



Introduction

2 minutes

Securing your Azure resources, such as virtual machines, websites, networks, and storage, is a critical function for any organization using the cloud. 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. Role-based access control (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.

As an example, 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, where you are responsible for keeping the company's assets secure, but still allowing users to access the resources they need. You've heard that RBAC can help you manage resources in Azure.

In this module, you will learn how to use role-based access control (RBAC) to manage access to resources in Azure.

Learning objectives

In this module, you will:

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

Next unit: What is RBAC?

Continue >



What is RBAC?

8 minutes

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.

Azure Active Directory (Azure AD) and Role-Based Access Control (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 Azure AD directory. Users, groups, and applications in that directory can manage resources in the Azure subscription. The subscriptions use Azure AD for single sign-on (SSO) and access management. You can extend your on-premises Active Directory to the cloud by using **Azure AD 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 Azure AD.

What is RBAC?

Role-based access control (RBAC) is an authorization system built on Azure Resource Manager that provides fine-grained access management of resources in Azure. With RBAC, you can grant the exact access that users need to do their jobs. For example, you

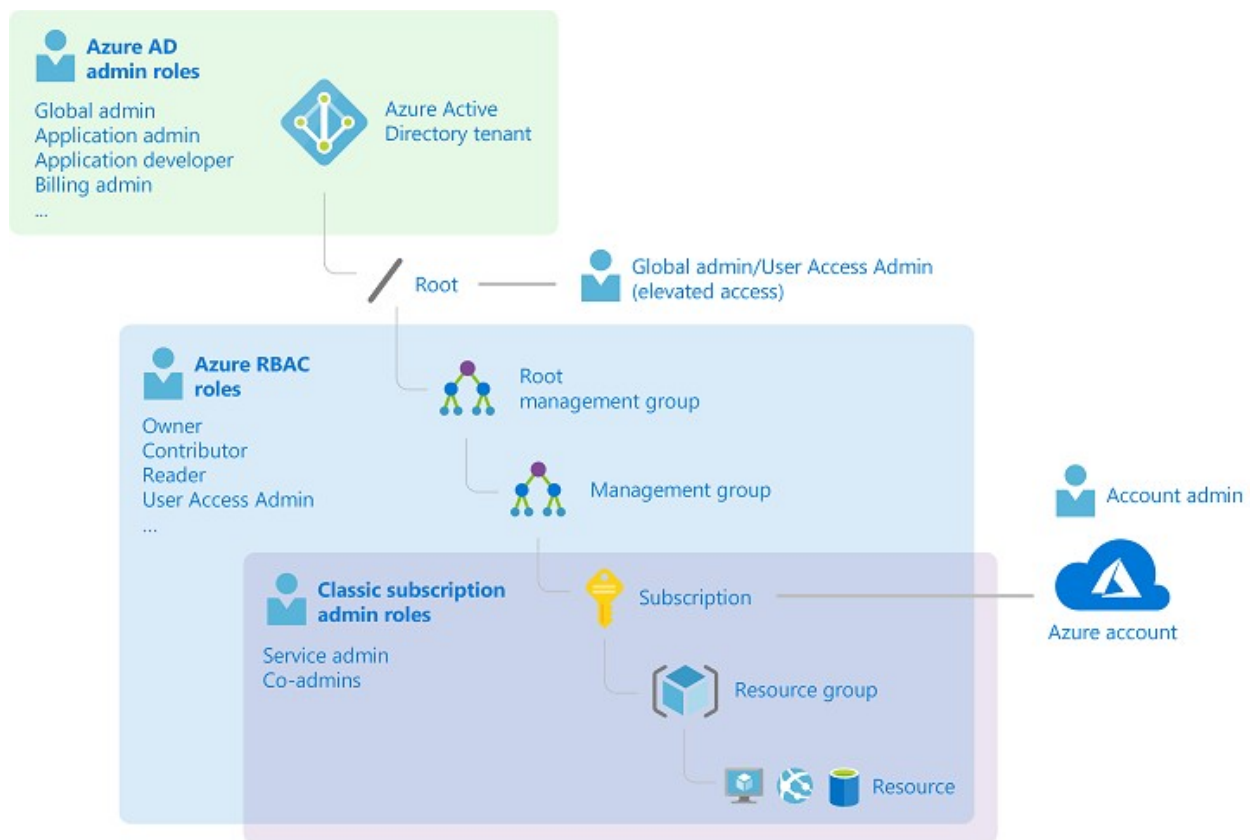
can use RBAC to let one employee manage virtual machines in a subscription while another manages SQL databases within the same subscription.

What is role-based access control?



You grant access by assigning the appropriate RBAC role to users, groups, and applications at a certain scope. The scope of a role assignment can be a 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 RBAC 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, RBAC roles, and Azure AD administrator roles are related at a high level. Roles assigned at a higher scope, like an entire subscription, are inherited by child scopes, like service instances.



In the preceding diagram, a subscription is associated with only one Azure AD tenant. Also note that a resource group can have multiple resources but is 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 RBAC?

