**Placement Empowerment Program**

**Cloud Computing and DevOps Centre**

**Set Up IAM Roles and Permissions**

**For a Virtual Machine**

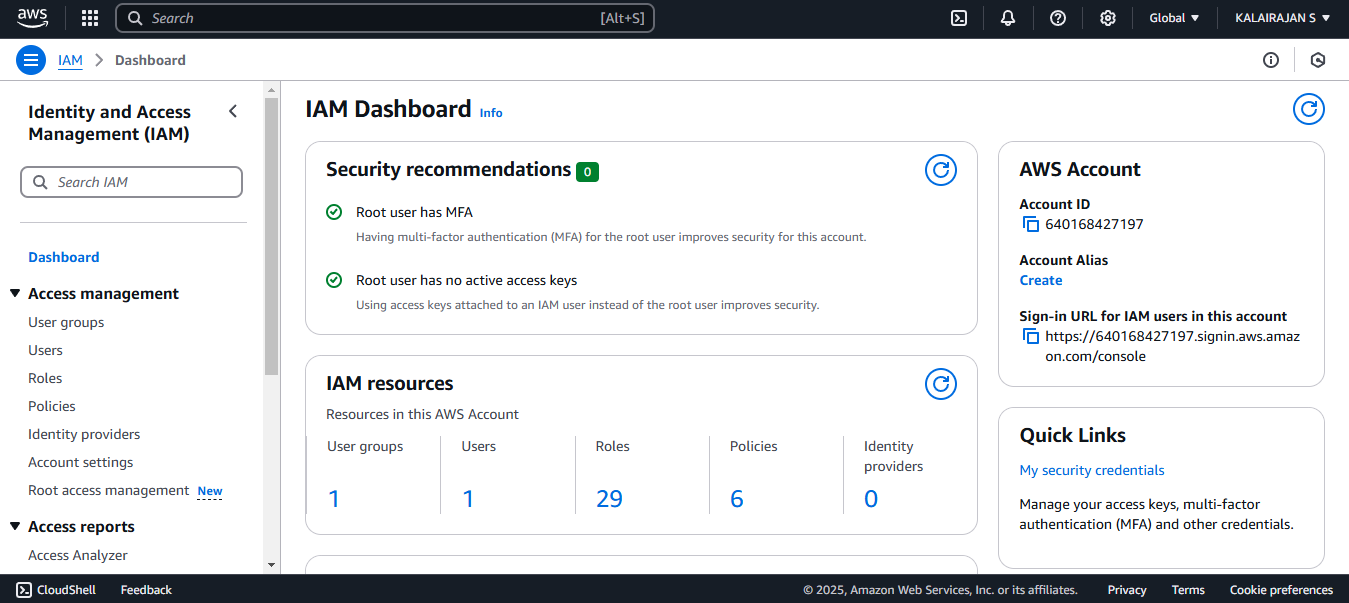
**Name: Kalairajan S Department: IT**



# Introduction

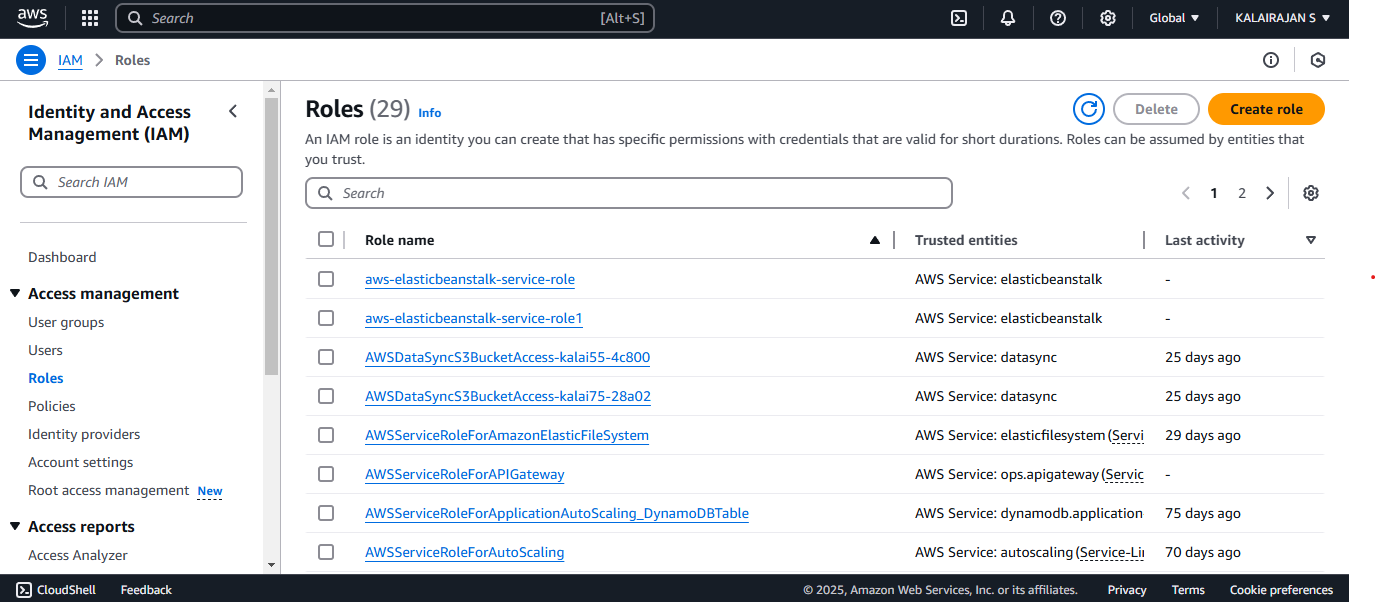
Identity and Access Management (IAM) is a crucial aspect of cloud security that allows administrators to control who can access specific resources and what actions they can perform. By setting up IAM roles and permissions, you ensure that only authorized users or services can interact with your virtual machine (VM). This guide provides step-bystep instructions for creating an IAM role and assigning it to a VM on your cloud platform.

