dem

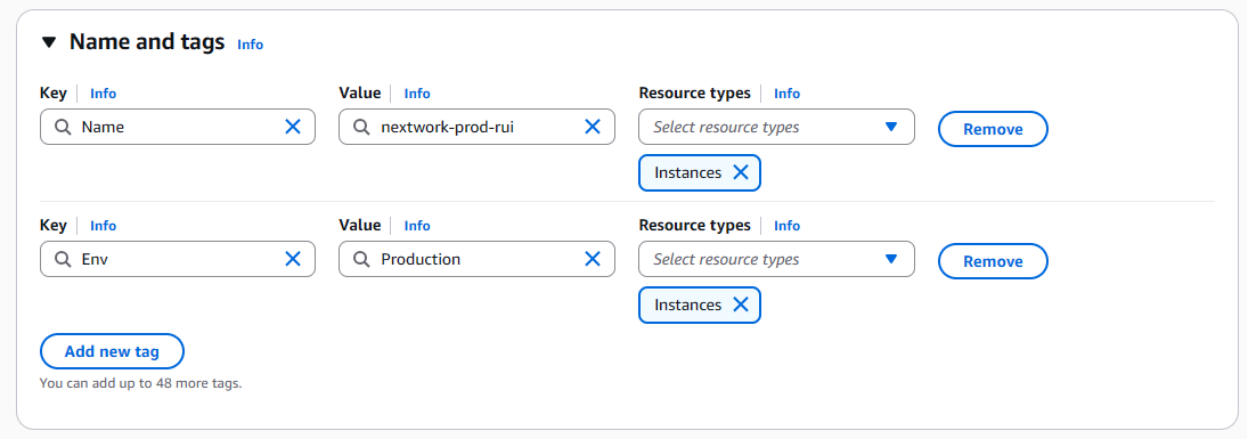
Task-4 : Cloud Security Implementation

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

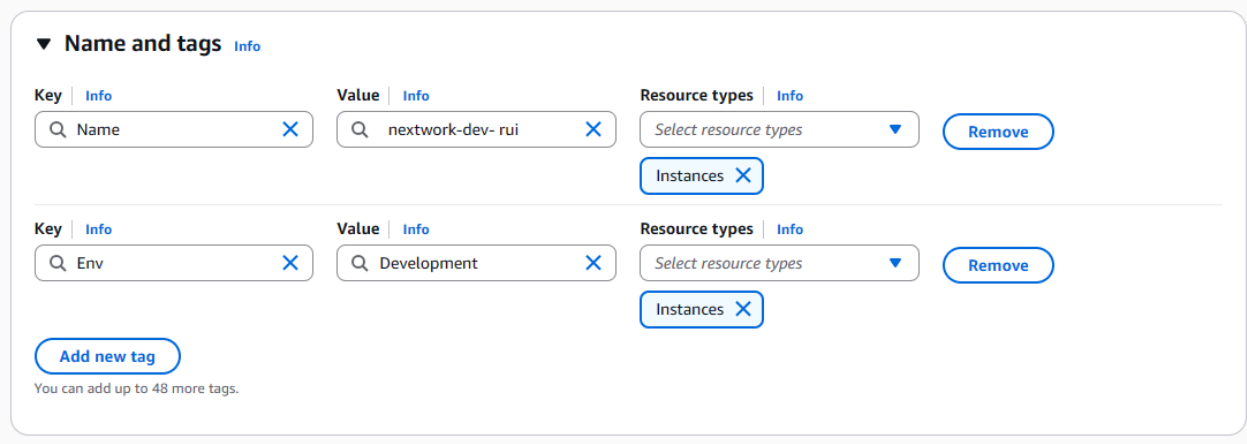
DELIVERABLE: CONFIGURED SECURITY POLICIES AND A REPORT DETAILING THE SETUP.

First you must Create two instances

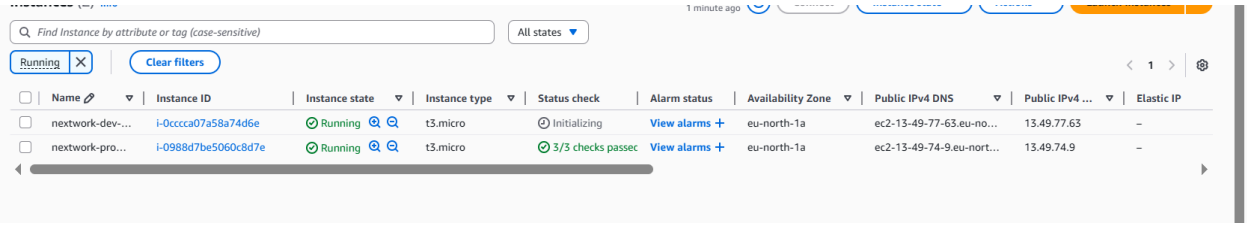
- Production Instances
- Development Instances



