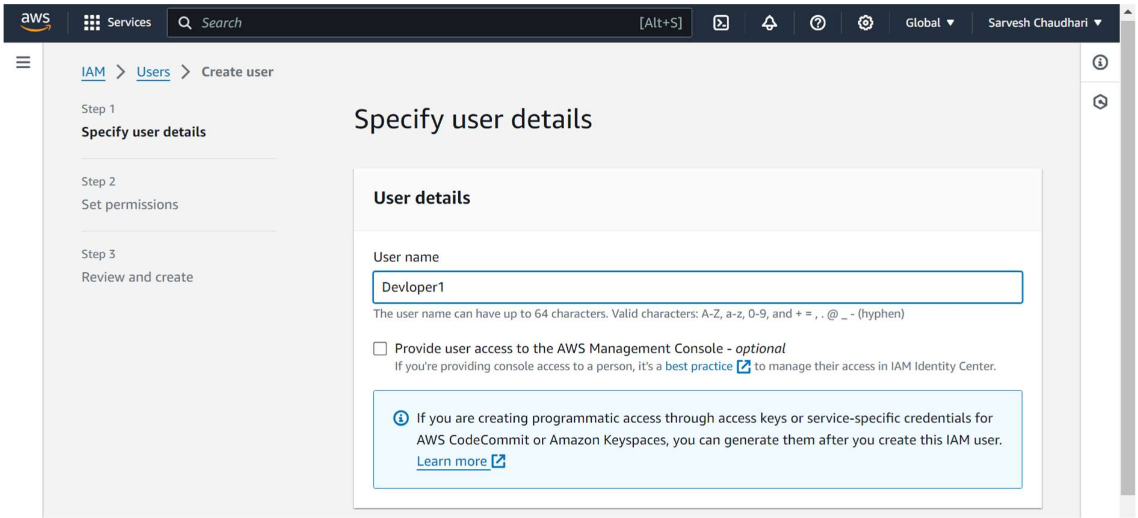
Objective:- Privacy access management using IAM

S1) create new user



IAM > Users > Create user

Step 1
**Specify user details**

Step 2
Set permissions

Step 3
Review and create

## Specify user details

**User details**

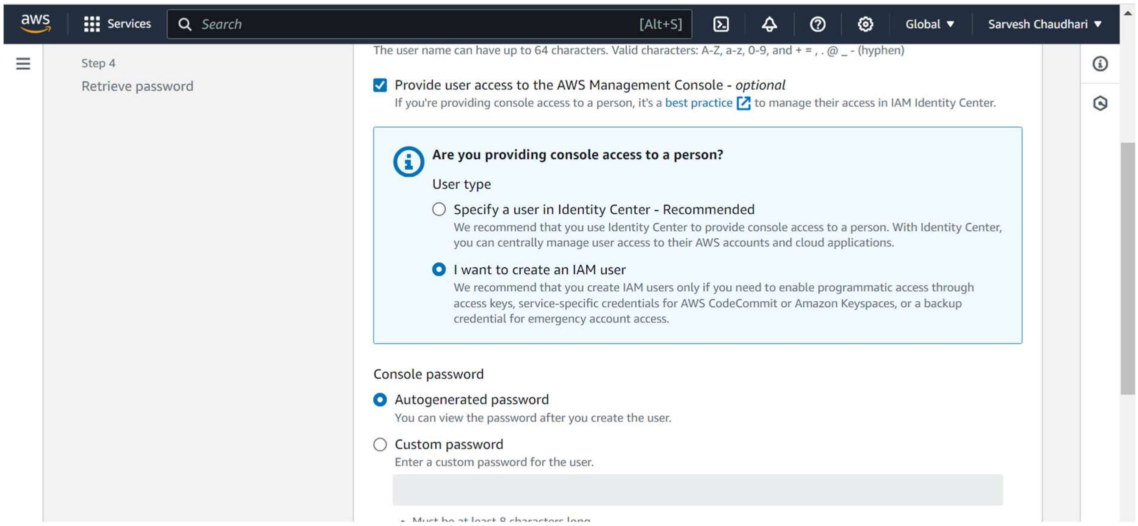
User name

Devloper1

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.

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



Step 4
Retrieve password

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.

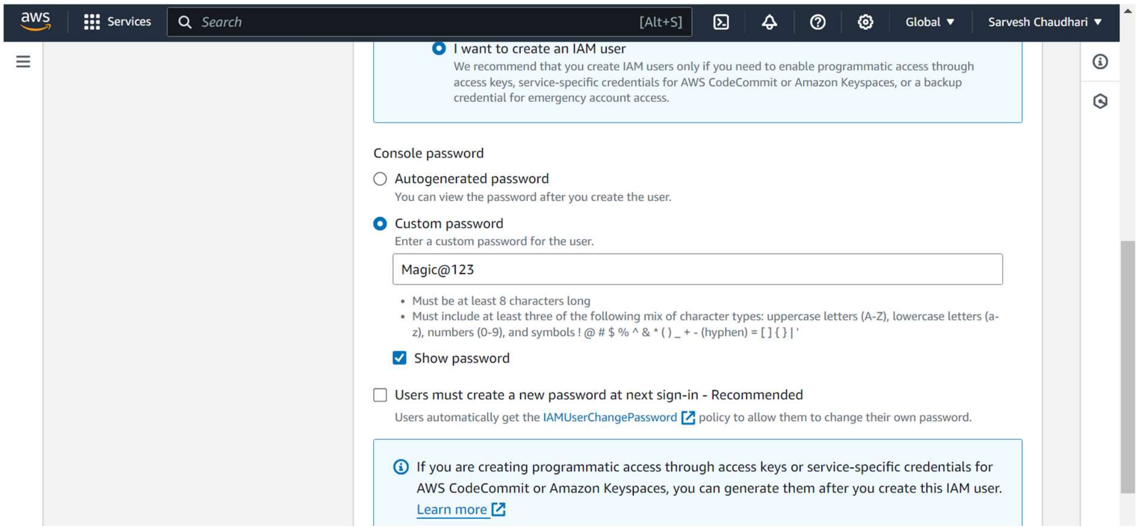
● I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

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



● 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.

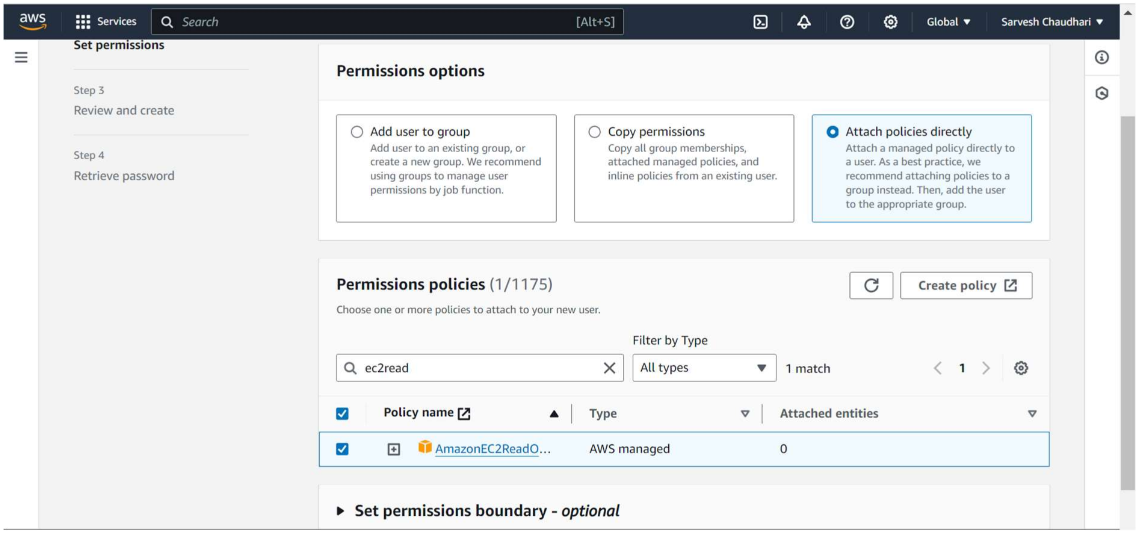
Magic@123

- 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



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.

Permissions policies (1/1175)

Choose one or more policies to attach to your new user.

Filter by Type

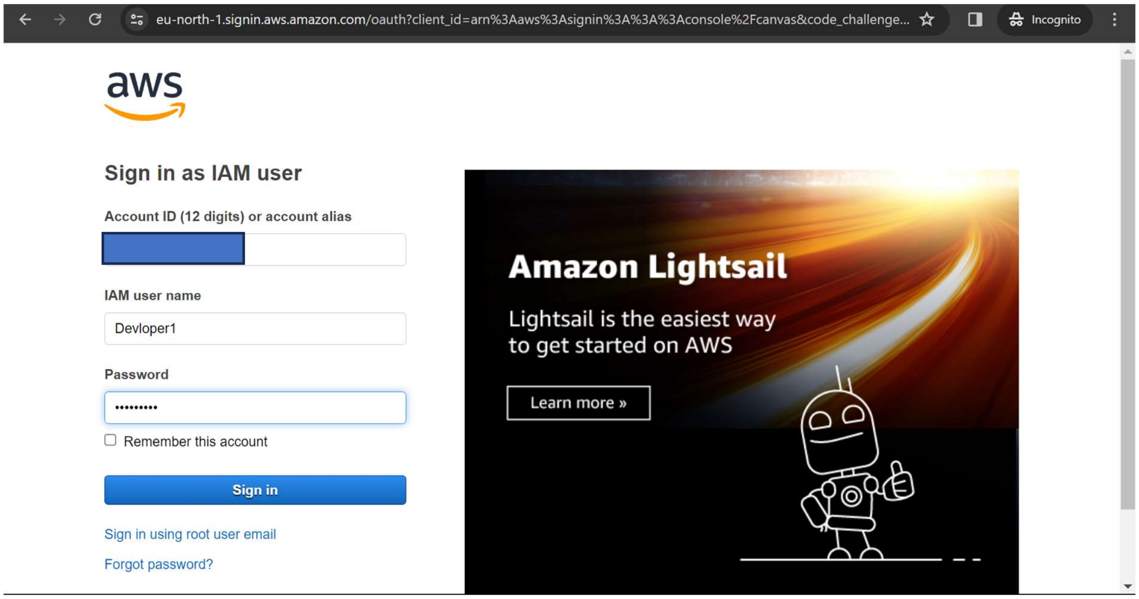
ec2read | All types | 1 match

| ☑ | Policy name | Type | Attached entities |
|---|---|---|---|
| ☑ | AmazonEC2ReadO... | AWS managed | 0 |

Now click on next and create user

Now copy the sign in url and paste in New Incognito tab

Enter user name and password


eu-north-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge...

