

Assignment 2 - Setup your person AWS account

ACCEPTANCE CRITERIA – Include the followings in the PDF:

- The IAM user after creation.
- CloudWatch billing alarm.
- SNS topic for the billing alarm.

Task 1 – Enable MFA

Enable MFA for the root user. Install and use Authy or similar MFA 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 to login to AWS. Refer: [Set Up an AWS Account and Create an Administrator User](#). Setting an alias for the account makes it easier to login. So you don't have to enter the account id.

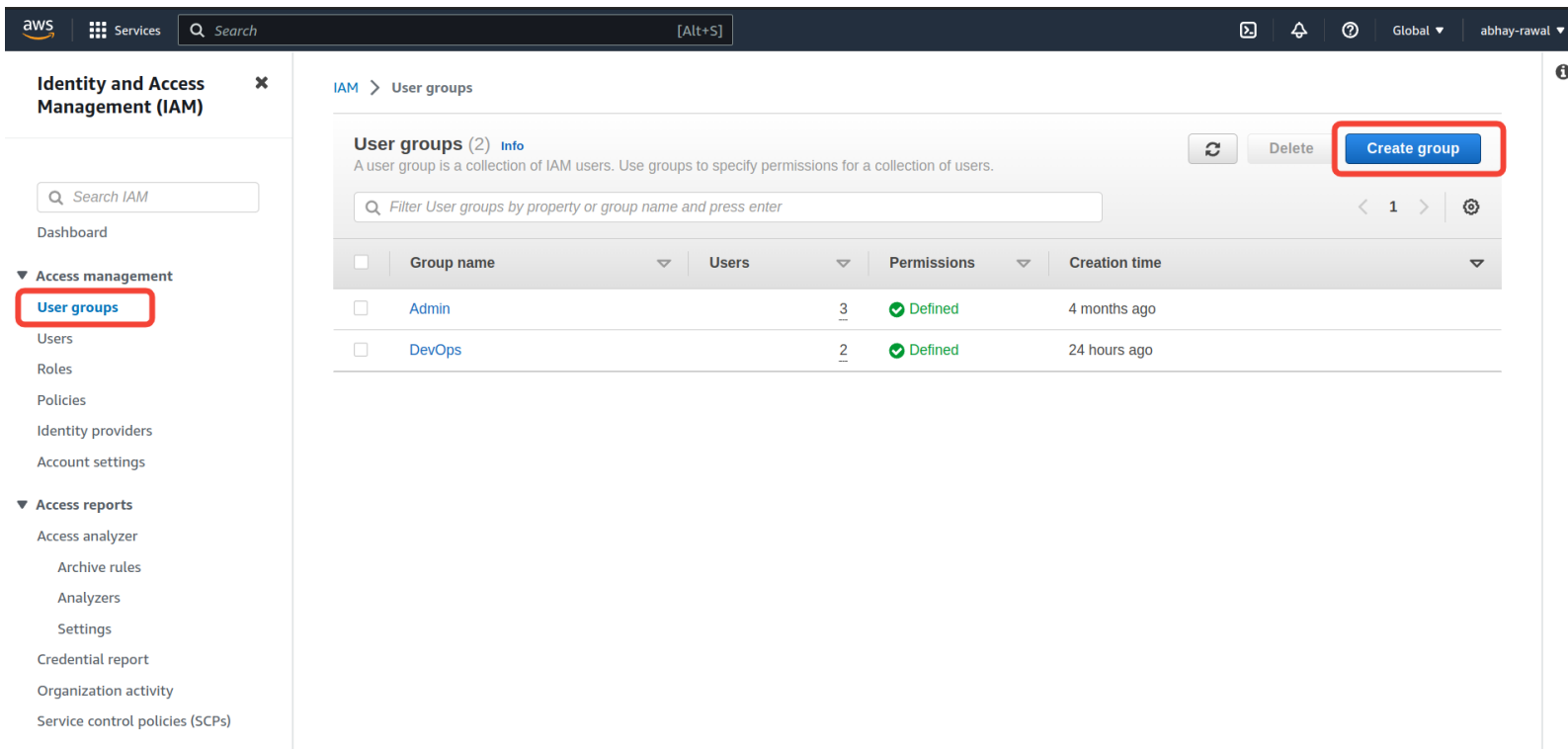
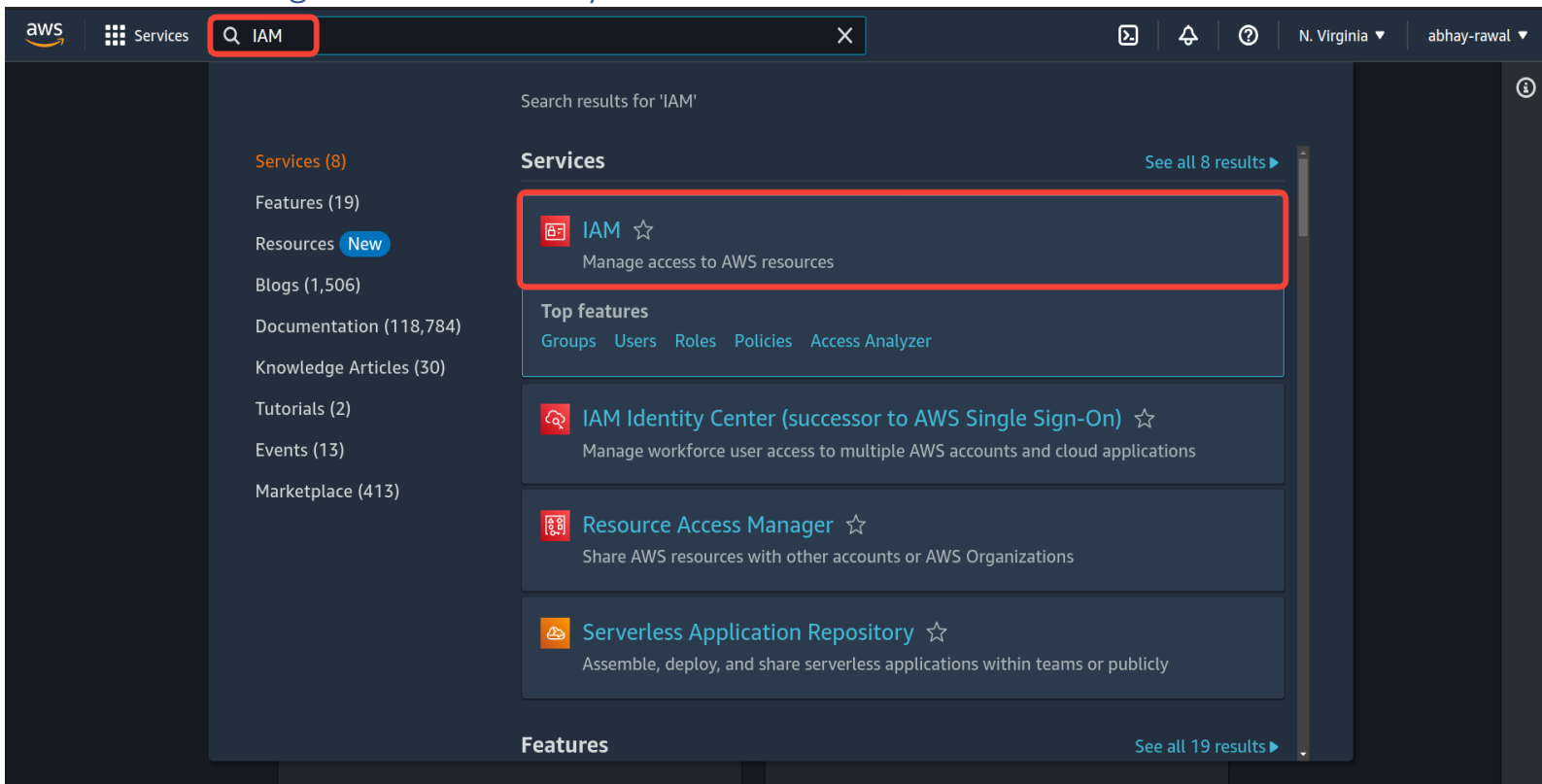
The best practice is always to use an IAM user. Never use your root user. If the IAM user credentials are compromised, you can login as a root and disable the IAM user.

