😊 Role Based Access Control

Role-Based Access Control (RBAC) in Azure Active Directory (Azure AD) is a method used to manage access to Azure resources. It allows administrators to assign permissions to users, groups, or applications based on their roles within the organization. RBAC helps ensure that users have the appropriate level of access to resources, reducing the risk of unauthorized access and data breaches.

Key components of RBAC in Azure AD include:

1. **Roles:** Azure provides built-in roles such as Owner, Contributor, and Reader, which define sets of permissions for managing Azure resources. Additionally, custom roles can be created to tailor access permissions to specific organizational requirements.
2. **Assignments:** Administrators assign roles to users, groups, or applications within Azure AD. These assignments determine the level of access granted to each entity.
3. **Scope:** RBAC assignments can be scoped at different levels, including management group, subscription, resource group, or individual resource. This allows for fine-grained control over access to specific resources or resource groups.
4. **Inheritance:** RBAC assignments can inherit permissions from higher-level scopes. For example, a role assigned at the subscription level automatically applies to all resources within that subscription unless explicitly overridden at a lower level.
5. **Dynamic Groups:** RBAC assignments can also be applied to dynamic groups in Azure AD. Dynamic groups automatically add or remove members based on user attributes or membership rules, simplifying access management for large organizations with frequently changing user populations.

😄 Use cases of RBAC:

Role-Based Access Control (RBAC) in Azure Active Directory (Azure AD) offers a variety of use cases across different industries and organizational sizes. Here are some common scenarios where RBAC is utilized:

1. **Access Control for Azure Resources:** RBAC allows organizations to control access to various Azure resources such as virtual machines, databases, storage accounts, and web applications. Administrators can assign roles like Owner, Contributor, or Reader to users, groups, or applications, defining their level of access to specific resources.
2. **Delegated Administration:** RBAC enables organizations to delegate administrative tasks while maintaining control over access permissions. Administrators can create custom roles with specific permissions tailored to different teams or departments, allowing them to perform their duties without granting unnecessary privileges.
3. **Compliance and Security:** RBAC helps organizations meet compliance requirements and enhance security by enforcing the principle of least privilege. By assigning roles based on job responsibilities, RBAC ensures that users only have access to the resources necessary to perform their duties, reducing the risk of unauthorized access and data breaches.

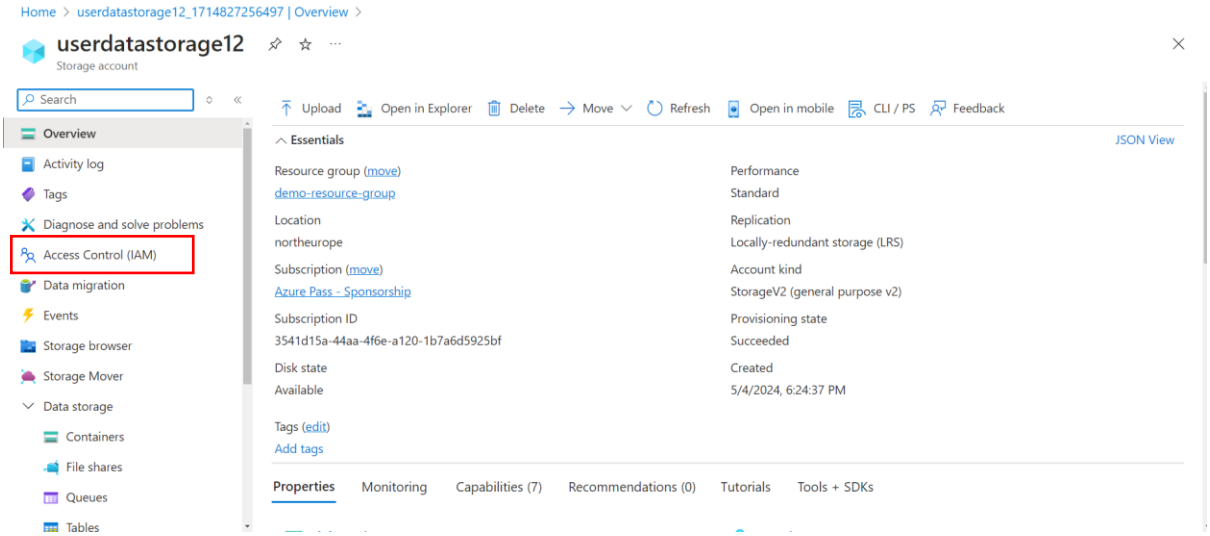
4. **Segregation of Duties (SoD):** RBAC facilitates segregation of duties by separating conflicting tasks among different roles. For example, organizations can define separate roles for development, testing, and production environments, preventing individuals from having unrestricted access to all stages of the software development lifecycle.
5. **Resource Cost Management:** RBAC can be used to control access to cost-related Azure resources, such as subscriptions, resource groups, and billing information. By assigning roles with appropriate permissions, organizations can ensure that only authorized users can view or manage cost data, helping to optimize resource usage and reduce expenses.
6. **Multi-Tenant Environments:** In multi-tenant scenarios, such as software as a service (SaaS) applications, RBAC allows tenants to control access to their own data and resources. Azure AD supports cross-tenant RBAC, enabling tenants to assign roles to users from other Azure AD tenants while maintaining security boundaries.
7. **Temporary Access:** RBAC can be used to grant temporary access to resources for specific tasks or projects. Administrators can assign roles with a defined expiration date, ensuring that access is automatically revoked when it is no longer needed, reducing the risk of lingering permissions.
8. **Auditing and Reporting:** RBAC provides granular audit logs and reporting capabilities, allowing organizations to track who accessed which resources and when. This helps organizations maintain visibility and accountability over access permissions, supporting compliance audits and security investigations.

We are setting up Azure role-based access control (RBAC) in this exercise to regulate and safeguard resource access. First, we create a virtual machine and storage account, then we give a demo user the proper read and contributor roles. Next, in order to show how to use the user access administrator position, we expand demo user1's rights so that they can designate roles to other users. The end goal is to ensure proper access control, enabling users to perform necessary tasks while maintaining security and governance. In order to preserve a safe workplace, we lastly tidy up by eliminating any superfluous duty assignments.

