Azure\_AD Blade consists of   
Users, groups, external identities,roles and administrator,administartive unit,Enerprize applications, devices, app registrartions, identity governance

**Custom domain name** : we need to add the MX or txt record and we need to add in the domain hosting site by entering the TXT records and need to verify in the azure.

AZureAD>> Custom Domain Name>>add new >>example.com>>add domain and need to verify.

Each Azure Ad Tenents are isolated to each other. Tenets are of 2 types Azure\_Ad & Azure\_Ad B2C.  
Azure AD Tenent/Directory : if user authenticate inside my org  
Azure AD B2C : if user authenticate outside my org

AzureAD>Manage tenet> New Tenent> Ad or B2c> details>captch> create.  
Switching tenets: Azure AD > manage tenets>select Switch tenet.

**Azure\_AD Licensing** :They are of three types  
 Azure Ad Free : user & group management, sync with on-prem, basic reports,SSO azure, password reset for cloud user only

Azure Ad Premium1 : Hybrid user & group Management(dynamic, password reset for on-prem users

Azure Ad Premium2 : AzureAD identity protection which has conditional access, PIM which is used to proved access for Just in time access.

**Azure\_AD users:** we can create their in the console and we can create guest users using invite of different email id.( can be used for the authentication & authorization)  
Bulk user creation and deletion (guest users as well)

**Azure\_Ad Groups:** 2 Types

Security Groups- : to give permissions / roles  
Microsoft 365 groups: Emails DL( collabaration)

Types: Assignment (manul), Dynamic groups/dynamic membership rules (query based)

Expiration: we can set the group deletion expiry by 365, and custom as well which allows to send the email notifications as well.

Naming Policy : Bolocked words (where we can add few words to block) it primarily add prefix & Add suffix its only applicable for the microsoft 365 groups not for security groups.

Deleted groups: which allows to soft delete for 30 days

**AD\_Registered Devices:** Directly registering to Azure\_AD without requiring org account to sign in to device.

**AD\_Joined Devices** : Ad joined devices are signed into using an org azure Ad account.  
Admins can secure and control azureAd joined devices using intune/Microsoft endpoint config manager  
(storage encrypted, password complexity, software installation, software updates)

**Azure\_AD Hybrid Joined Devices:** Org with existing on-prem Ad and require org account to sign-in. Hybrid azureAd joined devices require network line of sight to your on-premises domain controller periodically without this connection device becoming unusable.

SSO capability to both cloud and on-premises resources & conditional access through domain join and through intune.

Default value: Maximum no.of devices per user 50

AD register : Login to Vm>>settings>>account>>enter the email of example.com domain credentials to register the device.   
To view: Azure portal>> azureAD> devices>> all devices>> you can see the **device registered**

AD Joined: Login to vm >> settings>>account>>connect>>join AzureAD>> pass the credentials>> Note:GPO alsoapplied

Then the status can be changed from **register to joined**

**ROLES**

* Global Admin: Full access in Azure AD
* Security Admin : Have the permissions to manage security-related features in Microsoft 365 security center, Security center, Azure AD Identity protection, Azure information protection & O365 security & compliance center.
* Billing Admin: Make purchases, manage Subscription, manage support ticket & monitor service health.
* Global Reader: Having only full read access on mircosoft 365 services.
* User Admin : Where we can create, reset password and delete user  
  We can add custom roles and assign the built in roles to the users.

**Buit-in roles for Azure Resource**

* Owner: Allows you to manage everything including **access to resources**.
* Contributor: Allows you to manage everything **except managing access to resources.**
* Reader: Allows you to view everything but not to make any changes.
* User Access Admin: Allows you to manage user access to azure resources.  
    
  **Hierarchy:**  
  Management group  
  Subscription  
  Resource Group  
  Resource
* Administrative units: AzureAd> Administrative unit>>Add>>Name>>Assign roles>>

**MFA**:  
Disabled: disabled which means no MFA  
Enabled: It allows us to register for the MFA

Enforced:once it register for the first time it automatically moves to enforced state  
Maximum account is automatically locked out in minutes : 9999

Block and unblock user : where we can add users manually

Defult re-register MFA is : 180 days  
  
**Enable security defaults**: Azure\_AD >> properties>>manage security defaults >> Enable security defaults  
OpenATH : Software (authenticator app) & hardware (RSA tokens)  
**OATH**-Tokens:Open Authentications>> software (authenticator app) & hardware >> OATH-SHA-1 hardware key chain tokens which refresh 30-60 sec.  
 **PIM**

Default time bound access is 8hrs and we can increase it upto max of 24hrs

Approval Based activation of privileged access.

