

# 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.

#### Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

▼ Name and tags [Info](#)

Key [Info](#)

Q Name X

Value [Info](#)

Q network-prod-pavan X

Resource types [Info](#)

Select resource types ▼

Instances X

Remove

Key [Info](#)

Q Env X

Value [Info](#)

Q Production X

Resource types [Info](#)

Select resource types ▼

Instances X

Remove

Add new tag

You can add up to 48 more tags.

Create one Instance.

Change the value → Production.

Create another Instance.

Change the value → Development.

## Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

**▼ Name and tags** [Info](#)

Key [Info](#)

Value [Info](#)

Resource types [Info](#)

Select resource types

Instances

Remove

Key [Info](#)

Value [Info](#)

Resource types [Info](#)

Select resource types

Instances

Remove

Add new tag

You can add up to 48 more tags.

Instances (2/4) [Info](#) Last updated less than a minute ago Connect Instance state Actions Launch instances

All states

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input checked="" type="checkbox"/>	network-dev-...	i-05737f664244aa07b	Running	t3.micro	Initializing	View alarms +	us-east-1c	ec2-54-z
<input type="checkbox"/>	my-ec2-server	i-01f0972b82a53f424	Running	t3.micro	3/3 checks passec	View alarms +	us-east-1c	ec2-54-z
<input type="checkbox"/>	Multi-Instance	i-046383d0125352517	Running	t3.micro	3/3 checks passec	View alarms +	us-east-1c	ec2-54-z
<input checked="" type="checkbox"/>	network-prod-...	i-01ea0aca770c67860	Running	t3.micro	3/3 checks passec	View alarms +	us-east-1c	ec2-54-z

Here we can see that, two Instances are created.

**Identity and Access Management (IAM)**

Dashboard

Access management

User groups

Users

Roles

**Policies**

Identity providers

Account settings

Root access management

Access reports

Resource analysis

Unused access

Analyzer settings

Credential report

Organization activity

**Policies (1377)** [Info](#)

A policy is an object in AWS that defines permissions.

Filter by Type

All types

Policy name

Type

Used as

Description

<input type="radio"/>	<a href="#">AccessAnalyzerServiceRole...</a>	AWS managed	None	Allow Access Analyzer to analyze resou...
<input type="radio"/>	<a href="#">AdministratorAccess</a>	AWS managed - job function	None	Provides full access to AWS services an...
<input type="radio"/>	<a href="#">AdministratorAccess-Amplify</a>	AWS managed	None	Grants account administrative permisi...
<input type="radio"/>	<a href="#">AdministratorAccess-AWS...</a>	AWS managed	None	Grants account administrative permisi...
<input type="radio"/>	<a href="#">AIOpsAssistantPolicy</a>	AWS managed	None	Provides ReadOnly permissions requir...
<input type="radio"/>	<a href="#">AIOpsConsoleAdminPolicy</a>	AWS managed	None	Grants full access to Amazon AI Opera...
<input type="radio"/>	<a href="#">AIOpsOperatorAccess</a>	AWS managed	None	Grants access to the Amazon AI Opera...
<input type="radio"/>	<a href="#">AIOpsReadOnlyAccess</a>	AWS managed	None	Grants ReadOnly permissions to the A...
<input type="radio"/>	<a href="#">AlexaForBusinessDeviceSe...</a>	AWS managed	None	Provide device setup access to AlexaFo...
<input type="radio"/>	<a href="#">AlexaForBusinessFullAccess</a>	AWS managed	None	Grants full access to AlexaForBusiness ...
<input type="radio"/>	<a href="#">AlexaForBusinessGateway...</a>	AWS managed	None	Provide gateway execution access to A...

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

Click on Create Policy.

**Specify permissions** [Info](#)

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

**Policy editor** Visual JSON Actions ▼ □

▼ **Select a service**

Specify what actions can be performed on specific resources in a service.

