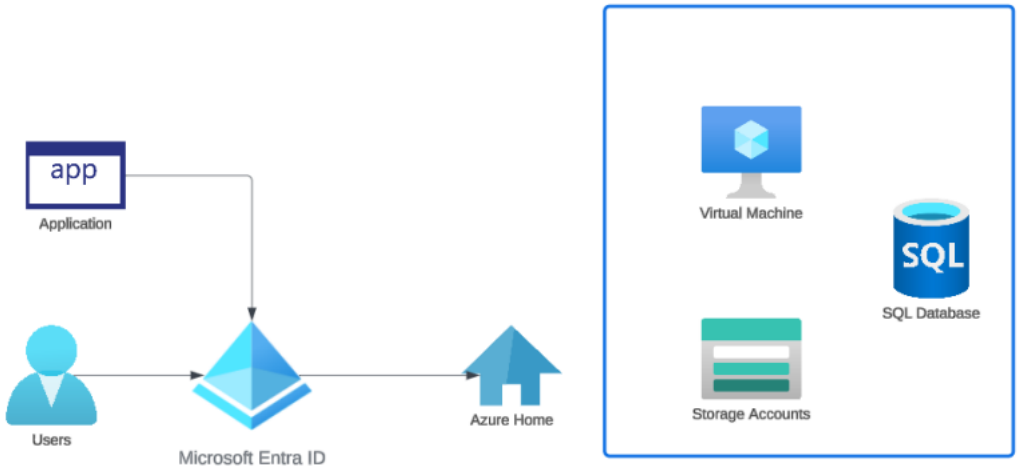
Manage Azure Identities and Governance

1. Microsoft Entra ID :

   This is a cloud based identity and access management service. This identity service can be used for azure, Microsoft 365 and other software-as-a-service application. Application can be linked to identity and be given access accordingly.

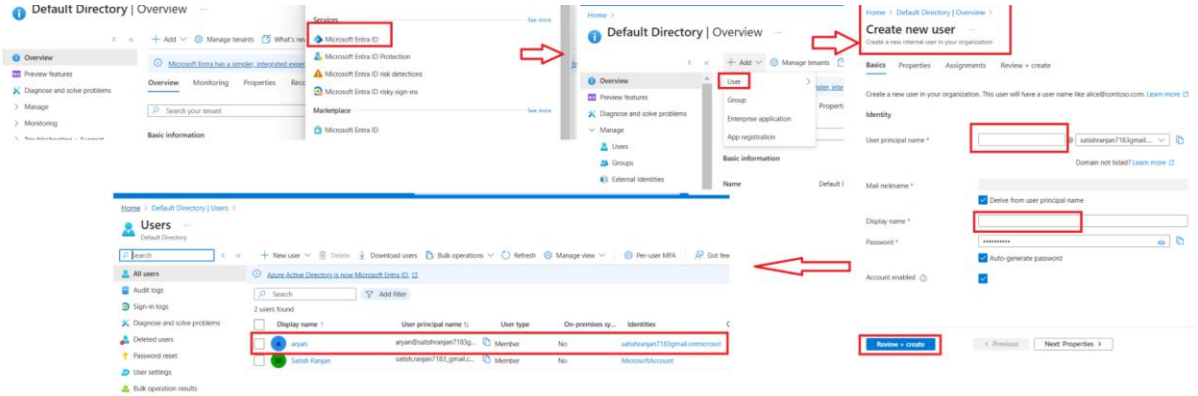
   We can define users in Microsoft Entra ID



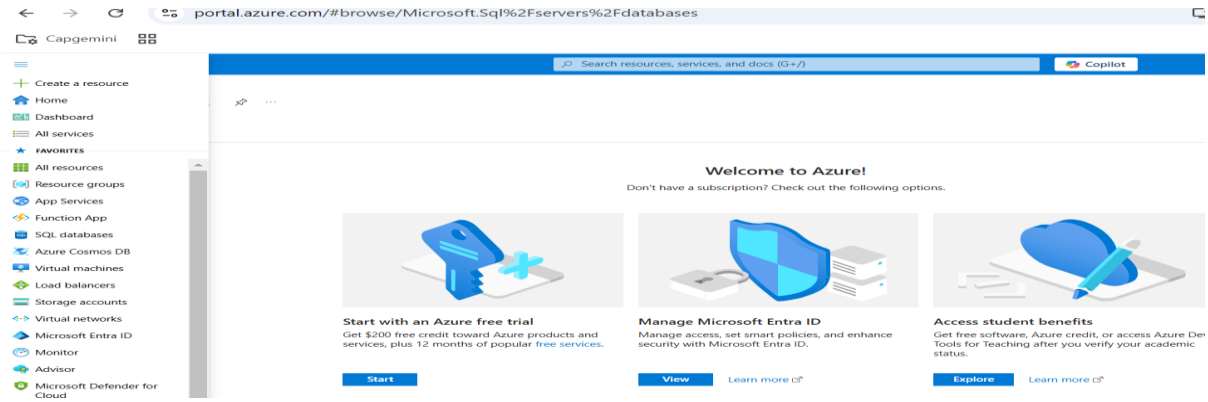
   Authentication: In Authentication, identity of the users are verified

   Authorization: In Authorization, permission are checked for the users.

2. Creating a User in Microsoft Entra ID



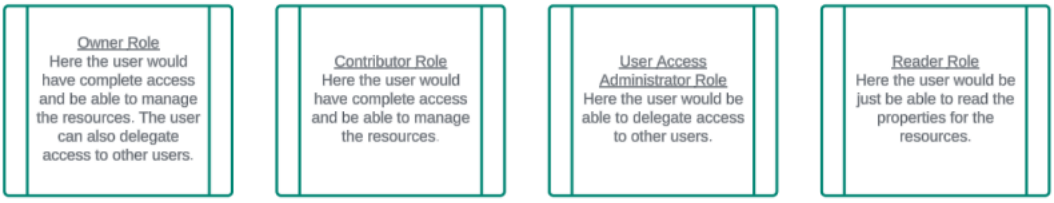
   Note: Only user have access to login in Azure, but they are not able to access azure resources, So for access azure resources, need to provide RBAC permission at resource level, resource group level, subscription level.



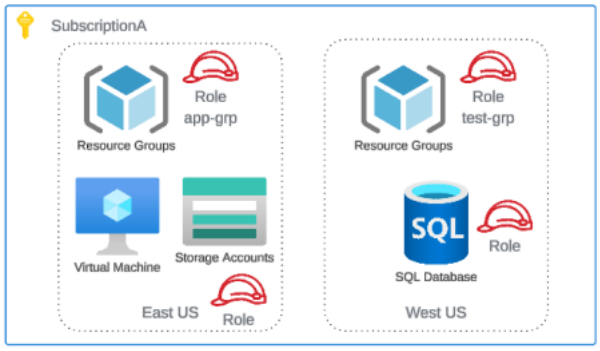
3. Role Based Access Control (RBAC) :

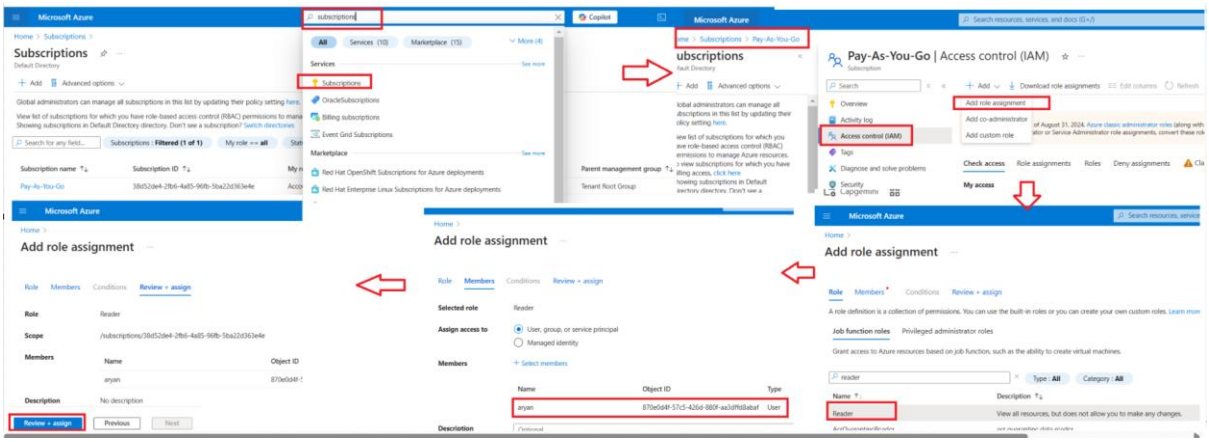
   Role-Based Access Control (RBAC) in Azure is a system for managing access to Azure resources by assigning roles to users, groups, and services. It enables you to control who can perform actions on specific resources in your Azure environment, and what actions they can perform.

   - ✓ We can assign different role to a user
   - ✓ There are many in-build roles.
   - ✓ We can define our own customer roles.
   - ✓ We can assign a role at the subscription level
   - ✓ We can assign a role at the resource group level
   - ✓ We can assign a role at the resource level
   - ✓ Simply Role means Permission, Permission of user to access specific resources.



