**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: Subiksha R 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 :**

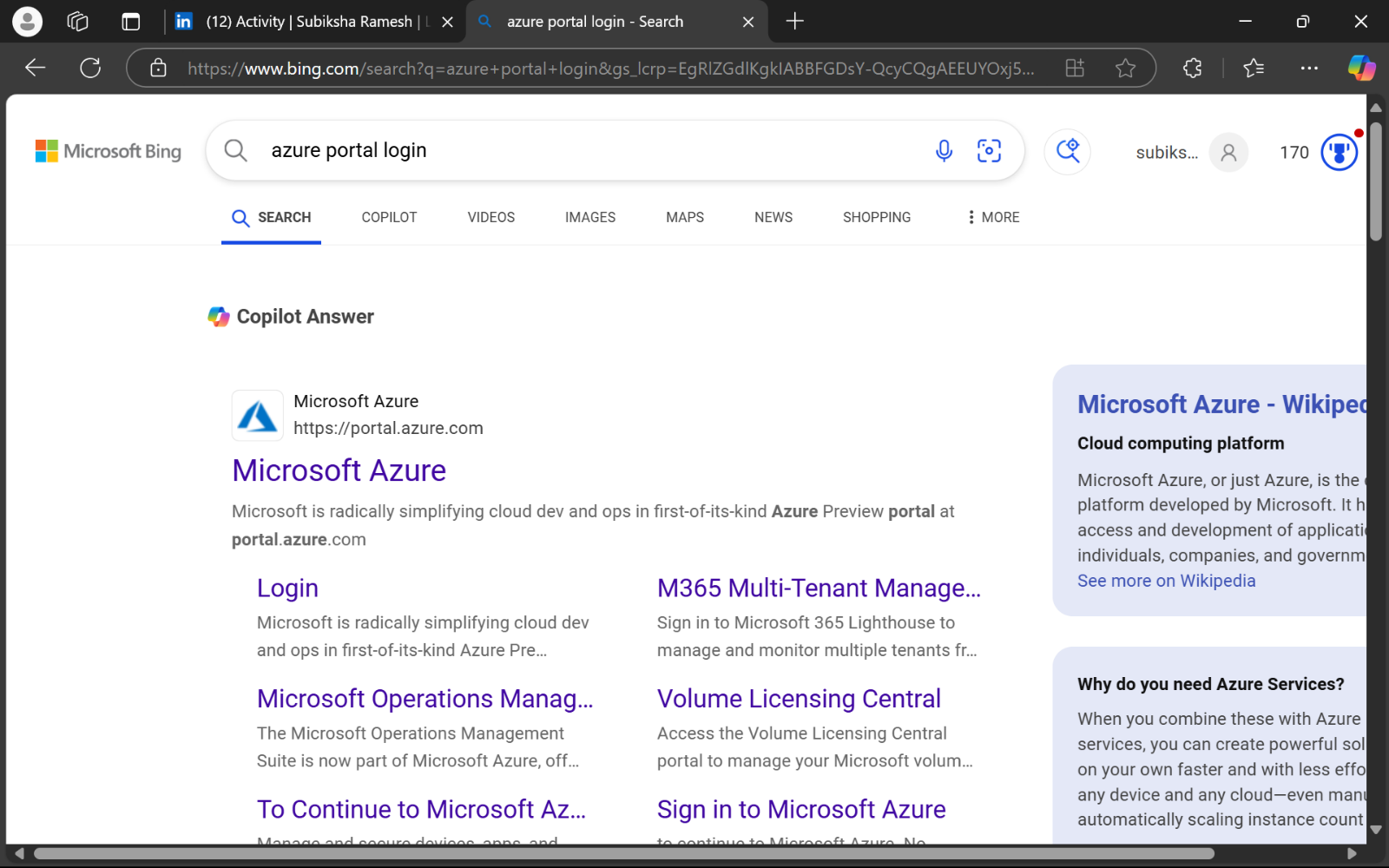
The objective of this task is to:

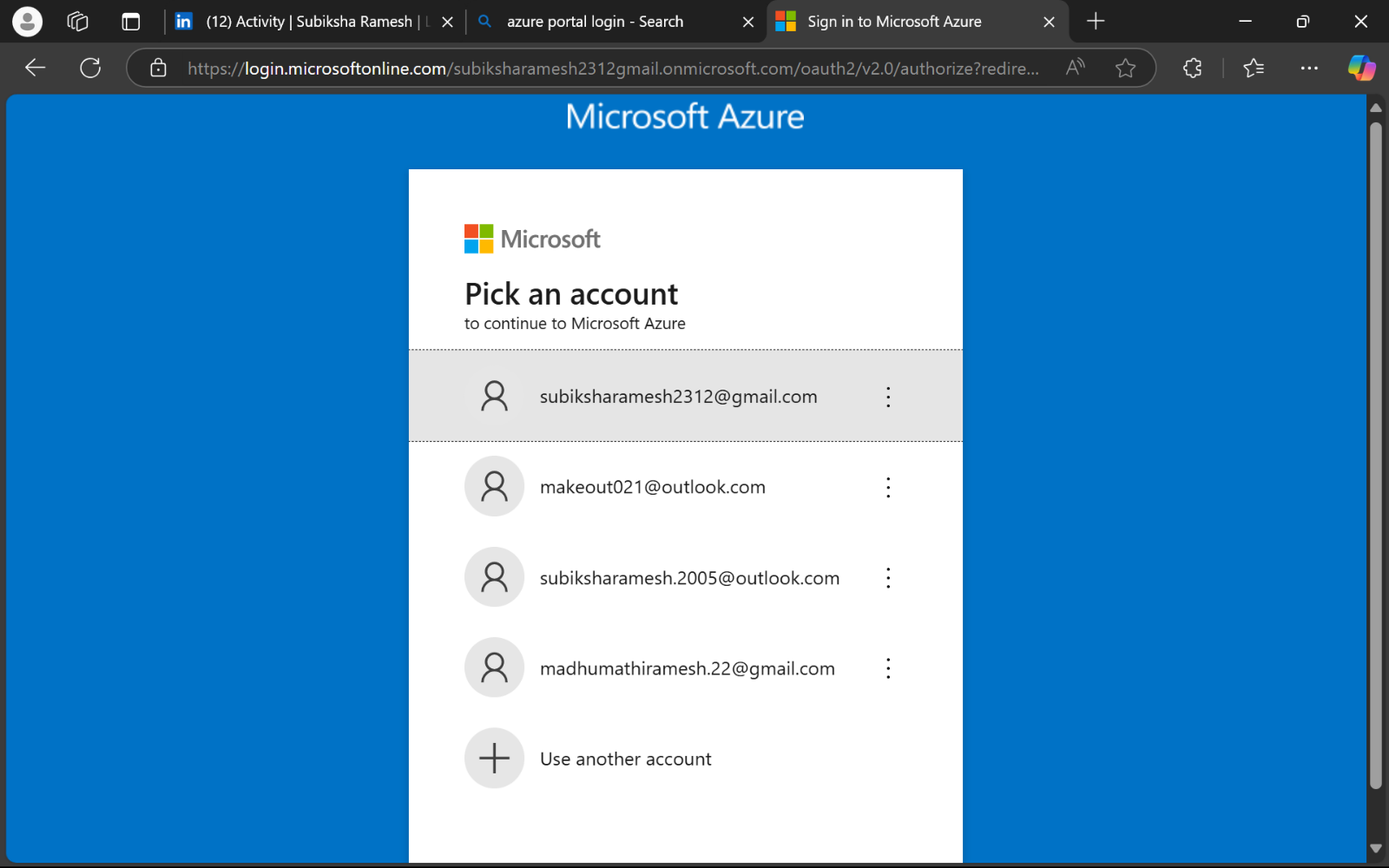
* Create a custom IAM role in the Azure portal.
* Assign the role to a Virtual Machine.
* Restrict/allow specific actions, such as starting and stopping the VM.
* Verify the role assignment and test access permissions.