Sign in as IAM user

Account ID (12 digits) or account alias

[redacted]

IAM user name

Devloper1

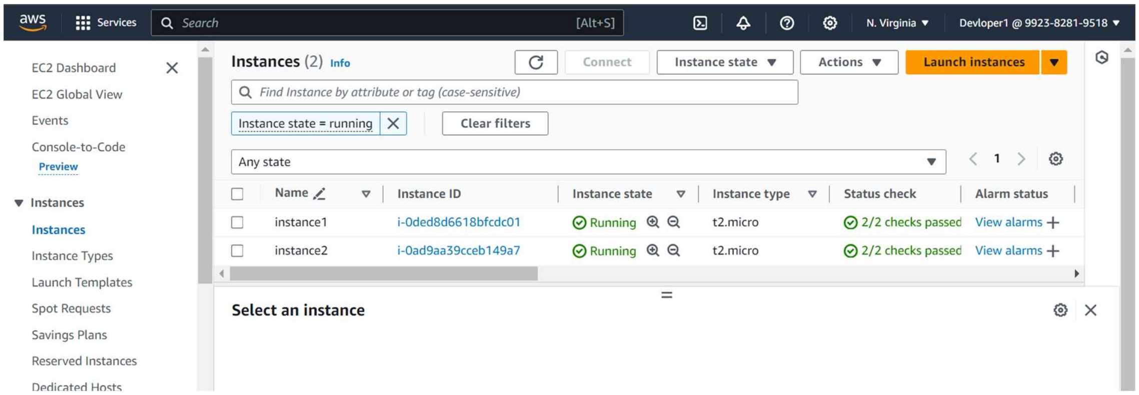
Password

•••••••••

□ Remember this account

Sign in
Sign in using root user email
Forgot password?
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »

After login go in instance check whether the permissions of read only is working or not



Instances (2) Info

Find Instance by attribute or tag (case-sensitive)

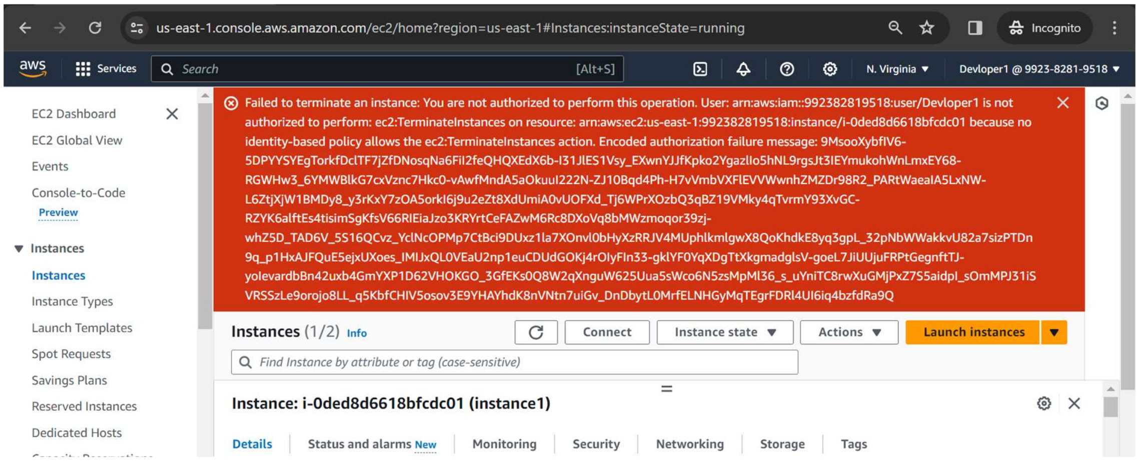
Instance state = running

Any state

| | Name | Instance ID | Instance state | Instance type | Status check | Alarm status |
|---|---|---|---|---|---|---|
| □ | instance1 | i-0ded8d6618bfcdc01 | ✓ Running | t2.micro | ✓ 2/2 checks passed | View alarms + |
| □ | instance2 | i-0ad9aa39cceb149a7 | ✓ Running | t2.micro | ✓ 2/2 checks passed | View alarms + |

Select an instance

Trying to terminate instance



Failed to terminate an instance: You are not authorized to perform this operation. User: arn:aws:iam::992382819518:user/Devloper1 is not authorized to perform: ec2:TerminateInstances on resource: arn:aws:ec2:us-east-1:992382819518:instance/i-0ded8d6618bfcdc01 because no identity-based policy allows the ec2:TerminateInstances action. Encoded authorization failure message: 9MsooXybfIV6-5DPYYSYEgTorkfDclTF7jZfDNosqNa6Fil2feQHQXEdX6b-I31JlES1Vsy_EXwnYJJfKpko2YgazlIo5hNL9rgsJt3IEYmukohWnLmxEY68-RGWHw3_6YMWBlkG7cxVznc7Hkc0-vAwfMndA5aOkuuI222N-ZJ10Bqd4Ph-H7vVmbVXFlEVVWwnhZMZDr98R2_PARtWaeaIA5LxNW-L6ZtjXjW1BMDy8_y3rKxY7zOA5orkI6j9u2eZt8XdUmiA0vUOFXd_Tj6WPrXOzbQ3qBZ19VMky4qTvrmY93XvGC-RZYK6alftEs4tisimSgKfsV66RIEiaJzo3KRYrtCeFAZwM6Rc8DXoVq8bMWzmoqor39zj-whZ5D_TAD6V_5S16QCvz_YclNcOPMp7CtBci9DUxz1la7XOnvl0bHyXzRRJV4MUphlkmlgwX8QoKhdkE8yq3gpL_32pNbWWakkvU82a7sizPTDn9q_p1HxAJFQuE5ejxUXoes_IMIJxQL0VEaU2np1euCDUdGOKj4rOlyFln33-gklYF0YqXDgTtXkgmadglsV-goeL7JiUUjuFRPtGegnftTJ-yolevardbBn42uxb4GmYXP1D62VHOKGO_3GfEKs0Q8W2qXnguW625Uua5sWco6N5zsMpMl36_s_uYniTC8rwXuGMjPxZ7S5aidpl_sOmMPJ31iSVRSSzLe9orojo8LL_q5KbfCHIV5osov3E9YHAYhdK8nVNtn7uiGv_DnDbytL0MrfELNHGyMqTEgrFDRl4UI6iq4bzfdRa9Q

Instances (1/2) Info

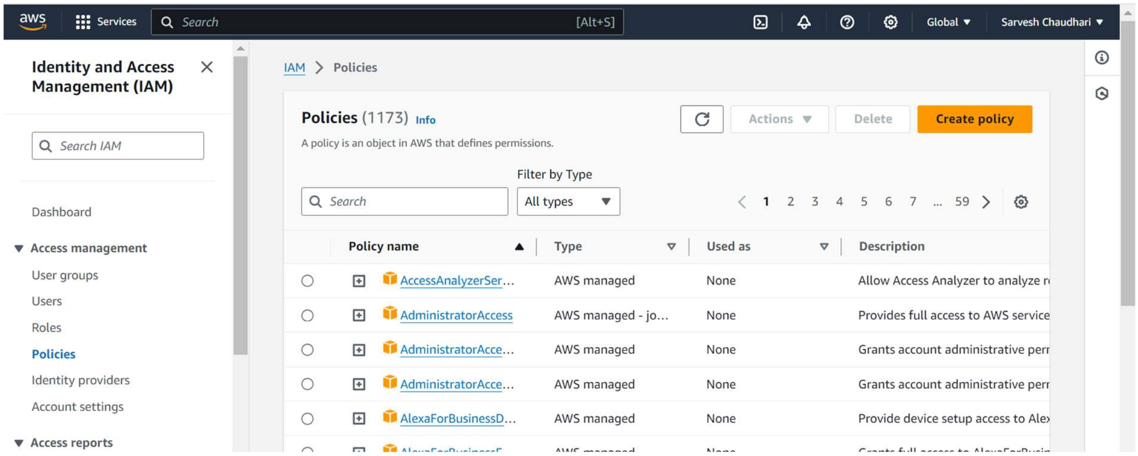
Find Instance by attribute or tag (case-sensitive)

Instance: i-0ded8d6618bfcdc01 (instance1)

SO here we can read only can not terminate and stop.

