CODTECH INTERNSHIP – Cloud Computing

Task-4 : Cloud Security Implementation

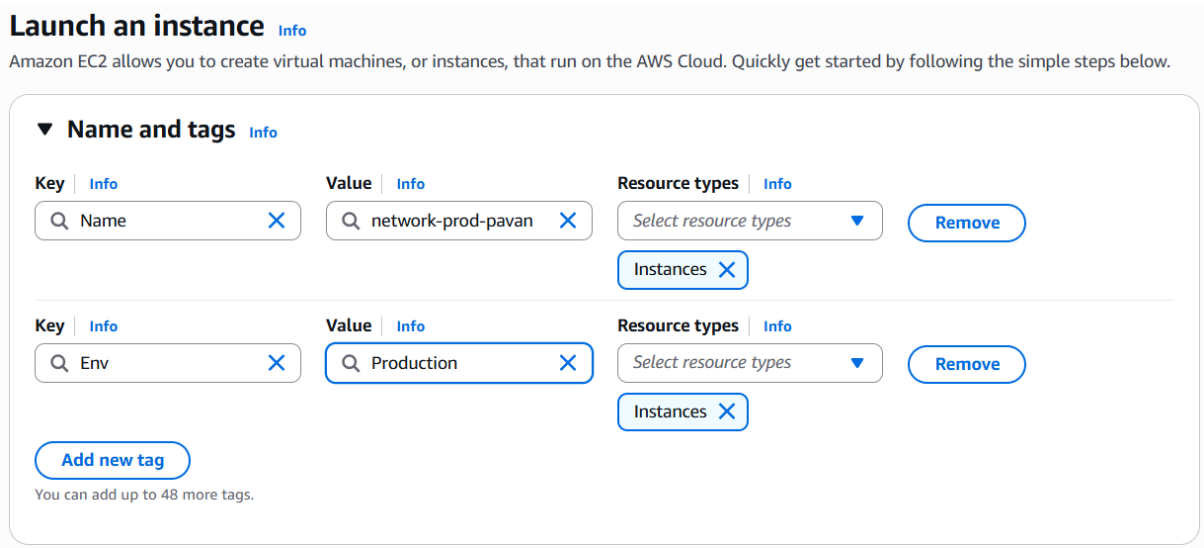
IMPLEMENT IAM POLICIES, SECURE STORAGE, AND DATA ENCRYPTION ON A CLOUD PLATFORM.

DELIVERABLE: CONFIGURED SECURITY POLICIES AND A REPORT DETAILING THE SETUP.

Steps to Complete Task:

Go to AWS → EC2 → Create two Instance.

- Production Instance.
- Development Instance.

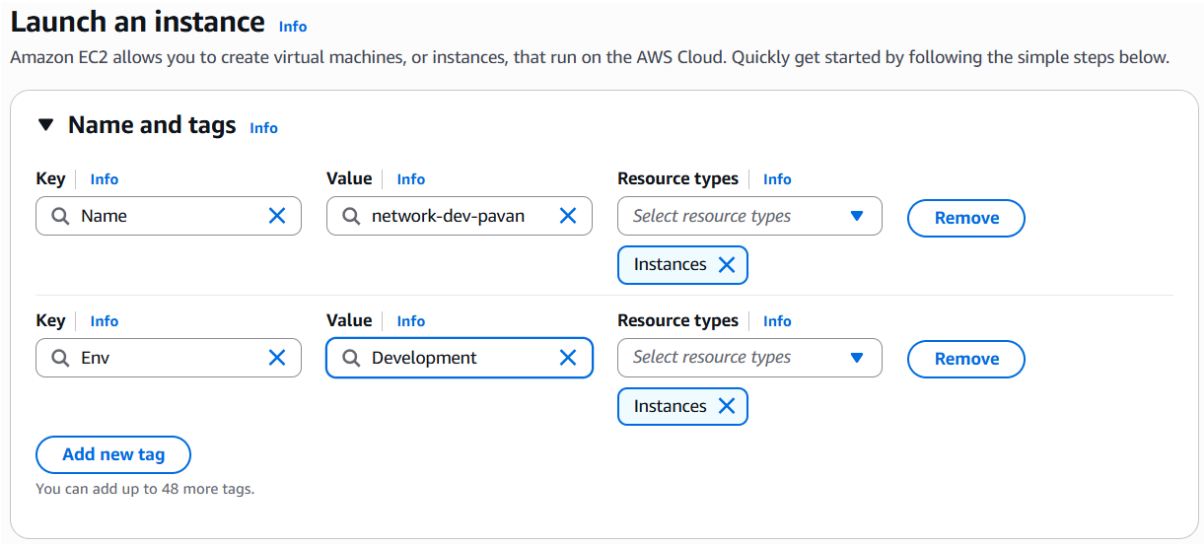


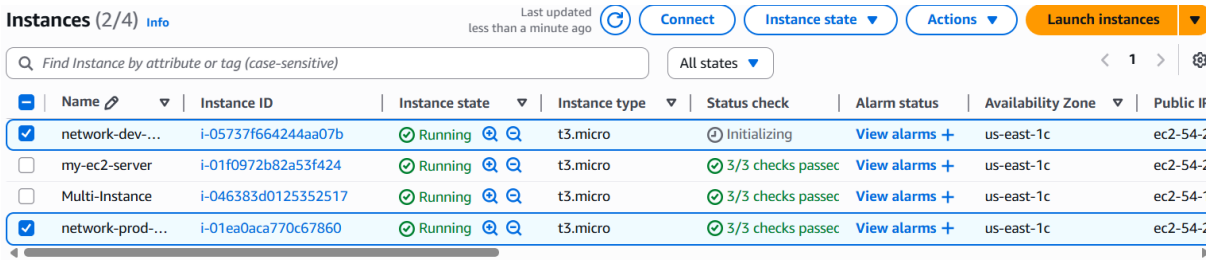
Create one Instance.

Change the value → Production.

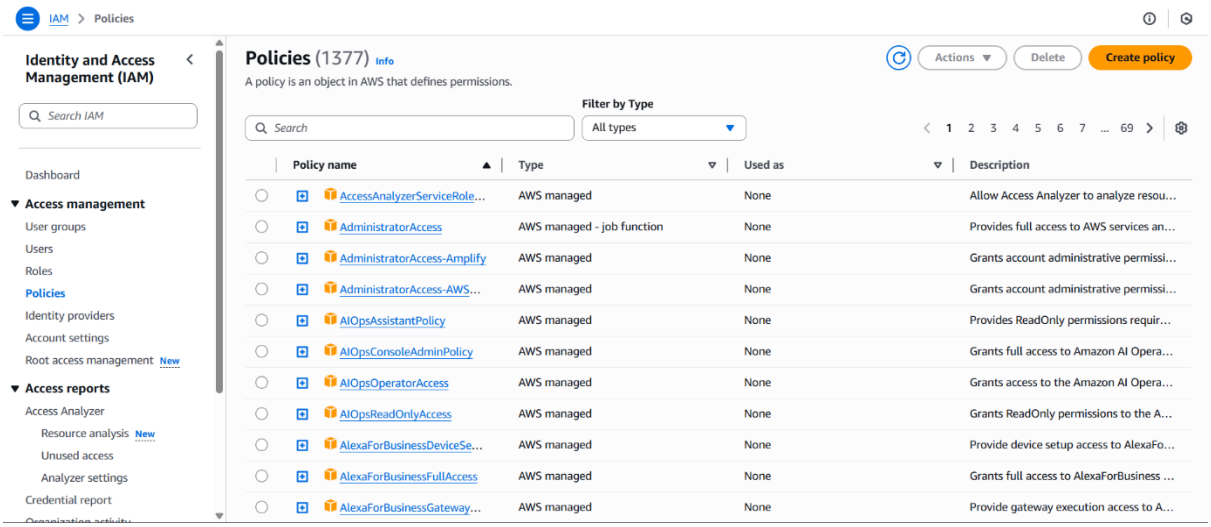
Create another Instance.