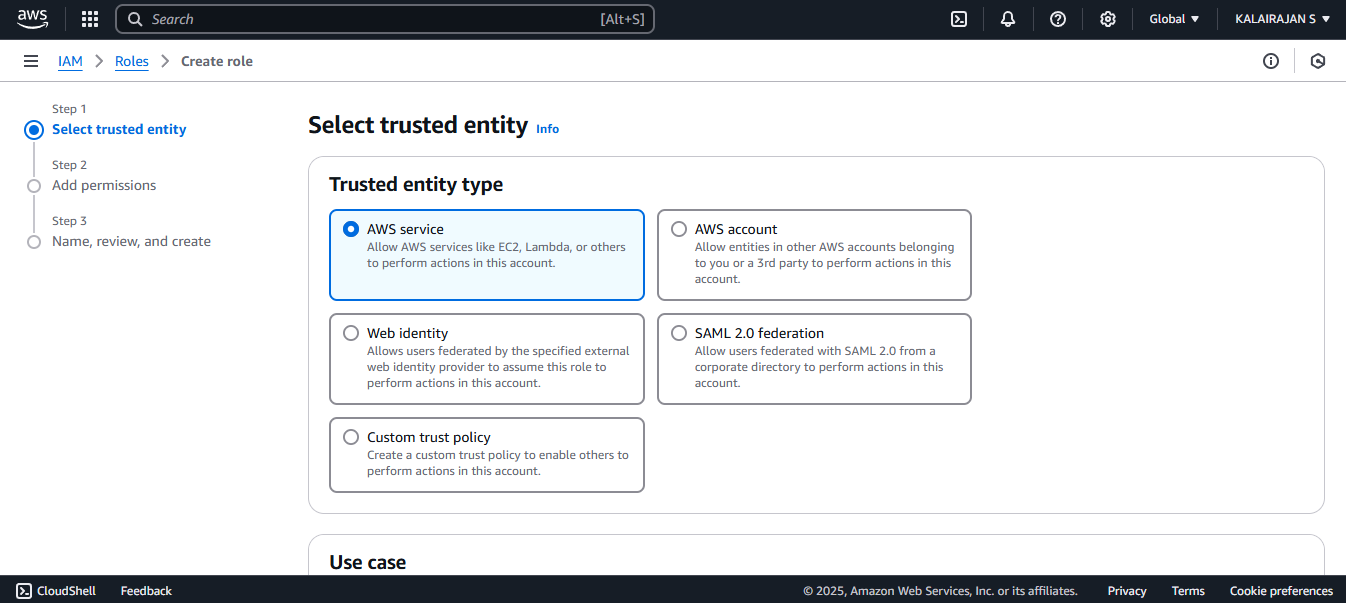
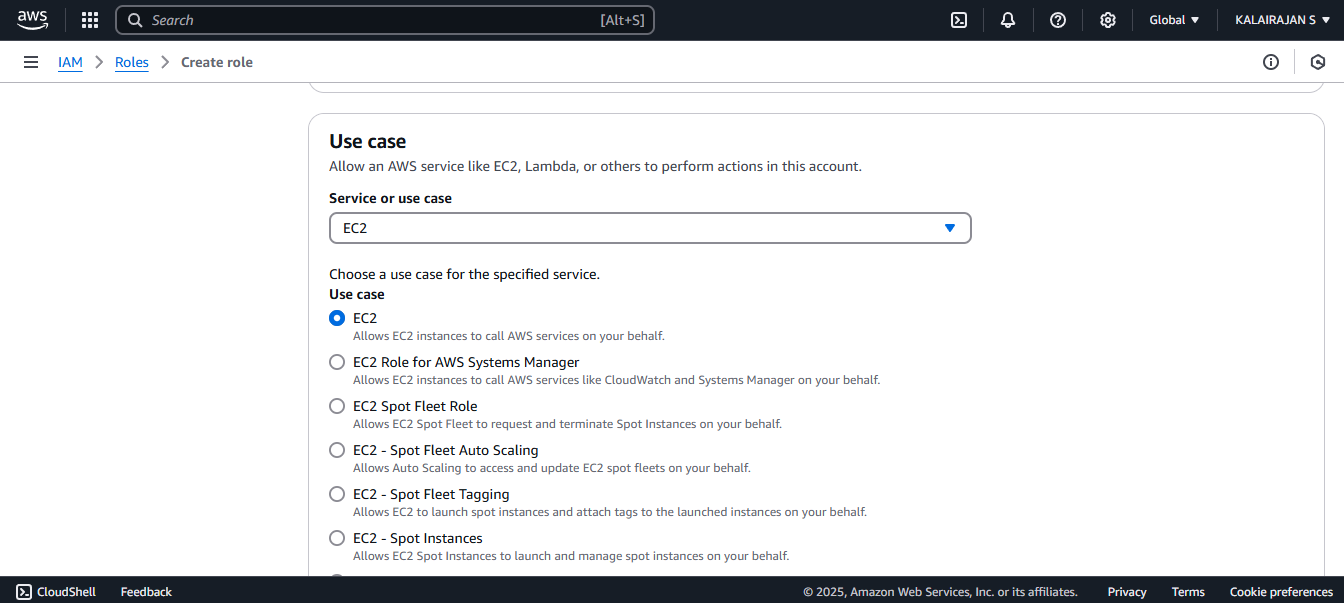
# Create an IAM Role



