

Secure your Azure resources with Azure role-based access control (Azure RBAC)

1. Introduction

<https://learn.microsoft.com/en-us/training/modules/secure-azure-resources-with-rbac/1-introduction>

Introduction

Completed

For any organization using the cloud, securing your Azure resources such as virtual machines, websites, networks, and storage is a critical function. You want to ensure that your data and assets are protected, but still grant your employees and partners the access they need to perform their jobs. Azure RBAC is an authorization system in Azure that helps you manage who has access to Azure resources, what they can do with those resources, and where they have access.

Suppose you work for First Up Consultants, which is an engineering firm that specializes in circuit and electrical design. They've moved their workloads and assets to Azure to make collaboration easier across several offices and other companies. You work in the IT department at First Up Consultants. You're responsible for keeping the company's assets secure, but still allowing users to access the resources they need. You've heard that Azure RBAC can help you manage resources in Azure.

In this module, you'll learn how to use Azure RBAC to manage access to resources in Azure.

Learning objectives

In this module, you'll:

- Verify access to resources for yourself and others.
- Grant access to resources.
- View activity logs of Azure RBAC changes.

2. What is Azure RBAC?

What is Azure RBAC?

Completed

When it comes to identity and access, most organizations that are considering using the public cloud are concerned about two things:

1. Ensuring that when people leave the organization, they lose access to resources in the cloud.
2. Striking the right balance between autonomy and central governance. For example, giving project teams the ability to create and manage virtual machines in the cloud, while centrally controlling the networks those VMs use to communicate with other resources.

Microsoft Entra ID and Azure RBAC work together to make it simple to carry out these goals.

Azure subscriptions

First, remember that each Azure subscription is associated with a single Microsoft Entra directory. Users, groups, and applications in that directory can manage resources in the Azure subscription. The subscriptions use Microsoft Entra ID for single sign-on (SSO) and access management. You can extend your on-premises Active Directory to the cloud by using **Microsoft Entra Connect**. This feature allows your employees to manage their Azure subscriptions by using their existing work identities. When you disable an on-premises Active Directory account, it automatically loses access to all Azure subscriptions connected with Microsoft Entra ID.

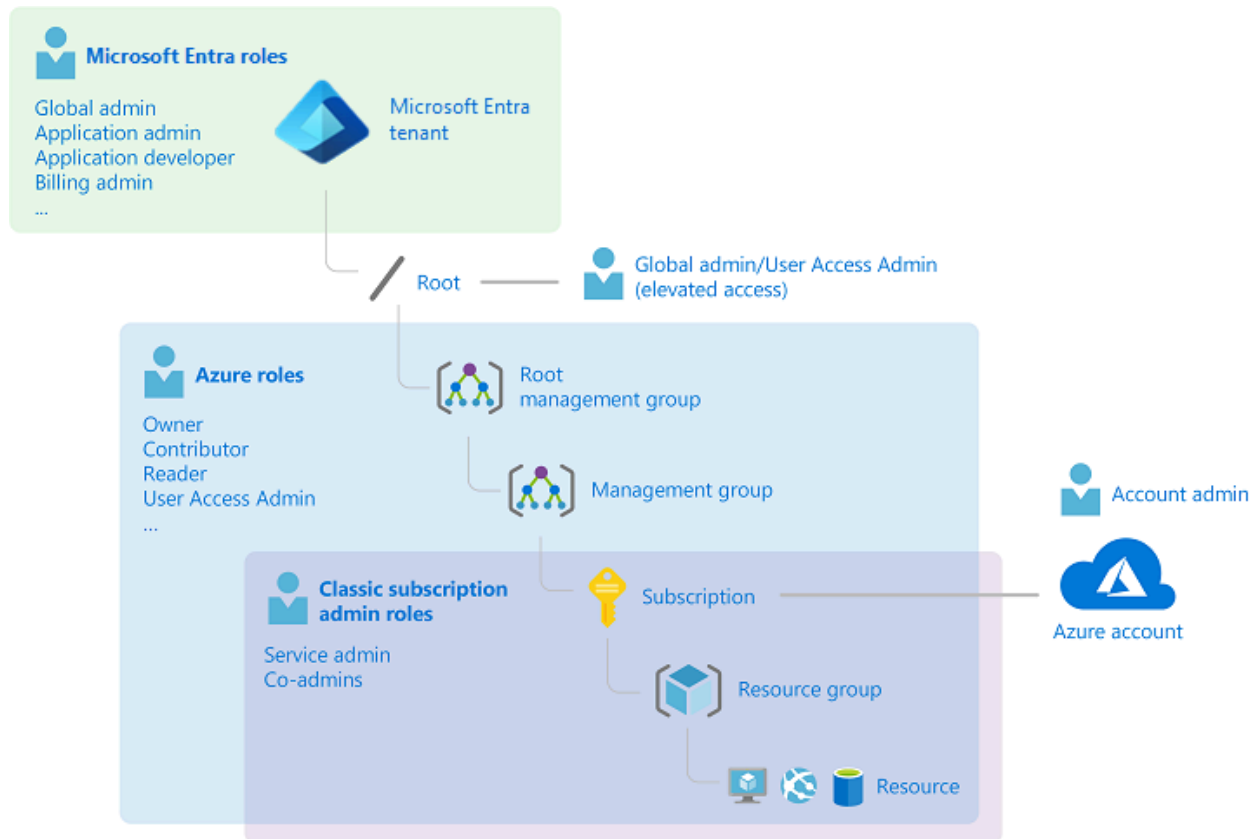
What's Azure RBAC?

Azure RBAC is an authorization system built on Azure Resource Manager that provides fine-grained access management for resources in Azure. With Azure RBAC, you can grant the exact access that users need to do their jobs. For example, you can use Azure RBAC to let one employee manage virtual machines in a subscription, while another manages SQL databases within the same subscription.

The following video describes Azure RBAC in detail:

You can grant access by assigning the appropriate Azure role to users, groups, and applications at a certain scope. The scope of a role assignment can be a management group, subscription, a resource group, or a single resource. A role assigned at a parent scope also grants access to the child scopes contained within it. For example, a user with access to a resource group can manage all the resources it contains like websites, virtual machines, and subnets. The Azure role that you assign dictates what resources the user, group, or application can manage within that scope.

The following diagram depicts how the classic subscription administrator roles, Azure roles, and Microsoft Entra roles are related at a high level. Child scopes, such as service instances, inherit roles assigned at a higher scope, like an entire subscription.



In the preceding diagram, a subscription is associated with only one Microsoft Entra tenant. Also note that a resource group can have multiple resources, but it's associated with only one subscription. Although it's not obvious from the diagram, a resource can be bound to only one resource group.

What can I do with Azure RBAC?

Azure RBAC allows you to grant access to Azure resources that you control. Suppose you need to manage access to resources in Azure for the development, engineering, and marketing teams. You've started to receive access requests, and you need to quickly learn how access management works for Azure resources.

Here are some scenarios you can implement with Azure RBAC:

- Allow one user to manage virtual machines in a subscription and another user to manage virtual networks.
- Allow a database administrator group to manage SQL databases in a subscription.
- Allow a user to manage all resources in a resource group, such as virtual machines, websites, and subnets.
- Allow an application to access all resources in a resource group.

Azure RBAC in the Azure portal

In several areas in the Azure portal, you'll see a pane named **Access control (IAM)**, also known as *identity and access management*. On this pane, you can see who has access to that area and their role. Using this same pane, you can grant or remove access.