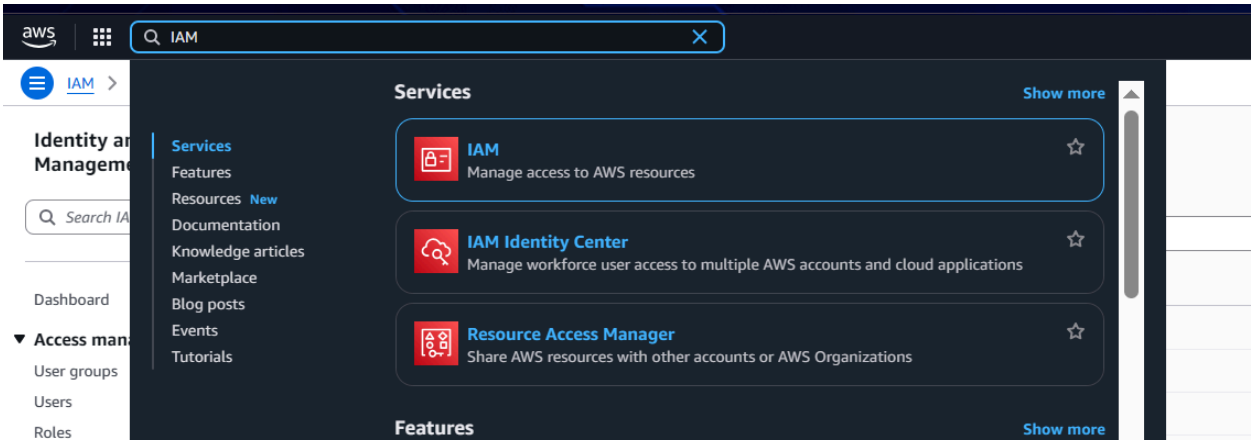
Here we need to add the Tag Production



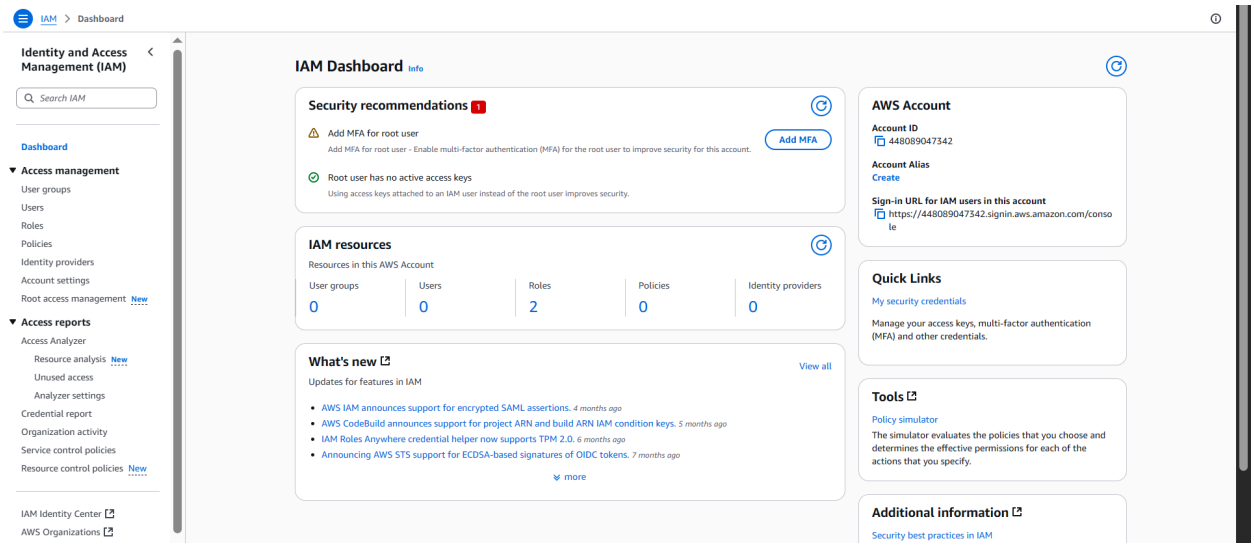
Here we need to add the Tag Development



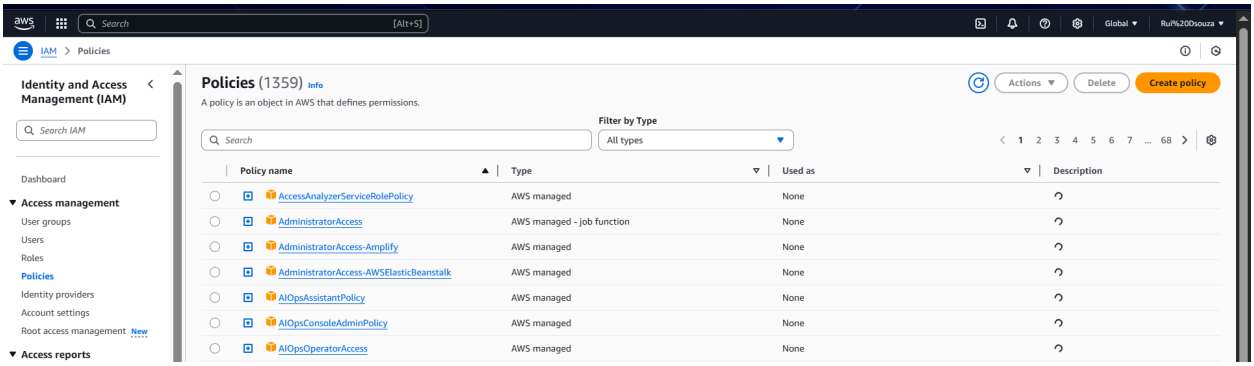
Here we create the 2 instances



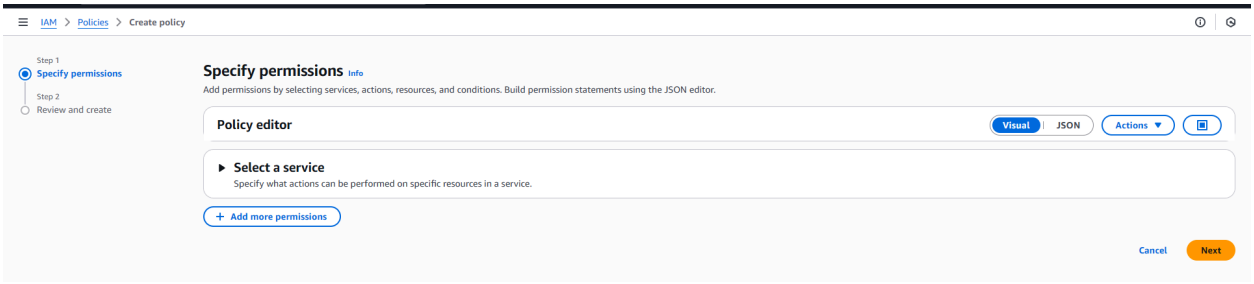
Now Go to IAM



Click Policies form the left menu.



click on Create policy



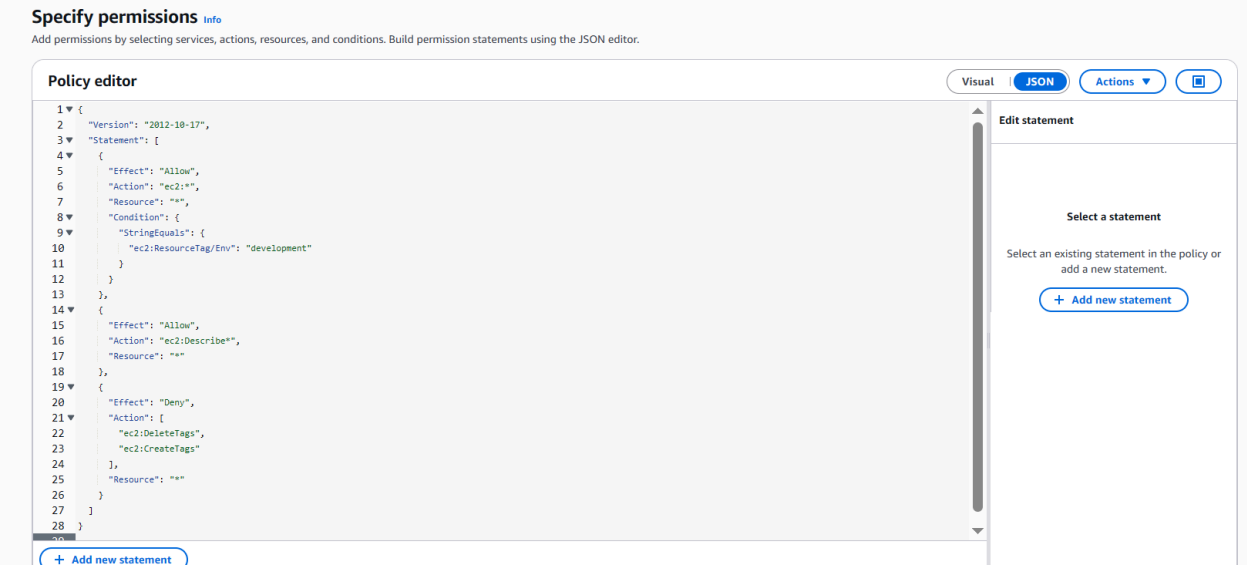
select the JSON mode

Copy the below json file.

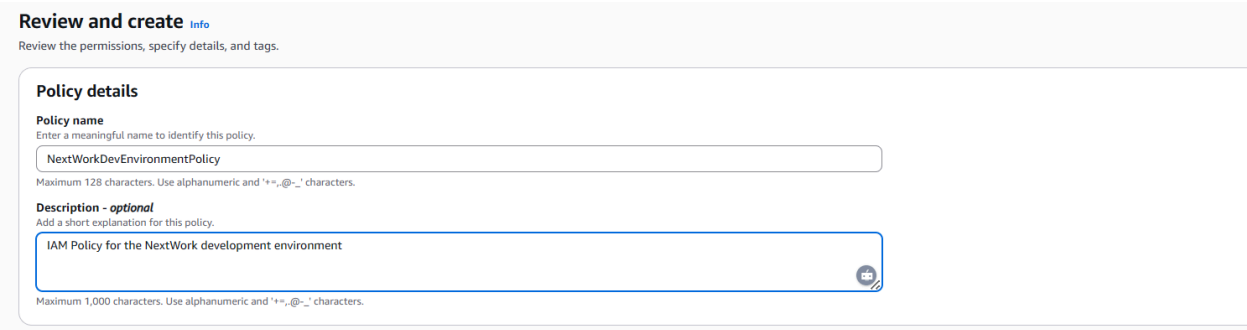
```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "ec2:*",
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "ec2:ResourceTag/Env": "development"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": "ec2:Describe*",
   "Resource": "*"
  },
  {
  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

