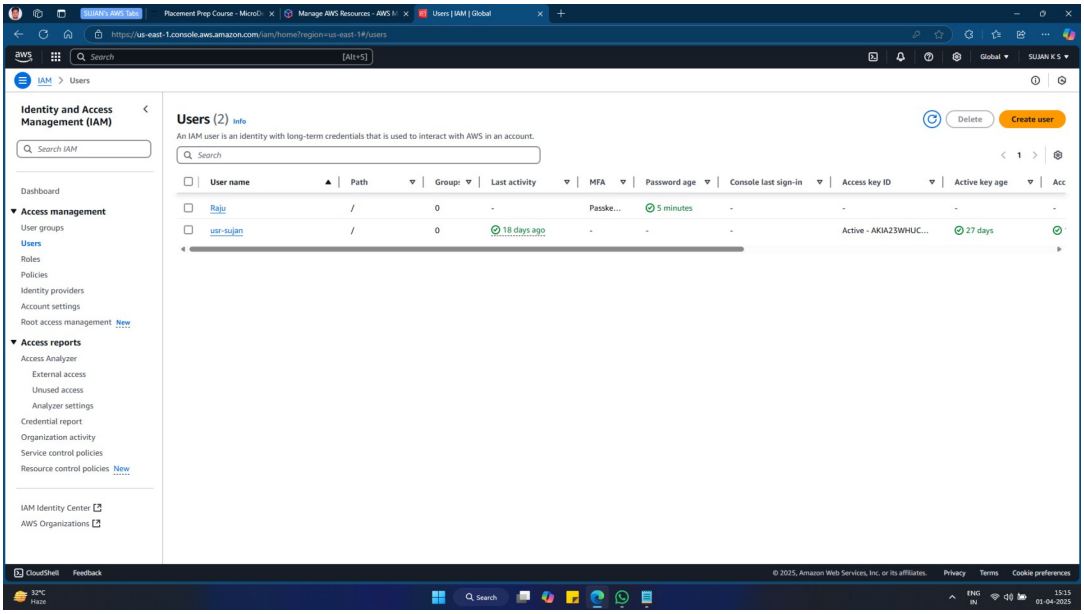
TASK 1 AWS IAM and EC2 Role Configuration

Task Overview

This document outlines the step-by-step implementation of IAM user creation, group management, MFA configuration, and EC2 role setup in AWS.

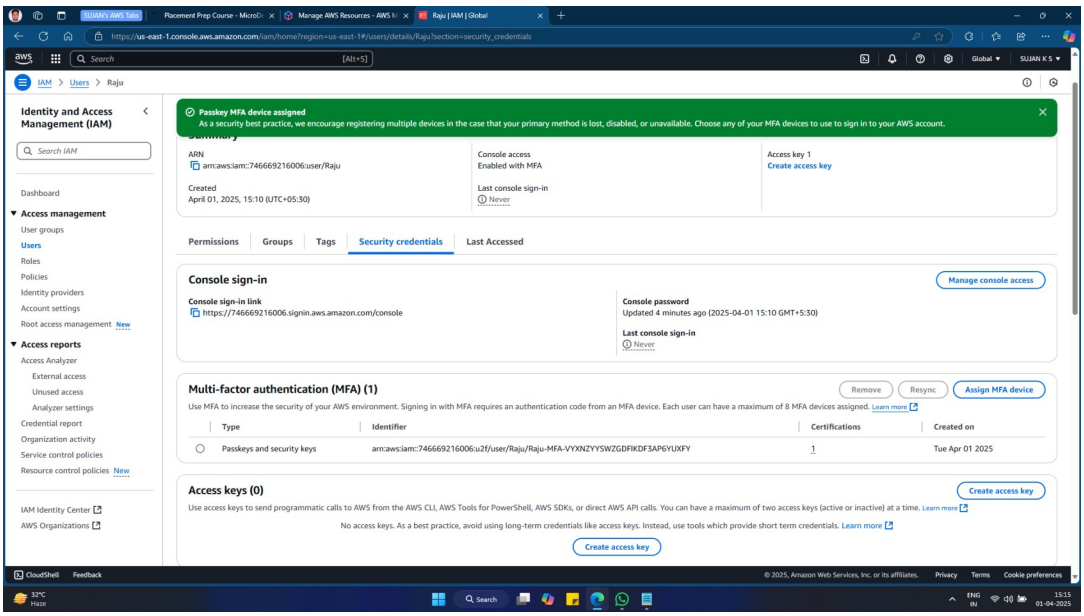
Task 1: Create an IAM User (Raju)

1. Log in to the AWS Management Console.
2. Navigate to IAM (Identity and Access Management).
3. Click on Users > Add user.
4. Enter the username: Raju.
5. Enable Programmatic access and AWS Management Console access.
6. Select Auto-generate password and require password reset on first login.
7. Click Next: Permissions, skip permissions assignment for now.
8. Click Create user.



