Secure identities using Azure active directory

Azure active directory

* Cloud based identity and access management solution
* Helps secure internal, external, and customer identities
* Access external services like office 365
* Access internal services like on premises apps in your workplace. Cloud based apps that your company has built
* Helps keep user identities secure with its variety of it provides

Identity score

* The value in which how effective your security is. Values from 1-233

Azure AD vs Active Directory

* Shares same name but have different capabilities
* Azure AD is a cloud based identity solution whereas active directory manages objects, like devices and users on premises networks.

|  |  |
| --- | --- |
| Azure AD | Active Directory |
| Used for tenants and allowing access to internet services like Azure and Microsoft 365 | Used on premises to allow access to devices such as printers, applications, and file services |

* They can be used both together to form a hybrid active directory. A single identity is used for authentication and to access resources and apps wherever they are. This is called a **hybrid identity**.

Authentication methods

|  |  |
| --- | --- |
| Azure AD and hash sync | Users password is hashed twice for access to both active directories. Same credentials can be used to access both. |
| Passthrough | Agent is installed for on on-premises servers. When azure ad tries to authenticate it is handled on on-premises servers |
| Federated | A more advanced method that uses features like a smart card for access. This uses a AD FS, active directory federated services |

European identity storage

* When subscribed to a service like Azure the storage by default is stored based on the location of the address.
* When in Europe data is stored there. However, if outside some data is stored in Europe by services used with Azure AD.

Sample Questions

What is a tenant in Azure AD? A tenant represents an entire organization.

**Understand Azure AD licenses and terminology**

Azure AD licenses

|  |  |
| --- | --- |
| Active directory fee | Manage users and reports, and you get necessary reports. Single sign on |
| Pay as you go | Lets you manage services as you go for consumers and the apps they use. |
| Office 365 apps | Free tier features with custom login and logout pages. Password reset for cloud users |
| Directory premium p1 | Most features |
| Active directory premium 2 p2 | All features of previous tiers plus identity protection |

Terms

|  |  |
| --- | --- |
| Identity | Has to identified and authenticated. Usually a user and password. |
| Account | Associated with data. Cannot exist without identity |
| Azure ad accountant | Identity created in Azure AD. Used for office 365 and its services |
| Azure subscription | Level of access to use services in azure. Each levels offers different restrictions and services |
| Multi-tenant | Allows multiple tenant access to same apps in a share environment |
| Custom domain | Domain you customized in azure. |
| Owner role | Role used to manage all resources in a group |
| Global admin | Full admin access capabilities |

* All users are given default permissions
* Guest users would need to be invited in order to have access. They have limited access compared to normal users

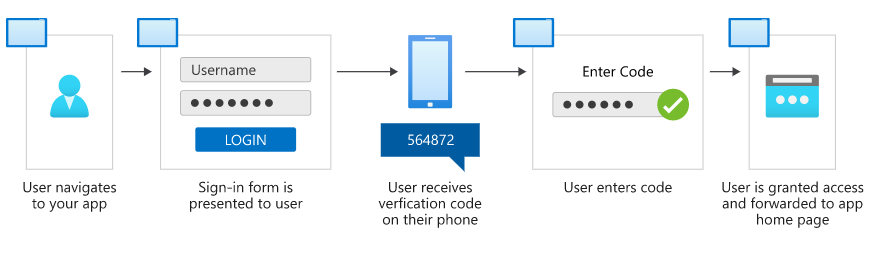
**Essential features of Azure AD**

Azure AD B2B

* Allows you to give users outside your organization guest access.
* Need to invite them, multi factor authentication can be used with invitation for a more secure authentication
* Feature is available in all tier subscriptions

Azure AD B2C

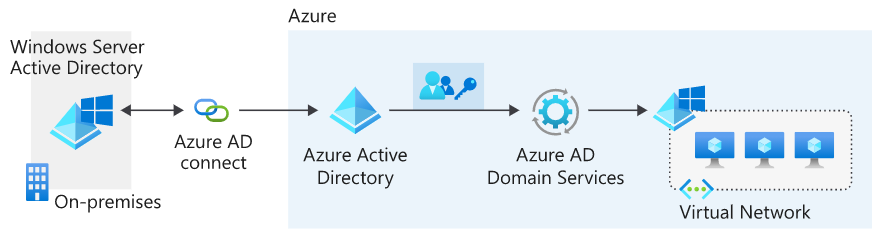
* Allows to manage custom user identities and access



* Pay as you go feature

Azure AD DS

* Can add virtual machines without need of domain controllers
* Internal members can access using azure credentials



**App management**

Azure AD app gallery

* Thousands of saas apps are found on the azure AD marketplace

Custom applications

* Company built in apps can be added and registered. You can control and monitor these apps as well

Non gallery applications

* Can manually add apps not found in the azure ad marketplace

On premises-apps

* Can be added by configuring the az add app proxy.

Conditional access policies

* These types of policies allow you to make sure users pass certain authentication challenges before use of apps is allowed. Like multi factor authentication. Offered in P1 and P2 tiers

Monitor app access

* Allows you to keep track of sign ins, access times, user details etc..

Identity protection

* Helps automatically detect, investigate, and remediate identity risks for users.
* Allows you to export information collected and send to a third-party tool to analyse info and solutions for it
* Example is an admin using identity protection to detect user risks and solves this by requiring the user to change the password upon receiving notification.
* Only offered in P2 tier

**Get started with Azure AD**

* In a scenario when deploying Azure active directory, it is done is phases
* Each stage covers a key aspect in deployment

Step 1 – build a secure foundation

* Add more than one global admin
* Monitor how admin roles are used
* Configure self-service password reset
* Create list of banned passwords
* Warn reuse of credentials
* Set time expiry for passwords
* Enforce multi factor authentication

Step 2 – add users, manage devices, and config sync

* Install and configure az add connect
* Use hash password sync
* Give user licenses at necessary levels
* Used azure ad b2b for external guest access

Step 3 – manage your applications

* Identity apps, see what apps are going to be used on premises and those you want to manage in Azure AD
* Allow azure ad users to sign in to on-premises account using azure ad account

Step 4 – monitor you admins, access reviews, and automate life cycles

* Allow only admin access after passing some identity challenges
* Save time by adding those with familiar information. Like all users who are from human resources department to a group called human resources
* User group-based access allows users in groups access to apps. Dynamic groups have users who are removed lose access

Finally create a tenant

1. Got to azure portal > create a resource
2. New > Home > azure active directory > create a directory, then complete forms
3. Then associate a subscription
4. Home > subscription > your subscription > change directory