



# 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

The screenshot shows the 'Name and tags' section of the AWS IAM console. It contains two tag entries:

Key	Value	Resource types	Action
Name	nextwork-prod-rui	Instances	Remove
Env	Production	Instances	Remove

At the bottom, there is an 'Add new tag' button and a note: 'You can add up to 48 more tags.'

Here we need to add the Tag Production

▼ **Name and tags** [Info](#)

Key [Info](#) Value [Info](#) Resource types [Info](#)

Q Name X Q network-dev- rui X Select resource types Remove

Instances X

Key [Info](#) Value [Info](#) Resource types [Info](#)

Q Env X Q Development X Select resource types Remove

Instances X

[Add new tag](#)

You can add up to 48 more tags.

Here we need to add the Tag Development

Find Instance by attribute or tag (case-sensitive) All states 1 minute ago

Running X Clear filters

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
<input type="checkbox"/>	network-dev-...	i-0ccca07a58a74d6e	Running	t3.micro	Initializing	<a href="#">View alarms +</a>	eu-north-1a	ec2-13-49-77-63.eu-no...	13.49.77.63	-
<input type="checkbox"/>	network-pro...	i-0988d7be5060c8d7e	Running	t3.micro	3/3 checks pass	<a href="#">View alarms +</a>	eu-north-1a	ec2-13-49-74-9.eu-nort...	13.49.74.9	-

Here we create the 2 instances

aws IAM

Identity and Access Management

Search IAM

Dashboard

▼ Access management

User groups

Users

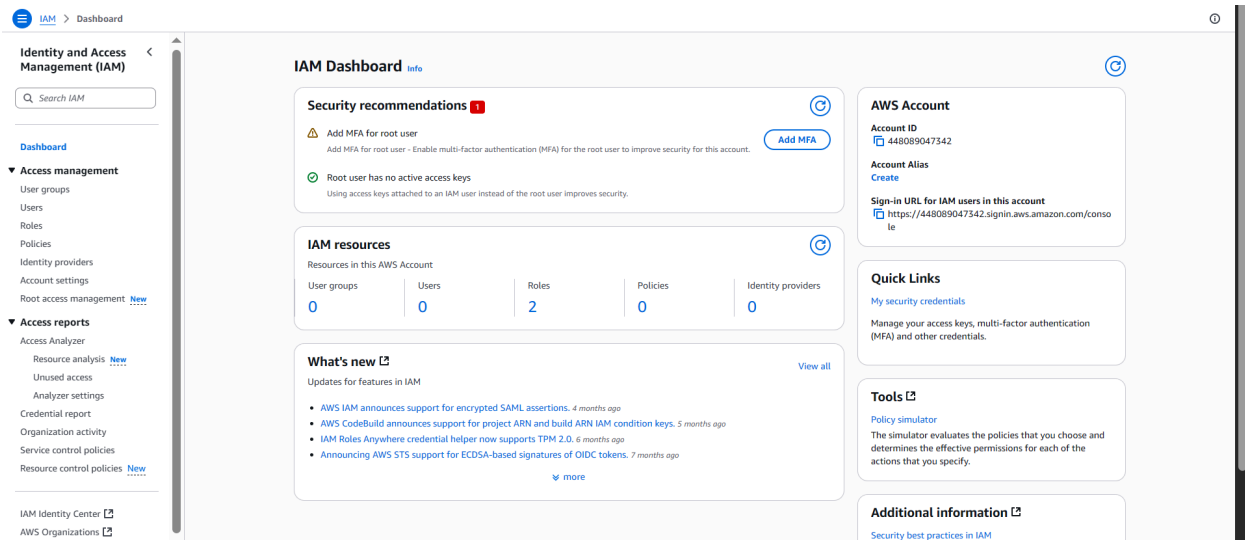
Roles

**Services** [Show more](#)

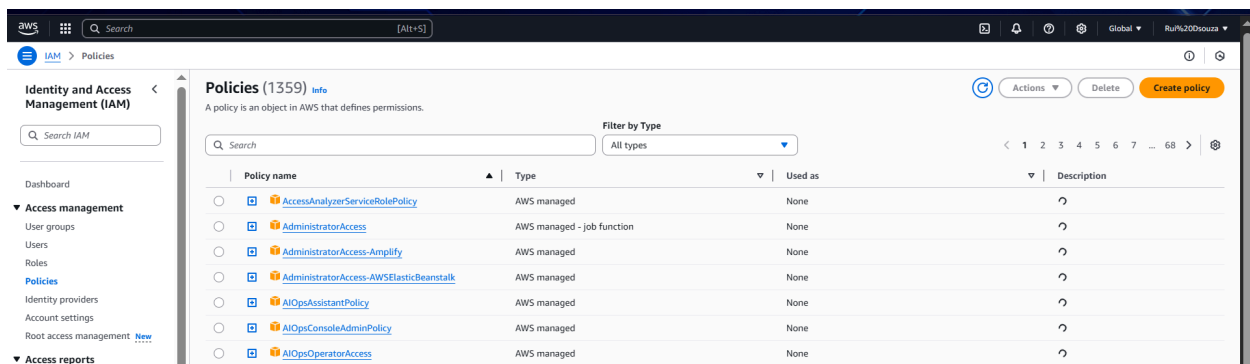
- IAM** Manage access to AWS resources
- IAM Identity Center** Manage workforce user access to multiple AWS accounts and cloud applications
- Resource Access Manager** Share AWS resources with other accounts or AWS Organizations

