

**Tony Shen**

# **HOW TO SET UP AWS CLOUDWATCH BILLING ALARMS**

---

# How to Set up AWS CloudWatch Billing Alarms

---

## Contents

Introduction .....	3
Billing Alarm (BA) Setup Procedure .....	3
Step 1 – Creating Admin user and group .....	3
Step 2 - Activating IAM user/role access to billing information .....	5
Step 3 – Creating billing access policies .....	8
Step 4 – Creating SNS topic .....	14
Step 5 – Creating Subscription .....	16
Step 6 – Creating CloudWatch Alarm .....	18
Summary .....	22
References .....	23

## How to Set up AWS CloudWatch Billing Alarms

---

### Glossary

Term	Description
AWS	Amazon Web Services
BA	Billing Alarm/Alert

## Introduction

By default only the root user can access AWS billing information. A common practice is using CloudWatch alarm feature to send alerts by email or by mobile simple text messages to designated alert recipients when billing exceeds certain thresholds. A recipient doesn't have to be an AWS IAM user.

CloudWatch works in conjunction with IAM service and SNS (Simple Notification Service) so as to deliver billing alarms to recipients in such as fashion.

## Billing Alarm (BA) Setup Procedure

BA setup procedure includes the following steps

1. Root user creates IAM user and group with Administrator permission policy, if such a user and group do not already exist. The user created is a non-root, Admin user.
2. Root user activates IAM user/role access to billing information
3. Admin user creates Billing Access policies
4. Admin user creates BA SNS topic, if it does not already exists
5. Admin user creates BA SNS topic subscription for a designated subscriber to receive alerts by email
6. The subscriber confirms the SNS topic subscription email
7. Admin user creates an alarm in CloudWatch and associates the alarm as the publisher with th SNS topic

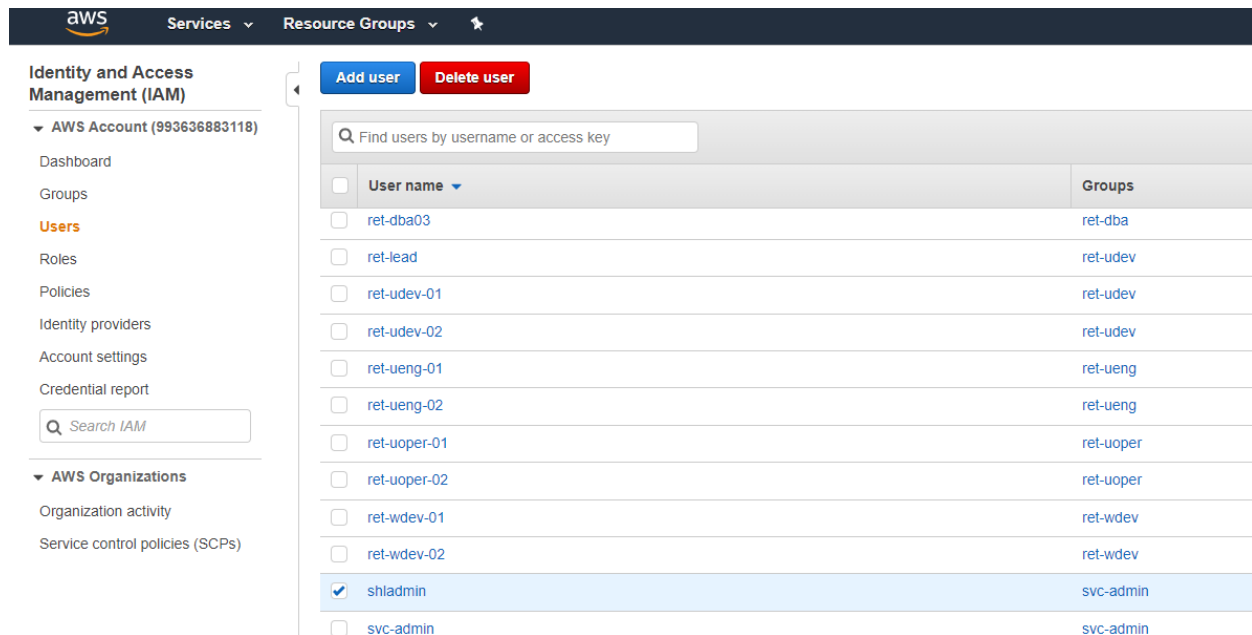
Here below is an example of going by this setup procedure with screen shots attached for illustration purposes.

