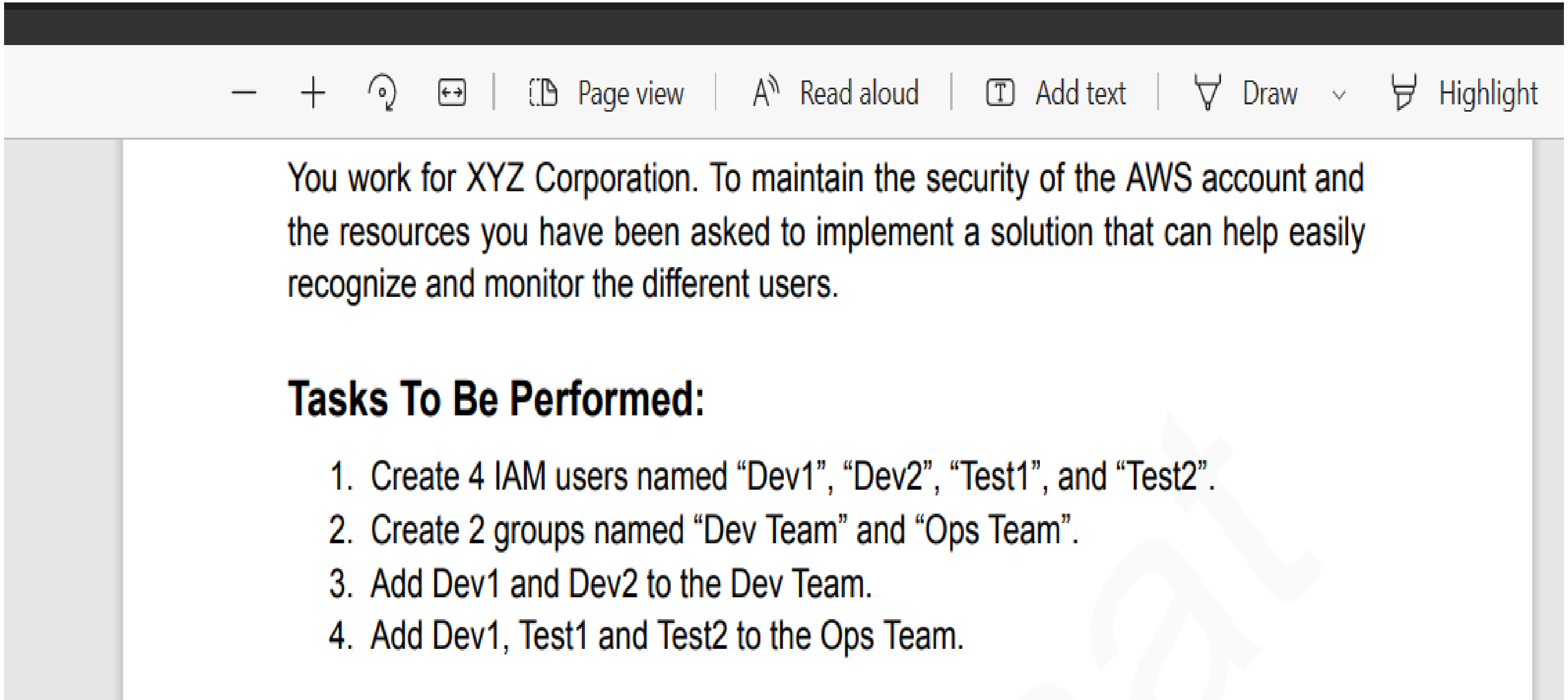
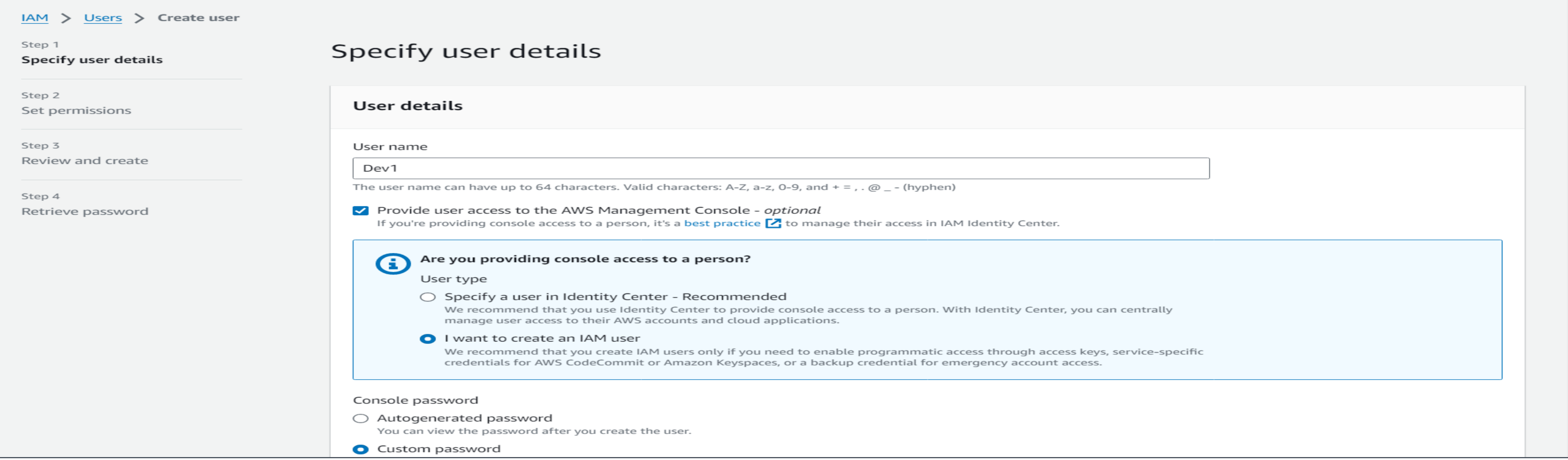
IAM Users



You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

Tasks To Be Performed:

1. Create 4 IAM users named “Dev1”, “Dev2”, “Test1”, and “Test2”.
2. Create 2 groups named “Dev Team” and “Ops Team”.
3. Add Dev1 and Dev2 to the Dev Team.
4. Add Dev1, Test1 and Test2 to the Ops Team.



IAM > Users > Create user

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

Dev1

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

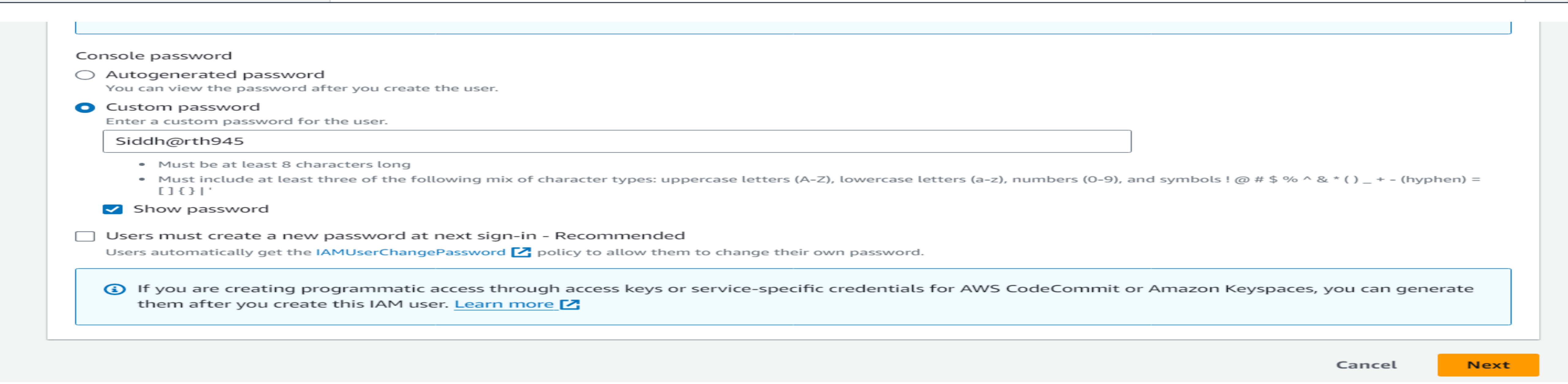
○ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

● 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



Console password

○ Autogenerated password
You can view the password after you create the user.

● Custom password
Enter a custom password for the user.

Siddh@rth945

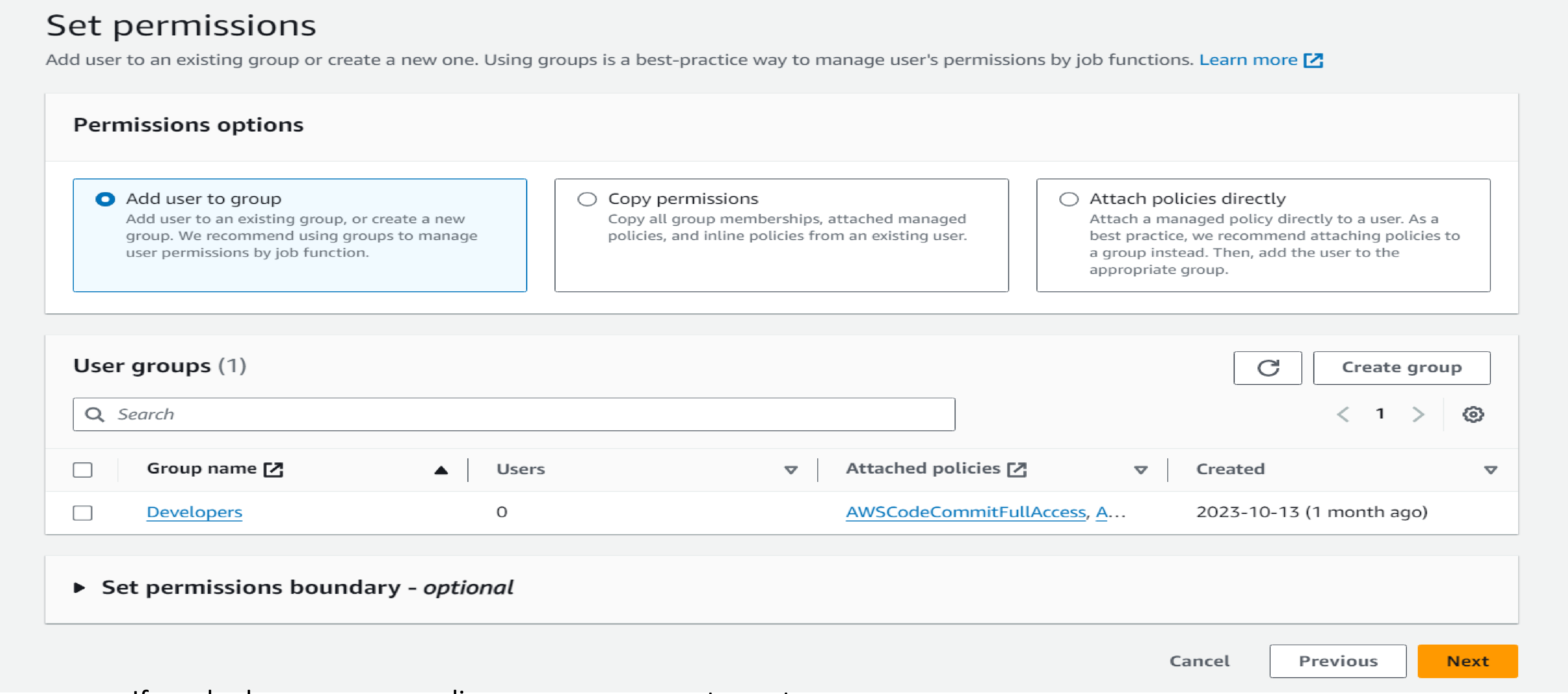
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

☑ 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

Always check user must create new password for real life case sceanario .



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.

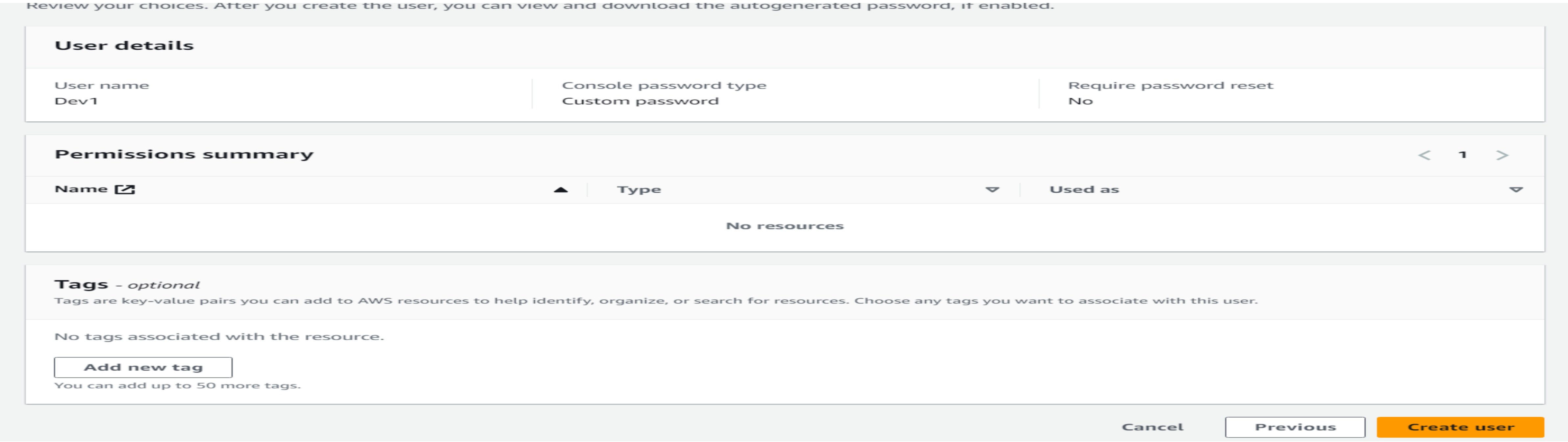
User groups (1)

□	Group name	Users	Attached policies	Created
□	Developers	0	AWSCodeCommitFullAccess, A...	2023-10-13 (1 month ago)

▸ Set permissions boundary - *optional*

If you had any group or policy you can or move to next.

Review and create user.



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

User details

User name	Console password type	Require password reset
Dev1	Custom password	No

Permissions summary

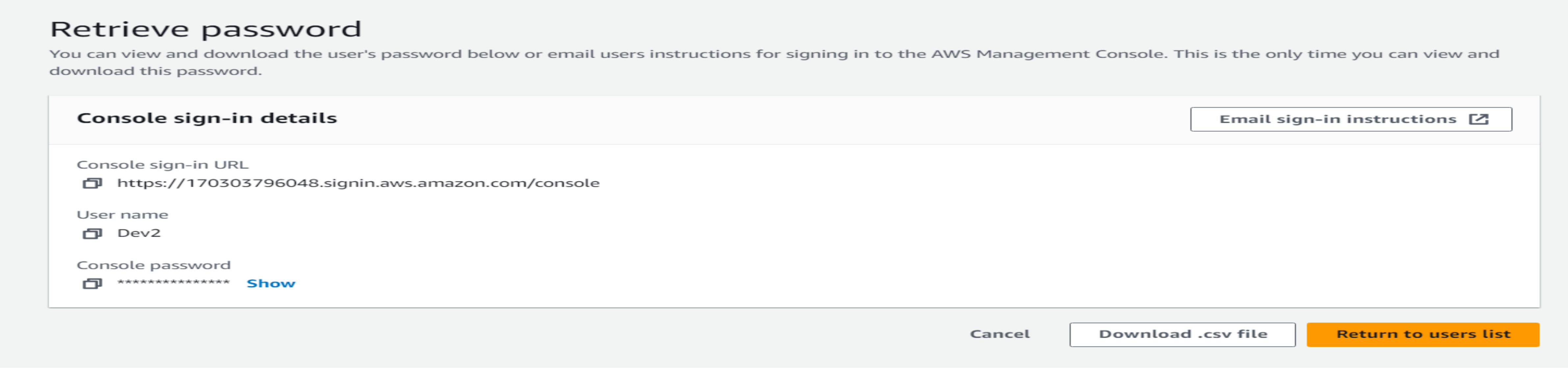
Name	Type	Used as
No resources		

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.

You can add up to 50 more tags.



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.