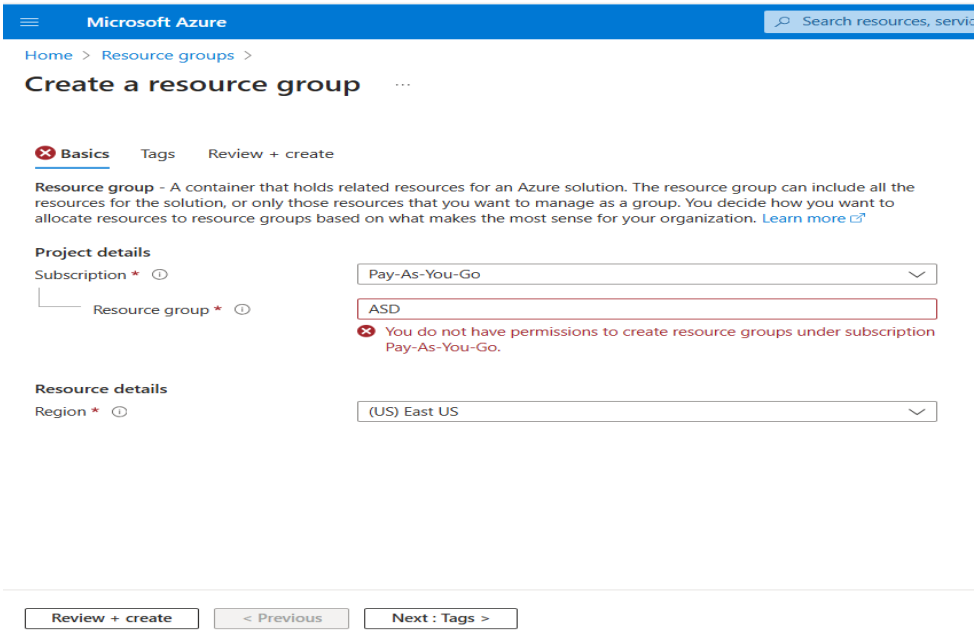
4. RBAC at Subscription level



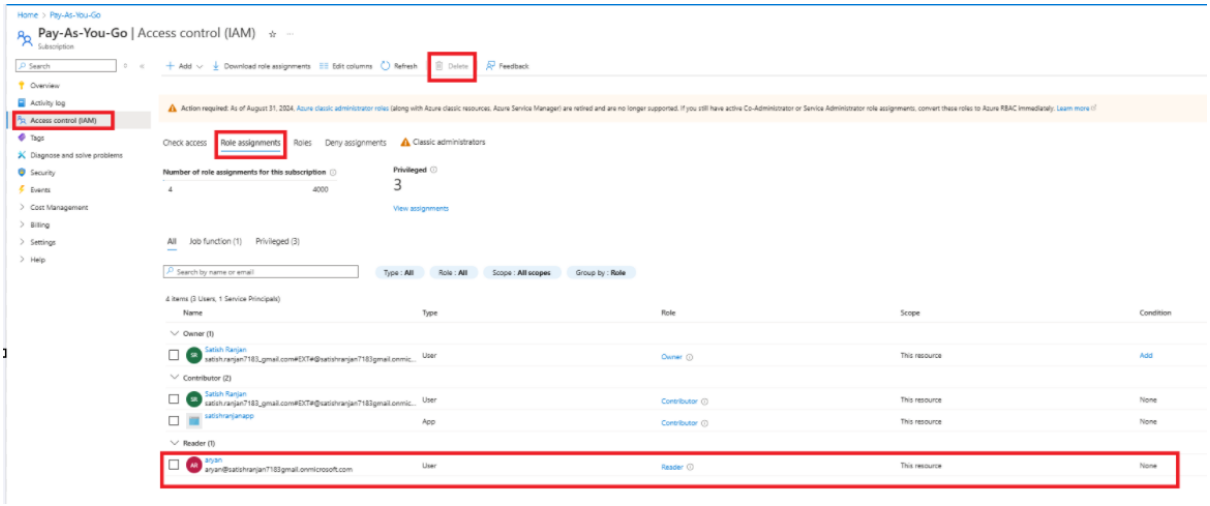


Now once user get subscription level Reader permission, then he can see all resources which already created in their account, user are not able to crate any resources due to reader permission issue

Capgemini

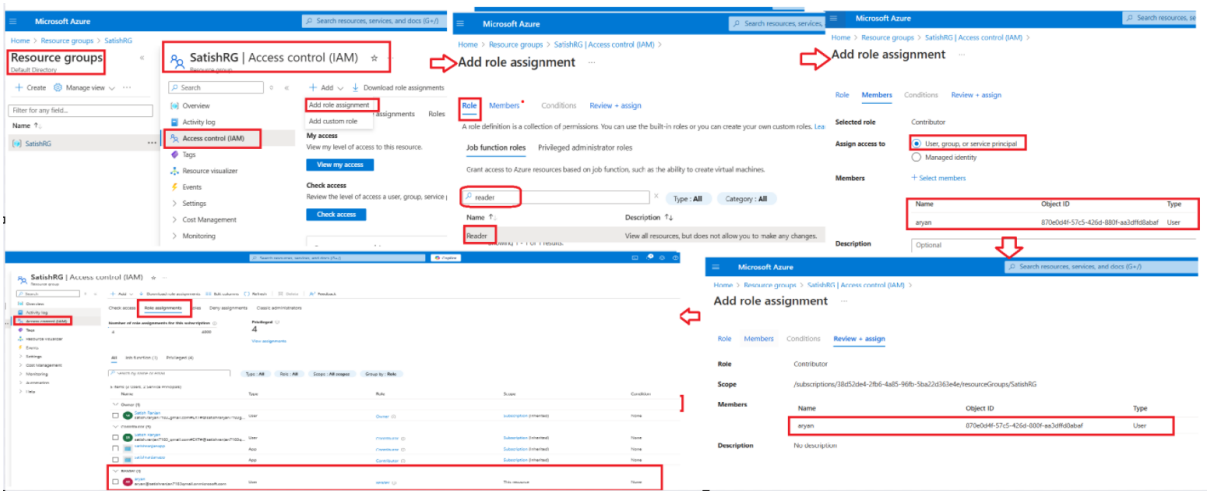


For Deleting Role: from owner account go to IAM-> RoleAssignmene->select username -> delete

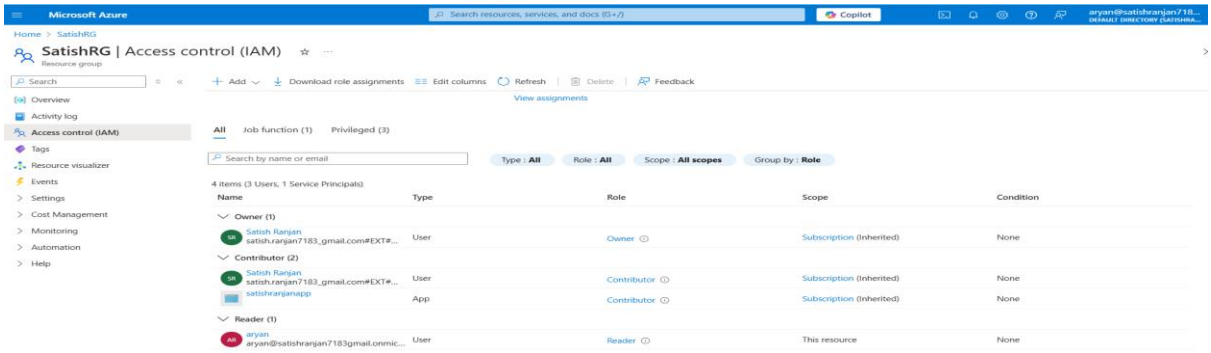


5. RBAC at Resource group Level

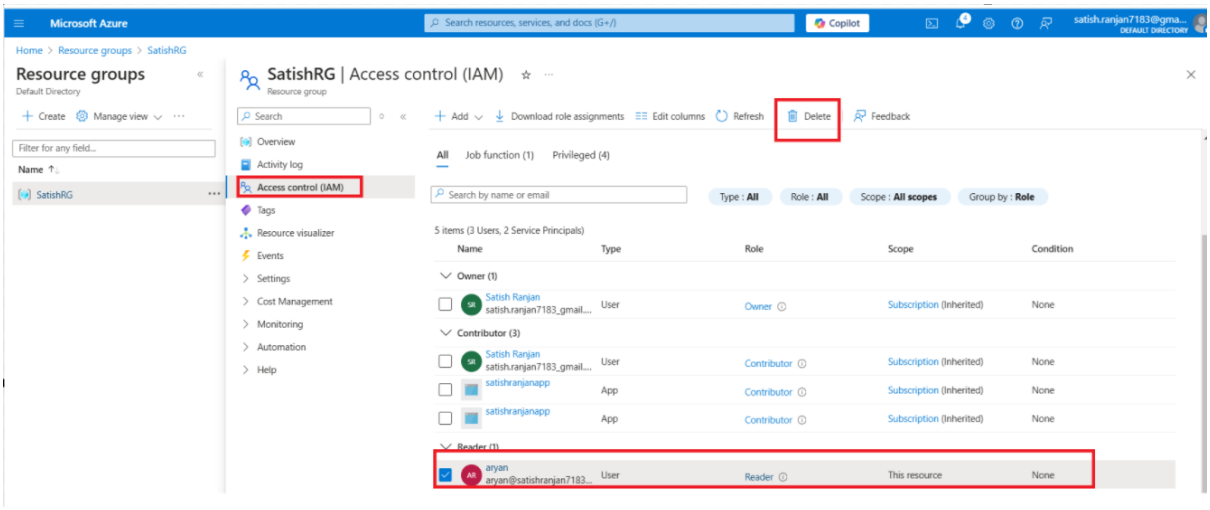
Well now we can view the other resources but can be stop the virtual machine?



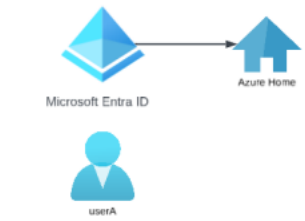
Other resources only they can view the resources, not able to manage or create new resources due to reader permission at resource group level.



For deleting:



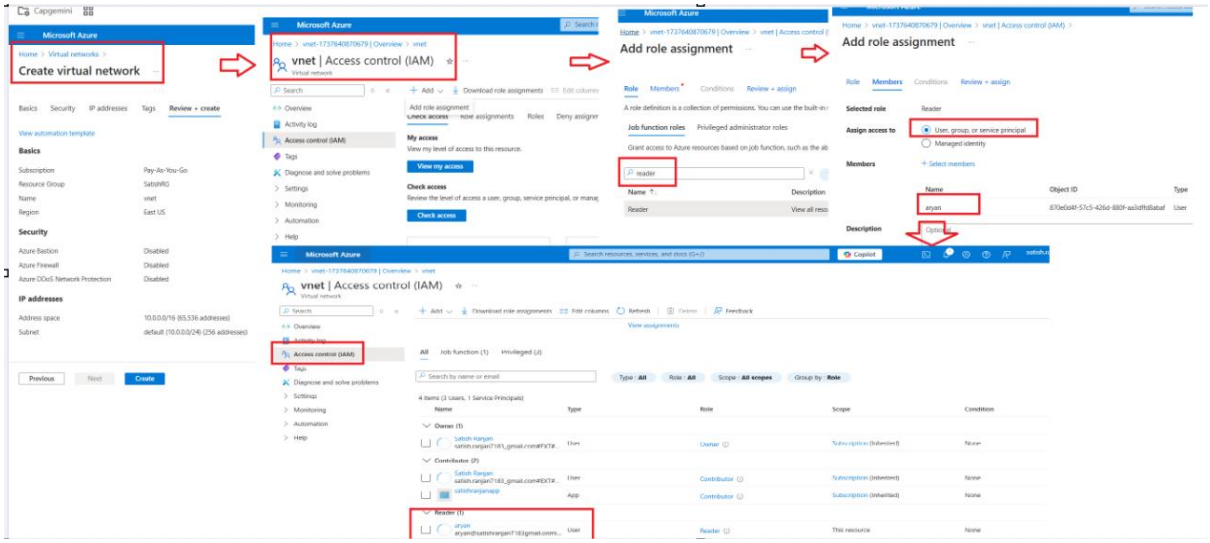
6. RBAC at Resource Level



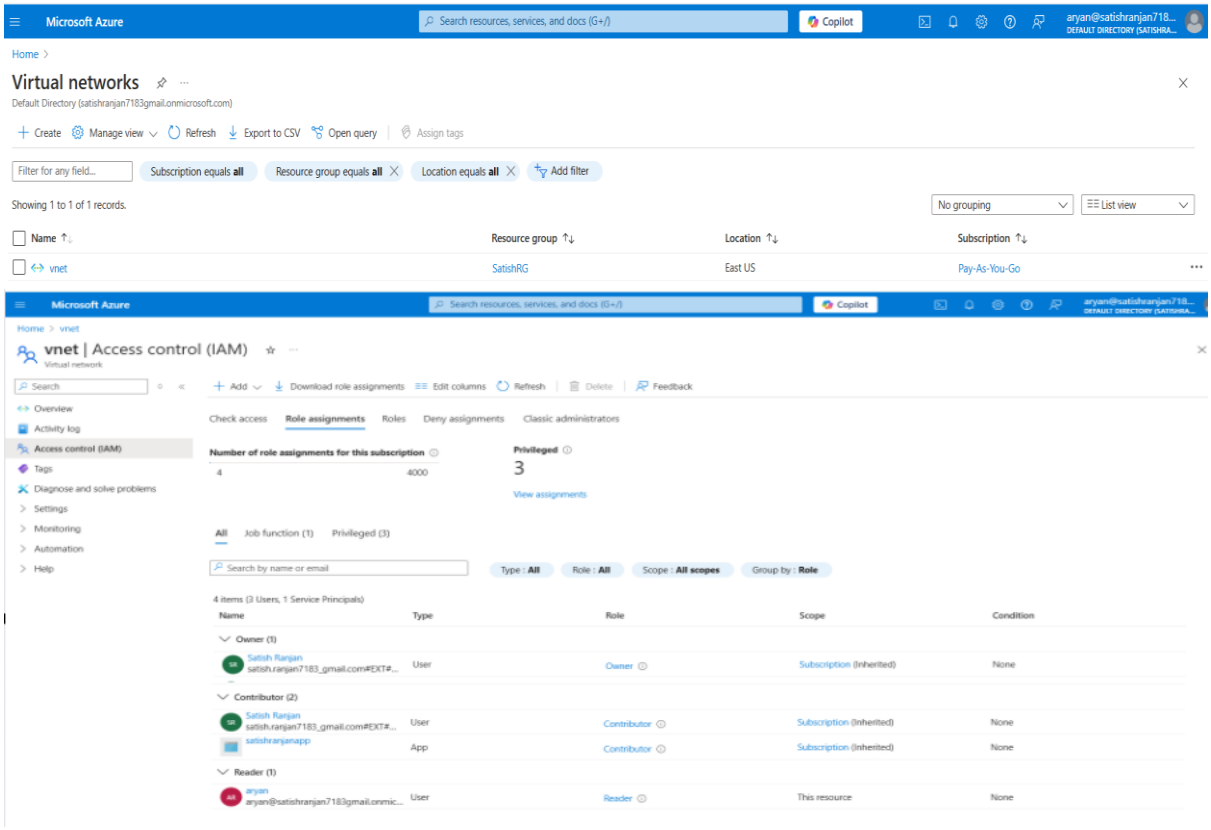
Let's give userA the reader role to the Azure virtual machine.

We will notice that we cannot see the other aspects of the virtual machine such as the virtual network etc.

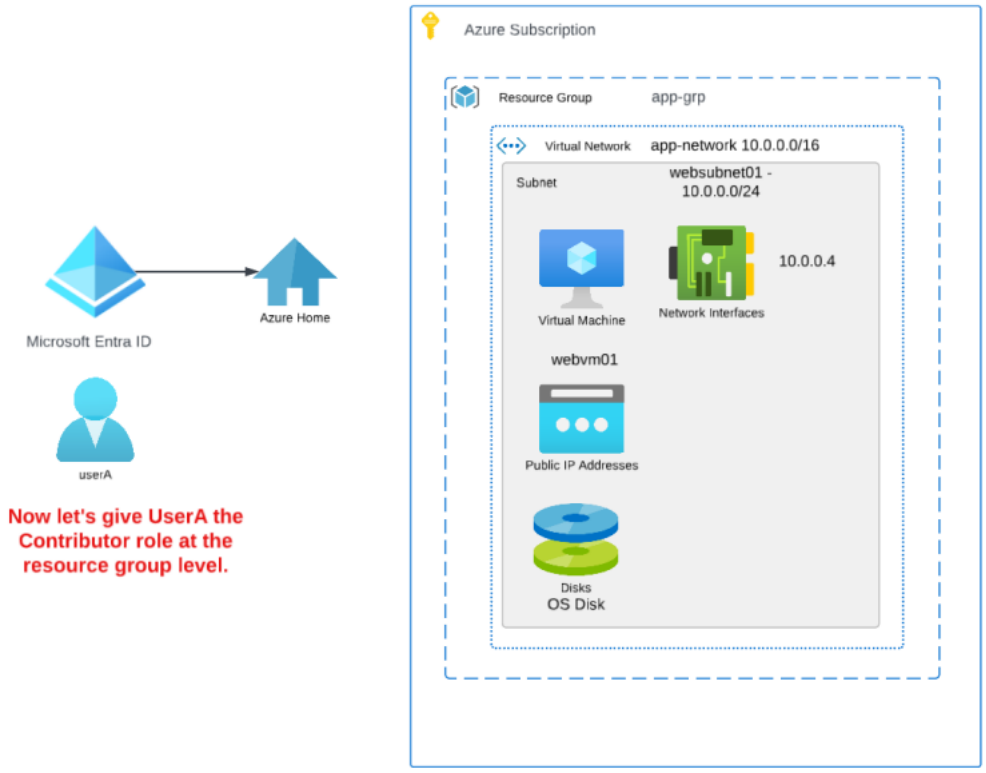
When we provide reader permission at specific resource like VM, so only other user can view VM, other resources like public IP not able to view due to reader permission restricted to only one resource VM.



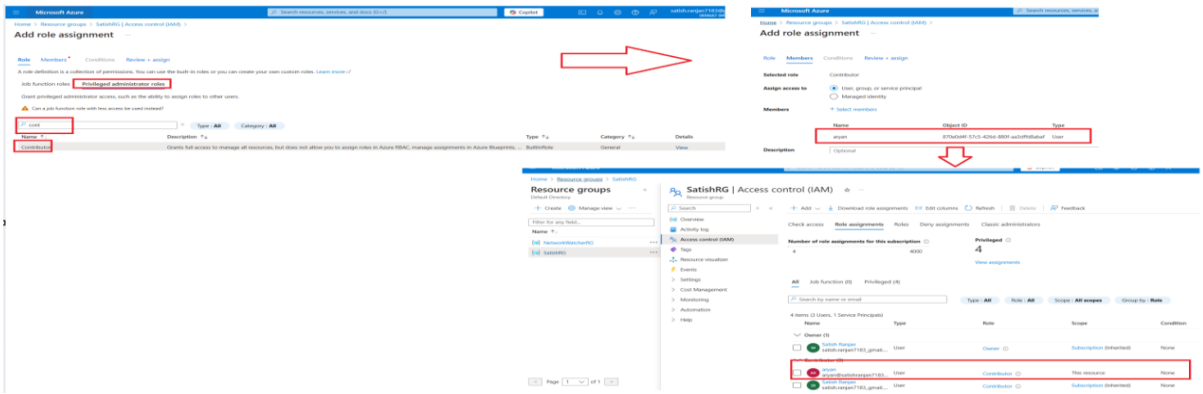
Now login with other user and resource is showing



7. RBAC at Contributor Role at Resource Group Level

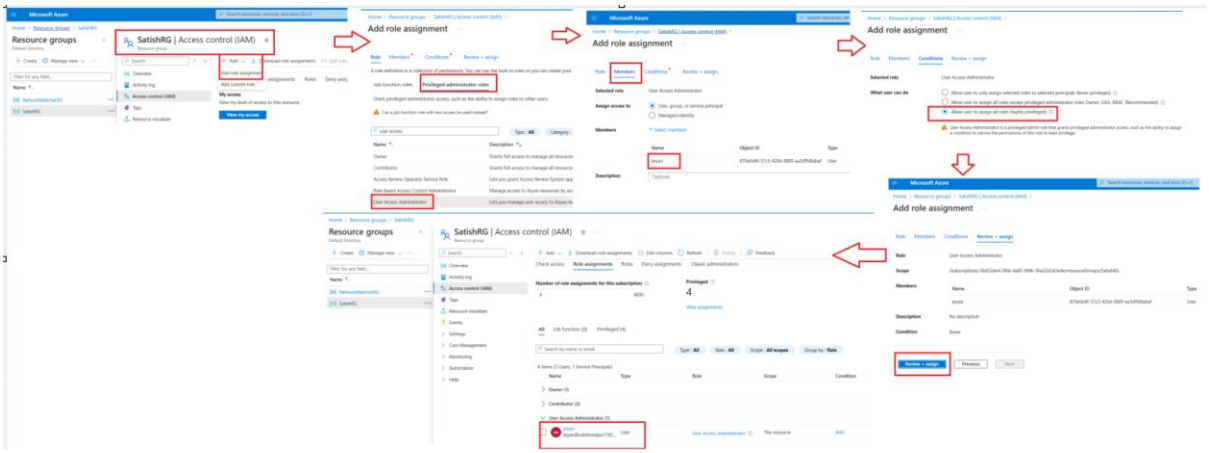


We can provide contributor rights at Resource Group level, then user can create and manage any resources.

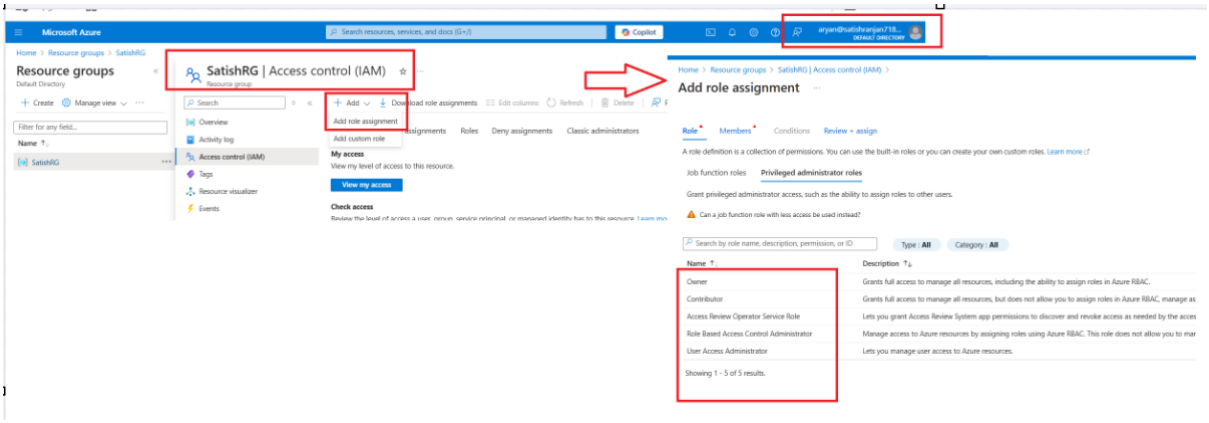


8. RBAC at User Access Administrator Role at Resource Group Level

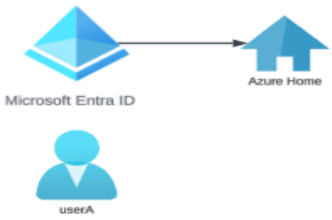
By Providing User Access Administrator Role, User can delegate/create other User account.