## Step 1 – Creating Admin user and group

Create an Admin user account if it does not already exist. In this example, Admin account already exists. Admin user name is "shladmin"

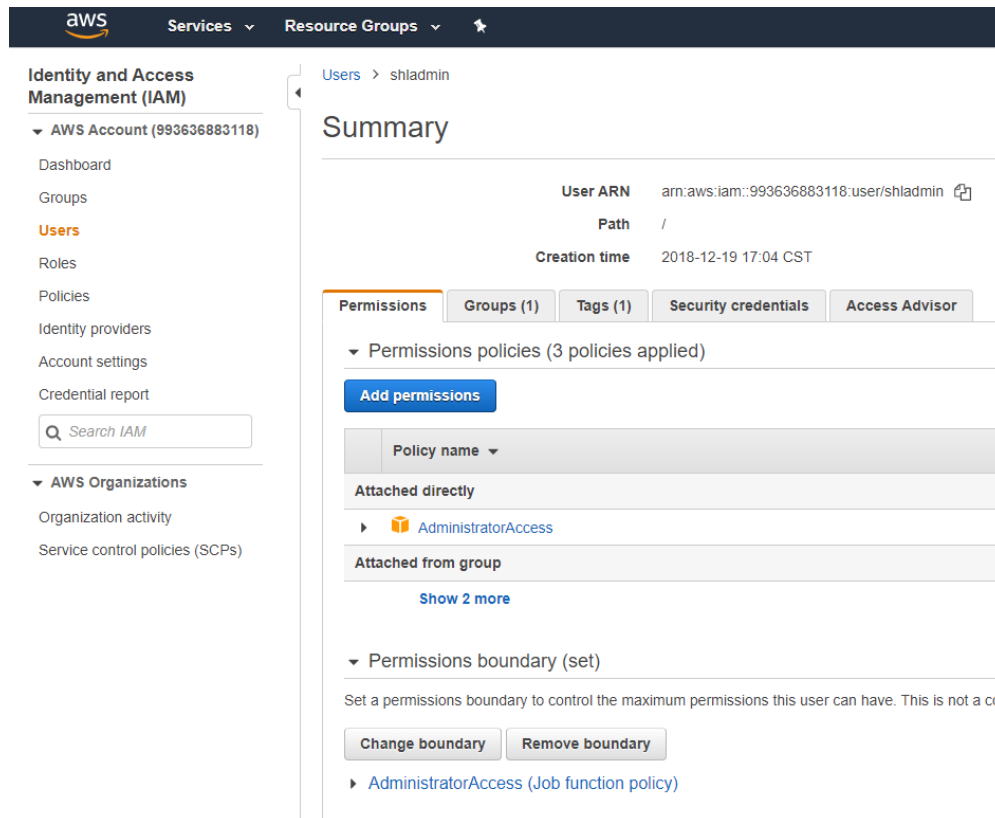
# How to Set up AWS CloudWatch Billing Alarms

Figure 1 – Admin user shladmin



Select and open the user. Make sure the user has “AdministratorAccess” policy attached.

