

**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: Kirthika S Department: CSE**

A black and white logo

Description automatically generated

**Introduction:**

Identity and Access Management (IAM) is a crucial security feature in cloud platforms that helps manage access to resources. IAM roles are used to grant specific permissions to users, groups, or services without needing to share long-term credentials. Instead of assigning permissions directly to users, IAM roles provide temporary credentials that define what actions a user or service can perform.

**Objective:**

**Understand IAM roles and policies** and their significance in cloud security.

**Create an IAM role** with the necessary permissions for a cloud service (e.g., storage, databases, APIs).

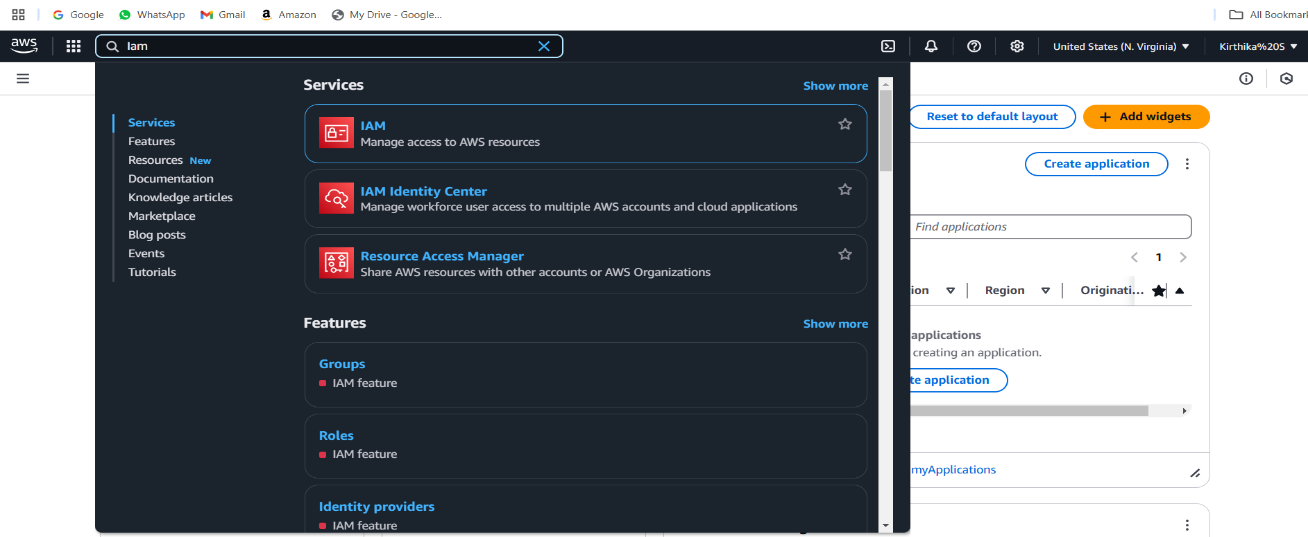
**Attach the IAM role** to a VM instance to enforce access controls.

