Table of Contents

[ACCESS MANAGEMENT 3](#_Toc159328325)

[MICROSOFT ENTRA 3](#_Toc159328326)

[AZURE ACTIVE DIRECTORY 3](#_Toc159328327)

[ON PREM VERSUS AZURE AD 4](#_Toc159328328)

[AD LICENCE OPTIONS 5](#_Toc159328329)

[AD TERMINOLOGIES 5](#_Toc159328330)

[TRUST BETWEEN SUBSCRIPTION AND AD 5](#_Toc159328331)

[CONFIGURING THE TRUST BETWEEN AD AND SUBSCRIPTION 5](#_Toc159328332)

[CREATING USER IN AD 7](#_Toc159328333)

[TYPES OF ACCESS CONTROL SYSTEMS 10](#_Toc159328334)

[RBAC ROLES (IAM – IDENTITY AND ACCESS MANAGEMENT) 11](#_Toc159328335)

[DIRECTORY ROLES (AD ROLES) 11](#_Toc159328336)

[SCOPE OF RBAC 12](#_Toc159328337)

[TYPES OF RBAC ROLES 12](#_Toc159328338)

[CREATING USER GROUP 18](#_Toc159328339)

[AZURE AD ROLES 19](#_Toc159328340)

[ASSIGNING AD ROLES 19](#_Toc159328341)

[BUILT IN AD ROLES 22](#_Toc159328342)

[JOINING A VM TO AD 22](#_Toc159328343)

[AZURE AD CUSTOM DOMAIN 24](#_Toc159328344)

[STEPS TO ADD CUSTOM DOMAIN 24](#_Toc159328345)

[INVITING GUEST USER 25](#_Toc159328346)

[CREATING GUEST USER 25](#_Toc159328347)

[USER CREATION / DELETION IN BULK 28](#_Toc159328348)

[CONDITIONAL ACCESS POLICY 28](#_Toc159328349)

[SETTING UP CONDITIONAL ACCESS POLICY 28](#_Toc159328350)

[EXAMPLE – CONDITIONAL ACCESS POLICY 29](#_Toc159328351)

[PASSWORDLESS AUTHENTICATION 31](#_Toc159328352)

[PASSWORDLESS AUTHENTICATION OPTIONS 31](#_Toc159328353)

[ADMINISTRATIVE UNITS 32](#_Toc159328354)

[LAB -ADMINISTRATIVE UNITS 33](#_Toc159328355)

[CONCEPT OF ZERO TRUST 37](#_Toc159328356)

[CLASSIC TRUSTED MODEL 37](#_Toc159328357)

[ZERO TRUST MODEL 38](#_Toc159328358)

[MULTIFACTOR AUTENTICATION(MFA) 39](#_Toc159328359)

[ENABLING MFA FOR USER 39](#_Toc159328360)

[HYBRID ENVIRONMENT IDENTITIES 42](#_Toc159328361)

[SETTING ADDS (ACTIVE DIRECTORY) IN ON-PREM WIDDOWS SERVER 42](#_Toc159328362)

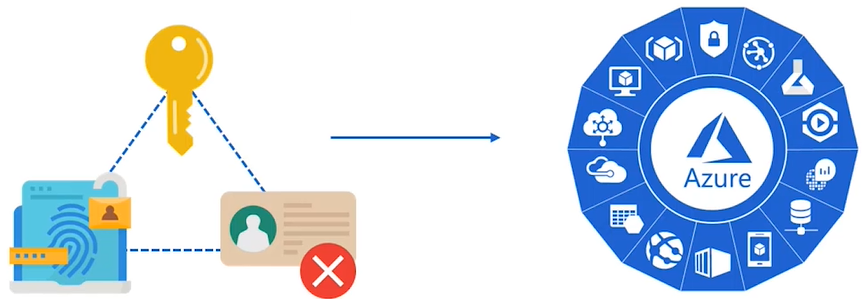
[TENANT 43](#_Toc159328363)

[SYNC USERS FROM ON PREM TO AD 45](#_Toc159328364)

[DEMO 45](#_Toc159328365)

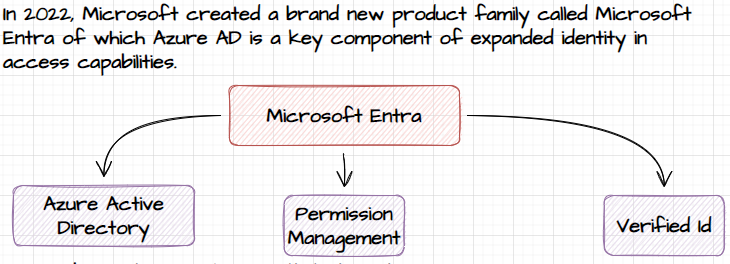
# ACCESS MANAGEMENT

* Access Management in cloud refers to a process that allows, denies, or restrict access to services or resources.
* This also includes, deciding who gets the access and to what extent, in cloud.



* Access Management in Azure can be achieved by RBAC(Role Based Access Control)

# MICROSOFT ENTRA



# AZURE ACTIVE DIRECTORY

* Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service.
* It serves as a comprehensive identity and access management solution for managing user identities and controlling access to resources in the Azure cloud environment and other integrated applications.
* The key benefit of Azure Active Directory is that we don’t need to implement any infrastructure.

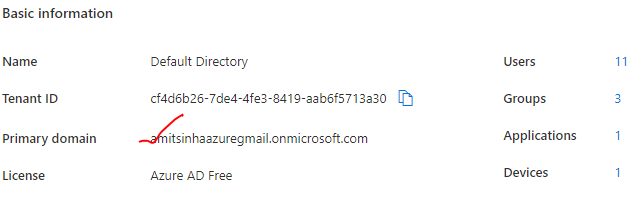
KEY FEATURES AND CAPABILITIES OF AZURE ACTIVE DIRECTORY INCLUDE:

* IDENTITY MANAGEMENT
  + Provides a centralized identity management system to manage user identities and access across various applications and services.
  + It allows administrators to create, manage, and synchronize user accounts, groups, and roles.
* SINGLE SIGN-ON (SSO)
  + Enables users to sign in once with their Azure AD credentials and access multiple applications and services without the need for separate sign-ins.
  + This enhances user experience and simplifies access management for administrators.
* MULTI-FACTOR AUTHENTICATION (MFA)
  + Supports multi-factor authentication, adding an extra layer of security to user sign-ins. (MFA requires users to provide additional verification, such as a code sent to their mobile device, in addition to their password.)
* APPLICATION MANAGEMENT
  + Provides application management capabilities, allowing administrators to register and manage applications in Azure AD.
  + This includes managing access permissions, defining single sign-on configurations, and enforcing security policies.
* ROLE-BASED ACCESS CONTROL (RBAC)
  + RBAC are used for authorization.
  + Allow administrators to assign granular access permissions to users and groups for Azure resources.
  + RBAC enables the principle of least privilege, ensuring users only have access to the resources they need.
* SEAMLESS INTEGRATION
  + Integrates with a wide range of Microsoft and third-party applications, including Office 365, Azure services, and thousands of Software-as-a-Service (SaaS) applications.
  + This enables organizations to centrally manage access to various resources.
* CONDITIONAL ACCESS
  + Conditional Access feature allows administrators to define policies that control access to resources based on specific conditions, such as user location, device compliance, or risk level.
  + This helps enforce security controls and prevent unauthorized access.

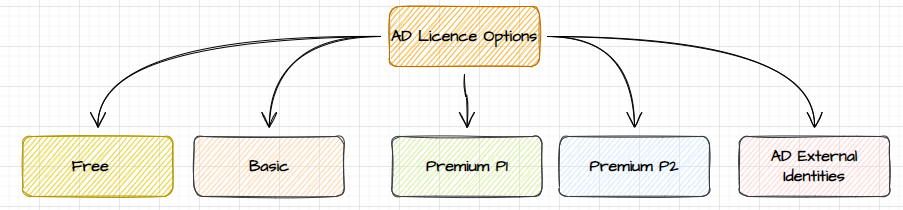
## ON PREM VERSUS AZURE AD

|  |  |
| --- | --- |
| ON PREM WINDOWS ACTIVE DIRECTORY | AZURE AD SERVICE |
| * In the on Prem set up we need to have a dedicated directory server aka Domain Controller. * On these domain controllers we need to enable/ install ADDS (Active Directory Domain Service). * These ADDS services need a domain name. * Now using ADDS - we can able create uses, group and join devices (desktop/ laptops etc.) under the ADDS domain. * The access control on the uses, group and devices are managed by Group Policies. | * In Azure provides a managed service for Active directory – hence we don’t need a dedicated directory server. * When we sign up for Azure, by default a **tenant** is created (tenant is also referred as directory). * *In the on prem side – a dedicated directory servers need to be set up for each organization, On the other hand Azure AD service is a distributed directory service.* * Since it’s a distributed service(global), the organization are uniquely identified by using tenant.   Note:   1. A tenant needs a primary domain name. By default. The tenant can have custom domain name as well. Adding the custom domain needs verification. |

**PRIMARY DOMAIN NAME**



## AD LICENCE OPTIONS



## AD TERMINOLOGIES

|  |  |
| --- | --- |
| TENANT | * A tenant is a unique representation of an organization in Azure Active Directory. * When we create an azure account by default, we get an instance of Azure AD. Every such instance is called tenant. * It a dedicated and trusted instance of Azure AD |
| DEFAULT DIRECTORY | * Each tenant has a dedicated and trusted Azure AD directory. * This includes tenant user, group and used to perform identity and access management of Azure resources. |

* In Azure Portal, apart from default directory we create a new directory as well. Creating a new directory is same as creating a new tenant itself.

WHY AN ORGAINIZATION WILL CREATE NEW DIRECTORY RATHER THAN USING THE DEFAULT DIRECTORY?

***User-case***: Let's say if an organization has many other companies under that organization, so they can create directories for each of the companies in that organization. Hence rather than creating the users under this one directory, we can create uses company’s directory.

## TRUST BETWEEN SUBSCRIPTION AND AD

* The subscription is used for grouping of resources and used for the billing aspect. All the resources are built against a particular subscription.

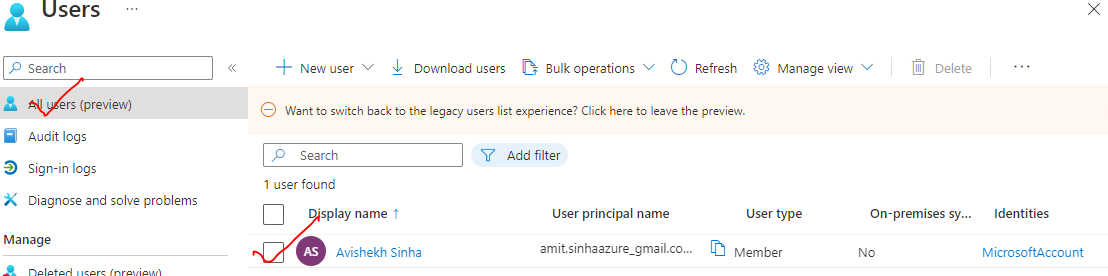
|  |  |
| --- | --- |
|  | * ***At any point in time, one subscription can trust one directory*** - so users are defined in this directory can be given access on resources that are defined in * It means that whatever users are defined in this directory can be given access on to the resources defined in that subscription. * Multiple subscriptions can also trust same active directory |

## CONFIGURING THE TRUST BETWEEN AD AND SUBSCRIPTION

|  |  |  |
| --- | --- | --- |
|  | Step 1: CREATE AN ACTIVE DIRECTORY(TENANT)   * Select Active Directory Service 🡪 Manage Tenant 🡪 Create * Select the Tenant type as “Azure Active Directory”   *Note - So if a company wants to have another directory in place for managing users separately, they can create another as the Active Directory*.   * Once a new directory is created then we can go ahead and create user into the AD. * We can also change the directory for a subscription * The users in the AD will get an access to the resources created in that subscription | |
|  | To change the directory for a subscription   1. Go to Subscription🡪 Change Directory 🡪 Select the directory | |
|  | | |
| DELETING A AD(TENANT) – Go to Active Directory 🡪 Manage Tenant 🡪 Select the tenant 🡪 Delete | | |
|  | |  |

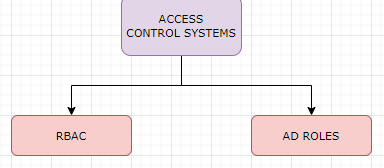
## CREATING USER IN AD

* When a user is created in azure- user can able to login to azure .
* While creating a user – user can be assigned with directory permission (shown below)
* Now when newly created user logs in - by default he will not have permission to view anything. **To give the access to the resources , resource group or subscription – We have to make use of RBAC permissions.**



|  |  |  |
| --- | --- | --- |
|  | | 1. To Create User🡪 New user 🡪 Create 2. The default domain is “*onmicrosoft.com*” 3. **The newly created user can login to Azure Portal, but by default it will have no access to any resource** 4. Access can be given to the user must be given explicit using RBAC |
|  | | **ASSIGNING DIRECTORY ROLES**   * Note – while creating the user – directory roles can be assigned to the user. * These roles will enable user to control active directory. |
|  | | |
|  | **ASSIGNING DIRECTORY ROLE**   * Go to the user 🡪 Assigned Roles 🡪 Add Assignment. * Example - if “Global Reader” permission has been given – then user can able to read the active directory in Azure. | |

## TYPES OF ACCESS CONTROL SYSTEMS



Note :

**RBAC and AD roles serve different purposes within Azure. RBAC focuses on managing access to Azure resources, while AD roles manage access to Azure AD resources and services.**

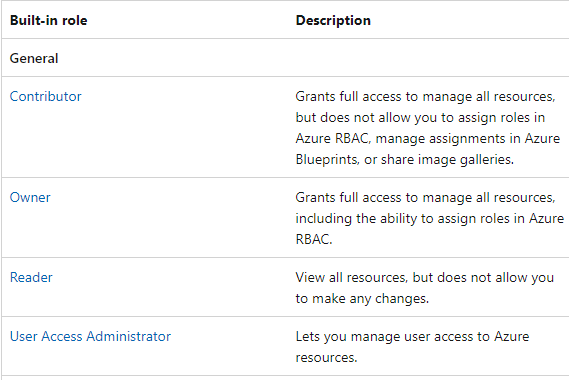
| **RBAC (Role-Based Access Control)** | **AD (Active Directory) Roles** |
| --- | --- |
| RBAC is a built-in access control system in Azure. | Azure AD roles are specific to Azure Active Directory. |
| **It manages access to Azure resources at different scopes (subscription, resource group, or resource level).** | **It manages access to Azure AD resources such as user accounts, groups, and applications.** |
| Uses roles to define sets of permissions for Azure resources. | Uses roles to define permissions for Azure AD resources. |
| Provides flexibility to assign granular permissions to users, groups, or applications. | Assigns roles to users or groups to control access levels within Azure AD. |
| **Offers built-in roles like Owner, Contributor, Reader, User Access Administrator, etc.** | **Offers built-in roles like Global Administrator, User Administrator, Application Administrator, etc.** |
| Permissions can be assigned directly to users, groups, or applications. | Permissions are assigned to users or groups in Azure AD, which then apply to Azure AD resources. |
| Can be used to manage access to resources across various Azure services. | Primarily used to manage access to Azure AD resources and services. |
| RBAC permissions can be customized, and new roles can be created. | AD roles can be customized within Azure AD, but new roles cannot be created. |

### RBAC ROLES (IAM – IDENTITY AND ACCESS MANAGEMENT)

* **RBAC in Azure is a built-in access control system that allows us to grant permissions to users, groups, or applications at different scopes (subscription, resource group, or resource level).**
* RBAC has defined sets of permissions called built-in roles, such as Owner, Contributor, Reader, and User Access Administrator, with varying levels of access.
* We can assign these roles to users or groups to control what they can do with Azure resources. For example, we can assign the Contributor role to a user, allowing them to manage and make changes to resources within a specific scope.

|  |  |
| --- | --- |
| **RBAC TERMINOLOGIES** | |
| SCOPE | * The subject on which the RBAC permission are applied. * It can be on resource, Resource group or Subscription levels |
| SECURITY PRINCIPLE | * To whom the permission is given. It can be a User, Group or Managed Identity |
| ROLE | * What permissions are given. Below are the basic built in RBAC roles. |
| SECURITY |  |

#### BASIC BUILT-IN RBACK ROLES



### DIRECTORY ROLES (AD ROLES)

* AD roles in Azure refer to the roles defined within Azure Active Directory, which is a cloud-based identity and access management service.
* **Azure AD roles are used to manage access to Azure AD resources, such as user accounts, groups, and applications.**
* Azure AD provides various **built-in roles, including Global Administrator, User Administrator, Application Administrator**, and many more.
* These roles determine the level of access and permissions users have within Azure AD. For example, the Global Administrator role has full control over Azure AD, while the User Administrator role can manage user accounts.

### SCOPE OF RBAC

* With RBAC in Azure, roles can be assigned at different scopes. The scope of RBAC are
  + **MANAGEMENT GROUP**
  + **SUBSCRIPTION**
  + **RESOURCE GROUP**
  + **INDIVIDUAL RESOURCE LEVELS.**

**THE ROLE-BASED ACCESS CAN BE GIVEN AT**

|  |  |
| --- | --- |
| RESOURCE LEVEL | * The access can be to a resource – for example - storage account or VM |
| RESOURCE GROUP LEVEL | * Access can be given at resource group level * If access is given at resource group level – it will give access to all resources in that resource group. |
| SUBSCRIPTION LEVEL | * If access is given at subscription level – it will give access to all resources in that subscription |

### TYPES OF RBAC ROLES

1. **BUILT IN ROLES**
2. **CUSTOM ROLES**

#### BUILD IN ROLES

* In Azure, there are several built-in RBAC (Role-Based Access Control) roles available that can be used to manage access and permissions to Azure resources.
* **These roles provide predefined sets of permissions that can be assigned to users, groups, or applications**.
* Azure has number of in-built roles - <https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>, but we can also create our own custom roles as well.