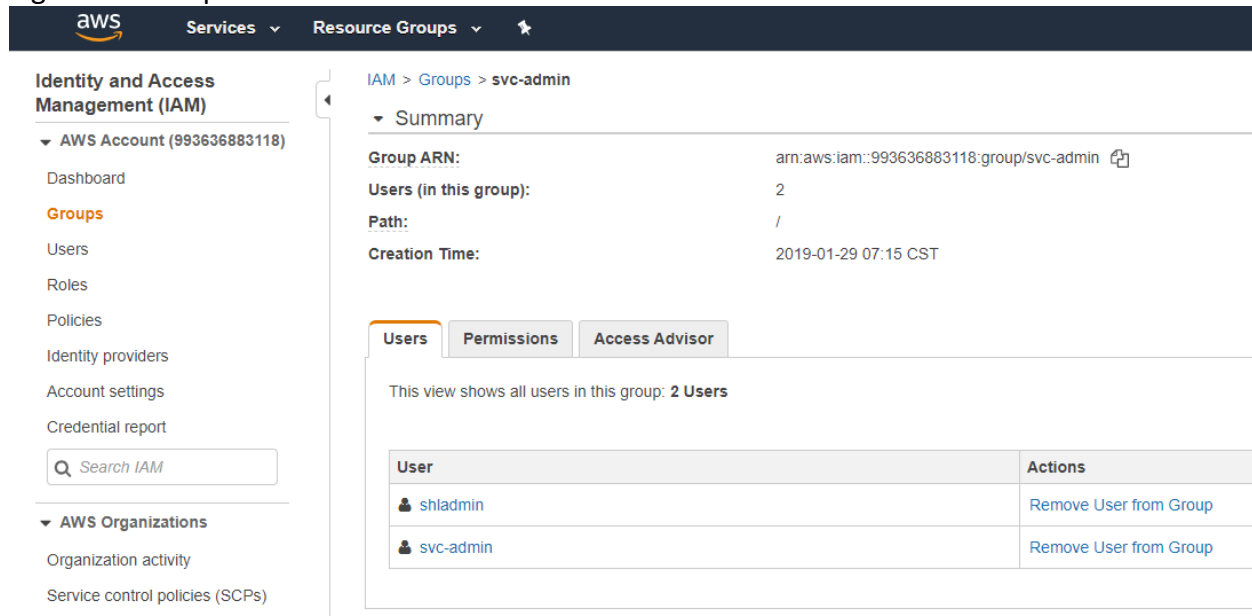
Figure 2 – AdministratorAccess policy attached to Admin user



# How to Set up AWS CloudWatch Billing Alarms

Create an Admin group if it does not already exist. In this example, the group already exists. Group name is “svc-admin”. The group has two users. “shladmin” is one of the users.

