Assignment 2 - Setup your person AWS account

Task 1 – Enable MFA

Enable MFA for the root user. Install and use **Authy** app on your phone. Refer: Enabling a virtual multi-factor authentication (MFA) device (console)

Task 2 – Create an IAM user

Create an admin group with an administrator policy. Create a user for yourself in that group. Always use that IAM user. Refer: Set Up an AWS Account and Create an Administrator User

> *The best practice is always to use an IAM user. Never use your root user. If the IAM user credentials are compromised, you can use the root user and disable the IAM user. If you lose your root user credentials, no one can do anything about it even AWS and your card is linked there.*

Task 3 – Set up a billing alarm

Refer: Create a billing alarm to monitor your estimated AWS charges

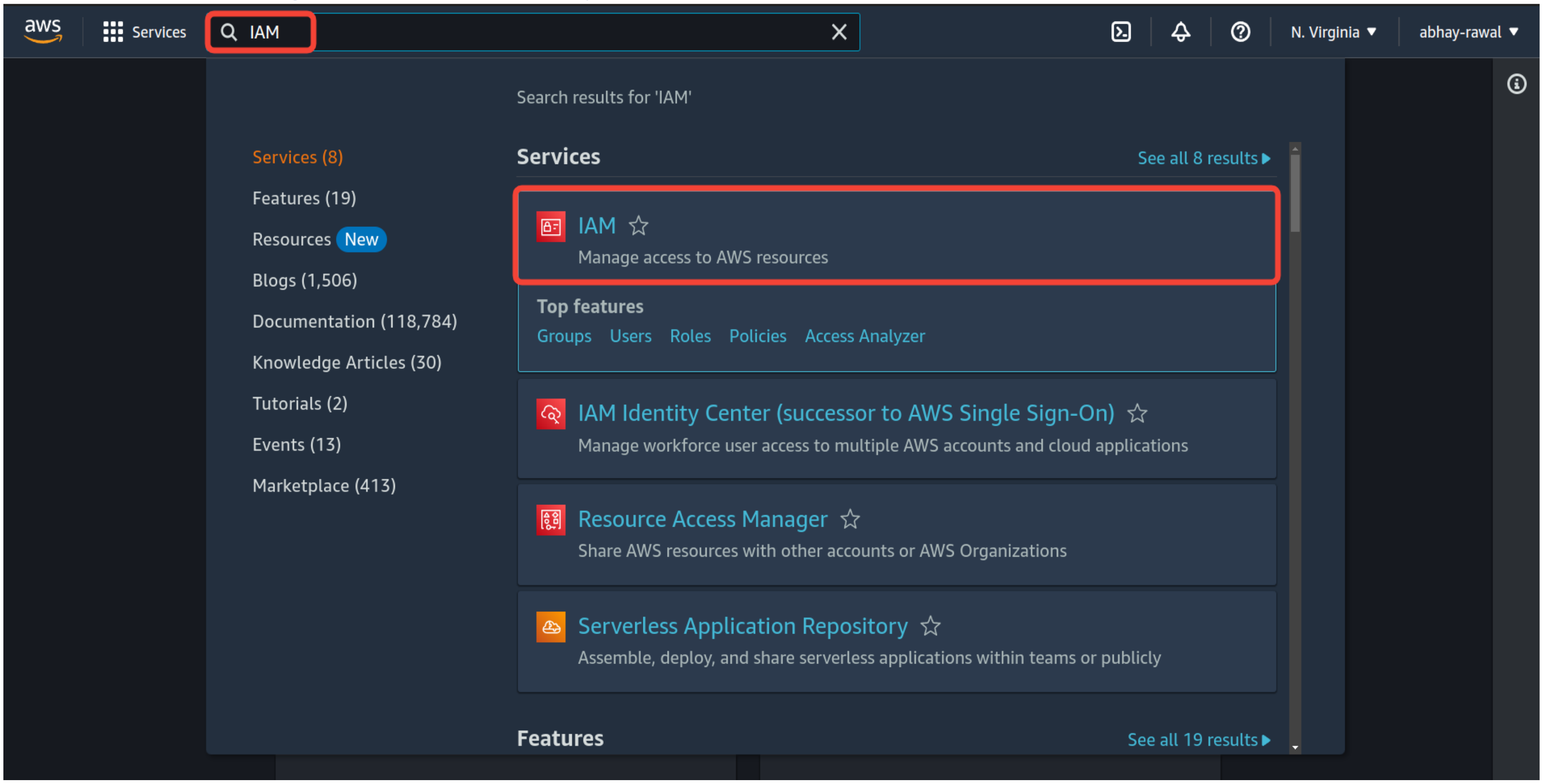
a. Make sure the region is **North Virginia**
b. Go to CloudWatch
c. In Alarms, you will see "Billing" which selects the billing metric automatically.

Task 4 – Practice IAM condition

List buckets based on a user tag. Write a custom IAM policy with a condition.
If the user has a "teams" tag which equals to "DevOps", then allow them to list buckets.

1. Create a custom IAM policy that allows ListBuckets and ListObjecs in a bucket with a condition, allow if the principle tag equals to DevOps. {tagName = teams, value = DevOps}
2. Create group named "Developer". Associate with the IAM policy above.
3. Create Two Users,
   a. User1-DevOps with a Tag "teams" ="DevOps"
   b. User2-Tester
4. Create S3 Bucket
5. Put Object/file to the Bucket
6. Test

Creating an IAM user for yourself



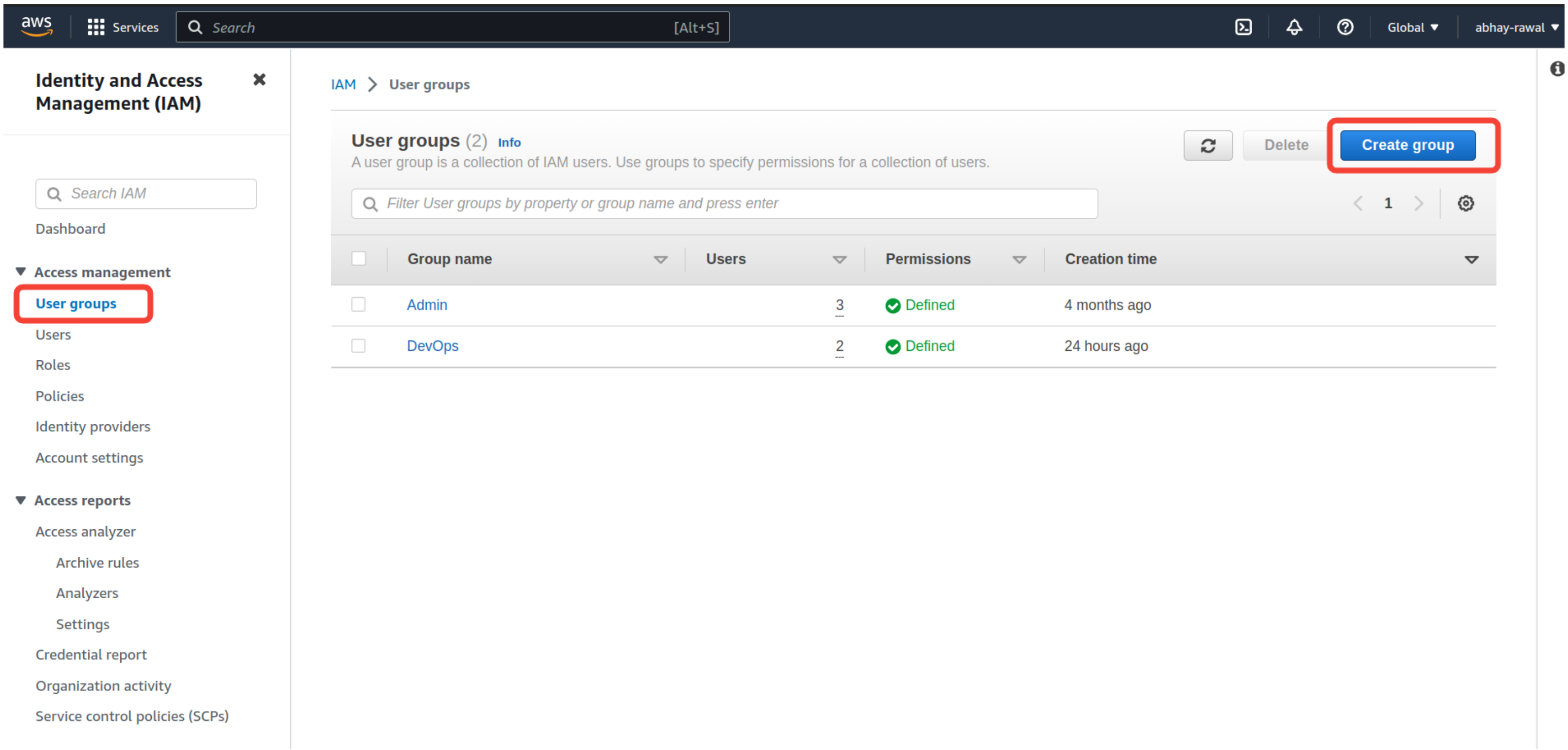
Search results for 'IAM'

IAM
Manage access to AWS resources

IAM Identity Center (successor to AWS Single Sign-On)
Manage workforce user access to multiple AWS accounts and cloud applications

Resource Access Manager
Share AWS resources with other accounts or AWS Organizations

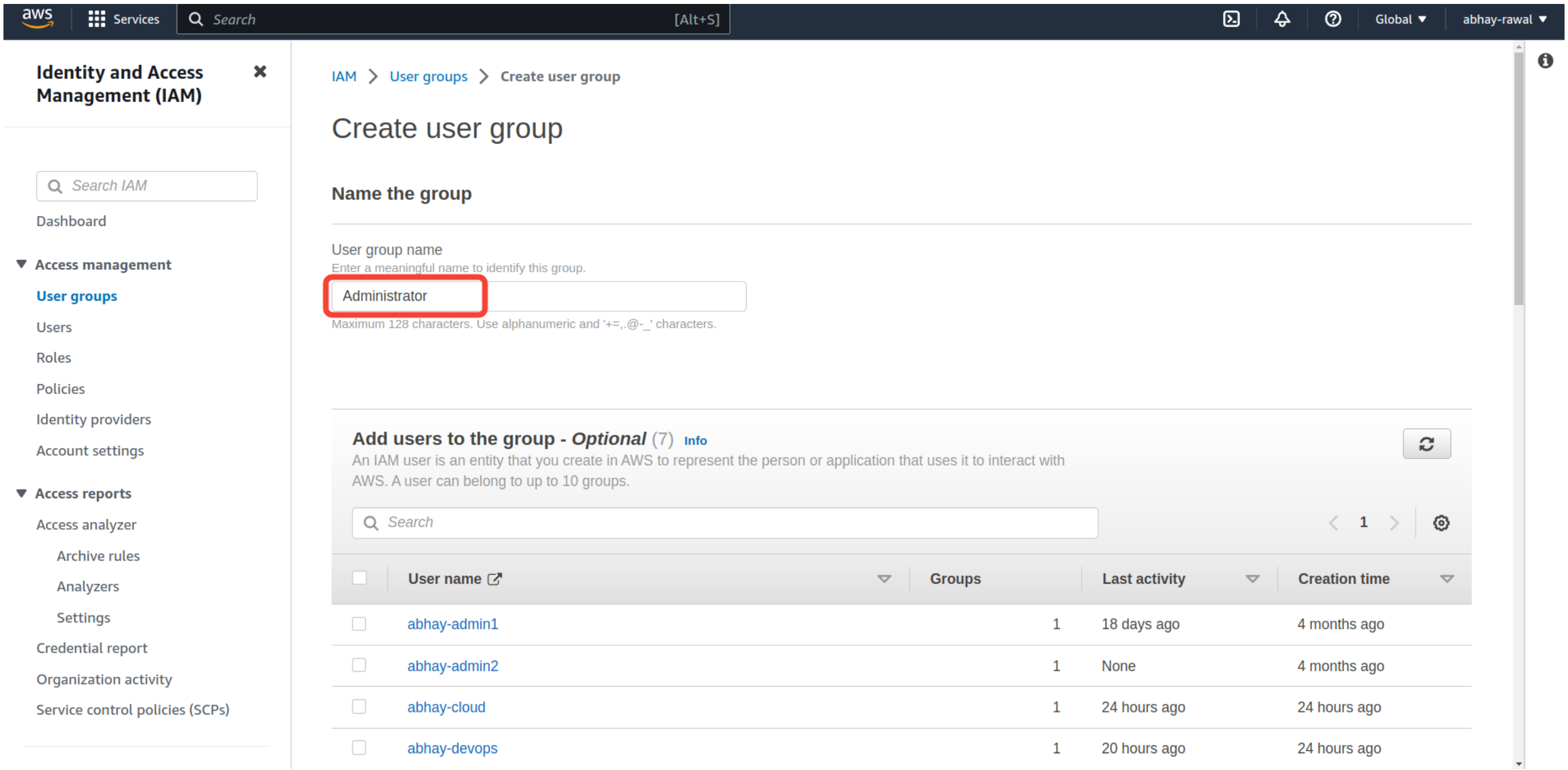
Serverless Application Repository
Assemble, deploy, and share serverless applications within teams or publicly



User groups (2) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

□	Group name	Users	Permissions	Creation time
□	Admin	3	✓ Defined	4 months ago
□	DevOps	2	✓ Defined	24 hours ago



Identity and Access Management (IAM)

Search IAM

- Dashboard
- ▼ Access management
  - User groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
- ▼ Access reports
  - Access analyzer
    - Archive rules
    - Analyzers
    - Settings
  - Credential report
  - Organization activity
  - Service control policies (SCPs)