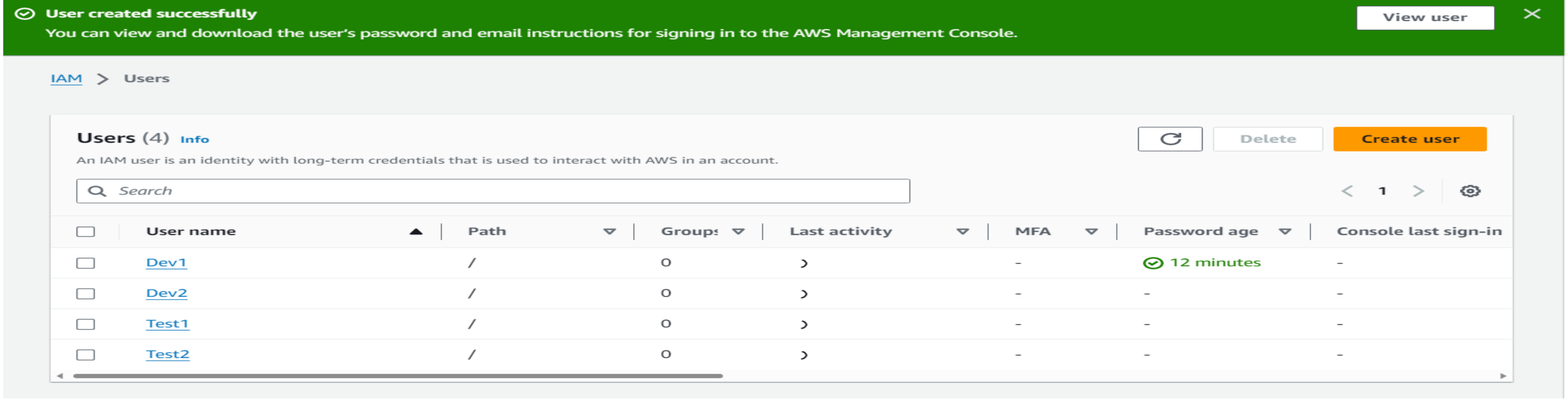
Console sign-in details

Console sign-in URL
https://170303796048.signin.aws.amazon.com/console

User name
Dev2

Console password
****

You can download .csv file which contain all details. Create the rest user in the same manner.



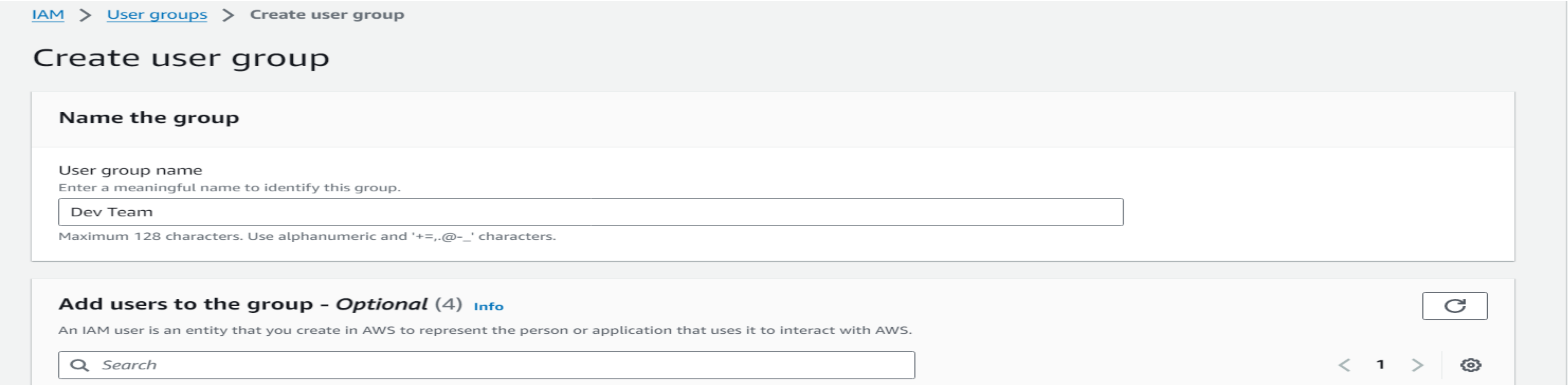
User created successfully

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

Users (4)

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	Password age	Console last sign-in
□	Dev1	/	0	›	-	✓ 12 minutes	-
□	Dev2	/	0	›	-	-	-
□	Test1	/	0	›	-	-	-
□	Test2	/	0	›	-	-	-



Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

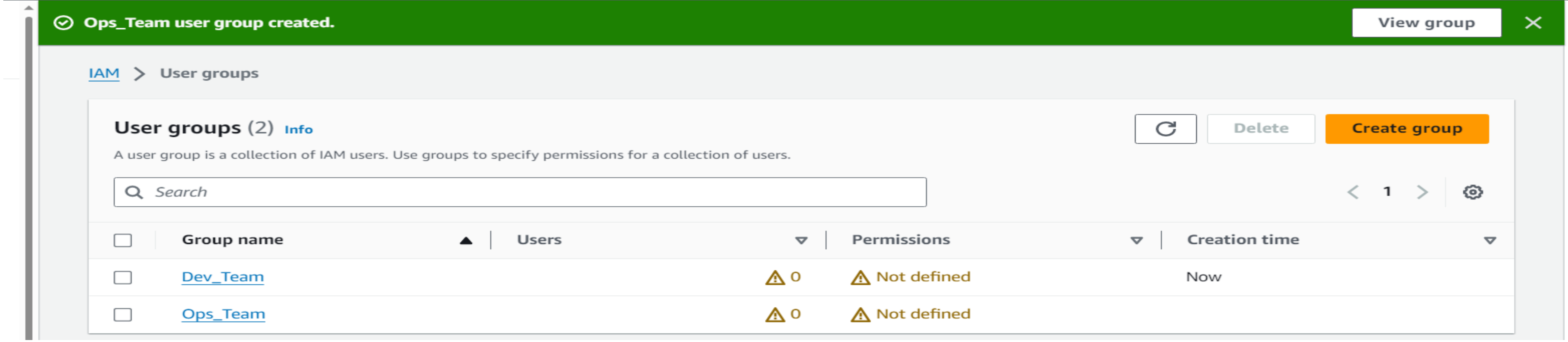
Dev Team

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

Add users to the group - *Optional* (4)

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

If we want to add user and policies , we can add now or we go directly to create group scroll down.



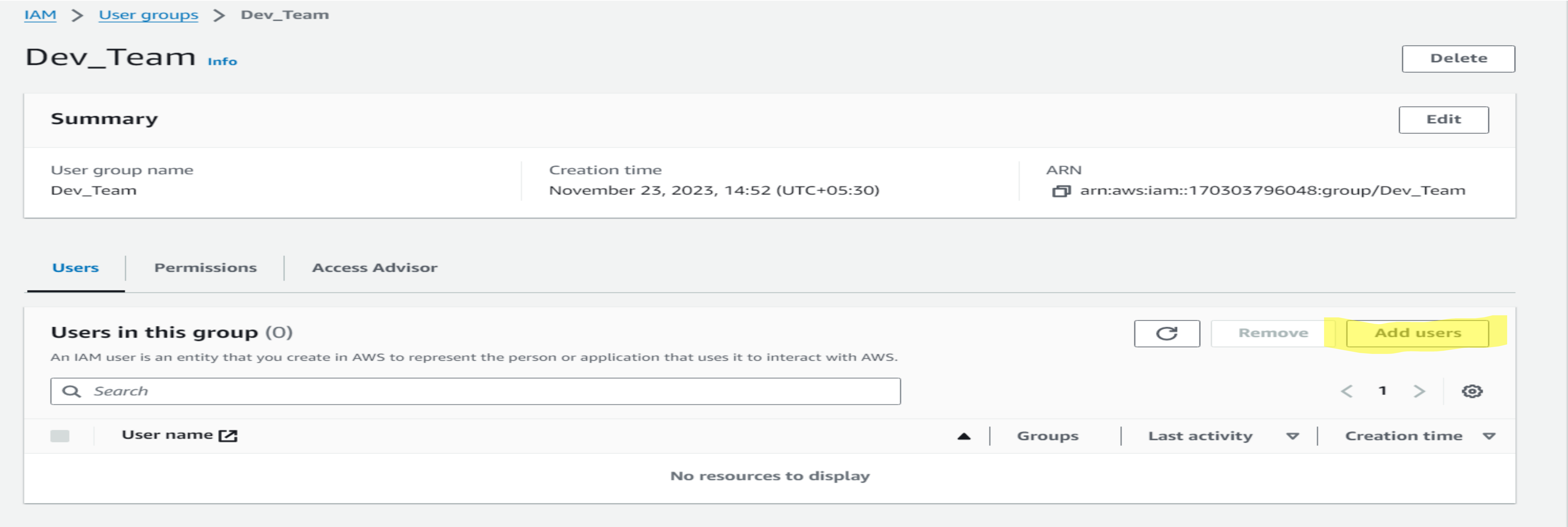
Ops_Team user group created.

IAM > User groups

User groups (2) 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
□	Dev_Team	⚠ 0	⚠ Not defined	Now
□	Ops_Team	⚠ 0	⚠ Not defined	



IAM > User groups > Dev_Team

Dev_Team Info

Summary

User group name
Dev_Team

Creation time
November 23, 2023, 14:52 (UTC+05:30)

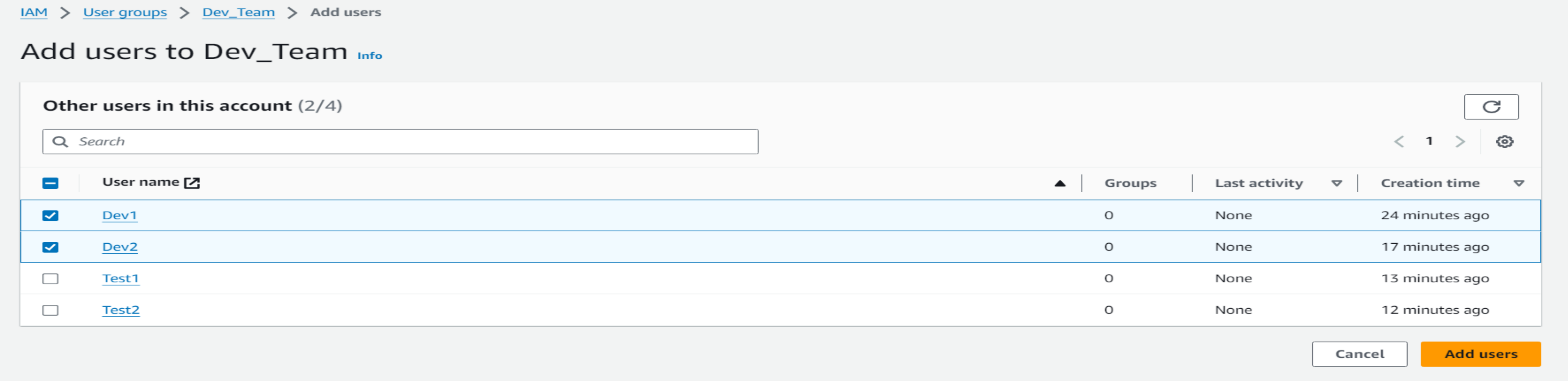
ARN
arn:aws:iam::170303796048:group/Dev_Team

Users in this group (0)

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

No resources to display



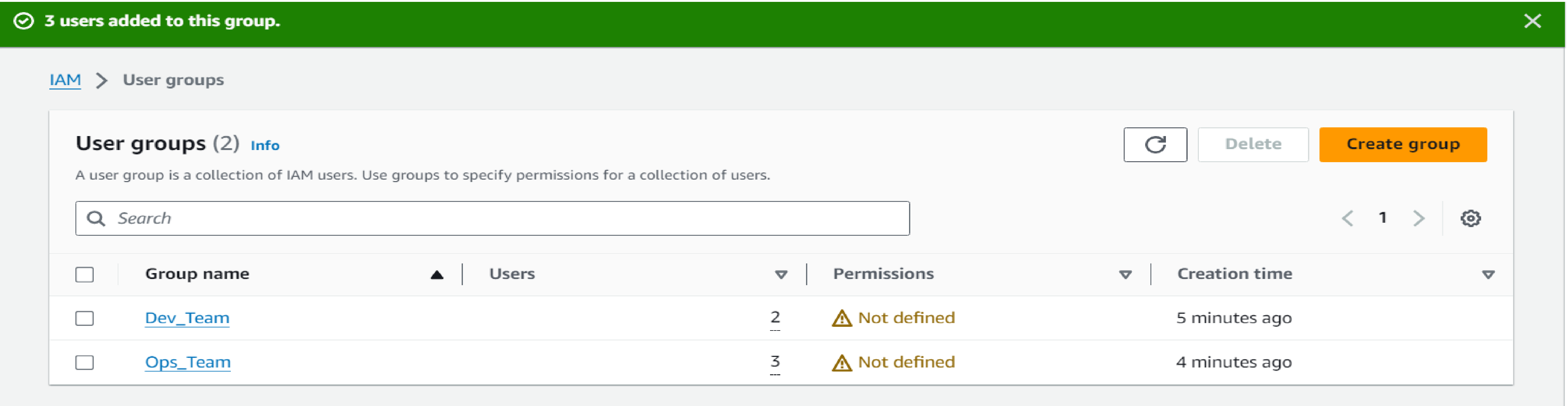
IAM > User groups > Dev_Team > Add users

Add users to Dev_Team Info

Other users in this account (2/4)

Search

☐	User name	Groups	Last activity	Creation time
☑	Dev1	0	None	24 minutes ago
☑	Dev2	0	None	17 minutes ago
☐	Test1	0	None	13 minutes ago
☐	Test2	0	None	12 minutes ago



3 users added to this group.

IAM > User groups

User groups (2) Info

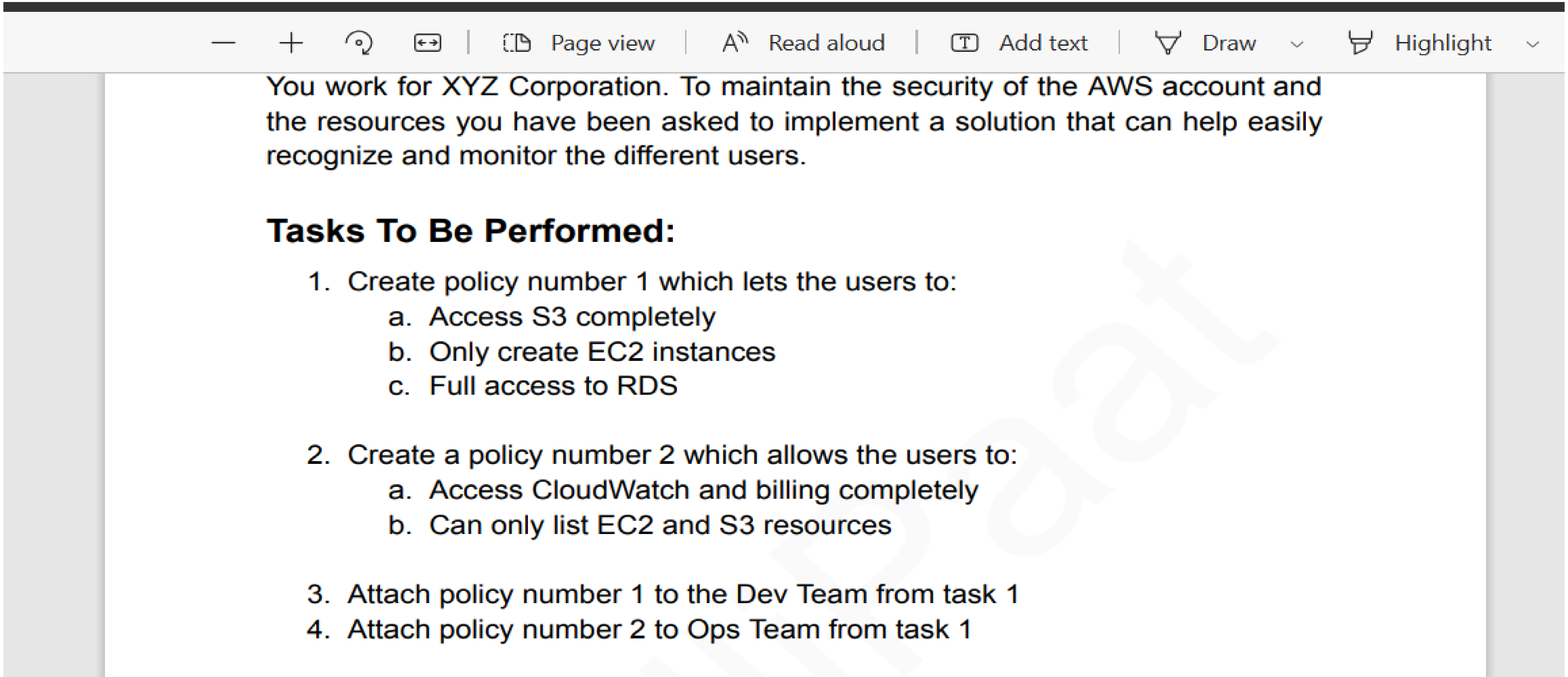
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Search

☐	Group name	Users	Permissions	Creation time
☐	Dev_Team	2	⚠ Not defined	5 minutes ago
☐	Ops_Team	3	⚠ Not defined	4 minutes ago

We can add the same user as many group as we want.