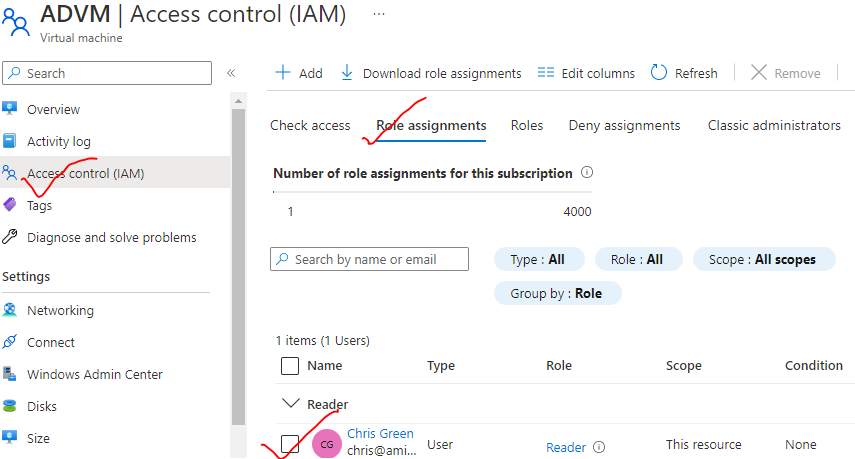
**COMMONLY USED BUILT-IN RBAC ROLES IN AZURE**

|  |  |
| --- | --- |
| **OWNER** | * This role has full access to manage all resources within a scope, including the ability to modify permissions, delete resources, and manage resource settings. |
| **CONTRIBUTOR** | * This role can create and manage all types of Azure resources but cannot grant access to other users or manage permissions. |
| **READER** | * This role has read-only access to view resources and their properties but cannot make any changes or perform any actions. |
| **USER ACCESS ADMINISTRATOR** | * This role can manage user access to Azure resources, including granting and revoking access permissions. |

##### ROLE BASED ASSIGNMENT – READER ROLE

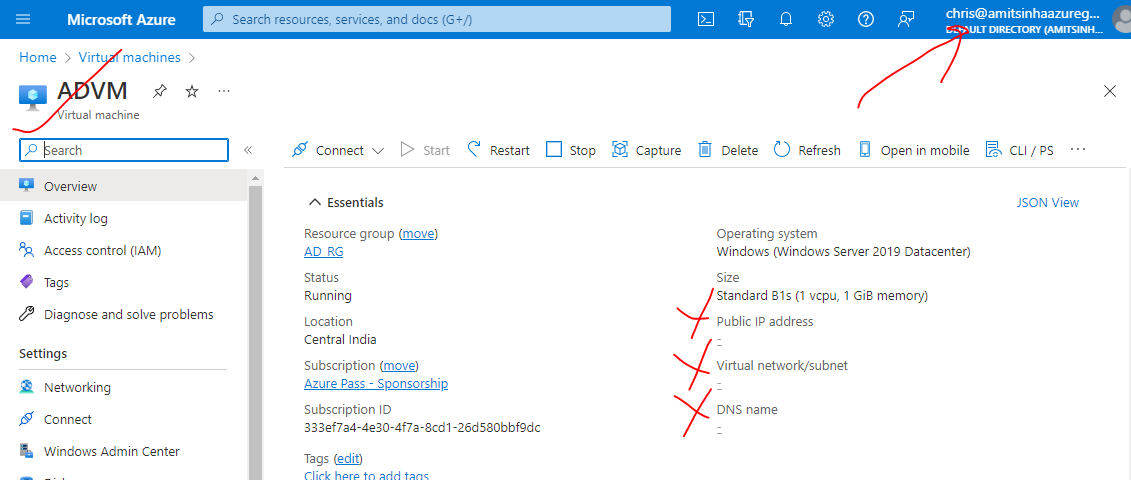
* Example – if we want to give access the Reader permission on VM level (Resource level)
* *Navigate to VM 🡪 IAM🡪 Add 🡪 Add Role Assignment*





WHEN USER LOGS IN AZURE PORTAL

* As the user has reader permission on VM only – hence he have will no access to public IP, VNET and DNS – as they are separate resources in Azure- which needs a separate role assignment.

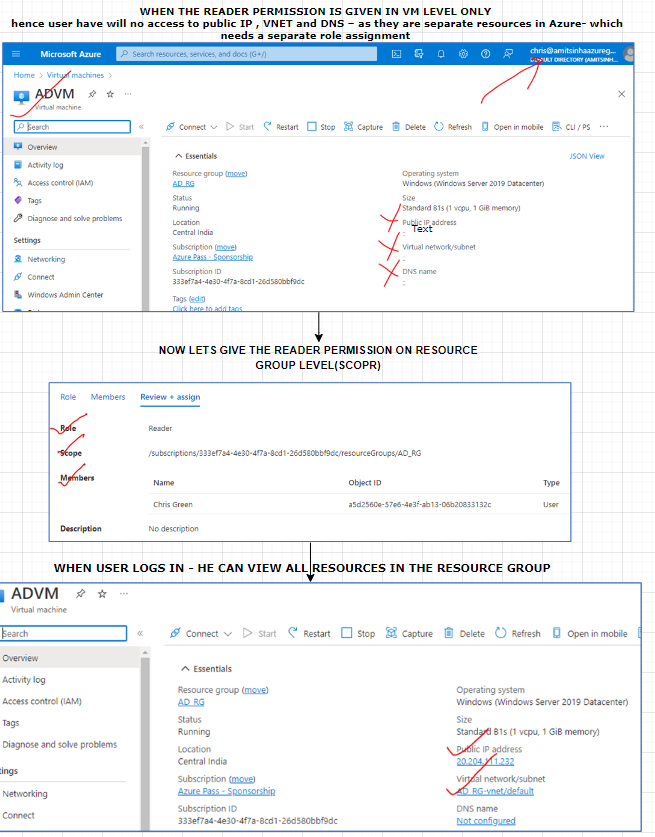


#### ROLE ASSIGNMENT IN DIFFERENT RBAC SCOPES

|  |  |
| --- | --- |
| RESOURCE LEVEL | * The access can be to a resource – for example - storage account or VM |
| RESOURCE GROUP LEVEL | * Access can be given at resource group level * If access is given at resource group level – it will give access to all resources in that resource group. |
| SUBSCRIPTION LEVEL | * If access is given at subscription level – it will give access to all resources in that subscription |

##### ROLE BASED ASSIGNMENT – RESOURCE GROUP LEVEL

* **IF WE ASSIGN A ROLE AT A RESOURCE GROUP LEVEL, IT WILL BE APPLIED TO (INHERITED BY) ALL THE RESOURCES WITHIN THE RESOURCE GROUP.**



##### ROLE BASED ASSIGNMENT – SUBSCRIPTION LEVEL

* If we assign a role to a the identity (user/ group) at the subscription level, then the role gets applied to or inherited to all resource groups that are part of that subscription.

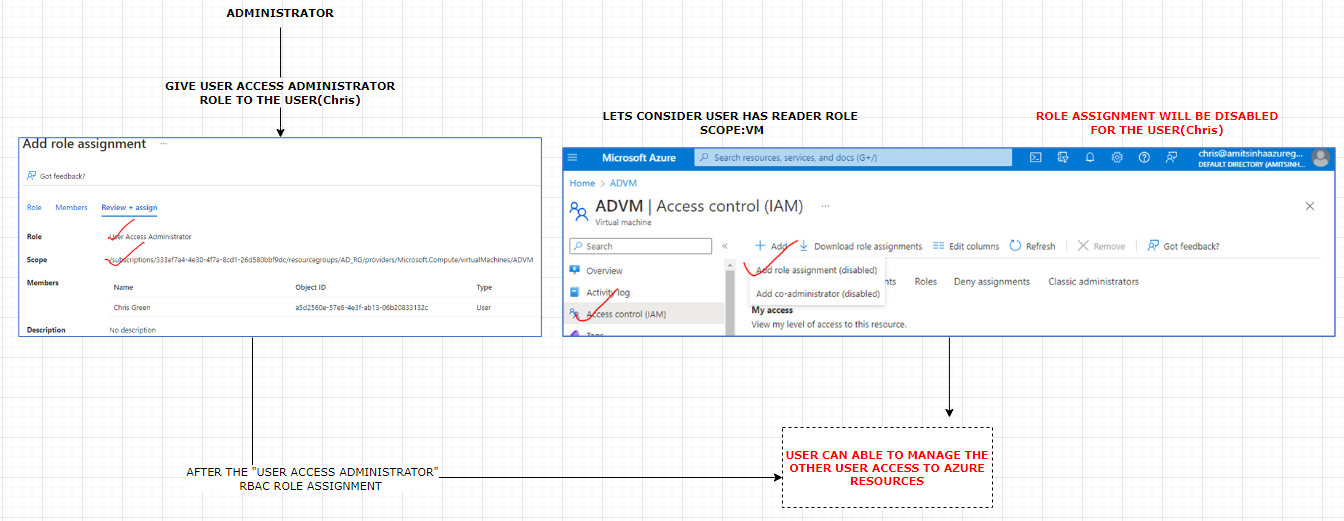
##### ROLE BASED ASSIGNMENT – CONTRIBUTOR LEVEL

* The Contributor role allows users to manage and make changes to Azure resources, except for granting access to others.

|  |  |
| --- | --- |
| Grants full access to manage all resources but does not allow to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries. | * When a user is assigned a role of reader – then no operation can be performed by the user except view. * To enable this capability – we can assign contributor role to the user. * For example - VM contributor role (To perform VM operations). In the below example - we are assigning *VM contributor Role* on resource group level |

##### ROLE BASED ASSIGNMENT – USER ACCESS ADMIN ROLE

* The role allows the user to give access to other users / add role-based access to another user. The “User Access Admin Role” – enable the user for role-based assignments.



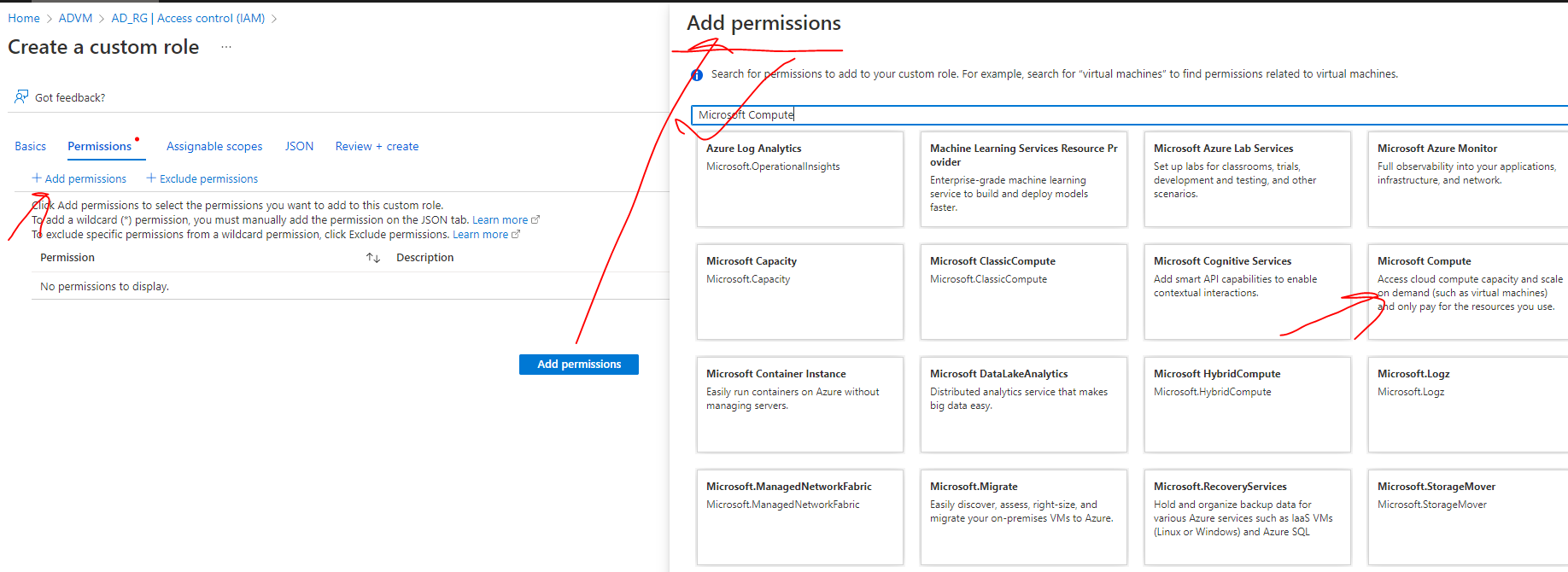
#### RBAC - CUSTOM ROLES

* <https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal>
* There are three ways that we can start to create a custom role.
  + **CLONE AN EXISTING ROLE**
  + **START FROM SCRATCH**
  + **START WITH A JSON FILE**
* The easiest way is to find an existing role that has most of the permissions you need and then clone and modify best on your scenario.
* In the Azure portal, **open a management group, subscription, or resource group** where we want the custom role to be assignable and then open **Access control (IAM)**.

##### CREATING CUSTOM ROLES – START FROM SCRATCH

|  |  |
| --- | --- |
|  | * In the Azure portal, **open a management group, subscription, or resource group** where we want the custom role to be assignable and then open **Access control (IAM)**. |
|  | * Let’s select “start from scratch”🡪 next |

* Let’s say we want to create role for a VM 🡪 select Microsoft Compute



* Select the required permission from the Compute permission list



|  |  |
| --- | --- |
|  | * Once the custom role is created – it can be then assigned to any level |

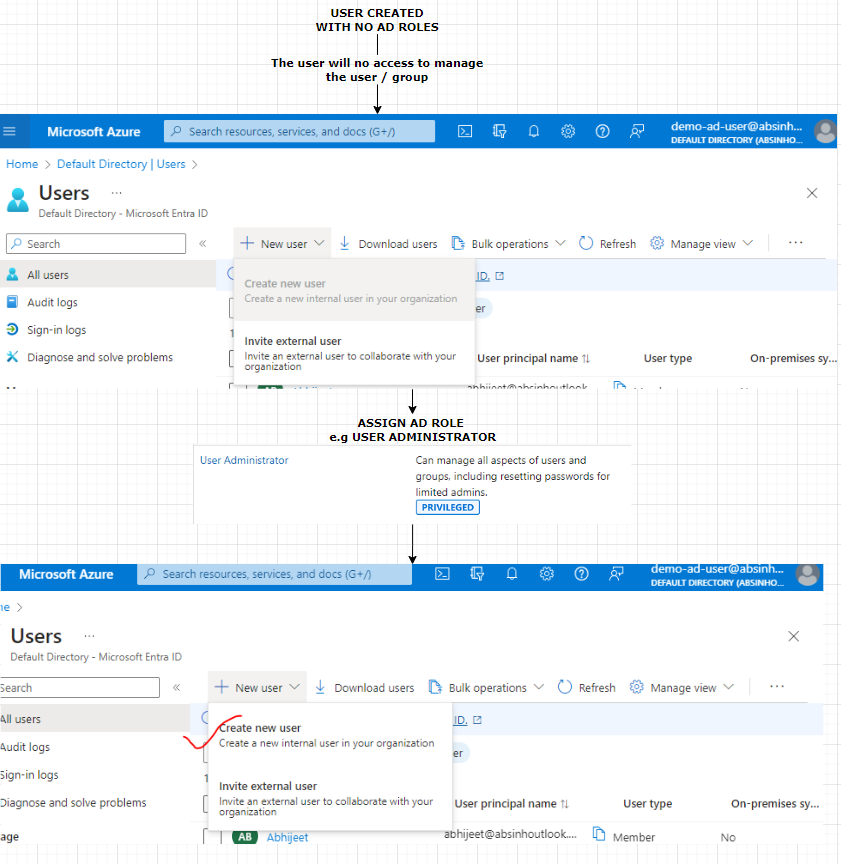
## CREATING USER GROUP

|  |  |
| --- | --- |
|  | * Go to Azure AD 🡪 Groups 🡪 New Group * Note – members can be added while creating the group itself or later too. * To add member to the group 🡪 Go to the group 🡪 Members 🡪 Add members. |
|  | |

## AZURE AD ROLES

* AD roles are purely meant to carry out tasks in Azure Active Directory only. AD roles are dedicated to managing the Active directory itself. for example, to create an application, create a user, create a group etc. For example - In an organization, these activities are they typically delegated to administrators.
* On the other hand, the RBAC are used to give a user access to resources within Azure.
* <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

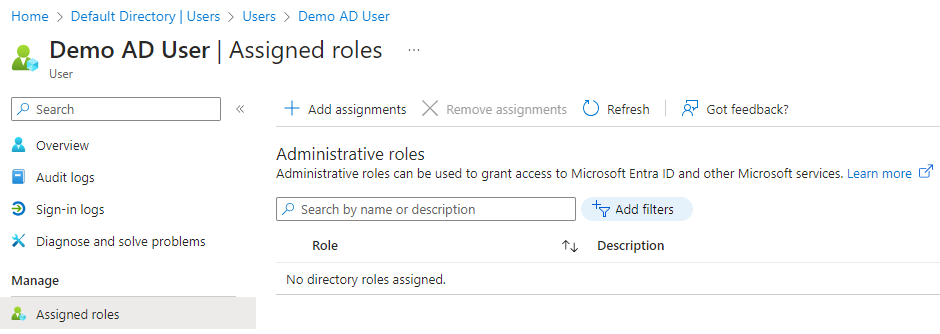
### ASSIGNING AD ROLES



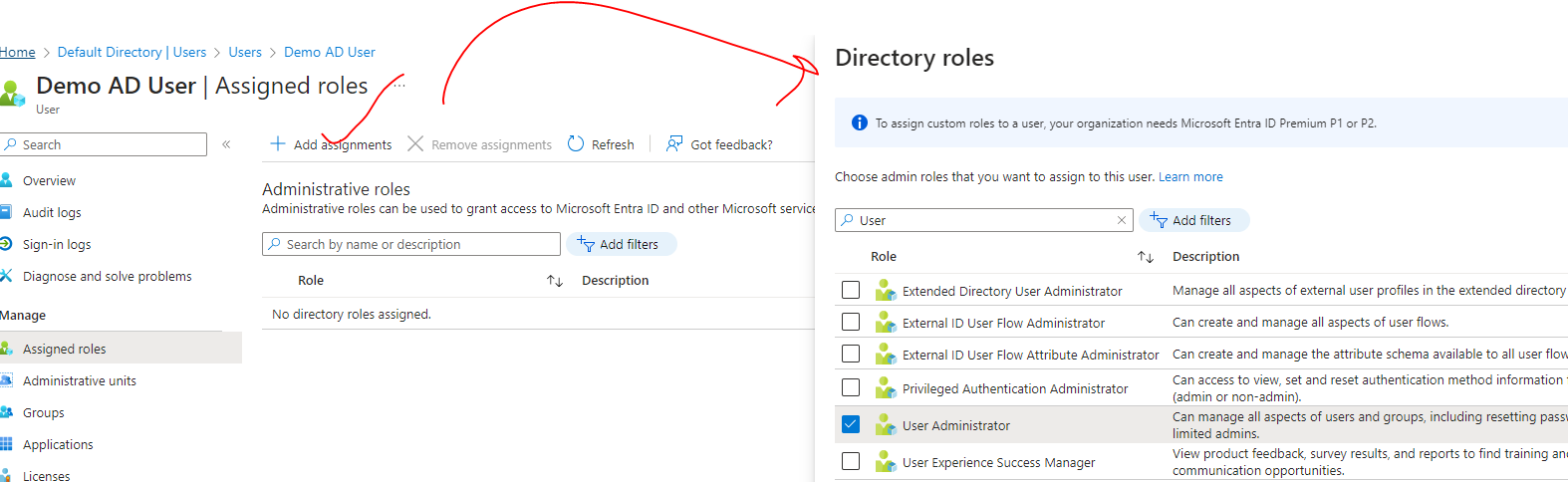
#### ASSIGNING AD ROLE TO USER

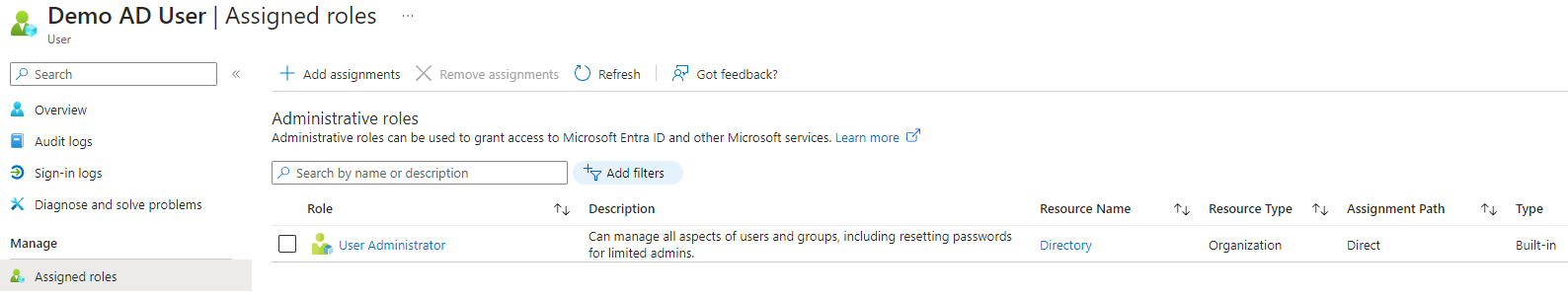
|  |
| --- |
| NOTE: For a user   1. Assigned Roles: THE IS USED TO ASSIGN AD ROLES. 2. Azure role assignments: THE IS USED TO ASSIGN RBAC ROLE TO THE USER |