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 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

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 Charon has been assigned the Backup Operator role for this resource group.

The screenshot shows the 'Access control (IAM)' pane for the 'sales-projectforecast' resource group. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM) (highlighted with a red box), Tags, Events, Settings, Quickstart, Resource costs, Deployments, Policies, Properties, Locks, Automation script, Monitoring, Insights (preview), Alerts, and Metrics. The main pane has tabs for 'Check access', 'Role assignments' (selected), 'Deny assignments', and 'Roles'. Below the tabs, there are filters for Name, Type, Role, Scope, and Group by. A table lists 9 items (6 Users, 1 Groups, 2 Service Principals). The first item, 'BACKUP OPERATOR', is highlighted with a red box. It shows a user 'Alain Charon' (alain@) assigned the 'Backup Operator' role to 'This resource'. Below this, a 'BILLING READER' role is assigned to the 'Sales Admins' group.

NAME	TYPE	ROLE	SCOPE
BACKUP OPERATOR			
AC Alain Charon alain@	User	Backup Operator	This resource
BILLING READER			
SA Sales Admins	Group	Billing Reader	Subscription (Inherited)

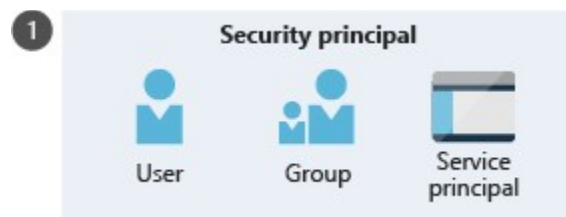
How does RBAC work?

You control access to resources using 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".

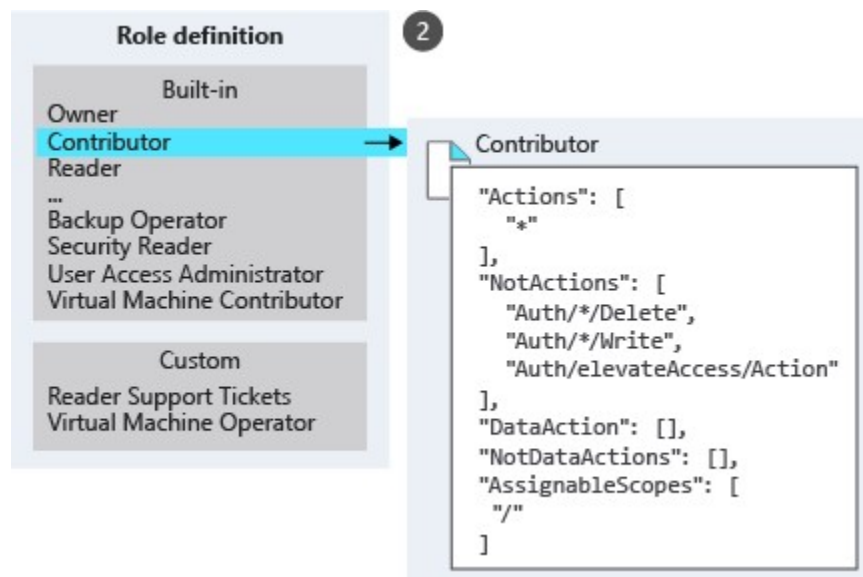
1. Security principal (who)

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



2. Role definition (what you can do)

A *role definition* is a collection of permissions. It's sometimes just called a role. A role definition lists the permissions that can be performed, 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 where the access applies to. This is helpful if you want to make someone a Website Contributor, but only for one resource group.

