**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: **SHIYAM MARTEIN A S** DEPARTMENT: **IT**



**Introduction**

IAM (Identity and Access Management) roles and permissions are essential for managing access control within a cloud environment. By configuring IAM roles, you can define what actions a Virtual Machine (VM) can perform and which resources it can access. This ensures security, prevents unauthorized access, and follows the principle of least privilege.

**Overview**

IAM roles are used to grant specific permissions to AWS, GCP, or Azure resources without using long-term credentials. Instead of assigning direct user permissions, IAM roles allow instances, applications, or services to assume predefined access levels dynamically.

**Objective**

**The primary objectives of this POC are:**

* Create an IAM role with necessary permissions.
* Attach the role to a VM instance.
* Define policies to allow/restrict access to specific services.
* Improve security by following best IAM practices.

**Importance**

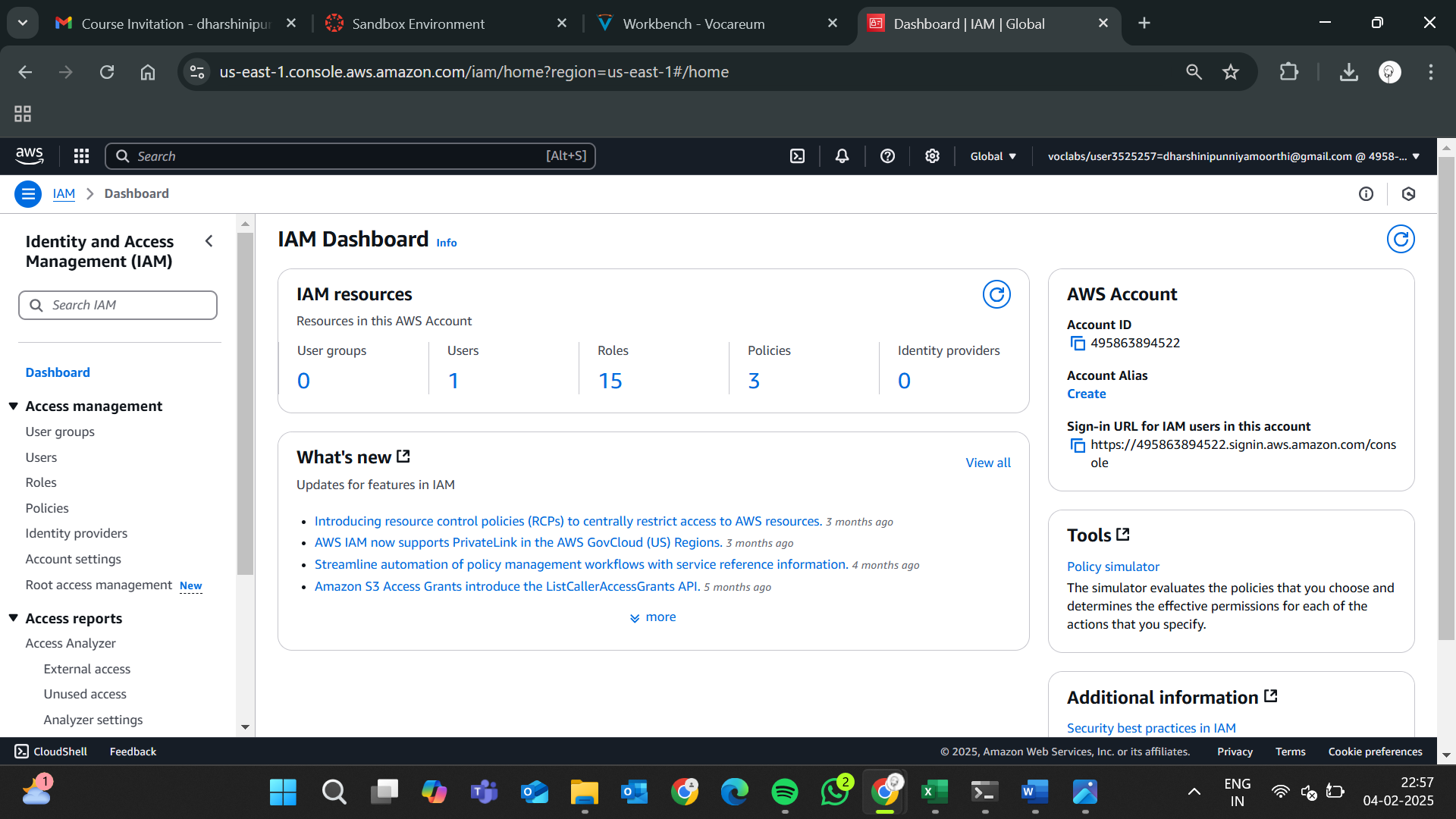
* **Enhanced Security**: Eliminates the need for storing sensitive credentials within the VM.
* **Access Control**: Ensures that the VM operates only within the permitted scope.
* **Audit and Monitoring**: Facilitates tracking of access and activities via cloud logs.
* **Scalability**: Allows dynamic role-based access without modifying user-level permissions.