IAM > User groups > Create user group

Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

Administrator

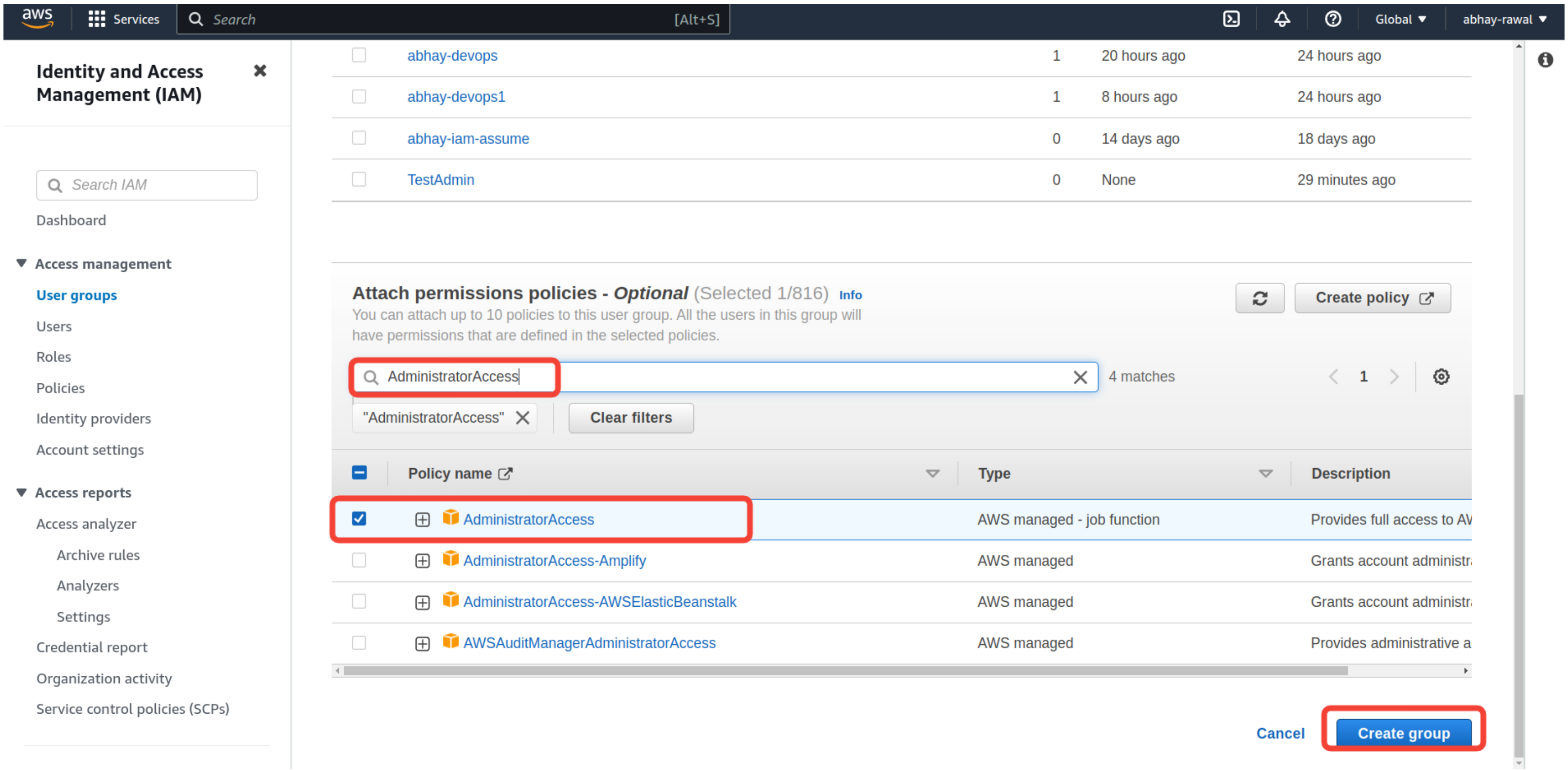
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (7) 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. A user can belong to up to 10 groups.

Search

	User name	Groups	Last activity	Creation time
□	abhay-admin1	1	18 days ago	4 months ago
□	abhay-admin2	1	None	4 months ago
□	abhay-cloud	1	24 hours ago	24 hours ago
□	abhay-devops	1	20 hours ago	24 hours ago



Identity and Access Management (IAM)

Search IAM

- Dashboard
- ▼ Access management
  - User groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
- ▼ Access reports
  - Access analyzer
    - Archive rules
    - Analyzers
    - Settings
  - Credential report
  - Organization activity
  - Service control policies (SCPs)

	User name	Groups	Last activity	Creation time
□	abhay-devops	1	20 hours ago	24 hours ago
□	abhay-devops1	1	8 hours ago	24 hours ago
□	abhay-iam-assume	0	14 days ago	18 days ago
□	TestAdmin	0	None	29 minutes ago

Attach permissions policies - *Optional* (Selected 1/816) Info

Create policy

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.

AdministratorAccess — 4 matches

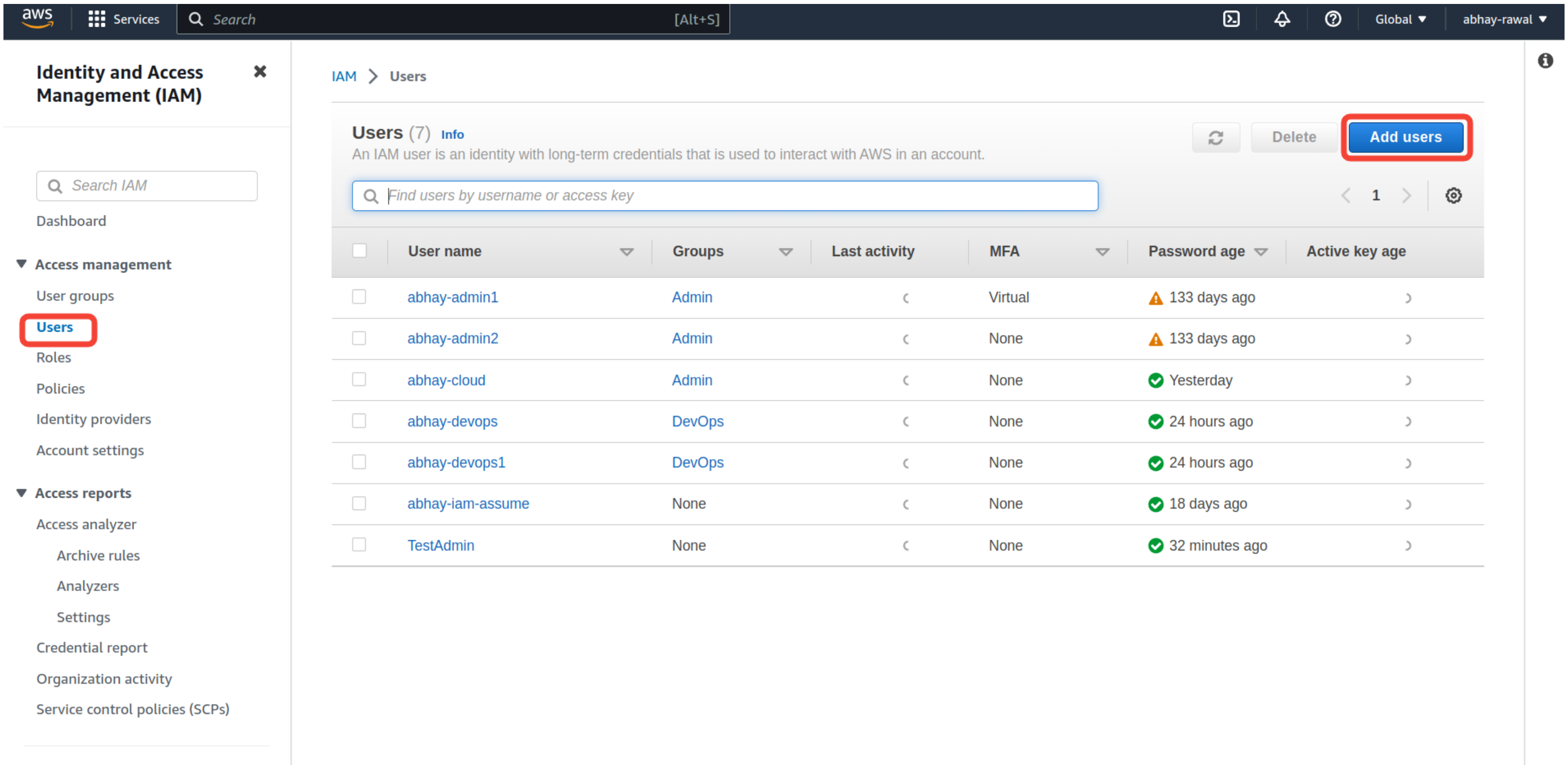
"AdministratorAccess" ✕ Clear filters

	Policy name	Type	Description
☑	⊞ AdministratorAccess	AWS managed - job function	Provides full access to AV
□	⊞ AdministratorAccess-Amplify	AWS managed	Grants account administr
□	⊞ AdministratorAccess-AWSElasticBeanstalk	AWS managed	Grants account administr
□	⊞ AWSAuditManagerAdministratorAccess	AWS managed	Provides administrative a

Cancel — Create group

Creating IAM users and adding to a group

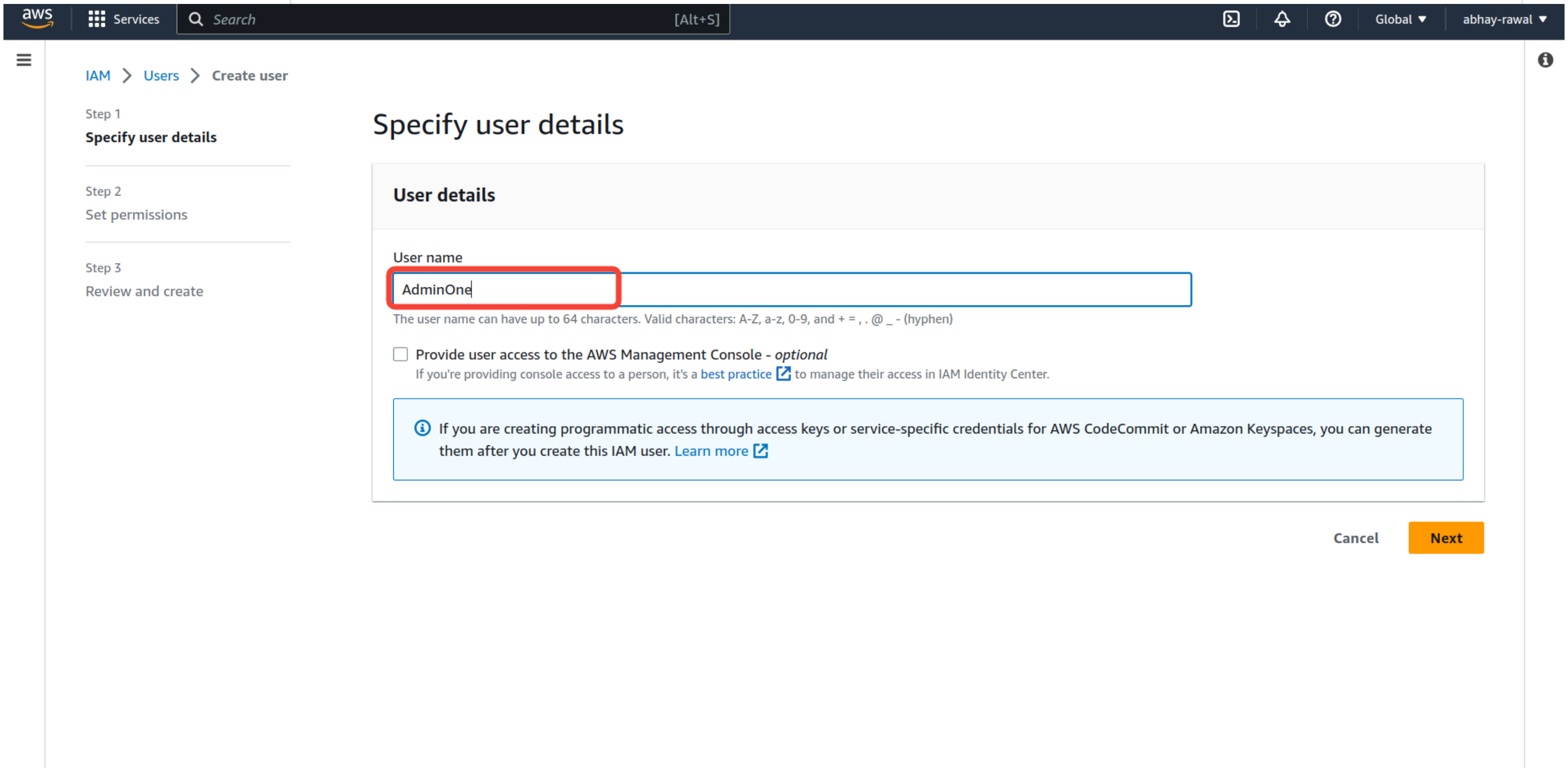
1. Sign into the AWS Management Console and open the IAM console
2. In the navigation pane, choose **Users** and then select **Add users.**



Users (7) Info

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

□	User name	Groups	Last activity	MFA	Password age	Active key age
□	abhay-admin1	Admin		Virtual	⚠ 133 days ago	
□	abhay-admin2	Admin		None	⚠ 133 days ago	
□	abhay-cloud	Admin		None	✓ Yesterday	
□	abhay-devops	DevOps		None	✓ 24 hours ago	
□	abhay-devops1	DevOps		None	✓ 24 hours ago	
□	abhay-iam-assume	None		None	✓ 18 days ago	
□	TestAdmin	None		None	✓ 32 minutes ago	