**Service**

Choose a service ▼

+ Add more permissions

Cancel Next

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

**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": "*"
26    }
27  ]
28 }
```

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**

VisualJSON

```
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": "*"
26    }
27  ]
28 }
```

Edi  
Se  
I  
|  
(

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

**Description - optional**  
Add a short explanation for this policy.  
  
Maximum 1,000 characters. Use alphanumeric and '+,=, @, \_' characters.

Give the Permissions for the Policy.

**NetworkDevEnvPolicy** [Info](#)

EditDelete

IAM Policy for the Network Development Environment

**Policy details**

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

Permissions

Entities attachedTagsPolicy versions (1)Last Accessed

**Permissions defined in this policy** [Info](#)

EditSummaryJSON

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

**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.


 **Policy NetworkDevEnvPolicy created.**

### NetworkDevEnvPolicy [Info](#)

IAM Policy for the Network Development Environment

[Edit](#) [Delete](#)

**Policy details**

Type Customer managed	Creation time July 17, 2025, 10:11 (UTC+05:30)	Edited time July 17, 2025, 10:11 (UTC+05:30)	ARN  am: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

**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

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

## AWS Account

**Account ID**  
 233720366258

**Account Alias**  
[Create](#)

**Sign-in URL for IAM users in this account**  
 <https://233720366258.signin.aws.amazon.com/console>

Task-4 : Cloud Security Implementation

6 | Page

## Create alias for AWS account 233720366258

Preferred alias

network-alias-pavan

Must be not more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen).

New sign-in URL

https://network-alias-pavan.signin.aws.amazon.com/console

IAM users will still be able to use the default URL containing the AWS account ID.

Cancel

Create alias

Give the name for preferred alias and click create.

✓ Alias network-alias-pavan created for this account.

New access analyzers available

Access Analyzer now analyzes internal access patterns to your critical resources within a single account or across your entire organization.

Create new analyzer

IAM Dashboard

Info

Security recommendations 0

✓

Root user has MFA

Having multi-factor authentication (MFA) for the root user improves security for this account.

✓

Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

AWS Account

Account ID

233720366258

Account Alias

network-alias-pavan [Edit](#) [Delete](#)

Sign-in URL for IAM users in this account

<https://network-alias-pavan.signin.aws.amazon.com/console>

Here we Created an alias user.

Task-4 : Cloud Security Implementation

7 | Page

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

## Create user group

### Name the group

#### User group name

Enter a meaningful name to identify this group.

network-dev-group

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

Give the name for the user group.

**Attach permissions policies - Optional** (1/1065) [Info](#)

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type:  All types 22 matches

	Policy name	Type	Used as	Description
<input type="checkbox"/>	AWSQuickSetupDevOps...	AWS managed	None	The AWSQuickSetupDevOpsGuruPerm...
<input checked="" type="checkbox"/>	NetworkDevEnvPolicy	Customer managed	None	IAM Policy for the Network Developme...

[Cancel](#) [Create user group](#)

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

network-dev-group user group created. [View group](#)

**User groups** (1) [Info](#) [Delete](#) [Create group](#)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	<a href="#">network-dev-group</a>	0	Defined	Now

The User Group was Created.

**Users** (0) [Info](#) [Delete](#) [Create user](#)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

	User name	Path	Group	Last activity	MFA	Password age	Console last sign-in
No resources to display							

Go to side menu and click user → Create User.



## User details

### User name

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ \_ - (hyphen)

### ☒ Provide user access to the AWS Management Console - *optional*

If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

#### Are you providing console access to a person?

##### User type

###### ☐ Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

###### ☒ I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

### Console password

#### ☒ Autogenerated password

You can view the password after you create the user.

#### ☐ Custom password

Enter a custom password for the user.


- Must be at least 8 characters long

- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & \* ( ) \_ + = (hyphen) = [ ] { } ' "

#### ☐ Show password

### ☒ Users must create a new password at next sign-in - Recommended

Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

 If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Give all the details like shown above.

## Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

### Permissions options

#### ☒ Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

#### ☐ Copy permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.

#### ☐ Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

### User groups (1/1)



Create group

Search

< 1 > ⚙

<input checked="" type="checkbox"/>	Group name	Users	Attached policies	Created
<input checked="" type="checkbox"/>	network-dev-group	0	NetworkDevEnvPolicy	2025-07-17 (4 minutes ago)

### ► Set permissions boundary - *optional*

Cancel

Previous

Next

Give the User group we created.

## Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

**User details**

User name  
network-dev-pavan

Console password type  
Autogenerated

Require password reset  
Yes

**Permissions summary**

< 1 >

Name	Type	Used as
<a href="#">IAMUserChangePassword</a>	AWS managed	Permissions policy
<a href="#">network-dev-group</a>	Group	Permissions group

**Tags - optional**  
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.  
No tags associated with the resource.  
[Add new tag](#)  
You can add up to 50 more tags.

[Cancel](#) [Previous](#) [Create user](#)

After giving all details click Create User.

**User created successfully**  
You can view and download the user's password and email instructions for signing in to the AWS Management Console.  
[View user](#)

Step 1  
Specify user details

Step 2  
Set permissions

Step 3  
Review and create

Step 4  
**Retrieve password**

**Retrieve password**

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

**Console sign-in details**

[Email sign-in instructions](#)

**Console sign-in URL**  
 <https://network-alias-pavan.signin.aws.amazon.com/console>

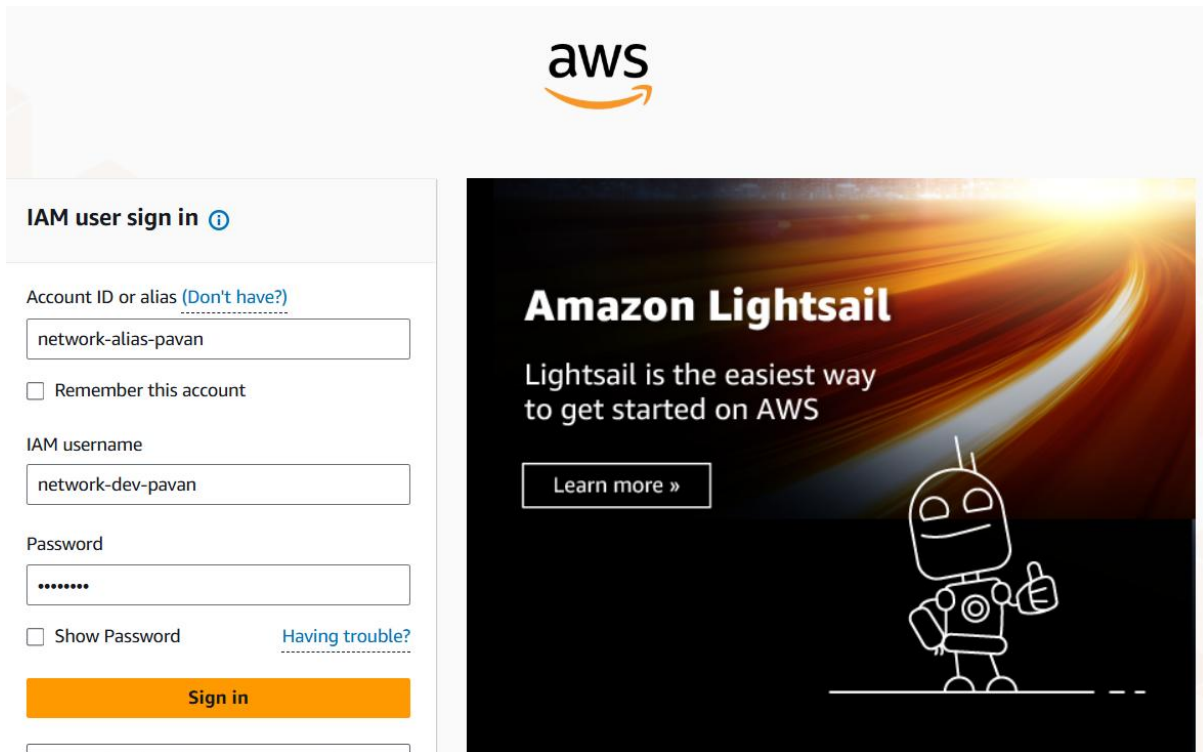
**User name**  
 network-dev-pavan

**Console password**  
 \*\*\*\*\* [Show](#)

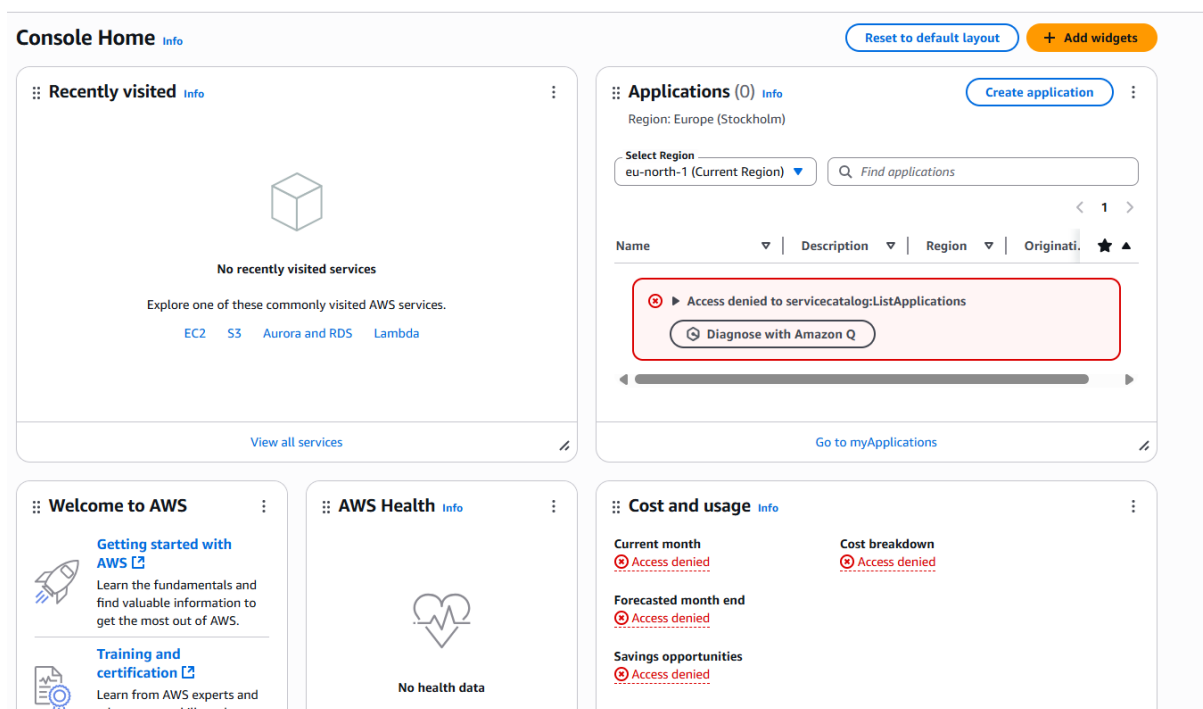
[Cancel](#) [Download .csv file](#) [Return to users list](#)

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.

Instances (1/4) Info								
Find Instance by attribute or tag (case-sensitive)					All states			
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	
<input type="checkbox"/>	network-dev-...	i-05737f664244aa07b	Running	t3.micro	3/3 checks passed	User: arn:aws:	us-east-1c	
<input type="checkbox"/>	my-ec2-server	i-01f0972b82a53f424	Running	t3.micro	3/3 checks passed	User: arn:aws:	us-east-1c	
<input type="checkbox"/>	Multi-Instance	i-046383d0125352517	Running	t3.micro	3/3 checks passed	User: arn:aws:	us-east-1c	