IAM Policies



You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

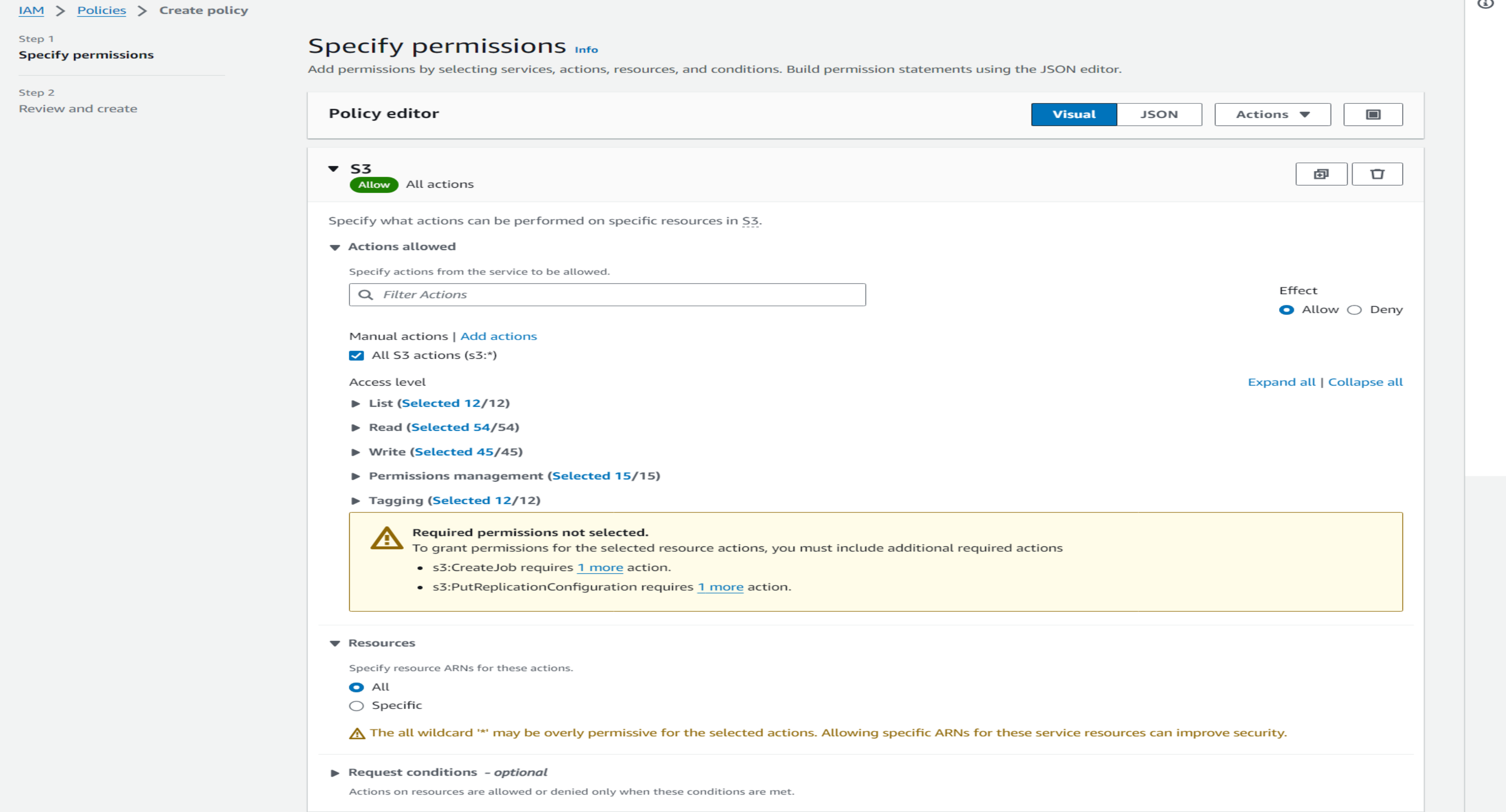
Tasks To Be Performed:

1. Create policy number 1 which lets the users to:
   a. Access S3 completely
   b. Only create EC2 instances
   c. Full access to RDS

2. Create a policy number 2 which allows the users to:
   a. Access CloudWatch and billing completely
   b. Can only list EC2 and S3 resources

3. Attach policy number 1 to the Dev Team from task 1
4. Attach policy number 2 to Ops Team from task 1

Policies-create policies-choose permissions -all s3 and RDS actions and resources .



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 ▼

▼ S3
Allow All actions

Specify what actions can be performed on specific resources in S3.

▼ Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Effect
● Allow ○ Deny

Manual actions | Add actions
☑ All S3 actions (s3:*)

Access level — Expand all | Collapse all

- ▶ List (Selected 12/12)
- ▶ Read (Selected 54/54)
- ▶ Write (Selected 45/45)
- ▶ Permissions management (Selected 15/15)
- ▶ Tagging (Selected 12/12)

Required permissions not selected.
To grant permissions for the selected resource actions, you must include additional required actions

- s3:CreateJob requires 1 more action.
- s3:PutReplicationConfiguration requires 1 more action.

▼ Resources

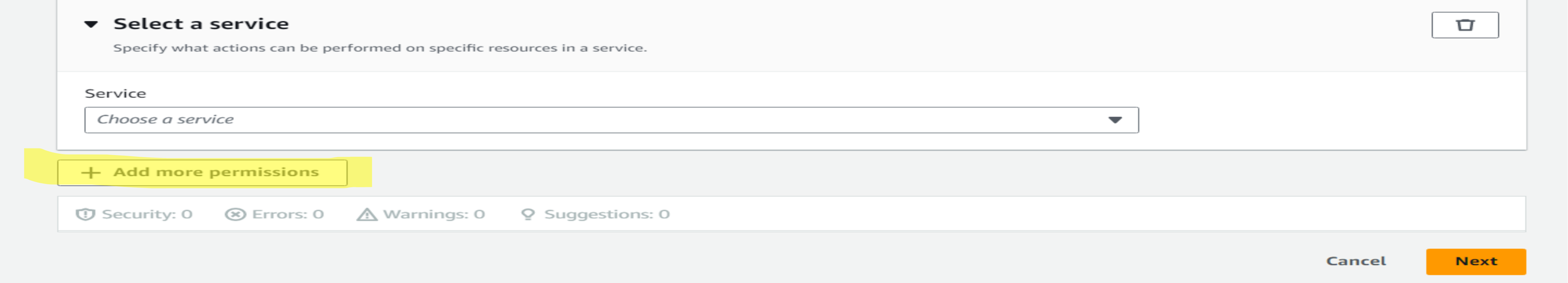
Specify resource ARNs for these actions.

● 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.



▼ **Select a service**

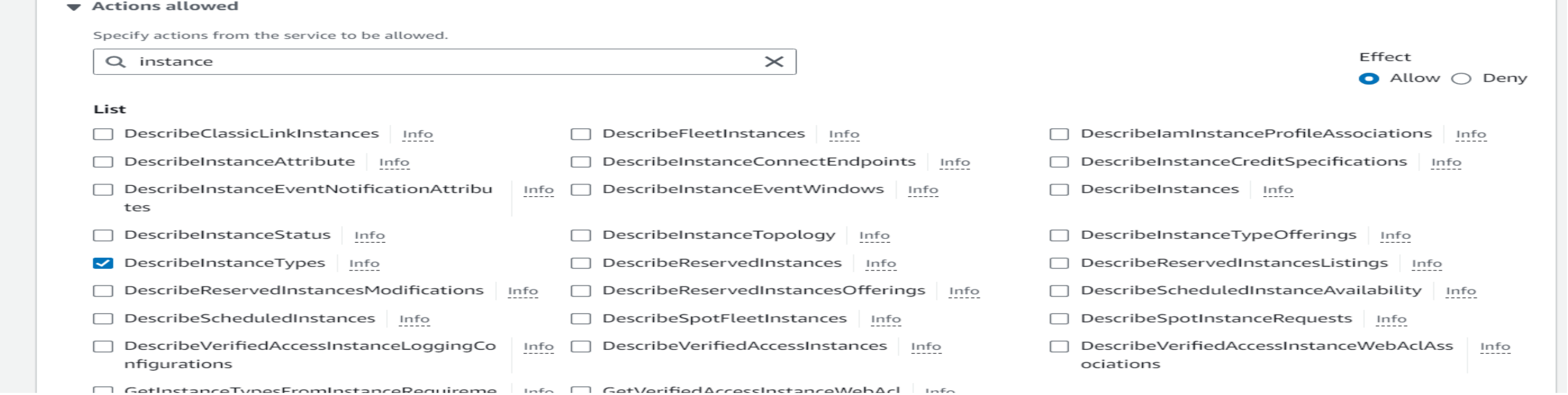
Specify what actions can be performed on specific resources in a service.

Service
Choose a service ▼

＋ Add more permissions

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

Cancel Next



▼ Actions allowed

Specify actions from the service to be allowed.

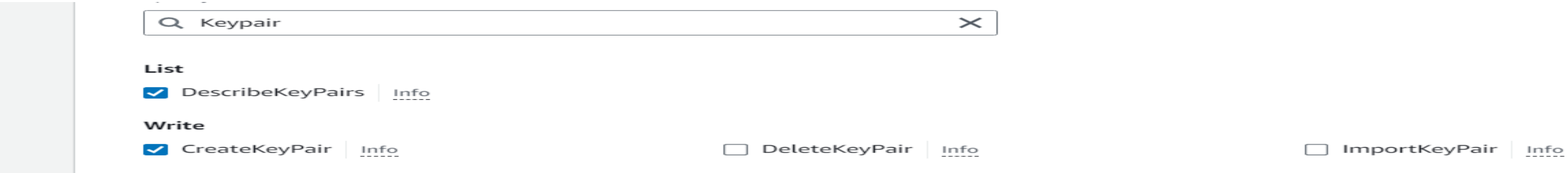
instance

Effect
● Allow ○ Deny

List

- ☐ DescribeClassicLinkInstances Info
- ☐ DescribeFleetInstances Info
- ☐ DescribeIamInstanceProfileAssociations Info
- ☐ DescribeInstanceAttribute Info
- ☐ DescribeInstanceConnectEndpoints Info
- ☐ DescribeInstanceCreditSpecifications Info
- ☐ DescribeInstanceEventNotificationAttributes Info
- ☐ DescribeInstanceEventWindows Info
- ☐ DescribeInstances Info
- ☐ DescribeInstanceStatus Info
- ☐ DescribeInstanceTopology Info
- ☐ DescribeInstanceTypeOfferings Info
- ☑ DescribeInstanceTypes Info
- ☐ DescribeReservedInstances Info
- ☐ DescribeReservedInstancesListings Info
- ☐ DescribeReservedInstancesModifications Info
- ☐ DescribeReservedInstancesOfferings Info
- ☐ DescribeScheduledInstanceAvailability Info
- ☐ DescribeScheduledInstances Info
- ☐ DescribeSpotFleetInstances Info
- ☐ DescribeSpotInstanceRequests Info
- ☐ DescribeVerifiedAccessInstanceLoggingConfigurations Info
- ☐ DescribeVerifiedAccessInstances Info
- ☐ DescribeVerifiedAccessInstanceWebAclAssociations Info
- ☐ GetInstanceTypesFromInstanceRequireme Info
- ☐ GetVerifiedAccessInstanceWebAcl Info

Search for services required to create an ec2 instance and choose.



Keypair

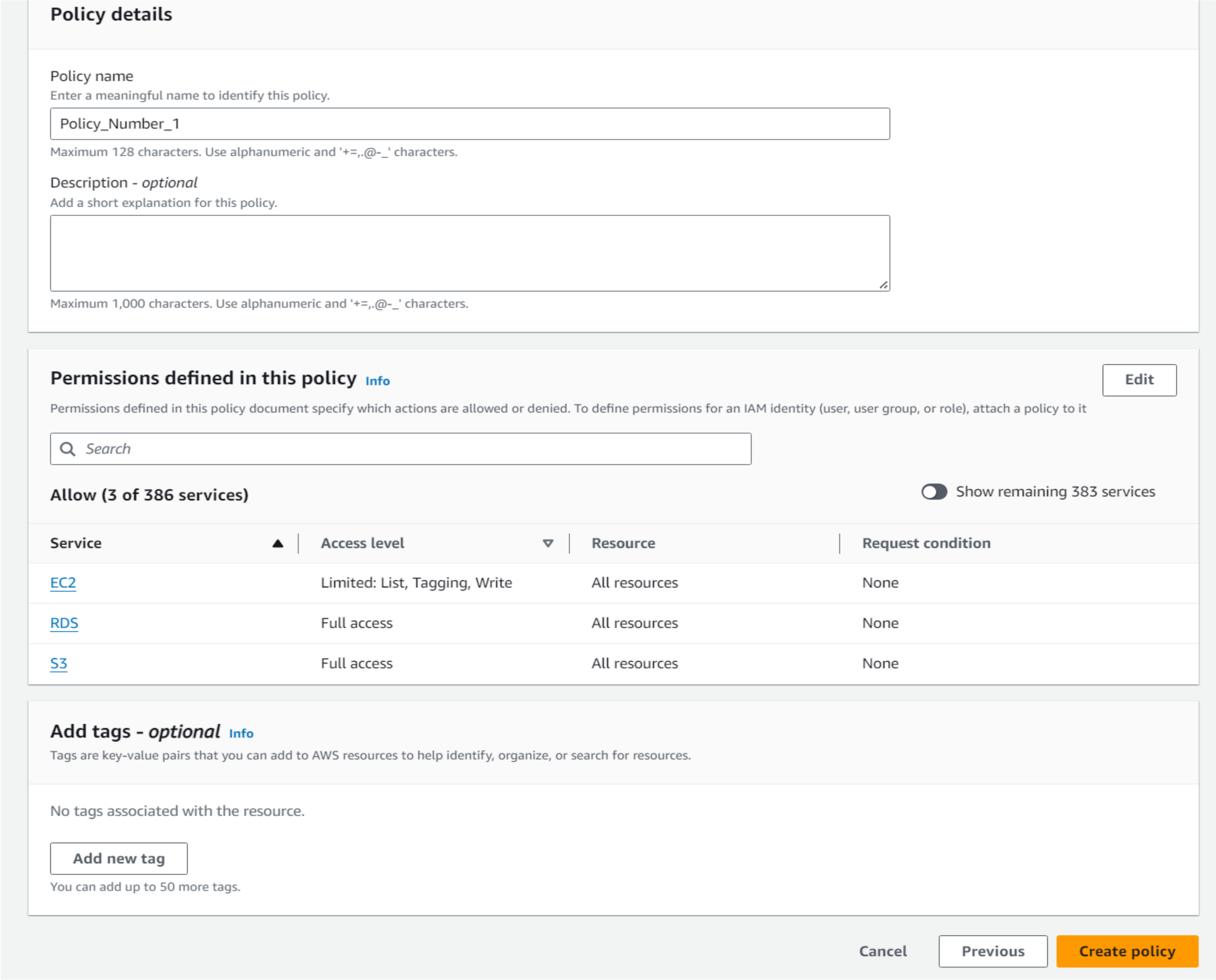
List

- ☑ DescribeKeyPairs Info

Write

- ☑ CreateKeyPair Info
- ☐ DeleteKeyPair Info
- ☐ ImportKeyPair Info

For vpc – describe vpcs
For subnet- describe subnets
For tag – describe and create
For security group – describe security rules and security group.
For volumes – create, attach and describe volumes.
For networkinterface- create , attach and describe
For instances- describe and describe instance type, run instance.
Allow all resources and next .



Policy details

Policy name

Enter a meaningful name to identify this policy.

Policy_Number_1

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

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 (3 of 386 services)

Show remaining 383 services

Service	Access level	Resource	Request condition
EC2	Limited: List, Tagging, Write	All resources	None
RDS	Full access	All resources	None
S3	Full access	All resources	None

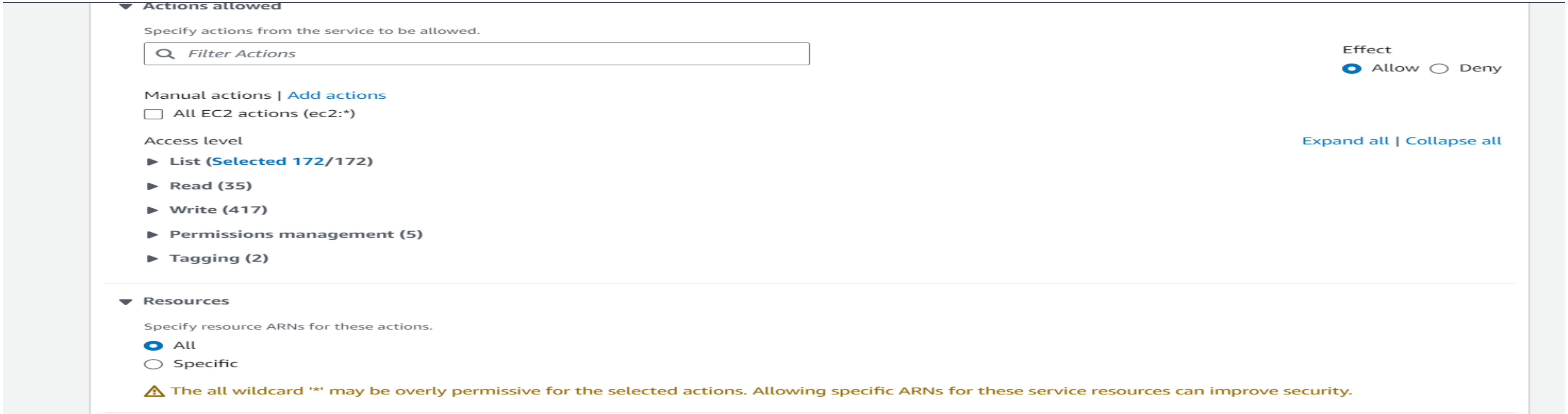
Add tags - *optional* Info

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.

You can add up to 50 more tags.

Choose billing and cloudwatch services allow all actions and resources.