**Features** [Show more](#)

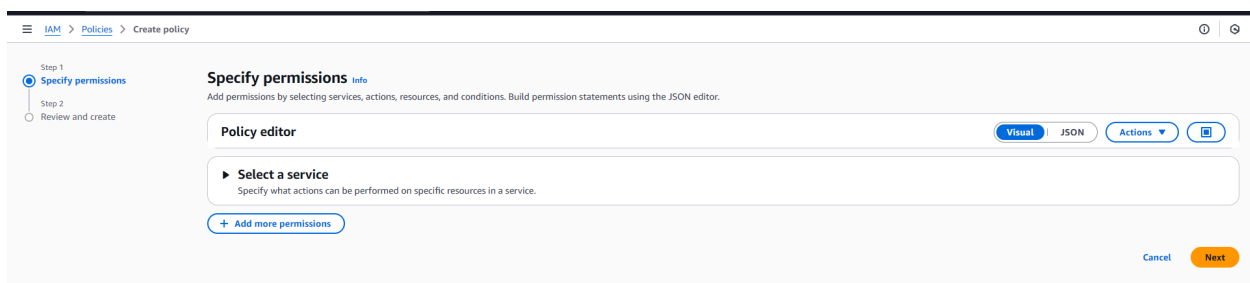
Now Go to IAM



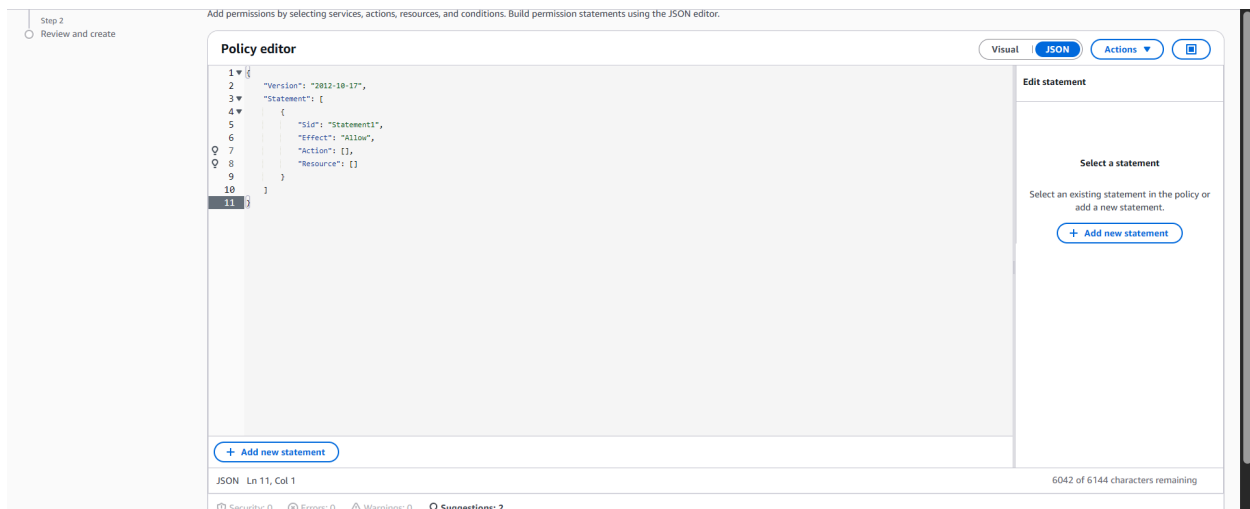
Click Policies from the left menu.



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

### Specify permissions [Info](#)

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

**Policy editor**

Visual **JSON** Actions

**Edit statement**

**Select a statement**

Select an existing statement in the policy or add a new statement.

[+ Add new statement](#)

```

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 }

```

[+ Add new statement](#)

paste it here and click next

### Review and create [Info](#)

Review the permissions, specify details, and tags.

#### Policy details

##### Policy name

Enter a meaningful name to identify this policy.

NextWorkDevEnvironmentPolicy

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

##### Description - optional

Add a short explanation for this policy.

IAM Policy for the NextWork development environment

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

give a name and description

Permissions defined in this policy
[Info](#)

Edit

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

Q Search

Explicit deny (1 of 442 services)

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

Allow (1 of 442 services)

Show remaining 441 services

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

Add tags - optional
[Info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Keep this as default and click create

Policy NextWorkDevEnvironmentPolicy created.

View policy

Policies (1360)
[Info](#)

Actions
Delete
Create policy

A policy is an object in AWS that defines permissions.

NextWorkDevEnvironmentPolicy
[Info](#)

Edit

Delete

IAM Policy for the NextWork development environment

Policy details

Type	Creation time	Edited time	ARN
Customer managed	June 18, 2025, 11:45 (UTC+05:30)	June 18, 2025, 11:45 (UTC+05:30)	arn:aws:iam::448089047342:policy/NextWorkDevEnvironmentPolicy

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

Q Search

Explicit deny (1 of 442 services)

