International Journal of IT & Knowledge Management (ISSN: 0973-4414)
Volume 11 • Issue 2 pp. 14-20 Jan 2018 - June 2018 www.csjournals.com

Window azure Active Directory Services for Maintaining Security & Access Control

[1] Rini Mahajan, [2]Dr. Manish Mahajan, [3]Dr. Dheerendra Singh
[1]Ph.D Research Scholar I. K. Gujral PTU Jalandhar, rinimahajan@gmail.com
[2]Associate Professor(Department of Computer Science) Chandigarh Engineering College, Landran, Mohali, India, manishmahajan4u@gmail.con
[3]Associate Professor (Department of Computer Science) at CCET, Sector 26,, Chandigarh, India, professordsingh@gmail.com

Abstract: Cloud computing is new technology that provides economical, easier, and more powerful processes and resources to customers over internet. Cloud computing dynamically delivers everything as a service over the Internet such as network, operating system, storage, hardware, software, and resources. All the services of cloud are on demand. Since cloud is internet based; thus many security and privacy issues must be taken into consideration. There are different types of threats and attack from which we have to secure ourselves. There are so many cloud providers in the market. One of the providers is Microsoft Azure. Taking in to consideration one of the major security issues is access control; the window azure active directory in one of the best solutions. This paper aims to discuss the importance of access control in the cloud environment as well as the support of active directory services in achieving secure access environment.
Keywords: Access control, Active directory, Identity Management, , Security, , SSO.

Introduction

The term **cloud is analogical to internet. So** the term ***cloud computing*** means "***a type of Internet-based computing,"*** where different services are delivered to an organization's computers and devices through the Internet. Cloud computing provides shared resources, software and information, to computers and devices on-demand [7, 8]. It is intended to construct a perfect system with powerful computing capability through a large number of relatively low-cost computing entities. It enables on demand network access to a shared pool of configurable computing resources e.g., networks, servers, storage, applications, and services. Another definition of cloud computing was also proposed by Buyya et al in terms of its utility to end user: "A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers" [1].
Cloud computing provides following services:

1. SaaS (Software as a Service) - This service is for the clients to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through an interface such as a web browser such email. The client is not required to own cloud infrastructure including network, servers, operating systems, storage.
2. PaaS (Platform as a Service) - This service provides clients to deploy applications onto the cloud infrastructure created using programming languages and tools supported by the provider.
3. IaaS (Infrastructure as a Service)- This service provides clients with the provision of processing, storage, networks, and other fundamental computing resources where the client is able to deploy and run software such as operating systems and applications [2].

Cloud computing is a better and economic way to run any business. We are not required to install apps on our system rather they run on a shared data centre. When we use any Cloud app then, we just log in, customize it, and start using it. This shows the power of cloud computing [3]. Clouds are of different types; they vary according to cost and security level:
a. Public Clouds: These types of clouds are either free of cost or very cheaper, but the security levels of such clouds are low.
b. Private Clouds: Cloud infrastructure for single organization only, may be managed by the organization or third party, on or off premise. These clouds are high in cost but provide better security.
c. Hybrid Clouds: It uses public clouds for general computing while sensitive information is kept within a private cloud.
d. Community Clouds: Cloud infrastructure shared by several organization that have shared concern, managed by organization or third party [9].
Cloud security issues

Although cloud computing environment is very efficient and economic for big organization, but one of the most important issues in cloud environment is security. Cloud providers are not totally aware of a specific organization's security and privacy needs. Cloud computing environment may be customized to meet an organization's requirements. Organizations demands that any selected public cloud computing solution is configured, deployed, and managed to meet their security, privacy, and other requirements. Cloud computing environment should meet server side organizational security and privacy requirements.
Since Cloud computing is internet based environment that's why Web browsers are a key element for client-side access to cloud computing services. The various available plug-ins and extensions for Web browsers are the main reasons for their security problems. Many browser add-ons also do not provide automatic updates, so it increases the persistence of any existing vulnerabilities. Security continues to be a major challenge for cloud computing, and it must be addressed if cloud computing is to be fully accepted. One of the major threats to cloud computing environment is non authorized access to data, application or infrastructure. For this to be implemented we need a strong access control mechanism in the cloud environment [19].