**Step-by-Step Overview**

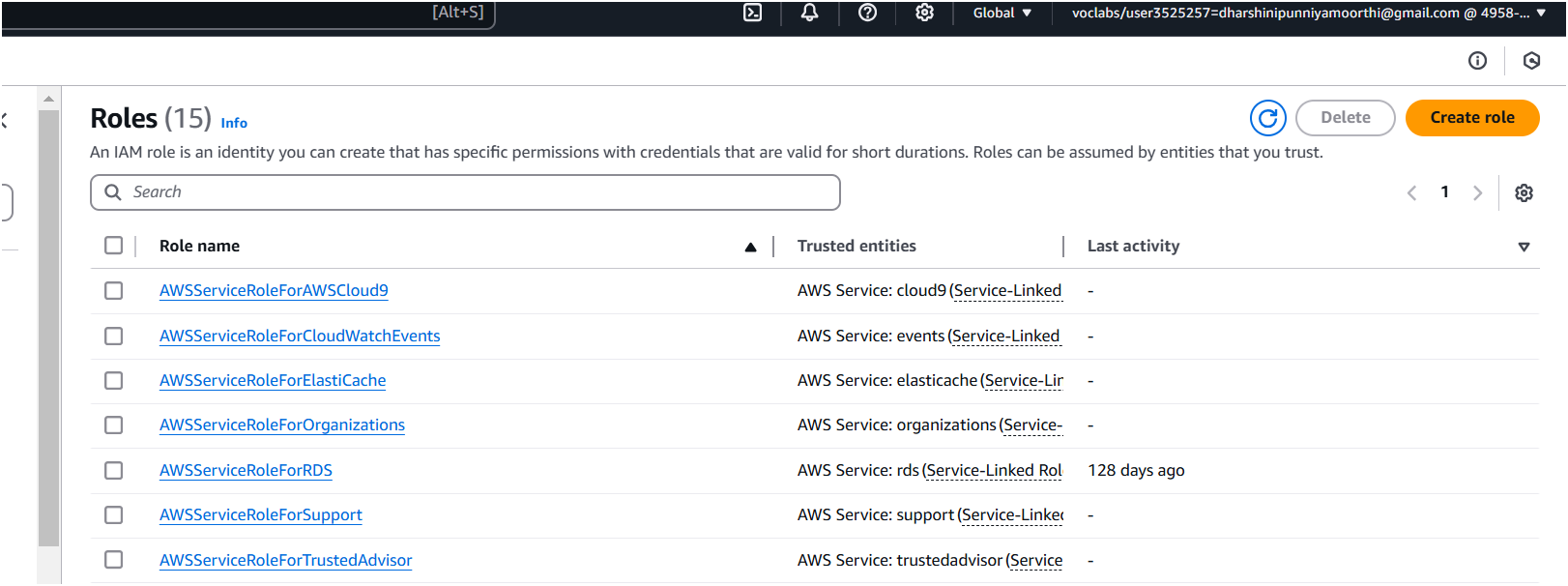
**Step 1:**

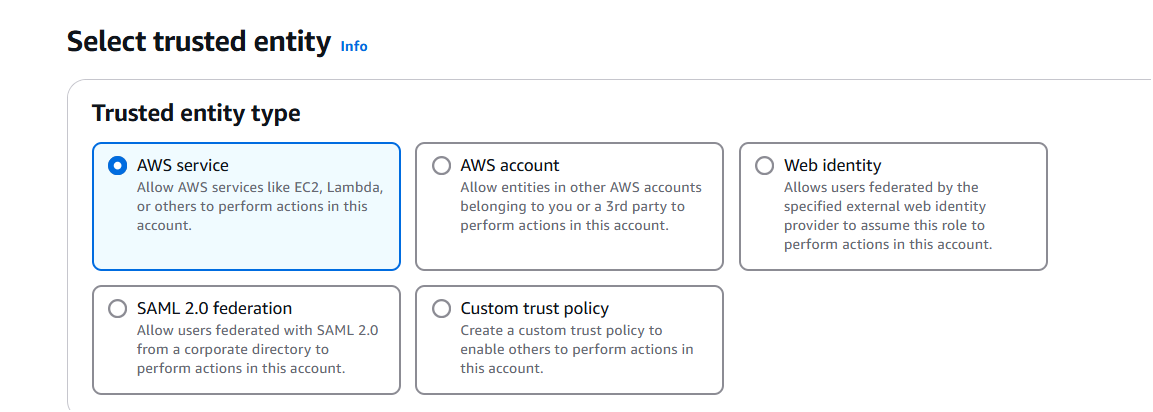
**Create an IAM Role:**

* Navigate to the **IAM Console** → **Roles**.