S2) Now creating policies

From left pannel go to policies > Create Policy

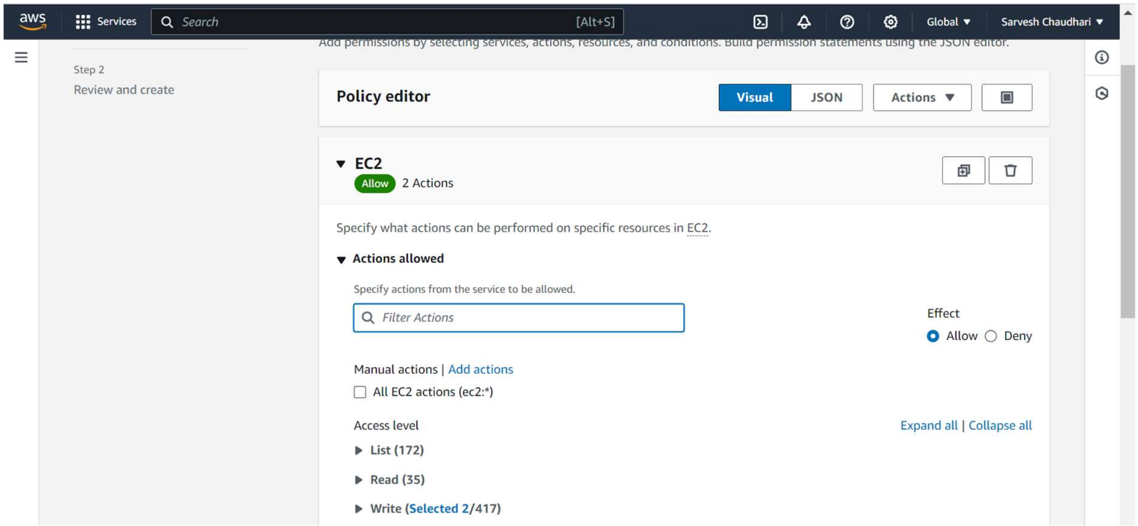


Policies (1173) Info

A policy is an object in AWS that defines permissions.

| | | Policy name | Type | Used as | Description |
|---|---|---|---|---|---|
| ○ | ⊞ | AccessAnalyzerSer… | AWS managed | None | Allow Access Analyzer to analyze r |
| ○ | ⊞ | AdministratorAccess | AWS managed - jo… | None | Provides full access to AWS service |
| ○ | ⊞ | AdministratorAcce… | AWS managed | None | Grants account administrative perr |
| ○ | ⊞ | AdministratorAcce… | AWS managed | None | Grants account administrative perr |
| ○ | ⊞ | AlexaForBusinessD… | AWS managed | None | Provide device setup access to Alex |

Then select service and there actions



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

Step 2
Review and create

Policy editor — Visual | JSON | Actions ▼

▼ EC2
Allow 2 Actions

Specify what actions can be performed on specific resources in EC2.

▼ Actions allowed

Specify actions from the service to be allowed.

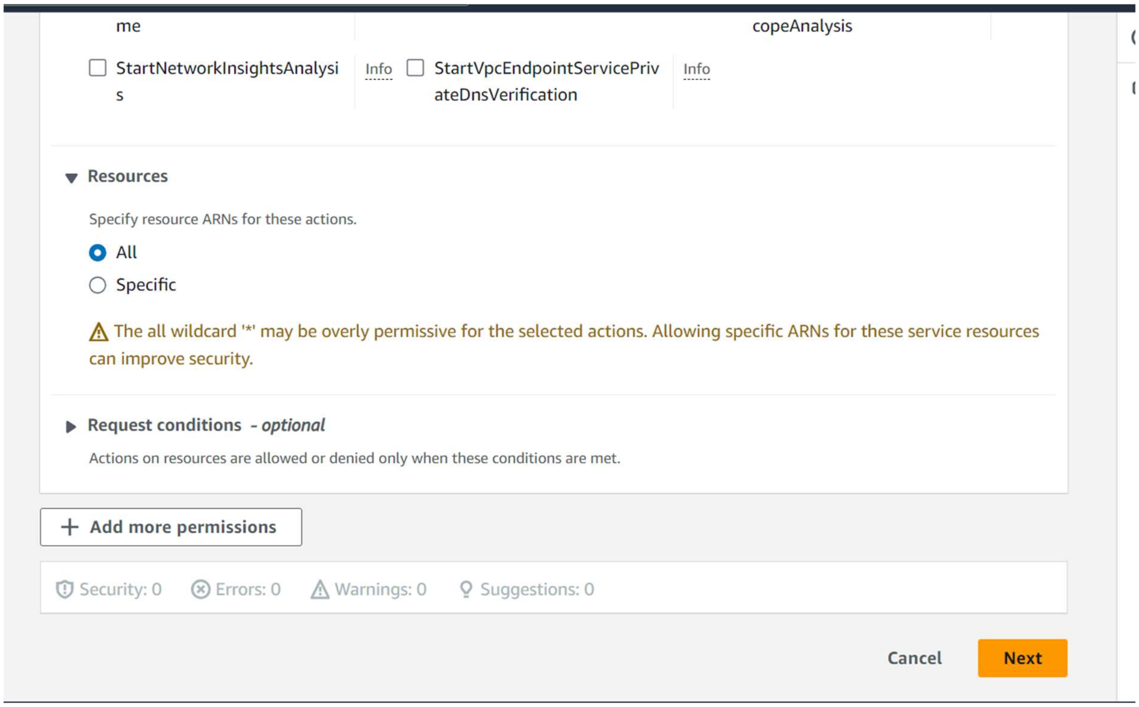
Filter Actions

Effect
● Allow ○ Deny

Manual actions | Add actions
□ All EC2 actions (ec2:*)

Access level — Expand all | Collapse all
▶ List (172)
▶ Read (35)
▶ Write (Selected 2/417)

Select all to give permission to all instances then next


me — copeAnalysis

□ StartNetworkInsightsAnalysis Info □ StartVpcEndpointServicePrivateDnsVerification Info

▼ Resources

Specify resource ARNs for these actions.

● All
○ Specific

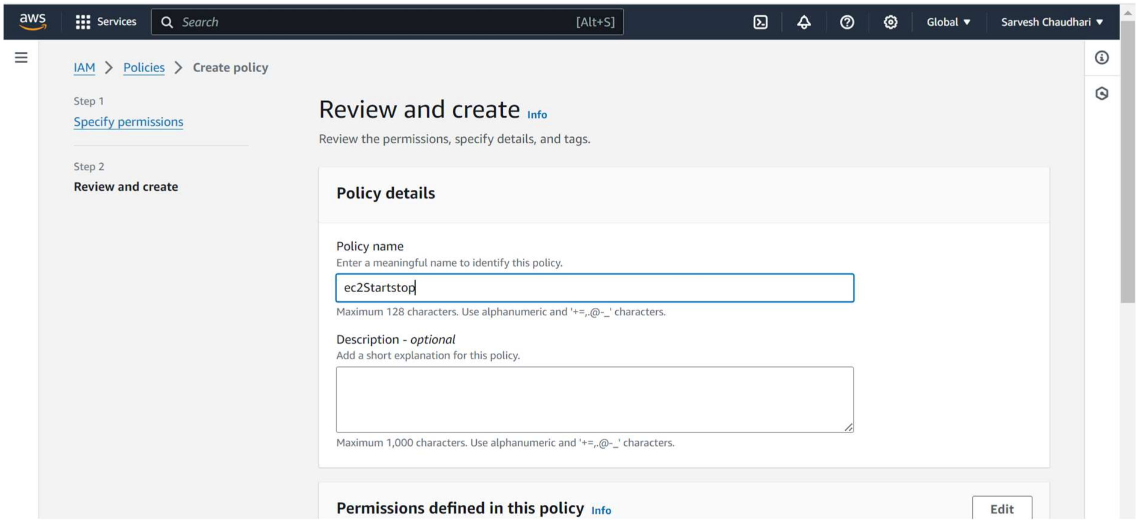
⚠ The all wildcard '*' may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

▶ Request conditions - *optional*

Actions on resources are allowed or denied only when these conditions are met.

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Now give name to policy then click on create policy.



Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

ec2Startstop

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

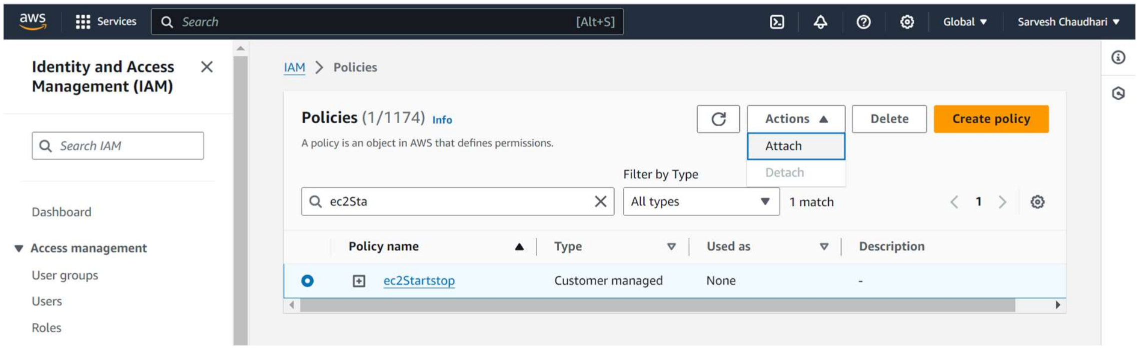
Description - *optional*

Add a short explanation for this policy.

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

Permissions defined in this policy

Now attach new created policy



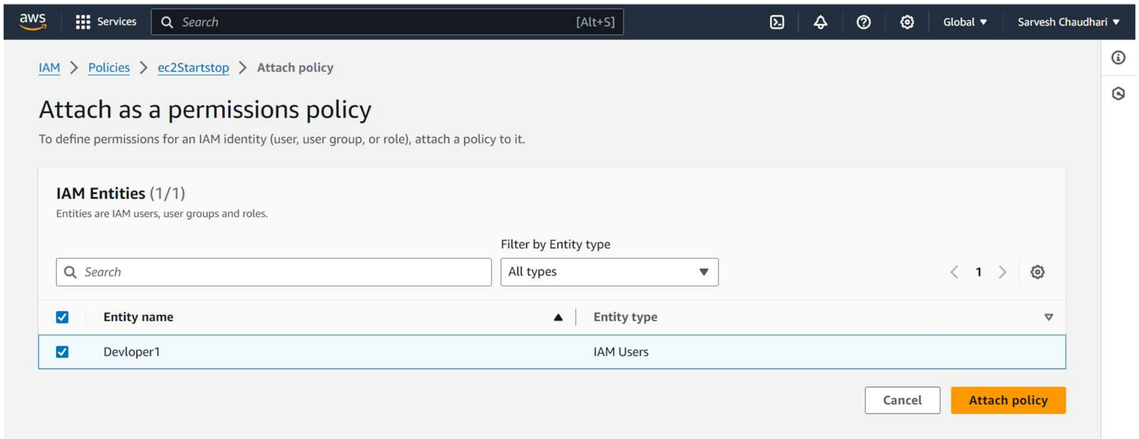
Policies (1/1174)

A policy is an object in AWS that defines permissions.

