AZURE ACTIVE DIRECTORY

1.0 Abstract

[a] [1] Organizations nowadays need scalability and control over user accounts that show a necessity of friendly and easy manageable Active Directory which is indeed provided by Microsoft Azure active directory. [b] [2] Organization are using Microsoft trusted windows AD that is not cloud-based service and in turn hard to manage, less secure, increases the workload of admin and scalability, and implementation of user accounts is hard. Azure Active Directory an another Microsoft trusted cloud-based AD overcomes all the problems faced in Windows AD (On-premise AD). The ON-premise AD has to be replaced by cloud-based AD and Azure AD is better than other cloud-based AD services in the market because of its reliability, market value, and efficiency. [c] With Azure AD Premium P1 subscription an organization account management is just a click away with less management and more security. [d] Since this is a cloud service, all management of database and security is managed by Microsoft itself, and no excessive management is required by organizations taking these subscriptions. [e]Overall, the Microsoft backed-up cloud-based service that gives easily manageable and secured features in terms of user account management is Azure Active directory.

[f] Keywords-Azure, Active directory, identity, and access management, cloud, On-premise AD, Premium P1, Microsoft

2.0 Executive Summary

[g] [3] Azure AD is an identity and access management cloud service which allows users to access multiple Microsoft cloud apps and other on-premise services using single-sign-on. [h]The service overcomes problems faced in using Windows AD(On-premise AD) like managing multiple credentials, burdening IT admin with loads of work, chances of the account getting compromised, and facing problems by admin in implementing other OS based accounts such as Linux or macOS. Also, Azure AD is better than other cloud-based AD services in the market because of its reliability, market value, and efficiency. [I] [L] The service is Cost-efficient and easily manageable as compared to the currently used Windows AD service. Maintaining Windows AD service includes resources that increase costs. Firstly, hardware managing and software licensing cost as AD is stored in a web server whose OS needs licensing. Secondly, IT technicians needed to install, configure, and maintain services in AD servers regularly. Thirdly, for Linux and macOS users additional add-on services are required. However, Azure AD is backed by Microsoft with 99.9% SLA in reliability and availability. For scalability, no installation and management are needed instead expansion of services is a click away. The subscription cost of Premium P1 service with all the services explained above is $6 user/ month also first 50,000 user activation is free and the organization will be charged for the account that is used. [J]The subscription of the service will enhance the organization in security, management, and

saving costs. [K]Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service which helps employees sign in and access external and internal resources, such as Microsoft 365, the Azure portal, other SaaS applications, and cloud and on-premise apps develop by organizations all through single sign-on. [M] Azure AD provides more security, easy management and single sign-on service with a lesser amount and the subscription to Premium P1 will give an organization a robust infrastructure.

3.0 Product Description

[4] The service is Azure Active directory which allows users to access multiple Microsoft cloud apps and other on-premise services using single-sign-on. The service allows organization to access thousands of Software as a Service (SaaS) first and third party applications using SSO. The application involves Office365 apps, ServiceNow, Concur, Salesforce and more. Microsoft's on-premise AD or windows AD has been in the market for so long and required add on 'Active Directory Domain Service (ADDS)' for authentication and authorization of account. With Azure AD in market, organizations tend towards this because of reduced cloud computing cost and cloud based authentication and authorization. Azure AD is "Identity and access management service" which is better than currently used windows AD in providing additional services, security, unburdening workload, user-friendliness, cost-effectiveness, and management. Azure AS provides more than 2000 already integrated SaaS application services from on-site or remote that will be accessed using single sign-on. The service saves time and resources with self-managing options and will be the first step in moving the organization towards the cloud.

[5] The steps involved to implement Azure AD. Step one includes building a foundation of security. Baseline of security features before importing or creating a normal user account ease the process. For example, deciding whether conditional access should be given to all and what access rights should be given to whom. The foundation step enables security from start and users will be introduced to new concepts only once. After initial baseline step two includes implementation of users, managing and synchronizing devices. Planning of guest accesses, synchronization of on-premise user account to cloud and enabling additional functionalities involved here. Step three involves managing applications for use. Amongst 2000+ SaaS application an organization can involve one or multiple according to the infrastructure using single sign-on. Last and fourth step involves managing user lifecycle and auditing privilege identities. When the account password should expire and require resetting and whom should have admin rights are decided here. The implementation steps are the key things to make full use of Azure AD.