* To assign AD roles to a user(Demo AD User) . Navigate to the user 🡪 Assigned roles



Step 1: Click on assigned roles 🡪 Select any AD roles (For example: **User Administrator**)





### BUILT IN AD ROLES

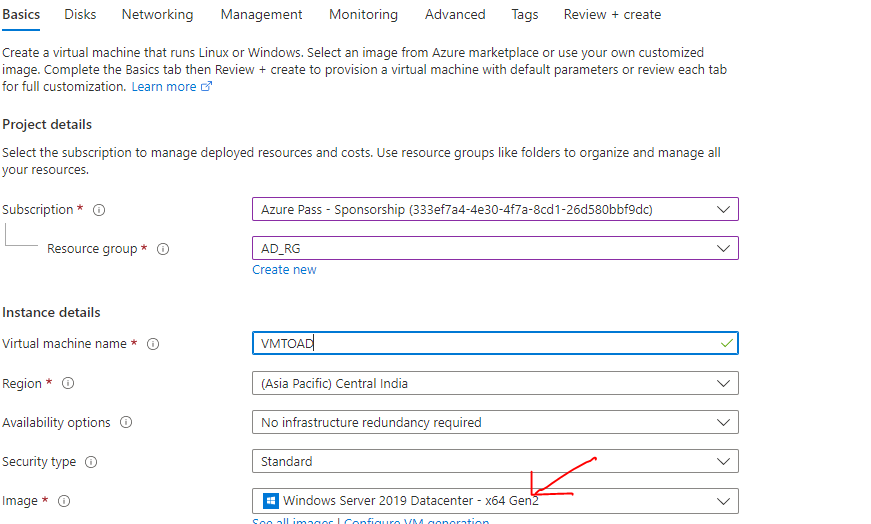
* <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference>

|  |  |
| --- | --- |
|  | * Navigate to Azure Active Directory 🡪 Roles and Administrators * Select the AD role e.g., User Administrator (<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#user-administrator> ) * Select the user (e.g **UserD**) to which AD roles must be assigned. * The AD roles can also be assigned to User Groups as well * The AD roles can be removed using Remove Assignment option, |
|  | |

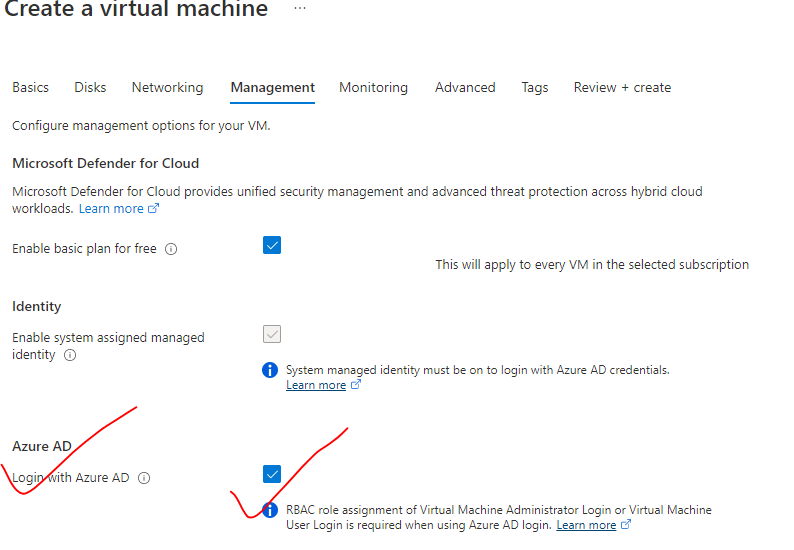
## JOINING A VM TO AD

* Windows 10 and based device, if you have Windows server 2019 can be joined to an Active Directory.

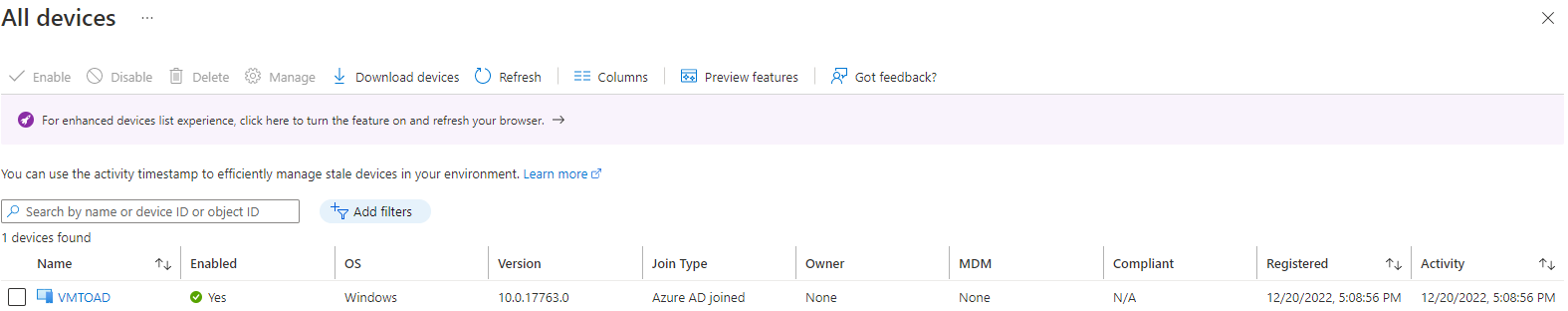
Step 1: Provision a Window 10 / Server VM



Step 2: Register the device with AD



* To check the connected device – Active Directory 🡪 Devices



## AZURE AD CUSTOM DOMAIN

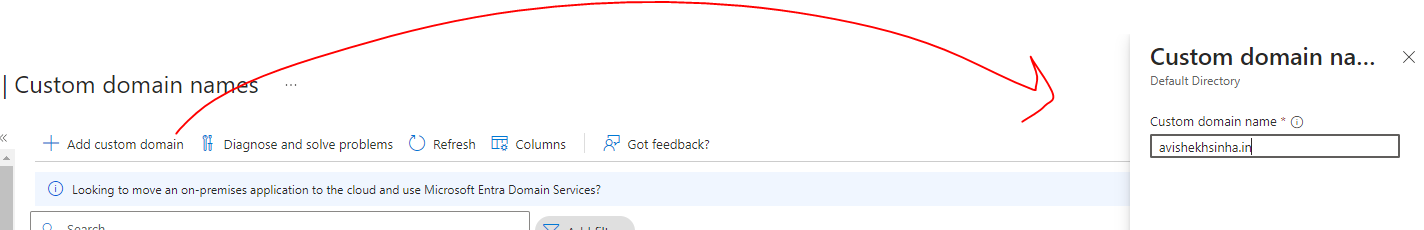
* In Azure Active Directory (Azure AD), we can add and configure a custom domain to use with the Azure AD tenant.
* This allows us to use our own domain name for user sign-in and other services within Azure AD.

### STEPS TO ADD CUSTOM DOMAIN

1. Under the Azure Active Directory menu, select "Custom domains" 🡪 Click on the "Add custom domain" button to start adding a new custom domain

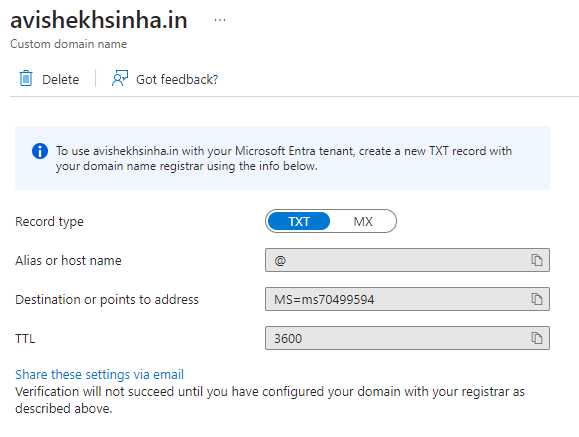


1. Enter the domain name we want to use, such as "avishekh.sinha.in," and click "Add domain."



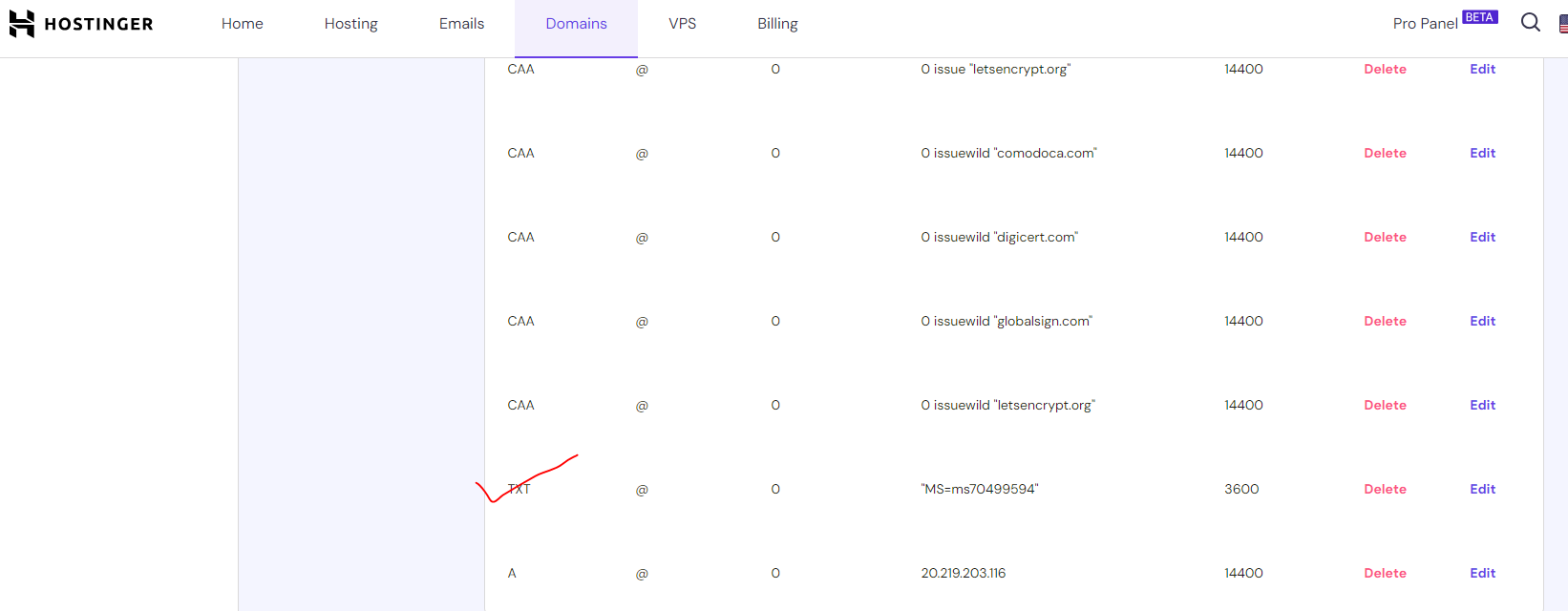
1. VERIFY DOMAIN OWNERSHIP

Azure AD will provide instructions for verifying the domain ownership. This typically involves adding a TXT or MX record to your DNS configuration with the provided values.

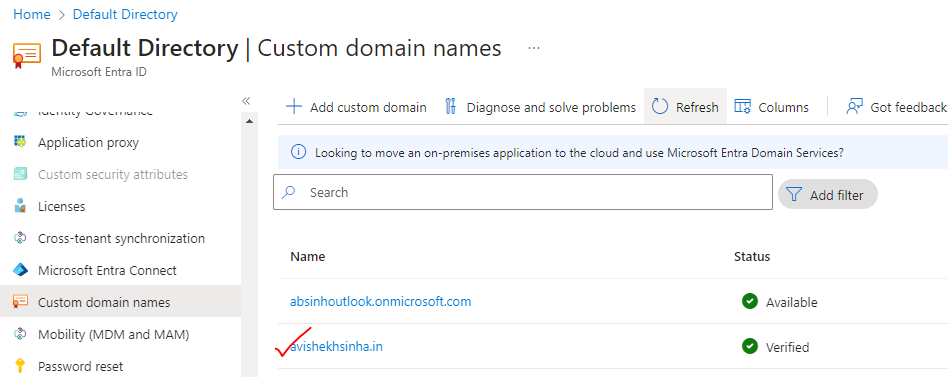


Add the text record in the in the

**TXT RECORD FROM DNS PROVIDER**



1. VERIFY DOMAIN:
   * Once we have added the necessary DNS records, click on the "Verify" button in the Azure portal to initiate the domain verification process.
   * Azure AD will verify the DNS records and confirm domain ownership.

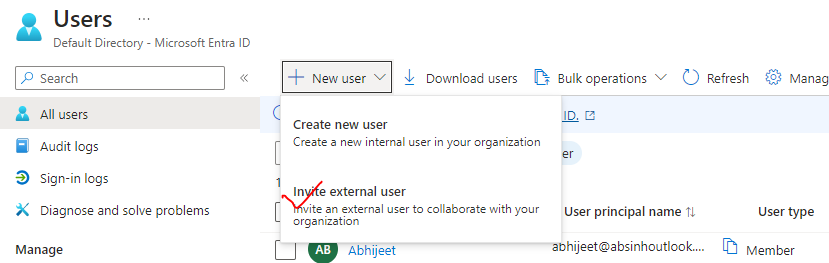


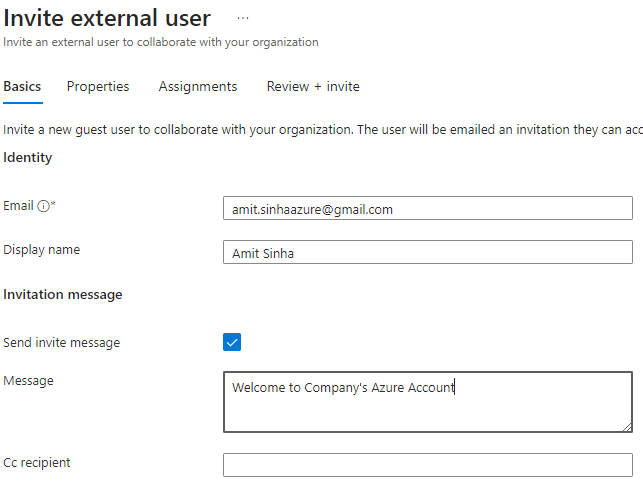
1. CONFIGURE USER SIGN-IN:
   * After the domain is verified, we can configure user sign-in using the custom domain.
   * **We have the option to set the custom domain as the default domain or allow users to sign in with both the custom domain and the initial <your-domain>.onmicrosoft.com domain.**

## INVITING GUEST USER

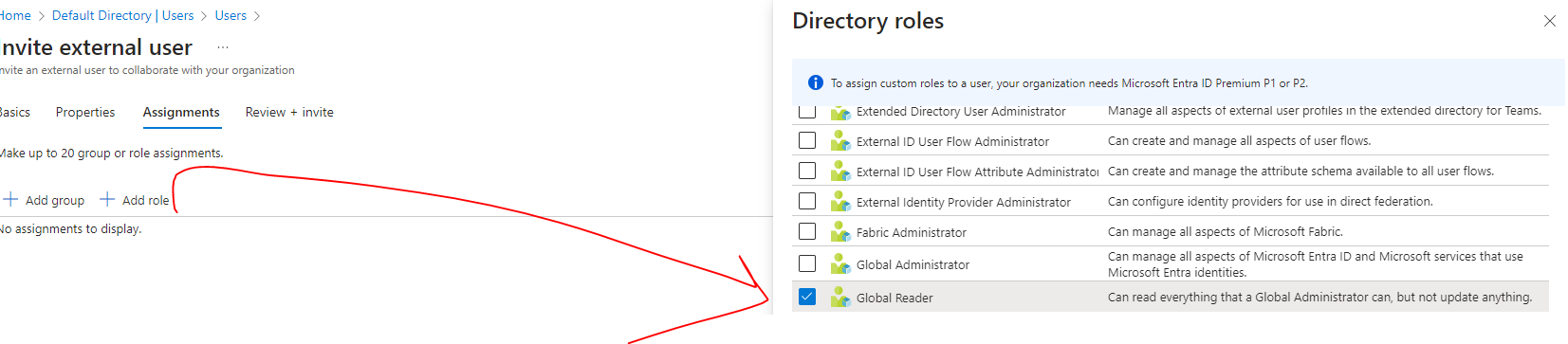
* Inviting a guest user in Azure Active Directory (AD) refers to the process of granting access to external users, who do not belong to your organization, to collaborate and access resources within your Azure AD tenant.
* When we invite a guest user, we are essentially extending an invitation for them to join our Azure AD environment as a guest. This allows them to sign in with their own credentials from a different organization or as an individual user.
* Guest users can be invited to collaborate on various Azure services, such as Azure DevOps, Azure B2B collaboration, Azure Portal, Azure Active Directory, and more. By inviting guest users, we can enable collaboration and resource access for partners, vendors, contractors, and other external users, while maintaining control over their permissions and access levels within your Azure AD tenant.