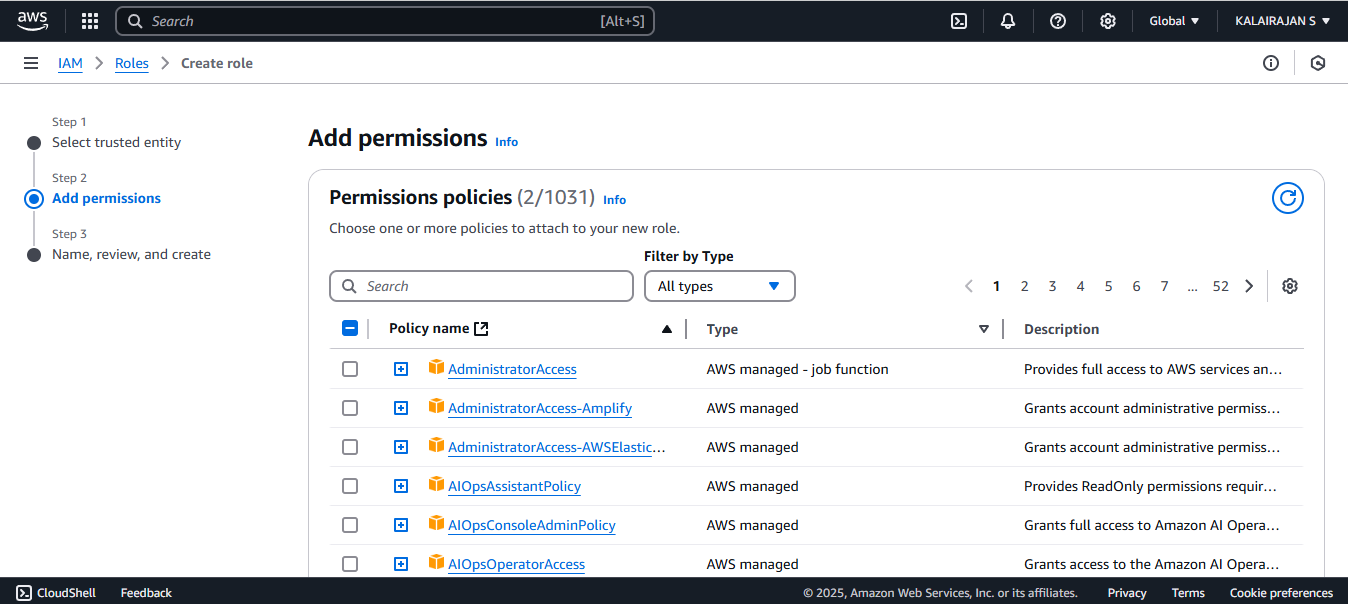
Navigate to the IAM service.