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.

Creating an IAM user for yourself



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

Analizers

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

< 1 >

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	abhay-admin1	1	18 days ago	4 months ago
<input type="checkbox"/>	abhay-admin2	1	None	4 months ago
<input type="checkbox"/>	abhay-cloud	1	24 hours ago	24 hours ago
<input type="checkbox"/>	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

Analizers

Settings

Credential report

Organization activity

Service control policies (SCPs)

abhay-devops

abhay-devops1

abhay-iam-assume

TestAdmin

Attach permissions policies - Optional (Selected 1/816) 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.

AdministratorAccess

4 matches

< 1 >

"AdministratorAccess"

Clear filters

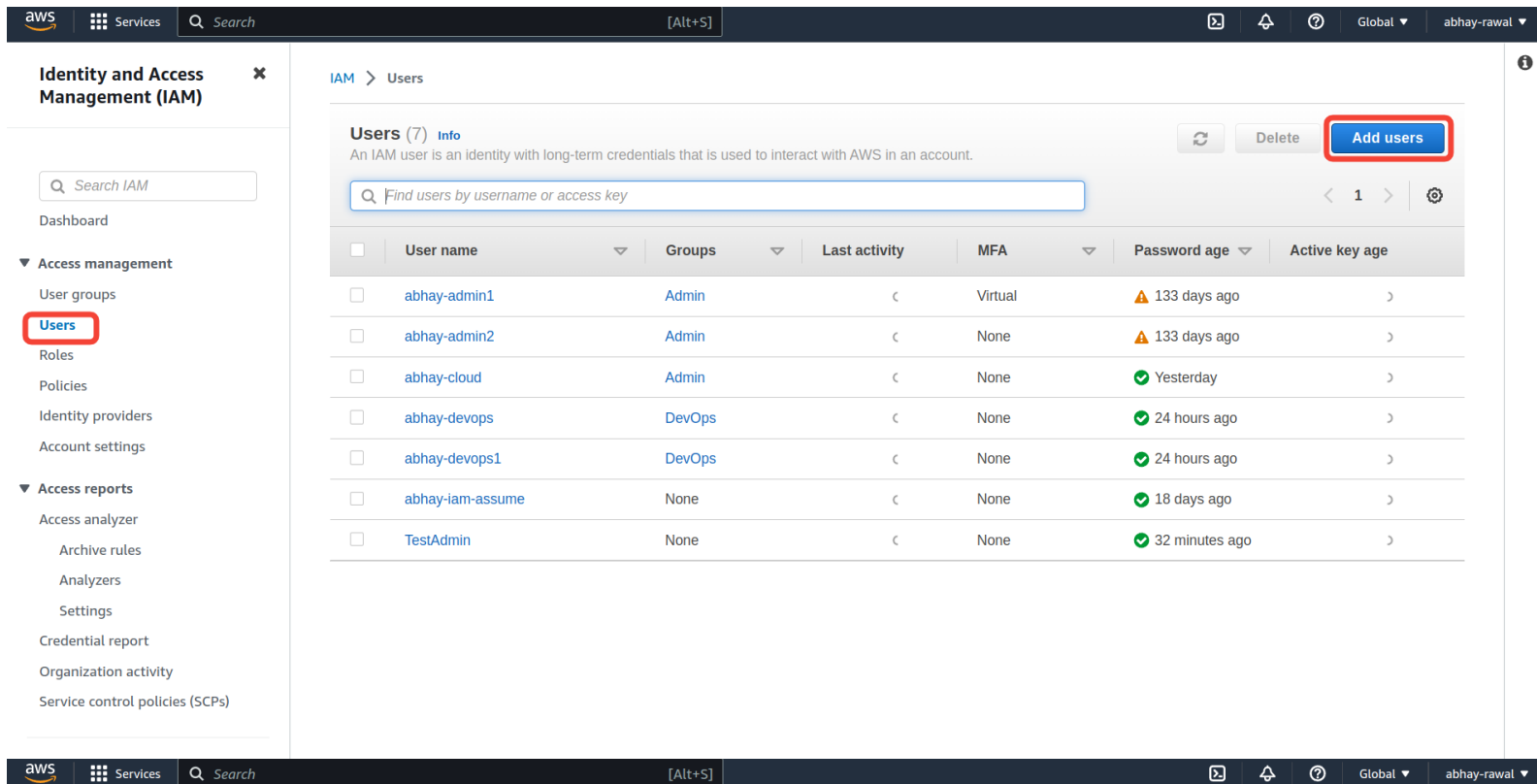
<input type="checkbox"/>	Policy name	Type	Description
<input checked="" type="checkbox"/>	AdministratorAccess	AWS managed - job function	Provides full access to A
<input type="checkbox"/>	AdministratorAccess-Amplify	AWS managed	Grants account administr
<input type="checkbox"/>	AdministratorAccess-AWSElasticBeanstalk	AWS managed	Grants account administr
<input type="checkbox"/>	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**.