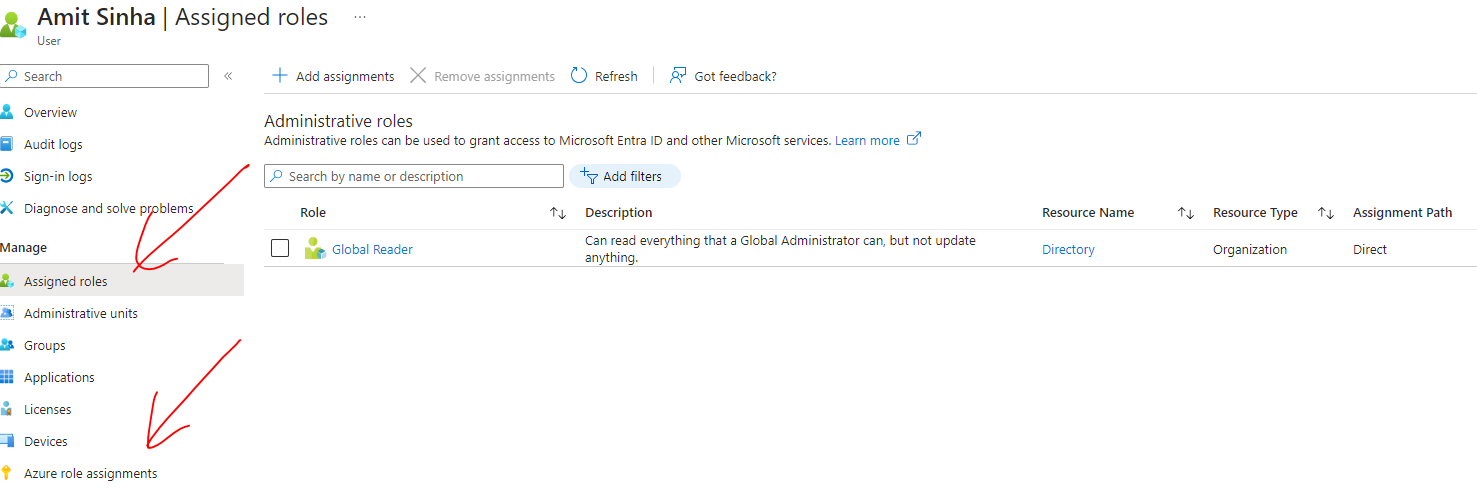
### CREATING GUEST USER



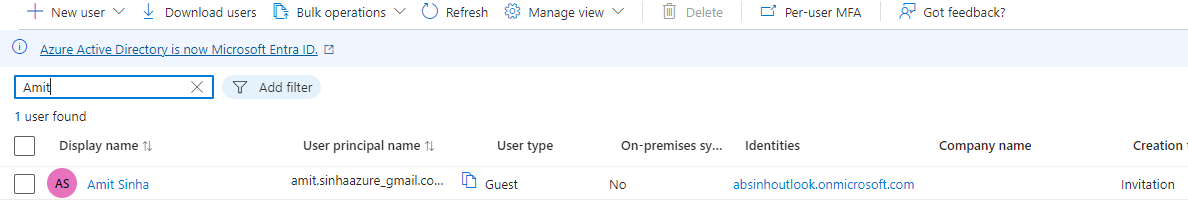


The external user can be assigned either AD roles or assign RBAC role

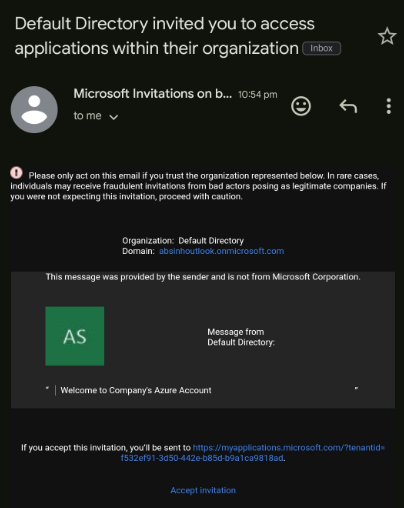




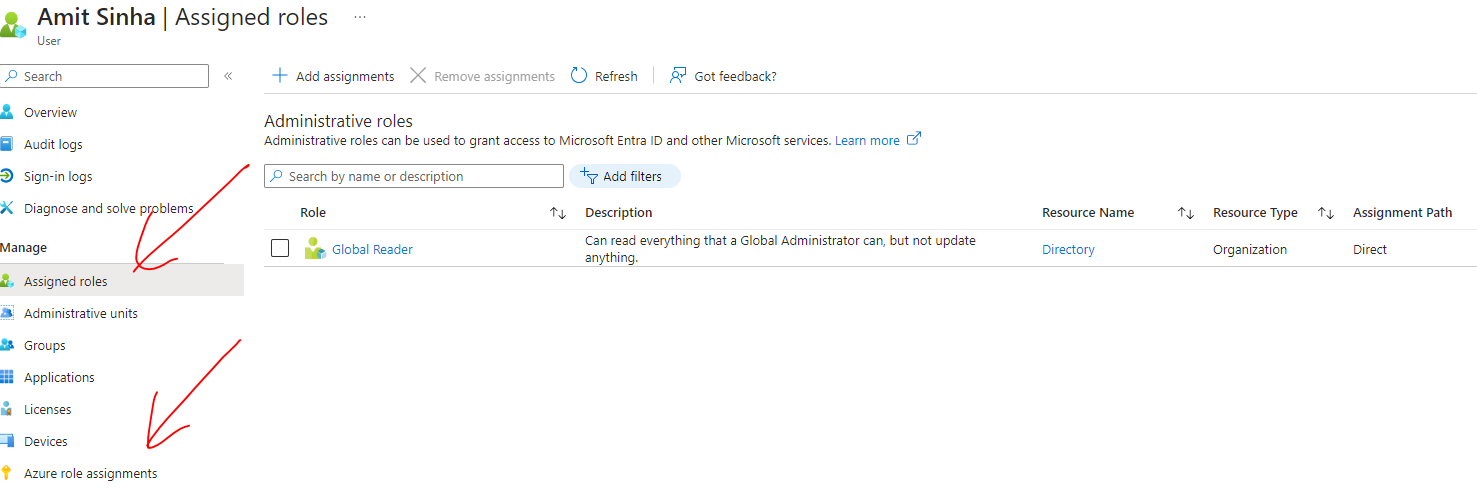
* **The user will be a guest user**



* The user will receive an email to accept the invitation - Accept the invitation 🡪 Log in to the Azure Account

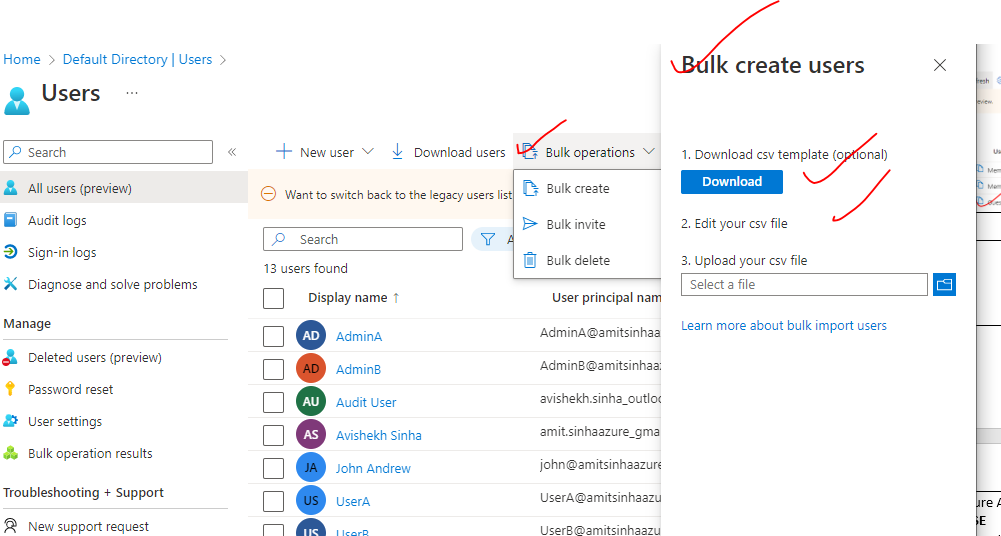


* After accepting the invitation – The guest user can login to the Azure Account.
* Initially the guest user don’t have access to any resources. Access has to be given explicitly



## USER CREATION / DELETION IN BULK

* For bulk creation/deletion of user, Navigate to Active directory 🡪 Bulk Operations
* Download the CSV and add the data to delete /create 🡪 Upload the CSV
* Sample - <https://github.com/avishekhsinhaRepo/Docs/blob/master/Azure/Documents/AD/UserCreateTemplate.csv>

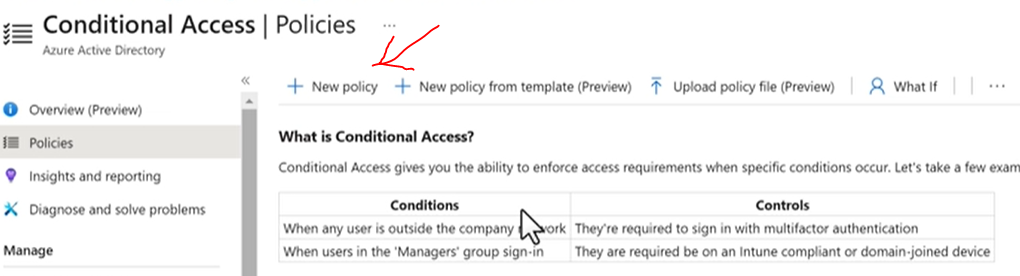


## CONDITIONAL ACCESS POLICY

* A conditional access policy is a security feature provided by Microsoft that allows us to set specific conditions and requirements for users to access the organization's resources.
* It helps protect sensitive data by enforcing additional security measures based on various factors such as user location, device compliance, application sensitivity, and user risk level.
* Example - When the user is logging in - only if they fulfill a certain, then allow them to authenticate, and at the same time, we could tell that they could only authenticate, if they also perform the action of multi-factor authentication.

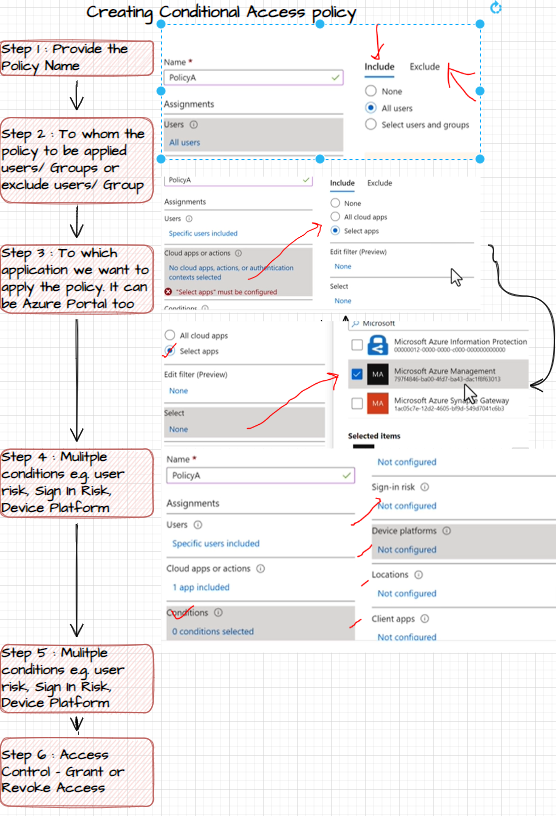
### SETTING UP CONDITIONAL ACCESS POLICY

* For conditional access policy – we need AD Premium (check in overview of AD)
* Navigate to AD 🡪 Security 🡪 Condition Access
* For applying the condition access policy 🡪 Create a Policy

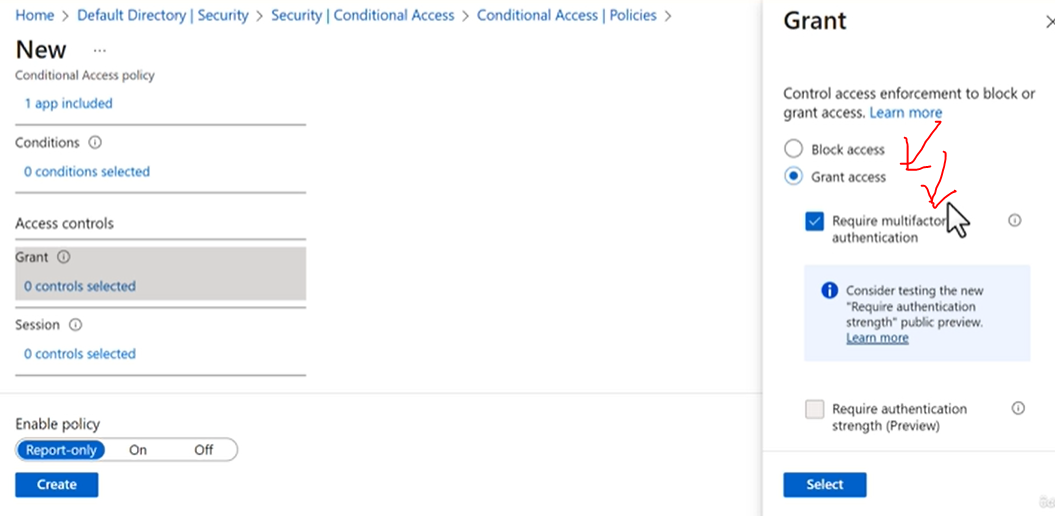


### EXAMPLE – CONDITIONAL ACCESS POLICY

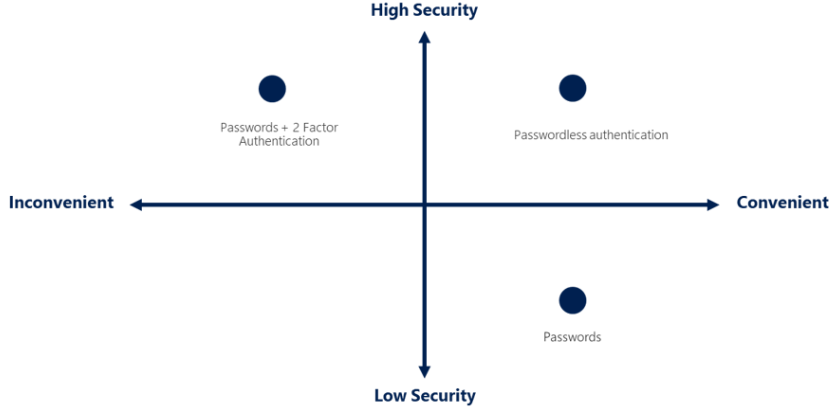
* In the below example – rather than enabling MFA on per user basics. We will make use of conditional access policy.



* In the above condition access policy – We are granting access to user/ group to login to Azure Portal(as we selected Microsoft Azure Management as selected apps). The users or users in the group can able to login to Azure Portal only after MFA



## PASSWORDLESS AUTHENTICATION



* Azure offers passwordless authentication as a more secure and convenient way to access resources.
* Passwordless authentication eliminates the need for users to remember and enter passwords by using alternative authentication methods.
* The Passwordless authentication are secure in the sense – it is tied to a device not to an account. Hence authentication is only possible we have access to the device.

## PASSWORDLESS AUTHENTICATION OPTIONS

* WINDOWS HELLO FOR BUSINESS
  + This feature allows users to sign in to their Windows devices using biometric authentication, such as facial recognition or fingerprint scanning, instead of a password.
  + It can be integrated with Azure Active Directory (Azure AD) for secure access to Azure resources.
* MICROSOFT AUTHENTICATOR APP
  + Azure AD supports the use of the Microsoft Authenticator app for passwordless authentication.
  + Users can verify their identity by approving a notification on their registered mobile device or by entering a PIN or biometric authentication through the app.
* FIDO2 SECURITY KEYS
  + Azure AD supports the use of FIDO2 security keys for passwordless authentication. These physical security keys provide an added layer of security by requiring users to insert the key into a USB port or use Bluetooth to authenticate their identity.
* TEMPORARY ACCESS CODES
  + Azure AD also offers the option to use temporary access codes sent via SMS or email as an alternative to passwords. Users receive a one-time code that they can use to authenticate their identity.

## ADMINISTRATIVE UNITS

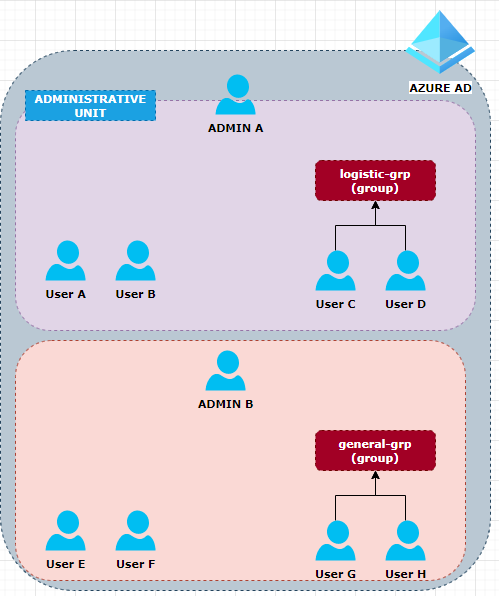
* Administrative Units in Azure Active Directory (Azure AD) provide a way to organize and manage users and resources within your organization.
* It is a logical grouping that helps us delegate administrative tasks and apply policies to specific subsets of users and resources.

