

Placement Empowerment Program

Cloud Computing and DevOps Centre

Setup IAM roles and permission : Create an IAM role on your cloud platform. Assign the role to your VM to restrict/allow specific action.

Name: Anumitha M

Department: AML

Introduction :

In modern cloud computing, managing access to resources is crucial to ensure security and proper usage of services. Azure IAM (Identity and Access Management) allows administrators to create custom roles with specific permissions to control who can access and perform operations on resources. This document outlines the creation of a custom IAM role, assigning it to a Virtual Machine (VM), and configuring specific actions such as starting, stopping, and reading VM properties.

Overview :

IAM roles enable fine-grained access control to cloud resources. Custom roles can be tailored to meet specific organizational needs, limiting access to only essential actions. In this task, we create a custom IAM role for managing virtual machines and assign it to a user while ensuring only allowed actions can be performed. This helps maintain security and operational efficiency.

Objective :

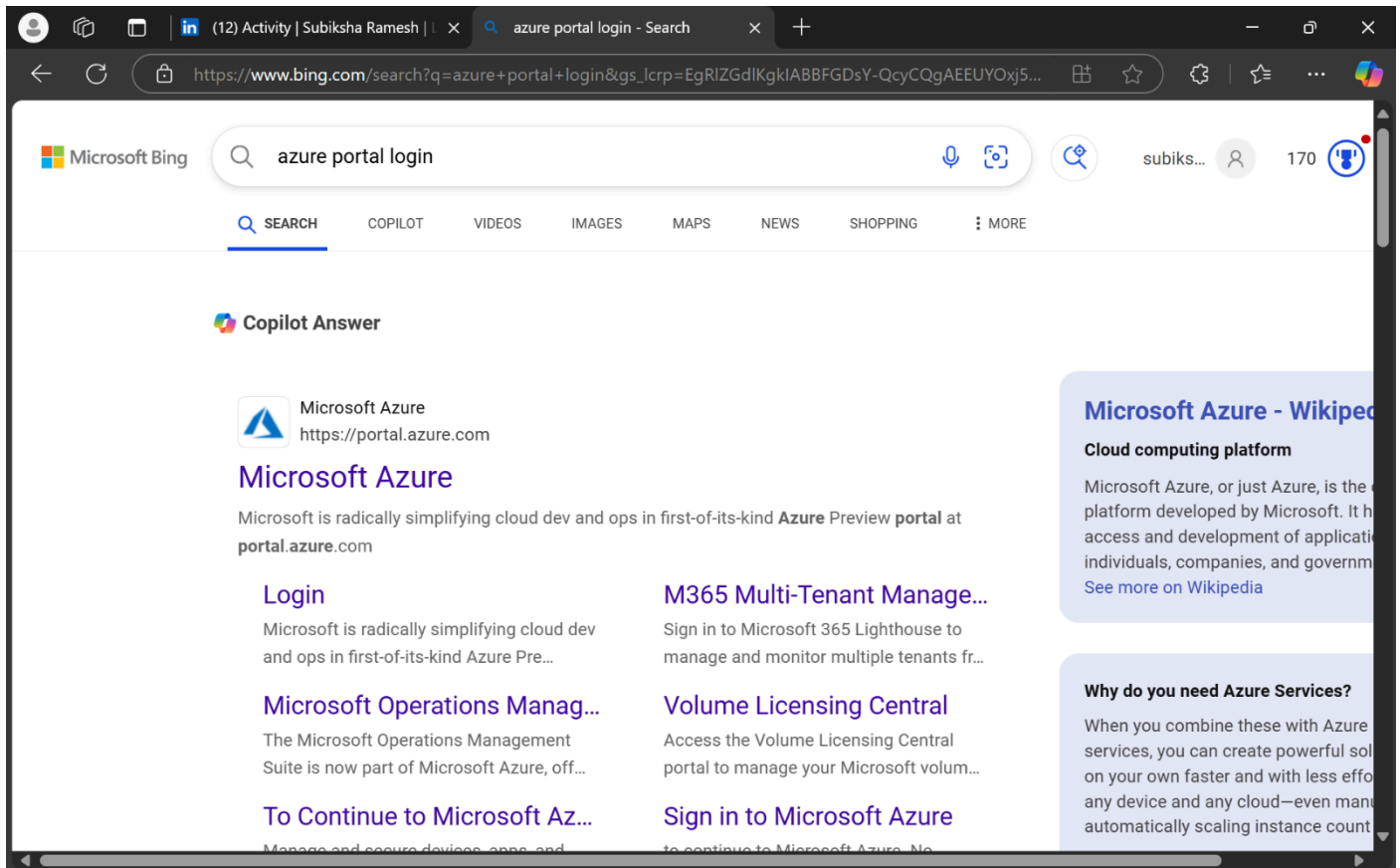
The objective of this task is to:

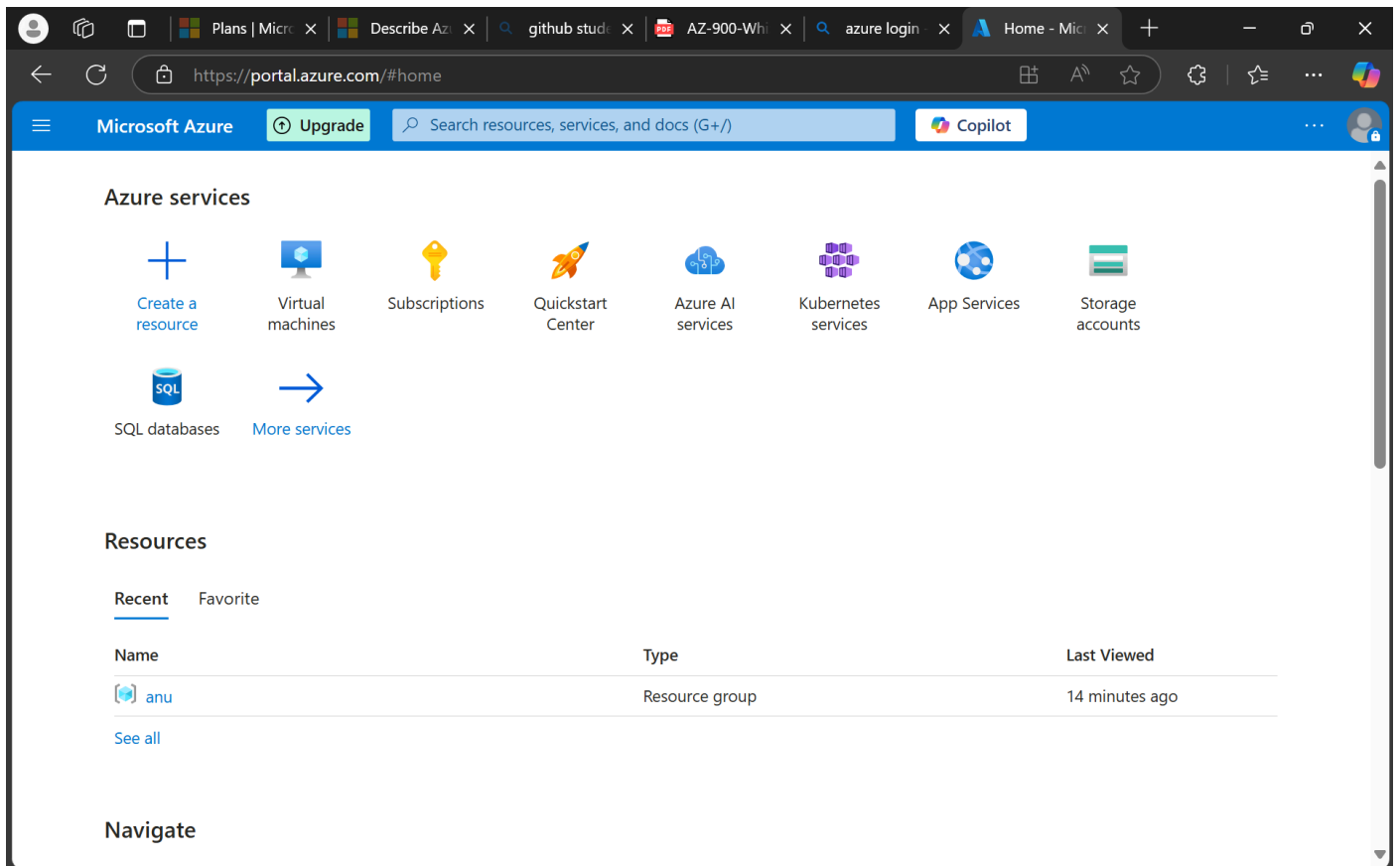
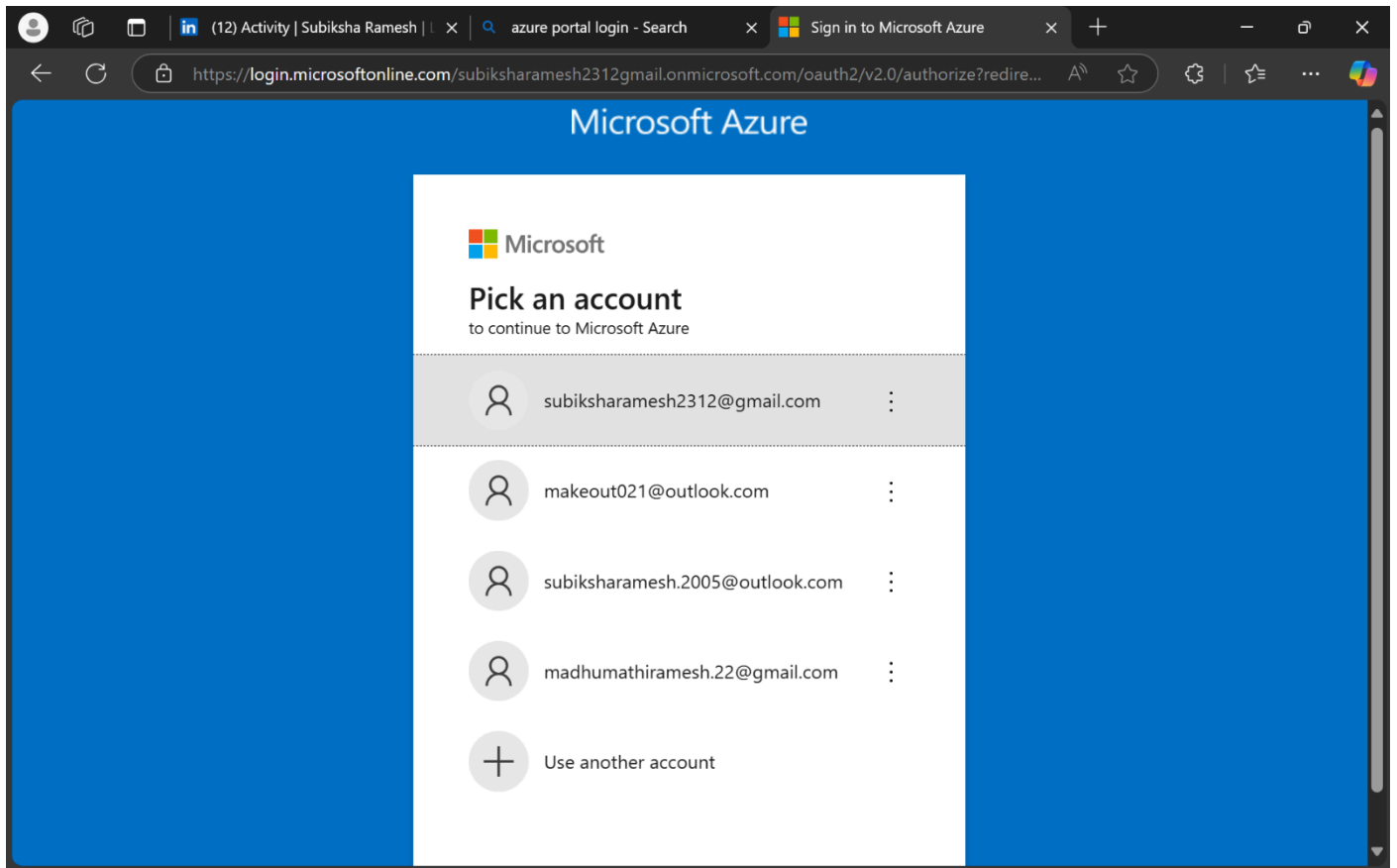
- Create a custom IAM role in the Azure portal.
- Assign the role to a Virtual Machine.
- Restrict/allow specific actions, such as starting and stopping the VM.
- Verify the role assignment and test access permissions.