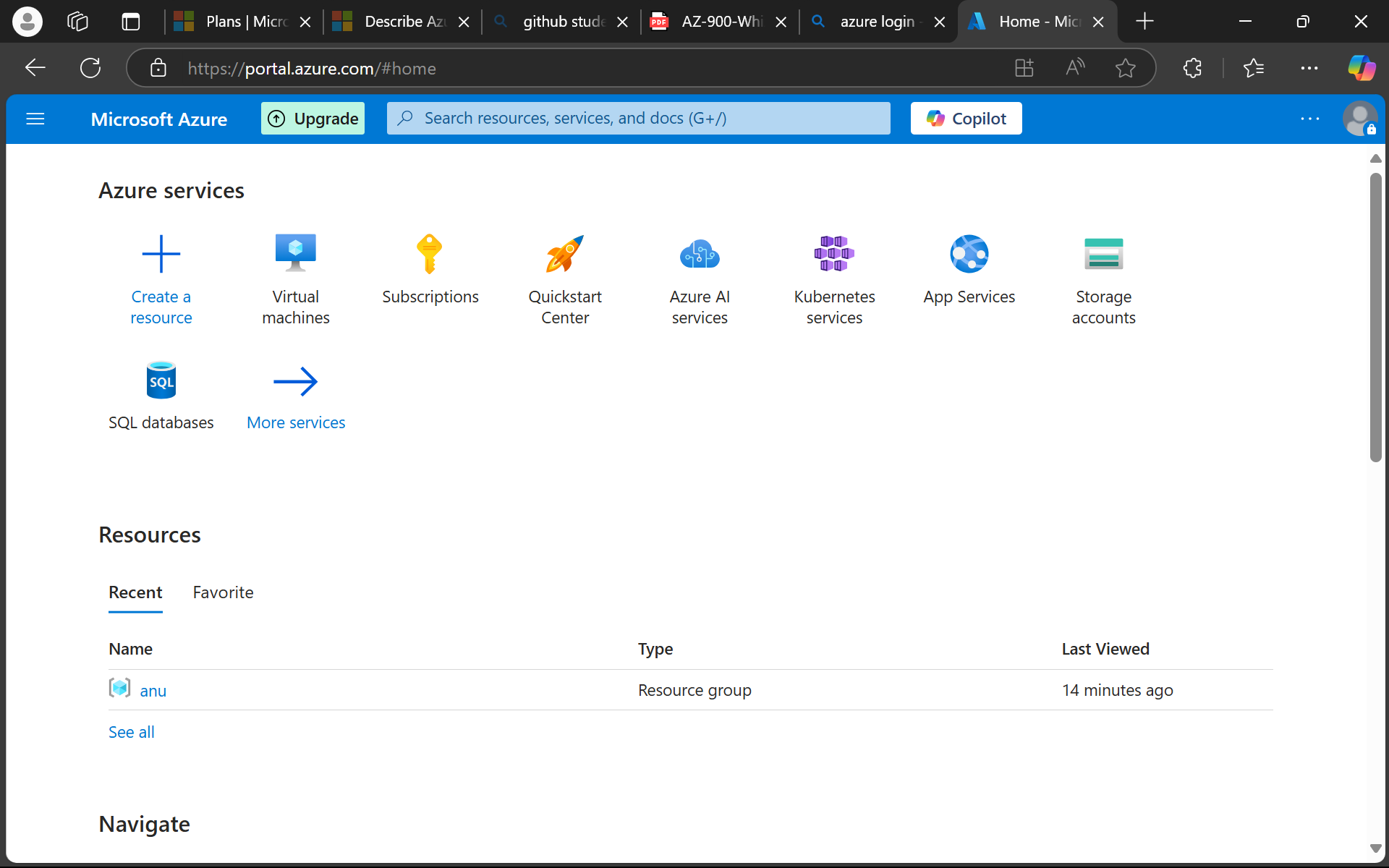
**Step-by-Step procedure :**

**STEP 1 : Access the Azure Portal**

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