**Verify and test permissions** to ensure the VM can perform only the intended actions

**Step 1:**

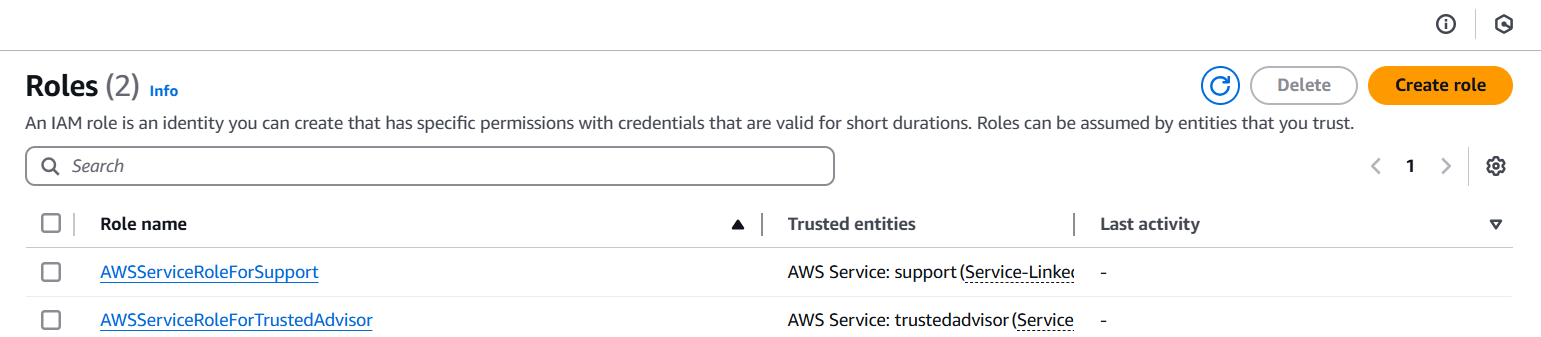
**Access IAM Services**

1. Sign in to your cloud platform’s console (AWS, Azure, or GCP).
2. Navigate to the **IAM (Identity and Access Management)** section



**Step 2:**

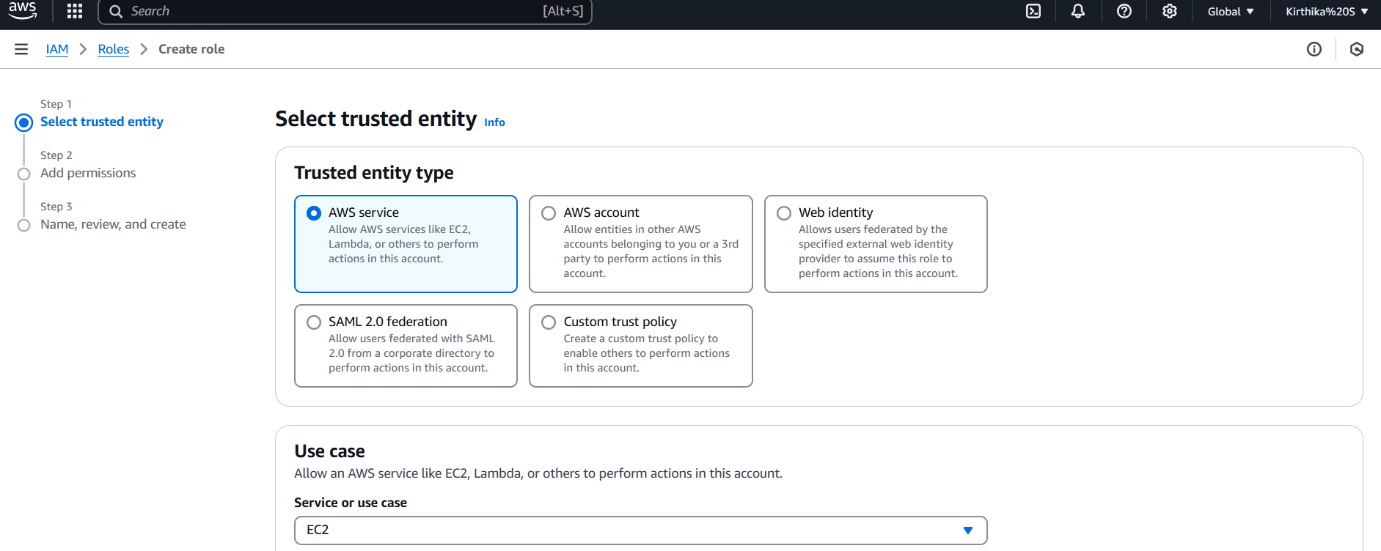
**Create a New IAM Role :** Click on **Create Role** (AWS)

****

**Step 3:**

Its move into next step **select trusted entity,** select AWS service

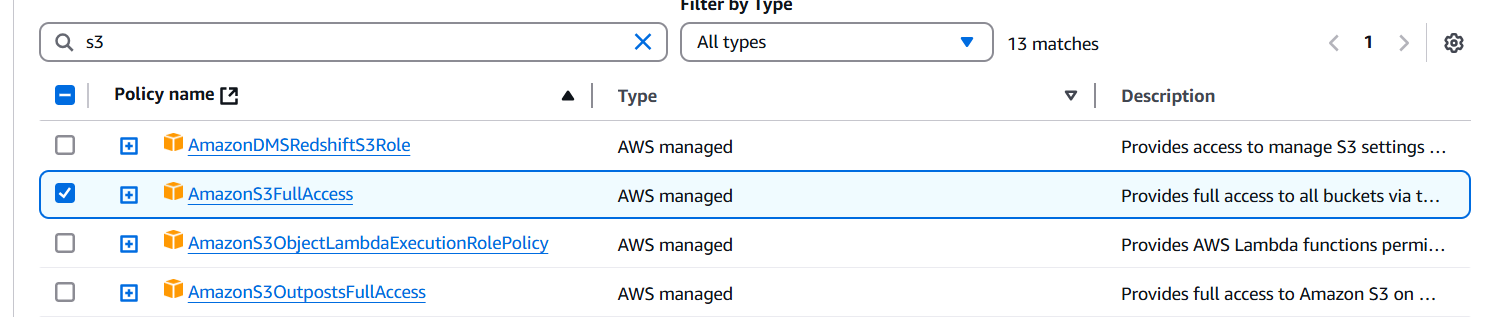
Choose **EC2** in the use case then click **Next,**