```
      "ec2:CreateTags"
    ],
    "Resource": "*"
   }
  ]
}
```

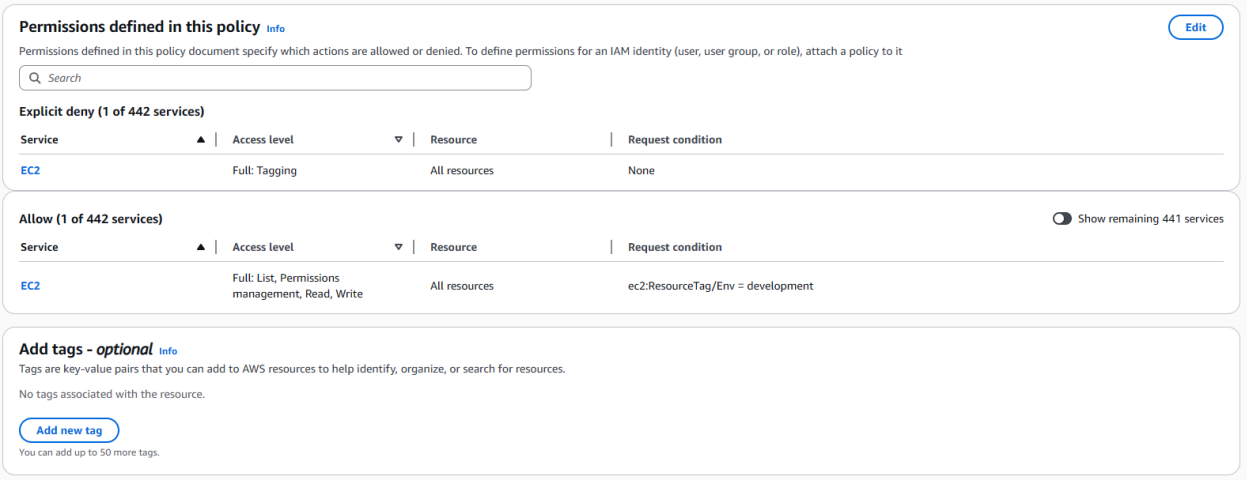
This json file will not allow an alias user to stop instances and delete tags



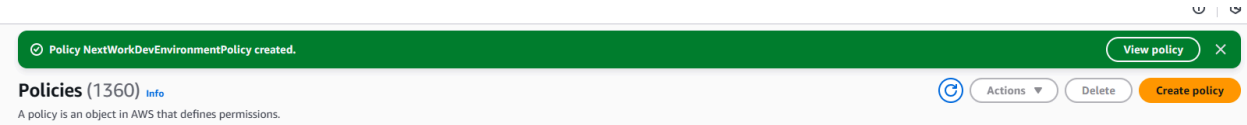
paste it here and click next

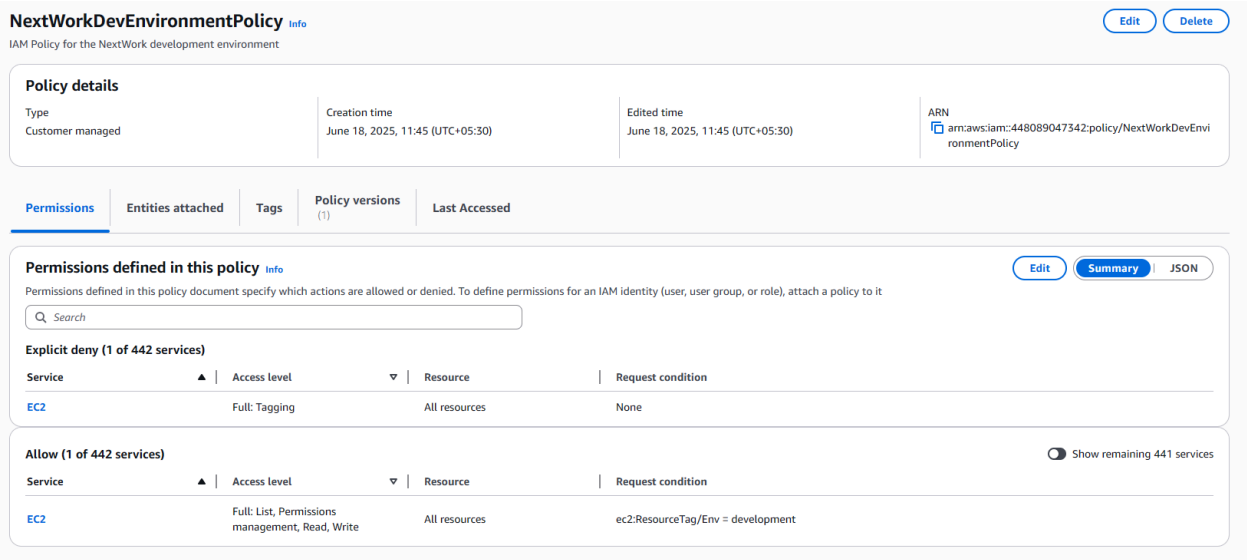


give a name and description

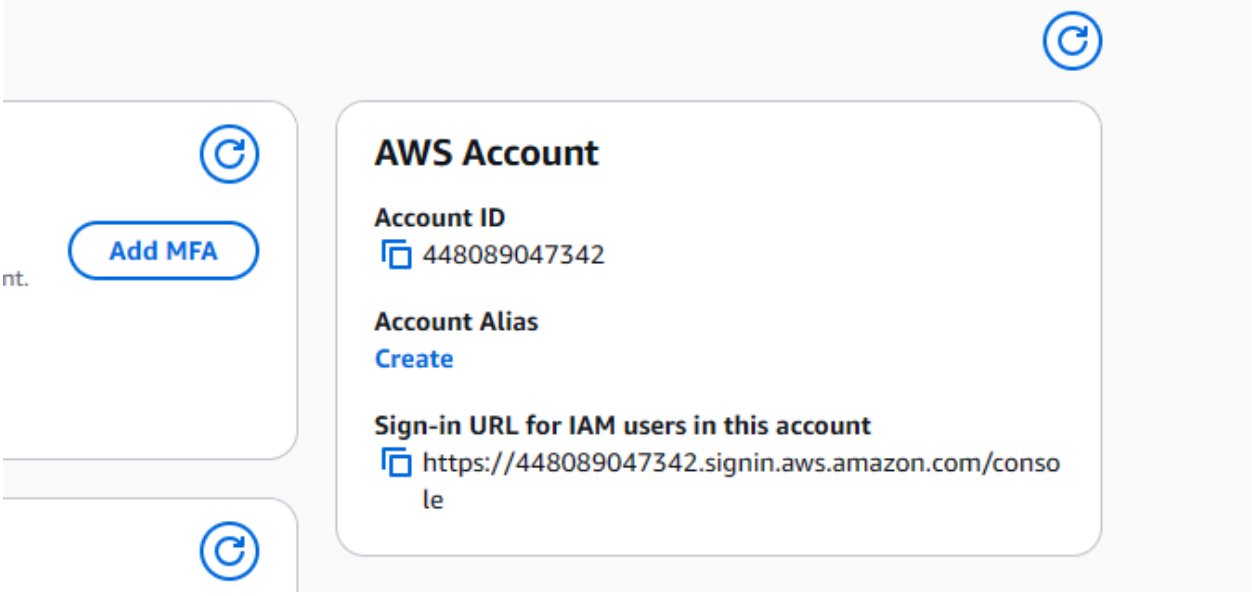


Keep this as default and click create

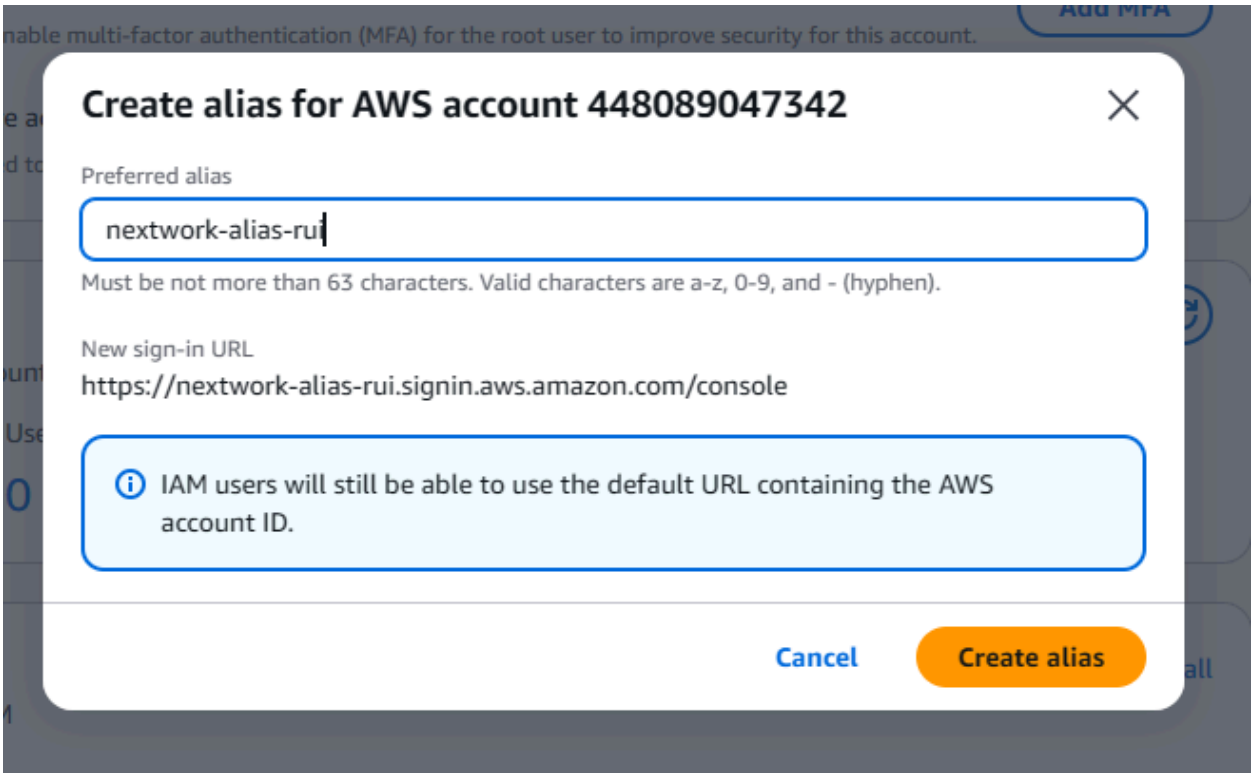




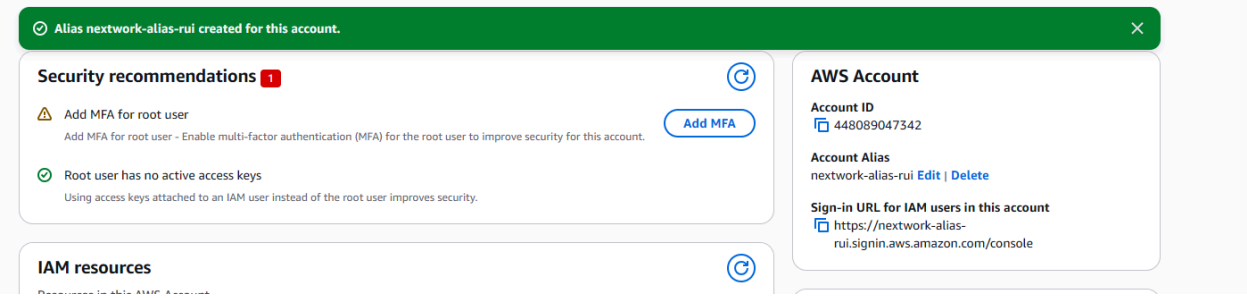