▼ 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 (Selected 172/172)

▶ Read (35)

▶ Write (417)

▶ Permissions management (5)

▶ Tagging (2)

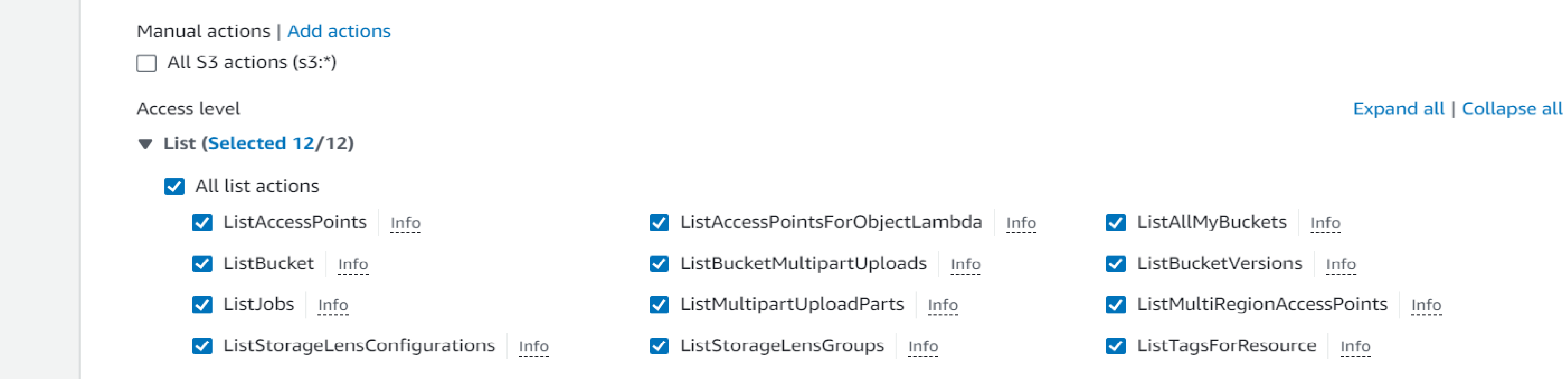
▼ Resources

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.



Manual actions | Add actions

□ All S3 actions (s3:*)

Access level

Expand all | Collapse all

▼ List (Selected 12/12)

☑ All list actions

☑ ListAccessPoints Info

☑ ListAccessPointsForObjectLambda Info

☑ ListAllMyBuckets Info

☑ ListBucket Info

☑ ListBucketMultipartUploads Info

☑ ListBucketVersions Info

☑ ListJobs Info

☑ ListMultipartUploadParts Info

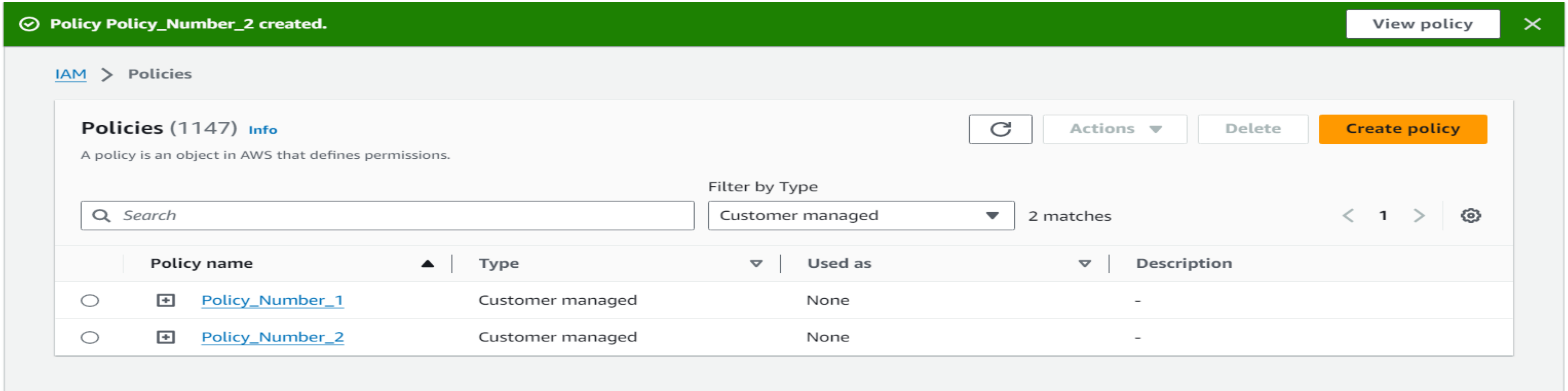
☑ ListMultiRegionAccessPoints Info

☑ ListStorageLensConfigurations Info

☑ ListStorageLensGroups Info

☑ ListTagsForResource Info

Choose another service s3 and ec2 allow all list actions and all resources.



Policy Policy_Number_2 created.

View policy

IAM > Policies

Policies (1147) Info

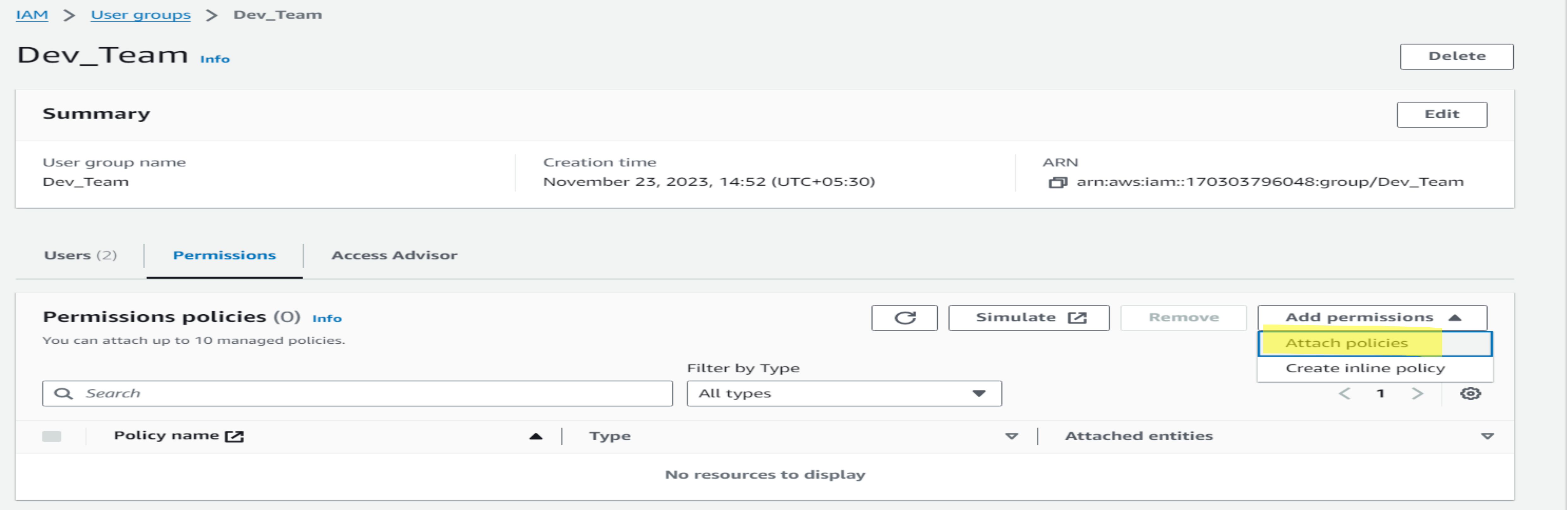
A policy is an object in AWS that defines permissions.

Actions ▼ | Delete | Create policy

Filter by Type

Search | Customer managed ▼ | 2 matches | < 1 >

	Policy name ▲	Type	Used as	Description
○	⊞ Policy_Number_1	Customer managed	None	-
○	⊞ Policy_Number_2	Customer managed	None	-



IAM > User groups > Dev_Team

Dev_Team Info

Delete

Summary

Edit

User group name	Creation time	ARN
Dev_Team	November 23, 2023, 14:52 (UTC+05:30)	arn:aws:iam::170303796048:group/Dev_Team

Users (2) | Permissions | Access Advisor

Permissions policies (0) Info

You can attach up to 10 managed policies.

Simulate | Remove | Add permissions ▲

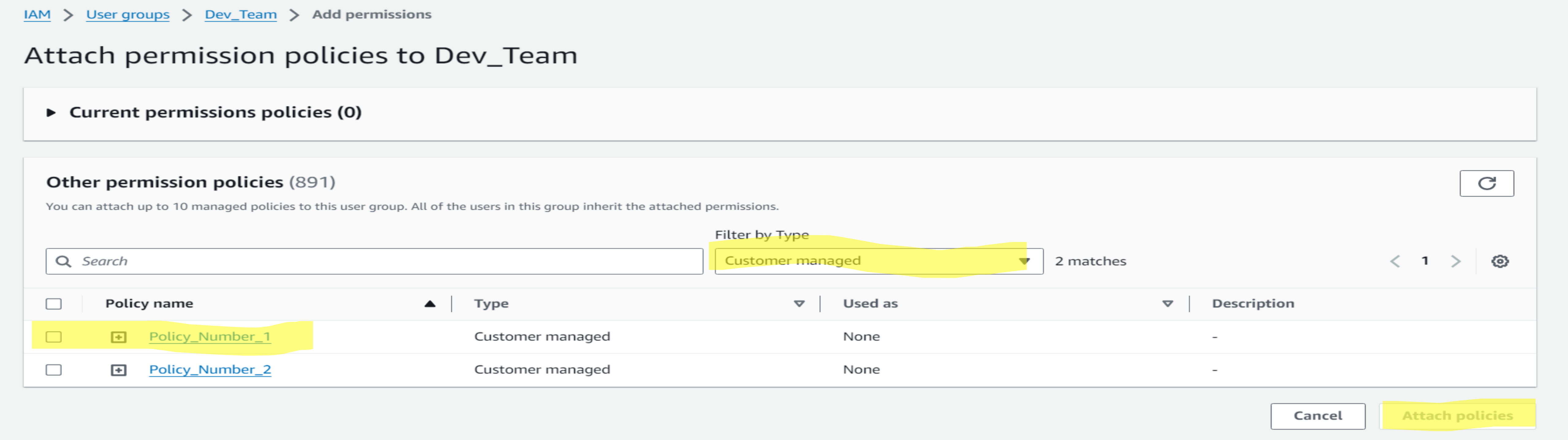
Attach policies

Create inline policy

Filter by Type

Search | All types ▼ | < 1 >

Policy name	Type	Attached entities
No resources to display		



IAM > User groups > Dev_Team > Add permissions

Attach permission policies to Dev_Team

▶ Current permissions policies (0)

Other permission policies (891)

You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.

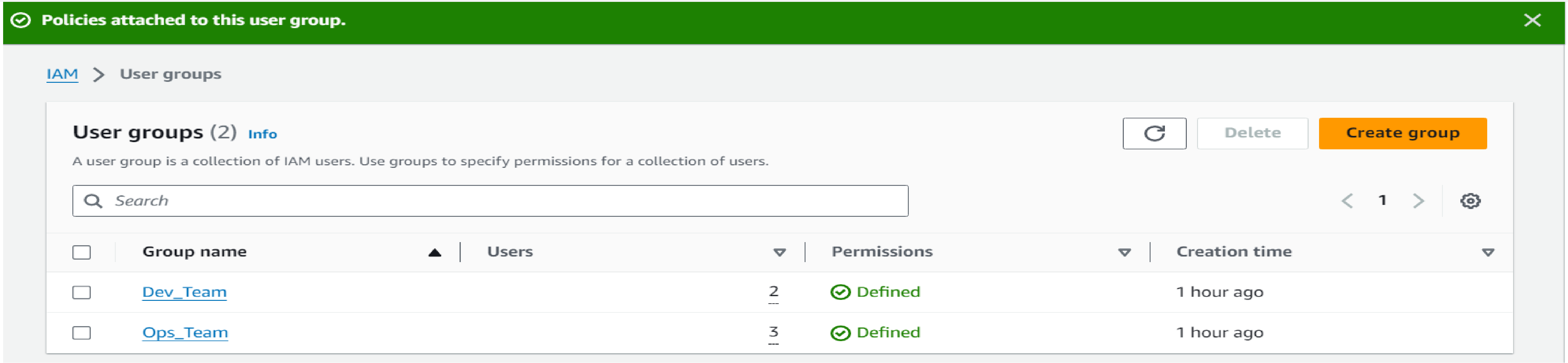
Filter by Type: Customer managed

Search

2 matches

□	Policy name	Type	Used as	Description
□	Policy_Number_1	Customer managed	None	-
□	Policy_Number_2	Customer managed	None	-

Cancel | Attach policies



Policies attached to this user group.

IAM > User groups

User groups (2) Info

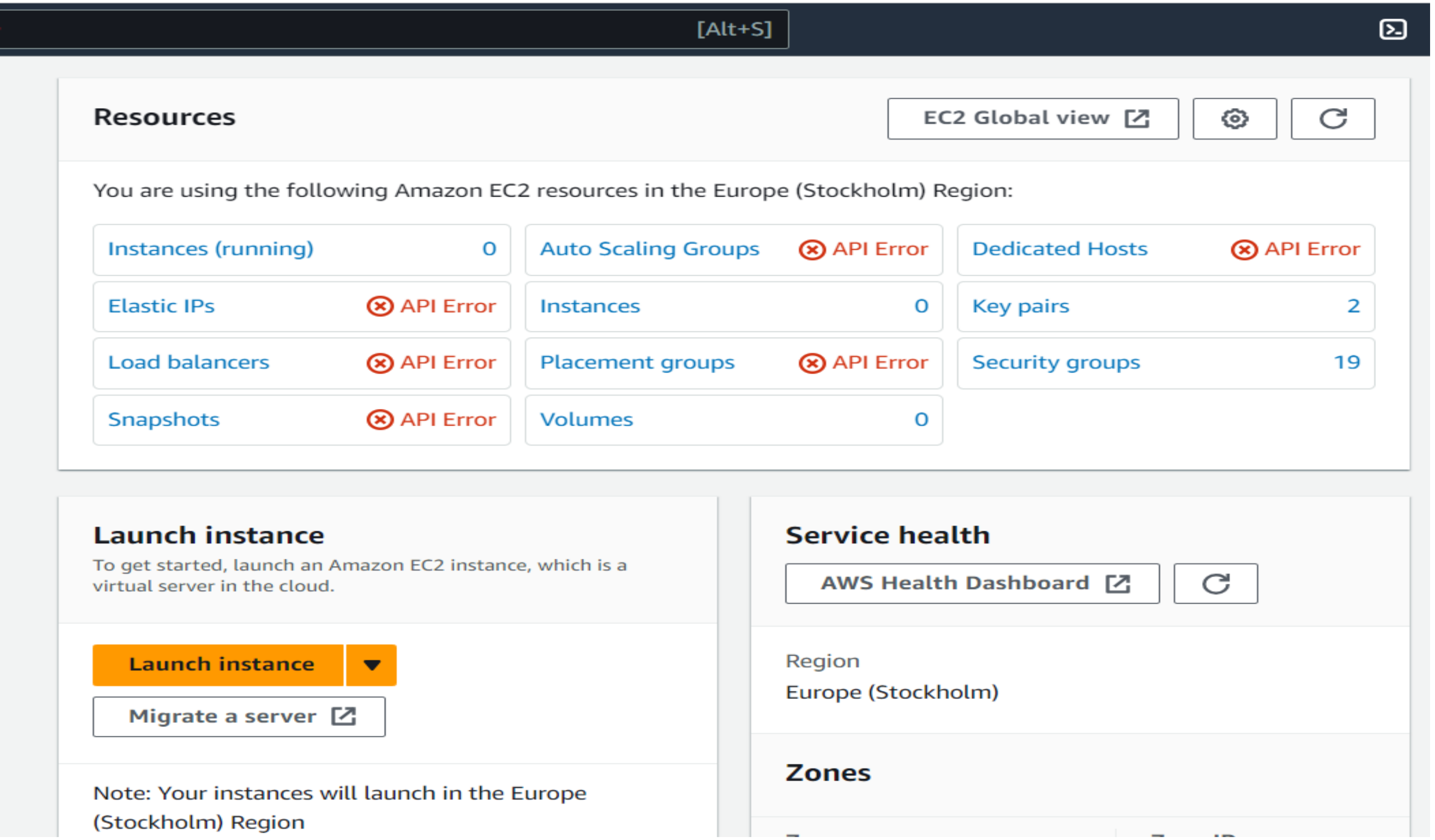
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Search

□	Group name	Users	Permissions	Creation time
□	Dev_Team	2	Defined	1 hour ago
□	Ops_Team	3	Defined	1 hour ago

Attach the policy number 2 in the same way to ops team.

Go to login as a IAM user using different browser copy and paste your real account 12 digit number – username-password.