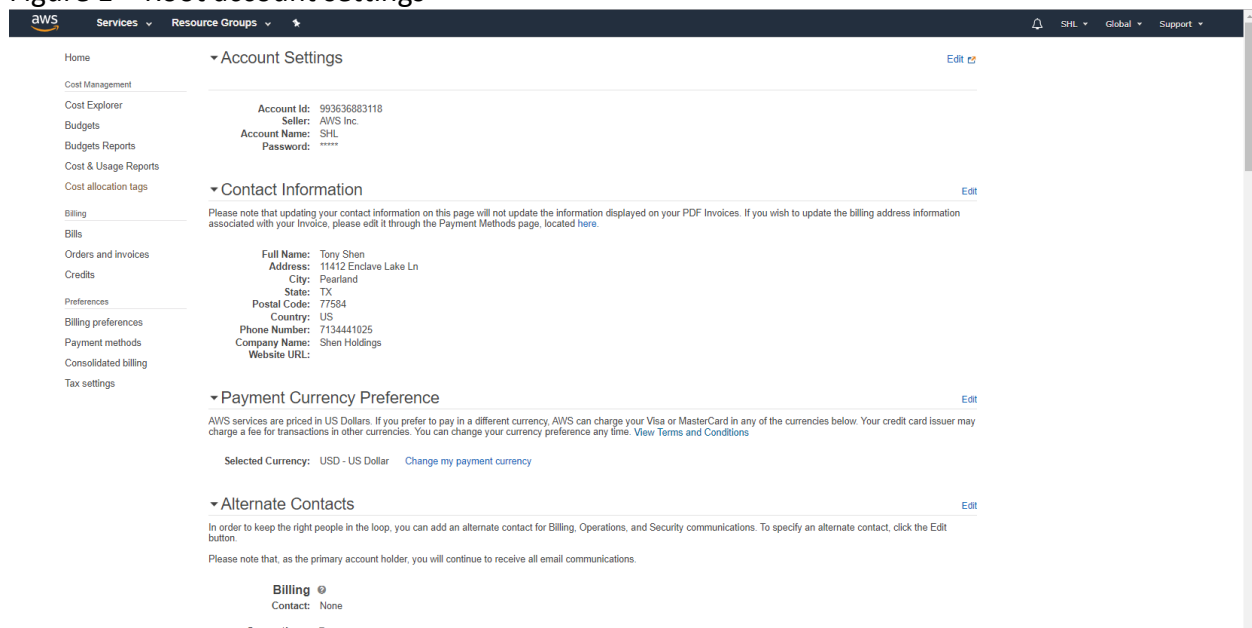
Figure 3 - Group svc-admin



## Step 2 - Activating IAM user/role access to billing information

Login in as root user. Click on My account at the right corner on Navigation Bar to display Account Settings

Figure 1 – Root account settings



# How to Set up AWS CloudWatch Billing Alarms

Scroll down to find “IAM User and Role Access to Billing Information”

Figure 2 –IAM User and Role Access to Billing Information

US West (N. California)	Enabled by default
Asia Pacific (Singapore)	Enabled by default
Asia Pacific (Sydney)	Enabled by default
Canada (Central)	Enabled by default

▼ IAM User and Role Access to Billing Information

Edit

You can give IAM users and federated users with roles permissions to access billing information. This includes access to Account Settings, Payment Methods, and Report pages. You control which users and roles can see billing information by creating IAM policies. For more information, see [Controlling Access to Your Billing Information](#).

**IAM user/role access to billing information is deactivated.**

▼ Reserved Instance Marketplace Settings

The Reserved Instance Marketplace gives you the flexibility to sell the remaining full months on your Reserved Instances. Manage your Reserved Instance Marketplace disbursement and tax information using options below.

[Manage Seller and Bank Account Information](#)

You can update your business name and bank account information so we can disburse funds to the appropriate location.

[Manage Tax Settings](#)

Change your tax information so that your 1099K or W-88EN is generated appropriately. Setting this information up also allows you to sell more than 200 transactions or \$20,000 in Reserved Instances.

▼ Account Contract Information

Edit

If this account is being used to service public sector customer, please provide the contract details in the fields below.

☐ Is this account being used to service a public sector customer? ⓘ

End User Organization Name: ⓘ

None

Contract Name: ⓘ

None

Contract Number: ⓘ

None

Task or Purchase Order Number: ⓘ

None

▼ Communication Preferences

Click on “Edit” on the right. “Activate IAM Access” shows up

# How to Set up AWS CloudWatch Billing Alarms

Figure 3 – Activate IAM Access

US West (N. California)	Enabled by default
Asia Pacific (Singapore)	Enabled by default
Asia Pacific (Sydney)	Enabled by default
Canada (Central)	Enabled by default

▼ IAM User and Role Access to Billing Information

You can give IAM users and federated users with roles permissions to access billing information. This includes access to Account Settings, Payment Methods, and Report pages. You control which users and roles can see billing information by creating IAM policies. For more information, see [Controlling Access to Your Billing Information](#).

☐ Activate IAM Access

Update

Cancel

▼ Reserved Instance Marketplace Settings

The Reserved Instance Marketplace gives you the flexibility to sell the remaining full months on your Reserved Instances. Manage your Reserved Instance Marketplace disbursement and tax information using options below.

[Manage Seller and Bank Account Information](#)

You can update your business name and bank account information so we can disburse funds to the appropriate location.

[Manage Tax Settings](#)

Change your tax information so that your 1099K or W-88EN is generated appropriately. Setting this information up also allows you to sell more than 200 transactions or \$20,000 in Reserved Instances.

▼ Account Contract Information

Edit

If this account is being used to service public sector customer, please provide the contract details in the fields below.

☐ Is this account being used to service a public sector customer? ⓘ

End User Organization Name: ⓘ

None

Contract Name: ⓘ

None

Contract Number: ⓘ

None

Task or Purchase Order Number: ⓘ

None

Click “Activate”. The message “IAM user/role access to billing information is activated” displays in response.