Step-by-Step procedure :

STEP 1 : Access the Azure Portal

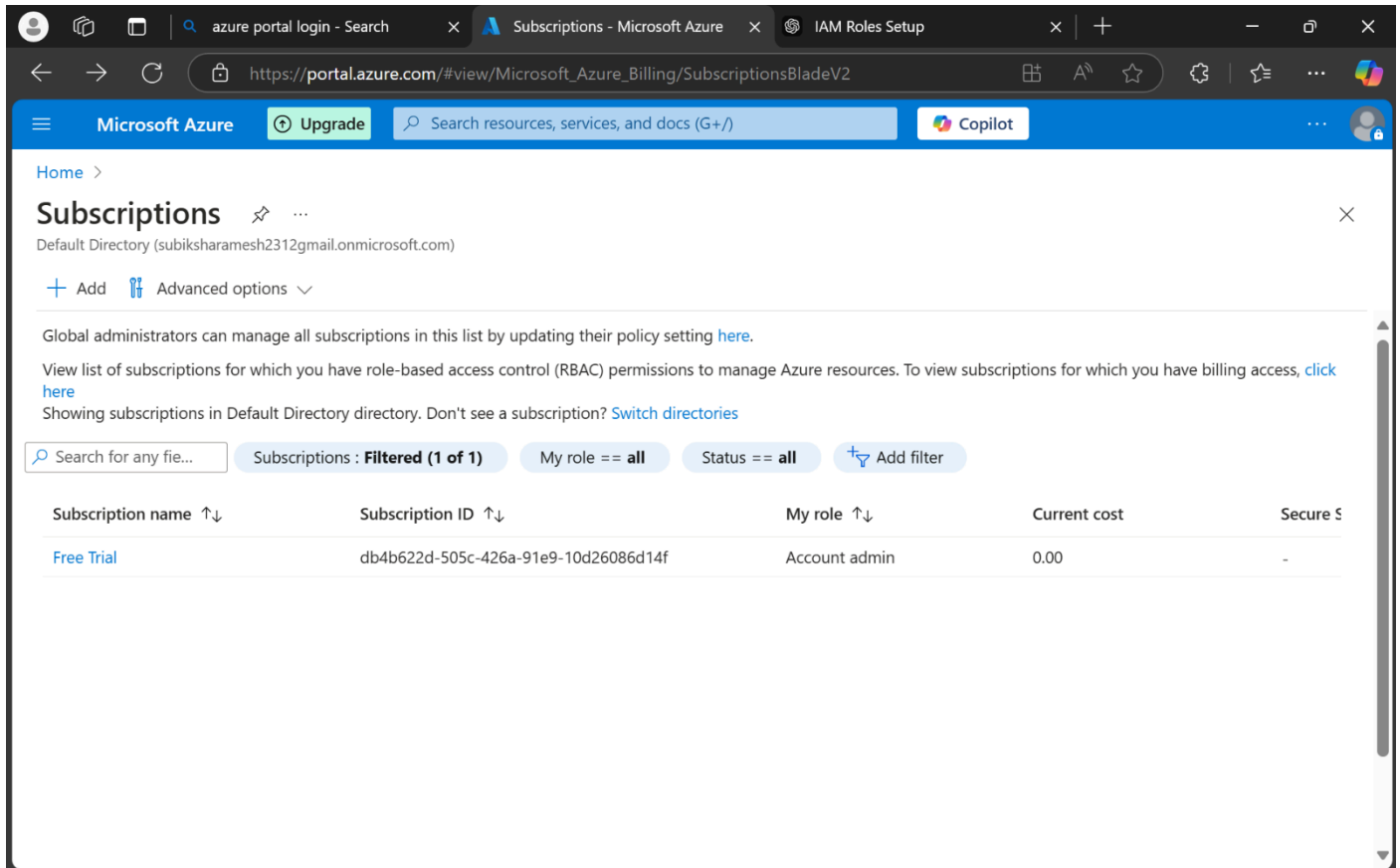
- Navigate to <https://portal.azure.com> and sign in with your credentials.





STEP 2 : Create a Custom IAM Role

- Go to the search bar and type Subscriptions; select your subscription.



The screenshot shows the Microsoft Azure portal interface. The browser tabs include 'azure portal login - Search', 'Subscriptions - Microsoft Azure', and 'IAM Roles Setup'. The address bar shows the URL 'https://portal.azure.com/#view/Microsoft_Azure_Billing/SubscriptionsBladeV2'. The page header includes the 'Microsoft Azure' logo, an 'Upgrade' button, a search bar, and a 'Copilot' button. The main content area is titled 'Subscriptions' and shows a list of subscriptions. A table displays one subscription: 'Free Trial' with ID 'db4b622d-505c-426a-91e9-10d26086d14f', role 'Account admin', and cost '0.00'. The table has columns for 'Subscription name', 'Subscription ID', 'My role', 'Current cost', and 'Secure S'.

Home >

Subscriptions

Default Directory (subiksharamesh2312gmail.onmicrosoft.com)

+ Add Advanced options

Global administrators can manage all subscriptions in this list by updating their policy setting [here](#).

View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have billing access, [click here](#)

Showing subscriptions in Default Directory directory. Don't see a subscription? [Switch directories](#)

Search for any fie... Subscriptions : Filtered (1 of 1) My role == all Status == all Add filter

Subscription name ↑↓	Subscription ID ↑↓	My role ↑↓	Current cost	Secure S
Free Trial	db4b622d-505c-426a-91e9-10d26086d14f	Account admin	0.00	-

azure portal login - Search | Free Trial - Microsoft Azure | IAM Roles Setup

https://portal.azure.com/#@subiksharamesh2312gmail.onmicrosoft.com/resource/subscriptions/db4b...

