

Lab : Configure IAM policies for secure cloud access

By the end of this lab, you will:

- Assign IAM Roles to users on their respective VMs.
 - Verify IAM permissions using role-based access control (RBAC).
 - Enable Auto-Shutdown for cost and security optimization.
 - Understand shared resource visibility in a common resource group.
-

Prerequisites

- All students are using the **same Azure account**.
- Each student has created an **Ubuntu Server VM** prefixed with their name (e.g., `YOUR_NAME-ubuntu-vm`) in the earlier lab.
- Students have an **additional user account** that they will assign IAM permissions to.
- All VMs are in a **shared resource group**, meaning students can see others' VMs but should only modify their own.

Note

- Since all students are using the **same Azure account and resource group**, they can see each other's VMs in **Virtual Machines**.
- However, **they should only manage their own VMs**

Step 1: Assign "Reader" Role to a User

1. **Log in** to the [Azure portal](#).
2. Go to **Virtual Machines** and locate your VM.
3. Click on your VM and go to **Access Control (IAM)**.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > ath-ubuntu-vm

ath-ubuntu-vm | Access control (IAM)

Virtual machine

Search

+ Add Download role assignments Edit columns Refresh Delete Fe

- Overview
- Activity log
- Access control (IAM)**
- Tags
- Diagnose and solve problems
- Connect
- Networking
 - Network settings
 - Load balancing
 - Application security groups
 - Network manager
- Settings
 - Disks
 - Extensions + applications

Check access Role assignments Roles Deny assignments Classic administrators

My access
View my level of access to this resource.
[View my access](#)

Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)
[Check access](#)

Grant access to this resource

Grant access to resources by assigning a role. [Learn more](#)

[Add role assignment](#)

View access to this resource

View the role assignments that grant access to this and other resources. [Learn more](#)

[View](#)

- Click **Add > Add role assignment**.
- Select **Reader** role.
- Under **Assign access to**, select **User, group, or service principal**.
- In **Select Members**, enter the additional user's username `iam-software-lab-demo`.

Add role assignment

[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 ↑↓
Reader	View all resources, but does not allow you to make any changes.
App Compliance Automation Administrator	Create, read, download, modify and delete reports objects and related other resource objects.
App Compliance Automation Reader	Read, download the reports objects and related other resource objects.
Avere Contributor	Can create and manage an Avere vFXT cluster.
Avere Operator	Used by the Avere vFXT cluster to manage the cluster
Azure Backup Snapshot Contributor	Provide permissions to backup identity to manage RPC snapshots
Azure Center for SAP solutions administrator	This role provides read and write access to all capabilities of Azure Center for SAP solutions.
Azure Center for SAP solutions reader	This role provides read access to all capabilities of Azure Center for SAP solutions.
Azure Center for SAP solutions service role	Azure Center for SAP solutions service role - This role is intended to be used for providing the permissions to user assigned managed ide..
Azure Container Storage Operator	Role required by a Managed Identity for Azure Container Storage operations
Azure Red Hat OpenShift Cloud Controller Manager R...	Enables permissions for the operator to manage and update the cloud controller managers deployed on top of OpenShift.

Review + assign

Previous

Next

Add role assignment

[Role](#) [Members](#) [Conditions](#) [Review + assign](#)

Selected role

Reader

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

Search by member name, email, or phone number

iam-software-lab-demo

iam-software-lab-demo
iam-software-lab-demo@courselabs.io

Selected members:

iam-software-lab-demo
iam-software-lab-demo@courselabs.io

Select

Close

8. Click **Review + Assign**.

Home > ath-ubuntu-vm

ath-ubuntu-vm | Access control (IAM) ☆ ...

Virtual machine

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Networking

Network settings

Load balancing

Application security groups

Network manager

Settings

Disks

+ Add

Download role assignments

Edit columns

Refresh

Delete

Feedback

<input type="checkbox"/>	ST	student4-azure-mfa@c...	User	Owner	Resource group (Inherited) None
<input type="checkbox"/>	ST	student5-azure-mfa@c...	User	Owner	Resource group (Inherited) None
<input type="checkbox"/>	ST	student6-azure-mfa@c...	User	Owner	Resource group (Inherited) None
<input type="checkbox"/>	ST	student7-azure-mfa@c...	User	Owner	Resource group (Inherited) None
<input type="checkbox"/>	ST	student8-azure-mfa@c...	User	Owner	Resource group (Inherited) None
<input type="checkbox"/>	ST	student9-azure-mfa@c...	User	Owner	Resource group (Inherited) None
Contributor (1)					
<input type="checkbox"/>		DevTestLabsAPI	App	Contributor	Subscription (Inherited) None
Reader (1)					
<input type="checkbox"/>	IA	iam-software-lab-demo	User	Reader	This resource None

Note: This user can only view the VM but doesn't have permissions to **start/stop the VM**.

Step 2: Upgrade User Role to "Virtual Machine Contributor"

1. Log back in as the original user (owner of the VM).
2. Navigate to **Virtual Machines > Access Control (IAM)**.
3. Click **Add role assignment**.
4. Select **Privileged administrator roles > Contributor**.