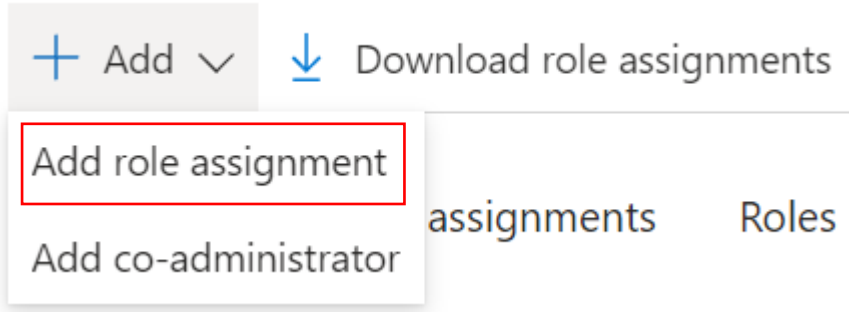
😄 To begin with the Lab:

😄 Reader Role

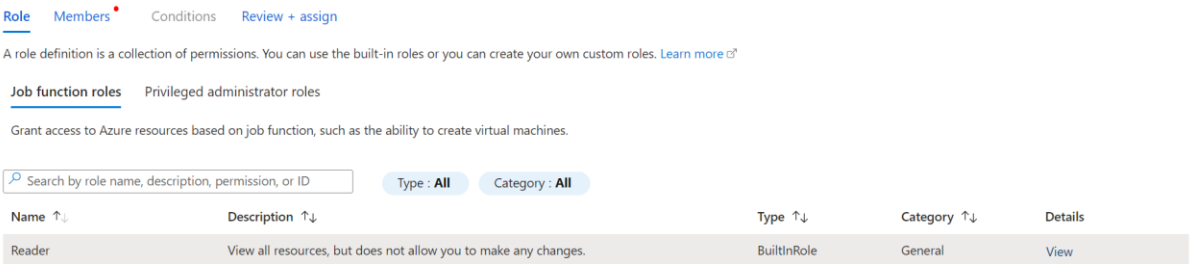
1. Now in your main account you need to create a storage account. For that navigate to it and click on create. After that you need to give it a name and choose the resource group and the region. Then just create your storage account.
2. Once your account is created you can also create a container in it.
3. Now you need to navigate to Access Control (IAM).



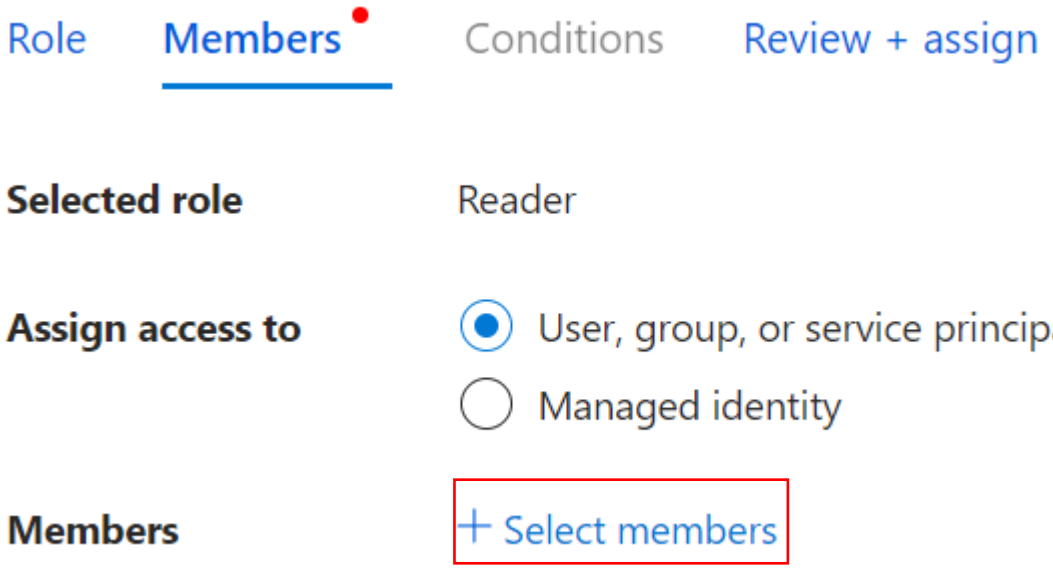
4. From there you need to click on add then choose add role assignment.



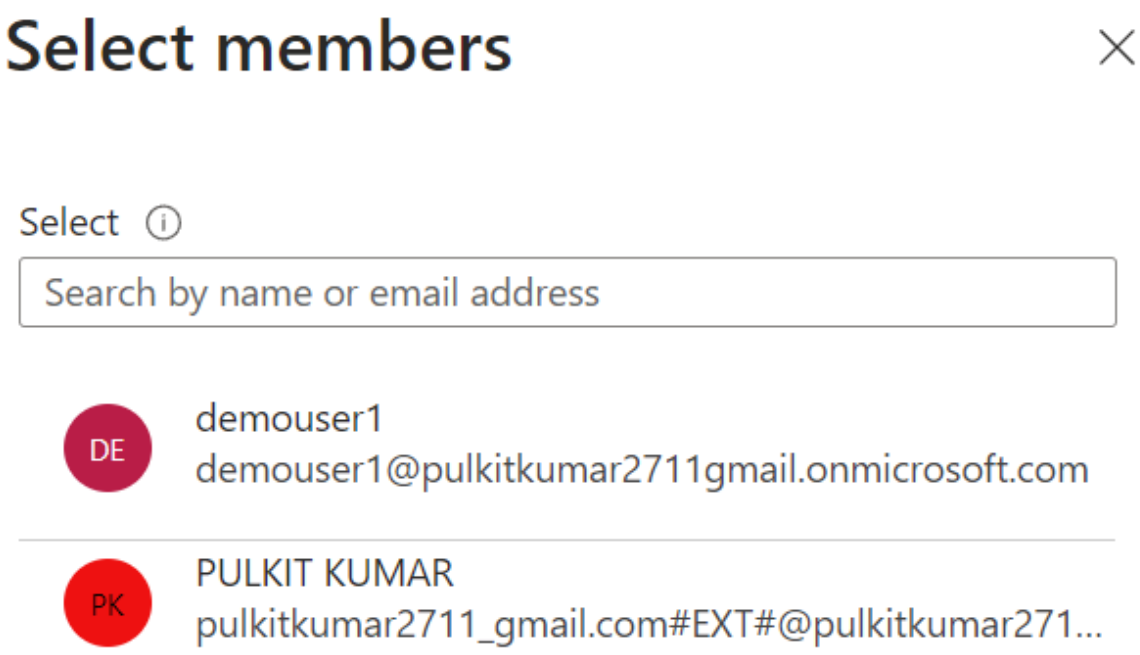
5. Now you need to choose reader role then move to members.