<input checked="" type="checkbox"/>	network-prod-...	i-01ea0aca770c67860	Running	t3.micro	3/3 checks passed	User: arn:aws:	us-east-1c	

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

Try to Stop the Instance.

### Stop instance

Stopping your instance allows you to reduce costs, modify settings, and troubleshoot problems.

Instance ID

Stop protection

[i-01ea0aca770c67860 \(network-prod-pavan\)](#)

Off (Can stop instance)

**You will be billed for associated resources**

After you stop the instance, you are no longer charged usage or data transfer fees for it. However, you will still be billed for associated Elastic IP addresses and EBS volumes.

**Associated resources**

You will continue to incur charges for these resources while the instance is stopped

Cancel
Stop

Click the Stop Button.

**Failed to stop the instance i-01ea0aca770c67860**

You are not authorized to perform this operation. User: arn:aws:iam::233720366258:user/network-dev-pavan is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-1:233720366258:instance/i-01ea0aca770c67860 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: VvCX47kAWi48hrqdpkg0HNThqQ05iy0AwfCYeJ2boblPLBFENm65POh4ZUhwgzb1qvSugEKEE0g7-TUBFIO6z-aJO9\_YDhulRimGC3JAid4PkizHnNrDbmgR1e9bE3r7-FjN1XqGrykOGYr\_QPMJe6ZQ2mptHlXNIORZOiUtlY5NbnCuybfzlpbuPT5MVfBswDQ-OR5u7SNDosikG3SwDMMXivTb7QmjXHNZtUJvIvDlMapCz0n79ad2Lz1B5ra4RLqPsnCV9sk4dp-MsjfSCDzfXhItOreWxB2xnbPtGuu0Am2lrEgdN2byJD9ul2gyglp4-jwtQ6941PP71VQrWcU00FJ9oGJG4z3LrR5rjJGkmQ9IHwEAsc60tFUDurJIT6ce2gEkvozHP1k9eE-IFuLhLiuW4Pp19d4H20-wHJCvg9UArFTihJU-r8hnU57gHAqO63fzgqgipv-9lxDtlgo3FDj6TxDFo4NnbGWuuy53DaOadA-rRW7miP-7a1OxPGVxDZlyff6faTmEbdlRlqkX9lcoBlHNEQfW/HAM4HvQX0deUpNf9yeMlxQxCW8XfdMhd6XwtJ31RKP\_8z-25\_Uk2NUBt4Jd1bzRqef\_QWai4WebyP8nsuKTqJR-BUFVqL8EZ2-z6rQuQwlmS9-SdJJCEJcaQsxK9PMYJLppKYdVA-iL-Mnb-5t4MGTeZOM04OkCl4z8EGEmWM-fKRvOjz7boDUd3oocY9-h6VtT1J0gS2ISZwqlafwEzAhsGpITp52fm8ud2w33tSz8yWKLUXe7d4NEan2CrVDmIClEt1fnFnn5tBxKlKVSsbFtHTQRH0aVrOkuM78layB85nxhP0NXG61qbnvDULhjatLxLF6y7cnlBgE-0ZyFA

[Diagnose with Amazon Q](#)

We cannot try to stop the Production Instance.

**Instance summary for i-05737f664244aa07b (network-dev-pavan)** [Info](#)

Updated less than a minute ago

<b>Instance ID</b> <a href="#">i-05737f664244aa07b</a>	<b>Public IPv4 address</b> <a href="#">54.242.13.95</a>   <a href="#">open address</a>	<b>Actions</b> <ul style="list-style-type: none"> <li>Stop instance</li> <li>Start instance</li> <li>Reboot instance</li> <li>Hibernate instance</li> <li>Terminate (delete) instance</li> </ul>
<b>IPv6 address</b> -	<b>Instance state</b> <span>Running</span>	