Home > ath-ubuntu-vm | Access control (IAM) >

Add role assignment ...

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?

Search by role name, description, permission, or ID

Type: All

Category: All



Name	Description	Type
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.	BuiltInRole
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, ...	BuiltInRole
Role Based Access Control Administrator	Manage access to Azure resources by assigning roles using Azure RBAC. This role does not allow you to manage access using other ways, s...	BuiltInRole
User Access Administrator	Lets you manage user access to Azure resources.	BuiltInRole

Showing 1 - 4 of 4 results.

5. Assign it to the same user `iam-software-lab-demo`.
6. Click **Review + Assign**.

Verification:

1. Click on your VM and go to **Access Control (IAM)**.
2. Click **View** button in View access to this resource.

Contributor (2)					
<input type="checkbox"/>	 DevTestLabsAPI	App	Contributor ⓘ	Subscription (Inherited)	None
<input type="checkbox"/>	 iam-software-lab-der	User	Contributor ⓘ	This resource	None


Now, this user has permissions to **start/stop the VM**.




Step 3: Configure Auto-Shutdown for Cost Optimization

1. Navigate to **Virtual Machines** in the Azure portal.
2. Select your VM.
3. Go to **Auto-shutdown**.
4. Enable auto-shutdown and set a **shutdown time**.
5. Optionally, enter an **email** for shutdown notifications.
6. Click **Save**.


The VM will shut down at the scheduled time automatically.

[Home](#) > [ath-ubuntu-vm](#)

 **ath-ubuntu-vm | Auto-shutdown** ☆ ...
Virtual machine

× × <<  Save  Discard  Feedback

▼ Operations

 **Auto-shutdown**

Enabled

☒ On ☐ Off

Scheduled shutdown

Time zone

Send notification before auto-shutdown?

☒ Yes ☐ No

Webhook URL ⓘ

Email address ⓘ

Step 4: Review Audit Logs

1. Navigate to **Activity Log**.
2. Apply filters:
 - Event severity
 - Timespan
3. View the logs in the Azure portal.

Verification:

- Logs should show the actions taken, including IAM role changes.

Home > ath-ubuntu-vm

ath-ubuntu-vm | Activity log

Activity log

Looking for Log Analytics? In Log Analytics you can search for performance, diagnostics, health logs, and more. [Visit Log Analytics](#)

Search

Subscription: Azure subscription 1 Event severity: All Timespan: Last 6 hours Resource group: software-ecosystem-student-tmp Resource: ath-ubuntu-vm Add Filter

7 items.

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
Create role assignment	Succeeded	5 minutes a...	Tue Feb 11 ...	Azure subscription 1	student0-azure-mfa@cou...
Create role assignment	Started	5 minutes a...	Tue Feb 11 ...	Azure subscription 1	student0-azure-mfa@cou...
Create role assignment	Succeeded	12 minutes ...	Tue Feb 11 ...	Azure subscription 1	student0-azure-mfa@cou...
Deallocate Virtual Machine	Succeeded	22 minutes ...	Tue Feb 11 ...	Azure subscription 1	student0-azure-mfa@cou...
Health Event InProgress	Updated	23 minutes ...	Tue Feb 11 ...	Azure subscription 1	student0-azure-mfa@cou...
'auditIfNotExists' Policy action.	Succeeded	40 minutes ...	Tue Feb 11 ...	Azure subscription 1	student0-azure-mfa@cou...
Health Event Updated	Updated	50 minutes ...	Tue Feb 11 ...	Azure subscription 1	student0-azure-mfa@cou...

Step 5: Delete VM

Make sure to delete the VM by clicking `Delete` button and selecting following options:

Microsoft Azure

Search resources, services, and docs (G+/)

Home > ath-ubuntu-vm

ath-ubuntu-vm

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Networking

Network settings

Load balancing

Application security groups

Network manager

Settings

Disks

Essentials

Resource group (move) software-ecosystem-student-tmp

Status Stopped (deallocated)

Location West US 2 (Zone 1)

Subscription (move) Azure subscription 1

Subscription ID 0e9ad9e1-3623-4512-91c4-bdca

Availability zone 1

Tags (edit) Add tags

Delete ath-ubuntu-vm

ath-ubuntu-vm

Virtual machine

Apply force delete

This virtual machine can be safely force deleted because all of its associated resources are being deleted.

You can also choose to delete associated resources at the same time. Resources that aren't deleted will be orphaned. Associated resources that are in use by other resources are not shown here.

Associated resource type	Quantity	Delete with VM
OS disk	1	<input checked="" type="checkbox"/>
Network interfaces	1	<input checked="" type="checkbox"/>
Public IP addresses	1	<input checked="" type="checkbox"/>

I have read and understand that this virtual machine as well as any selected associated resources listed above will be deleted.

Delete Cancel

Feedback

Conclusion

- Assigned IAM roles using RBAC.
- Verified role-based access.
- Configured auto-shutdown for cost efficiency.
- Reviewed logs for security auditing.