Here we created a Policy



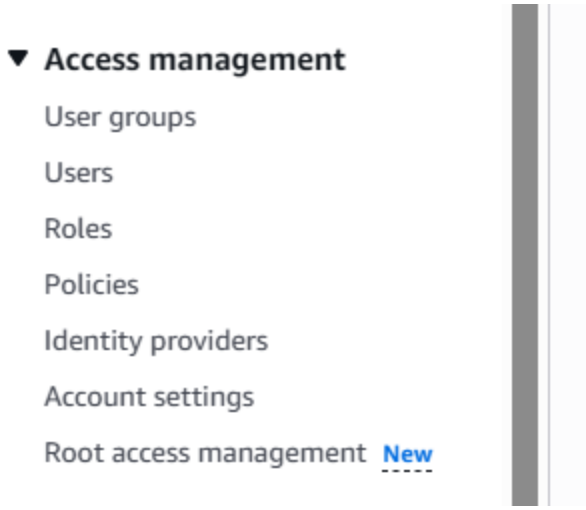
Now go to the dashboard → go to AWS Account → below Account Alias → click on Create



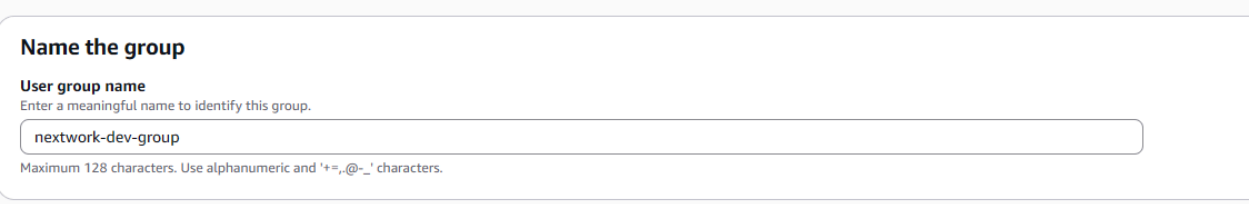
Give an name for it and click create



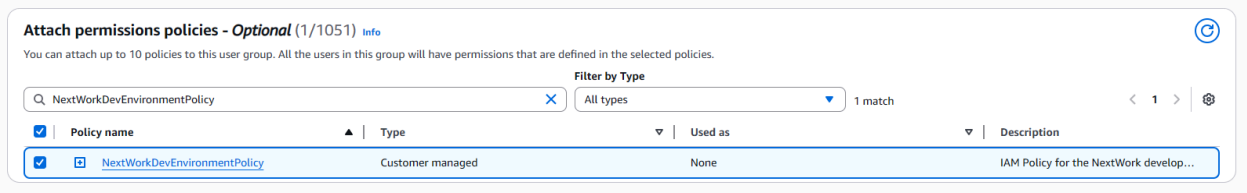
Here we created a alias user



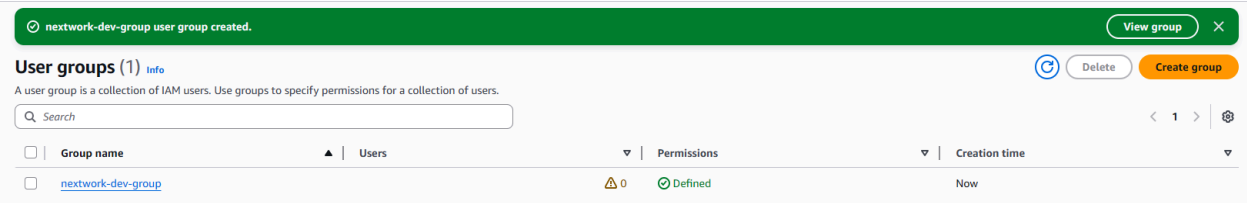
Now go to user groups from the left menu and click create group



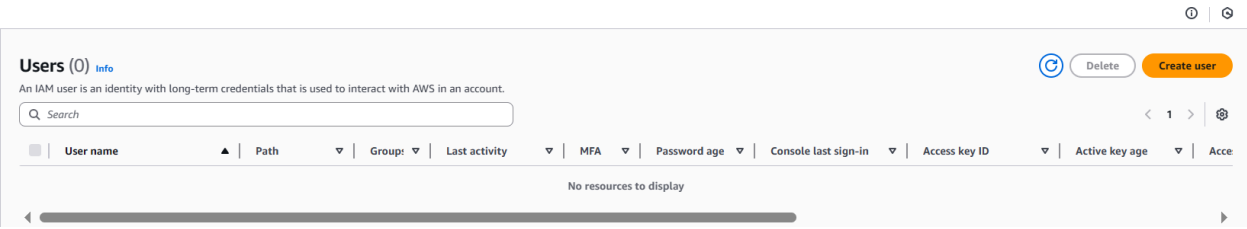
Give name



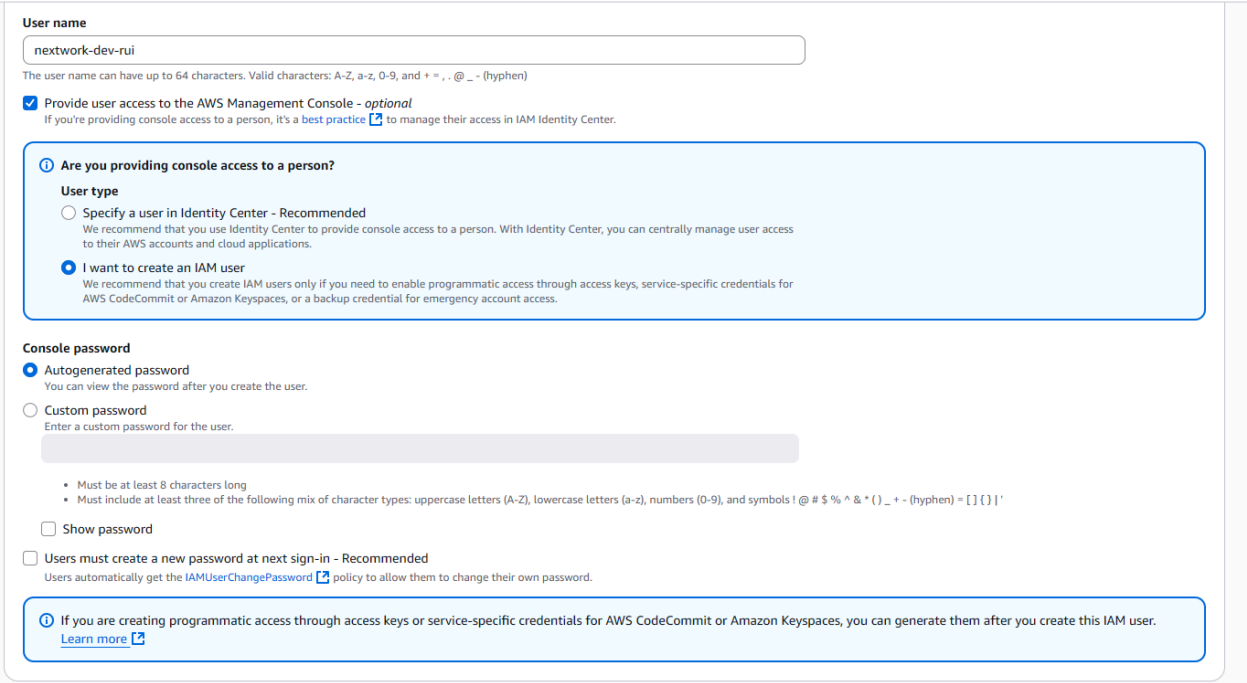