Change the value → Development.



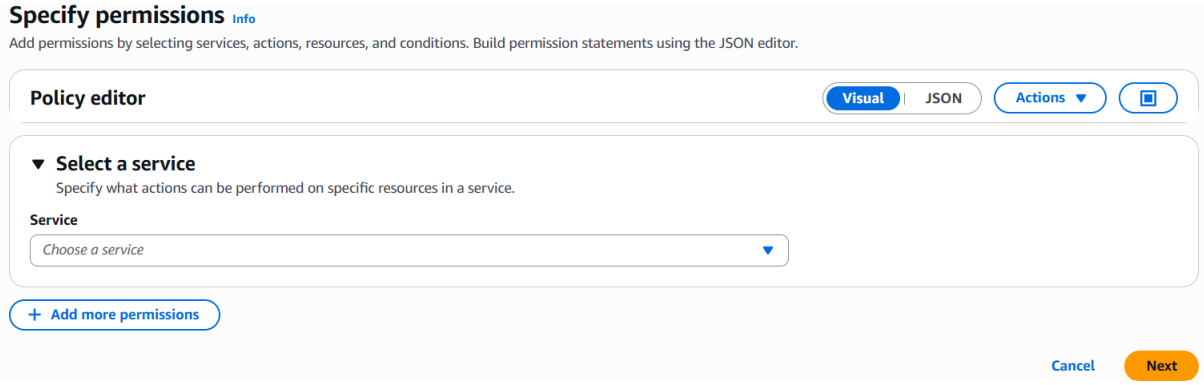


Here we can see that, two Instances are created.

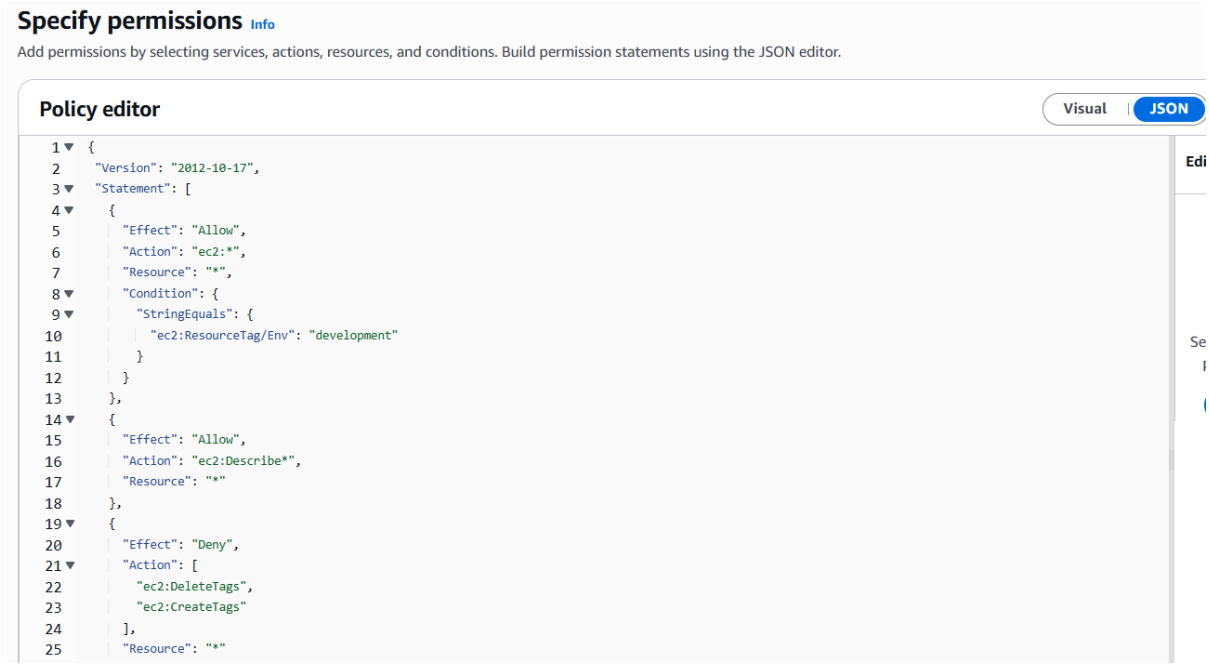


Now go to IAM → Policies (in left menu).

Click on Create Policy.



By Default it will be in visual, switch it to JSON mode.



Now paste the below JSON code in Policy editor.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Env": "development"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource": "*"
    }
  ]
}
```

This JSON code will not allow an alias user to stop an Instances and delete tags.

Paste code in Policy Editor.

Click Next.

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

Visual | JSON