The following shows an example of the Access control (IAM) pane for a resource group. In this example, Alain has been assigned the Backup Operator role for this resource group.

The screenshot shows the Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information (alain@contoso.com). The breadcrumb trail indicates the path: Home > Resource groups > sales-projectforecast. The main pane is titled 'sales-projectforecast | Access control (IAM)'. On the left, a sidebar lists various tools, with 'Access control (IAM)' highlighted. The main content area shows 'Check access' tabs and a summary of role assignments (58 out of 4000). Below this is a table of role assignments for the subscription, with 25 items listed. A red box highlights the first entry: 'Backup Operator' assigned to 'Alain' (alain@contoso.com) as a User, with the scope 'This resource' and condition 'None'.

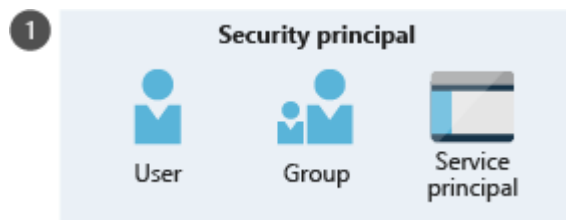
Name	Type	Role	Scope	Condition
Alain alain@contoso.com	User	Backup Operator	This resource	None
App2	App	Billing Reader	Subscription (Inherited)	None
Sales Admins	Group	Billing Reader	Subscription (Inherited)	None
user-assigned-identity	User-assigned Managed Identity	Billing Reader	Subscription (Inherited)	None

How does Azure RBAC work?

You can control access to resources using Azure RBAC by creating role assignments, which control how permissions are enforced. To create a role assignment, you need three elements: a security principal, a role definition, and a scope. You can think of these elements as *who*, *what*, and *where*.

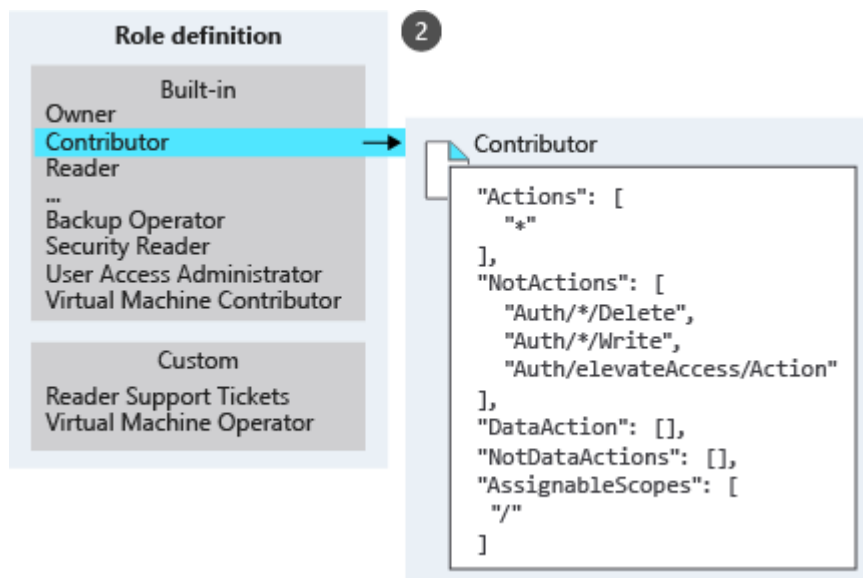
1. Security principal (who)

A *security principal* is just a fancy name for a user, group, or application to which you want to grant access.



2. Role definition (what)

A *role definition* is a collection of permissions. It's sometimes just called a role. A role definition lists the permissions the role can perform such as read, write, and delete. Roles can be high-level, like Owner, or specific, like Virtual Machine Contributor.



Azure includes several built-in roles that you can use. The following lists four fundamental built-in roles:

- **Owner:** Has full access to all resources, including the right to delegate access to others.
- **Contributor:** Can create and manage all types of Azure resources, but can't grant access to others.
- **Reader:** Can view existing Azure resources.
- **User Access Administrator:** Lets you manage user access to Azure resources.

If the built-in roles don't meet the specific needs of your organization, you can create your own custom roles.

3. Scope (where)

Scope is the level where the access applies. This is helpful if you want to make someone a Website Contributor but only for one resource group.

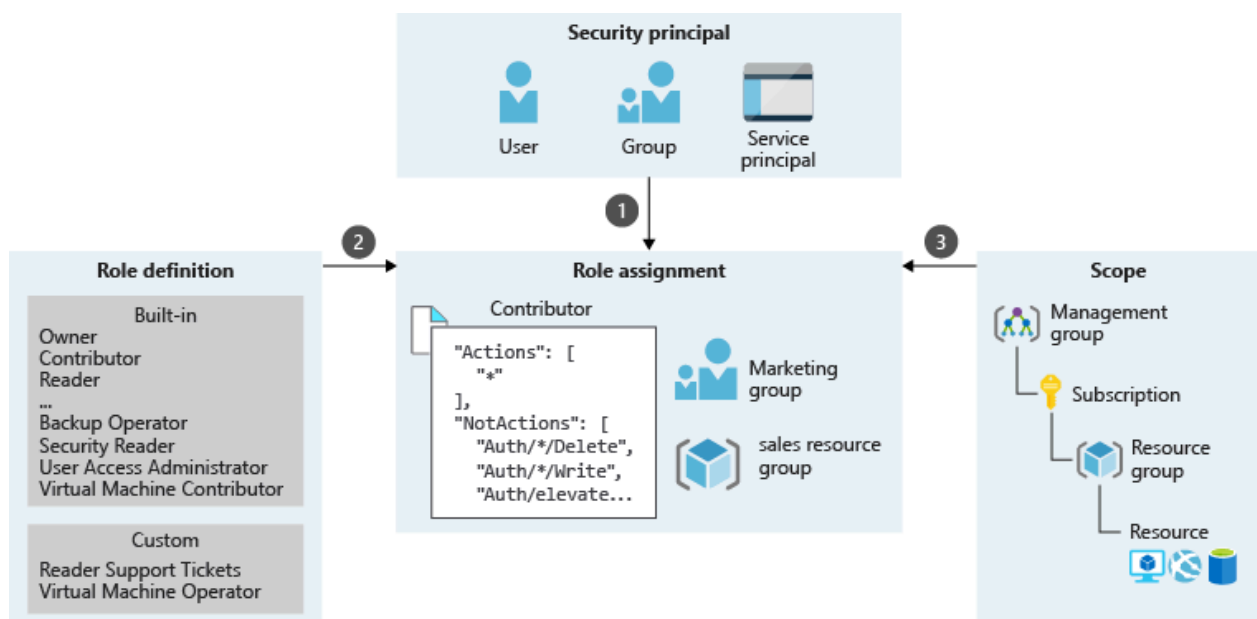
In Azure, you can specify a scope at multiple levels: management group, subscription, resource group, or resource. Scopes are structured in a parent-child relationship. When you grant access at a parent scope, the child scopes automatically inherit those permissions. For example, if a group is assigned the Contributor role at the subscription scope, it will inherit the role for all resource groups and resources within the subscription.



Role assignment

Once you have determined the who, what, and where, you can combine those elements to grant access. A *role assignment* is the process of binding a role to a security principal at a particular scope for the purpose of granting access. To grant access, you'll create a role assignment. To revoke access, you'll remove a role assignment.