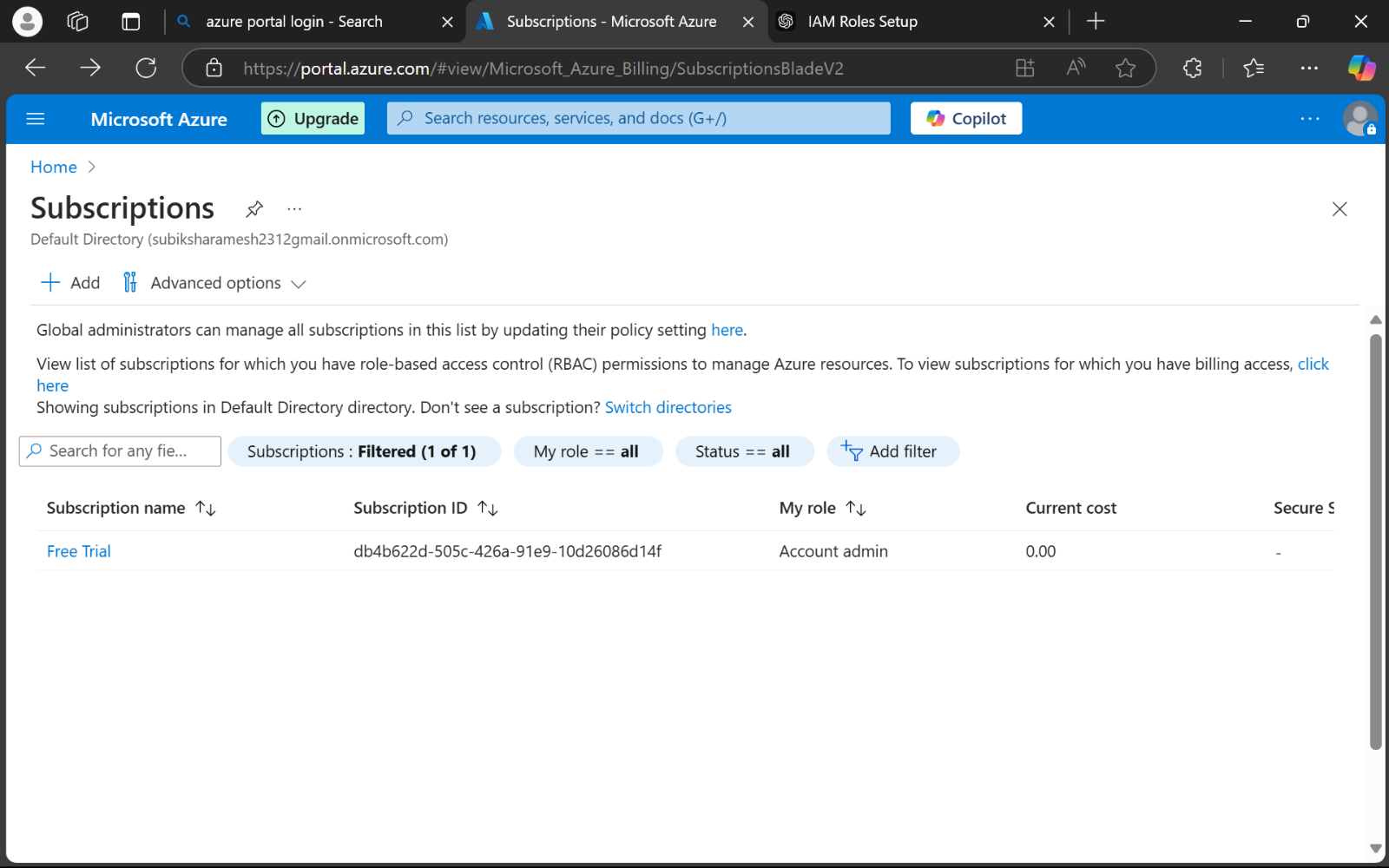


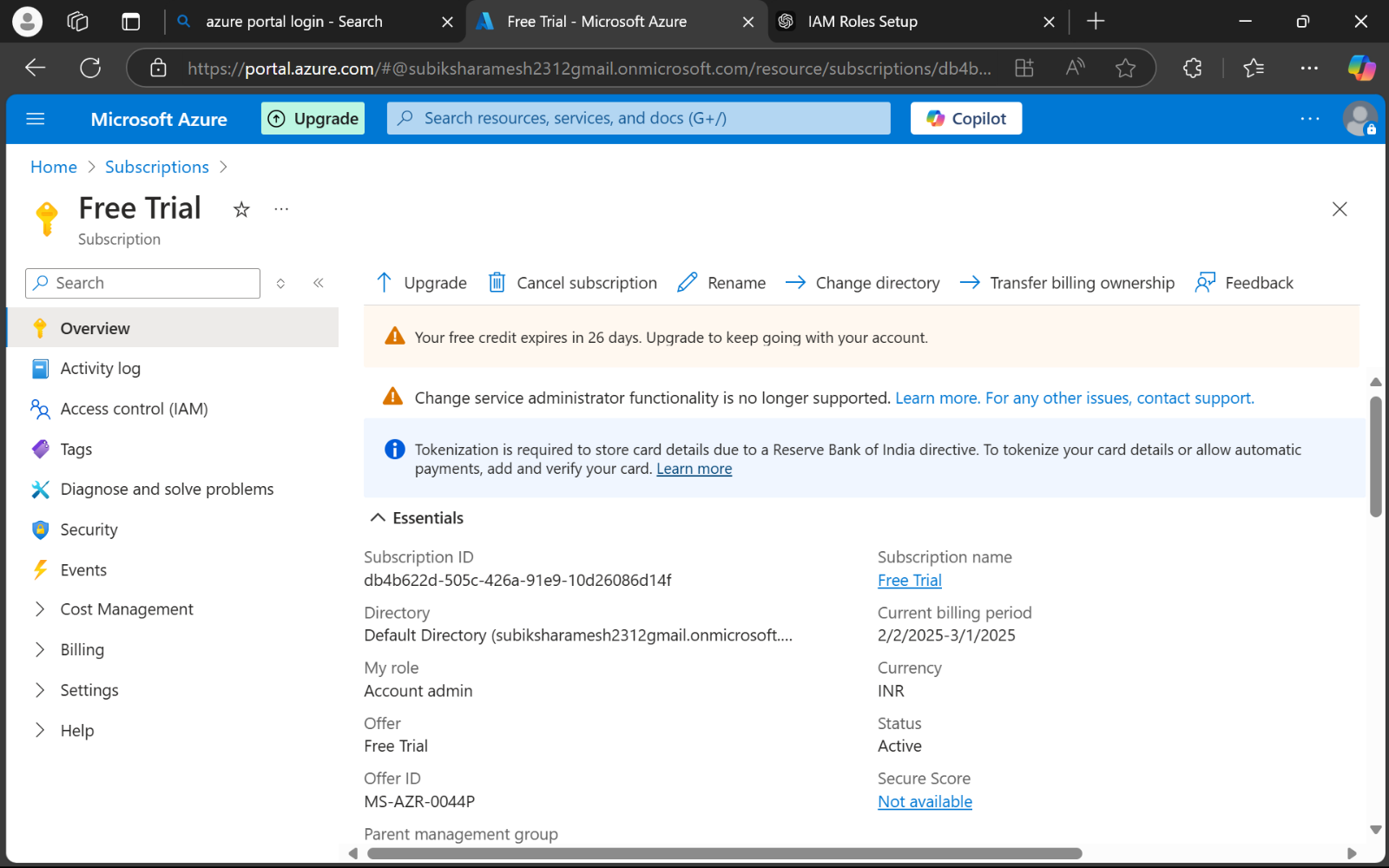


****

