**Placement Empowerment Program**

***Cloud Computing and DevOps Centre***

**Set Up IAM Roles and Permissions:** Create an IAM role on your cloud platform. Assign the role to your VM to restrict/allow specific actions.

Name: Kirubalini S I Department: IT



**Introduction**

In cloud environments like Azure, security is paramount. Controlling who has access to your resources and what actions they can perform is essential for protecting sensitive data and preventing unauthorized modifications. Azure's Role-Based Access Control (RBAC) provides a granular way to manage access to Azure resources, including VMs. By creating IAM roles and assigning them to your VMs, you can implement the principle of least privilege, ensuring that your VMs only have the necessary permissions to function, thereby minimizing potential security risks.

**Overview**

This process involves defining roles with specific sets of permissions and then assigning those roles to your VMs. We leverage Azure's managed identities for VMs, which simplifies credential management and enhances security. A managed identity acts as an authentication mechanism for the VM, allowing it to securely access other Azure resources without needing to manage explicit credentials. We'll cover creating both system-assigned and user-assigned managed identities and associating them with roles at appropriate scopes (e.g., resource group, subscription, or individual resource). The scope determines the level at which the permissions granted by the role apply.

**Objective**

The primary objectives of setting up IAM roles and permissions for VMs in Azure are:

**Enhance Security:** Implement the principle of least privilege, limiting the potential impact of a compromised VM.

**Simplify Access Management:** Centralize permission management through roles, making it easier to update and revoke access.

**Improve Auditability:** Track who has access to which resources and what actions they can perform.

**Automate Permission Management:** Integrate RBAC with automation tools for programmatic control over access.

**Meet Compliance Requirements:** Adhere to industry best practices and regulatory requirements for data security and access control.

**Importance**

Implementing robust IAM for VMs is crucial for several reasons:

**Data Protection:** Prevents unauthorized access to sensitive data stored on or accessed by VMs.

**Resource Security:** Protects VMs from unauthorized modifications or deletion.

**Compliance:** Helps organizations meet regulatory requirements related to data privacy and security.

**Operational Efficiency:** Streamlines access management, reducing administrative overhead.

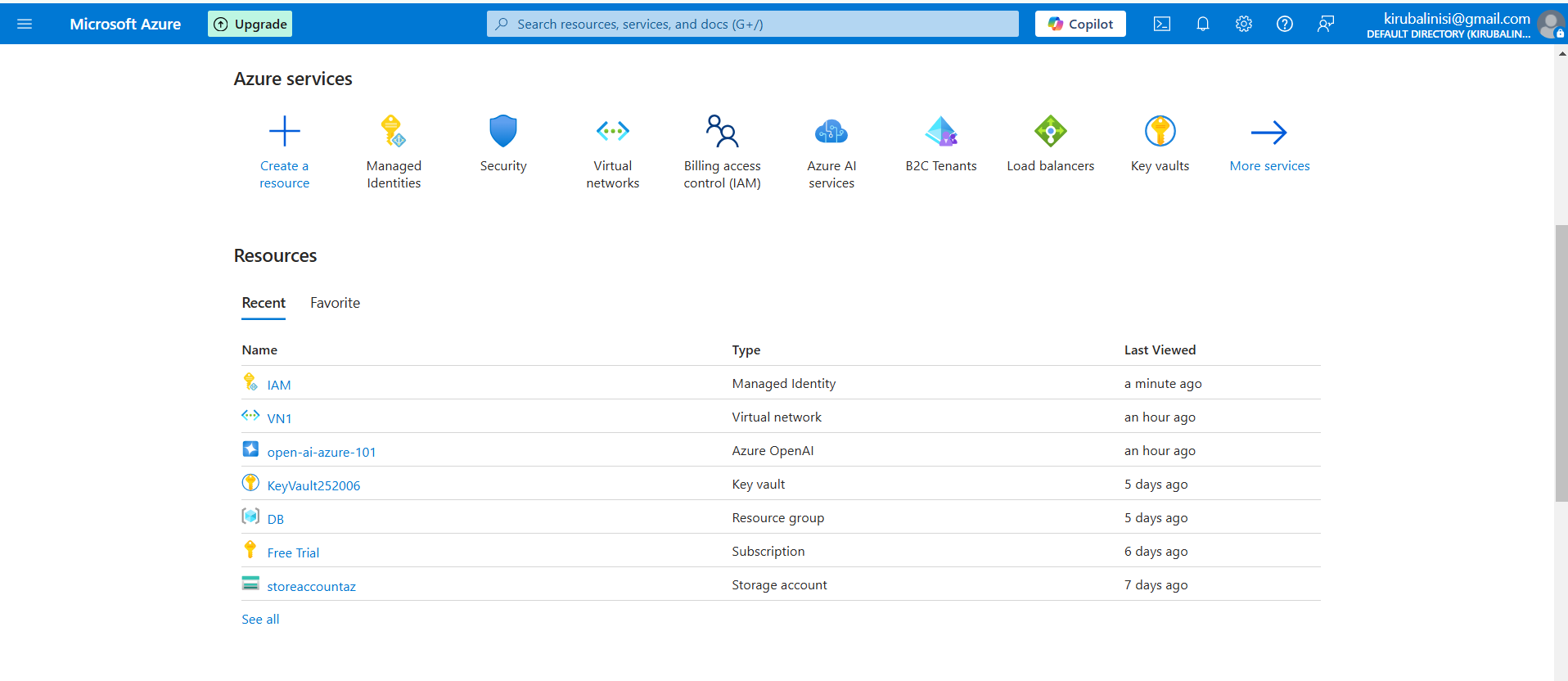
**Risk Mitigation:** Minimizes the risk of security breaches and data leaks.