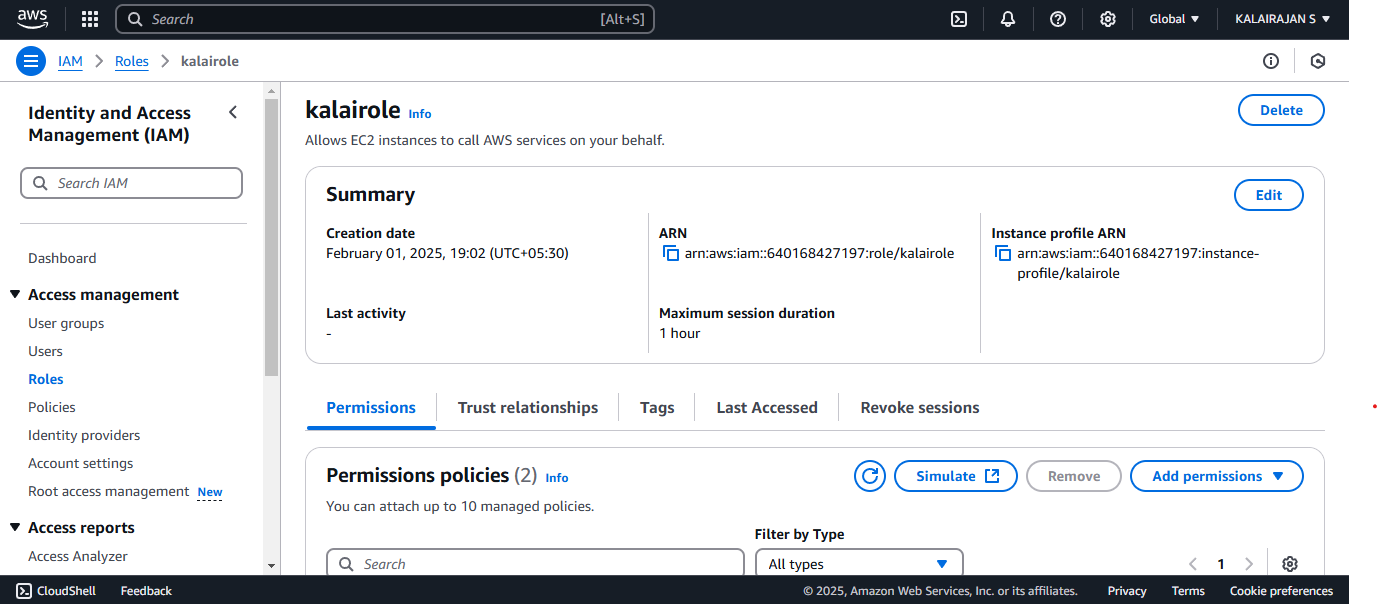
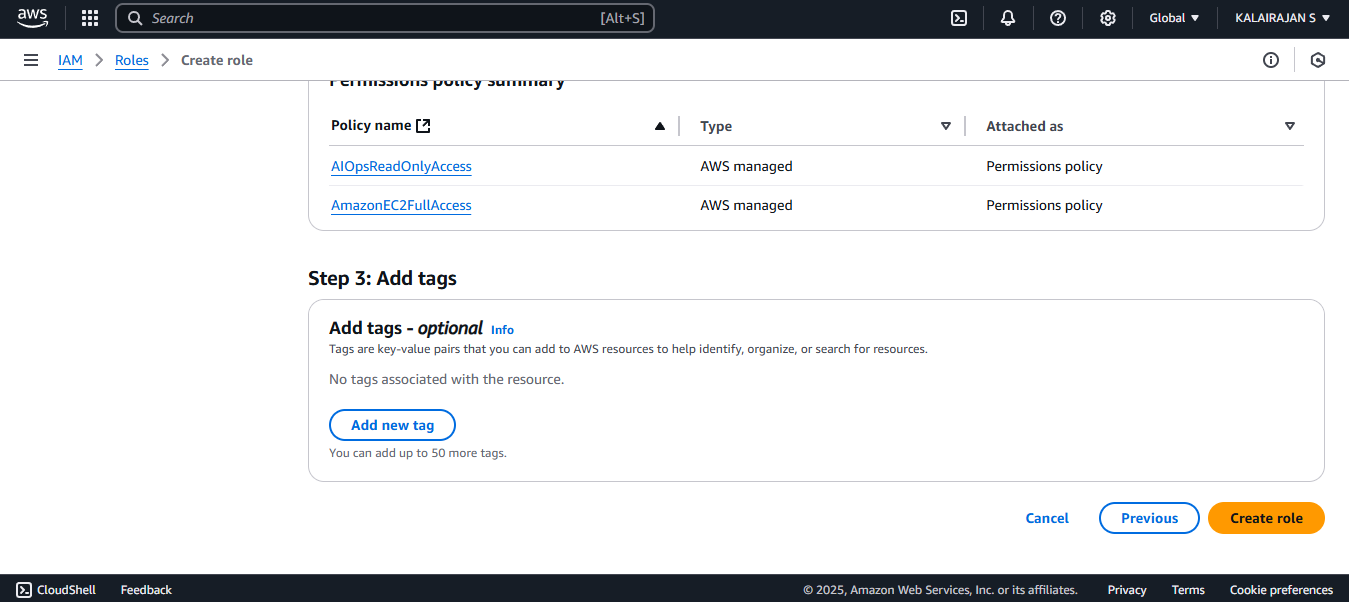