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > Subscriptions >

Free Trial

Subscription

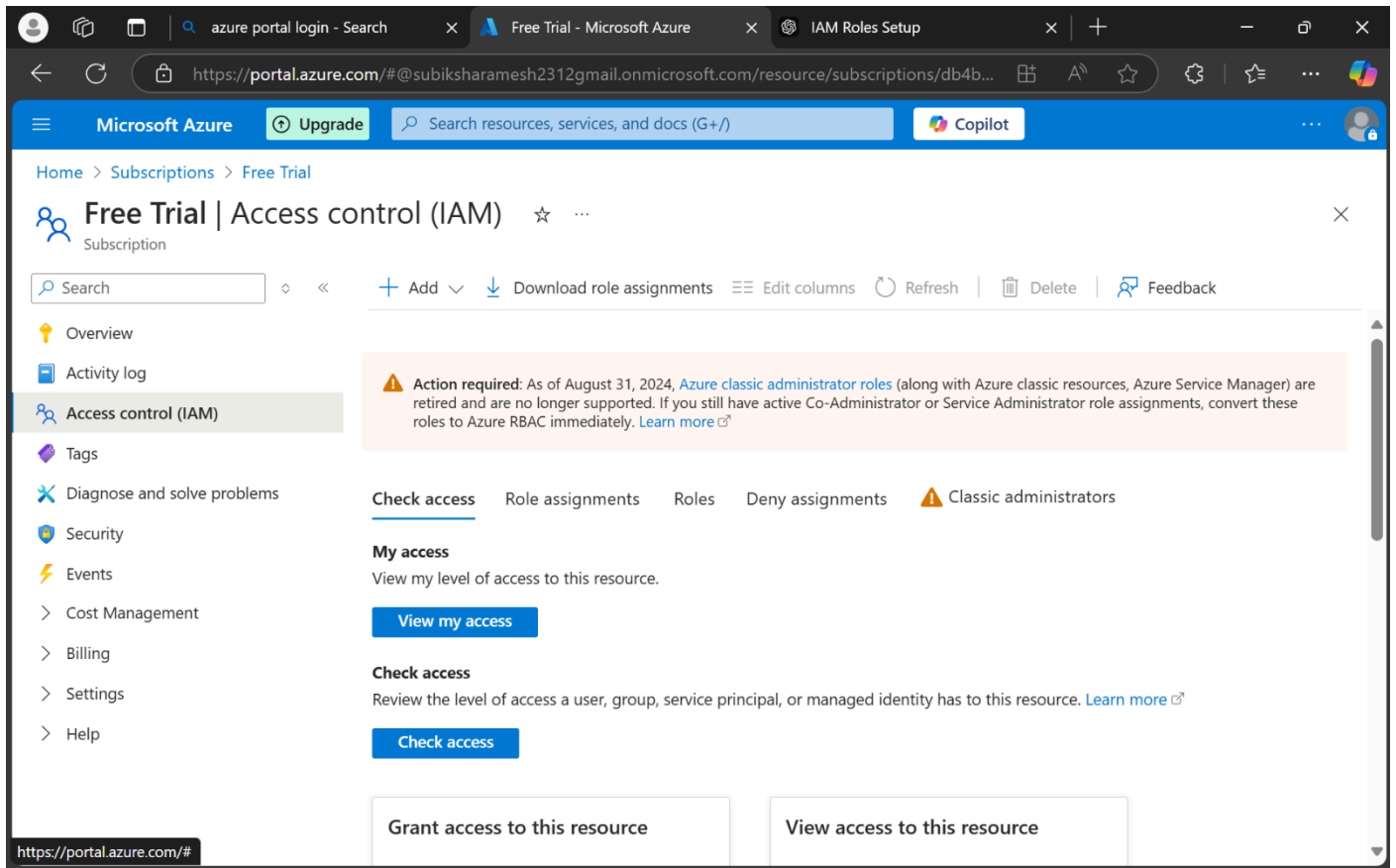
Search Upgrade Cancel subscription Rename Change directory Transfer billing ownership Feedback

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Security
- Events
- Cost Management
- Billing
- Settings
- Help

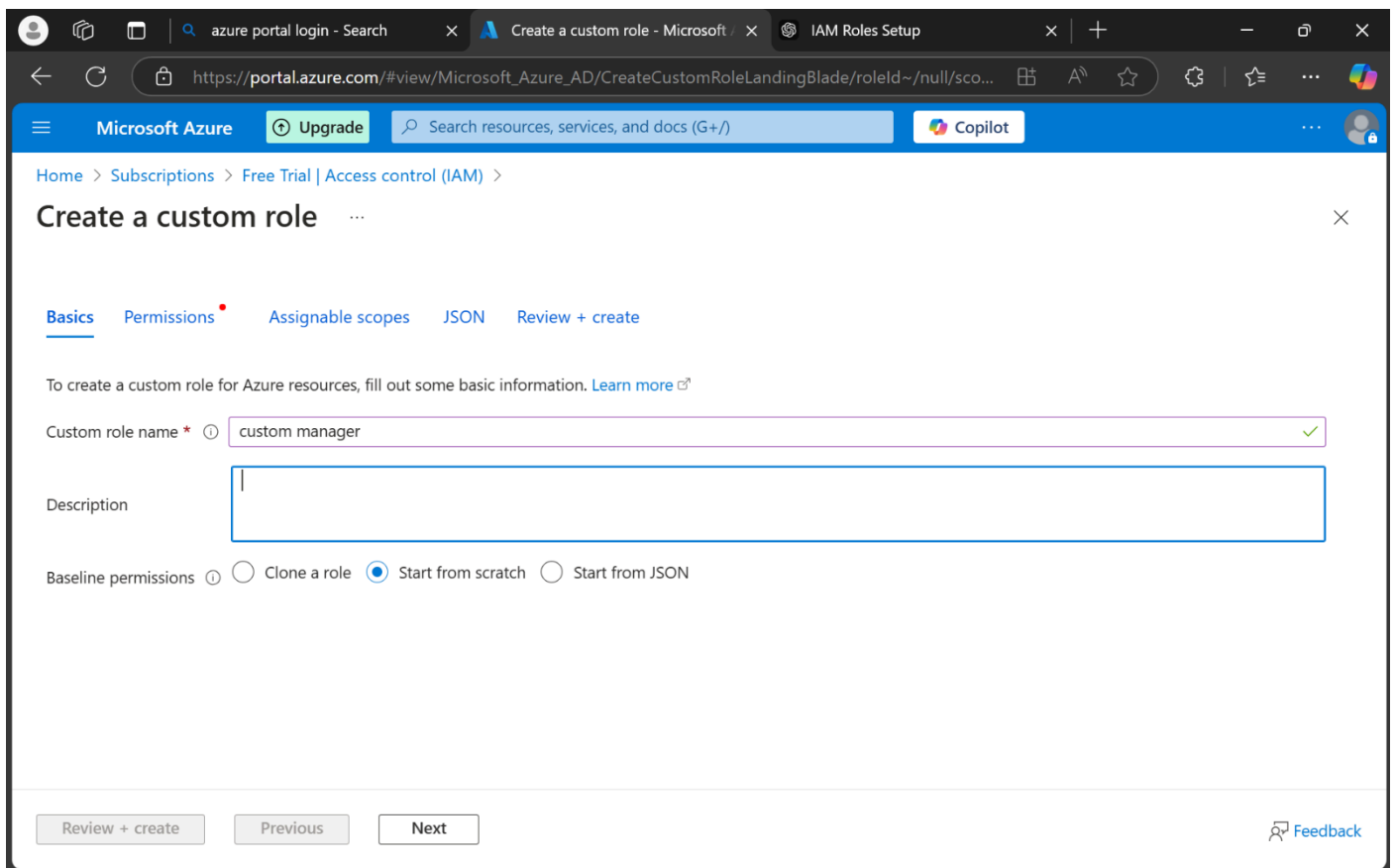
Essentials

Subscription ID	db4b622d-505c-426a-91e9-10d26086d14f	Subscription name	Free Trial
Directory	Default Directory (subiksharamesh2312gmail.onmicrosoft....)	Current billing period	2/2/2025-3/1/2025
My role	Account admin	Currency	INR
Offer	Free Trial	Status	Active
Offer ID	MS-AZR-0044P	Secure Score	Not available
Parent management group			