Specify user details

User details

User name: AdminOne

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*

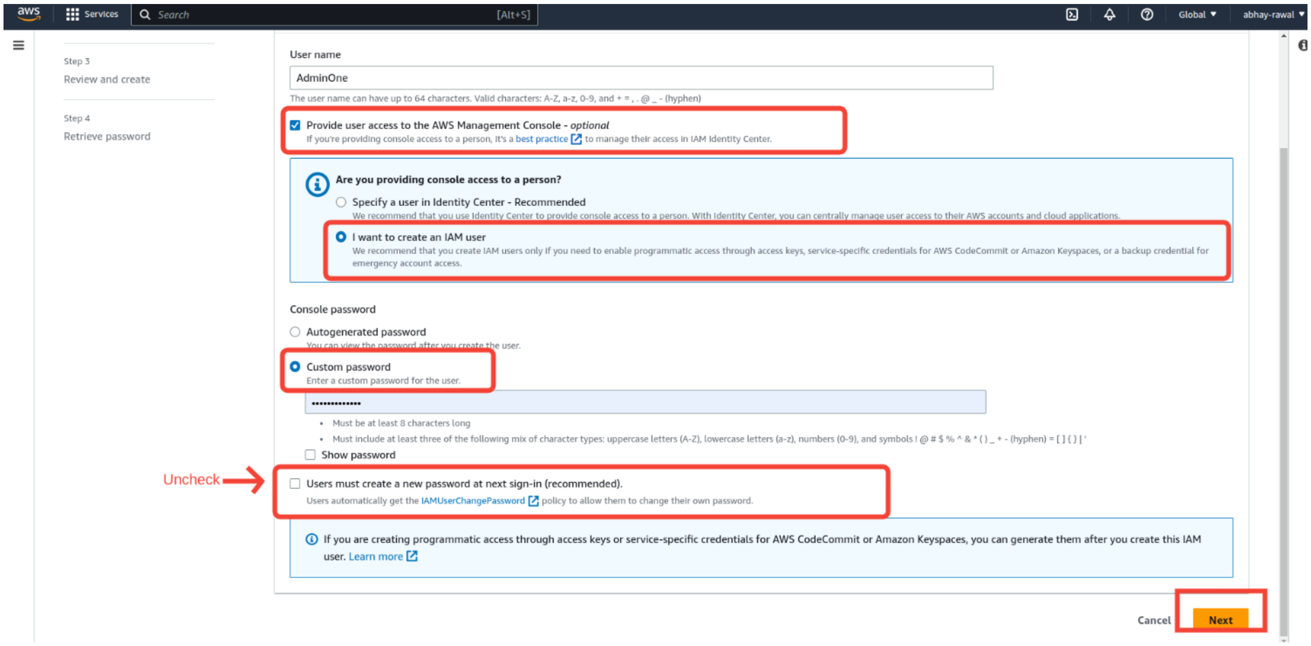
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

ⓘ 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

Note: 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.

a. Now we need to select if we want to Specify a user in Identity Center or Create an IAM user. **Choose "I want to create an IAM user".**

- After selecting **I want to create an IAM user,** you can choose one of the Password:
  a. **Autogenerated password.** Each user gets a randomly generated password that meets the account password policy. You can view or download the passwords when you get to the **Final** page.
  b. **Custom password.** Each user is assigned the password that you type in the box.
- For this demo uncheck **Users must create a new password at next sign-in.**
- Click Next



Step 3
Review and create

Step 4
Retrieve password

User name

AdminOne

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?

○ 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.

••••••••••••••

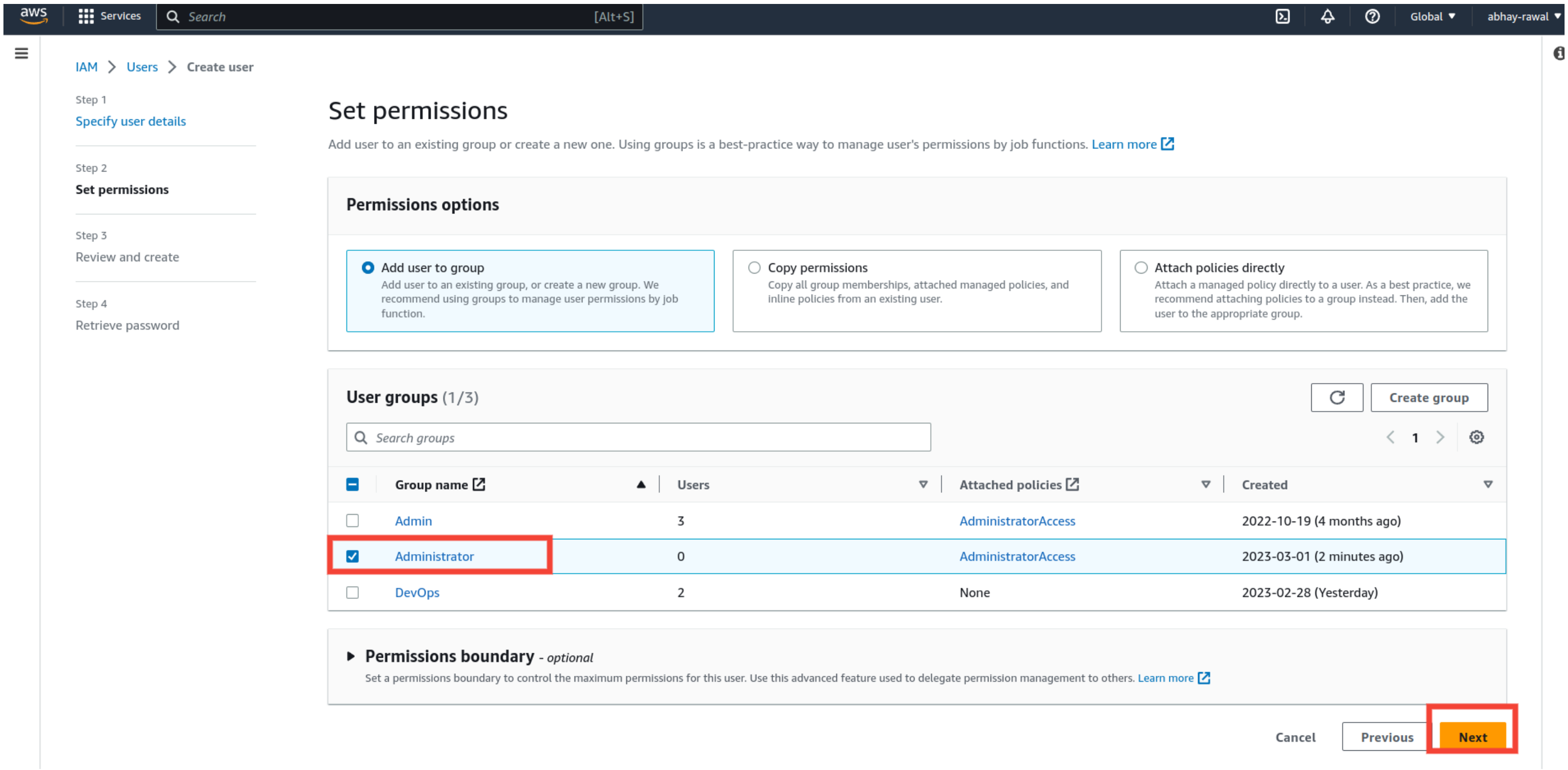
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ Show password

Uncheck →

□ 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



IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

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.

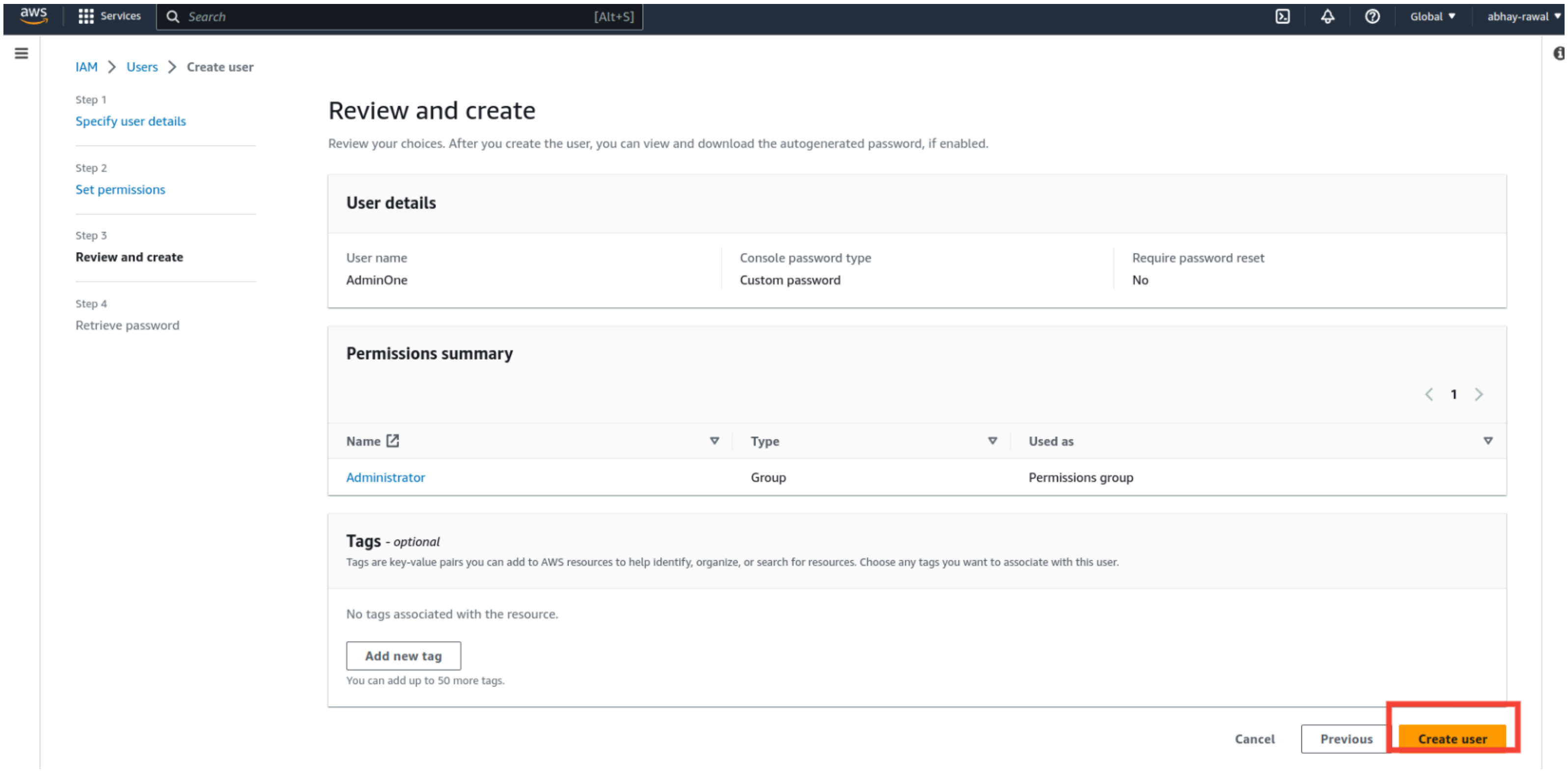
○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

○ 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 (1/3)

	Group name	Users	Attached policies	Created
□	Admin	3	AdministratorAccess	2022-10-19 (4 months ago)
☑	Administrator	0	AdministratorAccess	2023-03-01 (2 minutes ago)
□	DevOps	2	None	2023-02-28 (Yesterday)

Permissions boundary - *optional*
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more



IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

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	Console password type	Require password reset
AdminOne	Custom password	No

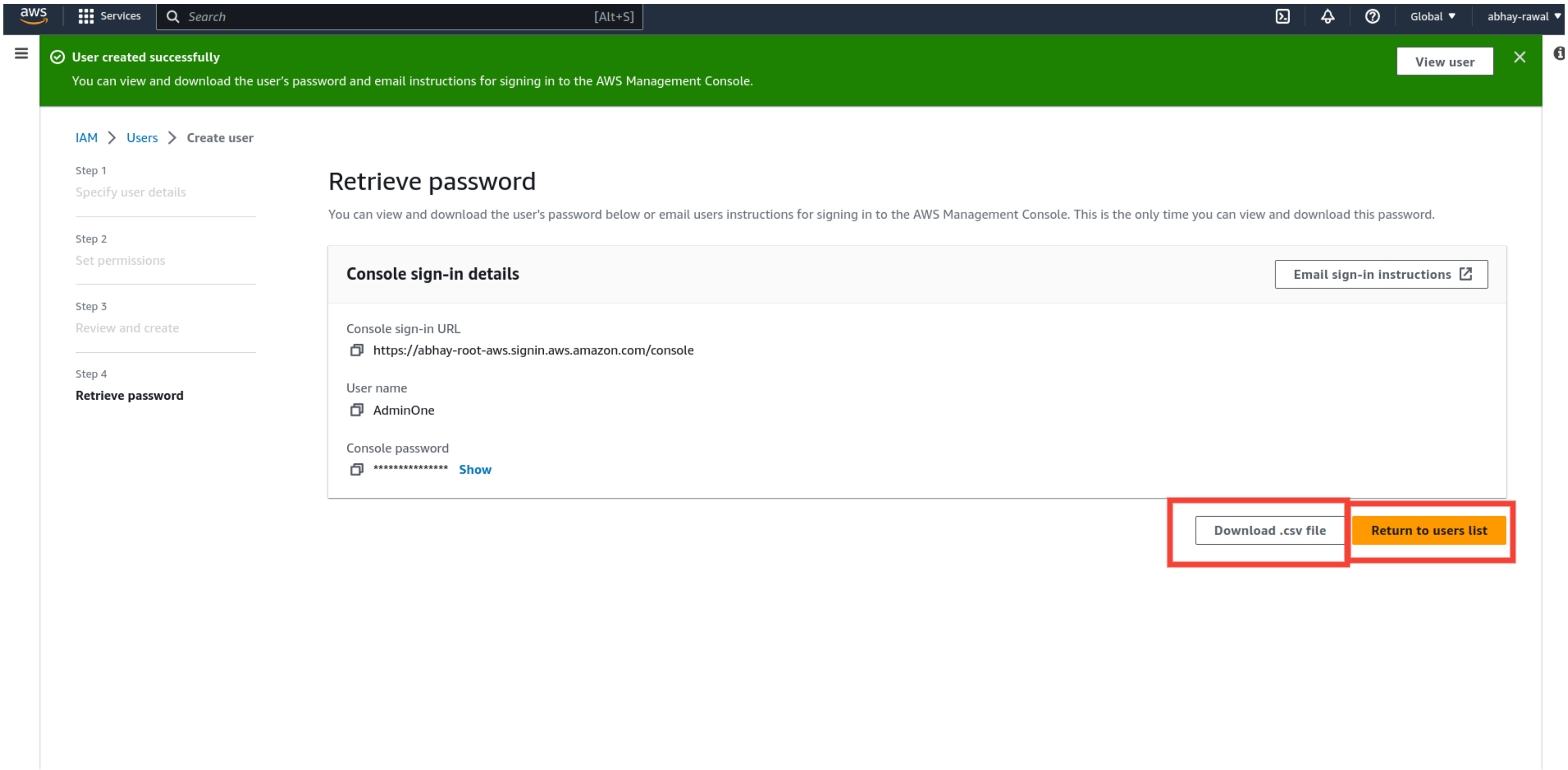
Permissions summary

Name	Type	Used as
Administrator	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.