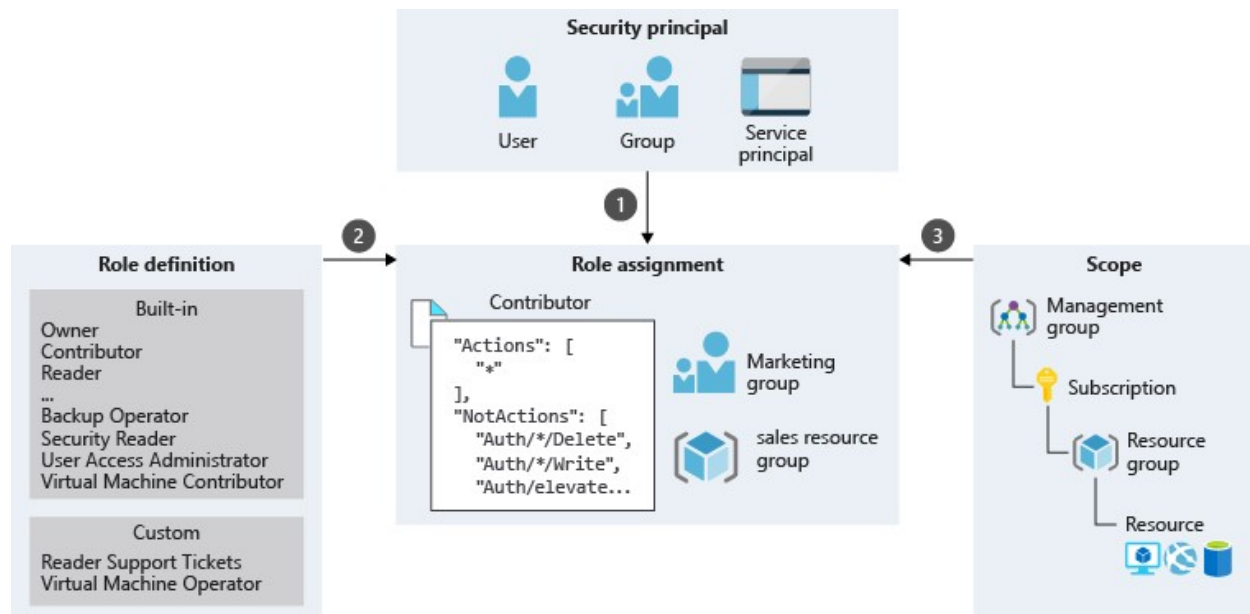
In Azure, you can specify a scope at multiple levels: management group, subscription, resource group, or resource. Scopes are structured in a parent-child relationship. When you grant access at a parent scope, those permissions are inherited by the child scopes. For example, if you assign the Contributor role to a group at the subscription scope, that role is inherited by all resource groups and resources in 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 create a role assignment. To revoke access, you remove a role assignment.

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



RBAC is an allow model

RBAC is an allow model. What this means is that when you are assigned a role, RBAC allows you to perform certain actions, such as read, write, or delete. So, 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, you will have read and write permissions on that resource group.

RBAC has something called `NotActions` permissions. Use `NotActions` to create a set of allowed permissions. The access granted by a role, 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. Then you subtract the following operations in `NotActions` to compute the effective permissions:

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

Next unit: Knowledge check - What is RBAC?

[Continue >](#)

Knowledge check - What is RBAC?

2 minutes

Check your knowledge

1. True or false: A role definition in Azure is a collection of permissions?

☒ True



A role definition in Azure is a collection of permissions with a name that you can assign to a user, group, or application.

☐ False

2. Suppose you want to assign a role to allow a user to create and manage Azure resources but not be able to grant access to others. Which of the following built-in roles would support this?

☐ Owner

☒ Contributor



A contributor can create and manage all types of Azure resources, but they can't grant access to other users.

☐ Reader

☐ User Access Administrator

3. What is the inheritance order for scope in Azure?

☐ Management group, Resource group, Subscription, Resource

☒ Management group, Subscription, Resource group, Resource



The inheritance order for scope is Management group, Subscription, Resource group, Resource. For example, if you assigned a Contributor role to a group at the Subscription

scope level, it will be inherited by all Resource groups and Resources.

- ☐ Subscription, Management group, Resource group, Resource
- ☐ Subscription, Resource group, Management group, Resource

Next unit: Exercise - List access using RBAC and the Azure portal

Continue >



Exercise - List access using RBAC and the Azure portal

8 minutes

This unit requires an Azure portal to complete.

An Azure Portal Lab provides free Azure resource access to complete the steps in this Unit. Azure Portal Labs do not affect your Azure subscription. You will not be charged.

Launch the Azure portal

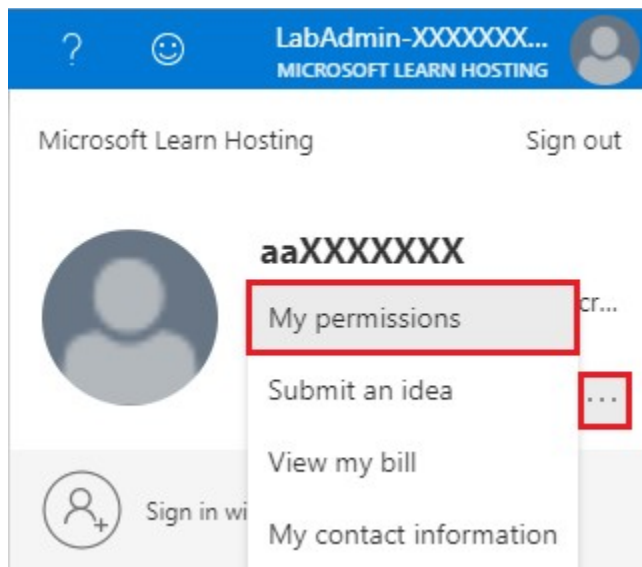
At First Up Consultants, you've been granted access to a resource group for the marketing team. You want to familiarize yourself with the Azure portal and see what roles are currently assigned.