Now login with user account and check user can delegate other user account:



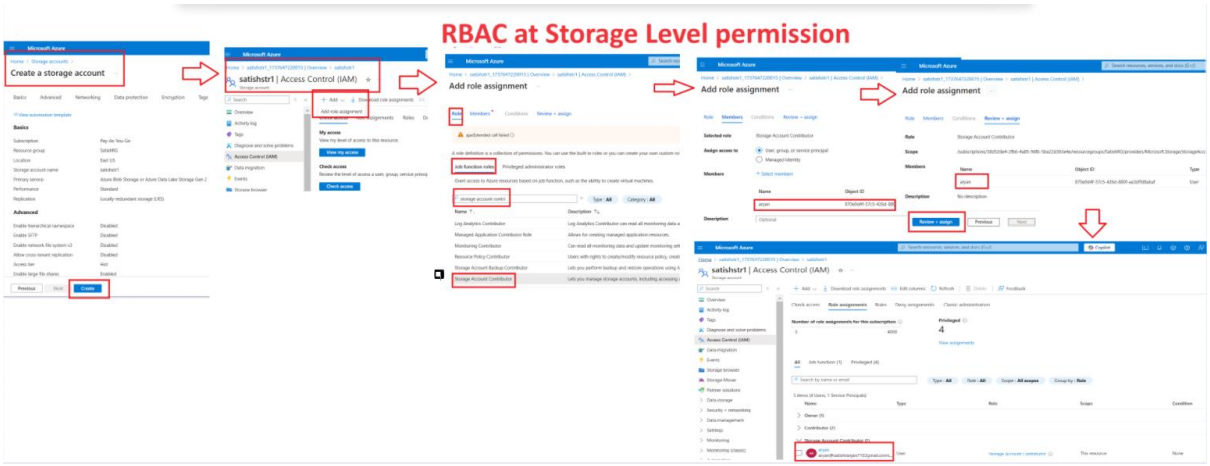
9. Role Assign for Azure Storage Account

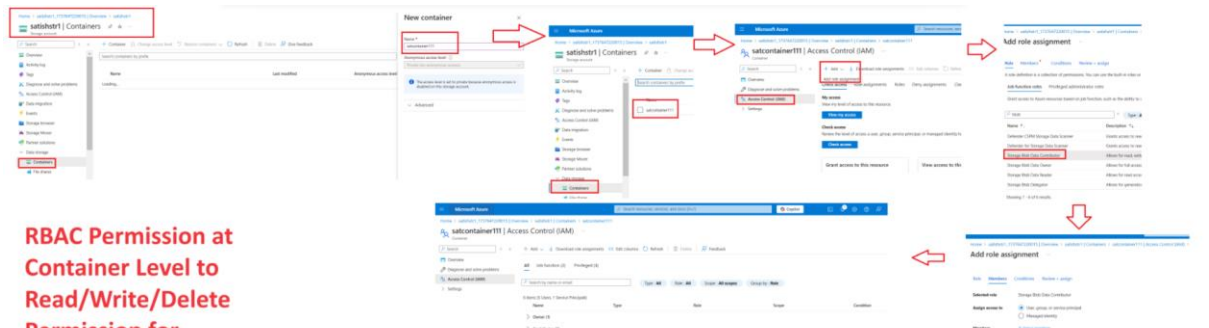


There are two way for providing RBAC permission for Storage Account:

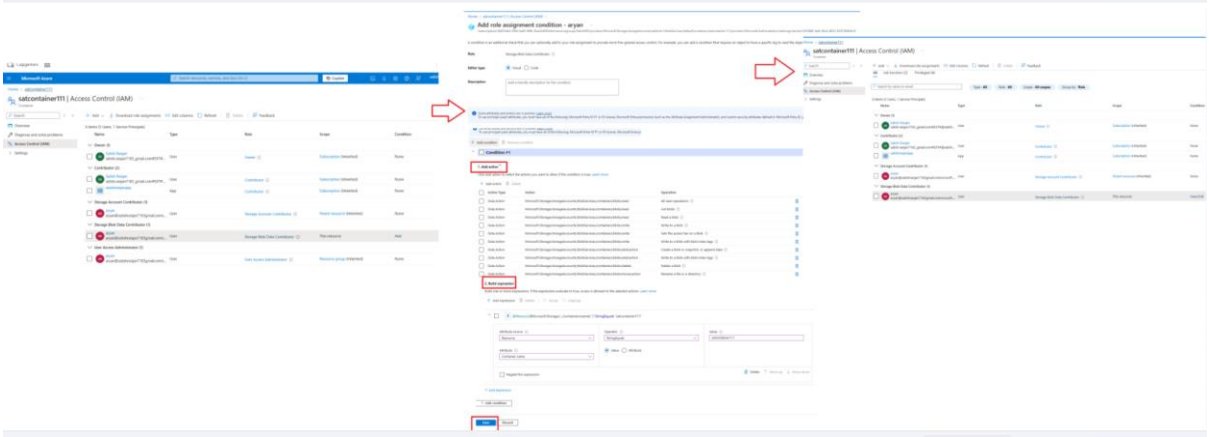
a. At Storage Account Level (Action Role) – Storage Account Contributor
b. For Read/write/delete permission for containers and blobs inside Storage Account (DataAction Role) – Storage blob Data Contributor/ Storage blob Data Reader

RBAC at Storage Level permission

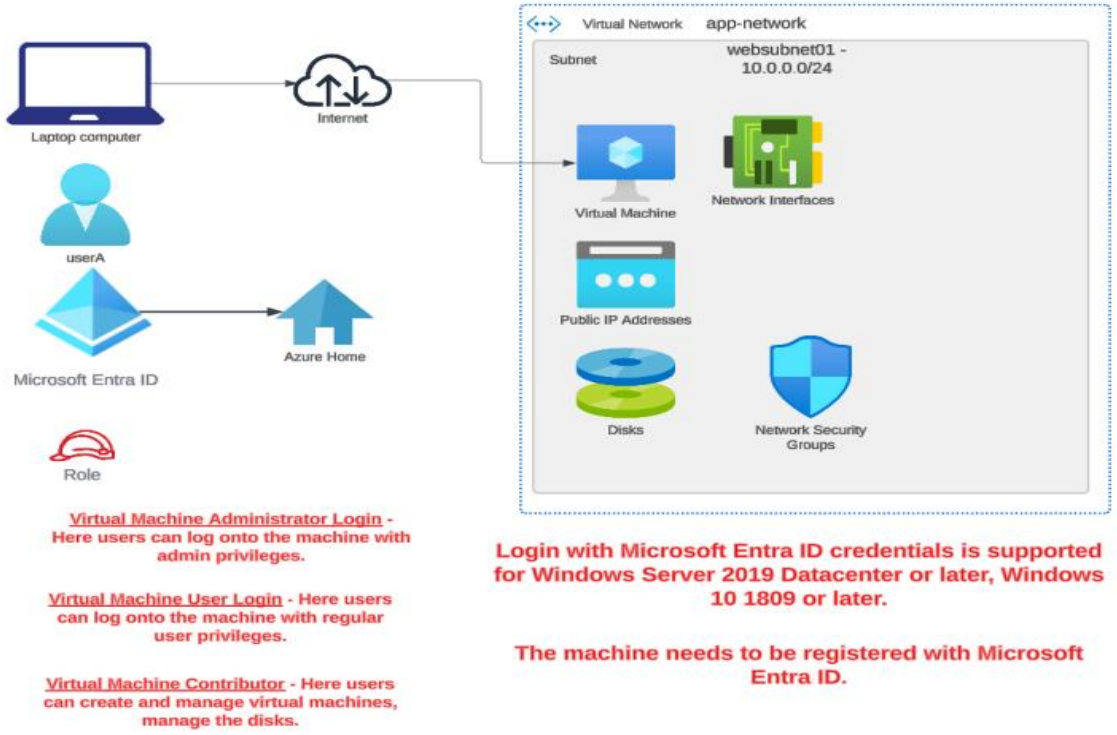




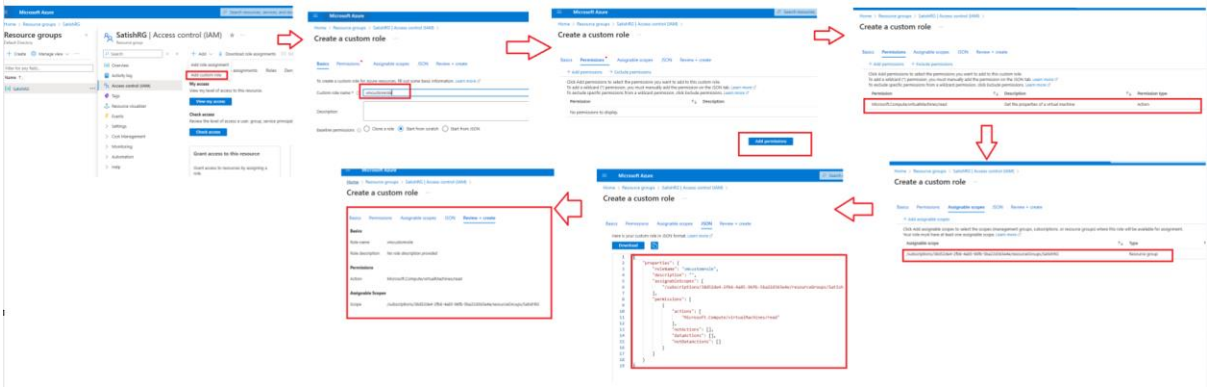
RBAC Permission at Container Level to Read/Write/Delete Permission for container and blob inside storage account

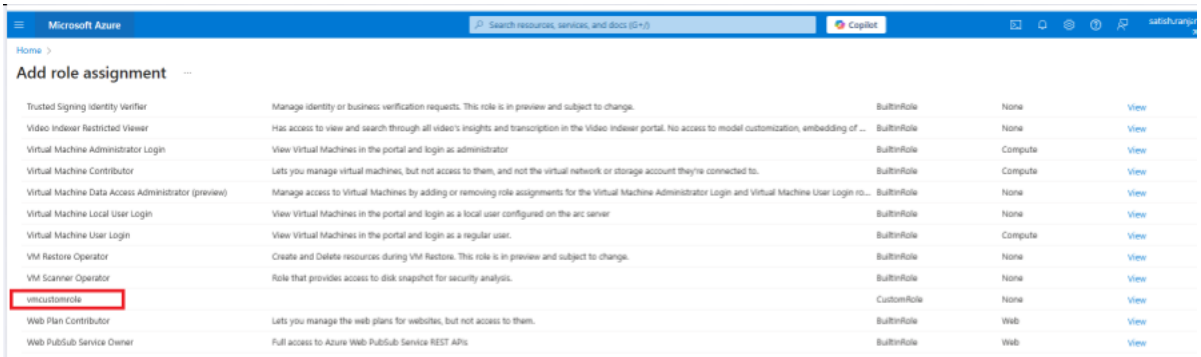


10. Role Assign for Virtual Machine
    a. Provide Reader role of Resource Group Level at least priviledge
    b. Provide Virtual Machine Administrator Login role at Virtual Machine level to managed virtual machine.

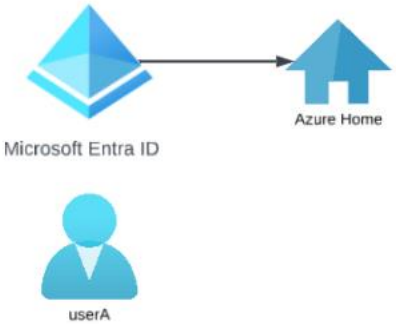


11. Custom Role





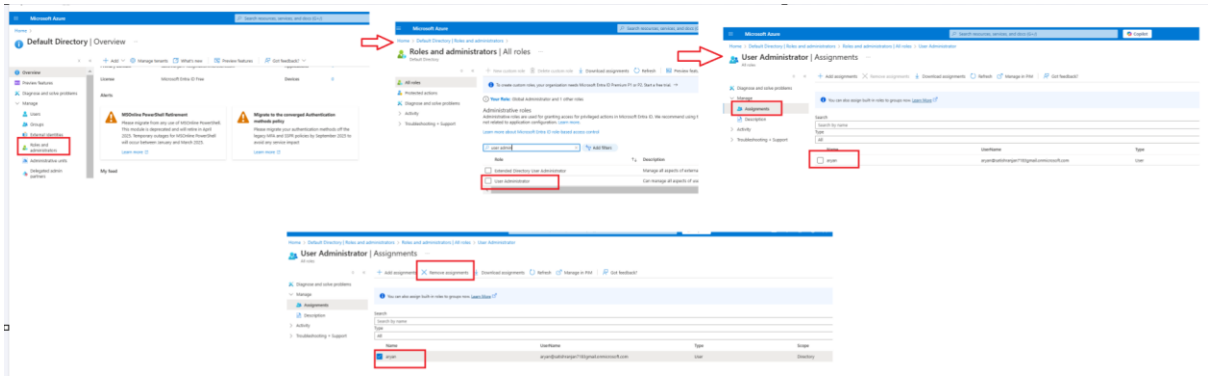
12. Microsoft Entra ID Roles



Microsoft Entra ID Roles

This gives users permissions to carry out operations within Microsoft Entra ID.