Identity Management and Access control in cloud

All the organizations have sensitive data and privacy information, it is important to keep those secure. Unauthorized access to information resources in the cloud is a major concern for an organization [10]. Identity and access management (IAM) is a significant function for every organization [11]. It can be defined as the "methods that provide an adequate level of protection for organization resources and data through rules and policies which are enforced on users via various techniques such as enforcing login password, assigning privileges to the users and provisioning user accounts"[12]. Access control is generally a policy or procedure that allows, denies or restricts access to a system. It may, as well, monitor and record all attempts made to access a system. Access Control may also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security [13]. Managing user's identity and providing adequate privacy and protection in the cloud is a great challenge. Identity and access control is mainly based on authentication and authorization. For a traditional network these mechanisms are static and controlled within the organization. But in case of cloud due to involvement of 3rd party, so the network boundary of an organization will extend into the service provider domain. Thus, application security and user access controls must compensate for the loss of network control and to strengthen risk assurance [14, 20]. IAM is the proven solution for cloud users. It reduces security reduces administrative expenses and improves efficiency.
These access IAM mechanisms are implemented in cloud platforms. There are so many cloud platforms such as Google, Amazon, and Microsoft Azure etc. Microsoft Azure is one of the most efficient cloud platforms. Its important factor is Azure active directory services. This paper concentrates on Window azure platform especially describing the advantages of using active directory services of it.

Window Azure

Microsoft Windows Azure platform is a group of cloud technologies, each of which provides a specific set of services to application developers. It provides an easily adaptable & flexible environment to support specific needs and services of the development team, customers and users. The Windows Azure platform enables developers and users to use existing Microsoft technologies to develop or use applications in the cloud [4].The Azure Service Platform is built on the Windows Azure cloud operating system, which provides a development, hosting, and management environment for cloud applications. Numerous services are available on top of the Azure operating system including Live Services and .NET Services. Microsoft is using a combination of Microsoft .NET framework and the Microsoft Visual Studio development tools to provide a base for developers to easily launch new solutions in the cloud. It is noted that both applications running in the cloud and outside of the cloud can use the Azure cloud platform. Windows Azure divides application instances into virtual machines (VMs). A Windows Azure developer creates Web role and Worker role instances, where a Web role accept incoming HTTP requests and Worker roles are triggered by Web roles via a queue. Any work performed by a Worker role instance can then be stored in the Azure storage or sent outside of the cloud network. Web role instances are stateless. To expand the performance of an application, multiple Worker role instances can be run across dedicated processor cores. If a Worker role or Web role fails, the Azure fabric restarts it [4].
Windows Azure platform comprises the following:

1. Windows Azure- it is a Windows environment for running applications and storing data on computers in Microsoft data centers. It consists of five components Compute, Storage Fabric Controller, Content Delivery & Network Connect.
2. Microsoft SQL Azure- This is used to store data in the cloud. It is built on Microsoft SQL Server. It includes three components SQL Azure Database, SQL Azure & SQL Azure Data Sync .Synchronization amongst various SQL Azure databases present in different Microsoft data centers is done by using Azure Data Sync.

3. Windows Azure Platform AppFabric- It provides infrastructure for applications. It consists of the following three components Service Bus, Access Control & Caching.
4. Windows Azure Marketplace: This helps customers to find and buy cloud applications and cloud-accessible data. It consists of two components DataMarket & AppMarket.[4]
   Other than these components one of the most important features of Window Azure is Active directory services.

Windows Azure Active Directory Access Control or Access Control Service (ACS) is a cloud-based service which provides an easy way of authenticating users to access to web applications and services. ACS integrates with standards-based identity providers, including enterprise directories such as Active Directory, and web identities such as Windows Live ID.Windows Azure Active Directory provides enterprise-level identity and access management for the cloud applications. It is a comprehensive identity and access management cloud solution. It combines core directory services, advanced identity governance, security and application access management. Windows Azure Active Directory also offers to developers an identity management platform to deliver access control to their applications, based on centralized policy and rules. Use of Windows Azure AD centrally manages users' access to Windows Azure and other Microsoft online services. It provides single sign-on across all cloud applications. It makes easier for end users to quickly and effectively launch cloud applications from within their personalized web-based Access Panel. Enable Multi-factor Authentication for enhanced security. Windows Azure Active Directory offers developers an effective way to integrate identity management in their applications. [15].