**ADMINISTRATIVE UNITS ALLOW US TO:**

* ORGANIZE USERS
  + We can group users based on different criteria, such as department, location, or business unit, into separate Administrative Units.
  + This makes it easier to manage and delegate administrative tasks to specific administrators or helpdesk teams.
* DELEGATE ADMINISTRATION:
  + We can assign administrative roles and permissions to specific Administrative Units, allowing administrators to manage users and resources within their assigned unit without having access to the entire Azure AD tenant.
* APPLY POLICIES:
  + Administrative Units can be used to apply policies and settings, such as password policies or conditional access policies, to specific groups of users or resources.

|  |  |
| --- | --- |
|  | * In Azure AD we create uses and assign roles/permission to them   **USE-CASE**   * Let's say that we have multiple departments in a company, and we want to create a admin for each department – who will only go ahead and manage the subset of users within that particular department. * Since Azure AD is a global directory. If we start creating users in global AD – it will be difficult to manage them all. * Hence to manage the users department wise – we can make use administrative units for each department. |

### LAB -ADMINISTRATIVE UNITS



**PART OF ADMINISTRATIVE UNIT**

* **Two users who are going to be part of an administrative unit + Admin User that is going to behave as the user administrator for the administrative unit** +**Two more users that are going to be part of a group(logistic-grp).**

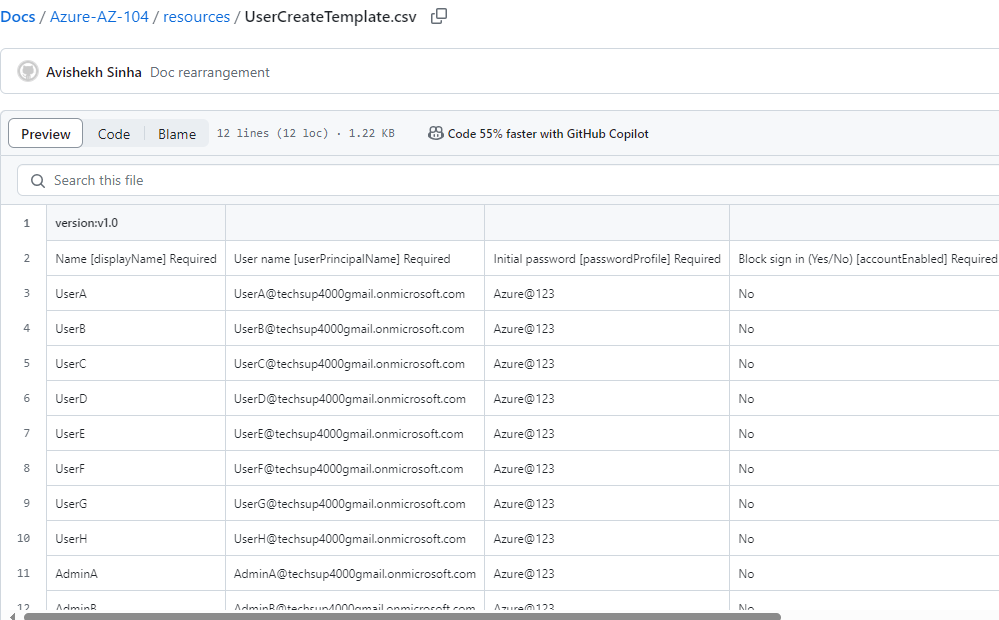
**NOT PART OF ADMINISTRATIVE UNIT**

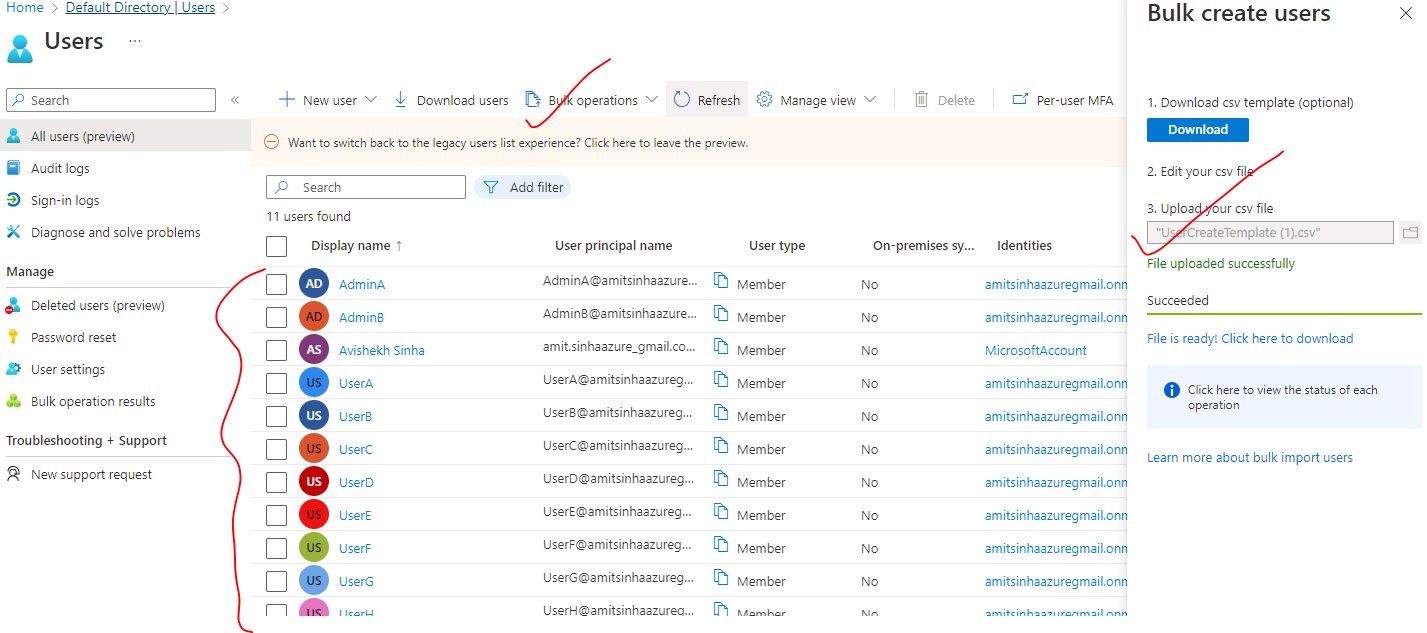
* **We're going to create some other users who are not going to be part of that unit + Some of these users are going to be part of another group known as general-grp.**

***Step 1:*** *Create user (Bulk Operation) – for the bulk creation of user Azure provides a template(as .xlsx) 🡪 Download the template 🡪 Add the data of users 🡪 Upload the sheet*

[Docs/Azure-AZ-104/resources/UserCreateTemplate.csv at master · avishekhsinhaRepo/Docs (github.com)](https://github.com/avishekhsinhaRepo/Docs/blob/master/Azure-AZ-104/resources/UserCreateTemplate.csv)

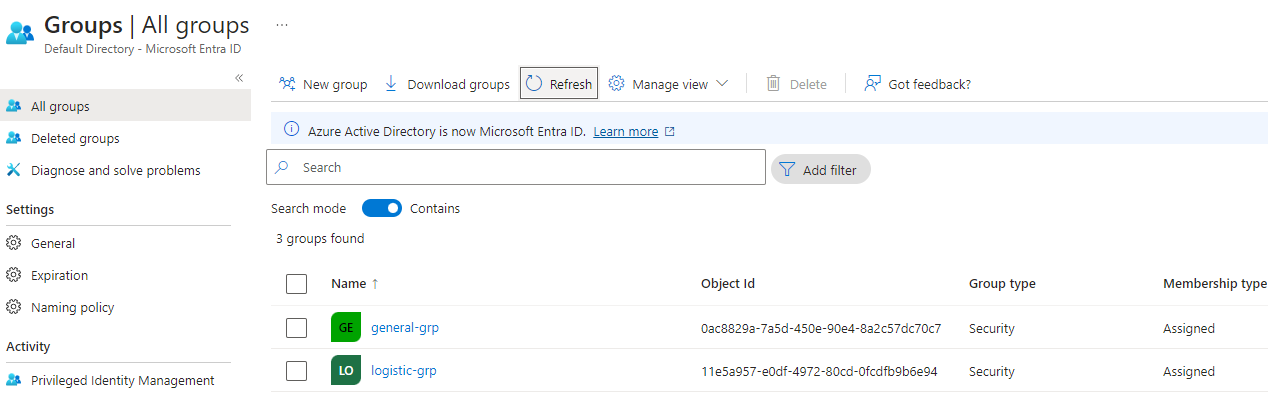
**\*\*\* update the domain name based on your domain account**





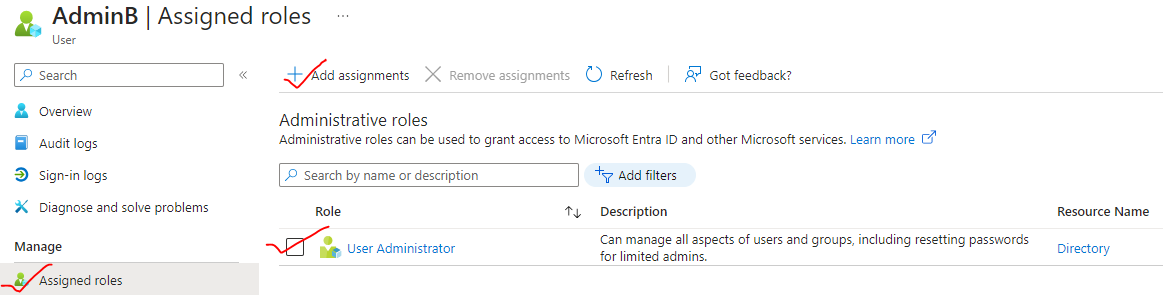
**Step 2:** Create the user groups

|  |  |
| --- | --- |
| Logistic Group – User C and User D | General Group – User G and User H |
|  |  |

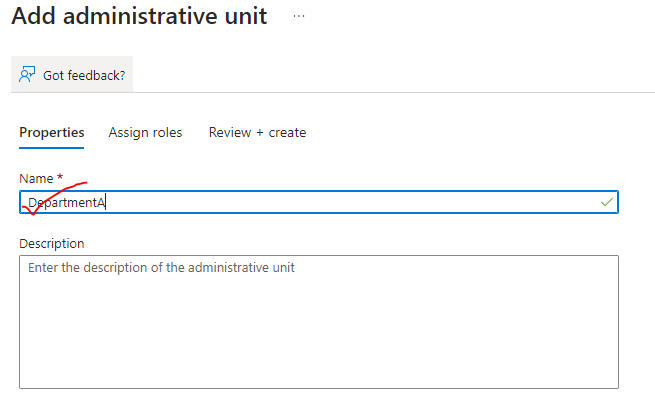


**Step 3:** ASSIGN “USER ADMINISTRATOR ROLE ” TO ADMINS

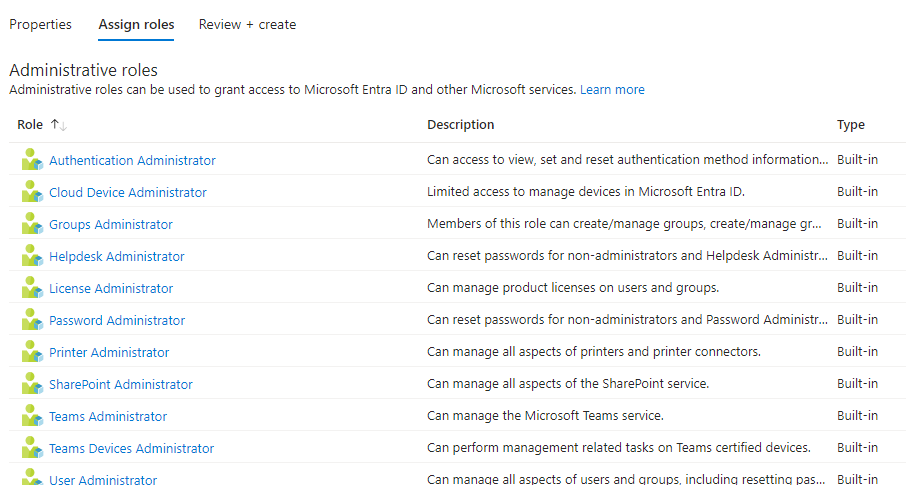
**ADMIN B**

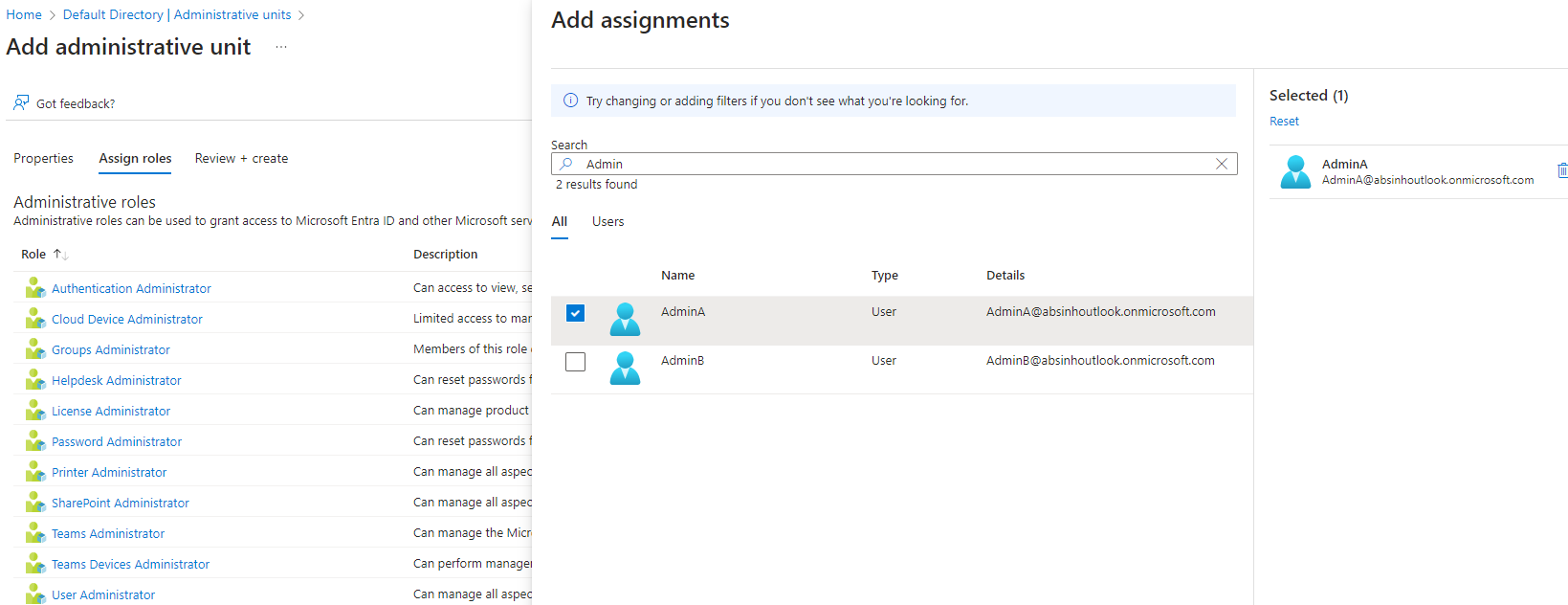


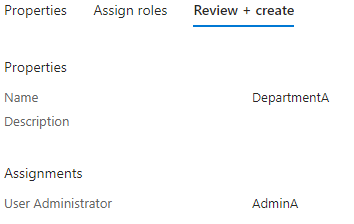
**STEP 4: CREATE THE ADMINISTRATIVE UNIT**



* There are certain roles that are available only as part of Administrative unit.
* Admin A will be assigned with “**User Administrator**” for the administrative unit







**So, the entire idea is - Admin A can able to manage**

1. **Logistic Group (this group is part of Administrative Unit)**
2. **User A and User B (Will be members of Admin Unit)**
3. **But - should not have the ability to manage other users that are outside the administrative unit.**

## CONCEPT OF ZERO TRUST

* Before understanding Zero Trust Security Model/Principle. Let’s To understand the concept of classic Trusted Model

## CLASSIC TRUSTED MODEL

* In a typical classic security model, especially when it comes to getting access to sensitive resources - is based on a concept - referred to as a trusted perimeter, or a trusted boundary for secure access.



* The classic example of a trusted perimeter or trust boundary is internal corporate network.
* Inside the corporate network at the corporate office, we've been able to restrict access to private or sensitive materials to entities or devices inside of that secure network.
* In other words, if you're on the internal corporate network, we have a higher level of trust to those sensitive resources.
* By comparison then - users and devices outside of that corporate network are non-trusted devices. The users, computers, and databases inside of our corporate network or our trusted perimeter are implicitly trusted, and anyone outside of that network is not trusted.



* For remote connection, in order to access our sensitive corporate resources we can set up a VPN client on that external work-from-home entity.
* VPN is simply an extension of that trusted perimeter or extending access to that internal corporate network.
* But, if we provide too much implicit trust to resources inside of a network, Just in case - if one of those internal users gets malware on their computer, well, it can cause havoc on that internal perimeter network because that implicitly trusted user may have too broad of a scope of access. Hence - for challenges like these, this is where the Zero Trust security model comes into play to effectively solve them.

## ZERO TRUST MODEL

* The foundation principle of Zero Trust in Azure is based on the concept of "**never trust, always verify**."
* It challenges the traditional security model that assumes trust once a user or device is inside the network perimeter. Instead, Zero Trust in Azure ensures that every access attempt is continuously verified and validated, regardless of the user's location or the network(trusted /untrusted network) they are connected to.

KEY FOUNDATION PRINCIPLES OF ZERO TRUST

* VERIFY EVERY ACCESS
  + Azure implements strong identity and access management practices, ensuring that every user and device attempting to access Azure resources is verified.
  + This involves multi-factor authentication (MFA) to confirm the user's identity and device health checks to assess the security posture.
* LEAST PRIVILEGE ACCESS
  + Azure enforces the principle of least privilege, which means that users are granted the minimum level of access required to perform their specific tasks.
  + This ensures that users only have access to the resources they need and minimizes the risk of unauthorized access.
* ASSUME BREACH
  + Zero Trust in Azure assumes that breaches can happen at any time. Therefore, Azure implements continuous monitoring and threat detection mechanisms to identify potential security incidents and respond to them promptly.
  + This proactive approach helps mitigate the impact of breaches and reduce the time to detect and respond to security threats.
* MICRO-SEGMENTATION
  + Azure supports network segmentation to create isolated environments within the Azure infrastructure. This allows organizations to separate resources into different subnets and control traffic flow between them using Network Security Groups (NSGs) and Azure Firewall.
  + Micro-segmentation reduces the attack surface and limits lateral movement within the network.
* DATA PROTECTION
  + Azure provides various data protection features, including encryption at rest and in transit, data classification, and access controls.
  + These measures help protect sensitive data from unauthorized access and ensure compliance with data privacy regulations.