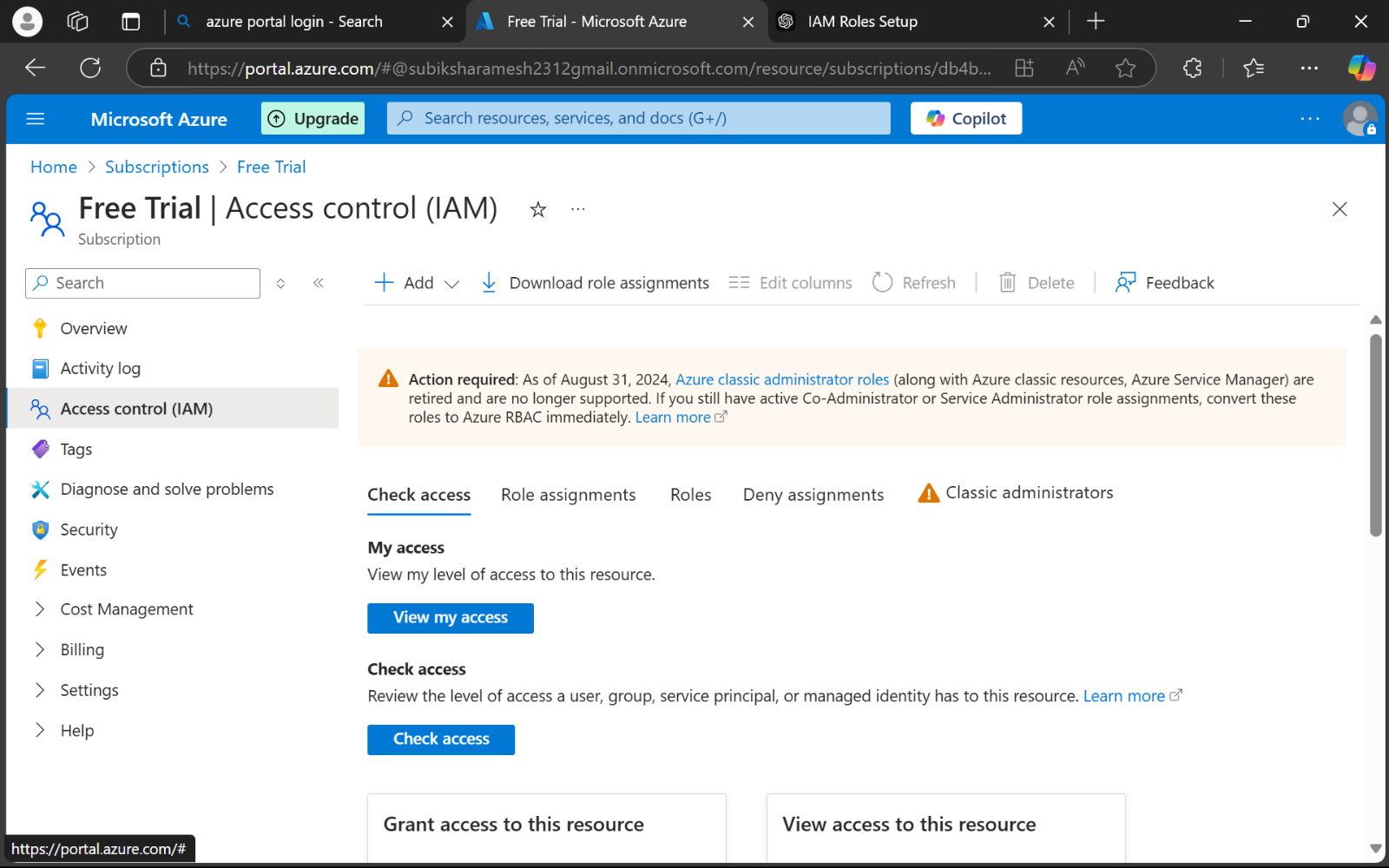
**STEP 2 : Create a Custom IAM Role**

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