The service gives additional options to organizations who want their infrastructure as hybrid. Hybrid infrastructure involves some services on-premised and some services on cloud. Most of the organization does not prefer moving their whole infrastructure towards cloud. In case of AD services there are organization that are using windows AD but synching it with Azure AD to have all privileges. The service provides additional tool as 'Azure AD connect' through which on-premise AD are synched to Azure AD. With this additional tool, separate user creation on Azure AD is not required. For example, an application 'A' is kept on-premise as organization wants to manage it locally but another application ‘B’ is implemented on cloud, now with AD connect synchronization of account can be done so a user who want to use both the application will use it using single sign-on and eventually a single account. Azure AD provide additional tool for synchronizing applications and supporting hybrid infrastructures.

[6] Because of Covid-19 situations, nearly 80% of the staff is working remotely this increases account compromising risk. Azure AD service protects accounts enabling policies like conditional access and MFA (multi-factor authentication). The conditional policy restricts access at the country or regional level also it enables analysts to govern any inappropriate login through behavior analysis. For instance, a user ‘A’ login usually login from a certain region remotely and suddenly one day a login from other region or country is observed, this will alarm the analysts indicating possibility of account being compromised. Further, MFA adds robust security by adding another factor of authentication, like one time passwords. Only password used for login is obsolete and less secure method as through scripts passwords can be predicted. With MFA, security is enhanced. The service gives features like MFA and conditional access enhancing security and avoiding compromising of accounts.

Enhance user experience and unburden workloads of IT admin. The self-service password reset (SSPR) option will allow users to change their passwords. With giving privilege to users of not memorizing multiple passwords for the various app, Azure AD provides a single sign-on (SSO) capability through which users can access multiple apps remembering single credentials. Additionally, users get optional rights where they can unlock their accounts that got locked due to expiration or failure logins. Also IT admin usually invest their time troubleshooting account related issues. The availability of these privileges will reduce the workload of IT admin who is generally managing account related issues also the productivity can be increased. So, this service provides capabilities that will save the time of the employee's increasing productivity.

Windows AD has certain limitations that are overcome by Azure AD. Firstly, Windows AD involves servers where account information is stored and management is done by organization itself while in Azure AD management is done by Microsoft. Secondly, with windows AD there are multiple credentials for the same user for multiple services as the organization is hybrid, means some applications/servers are on the cloud and some are on-premises. Azure AD service allows synching of on-premise windows AD or servers to the cloud and single-sign-on can be used to access every node. Thirdly, windows AD natively does not support accounts related to Linux machines or Linux based applications. Azure-based active directory supports macOS and Linux based accounts too. So, from providing cloud service and on-premise access through SSO to support different OS accounts Azure AD overcomes the default windows AD.

[7] The service is Cost-efficient and easily manageable as compared to the Windows AD service. Maintaining Windows AD service includes resources that increase costs. Firstly, the hardware managing and software licensing cost as AD is stored in a web server whose OS needs licensing. IT technicians needed to install, configure, and maintain services in AD servers regularly. Thirdly, for Linux and macOS additional add-on services are required. However, Azure AD is backed by Microsoft with 99.9% SLA in reliability and availability. For scalability, no installation

and management are needed instead expansion of services is just a click away. The subscription cost of Premium P1 service with all the services explained above is $6 user/ month also first 50,000 user activation is free and the organization will be charged for the account that is used. So, in terms of management and cost efficiency, Azure AD provides more services with a lesser amount.

4.0 Market Research and Analysis

[8] The Azure AD service has a high market share of 6.28% that is better than any AD service provided by the companies apart from Microsoft. Other AD's like Cisco Identity Services Engine, Okta, Amazon AWS Identity and Access Management (IAM), and Centrify all have a market share of about 5% or less. The service is widely accepted and most user friendly service in the market. Many Gulf based organizations choose this service for cloud based security. The market share signifies the value of the product, Azure AD an Identity and access management service of Microsoft tops the list.

