Table of Contents

[AZURE ACTIVE DIRECTORY 2](#_Toc122638727)

[ON PREM VERSUS AZURE AD 2](#_Toc122638728)

[AD TERMINOLOGIES 2](#_Toc122638729)

[SUBSCRIPTION AND AD 3](#_Toc122638730)

[CONFIGURING THE TRUST BETWEEN AD AND SUBSCRIPTION 3](#_Toc122638731)

[TYPES OF PERMISSIONS IN AZURE 4](#_Toc122638732)

[A. RBAC ROLES (IAM – IDENTITY AND ACCESS MANAGEMENT) 5](#_Toc122638733)

[B. DIRECTORY ROLES (AD ROLES) 5](#_Toc122638734)

[CREATING USER 5](#_Toc122638735)

[ROLE BASED ACCESS CONTROL (RBAC) 8](#_Toc122638736)

[ROLE BASED ASSIGNMENT – READER ROLE 8](#_Toc122638737)

[ROLE BASED ASSIGNMENT – RESOURCE GROUP LEVEL 10](#_Toc122638738)

[ROLE BASED ASSIGNMENT – SUBSCRIPTION LEVEL 10](#_Toc122638739)

[ROLE BASED ASSIGNMENT – CONTRIBUTOR LEVEL 10](#_Toc122638740)

[ROLE BASED ASSIGNMENT – USER ACCESS ADMIN ROLE 11](#_Toc122638741)

[CUSTOM ROLES 11](#_Toc122638742)

[AZURE AD ROLES 13](#_Toc122638743)

[CREATING USER GROUP 13](#_Toc122638744)

[CREATING DYNAMIC USER GROUP 14](#_Toc122638745)

[JOINING A VM TO AD 14](#_Toc122638746)

[MULTIFACTOR AUTHENTICATION 16](#_Toc122638747)

[SETTING UP PER USER MFA 16](#_Toc122638748)

[ADMINISTRATIVE UNITS 16](#_Toc122638749)

[LAB -ADMINISTRATIVE UNITS 17](#_Toc122638750)

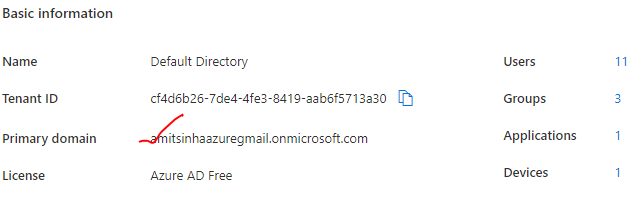
# AZURE ACTIVE DIRECTORY

* It an identity provider in Azure. With the help of active directory, we can create identities such as users.
* With the help of role-based access control, we can give permissions to these users over resources as part of Azure subscription.
* The key benefit of Azure Active Directory is that we don’t need to implement any infrastructure.
* Using active directory, we can CREATE USERS, USER GROUPS

## 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 verifiction. |

**PRIMARY DOMAIN NAME**



## 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 s 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.

## 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. |

## 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 go out and 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 | | |
|  | |  |

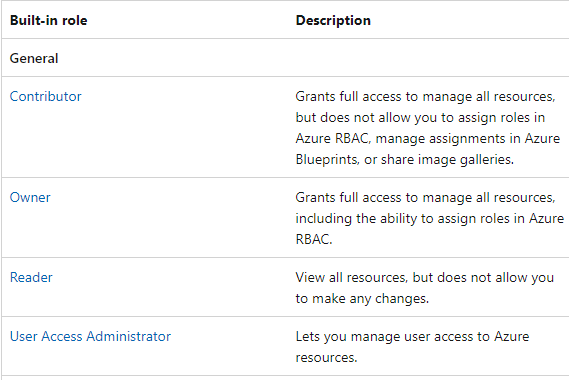
## TYPES OF PERMISSIONS IN AZURE

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

* The RBAC roles are given to the user to access the resources in Azure. It can be given on resource level, resource group level or subscription level.

|  |  |
| --- | --- |
| **RBAC TERMINOLOGIES** | |
| SCOPE | The subject on which the RBAC permission are applied. It can be a resource, Resource group and Subscription |
| 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. |