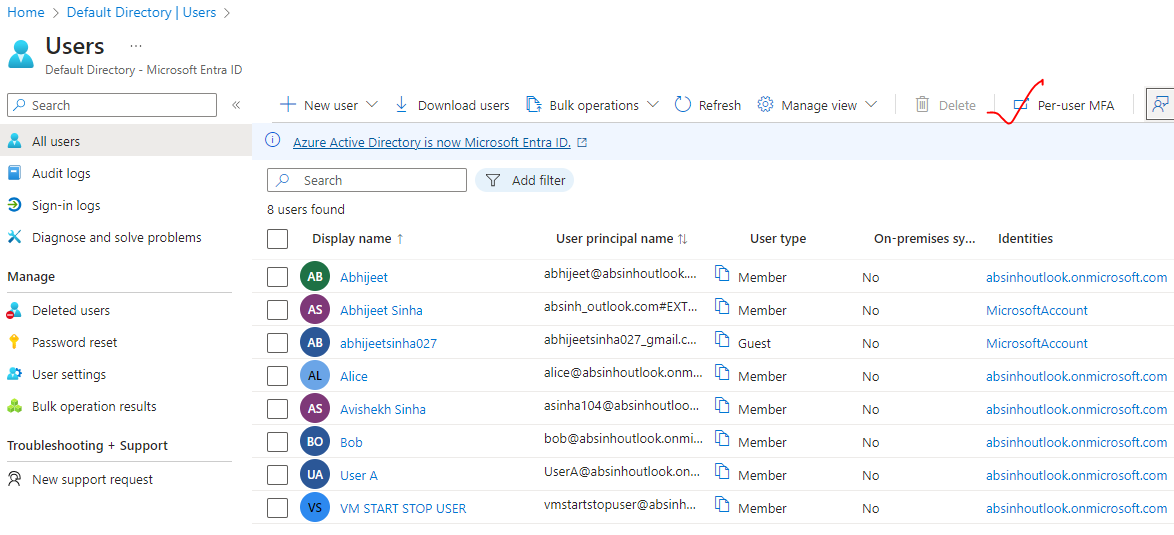
*By adhering to these foundation principles, organizations can build a Zero Trust architecture in Azure that enhances the overall security of their cloud resources, mitigates the risks of unauthorized access and data breaches, and provides better protection for sensitive information.*

# MULTIFACTOR AUTENTICATION(MFA)

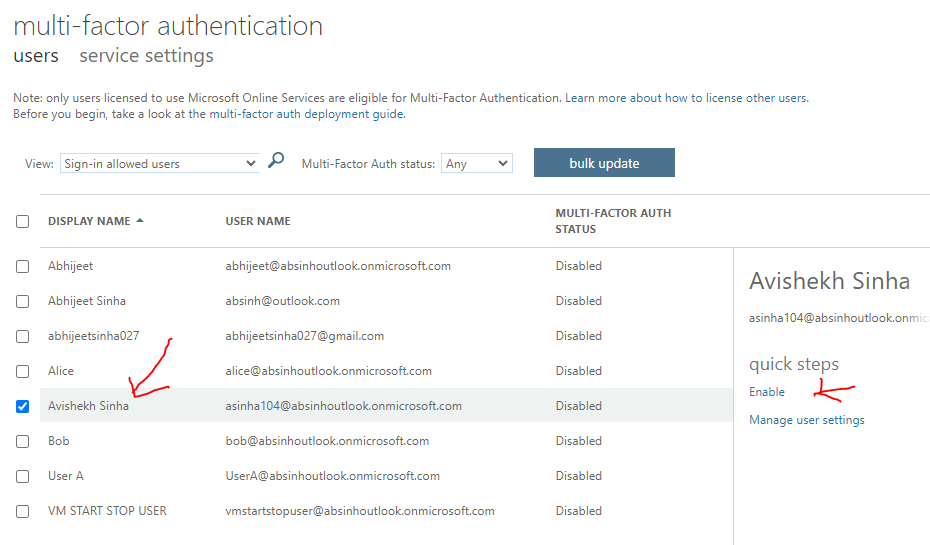
* In Azure, Multi-Factor Authentication (MFA) provides an extra layer of security to help protect user accounts from unauthorized access.
* MFA requires users to provide additional verification factors, such as a phone call, text message, or mobile app notification, in addition to their username and password.
* This helps to ensure that even if an attacker obtains a user's password, they still need the additional verification factor to gain access.

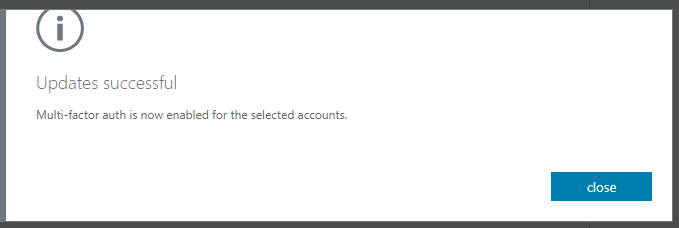
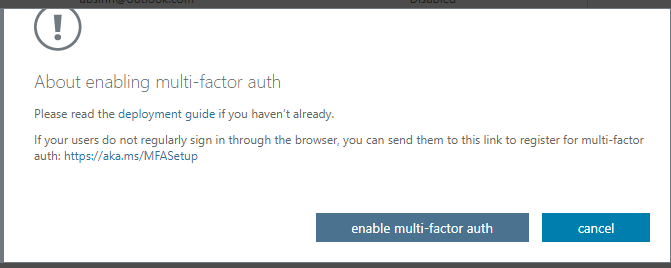
## ENABLING MFA FOR USER

* Navigate to Microsoft Entra Id 🡪 All Users 🡪 Per User MFA

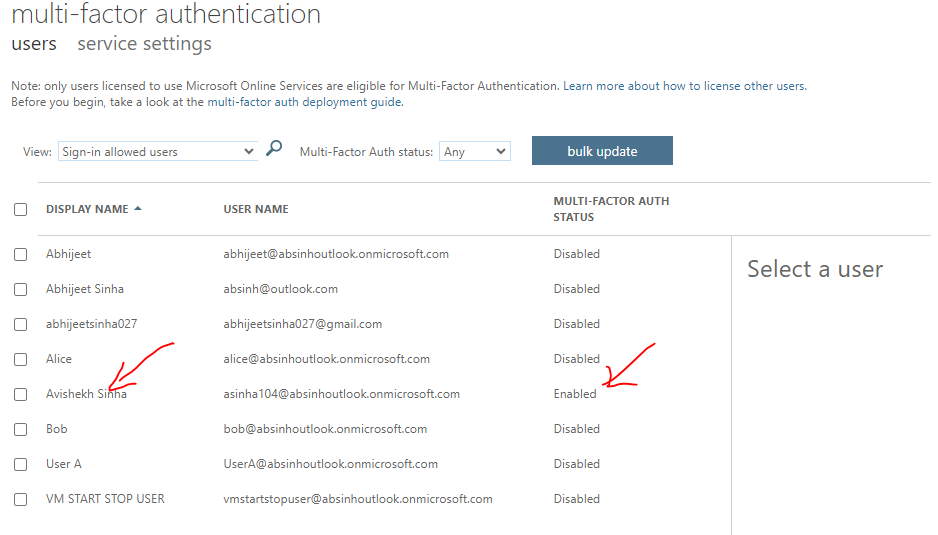


* To enable MFA for a user 🡪 Select the user 🡪 Enable🡪Enable MFA

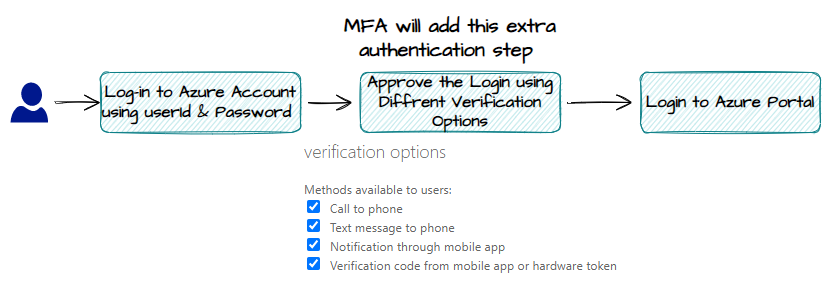




MFA ENABLED OF USER

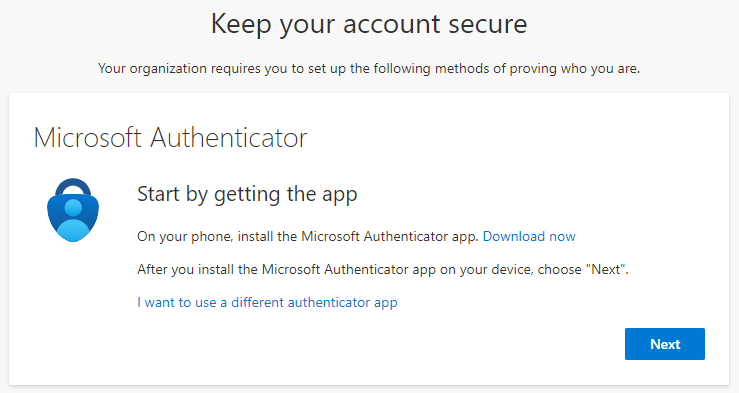


* Let’s login with the username for whom the MFA has been enabled. The MFA setting adds one more level of authentication. If Multi-Factor Authentication (MFA) is enabled for a user in Azure, they will need to perform additional verification steps when signing into their account.



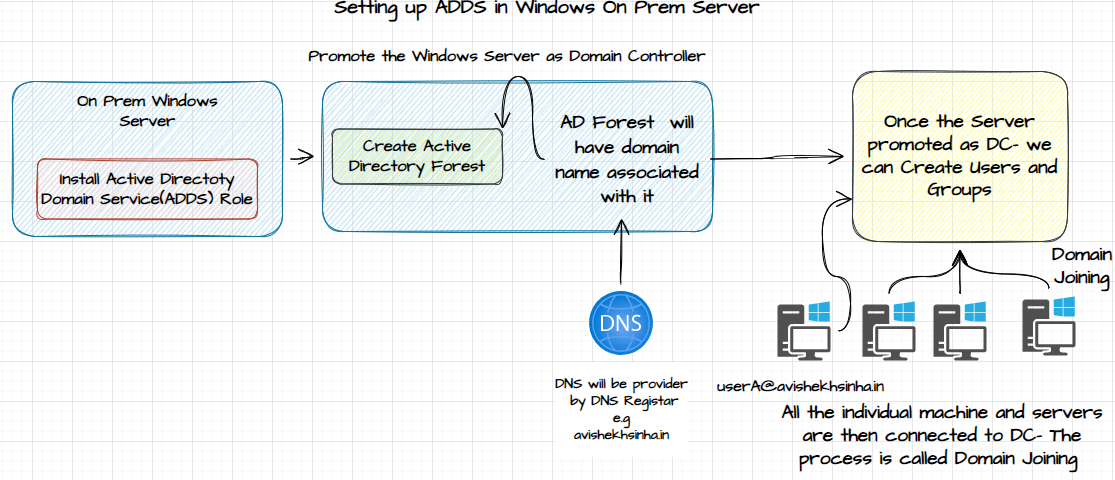
STEPS

1. **Sign-In**: The user initiates the sign-in process by entering their username and password as usual.
2. **Verification Methods:** 
   1. Depending on the MFA settings and user preferences, they will be prompted to choose a verification method. This can include options like a **phone call, text message (SMS), mobile app notification**, or using a verification code generated by a mobile app or hardware token.
3. **Additional Verification**: Once the user selects their preferred verification method, they will receive a phone call, text message, or app notification, or they will generate a verification code using their mobile app or hardware token.
4. **Provide Verification** **Code**: The user will enter the verification code received through their chosen method or generated by their mobile app or hardware token.
5. **Access Granted:** If the provided verification code is correct and matches the expected code, the user will be granted access to their Azure account.



# HYBRID ENVIRONMENT IDENTITIES

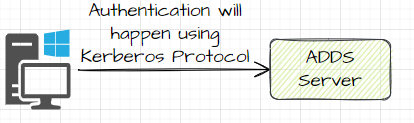
## SETTING ADDS (ACTIVE DIRECTORY) IN ON-PREM WIDDOWS SERVER



* Step 1: In the Windows server install ADDS (Active Directory Domain Service )Role
* Step 2: Promote the Windows Server as a Domain Controller. To promote the server as domain controller

1. Create an Active Directory Forest
2. The AD Forest has a DNS associated with it(eg. **avishekhsinha.in**).

* Step 3: Once the Server is promoted as a Domain Controller, We can be able to create users and groups
* Step 4: Connect the On Prem machine and Server and associate it with user and groups.
  + The authentication between the connected devices and ADDS Server can happen using Kerberos Protocol
  + *Kerberos is a network authentication protocol that provides a secure way for clients and servers to authenticate and communicate over a network*

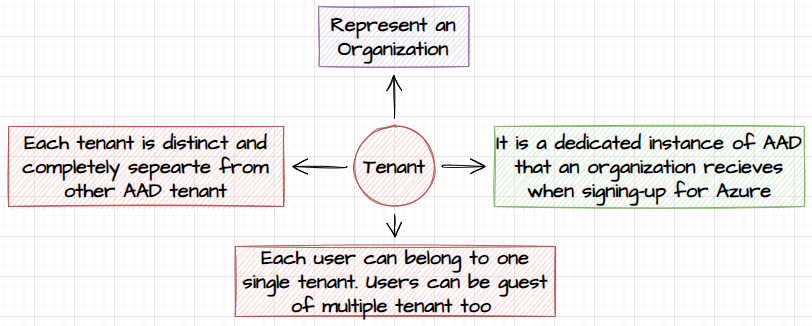


* Now – the central server will manage the users and group and provide authentication and authorization services for them.

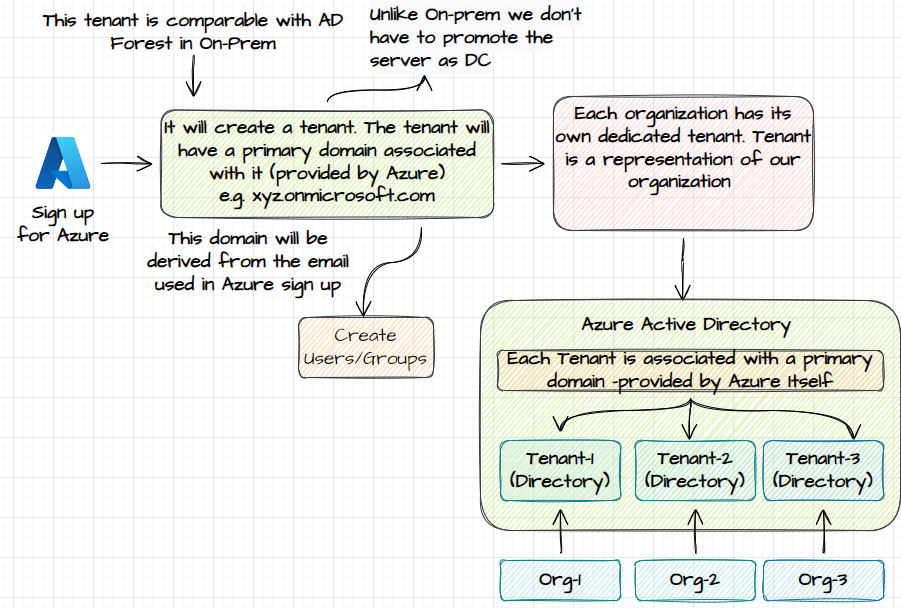
Note:

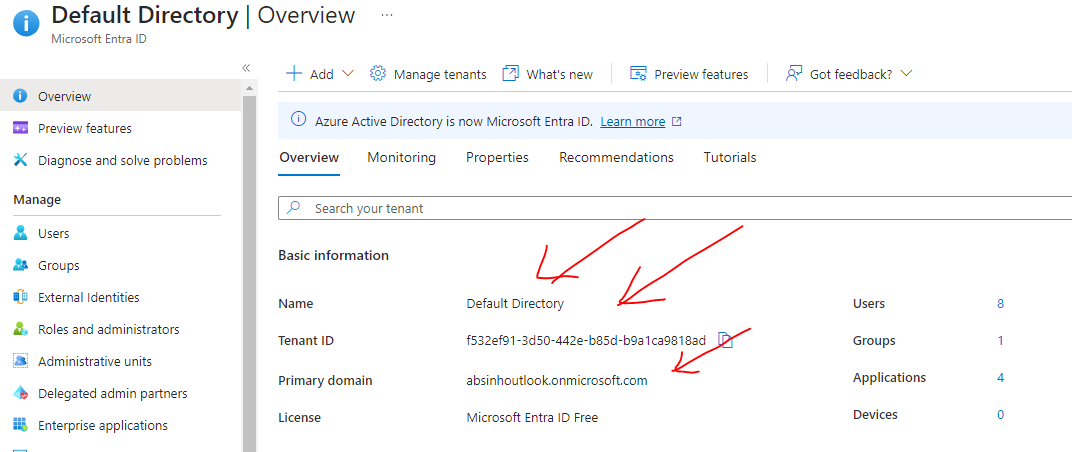
* Using the centralized Domain Controller – Group policy can also be applied /enforces to all the connected devices.
* This is how organization put restrictions on the work machines.

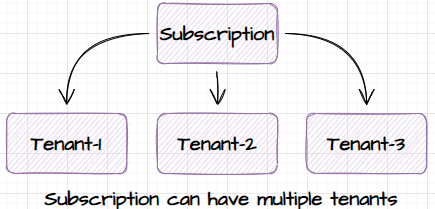
## TENANT



* When we signup for Azure, it creates a tenant for us. This tenant has primary domain associated with it , provided by Azure itself
* Tenant is unique representation of an organization. Each organization has it own dedicated tenant and associated domains.
* In the directory/tenant we can be able to create users and group

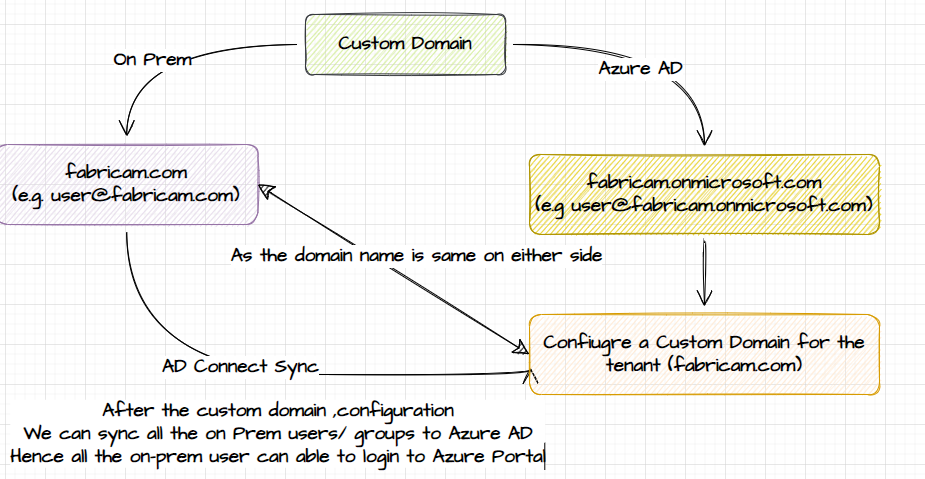






## SYNC USERS FROM ON PREM TO AD

* When the user are created in an AD, they are created with the primary domain(xyz.onmicrosoft.com), which Azure provides.
* In on prem (ADDS) the users are created company’s domain e.g (fabrikam.com)
* Now if we want to sync the on-prem users with Azure AD, we need to configure the domain , same as in on-prem(fabrikam.com)
* After the matching domain on either side – we can sync the user using a service called “AD Connect Sync”
* After the sync – all the users can able to login to portal using the same credential.
* They can able to only login to Azure Portal, without having any access to any of the resources.

