewall Manager 員 CLI 或 Firewall Manager 員 API 中`PutLoggingConfiguration`提出要求時，Firewall Manager 員會為您建立服務連結角色。

您必須擁有 `iam:CreateServiceLinkedRole` 許可才能啟用記錄。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您啟用 Firewall Manager 員記錄時，Firewall Manager 員會再次為您建立服務連結角色。

編輯 Firewall Manager 員的服務連結角色

Firewall Manager 員不允許您編輯 AWSServiceRoleForFMS 服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需更多資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除 Firewall Manager 員的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 如果您嘗試刪除資源時，Firewall Manager 員服務正在使用該角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

使用 IAM 刪除服務連結角色

使用 IAM 主控台、IAM CLI 或 IAM API 刪除 AWSServiceRoleForFMS服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

Firewall Manager 員服務連結角色的支援區域

Firewall Manager 員支援在提供服務的所有區域中使用服務連結角色。如需詳細資訊，請參閱 Firewall Manager 員端點和配額。

預防跨服務混淆代理人

混淆代理人問題屬於安全性議題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在中 AWS，跨服務模擬可能會導致混淆的副問題。在某個服務 (呼叫服務) 呼叫另一個服務 (被呼叫服務) 時，可能會發生跨服務模擬。可以操縱呼叫服務來使用其許可，以其不應有存取許可的方式對其他客戶的資源採取動作。為了預防這種情況， AWS 提供的工具可協助您保護所有服務的資料，而這些服務主體已獲得您帳戶中資源的存取權。

我們建議在資源策略中使用aws:SourceArn和aws:SourceAccount全域條件前後關聯索引鍵，以限制將其他服務 AWS Firewall Manager 提供給資源的權限。如果您想要僅允許一個資源與跨服務存取相關聯，則請使用 aws:SourceArn。如果您想要允許該帳戶中的任何資源與跨服務使用相關聯，請使用 aws:SourceAccount。

防範混淆代理人問題的最有效方法是使用 aws:SourceArn 全域條件內容索引鍵，以及資源的完整 ARN。如果不知道資源的完整 ARN，或者如果您指定了多個資源，請使用 aws:SourceArn 全域內容條件索引鍵搭配萬用字元 (*) 來表示 ARN 的未知部分。例如 arn:aws:fms:*:*account-id*:*。

如果 aws:SourceArn 值不包含帳戶 ID (例如 Amazon S3 儲存貯體 ARN)，您必須使用這兩個全域條件內容索引鍵來限制許可。

的值aws:SourceArn必須是 AWS Firewall Manager 管理員 AWS 帳戶。

下列範例說明如何使用 Firewall Manager 中的aws:SourceArn全域條件內容金鑰來避免混淆的副問題。

下列範例顯示如何使用 Firewall Manager 角色信任原則中的aws:SourceArn全域條件內容金鑰來避免混淆的副問題。用您自己的信息替換*##*和*## ID*。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
```

```
    "Principal": {
      "Service": "servicename.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": [
          "arn:aws:fms:Region:account-id:${*}",
          "arn:aws:fms:Region:account-id:policy/*"]
      },
      "StringEquals": {
        "aws:SourceAccount": "account-id"
      }
    }
  }
}
```

Firewall Manager 員中的記錄和監控

監控是維護 Firewall Manager 員和 AWS 解決方案的可靠性、可用性和效能的重要組成部分。您應該從 AWS 解決方案的所有部分收集監視資料，以便在發生多點失敗時更輕鬆地偵錯。 AWS 提供數種工具來監控 Firewall Manager 員資源並回應潛在事件：

Amazon CloudWatch 警報

您可以使用 CloudWatch 警示來監視指定期間內的單一量度。如果指標超過指定臨界值，則 CloudWatch 會傳送通知給 Amazon SNS 主題或 AWS Auto Scaling 政策。如需詳細資訊，請參閱使用 Amazon 監控 CloudWatch。

AWS CloudTrail 日誌

CloudTrail 提供使用者、角色或 AWS 服務在 Firewall Manager 員中所採取的動作記錄。使用收集的資訊 CloudTrail，您可以判斷向 Firewall Manager 發出的要求、提出要求的 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。如需更多詳細資訊，請參閱 使用 AWS CloudTrail 記錄 API 呼叫。

Firewall Manager 員的合規驗證

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於您資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上進行HIPAA安全與合規架構 — 本白皮書說明公司如何使用建立符合資格的應 AWS 用程HIPAA式。

> **Note**
>
> 並非所有 AWS 服務 人都HIPAA符合資格。如需詳細資訊，請參閱合HIPAA格服務參考資料。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準 AWS 服務 與技術研究所 (NIST)、支付卡產業安全標準委員會 () 和國際標準化組織 ()) 中保護安全控制指引的最佳實務作法，並將其對應至安全性控制。PCI ISO
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您因應各種合規性需求 PCIDSS，例如符合特定合規性架構所要求的入侵偵測需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

Firewall Manager 程式中的

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠在可用區域之間自動容錯移轉，而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱AWS 全域基礎結構。

AWS Firewall Manager中的基礎設施安全

作為託管服務， AWS Firewall Manager 受到 AWS 全球網絡安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的API呼叫透過網路存取 Firewall Manager 員。使用者端必須支援下列專案：

- 傳輸層安全性 (TLS)。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 具有完美前向保密（ ）的密碼套件，例如（短暫的迪菲-赫爾曼PFS）或DHE（橢圓曲線短暫迪菲-赫爾曼）。ECDHE現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與IAM主體相關聯的秘密存取金鑰來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 以產生暫時安全憑證以簽署請求。

AWS Firewall Manager 配額

AWS Firewall Manager 受以下配額約束 (先前稱為限制)。

AWS Firewall Manager 具有預設配額，您可能可以增加和固定配額。

由 Firewall Manager 員管理的安全群組政策和網路 ACL 政策受標準 Amazon VPC 配額約束。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的 Amazon VPC 配額。

每個 Firewall Manager 員 Network Firewall 策略都會建立具有關聯防火牆策略及其規則群組的 Network Firewall。這些 Network Firewall 資源受到《Net work Firewall 開發人員指南》中列出的AWS Network Firewall 配額限制。

軟配額

AWS Firewall Manager 每個區域的實體數量都有預設配額。您可以請求提高這些配額。

所有原則類型

資源	每個區域的預設配額
中每個組織的帳戶 AWS Organizations	各有不同。傳送給帳戶的邀請計入此配額。若受邀帳戶拒絕、管理帳戶取消邀請或邀請到期，便會退回計數。
中每個組織的 Firewall Manager 員策略 AWS Organizations。	50。「地區」規格Global並US East (N. Virginia) Region指相同的區域，因此此限制適用於兩者的總合併政策。
每個 Firewall Manager 員策略範圍內的組織單位。	20
在 Firewall Manager 員策略範圍內的帳戶（如果您明確包含和排除個別帳戶）。	200
如果您未明確包含或排除個別帳戶，則屬於 Firewall Manager 員策略範圍內的帳戶。	2,500
根據 Firewall Manager 員策略包含或排除資源的標籤。	8
每個帳號的資源集數目。	20
每個資源集的資源數目。	100
每個 Firewall Manager 員策略的資源集數目。	5

AWS WAF 政策

資源	每個區域的預設配額
AWS WAF 每個 Firewall Manager 員管理員帳戶的規則群	100
AWS WAF 每個 Firewall Manager 員帳戶的傳統規則群組。	10
每個 AWS WAF 策略的規則群組。	50

常見安全群組政策

資源	每個區域的預設配額。
每個原則的主要安全性群組。	3
Amazon VPC 執行個體範圍涵蓋每個帳戶的每個政策，包括共用的 VPC。	100

內容稽核安全群組政策

資源	每個區域的預設配額
稽核每個策略的安全性群組。	1
每個應用程式清單的應用	50
允許所有流量的規則的自訂受管理應用程式清單。	1
每個策略規則的自訂受管理應用程式列	1
每個帳戶的自訂受管應用程式清單	10
每個協議列表的協議。	5
原則中任何設定的自訂受管通訊協定清單。	1
每個帳戶的自訂受管協定清單。	10

網路 ACL 政策

資源	每個區域的預設配額
每個網路 ACL 原則的輸入規則數目，用於第一個或最後一個規則。例如，您可以有 5 個第一個和 0 個最後一個輸入規則，或者 2 個第一個和 3 個最後一個，但不能有 4 個第一個和 2 個最後一個。	5
每個網路 ACL 原則的輸出規則數目，用於第一個或最後一個規則。例如，您可以有 5 個第一個和 0 個最後一個輸出規則，或者 2 個第一個和 3 個最後一個，但不能有 4 個第一個和 2 個最後一個。	5

DNS 防火牆政策

資源	每個區域的預設配額
每個 DNS 防火牆策略的 DNS 防火牆規則群組。	2

硬配額

以下與之相關的每個區域配額 AWS Firewall Manager 無法變更。

所有原則類型

資源	每個地區的配額
AWS Organizations 組織中可以擁有的 Firewall Manager 員管理員數目上限。您必須擁有一位預設管理員，以及多達 9 個額外的 Firewall Manager 員管理員。	10

AWS WAF 政策

資源	每個地區的配額
AWS WAF 政策中規則群組的 Web ACL 容量單位 (WCU) 總計。	5,000

AWS WAF 經典政策

資源	每個地區的配額
AWS WAF 每個策略的傳統規則群組。	2：1 個客戶建立的規則群組和 1 個 AWS Marketplace 規則群組。
AWS WAF 每個 Firewall Manager 員 AWS WAF 傳統規則群組的傳統規則	10

安全性群組內容稽核策略

資源	每個地區的配額
策略中任何設定的 Firewall Manager 員受管理應用程式清單。	1
策略中任何設定的「Firewall Manager 員」管理通訊協定清單。	1

Network Firewall 策略

資源	每個地區的配額
可針對單一原則自動修復的 VPC 數目。	1,000
您可以為單一原則提供的 IPV4 CIDR 數目。	50

監控 AWS WAFAWS Firewall Manager，以及 AWS Shield Advanced

監控是維持服務可靠性、可用性和效能的重要組成部分。

> **Note**
>
> 如需使用「Shield 牌進階」監控進階資源和識別可能的 DDoS 事件的相關資訊，請參閱AWS Shield。

在您開始監控這些服務時，應該先建立包含下列問題之回答的監控計劃：

- 監控目標是什麼？
- 要監控哪些資源？
- 監控這些資源的頻率為何？
- 要使用哪些監控工具？
- 誰將執行監控任務？
- 發生問題時應該通知誰？

下一步是在各個時間點和不同的負載條件下測量效能，以在您的環境中確立 正常效能的基準。當您監控 Firewall Manager 員 AWS WAF、Shield Advanced 和相關服務時，會儲存歷史監控資料，以便您可以將其與目前的效能資料進行比較，識別正常的效能模式和效能異常，並設計解決問題的方法。

對於 AWS WAF，您應該至少監視下列項目以建立基準線：

- 允許的 Web 要求數目
- 封鎖的 Web 要求數目

主題

- 監控工具
- 使用 Amazon 監控 CloudWatch
- 使用 AWS CloudTrail記錄 API 呼叫

監控工具

AWS 提供了可用於監視 AWS WAF 和的各種工具 AWS Shield Advanced。您可以設定其中一些工具為您監控，但其他工具則需要手動介入。建議您盡可能自動化監控任務。

自動化監控工具

您可以使用以下自動監視工具來觀看 AWS WAF AWS Shield Advanced 和報告出現問題時：

- Web ACL 流量概觀儀表板 — 前往 AWS WAF 主控台中的 Web ACL 頁面並開啟「流量概觀」索引標籤，以存取 Web ACL 評估的 Web 流量摘要。

  流量概觀儀表板提供近乎即時的 Amazon CloudWatch 指標摘要，這些指標會在評估應用程式 Web 流量時 AWS WAF 收集到。您可以查看所有 Web 流量的摘要，以及智慧型威脅緩和規則群組評估的流量摘要。

  如需詳細資訊，請參閱網頁 ACL 流量概觀儀表板或移至主控台中的儀表板。

- Amazon CloudWatch 警示 — 觀看您指定期間內的單一指標，並根據指定臨界值在多個時段內相對於指定閾值的指標值執行一或多個動作。此動作是傳送到 Amazon Simple Notification Service (Amazon SNS) 主題或 Amazon EC2 Auto Scaling 政策的通知。警示只會呼叫持續狀態變更的動作。 CloudWatch 警示不會僅因為處於特定狀態而叫用動作；狀態必須已變更並維持指定數目的期間。如需詳細資訊，請參閱使用監視 CloudFront活動 CloudWatch。

  > **Note**
  >
  > CloudWatch 未啟用度量和警示 AWS Firewall Manager。

  您不僅可以按照中所述用 CloudWatch 於監視 AWS WAF 和 Shield 高級指標使用 Amazon 監控 CloudWatch，還應該使用 CloudWatch 來監視受保護資源的活動。如需詳細資訊，請參閱下列內容：

  - 使用 Amazon CloudFront 開發人員指南 CloudWatch中的監控 CloudFront 活動
  - API Gateway 開發人員指南中的 Amazon API Gateway 中的記錄和監控
  - CloudWatch E lastic Load Balancing 使用者指南中的應用程式負載平衡器指標
  - 在AWS AppSync 開發人員指南中進行監控和記錄
  - Amazon Cognito 開發人員指南中的記錄和監控

  - 檢視串流至記錄的應用程式執行程式 CloudWatch 記錄，並檢視AWS App Runner 開發人員指南 CloudWatch中回報的應用程式執行器服務
- Amazon CloudWatch 日誌 — 監控、存放和存取來自 AWS CloudTrail 或其他來源的日誌檔。如需詳細資訊，請參閱什麼是 Amazon CloudWatch 日誌？ 。
- Amazon CloudWatch 活動 — 自動化您的 AWS 服務並自動回應系統事件。來自 AWS 服務的事件會以近乎即時的速度傳遞至 E CloudWatch vents，而且您可以指定當事件符合您撰寫的規則時要採取的自動化動作。如需詳細資訊，請參閱什麼是 Amazon CloudWatch 活動？
- AWS CloudTrail 記錄監控 — 在帳戶之間共用記錄檔、即時監控記 CloudTrail 錄檔案，方法是將記錄檔傳送至 CloudWatch 記錄檔、以 Java 撰寫記錄處理應用程式，以及驗證您的記錄檔在傳送之後未變更。 CloudTrail若要取得更多資訊使用 AWS CloudTrail記錄 API 呼叫，請參閱《使用指南》中的〈AWS CloudTrail 使用 CloudTrail 記錄檔〉。
- AWS Config— 檢視您 AWS 帳戶中 AWS 資源的組態，包括資源彼此之間的關聯性，以及過去如何配置這些資源，以便您可以查看組態和關係在一段時間內的變化。

手動監控工具

監視的另一個重要組成部分， AWS Shield Advanced 涉 AWS WAF 及手動監視 CloudWatch 警報未涵蓋的項目。您可以檢視 AWS WAF、Shield Advanced 和其他 AWS Management Console 儀表板 CloudWatch，以查看 AWS 環境的狀態。我們建議您也檢查 Web ACL 和規則的記錄檔。

- 例如，若要檢視 AWS WAF 控制面板：
  - 在 [AWS WAF Web ACL] 頁面的 [要求] 索引標籤上，檢視符合您建立之每個規則的要求和要求總計圖表。如需詳細資訊，請參閱 檢視 Web 請求的範例。
- 檢視下列項目的 CloudWatch 首頁：
  - 目前警示與狀態
  - 警示與資源的圖表
  - 服務運作狀態

  此外，您可以使用執行 CloudWatch 以下操作：
  - 建立自訂儀表板以監控您注重的服務。
  - 用於疑難排解問題以及探索驅勢的圖形指標資料。
  - 搜尋並瀏覽所有資 AWS 源指標。
  - 建立與編輯要通知發生問題的警示。

使用 Amazon 監控 CloudWatch

您可以使用 Amazon 監控 Web 請求、Web ACL 和規則 CloudWatch，Amazon 會從中收集原始資料並處理 AWS Shield Advanced 成可讀 AWS WAF 且接近即時的指標。您可以使用 Amazon 中的統計信息 CloudWatch 來了解 Web 應用程序或服務的執行情況。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南 CloudWatch中的內容。

> **Note**
>
> CloudWatch Firewall Manager 員未啟用指標和警示。

您可以建立 Amazon CloudWatch 警示，在警示狀態變更時傳送 Amazon SNS 訊息。警示會監看您指定時段的單個指標，然後根據幾個時間段內與指定閾值相關的指標值來執行一或多個動作。此動作是傳送到 Amazon SNS 主題或 Auto Scaling 政策的通知。警示只會呼叫持續狀態變更的動作。CloudWatch 警示不會僅因為處於特定狀態而叫用動作；狀態必須已變更並維持指定數目的期間。

主題

- 檢視指標和維度
- AWS WAF 量度和維度
- AWS Shield Advanced 度量
- AWS Firewall Manager 通知

檢視指標和維度

測量結果會先依服務命名空間分組，然後依每個命名空間內的各種維度組合分組。 AWS Firewall Manager 不記錄指標。

- AWS WAF 命名空間是 `AWS/WAFV2`
- Shield 高級命名空間是 `AWS/DDoSProtection`

> **Note**
>
> AWS WAF 每分鐘報告一次量度。
> 「Shield 牌進階」會在活動期間每分鐘報告一次指標，其他時間則較少報告指標

使用下列程序來檢視 AWS WAF 和的測量結果 AWS Shield Advanced。

使用 CloudWatch 主控台檢視指標

1. 請登入 AWS Management Console 並開啟 CloudWatch 主控台，網址為 https://console.aws.amazon.com/cloudwatch/。
2. 如有必要，請將「地區」變更為資 AWS 源所在的地區。對於 CloudFront，選擇美國東部 (維吉尼亞北部) 區域。
3. 在導覽窗格的「量度」下，選擇「所有量度」，然後在「瀏覽」索引標籤下搜尋服務。

若要使用 AWS CLI 檢視測量結果

- 對於 AWS/WAFV2，請在命令提示字元中使用下列命令：