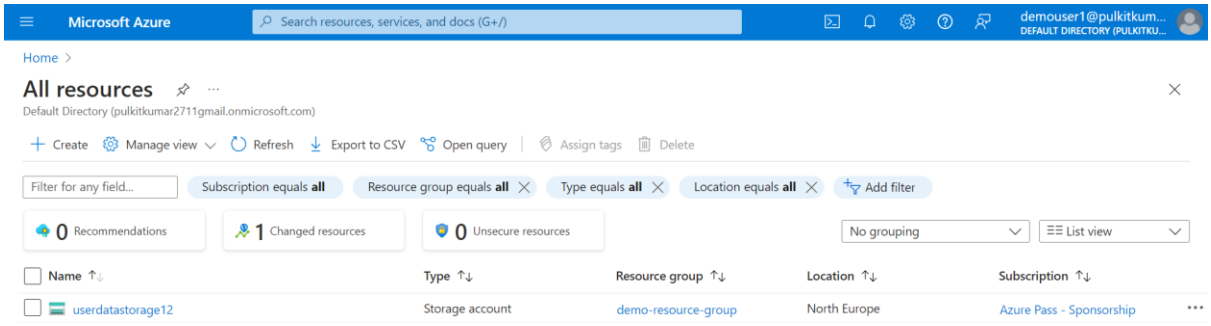
6. For members click on select members.



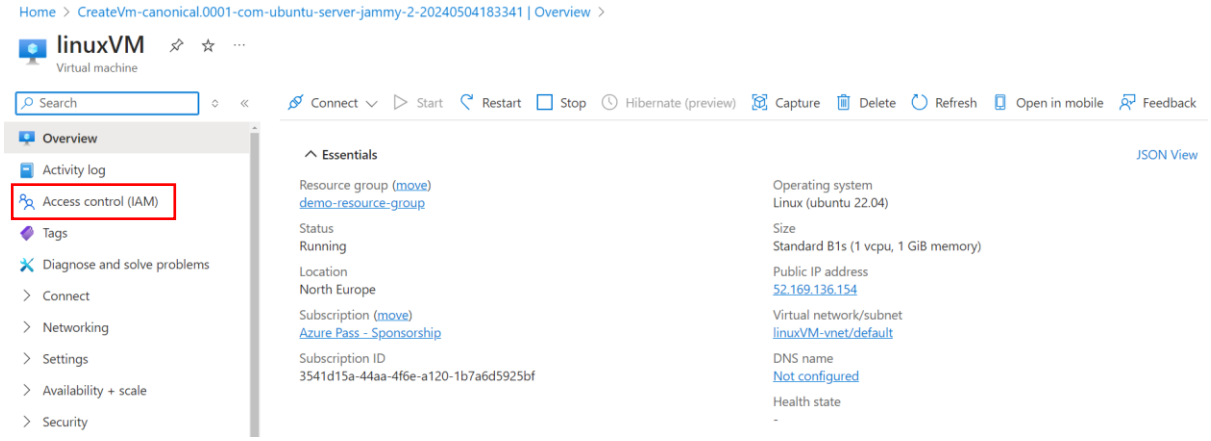
9. Now you need to choose your demo user account and then click on next.



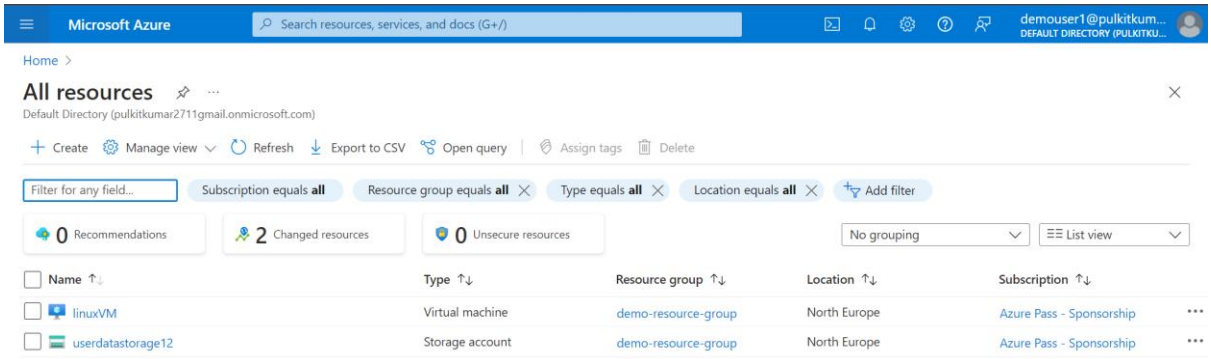
10. Then move to review and assign and create your role assignment.
11. After that you are going to create a virtual machine based on Ubuntu OS in its default settings. While using the size you can choose the lowest that is B1s.
12. Now move to your demo user tab and go to all resources. You can see your storage account here.
13. But if you are wondering that where is virtual machine, then you need to give the same permission for that too.



14. Now in your VM go to Access Control (IAM). Then do the same as you did for storage account choose the reader permission, after that choose your demo user as your member and click on review and assign.