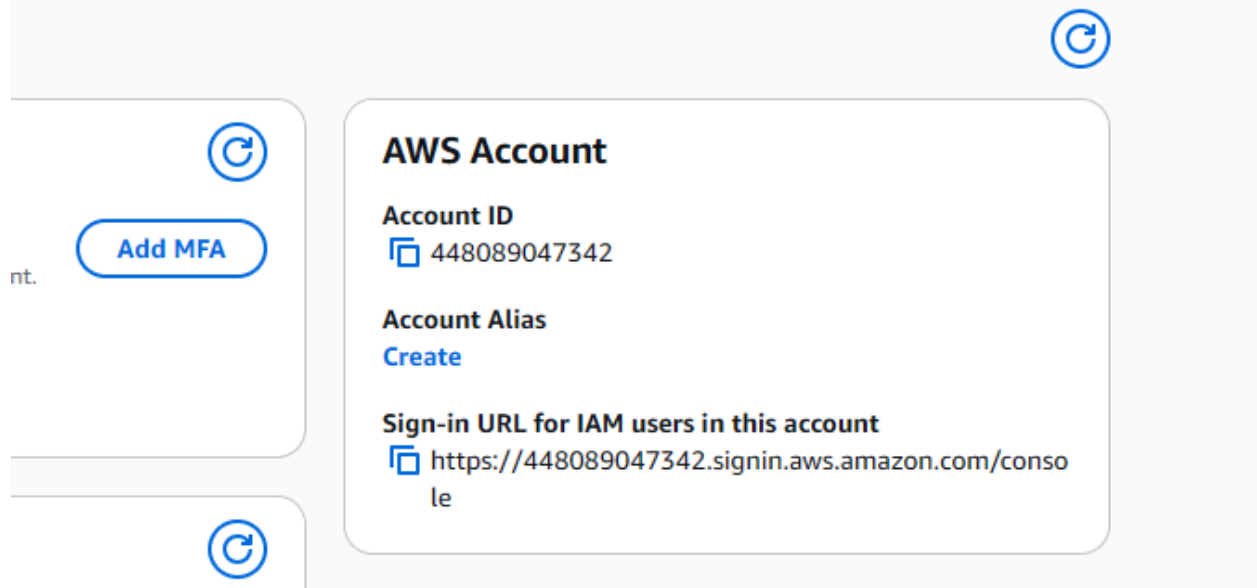
Service	Access level	Resource	Request condition
EC2	Full: Tagging	All resources	None

Allow (1 of 442 services)

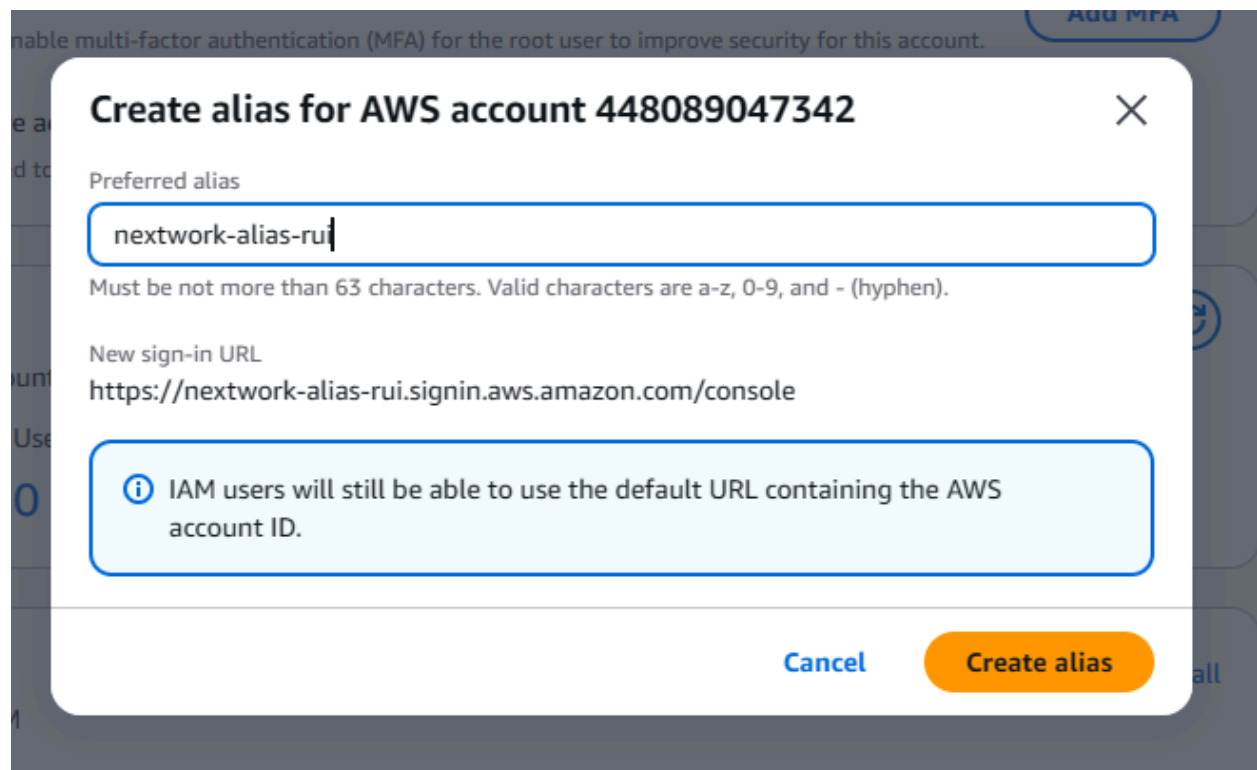
Show remaining 441 services

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

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

Alias nextwork-alias-rui created for this account.

### Security recommendations

- Add MFA for root user**  
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account. [Add MFA](#)
- Root user has no active access keys**  
Using access keys attached to an IAM user instead of the root user improves security.