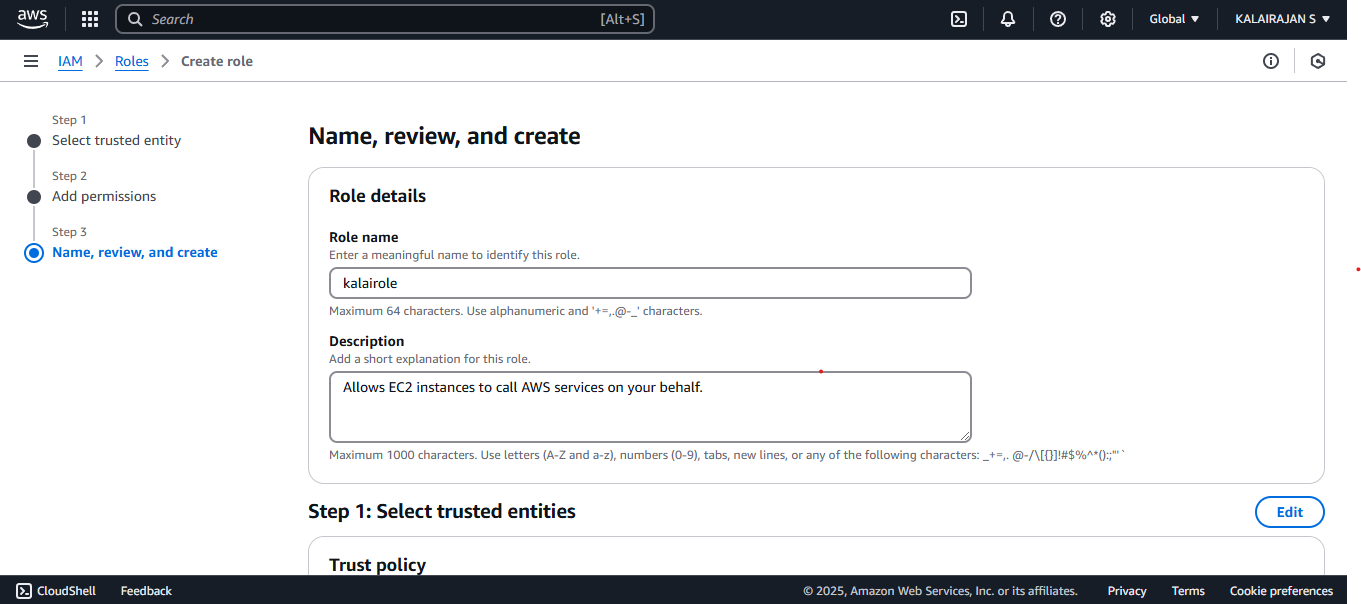
Create a new role:

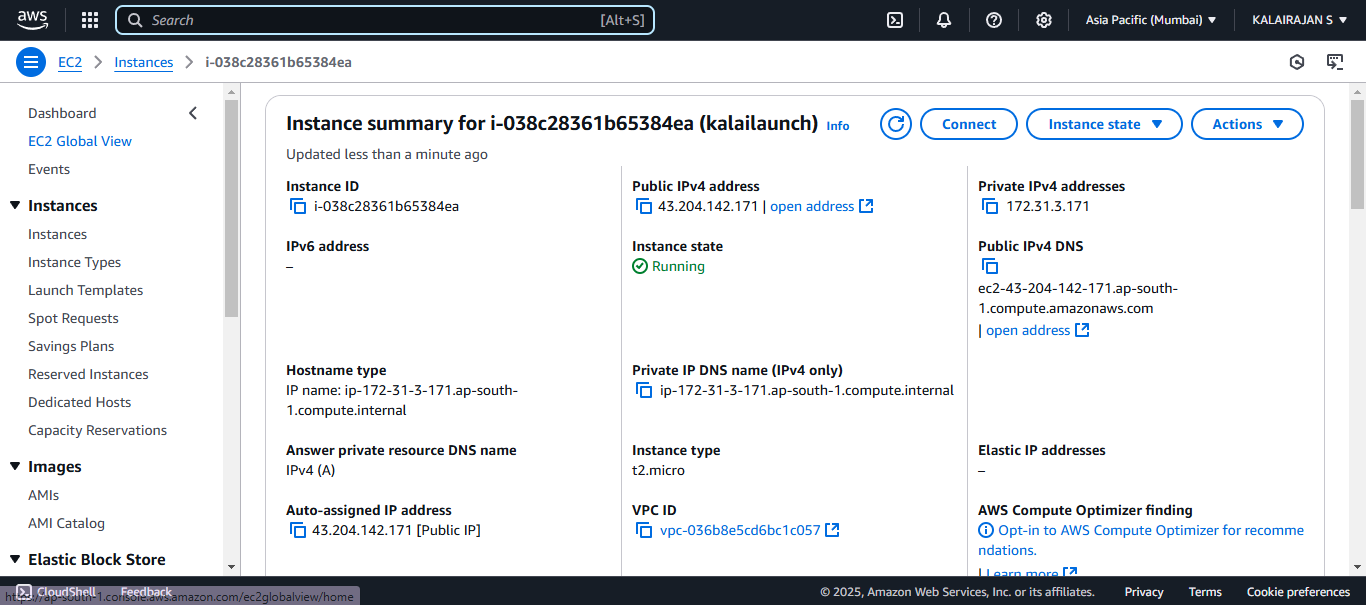
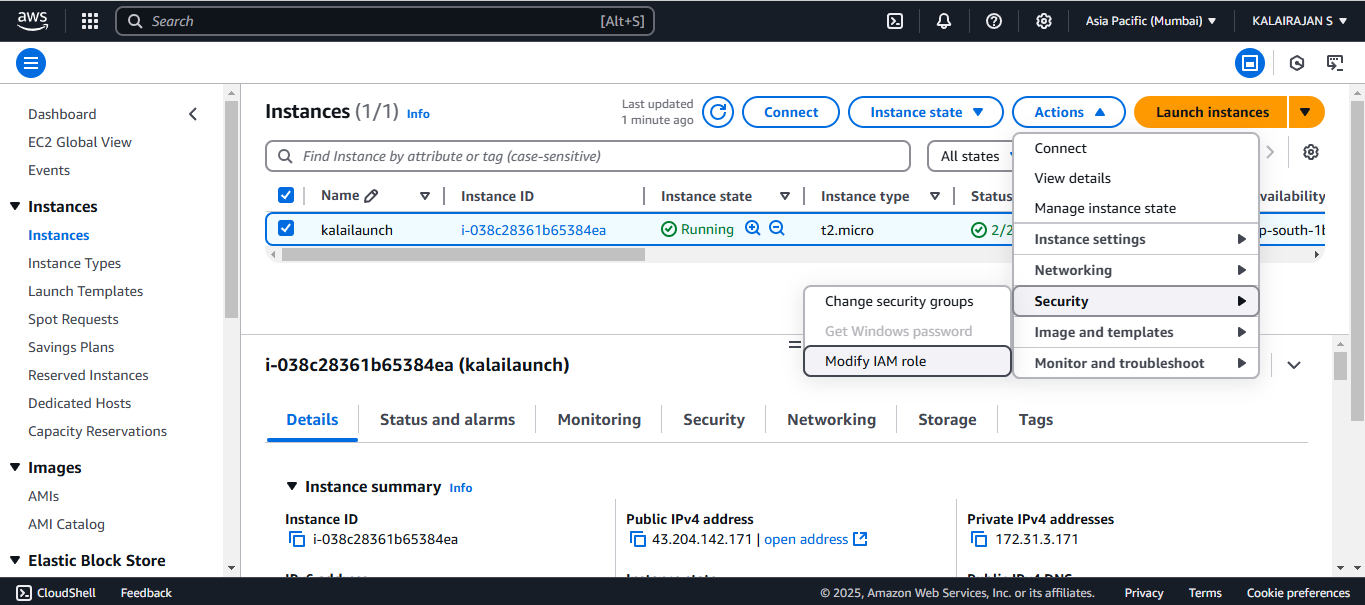