The following example shows how the Marketing group has been assigned the Contributor role at the sales resource group scope.



Azure RBAC is an allow model

Azure RBAC is an *allow* model. This means that when you're assigned a role, Azure RBAC allows you to perform certain actions such as read, write, or delete. If one role assignment grants you read permissions to a resource group, and a different role assignment grants you write permissions to the same resource group, then you'll have read and write permissions on that resource group.

Azure RBAC has something called `NotActions` permissions. You can use `NotActions` to create a set of not allowed permissions. The access a role grants—the *effective permissions*—is computed by subtracting the `NotActions` operations from the `Actions` operations. For example, the [Contributor](#) role has both `Actions` and `NotActions`. The wildcard (*) in `Actions` indicates that it can perform all operations on the control plane. You'd then subtract the following operations in `NotActions` to compute the effective permissions:

- Delete roles and role assignments
- Create roles and role assignments
- Grant the caller User Access Administrator access at the tenant scope
- Create or update any blueprint artifacts
- Delete any blueprint artifacts

3. Knowledge check - What is Azure RBAC?

<https://learn.microsoft.com/en-us/training/modules/secure-azure-resources-with-rbac/3-knowledge-check-rbac-overview>

Knowledge check - What is Azure RBAC?

Completed

4. Exercise - List access using Azure RBAC and the Azure portal

<https://learn.microsoft.com/en-us/training/modules/secure-azure-resources-with-rbac/4-list-access>

Exercise - List access using Azure RBAC and the Azure portal

Completed

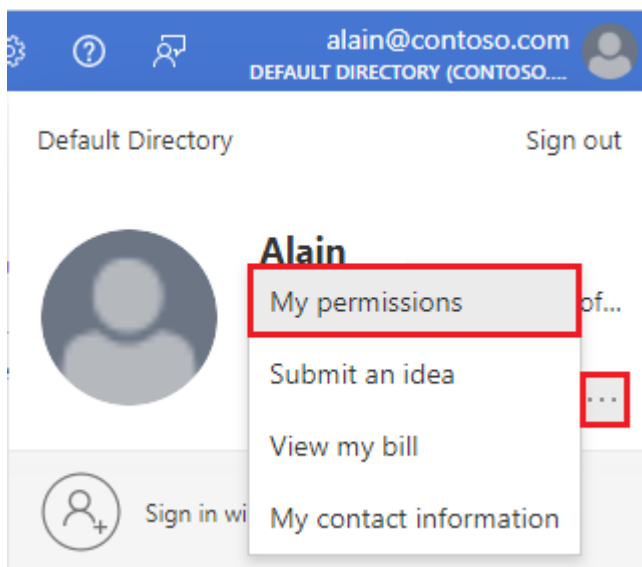
At First Up Consultants, you've been granted access to a resource group for the marketing team. You want to familiarize yourself with the Azure portal and see what roles are currently assigned.

You need an Azure subscription to complete the exercises. If you don't have an Azure subscription, create a [free account](#) and add a subscription before you begin. If you're a student, you can take advantage of the [Azure for students](#) offer.

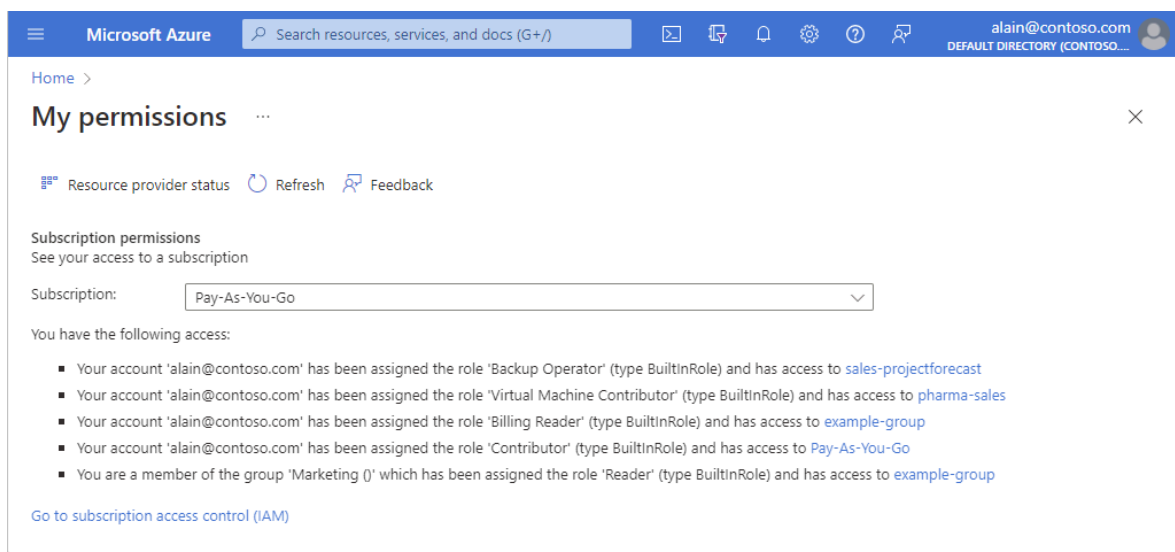
List role assignments for yourself

Follow these steps to see what roles are currently assigned to you.

1. Sign in to the [Azure portal](#).
2. On the **Profile** menu, select the ellipsis (...) to see more links.



3. Select **My permissions** to open the **My permissions** pane.

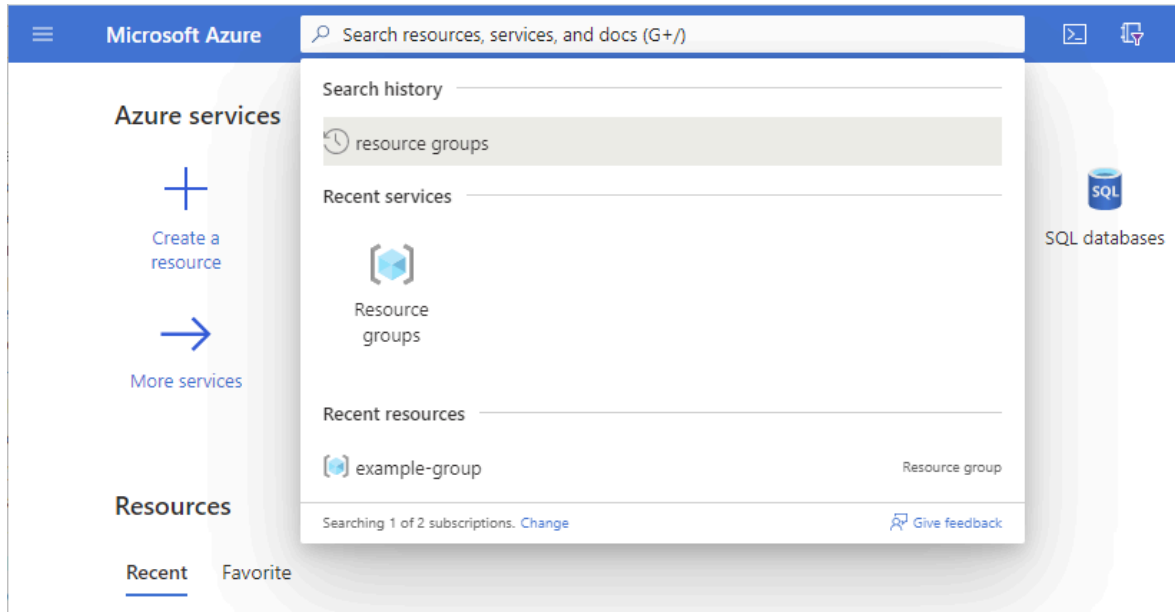


You'll find the roles that you've been assigned and the scope. Your list will look different.