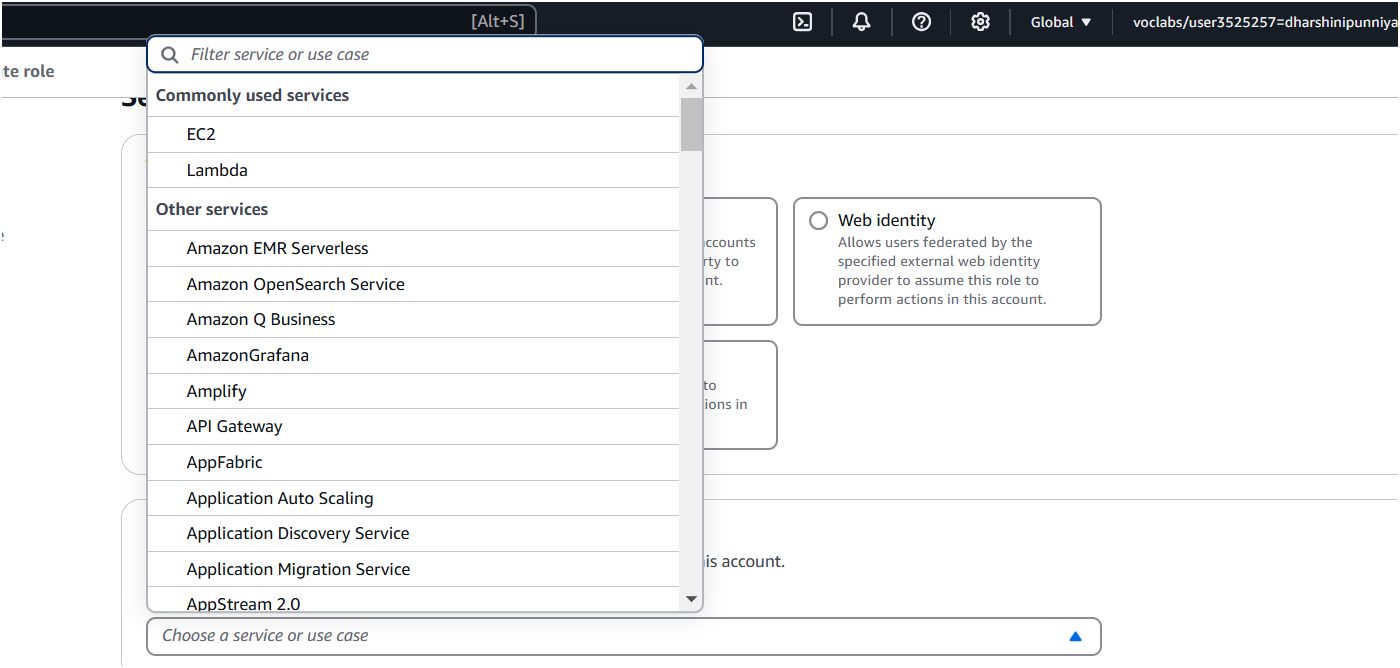


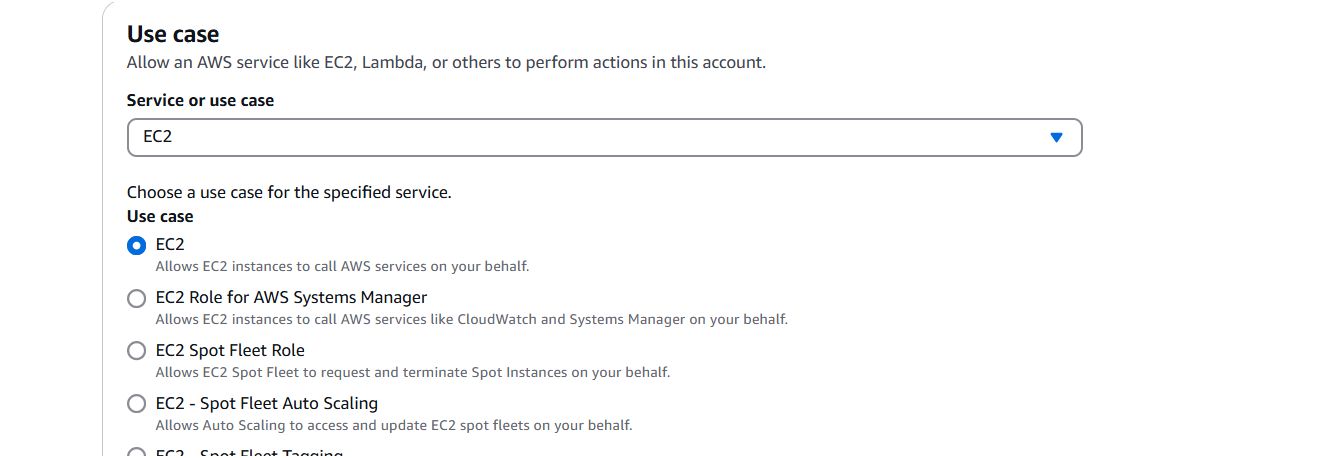
* Click **Create role** and select **AWS service** as a trusted entity.