MFA to activation of the roles

**Zero Trust Model**: it assumes the breach and verify each request as through it originates from an open N/W.

Similar to the MFA was introduced but it chceks( location,device state,app,risk,exceptions) then only allows or deny the request

**AzureIdentityProtectionRisk**: Each detected suspicious action is stored in a record called a **risk event.**  
Leaked credentials (LCS where it scans and identify and inform us to change the passcode)  
Sign in from anonymous Ip  
Impossible to travel to typical location  
Sign in from infected devices & unfamiliar locations  
**Userriskpolicy:** Based on the risk level either to allow or to block or to reset the password.

**Sign-in-Riskpolicy**:Based on the risk level either to allow or to block or to use MFA.primary diff between the user sign in and sign in is (specific to the current) applied to all browser traffic

Azure AD>>Security >> identity protection>> user risk/sign in (user,user risk, access)(user,sign in risk, access

**Powershelll Admin Azure\_Ad :**

Set-ExecutionPolicy Remote signed  
install-Module Az & Install-Module AzureAD   
Connect-AzAccount  
Get-Azsubscription  
Get-AzAduser -startswith R

**Privileged Identity Management (PIM)**

* Just-In-Time privileged access to azure
* Time bounded access to resources (default 8hr min 30 max 24hr)
* Approval to activate PIM access
* MFA to activate any role
* Notify when it gets activated.
* Access review to ensure users still need roles.
* Audit history for internal and external audit.
* PIM Workflow : Assign >> activate >> Approve >>Audit

**Conditional Access policy**

Azure AD>>security>>Identity protection>>Conditional access>>policy>New policy: Name,users(guest users as well) cloud apps or actions,condition:( user risk,sign in risk,device platform,location,client apps,filetr for device) grant access or block access>>session

Break Glass account : Prevent being accidental lockout of your azure AD org bcz you cant sign in or activate another users account as an admin.

**Access Reviews:**   
  
These can be seen under identity governance tab>>access review>>new ( teams+ groups, Apps) we need to add the reviewer and the duration >> action need to be taken when reviewer doesnt respond>>create.

**Audit**: ( Security admin or reader ) Aure ad>> monitoring section.

Sign in : provides the logs abt the user sign-in.

Audit: provides the logs abt the any changes which are applied to the tenant.

Provisioning: Provides the logs abt the creation of user or groups imported

**Azure AD Enterprise Apps**

AzureAD>> Enterprise Application>>New application>> search for the application>> Add >> assign user and groups and role to the App>>Single sign on (disabled,SAML,Passwordbased,Linked)>> provisional users>>conditional access policy>>Self service ( user request to access the app)

SAML config:   
AzureAD>> Enterprise App>> New app>search for the app>> add>> assign user and groups and roles to the app>> single sign on SAML>> open the app learn more then in the document and follow the steps we can see the steps written along with the **reply url and sign on url** specified >> open the app url as per the document and need to register the added users to the application inorder to have the SSO (which wont ask credentials to login to that app).

Identity Goverance  
Azure AD>> identity Govenance>>catalog>add>Add resources>> add new access packages( Name,resources,request(with in dir or without)fill the conditions,requester info (question & attributes),lifecycle (duration expiration),custom extension, create.

After creation we can add policy with in it. Once user has request the access using the myaccess.microsoft portal then we can see those request in the request balde of the access package. If it got assigned it will be appear on the assignments.

ADDS : it uses th LDAP and kerbose protocols

AzureADDS : which provides the managed domain services with a subset of the traditional ADDS features like domain joined,group policy,LDAP,kerbose and authentications as well.

AzureAD : doesnt supports kerbose and the GPO (to overcome we used to install AzureADDS)

Creation of AzureADDS

Azureportal>>AzureADDS>>New>>Name,DNS name,SKU,forest,Networking,admin,sync(all,scpoed),security settings,>>create.

Azure AD connect

Primary used for the connecting of the Onprem AD to the Azure AD.

Authentication options: PHS(password Hash sync),PTA (Pass through Authentication)agent requires to sync, ADFS (onprem).

Installation : Azureportal>>azure AD>>AzureAD connect>>download agent>>install it>>use express settings>>pass global admin credentials>>Enter the enterprise admin credentials>>Done.

Azure AD cloud Sync: which is similar to that of the Azure AD connect.

Azure AD>>Azure ad connect >> manage Azure AD cloud sync>>download agent>>installa and login>>create service adim (domain admin cred)>>Done.  
Then it reflects with in the portal>>New cloud sync confirg>> create.

Cloud sync config : scope, manage attributes, validate,settings (notification autodeletion) ,deploy.

Testing : create a user in the AD and then see if it reflects on azure AD. refresh

If it doesnt appear then open the cloud sync config >>restart sync. Then we can see the user in the AzureAD.

Azure service health   
status .azure.com which shows the all staus of the azure components Default is 2mins

Service health where we can create a rule>> health alerts , alert rules