[Alt+S]

Resources

EC2 Global view | ⚙ | ⟳

You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:

Instances (running)	0	Auto Scaling Groups	⊗ API Error	Dedicated Hosts	⊗ API Error
Elastic IPs	⊗ API Error	Instances	0	Key pairs	2
Load balancers	⊗ API Error	Placement groups	⊗ API Error	Security groups	19
Snapshots	⊗ API Error	Volumes	0		

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance ▼

Migrate a server

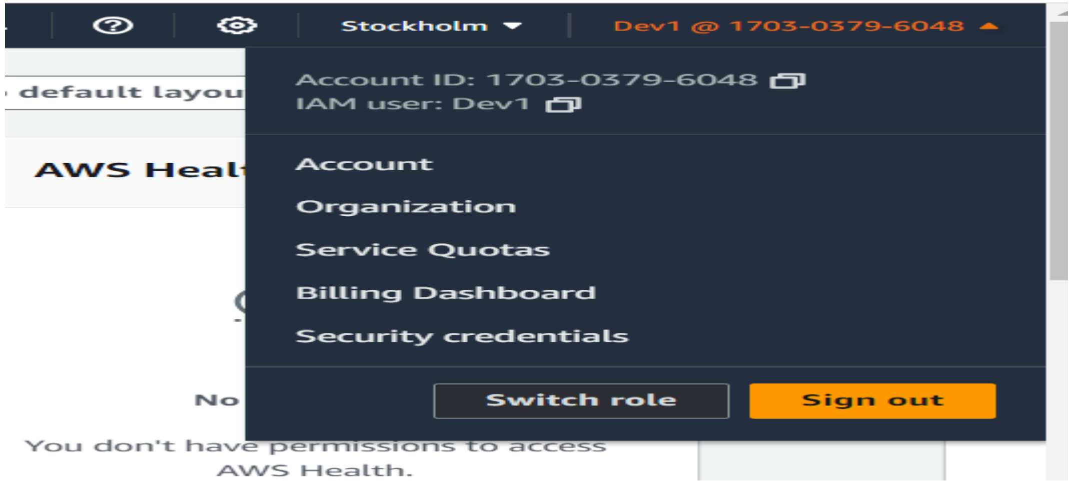
Note: Your instances will launch in the Europe (Stockholm) Region

Service health

AWS Health Dashboard | ⟳

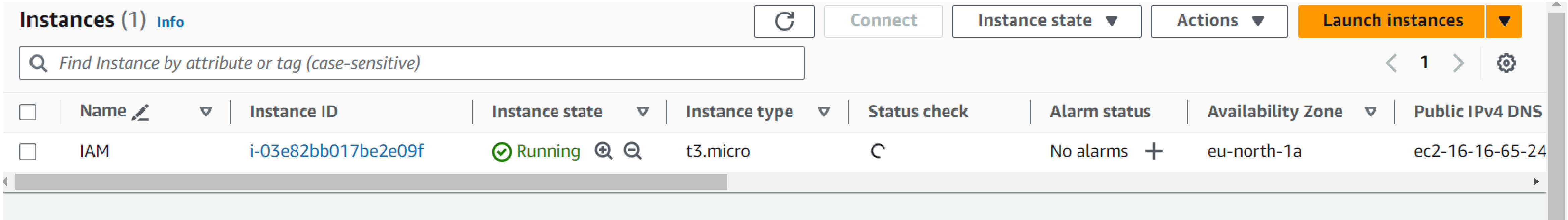
Region
Europe (Stockholm)

Zones



Account ID: 1703-0379-6048
IAM user: Dev1

You don't have permissions to access AWS Health.



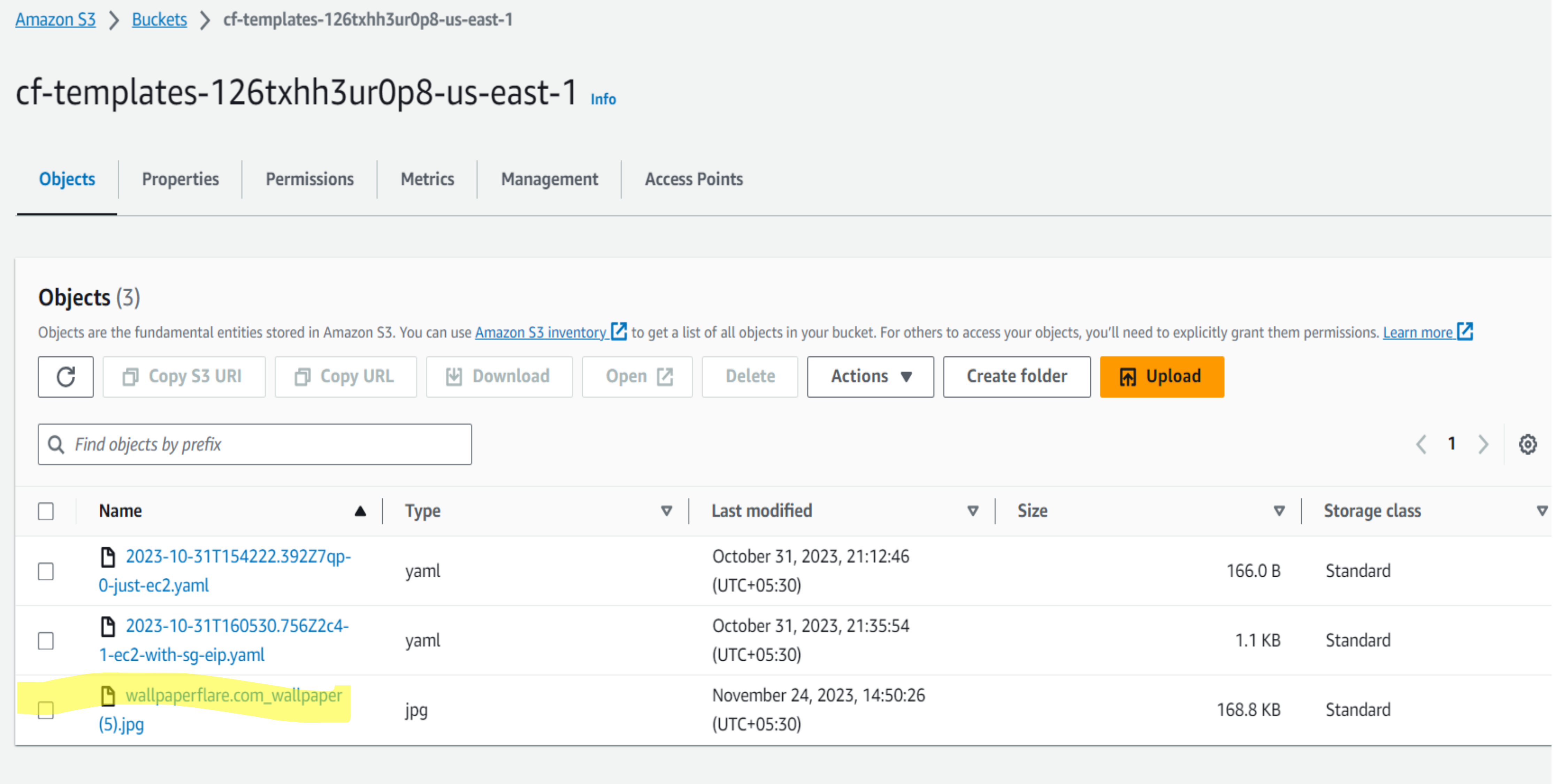
Instances (1) Info

Find Instance by attribute or tag (case-sensitive)

< 1 > ⚙

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
□	IAM	i-03e82bb017be2e09f	✓ Running	t3.micro		No alarms +	eu-north-1a	ec2-16-16-65-24

Since we gave permissions full access of S3 service so we can upload any file we want to and do all the task.



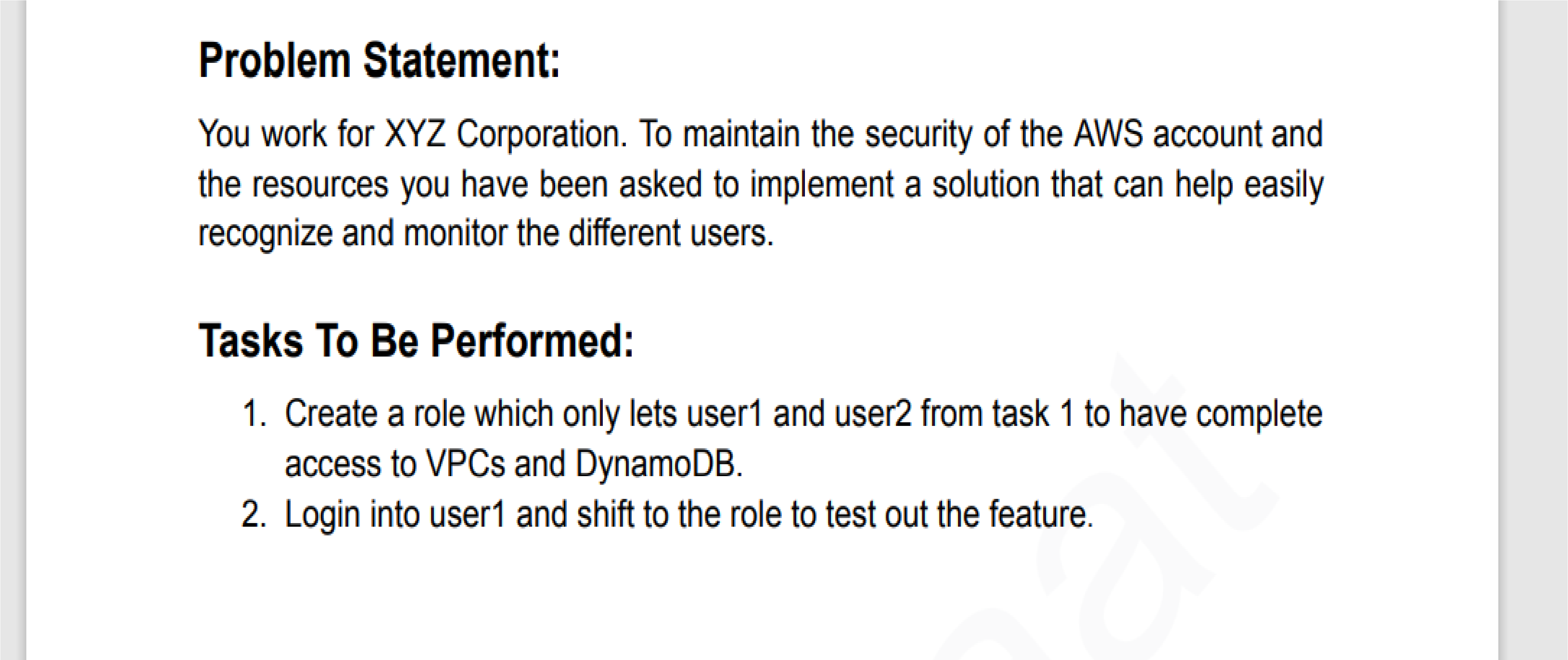
cf-templates-126txhh3ur0p8-us-east-1 Info

Objects (3)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name	Type	Last modified	Size	Storage class
□	2023-10-31T154222.392Z7qp-0-just-ec2.yaml	yaml	October 31, 2023, 21:12:46 (UTC+05:30)	166.0 B	Standard
□	2023-10-31T160530.756Z2c4-1-ec2-with-sg-eip.yaml	yaml	October 31, 2023, 21:35:54 (UTC+05:30)	1.1 KB	Standard
□	wallpaperflare.com_wallpaper (5).jpg	jpg	November 24, 2023, 14:50:26 (UTC+05:30)	168.8 KB	Standard

IAM Roles



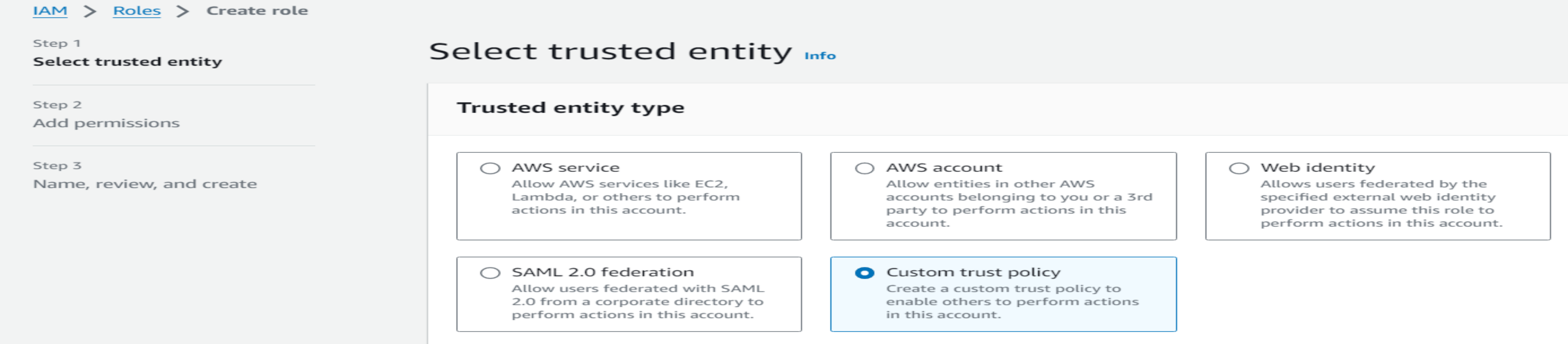
Problem Statement:

You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

Tasks To Be Performed:

1. Create a role which only lets user1 and user2 from task 1 to have complete access to VPCs and DynamoDB.
2. Login into user1 and shift to the role to test out the feature.

Not AWS account because we need to give id and password of our account.



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

○ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

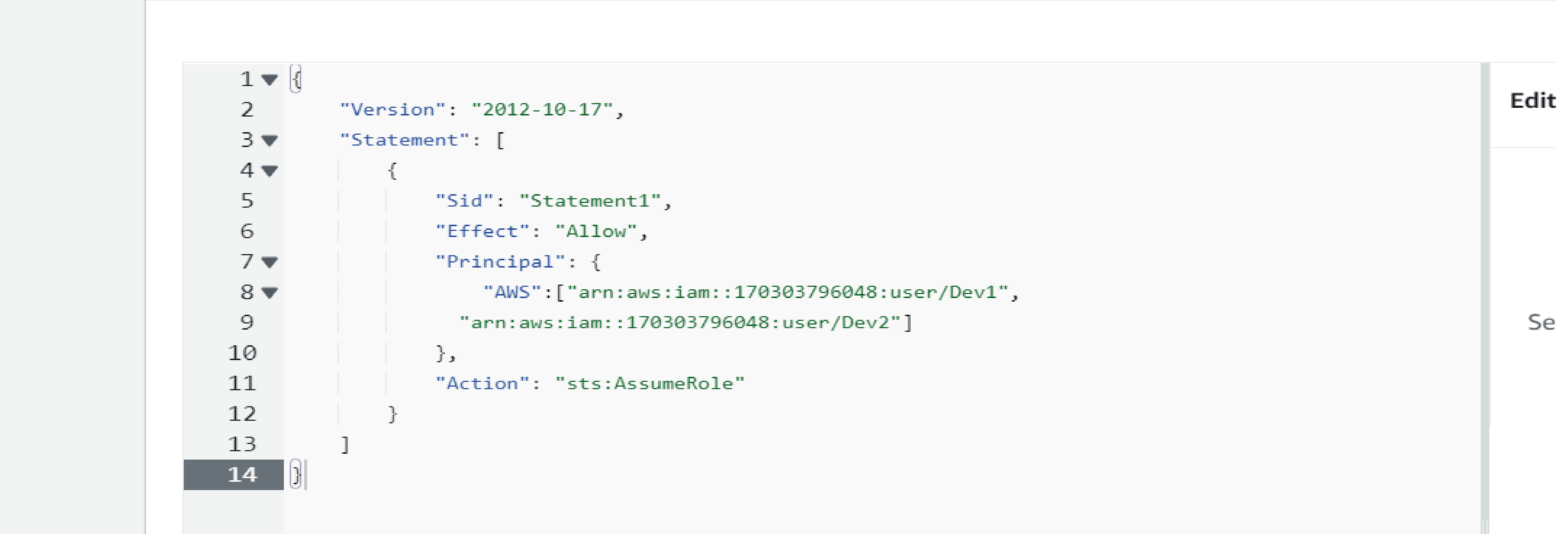
○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

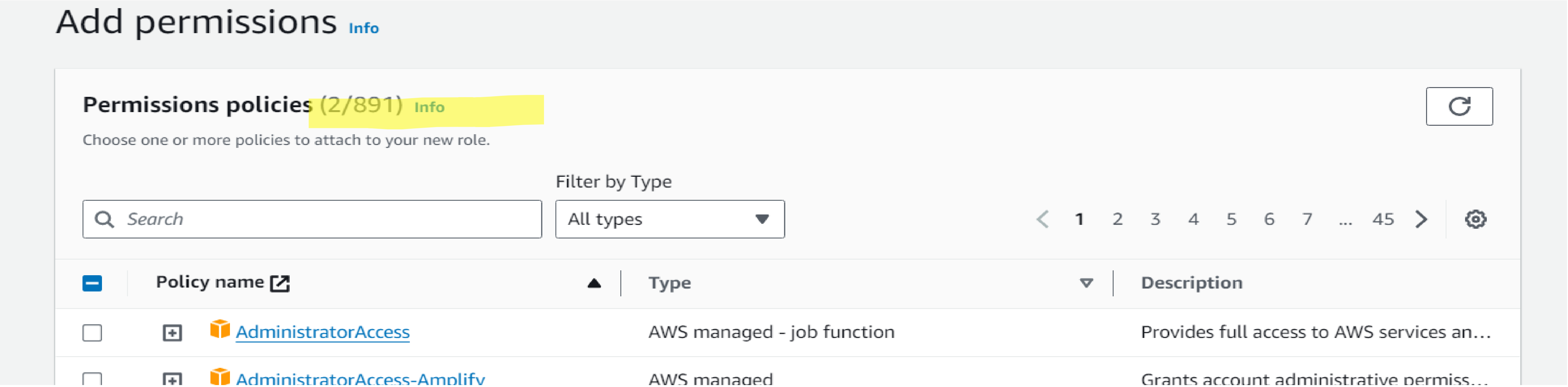
● Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Give the ARN id of those users you want to add in this roles.