**Step-by-Step Overview**

**Step 1:**

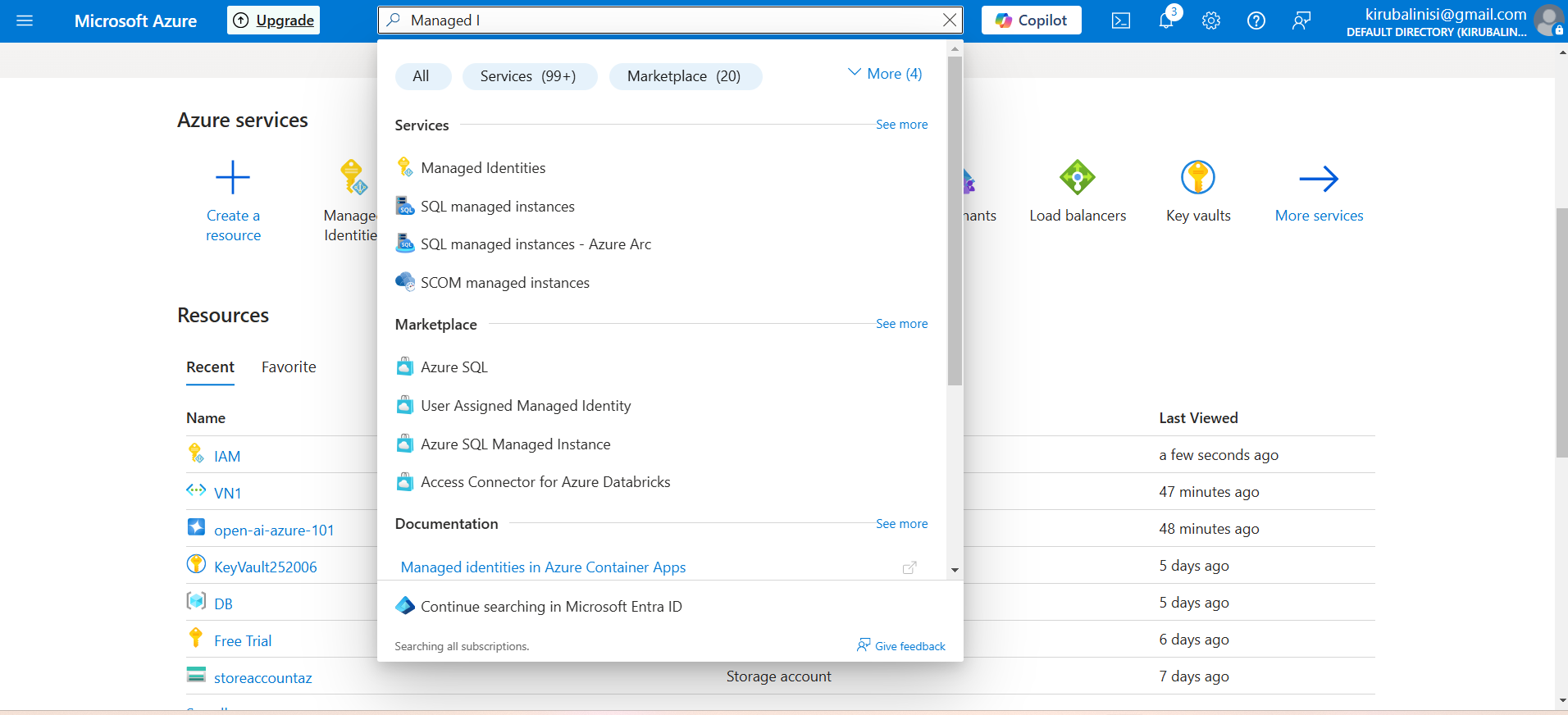
Open the Azure portal.