You can add up to 50 more tags.



User created successfully

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

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

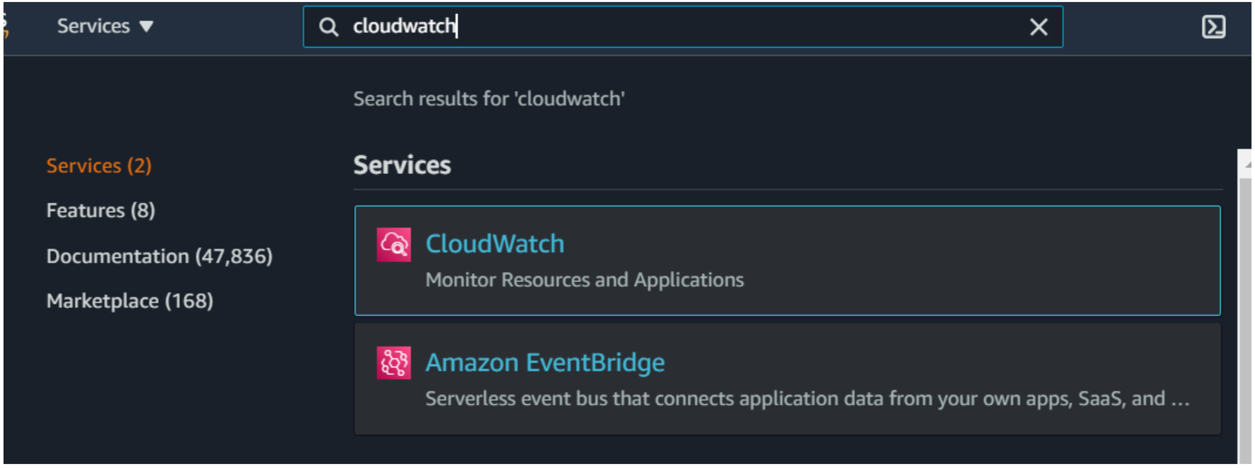
Console sign-in URL
https://abhay-root-aws.signin.aws.amazon.com/console

User name
AdminOne

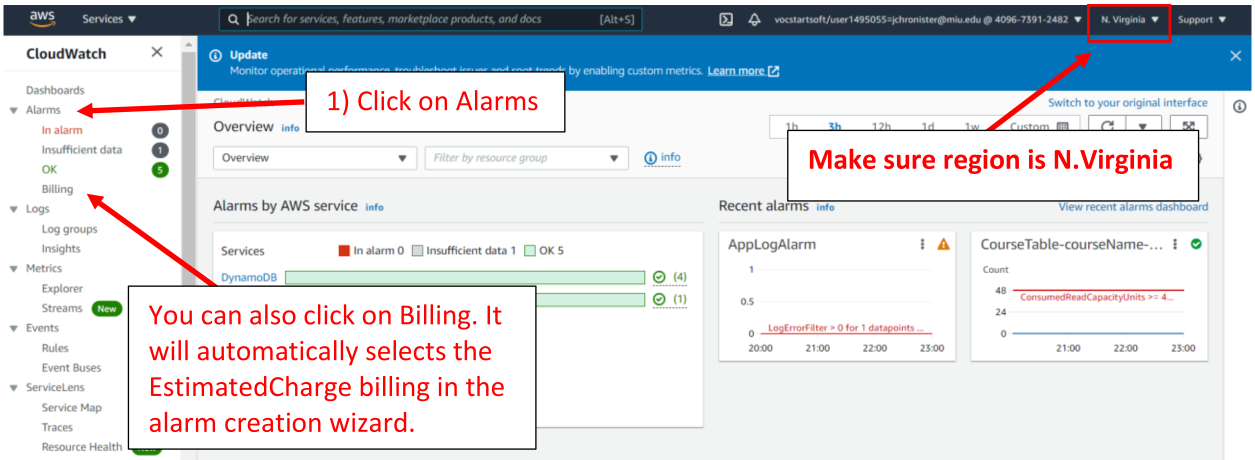
Console password
****

Setting up a billing alarm on CloudWatch

Go to the CloudWatch Display. Search or Find under All Services Management & Governance Group


Services ▼
cloudwatch
Search results for 'cloudwatch'
Services (2)
Features (8)
Documentation (47,836)
Marketplace (168)
Services
CloudWatch
Monitor Resources and Applications
Amazon EventBridge
Serverless event bus that connects application data from your own apps, SaaS, and …

Go to the Alarms Display. You must select us-east-1 **N.Virginia** region. Otherwise, billing metric is not there.

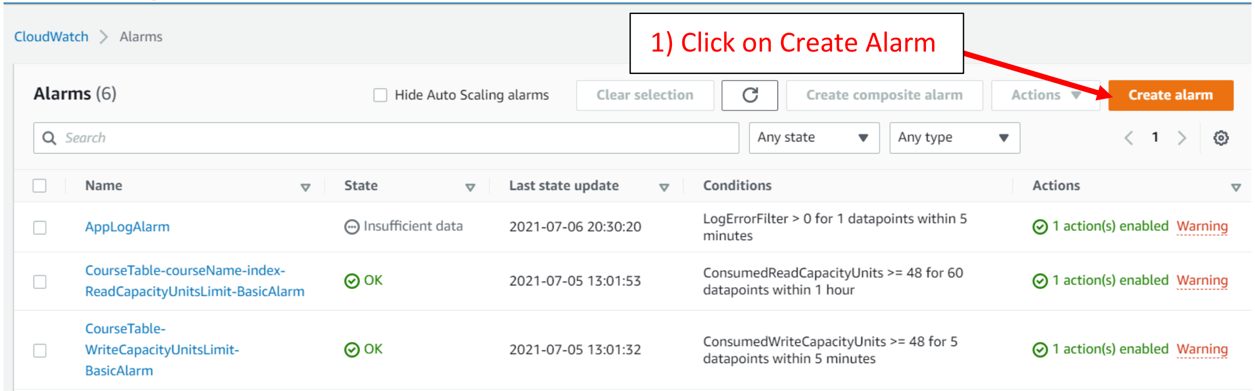


1) Click on Alarms

Make sure region is N.Virginia

You can also click on Billing. It will automatically selects the EstimatedCharge billing in the alarm creation wizard.

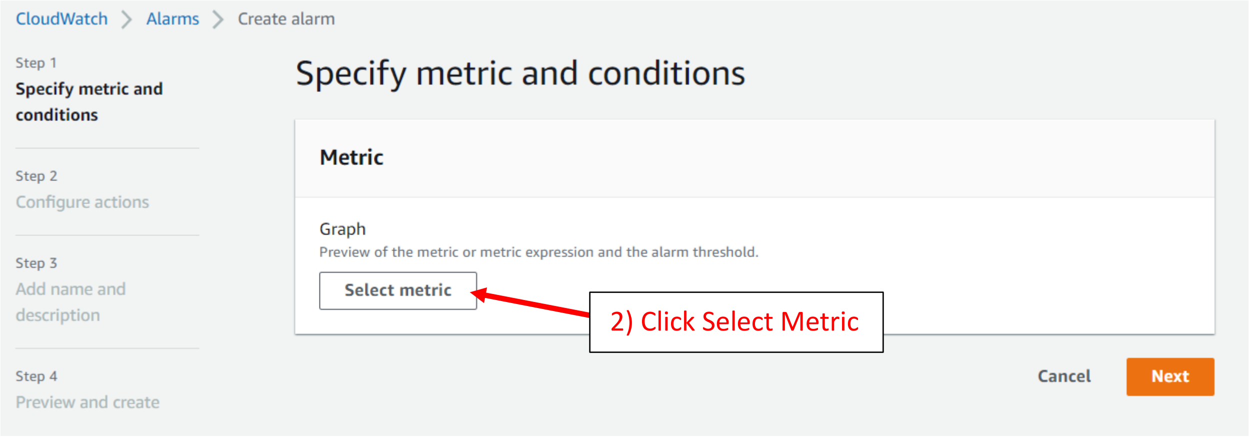
Create Billing Alarm



1) Click on Create Alarm

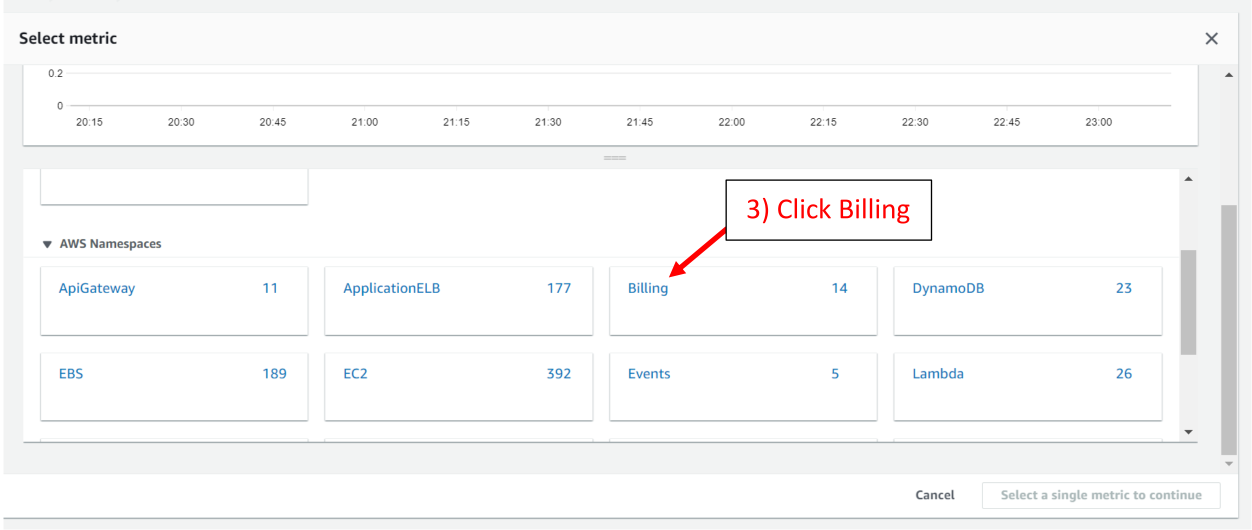
□	Name	State	Last state update	Conditions	Actions
□	AppLogAlarm	Insufficient data	2021-07-06 20:30:20	LogErrorFilter > 0 for 1 datapoints within 5 minutes	✓ 1 action(s) enabled Warning
□	CourseTable-courseName-index-ReadCapacityUnitsLimit-BasicAlarm	✓ OK	2021-07-05 13:01:53	ConsumedReadCapacityUnits >= 48 for 60 datapoints within 1 hour	✓ 1 action(s) enabled Warning
□	CourseTable-WriteCapacityUnitsLimit-BasicAlarm	✓ OK	2021-07-05 13:01:32	ConsumedWriteCapacityUnits >= 48 for 5 datapoints within 5 minutes	✓ 1 action(s) enabled Warning

…


CloudWatch > Alarms > Create alarm
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add name and description
Step 4
Preview and create
Specify metric and conditions
Metric
Graph
Preview of the metric or metric expression and the alarm threshold.
Select metric
Cancel
Next

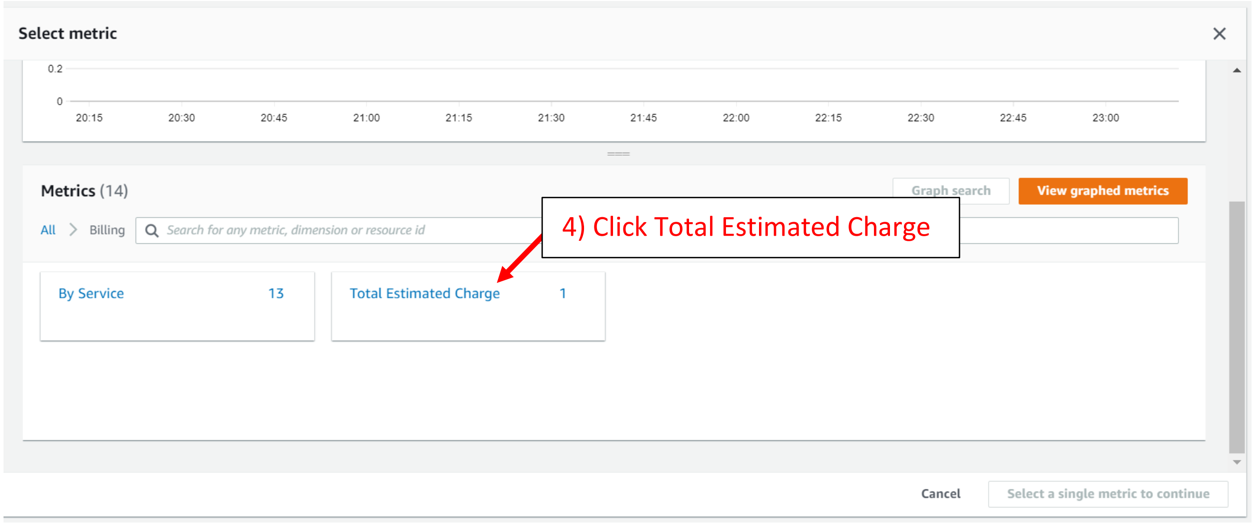
2) Click Select Metric

...