```
aws cloudwatch list-metrics --namespace "AWS/WAFV2"
```

針對「Shield 進階」，在命令提示字元中使用下列命令：

```
aws cloudwatch list-metrics --namespace "AWS/DDoSProtection"
```

AWS WAF 量度和維度

AWS WAF 每分鐘報告一次量度。 AWS WAF 在AWS/WAFV2命名空間中提供量度和維度。

您可以透過 AWS WAF 主控台，在 Web ACL 的流 AWS WAF 量概觀索引標籤中查看指標的摘要資訊。如需詳細資訊，請前往主控台，或參閱網頁 ACL 流量概觀儀表板。

您可以看到下列 Web ACL、規則、規則群組和標籤的量度。

- 您的規則 — 量度依規則動作分組。例如，當您在Count模式中測試規則時，其相符項目會列為 Web ACL 的Count度量。
- 您的規則群組 — 規則群組的量度會列在規則群組量度下。
- 另一個帳戶擁有的規則群組 — 規則群組量度通常只有規則群組擁有者才能看到。不過，如果您覆寫規則的規則動作，則該規則的度量會列在您的 Web ACL 量度下。此外，任何規則群組新增的標籤都會列在 Web ACL 量度中

此類別中的規則群組是AWS 的受管規則 AWS WAF另一個帳戶與您共用的由其他服務提供的規則群組、、和規則群組。AWS Marketplace 受管規則群組

- 標籤-在評估期間新增至 Web 要求的標籤會列在 Web ACL 標籤度量中。您可以存取所有標籤的量度，無論這些標籤是由您的規則和規則群組新增，還是由其他帳戶擁有的規則群組中的規則新增。

主題

- Web ACL、規則群組以及規則度量和維度
- 標示量度和維度
- 免費機器人可見度指標和維度

Web ACL、規則群組以及規則度量和維度

Web ACL、規則群組和規則測量結果

指標	描述
AllowedRequests	允許的 Web 要求數目。 報告條件：有非零值。 有效的統計資訊：總和
BlockedRequests	封鎖的 Web 要求數目。 報告條件：有非零值。 有效的統計資訊：總和
CountedRequests	計入的 Web 要求數目。 報告條件：有非零值。 計算的 Web 請求是指至少符合其中一個規則的請求。請求計數一般用於測試。 有效的統計資訊：總和
CaptchaRequests	套用了驗證碼控制項的網頁要求數目。

指標	描述
	報告條件：有非零值。 CAPTCHA 網頁要求是與具有CAPTCHA動作設定的規則相符的要求。此指標會記錄所有匹配的請求，無論它們是否具有有效的 CAPTCHA 令牌。 有效的統計資訊：總和
RequestsWithValidCaptchaToken	套用了 CAPTCHA 控制項且具有有效驗證碼權杖的網頁要求數目。 報告條件：有非零值。 有效的統計資訊：總和
CaptchasAttempted	終端使用者為了回應驗證碼難題挑戰而提交的解決方案數量。 報告條件：有非零值。 有效的統計資訊：總和
CaptchasSolved	提交成功解決難題的驗證碼拼圖解決方案的數量。 報告條件：有非零值。 有效的統計資訊：總和
ChallengeRequests	套用了挑戰控制項的 Web 要求數目。 報告條件：有非零值。 挑戰 Web 要求是符合具有Challenge動作設定的規則的要求。此量度會記錄所有符合的要求，不論它們是否具有有效的挑戰 Token。 有效的統計資訊：總和

指標	描述
RequestsWithValidChallengeToken	已套用挑戰控制項且具有有效挑戰權杖的 Web 要求數目。 報告條件：有非零值。 有效的統計資訊：總和
PassedRequests	傳遞的要求數目。這僅適用於經過規則群組評估但不符合任何規則群組規則的要求。 報告條件：有非零值。 傳遞的要求是不符合規則群組中任何規則的要求。 有效的統計資訊：總和

網頁 ACL、規則群組和規則維度

維度	描述
Region	除了 Amazon CloudFront 分發以外，所有受保護的資源類型都需要此項
Rule	下列其中一項： • Rule 的指標名稱。 • ALL，代表 WebACL 或 RuleGroup 內的所有規則。 • Default_Action (僅適用於與WebACL維度結合時)，表示指派給任何請求的動作，而該請求的評估未因 Web ACL 中的規則動作終止。
RuleGroup	RuleGroup 的指標名稱。
WebACL	WebACL 的指標名稱。

維度	描述
Country	請求的來源國。這是來自國際標準化組織 (ISO) 3166 標準的兩個字元名稱。例如，US 代表美國和 UA 代表烏克蘭。 如果請求具有X-Forwarded-For 標頭，則 AWS WAF 使用該標題來確定此設置。否則， AWS WAF 會使用用戶端 IP 的國家/地區。此決定與您在規則中使用的任何邏輯無關，以確定原籍國。 AWS WAF 確定使用 MaxMind GeoIP 數據庫的 IP 的位置。
Attack	根據您在 Web ACL 中使用的規則和規則群組，在要求中 AWS WAF 識別的攻擊類型。 您的規則和基準 AWS 管理規則群組中的規則可以識別攻擊類型。例如，跨網站指令碼 (XSS) 規則符合可識別 XSS 攻擊類型，而以速率為基礎的規則則可識別容量攻擊類型。攻擊類型通常表示終止 Web 請求評估的規則類型。
Device	傳送要求的用戶端裝置類型 (從 Web 要求的user-agent 標頭取得)。
ManagedRuleGroup	ManagedRuleGroup 的指標名稱。
ManagedRuleGroupRule	已符合ManagedRuleGroup 的規則。

標示量度和維度

根據規則評估期間以及您在 Web ACL 中使用的受管規則群組新增至要求的標籤量度。如需相關資訊，請參閱網頁要求上的標籤。

對於任何單一 Web 請求，最多可 AWS WAF 儲存 100 個標籤的指標。您的 Web ACL 評估可以套用 100 個以上的標籤，並與 100 個以上的標籤進行比對，但只有前 100 個標籤會反映在量度中。

標籤指標

指標	描述
AllowedRequests	已Allow套用動作設定之 Web 要求上的標籤數目。您可以在 Web 要求評估期間隨時新增這些標籤。 報告條件：有非零值。 有效的統計資訊：總和
BlockedRequests	已Block套用動作設定之 Web 要求上的標籤數目。您可以在 Web 要求評估期間隨時新增這些標籤。 報告條件：有非零值。 有效的統計資訊：總和
CountedRequests	依規則群組規則 (具有Count動作設定) 新增至 Web 要求的標籤數目。 此量度僅供規則群組的擁有者使用，適用於規則群組內的規則。在其他情況下，計數標籤量度會彙總到套用至要求的終止動作，例如Allow或Block。 報告條件：有非零值。 有效的統計資訊：總和
CaptchaRequests	已套用終止CAPTCHA動作之 Web 要求上的標籤數目。您可以在 Web 要求評估期間隨時新增這些標籤。 報告條件：有非零值。 有效的統計資訊：總和
ChallengeRequests	已套用終止Challenge動作之 Web 要求上的標籤數目。您可以在 Web 要求評估期間隨時新增這些標籤。 報告條件：有非零值。 有效的統計資訊：總和

指標	描述
AllowRuleMatch	產生關聯標籤並使用動作終止要求評估的相符規則數Allow目。 報告條件：有非零值。 有效的統計資訊：總和
BlockRuleMatch	產生關聯標籤並使用動作終止要求評估的相符規則數Block目。 報告條件：有非零值。 有效的統計資訊：總和
CountRuleMatch	產生關聯標籤並套用Count動作的符合規則數目。 如果使用相同的標籤和動作設定多個規則，則一個要求可能會產生此指標的多個執行個體。 報告條件：有非零值。 有效的統計資訊：總和
CaptchaRuleMatch	產生關聯標籤並使用動作終止要求評估的相符規則數CAPTCHA目。 報告條件：有非零值。 有效的統計資訊：總和
ChallengeRuleMatch	產生關聯標籤並使用動作終止要求評估的相符規則數Challenge目。 報告條件：有非零值。 有效的統計資訊：總和

指標	描述
CaptchaRuleMatchWithValidToken	產生關聯標籤並套用非終止動作CAPTCHA的符合規則數目。 如果使用相同的標籤和動作設定多個規則，則一個要求可能會產生此指標的多個執行個體。 報告條件：有非零值。 有效的統計資訊：總和
ChallengeRuleMatchWithValidToken	產生關聯標籤並套用非終止動作Challenge的符合規則數目。 如果使用相同的標籤和動作設定多個規則，則一個要求可能會產生此指標的多個執行個體。 報告條件：有非零值。 有效的統計資訊：總和

標籤尺寸

維度	描述
Region	除了 Amazon CloudFront 分發以外，所有受保護的資源類型都需要此項
WebACL	WebACL 的指標名稱。
RuleGroup	RuleGroup 的指標名稱。用於量度CountedRequests 。
LabelNamespace	新增至要求之標籤的命名空間前置詞。
Label	新增至要求的標籤名稱。
Context	作為標籤新增前後關聯的受管理規則群組。例如，權杖管理標籤的前後關聯awswaf:managed:tok

維度	描述
	en:accepted 是在請求上使用權杖管理的 AWS WAF 受管規則群組，例如機器人控制或 ATP 管理規則群組。此維度不適用於所有標籤。

免費機器人可見度指標和維度

當您未在 Web ACL 中使用機器人控制時，會將機器人控制受管規則群組 AWS WAF 套用至 Web 請求的取樣，而無需額外付費。這可以提供來自受保護資源的機器人流量的概念。如需機器人控制的相關資訊，請參閱AWS WAF 機器人控制規則群組。

免費的機器人可見度

指標	描述
SampleAllowedRequest	具Allow有動作的取樣要求數目。 報告條件：有非零值。 有效的統計資訊：總和
SampleBlockedRequest	具Block有動作的取樣要求數目。 報告條件：有非零值。 有效的統計資訊：總和
SampleCaptchaRequest	具CAPTCHA有動作的取樣要求數目。 報告條件：有非零值。 有效的統計資訊：總和
SampleChallengeRequest	具Challenge有動作的取樣要求數目。 報告條件：有非零值。 有效的統計資訊：總和
SampleCountRequest	具Count有動作的取樣要求數目。

指標	描述
	報告條件：有非零值。 有效的統計資訊：總和

免費的機器人可見度

維度	描述
`Region`	除了 Amazon CloudFront 分發以外，所有受保護的資源類型都需要此項
`WebACL`	`WebACL` 的指標名稱。
`BotCategory`	根據 Web 要求標籤，偵測到的機器人類別名稱。
`VerificationStatus`	根據 Web 要求標籤，偵測到的機器人驗證狀態的名稱。
`Signal`	根據 Web 請求標籤，偵測到的機器人訊號的名稱。

AWS Shield Advanced 度量

Shield Advanced 針對其保護的所有資源發佈 Amazon CloudWatch 偵測、緩解措施和主要貢獻者指標。這些指標可以為資源建立和設定 CloudWatch 儀表板和警示，從而提升您監視資源的能力。

Shield 進階主控台會顯示其記錄的許多指標摘要。如需相關資訊，請參閱DDoS 事件的可見性。

如果您為應用程式層保護啟用自動應用程式層 DDoS 緩解功能，

量度報告位置

Shield Advanced 會`us-east-1`針對下列項目報告美國東部 (維吉尼亞北部) 區域的量度：

- 全球服務 Amazon CloudFront 和 Amazon 路線 53.
- 保護群組。如需有關保護群組的資訊，請參閱AWS Shield Advanced 保護群組。

對於其他資源類型，「Shield 牌進階」會報告資源「區域」中的度量。

量度報告的時間

Shield A AWS dvanced CloudWatch 在 DDoS 事件期間向 Amazon 報告指標的頻率高於沒有事件正在進行的情況下。「Shield 牌進階」會在活動期間每分鐘報告一次指標，然後在活動結束後立即報告一次指標。

雖然沒有任何事件正在進行中，Shield Advanced 會在指派給資源的時間每天報告一次度量。此定期報告會保持量度處於作用中狀態，並可用於自訂 CloudWatch 警示和儀表板。

警報建議

我們建議您建立警報，以通知您需要注意的情況。作為起點，您可以為每個受保護的資源創建警報，該警報在DDoSDetected檢測指標非零時報告。此指標中的非零值並不一定意味著 DDoS 攻擊正在進行中，但我們建議您在指標處於此狀態時仔細查看資源狀態。

對於請求洪水，我們建議您為複合檢查建立警示，這些檢查也會考慮應用程式健康狀況和 Web 要求數量等因素。您可以選擇對報告各種攻擊向量維度的流量的其他三個量度發出警報。通過考慮應用程序的容量並在流量接近應用程序限制時發出警報，您可以創建一組規則，根據需要通知您，而不會產生太多不必要的噪音。

主題

偵測指標

Shield 進階提供命AWS/DDoSProtection名空間中的度量和維度。

偵測指標

指標	描述
DDoSDetected	指出特定 Amazon Resource Name (ARN) 是否正遭遇 DDoS 事件。 此測量結果在事件期間的值非零。
DDoSAttackBitsPerSecond	在特定 Amazon Resource Name (ARN) 的 DDoS 事件期間觀察到的位元組數。此指標僅適

指標	描述
	用於網路和傳輸層 (第 3 層和第 4 層) DDoS 事件。 此測量結果在事件期間的值非零。 單位：位元
DDoSAttackPacketsPerSecond	在特定 Amazon Resource Name (ARN) 的 DDoS 事件期間觀察到的封包數量。此指標僅適用於網路和傳輸層 (第 3 層和第 4 層) DDoS 事件。 此測量結果在事件期間的值非零。 單位：封包數
DDoSAttackRequestsPerSecond	在特定 Amazon Resource Name (ARN) 的 DDoS 事件期間觀察到的請求數量。本指標僅適用於 layer 3/4 的 DDoS 事件。本指標只會回報為最重大的 Layer 7 事件。 此測量結果在事件期間的值非零。 單位：請求

「Shield 牌進階」會在不包含其他維度的情況下DDoSDetected張貼 其餘的偵測指AttackVector標包括對應於攻擊類型的維度，從下列清單中：

- ACKFlood
- ChargenReflection
- DNSReflection
- GenericUDPReflection
- MemcachedReflection
- MSSQLReflection
- NetBIOSReflection
- NTPReflection

- PortMapper
- RequestFlood
- RIPReflection
- SNMPReflection
- SSDPReflection
- SYNFlood
- UDPFragment
- UDPTraffic
- UDPReflection

緩解指標

Shield 牌進階在AWS/DDoSProtection命名空間中提供量度和維度。

緩解指標

指標	描述
VolumePacketsPerSecond	針對偵測到的事件而部署的緩和措施捨棄或傳遞的每秒封包數目。 單位：封包數

緩解維度

維度	描述
ResourceArn	Amazon Resource Name (ARN)
MitigationAction	套用緩和措施的結果。可能的值為 Pass 或 Drop。

頂級貢獻者指標

Shield 進階在AWS/DDoSProtection命名空間中提供度量。

頂級貢獻者指標

指標	描述
VolumePacketsPerSecond	頂尖貢獻者每秒的封包數目。 單位：封包數
VolumeBitsPerSecond	頂尖貢獻者每秒的位元數。 單位：位

Shield Advanced 會根據特徵事件貢獻者的維度組合來張貼頂尖貢獻者量度。您可以針對任何主要貢獻者量度使用下列任何維度組合：

- ResourceArn, Protocol
- ResourceArn, Protocol, SourcePort
- ResourceArn, Protocol, DestinationPort
- ResourceArn, Protocol, SourceIp
- ResourceArn, Protocol, SourceAsn
- ResourceArn, TcpFlags

頂尖貢獻者維度

維度	描述
ResourceArn	Amazon 資源名稱（ARN）。
Protocol	IP 通訊協定名稱，TCP或UDP。
SourcePort	來源 TCP 或 UDP 連接埠。
DestinationPort	目的地 TCP 或 UDP 連接埠。
SourceIp	來源 IP 位址。
SourceAsn	來源自主系統編號 (ASN)。

維度	描述
TcpFlags	TCP 封包中存在的旗標組合，以破折號 (-) 分隔。受監控的旗標為ACKFIN、RST、、SYN。此尺寸值始終按字母順序排序顯示。例如：ACK-FIN-RST-SYN、ACK-SYN 和 FIN-RST。

AWS Firewall Manager 通知