##### BASIC BUILD-IN RBACK ROLES

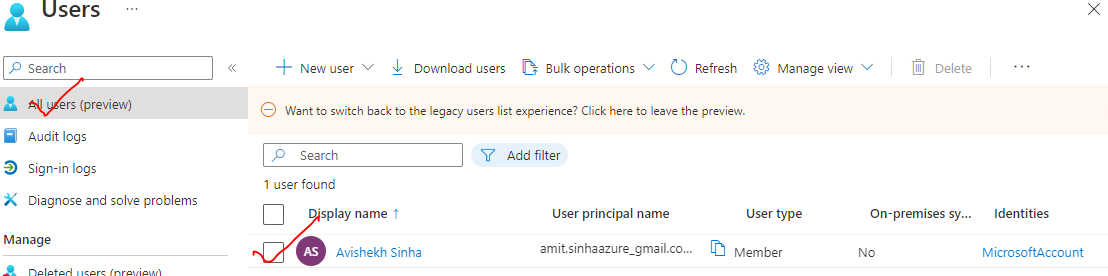


### DIRECTORY ROLES (AD ROLES)

* The roles are for managing the active directory itself. Note – these permissions are different from RBAC permission. Even if a user having owner permission (RBAC permission) – will not be able to manage Azure active directory. They need to have directory permission for such Active directory management tasks.
* Example of directory roles are *Global Admin / Global Reader*
* <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

## CREATING USER

* **When a user is created in azure- user can able to login to azure .**
* **While creating a user – user can be assigned with directory pernission (show 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. The Access to the user must be given explicitly |
|  | | **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. | |

## ROLE BASED ACCESS CONTROL (RBAC)

* When we created a user in Azure Active Directory then the user can be able to log into your account. This step was known as authentication to log into Azure account. But the user, we could not access any resource in the Azure account
* To give access - We must make use of ***role-based access control***. This step gives authorization to the user to access resources as part of the Azure account.

The role-based access can be given at

|  |  |
| --- | --- |
| RESOURCE LEVEL | Example - if we had a storage account, we could get access on to that user on to the storage account |
| RESOURCE GROUP LEVEL | This will then ensure that the user has access onto all resources that are part of the resource group. |
| SUBSCRIPTION LEVEL | The user will get access on to all the resource groups and in turn, all the resources that are part of that subscription. |

* 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.

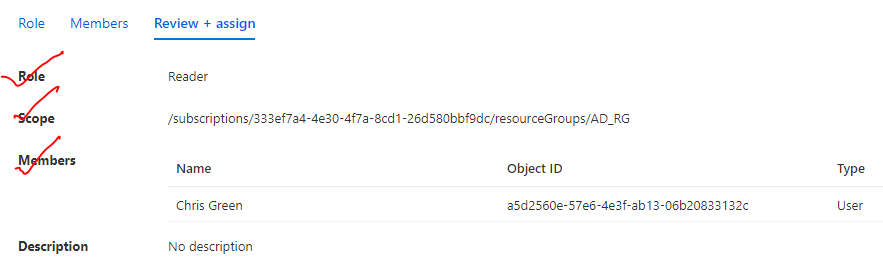
### ROLE BASED ASSIGNMENT – READER ROLE

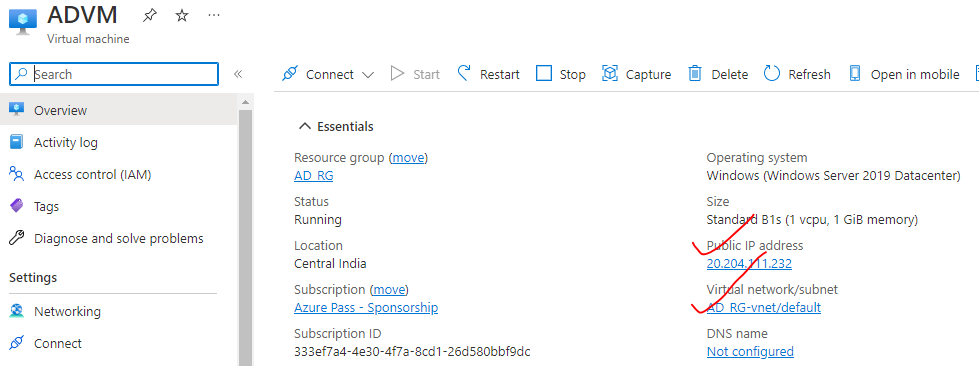
* Example – if we want to give access the Reader permission on VM level (Resource level)

|  |  |  |
| --- | --- | --- |
|  | * *Navigate to VM 🡪 IAM🡪 Add 🡪 Add Role Assignment* | |
|  | | * Select member to whom we want to give access to. * Review and Assign |
| * The VM(resource) has a user with a reader role | | |
| * Note - The user will have read permission on the VM but no access to public IP , VNET and DNS – as they are separate resources in Azure- which needs a separate role assignment. | | |

### ROLE BASED ASSIGNMENT – RESOURCE GROUP LEVEL

* Navigate to resource group and assign the permission (reader permission for this example) on the resource
* If we assign a role at a resource group level, it will apply to all of the resources within the resource group.