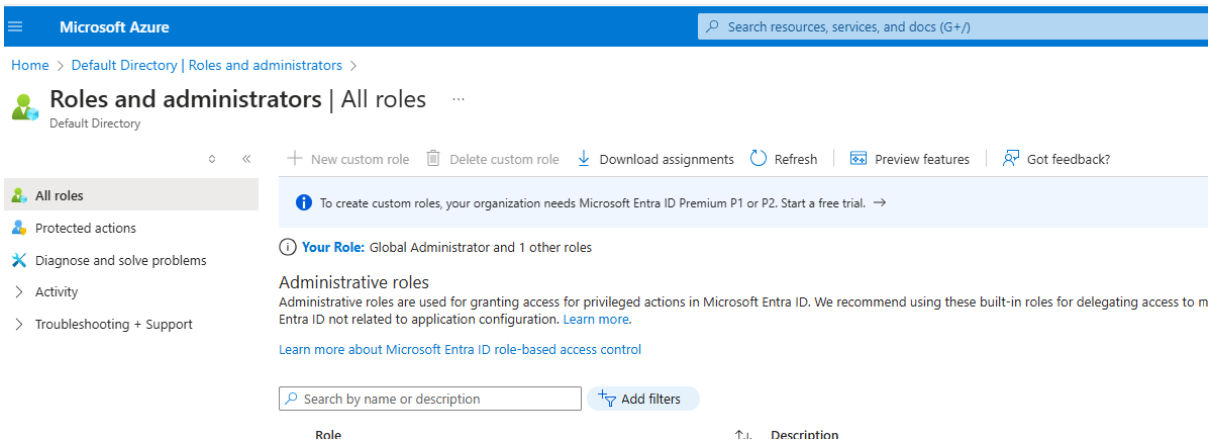
This is different from permissions given to resources to an Azure subscription.



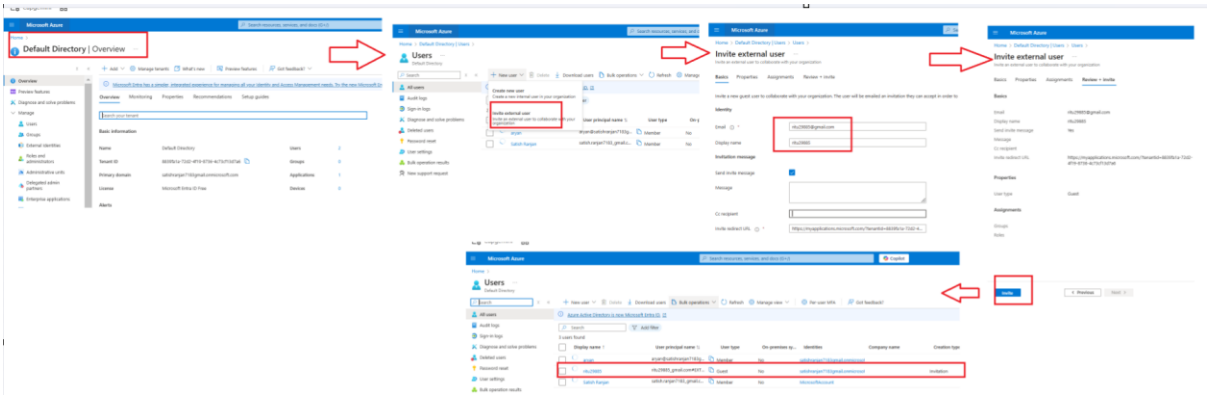
User has now been granted administrator rights through Entra ID roles. From this point forward, they have full administrative privileges, similar to that of an owner.

13. Microsoft Entra ID Custom Roles

For Creating Custom Role of Entra ID, Need to create P1 or P2. In Free trial not possible



14. Microsoft Entra ID - Inviting external identities

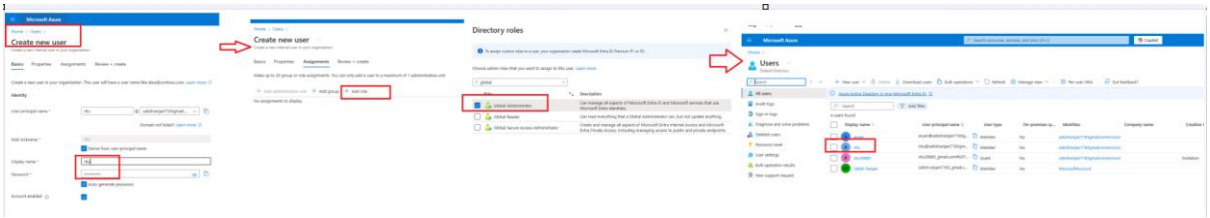


15. Microsoft Entra ID Licenses

Microsoft Entra ID Free: Provides user and group management, on-premises directory synchronization, basic reports, self-service password change for cloud users, and single sign on across azure, Microsoft 365, and many popular Saas apps.
Microsoft Entra ID P1:In addition to the free features, P1 also lets our hybrid user access both on-premises and cloud resources. It also supports advanced administration, such as dynamic membership groups, self-service group management, Microsoft identity manager, and cloud write-back capabilities, which allow self-service password reset for our on-premises users.
Microsoft Entra ID P2: In addition to the free and P1 features, P2 also offers Microsoft Entra ID protection to help provide-risk based conditional access to our apps and critical company data and privileged identity management to help discover, restrict, and monitor administrators and their access to resources and to provide just-in-time access when needed.

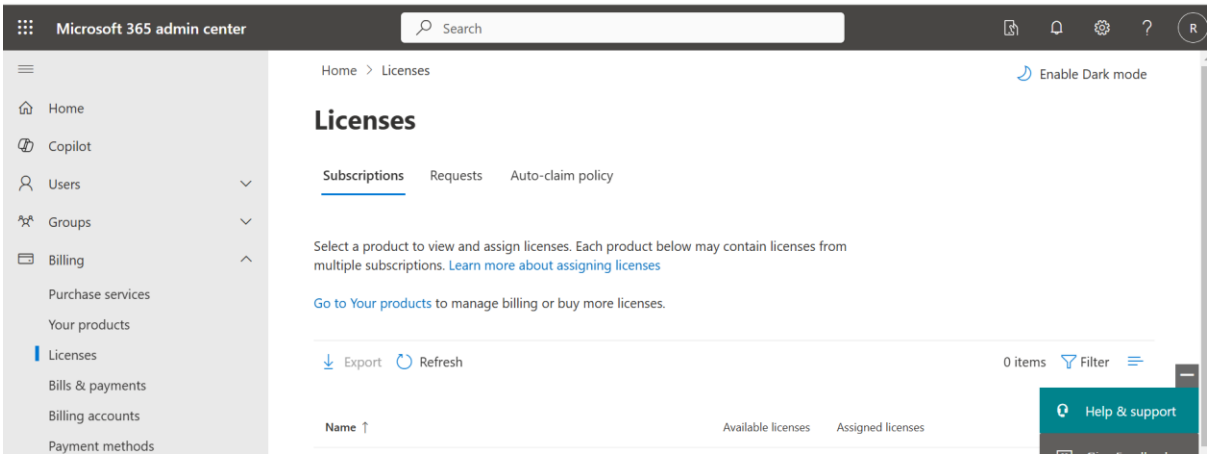
Step that need to follow

a. In Microsoft Entra Id, we first need to create a new user- We will assign the global administrator role to the user.

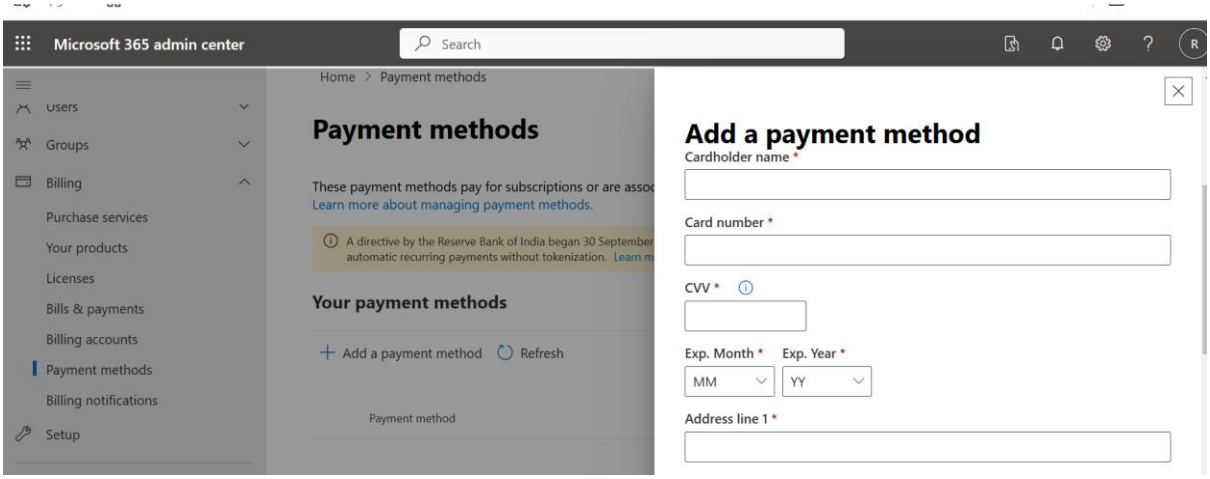


b. Then User, need to login in azure and change the password as part of the normal process for a new user