<b>Hostname type</b> IP name: ip-172-31-23-232.ec2.internal	<b>Private IP DNS name (IPv4 only)</b> <a href="#">ip-172-31-23-232.ec2.internal</a>	
<b>Answer private resource DNS name</b> IPv4 (A)	<b>Instance type</b> t3.micro	
<b>Auto-assigned IP address</b> <a href="#">54.242.13.95</a> [Public IP]	<b>VPC ID</b> <a href="#">vpc-08e22c0f8f3388754</a>	
<b>IAM Role</b> -	<b>Subnet ID</b> <a href="#">subnet-03e0a3db4a7ba8801</a>	<b>Private IPv4 address</b> <a href="#">172.31.23.2</a>
		<b>Public DNS</b> <a href="#">ec2-54-242-13-95.compute-1.amazonaws.com</a>   <a href="#">open address</a>
		<b>Elastic IP addresses</b> -
		<b>AWS Compute Optimizer finding</b> User: arn:aws:iam::233720366258:user/network-dev-pavan is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: * because no identity-based policy allows the compute-optimizer:GetEnrollmentStatus action <a href="#">Retry</a>
		<b>Auto Scaling Group name</b> -

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

Try to Stop the Instance.

**Stop instance** ×

Stopping your instance allows you to reduce costs, modify settings, and troubleshoot problems.

**Instance ID** | **Stop protection**

[i-05737f664244aa07b \(network-dev-pavan\)](#) | Off (Can stop instance)

**⚠ You will be billed for associated resources**

After you stop the instance, you are no longer charged usage or data transfer fees for it. However, you will still be billed for associated Elastic IP addresses and EBS volumes.

▶ **Associated resources**

You will continue to incur charges for these resources while the instance is stopped

[Cancel](#)
[Stop](#)

Click on Stop Button.

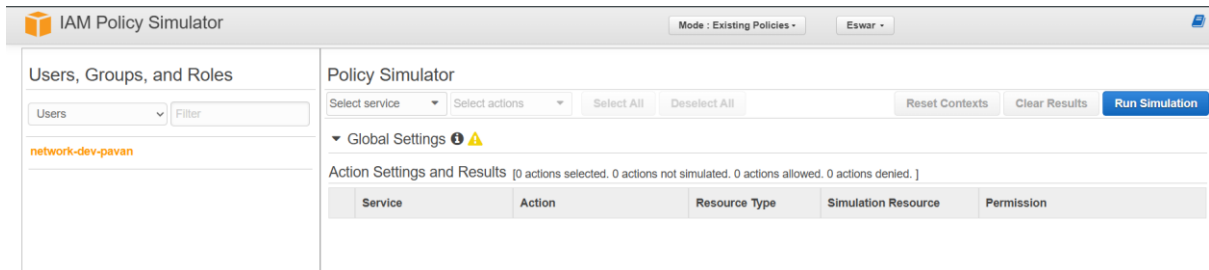
**⚠ Failed to stop the instance i-05737f664244aa07b** [Diagnose with Amazon Q](#) ×

You are not authorized to perform this operation. User: arn:aws:iam::233720366258:user/network-dev-pavan is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-1:233720366258:instance/i-05737f664244aa07b because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message:

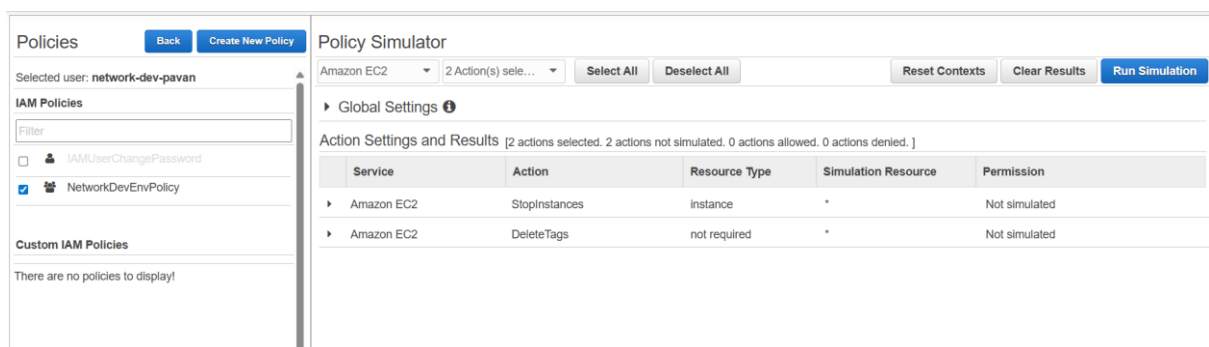
3nIQa4QaJLPaj9VnKqHZRTthKqOx\_C4veyNjx4oUYolVlqHGL\_x96HvBsrYZ3AWWueC13AZI5mA91APd7L4viVIVx5MOz\_j2YRGDP2ICQ47Df0uFDXXfDHTGzxA77fdCqUuKkoHYCnJA8DHRPU-pQK2Vli8ftvgj1tuswfqSvXGekmHBJNynrbZSIK260gGcNonHE9ip012DQX5PvDzcbv11ITINlqxvR9IKCsHtE04pIloVhHLmRpoD9IojPUD4GMYPIZ5JphyU5g8KP\_rb9BSx5DGeMGWycvFUSyE-79fHrhDosSIWjg7Kj1SxR9sQbhZpkjCQ-eE\_LyJJHRaFcVSWeCToan1I\_Pxl4\_u4AP2VwsOYXSF\_qxgzBWL56tmkhLLusugumLrqjG6xyUVVZ3V--JGQulmZz0oaTRVC9ciF2c3fmOZy0wud6ZmymIv8kPCbI\_VPSXeNPpUaujoDID1IxhaGutzymeT11RuJ\_DU9bwphekZF\_qtEPPC87LxlgIA1JU-pab5xE-tev6VIVJxt5qj\_D7oqauVFFAtCT\_wg\_6foCw2AK5aFVb4YQI8Q9o1Dd1v5ZGHcdJ9DjC6HQ8QYEEr1FcDjcTp8YjoUJTJmww\_gYrcYPrZlIX9JDc6o0-rm4ZWRLaPoQua3WBW96JMtZjIri4TYcucKU\_gv9QJWhgY9JHA3eSq4h1vr740447VydeKTFvIKztMUUrqGPoZ6QGNRjsk2pHHBozAlziKz5-STKjeyw2pLZRREbcKwmTzaGon2nWcnXMXvEzn\_W3FBWx9V9OdapJvGNgCZpqa0RrUwoYv\_ja7IP6BWFVZV2nKVSDeTQbhnW3XECmr0XeaQhffWMkBX-UoVE\_y9GSsnr13nOZYAHA