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 > Users

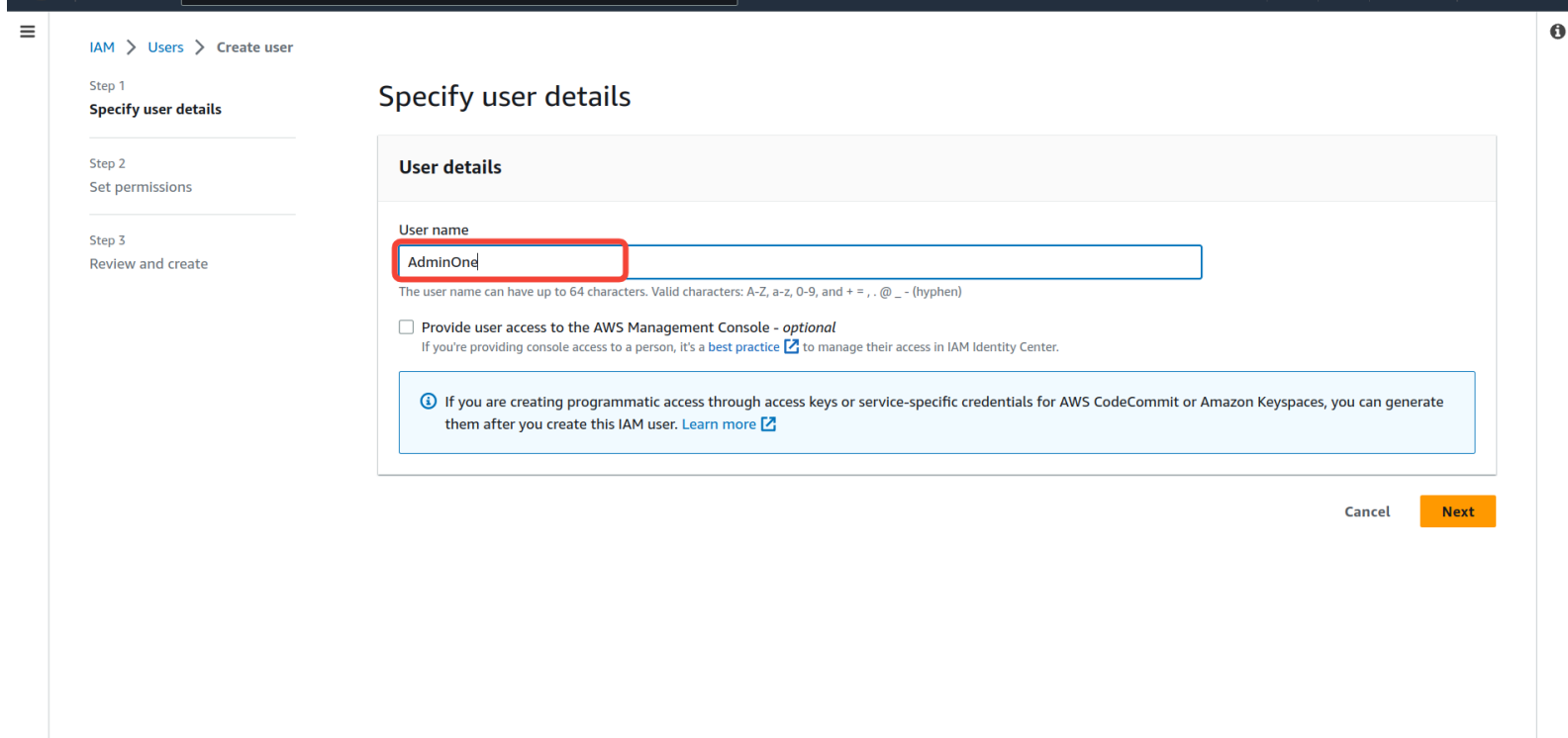
Users (7) Info

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

Find users by username or access key

	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	abhay-admin1	Admin	◀	Virtual	⚠ 133 days ago	➤
<input type="checkbox"/>	abhay-admin2	Admin	◀	None	⚠ 133 days ago	➤
<input type="checkbox"/>	abhay-cloud	Admin	◀	None	✅ Yesterday	➤
<input type="checkbox"/>	abhay-devops	DevOps	◀	None	✅ 24 hours ago	➤
<input type="checkbox"/>	abhay-devops1	DevOps	◀	None	✅ 24 hours ago	➤
<input type="checkbox"/>	abhay-iam-assume	None	◀	None	✅ 18 days ago	➤
<input type="checkbox"/>	TestAdmin	None	◀	None	✅ 32 minutes ago	➤

Buttons: Refresh, Delete, **Add users**



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

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](#)

Cancel **Next**

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

The screenshot shows the AWS IAM console 'Create user' page. The 'User name' field is 'AdminOne'. Under 'Are you providing console access to a person?', the 'I want to create an IAM user' option is selected. Under 'Console password', the 'Custom password' option is selected. A red arrow points to the 'Users must create a new password at next sign-in (recommended)' checkbox, which is unchecked. The 'Next' button is highlighted in orange.

aws

Services

Search

[Alt+S]

Global

abhay-rawal

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)

☐

Admin

3

AdministratorAccess

2022-10-19 (4 months ago)

☒ Administrator0AdministratorAccess2023-03-01 (2 minutes ago)

☐ DevOps2None2023-02-28 (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](#)

Cancel

Previous

Next

aws

Services

Search

[Alt+S]

Global

abhay-rawal

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

< 1 >

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.

Add new tag

You can add up to 50 more tags.

