

1.

- a. Create a user account that can login to the console
- b. Create a group and make sure that the group can only launch and stop EC2 instances using that previously created account.

The screenshot shows the AWS IAM console in the 'Specify user details' step. The breadcrumb navigation is 'IAM > Users > Create user'. A sidebar on the left lists the steps: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password). The main content area is titled 'Specify user details' and contains a 'User details' section. In this section, the 'User name' field is filled with 'Login-user'. Below this, there is a checkbox labeled 'Provide user access to the AWS Management Console - optional' which is checked. A note explains that this is a best practice for managing access in IAM Identity Center. A blue information box asks 'Are you providing console access to a person?' and offers two options: 'Specify a user in Identity Center - Recommended' and 'I want to create an IAM user', which is selected.

Step 1  
**Specify user details**

Step 2  
Set permissions

Step 3  
Review and create

Step 4  
Retrieve password

## Specify user details

### User details

User name

Login-user

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

This screenshot shows the lower portion of the 'Specify user details' step. It features a blue information box recommending the creation of IAM users for programmatic access. Below this, the 'Console password' section has two options: 'Autogenerated password' and 'Custom password'. The 'Custom password' option is selected, and a password field is visible with masked characters. A list of password requirements is provided: at least 8 characters long and including at least three of uppercase letters, lowercase letters, numbers, and symbols. There is also a 'Show password' checkbox. At the bottom, a checkbox 'Users must create a new password at next sign-in - Recommended' is checked, with a note that this policy allows users to change their own password. A final blue information box states that access keys or service-specific credentials can be generated after the user is created.

☒ 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](#)

← → ↻ https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create ☆

aws Services Search [Alt+S] Global Login-user @ 0518-7539-2745

EC2 VPC CloudWatch Route 53 RDS

Step 2  
**Set permissions**

Step 3  
Review and create

Step 4  
Retrieve password

**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 (1/1174)** [Refresh](#) [Create policy](#)

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

Search  Filter by Type

< 1 2 3 4 5 6 7 ... 59 > ⚙

<input type="checkbox"/>	<input type="checkbox"/> Policy name <a href="#">External link</a>	Type	Attached entities
<input type="checkbox"/>	<input type="checkbox"/> <a href="#">AccessAnalyzerServiceR...</a>	AWS managed	0
<input checked="" type="checkbox"/>	<input type="checkbox"/> <a href="#">AdministratorAccess</a>	AWS managed - job function	4

Login url /details download

← → ↻ https://signin.aws.amazon.com/clm?action=changepassword&userType=iam&redirect\_uri=https ☆

aws

You must change your password to continue

**AWS account** 051875392745

**IAM user name** Login-user

**Old password**

**New password**

**Retype new password**

[Confirm password change](#)

[Sign in using root user email](#)

English

[Terms of Use](#) [Privacy Policy](#) © 1996-2024, Amazon Web Services, Inc. or its affiliates.

b. Create a group and make sure that the group can only launch and stop EC2 instances using that previously created account.