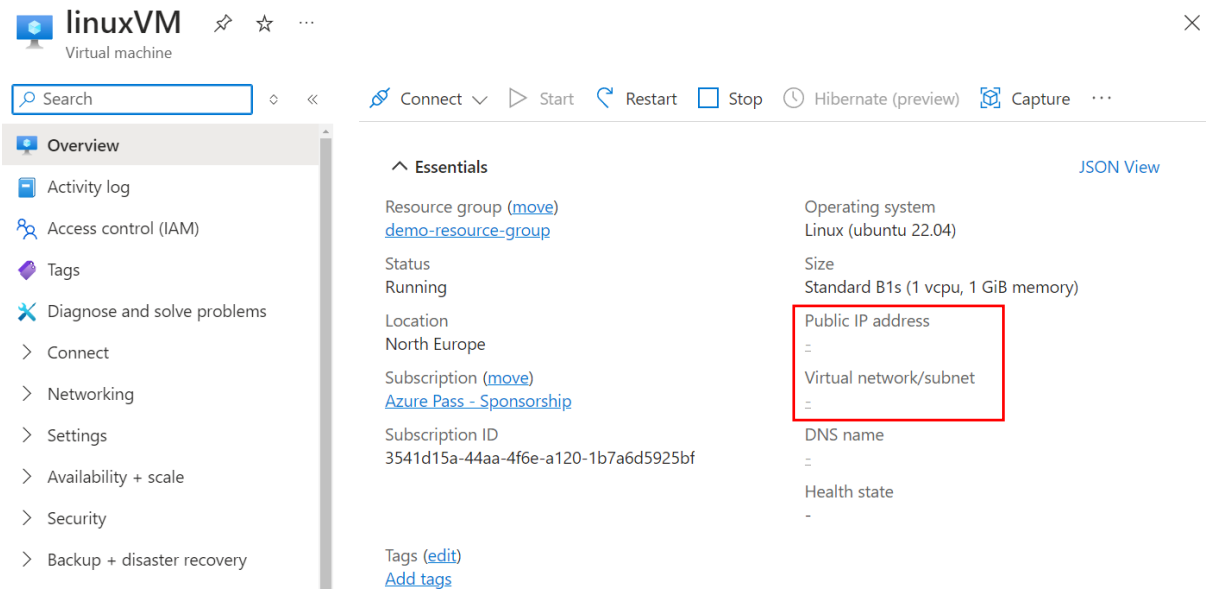


15. Then come back to your demo user and you'll be able to see the VM too.

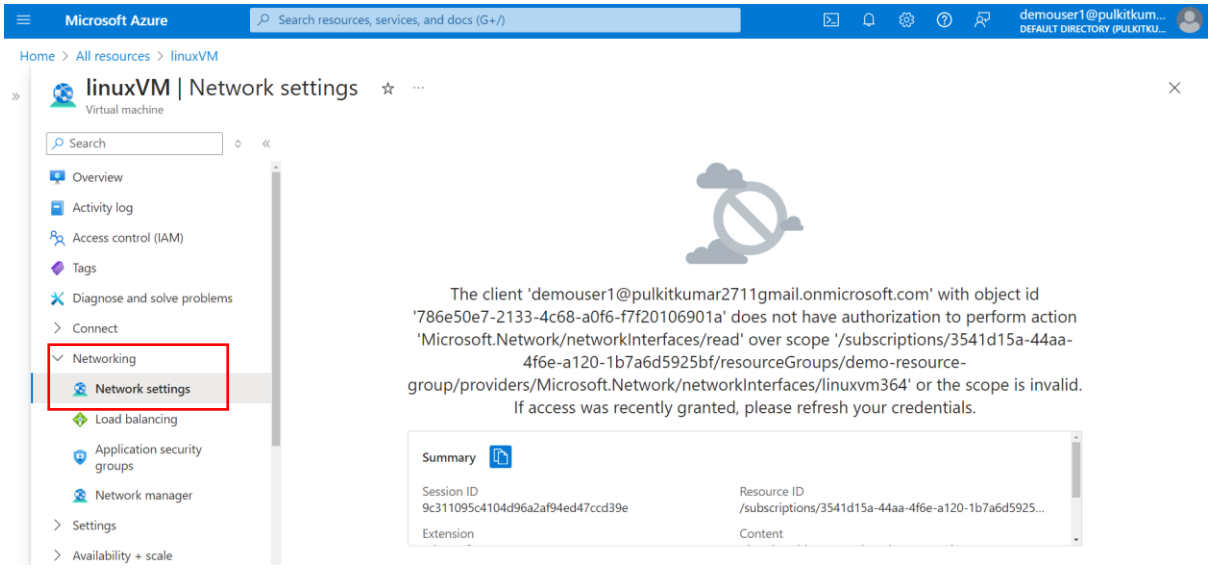


😁 Resource Group Level

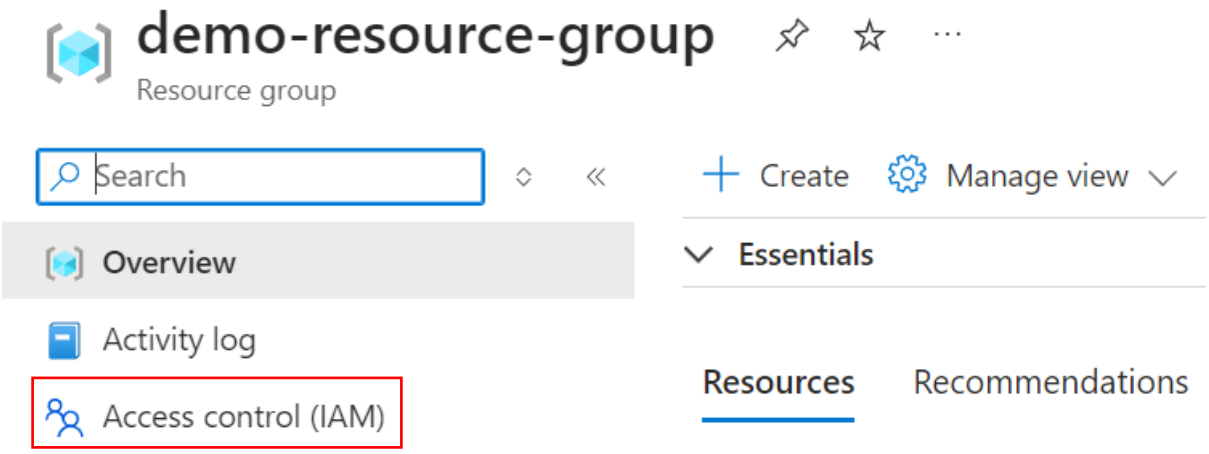
1. Now if you open your VM in you demo user, then you will notice that you cannot see the public IP address and virtual network of your VM.