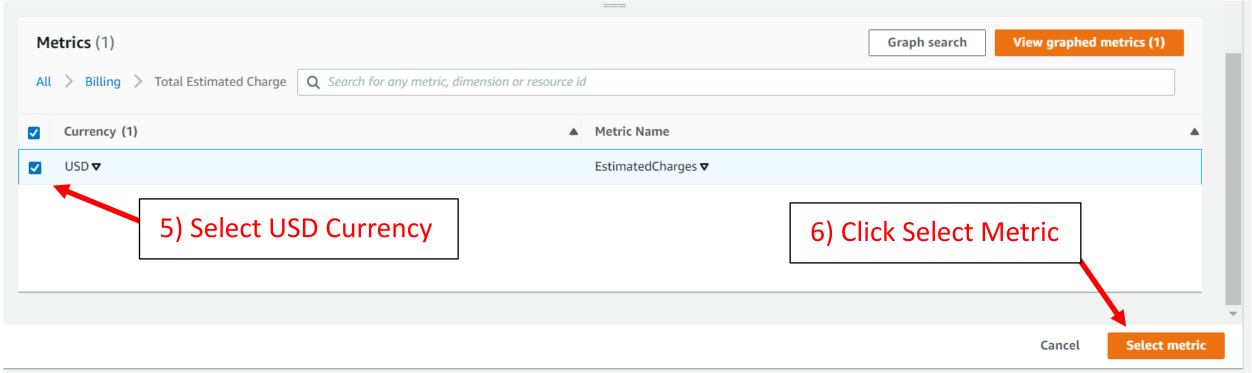
3) Click Billing

...



4) Click Total Estimated Charge

...

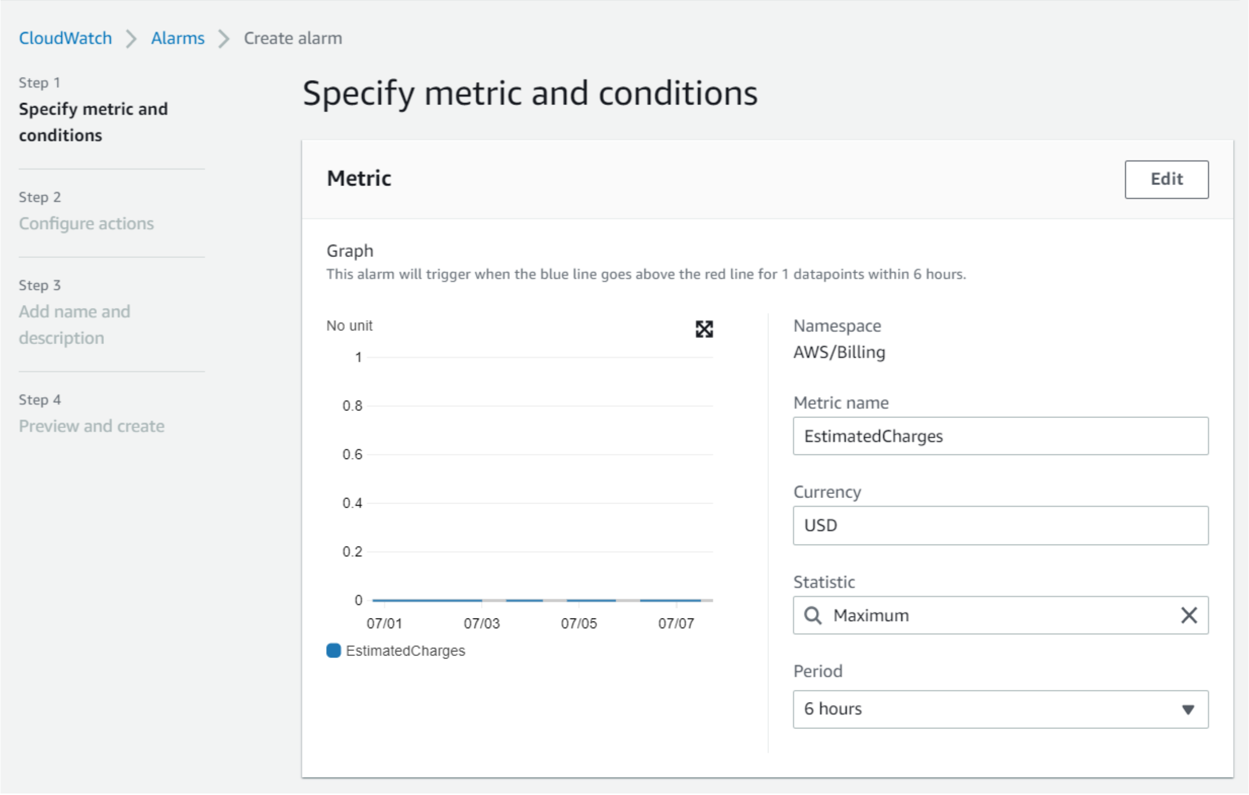

Graph search
View graphed metrics (1)
All > Billing > Total Estimated Charge
Search for any metric, dimension or resource id
Cancel
Select metric

Metrics (1)

☑ Currency (1)	Metric Name
☑ USD	EstimatedCharges

5) Select USD Currency

6) Click Select Metric



Specify metric and conditions

Metric

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 6 hours.

Namespace: AWS/Billing

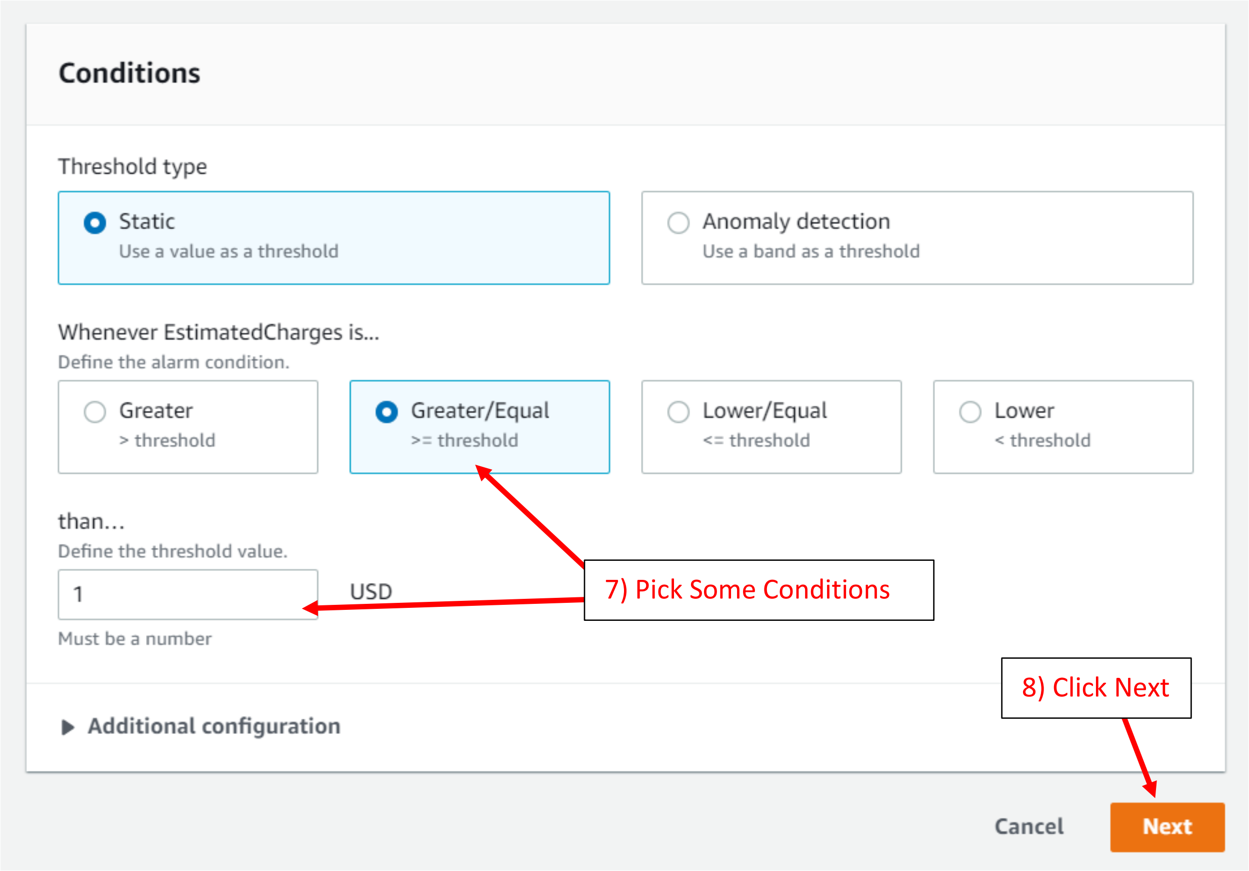
Metric name: EstimatedCharges

Currency: USD

Statistic: Maximum

Period: 6 hours

…



Conditions

Threshold type

● Static
Use a value as a threshold

○ Anomaly detection
Use a band as a threshold

Whenever EstimatedCharges is...
Define the alarm condition.

○ Greater
> threshold

● Greater/Equal
>= threshold

○ Lower/Equal
<= threshold

○ Lower
< threshold

than...
Define the threshold value.

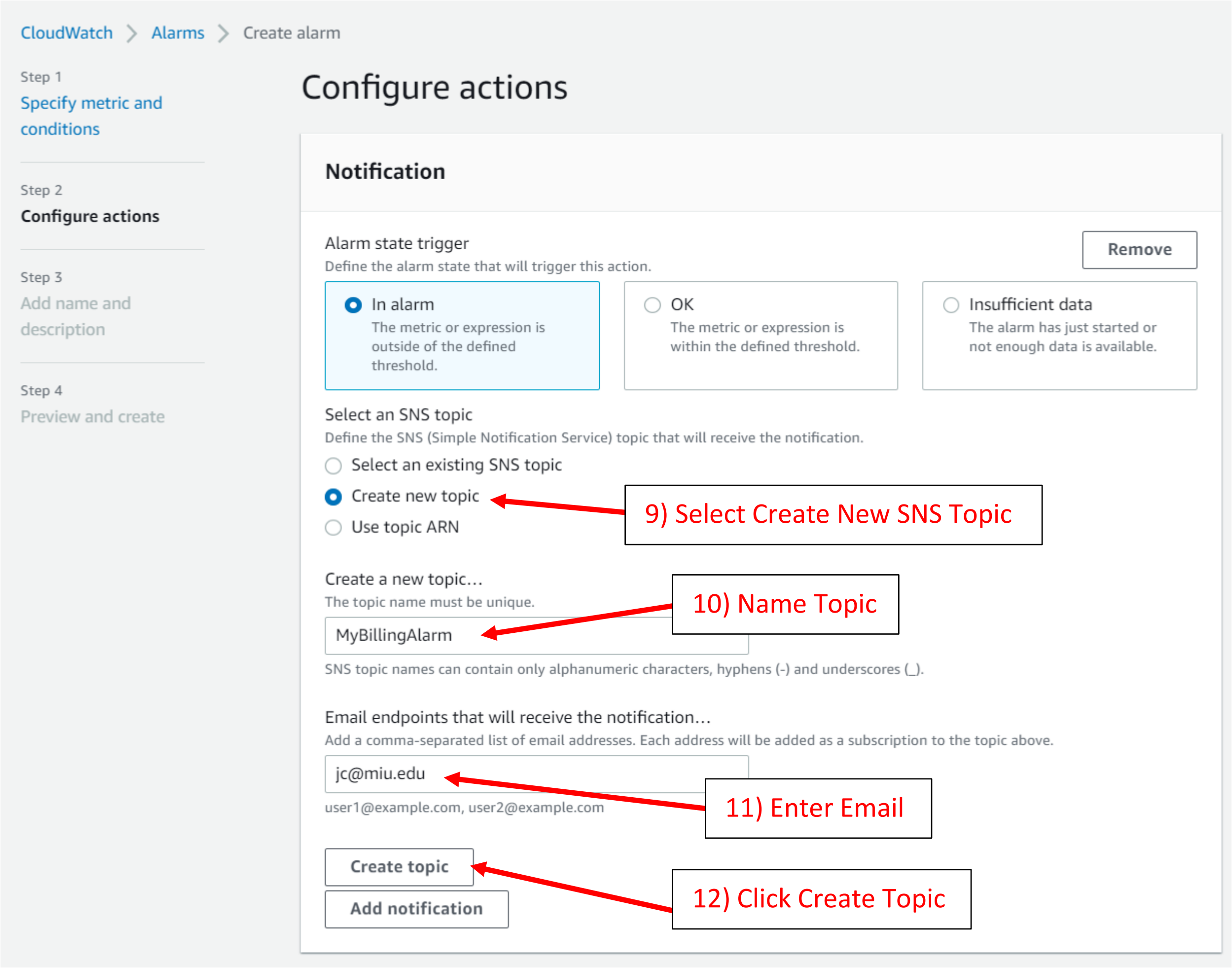
1 USD

Must be a number

▶ Additional configuration

7) Pick Some Conditions

8) Click Next



CloudWatch > Alarms > Create alarm

Step 1
Specify metric and conditions

Step 2
Configure actions

Step 3
Add name and description

Step 4
Preview and create

Configure actions

Notification

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

Remove

● 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.