List role assignments for a resource group

Follow these steps to see what roles are assigned at the resource group scope.

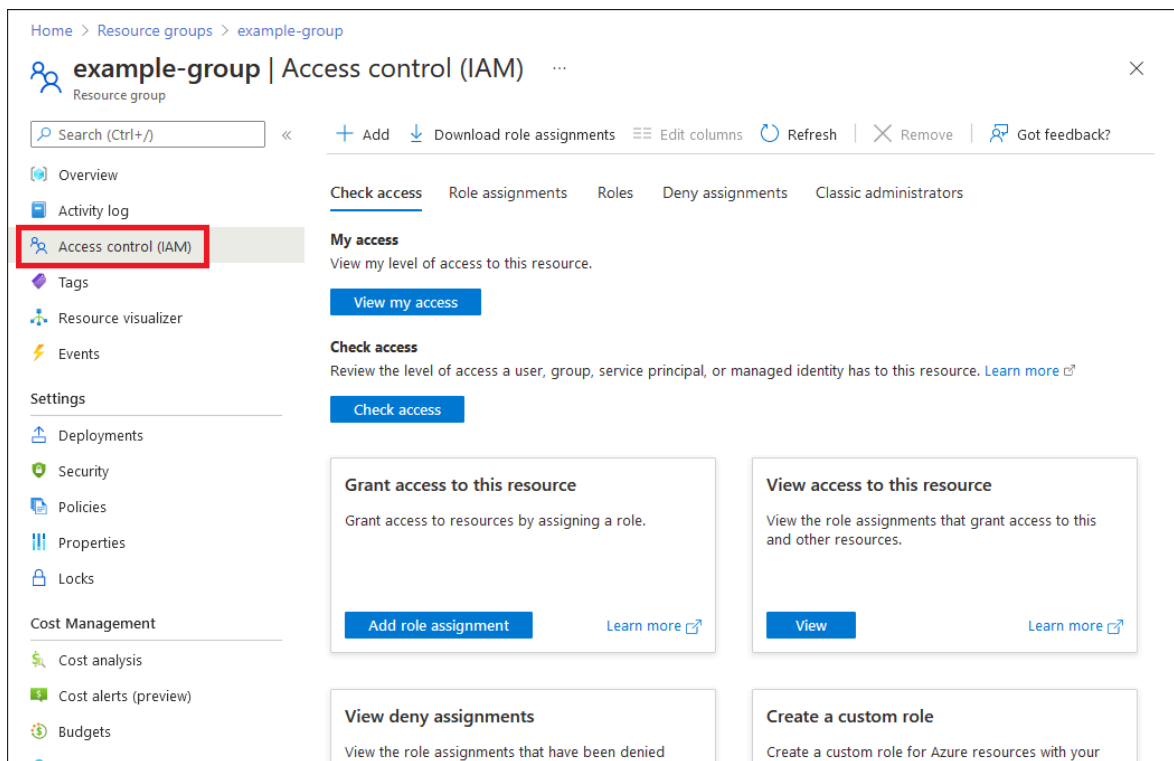
1. In the Search box at the top, search for and select **Resource groups**.



2. In the list of resource groups, select a resource group.

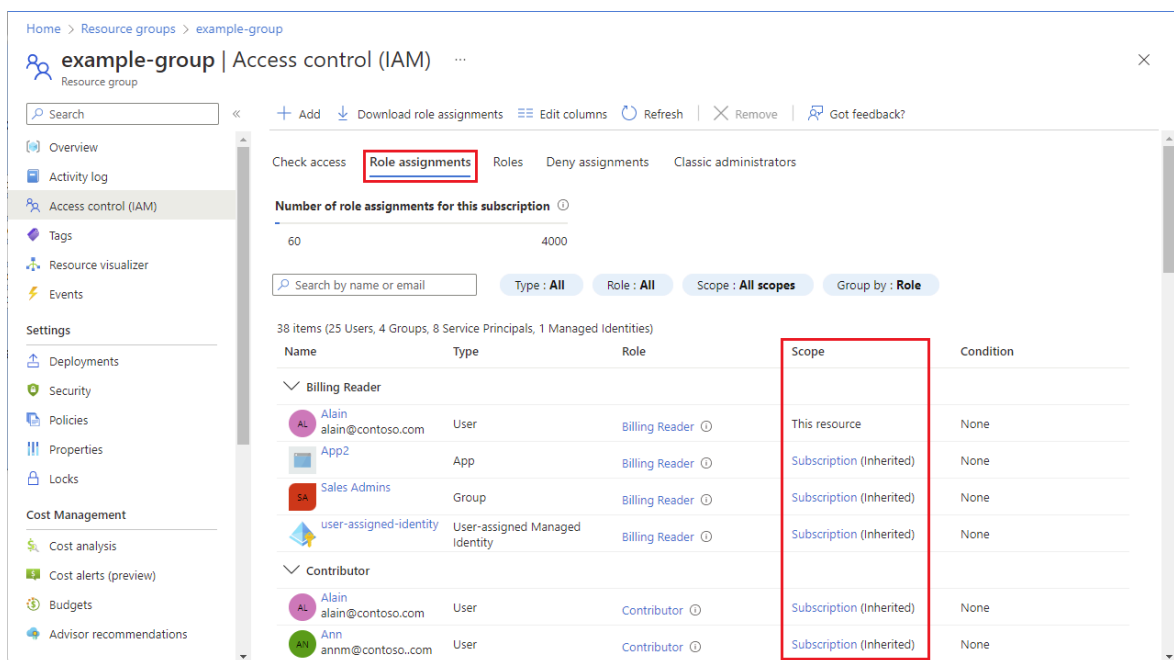
These steps use a resource group named **example-group**, but your resource group's name will be different.

3. On the left menu pane, select **Access control (IAM)**.



4. Select the **Role assignments** tab.

This tab shows who has access to the resource group. Notice that some roles are scoped to **This resource**, while others are **(Inherited)** from a parent scope.