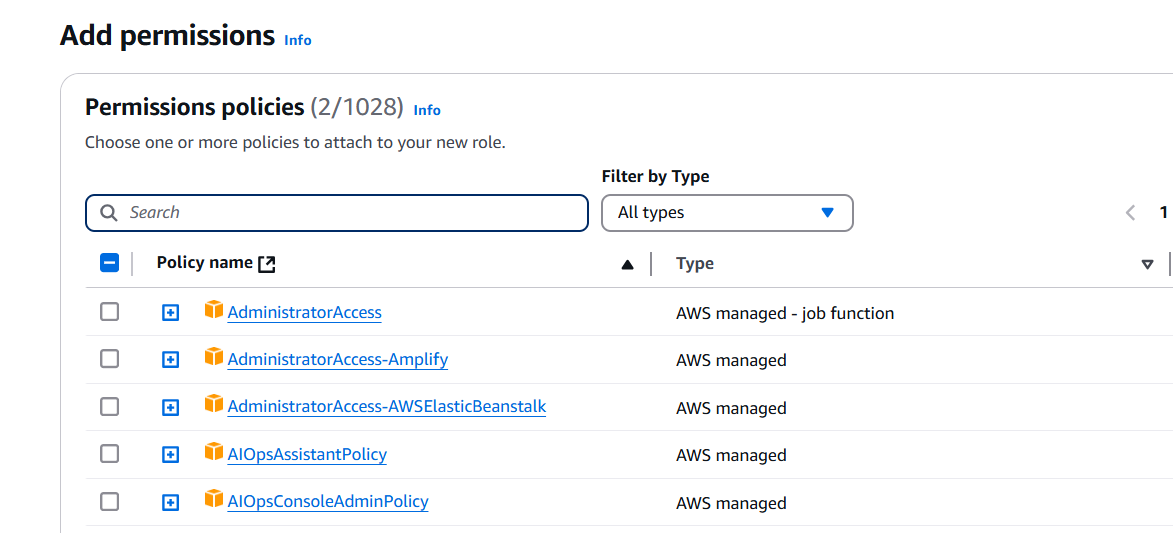


* Choose **EC2** as the use case.

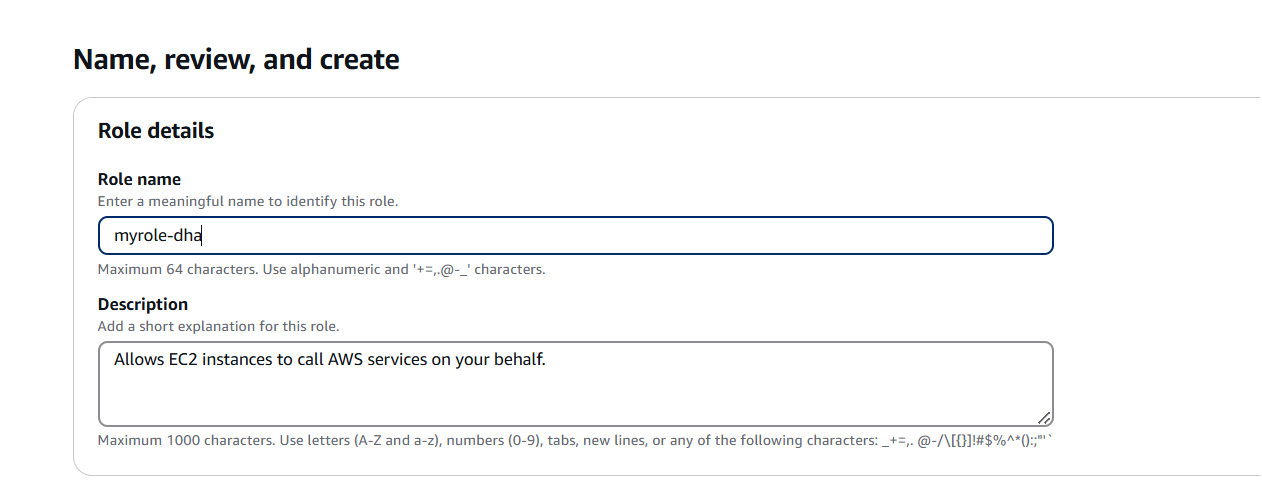




* Attach policies (e.g., AmazonS3ReadOnlyAccess for read-only S3 access).