Filter by Type

ec2Sta | All types | 1 match

| | Policy name | Type | Used as | Description |
|---|---|---|---|---|
| ● | ec2Startstop | Customer managed | None | - |



Attach as a permissions policy

To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

IAM Entities (1/1)

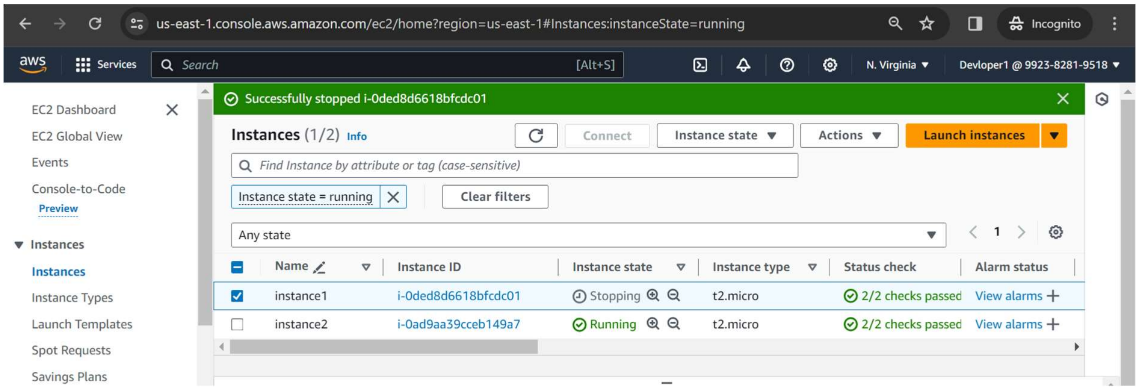
Entities are IAM users, user groups and roles.

Filter by Entity type

Search | All types

| ☑ | Entity name | Entity type |
|---|---|---|
| ☑ | Devloper1 | IAM Users |

Now in user account instance1 is stopped to check access is granted or not.



us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:instanceState=running

Successfully stopped i-0ded8d6618bfcdc01

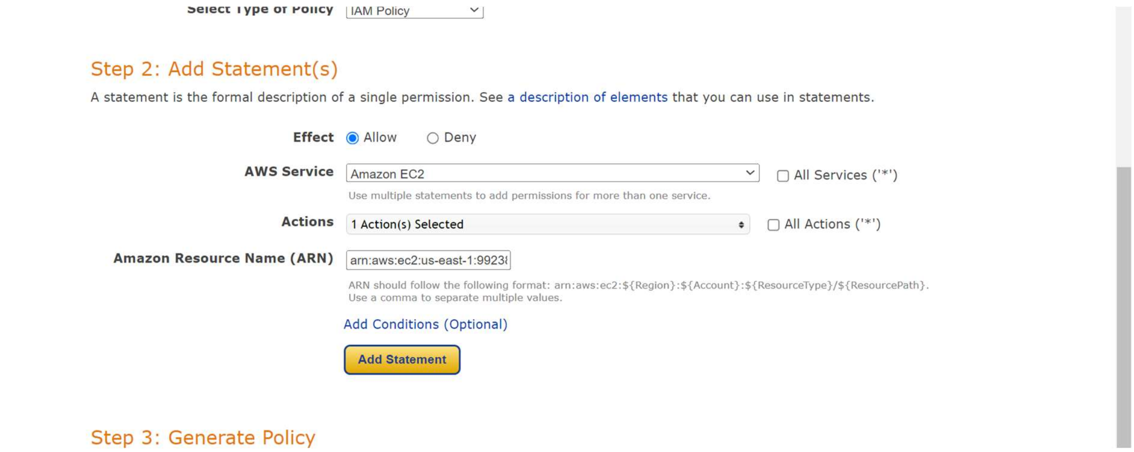
Instances (1/2)

Instance state = running

Any state

| | Name | Instance ID | Instance state | Instance type | Status check | Alarm status |
|---|---|---|---|---|---|---|
| ☑ | instance1 | i-0ded8d6618bfcdc01 | Stopping | t2.micro | 2/2 checks passed | View alarms + |
| □ | instance2 | i-0ad9aa39cceb149a7 | Running | t2.micro | 2/2 checks passed | View alarms + |

Now go to policy generator website of AWS



Select Type of Policy: IAM Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect ● Allow ○ Deny

AWS Service: Amazon EC2 □ All Services ('*')

Use multiple statements to add permissions for more than one service.

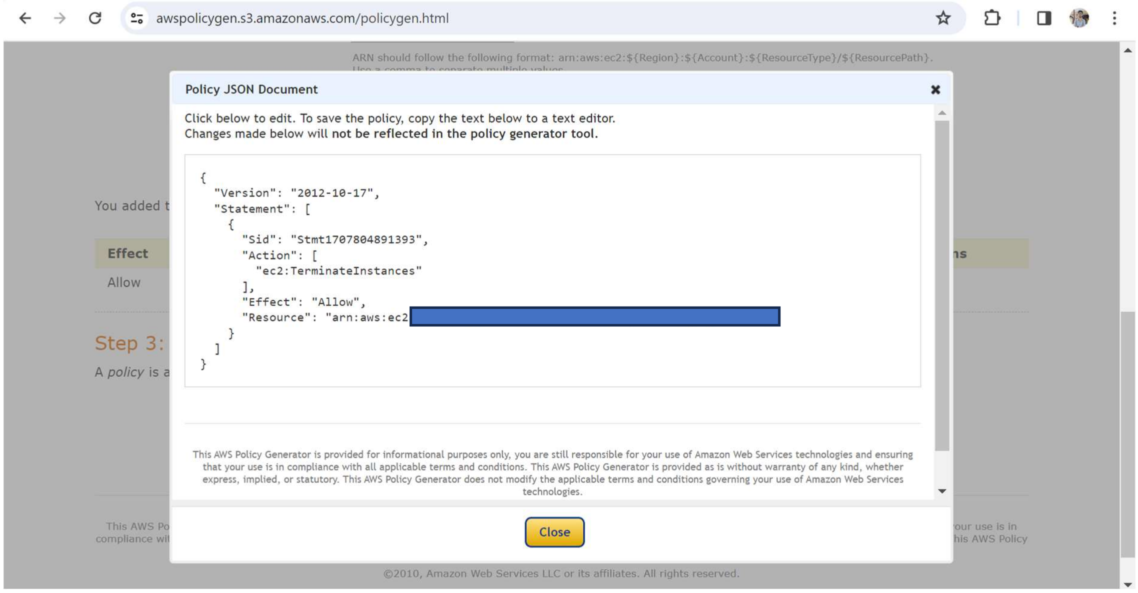
Actions: 1 Action(s) Selected □ All Actions ('*')

Amazon Resource Name (ARN): arn:aws:ec2:us-east-1:99238

ARN should follow the following format: arn:aws:ec2:${Region}:${Account}:${ResourceType}/${ResourcePath}.
Use a comma to separate multiple values.

Step 3: Generate Policy

Add statement > Generate Policy



awspolicygen.s3.amazonaws.com/policygen.html

Policy JSON Document

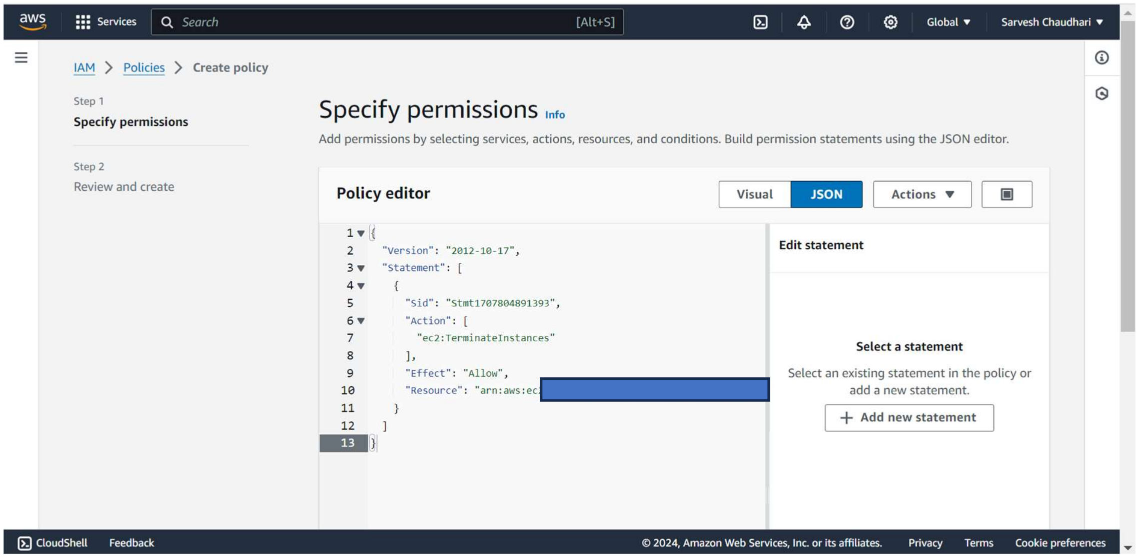
Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will **not be reflected in the policy generator tool.**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1707804891393",
      "Action": [
        "ec2:TerminateInstances"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2[redacted]
    }
  ]
}
```

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.

Copy the policy JSON code and paste it in AWS policy editor



IAM > Policies > Create policy

Step 1
**Specify permissions**

Step 2
Review and create

## Specify permissions Info

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

**Policy editor**

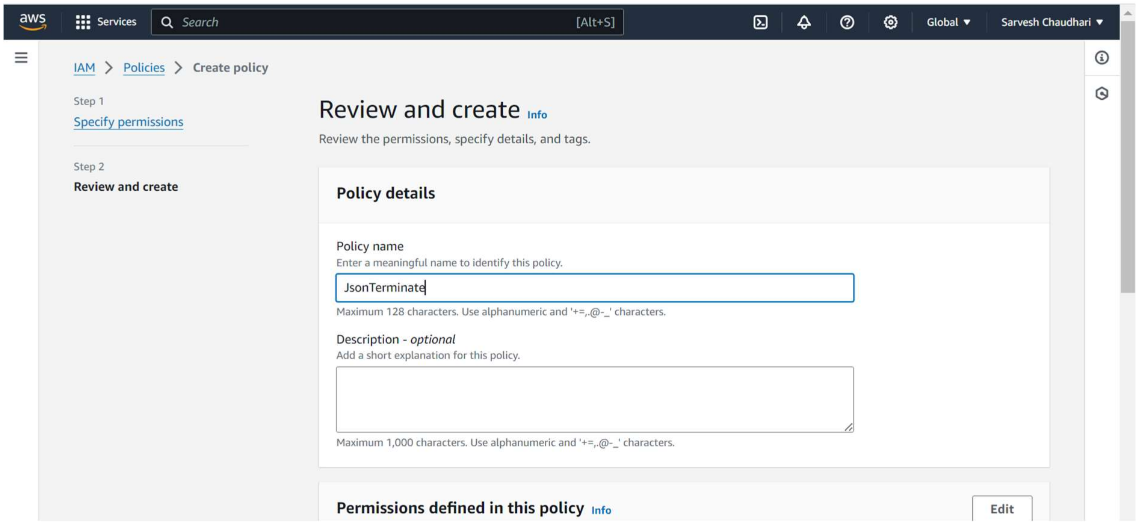
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1707804891393",
      "Action": [
        "ec2:TerminateInstances"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec[redacted]
    }
  ]
}
```