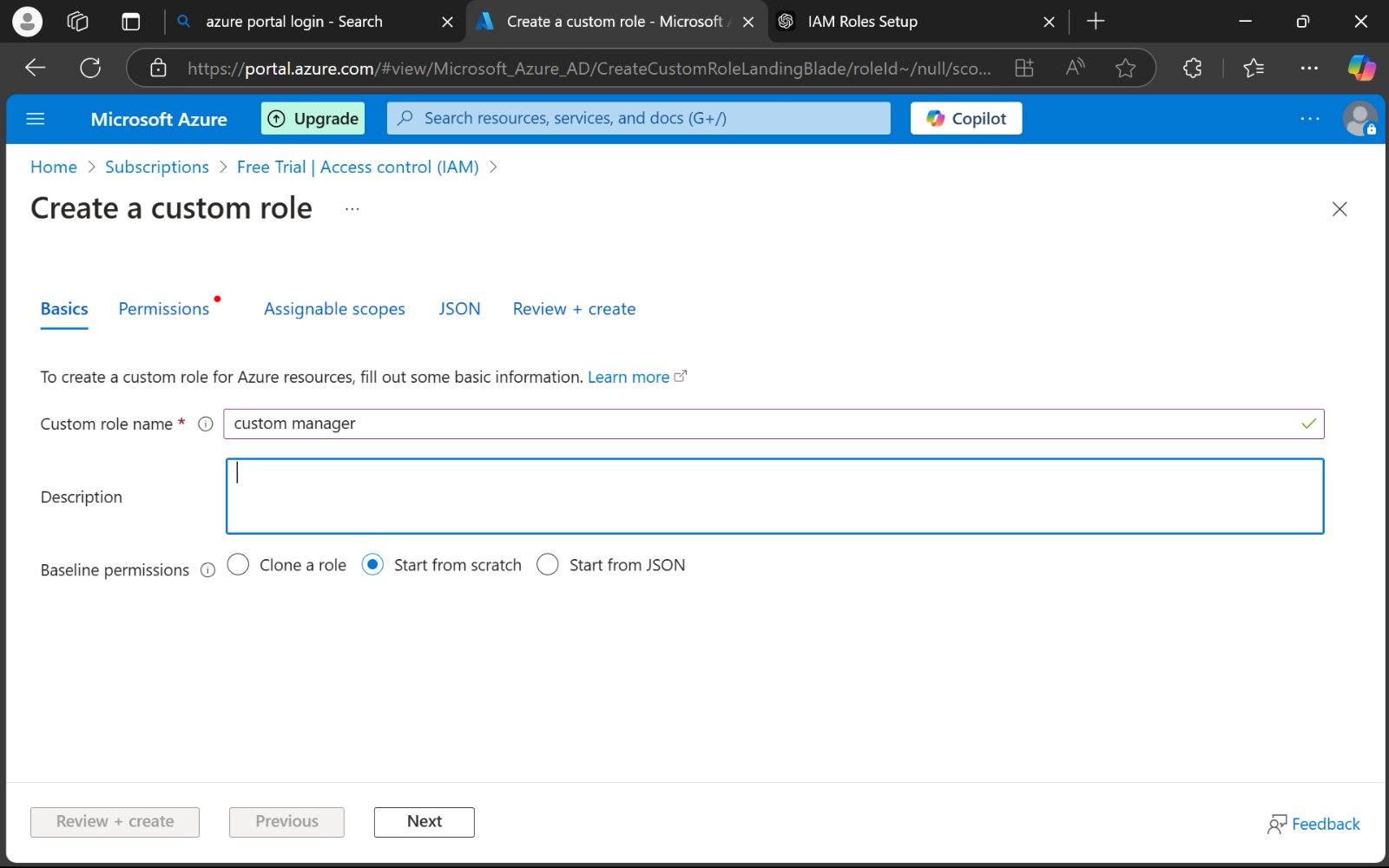
****

****

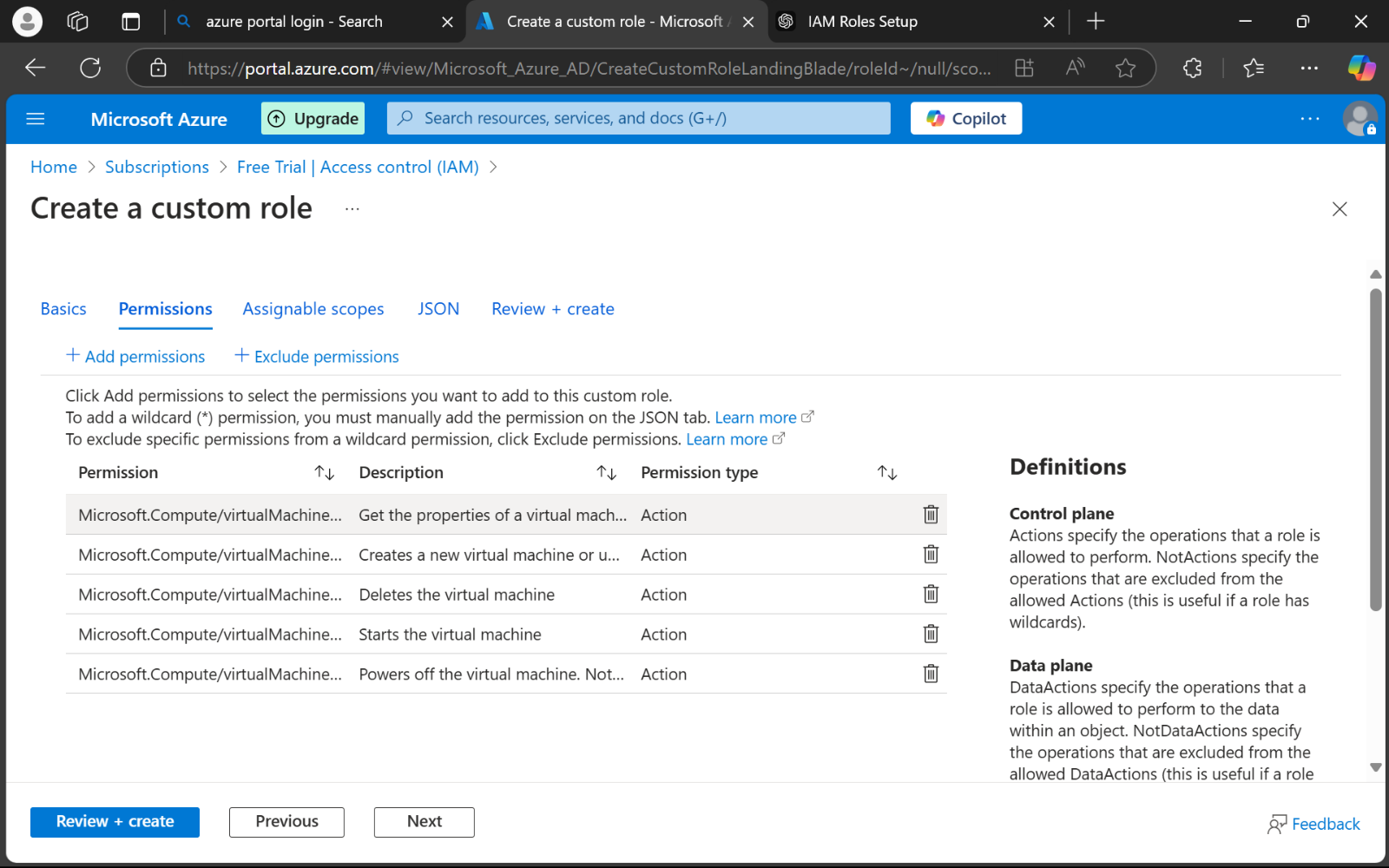
**STEP 3 :** In the left pane, select Access Control (IAM).