give the policy that we have created and press create



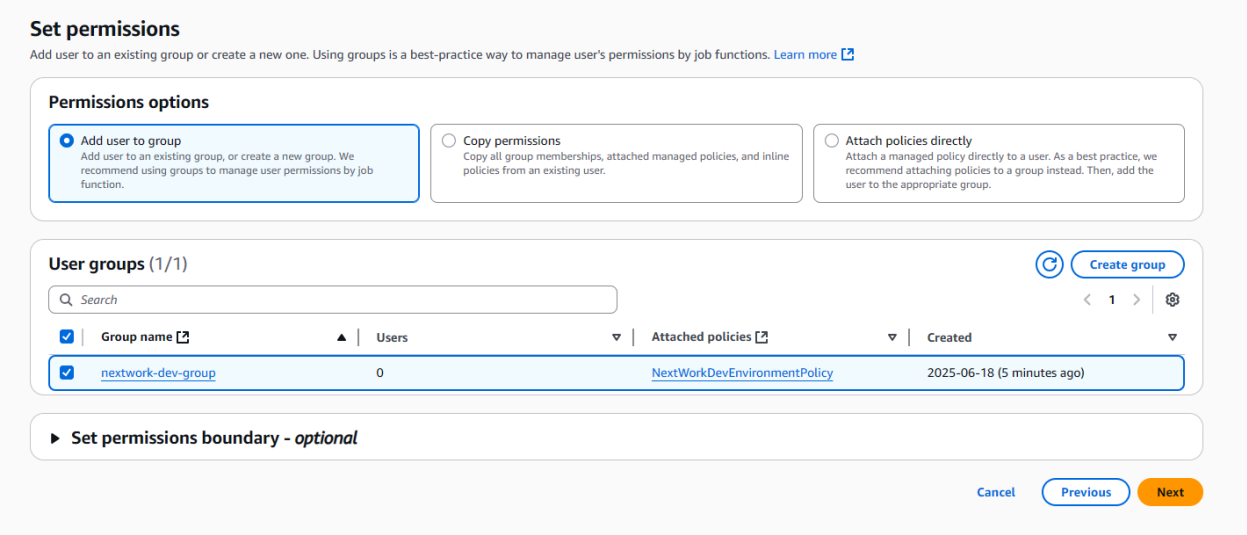
Here we created a user group



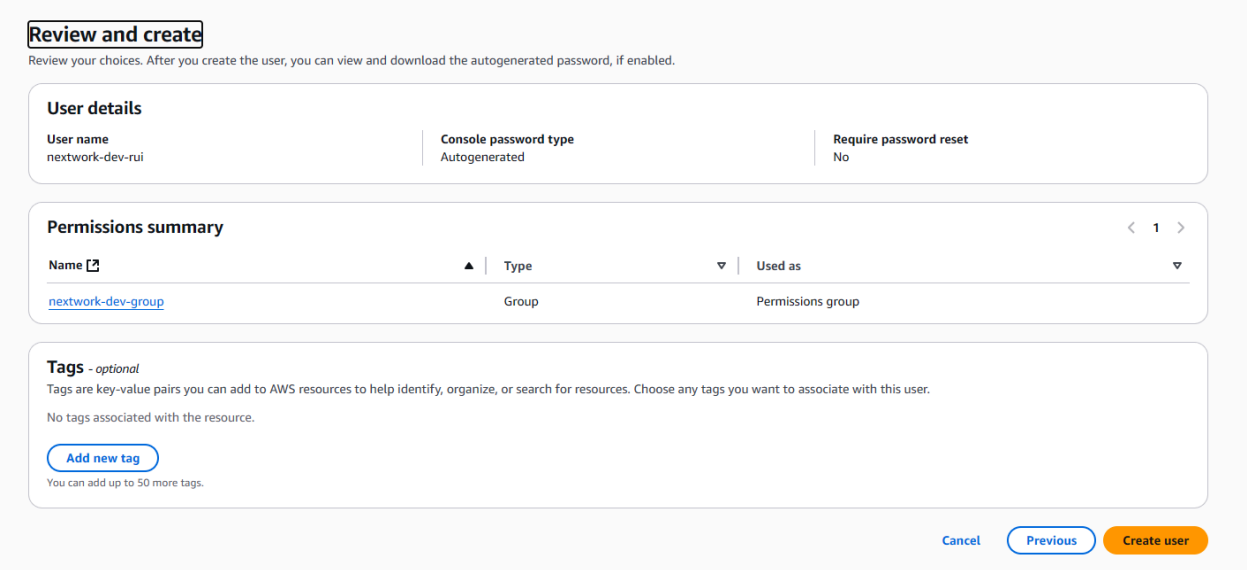
Go to the same side menu and click user → create user



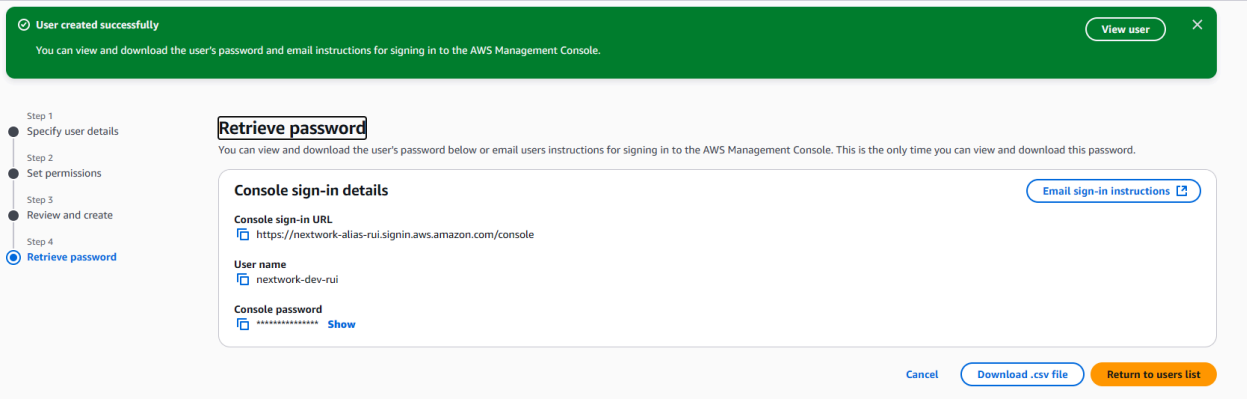
put in all the details show above



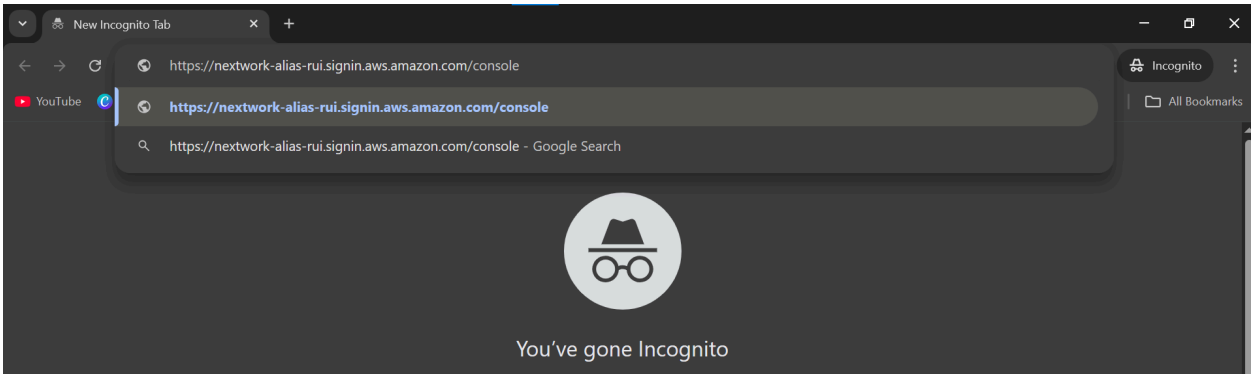
Give the user group we created



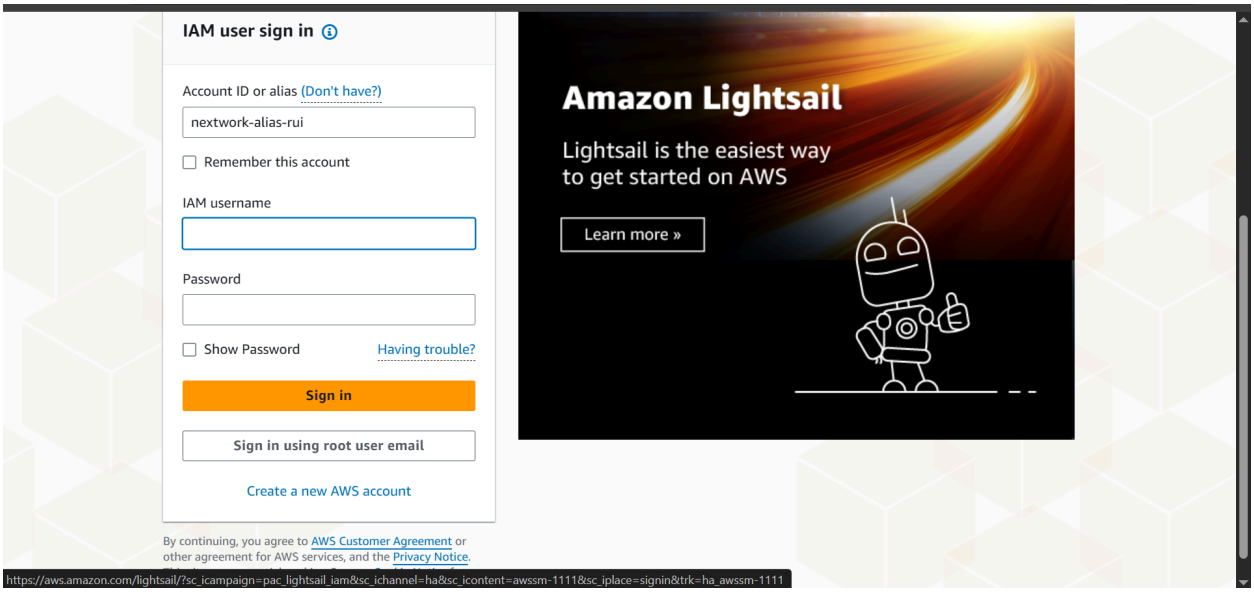
Press create user



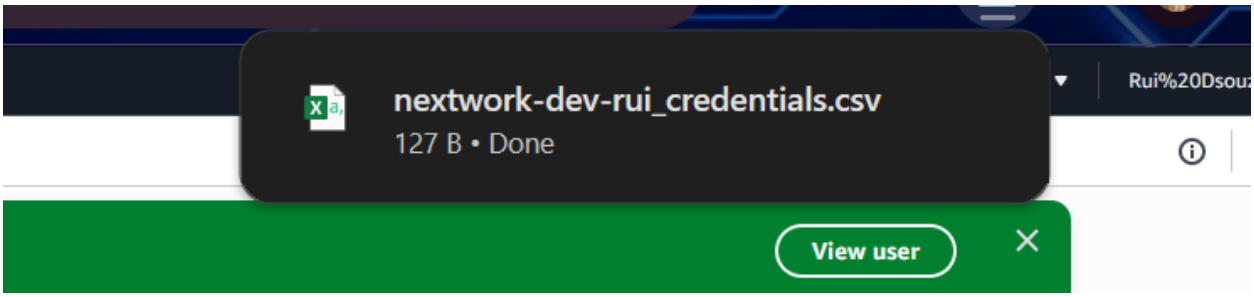
Here we created a user

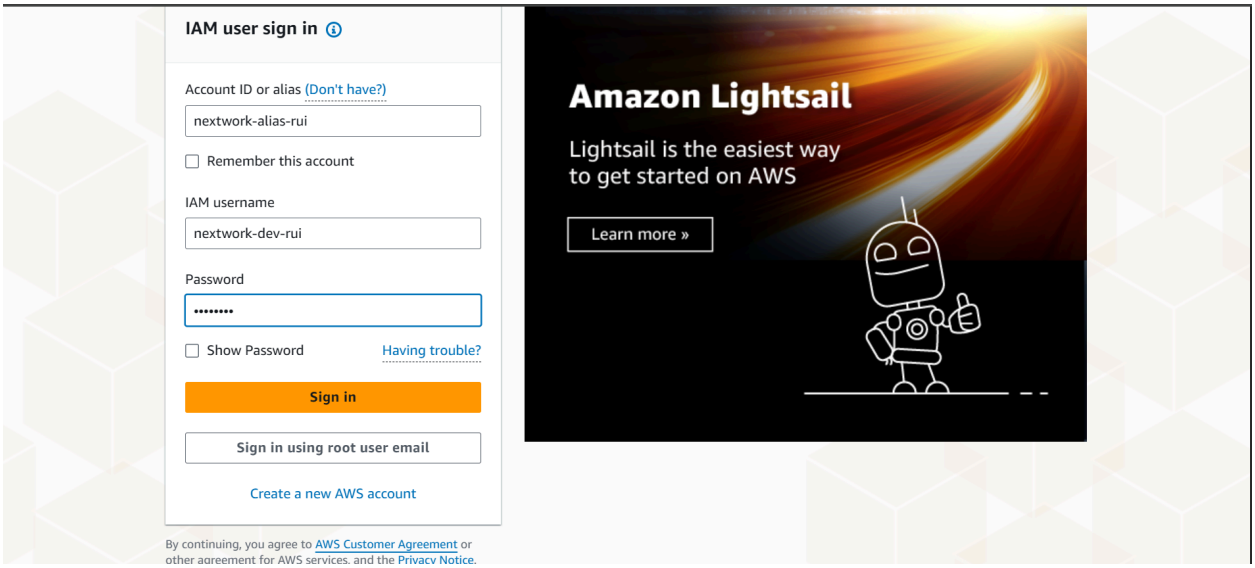