List role assignments for yourself

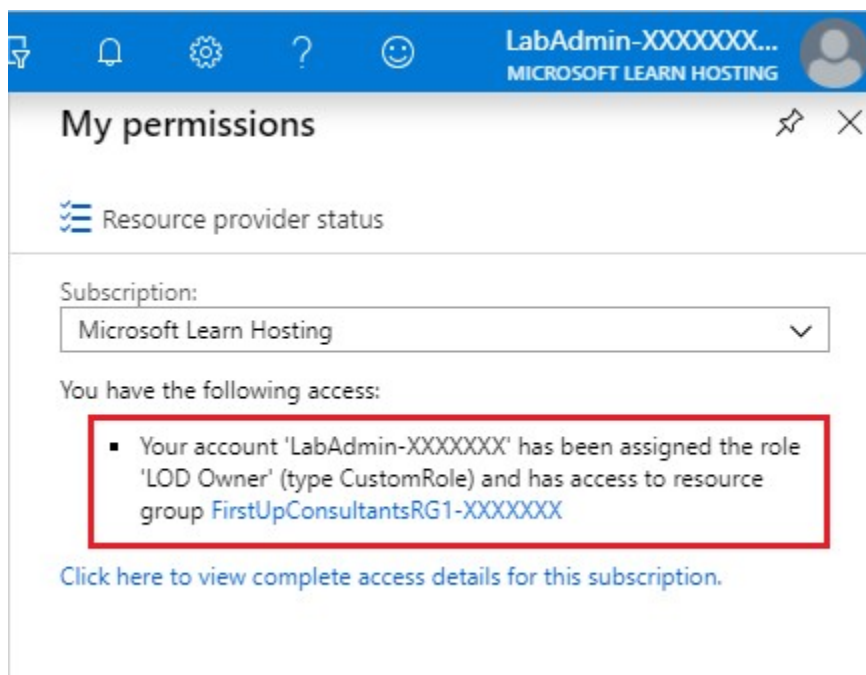
Follow these steps to see what roles are currently assigned to you.

1. Launch the lab experience.
2. At the top of the instructions for the lab, select the **Resources** tab.
3. Look for the Admin username like **LabAdmin-XXXXXXX** and the password.
4. Sign in to the lab experience by using the lab Admin username and password.
5. In the upper-right corner of the Azure portal, click your username to open the menu.

6. Make sure you are signed in as **LabAdmin-XXXXXXX**. If not, sign out and sign in using the username and password on the **Resources** tab.
7. Click the ellipsis (...) to see more links.



8. Click **My permissions** to open the My permissions pane.

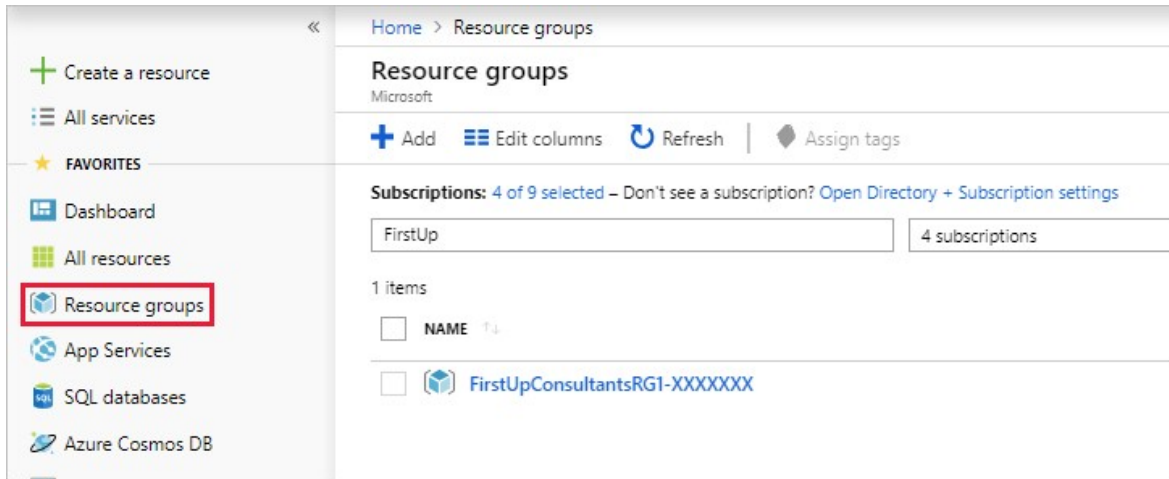


On the My permissions pane, you can see the roles that you have been assigned and the scope. Your list will look different.