[9] The service is widely accepted and the most used service in US and software industries. First, computer software industries utilize this service to the highest by 26% with 1334 companies followed by IT service industries to 10% with 499 companies and lastly Health care industries to 5% with 262 companies worldwide. Second, US are the top customer using Azure AD followed by UK and Canada. Third, companies with varying strength use this service. 19 % of small companies with less than 50 employees to 36% of large size industries of employee's strength greater than 1000 use this service. Azure AD is a widely known and used service all over US and software companies.

[10] Microsoft Azure AD successful customer story signifies its promising service with reliability. Nuffield Health is a UK based health care organization that relies on Microsoft service because of cost-effectiveness, easy management, and trust. In 2016 while crossing million members the company acquire Azure AD and provides an online portal with SSO that consolidates all services. With a unified system giving the customer access to view their health care records and data to their gym membership plans. The company claims with this service they give their user a good experience with high reliability and security. The Nullified Health Company has now made their management easy as no person has to call for appointments, inquiry, or other stuff as their online portal with Azure AD support provides a robust user experience.

[11] Microsoft Azure AD supports more languages and features than the OKTA identity cloud. Both are cloud service and supports single sign ON however Azure AD gives important feature like Self-service password management where users can manage problem-related to their credentials. Also, security and usage reports are given by Azure AD which identifies user account security and usage logs. These features are not supported in the OKTA identity cloud. Additionally, Okta identity supports English and French whereas Azure AD supports every well known and highly used language apart from Hindi. Azure AD has more features and supports more languages as compared to the OKTA identity cloud and strives for big business in return.

[12] Azure AD is offered by Microsoft Azure cloud services whereas AWS IAM is offered by Amazon. Azure AD is better in rating, unique categories and service cost as compared to AWS IAM. Azure AD service is better in ratings in terms of use, easy setup and ease for admin with high responses online. AWS IAM does not provide unique categories while Azure AD provides User provisioning and governance tools, AD connect, SSPR Self service password reset) and more. Also 46.6% of the enterprise with greater than 1000 employee use Azure AD while only 43.1 percent use AWS IAM service. For cloud service cost, Azure is cheaper than AWS. For example, the storage parameter in azure for 50TB frequent access is $0.208 per GB whereas AWS is $0.230 per GB. So, Azure services are usually cheaper than those of AWS cloud services.

5.0 Finance and Economics

Financial investment requires an initial cost of subscription and new employees with Azure AD knowledge or existing employee's training in the field. The subscription cost depends on the number of users in an organization. For the initial 1000 employees, $6000 needs to be paid if all accounts are used, there will be no activation charge for an account as 50000 account activation is free in Premium P1. Firstly, for the transition of accounts to Azure AD from windows AD new employees or existing trained employees are needed to make accounts and provide accesses. The best approach is to train existing IT admin as they are already aware of account policy and the related accesses it holds; the course that includes Azure AD implementation in-depth and introduces other services of Azure too is "Microsoft AZ 500" with $117.16 per user but after 95% discount ongoing it is $6.17. So, the initial subscription and training cost is the only financial aspects needed to implement this service.

6.0 Management Team

Azure AD implementation needs the involvement of management team with at least 10 people and the contribution of the IT admin team. For organizations with 1000 employees at least 10 trained members with knowledge on AZURE AD implementation and IT team collaboration eases the transition. First, an account needs to be made at Azure AD. Second, access and rights to that account need to be given by trained members. Third, account activity needs to be checked and ensure if every access is working fine. Fourth, an old account from windows AD needs to be revoked by the IT admin. Also, all users who have an account on Azure AD need to be trained by the management team on how to enable MFA and use self password recovery and unlocking services. The time duration to implementation and synchronization require 30 to 90 days. So, a trained management team and IT admin work for particular time duration is required in a process to implement accounts.

7.0 Risks and Assumptions

[13] Some businesses using Azure AD face speed issues. Microsoft Azure has 54 regions over the globe which offers availability to 140 countries for announced regions. Availability regions

provide easy data access. Countries like Europe, Australia, India, Japan, China, and United states have multiple available regions and data access is speedy. But in South America single available region as "Brazil South" has two announced regions which are inactive for now. Also Canada has two regions and both are located at eastern region of the country. No availability of nearly regions or inactive regions causes speed issues to organizations in that region or has network in that region. With regions scarcity in some areas or long available region distance, speed issue triggers.