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

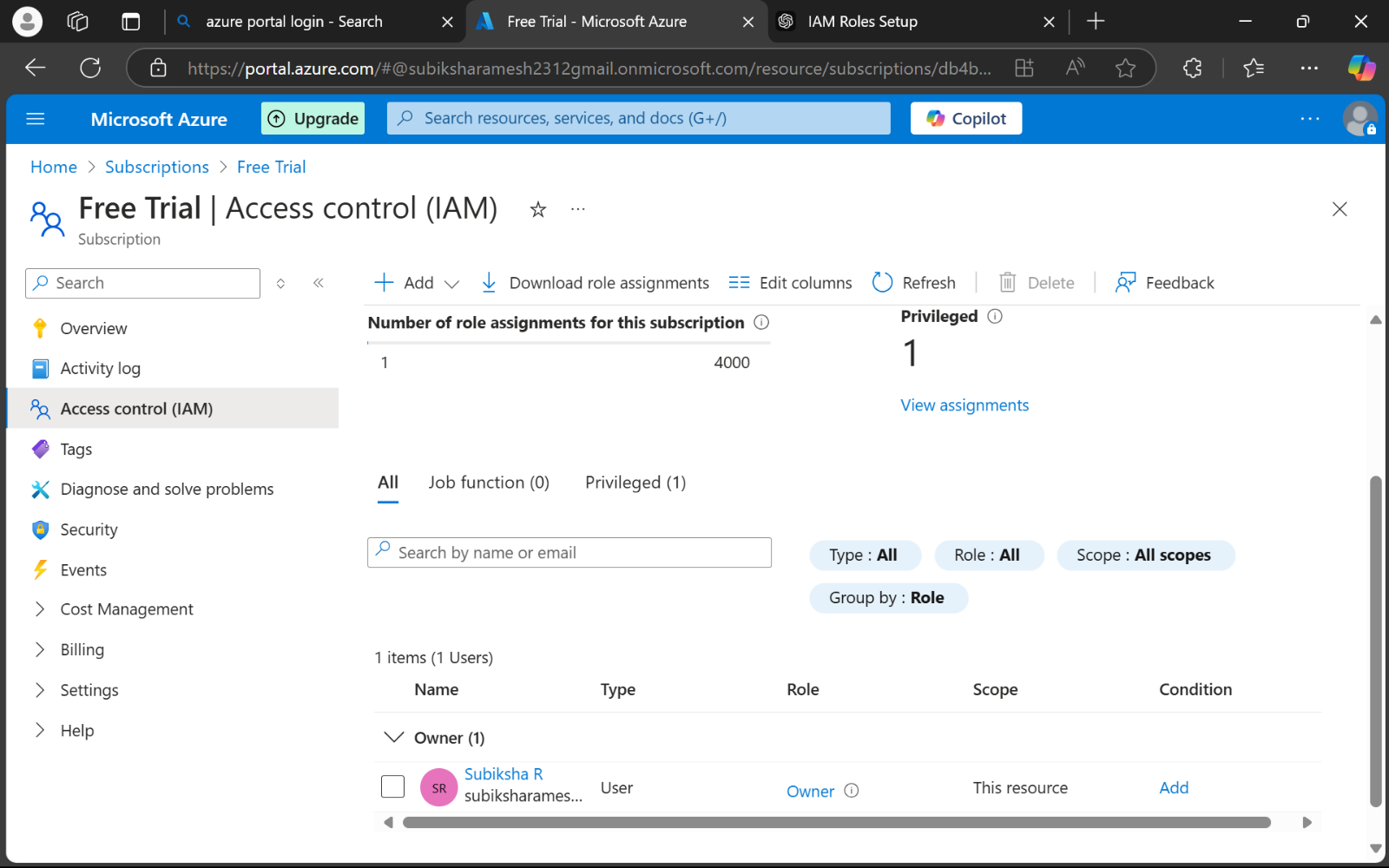


**STEP 5 :** Click on Roles > + Add > Create Custom Role.

****

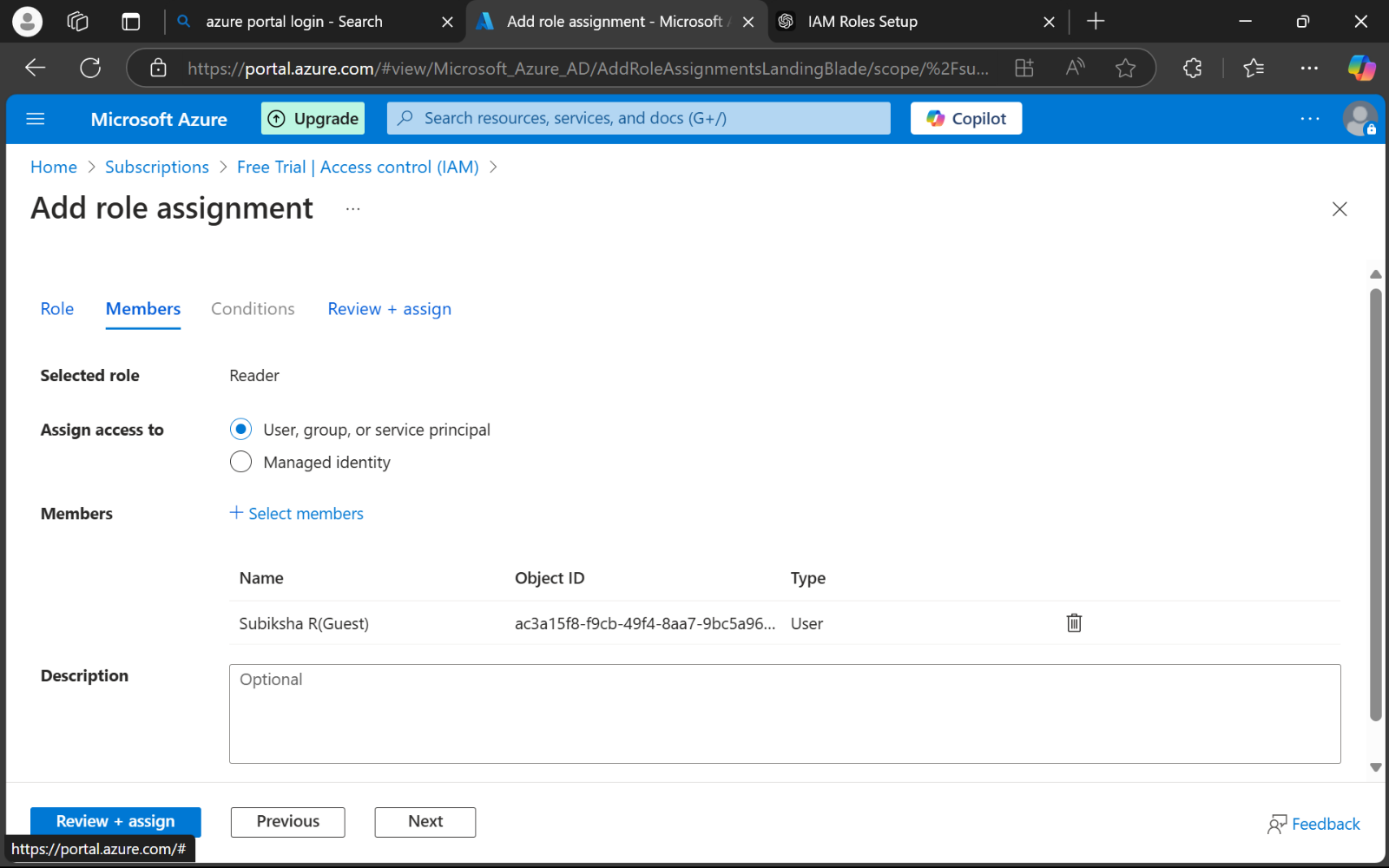
**STEP 6 :** Click Add and then Next.