**Edit statement**

**Select a statement**

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

Click on next



IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
**Review and create**

## Review and create Info

Review the permissions, specify details, and tags.

**Policy details**

Policy name
Enter a meaningful name to identify this policy.
JsonTerminate
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

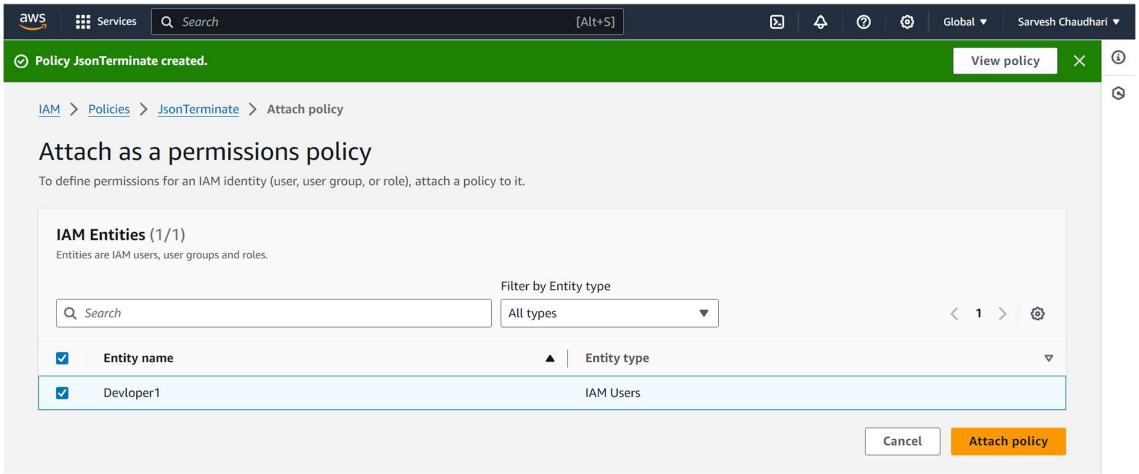
Description - *optional*
Add a short explanation for this policy.

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

**Permissions defined in this policy** Info

Now scroll down and then create policy

Our policy created successfully now attach this policy to user



Policy JsonTerminate created.

## Attach as a permissions policy

To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

**IAM Entities** (1/1)

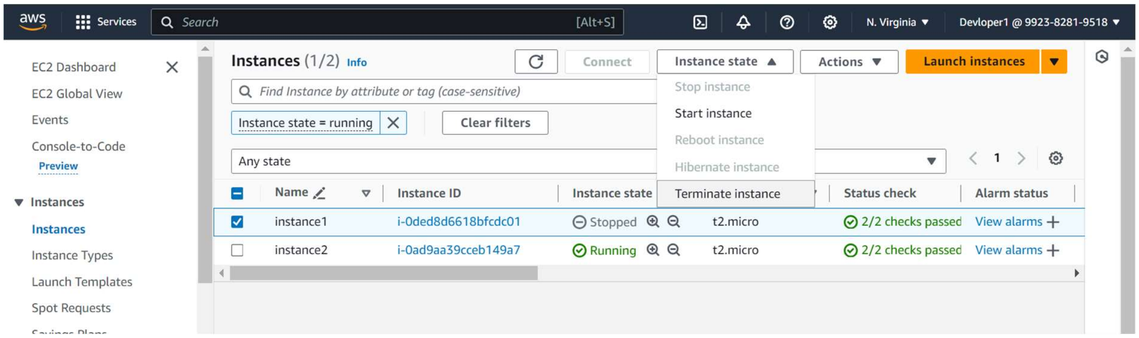
Entities are IAM users, user groups and roles.

Filter by Entity type: All types

| ☑ | Entity name | Entity type |
|---|---|---|
| ☑ | Devloper1 | IAM Users |

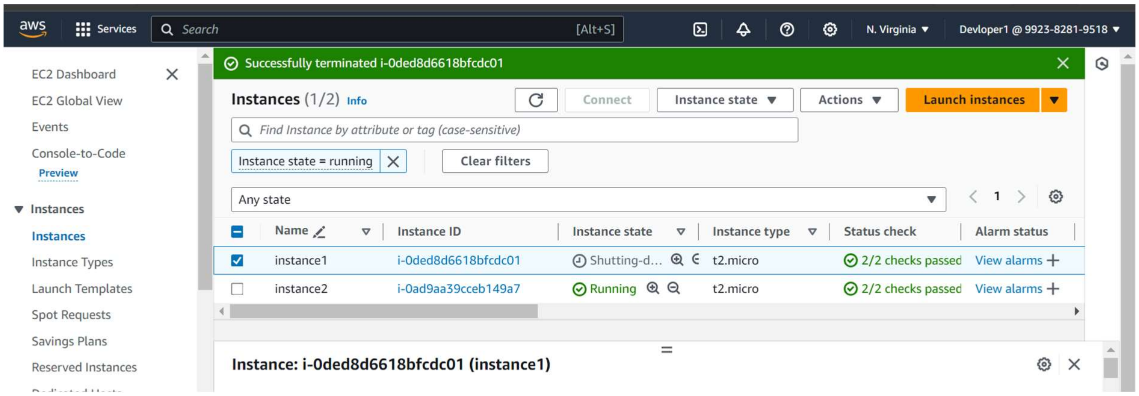
Click on Attach Policy

Now trying permissions are granted or not



**Instances** (1/2)

| ☐ | Name | Instance ID | Instance state | Instance type | Status check | Alarm status |
|---|---|---|---|---|---|---|
| ☑ | instance1 | i-0ded8d6618bfcdc01 | Stopped | t2.micro | 2/2 checks passed | View alarms + |
| ☐ | instance2 | i-0ad9aa39cceb149a7 | Running | t2.micro | 2/2 checks passed | View alarms + |



Successfully terminated i-0ded8d6618bfcdc01

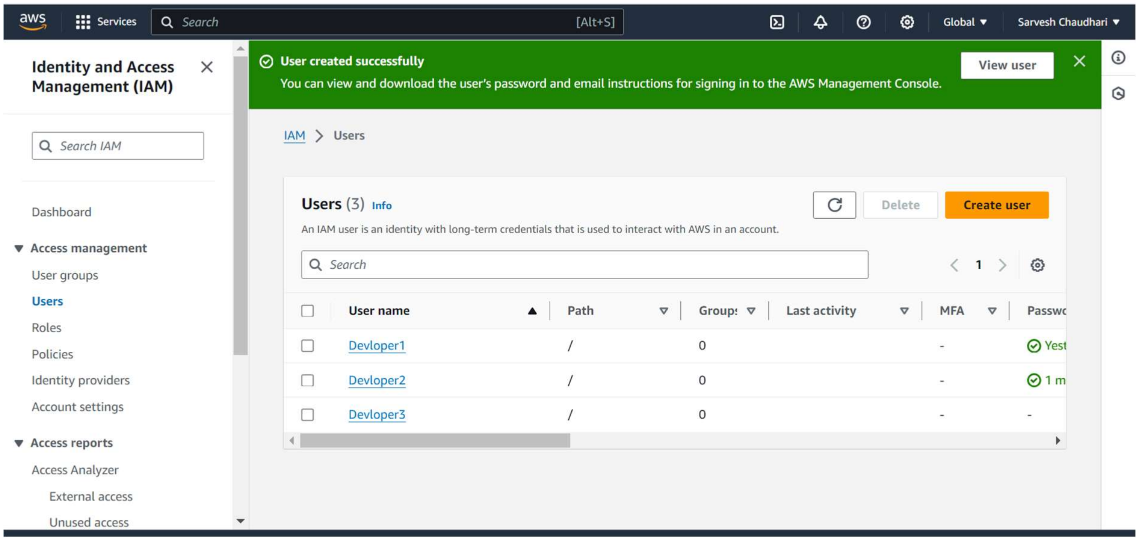
**Instances** (1/2)

| ☐ | Name | Instance ID | Instance state | Instance type | Status check | Alarm status |
|---|---|---|---|---|---|---|
| ☑ | instance1 | i-0ded8d6618bfcdc01 | Shutting-d... | t2.micro | 2/2 checks passed | View alarms + |
| ☐ | instance2 | i-0ad9aa39cceb149a7 | Running | t2.micro | 2/2 checks passed | View alarms + |

**Instance: i-0ded8d6618bfcdc01 (instance1)**

Now creating Groups

1st Created 3 dummy users now creating group from it.