Require platform expertise that is hard to achieve. Azure AD implementation involves proper planning by someone who is aware of the service and the infrastructure of the organization. Getting a team on this is challenging for organizations as a result bad planning creates loopholes. For example the four steps involved in implementation as discussed above should be followed and baseline should be created. Improper privilege access or bad policies while implementation makes accounts and infrastructure less secure. So, better planning in implementing Azure AD is hard as platform expertise is challenging.

8.0 Conclusions

The organizations often consider moving their infrastructure to the cloud to have better security and easy management. Azure AD with additional services like security, unburdening workload, user-friendliness, cost-effectiveness, and management also support user account shifting to cloud infrastructure. The service is backed up by Microsoft and termed as the most reliable and secured service of Active directory. The service is replacing the traditional ON-premise windows AD. Also, this cloud service competes with other AD cloud services in the market in terms of cost and security. With the emerging need for robust infrastructure by organizations, Azure AD gives features that fulfill every requirement.

Bibliography:

[1] Kelley, Diana**. “**Bolster Security to Enable Collaboration and Customer.**”** *Microsoft.* Published May 11, 2020. Accessed October 01, 2020. Available*:* https://news.microsoft.com/en-ph/2020/05/11/bolster-security-to-enable-collaboration-and-customer-engagement/

[2] Trivedi, Kunal. "Active Directory Vs Azure Active Directory." *C#Corner*. Published July 01, 2007. Accessed September 25, 2020. Available:https://www.c-sharpcorner.com/article/active-directory-vs-azure-active-directory/

[3] Microsoft Azure. "Azure Active Directory." *Microsoft Azure*. Accessed September 10, 2020. Available: https://azure.microsoft.com/en-ca/services/active-directory/

[4] Oxford Computer Training. “What ia Azure AD?” *Oxford Computer Training*. Accessed September 25, 2020. Available:https://oxfordcomputertraining.com/glossary/what-is-azure-ad/#:~:text=Azure AD (Active Directory) is Microsoft’s multi-tenant, cloud-based,like Office 365, Salesforce.com, ServiceNow, Concur and others.

[5] Microsoft. “Azure Active Directory feature deployment guide.” *Microsoft.* Published July 20, 2020. Accessed September 25, 2020. Available: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-deployment-checklist-p2

[6] Microsoft. "Using the location condition in a Conditional Access policy." *Microsoft*. Published June, 6 2020. Accessed September 5, 2020. Available: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

[7] Microsoft Azure. “Azure Active Directory pricing.” *Microsoft Azure*. Accessed September 20, 2020. Available: https://azure.microsoft.com/en-us/pricing/details/active-directory/

[8] Enlyft. “Companies using Microsoft Azure Active Directory.*”* *Enlyft*. Accessed September 23, 2020. Available: https://enlyft.com/tech/products/microsoft-azure-active-directory

[9] Enlyft. “Identity & Access Management products.” *Enlyft*. Accessed September 23, 2020. Available: https://enlyft.com/tech/identity-access-management

[10] Microsoft. “With Azure AD B2C, top UK healthcare provider now offers a secure web portal as user-friendly as its facilities.” *Customer Stories*. Accessed September 29, 2020. Available: https://customers.microsoft.com/en-us/story/nuffield-health-with-azure-ad-b2c

[11] Finance Online. “Compare Microsoft Azure Active Directory vs Okta Identity Cloud.” *Finance online*. Accessed September 23, 2020. Available:https://comparisons.financesonline.com/microsoft-azure-active-directory-vs-okta-identity-cloud

[12] Perry, Yifat. “Azure vs AWS Pricing: Comparing Apples to Apples.” *NetApp*. Published September 10, 2020. Accessed September 23, 2020. Available: https://cloud.netapp.com/blog/azure-vs-aws-pricing-comparing-apples-to-apples-azure-aws-cvo-blg

[13] Brandongaille. "15 Microsoft Azure Advantages and Disadvantages" *Brandongaille Small business & marketing advice*. Accessed October 03, 2020. Available: https://brandongaille.com/15-microsoft-azure-advantages-and-disadvantages/