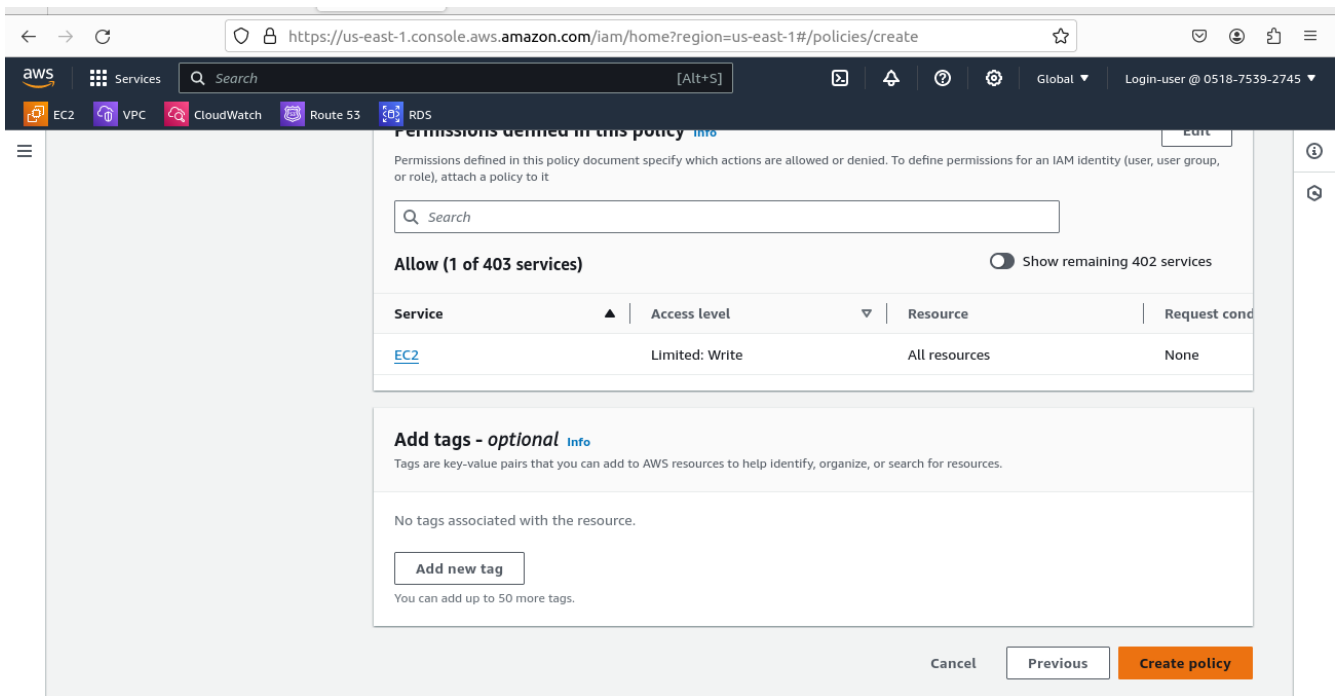
## CREATE POLICY

The screenshot shows the AWS IAM console interface for creating a new policy. The browser address bar displays `https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create`. The navigation bar includes the AWS logo, a search bar, and service icons for EC2, VPC, CloudWatch, Route 53, and RDS. The user is logged in as 'Login-user @ 0518-7539-2745'. The breadcrumb trail indicates the path: IAM > Policies > Create policy. On the left, a sidebar shows 'Step 1 Specify permissions' as the active step, with 'Step 2 Review and create' listed below it. The main content area is titled 'Specify permissions' with an 'Info' link. Below the title, it says 'Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.' The 'Policy editor' section has tabs for 'Visual', 'JSON' (which is selected), and 'Actions'. The JSON editor contains the following code:

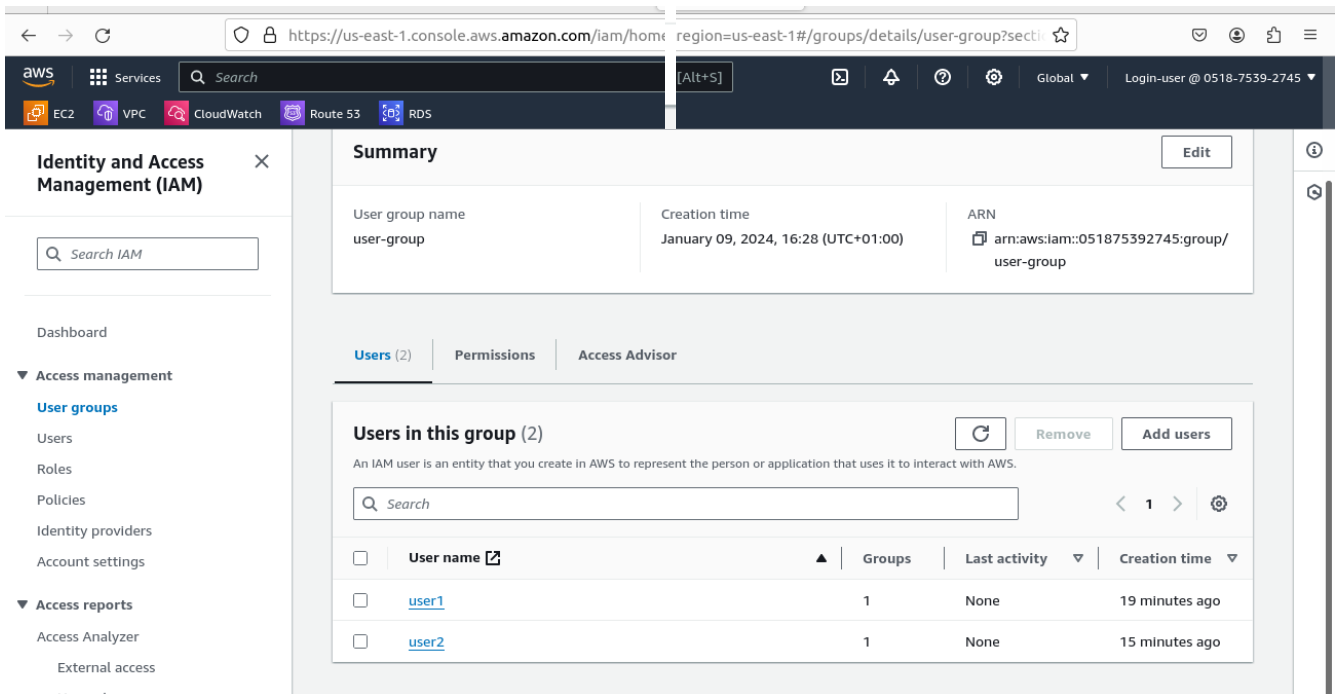
```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "ec2:RunInstances",
8         "ec2:TerminateInstances"
9       ],
10      "Resource": "*"
11    }
12  ]
13 }
14
```

To the right of the JSON editor is the 'Edit statement' section, which prompts the user to 'Select a statement' and provides a '+ Add new statement' button.

The screenshot shows the 'Review and create' step of the AWS IAM console policy creation process. The browser address bar remains the same. The breadcrumb trail is now IAM > Policies > Create policy > Review and create. The sidebar shows 'Step 2 Review and create' as the active step. The main content area is titled 'Review the permissions, specify details, and tags.' The 'Policy details' section contains two text input fields: 'Policy name' with the value 'launch-stop-instance' and 'Description - optional' with the value 'permission to launch and terminate Instance'. Below these fields are character limits: 'Maximum 128 characters. Use alphanumeric and '+=, @, \_' characters.' for the name, and 'Maximum 1,000 characters. Use alphanumeric and '+=, @, \_' characters.' for the description. The 'Permissions defined in this policy' section includes an 'Info' link, a brief explanation of permissions, and a search bar.



USER GROUP: HAS 2 USERS: USER1 AND USER2



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*"
    }
  ]
}
```

[illegible]

2a. Provide permission to let the user of a previously created account to create VPCs, Subnets, NACL and security groups  
(create custom IAM policies for these actions and attach them to the user/GROUP)

← → ↻ <https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create> ☆

aws Services Search [Alt+S] Global Login-user @ 0518-7539-2745

EC2 VPC CloudWatch Route 53 RDS

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

Visual **JSON** Actions

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "ec2:CreateVpc",
8         "ec2:CreateSubnet",
9         "ec2:CreateNetworkAcl",
10        "ec2:CreateSecurityGroup"
11      ],
12      "Resource": "*"
13    }
14  ]
15 }
```

#### Edit statement

Remove

#### Add actions

Choose a service

Filter services

#### Included

EC2

#### Available

AMP  
API Gateway

← → ↻ <https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create> ☆

aws Services Search [Alt+S] Global Login-user @ 0518-7539-2745

EC2 VPC CloudWatch Route 53 RDS

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.