now go to Incognito tab in your browser and paste the Console sign-In URL

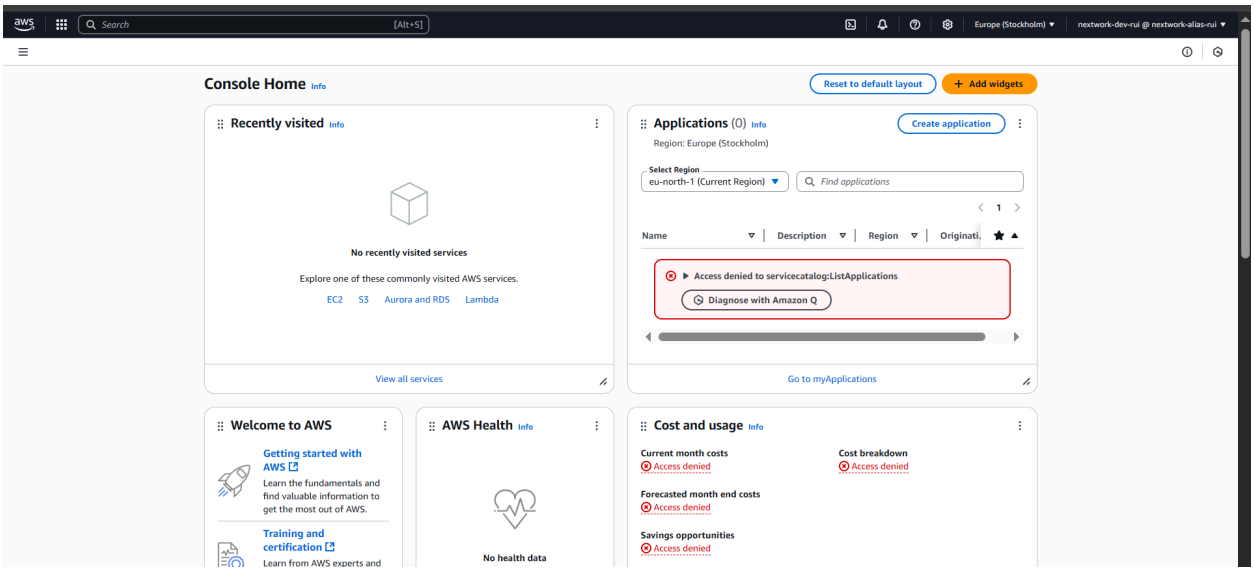


You can use the details given on the porta itself or download the csv file anyone can work

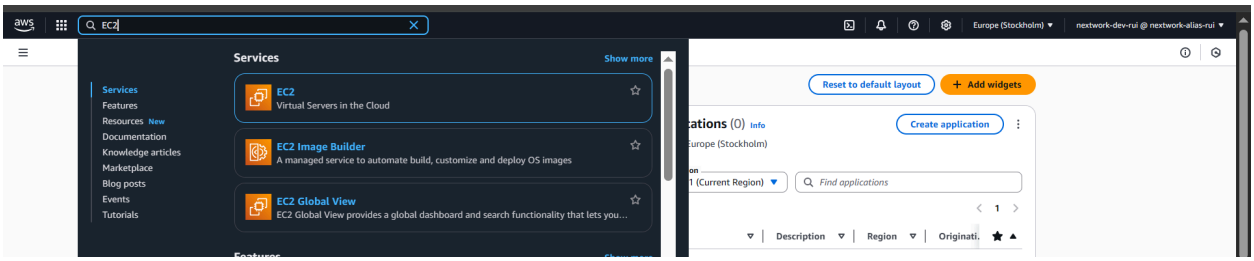




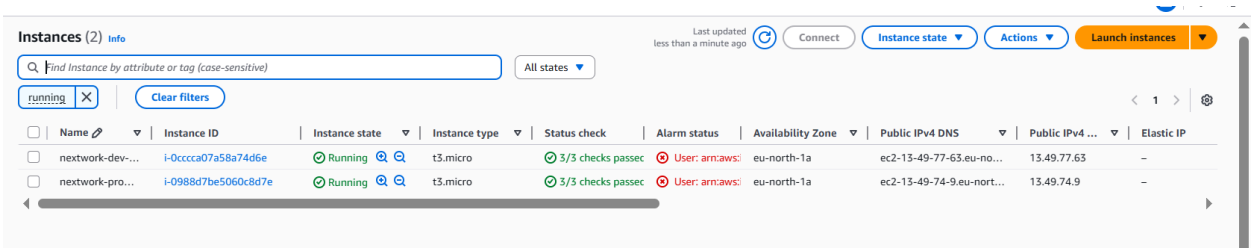
Fill out the login details

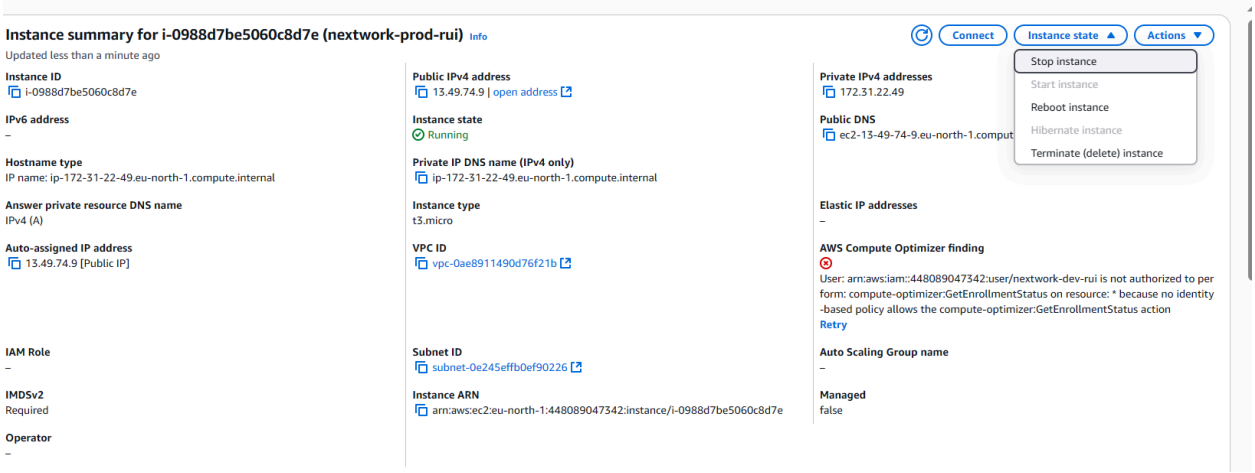


here you will see that there are limited access to you this access is based on the policy we created

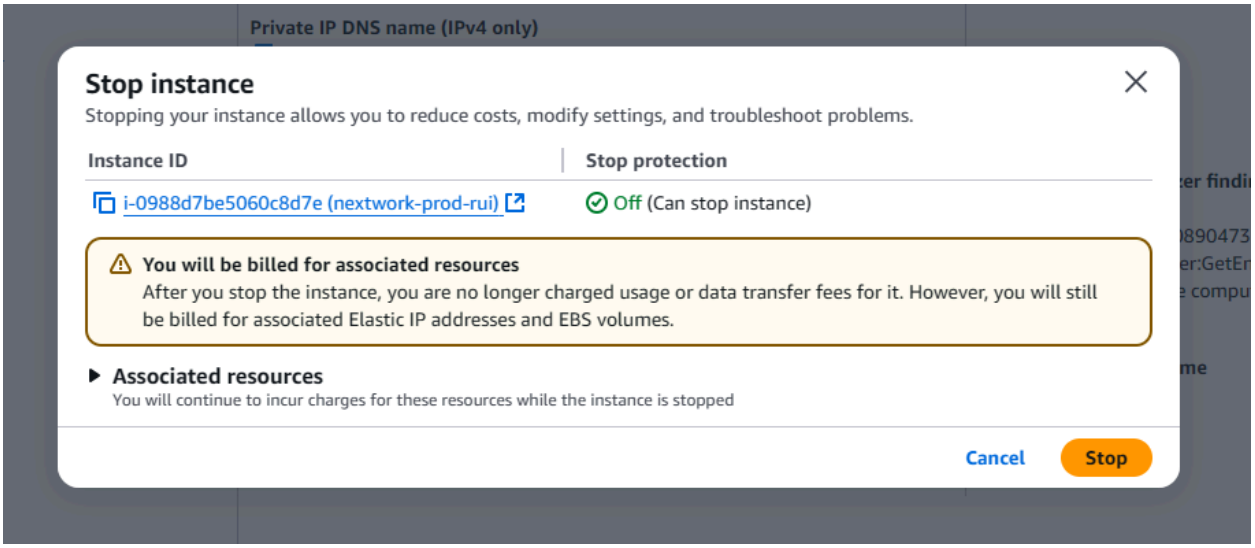