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

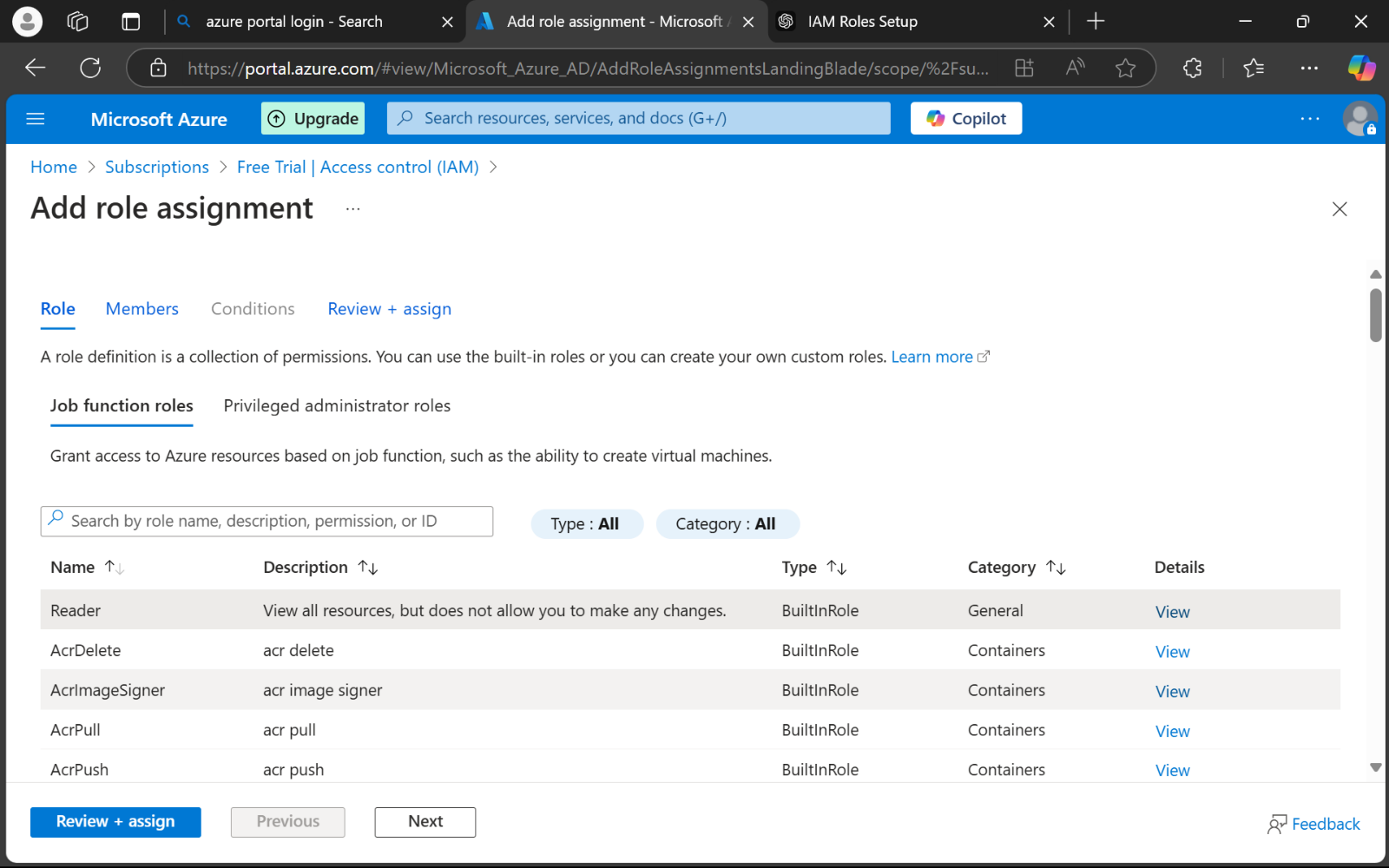


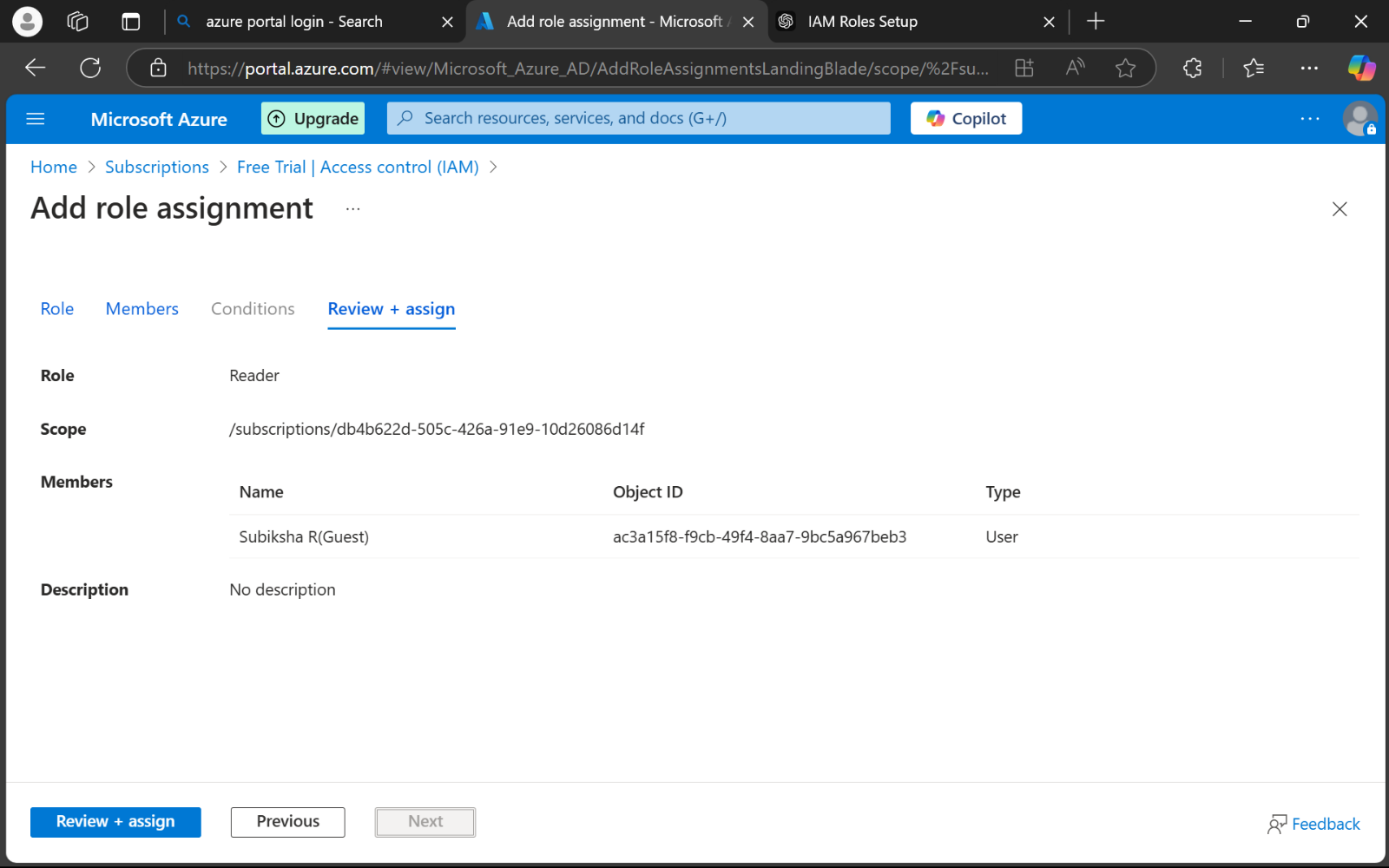
**STEP 7 : Assign the Custom Role to a VM.