```
1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Effect": "Allow",
6        "Action": "ec2:*",
7        "Resource": "*",
8        "Condition": {
9          "StringEquals": {
10           "ec2:ResourceTag/Env": "development"
11         }
12       }
13     },
14     {
15       "Effect": "Allow",
16       "Action": "ec2:Describe*",
17       "Resource": "*"
18     },
19     {
20       "Effect": "Deny",
21       "Action": [
22         "ec2:DeleteTags",
23         "ec2:CreateTags"
24       ],
25       "Resource": "*"
```

Give a name and Description.

Review and create Info

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

NetworkDevEnvPolicy

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*

Add a short explanation for this policy.

IAM Policy for the Network Development Environment

Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

Give the Permissions for the Policy.

NetworkDevEnvPolicy Info

IAM Policy for the Network Development Environment

Edit | Delete

Policy details

Type	Creation time	Edited time	ARN
Customer managed	July 17, 2025, 10:11 (UTC+05:30)	July 17, 2025, 10:11 (UTC+05:30)	arn:aws:iam::233720366258:policy/NetworkDevEnvPolicy

Permissions | Entities attached | Tags | Policy versions (1) | Last Accessed

Permissions defined in this policy Info

Edit | Summary | JSON

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

Explicit deny (1 of 446 services)

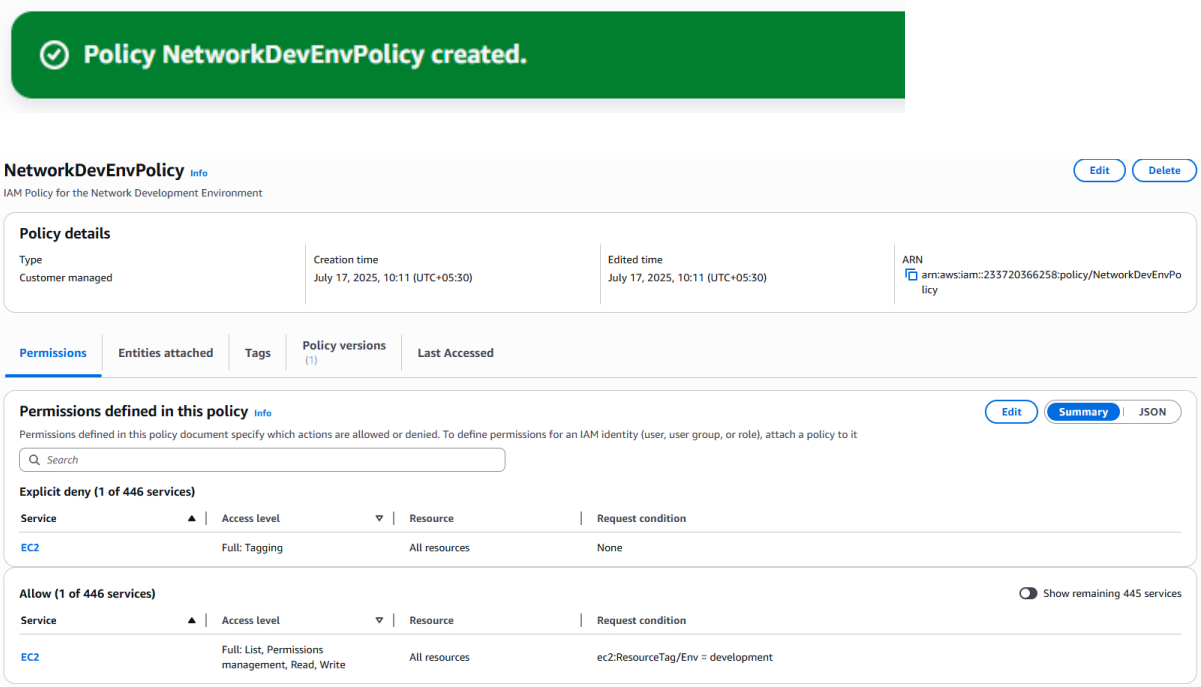