### ROLE BASED ASSIGNMENT – SUBSCRIPTION LEVEL

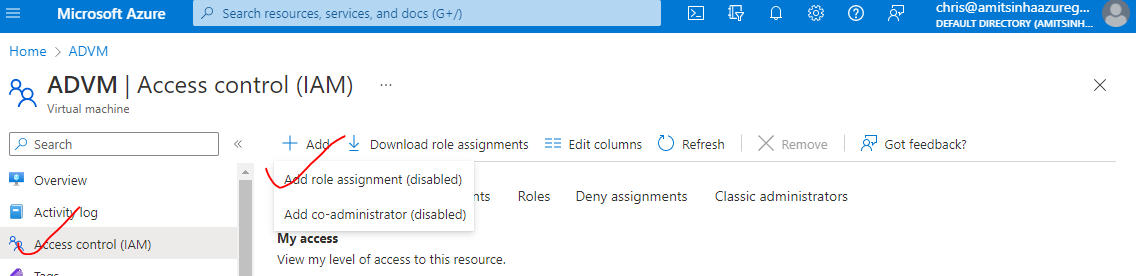
* If we give access at the subscription level, then the role gets applied to all resource groups that are part of that subscription.

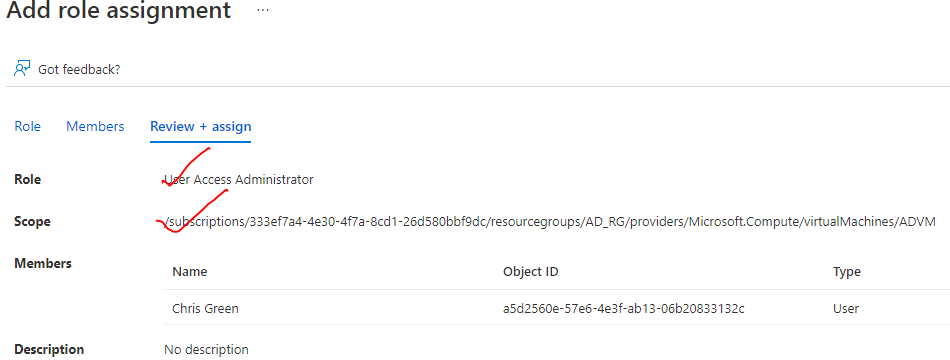
### ROLE BASED ASSIGNMENT – CONTRIBUTOR LEVEL

|  |  |
| --- | --- |
| 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.