Windows Azure Access Control Service (ACS) is a Windows-owned cloud-based service that provides an easy way of authenticating and authorizing users to gain access to web applications and services while allowing the features of authentication and authorization to be factored out of the application code. ACS is built on the principles of claims-based identity -- a consistent approach to creating authentication mechanisms for applications running on-premises or in the cloud. Claims-based identity provides a common way for applications and services to get the identity information they need about users inside their organization, in other organizations, and on the internet [16].

[3] Azure active directory services- Azure Active Directory (Azure AD) is Microsoft's multi-tenant, cloud based directory and identity management service. Azure AD combines core directory services, advanced identity governance, and application access management. Azure AD also offers a rich, standards-based platform that enables developers to deliver access control to their applications, based on centralized policy and rules. For IT Administrators, Azure AD provides an affordable, easy to use solution to give employees and business organizations single sign-on (SSO) access to thousands of cloud SaaS Applications like Office365, Salesforce.com, DropBox, and Concur. For application developers, Azure AD lets us focus on building application by making it fast and simple to integrate with a world class identity management solution used by millions of organizations around the world. Azure AD also includes a full suite of identity management capabilities including multi-factor authentication, device registration, self-service password management, self-service group management, privileged account management, role based access control, application usage monitoring, rich auditing and security monitoring and alerting. These capabilities can help secure cloud based applications, streamline IT processes, cut costs and help ensure that corporate compliance goals are met. Additionally, with just four clicks, Azure AD can be integrated with an existing Windows Server Active Directory; giving organizations the ability to leverage their existing on-premises identity investments to manage access to cloud based SaaS applications [18]. Azure Active Directory (AD) provides the core directory and identity management capabilities behind most of Microsoft's cloud services. We can either use the Azure Management Portal or the Office 365 Admin Center to manage organization's directory data. We can do various tasks using this active directory services such as:

- Create and manage user and group accounts
- Manage various cloud services subscribed by the users.
- On-premises integration with our directory service.
- The Azure Management read from and writes to a single shared instance of Azure AD that is associated with our organization's directory.
- We can assign different types of administrators to performing various tasks such as creating and editing users, managing billing operations, and resetting passwords.
- Global administrators grant permissions to different administrators within the

Access control using azure Directory services-

Azure Active Directory uses Conditional access rules. Conditional access works both with mobile and desktop applications that use modern authentication. We can use Azure AD sign-in pages in applications that use modern authentication. A message is shown if the user's access is blocked. Modern authentication is required for the device to authenticate with Azure AD, so that device-based conditional access policies are evaluated.
By adopting more and more different cloud applications by the organizations, the need for management and controls becomes crucial. In cloud scenarios grant users access to different applications and resources are required. Azure Active Directory in this case offers a wide set of features to support these scenarios. Some of the primary functionalities like account management, Multi-Factor Authentication are common practice nowadays. When it comes to controlling and granting access to applications or managing authorization in a cloud scenario and integrating with our environment, it suddenly starts to be a little bit blurry. Active Directory key Access Control features and it will provide a practice to combine these features which will help IT organizations to manage and service their organization in an efficient and compliant way.

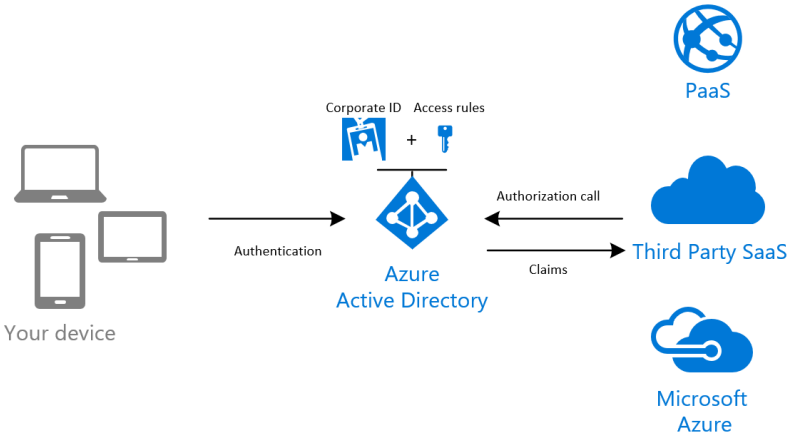

Figure-1 Working of Active Directory Services [24]