now go to → EC2 → select production instance

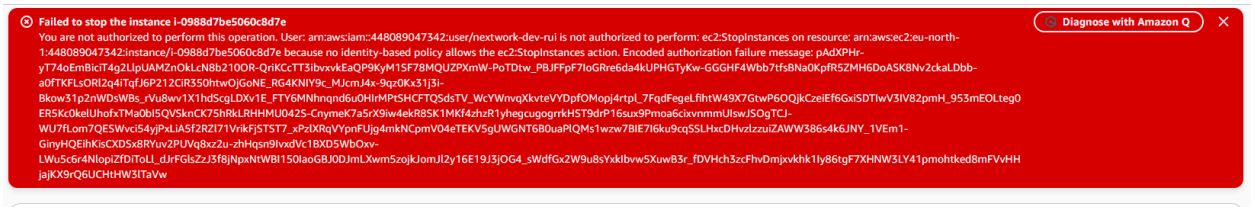




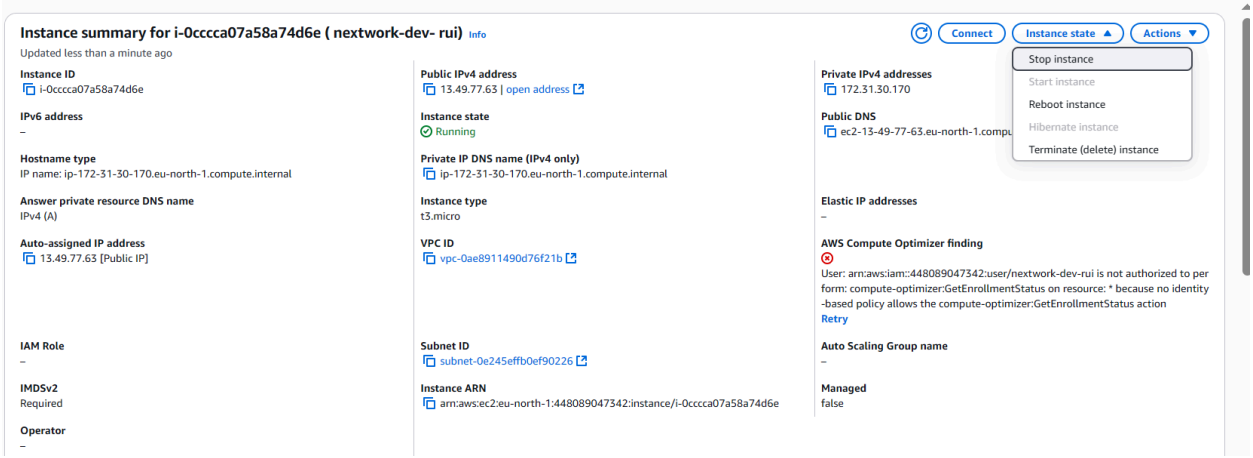
try stopping it



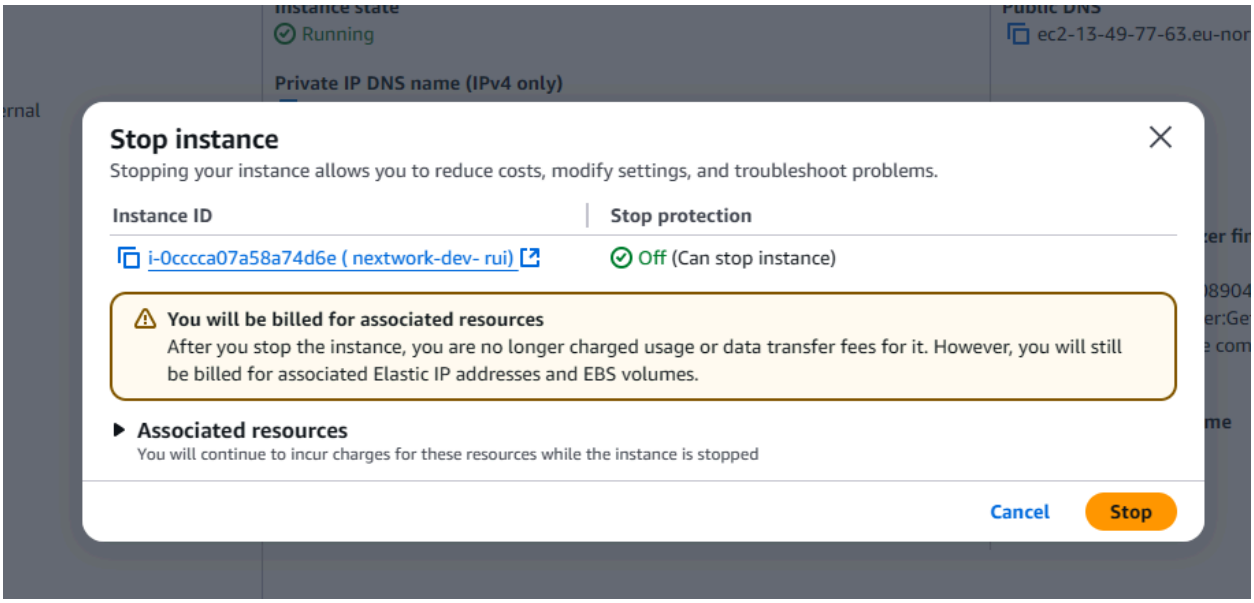
click stop



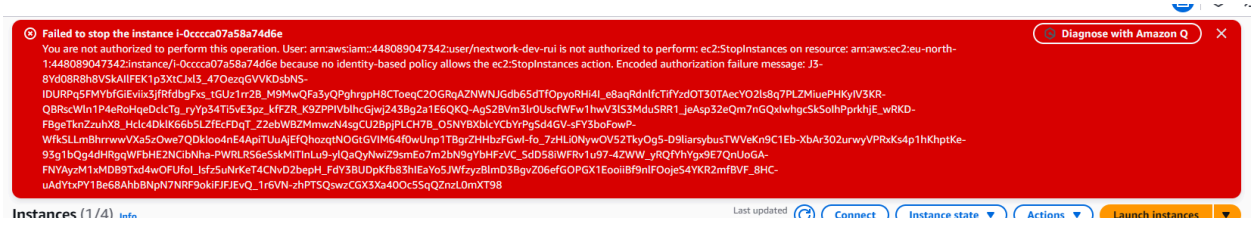
here we can not stop the production instance



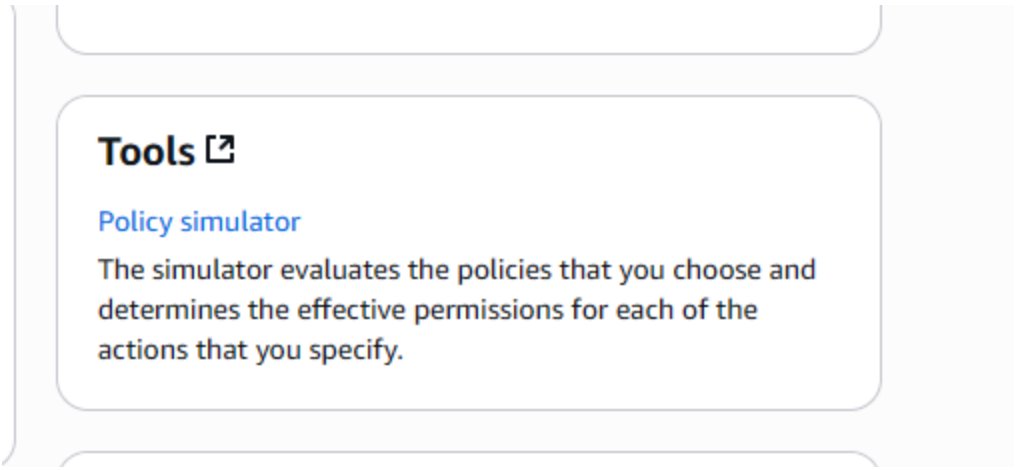
same way try it for development instance



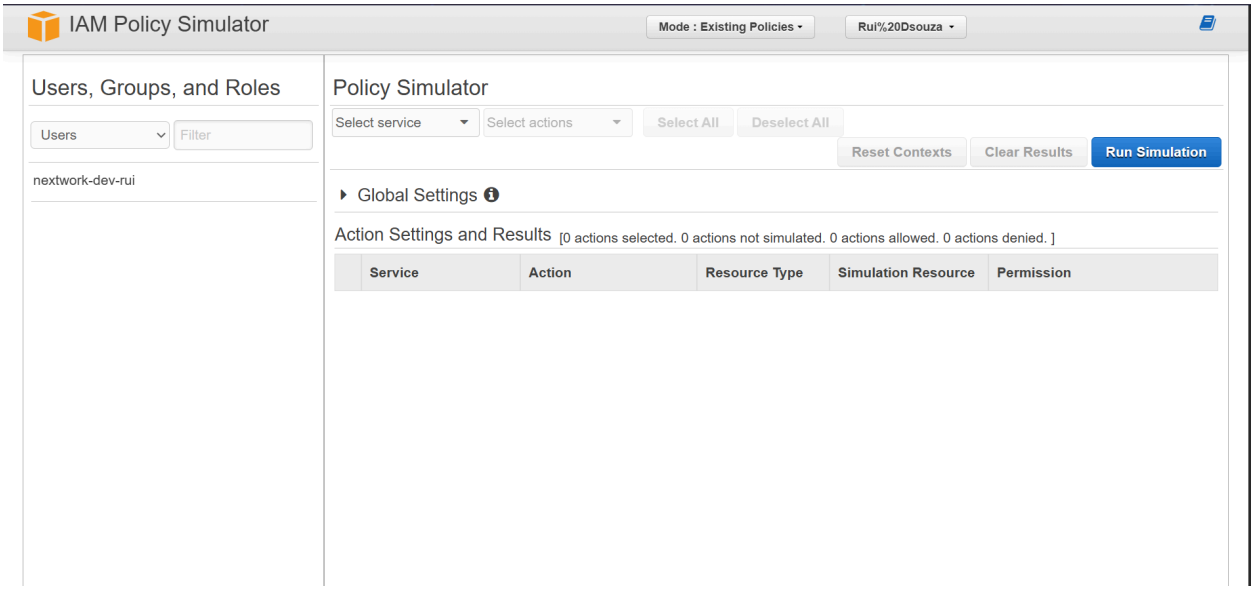
Click stop

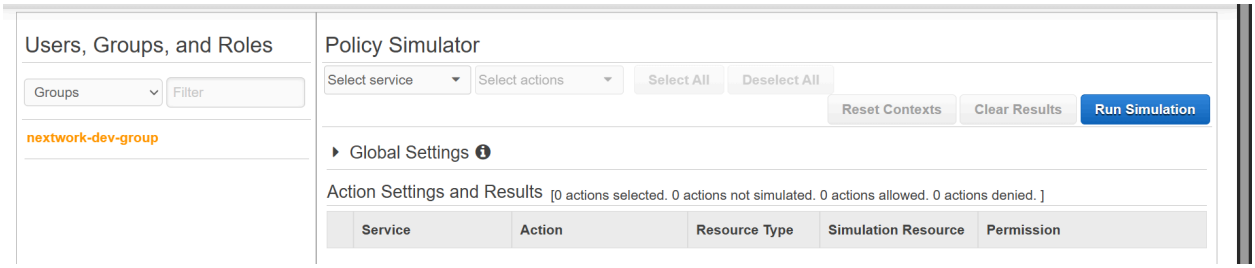