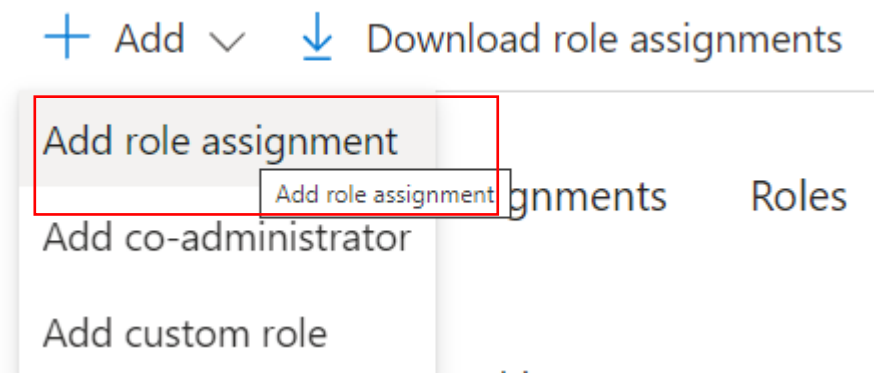
2. Then move to networking settings, there you will see that the user don't have the permission to view this.



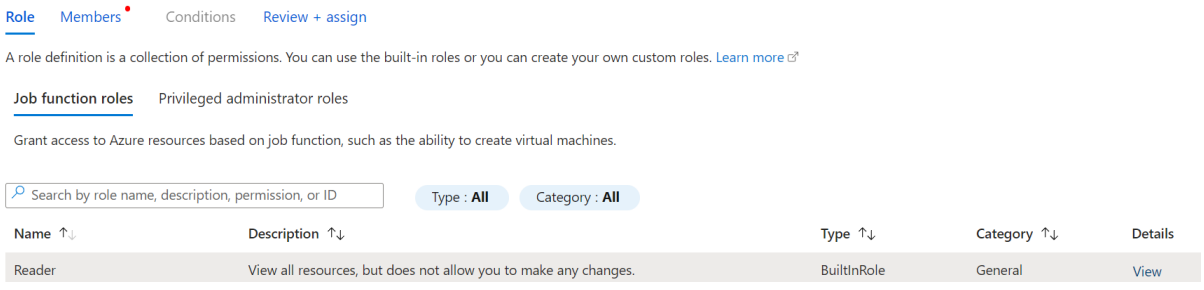
3. This is because these are the separate resources in VM and we need to give permission for all of these resources.
4. Now in your root account or main account open your resource group where you have created all the resources, here also you can see the Access control (IAM). Click on it.



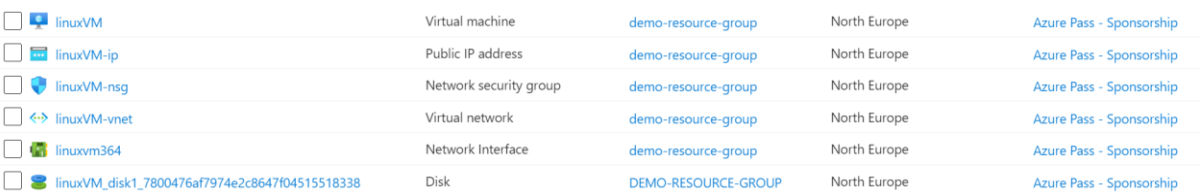
5. Here, again you have to choose add role assignment.



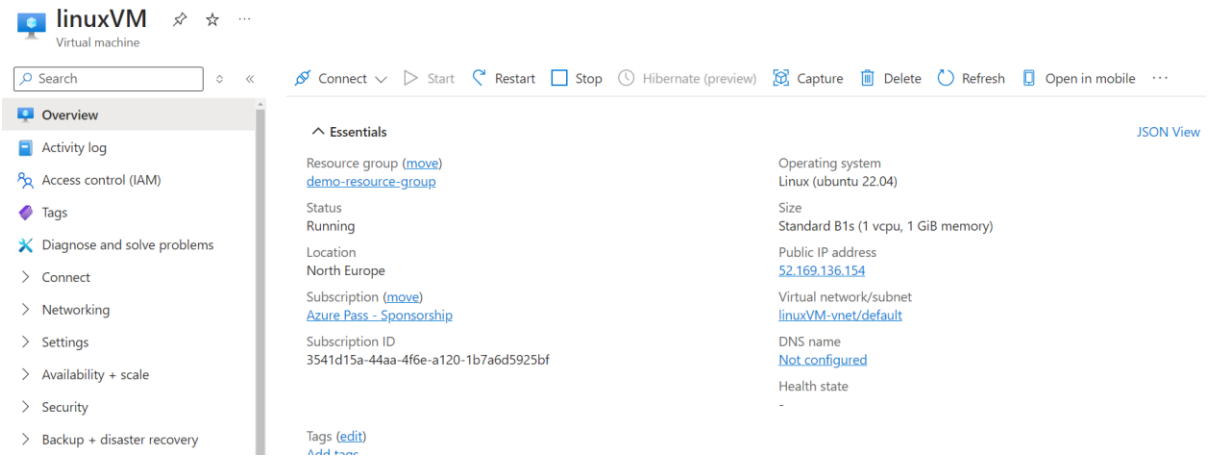
6. Then choose the reader role for it and then move to members here you have to choose demo user and then move to review and assign and create you role assignment.



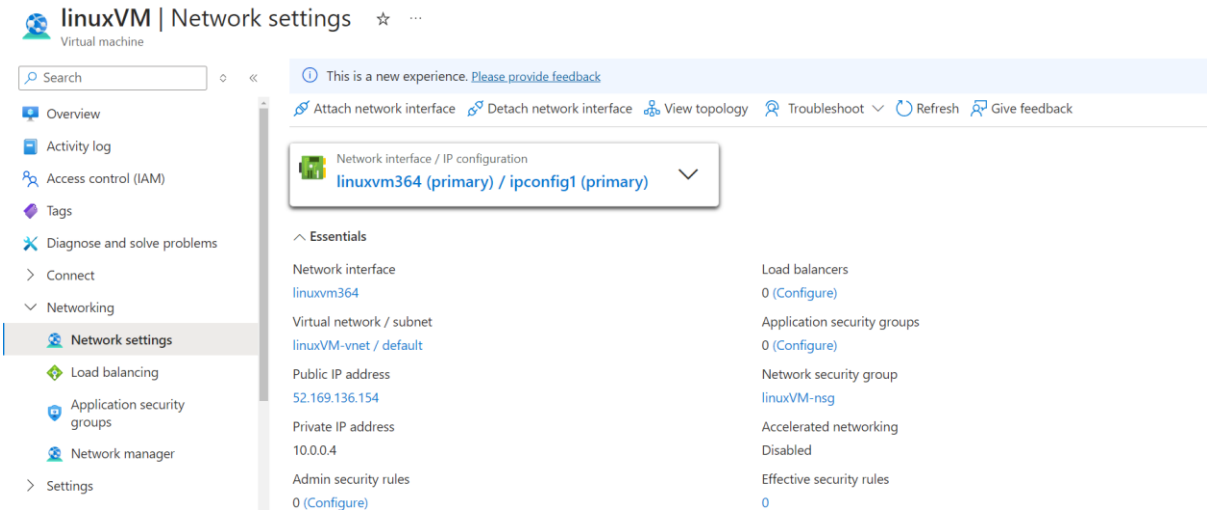
7. After that go back to your demo user tab and refresh for all resources and you will be able to see all resources in your resource group.



