**Placement Empowerment Program**

***Cloud Computing and DevOps Centre***

**DAY 10 TASK:**

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:SHAHANA.M.S Department: ADS



**Introduction**

Identity and Access Management (IAM) is a critical security feature in cloud computing that helps manage user and service permissions. By setting up IAM roles, you can grant specific permissions to resources while ensuring security and compliance. Assigning an IAM role to a Virtual Machine (VM) allows it to interact securely with cloud services without using hardcoded credentials.

**Objective**

* To create an IAM role on a cloud platform (AWS, Azure, or GCP).
* To assign the IAM role to a Virtual Machine (VM).
* To define specific permissions for allowing or restricting actions.
* To ensure secure and controlled access to cloud resources.

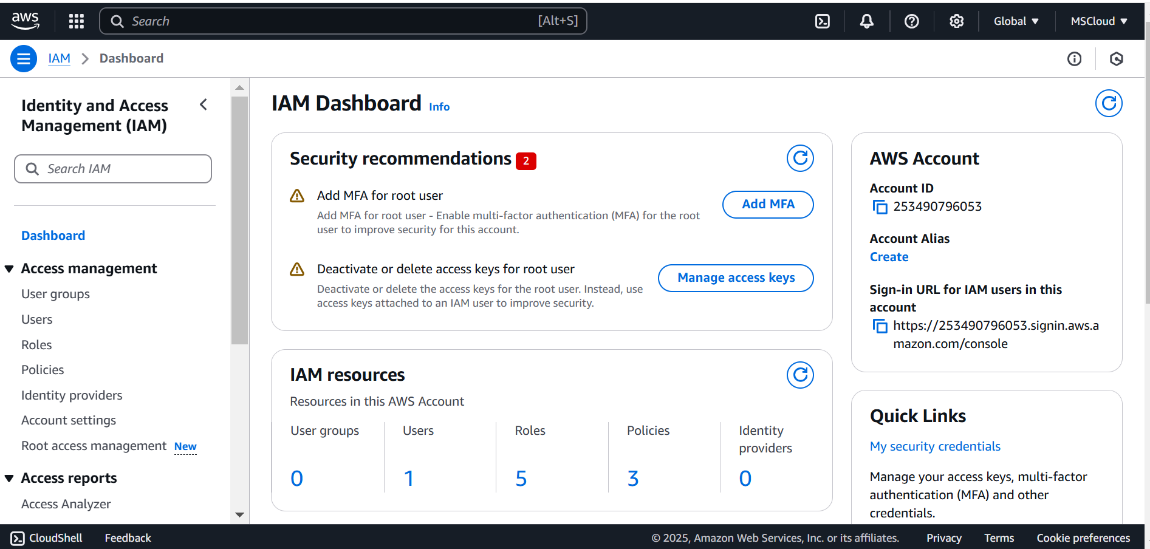
**Importance**

* **Security Best Practices**: Reduces the risk of unauthorized access and credential leaks.
* **Granular Access Control**: Assigns precise permissions to resources based on roles.
* **Automation & Efficiency**: Enables VMs to access cloud services without manual credential management.
* **Compliance & Governance**: Helps organizations meet security and regulatory requirements.

**STEP-BY-STEP OVERVIEW:**

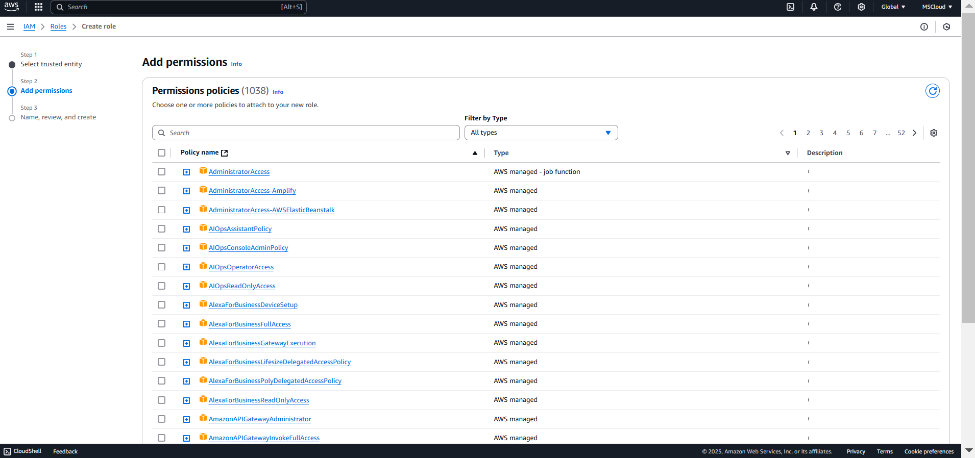
Step 1: Go to AWS Management Console.