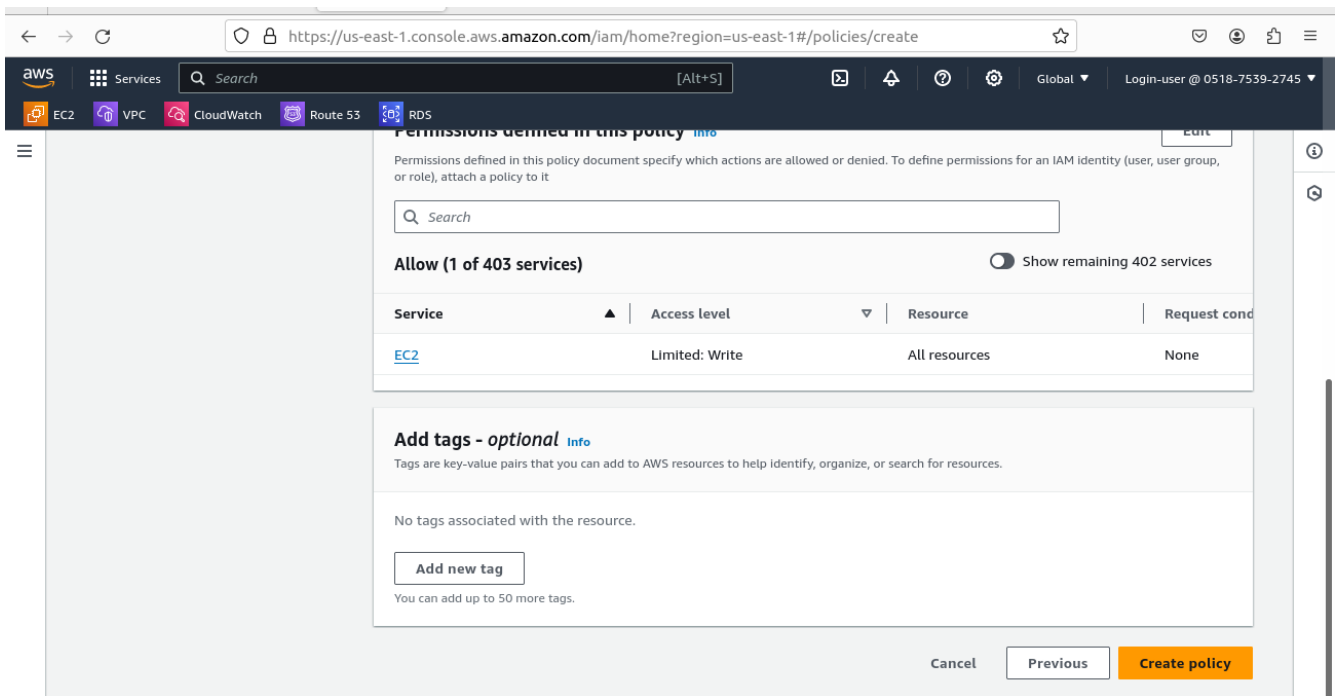
### Permissions defined in this policy [Info](#)

[Edit](#)