**Step 4:**

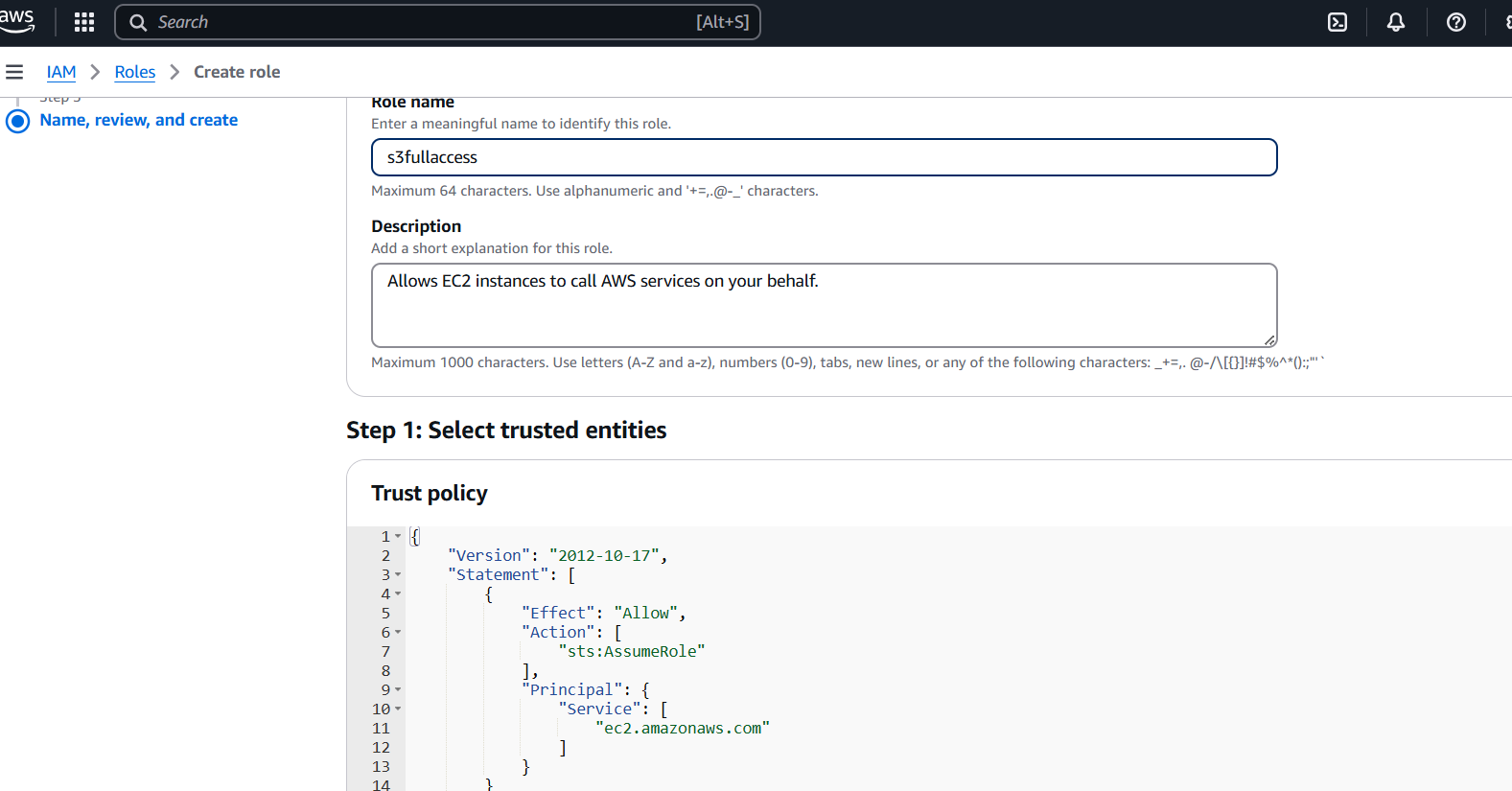
Select or create a policy that defines what the role can do.