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Principal": {
                "AWS":["arn:aws:iam::170303796048:user/Dev1",
              "arn:aws:iam::170303796048:user/Dev2"]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Search for service choose and move to next. I have choose DynamoDB and VPC full access.



Add permissions Info

Permissions policies (2/891) Info

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

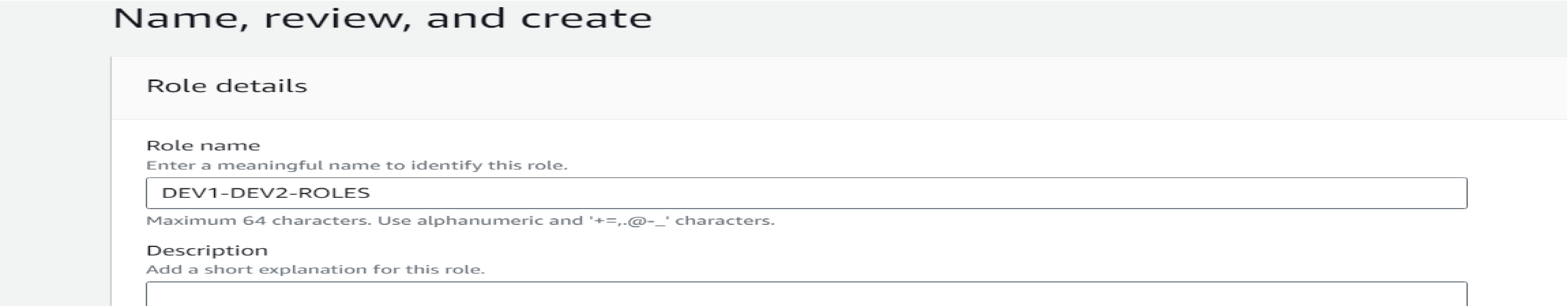
Search

Filter by Type

All types ▼

< 1 2 3 4 5 6 7 ... 45 >

		Policy name	Type	Description
□	⊞	AdministratorAccess	AWS managed - job function	Provides full access to AWS services an...
□	⊞	AdministratorAccess-Amplify	AWS managed	Grants account administrative permiss...



Name, review, and create

Role details

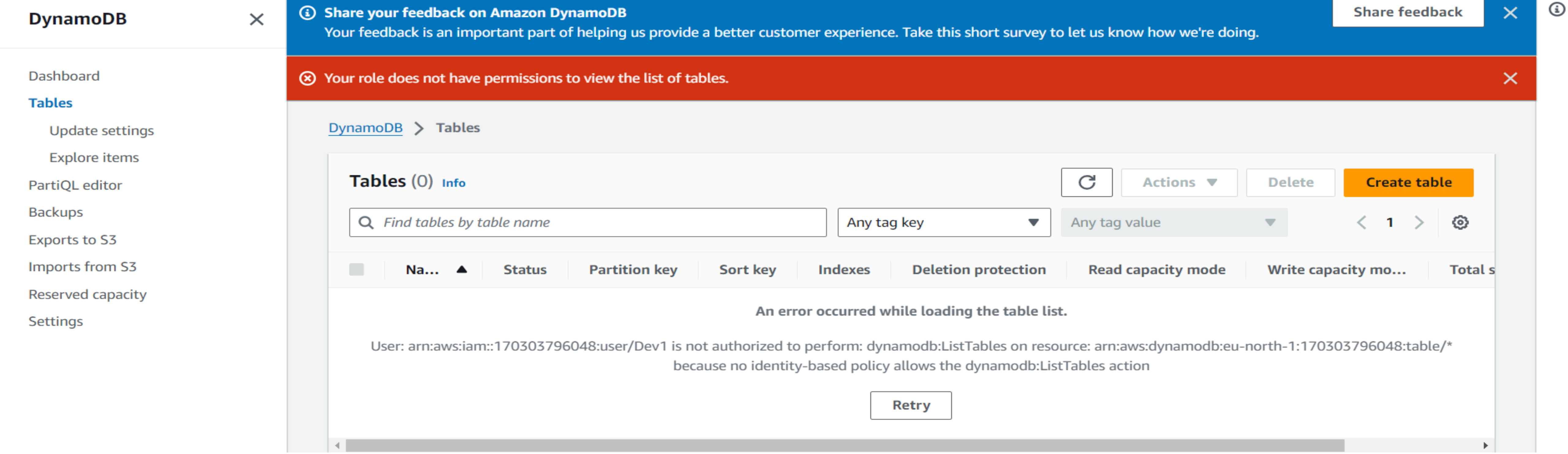
Role name
Enter a meaningful name to identify this role.

DEV1-DEV2-ROLES

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this role.

Name the role and create role. Roles are temporary access and policies are permanent access . Roles also help to attach further policies after creating the user.



Share your feedback on Amazon DynamoDB
Your feedback is an important part of helping us provide a better customer experience. Take this short survey to let us know how we're doing.

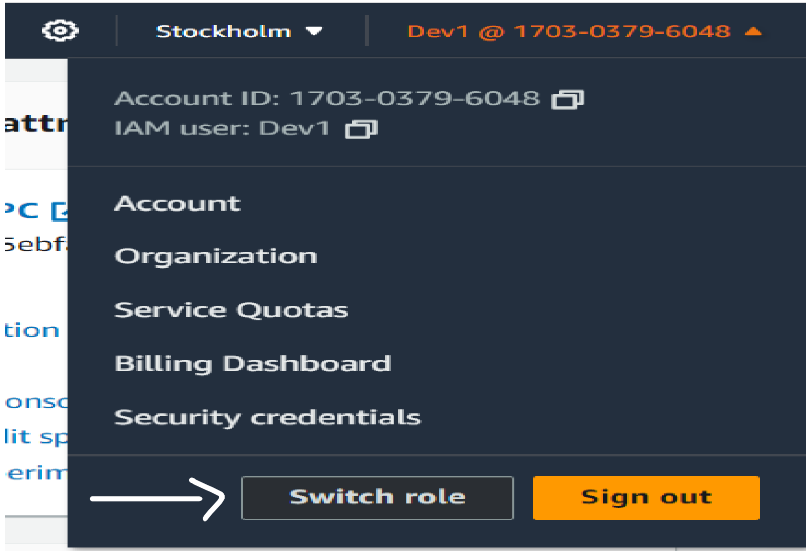
Your role does not have permissions to view the list of tables.

Tables (0) Info

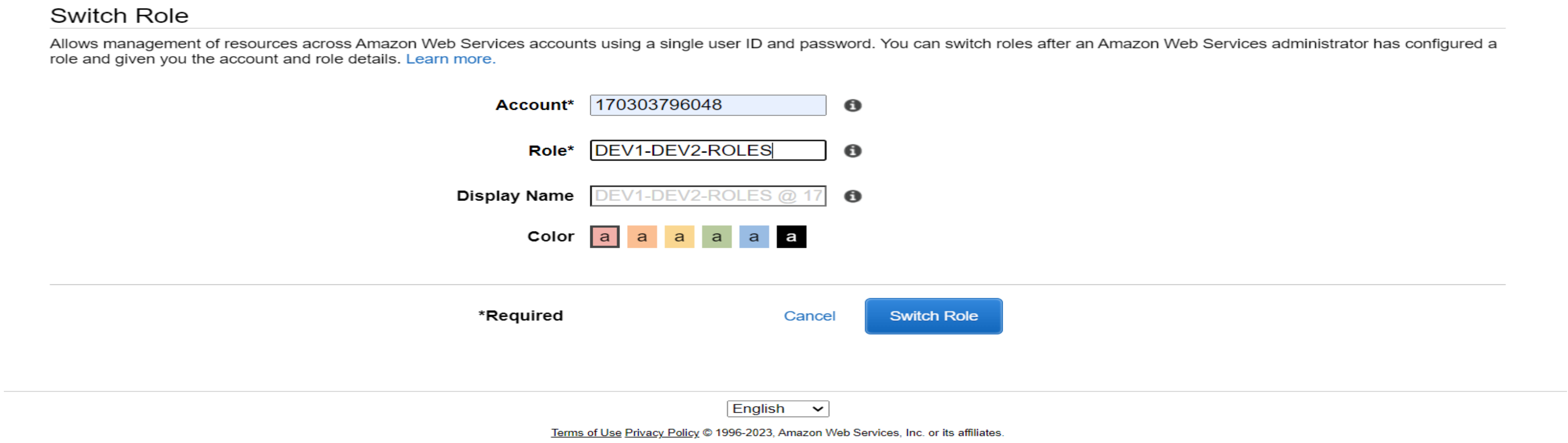
☐	Na... ▲	Status	Partition key	Sort key	Indexes	Deletion protection	Read capacity mode	Write capacity mo...	Total s

An error occurred while loading the table list.

User: arn:aws:iam::170303796048:user/Dev1 is not authorized to perform: dynamodb:ListTables on resource: arn:aws:dynamodb:eu-north-1:170303796048:table/* because no identity-based policy allows the dynamodb:ListTables action



Account ID: 1703-0379-6048
IAM user: Dev1



Switch Role

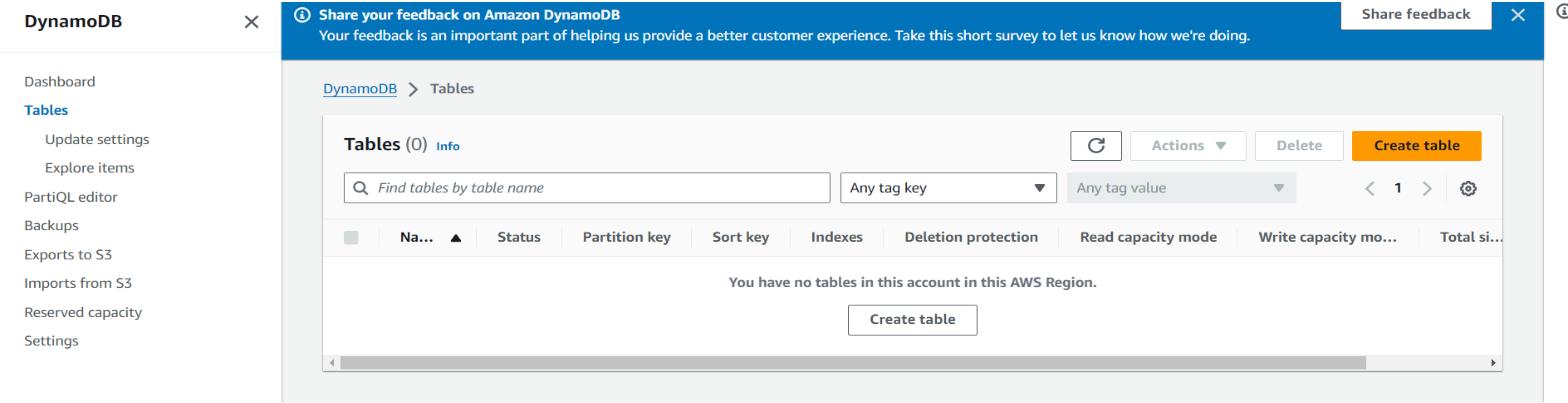
Allows management of resources across Amazon Web Services accounts using a single user ID and password. You can switch roles after an Amazon Web Services administrator has configured a role and given you the account and role details. Learn more.

Account*	170303796048
Role*	DEV1-DEV2-ROLES
Display Name	DEV1-DEV2-ROLES @ 17
Color	a a a a a a

*Required

Terms of Use Privacy Policy © 1996-2023, Amazon Web Services, Inc. or its affiliates.

As we switch to the roles we have full access of DynamoDB .



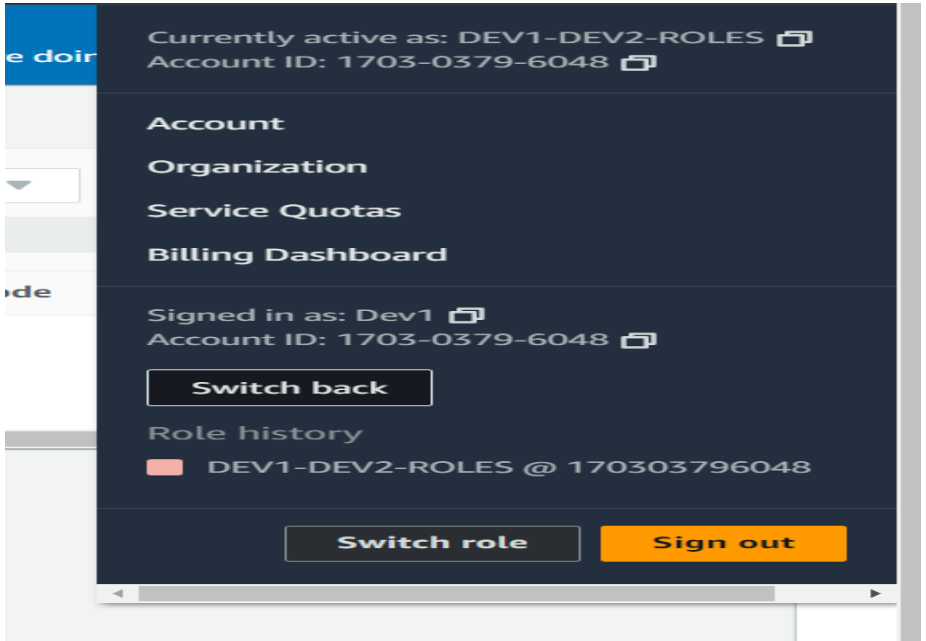
Share your feedback on Amazon DynamoDB
Your feedback is an important part of helping us provide a better customer experience. Take this short survey to let us know how we're doing.

Tables (0)

Find tables by table name

Na... ▲	Status	Partition key	Sort key	Indexes	Deletion protection	Read capacity mode	Write capacity mo...	Total si...

You have no tables in this account in this AWS Region.

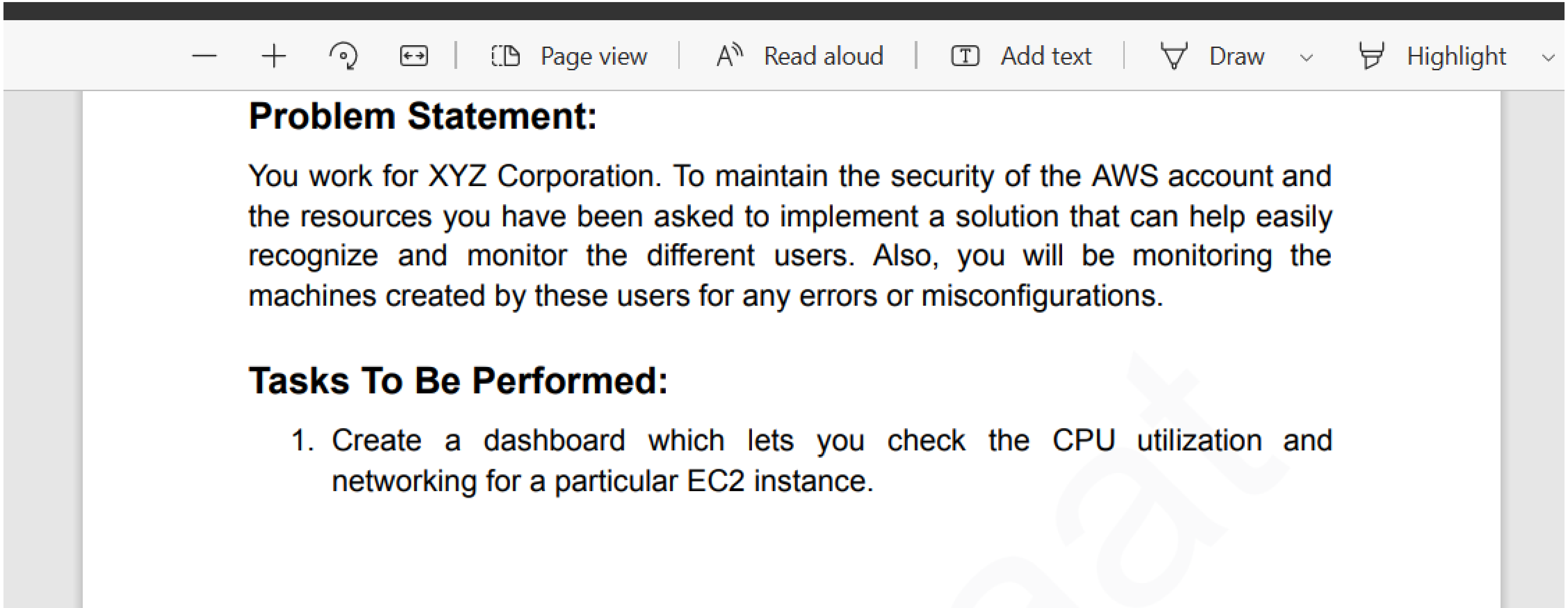


Currently active as: DEV1-DEV2-ROLES
Account ID: 1703-0379-6048

Signed in as: Dev1
Account ID: 1703-0379-6048

Role history
DEV1-DEV2-ROLES @ 170303796048

CloudWatch Dashboard



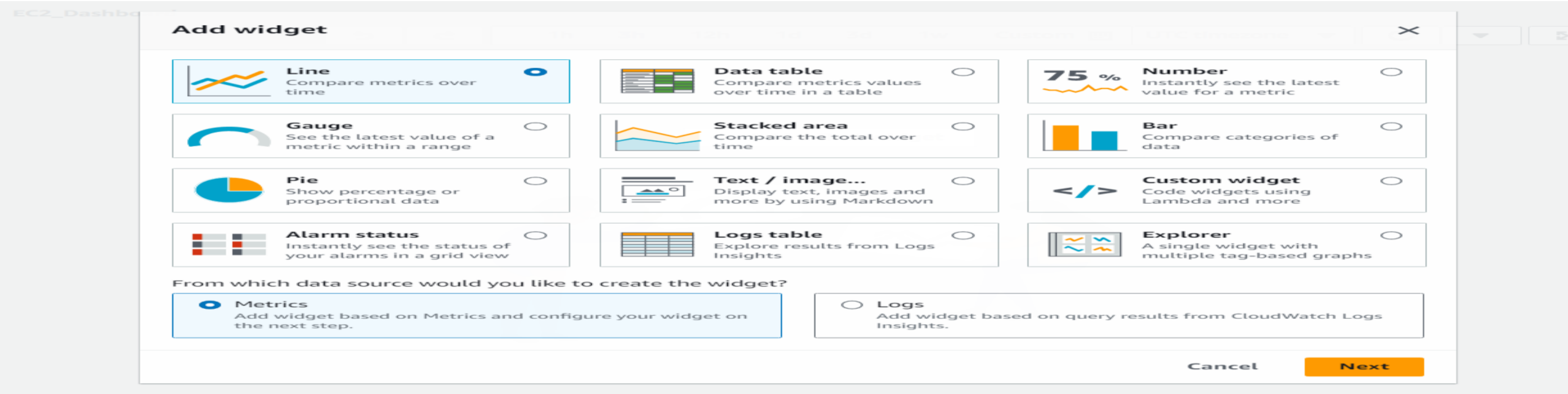
Problem Statement:

You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users. Also, you will be monitoring the machines created by these users for any errors or misconfigurations.