### IAM resources

Resources in this AWS Account

### AWS Account

**Account ID**  
448089047342

**Account Alias**  
nextwork-alias-rui [Edit](#) | [Delete](#)

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

Here we created a alias user

- ▼ **Access management**
  - User groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
  - Root access management [New](#)

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

### Name the group

**User group name**  
Enter a meaningful name to identify this group.

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

Give name

### Attach permissions policies - *Optional* (1/1051) [Info](#)

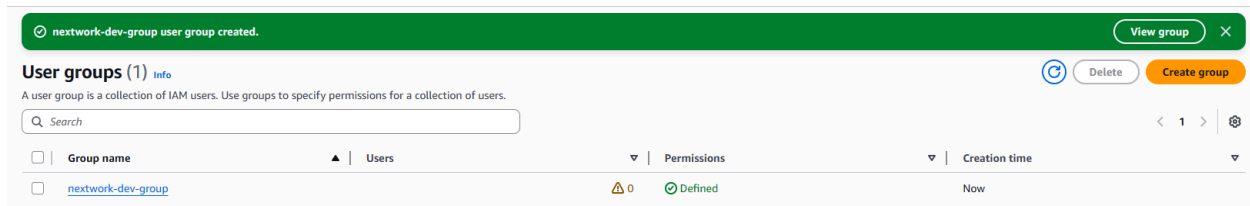
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

[×](#) **Filter by Type** [All types](#) [1 match](#)

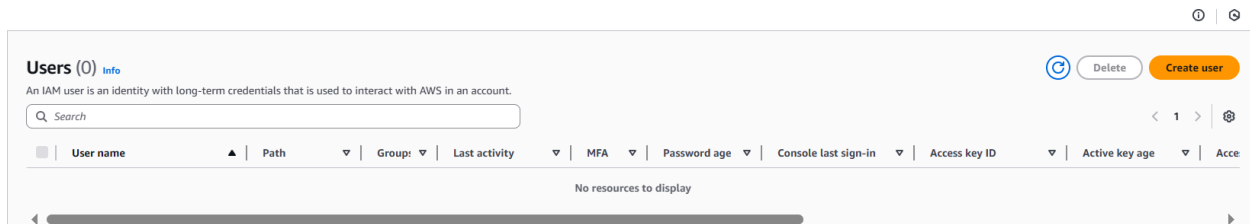
<input checked="" type="checkbox"/>	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	<a href="#">NextWorkDevEnvironmentPolicy</a>	Customer managed	None	IAM Policy for the NextWork develop...



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

**User name**

network-dev-rui

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](#)

put in all the details show 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)

Search



Create group

< 1 > ⚙

<input checked="" type="checkbox"/>	Group name	Users	Attached policies	Created
<input checked="" type="checkbox"/>	network-dev-group	0	NextWorkDevEnvironmentPolicy	2025-06-18 (5 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-rui

Console password type  
Autogenerated

Require password reset  
No

### Permissions summary

< 1 >

Name	Type	Used as
network-dev-group	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

Press 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**

**Console sign-in URL**

<https://nextwork-alias-rui.signin.aws.amazon.com/console>

**User name**

[nextwork-dev-rui](#)

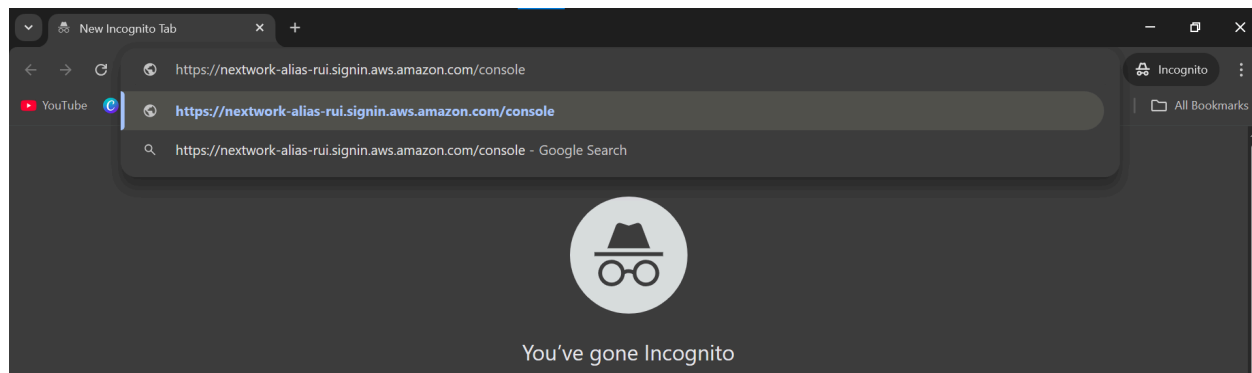
**Console password**

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

[Email sign-in instructions](#)

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

Here we created a user



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

### IAM user sign in

Account ID or alias (Don't have?)

☐ Remember this account

IAM username

Password

☐ Show Password [Having trouble?](#)

[Sign in](#)

[Sign in using root user email](#)

[Create a new AWS account](#)

By continuing, you agree to [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#).