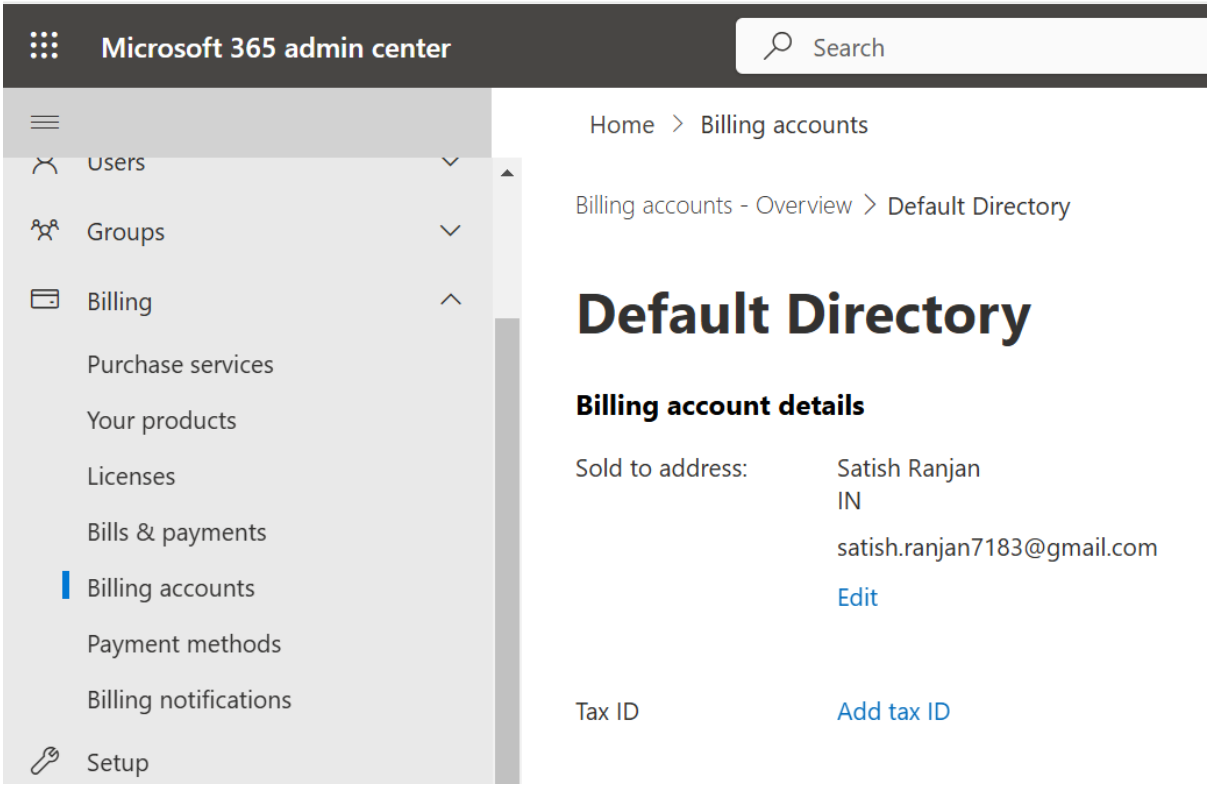
c. Then we need to log onto Microsoft 365 Admin Center with global user (https://admin.microsoft.com/Adminportal/Home#/licenses)



d. Need to add a valid payment method. Please note that the trial license don't incur a charge

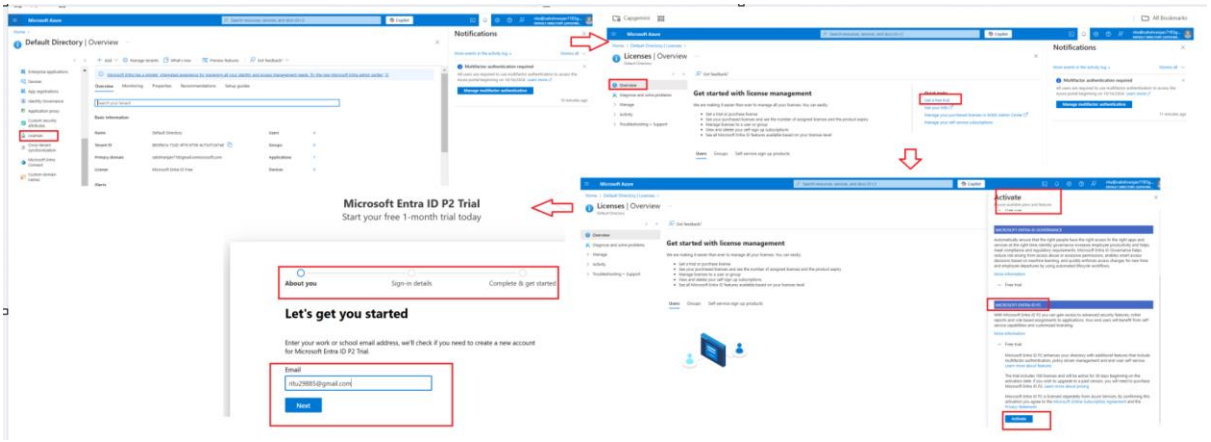


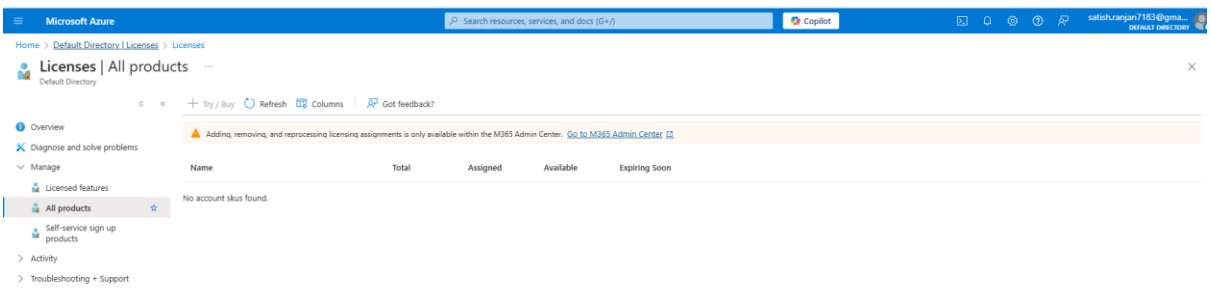
e. Then in billing account, there will be valid email address



f. Then in azure login to global user account, we can subscribe for free trial license for EntraID P2 for a month

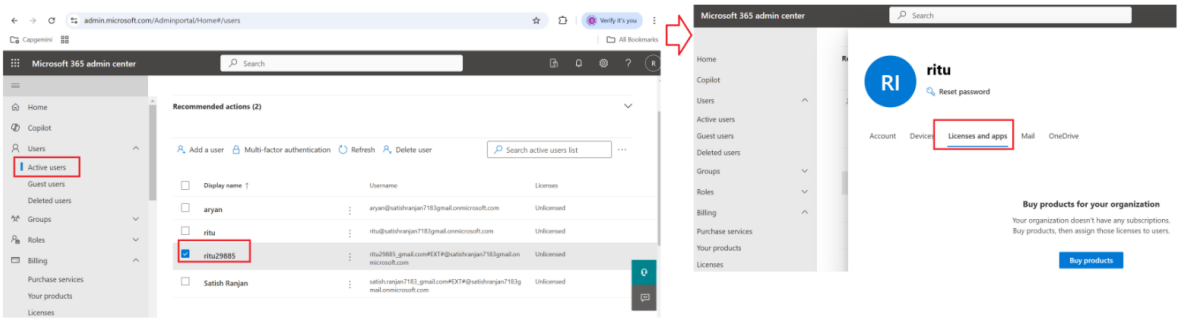
g. Now login from user account and then activate P2 License.





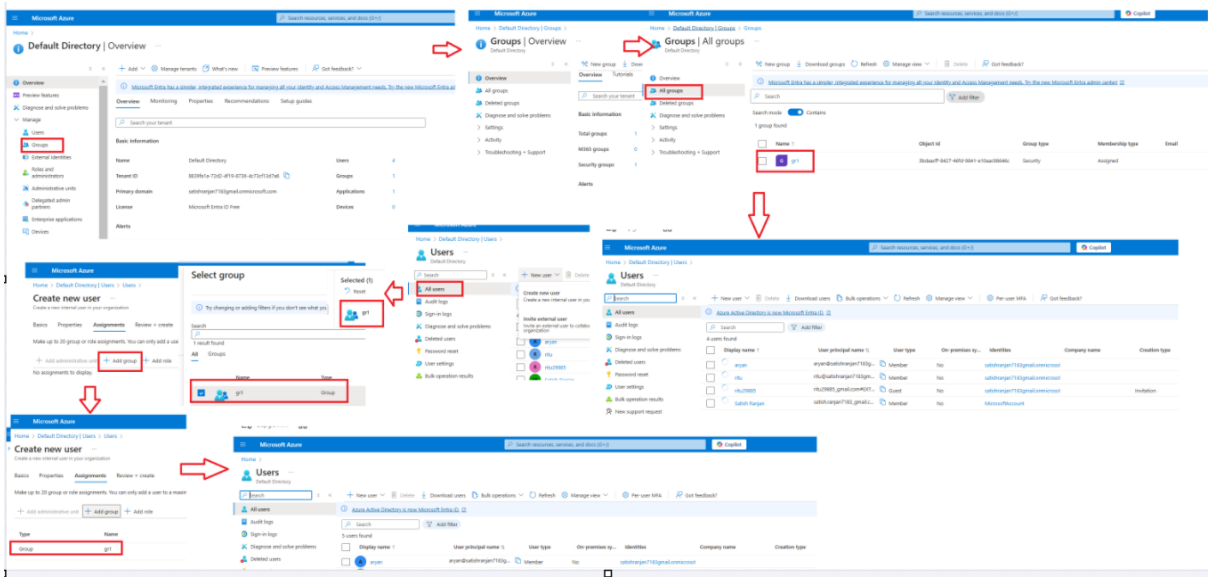
16. Assigning licenses to users

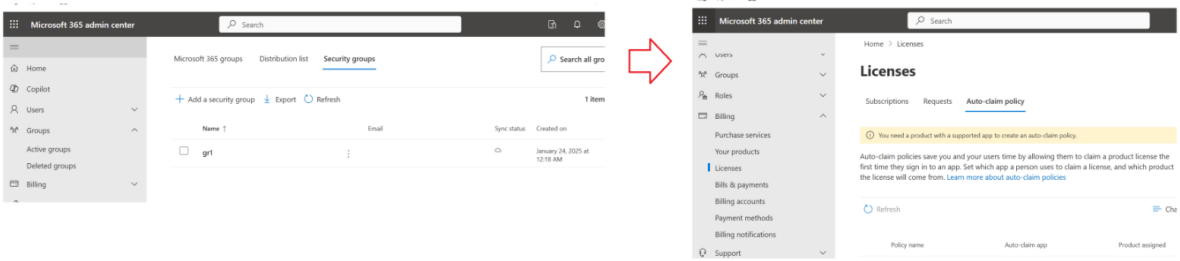
    we need to log onto Microsoft 365 Admin Center with global user (https://admin.microsoft.com/Adminportal/Home#/licenses)



17. Assigning licenses to Groups

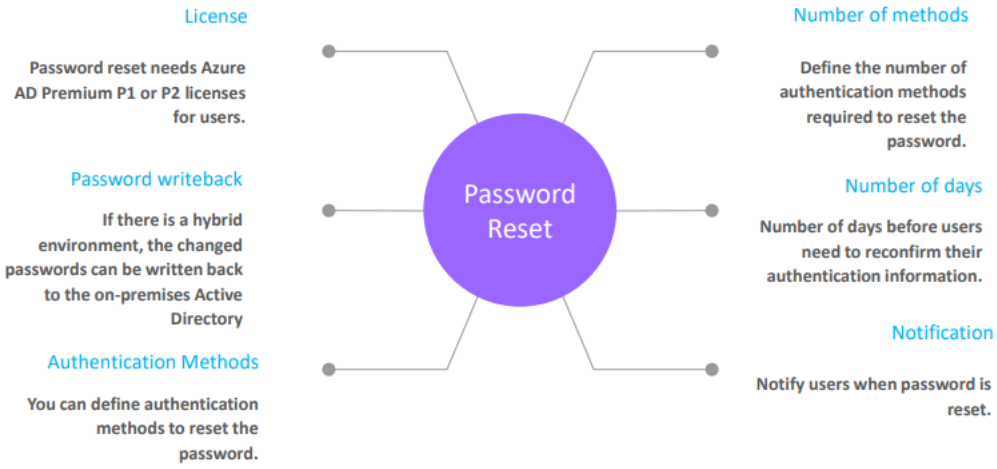
    First we create a group, add users in group from Entra ID in owner account.