User created successfully

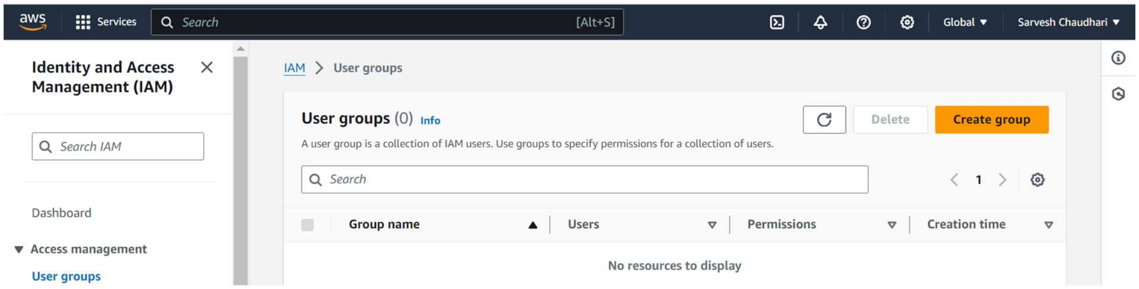
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Users (3) Info

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

| ☐ | User name | Path | Groups | Last activity | MFA | Passwo |
|---|---|---|---|---|---|---|
| ☐ | Devloper1 | / | 0 | | - | ✓ Yest |
| ☐ | Devlopr2 | / | 0 | | - | ✓ 1 m |
| ☐ | Devloper3 | / | 0 | | - | - |

Now go to users then click on create groups.



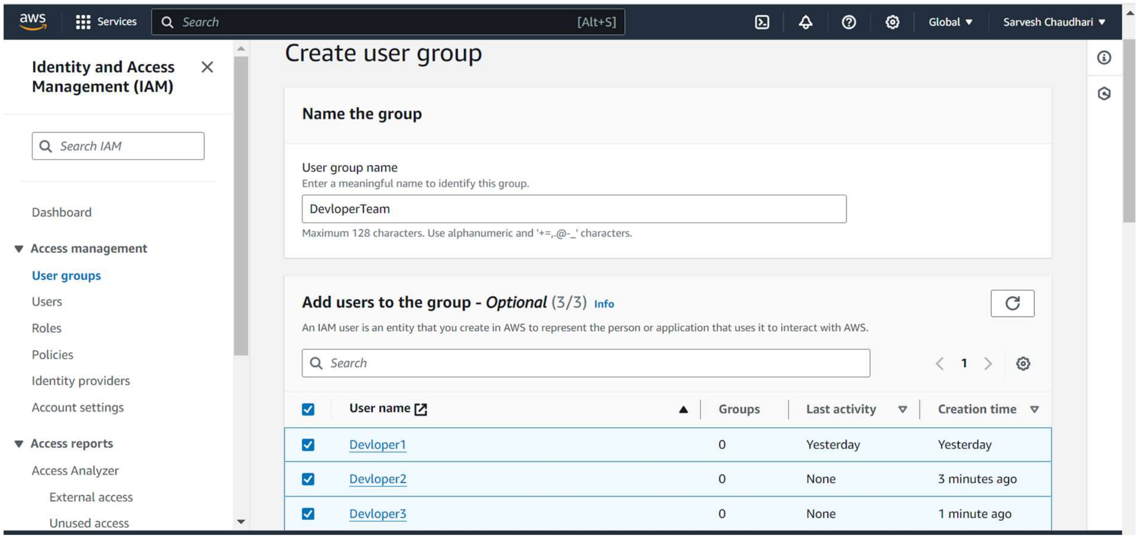
User groups (0) Info

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 |
|---|---|---|---|---|

No resources to display

Now give group name and then add users to that group



Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

DevloperTeam

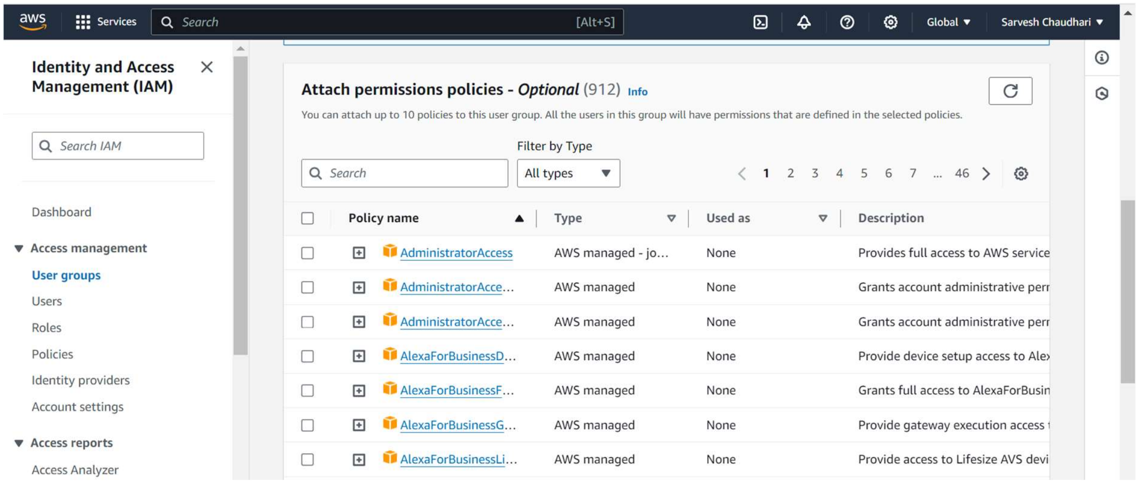
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (3/3) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

| ☑ | User name | Groups | Last activity | Creation time |
|---|---|---|---|---|
| ☑ | Devloper1 | 0 | Yesterday | Yesterday |
| ☑ | Devloper2 | 0 | None | 3 minutes ago |
| ☑ | Devloper3 | 0 | None | 1 minute ago |

Now we can add permission or can add permission latter



Attach permissions policies - *Optional* (912) Info

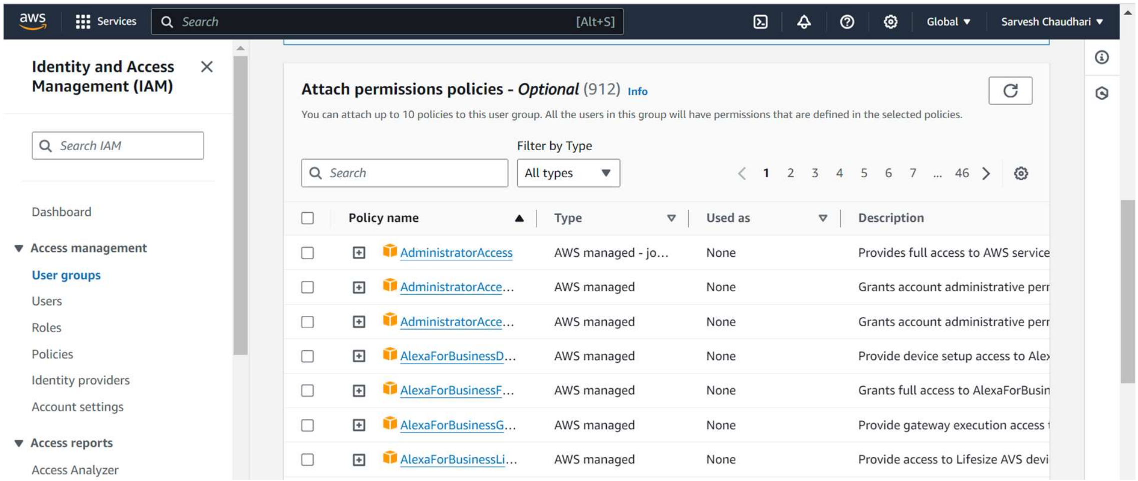
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type: All types

| □ | Policy name | Type | Used as | Description |
|---|---|---|---|---|
| □ | AdministratorAccess | AWS managed - jo… | None | Provides full access to AWS service |
| □ | AdministratorAcce… | AWS managed | None | Grants account administrative perr |
| □ | AdministratorAcce… | AWS managed | None | Grants account administrative perr |
| □ | AlexaForBusinessD… | AWS managed | None | Provide device setup access to Alex |
| □ | AlexaForBusinessF… | AWS managed | None | Grants full access to AlexaForBusin |
| □ | AlexaForBusinessG… | AWS managed | None | Provide gateway execution access |
| □ | AlexaForBusinessLi… | AWS managed | None | Provide access to Lifesize AVS devi |

Now click on create group.

Now go permission policies then  select EC2full access



Attach permissions policies - *Optional* (912) Info

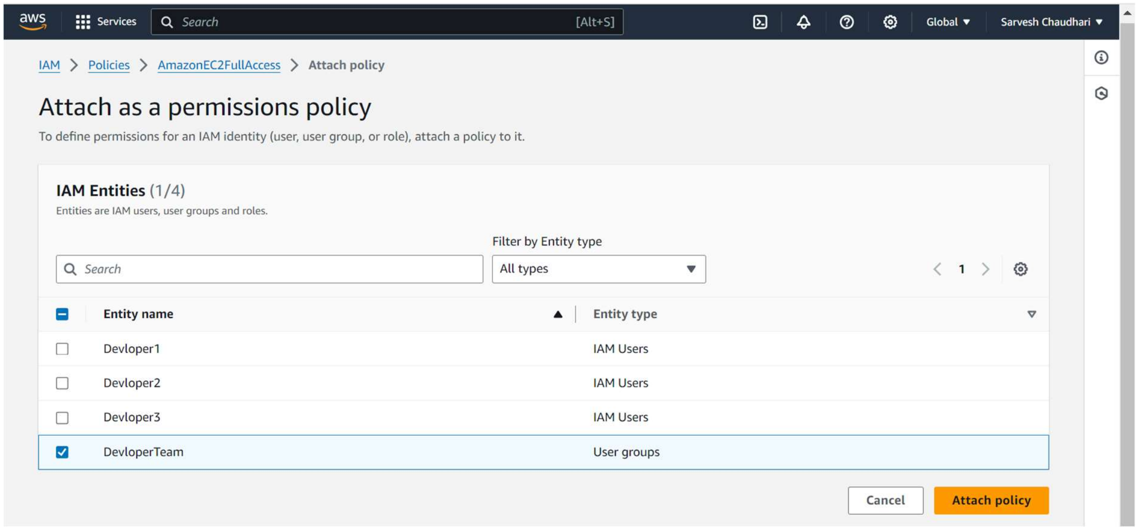
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type: All types

| □ | Policy name | Type | Used as | Description |
|---|---|---|---|---|
| □ | AdministratorAccess | AWS managed - jo… | None | Provides full access to AWS service |
| □ | AdministratorAcce… | AWS managed | None | Grants account administrative perr |
| □ | AdministratorAcce… | AWS managed | None | Grants account administrative perr |
| □ | AlexaForBusinessD… | AWS managed | None | Provide device setup access to Alex |
| □ | AlexaForBusinessF… | AWS managed | None | Grants full access to AlexaForBusin |
| □ | AlexaForBusinessG… | AWS managed | None | Provide gateway execution access |
| □ | AlexaForBusinessLi… | AWS managed | None | Provide access to Lifesize AVS devi |

then select permission and from action select attach.