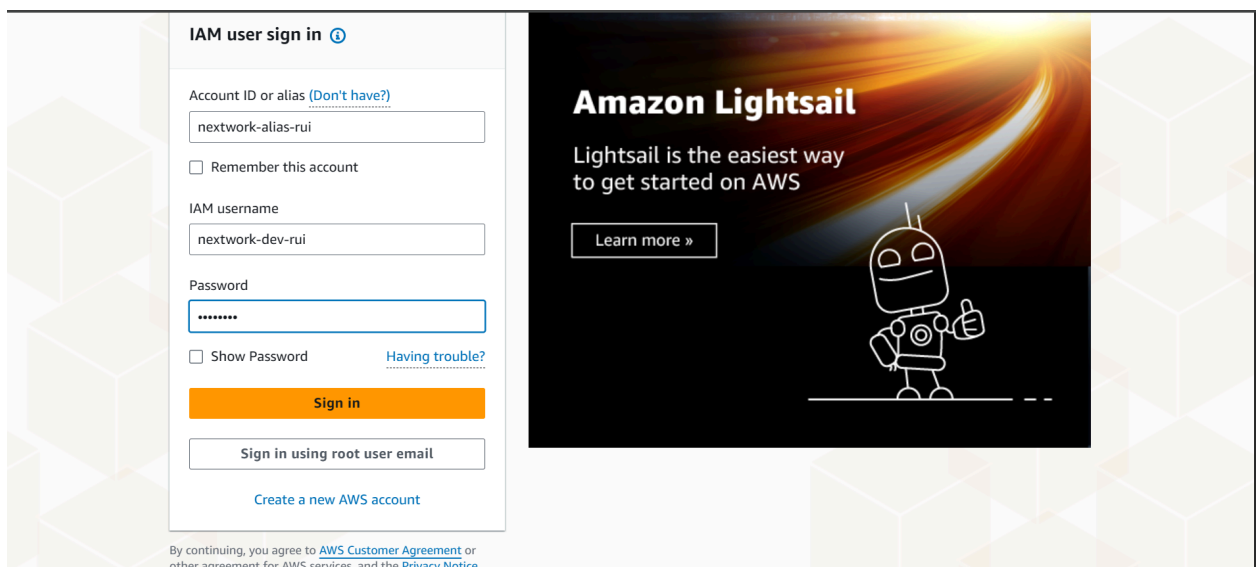
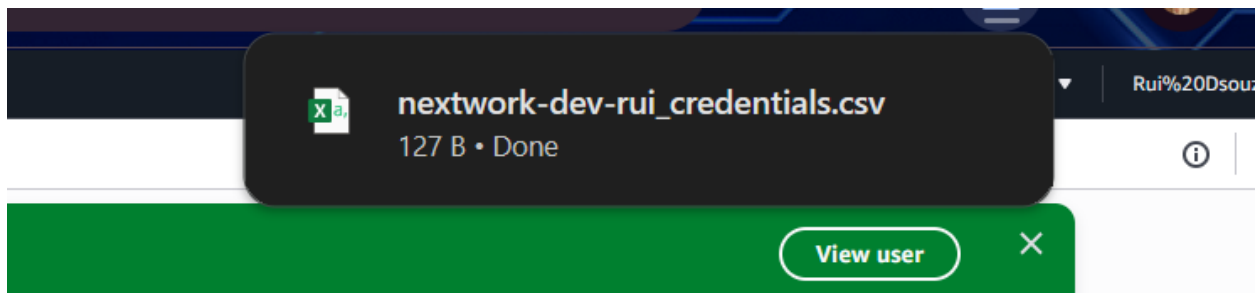
Amazon Lightsail

Lightsail is the easiest way to get started on AWS

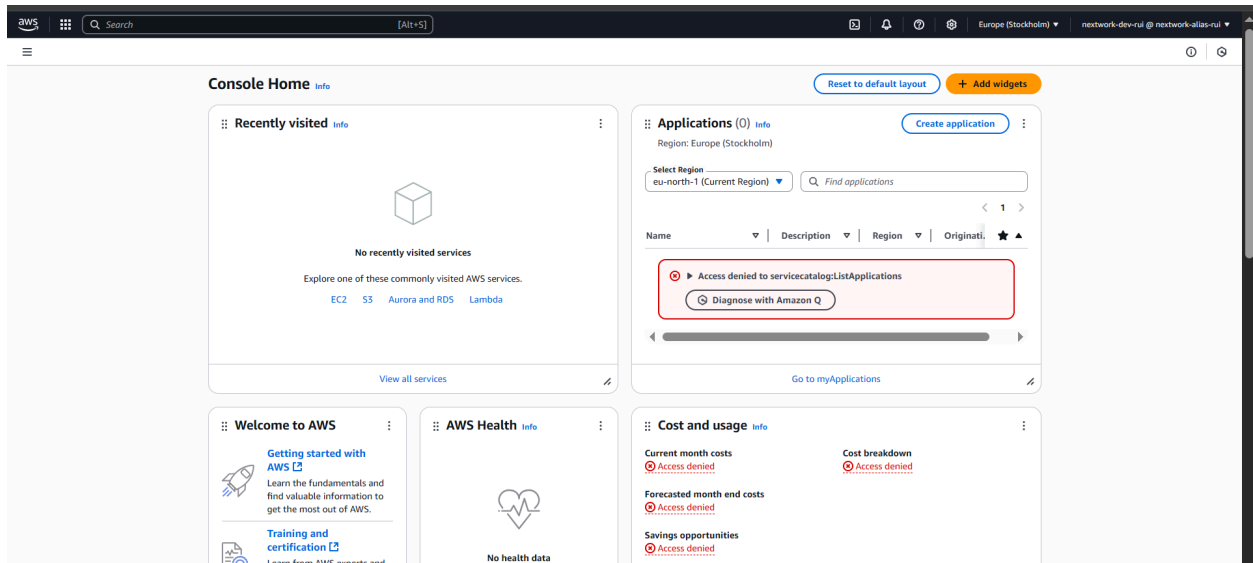
[Learn more »](#)

https://aws.amazon.com/lightsail/?sc\_icampaign=pac\_lightsail\_iam&sc\_ichannel=ha&sc\_content=awssm-1111&sc\_iplace=signin&trk=ha\_awssm-1111

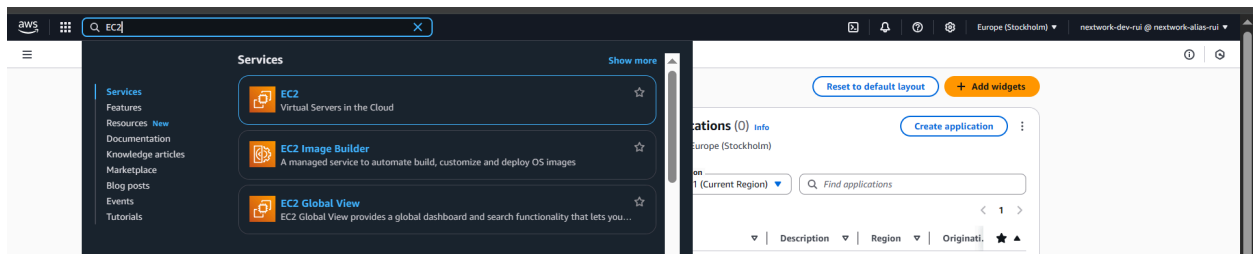
You can use the details given on the porta itself or download the csv file anyone can work