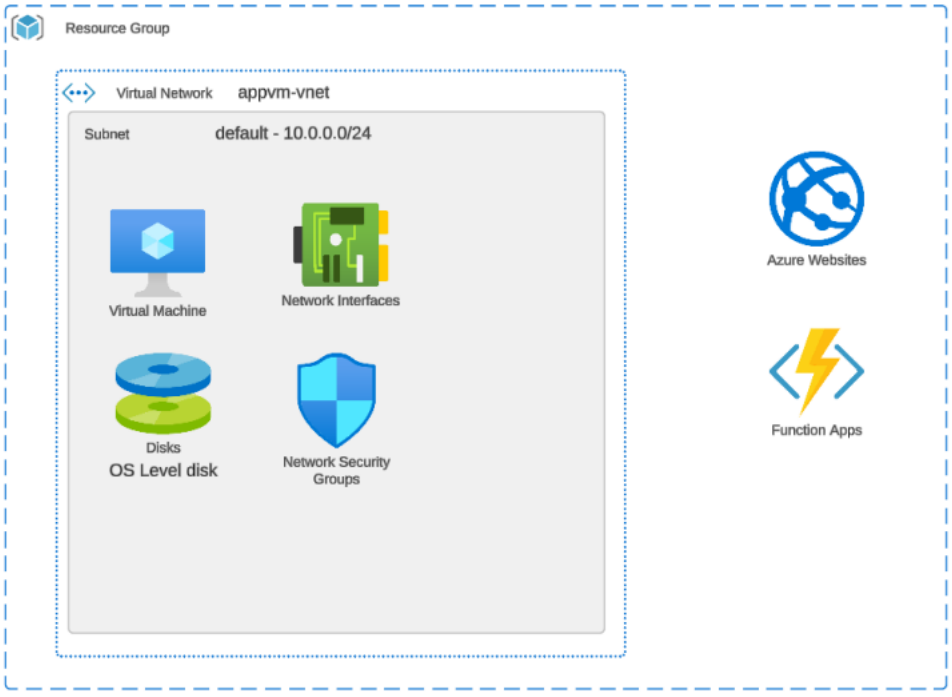
    Assign Group License onto Microsoft 365 Admin Center-> license-> click on license option

18. What is self-service password reset



19. Enabling self-service password reset : Need Premium P2 Account
20. Performing a self-service password reset : Need Premium P2 Account
21. Resource tag

Resource groups help to logically group resources.



If we want to filter resources based on resource group that can be done.

If we want to filter costs based on resource group that is also possible.

A company might have different departments

A company might have different Applications

Applications could have diferent tiers

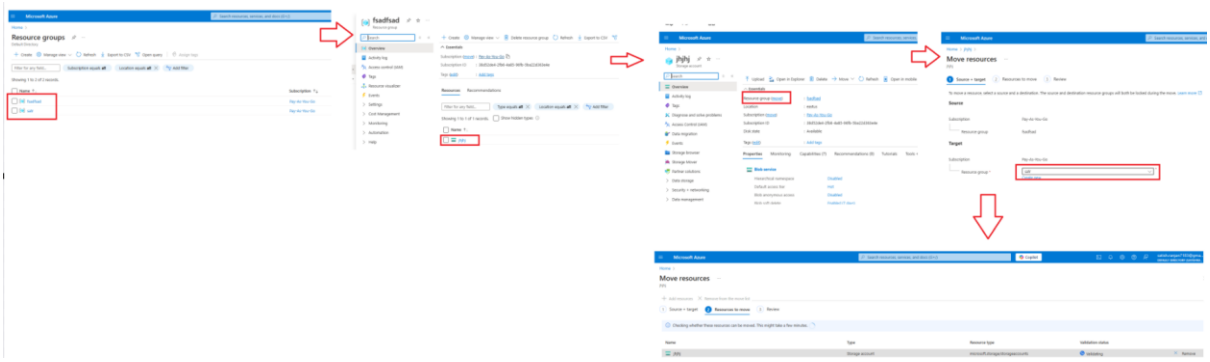
Applications could have different Environments

Companies want to be able to discern the different resources via these different attributes.

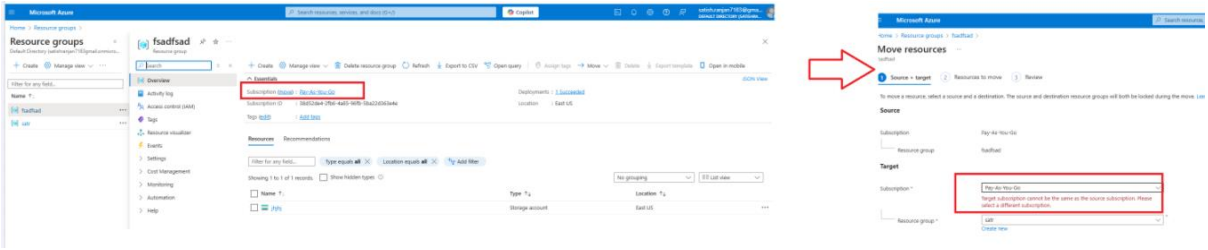
You can add tags to resources, this is extra metadata added to the resources.

It just gives an extra way to organize resources. Even from a billing aspect you can filter resources based on resource tags.

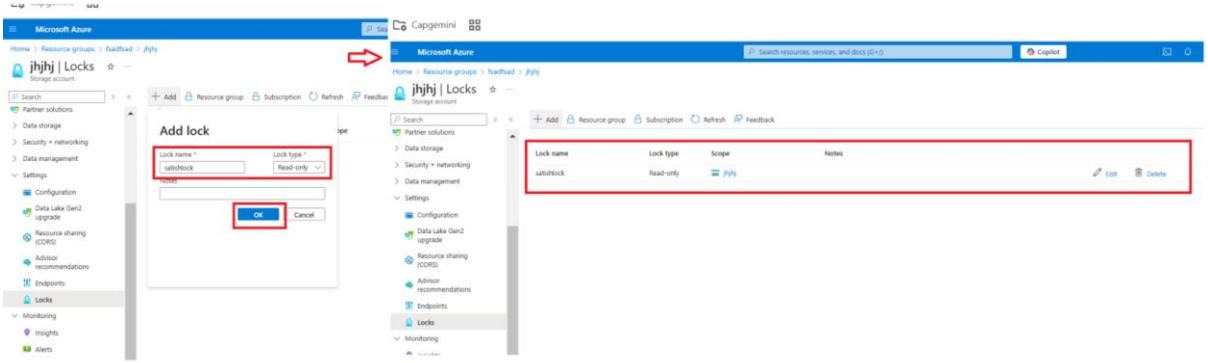
22. Moving resources across resource groups at resource level



23. Moving resources across subscription at resource group level



24. Locking resources



25. Locks and moving resources

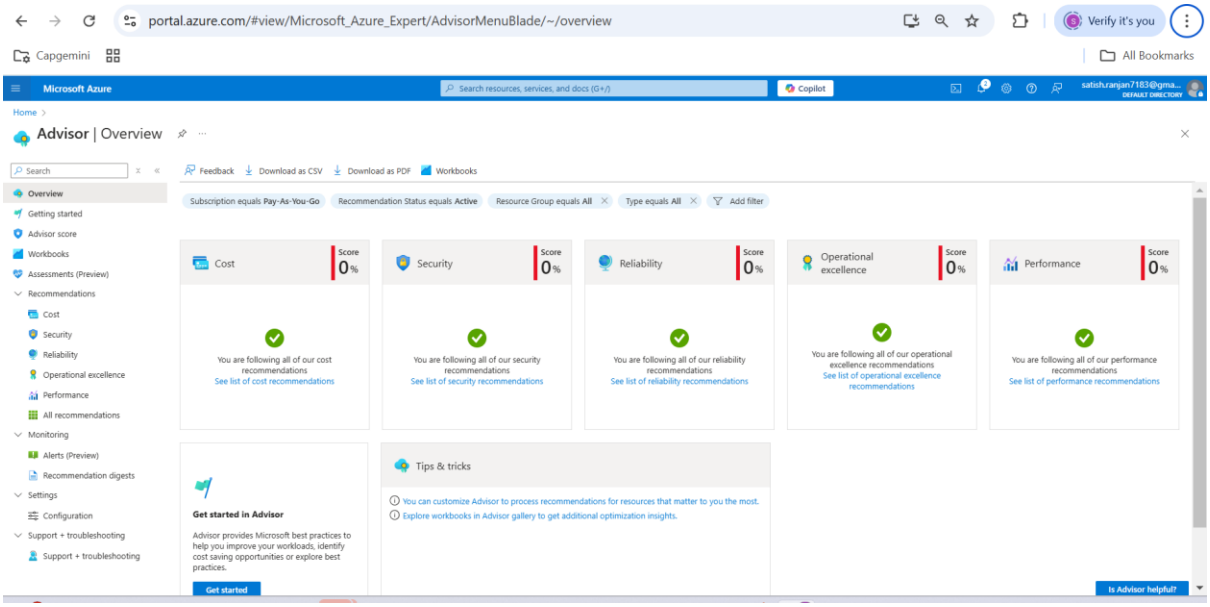
First need to delete/remove locks, then we can move our resource from one Resource group to another Resource group Or one subscription to another subscription.

26. Azure Advisor

Azure Advisor is a free tool in Microsoft Azure that helps you optimize your cloud resources. It provides personalized best practices and recommendations in four key areas:

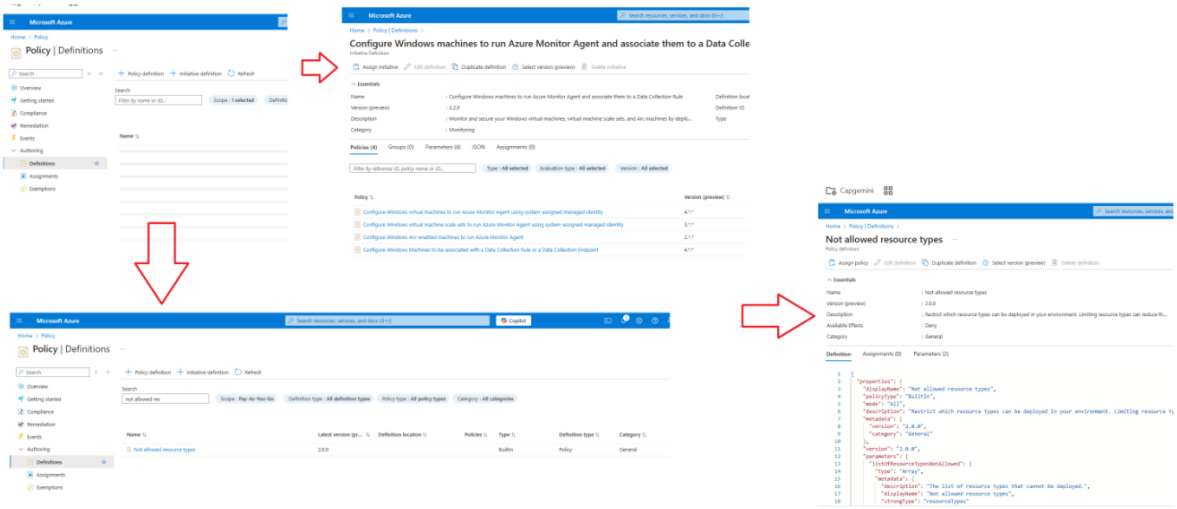
1. **Cost**: Suggests ways to save money by optimizing resource usage (e.g., shutting down unused VMs or using smaller instances).
2. **Security**: Identifies potential security risks and suggests actions to improve your security posture (e.g., enabling multi-factor authentication or securing your storage accounts).
3. **Performance**: Recommends actions to improve the performance of your services (e.g., resizing resources for better performance).

