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

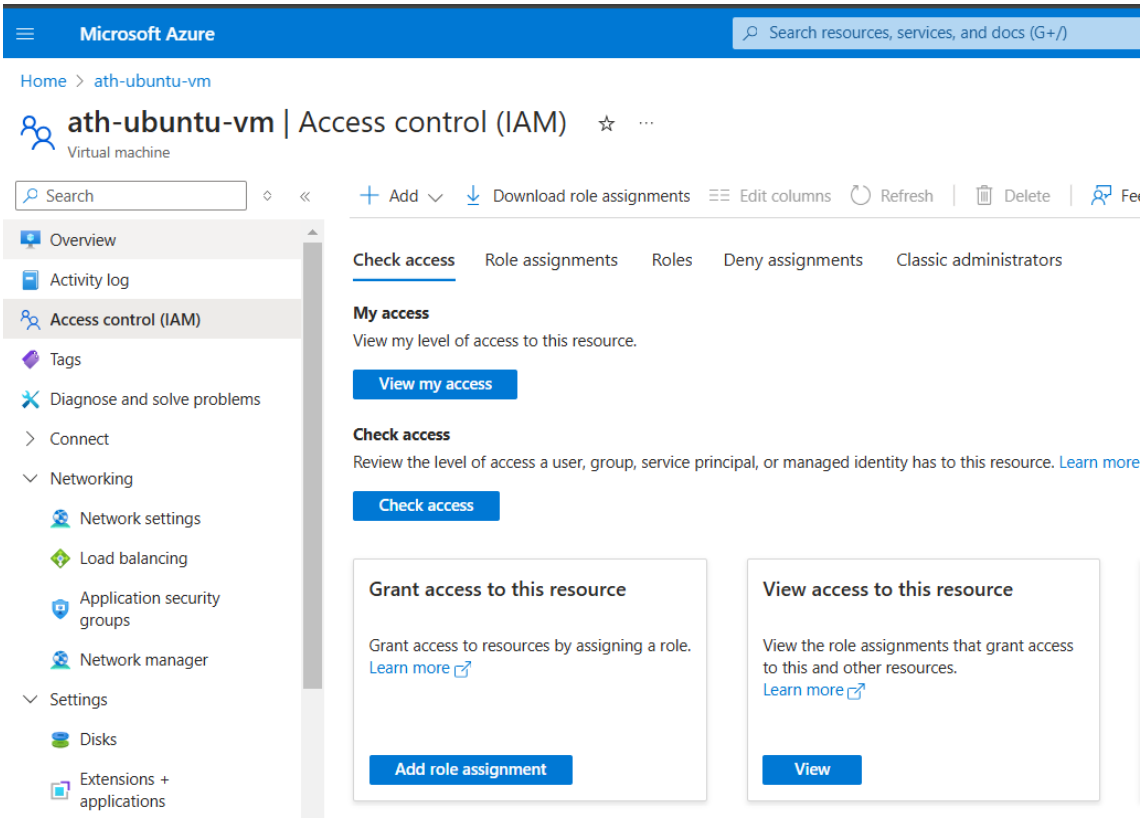
- All students are using the **same Azure account**.
- Each student has created an **Ubuntu Server VM** prefixed with their name (e.g., `YOUR_NAME-ubuntu-vm`) in the earlier lab.
- Students have an **additional user account** that they will assign IAM permissions to.
- All VMs are in a **shared resource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



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

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 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