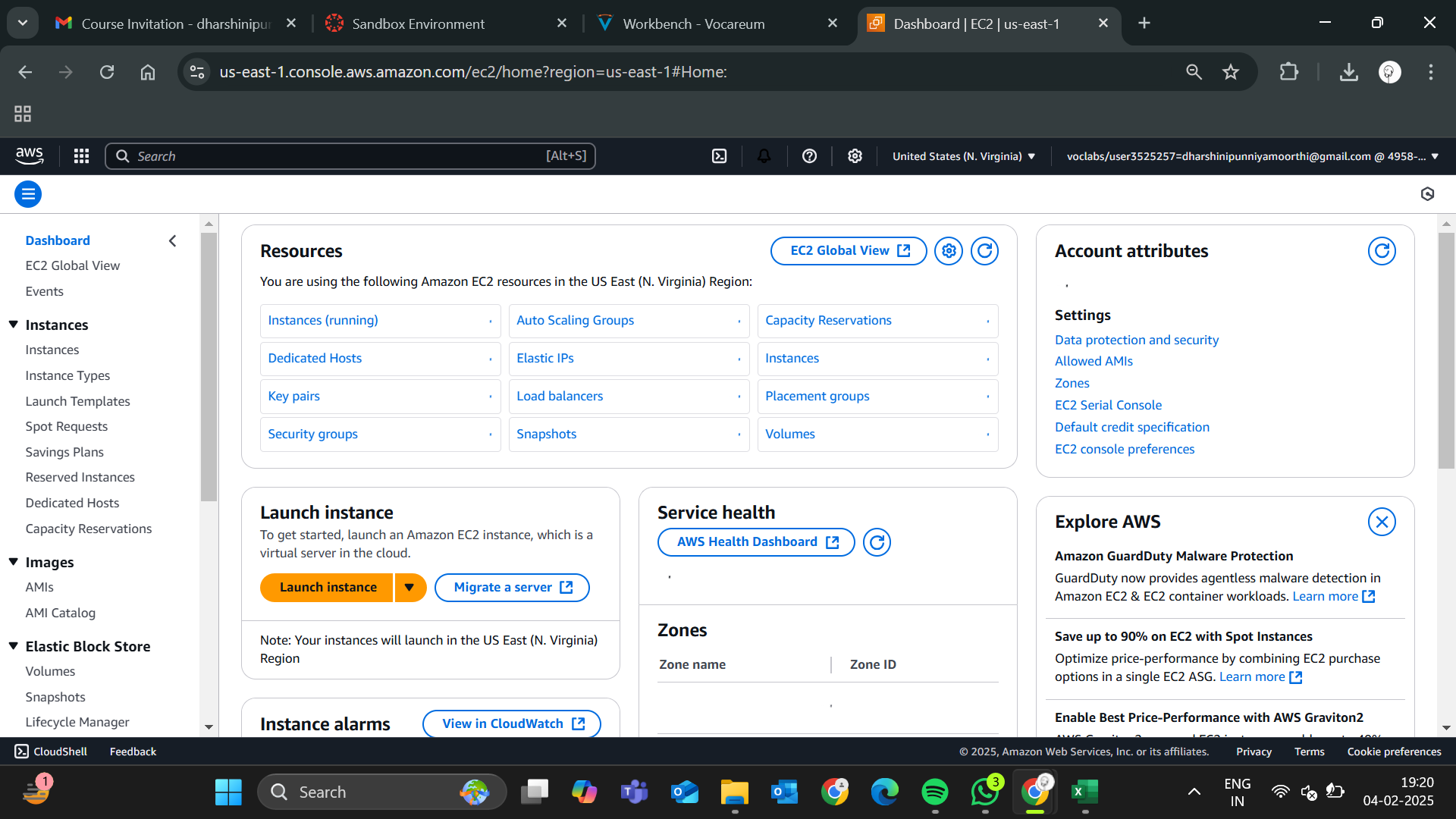
* Name the role and create it.



