



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).

Home > userdatastorage12_1714827256497 | Overview >

userdatastorage12 Storage account

Search | Overview | Essentials | JSON View

Activity log | Tags | Diagnose and solve problems | **Access Control (IAM)** | Data migration | Events | Storage browser | Storage Mover | Data storage | Containers | File shares | Queues | Tables

Resource group (move) | demo-resource-group | Location | northeurope | Subscription (move) | Azure Pass - Sponsorship | Subscription ID | 3541d15a-44aa-4f6e-a120-1b7a6d5925bf | Disk state | Available | Tags (edit) | Add tags

Performance | Standard | Replication | Locally-redundant storage (LRS) | Account kind | StorageV2 (general purpose v2) | Provisioning state | Succeeded | Created | 5/4/2024, 6:24:37 PM

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

+ Add ▾ Download role assignments

Add role assignment

assignments Roles

Add co-administrator

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

Role Members Conditions Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

Search by role name, description, permission, or ID Type: All Category: All

Name ↑	Description ↑	Type ↑↓	Category ↑↓	Details
Reader	View all resources, but does not allow you to make any changes.	BuiltInRole	General	View

6. For members click on select members.

Role **Members** • Conditions Review + assign

Selected role Reader

Assign access to User, group, or service principal
 Managed identity

Members + Select members

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

Select members X

Select (i)

Search by name or email address



demouser1
demouser1@pulkitkumar2711@gmail.onmicrosoft.com



PULKIT KUMAR
pulkitkumar2711_gmail.com#EXT#@pulkitkumar271...

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.

The screenshot shows the Microsoft Azure 'All resources' page. At the top, there's a search bar and a navigation bar with options like 'Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', 'Assign tags', and 'Delete'. Below the navigation bar, there are several filter buttons: 'Subscription equals all', 'Resource group equals all', 'Type equals all', 'Location equals all', and an 'Add filter' button. The main table lists resources under categories: 'Recommendations' (0), 'Changed resources' (1), and 'Unsecure resources' (0). The first resource listed is a 'Storage account' named 'userdataservice12', which is part of the 'demo-resource-group' in 'North Europe' under the 'Azure Pass - Sponsorship' subscription.

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.

The screenshot shows the Azure VM Overview page for a VM named 'linuxVM'. On the left, there's a sidebar with options like 'Activity log', 'Access control (IAM)' (which is highlighted with a red box), 'Tags', 'Diagnose and solve problems', 'Connect', 'Networking', 'Settings', 'Availability + scale', and 'Security'. The main pane displays the VM's details under the 'Essentials' section, including its resource group ('demo-resource-group'), operating system ('Linux (Ubuntu 22.04)'), status ('Running'), location ('North Europe'), subscription ('Azure Pass - Sponsorship'), subscription ID ('3541d15a-44aa-4f6e-a120-1b7a6d5925bf'), public IP address ('52.169.136.154'), virtual network/subnet ('linuxVM-vnet/default'), DNS name ('Not configured'), and health state ('-').

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

The screenshot shows the Microsoft Azure 'All resources' page again. The 'Access control (IAM)' section from the previous screenshot has been completed, and the VM is now visible in the list of resources. It appears under the 'Changed resources' category with a count of 2. The VM is listed as a 'Virtual machine' with the name 'linuxVM', located in 'demo-resource-group' in 'North Europe' under the 'Azure Pass - Sponsorship' subscription.

😊 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.

The screenshot shows the Azure portal interface for a virtual machine named 'linuxVM'. The left sidebar contains navigation links like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Networking, Settings, Availability + scale, Security, and Backup + disaster recovery. The main content area is titled 'Essentials' and includes fields for Resource group, Status, Location, Subscription, Tags, and Public IP address. The 'Public IP address' field is highlighted with a red box.

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

The screenshot shows the 'Network settings' page for the 'linuxVM' virtual machine. The left sidebar has a red box around the 'Networking' section, which contains 'Network settings', 'Load balancing', 'Application security groups', 'Network manager', 'Settings', and 'Availability + scale'. The main content area displays a message about missing permissions to read network interfaces, along with a summary table showing Session ID, Resource ID, Extension, and Content.

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.

The screenshot shows the Azure Resource Group 'demo-resource-group' overview page. At the top, there's a search bar and navigation links for 'Create' and 'Manage view'. Below the search bar, there are tabs: 'Overview' (selected), 'Activity log', and 'Access control (IAM)'. The 'Access control (IAM)' tab is highlighted with a red box. On the right, there are sections for 'Resources' and 'Recommendations'.

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

The screenshot shows the 'Add role assignment' dialog box. It has a 'Role' dropdown set to 'Add co-administrator' and a 'Members' tab selected. There are buttons for 'Add role assignment' (highlighted with a red box) and 'Download role assignments'. Below the dialog, there's a link to 'Add custom role'.

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.

The screenshot shows the 'Reader' role definition page. The 'Members' tab is selected. The table lists the Reader role with its description: 'View all resources, but does not allow you to make any changes.' The 'Members' column shows a single entry for 'demo'.

Name	Description	Type	Category	Details
Reader	View all resources, but does not allow you to make any changes.	BuiltinRole	General	View

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.