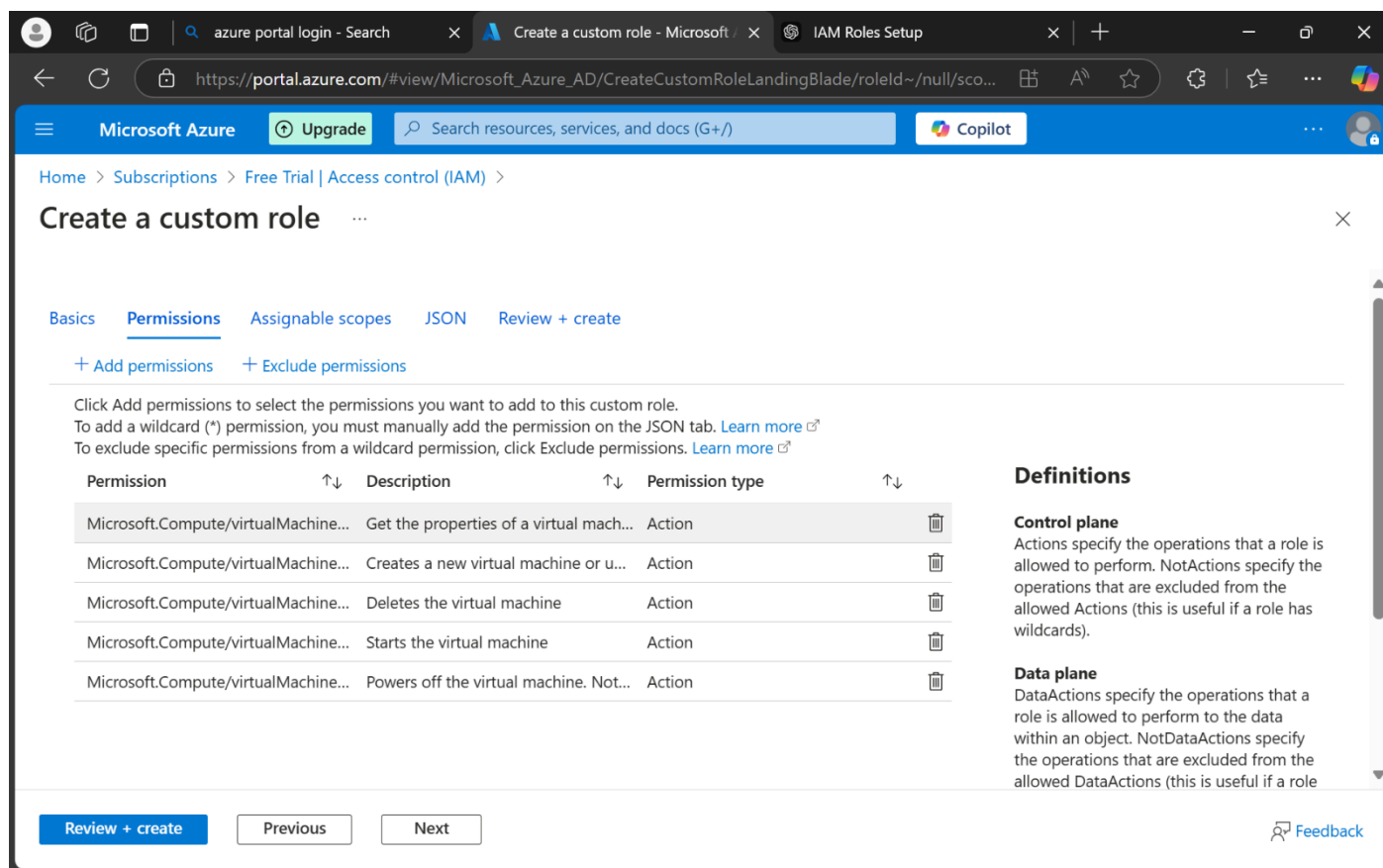
STEP 3 : In the left pane, select Access Control (IAM).



STEP 4 : Click on Roles > + Add > Create Custom Role.



STEP 5 : Click on Roles > + Add > Create Custom Role.



The screenshot shows the 'Create a custom role' page in the Azure portal, specifically the 'Permissions' tab. The page has a blue header with the Microsoft Azure logo, an 'Upgrade' button, a search bar, and a 'Copilot' button. The breadcrumb trail is 'Home > Subscriptions > Free Trial | Access control (IAM) >'. The main title is 'Create a custom role'. Below the title are tabs for 'Basics', 'Permissions' (selected), 'Assignable scopes', 'JSON', and 'Review + create'. Under the 'Permissions' tab, there are links for '+ Add permissions' and '+ Exclude permissions'. A text block explains how to add permissions and wildcards. A table lists five permissions for the 'Microsoft.Compute/virtualMachine...' resource type, all of type 'Action'. To the right, the 'Definitions' section explains 'Control plane' and 'Data plane' actions. At the bottom, there are buttons for 'Review + create', 'Previous', and 'Next', along with a 'Feedback' link.

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > Subscriptions > Free Trial | Access control (IAM) >

Create a custom role

Basics **Permissions** Assignable scopes JSON Review + create

+ Add permissions + Exclude permissions

Click Add permissions to select the permissions you want to add to this custom role.
To add a wildcard (*) permission, you must manually add the permission on the JSON tab. [Learn more](#)
To exclude specific permissions from a wildcard permission, click Exclude permissions. [Learn more](#)

Permission	↑↓	Description	↑↓	Permission type	↑↓
Microsoft.Compute/virtualMachine...		Get the properties of a virtual mach...		Action	
Microsoft.Compute/virtualMachine...		Creates a new virtual machine or u...		Action	
Microsoft.Compute/virtualMachine...		Deletes the virtual machine		Action	
Microsoft.Compute/virtualMachine...		Starts the virtual machine		Action	
Microsoft.Compute/virtualMachine...		Powers off the virtual machine. Not...		Action	