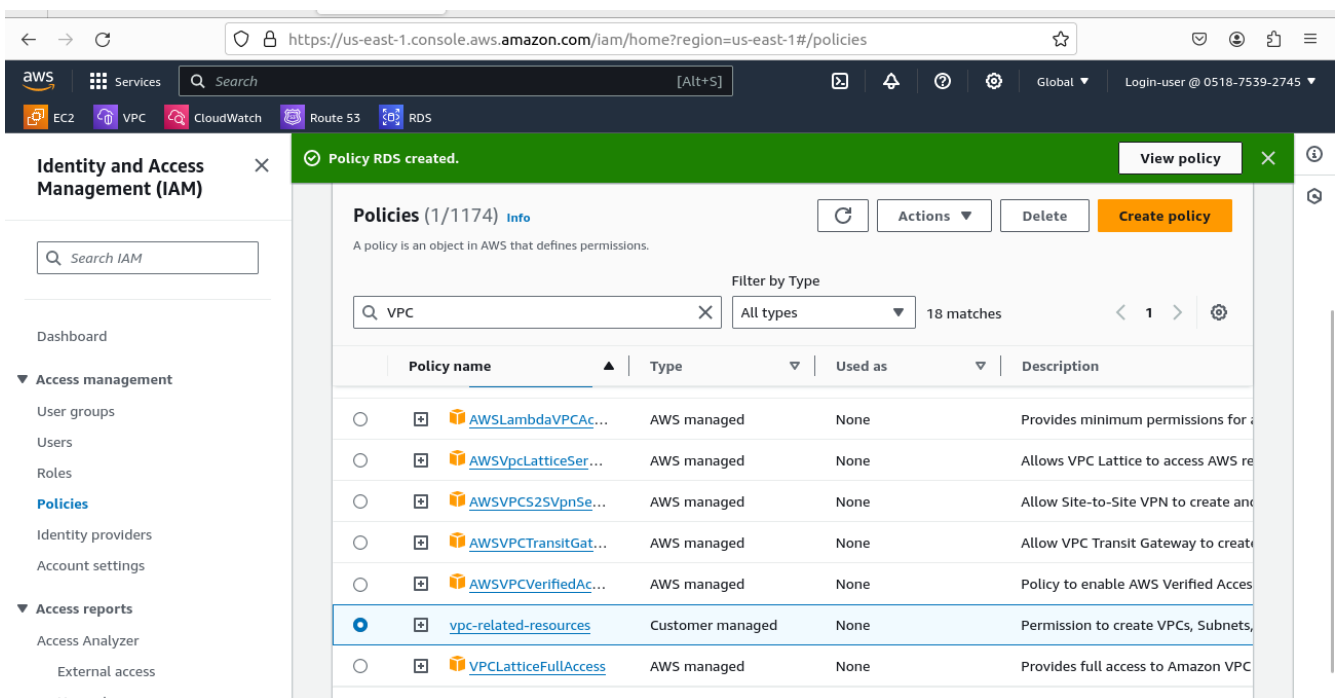
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (1 of 403 services) ☐ Show remaining 402 services

Service	Access level	Resource	Request cond
EC2	Full control	All resources	



ATTACH THE CUSTOM 'vpc-related-policy' TO THE GROUP CREATED IN EXERCISE 2 ABOVE



The screenshot shows the AWS IAM console interface. The breadcrumb navigation is IAM > Policies > vpc-related-resources > Attach policy. The main heading is "Attach as a permissions policy" with a subtext: "To define permissions for an IAM Identity (user, user group, or role), attach a policy to it."

The "IAM Entities (16)" section shows a list of entities. The "Filter by Entity type" dropdown is set to "All types". The table below lists the entities:

Entity name	Entity type
aws-elasticbeanstalk-service-role	Roles
AWSBackupDefaultServiceRole	Roles
Dev-Team	User groups
Dev1	IAM Users
Dev2	IAM Users
Instance-profile	Roles
lambda_role	Roles
Login-user	IAM Users
myfunction-role-xb7ynfgq	Roles
myredshifts3access	Roles
ops-Team	User groups
rds-monitoring-role	Roles
Test1	IAM Users
Test2	IAM Users
<input checked="" type="checkbox"/> user-group	User groups
VPC-DYNAMODB-ROLE	Roles

At the bottom right, there are two buttons: "Cancel" and "Attach policy".

b. Further add the permission so that the user can create RDS instance



← → ↺

https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create

☆

🔔 👤 📄 ☰

aws

Services

Search

[Alt+S]

📄 🔔 ⓘ ⚙️

Global ▾

Login-user @ 0518-7539-2745 ▾

EC2 VPC CloudWatch Route 53 RDS

☰

Policy vpc-related-resources created. View policy ✕ ⓘ

[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.