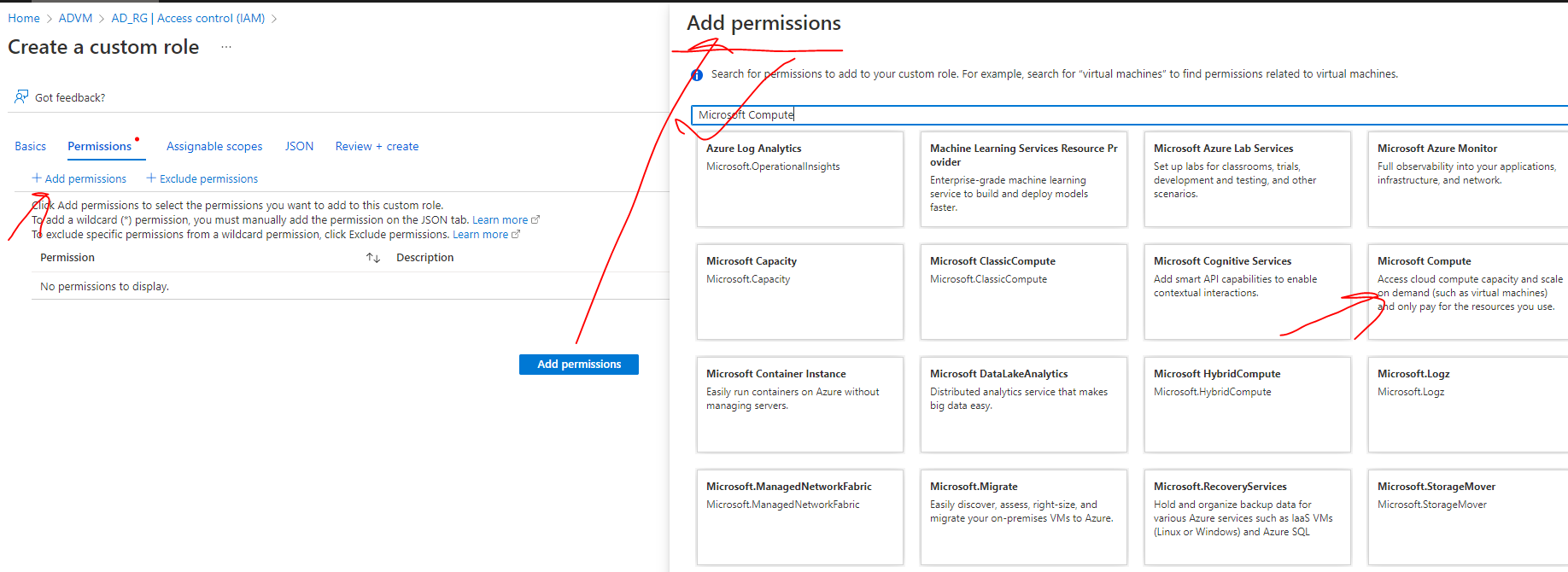


### CUSTOM ROLES

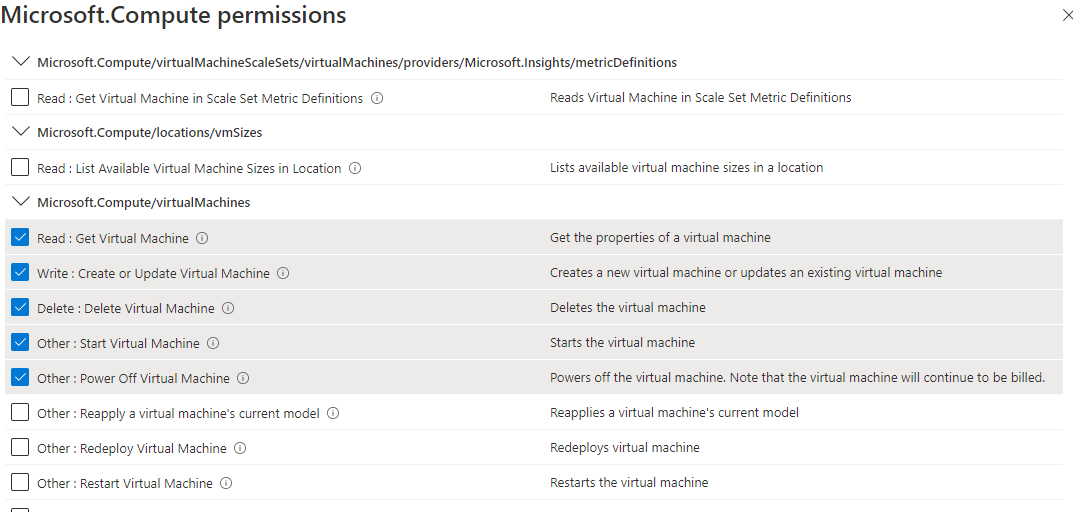
* Apart from build in roles -we can create custom roles too. For example, to assign a custom role on resource group level.

|  |  |
| --- | --- |
|  | * Navigate to IAM🡪 Add custom rule * While creating a custom role – we have an option to   + Clone a role   + Start from scratch   + Start from JSON |
|  | * 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 |

## 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>

### GRANTING AD ROLES

|  |  |
| --- | --- |
|  | * 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, |
|  | |