8. Now you can see the public IP address and Virtual network.

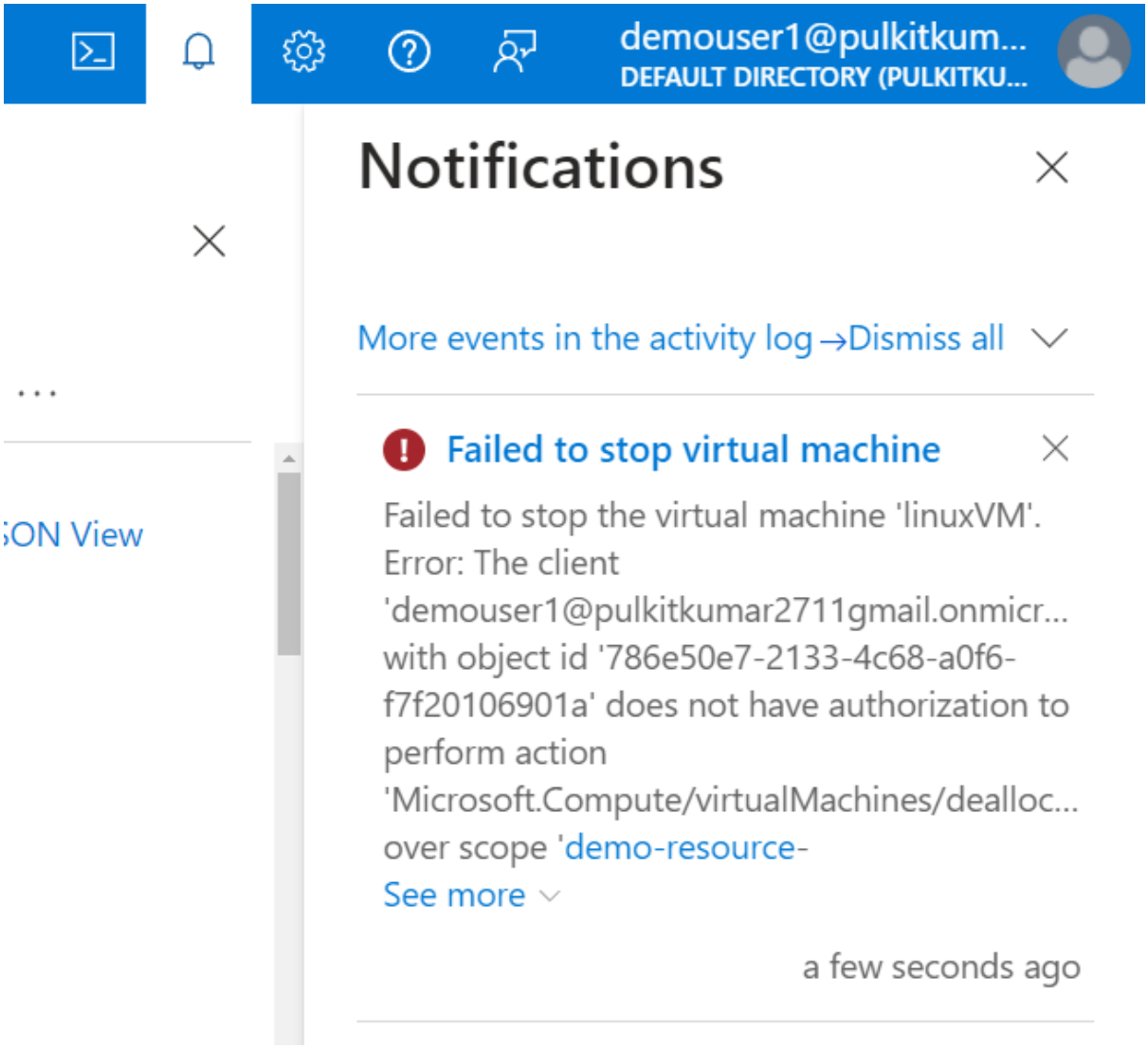


9. Also, you have access to network settings also.

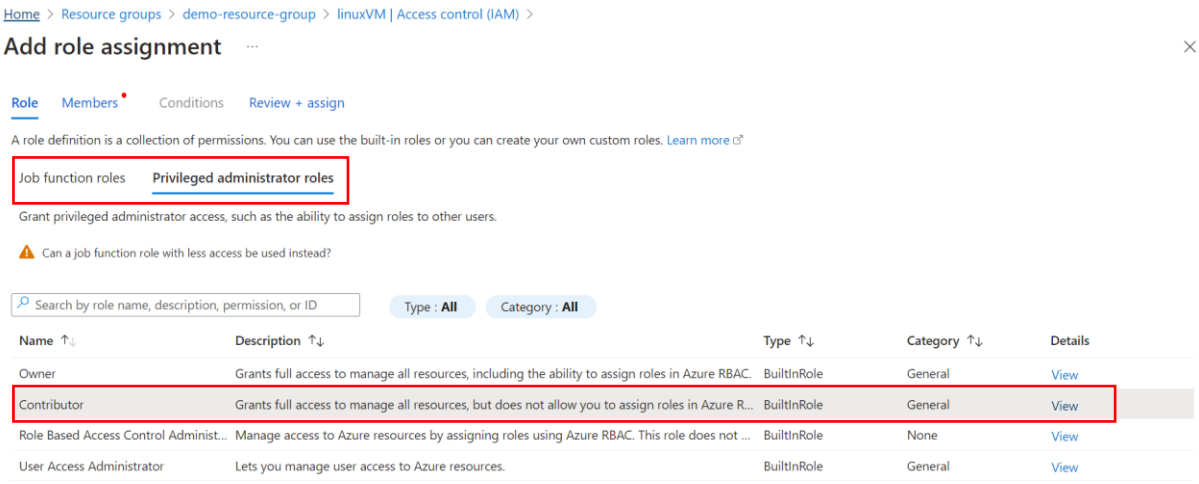


😁 Contributor Role

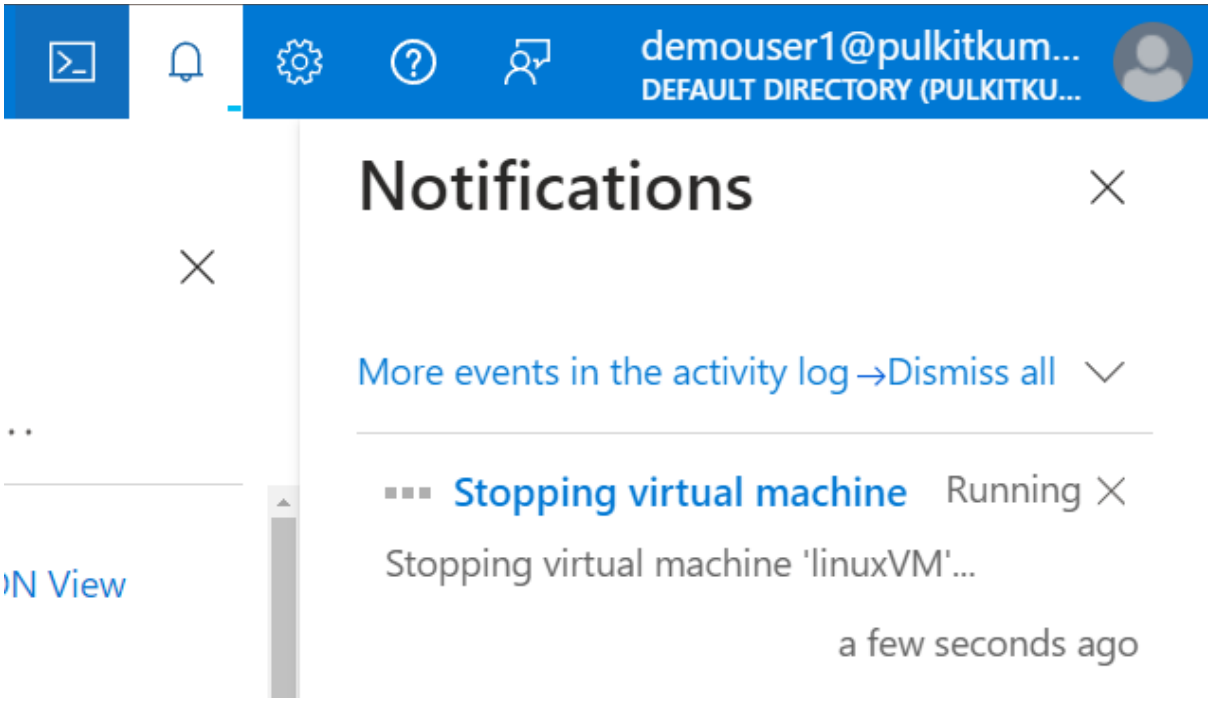
1. From your demo user try to stop the Virtual machine, immediately you will get this error, failed to stop.
2. This is because until now we have given permission to read only. If we try to perform any action in it, then it will simply say no to us.



3. So, to have the capability to stop the VM we need the contributor role in place.