Service	Access level	Resource	Request condition
EC2	Full: Tagging	All resources	None

Allow (1 of 446 services)

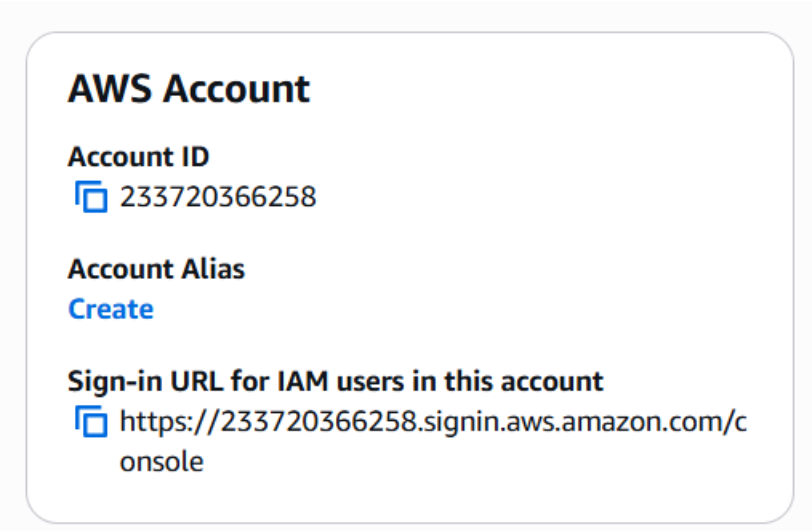
Show remaining 445 services

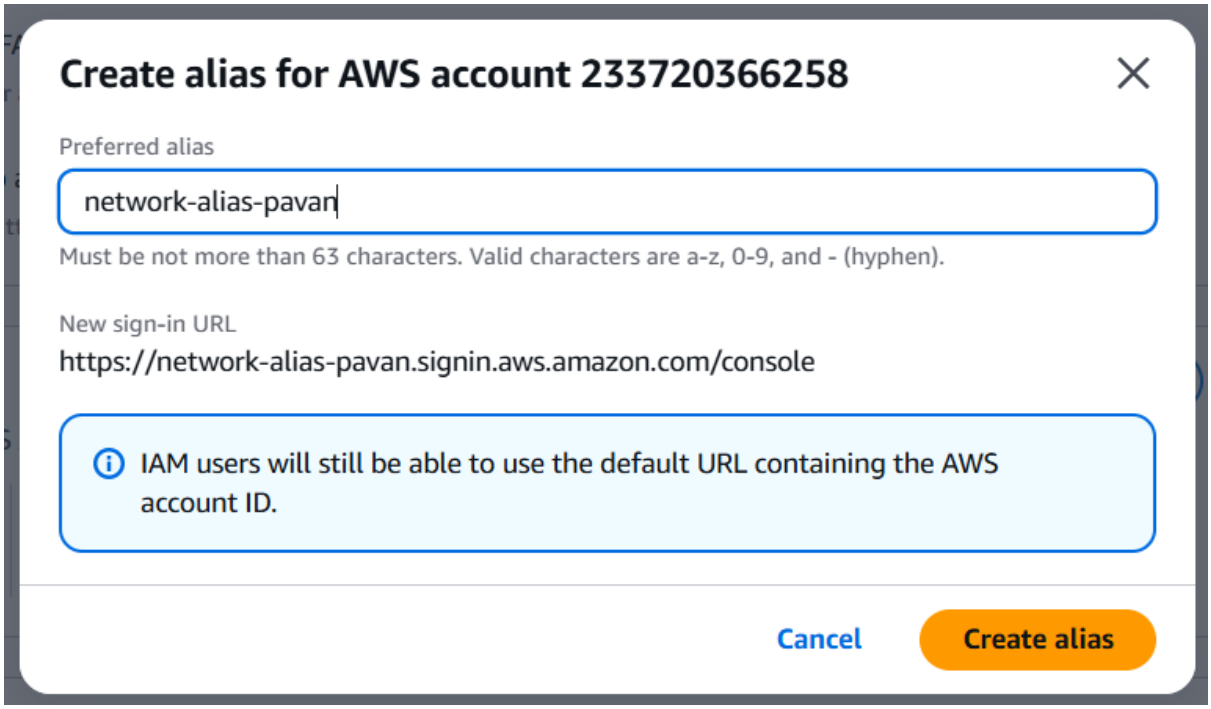
Service	Access level	Resource	Request condition
EC2	Full: List, Permissions management, Read, Write	All resources	ec2:ResourceTag/Env = development

The Policy for the Instance is Created.

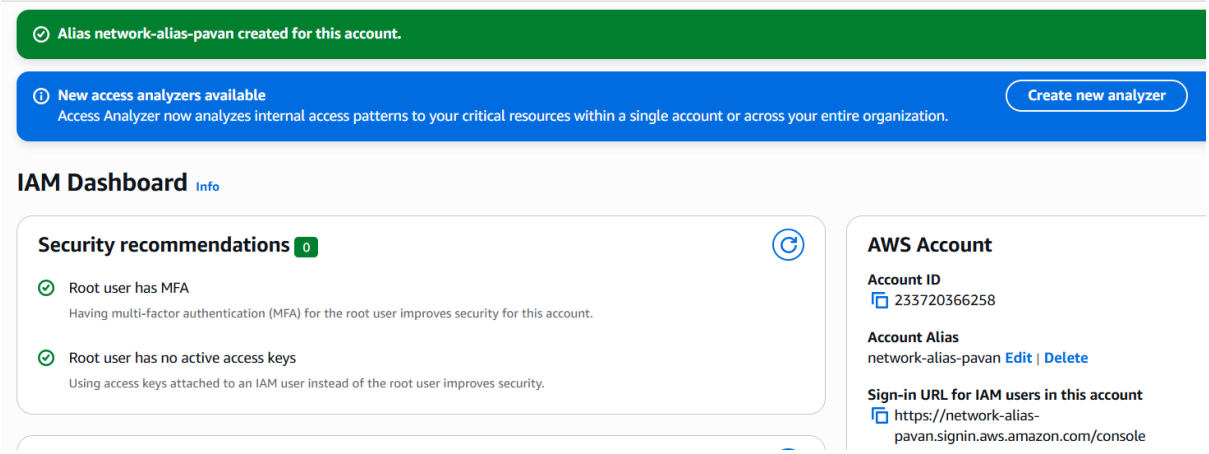


Go to IAM Dashboard → do to AWS account → Search for the Account Alias → Click on Create



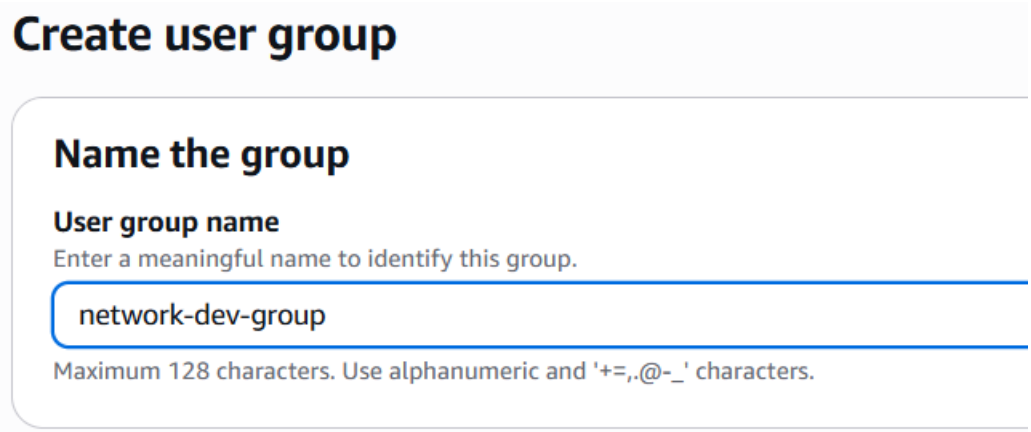


Give the name for preferred alias and click create.

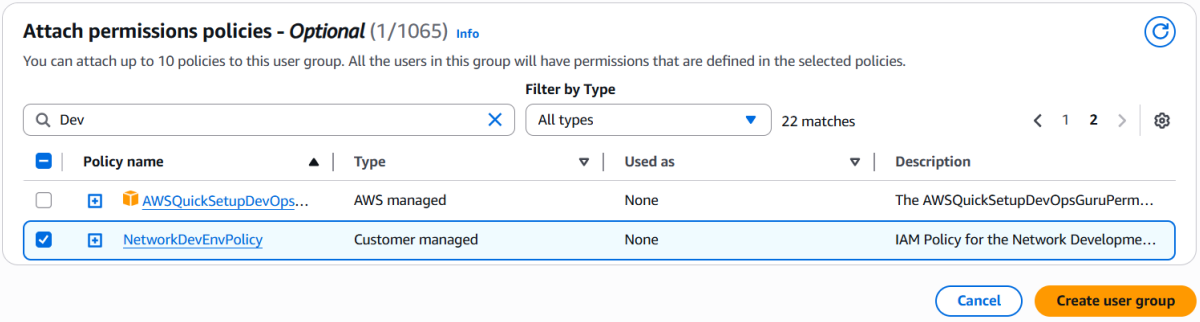


Here we Created an alias user.