Task 2: Enable Multi-Factor Authentication (MFA) for Raju

1. In the IAM Console, select the user Raju.
2. Go to the Security credentials tab.
3. Under Multi-Factor Authentication (MFA), click Manage MFA device.
4. Choose Virtual MFA device and scan the QR code using an authenticator app (Google Authenticator/Authy).
5. Enter the two consecutive MFA codes generated.
6. Click Activate MFA.

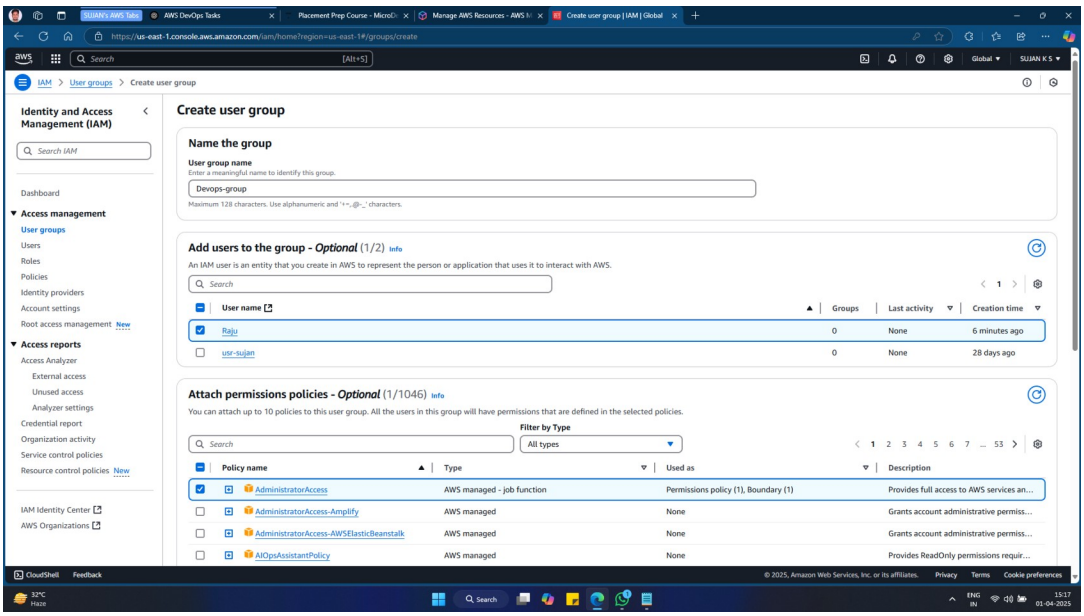


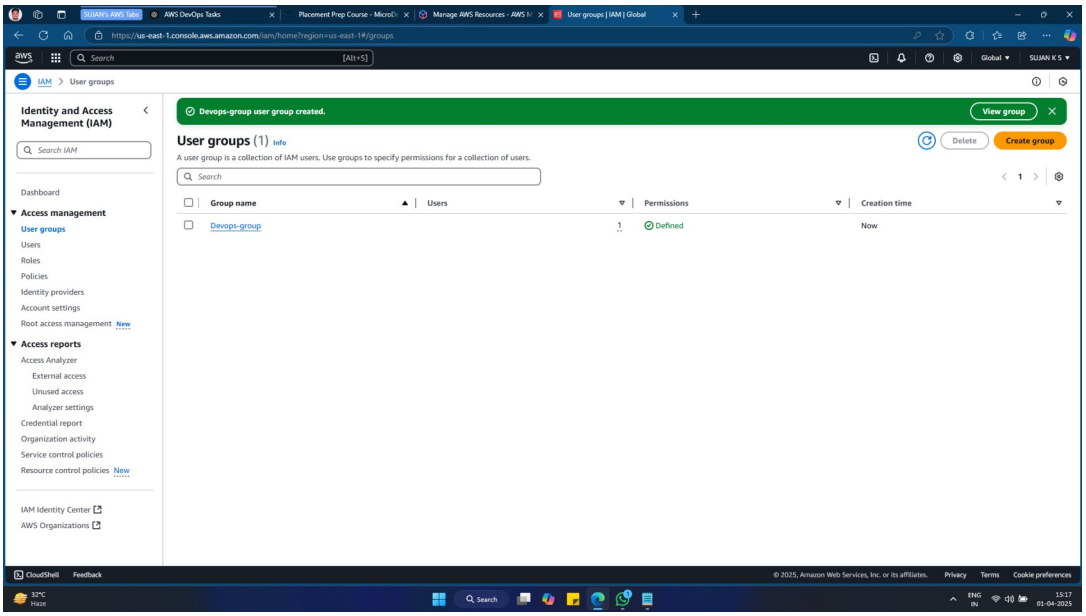
Task 3: Create the "Devops" Group and Assign Administrator Access