**

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



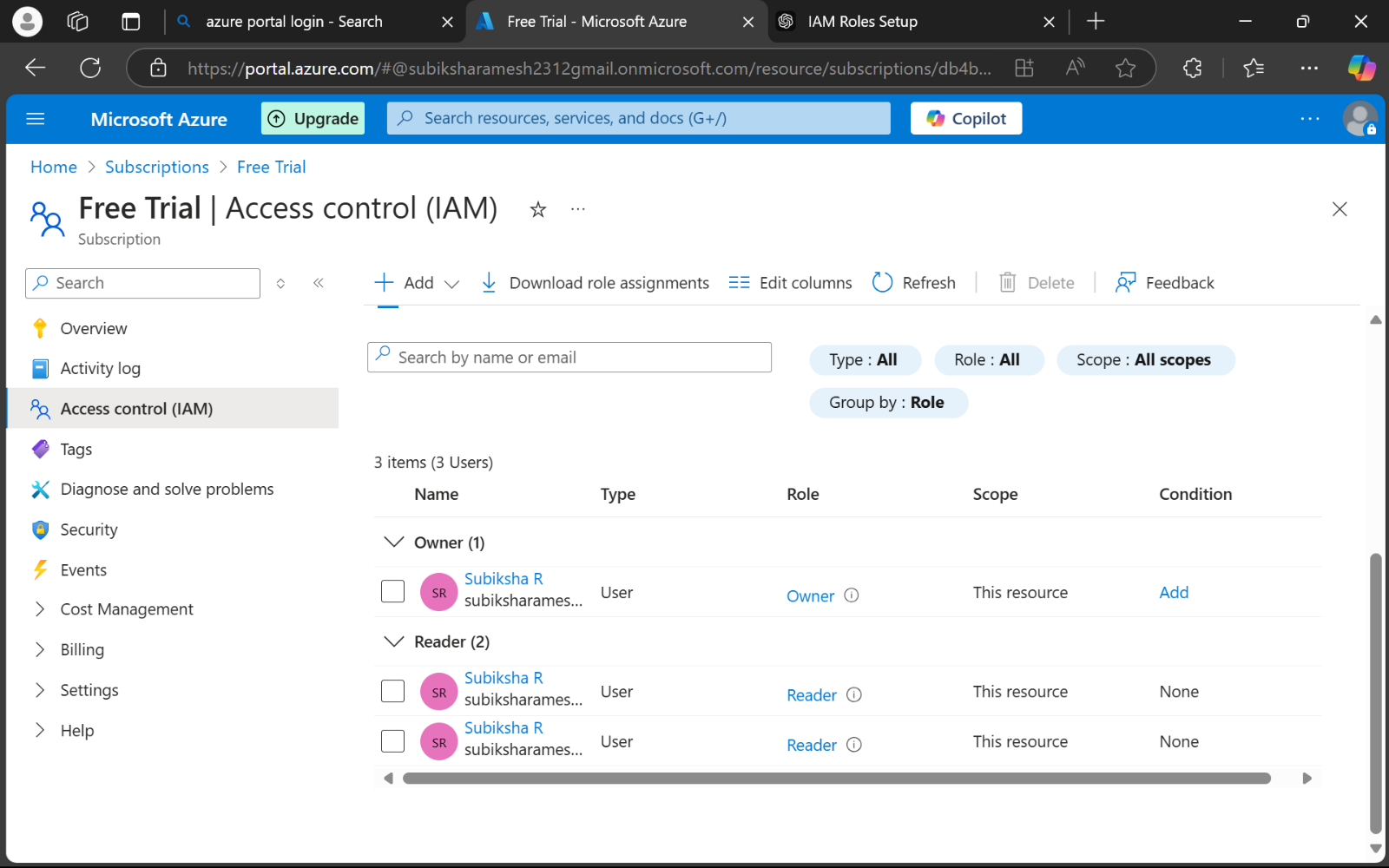
**STEP 8 :** Click + Add > Add Role Assignment.





**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.