AWS Firewall Manager 不會記錄指標，因此您無法專門為 Firewall Manager 員建立 Amazon CloudWatch 警示。不過，您可以設定 Amazon SNS 通知，提醒您潛在攻擊。若要在 Firewall Manager 員中建立 Amazon SNS 通知，請參閱步驟 4：設定 Amazon SNS 通知和 Amazon CloudWatch 警示。

使用 AWS CloudTrail記錄 API 呼叫

AWS WAF AWS Shield Advanced、與服務整 AWS Firewall Manager 合 AWS CloudTrail，可提供使用者、角色或服務所採取之動作記錄的 AWS 服務。 CloudTrail 擷取這些服務的 API 呼叫子集作為事件，包括來自「 AWS WAF Shield 牌進階」或「Firewall Manager 員」主控台的呼叫 AWS WAF，以及從「Shield 牌進階」或「Firewall Manager 員」API 的程式碼呼叫。如果您建立追蹤，您可以啟用持續傳遞 CloudTrail 事件到 Amazon S3 儲存貯體，包括事件 AWS WAF、防 Shield 進階或 Firewall Manager 員。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷對這些服務提出的要求、提出要求的來源 IP 位址、提出要求的人員、提出要求的時間以及其他詳細資訊。

若要進一步了解 CloudTrail，包括如何設定和啟用它，請參閱AWS CloudTrail 使用者指南。

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。當「Shield 牌進階」或「Firewall Manager 員」中 AWS WAF發生受支援的事件活動時，該活動會與 CloudTrail事件歷史記錄中的其他 AWS 服務事件一起記錄在事件中。您可以在您的. 中檢視、搜尋和下載最近的活動 AWS 帳戶。如需詳細資訊，請參閱檢視具有事 CloudTrail 件記錄的事件。

如需持續記錄您 AWS 帳戶的事件 (包括「Shield 牌進階」或「Firewall Manager 員」的事件)，請 AWS WAF建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。在主控台建立追蹤記錄時，該追蹤記錄預設會套用到所有區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定的 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 記錄檔並從多個帳戶接收 CloudTrail記錄檔

AWS WAF 中的資訊 AWS CloudTrail

所有 AWS WAF 動作均由「API 參考」記錄 AWS CloudTrail 並記錄在「AWS WAF API 參考」中。例如，呼叫`ListWebACL``UpdateWebACL`、以及`DeleteWebACL`產生 CloudTrail 記錄檔中的項目。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 是否要求是使用 root 使用者認證
- 提出該請求時，是否使用了特定角色或聯合身分使用者的臨時安全憑證
- 請求是否由其他 AWS 服務提出

如需詳細資訊，請參閱 CloudTrailuserIdentity 元素。

範例： AWS WAF 記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 AWS CloudTrail 記錄檔包含一或多個記錄項目。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

以下是 AWS WAF Web ACL 作業的 CloudTrail 記錄項目範例。

範例：的 CloudTrail 記錄項目 `CreateWebACL`

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
```

```
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T03:43:07Z"
      }
    }
  },
  "eventTime": "2019-11-06T03:44:21Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "CreateWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "defaultAction": {
      "block": {}
    },
    "description": "foo",
    "rules": [
      {
        "name": "foo",
        "priority": 1,
        "statement": {
          "geoMatchStatement": {
            "countryCodes": [
              "AF",
              "AF"
            ]
          }
        },
        "action": {
          "block": {}
        },
        "visibilityConfig": {
          "sampledRequestsEnabled": true,
```

```
          "cloudWatchMetricsEnabled": true,
          "metricName": "foo"
        }
      }
    ],
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    }
  },
  "responseElements": {
    "summary": {
      "name": "foo",
      "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
      "description": "foo",
      "lockToken": "67551e73-49d8-4363-be48-244deea72ea9",
      "aRN": "arn:aws:wafv2:us-east-1:112233445566:global/webacl/foo/
ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b"
    }
  },
  "requestID": "c51521ba-3911-45ca-ba77-43aba50471ca",
  "eventID": "afd1a60a-7d84-417f-bc9c-7116cf029065",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

範例：的 CloudTrail 記錄項目 GetWebACL

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AssumedRole",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AssumedRole",
        "arn": "arn:aws:iam::112233445566:role/Admin",
```

```
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:18:28Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "GetWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "webacl"
  },
  "responseElements": null,
  "requestID": "f2db4884-4eeb-490c-afe7-67cbb494ce3b",
  "eventID": "7d563cd6-4123-4082-8880-c2d1fda4d90b",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```


範例：的 CloudTrail 記錄項目 UpdateWebACL


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
```

```
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:20:56Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "UpdateWebACL",
  "awsRegion": ""us-east-1,
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "defaultAction": {
      "block": {}
    },
    "description": "foo",
    "rules": [
      {
        "name": "foo",
        "priority": 1,
        "statement": {
          "geoMatchStatement": {
            "countryCodes": [
              "AF"
            ]
          }
        },
        "action": {
          "block": {}
        },
        "visibilityConfig": {
          "sampledRequestsEnabled": true,
```

```
          "cloudWatchMetricsEnabled": true,
          "metricName": "foo"
        }
      }
    ],
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    },
    "lockToken": "67551e73-49d8-4363-be48-244deea72ea9"
  },
  "responseElements": {
    "nextLockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
  "requestID": "41c96e12-9790-46ab-b145-a230f358f2c2",
  "eventID": "517a10e6-4ca9-4828-af90-a5cff9756594",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

範例：的 CloudTrail 記錄項目 DeleteWebACL

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/session-name",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
```

```
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:25:17Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "DeleteWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "lockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
  "responseElements": null,
  "requestID": "71703f89-e139-440c-96d4-9c77f4cd7565",
  "eventID": "2f976624-b6a5-4a09-a8d0-aa3e9f4e5187",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

範例： AWS WAF 傳統記錄檔項目

AWS WAF 「經典」是的先前版本 AWS WAF。如需相關資訊，請參閱AWS WAF 經典。

日誌項目會示範 `CreateRule`、`GetRule`、`UpdateRule` 和 `DeleteRule` 操作：

```
{
  "Records": [
   {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
```

```
      "eventTime": "2016-04-25T21:35:14Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "CreateRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "name": "0923ab32-7229-49f0-a0e3-66c81example",
        "changeToken": "l9434322-8685-4ed2-9c5b-9410bexample",
        "metricName": "0923ab32722949f0a0e366c81example"
      },
      "responseElements": {
        "rule": {
          "metricName": "0923ab32722949f0a0e366c81example",
          "ruleId": "12132e64-6750-4725-b714-e7544example",
          "predicates": [

          ],
          "name": "0923ab32-7229-49f0-a0e3-66c81example"
        },
        "changeToken": "l9434322-8685-4ed2-9c5b-9410bexample"
      },
      "requestID": "4e6b66f9-d548-11e3-a8a9-73e33example",
      "eventID": "923f4321-d378-4619-9b72-4605bexample",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:22Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "GetRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
```

```
      "requestParameters": {
        "ruleId": "723c2943-82dc-4bc1-a29b-c7d73example"
      },
      "responseElements": null,
      "requestID": "8e4f3211-d548-11e3-a8a9-73e33example",
      "eventID": "an236542-d1f9-4639-bb3d-8d2bbexample",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:13Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "UpdateRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "ruleId": "7237b123-7903-4d9e-8176-9d71dexample",
        "changeToken": "32343a11-35e2-4dab-81d8-6d408example",
        "updates": [
          {
            "predicate": {
              "type": "SizeConstraint",
              "dataId": "9239c032-bbbe-4b80-909b-782c0example",
              "negated": false
            },
            "action": "INSERT"
          }
        ]
      },
      "responseElements": {
        "changeToken": "32343a11-35e2-4dab-81d8-6d408example"
      },
      "requestID": "11918283-0b2d-11e6-9ccc-f9921example",
```