## 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 | |

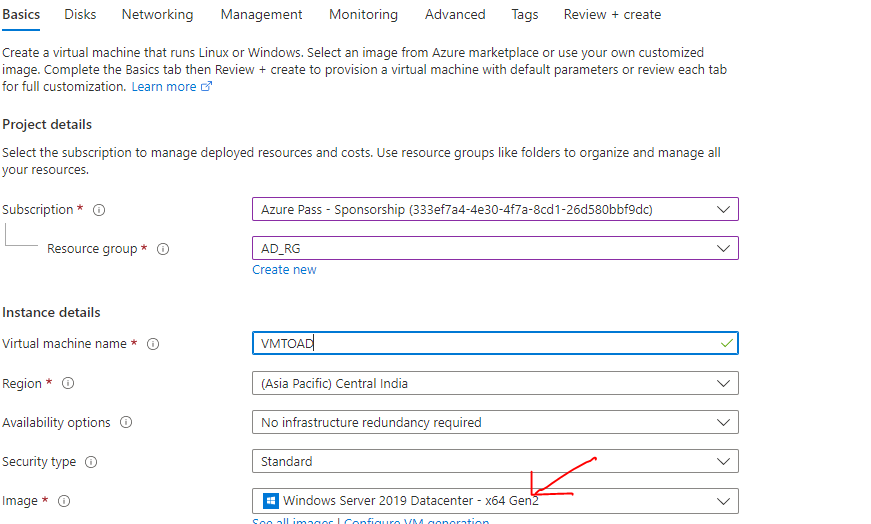
### CREATING DYNAMIC USER GROUP

* In a user group we must manually assign members onto a group. But you also have this facility of dynamic groups wherein users can automatically be added onto a group.

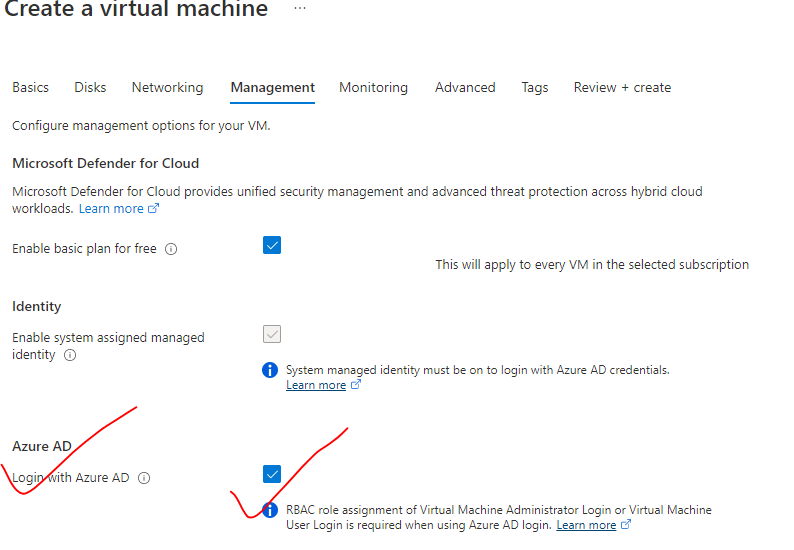
## JOINING A VM TO AD

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

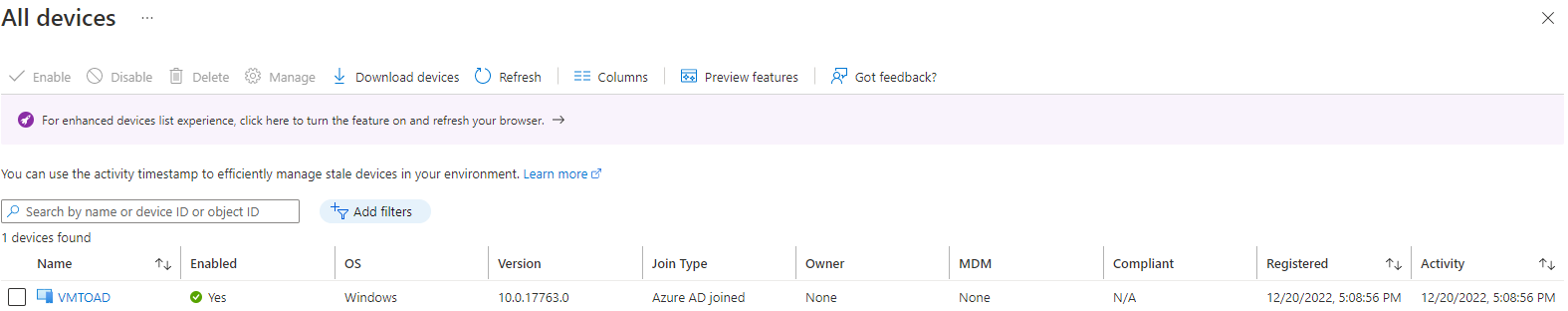
Step 1: Provision a Window 10 / Server VM