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

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

iam-software-lab-demo

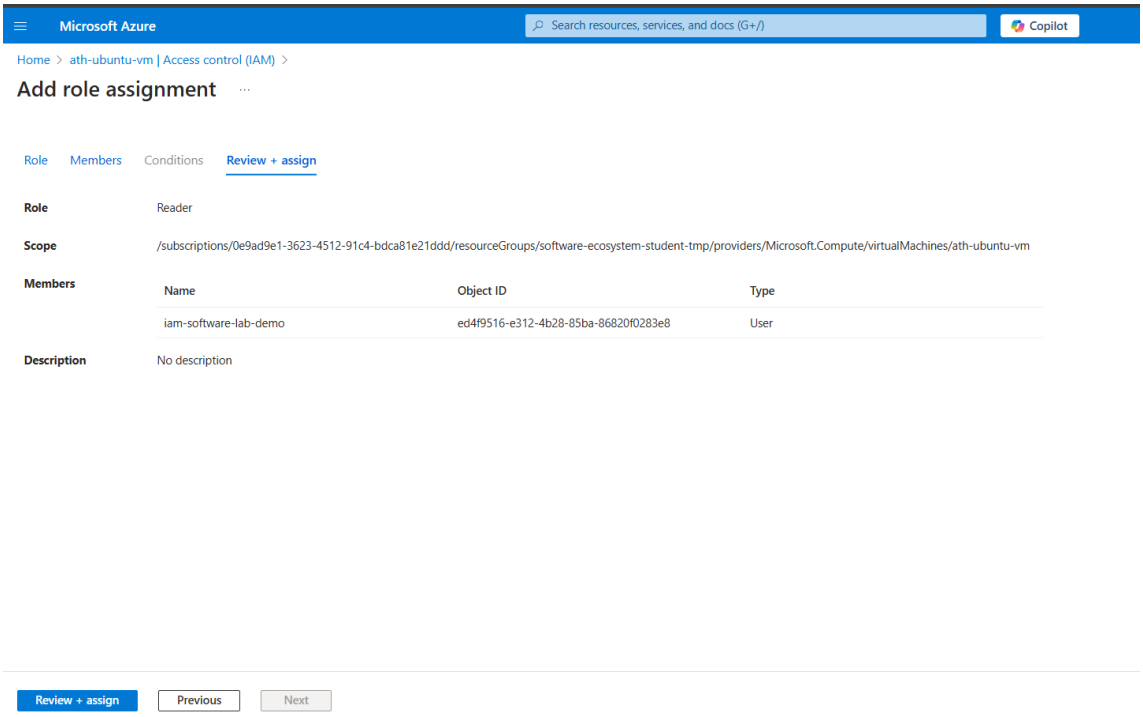
IA iam-software-lab-demo
iam-software-lab-demo@courselabs.io

Selected members:

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

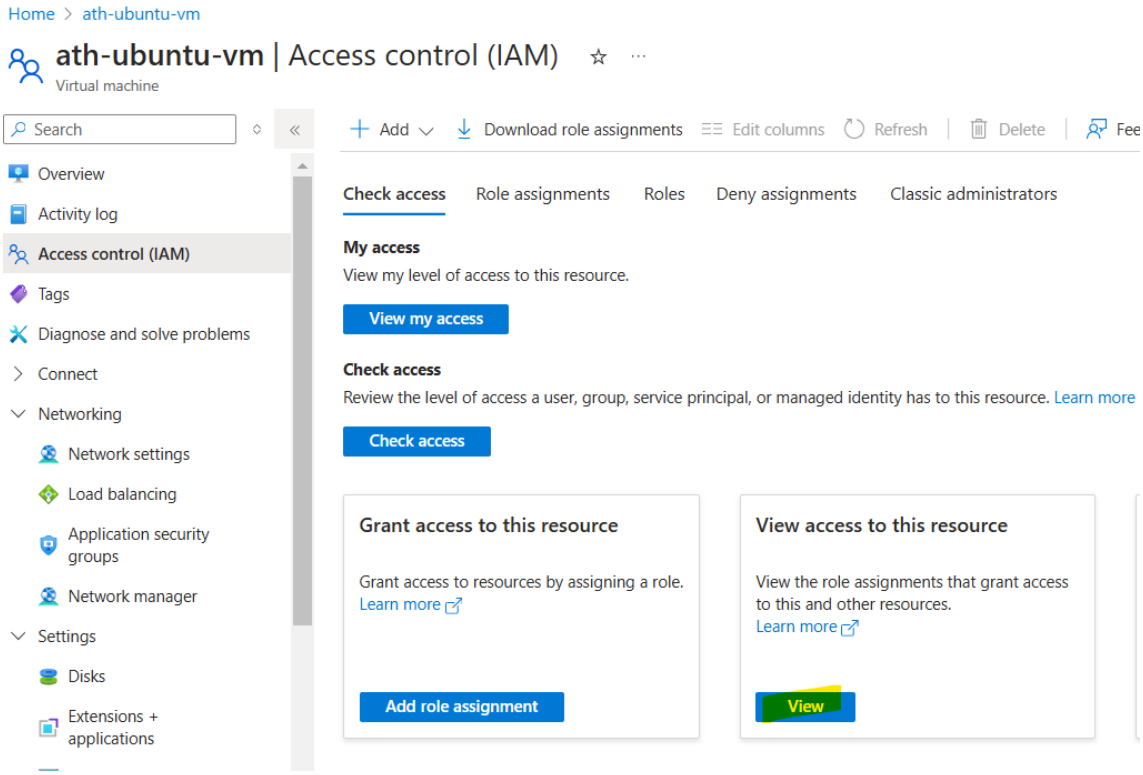
Select | Close

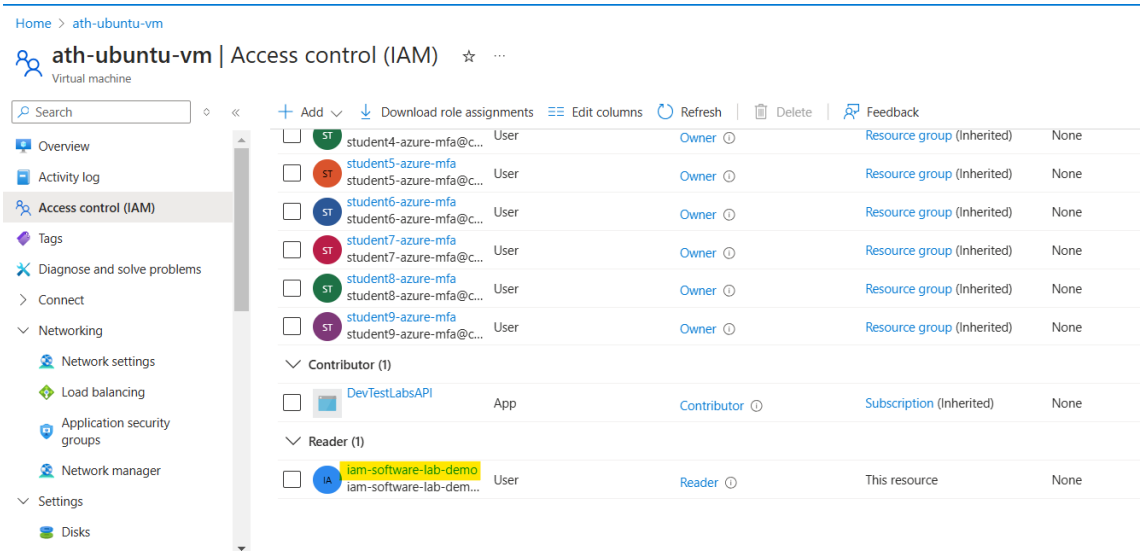
8. Click **Review + Assign**.