```
      "eventID": "00032abc-5bce-4237-a8ee-5f1a9example",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:28Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "DeleteRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "changeToken": "fd232003-62de-4ea3-853d-52932example",
        "ruleId": "3e3e2d11-fd8b-4333-8b03-1da95example"
      },
      "responseElements": {
        "changeToken": "fd232003-62de-4ea3-853d-52932example"
      },
      "requestID": "b23458a1-0b2d-11e6-9ccc-f9928example",
      "eventID": "a3236565-1a1a-4475-978e-81c12example",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    }
  ]
}
```


AWS Shield Advanced 中的資訊 CloudTrail

AWS Shield Advanced 支援將下列動作記錄為記 CloudTrail 錄檔中的事件：

- ListAttacks
- DescribeAttack

- CreateProtection
- DescribeProtection
- DeleteProtection
- ListProtections
- CreateSubscription
- DescribeSubscription
- GetSubscriptionState

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 要求是否使用 root 使用者認證提出
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱CloudTrail 使 userIdentity 元素。

範例：Shield 進階記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範`DeleteProtection`和`ListProtections`動作的 CloudTrail 記錄項目。

```
[
 {
   "eventVersion": "1.05",
   "userIdentity": {
     "type": "IAMUser",
     "principalId": "123456789098765432123 1",
     "arn": "arn:aws:iam::123456789012:user/SampleUser",
     "accountId": "123456789012",
     "accessKeyId": "1AFGDT647FHU83JHFI81H",
     "userName": "SampleUser"
   },
```

```
    "eventTime": "2018-01-10T21:31:14Z",
    "eventSource": "shield.amazonaws.com",
    "eventName": "DeleteProtection",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
    "requestParameters": {
      "protectionId": "12345678-5104-46eb-bd03-agh4j8rh3b6n"
    },
    "responseElements": null,
    "requestID": "95bc0042-f64d-11e7-abd1-1babdc7aa857",
    "eventID": "85263bf4-17h4-43bb-b405-fh84jhd8urhg",
    "eventType": "AwsApiCall",
    "apiVersion": "AWSShield_20160616",
    "recipientAccountId": "123456789012"
  },
  {
    "eventVersion": "1.05",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "123456789098765432123",
      "arn": "arn:aws:iam::123456789012:user/SampleUser",
      "accountId": "123456789012",
      "accessKeyId": "1AFGDT647FHU83JHFI81H",
      "userName": "SampleUser"
    },
    "eventTime": "2018-01-10T21:30:03Z",
    "eventSource": "shield.amazonaws.com",
    "eventName": "ListProtections",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "6accca40-f64d-11e7-abd1-1bjfi8urhj47",
    "eventID": "ac0570bd-8dbc-41ac-a2c2-987j90j3h78f",
    "eventType": "AwsApiCall",
    "apiVersion": "AWSShield_20160616",
    "recipientAccountId": "123456789012"
  }
]
```

AWS Firewall Manager 中的資訊 CloudTrail

AWS Firewall Manager 支援將下列動作記錄為記 CloudTrail 錄檔中的事件：

- AssociateAdminAccount
- DeleteNotificationChannel
- DeletePolicy
- DisassociateAdminAccount
- PutNotificationChannel
- PutPolicy
- GetAdminAccount
- GetComplianceDetail
- GetNotificationChannel
- GetPolicy
- ListComplianceStatus
- ListPolicies

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 要求是否使用 root 使用者認證提出
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱CloudTrail 使 userIdentity 元素。

範例：Firewall Manager 員記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範 `GetAdminAccount-->` 動作的 CloudTrail 記錄項目。

```
{
```

```
                "eventVersion": "1.05",
                "userIdentity": {
                                "type": "AssumedRole",
                                "principalId": "123456789098765432123 1",
                                "arn": "arn:aws:sts::123456789012:assumed-role/Admin/
SampleUser",
                                "accountId": "123456789012",
                                "accessKeyId": "1AFGDT647FHU83JHFI81H",
                                "sessionContext": {
                                                "attributes": {
                                                                "mfaAuthenticated":
 "false",
                                                                "creationDate":
 "2018-04-14T02:51:50Z"
                                                               },
                                                "sessionIssuer": {
                                                                "type": "Role",
                                                                "principalId":
 "123456789098765432123 1",
                                                                "arn":
 "arn:aws:iam::123456789012:role/Admin",
                                                                "accountId":
 "123456789012",
                                                                "userName": "Admin"
                                                                 }
                                                  }
                                },
                "eventTime": "2018-04-14T03:12:35Z",
                "eventSource": "fms.amazonaws.com",
                "eventName": "GetAdminAccount",
                "awsRegion": "us-east-1",
                "sourceIPAddress": "72.21.198.65",
                "userAgent": "console.amazonaws.com",
                "requestParameters": null,
                "responseElements": null,
                "requestID": "ae244f41-3f91-11e8-787b-dfaafef95fc1",
                "eventID": "5769af1e-14b1-4bd1-ba75-f023981d0a4a",
                "eventType": "AwsApiCall",
                "apiVersion": "2018-01-01",
                "recipientAccountId": "123456789012"
    }
```

使用和應用 AWS Shield Advanced 程 AWS WAF 式介面

本節說明如何向 AWS WAF 和 Shield 進階 API 發出要求，以便在中建立和管理匹配組、規則和網路 ACL，以 AWS WAF 及您在 Shield Advanced 中的訂閱和保護。本節可讓您熟悉請求元件、回應內容，以及如何驗證請求。

主題

使用 AWS 軟體開發套件

如果您使用 AWS 提供 SDK 的語言，請使用 SDK，而不是嘗試通過 API 工作。SDK 讓驗證變得更簡單、輕鬆與您的開發環境整合，並提供輕鬆存取 AWS WAF 和 Shield 進階命令。如需 AWS SDK 的詳細資訊，請參閱主題下載工具設定您的帳戶以使用服務中的。

向高級發出 HTTPS 請求 AWS WAF 或 Shield 高級

AWS WAF 和 Shield 進階要求是 HTTPS 要求，如 RFC 26 16 所定義。像任何 HTTP 請求，對 AWS WAF 或 Shield 高級的請求包含請求方法，URI，請求標頭和請求主體。回應包含 HTTP 狀態碼、回應標題，有時還包括回應內文。

請求 URI

請求 URI 始終是一個單一斜線 /。

HTTP 標頭

AWS WAF 和 Shield 進階需要 HTTP 要求標頭中的下列資訊：

主機 (必要)

指定您資源所建立地點的端點。如需端點的相關資訊，請參閱AWS 服務端點。例如， CloudFront 分佈的`Host`標頭值 AWS WAF 為`waf.amazonaws.com:443`。

x-amz-date 或日期 (必填)

用來建立 Authorization 標頭中包含的簽章的日期。指定 ISO 8601 標準的格式，以 UTC 時間，如下所示：

```
x-amz-date: 20151007T174952Z
```

您必須包含 x-amz-date 或 Date。(有些 HTTP 用戶端程式庫不讓您設定 Date 標頭)。當x-amz-date標頭存在時，在驗證請求時 AWS WAF 忽略任何Date標頭。

收到請求時，時間戳記必須在 AWS 系統時間的 15 分鐘內。若為非，請求失敗並發生 RequestExpired 錯誤碼，以防止其他人重播您的請求。

授權 (必要)

請求驗證所需的資訊。如需建構此標頭的詳細資訊，請參閱對請求進行身分驗證。

X-Amz-Target (必要)

AWSWAF_ 或 AWSShield_ 串接，API 版本無需標點符號、句點 (.) 和操作的名稱，例如：

AWSWAF_20150824.CreateWebACL

內容類型 (條件)

指定內容類型為 JSON 和 JSON 的版本，如下所示：

```
Content-Type: application/x-amz-json-1.1
```

條件：需要請POST求。

內容長度 (條件)

根據 RFC 2616 的訊息長度 (無標題)。

條件：如果請求內文本身包含資訊 (大多數工具組將自動新增此標題)，則為必填項目。

以下示範 HTTP 標頭在 AWS WAF中如何建立 web ACL：

```
POST / HTTP/1.1
Host: waf.amazonaws.com:443
X-Amz-Date: 20151007T174952Z
Authorization: AWS4-HMAC-SHA256
```

```
               Credential=AccessKeyID/20151007/us-east-2/waf/aws4_request,
               SignedHeaders=host;x-amz-date;x-amz-target,

 Signature=145b1567ab3c50d929412f28f52c45dbf1e63ec5c66023d232a539a4afd11fd9
X-Amz-Target: AWSWAF_20150824.CreateWebACL
Accept: */*
Content-Type: application/x-amz-json-1.1; charset=UTF-8
Content-Length: 231
Connection: Keep-Alive
```

HTTP 請求內文

許多 AWS WAF 和 Shield 進階 API 動作會要求您在要求主體中包含 JSON 格式的資料。

下列範例要求會使用簡單的 JSON 陳述式來更新，IPSet以包含 IP 位址 192.0.2.44 (以 CIDR 標記法表示為 192.0.2.44/32)：

```
POST / HTTP/1.1
Host: waf.amazonaws.com:443
X-Amz-Date: 20151007T174952Z
Authorization: AWS4-HMAC-SHA256
               Credential=AccessKeyID/20151007/us-east-2/waf/aws4_request,
               SignedHeaders=host;x-amz-date;x-amz-target,

 Signature=145b1567ab3c50d929412f28f52c45dbf1e63ec5c66023d232a539a4afd11fd9
X-Amz-Target: AWSWAF_20150824.UpdateIPSet
Accept: */*
Content-Type: application/x-amz-json-1.1; charset=UTF-8
Content-Length: 283
Connection: Keep-Alive

{
   "ChangeToken": "d4c4f53b-9c7e-47ce-9140-0ee5ffffffff",
   "IPSetId": "69d4d072-170c-463d-ab82-0643ffffffff",
   "Updates": [
      {
         "Action": "INSERT",
         "IPSetDescriptor": {
            "Type": "IPV4",
            "Value": "192.0.2.44/32"
         }
      }
   ]
```

```
}
```

HTTP 回應

「所有」 AWS WAF 和「Shield 牌」進階 API 動作會在回應中包含 JSON 格式的資料。

以下為 HTTP 回應中一些重要的標頭，以及在應用程式中如何應用他們，如果適用的話：

HTTP/1.1

此標頭後面有狀態碼。狀態碼 200 表示操作成功。

類型：字串

X-同步 RequestId

由 AWS WAF 或 Shield Advanced 建立的值，可唯一識別您的請求，例如，K2QH8DN0U907N97FNA2GDLL80BVV4KQNSO5AEMVJF66Q9ASUAAJG。如果您遇到問題 AWS WAF， AWS 可以使用此值來解決問題。

類型：字串

內容長度

回應內文的長度，以位元組為單位。

類型：字串

日期

舉例來說， AWS WAF 或神 Shield 進階回應的日期和時間，例如 2015 年 10 月 7 日星期三 12:00:00 格林威治標準時間。

類型：字串

錯誤回應

如果請求的結果是錯誤，則 HTTP 回應會包含下列值：

- JSON 錯誤文件做為回應本文
- 內容類型
- 適用的 3xx、4xx 或 5xx HTTP 狀態碼

以下為 JSON 文件的範例：

```
HTTP/1.1 400 Bad Request
x-amzn-RequestId: b0e91dc8-3807-11e2-83c6-5912bf8ad066
x-amzn-ErrorType: ValidationException
Content-Type: application/json
Content-Length: 125
Date: Mon, 26 Nov 2012 20:27:25 GMT

{"message":"1 validation error detected: Value null at 'TargetString' failed to satisfy
 constraint: Member must not be null"}
```

對請求進行身分驗證

如果您使用提 AWS 供 SDK 的語言，建議您使用 SDK。與使用 AWS WAF 或 Shield 進階 API 相比，所有 AWS SDK 都能大幅簡化簽署要求的程序，並為您節省大量時間。此外，SDK 可與您的開發環境輕鬆整合，並可輕鬆存取相關命令。

AWS WAF 和 Shield Advanced 要求您透過簽署要求來驗證您傳送的每個要求。若要簽署請求，請您使用密碼編譯雜湊函數來計算數位簽章，其根據輸入傳回雜湊值。此輸入包含請求和私密存取金鑰的文字。雜湊函數會傳回一個雜湊值，您將此值包含在請求中做為簽章。該簽章是請求 `Authorization` 標頭中的一部分。

收到您的要求後， AWS WAF 或 Shield Advanced 會使用您用來簽署要求的相同雜湊函數和輸入來重新計算簽章。如果產生的簽章符合要求中的簽章， AWS WAF 或「Shield 牌進階」會處理要求。如果不是，則會拒絕該請求。

AWS WAF 和 Shield 高級支持使用AWS 簽名版本 4 進行身份驗證。計算簽章的程序可以分成三個任務：

任務 1：建立正式請求

在正式格式中，如 https://docs.aws.amazon.com/general/latest/gr/sigv4-create-canonical-request.html 中的Amazon Web Services 一般參考任務 1：建立簽章版本 4 的正式請求 所述，建立您的 HTTP 請求。

任務 2：建立登入字串

建立一個字串，您會使用此字串做為密碼編譯雜湊函數的其中一個輸入值。此字串稱為簽署字串，是下列值的串接：

- 雜湊演算法的名稱
- 要求日期
- 登入資料範圍字串
- 標準化請求之前的任務

登入資料範圍字串本身是日期、區域和服務資訊的串連。

針對 X-Amz-Credential 參數，請指定下列：

- 此端點的程式碼，為您正在傳送請求 us-east-2 的對象
- 使用於服務縮寫的 waf

例如：