Tasks To Be Performed:

1. Create a dashboard which lets you check the CPU utilization and networking for a particular EC2 instance.

Cloudwatch – dashboard – create dashboard – name – choose which style you want and next



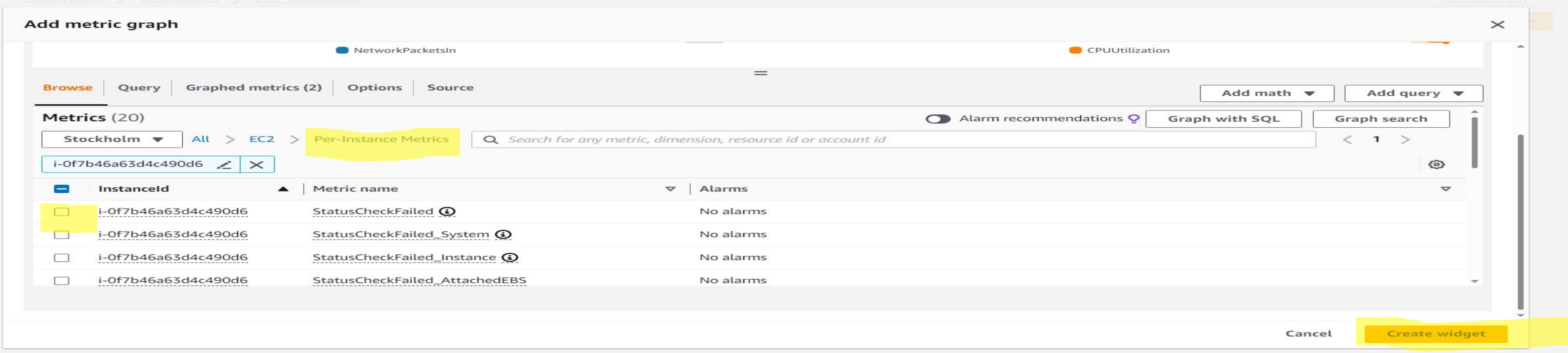
Add widget

- ● **Line** Compare metrics over time
- ○ **Data table** Compare metrics values over time in a table
- ○ **Number** Instantly see the latest value for a metric
- ○ **Gauge** See the latest value of a metric within a range
- ○ **Stacked area** Compare the total over time
- ○ **Bar** Compare categories of data
- ○ **Pie** Show percentage or proportional data
- ○ **Text / image...** Display text, images and more by using Markdown
- ○ **Custom widget** Code widgets using Lambda and more
- ○ **Alarm status** Instantly see the status of your alarms in a grid view
- ○ **Logs table** Explore results from Logs Insights
- ○ **Explorer** A single widget with multiple tag-based graphs

From which data source would you like to create the widget?

- ● Metrics Add widget based on Metrics and configure your widget on the next step.
- ○ Logs Add widget based on query results from CloudWatch Logs Insights.

Go for pre instance metrics – enter instance id – enter – now all details visible – select requires one and create widget. Choose network packets in and CPU utilization.



Add metric graph

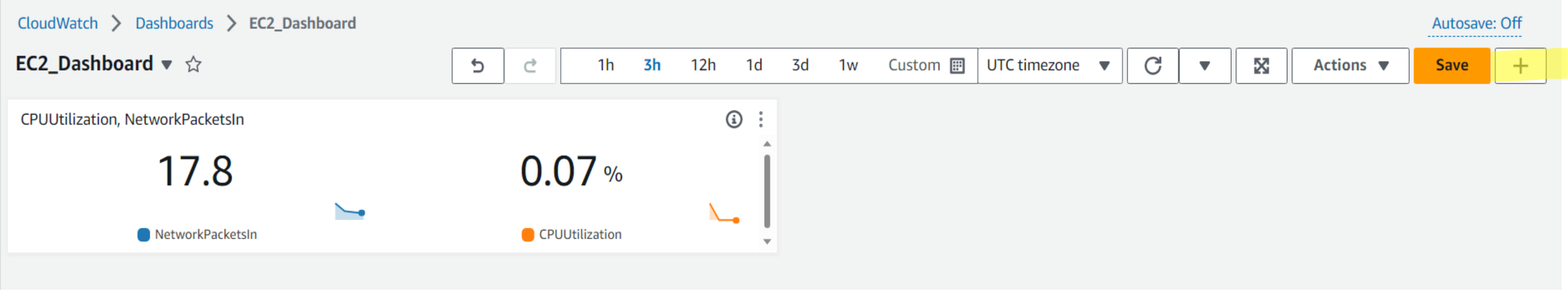
Metrics (20)

Stockholm > All > EC2 > Per-Instance Metrics

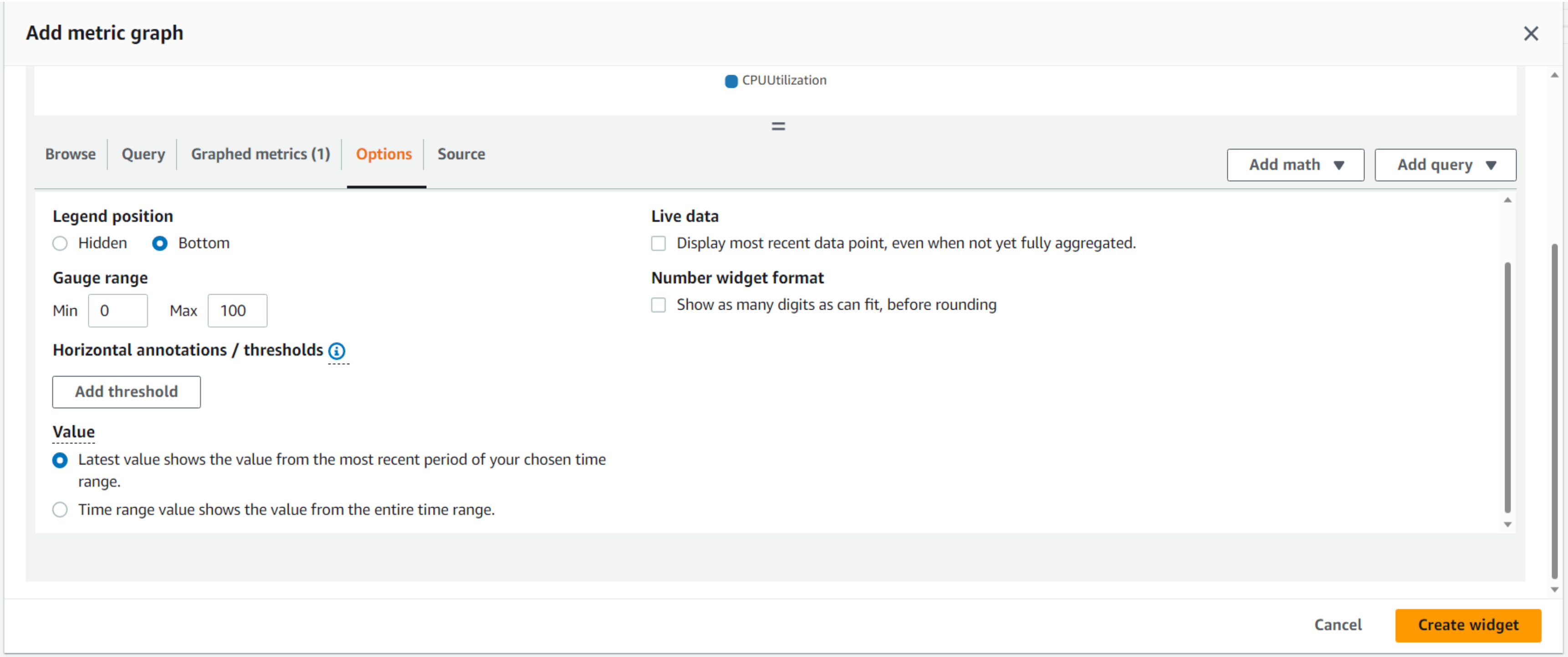
Search for any metric, dimension, resource id or account id

i-0f7b46a63d4c490d6

	InstanceId	Metric name	Alarms
□	i-0f7b46a63d4c490d6	StatusCheckFailed	No alarms
□	i-0f7b46a63d4c490d6	StatusCheckFailed_System	No alarms
□	i-0f7b46a63d4c490d6	StatusCheckFailed_Instance	No alarms
□	i-0f7b46a63d4c490d6	StatusCheckFailed_AttachedEBS	No alarms



If we want to add another widget hit the plus icon do the same following steps , I choose guage give upper and lower limit – create widget.



Legend position

○ Hidden ● Bottom

Gauge range

Min 0 Max 100

Horizontal annotations / thresholds

Value

● Latest value shows the value from the most recent period of your chosen time range.

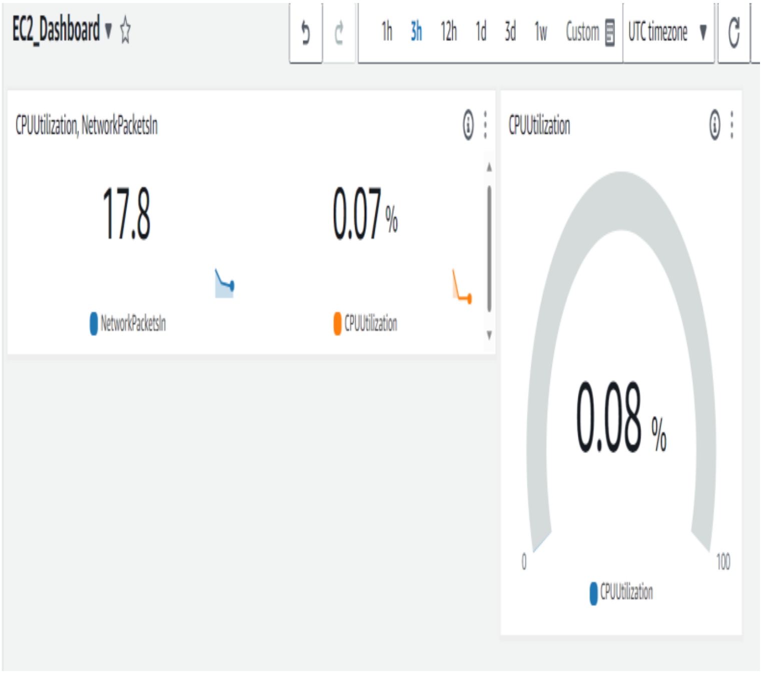
○ Time range value shows the value from the entire time range.

Live data

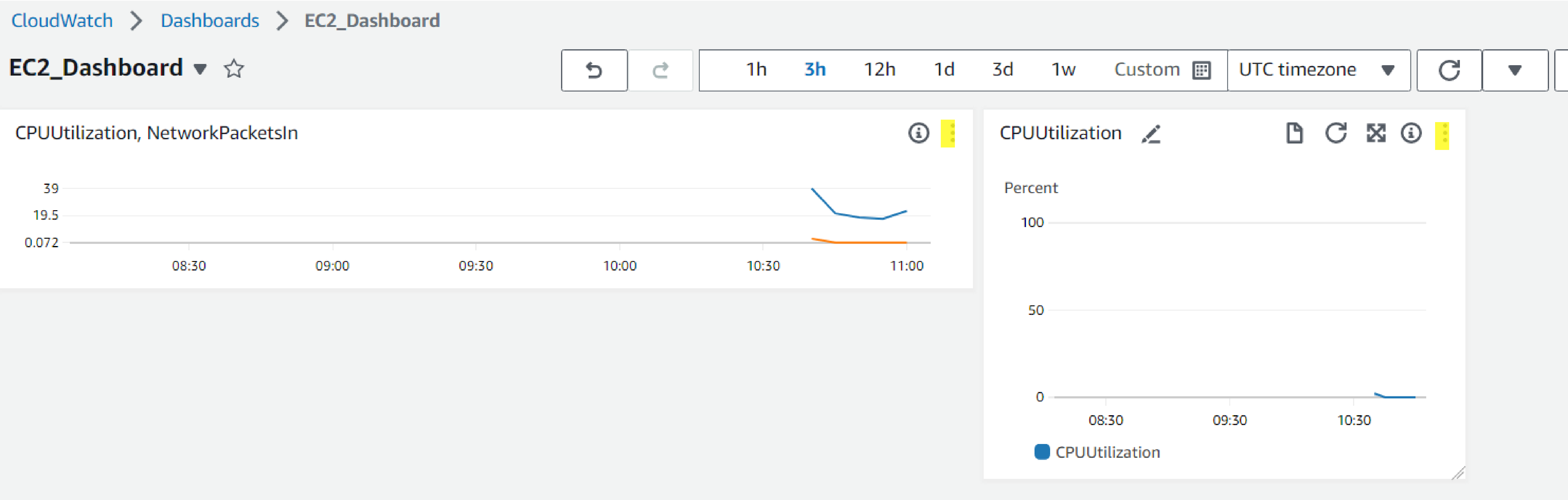
□ Display most recent data point, even when not yet fully aggregated.

Number widget format

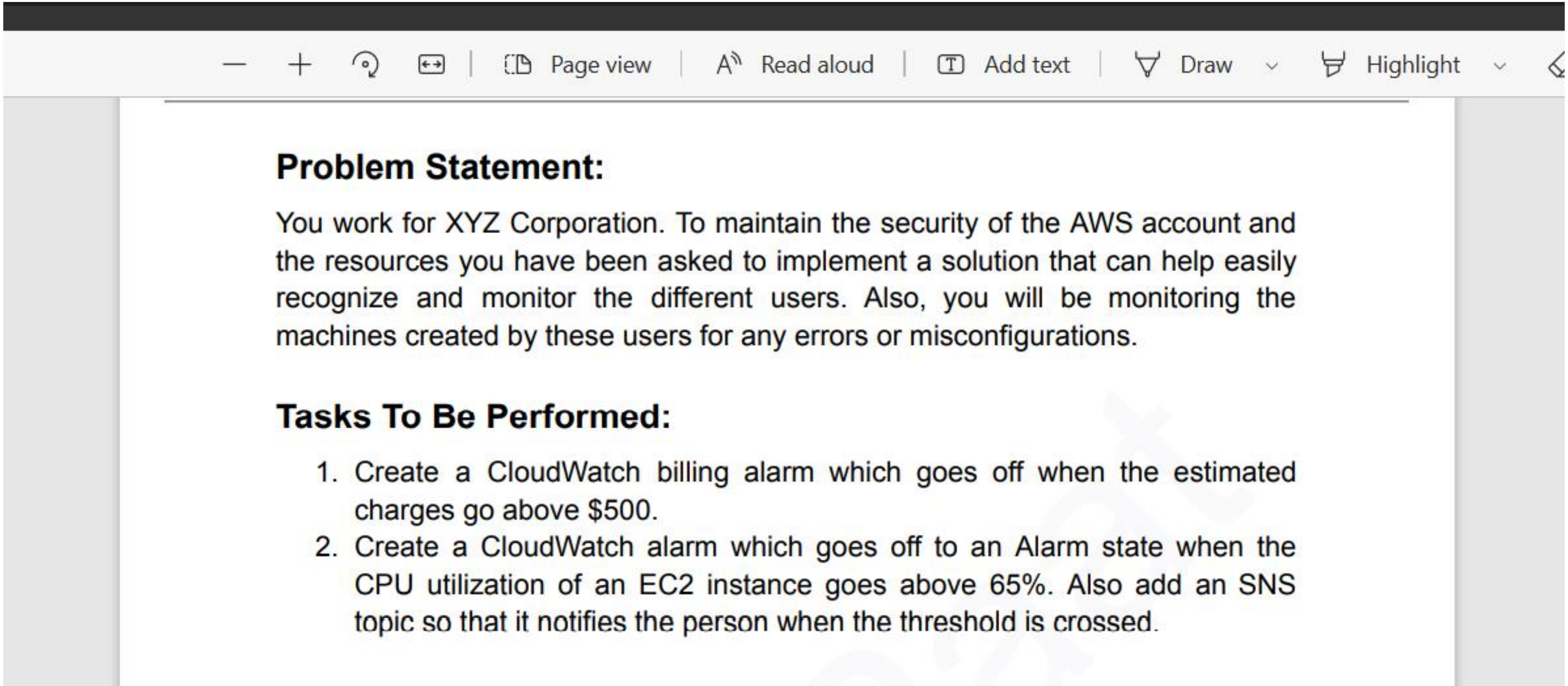
□ Show as many digits as can fit, before rounding



If we want to change the graph style – click on three dots- widget type and choose.