Cancel

Previous

Create user

 **User created successfully**

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

View user 


[IAM](#) > [Users](#) > Create user


- Step 1
Specify user details
- Step 2
Set permissions
- Step 3
Review and create
- Step 4
Retrieve password


Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details [Email sign-in instructions](#)

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

User name
 AdminOne

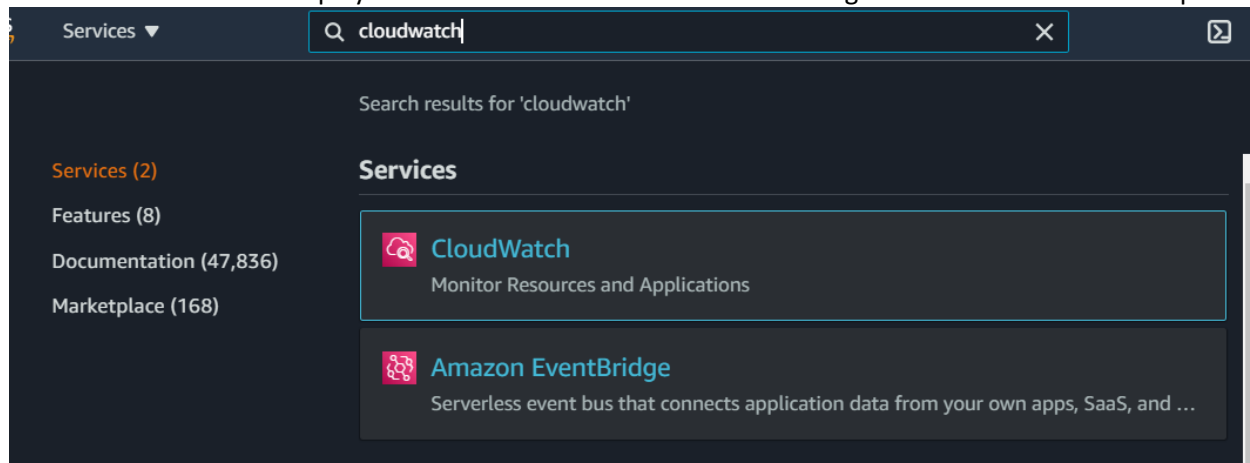
Console password
 ***** [Show](#)