```
X-Amz-Credential=AKIAIOSFODNN7EXAMPLE/20130501/us-east-2/waf/
aws4_request
```

任務 3：建立簽章

使用接受兩個輸入字串的密碼編譯雜湊函數來建立請求的簽章：

- 您的簽署字串，來自任務 2。
- 金鑰衍生。藉由從您的私密存取金鑰開始來計算此衍生金鑰和使用登入資料範圍字串，來建立一系列雜湊型訊息身分驗證代碼 (HMACs)。

相關資訊

以下相關資源可協助您使用此服務。

下列資源可用於 AWS WAF AWS Shield Advanced、和 AWS Firewall Manager。

- 實施指南 AWS WAF — 技術出版物，其中包含有關實施 AWS WAF 以保護現有和新 Web 應用程序的當前建議。
- AWS 討論區 — 以社群為基礎的論壇，用來討論與此服務及其他 AWS 服務相關的技術問題。
- AWS WAF 討論區 — 以社群為基礎的論壇，供開發人員討論相關的技術問題。 AWS WAF
- Shield 進階論壇 — 一個以社群為基礎的論壇，供開發人員討論與 Shield Advanced 相關的技術問題。
- AWS WAF 產品資訊 — 主要網頁，以取得相關資訊 AWS WAF，包括功能、定價等。
- Shield 進階產品資訊 — 有關「Shield 牌進階」資訊的主要網頁，包括功能、價格等。

以下資源可用於 Amazon Web Services。

- 課程和研討會 — 除了可以幫助提高 AWS 技能並獲得實踐經驗的自定進度實驗室之外，還可以鏈接到基於角色和專業課程的鏈接。
- AWS 開發人員中心 — 探索教學課程、下載工具，以及瞭解 AWS 開發人員活動。
- AWS 開發人員工具 — 開發人員工具、SDK、IDE 工具組，以及用於開發和管理 AWS 應用程式的命令列工具的連結。
- 入門資源中心 — 瞭解如何設定 AWS 帳戶、加入 AWS 社群，以及啟動您的第一個應用程式。
- 實作教學課程 — 按照 step-by-step 教學課程啟動您的第一個應用程式 AWS。
- AWS 白皮書 — 完整的技術 AWS 白皮書清單連結，涵蓋架構、安全性和經濟等主題，並由 AWS 解決方案架構師或其他技術專家撰寫。
- AWS Support 中心 — 建立和管理 AWS Support 案例的中心。同時也包含其他實用資源的連結，例如論壇、技術常見問答集、服務健康狀態和 AWS Trusted Advisor.
- AWS Support— 有關資訊的主要網頁 AWS Support one-on-one, 快速回應的支援管道，可協助您在雲端中建置和執行應用程式.
- 聯絡我們 – 查詢有關 AWS 帳單、帳戶、事件、濫用與其他問題的聯絡中心。
- AWS 網站條款 — 有關我們的版權和商標的詳細資訊；您的帳戶、授權和網站存取權限；以及其他主題。

文件歷史紀錄

本頁列出本文件的重大變更。

服務功能有時會逐步推出至提供服務的 AWS 區域。我們僅針對第一個版本更新此文件。我們不會提供有關區域可用性的資訊，也不會宣布後續區域的推展情況。如需有關服務功能的區域可用性，以及訂閱更新相關通知的資訊，請參閱有什麼新功能 AWS？ 。

變更	描述	日期
新增每個組織的通話配額 ListResourcesForWebACL	AWS WAF 現在限制組織中任何單一區域的帳戶撥打的ListResourcesForWebACL 通話次數。	2024年7月26日
AWS Firewall Manager 安全策略更新	更新FMSServiceRolePolicy 以新增讀取 Network Firewall TLS 組態資訊的權限。	2024年7月22日
已更新的 AWS 受管規則 AWS WAF	已更新應 WordPress 用程式規則群組。	2024年7月15日
已更新的 AWS 受管規則 AWS WAF	更新 Linux 作業系統規則群組。	2024年7月12日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2024 年 7 月 9 日
已更新的 AWS 受管規則 AWS WAF	更新PHP應用程式和 Windows 作業系統規則群組。	2024年7月3日
澄清JSON身體解析的工作原理	已更新JSON主體檢查的涵蓋範圍，以釐清如何 AWS WAF 處理剖析和主體剖析後援行為。	2024年6月25 日
已更新的 AWS 受管規則 AWS WAF	更新 Linux 作業系統規則群組。	2024年6月6日

AWS WAF 受管理原則變更	已更新`WAFV2LoggingServiceRolePolicy` 並`AWSServiceRoleForWAFV2Logging` 將陳述式 IDs (Sid) 新增至權限設定。	2024年6月3 日
AWS WAF 受管原則變更追蹤	AWS WAF 開始追蹤受管理策略`WAFV2LoggingServiceRolePolicy` 和服務連結角色`AWSServiceRoleForWAFV2Logging` 的變更。	2024年6月3 日
已更新的 AWS 受管規則 AWS WAF	Bot Control ATP、和ACFP受管規則群組現在已建立版本化，並會提供版本更新的SNS通知，與其他版本化的 AWS 受管理規則相同。	2024年5月29 日
已更新的 AWS 受管規則 AWS WAF	更新POSIX作業系統規則群組、`AWSManagedRulesUnixRuleSet` 。	2024年5月28日
CAPTCHA和Challenge動作	增加了瀏覽器客戶端需HTTPS要運行CAPTCHA謎題和無聲挑戰的澄清。	2024年5月24日
與 Amazon 安全湖集成	您現在可以使用安全湖來收集網路ACL流量資料。如需詳細資訊，請參閱 Amazon 安全湖使用者指南中的從 AWS 服務收集資料。	2024年5月22 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2024年5月21 日
已更新的 AWS 受管規則 AWS WAF	已更新資SQLi料庫規則群組。	2024 年 5 月 14 日

已更新的 AWS 受管規則 AWS WAF	更新已知的錯誤輸入和POSIX作業系統規則群組。	2024年5月8日
已更新的 AWS 受管規則 AWS WAF	更新視窗作業系統規則群組。	2024年5月3日
AWS WAF 移動SDK安卓科特林代碼示例	為基於科特林的 Android 整合新增範例程式碼。	2024年5月2日
AWS WAF 量度新增維度和新量度	AWS WAF 新增規則量度`ManagedRuleSetRule` 中的新維度，並為標籤量度的相符規則動作新增量度。	2024年5月2日
AWS Firewall Manager 支援網路ACL原則	Firewall Manager 員現在支援透過 Firewall Manager 員VPC網路ACL政策管理 Amazon 網路存取控制清單 (ACLs)。	2024年4月25日
AWS Firewall Manager 安全策略更新	更新`FMSServiceRolePolicy` 以新增管理網路的權限ACLs。	2024年4月22 日
更新了健康狀態檢查指標	我們從運作狀態檢查中常用的量度清單中移除了一些量度。	2024年4月16日
Firewall Manager 員安全群組原則的更新	我們已更新使用稽核安全性群組原則，並改善文件。請參閱使用情況稽核策略一節以及最佳做法和限制章節。	2024年4月2日
更新機器人控制範例	已新增說明目標檢驗等級的範例，並更新現有範例以反映最佳實務。	2024年3月27日
更新的ATP例子	已新增說明回應檢查組態的範例，並更新現有範例以反映最佳作法。	2024年3月27日

更新的ACFP例子	已新增說明回應檢查組態的範例。	2024年3月27日
更新 Amazon CloudWatch 日誌日誌流限制	AWS WAF 將記錄發佈至記 CloudWatch 錄資料流時，不再具有每個網頁的ACL限制。	2024年3月27日
AWS Shield Advanced 應用程式層 (第 7 層) 保護	已更新應用程式層偵測和緩解、Web ACL 使用、速率型規則以及自動應用程式層DDoS緩解的一般和最佳實務指南。	2024年3月14日
已更新的 AWS 受管規則 AWS WAF	更新 IP 信譽規則群組。	2024年3月13日
車身檢查尺寸限制的變更	AWS WAF 現在支援某些區域資源的較大車身檢查尺寸限制。	2024年3月7日
AWS WAF 以速率為基礎的規則的可設定評估	您現在可以將以速率為基礎的規則用來計算請求的時間範圍，設定為 1、2、5 或 10 分鐘。預設值為 5，這是此版本之前的唯一選項。	2024年2月28日
和的擴充記錄資CAPTCHA訊Challenge	最上層`captchaResponse` 和`challengeResponse` 欄位現在會填入要套用至要求的最後一個動作，無論是終止還是非終止。在此之前，只會針對終止動作填入這些欄位。	2024年2月22 日
JavaScript CAPTCHAAPI金鑰管理	您現在可以透過刪除 CAPTCHA JS API 鍵 AWS WAF APIs。	2024年2月6日

AWS WAF CAPTCHA音頻拼圖	CAPTCHA拼圖的音頻版本現在支持多種語言。	2024年2月6日
AWS WAF 挑戰和CAPTCHA令牌標籤	權杖管理現在會為CAPTCHA權杖新增標籤，並增強了挑戰權杖的權杖標籤。	2023 年 12 月 20 日
已更新的 AWS 受管規則 AWS WAF	更新已知錯誤輸入規則群組。	2023年12月16 日
已更新的 AWS 受管規則 AWS WAF	更新已知錯誤輸入規則群組。	2023 年 12 月 14 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2023 年 12 月 6 日
已更新的 AWS 受管規則 AWS WAF	更新下列規則群組： AWS WAF 機器人控制。	2023 年 12 月 5 日
更新的 Firewall Manager AWS Config 員	如果您使用的是自訂IAM角色，而不是的「Firewall Manager 員」管理角色 AWS Config，則必須確保您的權限原則允許記 AWS Config 錄程式記錄 Firewall Manager 員資源。	2023 年 11 月 17 日
AWS WAF 控制台面板	我們更正了ACL在控制台中查看所有規則和採樣請求的指導。 AWS WAF	2023 年 11 月 17 日
已更新的 AWS 受管規則 AWS WAF	更新了機器人控制規則群組。	2023 年 11 月 14 日
AWS WAF 控制台具有新的 Web ACL 儀表板	AWS WAF 主控台中的網ACL頁具有新的 Web 流量概觀儀表板。	2023 年 11 月 14 日

更新的ATP受管規則群組	已更正規則`VolumetricIpFailedLoginResponseHigh` 與的標籤資訊`VolumetricSessionFailedLoginResponseHigh` 。	2023 年 11 月 13 日
更新的ACFP受管規則群組	已更正規則`VolumetricIPSuccessfulResponse` 與的標籤資訊`VolumetricSessionSuccessfulResponse` 。	2023 年 11 月 13 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2023 年 11 月 2 日
防 Shield 進階自動應用程式層 DDoS緩解	Shield Advanced 現在會在自動緩和規則群組中維護以速率為基礎的規則，以限制來自已知為DDoS攻擊來源之 IP 位址的要求數量。	2023 年 10 月 31 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2023 年 10 月 30 日
機器人控制受管規則群組移除要求的信號標籤 CSP	Bot Control 受管理規則群組移除了指示雲端服務提供者 (CSP) 的信號標籤。	2023 年 10 月 28 日
要求的機器人控制受管規則群組信號標籤 CSP	Bot Control 受管規則群組訊號標籤包含指示雲端服務提供者 (CSP) 的標籤。	2023 年 10 月 27 日
更新的 AWS WAF IAM權限資訊	針對管理 Web ACL 關聯的 AWS WAF 動作，原則動作區段現在會列出每個 Web 應用程式資源類型的權限需求。	2023 年 10 月 25 日

修改過的網頁的 Firewall Manager 員 ACLs	當您啟用非關聯網路的管理時 ACLs，Firewall Manager 不會將修改過的網頁納ACLs入一次性清除未使用的資源中。	2023 年 10 月 19 日
已更新的 AWS 受管規則 AWS WAF	更新POSIX作業系統規則群組、`AWSManagedRulesUnixRuleSet` 。	2023 年 10 月 12 日
AWS WAF 量度新增維度	AWS WAF 已新增用於檢視 Web ACL 量度的新維度。	2023 年 10 月 12 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2023 年 10 月 11 日
更新至 AWS WAF 行動裝置 SDK規格	已將作`storeTokenInCookieStorage` 業新增至`WAFTokenProvider` 。	2023 年 10 月 11 日
例外部署 AWS 管理的規則 AWS WAF	已更新已知錯誤輸入規則群組的兩個靜態版本，並將預設版本更新為指向最新的靜態版本。	2023 年 10 月 4 日
AWS WAF HTML實體解碼文字轉換	擴充了HTML實體解碼文字轉換的功能。	2023 年 10 月 4 日
為 Firewall Manager 員安全組通用策略添加了新選項	「Firewall Manager 員」現在可以將安全群組參考分發給複本安全群	2023 年 10 月 3 日
AWS WAF 增加了JA3指紋檢查	您現在可以針對 Amazon CloudFront 分發和應用程式負載平衡器，對 Web 請求的JA3指紋執行完全比對。	2023 年 9 月 26 日
Firewall Manager 員安全群組原則規則設定的更新	Firewall Manager 員現在支援從主要安全群組參照到複本安全群組的安全性群組。	2023 年 9 月 25 日

更新防 Shield 進階自動應用程式層DDoS緩解	Firewall Manager 員現在支援 Application Load Balancer 資源，以DDoS防 Shield 進階原則設定為自動應用程式層	2023 年 9 月 14 日
已更新的 AWS 受管規則 AWS WAF	更新下列規則群組： AWS WAF 機器人控制。	2023 年 9 月 6 日
AWS WAF 機器人控制	Bot Control 受管規則群組的目標保護層級現在會檢查 IP 位址之間是否重複使用權杖。它現在還提供流量統計數據的可選機器學習分析，以檢測一些與機器人相關的活動。	2023 年 9 月 6 日
更新至 AWS WAF 行動裝置 SDK規格	將最小值、最大值和預設值`tokenRefreshDelaySec` 從最小 300、最大 600 以及預設值 300 降低為最小 88、最大 300 和預設值 88。	2023 年 9 月 5 日
已更新的 AWS 受管規則 AWS WAF	更新了 AWS WAF 機器人控制規則群組。	2023 年 8 月 30 日
防 Shield 進階自動應用程式層DDoS緩解	已新增用 AWS CloudFormation 來管理您搭配自動應用程式層DDoS緩和功ACLs能所使用之 Web 的指引。	2023 年 8 月 30 日