[Home - Microsoft Azure](https://portal.azure.com/#home)



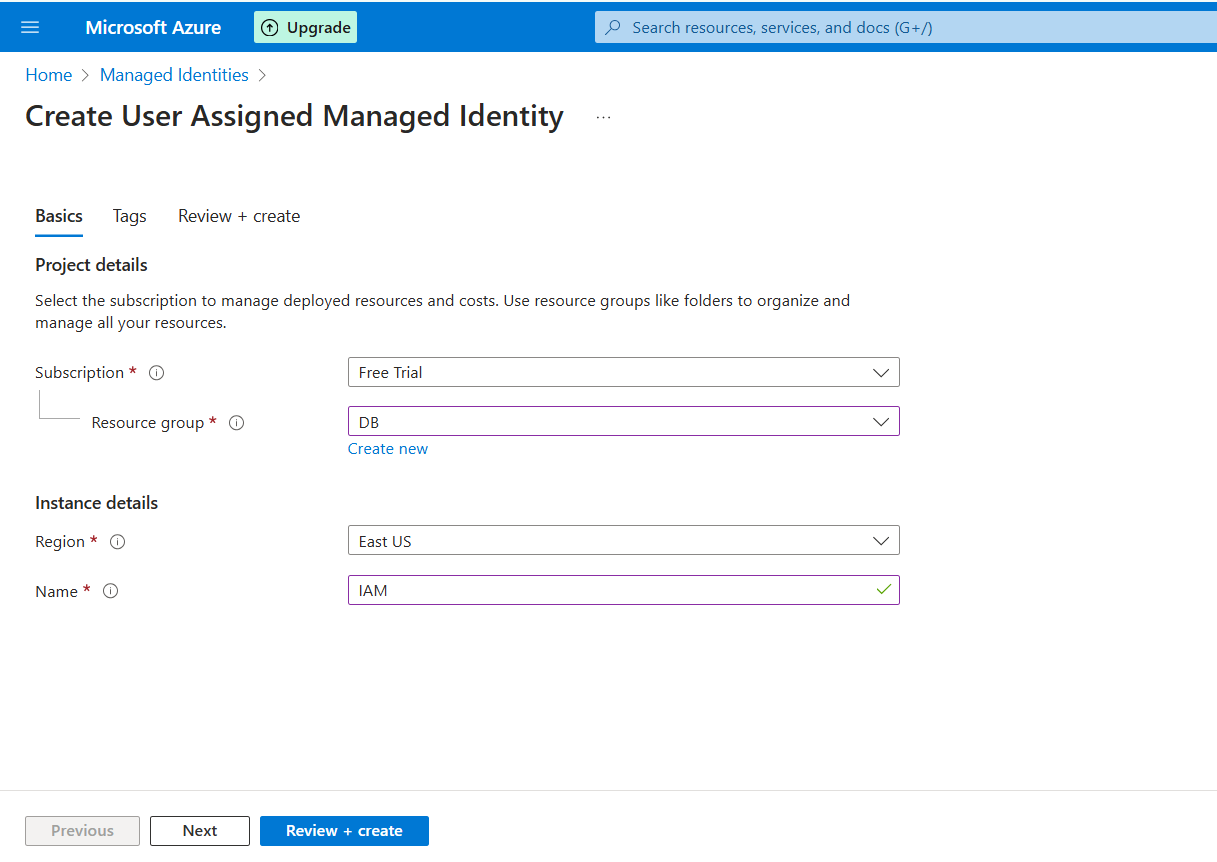
**Step 2:**

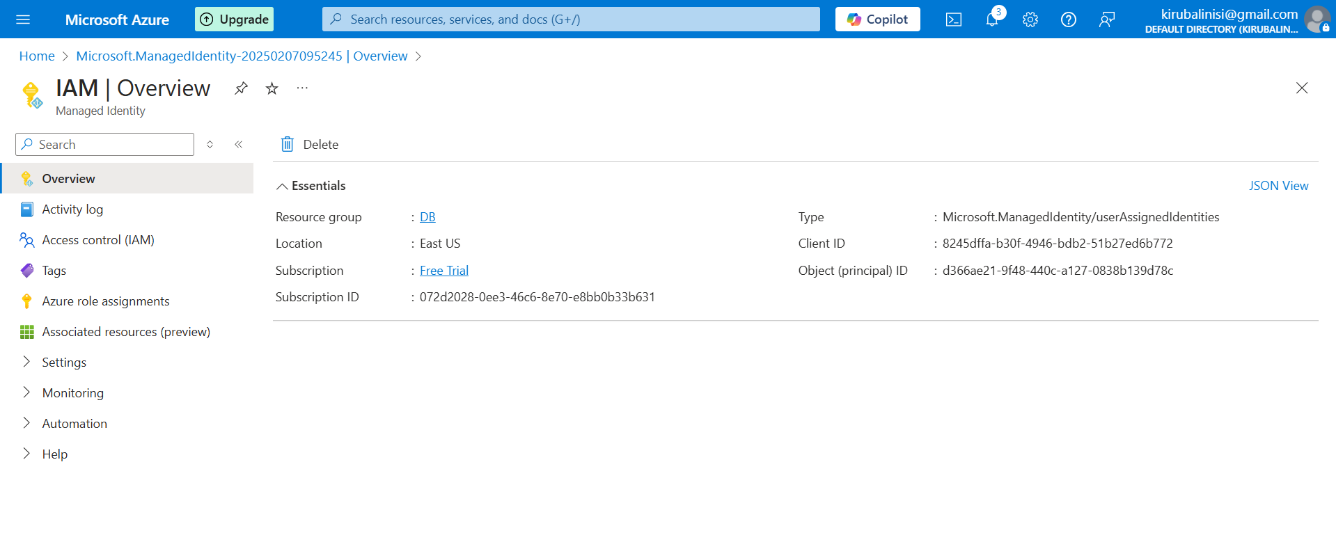
Create a User-Assigned Managed Identity, search Managed Identity in Search bar.



**Step 3**:

Select Managed Identities and Click on "REVIEW + CREATE”, Once you have filled the required details and click on "CREATE" to create the Managed Identities.