Step 2: Register the device with AD



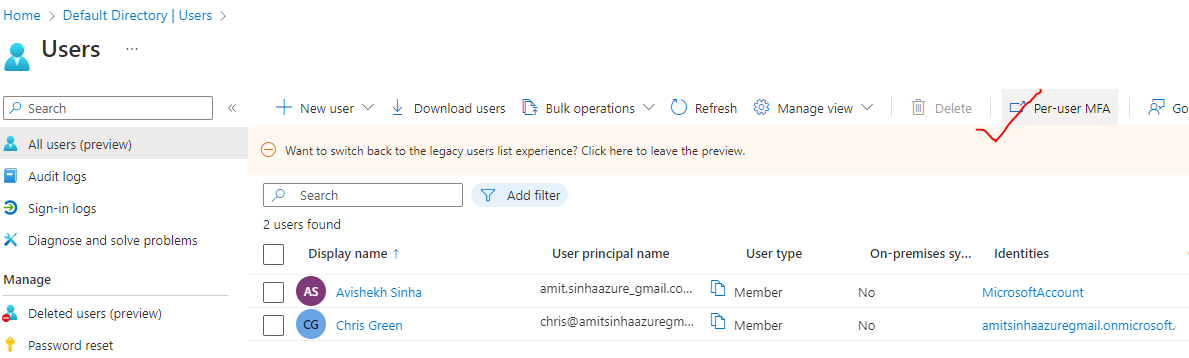
* To check the connected device – Active Directory 🡪 Devices