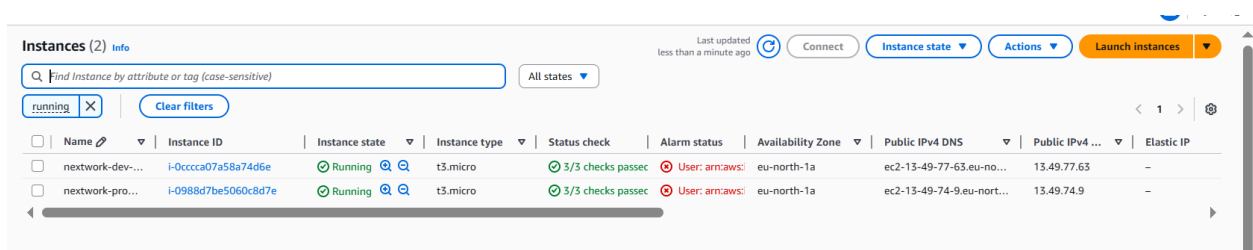
Fill out the login details



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



**Instance summary for i-0988d7be5060c8d7e (network-prod-rui)** [Info](#)

Updated less than a minute ago

<b>Instance ID</b> <a href="#">i-0988d7be5060c8d7e</a>	<b>Public IPv4 address</b> <a href="#">13.49.74.9</a>   <a href="#">open address</a>	<b>Private IPv4 addresses</b> <a href="#">172.31.22.49</a>
<b>IPv6 address</b> -	<b>Instance state</b> <span>Running</span>	<b>Public DNS</b> <a href="#">ec2-13-49-74-9.eu-north-1.compute</a>
<b>Hostname type</b> IP name: ip-172-31-22-49.eu-north-1.compute.internal	<b>Private IP DNS name (IPv4 only)</b> <a href="#">ip-172-31-22-49.eu-north-1.compute.internal</a>	<b>Elastic IP addresses</b> -
<b>Answer private resource DNS name</b> IPv4 (A)	<b>Instance type</b> t3.micro	<b>AWS Compute Optimizer finding</b> <span>⚠</span> User: arn:aws:iam::448089047342:user/network-dev-rui 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-assigned IP address</b> <a href="#">13.49.74.9</a> [Public IP]	<b>VPC ID</b> <a href="#">vpc-0ae8911490d76f21b</a>	<b>Auto Scaling Group name</b> -
<b>IAM Role</b> -	<b>Subnet ID</b> <a href="#">subnet-0e245effb0ef90226</a>	<b>Managed</b> false
<b>IMDSv2</b> Required	<b>Instance ARN</b> <a href="#">arn:aws:ec2:eu-north-1:448089047342:instance/i-0988d7be5060c8d7e</a>	
<b>Operator</b> -		

try stopping it

**Stop instance**

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

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

[i-0988d7be5060c8d7e \(network-prod-rui\)](#) | 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 stop

**Failed to stop the instance i-0988d7be5060c8d7e** [Diagnose with Amazon Q](#) [X](#)

You are not authorized to perform this operation. User: arn:aws:iam::448089047342:user/network-dev-rui is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:eu-north-1:448089047342:instance/i-0988d7be5060c8d7e because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: pAdXPHr-yT74oEmBicIT4p2LlpUAMZnOkLcN8b2100R-QrKCCtT3ibxvxEaQP9KyM1SF78MOUZPxmW-PoTDtw\_P8JFFpF7loGRe6da4kUPHGTYkw-GGGHF4Wbb7fS8Na0Kpfr5ZMH6DoASK8Nv2ckaLDbb-a0FTKFLsORl2q4ITqfJSP212CIR350htwOjGoNE\_RG4KNIY9c\_MJcmJ4x-9qzOKx31J3i-Bkow31p2nWDSWBs\_vU8vwy1X1hdScqLDXv1E\_FTY6MNHnqnd6u0HirMPsSHCFTQ5dTV\_WcyWnvqXkvteVYDplOMopj4rtpL7FqdFeggeLfhtW49X7GtwP60QKcZeiE6GxiSDTIWV3IV82pmH\_953mEOLtegoER5KcOkelUhofxTMaObi5QVSknCk75hrkLRHHMU042S-Cnymek7a5x9iw4ekR8SK1MKf4zhzR1yhegcugogrrkHST9drP16sux9Pmoa6cixvnmmlUlsWJSOgTCJ--WU7FLom7QESWwci54yPpLiA5f2RZl71VrikfJSTST7\_xPzXRqVYpFujg4mkNCpmV04eTEKV5gUWGNt6B0uaPIQM51wzw7BIE7l6ku9cq\$SLHxcDHvzlzzuIZAWW3864ak6JNY\_1VEm1-GinyHqEihKsCXDSx8RYuv2PUVq8xz2u-zhHqsn9lvdVc1BXDSWbOxy-LWu5c6r4NlopiZfDIToLL\_dJrFGLsZzJ3f8JNpxNIWBI150aoGBJODJmLXwm5z0jKJomJL2y16E19J3JOG4\_sWdGx2W9u8sYxklbw5XuwB3r\_IDVHch3zcFhvDmjxvkhk1y86tgF7XHNW3LY41pmohtked8mFVvHjjakX9rQ6UCHHw3ItaVw