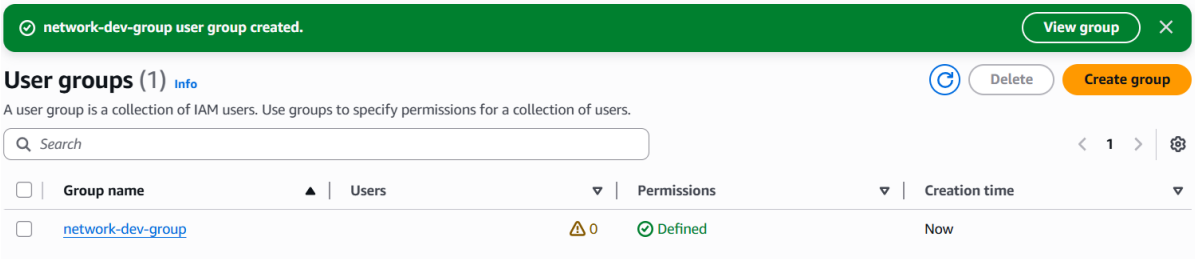
Now go to User Group in left menu and Click to Create Group.



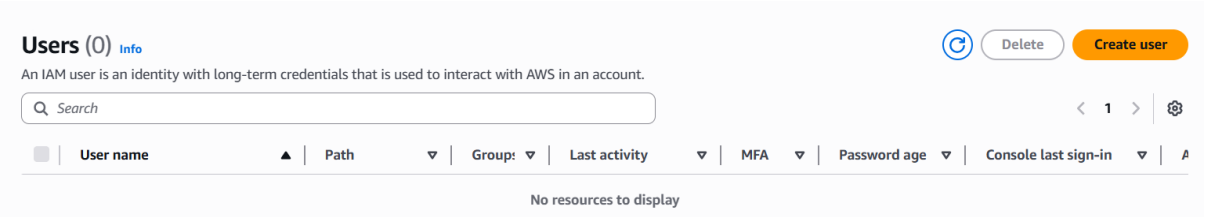
Give the name for the user group.



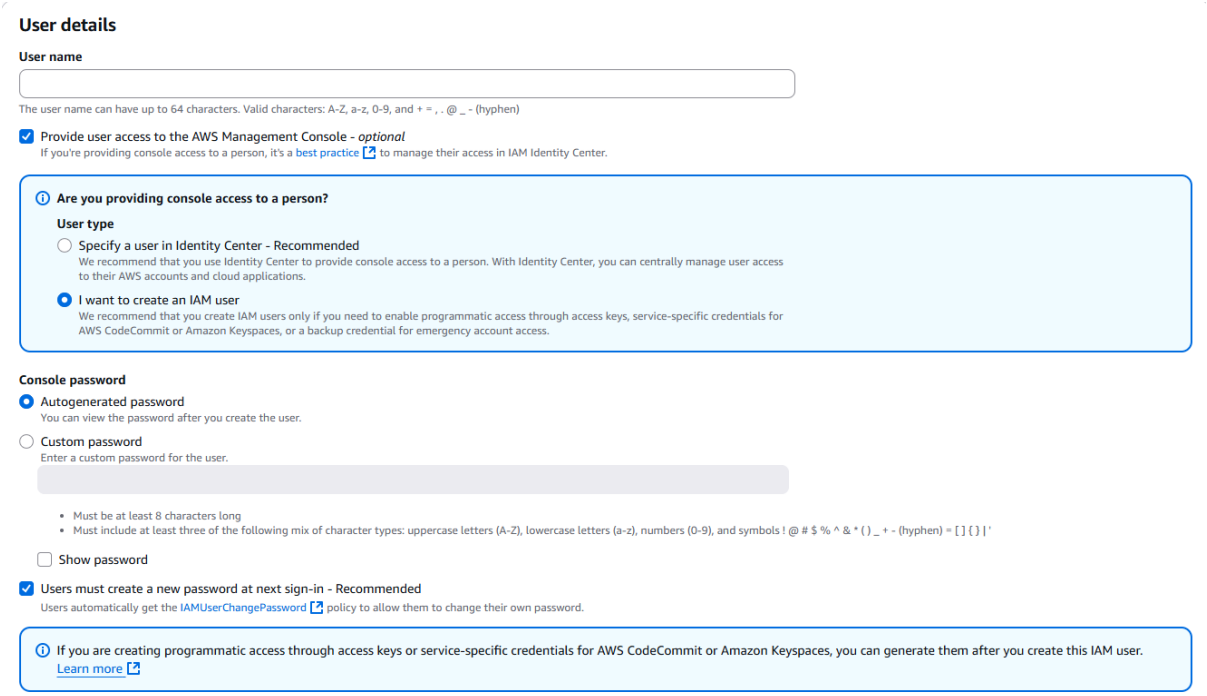
Select the Policy that we created and click Create User Group.



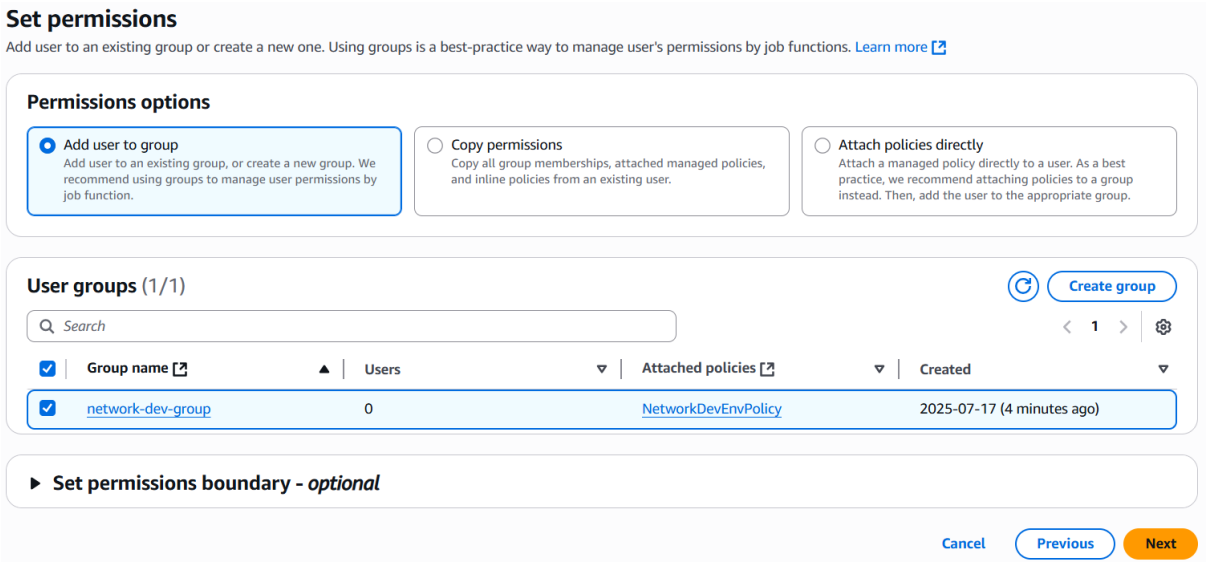
The User Group was Created.



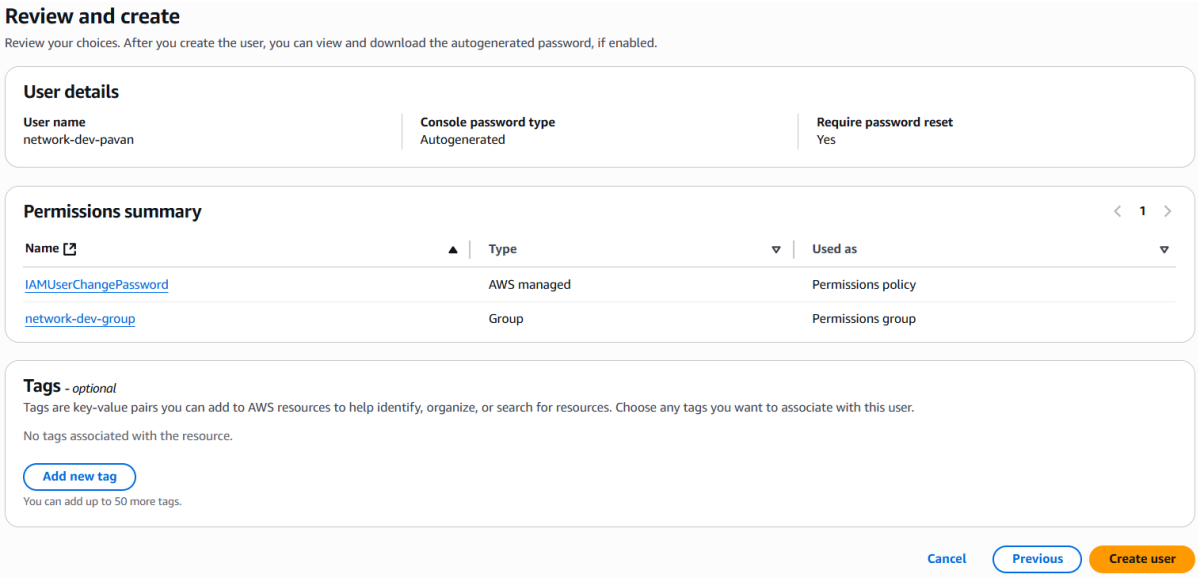
Go to side menu and click user → Create User.



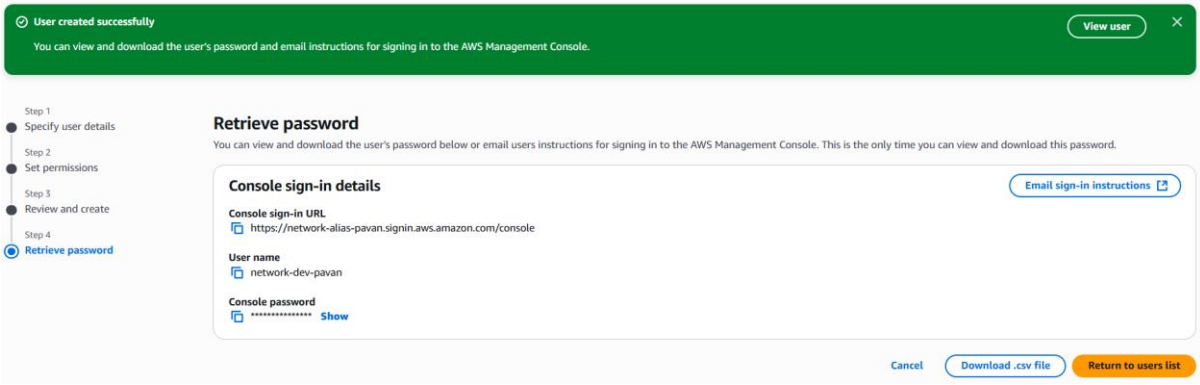
Give all the details like shown above.



Give the User group we created.

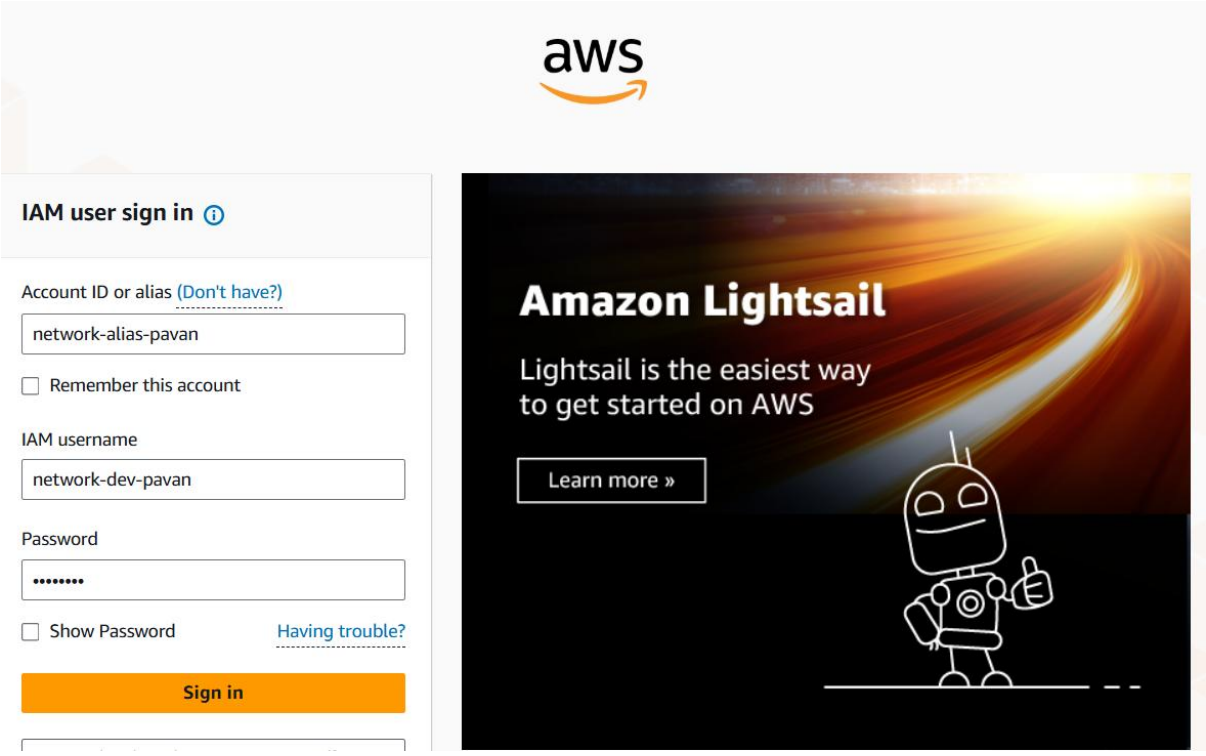


After giving all details click Create User.

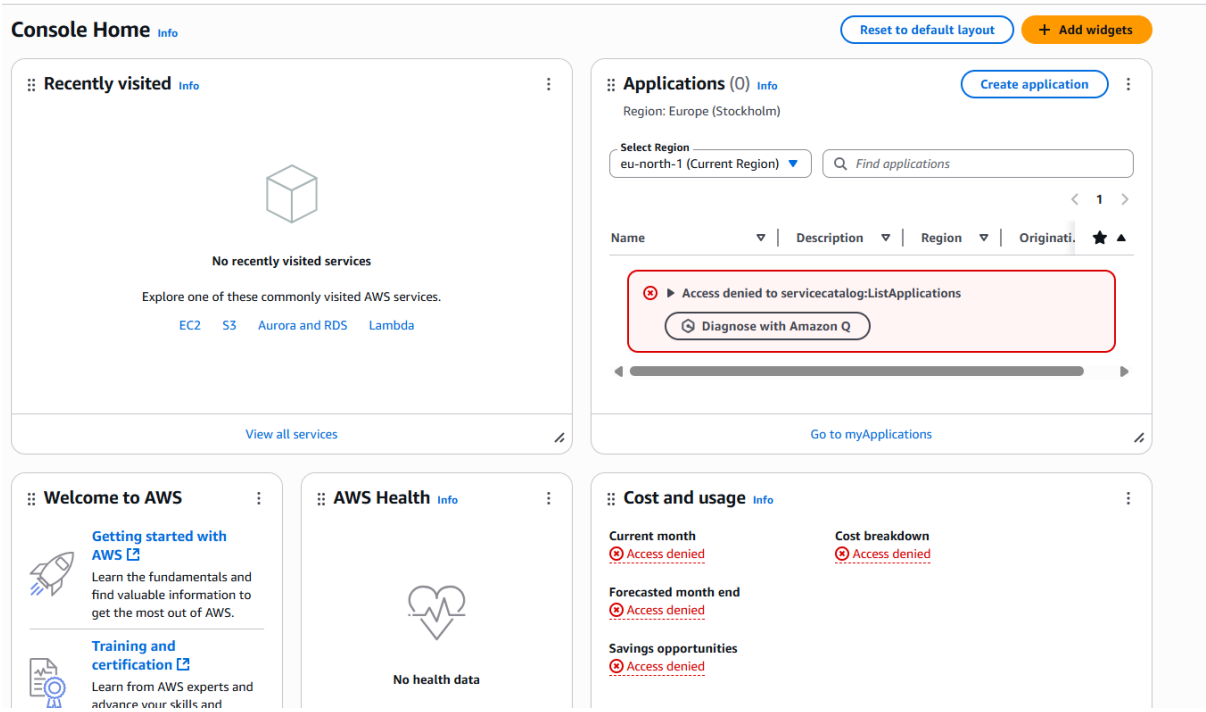


We have Created an User.