1. In the IAM Console, go to User Groups.
2. Click Create group and name it Devops.
3. Click Attach policies and search for AdministratorAccess.
4. Select AdministratorAccess and click Create group.

Task 4: Add Raju to the Devops Group

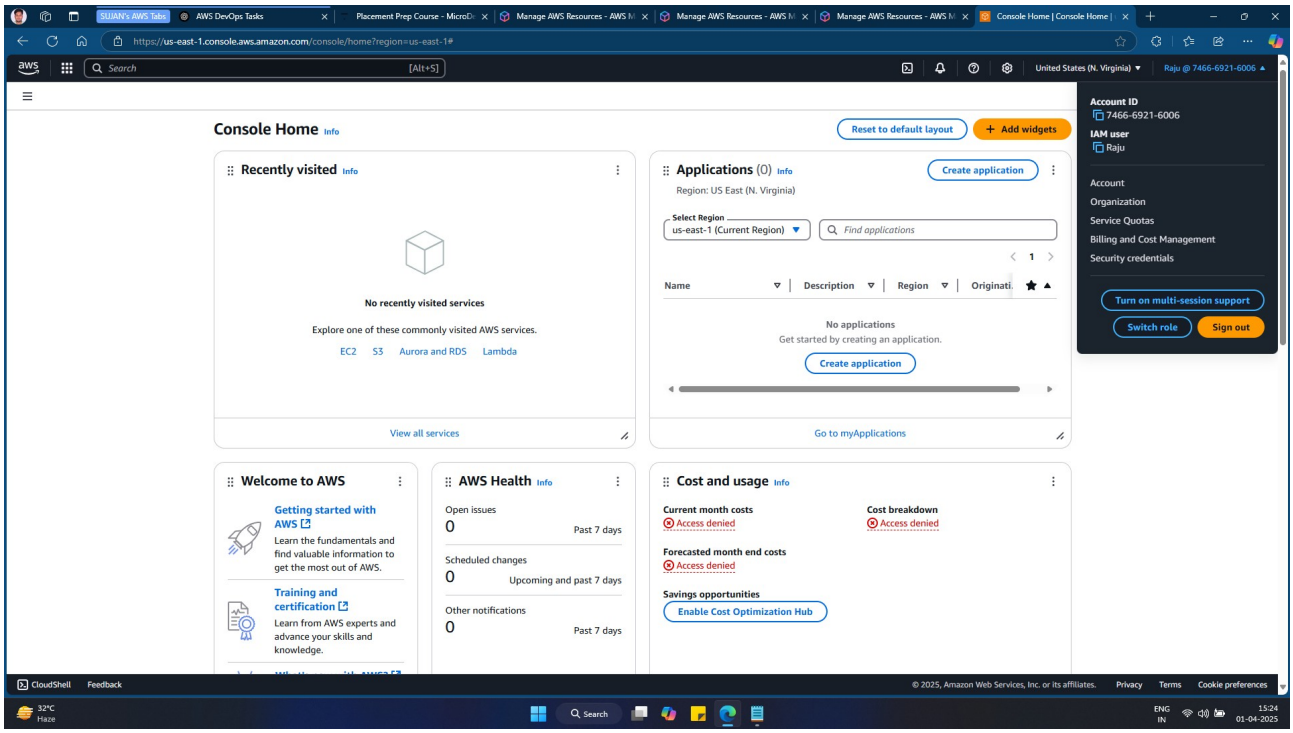
1. Go to Users and select Raju.
2. Click Add user to groups.
3. Select the Devops group and click Add to group.