Select an 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

9) Select Create New SNS Topic

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

MyBillingAlarm

10) Name 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.

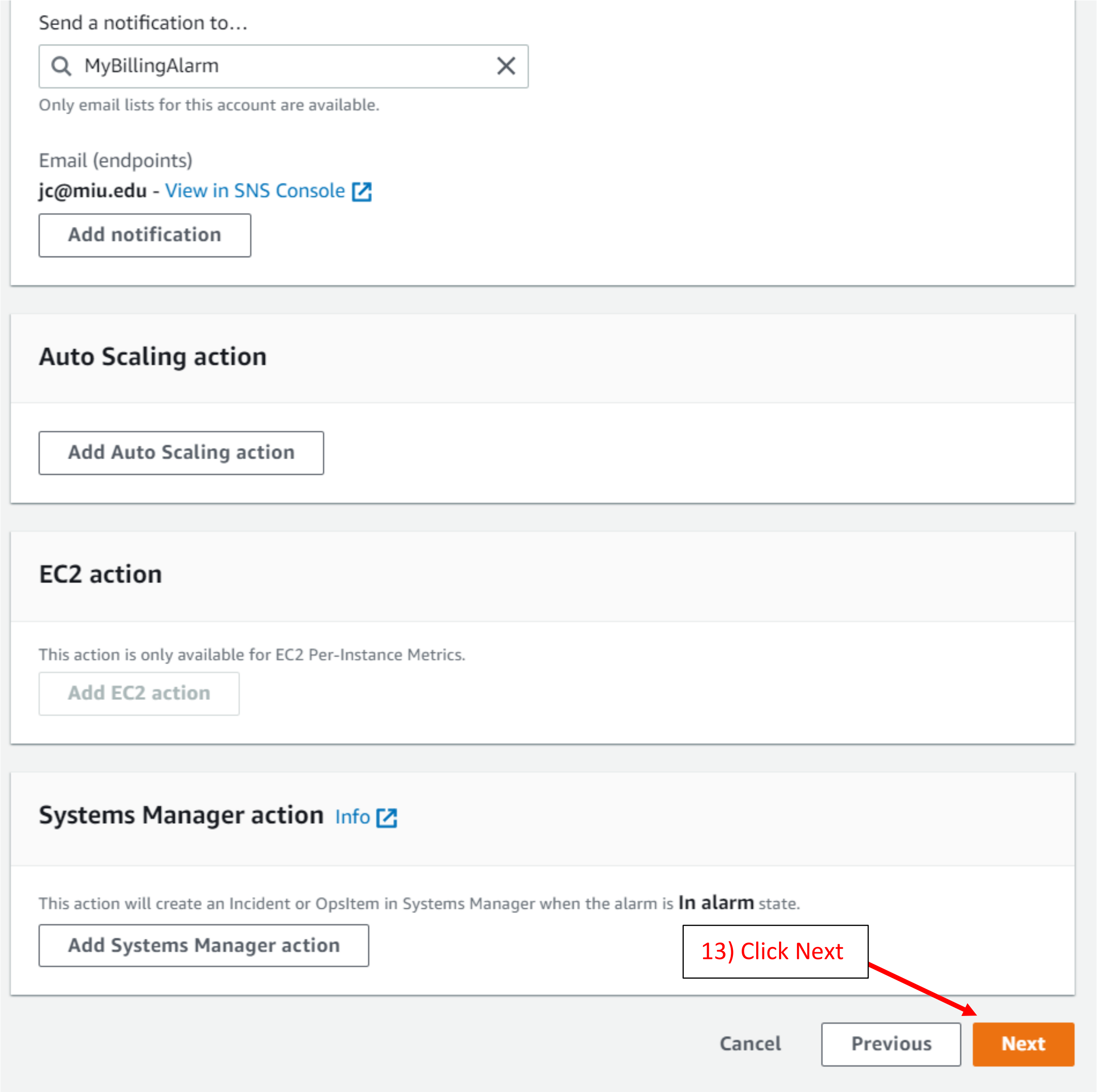
jc@miu.edu

11) Enter Email

user1@example.com, user2@example.com

12) Click Create Topic

…



Send a notification to…

MyBillingAlarm

Only email lists for this account are available.

Email (endpoints)

jc@miu.edu - View in SNS Console

Auto Scaling action

EC2 action

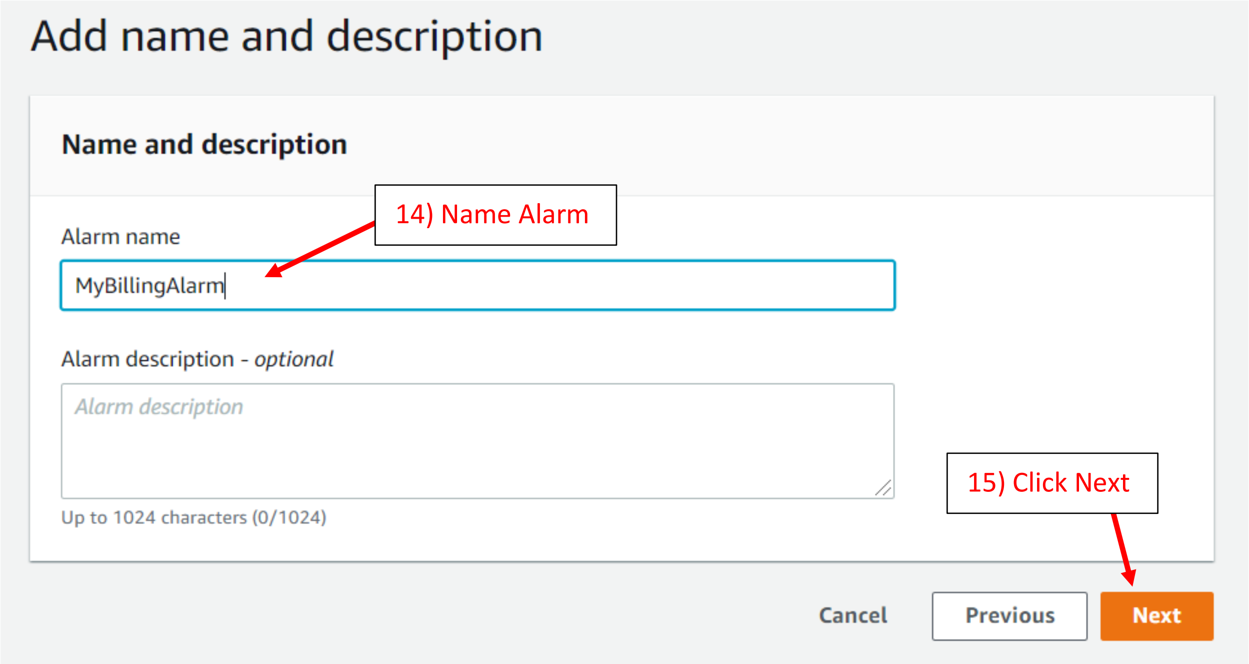
This action is only available for EC2 Per-Instance Metrics.

Systems Manager action Info

This action will create an Incident or OpsItem in Systems Manager when the alarm is **In alarm** state.

13) Click Next

…



Add name and description

Name and description

Alarm name

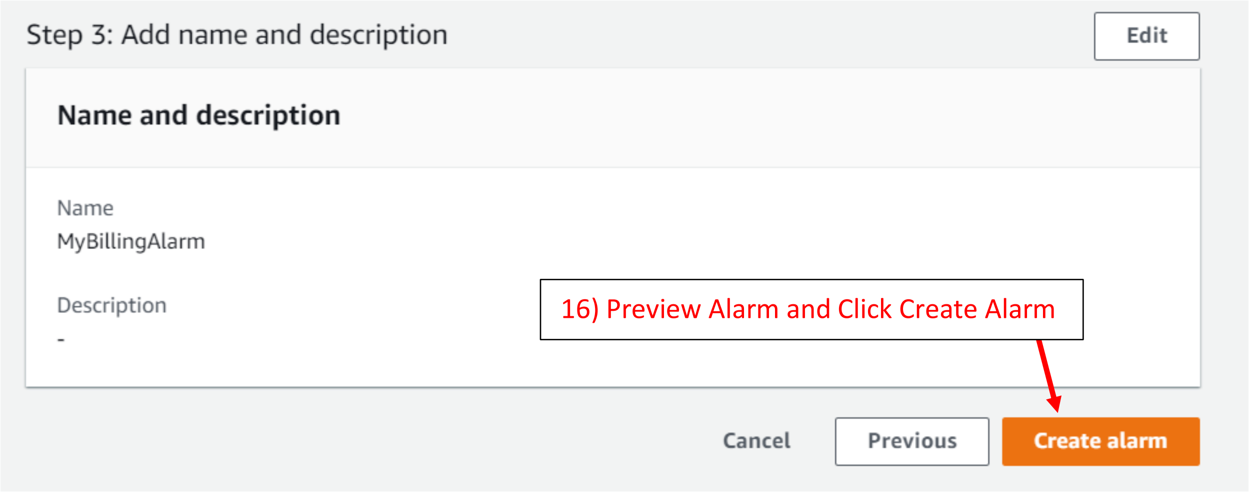
MyBillingAlarm

Alarm description - *optional*

14) Name Alarm

15) Click Next

...



Step 3: Add name and description

Name and description

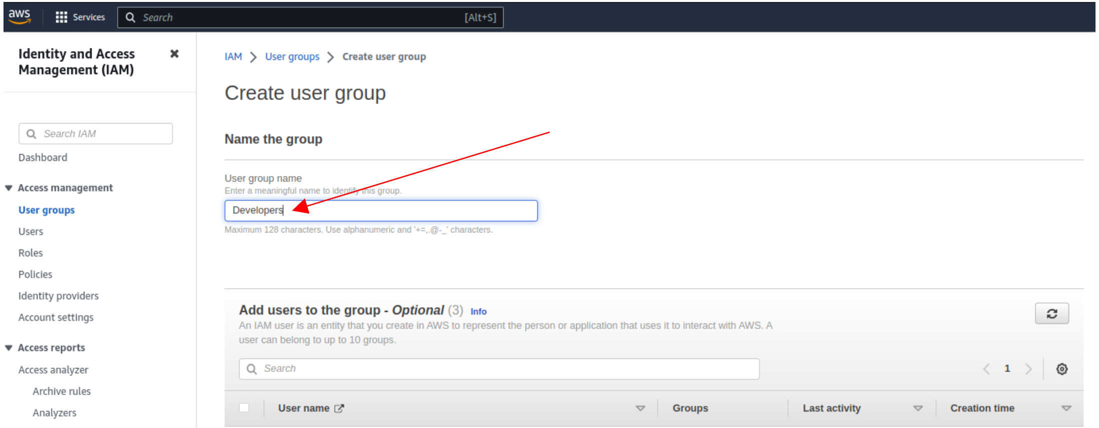
Name
MyBillingAlarm

Description
-

16) Preview Alarm and Click Create Alarm

Practicing an IAM policy with a condition

1 Create group named “Developer”



IAM > User groups > Create user group

Create user group

Name the group

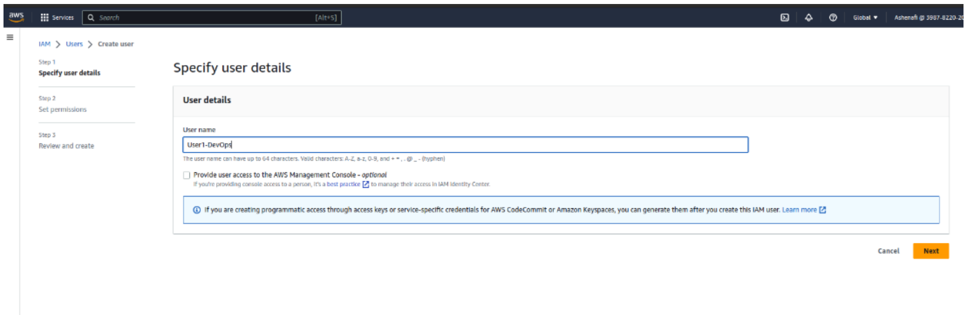
User group name
Enter a meaningful name to identify this group.
Developers
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (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. A user can belong to up to 10 groups.