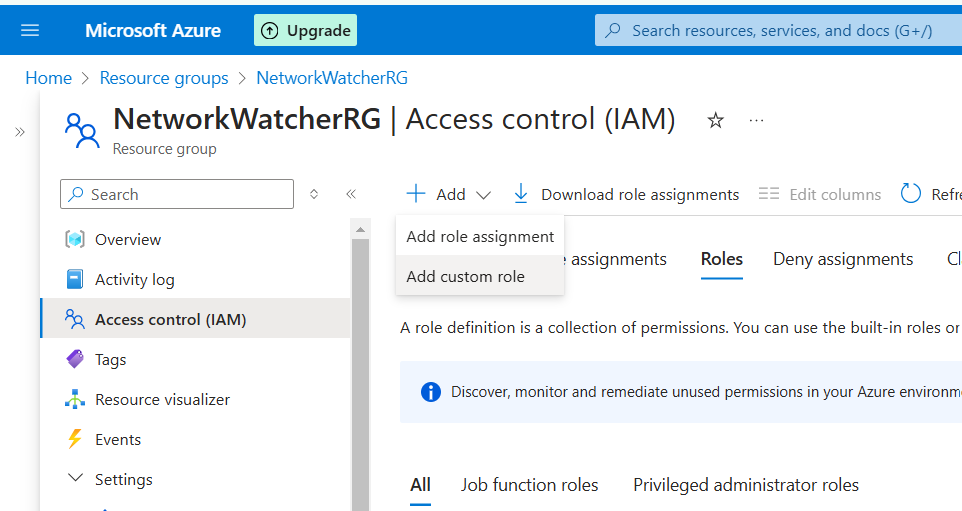




**Step 4:**

Create a Custom Role.

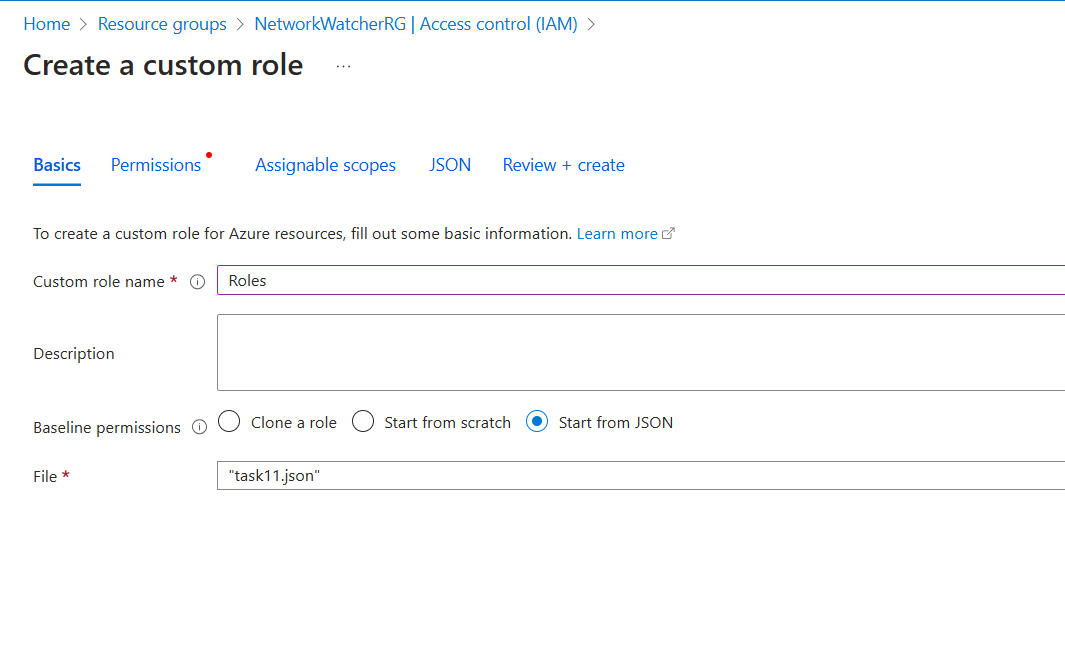
* Navigate to Resource group and select "Access Control (IAM)" and then "Roles".
* And Click "ADD" and select custom role.