4. For that we need to go to Azure admin account or say root account. From there we need to open our Virtual machine from our resource group, then we again navigate to IAM and click on add role assignment.
5. Now here first you have to choose Privileged administrator roles, after that you have to choose Contributor role as shown below.



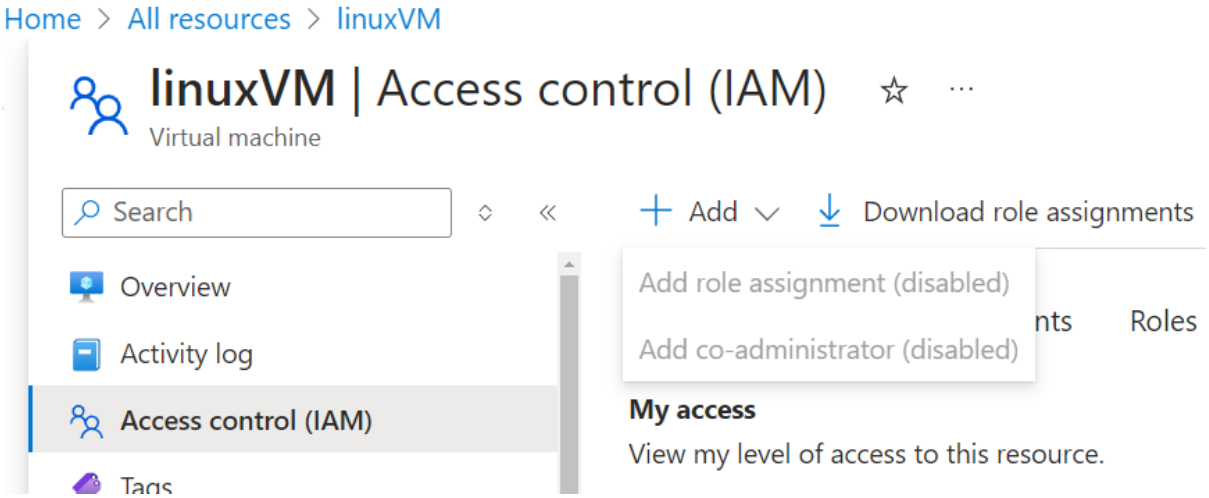
6. After that move to members choose your demo user account and then move to review and assign and create your role assignment.
7. Once your role is added, now you need to move to demo user tab and try to stop the VM again.
8. This time you'll be able to stop the VM.