Azure Active Directory Conditional Access offers the ability to allow or deny access based on defined conditions. This condition might be based on the source IP address of the user or an Azure Active Directory group. The policy defined in the access rule defines if the user needs to login using an extra authentication factor to prove his identity. This enables one centralized approach by using this access rules for all our enterprise Cloud applications. In addition to the use of Conditional Access, it is considered a common practice to control access to applications using Azure Active Directory groups. The membership of an application group defines if we may access the application [22].

Authorization- an Authorization call is a verification request which is send to the authorization provider at the moment the user tries to access a certain functionality or resource. In Azure Active Directory the Graph API can be used to check the user's membership or role defined.

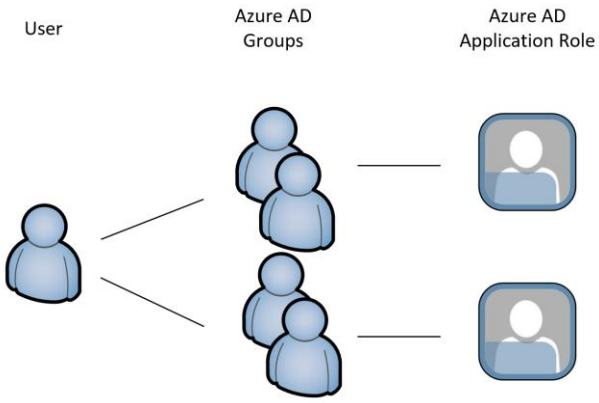

Figure-2- Authorization Model [24]

Azure Active Directory authentication- it Azure Active Directory authentication is a mechanism of connecting to Microsoft Azure SQL Database and SQL Data Warehouse by using identities in Azure Active Directory

(Azure AD) to centrally manage the identities of database users and other Microsoft services in one central location. Benefits include the following:

- It provides an alternative to SQL Server authentication.
- Helps stop the proliferation of user identities across database servers.
- Allows password rotation in a single place
- Customers can manage database permissions using external (AAD) groups.
- It can eliminate storing passwords by enabling integrated Windows authentication and other forms of authentication supported by Azure Active Directory.
- Azure AD authentication uses contained database users to authenticate identities at the database level.
- Azure AD supports token-based authentication for applications connecting to SQL Database.
- Azure AD authentication supports ADFS (domain federation) or native user/password authentication for a local Azure Active Directory without domain synchronization.
- Azure AD supports connections from SQL Server Management Studio that use Active Directory Universal Authentication, which includes Multi-Factor Authentication (MFA). MFA includes strong authentication with a range of easy verification options — phone call, text message, smart cards with pin, or mobile app notification Azure ad creates trust among the users [23].
- Simplify access and control of software as a service (SaaS) applications.
- Reduce the IT burden with self-service identity and access management.
- Improve security posture with cloud services.
- Easily meet reporting requirements.
- Rapidly develop and deploy new enterprise [18]

Administrator structure

When using Azure AD authentication, there are two Administrator accounts for the SQL Database server; the original SQL Server administrator and the Azure AD administrator. Only the administrator based on an Azure AD account can create the first Azure AD contained database user in a user database. The Azure AD administrator login can be an Azure AD user or an Azure AD group. When the administrator is a group account, it can be used by any group member, enabling multiple Azure AD administrators for the SQL Server instance. Using group account as an administrator enhances manageability by allowing us to centrally add and remove group members in Azure AD without changing the users or permissions in SQL Database. Only one Azure AD administrator (a user or group) can be configured at any time.