Definitions

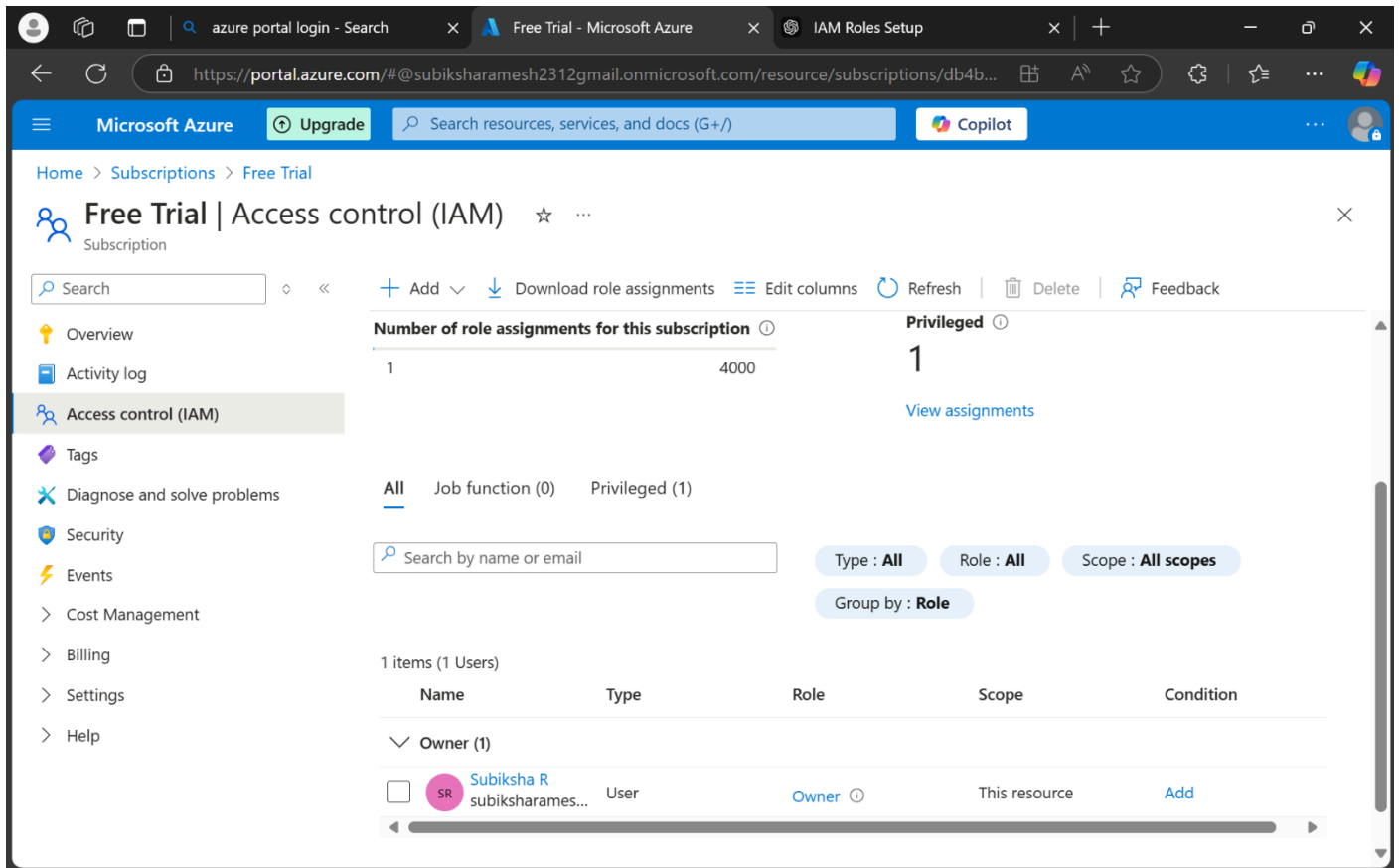
Control plane
Actions specify the operations that a role is allowed to perform. NotActions specify the operations that are excluded from the allowed Actions (this is useful if a role has wildcards).

Data plane
DataActions specify the operations that a role is allowed to perform to the data within an object. NotDataActions specify the operations that are excluded from the allowed DataActions (this is useful if a role

Review + create Previous Next Feedback

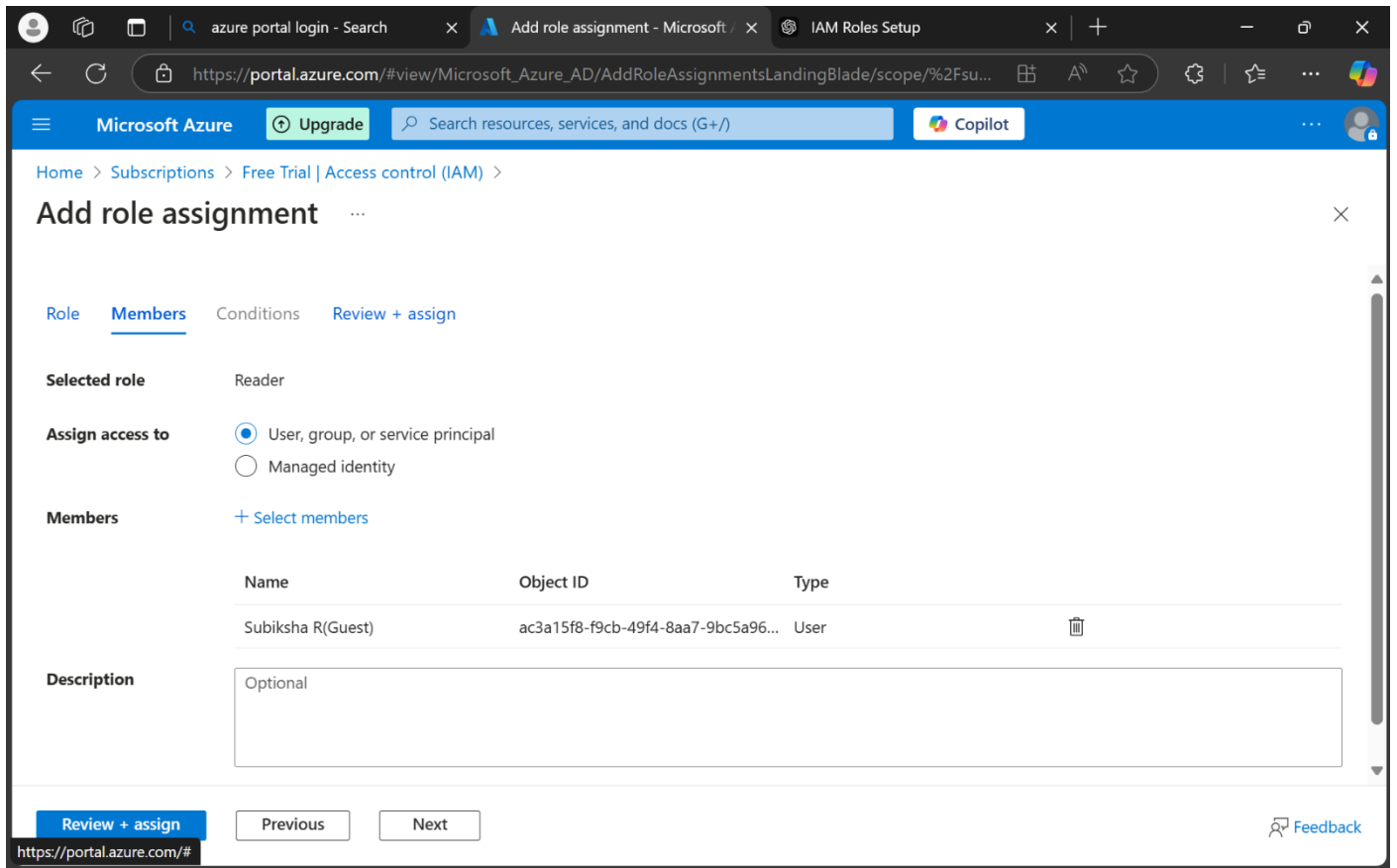
STEP 6 : Click Add and then Next.