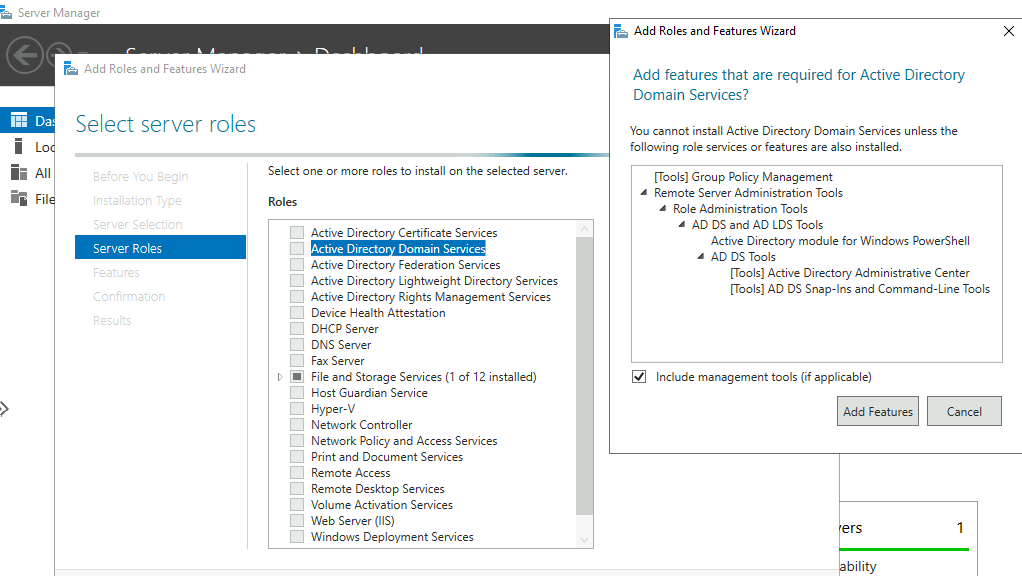


### DEMO

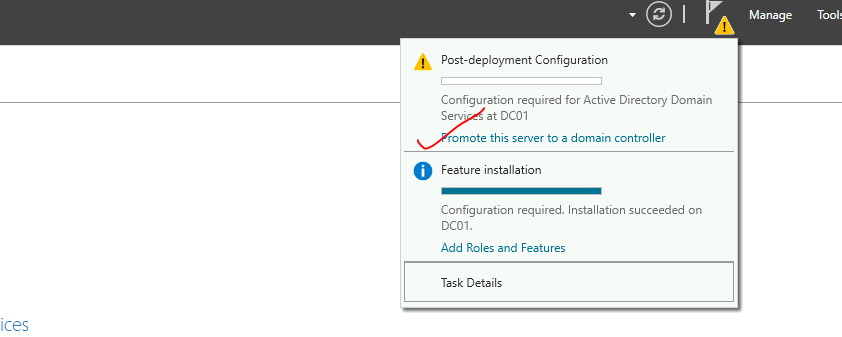
* In the below example
  + We will set up a Domain controller server
  + Create an user in ADDS , with a custom domain(**avishekhsinha.in**)
  + Sync the user in Azure Active Directory

#### SETTING UP ON PREM DOMAIN CONTROLLER

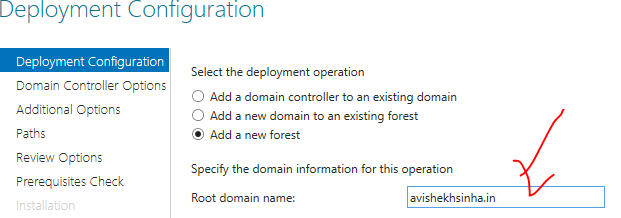
* Step 1: Create a Windows VM (Note ADDS are only supported for Windows) – Lets consider it as server a on-prem.
* Step 2: Install ADDS. Go to Server Manager🡪Roles 🡪 ADDS



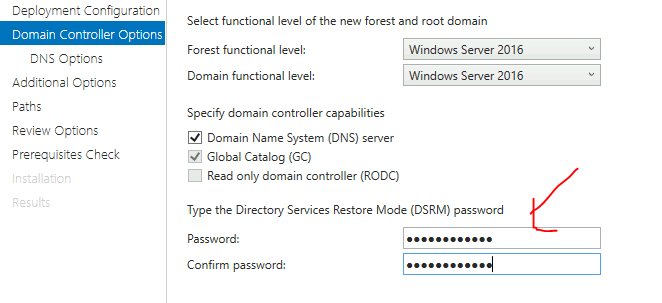
Step 3: Promote the Server to a domain controller.

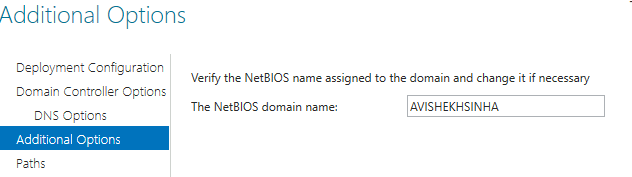


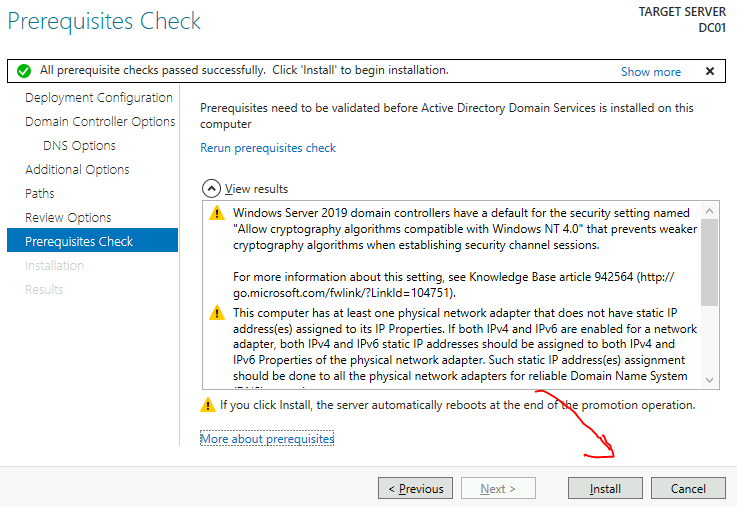
Step 4: Add a New Forest (it has a domain associated with it)



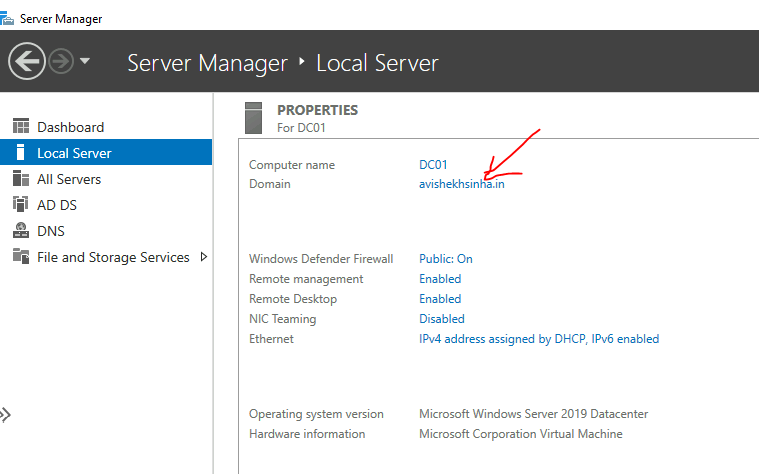
Provide a DSRM Password



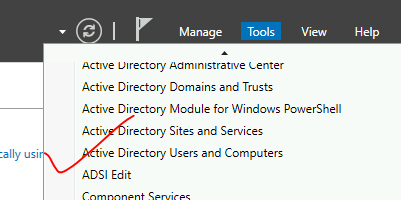


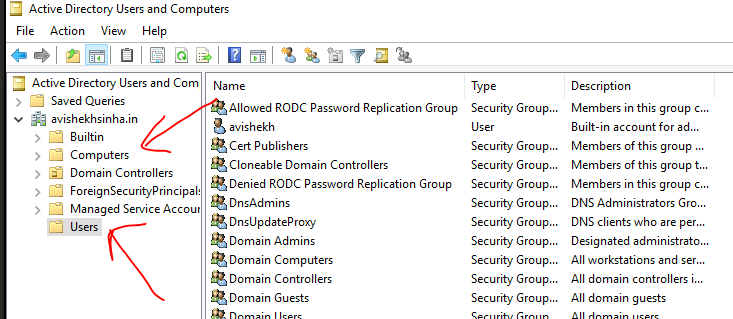


* After DC promotion the Server will restart
* The FQDN of the DC Server will be : DC01.avishekhsinha.in

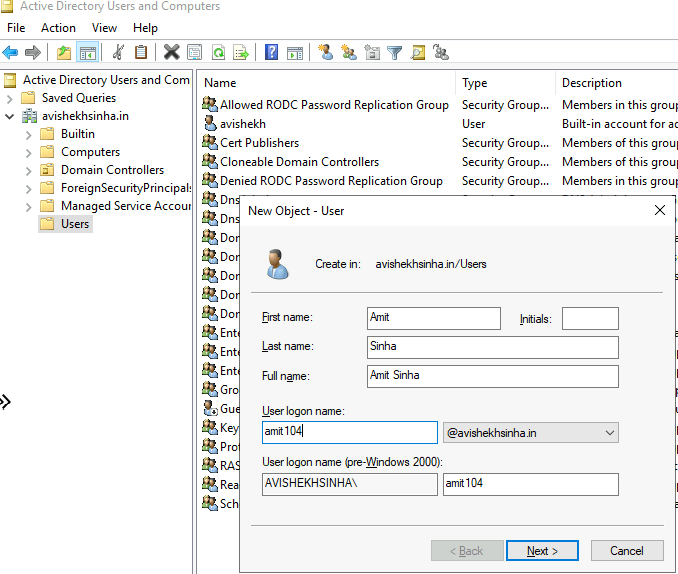


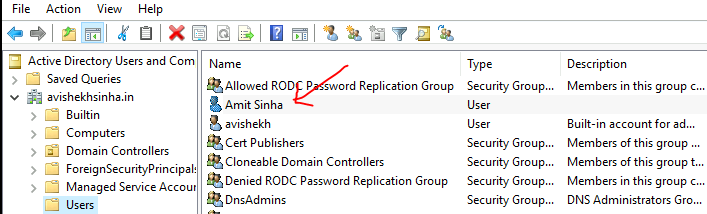
Step 5: Add users to ADDS. In the Server Manager 🡪 Tools 🡪 Active Directory users and Computer





* All the connected machine (individual or server will appear in Computers Section)
* All the new user will appear in “Users” section. Lets Add a new user

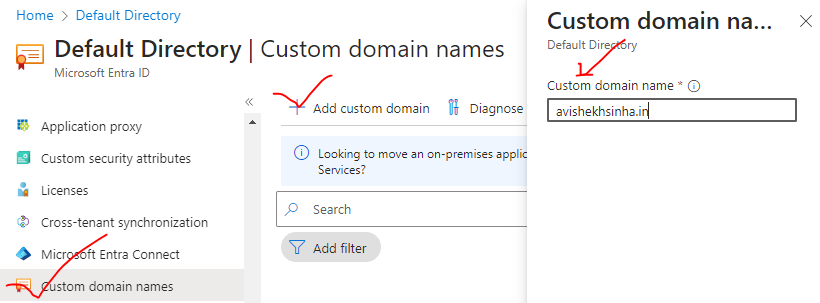




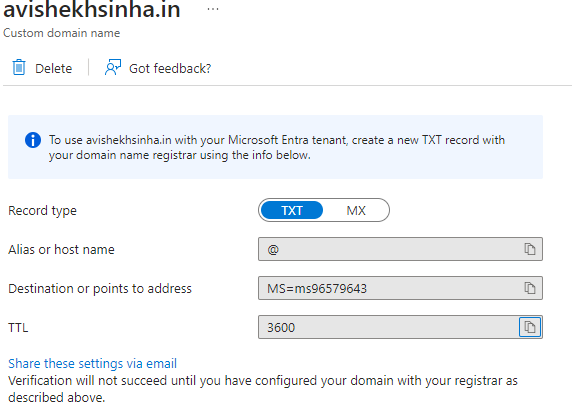
#### SETTING UP AZURE ACTIVE DIRECTORY

##### ADD AND VERIFY CUSTOM DOMAIN

* Add a custom domain name in Azure AD- matching the custom domain in AD forest



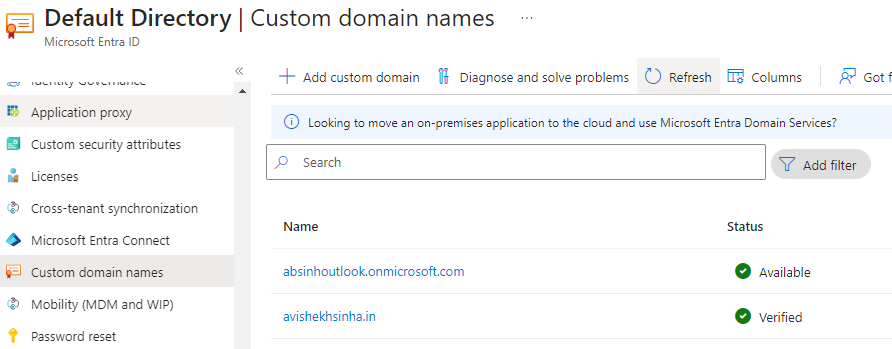
VERIFY THE CUSTOM DOMAIN



TXT RECORD ADDED DOMAIN REGISTAR – ZONE FILE

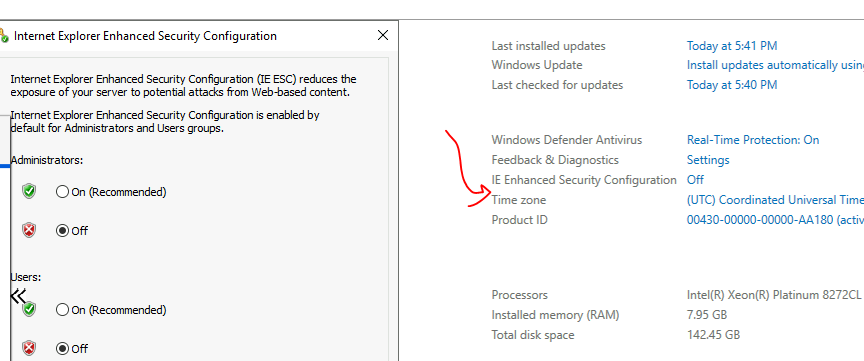


DOMAIN VERIFIED



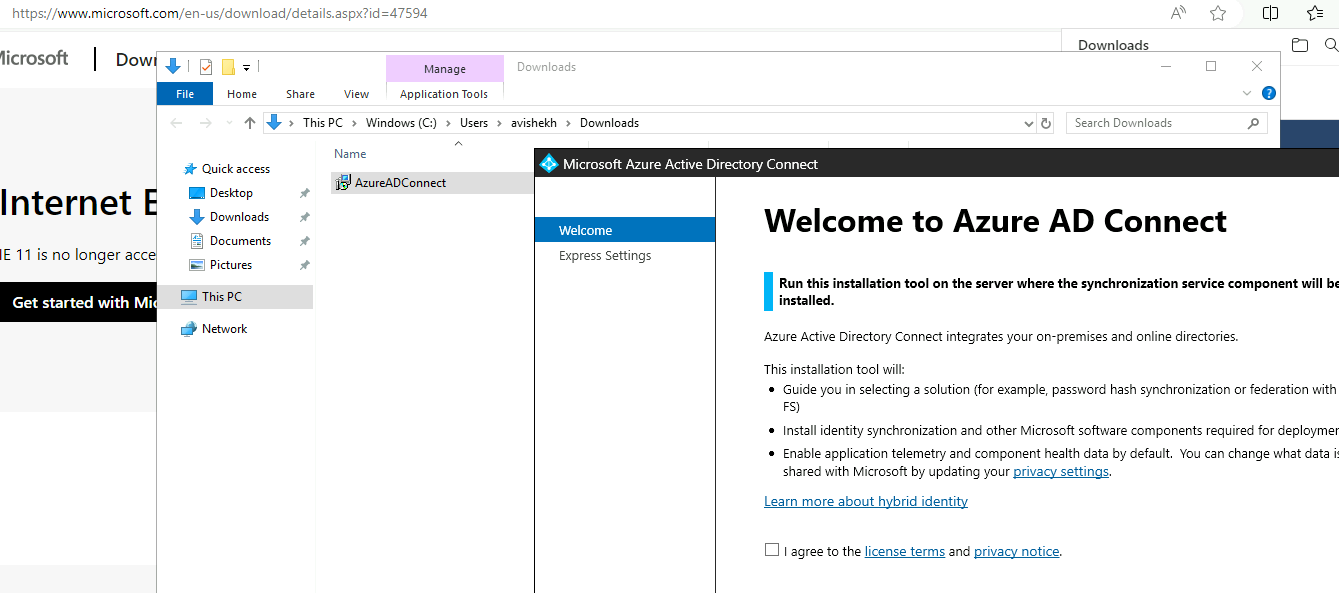
##### SYNC THE ON PREM USERS TO AD

|  |  |
| --- | --- |
|  | DOWNLOAD THE AD CONNECT SYNC AGENT IN THE ON PRE DOMAIN CONTROLLER  Note : Turn off the IE enhanced Security Configuration |

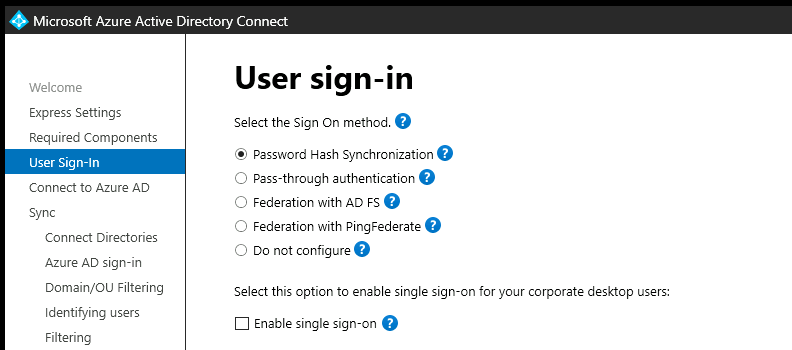


###### INSTALL AZURE AD CONNECT

Azure Active Directory (Azure AD) Connect is a tool that enables synchronization of on-premises directories with Azure AD