RDS

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

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

permission to create RDS instance

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

#### 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

← → ↺

https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create

☆

🔔 👤 📄 ☰

aws

Services

Search

[Alt+S]

📄 🔔 ⓘ ⚙️

Global ▾

Login-user @ 0518-7539-2745 ▾

EC2 VPC CloudWatch Route 53 RDS

☰

Policy vpc-related-resources created. View policy ✕ ⓘ

or role), attach a policy to it

🔍 Search

Allow (1 of 403 services)

Show remaining 402 services

Service	Access level	Resource	Request cond
<a href="#">RDS</a>	Limited: Write	All resources	None

#### Add tags - optional Info

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

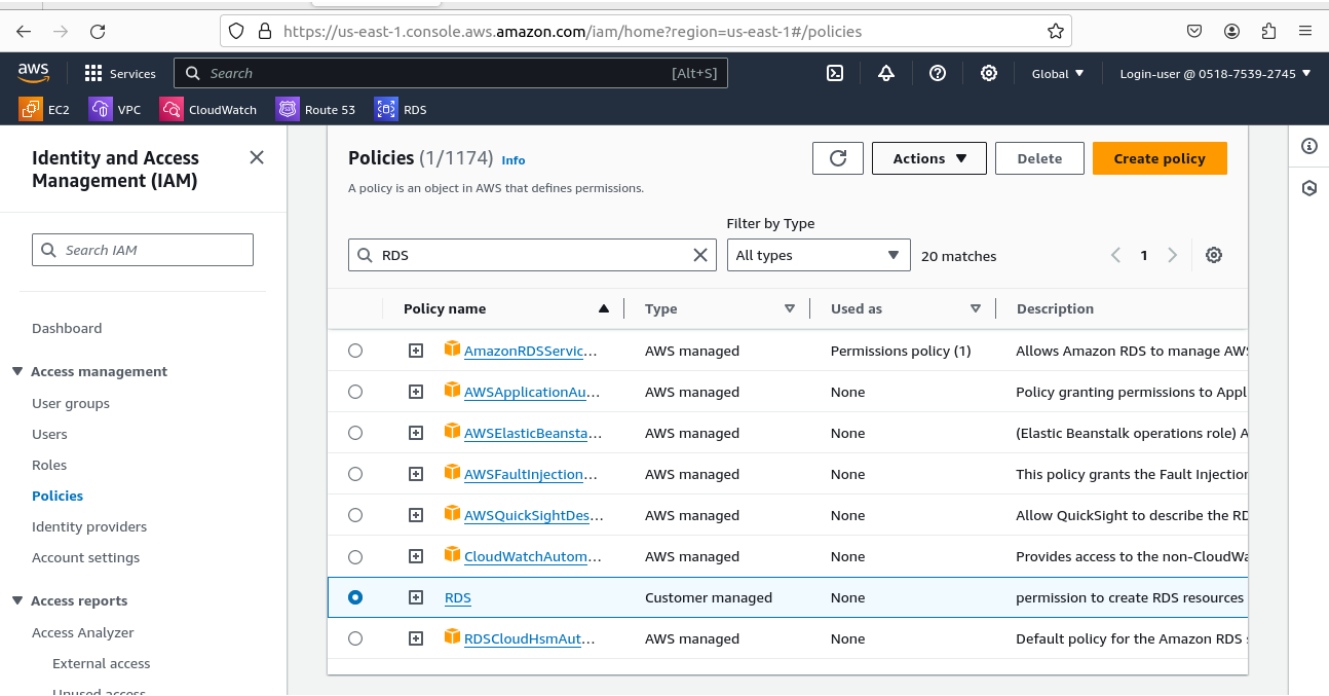
No tags associated with the resource.