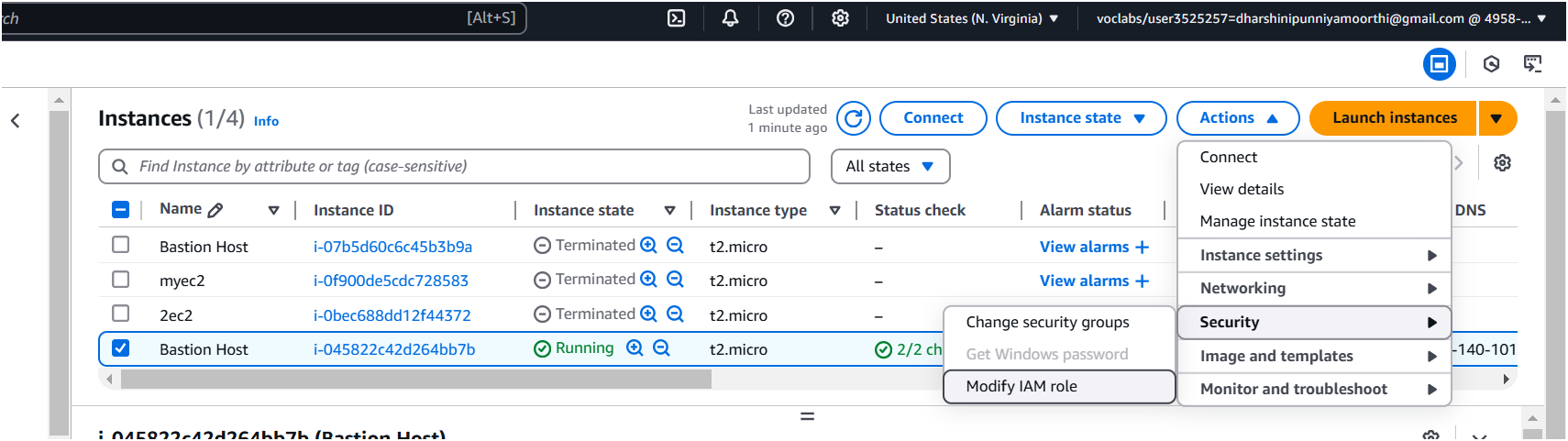
**Step 2:**

**Attach the Role to an EC2 Instance:**