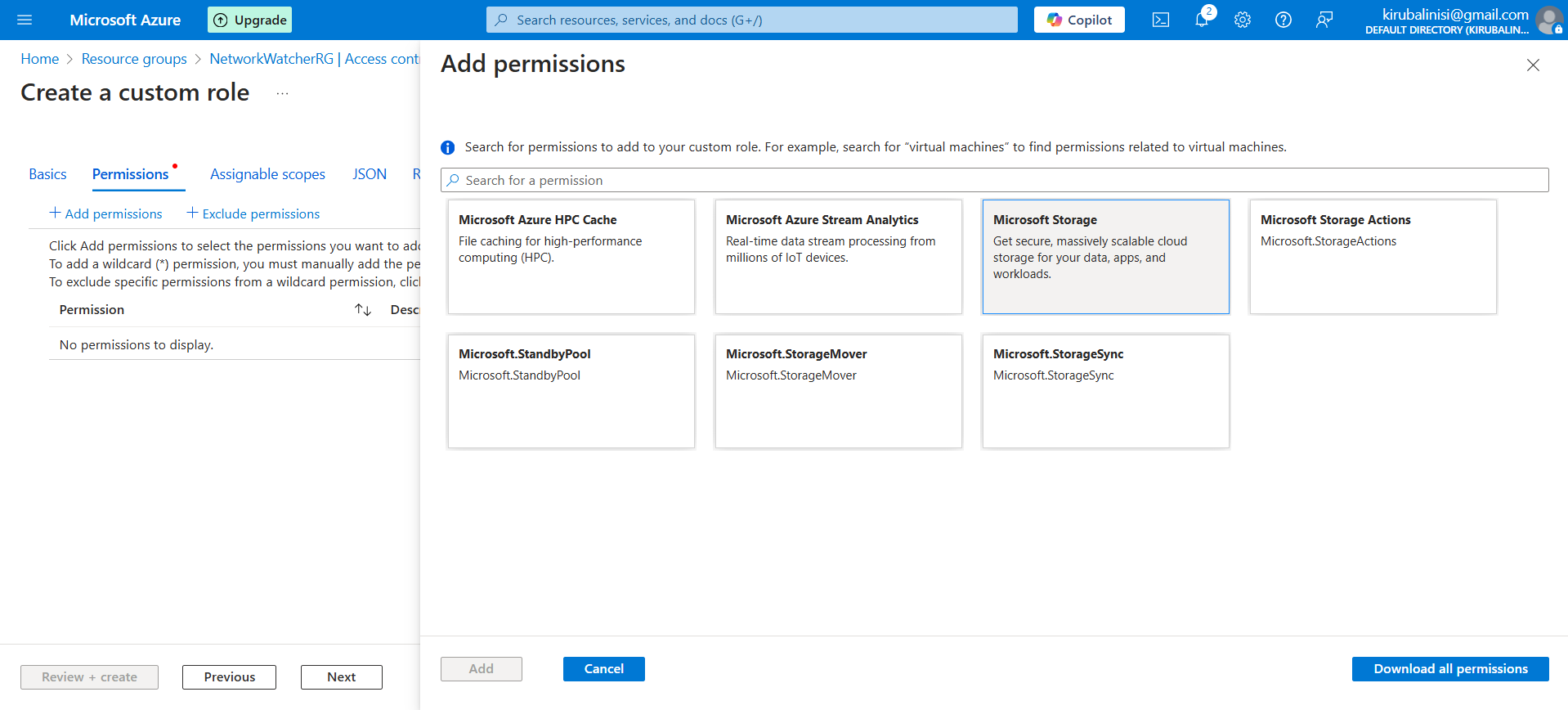
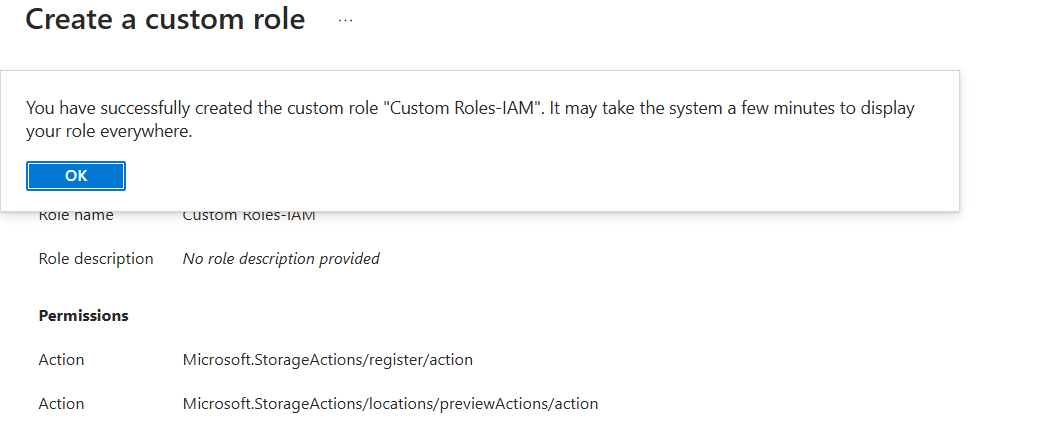
**Step 5:**