Now select either user or group then click on attach policy



IAM > Policies > AmazonEC2FullAccess > Attach policy

Attach as a permissions policy

To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

**IAM Entities** (1/4)

Entities are IAM users, user groups and roles.

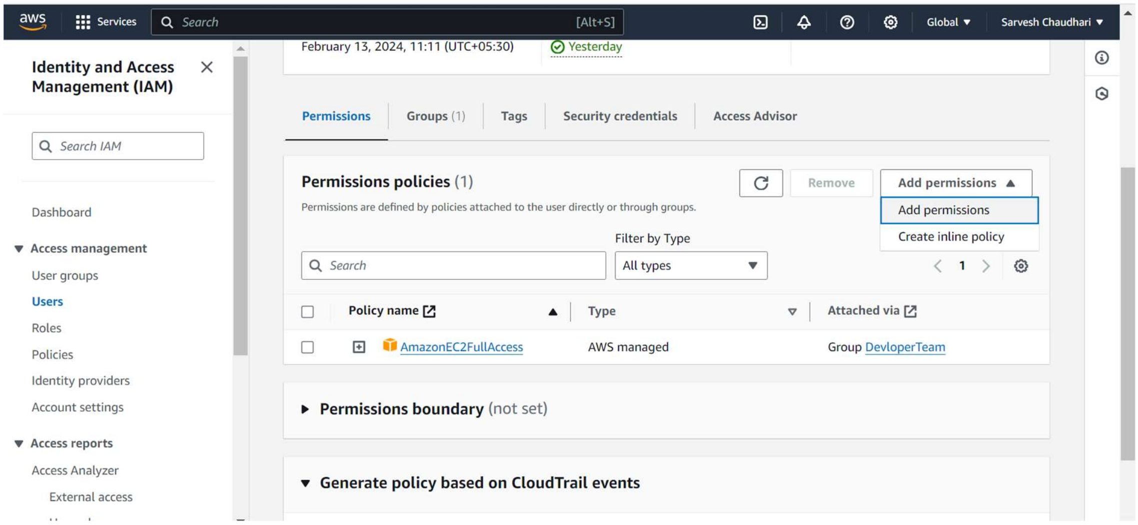
Search | Filter by Entity type: All types

| | Entity name | Entity type |
|---|---|---|
| □ | Devloper1 | IAM Users |
| □ | Devloper2 | IAM Users |
| □ | Devloper3 | IAM Users |
| ☑ | DevloperTeam | User groups |

Now policy are attached.

Now developer team permission allowed now we devloper1 we denying permission to delete

Now click on devloper1 we will add permission



February 13, 2024, 11:11 (UTC+05:30) | Yesterday

**Permissions policies** (1)

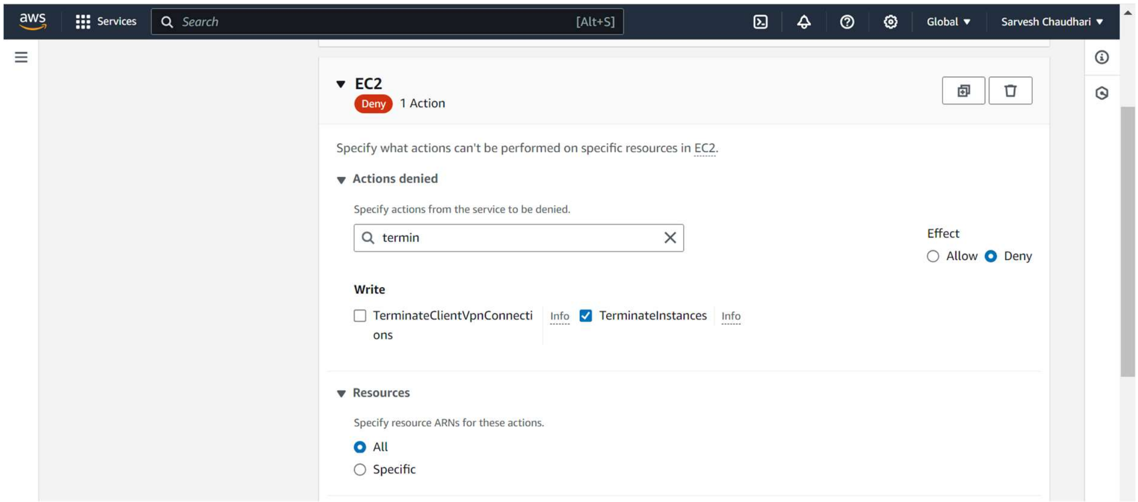
Permissions are defined by policies attached to the user directly or through groups.

| □ | Policy name | Type | Attached via |
|---|---|---|---|
| □ | AmazonEC2FullAccess | AWS managed | Group DevloperTeam |

▶ **Permissions boundary** (not set)

▼ **Generate policy based on CloudTrail events**

Create inline policy then search terminate instance and deny permission and create policy



EC2

Deny 1 Action

Specify what actions can't be performed on specific resources in EC2.

Actions denied

Specify actions from the service to be denied.

termin

Effect

○ Allow ● Deny

Write

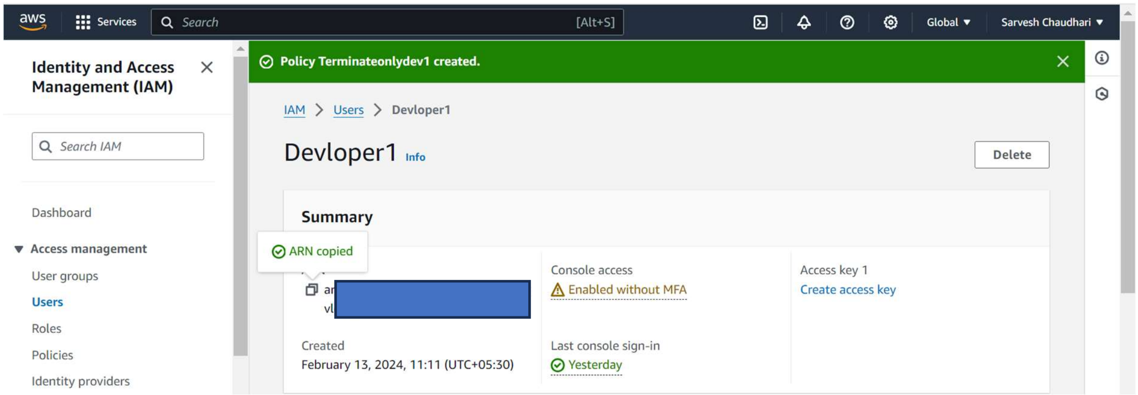
☐ TerminateClientVpnConnections Info ☑ TerminateInstances Info

Resources

Specify resource ARNs for these actions.

● All

○ Specific



Policy Terminateonlydev1 created.

IAM > Users > Devloper1

Devloper1 Info

Delete

Summary

ARN copied

ar [redacted]
vl

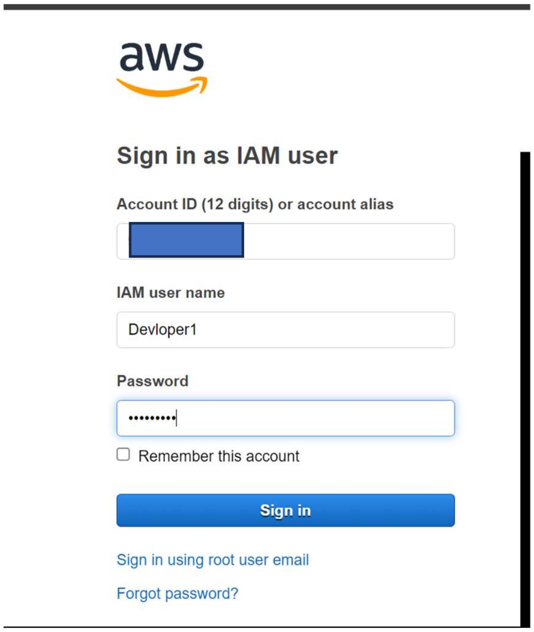
Console access
Enabled without MFA

Access key 1
Create access key

Created
February 13, 2024, 11:11 (UTC+05:30)

Last console sign-in
Yesterday

Now signing with devloper1 account



Sign in as IAM user

Account ID (12 digits) or account alias

[redacted]