新增 Firewall Manager 員內容稽核安全性群組原則	已新增稽核過於寬鬆規則群組的新選項，並改善主控台程序描述。	2023 年 8 月 29 日

新的 Firewall Manager 員防 Shield 和 AWS WAF 策略選項	如果您ACLs在 AWS WAF 和 Shield 中啟用非關聯網路的管理，則 Firewall Manager 員只會ACLs在至少一個資源使用網頁時，才ACLs會在策略範圍內的帳號中建立 Web。	2023 年 8 月 9 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2023 年 7 月 26 日
以速率為基礎的規則彙總路徑 URI	您現在可以在以速率為基礎的規則的自訂彙總索引鍵中指定URI路徑。	2023 年 7 月 19 日
新增 AWS WAF原則規則選項 AWS Firewall Manager	AWS Firewall Manager 添加了對配置 AWS WAF Web 請求主體檢查大小限制的支持。	2023 年 7 月 18 日
AWS WAF 受管理原則變更	已更新`AWSWAFFullAccessPolicy`、`AWSWAFConsoleFullAccess`、和`AWSWAFReadOnlyAccess`，`AWSWAFConsoleReadOnlyAccess` 以將 AWS 已驗證存取權新增至您可以使用保護的資源類型 AWS WAF。	2023 年 6 月 13 日
已更新的 AWS 受管規則 AWS WAF	已更新規則群組`AWSManagedRulesACFPRuleSet`。	2023 年 6 月 13 日
防止 AWS WAF 欺詐控制帳戶接管的更新（ ）ATP	您現在可以使用規則運算式指定ATP受管規則群組的登入端點。	2023 年 6 月 13 日

新的信息 CAPTCHA JavaScript API	新章節說明如何在 AWS WAF 回應要求時提供自訂CAPTCHA謎題CAPTCHA。	2023 年 6 月 13 日
新增ACFP受管規則群組	使用新的規則群組AWSManagedRulesACFPRuleSet 偵測並封鎖詐騙帳戶建立嘗試。	2023 年 6 月 13 日
新的 AWS WAF 欺詐控制帳戶創建欺詐預防（ACFP）	您可以使用新的詐 AWS WAF 騙控制帳戶建立詐騙預防 (ACFP) 受管規則群組，偵測並封鎖詐騙帳戶建立嘗試AWSManagedRulesACFPRuleSet 。使用受保護的 CloudFront 分配，您還可以使用阻止ACFP來自客戶的新帳戶創建嘗試，這些客戶最近提交了太多失敗的帳戶創建嘗試。	2023 年 6 月 13 日
AWS WAF 受管理原則變更	已更新AWSWAFFullAccessPolicy AWSWAFConsoleFullAccess 、AWSWAFReadOnlyAccess 、和AWSWAFConsoleReadOnlyAccess 更正 AWS App Runner 服務的存取設定。	2023 年 6 月 6 日
新增 Firewall Manager 員安全群組原則的限制	如果共用稍後VPC未共用，則 Firewall Manager 員將不會刪除相關聯帳戶中的複本安全性群組。	2023 年 6 月 2 日
新的 AWS WAF 請求組件：Header order	您現在可以比對要求中標頭名稱的排序清單。	2023 年 5 月 30 日

已更新的 AWS 受管規則 AWS WAF	已更新 Linux 作業系統規則集。	2023 年 5 月 22 日
更新了 AWS WAF 規則部分的組織	列出的 rules 陳述式現在會依陳述式類型分組。	2023 年 5 月 16 日
移動的主題：列出受速率限制的 IP 位址	列出受速率型規則限制之 IP 位址的主題現在位於以速率為基礎的規則主題之下。	2023 年 5 月 16 日
以費率為基礎的規則擴充選項	您現在可以根據 IP 位址以外的彙總金鑰來分級限制 Web 要求，並且可以使用金鑰組合來彙總。您也可以對符合範圍向下陳述式的所有要求進行速率限制，而無需進一步彙總。	2023 年 5 月 16 日
Firewall Manager 配額增加	將每個組織的 Firewall Manager 員策略數目 AWS Organizations 從 20 增加到 50 個。將每個原則的主要安全群組數目上限從一個增加到三個。將最大數目WCUs從軟配額變更為硬配額。	2023 年 5 月 5 日
增加WCUs每個規則群組的上限	您現在可以使用每個規則群組最多 5,000 個 Web ACL 容量單位 (WCUs)，而不需要增加支援。這個新的限制無法提高。	2023 年 5 月 1 日
AWS WAF 具有前置字元的 Amazon S3 日誌儲存貯體位置	AWS WAF 現在允許 Amazon S3 日誌儲存貯體名稱中使用前置詞。	2023 年 5 月 1 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2023 年 4 月 28 日

AWS 已驗證存取執行個體的支援新增至 AWS WAF	您現在可以將 AWS WAF Web ACL 與「已驗證存取」執行個體建立關聯。此變更僅適用於最新版本的 ， AWS WAF 而不適用於 AWS WAF 經典版本。	2023 年 4 月 28 日
修訂了與多個 Firewall Manager 員合作的章節	您現在可以指定多個 Firewall Manager 員管理員來建立和管理組織的防火牆資源。	2023 年 4 月 24 日
AWS Firewall Manager 受管理策略更新	已更新`FMSServiceRolePolicy` 。	2023 年 4 月 21 日
新的用 JavaScript 戶端應用程式整合 CAPTCHA	您現在可以在用 JavaScript 戶端應用程式中自訂CAPTCHA拼圖的位置和特性。	2023 年 4 月 20 日
應用程式整合重新命名為智慧威脅	我們將用戶端應用程式整合的現有功能重新命名為智慧威脅整合，以協助區分新的CAPTCHA應用程式整合JavaScript。	2023 年 4 月 20 日
ACLWCUs超過 1,500 個網頁的可變定價	在您的 Web 中使用超過 1,500 個 Web ACL 容量單位 (WCUs) 會ACL產生額外的成本，這些成本會隨著 Web 使ACLWCU用量的增加和減少而自動調整。網絡的ACL最大值是 5,000 WCUs。	2023 年 4 月 11 日
增加WCUs每個網頁的上限ACL	您現在每個網頁最多可以使用 5,000 個 Web ACL 容量單位 (WCUs)，ACL而不需要增加支援。這個新的限制無法提高。	2023 年 4 月 11 日

CloudFront 網絡的車身檢查尺寸限制 ACLs	對於ACLs保護 Amazon CloudFront 分發的網路，您可以在 Web ACL 組態中將主體檢查大小限制增加到 64 KB。	2023 年 4 月 11 日
車身檢查尺寸增加 CloudFront	Amazon CloudFront 分佈的最大 AWS WAF 身體檢查大小限制從 8 KB 增加到 64 KB。的預設檢驗大小限制 CloudFront 為 16 KB。	2023 年 4 月 11 日
新增 AWS WAF原則規則選項 AWS Firewall Manager	AWS Firewall Manager 新增對 AWS WAF 詐騙控制帳戶接管預防 (ATP) 和 AWS WAF 機器人控制 AWS 受管規則群組、Amazon S3 記錄目標、規則動作覆寫和規則動作以CAPTCHA及Challenge 權杖網域清單的支援。	2023 年 4 月 7 日
Firewall Manager 員支援 Amazon S3 儲存貯體做為日誌記錄目的 AWS WAF 地	您現在可以在 AWS WAF 政策中使用 Amazon S3 儲存貯體做為記錄目的地。	2023 年 4 月 7 日
AWS WAF 受管理原則變更	已更新AWSWAFFullAccessPolicy AWSWAFConsoleFullAccess 、AWSWAFReadOnlyAccess 、和，AWSWAFConsoleReadOnlyAccess 以將 AWS App Runner 服務新增至您可以使用保護的資源類型 AWS WAF。	2023 年 3 月 30 日

新增有關安全群組原則中標籤使用情況的警告	如果策略具有與組織的標籤策略衝突的標記，Firewall Manager 將不會更新現有安全群組的標記或建立新的安全群組。	2023 年 3 月 28 日
更新服務角色資訊	已更新如何搭配 Firewall Manager 員使用服務角色。	2023 年 3 月 8 日
更正關於以速率為基礎的規則如何執行速率限制	以費率為基礎的規則，具有向下範圍陳述式，僅限比率限制要求符合規則的範圍向下陳述式。我們指出限制適用於任何速率限制 IP 地址的所有請求。	2023 年 3 月 1 日
已更新的 AWS 受管規則 AWS WAF	已更新應PHP用程式規則群組。	2023 年 2 月 27 日
增加了對於 AWS App Runner 支持 AWS WAF	您現在可以將 AWS WAF Web ACL 與 AWS App Runner 服務相關聯。此變更僅適用於最新版本的， AWS WAF 而不適用於 AWS WAF 經典版本。	2023 年 2 月 23 日
更新了IAM指引 AWS Firewall Manager	更新指南以符合最IAM佳做法。如需詳細資訊，請參閱 IAM.	2023 年 2 月 16 日
已更新的 AWS 受管規則 AWS WAF	已更新規則群組，`AWSManagedRulesATPRuleSet` 以在保護 Amazon CloudFront 分發的 Web ACLs 中新增登入回應檢查。	2023 年 2 月 15 日
AWS WAF 防止欺詐控制帳戶接管（ATP）登錄響應檢查	對於受保護的 CloudFront 發行版，您現在可以使用封鎖ATP來自最近提交過多次登入嘗試失敗的用戶端的新登入嘗試。	2023 年 2 月 15 日

已更新的 AWS 受管規則 AWS WAF	更新核心規則集。	2023 年 1 月 25 日
智慧型威脅緩解的最佳做法	新增一節，ATP其中包含實作 Bot Control 以及其他智慧型威脅緩解功能的最佳做法。	2023年1月22 日
如何檢查 HTTP /2 偽標題	已新增將 HTTP /2 個虛擬標頭對應至其對應 Web 要求元件的區段。	2023 年 1 月 20 日
更新了 AWS WAF 經典版的IAM指引	更新指南以符合最IAM佳做法。如需詳細資訊，請參閱 IAM.	2023 年 1 月 3 日
更新了IAM指引 AWS WAF	更新指南以符合最IAM佳做法。如需詳細資訊，請參閱 IAM.	2023 年 1 月 3 日
更新了IAM指引 AWS Shield	更新指南以符合最IAM佳做法。如需詳細資訊，請參閱 IAM.	2023 年 1 月 3 日
更新 Amazon Route 53 解析器DNS防火牆政策	已新增刪除 Amazon Route 53 解析器DNS防火牆規則群組的相關資訊。	2022 年 12 月 29 日
已更新的 AWS 受管規則 AWS WAF	已更新 Linux 作業系統規則集。	2022 年 12 月 15 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集。	2022 年 12 月 5 日
Firewall Manager 器添加了對 Fortigate 雲原生防火牆（CNF）即服務策略的支持	Firewall Manager 器現在支持 Fortigate 策略CNF。	2022 年 12 月 2 日

已移除DNS防火牆政策的 AWS Config 需求	對於DNS防火牆策略，您現在只需要為資源類型啟用 Config EC2 VPC。	2022 年 11 月 17 日
AWS Firewall Manager 受管理策略更新	已更新`FMSServiceRolePolicy` 。	2022 年 11 月 15 日
擴充 AWS WAF CAPTCHA拼圖的語言選項	CAPTCHA拼圖現在提供多種語言的書面說明。每個音頻拼圖中的說明仍然僅以英文提供。	2022 年 11 月 11 日
資源集的新 Firewall Manager 員配額	已新增資源集的配額。	2022 年 11 月 8 日
新增對資源集的支援	您可以建立資源集，以將資源分組到 Firewall Manager 員策略中進行管理。	2022 年 11 月 8 日
添加從網絡防火牆導入防火牆的支持	您現在可以使用資源集匯入和管理 Network Firewall 策略中的現有防火牆。	2022 年 11 月 8 日
AWS Firewall Manager 受管理策略更新	已更新`AWSFMAdminReadOnlyAccess` 。	2022 年 11 月 2 日
Geo match 聲明現在為國家和地區的請求添加標籤	您現在可以透過結合地理位置比對與標籤比對，在區域層級管理地理請求來源。	2022 年 10 月 31 日
已重新命名頂層區段：受管理的保護	此區段現名為 AWS WAF 智慧型威脅緩解功能，與我們的行銷頁面保持一致。	2022 年 10 月 27 日
Bot Control 受管規則群組中的新目標防護層級	Bot Control 受管規則群組現在會針對複雜機器人的偵測和緩解提供額外的目標規則。此保護等級需支付額外費用。	2022 年 10 月 27 日

有關 AWS WAF 令牌的新部分	瞭解如何 AWS WAF 使用 Token 進行智慧型威脅緩解。	2022 年 10 月 27 日
已新增更新 Firewall Manager 員 Network Firewall 策略的重要	當您更新 Firewall Manager 員策略時，策略所建立的所有 Network Firewall 策略都會更新為 Firewall Manager 員策略的 Network Firewall 策略組態。	2022 年 10 月 27 日
規則群組中的動作覆寫	您現在可以將規則群組中規則的動作覆寫為任何規則動作設定。與先前的Count動作覆寫一樣，您可以將覆寫套用至規則群組中的所有規則以及個別規則。	2022 年 10 月 27 日
AWS WAF 新Challenge規則動作選項	您可以將規則配置為使用 Challenge, 以驗證請求是由瀏覽器發送。	2022 年 10 月 27 日
AWS WAF 允許跨多個受保護的應用程式共用	您可以透過設定 Web 的 Token 網域清單，在多個受保護的應用程式中啟用權杖使用ACL。	2022 年 10 月 27 日
所有標題規格不區分大小寫	將所有標題規範更改為不區分大小寫。這與單頭行為匹配。	2022 年 10 月 26 日
AWS Firewall Manager 受管理原則變更	的更正`AWSFMAdminFullAccess` .	2022 年 10 月 21 日
已更新的 AWS 受管規則 AWS WAF	更新已知錯誤輸入規則群組。	2022 年 10 月 20 日
已更新的 AWS 受管規則 AWS WAF	更新已知錯誤輸入規則群組。	2022 年 10 月 5 日
更新至 AWS WAF 行動裝置 SDK規格	將預設值`tokenRefreshDelaySec` 從 600 (10 分鐘) 降低為 300 (5 分鐘)。	2022 年 9 月 30 日

已更新的 AWS 受管規則 AWS WAF	更正本文件中針對下列規則群組提供的標籤名稱：POSIX 作業系統、PHP應用程式、WordPress 應用程式。	2022 年 9 月 19 日
新增 AWS WAF原則規則選項 AWS Firewall Manager	AWS Firewall Manager 現在支援 AWS WAF 原則中預設 Web 動作的自訂 Web 要求和回應。	2022 年 9 月 9 日