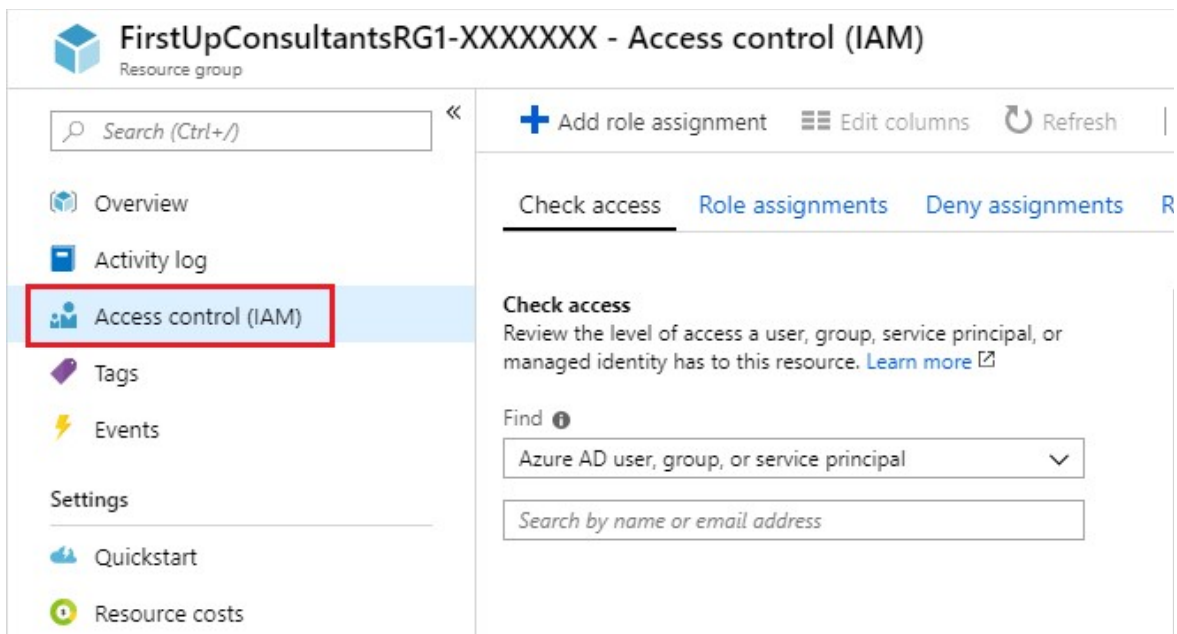
List role assignments for a resource group

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

1. In the navigation list, click **Resource groups**.



2. Find and click the resource group named **FirstUpConsultantsRG1-XXXXXXX**.
3. Click **Access control (IAM)**.



4. Click the **Role assignments** tab.

You can see who has access to this resource group. Notice that some roles are scoped to **This resource** while others are **(Inherited)** from a parent scope.

[+ Add role assignment](#)
[Edit columns](#)
[Refresh](#)
[Remove](#)




[Check access](#)
[Role assignments](#)
[Deny assignments](#)
[Roles](#)

Manage access to Azure resources for users, groups, service principals and managed identities at this scope by creating role assignments. [Learn more](#)

Name
 Type
 Role

Scope
 Group by

7 items (4 Users, 2 Groups, 1 Service Principals)











<input type="checkbox"/>	NAME	TYPE	ROLE	SCOPE
LOD OWNER				
	aaXXXXXXXX LabAdmin-XXXXXXXX...	User	LOD Owner	This resource
LOD READER				
	aaXXXXXXXX LabUser-XXXXXX@...	User	LOD Reader	This resource
OWNER				
	Subscription Admini...	Group	Owner	Subscription (Inherited)

List roles

As you learned in the previous unit, a role is a collection of permissions. Azure has over 70 built-in roles that you can use in your role assignments. Follow this step to list the roles.

- At the top of the pane, click the **Roles** tab to see a list of all the built-in and custom roles.

You can see the number of users and groups that are assigned to each role.

+ Add role assignment Edit columns Refresh Remove			
Check access Role assignments Deny assignments Roles			
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			
NAME	TYPE	USERS	GROUPS
 Owner ⓘ	BuiltInRole	2	2
 Contributor ⓘ	BuiltInRole	0	0
 Reader ⓘ	BuiltInRole	0	0
 LOD Owner ⓘ	CustomRole	1	0
 LOD Reader ⓘ	CustomRole	1	0
 Security Reader ⓘ	BuiltInRole	0	1
 AcrImageSigner ⓘ	BuiltInRole	0	0
 AcrPull ⓘ	BuiltInRole	0	0
 AcrPush ⓘ	BuiltInRole	0	0
 AcrQuarantineReader ⓘ	BuiltInRole	0	0

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.