Now Go to the New tab in browser and paste the Console Sign-in URL.

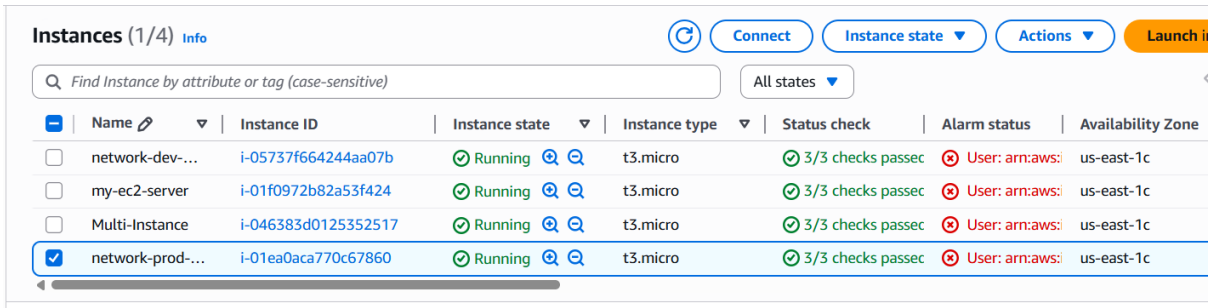


Now Fill in the Login Details we got after the user creation.



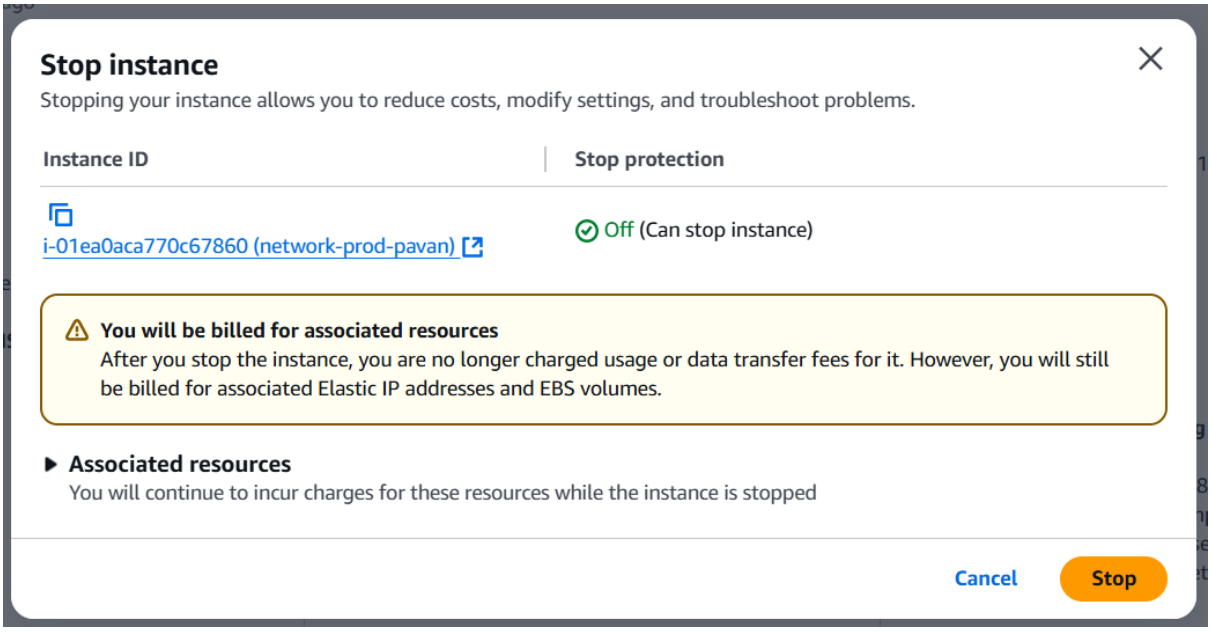
Here we can see there are limited access to this account based on the policy we created.

Go to EC2 → Select Production Instance.



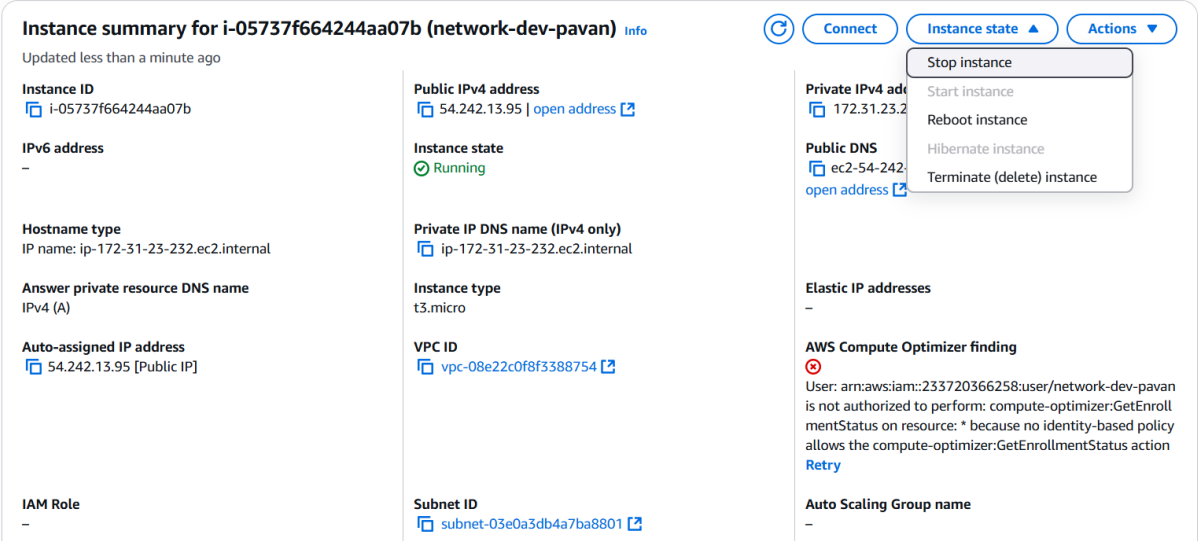
Click on Instance ID → Open it → Go to Actions → Stop Instance.

Try to Stop the Instance.



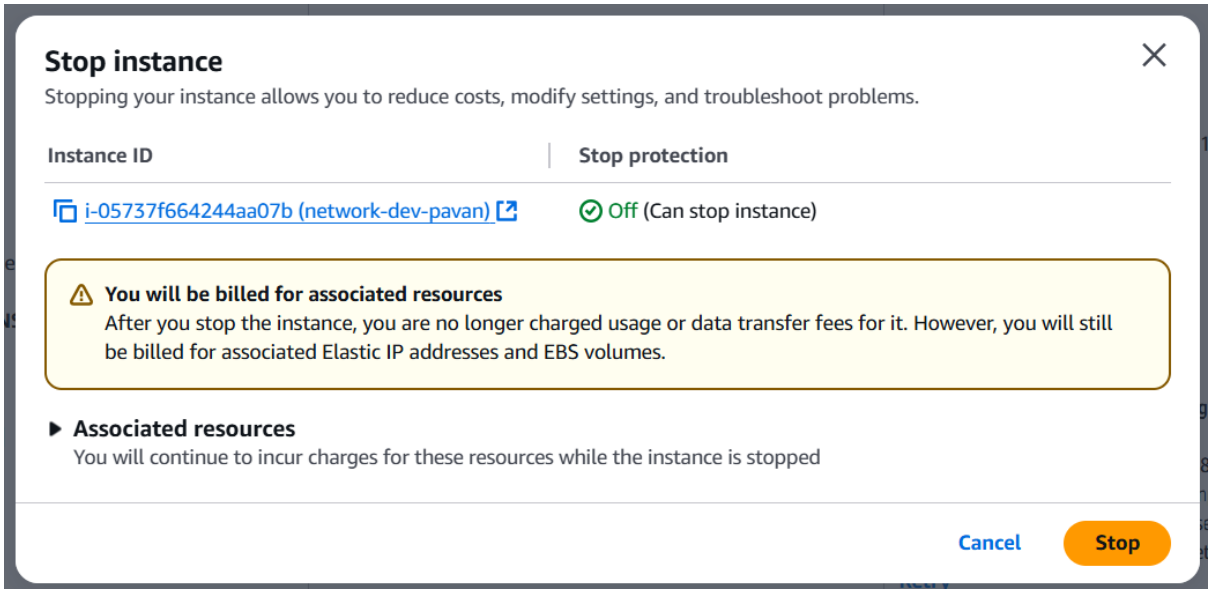
Click the Stop Button.

We cannot try to stop the Production Instance.



Now Click on Instance ID → Open it → Go to Actions → Stop Instance.

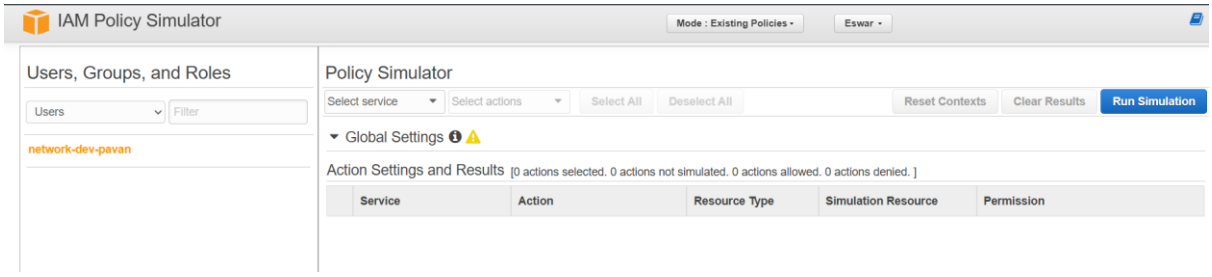
Try to Stop the Instance.