已更新的 AWS 受管規則 AWS WAF	更新下列規則群組：IP 信譽。	2022 年 8 月 30 日
AWS WAF 受管理原則變更	已更新`AWSWAFFullAccessPolicy`、`AWSWAFConsoleFullAccess`、`AWSWAFReadOnlyAccess`、和`AWSWAFConsoleReadOnlyAccess`，將 Amazon Cognito 使用者集區新增至您可以使用保護的資源類型。 AWS WAF	2022 年 8 月 25 日
AWS WAF 防止欺詐控制帳戶接管 ( ) ATP	您現在可以在 Amazon CloudFront 分發中使用 AWS WAF 詐騙控制帳戶接管預防 (ATP) 功能。	2022 年 8 月 24 日
已更新的 AWS 受管規則 AWS WAF	更新下列規則群組：已知錯誤輸入。	2022 年 8 月 22 日
已更新的 AWS 受管規則 AWS WAF	已更新下列規則群組：`AWSManagedRulesATPRuleSet`	2022 年 8 月 11 日

增加了對 Amazon Cognito 用戶池的支持 AWS WAF	您現在可以將 AWS WAF 網路ACL與 Amazon Cognito 使用者集區建立關聯。此變更僅適用於最新版本的， AWS WAF 而不適用於 AWS WAF 經典版本。	2022 年 8 月 11 日
已針對已建立版本的 AWS 受管規則規則群組新增部署章節	已新增記錄已建立版本之 AWS 受管理規則群組之部署的新章節。本節包含有關在候選發行版本部署期間如何命名預設版本的資訊。	2022 年 7 月 29 日
更新設定 Network Firewall 策略記錄的需求	新增使用加密 Amazon S3 儲存貯體做為日誌目標的 Network Firewall 政策的需求。	2022 年 7 月 26 日
SQLi規則陳述式的敏感度層級選項	您現在可以提高SQL注入規則陳述式的敏感度。這不會變更現有陳述式的行為，其敏感度層級為預設值LOW。	2022 年 7 月 15 日
添加 Network Firewall 策略配置選項	Firewall Manager 員現在支援 Network Firewall 防火牆策略組態中的狀態評估順序和預設處理行動	2022 年 7 月 14 日
Firewall Manager 員安全群組原則規則設定的更新	Firewall Manager 員現在支援從主要安全性群組到複本安全群組的標籤散發。	2022 年 7 月 7 日
AWS Shield 指南的更新	擴充 Shield 指南中的資訊，以說明 Shield 如何執行事件緩解。	2022年6月24日
更新的測試和調整 AWS WAF 保護指南	測試和調整 AWS WAF 的一般指引已更新，現在是最上層的主題。	2022 年 6 月 20 日

已更新的 AWS 受管規則 AWS WAF	更新下列規則群組：核心規則集 (CRS)。	2022 年 6 月 9 日
新的 Firewall Manager 器混淆副指導	已新增有關如何避免「Firewall Manager 員」混淆的副問題的指引。	2022 年 6 月 1 日
已更新的 AWS 受管規則 AWS WAF	更新下列規則群組：核心規則集 (CRS)。	2022 年 5 月 24 日
新的 AWS WAF 請求元件：Headers和 Cookies	您現在可以檢查 Web 請求中的 Cookie，除了只有一個標頭之外，您還可以檢查 Web 請求中的所有標頭。	2022 年 4 月 29 日
AWS WAF 處理過大的主體，標題和 cookie 請求組件	您現在可以在檢查這些元件的規則中指定 AWS WAF 應如何處理超大要求主體、標頭和 Cookie。您已經建立用來檢查這些元件的規則具有符合超大處理新Continue選項的行為。	2022 年 4 月 29 日
AWS WAF Amazon S3 日誌政策更改	更新了 Amazon S3 日誌許可政策和示例。	2022 年 4 月 12 日
應用程式負載平衡器現在提供自動應 AWS Shield Advanced 用程式層DDoS緩解選項	Shield Advanced 現在支援應用程式負載平衡器的自動應用程式層DDoS緩解功能，使其可用於所有應用程式層保護。您可以將 Shield Advanced 設定為自動計數或封鎖屬於受保護資源之應用程式層DDoS攻擊一部分的 Web 要求。	2022 年 4 月 8 日
為受管規則群組新增目前預設版本設定的指標	受管規則群組版本清單現在會指出目前的預設版本。	2022 年 4 月 8 日

已更新的 AWS 受管規則 AWS WAF	更新下列規則群組： AWS WAF 機器人控制。	2022 年 4 月 6 日
已更新的 AWS 受管規則 AWS WAF	更新下列規則群組：已知錯誤輸入。	2022 年 3 月 31 日
已更新的 AWS 受管規則 AWS WAF	更新下列規則群組：已知錯誤輸入。	2022 年 3 月 30 日
Firewall Manager 器增加了對帕洛阿爾托網絡雲下一代防火牆的支持（ ）NGFW	Firewall Manager 器現在支持帕洛阿爾托網絡雲下一代防火牆（NGFW）。	2022 年 3 月 30 日
將對帕洛阿爾托網絡雲NGFW的支持添加到 AWS Firewall Manager	AWS Firewall Manager 現在支持帕洛阿爾托網絡雲下一代防火牆（NGFW）策略。	2022 年 3 月 30 日
AWS Shield 指南的更新	擴充 Shield 指南中的資訊，以說明 Shield 如何執行事件偵測，並提供DDoS彈性架構的範例。	2022 年 3 月 16 日
AWS Shield 指南的更新	擴展了 Shield 指南中的資訊，並改善了各個部分的組織。主要變更在以下護 Shield 指南章節中：護 Shield 回應小組 (SRT) 支援 AWS Shield Advanced、中的資源保護以及DDoS事件能見度。	2022 年 2 月 28 日
Firewall Manager 器現在支持 Network Firewall 集中部署模型	已新增說明如何設定使用分散式和集中式部署模型之原則的新程序。	2022 年 2 月 24 日

Firewall Manager 員新增對 AWS Network Firewall 集中式部署模型的支援	您現在可以將 AWS Network Firewall 原則設定為使用分散式或集中式部署模型。使用分散式部署模型，Firewall Manager 會在策略範圍內的每個VPC端點中建立並維護防火牆端點。使用集中式部署模型，「Firewall Manager 員」會在單一檢查中建立並維護防火牆端點VPC。	2022 年 2 月 24 日
將對 AWS WAF 受管規則群組版本化的支援新增至 AWS Firewall Manager	AWS Firewall Manager 現在支援 Firewall Manager 員 AWS WAF 策略中的 AWS WAF 受管規則群組版本化	2022 年 2 月 18 日
AWS Firewall Manager 受管理原則變更	更新至`FMSServiceRolePolicy` 。	2022 年 2 月 16 日
已更新的 AWS 受管規則 AWS WAF	更新下列規則群組：IP 信譽清單。	2022 年 2 月 15 日
已更新的 AWS 受管規則 AWS WAF	更新 AWS WAF 詐騙控制帳戶接管預防 (ATP) 規則群組`AWSManagedRulesATPRuleSet` 。	2022 年 2 月 11 日
更改指 AWS WAF 南的組織	已新增受管理保護的新頂層區段。將CAPTCHA區段從「規則」下移至「新的受管理的保護」區段下。將「標籤」區段從「規則」下移至其自己的頂層區段。	2022 年 2 月 11 日

AWS WAF 用戶端應用程式	使用 AWS WAF JavaScript 和行動用戶端將您的用戶端應用程式與智慧型威脅緩和 AWS 受管規則群組整合，APIs以增強偵測。	2022 年 2 月 11 日
AWS WAF 防止欺詐控制帳戶接管 ( ) ATP	您可以使用新的 AWS WAF 詐騙控制帳戶接管預防 (ATP) 受管規則群組，偵測並封鎖帳戶接管嘗試。`AWSManagedRulesATPRuleSet`	2022 年 2 月 11 日
已更新的 AWS 受管規則 AWS WAF	更新下列規則群組：已知錯誤輸入。	2022 年 1 月 28 日
AWS WAF 受管理原則變更	已更新`AWSWAFFullAccessPolicy` 並`AWSWAFConsoleFullAccess` 更正記錄權限。	2022 年 1 月 11 日
已更新的 AWS 受管規則 AWS WAF	更新下列規則群組：核心規則集 (CRS)、SQLi資料庫。	2022 年 1 月 10 日
Firewall Manager 器支持 Shield 高級自動應用層DDoS緩解	Firewall Manager 員防 Shield Amazon CloudFront 資源的進階政策現在包含對自動應用程式層DDoS緩解的支援。	2022 年 1 月 7 日
AWS Firewall Manager 受管理原則變更	更新至`FMSServiceRolePolicy` 。	2022 年 1 月 7 日
已更新的 AWS 受管規則 AWS WAF	更新下列規則群組：已知錯誤輸入。	2021 年 12 月 17 日
已更新的 AWS 受管規則 AWS WAF	更新下列規則群組：已知錯誤輸入。	2021年12月11日

已更新的 AWS 受管規則 AWS WAF	更新下列規則群組：已知錯誤輸入。	2021 年 12 月 10 日
新的 AWS Shield Advanced 服務連結角色	已新增`AWSServiceRoleForAWSShield` 以支援自動應用程式層DDoS緩解功能。	2021 年 12 月 1 日
新的 AWS Shield 受管理策略	已新增`AWSShieldServiceRolePolicy` 以支援自動應用程式層DDoS緩解功能。	2021 年 12 月 1 日
自動應用程式層DDoS緩解選項現在可用 AWS Shield Advanced 於 CloudFront	Shield 牌進階現在支援 Amazon CloudFront 分發的自動應用程式層DDoS緩解功能。您可以將 Shield Advanced 設定為自動計數或封鎖屬於發佈版本中應用程式層DDoS攻擊一部 CloudFront分的 Web 要求。	2021 年 12 月 1 日
已更新的 AWS 受管規則 AWS WAF	更新下列規則群組：核心規則集 (CRS)、Windows 作業系統、Linux 作業系統和 IP 信譽清單。	2021 年 11 月 23 日
AWS Firewall Manager 受管理原則變更	更新至`FMSServiceRolePolicy` 。	2021 年 11 月 18 日
擴充的記錄選項 AWS WAF	您現在可以將網路ACL流量記錄到 Amazon CloudWatch 日誌日誌群組或亞馬遜簡單儲存服務 (Amazon S3) 儲存貯體。這些選項是記錄到 Amazon 資料 Firehose 交付串流的現有選項之外。	2021 年 11 月 15 日

AWS WAF 受管理原則變更	已更新AWSWAFFullAccessPolicy 並AWSWAFConsoleFullAccess 支援其他記錄目的地。	2021 年 11 月 15 日
AWS WAF 新CAPTCHA規則動作選項	您可以配置規則以CAPTCHA針對 Web 請求運行，並在需要時向客戶端發送CAPTCHA問題。	2021 年 11 月 8 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集 (CRS) 規則群組。	2021 年 10 月 27 日
已更新的 AWS 受管規則 AWS WAF	所有 AWS 受管規則規則群組現在都支援標籤。規則描述包括標籤規格。	2021 年 10 月 25 日
Firewall Manager 員支援 Network Firewall 記錄	AWS Firewall Manager 現在支援 Network Firewall 策略的記錄檔篩選。	2021 年 10 月 4 日
AWS Firewall Manager 受管理原則變更	更新至FMSServiceRolePolicy 。	2021 年 9 月 29 日
添加正則表達式匹配	您現在可以將 Web 要求與單一規則運算式進行比對。	2021 年 9 月 22 日
規則群組內的速率型規 AWS WAF 則	您現在可以在規則群組內定義以比率為基準的規 AWS WAF 則。在中 AWS Firewall Manager， AWS WAF 原則完全支援此功能。	2021 年 9 月 13 日
Firewall Manager 員支援 AWS WAF 記錄檔	AWS Firewall Manager 現在支援 AWS WAF 策略的記錄檔篩選。	2021 年 8 月 31 日

自動移除 out-of-scope 資源保護 AWS Firewall Manager	AWS Firewall Manager 可讓您從離開策略範圍的資源自動移除保護。	2021 年 8 月 25 日
AWS Firewall Manager 受管理原則變更	更新至`FMSServiceRolePolicy` 。	2021 年 8 月 12 日
為受管規則群組新增版本控制	受管規則群組提供者現在可以版本化其規則群組。	2021 年 8 月 9 日
修改 AWS Firewall Manager 管理員需求	您可以使用組織的管理帳戶做為 Firewall Manager 員帳戶。這是不允許的。	2021 年 8 月 2 日
Firewall Manager 員配額增	在 Firewall Manager 員政策範圍內，您可以擁有的 Amazon VPC 執行個體數量從 10 個增加到 100 個。	2021 年 7 月 28 日
AWS Firewall Manager 支持 AWS Network Firewall 路由表監控	AWS Firewall Manager 現在支援路由表監控，並針對設定錯誤路由的 AWS Network Firewall 原則提供補救動作建議給安全管理員。	2021 年 7 月 8 日
AWS WAF 其他文字轉換選項	文字轉換的擴充選項，您可以先套用至 Web 要求元件，然後再檢查這些元件。	2021 年 6 月 24 日
修改 Firewall Manager 員 AWS WAF 策略資源的命名	Firewall Manager 員為您的 AWS WAF 策略管理的 Web ACLs、規則群組和記錄的命名已變更。	2021 年 5 月 26 日
已更新的 AWS 受管規則 AWS WAF	更新了對 IP 信譽清單標籤的支援，並移除 Amazon IP 信譽清單規則名稱上的尾碼。	2021 年 5 月 4 日

新增 AWS Organizations 委派管理員的支援	當您設定管理 AWS Firewall Manager 員帳戶時，「Firewall Manager 員」現在會將該帳戶指定為「Firewall Manager 員」的 AWS Organizations 委派管理員。透過此變更，當您設定 Firewall Manager 員管理員帳戶時，必須提供組織管理帳戶以外的成員帳戶。這項變更不會影響您現有的設定。	2021 年 4 月 30 日
已更新的 AWS 受管規則 AWS WAF	更新了 AWS WAF 機器人控制規則群組。	2021 年 4 月 1 日
Count在規則群組中將個別規則動作設定為	您現在可以將規則群組中的個別規則動作設定為Count。現有覆寫 (位於規則群組層級) 的資訊已更正。	2021 年 4 月 1 日