Fill in the details required to create custom role

* Create a JSON file with a code



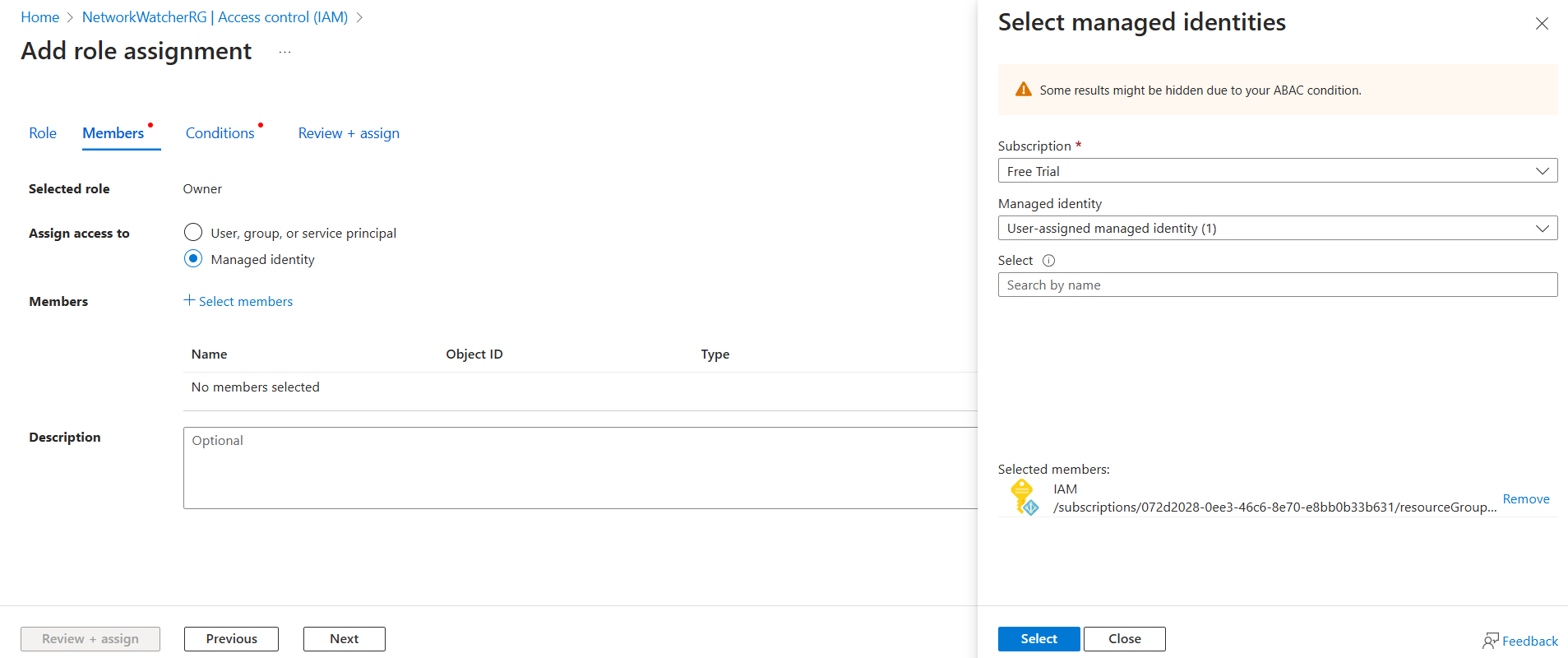
* In permissions select Action that is related to your code And then click "REVIEW + CREATE” which take a few minutes to be created