here we can not stop the development instance

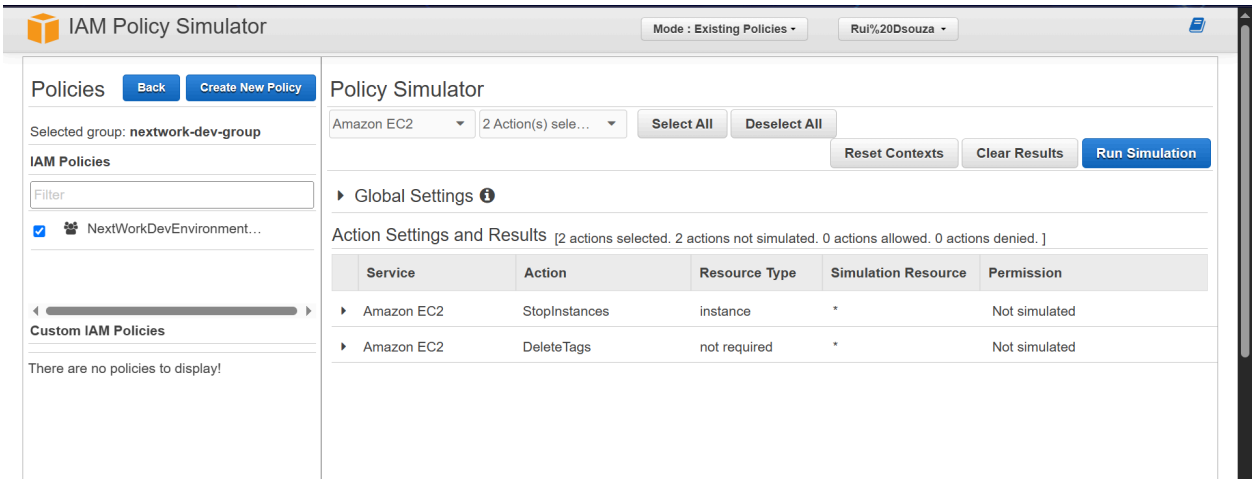


first logout from alias account → Now go to root account → go to IAM dashboard → Policy simulator → click it





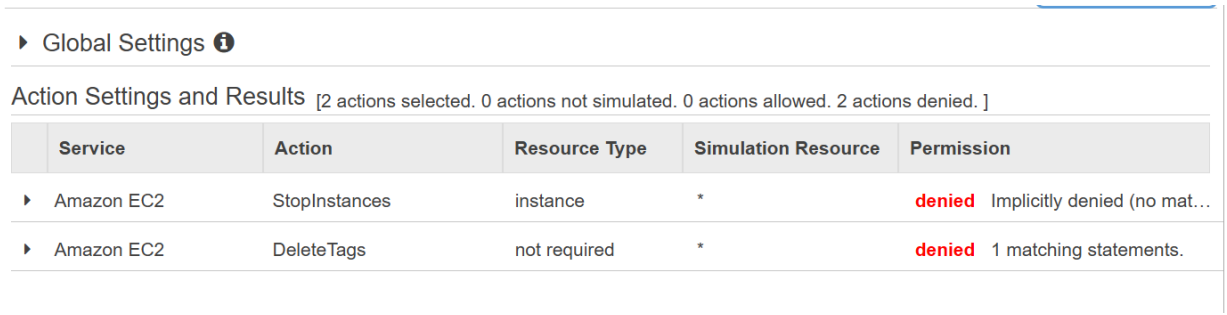
select user and the name



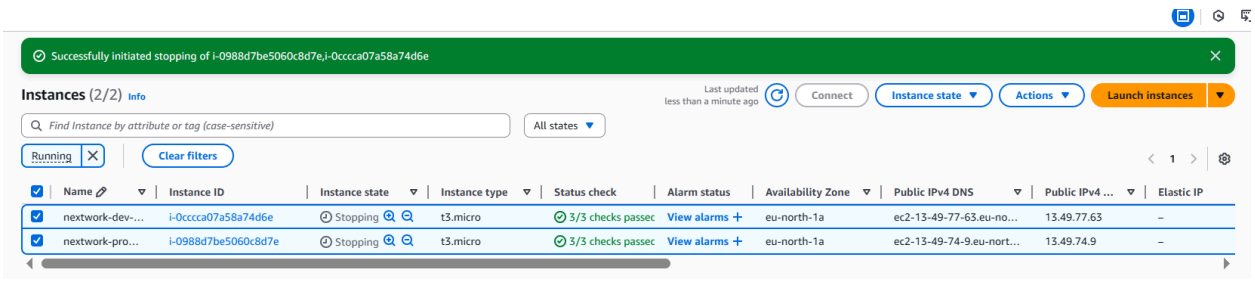
Select Service → EC2

Select action → StopInstance & Delete Tags

Click Run Simulation



Here we can see that the policy say we don't have Permission



Finally stop the instances this is how we use IAM for access management