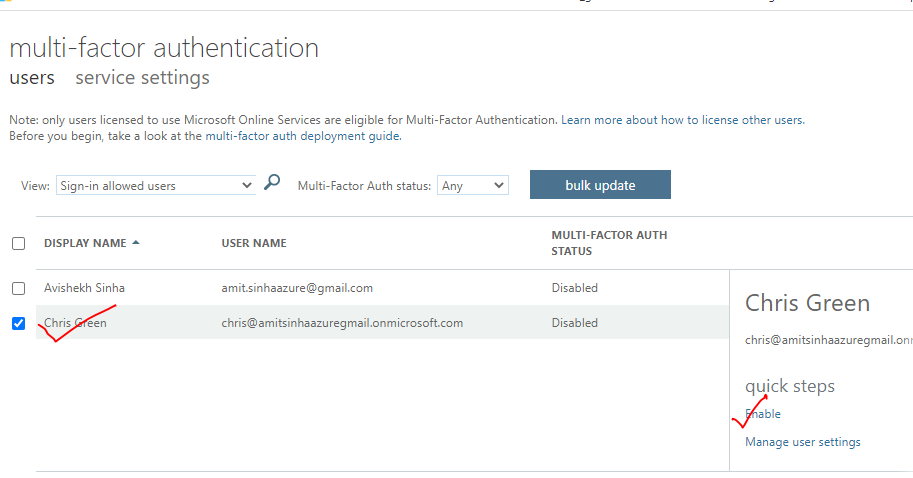
## MULTIFACTOR AUTHENTICATION

### SETTING UP PER USER MFA

* Go to Active directory 🡪 Per user MFA



* Select user 🡪 Enable

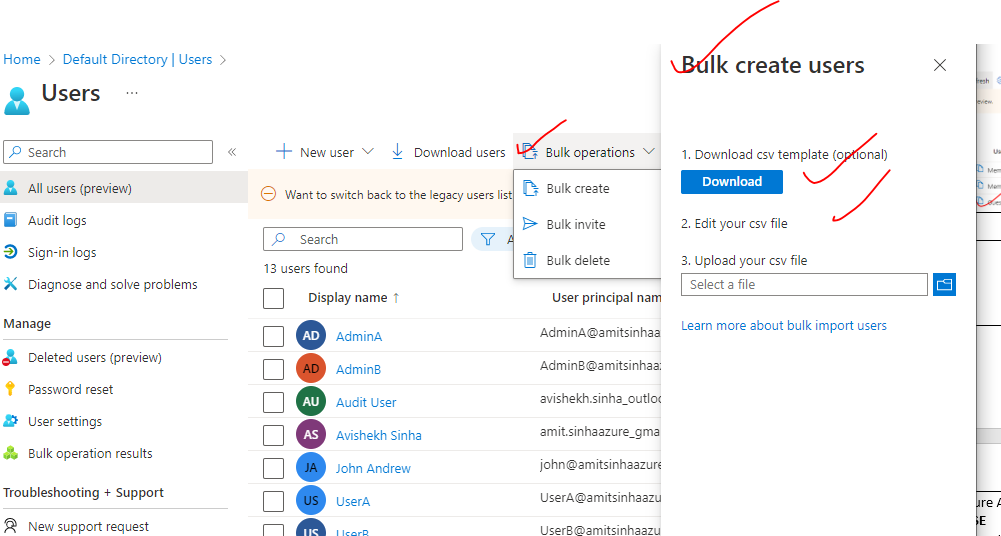


## INVITING GUEST USER

|  |  |
| --- | --- |
|  | * Normally we invite external users who are external to the organization or consultants who just need access to resources for a brief period * In the below example – lets invite the user having outlook.com account. * Go to Active directory 🡪 Users 🡪 Invite User * The user will receive an email to accept the invitation * 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>



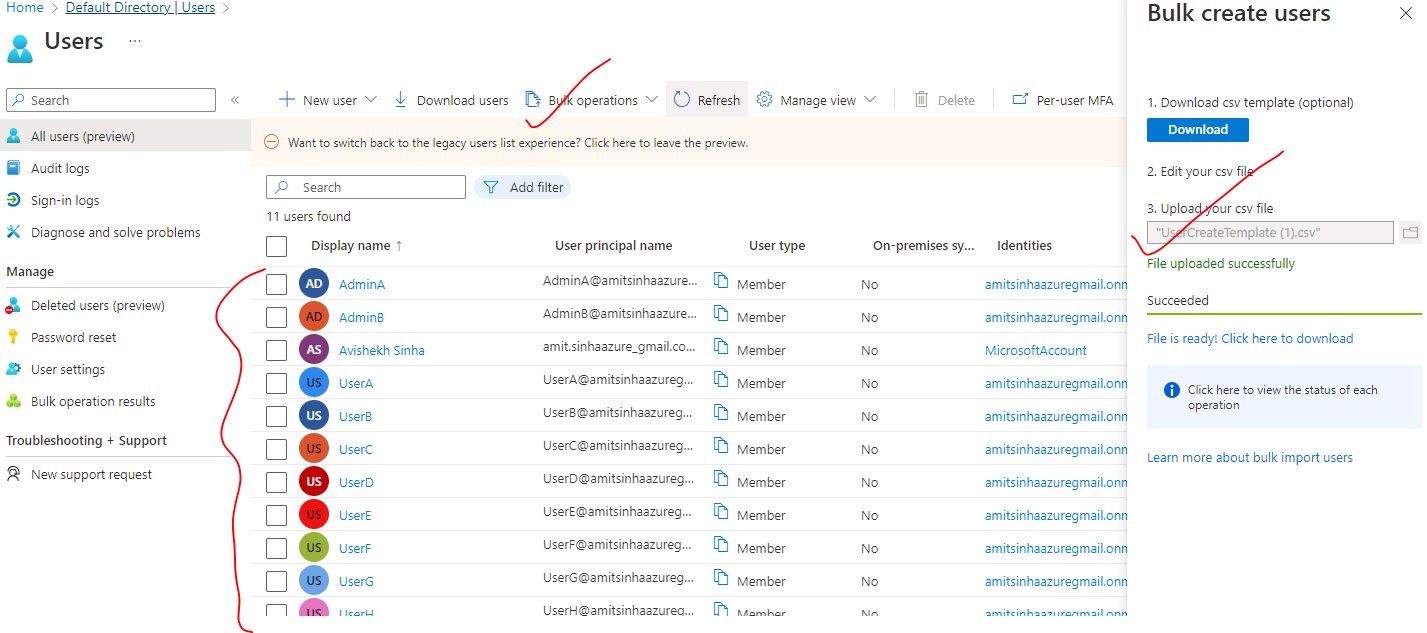
## ADMINISTRATIVE UNITS

|  |  |
| --- | --- |
|  | * In Azure AD we create uses and assign roles/permission to them   **USER 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

|  |  |
| --- | --- |
|  | * We are going to have two users who are going to be part of an administrative unit. * We are also going to have another user known as admin that is going to behave as the user administrator for the administrative unit. * We'll have two more users that are going to be part of a group(logistic-grp). * That group is going to be 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*



**Step 2:** Create the user groups

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

**Step 3:** Create 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.