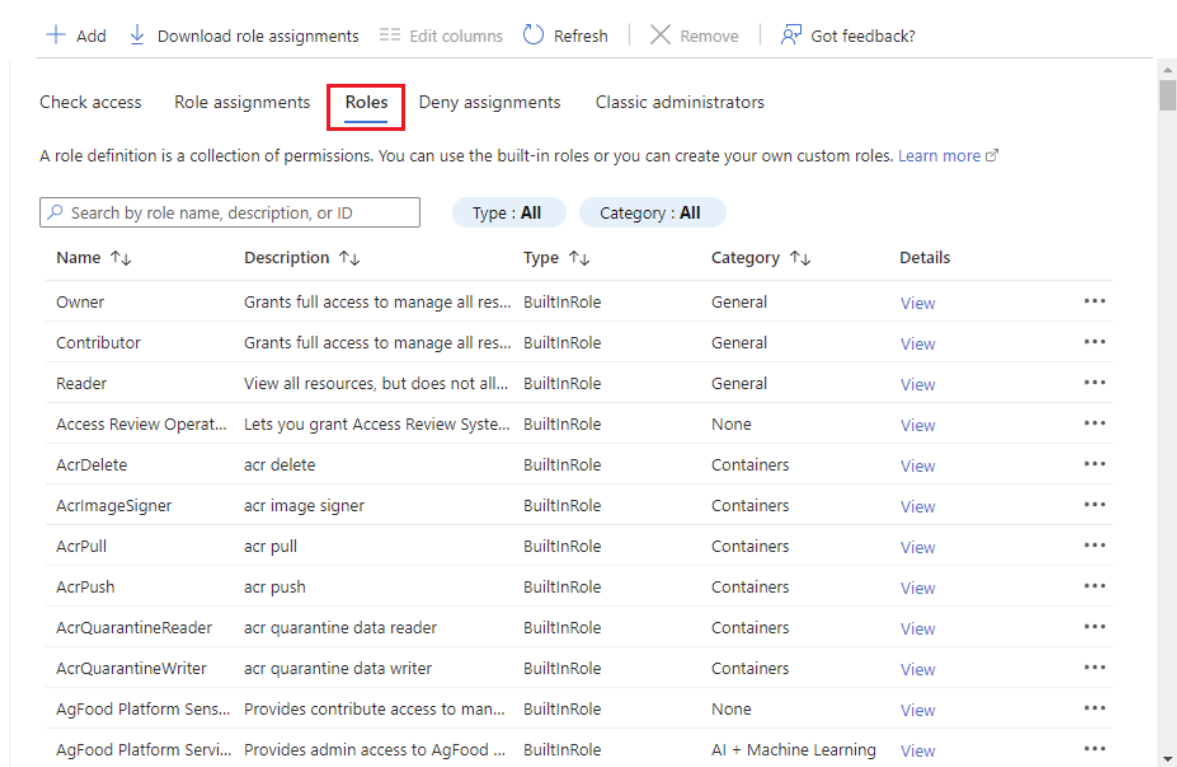


List roles

As you learned in the previous unit, a role is a collection of permissions. Azure has more than 70 built-in roles that you can use in your role assignments. To list the roles:

- In the menu bar at the top of the pane, select the **Roles** tab to list of all the built-in and custom roles.

Select a role's **View** link in the **Details** column, then select the **Assignments** tab to display the number of users and groups assigned to that role.



Check access Role assignments **Roles** Deny assignments Classic administrators

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](#)

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

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Owner	Grants full access to manage all res...	BuiltInRole	General	View ...
Contributor	Grants full access to manage all res...	BuiltInRole	General	View ...
Reader	View all resources, but does not all...	BuiltInRole	General	View ...
Access Review Operat...	Lets you grant Access Review Syste...	BuiltInRole	None	View ...
AcrDelete	acr delete	BuiltInRole	Containers	View ...
AcrImageSigner	acr image signer	BuiltInRole	Containers	View ...
AcrPull	acr pull	BuiltInRole	Containers	View ...
AcrPush	acr push	BuiltInRole	Containers	View ...
AcrQuarantineReader	acr quarantine data reader	BuiltInRole	Containers	View ...
AcrQuarantineWriter	acr quarantine data writer	BuiltInRole	Containers	View ...
AgFood Platform Sens...	Provides contribute access to man...	BuiltInRole	None	View ...
AgFood Platform Servi...	Provides admin access to AgFood ...	BuiltInRole	AI + Machine Learning	View ...

In this unit, you learned how to list the role assignments for yourself in the Azure portal. You also learned how to list the role assignments for a resource group.

5. Exercise - Grant access using Azure RBAC and the Azure portal

<https://learn.microsoft.com/en-us/training/modules/secure-azure-resources-with-rbac/5-grant-access>

Exercise - Grant access using Azure RBAC and the Azure portal

Completed

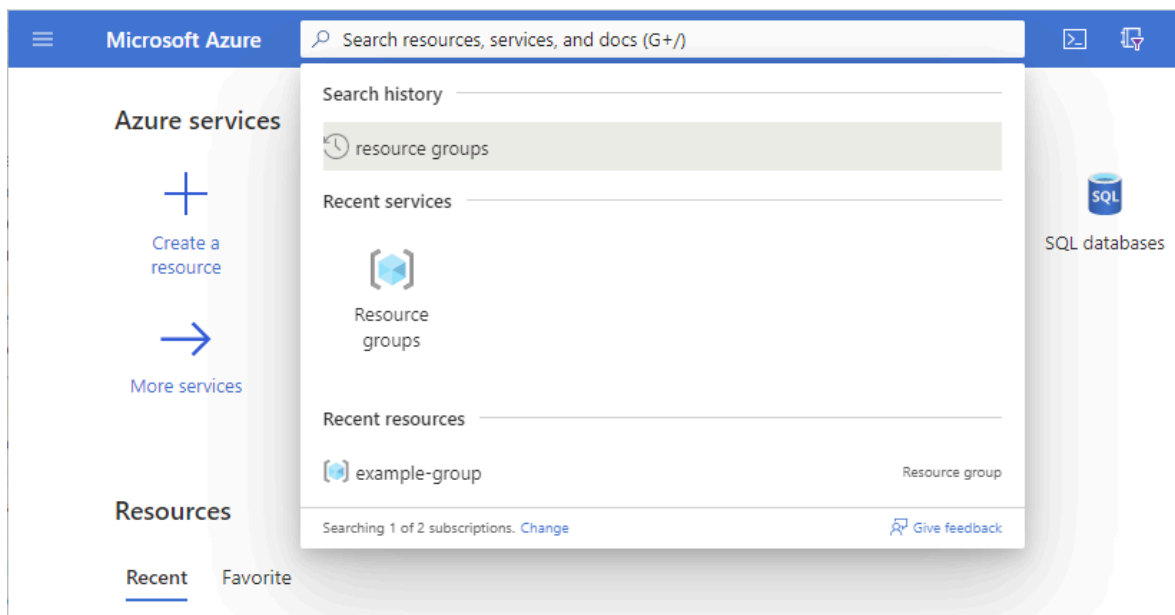
A coworker named Alain at First Up Consultants needs permission to create and manage virtual machines for a project on which they're working. Your manager has asked that you handle this

request. Using the best practice to grant users the least privileges to get their work done, you decide to assign Alain the Virtual Machine Contributor role for a resource group.

Grant access

Follow this procedure to assign the Virtual Machine Contributor role to a user at the resource group scope.