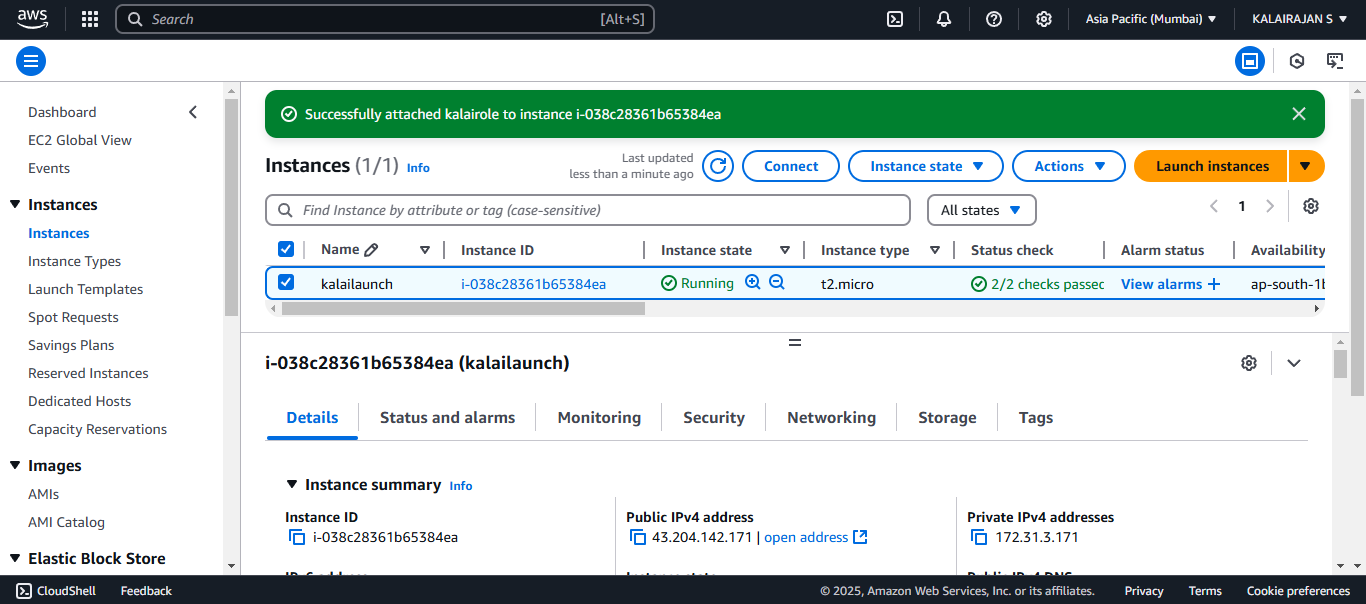
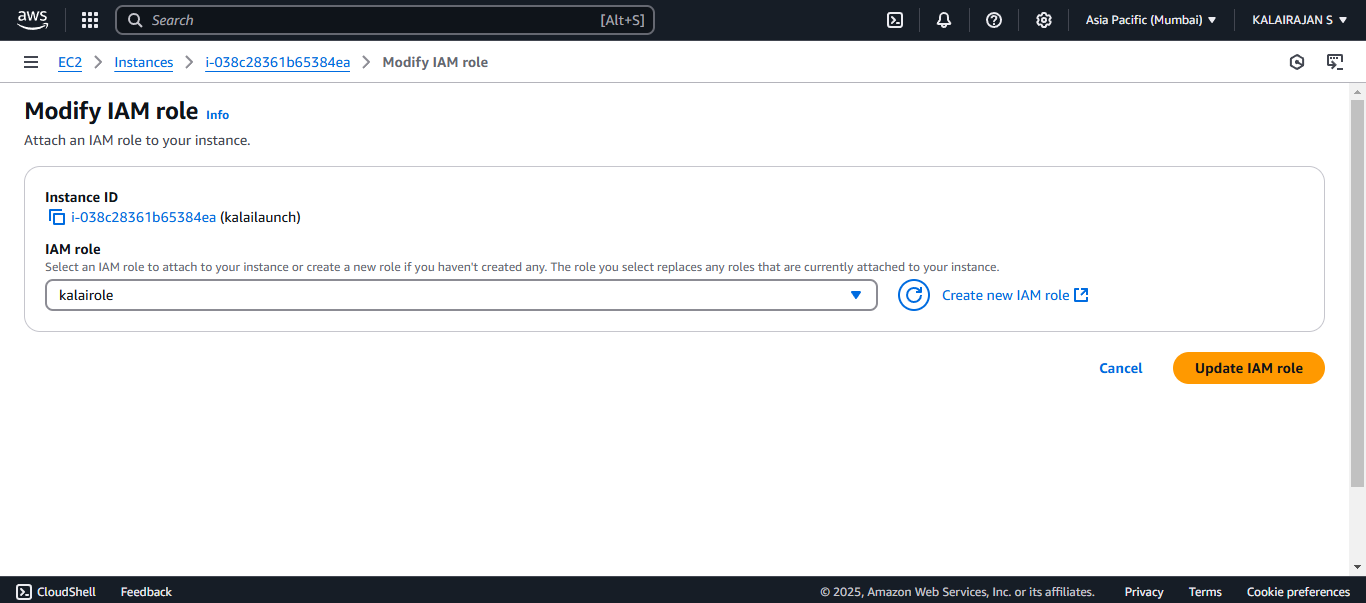
Select the type of trusted entity (such as a service account or a specific user group  

Attach necessary permissions: Assign policies that define allowed actions (e.g., read-only access, full control, or specific API permissions).



 Role is created.

Assign the Role to a Virtual Machine Modify Instance IAM Role:Select the EC2 instance you want to assign the IAM role to. Click Actions > Security > Modify IAM Role. Choose the IAM role created earlier from the dropdown.  

 Now your EC2 instance has the IAM role attached with the required permissions.

Conclusion:

Setting up IAM roles and permissions for your EC2 instance ensures secure and controlled access to AWS resources. Regularly review and update permissions to align with security best practices. By implementing IAM roles correctly, you reduce security risks and maintain a secure AWS environment.