IAM user name

Devloper1

Password

•••••••••

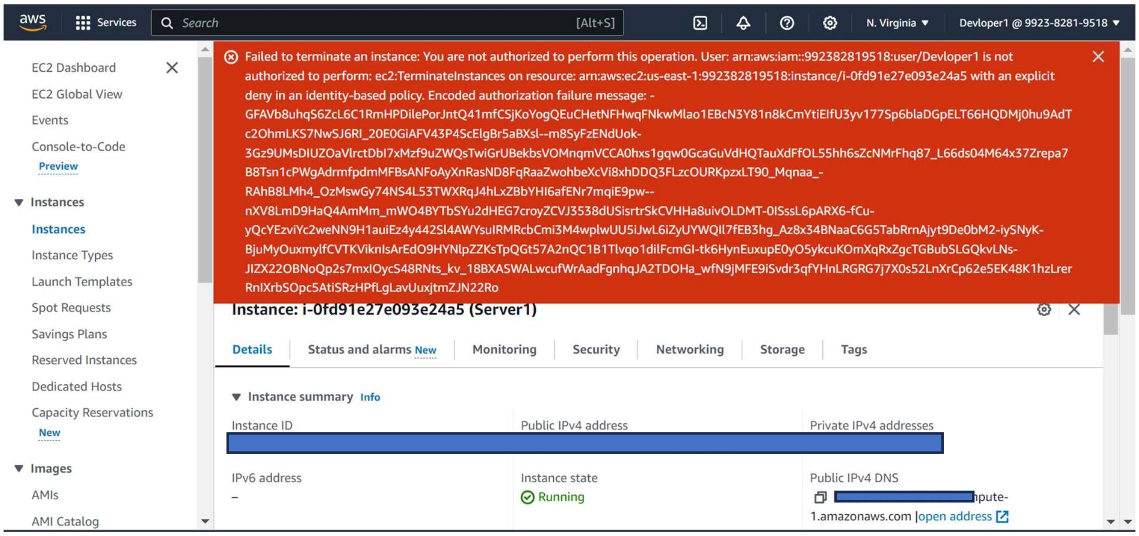
☐ Remember this account

Sign in

Sign in using root user email

Forgot password?

Now using this account tried to terminate the instance but as permission is not allowed instance can not terminate by devloper1 account



```
Failed to terminate an instance: You are not authorized to perform this operation. User: arn:aws:iam::992382819518:user/Devloper1 is not
authorized to perform: ec2:TerminateInstances on resource: arn:aws:ec2:us-east-1:992382819518:instance/i-0fd91e27e093e24a5 with an explicit
deny in an identity-based policy. Encoded authorization failure message: -
GFAVb8uhqS6ZcL6C1RmHPDilePorJntQ41mfCSjKoYogQEuCHetNFHwqFNkwMlao1EBcN3Y81n8kCmYtiElfU3yv177Sp6blaDGpELT66HQDMj0hu9AdT
c2OhmLKS7NwSJ6RI_20E0GiAFV43P4ScElgBr5aBXsl--m8SyFzENdUok-
3Gz9UMsDIUZOaVlrctDbI7xMzf9uZWQsTwiGrUBekbsVOMnqmVCCA0hxs1gqw0GcaGuVdHQTauXdFfOL55hh6sZcNMrFhq87_L66ds04M64x37Zrepa7
B8Tsn1cPWgAdrmfpdmMFBsANFoAyXnRasND8FqRaaZwohbeXcVi8xhDDQ3FLzcOURKpzxLT90_Mqnaa_-
RAhB8LMh4_OzMswGy74NS4L53TWXRqJ4hLxZBbYHI6afENr7mqiE9pw--
nXV8LmD9HaQ4AmMm_mWO4BYTbSYu2dHEG7croyZCVJ3538dUSisrtrSkCVHHa8uivOLDMT-0ISssL6pARX6-fCu-
yQcYEzviYc2weNN9H1auiEz4y442Sl4AWYsuIRMRcbCmi3M4wplwUU5iJwL6iZyUYWQIl7fEB3hg_Az8x34BNaaC6G5TabRrnAjyt9De0bM2-iySNyK-
BjuMyOuxmylfCVTKViknIsArEdO9HYNlpZZKsTpQGt57A2nQC1B1Tlvqo1dilFcmGI-tk6HynEuxupE0yO5ykcuKOmXqRxZgcTGBubSLGQkvLNs-
JIZX22OBNoQp2s7mxIOycS48RNts_kv_18BXASWALwcufWrAadFgnhqJA2TDOHa_wfN9jMFE9iSvdr3qfYHnLRGRG7j7X0s52LnXrCp62e5EK48K1hzLrer
RnIXrbSOpc5AtiSRzHPfLgLavUuxjtmZJN22Ro
```

Instance: i-0fd91e27e093e24a5 (Server1)

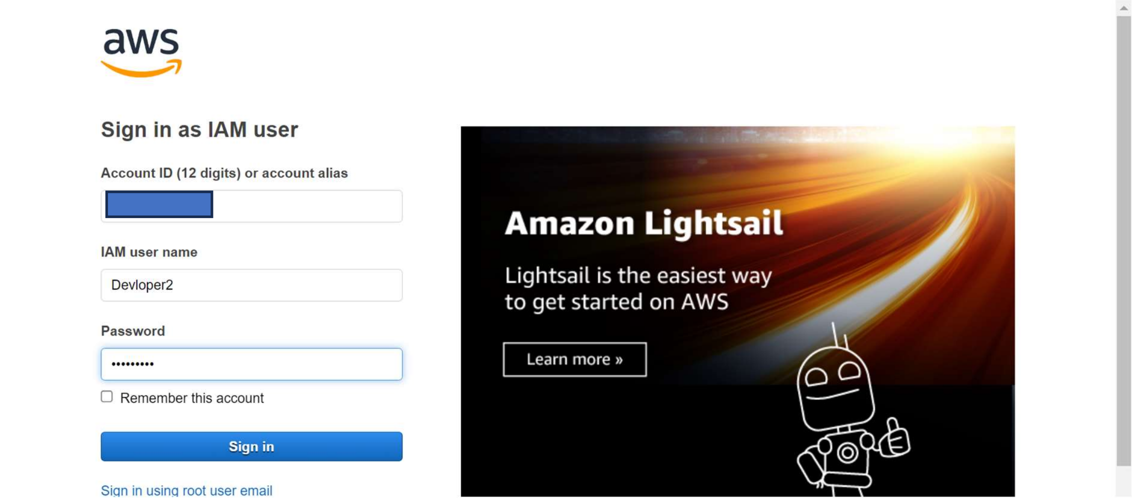
Instance ID
Public IPv4 address
Private IPv4 addresses
[redacted]

IPv6 address
–

Instance state
Running

Public IPv4 DNS
[redacted]pute-1.amazonaws.com |open address

Now signing with devoper2 account


aws
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »

Sign in as IAM user

Account ID (12 digits) or account alias
[redacted]

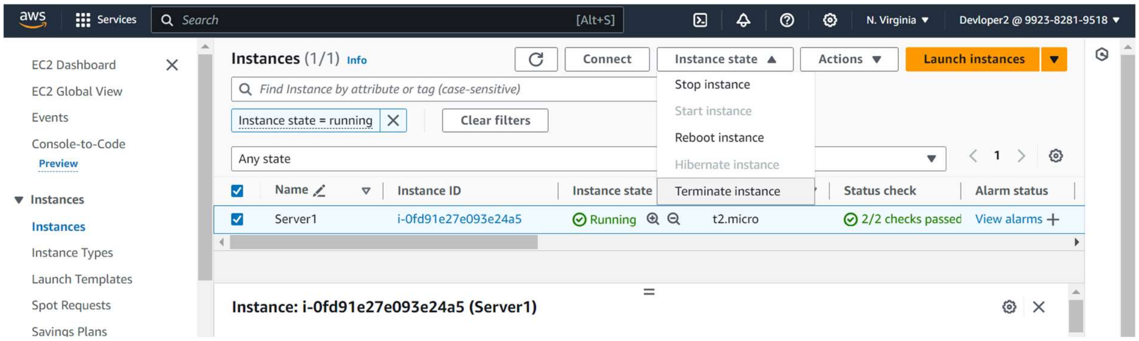
IAM user name
Devloper2

Password
•••••••••

□ Remember this account

Sign in
Sign in using root user email

Trying to terminate instance with devoper2 account

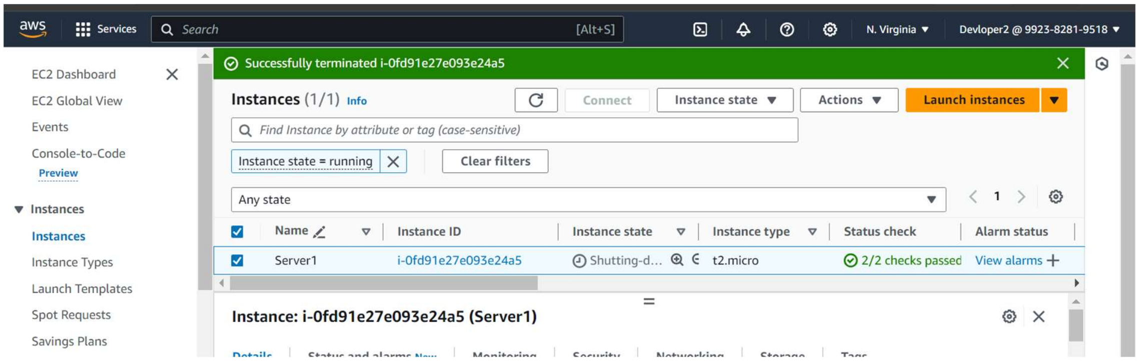


Instance state = running ✕

| ☑ | Name | Instance ID | Instance state | | Status check | Alarm status |
|---|---|---|---|---|---|---|
| ☑ | Server1 | i-0fd91e27e093e24a5 | Running | t2.micro | 2/2 checks passed | View alarms + |

Instance: i-0fd91e27e093e24a5 (Server1)

As expected devoper2 has permission to terminate so instance is terminated.



Successfully terminated i-0fd91e27e093e24a5

Instances (1/1)

Find Instance by attribute or tag (case-sensitive)

Instance state = running

Any state

| ☑ | Name | Instance ID | Instance state | Instance type | Status check | Alarm status |
|---|---|---|---|---|---|---|
| ☑ | Server1 | i-0fd91e27e093e24a5 | Shutting-d… | t2.micro | 2/2 checks passed | View alarms + |

Instance: i-0fd91e27e093e24a5 (Server1)