□	User name	Groups	Last activity	Creation time

2 Create Two Users E.g

- User1-DevOps with Tag “teams” =”DevOps”



IAM > Users > Create user

Step 1 Specify user details
Step 2 Set permissions
Step 3 Review and create

Specify user details

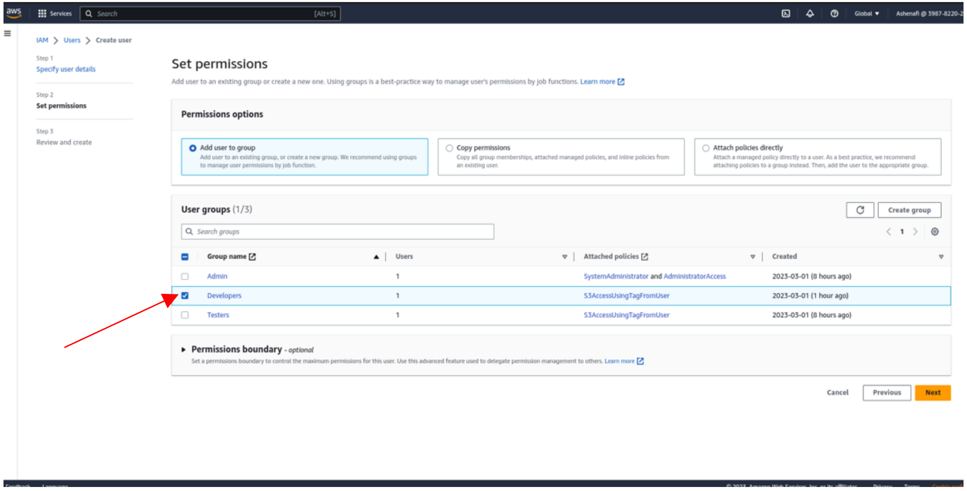
User details

User name
User1-DevOps
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

Add the user to Developer user Group



IAM > Users > Create user

Step 1 Specify user details
Step 2 Set permissions
Step 3 Review and create

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.

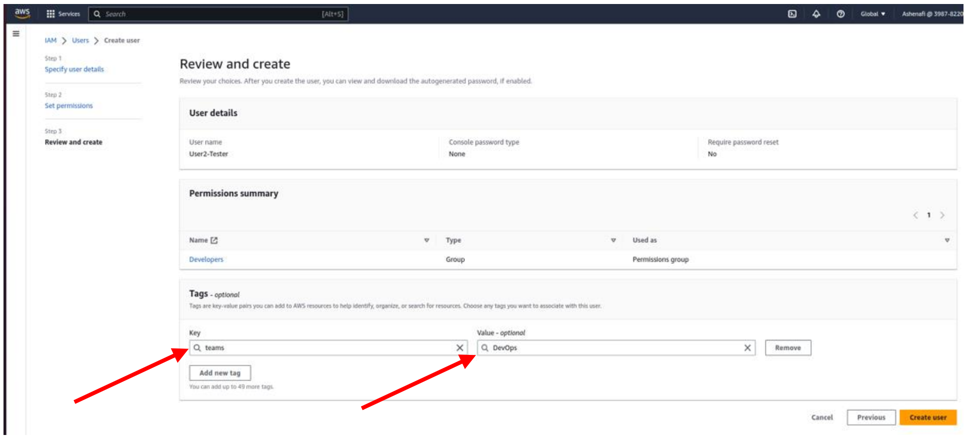
○ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1/3)

	Group name	Users	Attached policies	Created
□	Admin	1	SystemAdministrator and AdministratorAccess	2023-03-01 (8 hours ago)
☑	Developers	1	S3AccessUsingTagFromUser	2023-03-01 (1 hour ago)
□	Testers	1	S3AccessUsingTagFromUser	2023-03-01 (8 hours ago)

Permissions boundary - *optional*
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more

Add tag to user



Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

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	Console password type	Require password reset
User2-Tester	None	No

Permissions summary

Name	Type	Used as
Developers	Group	Permissions group

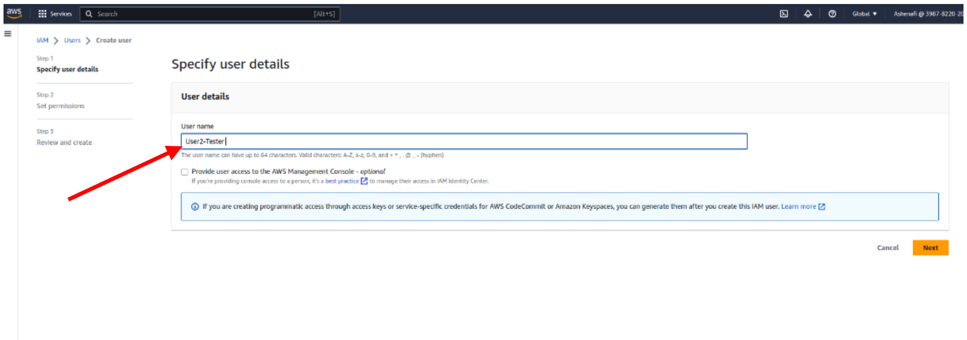
Tags - *optional*

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.

Key: teams
Value - *optional*: DevOps

You can add up to 49 more tags.

- User2-Tester



Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Specify user details

User details

User name: User2-Tester

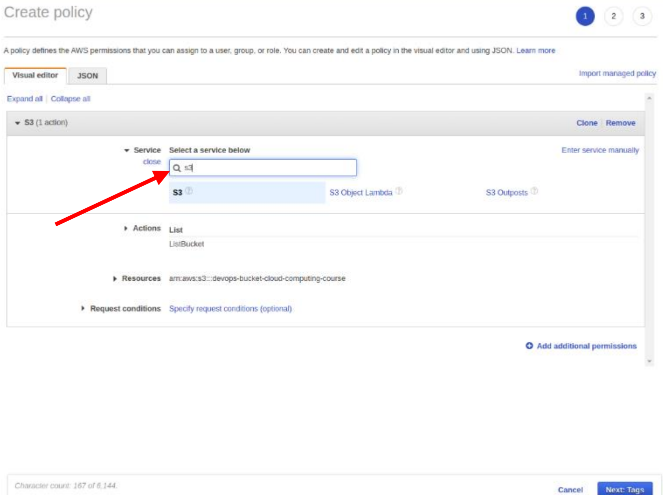
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☐ 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

-

3 Create S3 Bucket
devops-bucket-cloud-computing-course
4 Put Object/file to the Bucket
file1.txt
5 Create a custom IAM policy with Condition {tag name= teams value=DevOps}



Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

S3 (1 action)

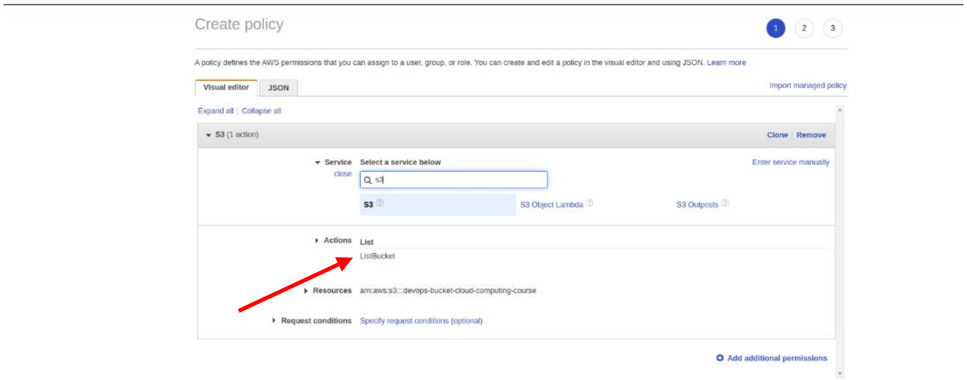
Service: Select a service below: s3 → S3

Actions: List
ListBucket

Resources: arn:aws:s3:::devops-bucket-cloud-computing-course

Request conditions: Specify request conditions (optional)

Character count: 167 of 6,144.



Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

S3 (1 action)

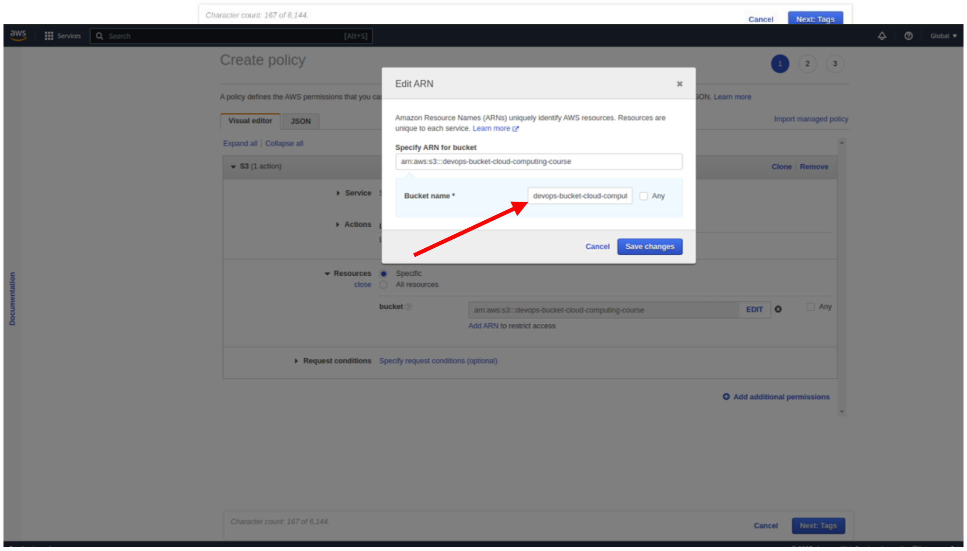
Service: Select a service below — s3

S3 · S3 Object Lambda · S3 Outposts

Actions: List — ListBucket

Resources: arn:aws:s3:::devops-bucket-cloud-computing-course

Request conditions: Specify request conditions (optional)



Character count: 167 of 6,144.

Edit ARN

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more

Specify ARN for bucket: arn:aws:s3:::devops-bucket-cloud-computing-course

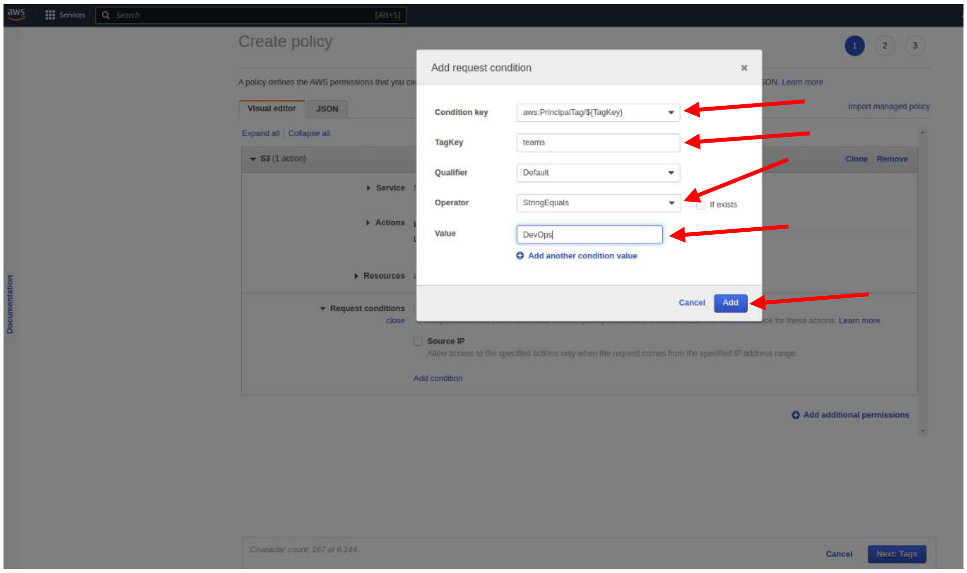
Bucket name *: devops-bucket-cloud-comput ☐ Any

Resources: ● Specific ○ All resources

bucket: arn:aws:s3:::devops-bucket-cloud-computing-course ☐ Any

Add ARN to restrict access

Request conditions: Specify request conditions (optional)



Add request condition

Condition key: aws:PrincipalTag/${TagKey}

TagKey: teams

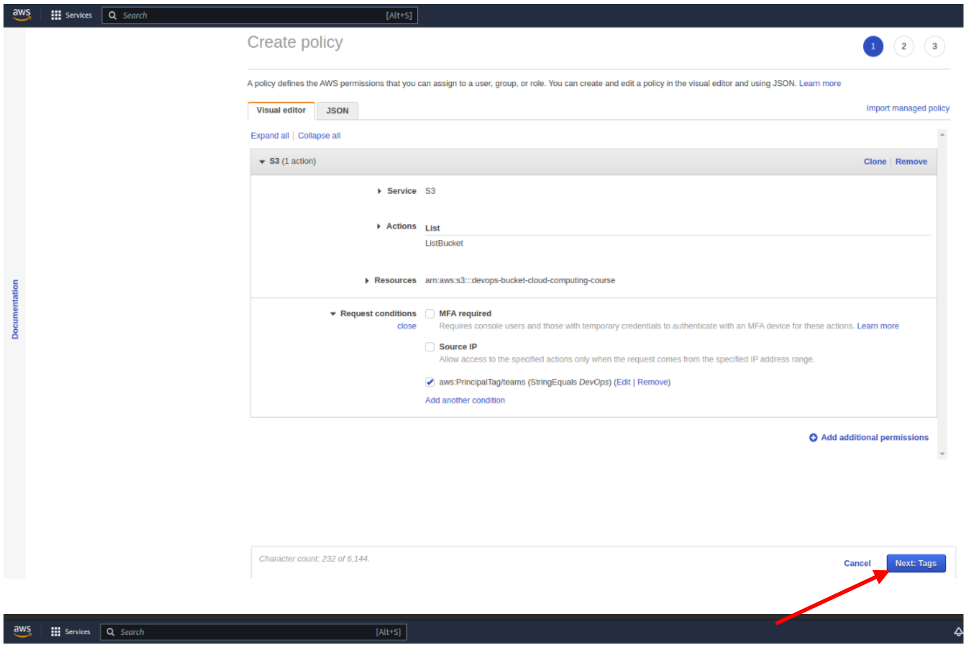
Qualifier: Default

Operator: StringEquals ☐ If exists

Value: DevOps

☐ Source IP
Allow access to the specified actions only when the request comes from the specified IP address range.