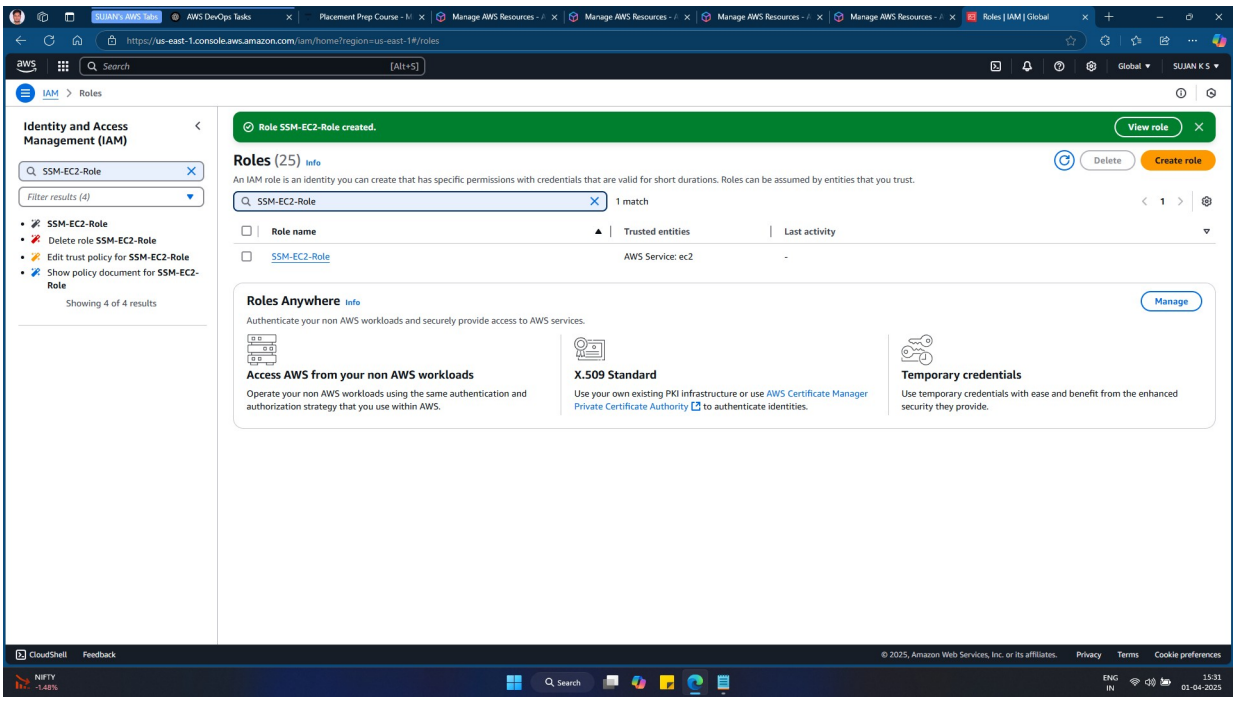
Task 5: Login as Raju with MFA

1. Open the AWS Management Console.
2. Enter the username: Raju.
3. Use the auto-generated password received.
4. Enter the MFA code from the authentication app.
5. Successfully log in to the AWS account.



Task 6: Create an IAM Role for Systems Manager (SSM) to Access EC2 in a Private Subnet

1. In the IAM Console, go to Roles.
2. Click Create Role.
3. Choose AWS service > EC2.
4. Click Next: Permissions.
5. Search for and attach the AmazonSSMManagedInstanceCore policy.
6. Click Next: Review.
7. Enter Role Name: SSM-EC2-Role.
8. Click Create Role.



Conclusion

The IAM user "Raju" was successfully created, secured with MFA, and assigned to the "Devops" group with AdministratorAccess permissions. Additionally, an SSM Role was created for EC2 instances in a private subnet, enabling seamless Systems Manager access.

This implementation ensures secure access management, group-based permissions, and EC2 role-based authorization following AWS best practices.

Submitted by: Sujan K S

Date: 01-04-2025