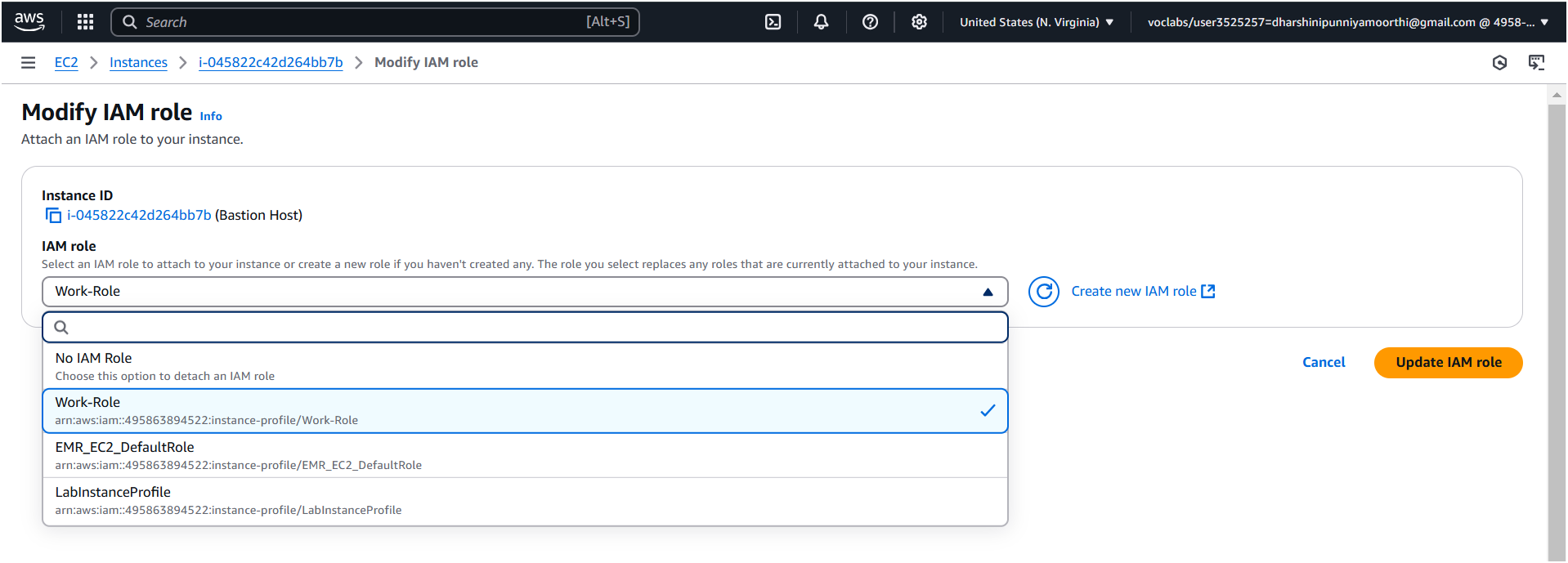
* Go to **EC2 Console** → Select your instance.