here we can not stop the production instance

**Instance summary for i-0cccca07a58a74d6e ( nextwork-dev- rui)** [info](#)

Updated less than a minute ago

<b>Instance ID</b> <a href="#">i-0cccca07a58a74d6e</a>	<b>Public IPv4 address</b> <a href="#">13.49.77.63</a>   <a href="#">open address</a>	<b>Private IPv4 addresses</b> <a href="#">172.31.30.170</a>
<b>IPv6 address</b> -	<b>Instance state</b> <span>Running</span>	<b>Public DNS</b> <a href="#">ec2-13-49-77-63.eu-north-1.compu</a>
<b>Hostname type</b> IP name: ip-172-31-30-170.eu-north-1.compute.internal	<b>Private IP DNS name (IPv4 only)</b> <a href="#">ip-172-31-30-170.eu-north-1.compute.internal</a>	<b>Elastic IP addresses</b> -
<b>Answer private resource DNS name</b> IPv4 (A)	<b>Instance type</b> t3.micro	<b>AWS Compute Optimizer finding</b> <span>⚠</span> User: arn:aws:iam::448089047342:user/nextwork-dev-rui 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-assigned IP address</b> <a href="#">13.49.77.63</a> [Public IP]	<b>VPC ID</b> <a href="#">vpc-0ae8911490d76f21b</a>	<b>Auto Scaling Group name</b> -
<b>IAM Role</b> -	<b>Subnet ID</b> <a href="#">subnet-0e245effb0ef90226</a>	<b>Managed</b> false
<b>IMDSv2</b> Required	<b>Instance ARN</b> <a href="#">arn:aws:ec2:eu-north-1:448089047342:instance/i-0cccca07a58a74d6e</a>	
<b>Operator</b> -		

same way try it for development instance

**Stop instance**

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

<b>Instance ID</b> <a href="#">i-0cccca07a58a74d6e ( nextwork-dev- rui)</a>	<b>Stop protection</b> <span>Off</span> (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 stop

**Failed to stop the instance i-0cccca07a58a74d6e** [Diagnose with Amazon Q](#)

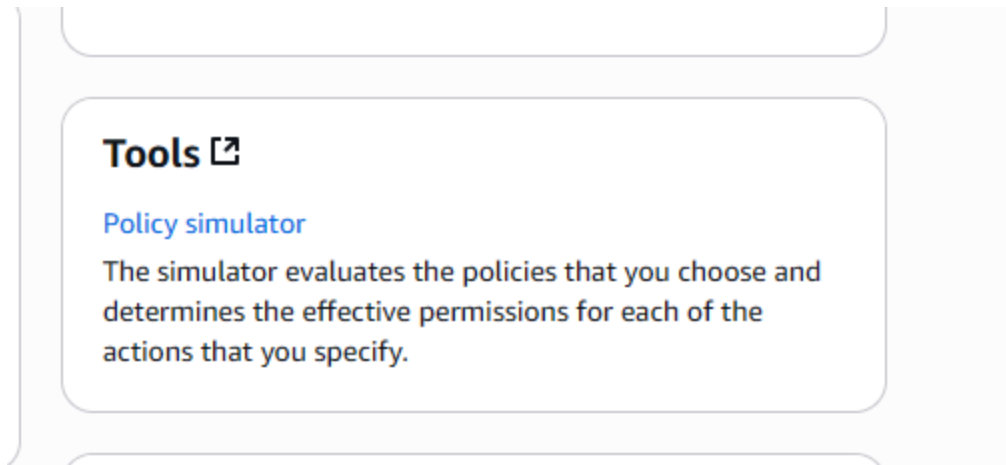
You are not authorized to perform this operation. User: arn:aws:iam::448089047342:user/nextwork-dev-rui is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:eu-north-1:448089047342:instance/i-0cccca07a58a74d6e because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: J3-8Yd08R8h8VSKAIIFEK1p3XtCJxI3\_470ezqGVVKDsbNS-

IDURPq5FMYbfGieVlix3jRfIdbgFxs\_1GUz1n2B\_M9MwQFa3yQPghrgpH8CToeqC2OGRqAZNWNJGdb65dTTOpyoRH4Id\_e8aqRdnIfCtIfYzDOT30TAecYO2ls8q7PLZMuePHKyIV3KR-QBRscWin1P4eRoHqEdcTg\_ryYp34T1SvE3pz\_KfZR\_K3ZPP1VblhcGjw243Bg2a1EGQKQ-Ag52Bvm3lr0UscfWFW1hwV3IS3MduSRRT1\_jeAsp32eQm7nGQxwhgcSK5ohhprkhjE\_wRKD-FBgeTknZauiX8\_Hdc4DKIK665LZTECFDgt\_Z2ebW6ZMmwzN4agCuzBpPLCH7B\_OSNYBXbCYbYrPg5d4GV-sPY3bofowP-WfKSL1nBhrrvwYpAs5rDwPQDkiooEFAApjTUAJEFQhsegtMOqGUMf540wUpjT1Bp2HbzGfw-flo\_2JhLDNywOV52TlyOq5\_D9llarybusTWNkrnC1Eb-XbAr302urwyVPRxKs4p1hKhptKe-9Xg1bQq4d4H8qWfWME2NCIBh8PwRLRS6e54MitTnlUd\_YfQyQyNw29meEo7m3bN9yYbMFxVC\_54058WFRv1u97\_4ZMW\_yRQfVhtp9E7QnUo6A-FNAYayM1xMD89Td4wOFUfoL\_ufs5uNkeT4CNvD2bepH\_Fdy3BUDpKfb83hEaYo5JNfzyaBlmD3BgVZ06efGOPGX1EoolBf9nIfOoje54YXR2mfBVF\_BHC-uAdYtxPY1Be68A8bBNpN7NRF9okIFJFEvQ\_1r6VN-zhPT5QswzCGX3Xa400c5SqQZnzL0mXT98