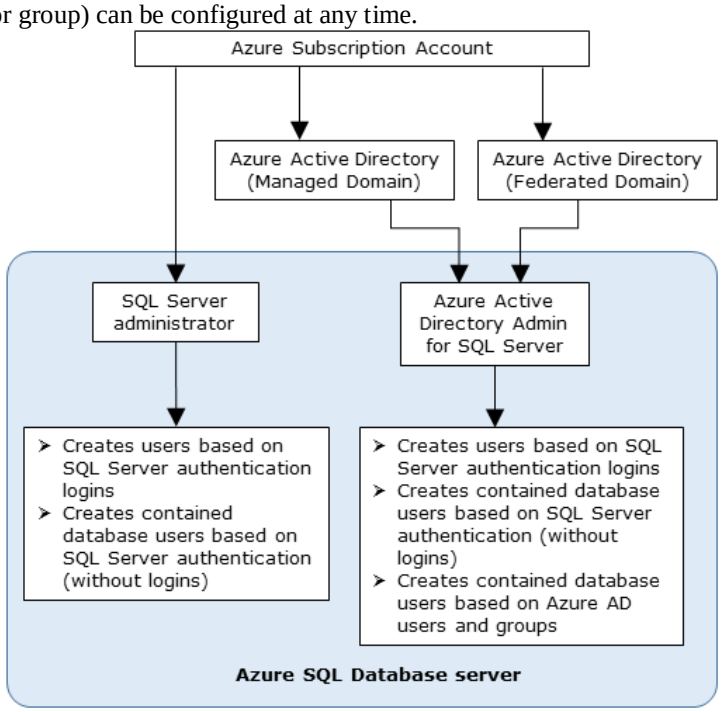

Figure-3 Azure SQL Database Server [21]

Azure Active Directory Identity Protection is a feature of the Azure AD Premium P2 edition that enables us to:

- Detect potential vulnerabilities affecting the organization's identities

- Configure automated responses to detected suspicious actions that are related to an organization's identities
- Investigate suspicious incidents and take appropriate action to resolve them

The vast majority of security breaches take place when attackers gain access to an environment by stealing a user's identity. Over the years, attackers have become increasingly effective in leveraging third party breaches and using sophisticated phishing attacks. As soon as an attacker gains access to even low privileged user accounts, it is relatively easy for them to gain access to important company resources through lateral movement. As a consequence of this, we need to:

- Protect all identities regardless of their privilege level.
- Proactively prevent compromised identities from being abused.

Azure Active Directory Identity Protection is more than a monitoring and reporting tool. To protect our organization's identities, we can configure risk-based policies that automatically respond to detected issues when a specified risk level has been reached.

Advantages of active directory services

Azure Active Directory is a cloud-based directory and identity management service that offers a more streamlined set of services than Windows Server Active Directory. Azure AD offers a convenient and cost-effective way to get many of Windows Server AD's most important features without having to invest in a complete AD cloud infrastructure. Through identification Azure AD improves security ensuring only authorized users access the IT environment:

1. Cloud Credentials and Single Sign-On

Windows Server Active Directory provides true single sign-on capability. For using it we need to set up active directory and connect it to Azure AD using Active Directory Federation Services (ADFS). Federated identities are compatible with multifactor authentication, and their password hashes are never synchronized to the cloud. ADFS allows users to be blocked instantly, and the log-on restrictions from Windows Server AD are also applied when accessing cloud services. Create and manage a single identity for each user across entire enterprise, keeping users, groups, and devices in sync with Azure Active Directory Connect. Provide single sign-on access to all applications including thousands of pre-integrated SaaS apps or provide secure remote access to on-premises SaaS applications using the Azure AD Application Proxy. [18, 21]

2. Secure Access to Cloud Apps-Developers can utilize Azure AD for their cloud apps, eliminating the need to implement a database of usernames and passwords. This not only reduces the cost of deploying apps but also allows organizations to leverage a proven security solution.[21]

3. Microsoft Passport

Passwords have long been considered to be insecure, as they can easily be compromised using social engineering and can be replayed or exposed if a server is hacked. Instead of issuing user names and passwords, Microsoft Passport allows Windows 10 users to authenticate using a gesture. The Windows 10 device needs to be enrolled with Azure AD; to unlock the device, the user needs to input a PIN or provide biometric authentication in the form of Windows Hello. A Windows 10 mobile device can be used as a second factor when logging into a PC, potentially making this implementation of two-factor authentication cheaper than other solutions. [17, 21]

Conclusion

Although cloud computing is very economical, flexible and dynamic; but before adapting it we should be aware of its security issues. In all the security issues Identity and access control plays major role. This mechanism is well implemented in window azure using azure directory services. These services can easily be incorporated with traditional active directory of the organization and provides a robust security structure for it.