Example: If the VM needs access to an **S3 bucket** (Eg: **AmazonS3FullAccess**) attach the appropriate storage permissions.



**Step 5:**

Create Role name,



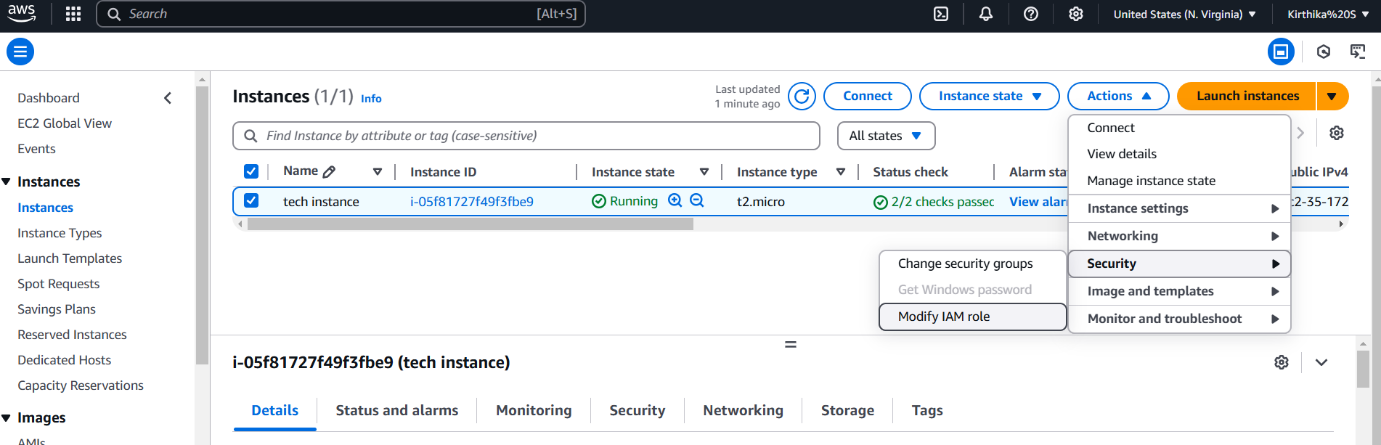
**Step 6:**

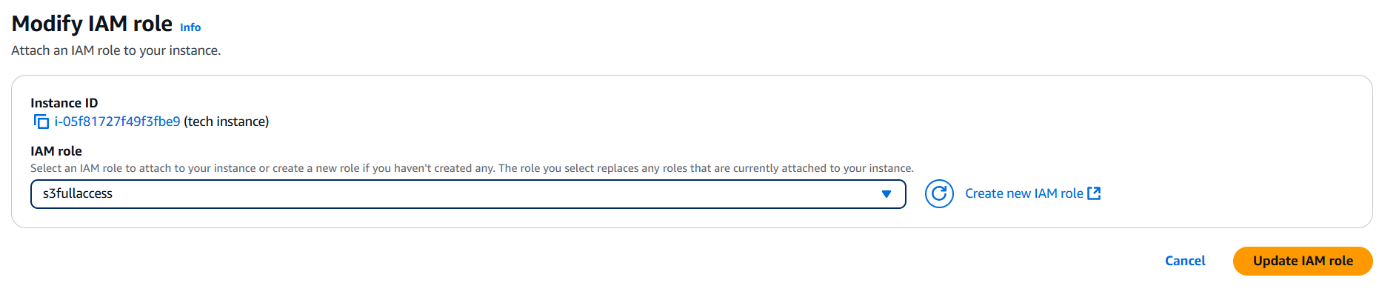
Navigate to your **Compute Engine (GCP)** / **EC2 Instances (AWS)** / **Virtual Machines (Azure)** section.

Select the VM instance where you want to assign the role.

Under "Actions," choose **Modify IAM Role** and select the created role.

Save the changes.