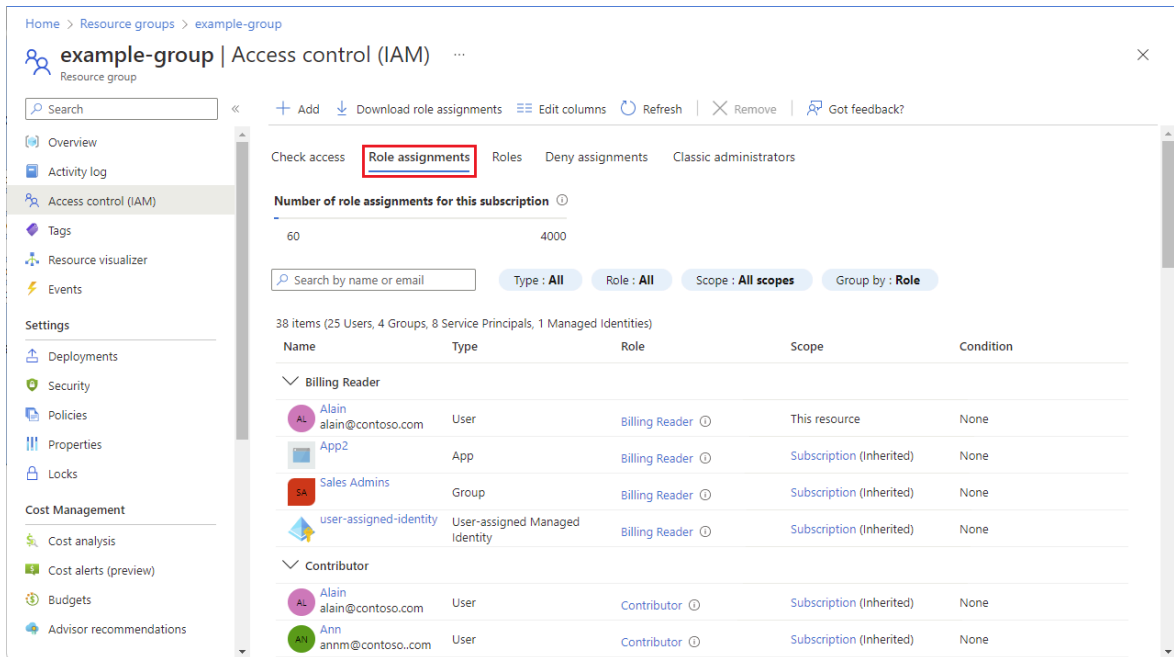
1. Sign in to the [Azure portal](#) as an administrator that has permissions to assign roles, such as [User Access Administrator](#) or [Owner](#).
2. In the Search box at the top, search for **Resource groups**.



3. In the list of resource groups, select a resource group.

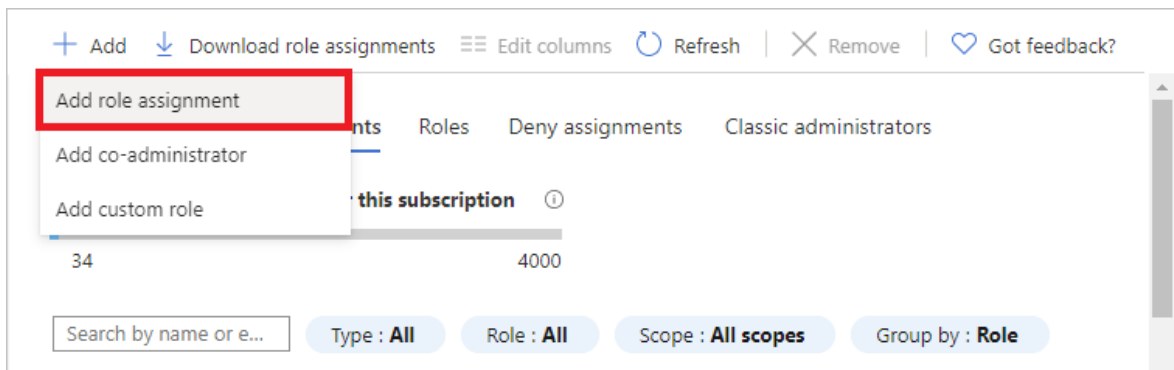
These steps use a resource group named **example-group**, but your resource group's name will be different.

4. On the left menu pane, select **Access control (IAM)**.
5. Select the **Role assignments** tab to display the current list of role assignments at this scope.



6. Select **Add > Add role assignment**.

If you don't have permissions to assign roles, the **Add role assignment** option will be disabled.



The **Add role assignment** page opens.

7. On the **Role** tab, search for and select **Virtual Machine Contributor**.

Home > Resource groups > example-group | Access control (IAM) >

Add role assignment

Got feedback?

Role Members 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](#)

virtual machine Type: All Category: All

Showing 10 of 372 roles

Name	Description	Type	Category	Details
Classic Virtual Machine Contributor	Lets you manage classic virtual machines, but not access to them, and not t...	BuiltInRole	Compute	View
Desktop Virtualization Power On Contributor	This role is in preview and subject to change. Provide permission to the Azur...	BuiltInRole	None	View
Desktop Virtualization Power On Off Contr...	This role is in preview and subject to change. Provide permission to the Azur...	BuiltInRole	None	View
Desktop Virtualization Virtual Machine Cont...	This role is in preview and subject to change. Provide permission to the Azur...	BuiltInRole	None	View
DevTest Labs User	Lets you connect, start, restart, and shutdown your virtual machines in your ...	BuiltInRole	Devops	View
Virtual Machine Administrator Login	View Virtual Machines in the portal and login as administrator	BuiltInRole	Compute	View
Virtual Machine Contributor	Lets you manage virtual machines, but not access to them, and not the virtu...	BuiltInRole	Compute	View
Virtual Machine Local User Login	View Virtual Machines in the portal and login as a local user configured on t...	BuiltInRole	None	View
Virtual Machine Operator	Can monitor and restart virtual machines.	CustomRole	None	View

Review + assign Previous Next

8. Select **Next**.

9. On the **Members** tab, select **Select members**.

10. Search for and select a user.

Home > Resource groups > example-group | Access control (IAM) >

Add role assignment

Got feedback?

Role **Members** Review + assign

Selected role
Virtual Machine Contributor

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

Members
[+ Select members](#)

Name	Object ID	Type
No members selected		

Description
Optional

Review + assign Previous Next

Select members

Select

alain

AT Alain Team

Selected members:

AL Alain
alain@contoso.com [Remove](#)

Select Close

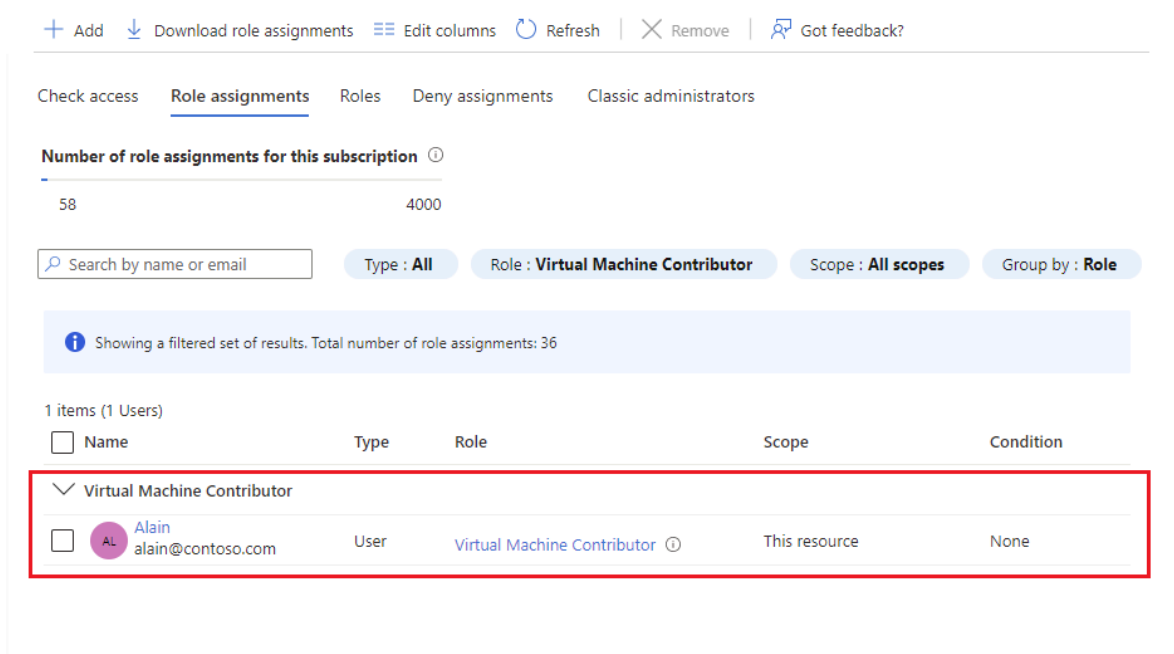
11. Select **Select** to add the user to the Members list.