受管規則群組的向下語句	您現在可以在受管規則群組中使用範圍向下陳述式，方式與使用速率型陳述式相同。	2021 年 4 月 1 日
日誌過濾	您現在可以根據規則動作和標籤篩選記錄的 Web ACL 流量。	2021 年 4 月 1 日
AWS WAF 標籤, 上, 网, 請求	您可以設定規則，將標籤新增至相符的 Web 要求，以及比對由其他規則新增的標籤。	2021 年 4 月 1 日
AWS WAF 機器人控制	您可以使用全新的 Bot Control 功能來監控和控制 AWS WAF 機器人流量，該功能結合了 Bot Control 受管理規則群組與 Web 要求標籤、範圍陳述式和記錄篩選。	2021 年 4 月 1 日

Firewall Manager 器支持 Amazon Route 53 解析器DNS 防火牆政策	AWS Firewall Manager 支援 Amazon Route 53 解析器DNS 防火牆輸出DNS流量篩選的集中管理。VPCs	2021 年 3 月 31 日
自定義請求和響應處理	您可以為 AWS WAF 不會封鎖的 Web 要求加入自訂標頭，也可以針對封鎖的 Web 要求傳送自訂回應。 AWS WAF 這適用於 Web ACL 預設處理行動和規則動作設定。	2021 年 3 月 29 日
AWS Firewall Manager 受管理原則變更	更新至`FMSServiceRolePolicy` 。	2021年3月17日
已更新的 AWS 受管規則 AWS WAF	更新下列規則群組：核心規則集 (CRS)、管理員防護、已知錯誤輸入，以及 Linux 作業系統。	2021 年 3 月 3 日
AWS Shield 受管原則變更追蹤	Shield 開始追蹤其 AWS 受管理政策的變更。	2021 年 3 月 3 日
AWS Firewall Manager 受管原則變更追蹤	Firewall Manager 員開始追蹤其 AWS 受管理策略的變更。	2021 年 3 月 2 日
AWS WAF 受管原則變更追蹤	AWS WAF 開始追蹤其 AWS 受管理策略的變更。	2021 年 3 月 1 日
檢查網絡請求主體的解析 JSON	添加了以解析和過濾JSON方式檢查 Web 請求主體的選項。這是現有選項以純文本檢查 Web 請求主體的補充。	2021 年 2 月 12 日
Firewall Manager 程式支 AWS Network Firewall 援	AWS Firewall Manager 支援中央管理 AWS Network Firewall 網路流量篩選VPCs。	2020 年 11 月 17 日

新增對 AWS Shield Advanced 保護群組的支援	您現在可以將受保護的資源分組為邏輯群組，並統一管理其保護。	2020 年 11 月 13 日
增加了對於 AWS AppSync 支持 AWS WAF	您現在可以將 AWS WAF 網頁ACL與 AWS AppSync GraphQL API 建立關聯。此變更僅適用於最新版本的， AWS WAF 而不適用於 AWS WAF 經典版本。	2020 年 10 月 1 日
已更新的 AWS 受管規則 AWS WAF	更新視窗作業系統規則集。	2020 年 9 月 23 日
已更新的 AWS 受管規則 AWS WAF	更新規則集PHP應用程式和POSIX作業系統。	2020 年 9 月 16 日
更新 AWS Shield 主控台	AWS Shield 提供新的主控台選項，並改善使用者體驗。說明文件中的主控台指引適用於新主控台。	2020 年 9 月 1 日
Firewall Manager 員更新一般安全性群組原則	AWS Firewall Manager 通用安全群組原則現在透過主控台實作支援應用程式負載平衡器和傳統負載平衡器資源類型。通用原則的原則範圍設定中提供了新選項。	2020 年 8 月 11 日
已更新的 AWS 受管規則 AWS WAF	更新核心規則集。	2020 年 8 月 7 日
Firewall Manager 程式支援 AWS WAF 記錄	AWS Firewall Manager 現在支援原則的集中式記錄設 AWS WAF 定。	2020 年 7 月 30 日

在 Web 請求中指定 IP 地址位置	新增了從您指定的HTTP標頭使用 IP 位址的選項，而不是使用 Web 請求來源。備用標題通常是X-Forwarded-For（XFF），但您可以指定任何標題名稱。您可以使用此選項進行 IP 集比對、地理比對和以速率為基礎的規則計數彙總。	2020 年 7 月 9 日
Firewall Manager 員更新內容稽核安全性群組策略	AWS Firewall Manager 具有內容稽核安全性群組策略的擴充功能，包括受管理的規則選項、使用受管理應用程式和通訊協定清單，以及資源違規的詳細資料。	2020 年 7 月 7 日
Firewall Manager 員受管理	AWS Firewall Manager 現在支持託管應用程序和協議列表。Firewall Manager 器管理一些列表，您可以創建和管理自己的列表。	2020 年 7 月 7 日
Firewall Manager 員支援VPCs共用一般安全性群組原則	AWS Firewall Manager 現在支援在共用中使用一般安全性群組原則VPCs。除了在範圍內帳戶VPCs擁有的帳戶中使用它們之外，您還可以執行此操作。	2020 年 5 月 26 日
已更新的 AWS 受管規則 AWS WAF	已新增的 AWS 受管規則中每個規則的文件 AWS WAF。	2020 年 5 月 20 日
已更新的 AWS 受管規則 AWS WAF	更新 Linux 作業系統規則群組。	2020 年 5 月 19 日
新增將 AWS WAF 傳統資源移轉至 AWS WAF (v2) 的支援	您現在可以使用主控台或API匯出 AWS WAF 傳統資源，以移轉至最新版本的 AWS WAF。	2020 年 4 月 27 日

在政策範圍中新增對 AWS Organizations 組織單位的支援	AWS Firewall Manager 現在支援使用 AWS Organizations 組織單位 (OUs) 來指定原則範圍。除了包含或排除特定帳戶之外，您還可以使用OUs在範圍內包含或排除帳戶。指定 OU 與指定 OU 及其任何子系中的所有帳戶相同OUs，包括稍後新增的任何子系OUs和帳戶。	2020 年 4 月 6 日
將對 AWS WAF （v2）的支持添加到 AWS Firewall Manager	AWS Firewall Manager 除了以前的版本 AWS WAF 經典之外 AWS WAF，現在還支持最新版本。	2020 年 3 月 31 日
一 AWS Firewall Manager 般安全性群組原則的更新	AWS Firewall Manager 通用安全群組原則現在可以選擇將政策套用到範圍內 Amazon EC2 執行個體中的所有彈性網路界面。您仍然可以選擇只將原則套用至預設彈性網路界面。	2020 年 3 月 11 日
已更新的 AWS 受管規則 AWS WAF	AWS AWS WAF 新增規則群組的受管規`AWSManagedRulesAnonymousIpList` 則。	2020 年 3 月 6 日
已更新的 AWS 受管規則 AWS WAF	AWS AWS WAF 更新 WordPress 應用程式和規`AWSManagedRulesCommonRuleSet` 則群組的受管規則。	2020 年 3 月 3 日

為 AWS Shield Advanced 保護選項添加了 Amazon Route 53 健康檢查	Shield 牌進階現在支援使用 Amazon Route 53 運作狀態檢查關聯，以提高威脅偵測和緩解的準確性。	2020 年 2 月 14 日
已更新的 AWS 受管規則 AWS WAF	AWS 的受管理規則 AWS WAF 已更新資SQL料庫規則群組，以新增檢查郵件URI。	2020 年 1 月 23 日
Firewall Manager 員安全性群組使用稽核策略的新選項	Firewall Manager 員為安全性群組使用稽核策略提供了新選項。您現在可以設定安全群組在被視為不相容之前，必須保持未使用的最小分鐘數。根據預設，此分鐘設定為零。	2020 年 1 月 14 日
Firewall Manager 員 AWS WAF 策略的新選項	Firewall Manager 員為 AWS WAF 策略提供了新選項。您現在可以選擇從範圍內的資源中移除所有現有的 Web ACL 關聯，然後再將原則的新 Web ACLs 關聯與它們建立關聯。	2020 年 1 月 14 日
已更新的 AWS 受管規則 AWS WAF	AWS 的受管理規則 AWS WAF 已更新核心規則集和SQL資料庫規則群組中規則的文字轉換。	2019 年 12 月 20 日
AWS Firewall Manager 與整合 AWS Security Hub	AWS Firewall Manager 現在會針對不合規的資源和攻擊建立發現項目，並將其傳送至 AWS Security Hub。	2019 年 12 月 18 日

AWS WAF 版本 2 的發行	AWS WAF 開發人員指南的新版本。您可以使用JSON格式管理 Web ACL 或規則群組。擴充的功能包括邏輯規則陳述式、規則陳述式巢狀，以及對 IP 位址和位址範圍的完整CIDR支援。規則不再是 AWS 資源，而只存在於 Web ACL 或規則群組的前後關聯中。對於現有客戶，服務的先前版本現在稱為「 AWS WAF 傳統」。在、和中 APIsSDKs，C AWS WAF lassic 會保留其命名配置CLIs，且這個最新版本會根據上下文加上新增的「V2」或「v2」來參照。 AWS WAF AWS WAF 無法存取在 AWS WAF 傳統版中建立的 AWS 資源。若要在中使用這些資源 AWS WAF，您需要移轉它們。	2019 年 11 月 25 日
AWS 的受管規則規則群組 AWS WAF	新增 AWS 受管規則規則群組。這些對 AWS WAF 客戶來說是免費的。	2019 年 11 月 25 日
AWS Firewall Manager 支援 Amazon Virtual Private Cloud 安全群組	為 Firewall Manager 器添加了對 Amazon VPC 安全組的支持。	2019 年 10 月 10 日
AWS Firewall Manager 支援 AWS Shield Advanced	為 Firewall Manager 員新增防 Shield 進階的支援。	2019 年 3 月 15 日
教學課程：建立階層原則	新增在 AWS Firewall Manager 中建立階層政策的教學課程。	2019 年 2 月 11 日

規則群組中的規則層級控制	您現在可以從規 AWS Marketplace 則群組以及您自己的規則群組中排除個別規則。	2018 年 12 月 12 日
AWS Shield Advanced 支援 AWS Global Accelerator 標準加速器	Shield 牌進階現在可以保護 AWS Global Accelerator 標準加速器。	2018 年 11 月 26 日
AWS WAF 支持 Amazon API 網關	AWS WAF 現在保護 Amazon API 網關APIs。	2018 年 10 月 25 日
擴充 AWS 屏蔽進階入門精靈	新精靈提供建立以速率為基礎的規則和 Amazon CloudWatch 活動的機會。	2018 年 8 月 31 日
AWS WAF logging	啟用日誌記錄以獲取有關您的 Web 分析流量的詳細信息 ACL。	2018 年 8 月 31 日
Support 條件下的查詢參數	建立測試條件時，您現在可以搜尋請求的特定參數。	2018 年 6 月 5 日
Shield 牌進階入門精靈	推出新的簡化程序來訂閱 AWS 護 Shield 進階版。	2018 年 6 月 5 日
擴充的允許CIDR範圍	建立 IP 比對條件時， AWS WAF 現在支援位IPv4址範圍：/8 以及 /16 到 /32 之間的任何範圍。	2018 年 6 月 5 日

二零一八年之前

下表說明 2018 年之前每個版本的《AWS WAF 開發人員指南》中的重要變更。

變更	API 版本	描述	版本日期
更新	2016-08-24	AWS Marketplace 規則群組	2017 年 11 月

變更	API 版本	描述	版本日期
更新	2016-08-24	Shield 進階支援彈性 IP 地址。	2017 年 11 月
更新	2016-08-24	全球威脅儀表板	2017 年 11 月
更新	2016-08-24	防 DDoS 網站教學課程	2017年 10 月
更新	2016-08-24	Geo 和 regex 條件	2017年 10 月
更新	2016-08-24	速率為基礎的規則	2017 年 6 月
更新	2016-08-24	重組	2017 年 4 月
更新	2016-08-24	新增 DDOS 保護和支援應用程式負載平衡器的資訊	2016 年 11 月
新功能	2015-08-24	您現在可以 AWS WAF 透過這項 AWS 服務記錄帳戶的 API 呼叫 AWS CloudTrail，並將日誌檔案傳送到 S3 儲存貯體的服務記錄所有 API 呼叫。 CloudTrail 記錄檔可用於啟用安全性分析、追蹤 AWS 資源的變更，以及協助法規遵循稽核。整合 AWS WAF 並 CloudTrail 可讓您判斷要對 AWS WAF API 發出哪些要求、發出每個要求的來源 IP 位址、提出要求的人員、提出要求的時間等等。 如果您已經在使用 AWS CloudTrail，您將開始在 CloudTrail 日誌中看到 AWS WAF API 調用。如果您尚未啟 CloudTrail 用您的帳戶，可以 CloudTrail 從啟用AWS Management Console。啟用無須額外付費 CloudTrail，但 Amazon S3 和 Amazon SNS 的使用需支付標準費率。	2016 年 4 月 28 日

變更	API 版本	描述	版本日期
新功能	2015-08-24	您現在可以使用 AWS WAF 來允許、封鎖或計算看似包含惡意指令碼 (稱為跨網站指令碼或 XSS) 的 Web 要求。攻擊者有時會將惡意指令碼插入到 web 請求中，利用 web 應用程式的漏洞。如需詳細資訊，請參閱 跨網站指令碼攻擊規則陳述式。	2016 年 3 月 29 日
新功能	2015-08-24	在此版本中， AWS WAF 新增下列功能： • 您可以設定為根據要求的指定部分 (例如查詢字串或 URI) 的長度 AWS WAF 來允許、封鎖或計數 Web 要求。如需詳細資訊，請參閱 大小約束規則陳述式。 • 您可以設定 AWS WAF 為根據要求主體中的內容允許、封鎖或計數 Web 要求。這也是請求的一部分，其中包含您想傳送至您的 web 伺服器做為 HTTP 請求內文的額外資料，您要傳送到您的 Web 伺服器的 HTTP 請求的內文，例如資料表單。此功能適用於字串、SQL injection 符合條件，和在第一個項提及的新容量限制條件。如需詳細資訊，請參閱 Web 請求組件規格和處理。	2016 年 1 月 27 日
新功能	2015-08-24	現在，您可以使用 AWS WAF 控制台來選擇要與 Web ACL 相關聯的 CloudFront 發行版。如需詳細資訊，請參閱關聯或取消 Web ACL 與分佈的關聯。 CloudFront	2015 年 11 月 16 日
初始版本	2015-08-24	這是《AWS WAF 開發人員指南》的第一個版本。	2015 年 10 月 6 日

AWS 詞彙表

有關最新 AWS 術語，請參閱AWS 詞彙表 參考文獻中的AWS 詞彙表。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。