- Complete the setup and click **Create**.

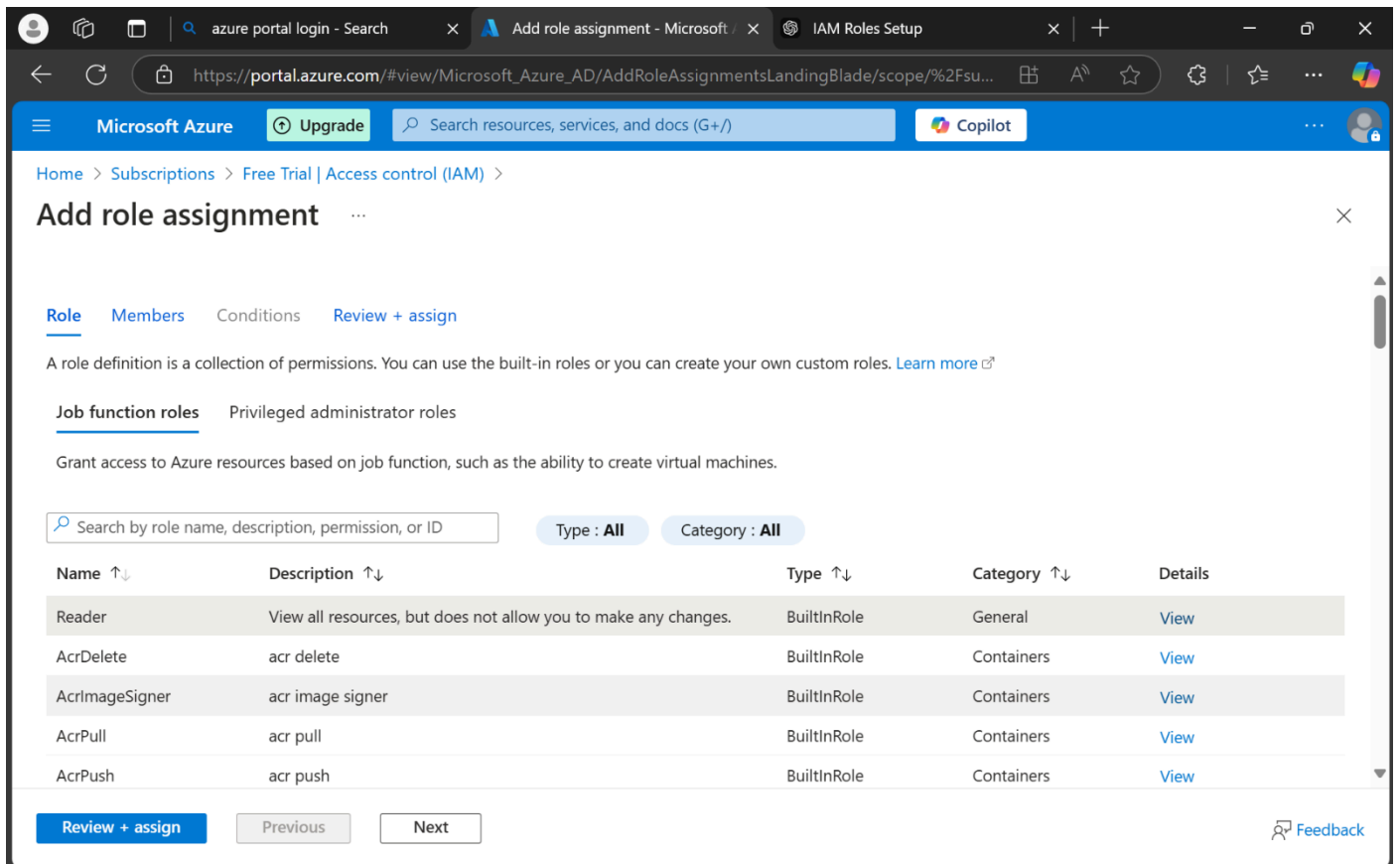


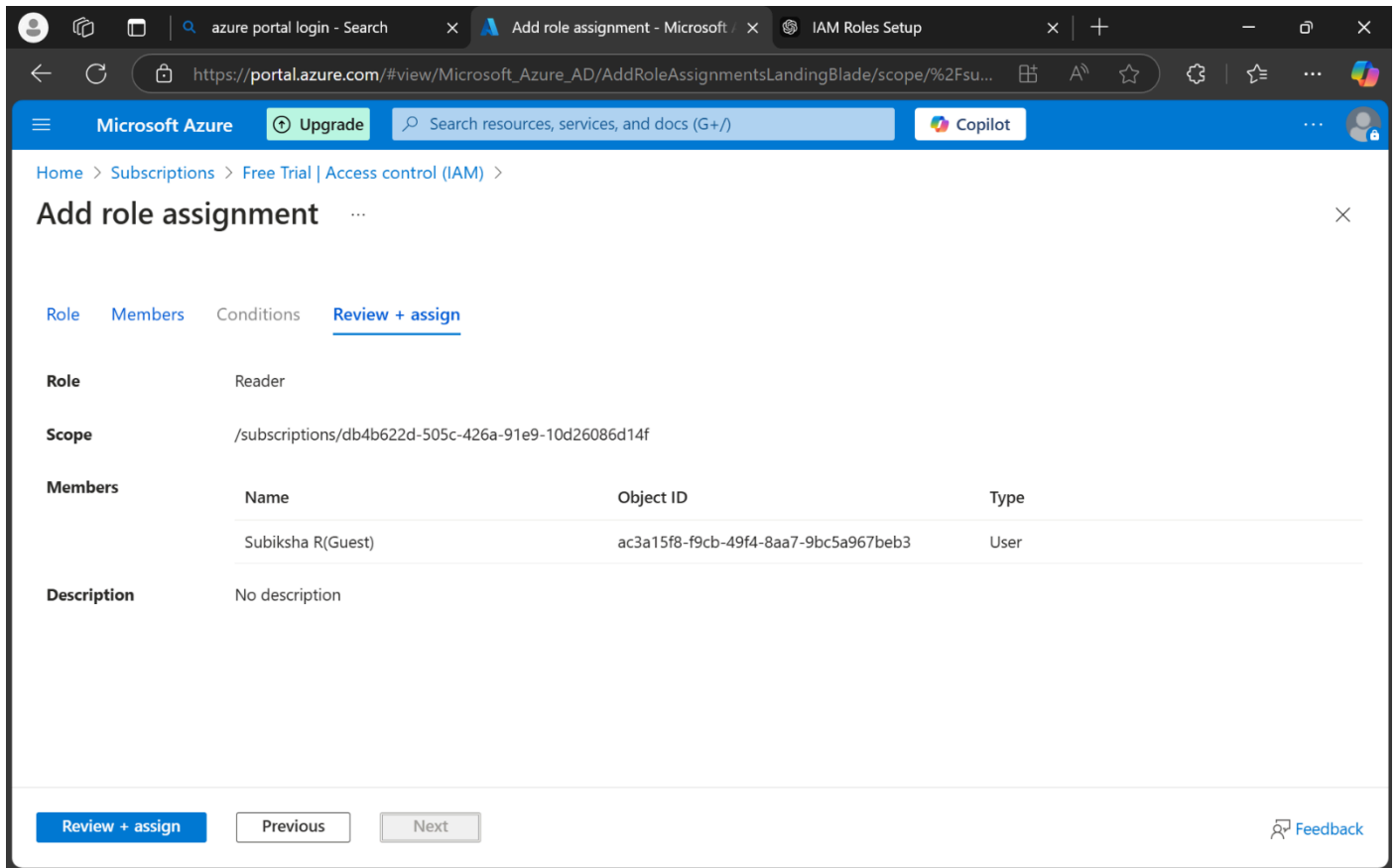
STEP 7 : Assign the Custom Role to a VM.

- Navigate to the specific **Virtual Machine** in your Azure portal.
- On the left menu, select **Access Control (IAM)**.



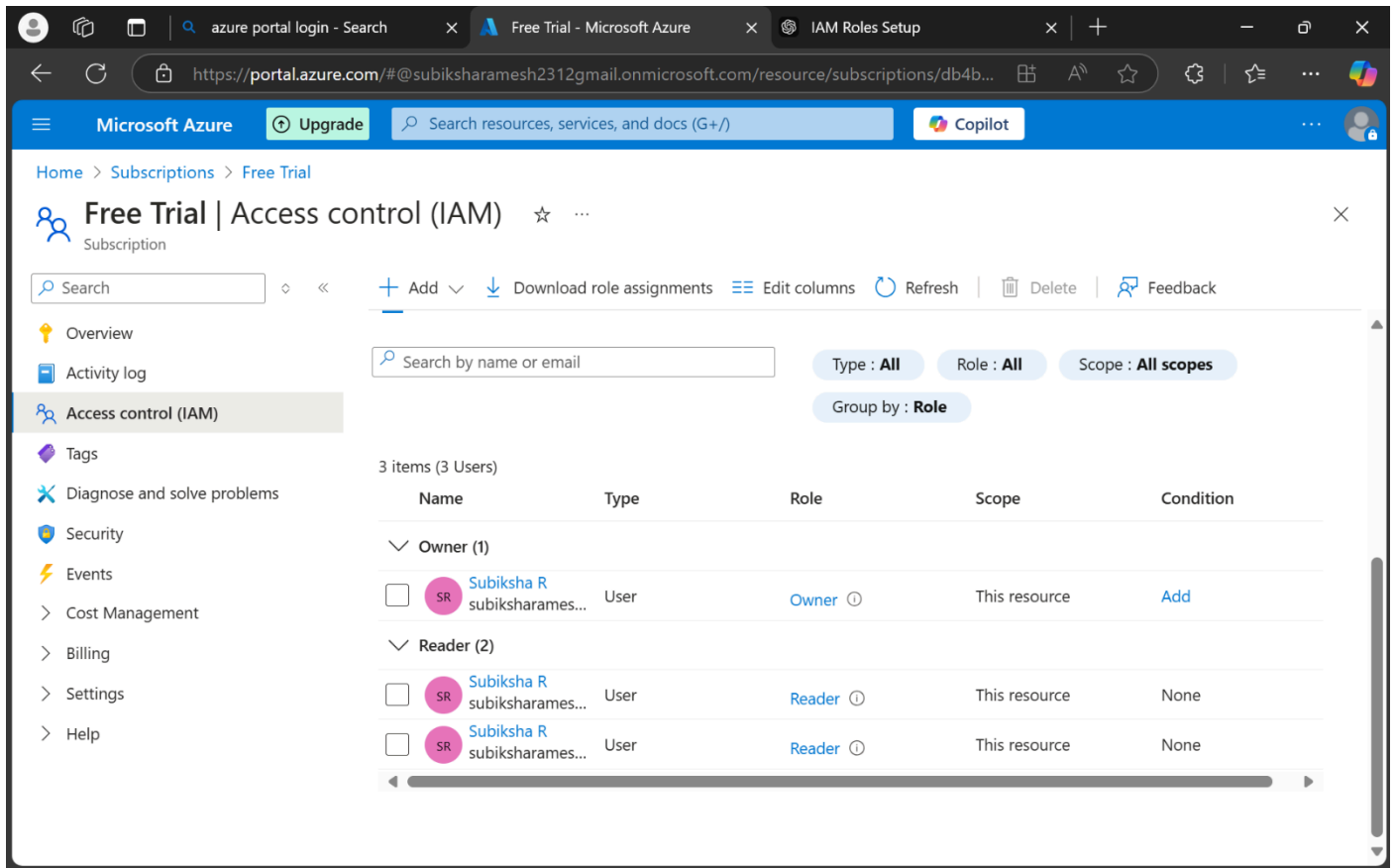
STEP 8 : Click + Add > Add Role Assignment.





STEP 9 :

- In the **Role** dropdown, select the custom role you just created.
- Under **Assign Access To**, choose **User, Group, or Service Principal**.
- Search for the specific user or service principal.
- Click **Save**.



Outcome :

By completing this task, a custom IAM role was successfully created and assigned to an Azure VM. The user with this role can now perform only the allowed actions (start, stop, and read properties of the VM) while restricted actions such as deleting the VM remain blocked. This ensures secure and efficient resource management in the cloud environment.