CloudWatch Alarms



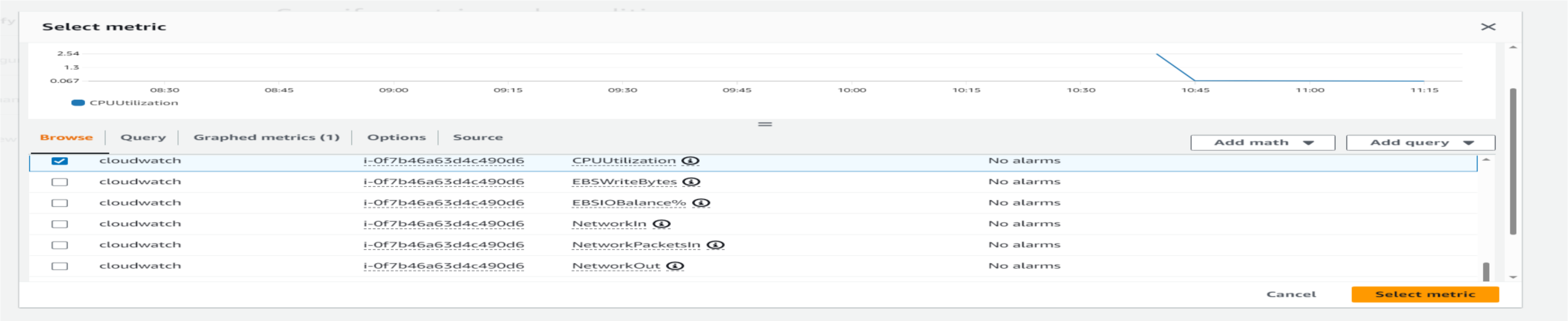
Problem Statement:

You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users. Also, you will be monitoring the machines created by these users for any errors or misconfigurations.

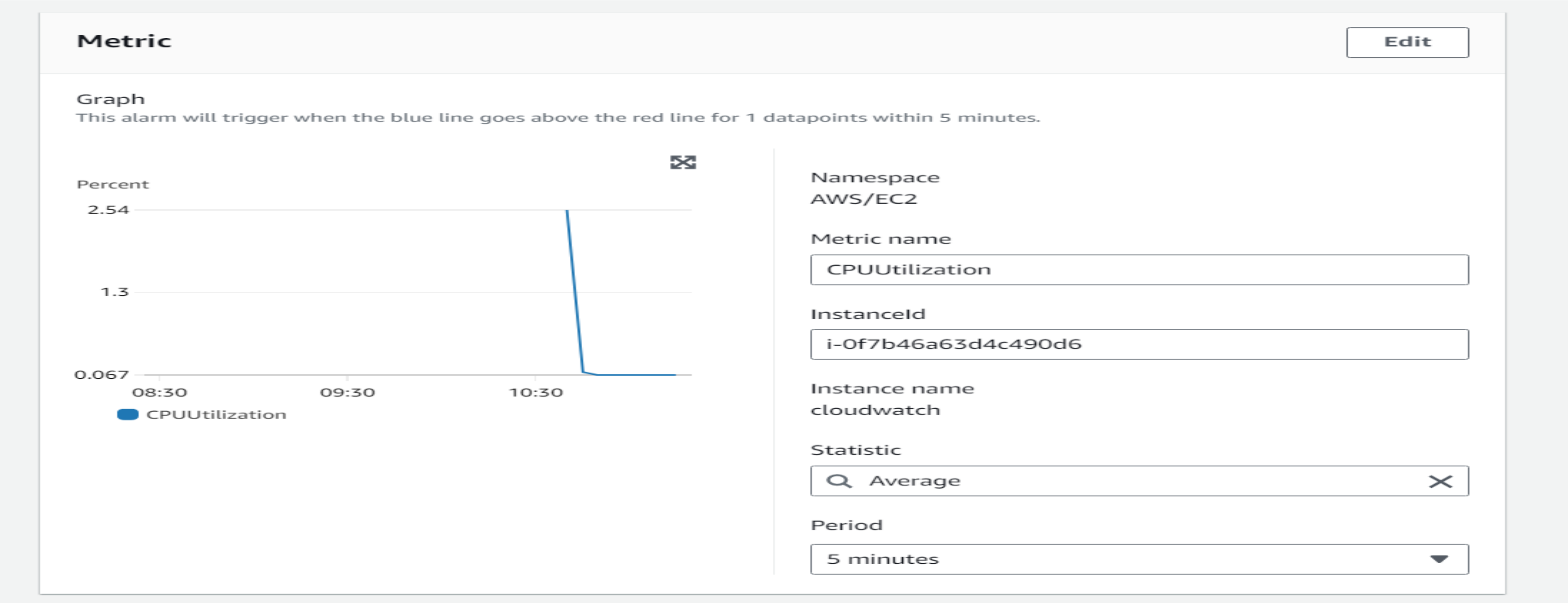
Tasks To Be Performed:

1. Create a CloudWatch billing alarm which goes off when the estimated charges go above $500.
2. Create a CloudWatch alarm which goes off to an Alarm state when the CPU utilization of an EC2 instance goes above 65%. Also add an SNS topic so that it notifies the person when the threshold is crossed.

Go to all alarms – create new alarm – select metrics – do the same steps as creating the dashboard until here.



☑	cloudwatch	i-0f7b46a63d4c490d6	CPUUtilization	No alarms
□	cloudwatch	i-0f7b46a63d4c490d6	EBSWriteBytes	No alarms
□	cloudwatch	i-0f7b46a63d4c490d6	EBSIOBalance%	No alarms
□	cloudwatch	i-0f7b46a63d4c490d6	NetworkIn	No alarms
□	cloudwatch	i-0f7b46a63d4c490d6	NetworkPacketsIn	No alarms
□	cloudwatch	i-0f7b46a63d4c490d6	NetworkOut	No alarms



Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.

Namespace
AWS/EC2

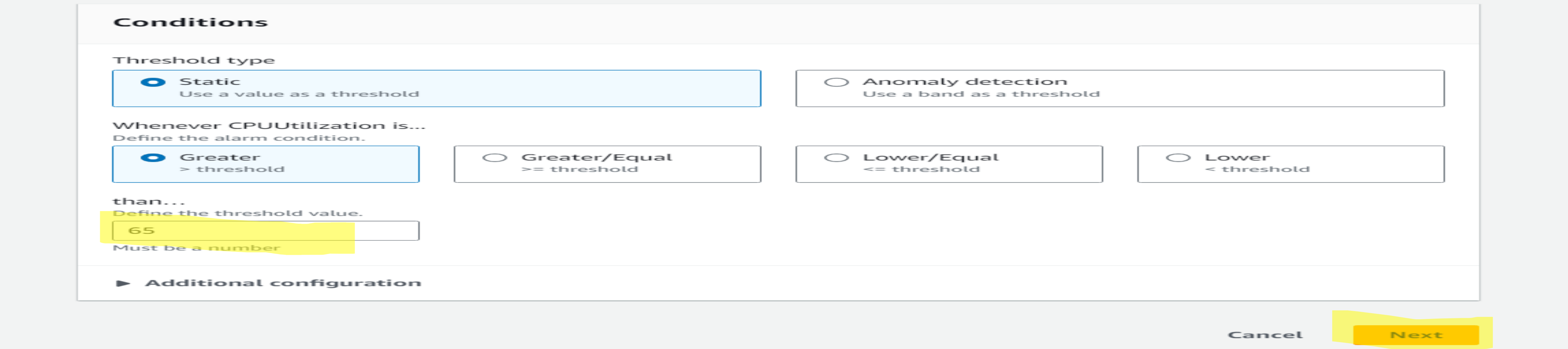
Metric name
CPUUtilization

InstanceId
i-0f7b46a63d4c490d6

Instance name
cloudwatch

Statistic
Average

Period
5 minutes



Conditions

Threshold type

● Static
Use a value as a threshold

○ Anomaly detection
Use a band as a threshold

Whenever CPUUtilization is...
Define the alarm condition.

● Greater
> threshold

○ Greater/Equal
>= threshold

○ Lower/Equal
<= threshold

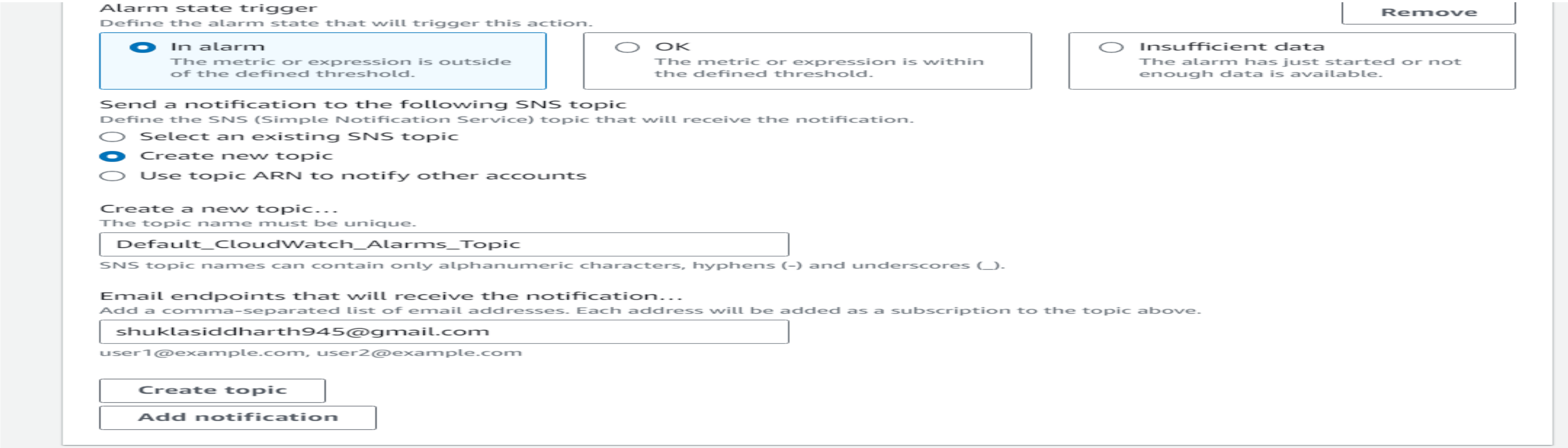
○ Lower
< threshold

than...
Define the threshold value.

65

Must be a number

► Additional configuration



Alarm state trigger
Define the alarm state that will trigger this action.

● In alarm
The metric or expression is outside of the defined threshold.

○ OK
The metric or expression is within the defined threshold.

○ Insufficient data
The alarm has just started or not enough data is available.

Send a notification to the following SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.

○ Select an existing SNS topic
● Create new topic
○ Use topic ARN to notify other accounts

Create a new topic...
The topic name must be unique.

Default_CloudWatch_Alarms_Topic

SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).

Email endpoints that will receive the notification...
Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

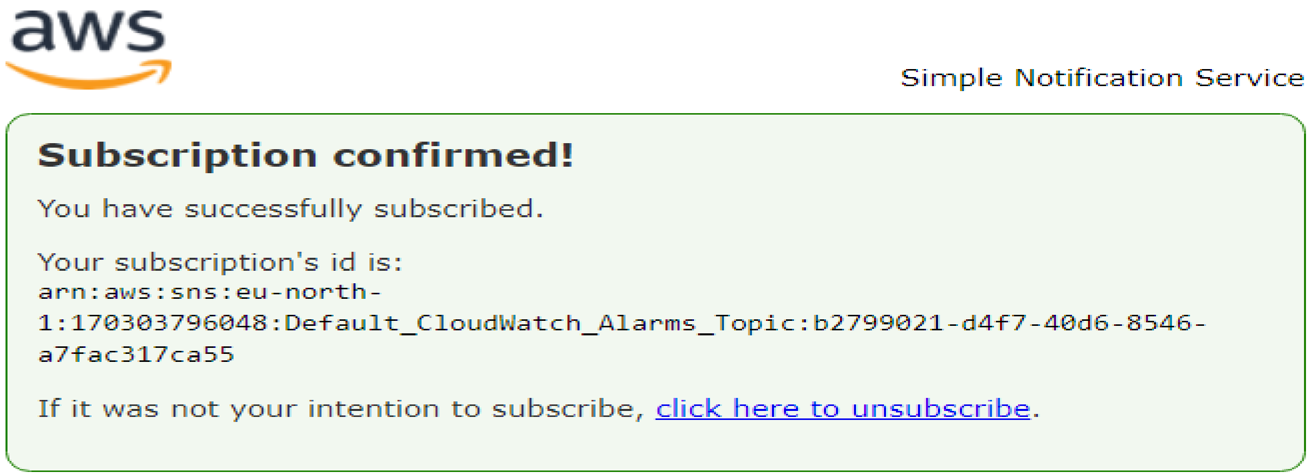
shuklasiddharth945@gmail.com

user1@example.com, user2@example.com

Create a topic – next – name the alarm review and create alarm.

Check your email – confirm subscription.

For creating the billing alarm you need to go the North Virginia region specifically – choose billing create billing alarm rest the steps are same .



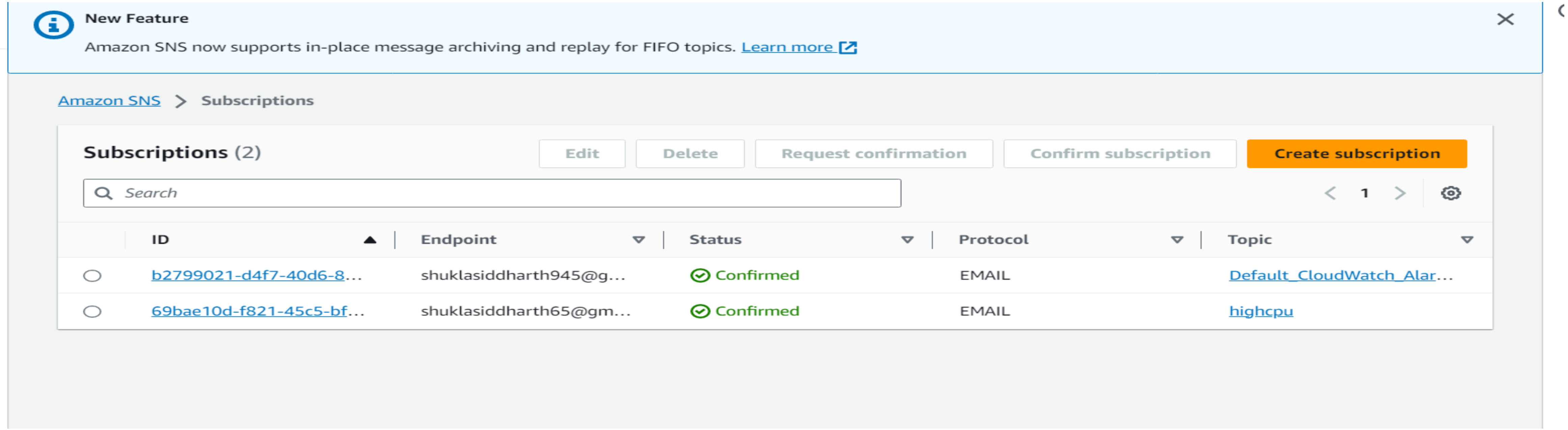
Simple Notification Service

Subscription confirmed!

You have successfully subscribed.

Your subscription's id is:
arn:aws:sns:eu-north-1:170303796048:Default_CloudWatch_Alarms_Topic:b2799021-d4f7-40d6-8546-a7fac317ca55

If it was not your intention to subscribe, click here to unsubscribe.



New Feature

Amazon SNS now supports in-place message archiving and replay for FIFO topics. Learn more

Amazon SNS > Subscriptions

Subscriptions (2)

	ID	Endpoint	Status	Protocol	Topic
○	b2799021-d4f7-40d6-8...	shuklasiddharth945@g...	Confirmed	EMAIL	Default_CloudWatch_Alar...
○	69bae10d-f821-45c5-bf...	shuklasiddharth65@gm...	Confirmed	EMAIL	highcpu