Verification:

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

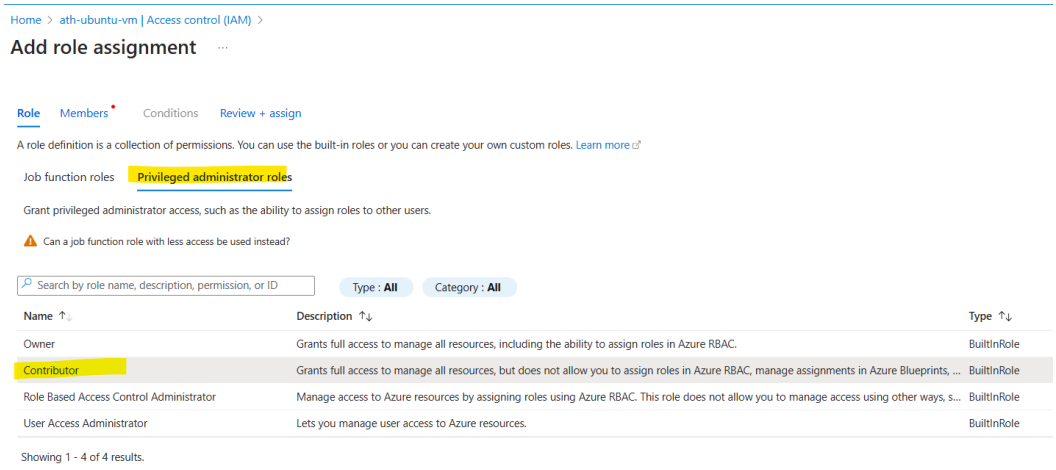




Note: This user can only view the VM but doesn't have permissions to **start/stop the VM**.

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

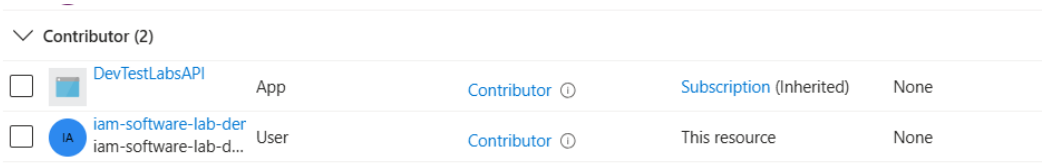
1. Log back in as the original user (owner of the VM).
2. Navigate to **Virtual Machines** > **Access Control (IAM)**.
3. Click **Add role assignment**.
4. Select **Privileged administrator roles** > **Contributor**.



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.

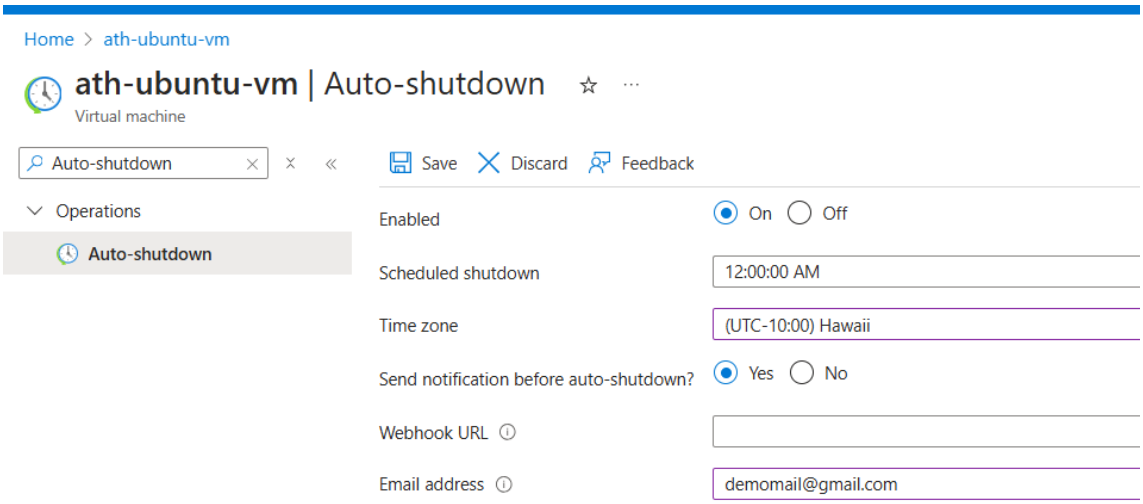


Now, this user has permissions to **start/stop the VM**.