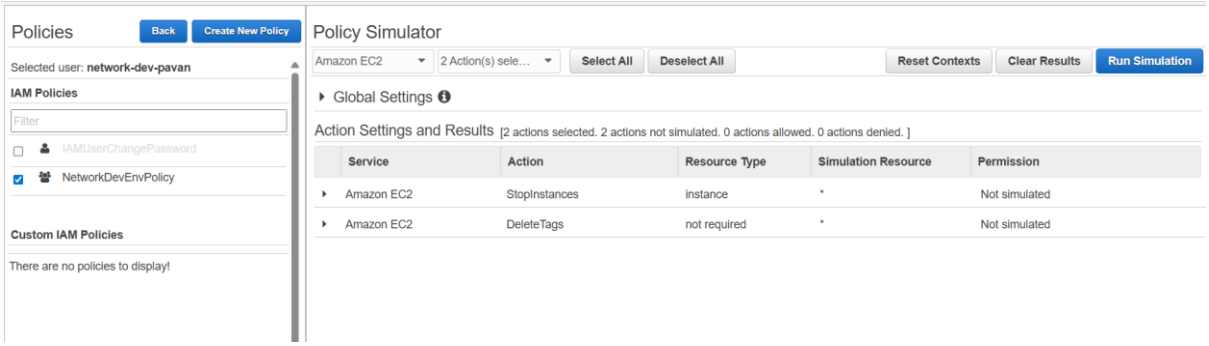
Click on Stop Button.

Now also we cannot stop the Development Instance.

Now Logout from Alias account → Go to root account → Go to IAM Dashboard → Policy simulator click on it.



Select User and the Name.



Select Service → EC2

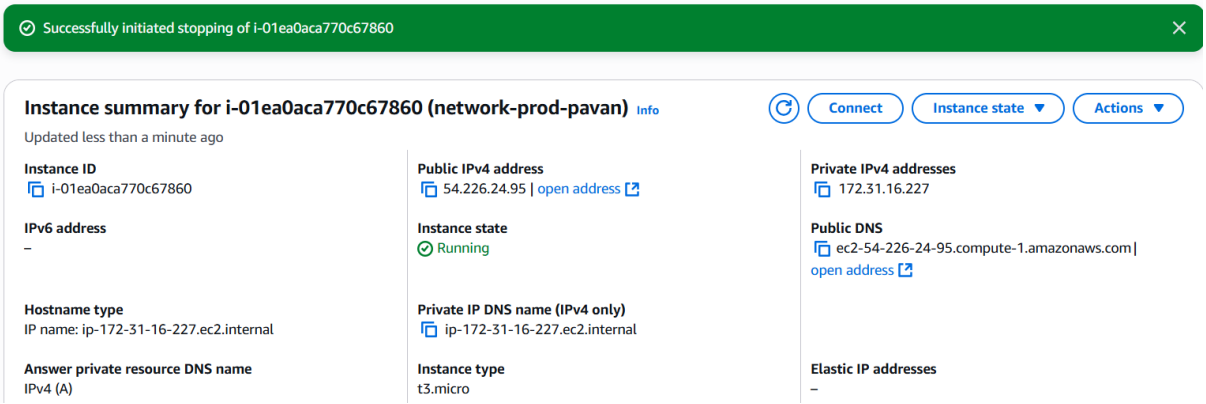
Select Action → Stop Instance & Delete Tags

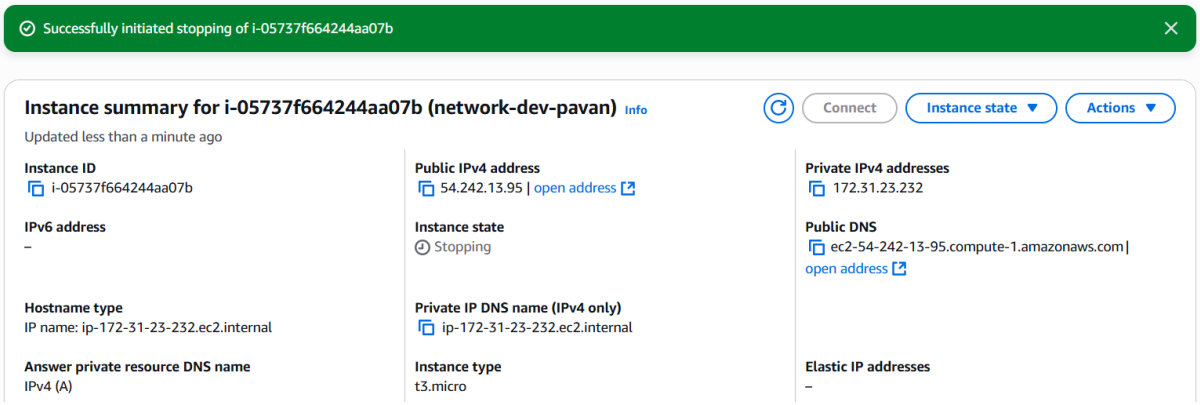
Click Run Simulation.

It tells that we don't have permissions to Policy.

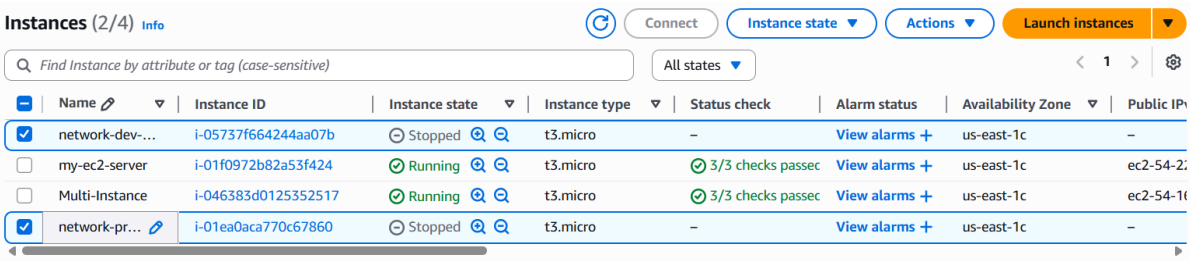
Now If we try to Stop the Instance of Development and Production.

We can easily Stop the Instance.





Finally We, have Stopped the Production and Development Instances.



This is how we use IAM for Access Management.