<input type="checkbox"/> linuxVM	Virtual machine	demo-resource-group	North Europe	Azure Pass - Sponsorship
<input type="checkbox"/> linuxVM-ip	Public IP address	demo-resource-group	North Europe	Azure Pass - Sponsorship
<input type="checkbox"/> linuxVM-nsg	Network security group	demo-resource-group	North Europe	Azure Pass - Sponsorship
<input type="checkbox"/> linuxVM-vnet	Virtual network	demo-resource-group	North Europe	Azure Pass - Sponsorship
<input type="checkbox"/> linuxvm364	Network Interface	demo-resource-group	North Europe	Azure Pass - Sponsorship
<input type="checkbox"/> linuxVM_disk1_7800476af7974e2c8647f04515518338	Disk	DEMO-RESOURCE-GROUP	North Europe	Azure Pass - Sponsorship

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

The screenshot shows the Azure portal interface for a virtual machine named 'linuxVM'. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Networking, Settings, Availability + scale, Security, and Backup + disaster recovery. The main content area is titled 'Essentials' and displays the following information:

Setting	Value
Resource group	(move) demo-resource-group
Status	Running
Location	North Europe
Subscription	(move) Azure Pass - Sponsorship
Subscription ID	3541d15a-44aa-4f6e-a120-1b7a6d5925bf
Operating system	Linux (ubuntu 22.04)
Size	Standard B1s (1 vcpu, 1 GiB memory)
Public IP address	52.169.136.154
Virtual network/subnet	linuxVM-vnet/default
DNS name	Not configured
Health state	-

At the bottom of the essentials section, there are 'Tags (edit)' and 'Add more' buttons.

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

The screenshot shows the 'Network settings' page for the 'linuxVM' virtual machine. The left sidebar has a 'Networking' section with 'Network settings' selected, which is highlighted with a blue bar. Other options include Load balancing, Application security groups, and Network manager. The main content area shows the 'Network interface / IP configuration' for 'linuxvm364 (primary) / ipconfig1 (primary)'. The 'Essentials' section displays the following network details:

Setting	Value
Network interface	linuxvm364
Virtual network / subnet	linuxVM-vnet / default
Public IP address	52.169.136.154
Private IP address	10.0.0.4
Admin security rules	0 (Configure)
Load balancers	0 (Configure)
Application security groups	0 (Configure)
Network security group	linuxVM-nsg
Accelerated networking	Disabled
Effective security rules	0

😊 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.

The screenshot shows the Azure portal interface with a blue header bar. On the left, there's a navigation menu with 'JSON View' selected. The main content area has a title 'Notifications' with a close button 'X'. Below it, there's a message 'More events in the activity log → Dismiss all' with a dropdown arrow. A horizontal line separates this from a list of notifications. The first notification is a failed action: 'Failed to stop virtual machine' with an exclamation mark icon. It details the error: 'Failed to stop the virtual machine 'linuxVM''. It mentions an error from the client with object id '786e50e7-2133-4c68-a0f6-f7f20106901a' and states that the user does not have authorization to perform the action. It also specifies the scope as 'Microsoft.Compute/virtualMachines/dealloc...' over scope 'demo-resource-'. There's a 'See more' link and a timestamp 'a few seconds ago'.

More events in the activity log → Dismiss all

Failed to stop virtual machine

Failed to stop the virtual machine 'linuxVM'.
Error: The client
'demouser1@pulkitkumar2711gmail.onmicrosoft.com'
with object id '786e50e7-2133-4c68-a0f6-f7f20106901a' does not have authorization to
perform action
'Microsoft.Compute/virtualMachines/dealloc...' over scope 'demo-resource-'
[See more](#)

a few seconds ago

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.

Add role assignment

X

Role Members * Conditions Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Job function roles **Privileged administrator roles**

Grant privileged administrator access, such as the ability to assign roles to other users.

⚠️ Can a job function role with less access be used instead?

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.	BuiltInRole	General	View
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure R...	BuiltInRole	General	View
Role Based Access Control Administ...	Manage access to Azure resources by assigning roles using Azure RBAC. This role does not ...	BuiltInRole	None	View
User Access Administrator	Lets you manage user access to Azure resources.	BuiltInRole	General	View

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.



Notifications

X

More events in the activity log → [Dismiss all](#) ▾

...

...

...

Stopping virtual machine Running X

Stopping virtual machine 'linuxVM'...

a few seconds ago

N View

😊 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.

Home > All resources > linuxVM

The screenshot shows the 'Access control (IAM)' page for a virtual machine named 'linuxVM'. The 'Add' button is highlighted, and a tooltip indicates that role assignments are disabled. The 'My access' section shows that the user has no access to this resource.

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.

Add role assignment ...

The screenshot shows the 'Add role assignment' dialog. The 'Privileged administrator roles' tab is selected. A search bar shows 'user'. A table lists the 'User Access Administrator' role, which is described as letting you manage user access to Azure resources. The 'Details' column shows it's a 'BuiltInRole' under the 'General' category.

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

Home >

Add role assignment ...

The screenshot shows the 'Add role assignment' dialog with the 'Conditions' tab selected. The 'Selected role' is set to 'User Access Administrator'. In the 'What user can do' section, the 'Allow user to assign all roles (highly privileged)' option is selected. A note at the bottom states that User Access Administrator is a highly privileged role and recommends adding a condition to narrow its permissions.

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

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

The screenshot shows the 'Access control (IAM)' blade for a virtual machine named 'linuxVM'. The 'Add' button is highlighted, and a tooltip shows options like 'Add role assignment' and 'Add co-administrator'. The 'My access' section is also visible.

- 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.
- Then just select them and delete them.

The screenshot shows the 'Role assignments' blade for the 'linuxVM' virtual machine. The 'Role assignments' tab is selected, showing 7 assignments. A 'View assignments' link is visible.