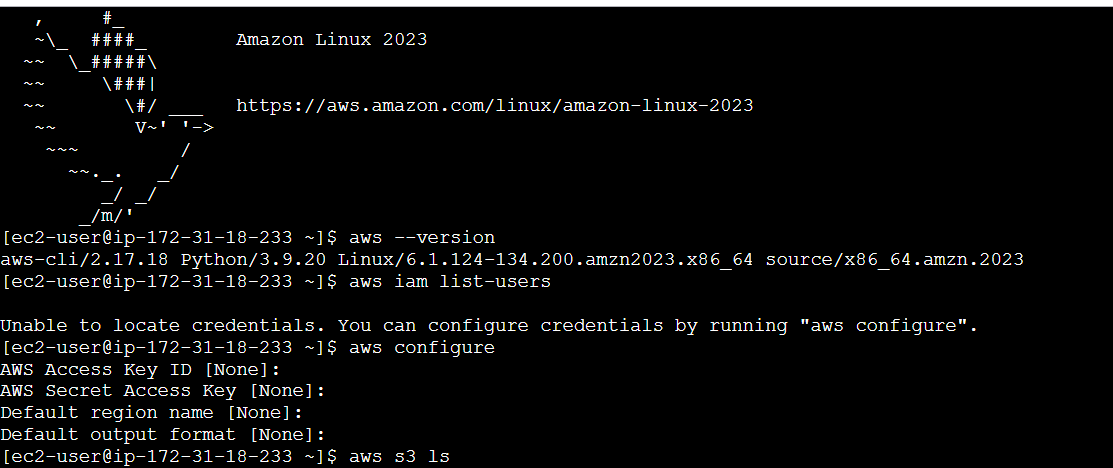




**Step 7:**

Run commands to check access permissions

Use **aws s3 ls** (if storage permissions are assigned).

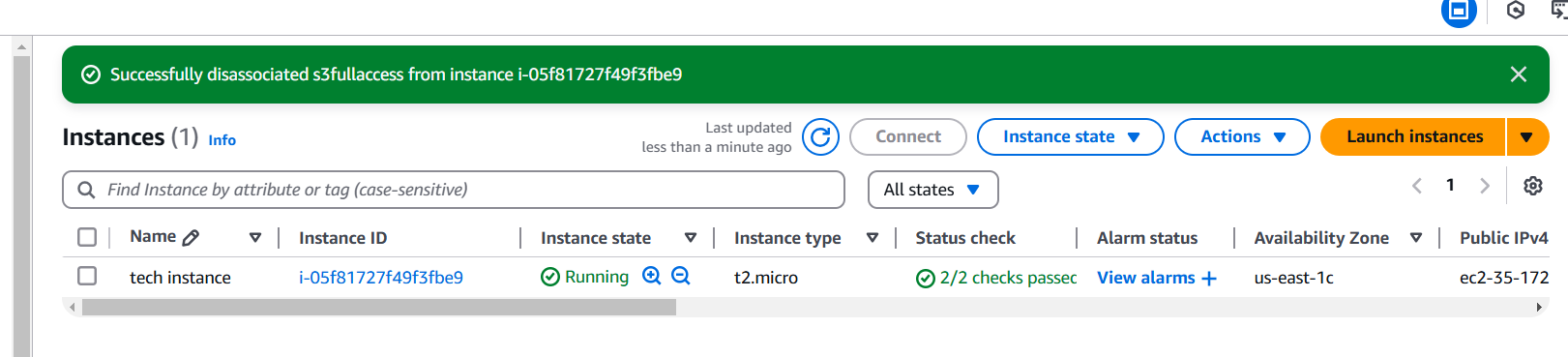


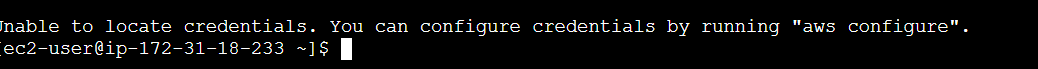
**Step 8:**

Again , under "Actions," choose **Modify IAM Role**.

Save the changes.

If access is denied, review and update IAM policies accordingly.





**Overview:**

Setting up IAM roles and permissions correctly ensures secure access management for your VM instances. Instead of using static credentials, IAM roles provide temporary permissions, enhancing security and reducing risks. By carefully defining permissions, you can prevent unauthorized access while allowing necessary operations.