12. Select **Next**.

13. On the **Review + assign** tab, review the role assignment settings.

14. Select **Review + assign** to assign the role.

After a few moments, the user is assigned the Virtual Machine Contributor role at the resource group scope. The user can now create and manage virtual machines just within this resource group.



Top navigation: + Add, Download role assignments, Edit columns, Refresh, Remove, Got feedback?

Check access | **Role assignments** | Roles | Deny assignments | Classic administrators

Number of role assignments for this subscription ⓘ
58 / 4000

Search by name or email | Type : All | Role : Virtual Machine Contributor | Scope : All scopes | Group by : Role

Showing a filtered set of results. Total number of role assignments: 36

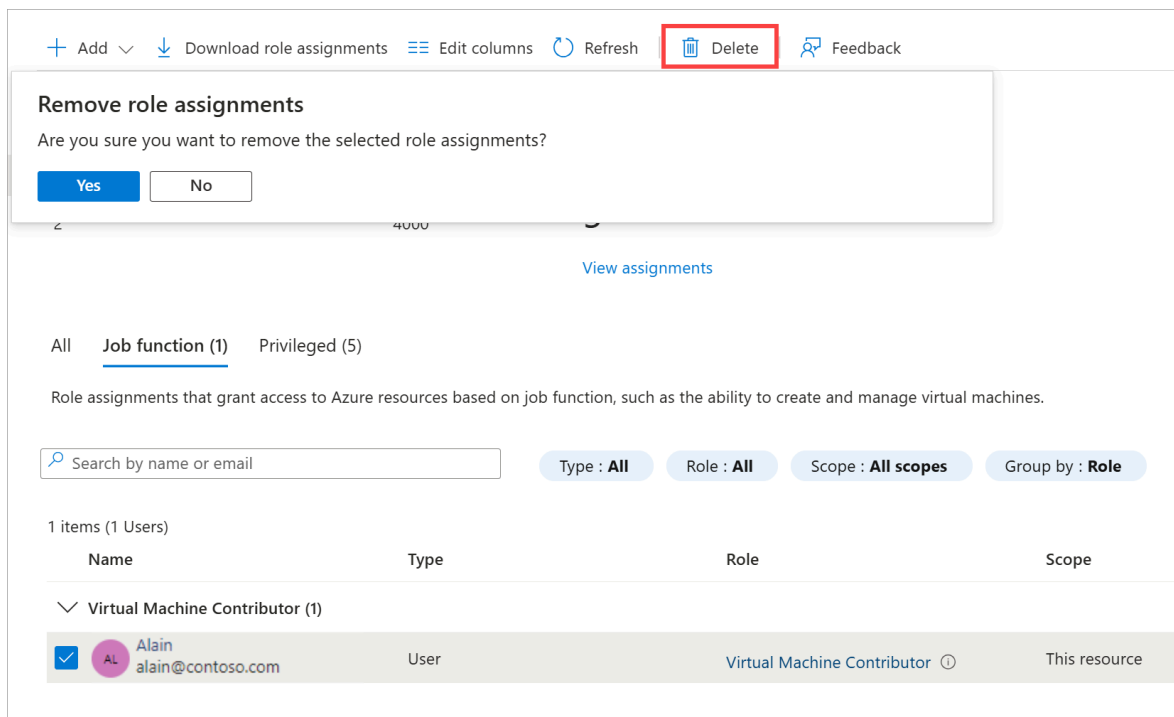
1 items (1 Users)

☐	Name	Type	Role	Scope	Condition
☒	Virtual Machine Contributor				
☐	 Alain alain@contoso.com	User	Virtual Machine Contributor ⓘ	This resource	None

Remove access

In Azure RBAC, you can remove a role assignment to remove access.

1. In the list of role assignments, select **View Assignments**.
2. Search for and check the box for the user with the Virtual Machine Contributor role.
3. Select **Delete**.



4. In the **Remove role assignments** message that appears, select **Yes**.

In this unit, you learned how to grant a user access to create and manage virtual machines in a resource group using the Azure portal.

6. Exercise - View activity logs for Azure RBAC changes

<https://learn.microsoft.com/en-us/training/modules/secure-azure-resources-with-rbac/6-view-activity-logs>

Exercise - View activity logs for Azure RBAC changes

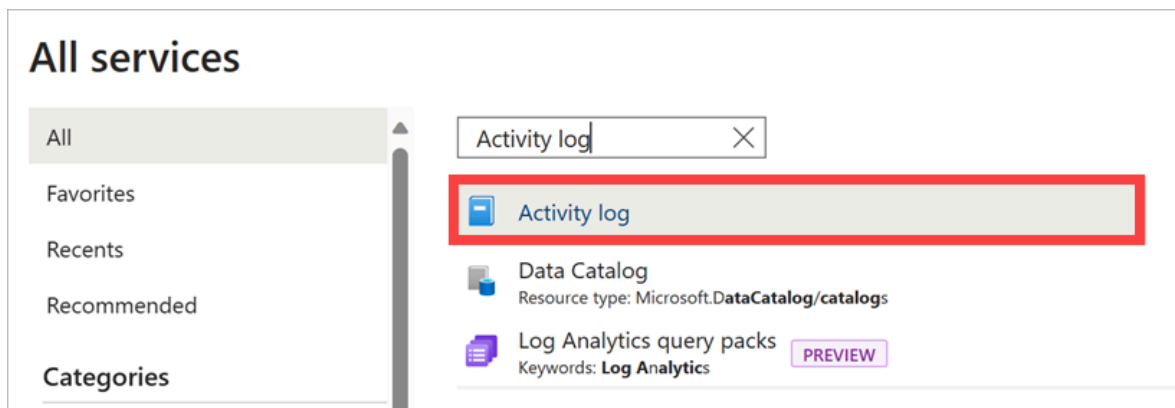
Completed

First Up Consultants reviews Azure RBAC changes quarterly for auditing and troubleshooting purposes. You know that changes get logged in the [Azure Activity Log](#). Your manager has asked if you can generate a report of the role assignment and custom role changes for the last month.