Next unit: Exercise - Grant access using RBAC and the Azure portal

Continue >



Exercise - Grant access using RBAC and the Azure portal

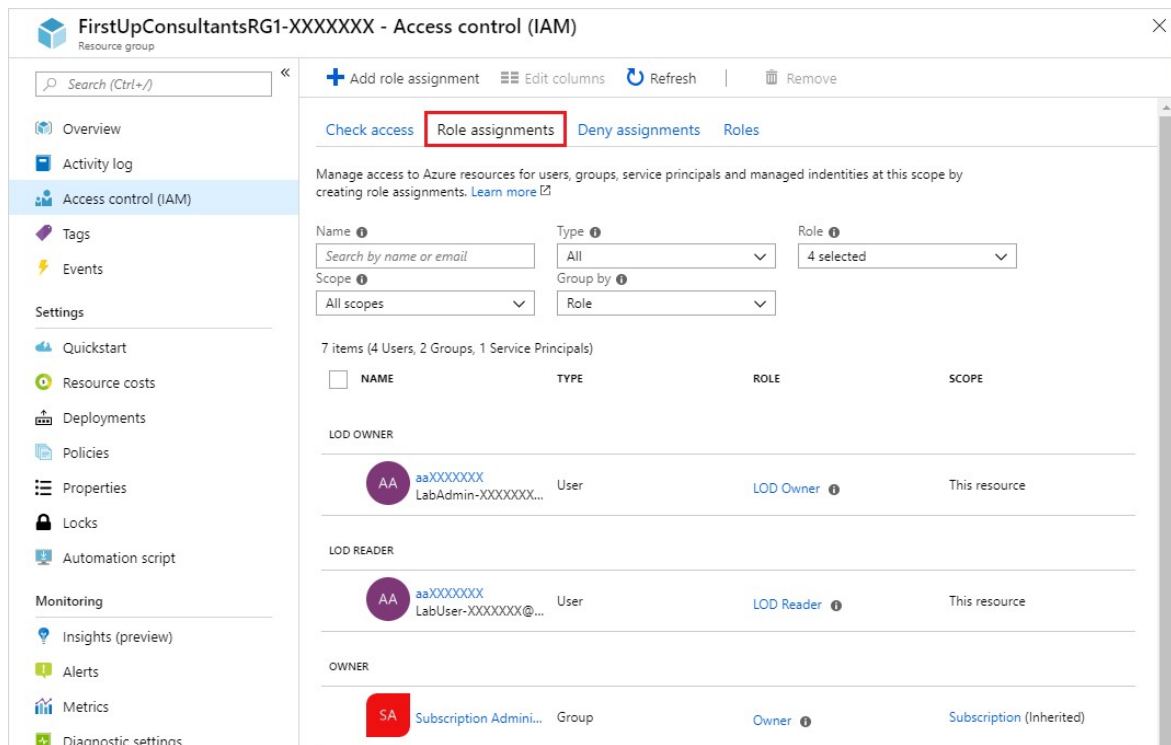
8 minutes

A co-worker named Alain at First Up Consultants needs the ability to create and manage virtual machines for a project he is working on. 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.

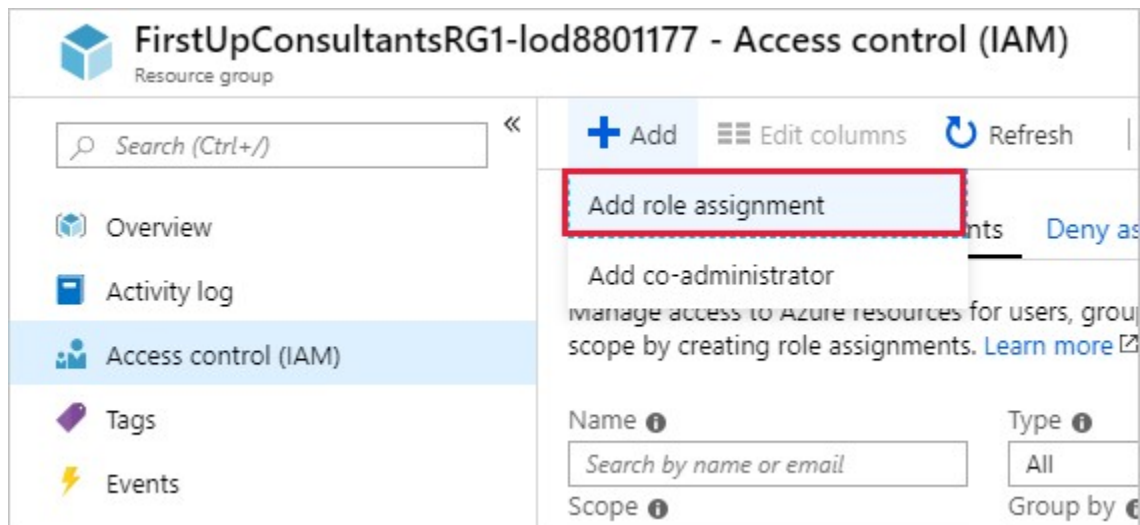
Grant access

Follow these steps to assign the Virtual Machine Contributor role to a user at the resource group scope.

1. In the navigation list, click **Resource groups**.
2. Find and click the **FirstUpConsultantsRG1-XXXXXXX** resource group.
3. Click **Access control (IAM)**.
4. Click the **Role assignments** tab to see the current list of role assignments.



5. At the top, click **Add role assignment**.



The **Add role assignment** pane opens.

Add role assignment

Role ⓘ

Select a role

Assign access to ⓘ

Azure AD user, group, or service principal

Select ⓘ

Search by name or email address

AA

aaXXXXXXX
LabAdmin-XXXXXXX

AA

aaXXXXXXX
LabAdmin-XXXXXXX

AA

aaXXXXXXX

Selected members:

No members selected. Search for and add one or more members you want to assign to the role for this resource.