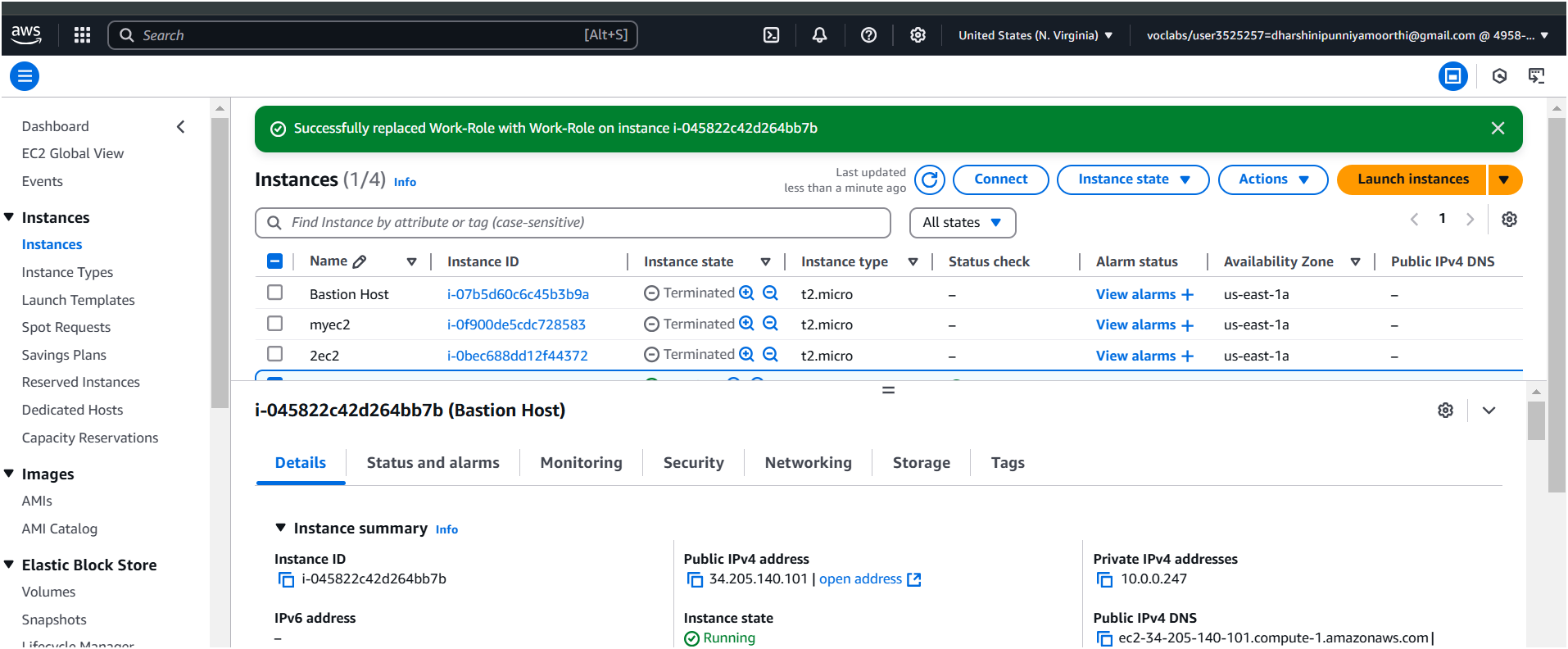


* Click **Actions** → **Security** → **Modify IAM Role**.



* Select the newly created IAM role and attach it.





**Expected Outcome:**

By the end of this process, you will have:

* The IAM role is successfully created and assigned to the VM.
* The VM is granted only the specified permissions without using credentials.
* The configured access restrictions work as expected, improving security.
* The role-based access can be monitored and modified as needed.

By following these steps, you ensure secure and efficient access control for your cloud-based virtual machines.