Step 2: Search IAM in the search bar and then on the left select roles , then create roles accordingly as the image below:

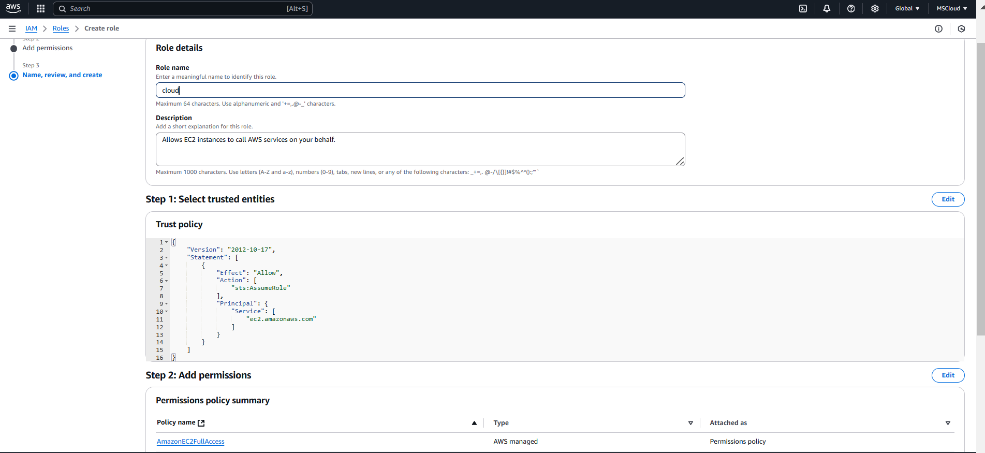


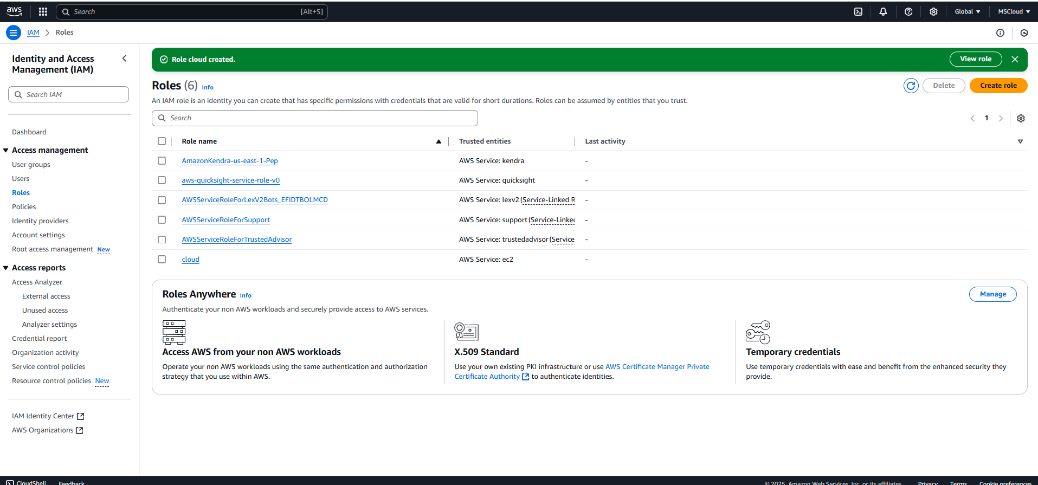
.

Step 3: On the Permissions page, you can check on the following services and click one you match with and then click next.(I have selected related to EC2.)