References

[1] Rajkumar Buyya, Chee Shin Yeo, and Srikumar Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities, " The 10th IEEE International Conference on High Performance Computing and Communications, 2008.

[2]Harold C. Lim, Shivnath Babu, Jeffrey S. Chase, Sujay S. Parekh , "Automated Control in Cloud computing: Challenges and Opportunities", in proceeding of ACDC'09, June 19, Barcelona, Spain, pp. 13-18, 2009.

[3] Chris A. Mattmann, Nenad Medvidovic,, T. S. Mohan, Owen O Malley, "Workshop on Software Engineering for Cloud Computing", ICSE'11, May 21–28, Waikiki, Honolulu, HI, pp. 1196-1197, 2011.

[4] D. Chappell,(2008) "Introducing the Azure Services Platform - an early look at Windows Azure, .NET services, SQL services and Live services", October 2008.

http://download.microsoft.com/download/e/4/3/e43bb484-3b52-4fa8-a9f9ec60a32954bc/ Azure_Services_Platform.pdf, 2008.
[5] http://www.nsa.gov/research/_files/publications/cloud_computing_overview.pdf20
[6] P. P. Khairnar and P. V. S. Ubale, "Cloud Computing Security Issues And Challenges," vol. 2, no. 2, pp. 1–13, 2013.
[7] Hassan, Qusay (2011). "Demystifying Cloud Computing" (PDF). The Journal of Defense Software Engineering. CrossTalk. **2011** (Jan/Feb): 16–21. Retrieved 11 December 2014.
[8]Peter Mell and Timothy Grance (September 2011). The NIST Definition of Cloud Computing (Technical report). National Institute of Standards and Technology: U.S. Department of Commerce. doi:10.6028/NIST.SP.800-145. Special publication 800-145.
[9] Xue Jing 1 Zhang Jian-jun2 "A Brief Survey on the Security Model of Cloud Computing" 2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science
[10]Wayne Jansen and Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", National Institute of Standards and Technology Draft Special Publication 800-144, January 2011.
[11] Krešimir Popović and Željko Hocenski, "Cloud computing security issues and challenges", IEEE, MIPRO 2010, May 24- 28, 2010, Opatija, Croatia.
[12] Sameera Abdulrahman Almulla and Chan Yeob Yeun, "Cloud Computing Security Management", Engineering Systems Management and Its Applications (ICESMA), 2010 Second International Conference on Issue Date: March 30 2010- April 1 2010 , pp 1 - 7, Sharjah, pp.2-5.
[13] Abdul Raouf Khan, "Access Control in Cloud Computing Environment", Asian Research Publishing Network (ARPN), Journal of Engineering and Applied Sciences, ISSN 1819-6608, VOL. 7, NO. 5, pp. 613-615, MAY 2012.
[14] V.KRISHNA REDDY and Dr.L.S.S.REDDY, "Security Architecture of Cloud Computing", V.Krishna Reddy et al. /International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 9 September 2011, pp.7151-7152.
[15] http://msdn.microsoft.com/library/hh147631.aspx.
[16]http://www.windowsazure.com/en-us/documentation/articles/active-directory-dotnet-how-to-use-access-control/
[17] https://blog.netwrix.com/2016/07/28/three-ways-azure-active-directory-improves-security/
[18]Microsoft "Azure Active Directory Solutions for Identity and Access Management," no. February, 2015.
[19] V. Sravan and K. Maddineni, "Security Techniques for Protecting Data in Cloud Computing," thesis November, 2011.
[20] R. Charanya, M.Aramudhan "Survey on Access Control Issues in Cloud Computing," 2016 @IEEE.
[21] https://blog.netwrix.com/2016/07/28/three-ways-azure-active-directory-improves-security
[22] https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-azure-portal
[23] https://docs.microsoft.com/en-us/azure/active-directory/active-directory-administer
[24] https://azure.microsoft.com/en-in/services/active-directory