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.

Successfully initiated stopping of i-01ea0aca770c67860

**Instance summary for i-01ea0aca770c67860 (network-prod-pavan)** Info

Updated less than a minute ago

**Instance ID**  
i-01ea0aca770c67860

**IPv6 address**  
-

**Hostname type**  
IP name: ip-172-31-16-227.ec2.internal

**Answer private resource DNS name**  
IPv4 (A)

**Public IPv4 address**  
54.226.24.95 | open address

**Instance state**  
Running

**Private IP DNS name (IPv4 only)**  
ip-172-31-16-227.ec2.internal

**Instance type**  
t3.micro

**Private IPv4 addresses**  
172.31.16.227

**Public DNS**  
ec2-54-226-24-95.compute-1.amazonaws.com | open address

**Elastic IP addresses**  
-

Connect Instance state Actions

Successfully initiated stopping of i-05737f664244aa07b

**Instance summary for i-05737f664244aa07b (network-dev-pavan)** Info

Updated less than a minute ago

**Instance ID**  
i-05737f664244aa07b

**IPv6 address**  
-

**Hostname type**  
IP name: ip-172-31-23-232.ec2.internal

**Answer private resource DNS name**  
IPv4 (A)

**Public IPv4 address**  
54.242.13.95 | open address

**Instance state**  
Stopping

**Private IP DNS name (IPv4 only)**  
ip-172-31-23-232.ec2.internal

**Instance type**  
t3.micro

**Private IPv4 addresses**  
172.31.23.232

**Public DNS**  
ec2-54-242-13-95.compute-1.amazonaws.com | open address

**Elastic IP addresses**  
-

Connect Instance state Actions

Finally We, have Stopped the Production and Development Instances.

Instances (2/4) Info

Connect Instance state Actions Launch instances

Find Instance by attribute or tag (case-sensitive) All states

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input checked="" type="checkbox"/>	network-dev...	i-05737f664244aa07b	Stopped	t3.micro	-	View alarms +	us-east-1c	-
<input type="checkbox"/>	my-ec2-server	i-01f0972b82a53f424	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1c	ec2-54-2...
<input type="checkbox"/>	Multi-Instance	i-046383d0125352517	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1c	ec2-54-1...
<input checked="" type="checkbox"/>	network-pr...	i-01ea0aca770c67860	Stopped	t3.micro	-	View alarms +	us-east-1c	-

This is how we use IAM for Access Management.