[Learn more about RBAC](#)

Save

Discard

6. In the **Role** drop-down list, select **Virtual Machine Contributor**.

7. In the **Select** list, select **LabUser-XXXXXXX**.

You can find the username on the **Resources** tab next to the instructions.

Add role assignment

Role ⓘ

Virtual Machine Contributor

Assign access to ⓘ

Azure AD user, group, or service principal

Select ⓘ

Search by name or email address

AA

aaXXXXXXX

LabAdmin-XXXXXXX

AA

aaXXXXXXX

LabAdmin-XXXXXXX

AA

aaXXXXXXX

Selected members:

AA

aaXXXXXXX

LabUser-XXXXXXX

Remove

Save

Discard

8. Click **Save** to create the role assignment.

After a few moments, the **LabUser-XXXXXXX** user is assigned the Virtual Machine Contributor role at the **FirstUpConsultantsRG1-XXXXXXX** resource group scope. The user can now create and manage virtual machines just within this resource group.

+ Add role assignment Edit columns Refresh Remove			
SA	Subscription Admini...	Group	Owner <i>i</i> Subscription (Inherited)
SECURITY READER			
SS	Subscription Securit...	Group	Security Reader <i>i</i> Subscription (Inherited)
VIRTUAL MACHINE CONTRIBUTOR			
AA	aaXXXXXXX LabUser-XXXXXXX	User	Virtual Machine Contributor <i>i</i> This resource

Remove access

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

1. In the list of role assignments, select the **LabUser-XXXXXXX** user with the Virtual Machine Contributor role.
2. Click **Remove**.

+ Add role assignment Edit columns Refresh			Remove
<h3>Remove role assignments</h3> <p>Are you sure you want to remove the selected role assignments?</p>			
<div> <input checked="" type="button" value="Yes"/> <input type="button" value="No"/> </div>			
SS	Subscription Securit...	Group	Security Reader <i>i</i>
VIRTUAL MACHINE CONTRIBUTOR			
<input checked="" type="checkbox"/>	AA	aaXXXXXXX LabUser-XXXXXXX	User Virtual Machine Contributor <i>i</i>

3. In the **Remove role assignments** message that appears, click **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.

Next unit: Exercise - View activity logs for RBAC changes

[Continue >](#)



Exercise - View activity logs for RBAC changes

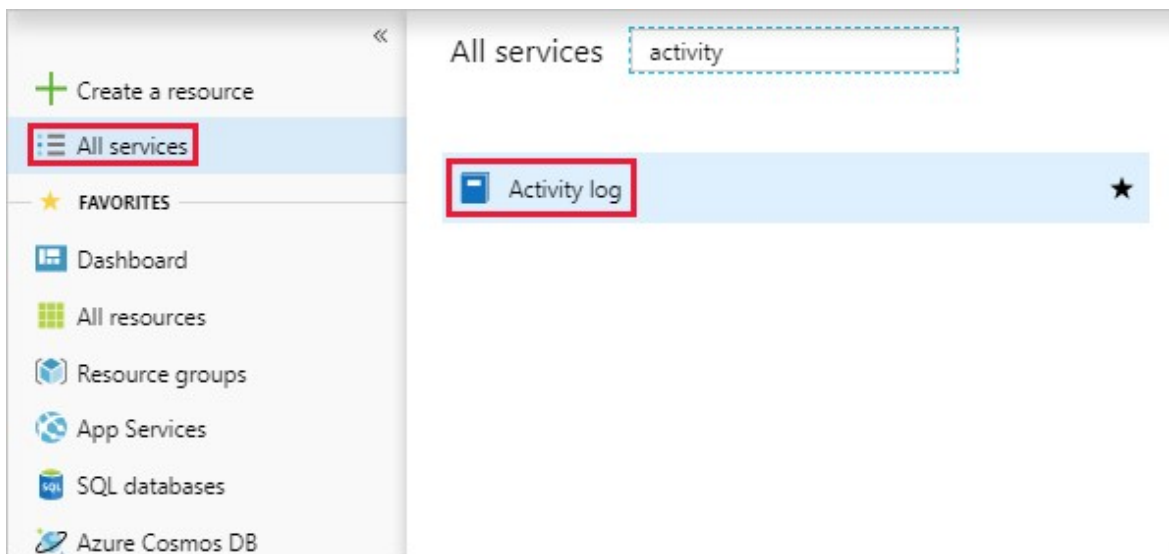
4 minutes

First Up Consultants reviews role-based access control (RBAC) changes quarterly for auditing and troubleshooting purposes. You know that changes get logged in [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. Click **All services** and then find **Activity log**.



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

Home > Activity log

Activity log

Edit columns Refresh Export to Event Hub Download as CSV Logs Pin current filters Reset filters

Search Quick Insights

Subscription : Microsoft Learn Hosting (prod) - 5 Timespan : Last 6 hours Event severity : All Add Filter

First 7 items.