4. **Reliability**: Provides suggestions to improve the reliability and availability of your resources (e.g., setting up backup or using Availability Sets).
   In short, **Azure Advisor** helps you make the most of your Azure resources by giving you simple, actionable tips to improve cost-efficiency, security, performance, and reliability.

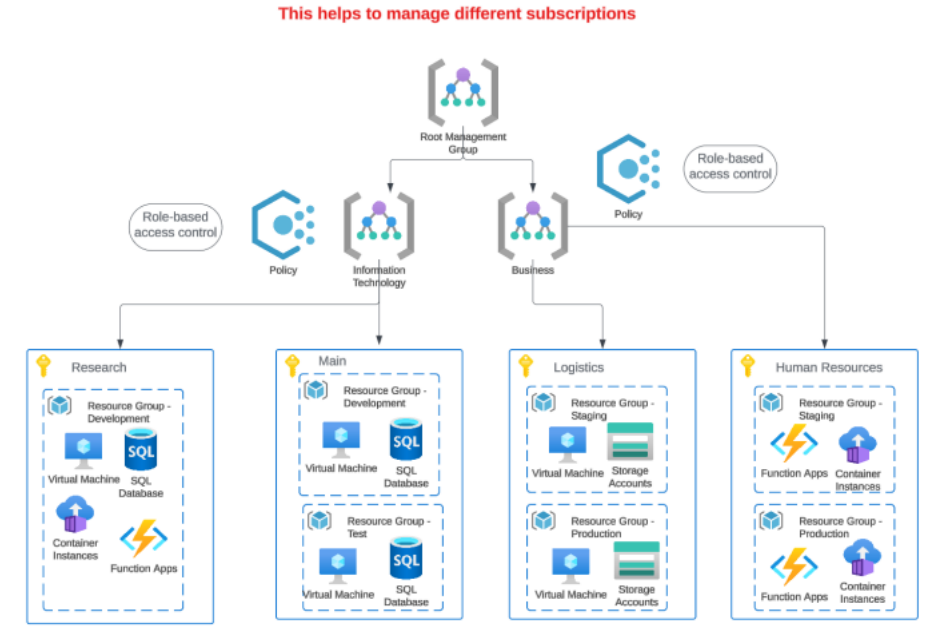


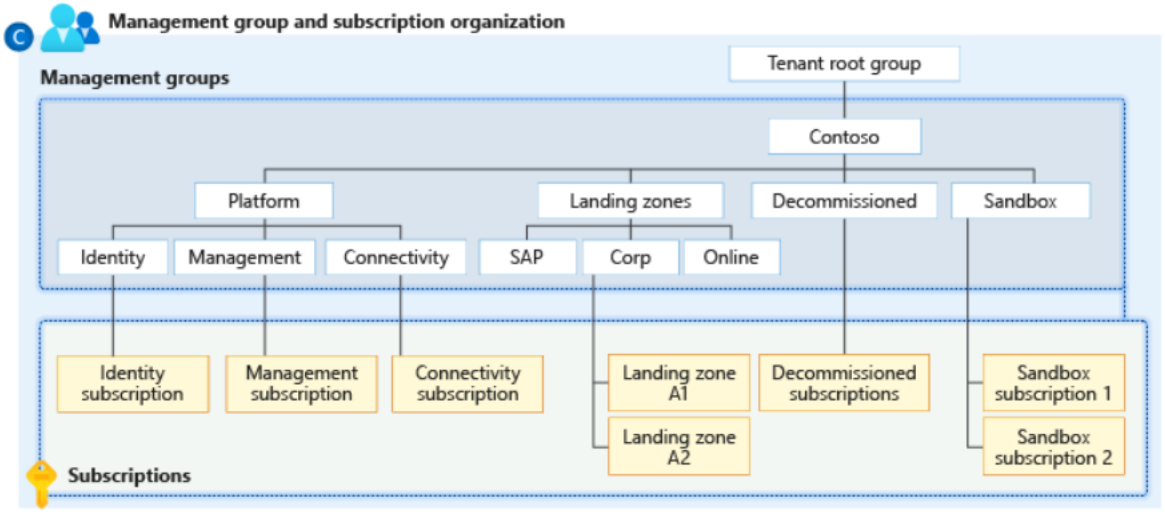
27. Using the azure policy service
    Azure Policy helps to govern our resources. We can define rules that resources need to comply by.
    Lets say a company only wants VM to be constrained to a particular region. Or machine need to be of certain SKU.
    We can use build-in policy for this
    We can also define our own policies.
    We can also define an initiative which is list of policies.

28. Azure policy not allowed resource type

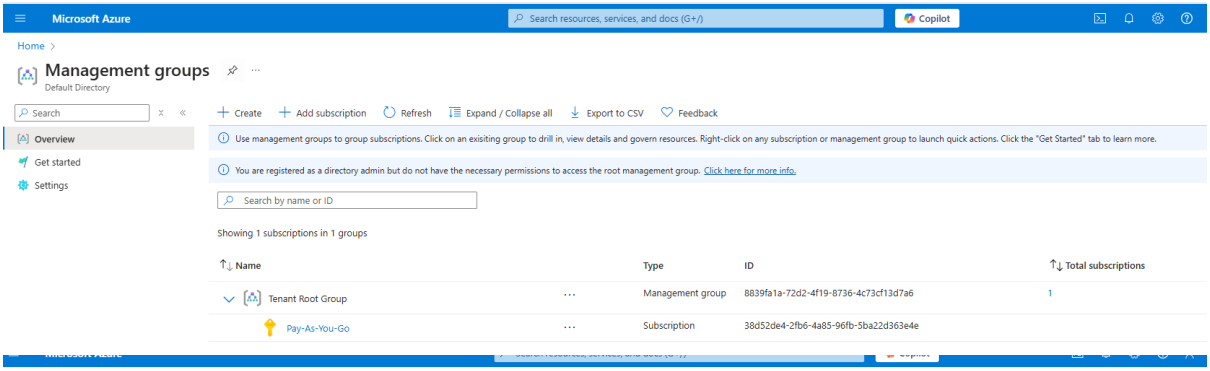


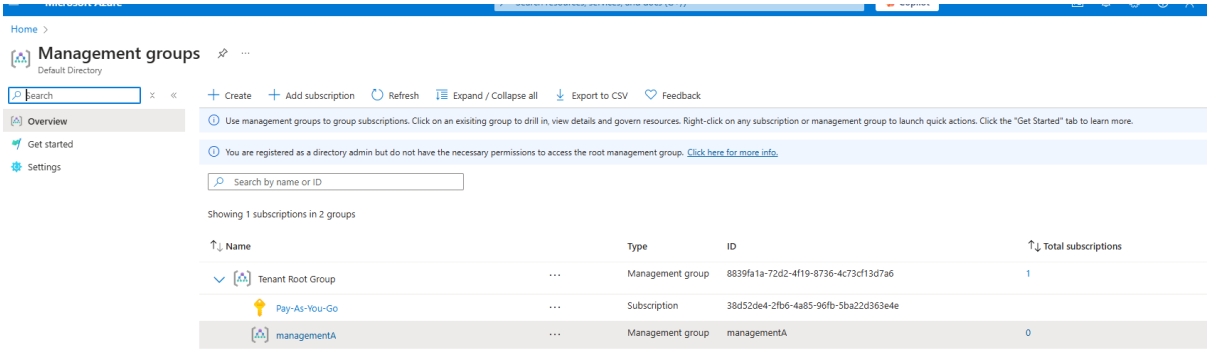
29. Management group

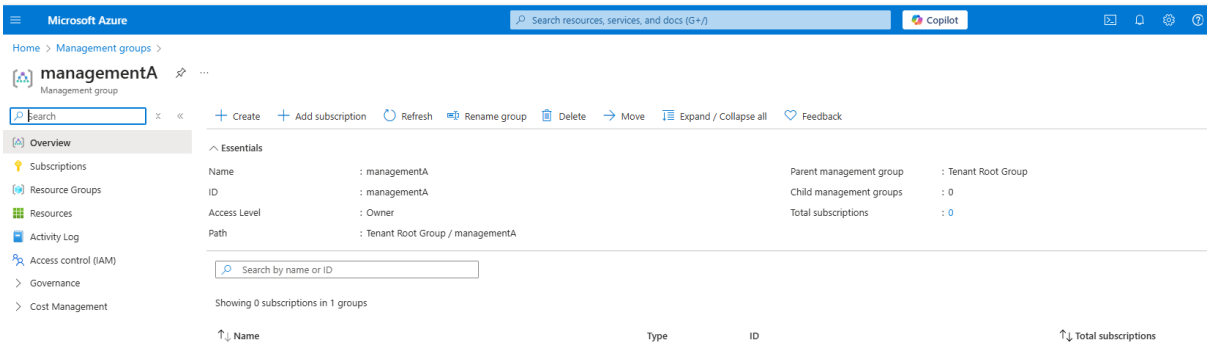




30. Looking at management group


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home
Management groups
Default Directory
Search
Overview
Get started
Settings
Create
Add subscription
Refresh
Expand / Collapse all
Export to CSV
Feedback
Use management groups to group subscriptions. Click on an exisiting group to drill in, view details and govern resources. Right-click on any subscription or management group to launch quick actions. Click the "Get Started" tab to learn more.
You are registered as a directory admin but do not have the necessary permissions to access the root management group. Click here for more info.
Search by name or ID
Showing 1 subscriptions in 1 groups
Name
Type
ID
Total subscriptions
Tenant Root Group
Management group
8839fa1a-72d2-4f19-8736-4c73cf13d7a6
1
Pay-As-You-Go
Subscription
38d52de4-2fb6-4a85-96fb-5ba22d363e4e


Home
Management groups
Default Directory
Search
Overview
Get started
Settings
Create
Add subscription
Refresh
Expand / Collapse all
Export to CSV
Feedback
Use management groups to group subscriptions. Click on an exisiting group to drill in, view details and govern resources. Right-click on any subscription or management group to launch quick actions. Click the "Get Started" tab to learn more.
You are registered as a directory admin but do not have the necessary permissions to access the root management group. Click here for more info.
Search by name or ID
Showing 1 subscriptions in 2 groups
Name
Type
ID
Total subscriptions
Tenant Root Group
Management group
8839fa1a-72d2-4f19-8736-4c73cf13d7a6
1
Pay-As-You-Go
Subscription
38d52de4-2fb6-4a85-96fb-5ba22d363e4e
managementA
Management group
managementA
0


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home
Management groups
managementA
Management group
Search
Overview
Subscriptions
Resource Groups
Resources
Activity Log
Access control (IAM)
Governance
Cost Management
Create
Add subscription
Refresh
Rename group
Delete
Move
Expand / Collapse all
Feedback
Essentials
Name : managementA
ID : managementA
Access Level : Owner
Path : Tenant Root Group / managementA
Parent management group : Tenant Root Group
Child management groups : 0
Total subscriptions : 0
Search by name or ID
Showing 0 subscriptions in 1 groups
Name
Type
ID
Total subscriptions

31.