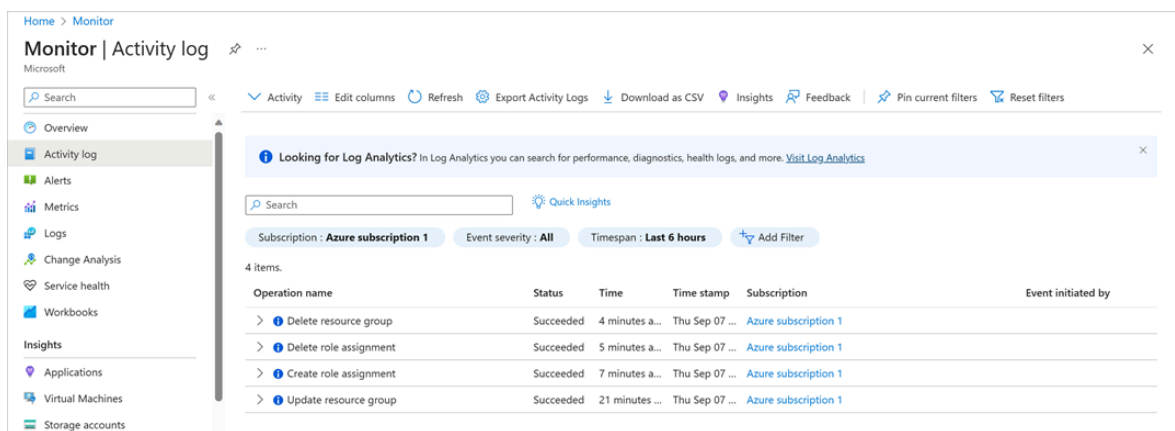
View activity logs

The easiest way to get started is to view the activity logs with the Azure portal.

1. Select **All services**, then search for **Activity log**.



2. Select **Activity log** to open the activity log.

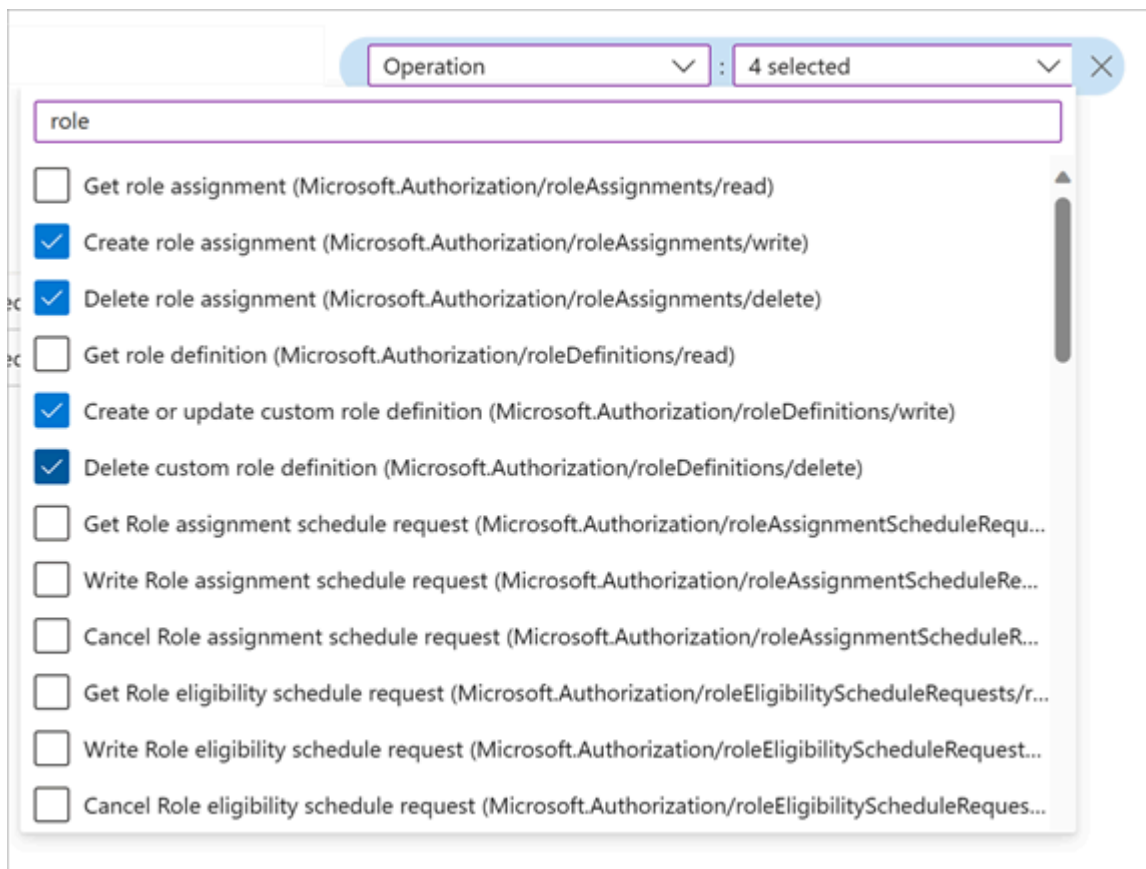


3. Set the **Timespan** filter to **Last month**.

4. Add an **Operation** filter and type **role** to filter the list.

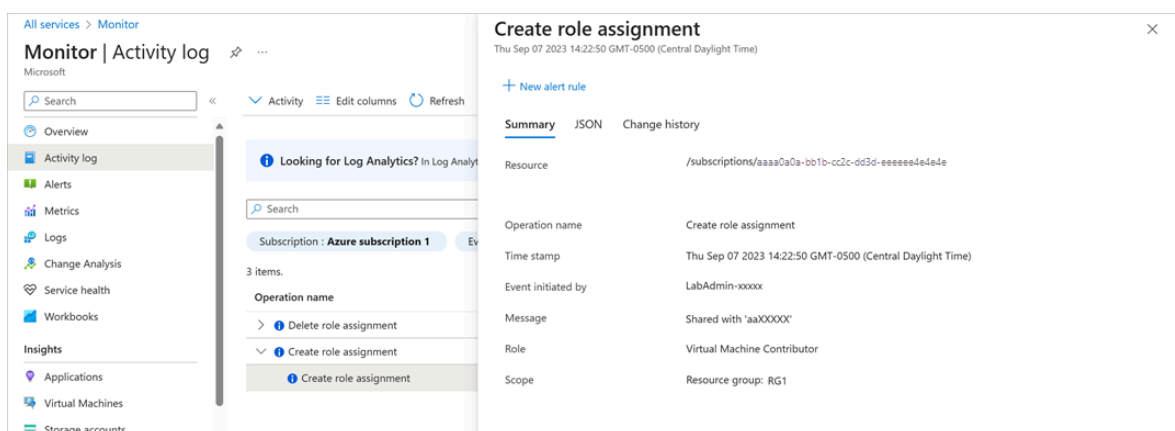
5. Select the following Azure RBAC operations:

- Create role assignment (roleAssignments)
- Delete role assignment (roleAssignments)
- Create or update custom role definition (roleDefinitions)
- Delete custom role definition (roleDefinitions)



After a moment, you'll get a list of all the role assignment and role definition operations for the last month. There's also a button at the top of the screen to download the activity log as a CSV file.

6. Select one of the operations to get the activity log details.



In this unit, you learned how to use Azure Activity Log to list Azure RBAC changes in the portal and generate a simple report.

7. Module assessment

Module assessment

Completed

8. Summary

<https://learn.microsoft.com/en-us/training/modules/secure-azure-resources-with-rbac/8-summary>

Summary

Completed

In this module, you learned about Azure RBAC, and how you can use it to secure your Azure resources. To grant access, you assign users a role at a particular scope. Using Azure RBAC, you can grant only the amount of access to users that they need to perform their jobs.

Azure RBAC has more than 200 built-in roles. However, if your organization needs specific permissions, you can create your own custom roles. Azure keeps track of your Azure RBAC changes in case you need to see what changes were made in the past.

Further reading

To continue learning about Azure RBAC, check out [What is Azure role-based access control \(Azure RBAC\)?](#).