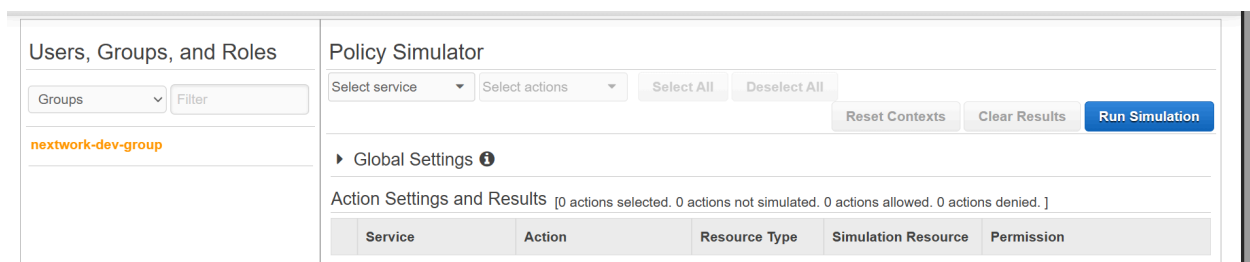
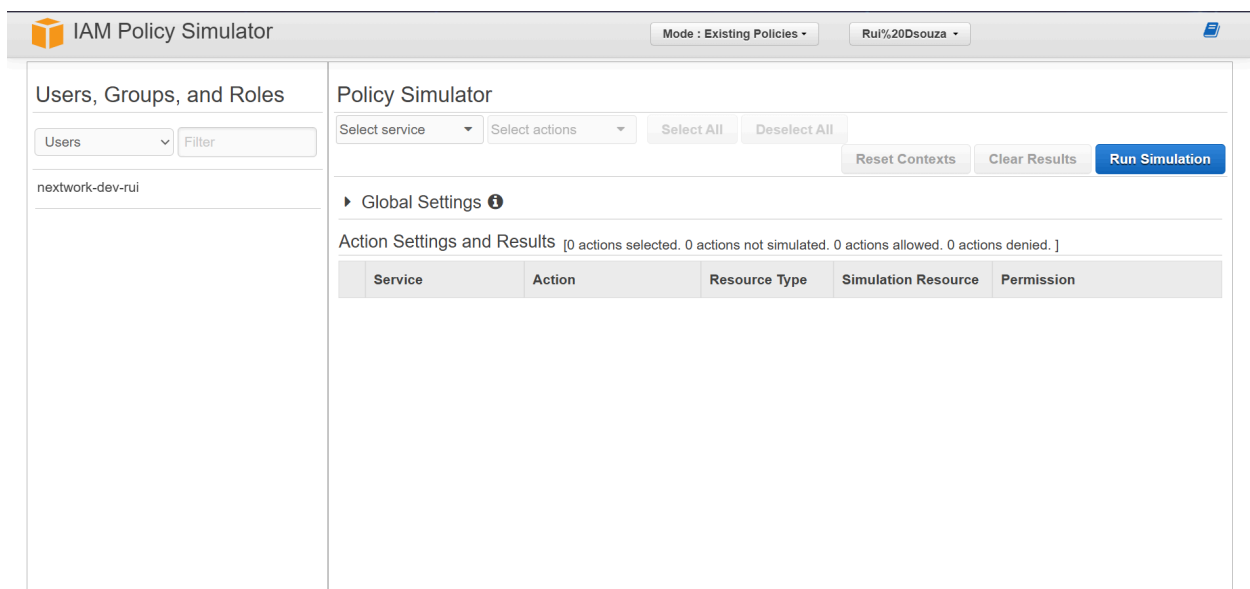
Instances (1 / 4) [info](#)

[Last updated](#)
[Connect](#)
[Instance state](#)
[Actions](#)
[Launch instances](#)

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



**IAM Policy Simulator**

Mode: Existing Policies | Rui%20Dsouza

**Policies** | Back | Create New Policy

Selected group: **network-dev-group**

**IAM Policies**

Filter

☒ NextWorkDevEnvironment...

Custom IAM Policies

There are no policies to display!

**Policy Simulator**

Amazon EC2 | 2 Action(s) sele... | Select All | Deselect All

Reset Contexts | Clear Results | **Run Simulation**

Global Settings ⓘ

Action Settings and Results [2 actions selected. 2 actions not simulated. 0 actions allowed. 0 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
Amazon EC2	StopInstances	instance	*	Not simulated
Amazon EC2	DeleteTags	not required	*	Not simulated

Select Service → EC2

Select action → StopInstance & Delete Tags

Click Run Simulation

Global Settings ⓘ

Action Settings and Results [2 actions selected. 0 actions not simulated. 0 actions allowed. 2 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
Amazon EC2	StopInstances	instance	*	<b>denied</b> Implicitly denied (no mat...
Amazon EC2	DeleteTags	not required	*	<b>denied</b> 1 matching statements.

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

Successfully initiated stopping of i-0988d7be5060c8d7e | i-0ccca07a58a74d6e

**Instances (2/2)** Info

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

Running | Clear filters

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
network-dev-...	i-0ccca07a58a74d6e	Stopping	t3.micro	3/3 checks pass	View alarms +	eu-north-1a	ec2-13-49-77-63.eu-no...	13.49.77.63	-
network-pro-...	i-0988d7be5060c8d7e	Stopping	t3.micro	3/3 checks pass	View alarms +	eu-north-1a	ec2-13-49-74-9.eu-nort...	13.49.74.9	-

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