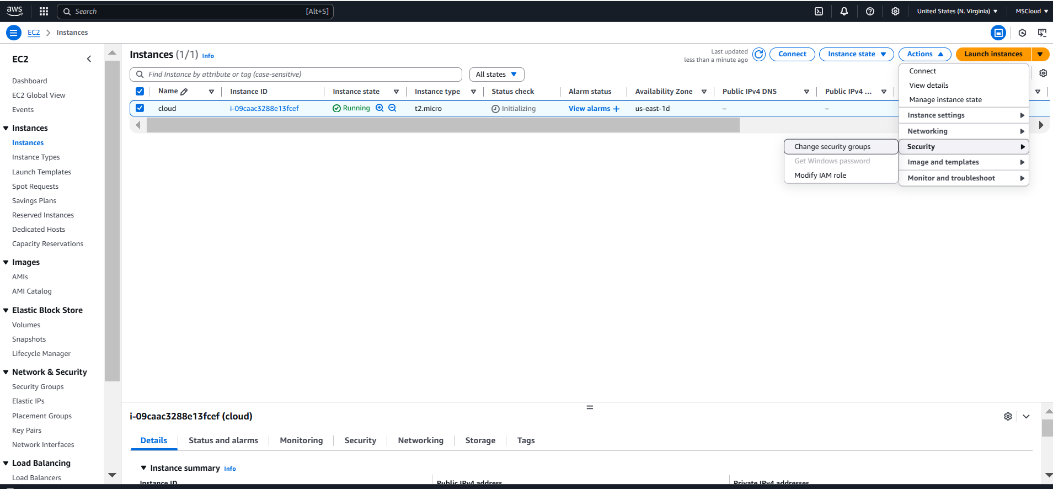


Step 4: Enter your role name under the box of Role name and then click create role in the below.

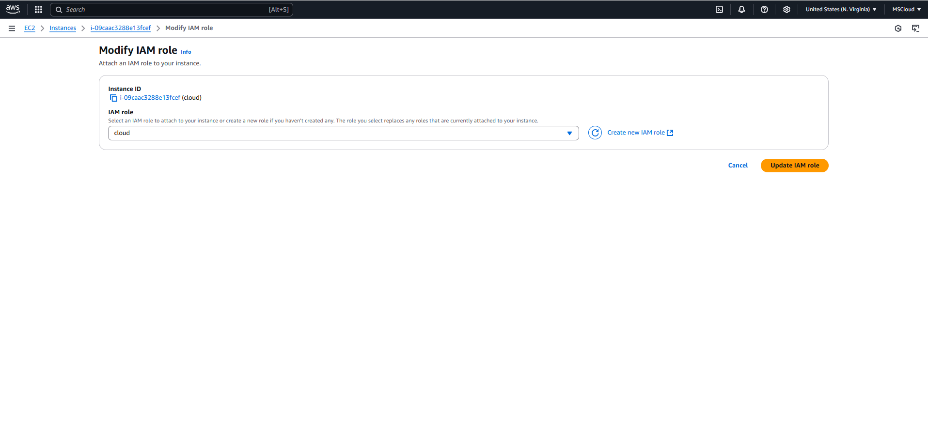


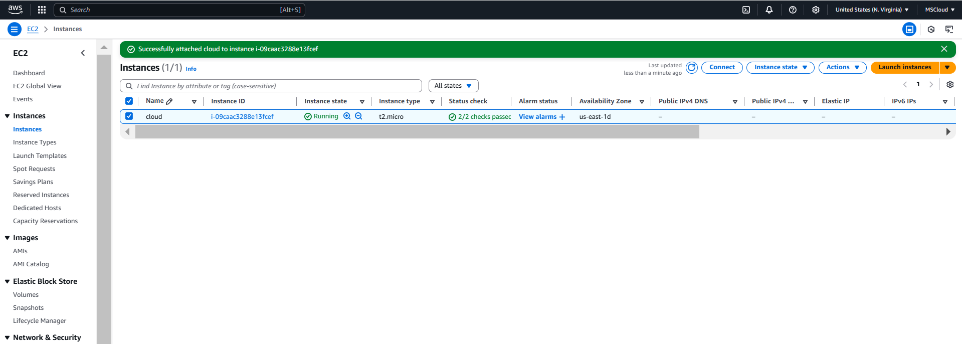


Step 5: Then create an instance and select Actions>security>modify IAM role.

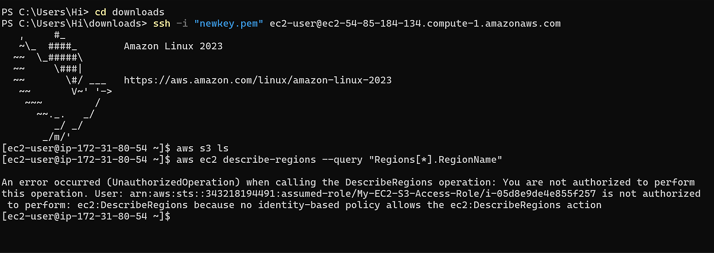


Step 9:In the Modify IAM role window, you should see a dropdown for IAM role. Select the role you created earlier (e.g., My-EC2-S3-Access Role). Click Update IAM role to apply the changes.





Step 10: open command prompt and then go to downloads in order to access .pem (key) you have and you have copy the SSH client code and finally proceed with the following prompts in the image :



**Outcome**

* Successfully creating and assigning an IAM role to a VM.
* Understanding how IAM roles manage permissions securely.
* Enabling a VM to interact with cloud services without hardcoded credentials.
* Strengthening security by following least privilege principles.