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION	EVENT INITIATED BY
▶ Delete role assignment	Succeeded	22 min ago	Fri Dec 14 20...	Microsoft Learn Hosting (prod) - 5	LabAdmin-XXXXXXX
▶ Create role assignment	Succeeded	33 min ago	Fri Dec 14 20...	Microsoft Learn Hosting (prod) - 5	LabAdmin-XXXXXXX
▶ Create policy assignment	Started	2 h ago	Fri Dec 14 20...	Microsoft Learn Hosting (prod) - 5	
▶ Create role assignment	Succeeded	2 h ago	Fri Dec 14 20...	Microsoft Learn Hosting (prod) - 5	
▶ Create role assignment	Succeeded	2 h ago	Fri Dec 14 20...	Microsoft Learn Hosting (prod) - 5	
▶ Create policy assignment	Succeeded	2 h ago	Fri Dec 14 20...	Microsoft Learn Hosting (prod) - 5	
▶ Update resource group	Succeeded	2 h ago	Fri Dec 14 20...	Microsoft Learn Hosting (prod) - 5	

Delete role assignment

- Set the **Timespan** filter to **Last month**.
- Add an **Operation** filter and type **role** to filter the list.
- Select the following RBAC operations:
 - Create role assignment (roleAssignments)
 - Delete role assignment (roleAssignments)
 - Create or update custom role definition (roleDefinitions)
 - Delete custom role definition (roleDefinitions)

Operation : 4 selected Add Filter

role

OPERATION NAME	STATUS	TIME	SUBSCRIPTION
<input type="checkbox"/> Get role assignment (roleAs			
<input checked="" type="checkbox"/> Create role assignment (role			
<input checked="" type="checkbox"/> Delete role assignment (role			
<input type="checkbox"/> Get role definition (roleDefi			
<input checked="" type="checkbox"/> Create or update custom ro			
<input checked="" type="checkbox"/> Delete custom role definitio			
<input type="checkbox"/> Get Deployment Slot Role (
<input type="checkbox"/> Add Deployment Slot Role (
<input type="checkbox"/> Get the Domain Names Slot			
<input type="checkbox"/> Get Deployment Slot Role E			

After a few moments, you'll see all the role assignment and role definition operations for the last month. It also includes a link to download the activity log as a CSV file.

6. Click one of the operations to see the activity log details.

The screenshot displays the Azure Activity Log interface. At the top, there's a header 'Activity log' with a search bar and various action buttons like 'Edit columns', 'Refresh', 'Export to Event Hub', 'Download as CSV', 'Logs', 'Pin current filters', and 'Reset filters'. Below the header, there's a filter section with 'Subscription : Microsoft Learn Hosting (prod) - 5', 'Timespan : Last month', 'Event severity : All', and 'Operation : 4 selected'. A table lists 5 items. The third item, 'Create role assignment', is selected and highlighted in blue. Below the table, a detailed view of the selected operation is shown, including fields for 'Operation name', 'Time stamp', 'Event initiated by', 'Message', 'Role', 'Scope', and 'Resource group'.

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION	EVENT INITIATED BY
Delete role assignment	Succeeded	13 min ago	Fri Dec 14 20...	Microsoft Learn Hosting (prod) - 5	LabAdmin-XXXXXXX
Create role assignment	Succeeded	24 min ago	Fri Dec 14 20...	Microsoft Learn Hosting (prod) - 5	LabAdmin-XXXXXXX
Create role assignment	Started	24 min ago	Fri Dec 14 20...	Microsoft Learn Hosting (prod) - 5	LabAdmin-XXXXXXX

Create role assignment

+ Add activity log alert

Summary JSON

Operation name
Create role assignment

Time stamp
Fri Dec 14 2018 17:53:14 GMT-0800 (Pacific Standard Time)

Event initiated by
LabAdmin-XXXXXXX

Message
Shared with 'aaXXXXXXX'.

Role
Virtual Machine Contributor

Scope
Resource group: 'FirstUpConsultantsRG1-XXXXXXX'

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

Next unit: Knowledge check - Using RBAC

Continue >



Knowledge check - Using RBAC

3 minutes

Check your knowledge

1. True or false: To grant a user access to Azure resources, you create a role assignment?

☒ True



A role assignment is the process of binding a role to a security principal at a particular scope for the purpose of granting access.

☐ False

2. Suppose a developer needs full access to a resource group. If you are following least-privilege best practices, what scope should you specify?

☐ Resource

☒ Resource group



Following least-privilege best practices, you grant only the access the user needs to do their job. In this case, you should set the scope to the resource group.

☐ Subscription

Next unit: Summary

Continue >



Summary

2 minutes

In this module, you learned about role-based access control (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 RBAC, you can grant only the amount of access to users that they need to perform their jobs. RBAC has over 70 built-in roles, but if your organization needs specific permissions, you can create your own custom roles. Azure keeps track of your RBAC changes, in case you need to see what changes were made in the past.

Further reading

Here are some additional resources you can use to continue learning about RBAC.

- [RBAC built-in roles](#)

Module complete:

Unlock achievement