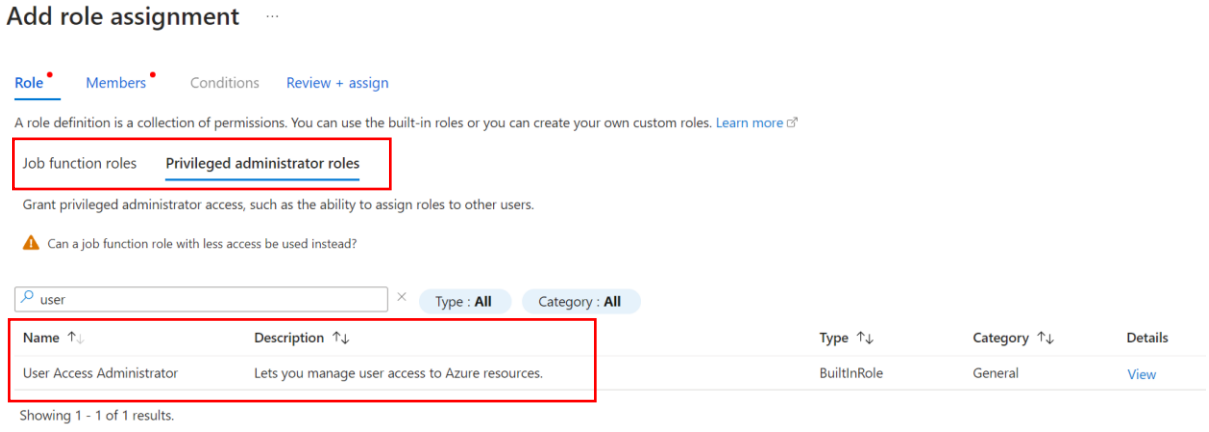
😁 User Access Administrator Role

1. Let's suppose if you have another user let say demouser2. And you want to give this user some role-based permission and you want to do that by using demouser1 account then how can you do that? You will not have the privilege to go to your Azure Admin user account and give permission.
2. For that you have to assign the user access administrator role to user1 so that it can assign the permission to user2.

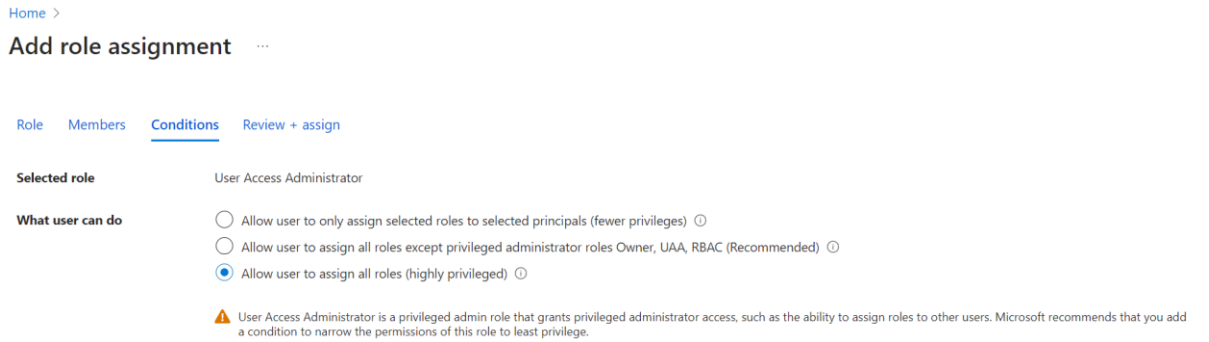
3. Currently, if you will go to demo user1 and open your VM and try to access the IAM then you will see that adding role is disabled.



4. So, to enable it you need to open your Admin user account and go to your VM then open your IAM and click on add role assignment.
5. Then choose privileged administrator roles and search for user access administrator. Choose this role then choose the demo user1 as your member and then click on review and assign.

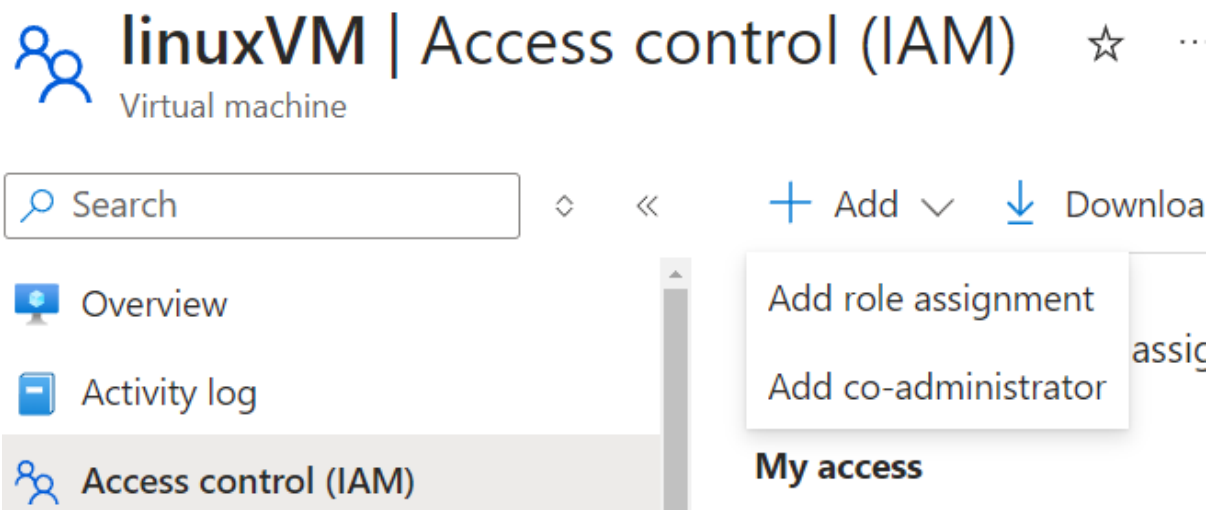


6. Then in the conditions you need to choose allow use to assign all roles.



7. Then just move to the review page and create your role assignment.

8. Now go to demo user tab and refresh the page, then you will see that you can add the role assignment now.



9. Once you are done with this lab now you need to delete your role assignment. For that in your VM go to IAM then choose role assignments here you will see all your roles assigned.
10. Then just select them and delete them.