Add new tag

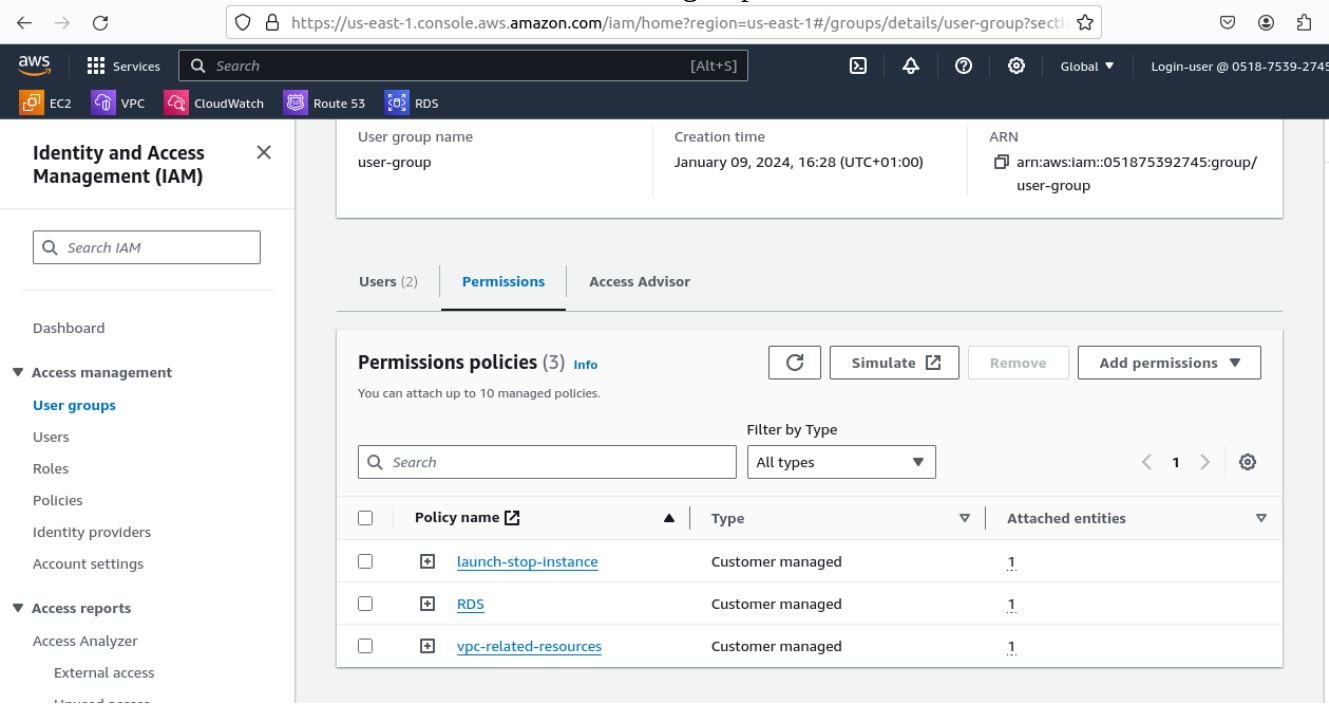
You can add up to 50 more tags.

Cancel Previous Create policy

# ATTACH CUSTOM RDS POLICY



## 3 CUSTOM POLICIES ATTACHED TO THE “user-group”



Explore security options to protect the AWS resources and secure the permissions provided to the group.

This will involve setting up measures such as IAM policies, security groups, network ACLs, and other security i.e data encryption, monitoring logging, regular audit and compliance checks, backup and recover to protect the infrastructure in AWS.