Download .csv file

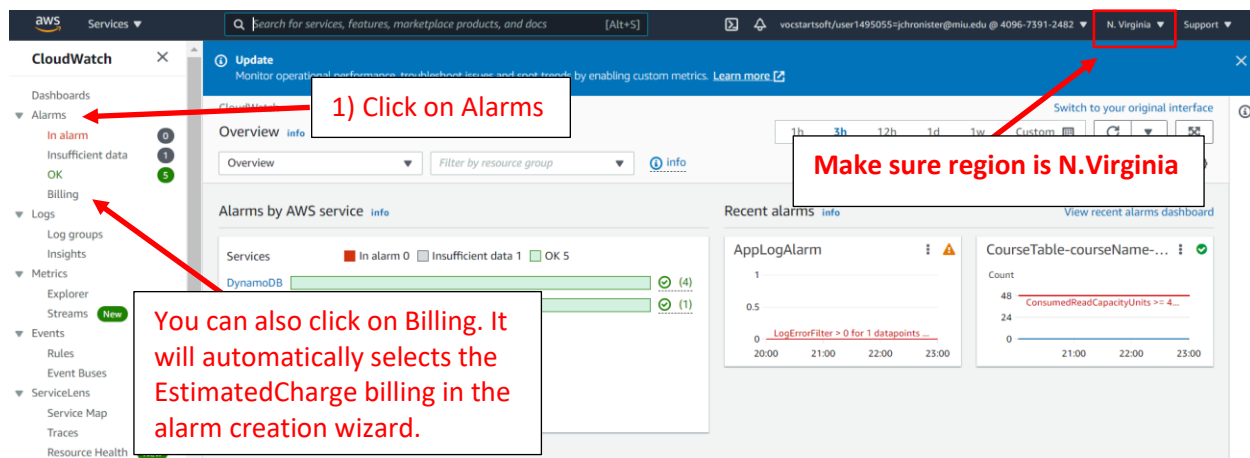
Return to users list

Setting up a billing alarm on CloudWatch

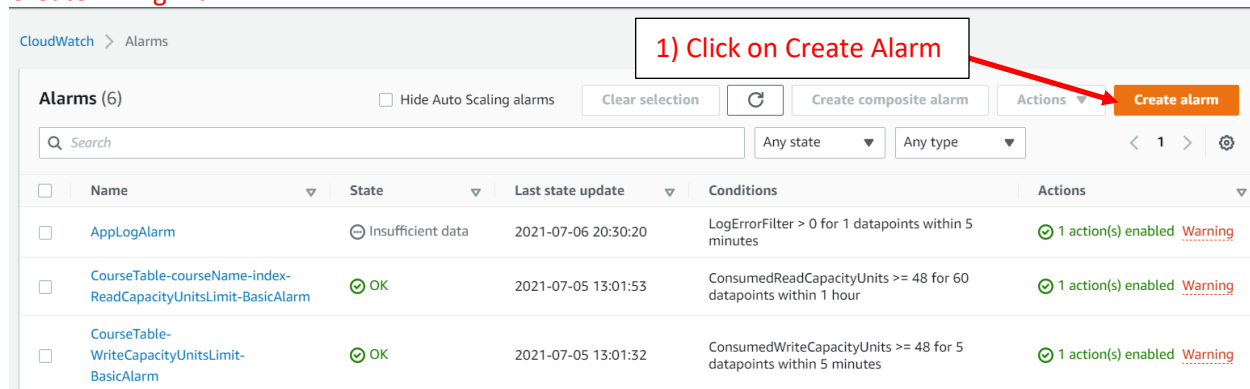
Go to the CloudWatch Display. Search or Find under All Services Management & Governance Group



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



Create Billing Alarm



Step 1

Specify metric and conditions

Step 2

Configure actions

Step 3

Add name and description

Step 4

Preview and create

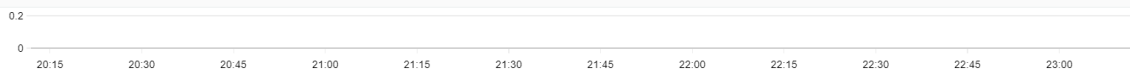
Specify metric and conditions

Metric**Graph**

Preview of the metric or metric expression and the alarm threshold.

Select metric**2) Click Select Metric**

Cancel

Next**Select metric**

▼ AWS Namespaces

ApiGateway

11

ApplicationELB

177

Billing

14

DynamoDB

23

EBS

189

EC2

392

Events

5

Lambda

26

Cancel

Select a single metric to continue

Select metric**Metrics (14)**All > Billing

Graph search

View graphed metrics

By Service

13

Total Estimated Charge

1

4) Click Total Estimated Charge

Cancel

Select a single metric to continue

Metrics (1)

Graph searchView graphed metrics (1)

All > Billing > Total Estimated Charge

Search for any metric, dimension or resource id

Currency (1)

Metric Name

USD

EstimatedCharges

5) Select USD Currency

6) Click Select Metric

CancelSelect metric

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

Edit

Graph

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

No unit

1

0.8

0.6

0.4

0.2

0

07/0107/0307/0507/07

EstimatedCharges

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

7) Pick Some Conditions

8) Click Next

► Additional configuration

Cancel

Next

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

user1@example.com, user2@example.com

11) Enter Email

Create topic

Add notification

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](#) 🔗

Add notification

Auto Scaling action

Add Auto Scaling action

EC2 action

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

Add EC2 action

Systems Manager action [Info](#) 🔗

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

Add Systems Manager action

13) Click Next

Cancel

Previous

Next

Add name and description

Name and description

Alarm name

MyBillingAlarm

Alarm description - optional

Alarm description

Up to 1024 characters (0/1024)

14) Name Alarm

15) Click Next

Cancel

Previous

Next

...

Step 3: Add name and description

Name and description

Name

MyBillingAlarm

Description

-

16) Preview Alarm and Click Create Alarm

Cancel

Previous

Create alarm

Edit