PROVIDE THE SIGN IN METHOD FOR USER

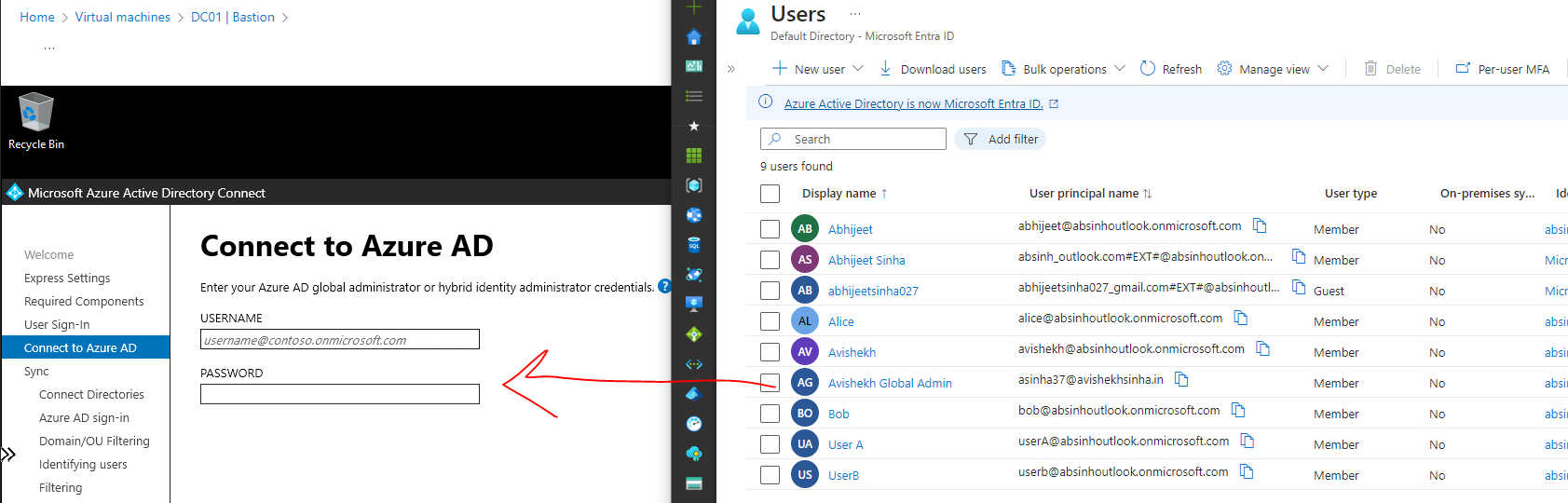


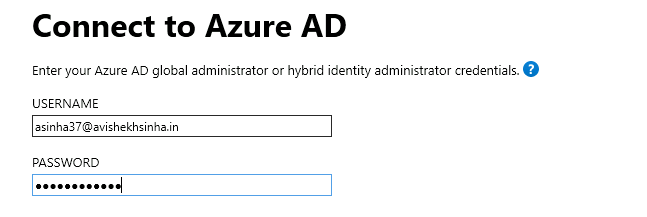
Azure Active Directory (Azure AD) Connect provides various user sign-in methods to allow users to authenticate and access resources in Azure and other integrated applications.

1. PASSWORD HASH SYNCHRONIZATION (PHS)
   1. This method synchronizes user passwords from on-premises Active Directory to Azure AD.
   2. When users sign in to Azure or other integrated applications, their passwords are verified against the hashed passwords stored in Azure AD.
2. PASS-THROUGH AUTHENTICATION (PTA)
   1. With PTA, user passwords are validated directly against on-premises Active Directory.
   2. When users sign in, their passwords are securely passed to the on-premises Active Directory for verification, without being stored or synced to Azure AD.
3. FEDERATION WITH ACTIVE DIRECTORY FEDERATION SERVICES (AD FS)
   1. This method uses AD FS to establish trust between the on-premises Active Directory and Azure AD.
   2. Users authenticate against the on-premises AD FS infrastructure, which then issues security tokens to Azure AD for access to resources.

PROVIDE THE CREDENTIAL OF GLOBAL ADMIN IN AZURE AD

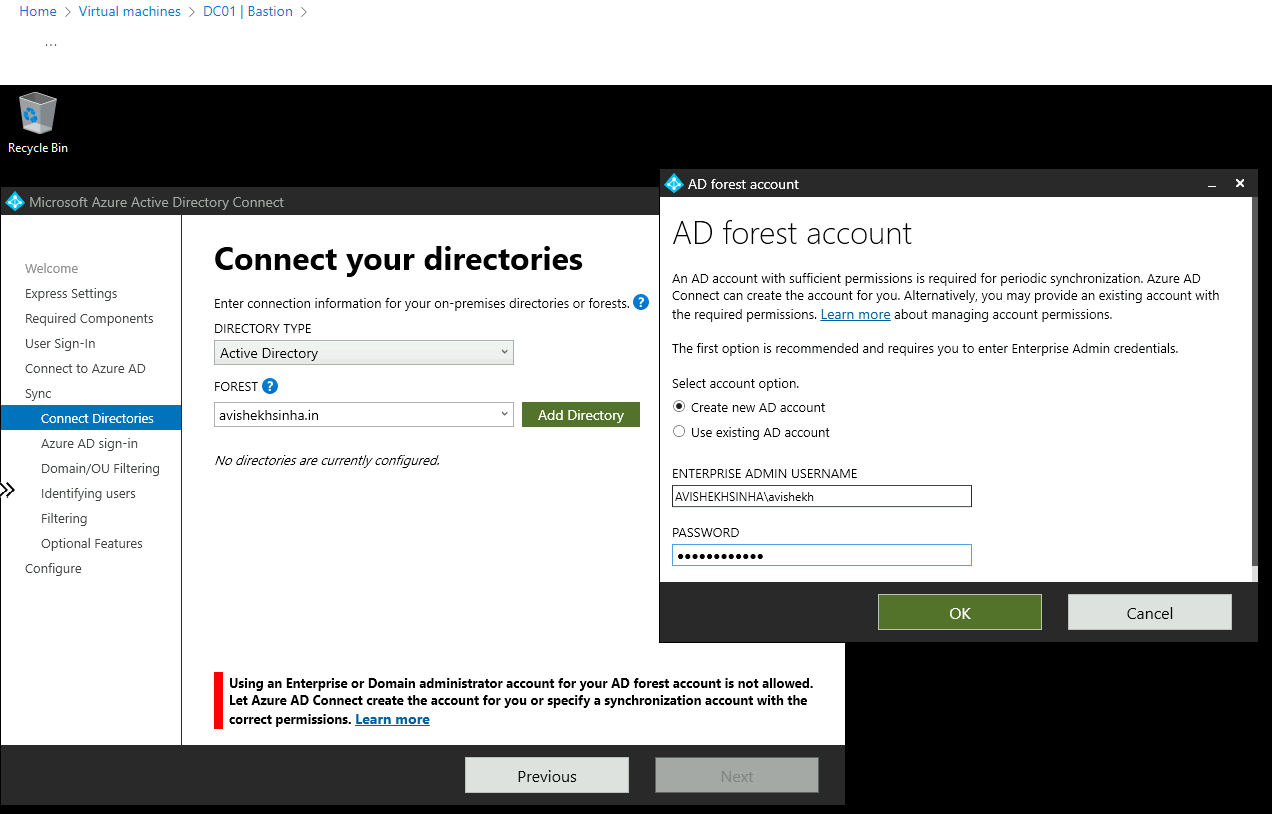
* If no global admin user is present – create a new user with a Permission of “Global Administrator”

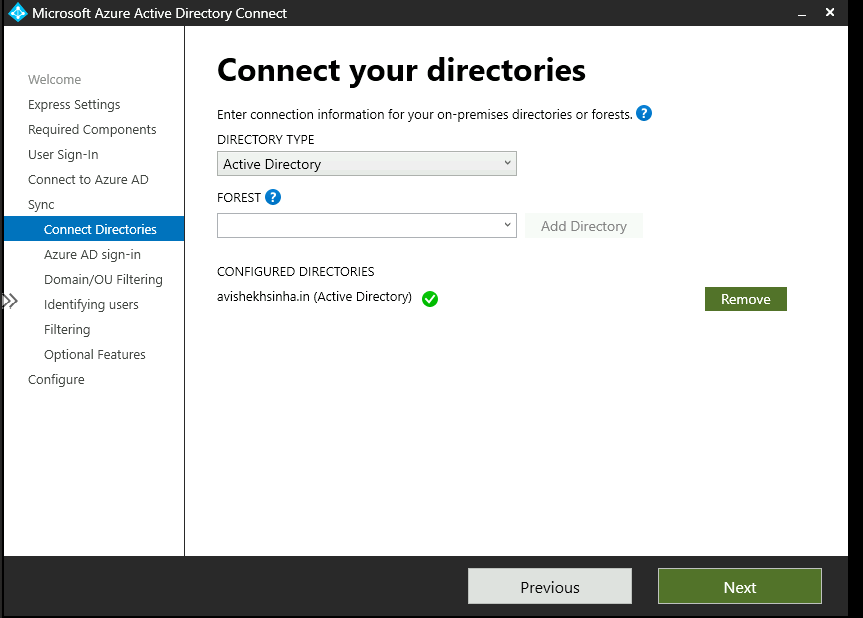


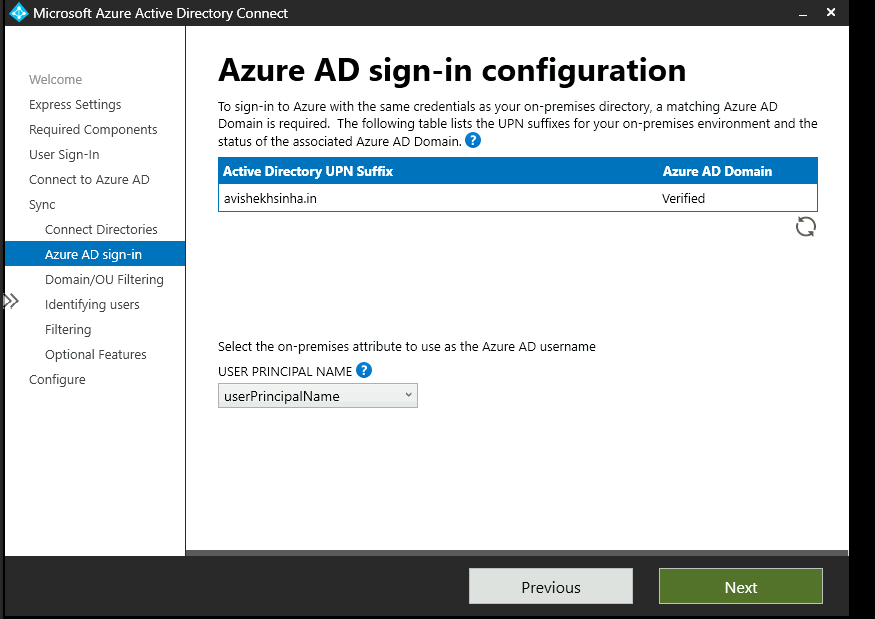


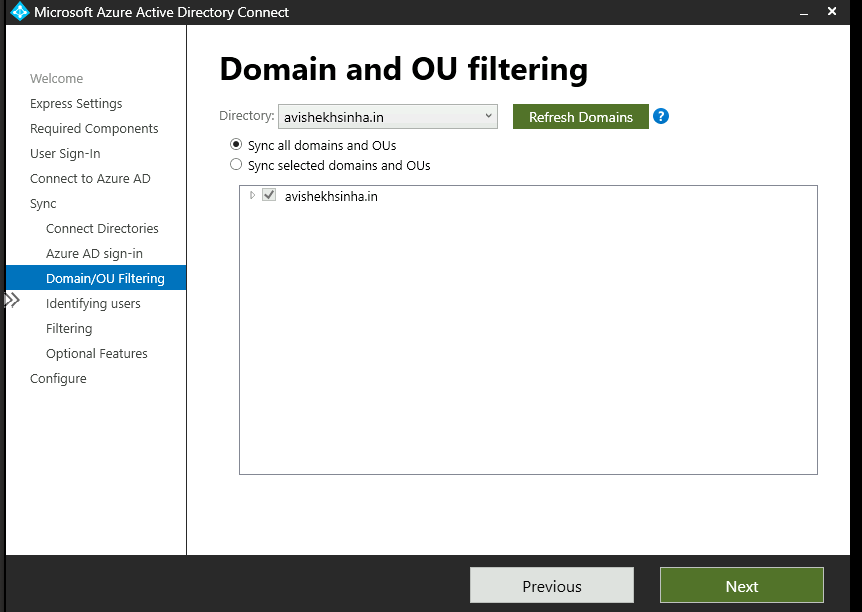
PROVIDE THE CREDENTIAL OF DOMAIN CONTROLLER SERVER

* This will be the credential of the Windows VM – configured while creating the VM



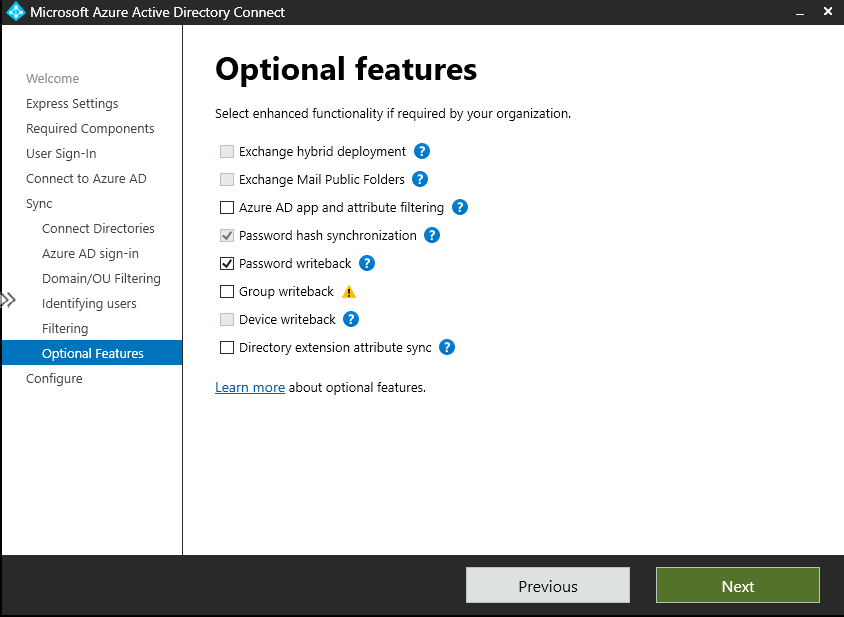


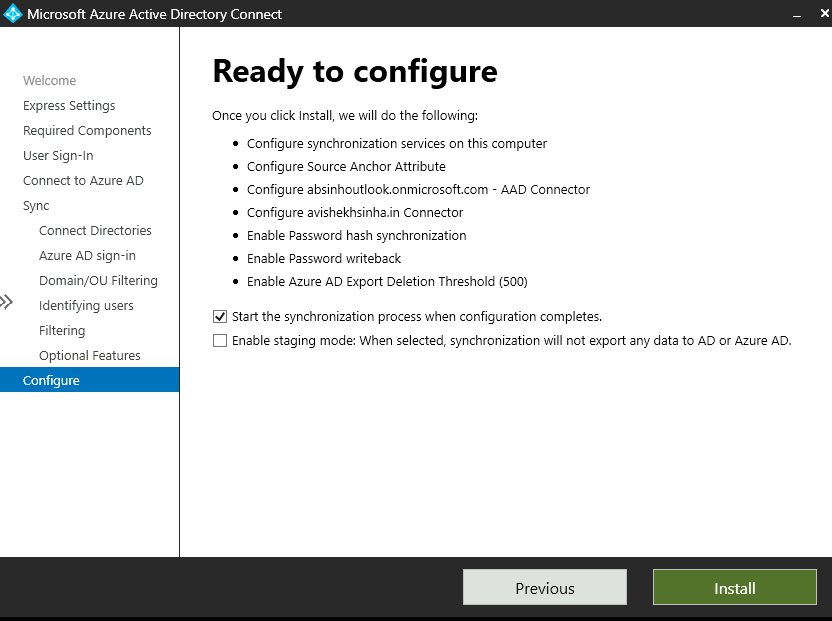


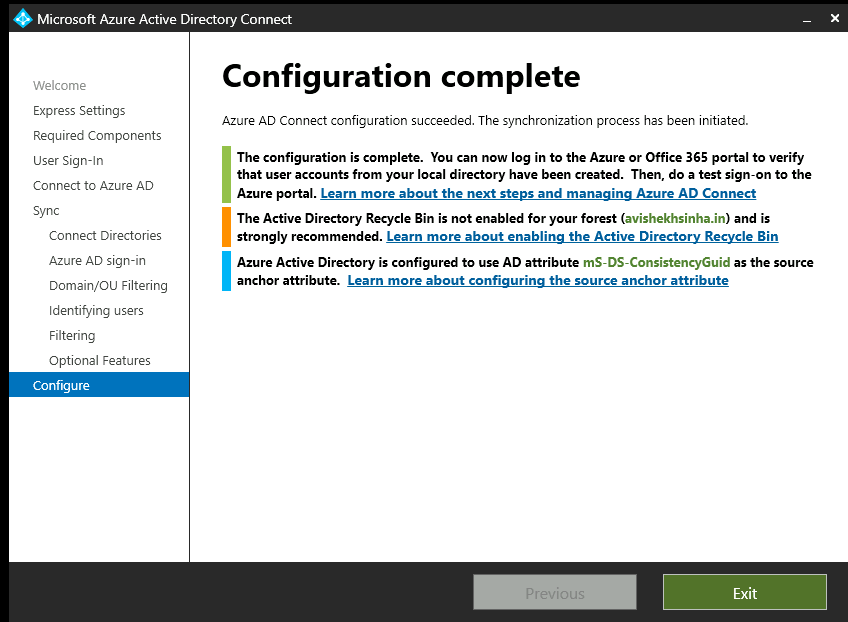


ENABLE THE PASSWORD WRITE BACK OPTION

* Password Writeback is a feature of Azure Active Directory (Azure AD) that allows users to change or reset their passwords in the cloud and have those changes written back to the on-premises Active Directory (AD) environment.
* This feature is particularly useful for organizations that have deployed Azure AD Connect to synchronize their on-premises AD with Azure AD.
* With Password Writeback enabled, users can utilize self-service password reset (SSPR) capabilities in Azure AD to change or reset their passwords through various methods, such as web portals, mobile apps, or even through the Windows login screen. When a password change or reset is initiated in Azure AD, the new password is securely transmitted back to the on-premises AD environment and updated accordingly.







THE USER HAS BEEN SYCHRONIZED IN AZURE AD