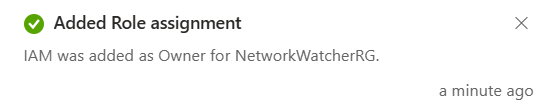


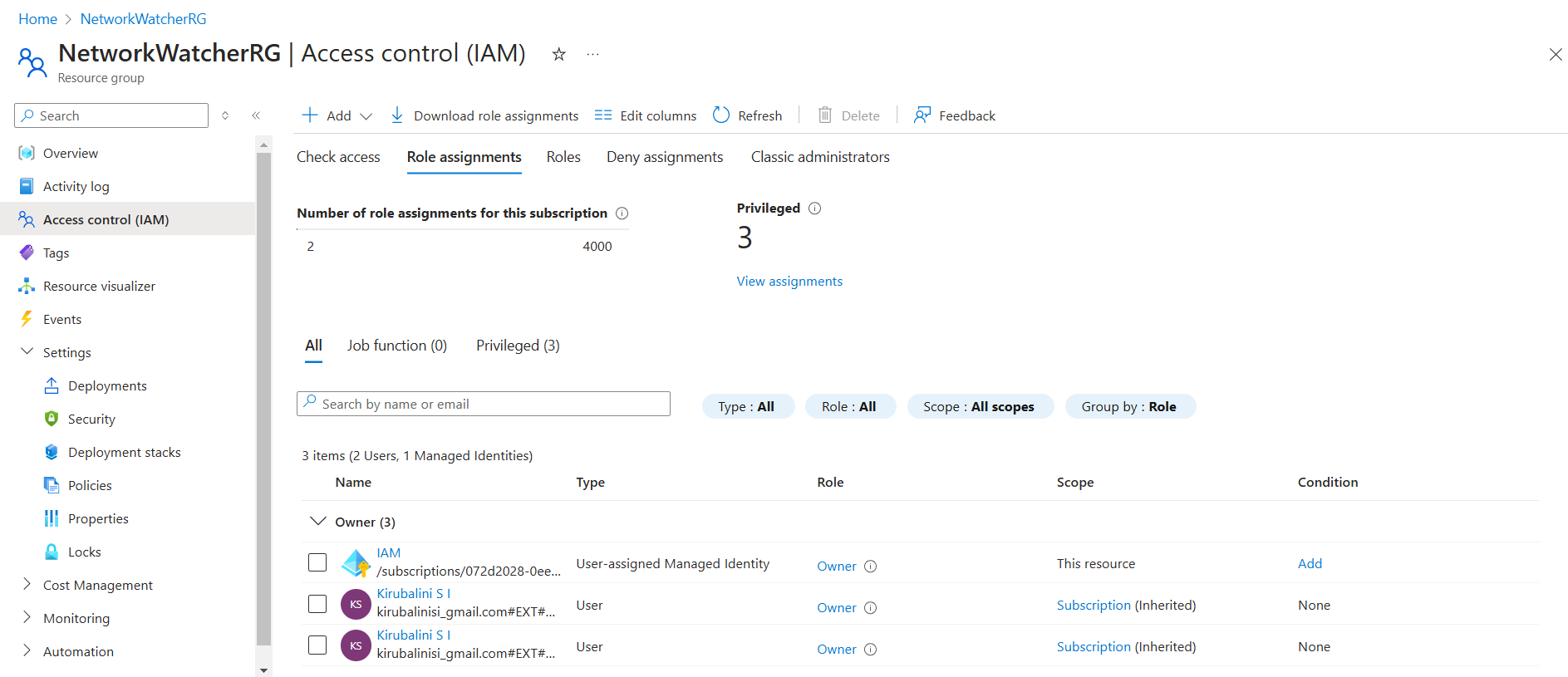
**Step 6:**

Assign the Role to the Managed Identity

* Select "Access Control (IAM)", Click "Add role assignment"
* Select "Managed identity", Click "Select members" Choose the user-assigned managed identity you created

****

****

****

**Expected Outcome**

By successfully implementing IAM roles and permissions for VMs in Azure, you can expect the following outcomes:

**Secure VMs:** VMs operate with the minimum necessary permissions, reducing the attack surface.

**Controlled Access:** Only authorized users and services can access and manage VMs and related resources.

**Simplified Administration:** Managing permissions is centralized and streamlined.

**Improved Auditability:** Access logs provide a clear trail of who accessed what and when.

**Automated Governance:** Permissions can be managed programmatically, enabling consistent and scalable security policies.

**Reduced Security Risks:** The overall security posture of your Azure environment is significantly improved.