Character count: 167 of 6,144.



Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

S3 (1 action)

Service: S3

Actions: List
ListBucket

Resources: arn:aws:s3:::devops-bucket-cloud-computing-course

Request conditions (close)

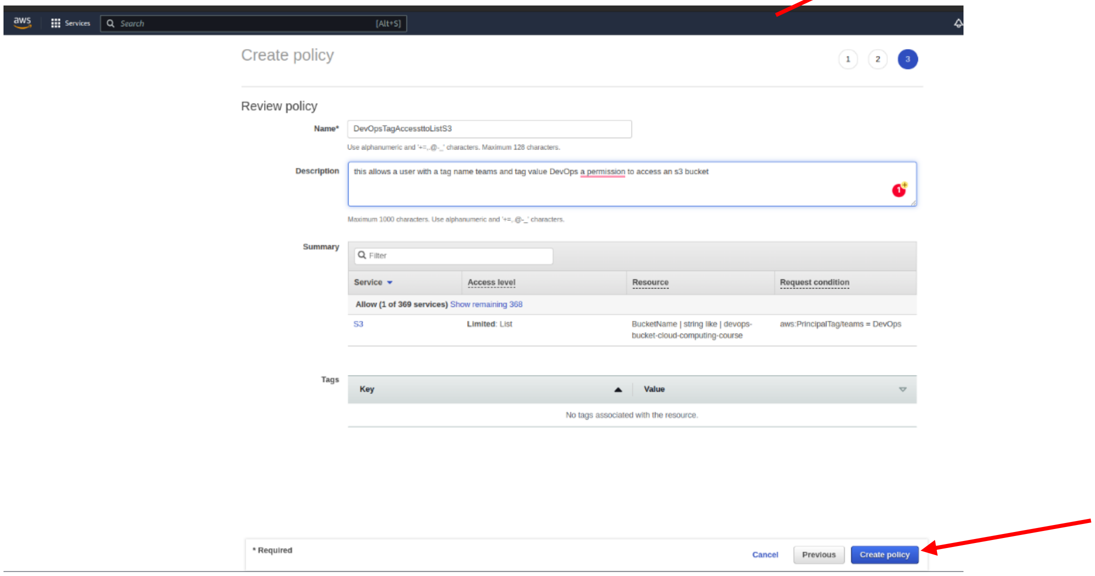
□ MFA required
Requires console users and those with temporary credentials to authenticate with an MFA device for these actions. Learn more

□ Source IP
Allow access to the specified actions only when the request comes from the specified IP address range.

☑ aws:PrincipalTag/teams (StringEquals *DevOps*) (Edit | Remove)

Add another condition

Character count: 232 of 6,144.



Create policy

Review policy

Name*: DevOpsTagAccesstoListS3
Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

Description: this allows a user with a tag name teams and tag value DevOps a permission to access an s3 bucket
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

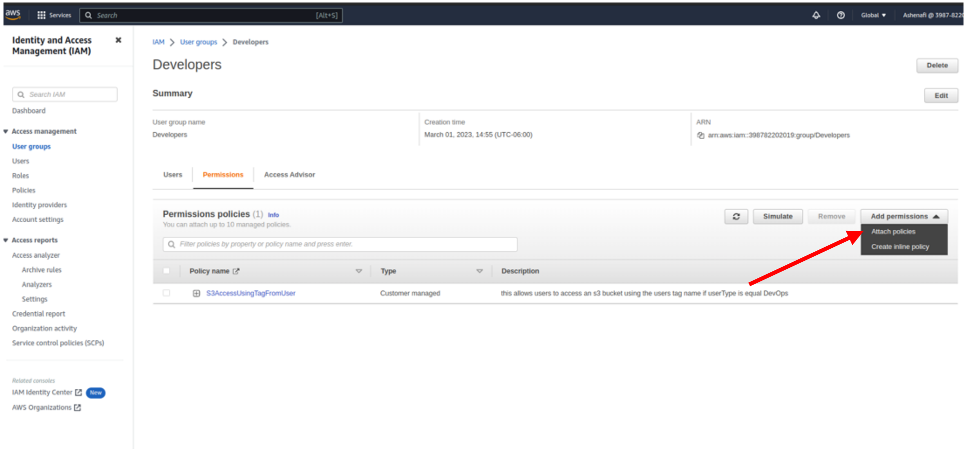
Service	Access level	Resource	Request condition
Allow (1 of 369 services) Show remaining 368			
S3	Limited: List	BucketName | string like | devops-bucket-cloud-computing-course	aws:PrincipalTag/teams = DevOps

Tags

Key	Value
No tags associated with the resource.	

* Required

Attach the create Policy to the user group “Developers”



Identity and Access Management (IAM)

IAM > User groups > Developers

Developers

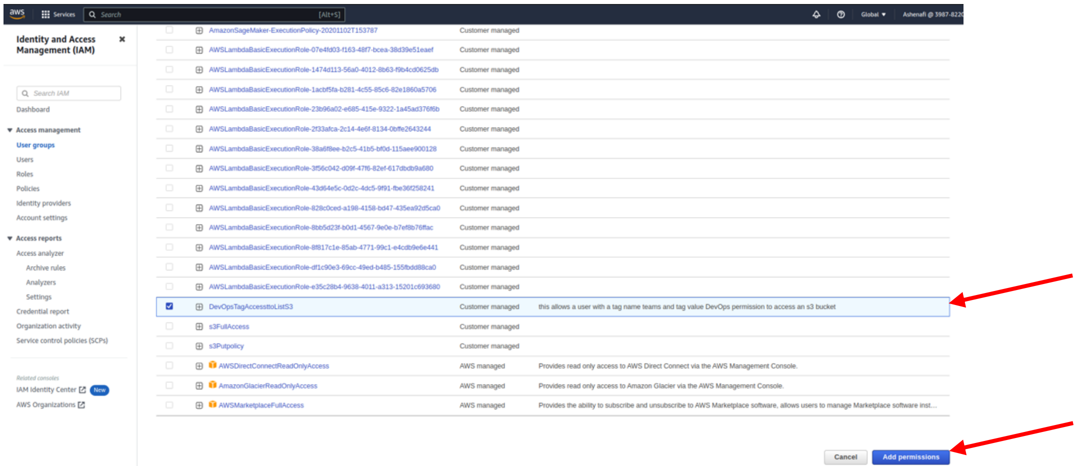
Summary

User group name	Creation time	ARN
Developers	March 01, 2023, 14:55 (UTC-06:00)	arn:aws:iam::398782202019:group/Developers

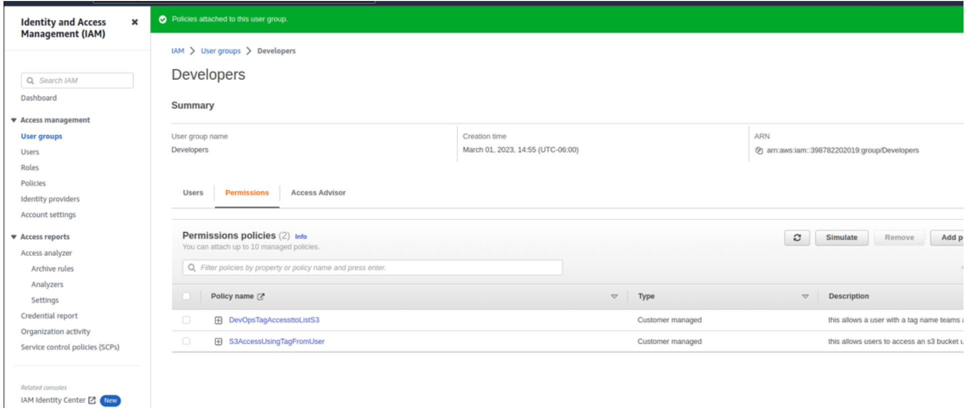
Permissions policies (1)
You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.

Policy name	Type	Description
S3AccessUsingTagFromUser	Customer managed	this allows users to access an s3 bucket using the users tag name if userType is equal DevOps



	Policy name	Type	Description
□	⊞ AmazonSageMaker-ExecutionPolicy-20201102T153787	Customer managed	
□	⊞ AWSLambdaBasicExecutionRole-07e4fd03-f163-48f7-bcea-38d39e51eaef	Customer managed	
□	⊞ AWSLambdaBasicExecutionRole-1474d113-56a0-4012-8b63-f9b4cd0625db	Customer managed	
□	⊞ AWSLambdaBasicExecutionRole-1acbf5fa-b281-4c55-85c6-82e1860a5706	Customer managed	
□	⊞ AWSLambdaBasicExecutionRole-23b96a02-e685-415e-9322-1a45ad376f6b	Customer managed	
□	⊞ AWSLambdaBasicExecutionRole-2f33afca-2c14-4e6f-8134-0bffe2643244	Customer managed	
□	⊞ AWSLambdaBasicExecutionRole-38a6f8ee-b2c5-41b5-bf0d-115aee900128	Customer managed	
□	⊞ AWSLambdaBasicExecutionRole-3f56c042-d09f-47f6-82ef-617dbdb9a680	Customer managed	
□	⊞ AWSLambdaBasicExecutionRole-43d64e5c-0d2c-4dc5-9f91-fbe36f258241	Customer managed	
□	⊞ AWSLambdaBasicExecutionRole-828c0ced-a198-4158-bd47-435ea92d5ca0	Customer managed	
□	⊞ AWSLambdaBasicExecutionRole-8bb5d23f-b0d1-4567-9e0e-b7ef8b76ffac	Customer managed	
□	⊞ AWSLambdaBasicExecutionRole-8f817c1e-85ab-4771-99c1-e4cdb9e6e441	Customer managed	
□	⊞ AWSLambdaBasicExecutionRole-df1c90e3-69cc-49ed-b485-155fbdd88ca0	Customer managed	
□	⊞ AWSLambdaBasicExecutionRole-e35c28b4-9638-4011-a313-15201c693680	Customer managed	
☑	⊞ DevOpsTagAccesstoListS3	Customer managed	this allows a user with a tag name teams and tag value DevOps permission to access an s3 bucket
□	⊞ s3FullAccess	Customer managed	
□	⊞ s3Putpolicy	Customer managed	
□	⊞ AWSDirectConnectReadOnlyAccess	AWS managed	Provides read only access to AWS Direct Connect via the AWS Management Console.
□	⊞ AmazonGlacierReadOnlyAccess	AWS managed	Provides read only access to Amazon Glacier via the AWS Management Console.
□	⊞ AWSMarketplaceFullAccess	AWS managed	Provides the ability to subscribe and unsubscribe to AWS Marketplace software, allows users to manage Marketplace software inst…



Policies attached to this user group.

IAM > User groups > Developers

Developers

Summary

User group name	Creation time	ARN
Developers	March 01, 2023, 14:55 (UTC-06:00)	arn:aws:iam::398782202019:group/Developers

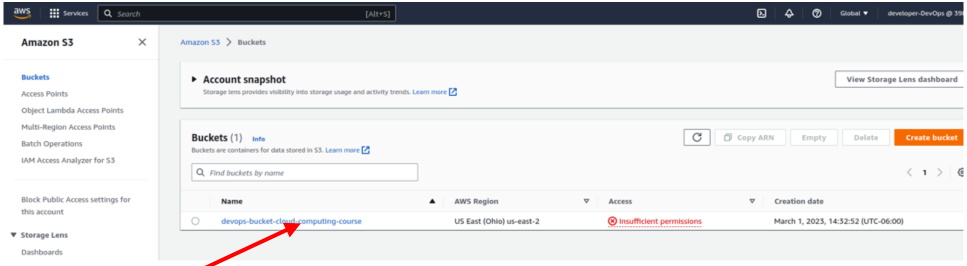
Permissions policies (2) Info

You can attach up to 10 managed policies.

□	Policy name	Type	Description
□	⊞ DevOpsTagAccesstoListS3	Customer managed	this allows a user with a tag name teams a
□	⊞ S3AccessUsingTagFromUser	Customer managed	this allows users to access an s3 bucket u

6 Test

Log in using both users created above and try to access you S3 buckets DevOpsUser with tag name “teams” and tag value “DevOps”



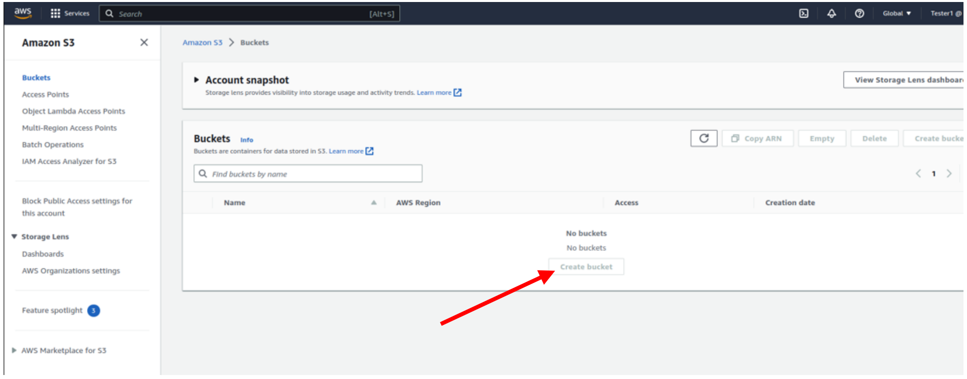
Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets (1) Info

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	devops-bucket-cloud-computing-course	US East (Ohio) us-east-2	Insufficient permissions	March 1, 2023, 14:32:52 (UTC-06:00)

Tester User with not tag name and value



Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets Info

Buckets are containers for data stored in S3. Learn more

Name	AWS Region	Access	Creation date

No buckets

No buckets