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.

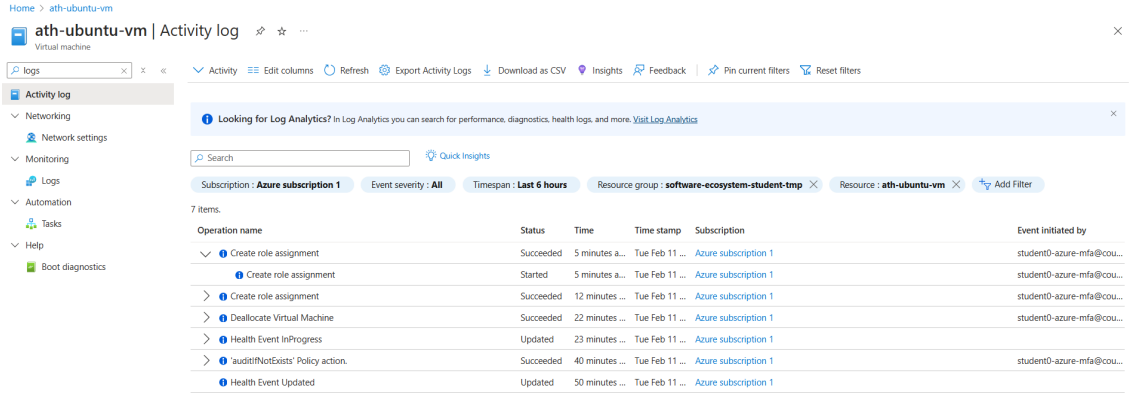


Step 4: Review Audit Logs

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

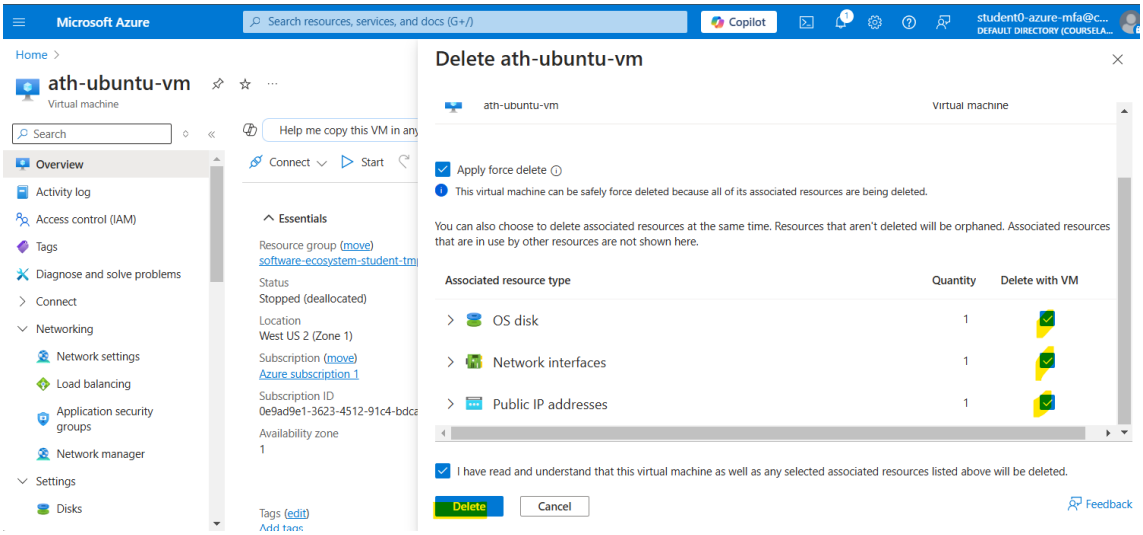
Verification:

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



Step 5: Delete VM

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



Conclusion

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