Figure 4 – IAM user/role access to billing information is activated

US West (N. California)	Enabled by default
Asia Pacific (Singapore)	Enabled by default
Asia Pacific (Sydney)	Enabled by default
Canada (Central)	Enabled by default

▼ IAM User and Role Access to Billing Information

Edit

You can give IAM users and federated users with roles permissions to access billing information. This includes access to Account Settings, Payment Methods, and Report pages. You control which users and roles can see billing information by creating IAM policies. For more information, see [Controlling Access to Your Billing Information](#).

**IAM user/role access to billing information is activated.**

▼ Reserved Instance Marketplace Settings

The Reserved Instance Marketplace gives you the flexibility to sell the remaining full months on your Reserved Instances. Manage your Reserved Instance Marketplace disbursement and tax information using options below.

[Manage Seller and Bank Account Information](#)

You can update your business name and bank account information so we can disburse funds to the appropriate location.

[Manage Tax Settings](#)

Change your tax information so that your 1099K or W-88EN is generated appropriately. Setting this information up also allows you to sell more than 200 transactions or \$20,000 in Reserved Instances.

▼ Account Contract Information

Edit

If this account is being used to service public sector customer, please provide the contract details in the fields below.

☐ Is this account being used to service a public sector customer? ⓘ

End User Organization Name: ⓘ

None

Contract Name: ⓘ

None

Contract Number: ⓘ

None

Task or Purchase Order Number: ⓘ

None

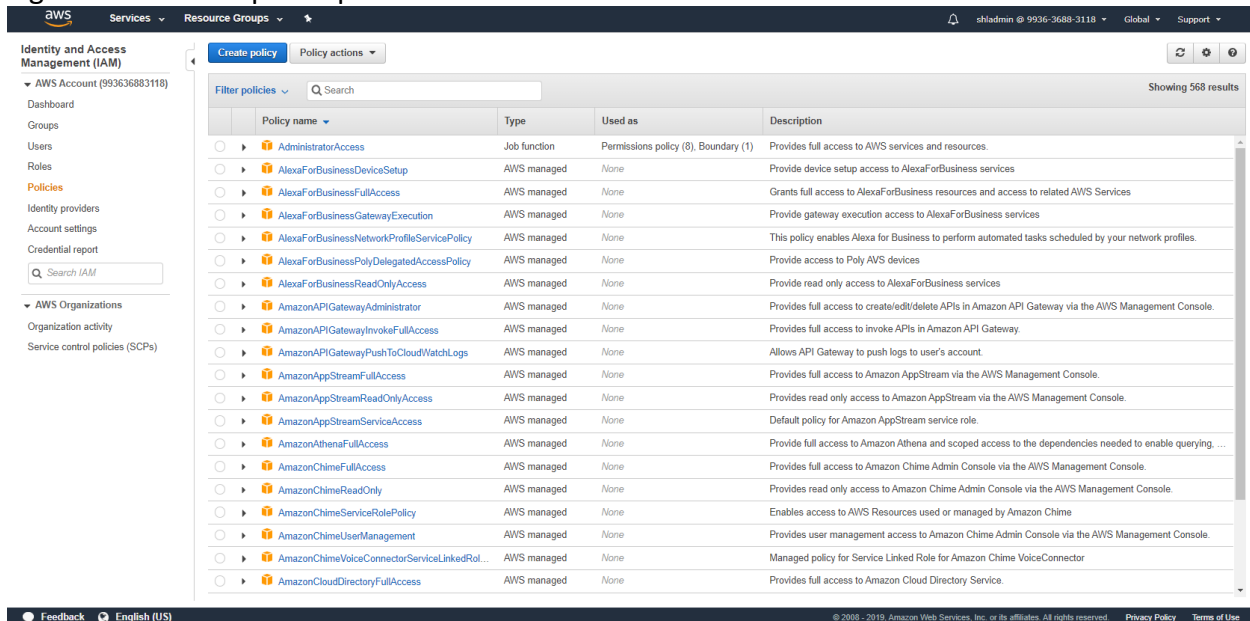


# How to Set up AWS CloudWatch Billing Alarms

## Step 3 – Creating billing access policies

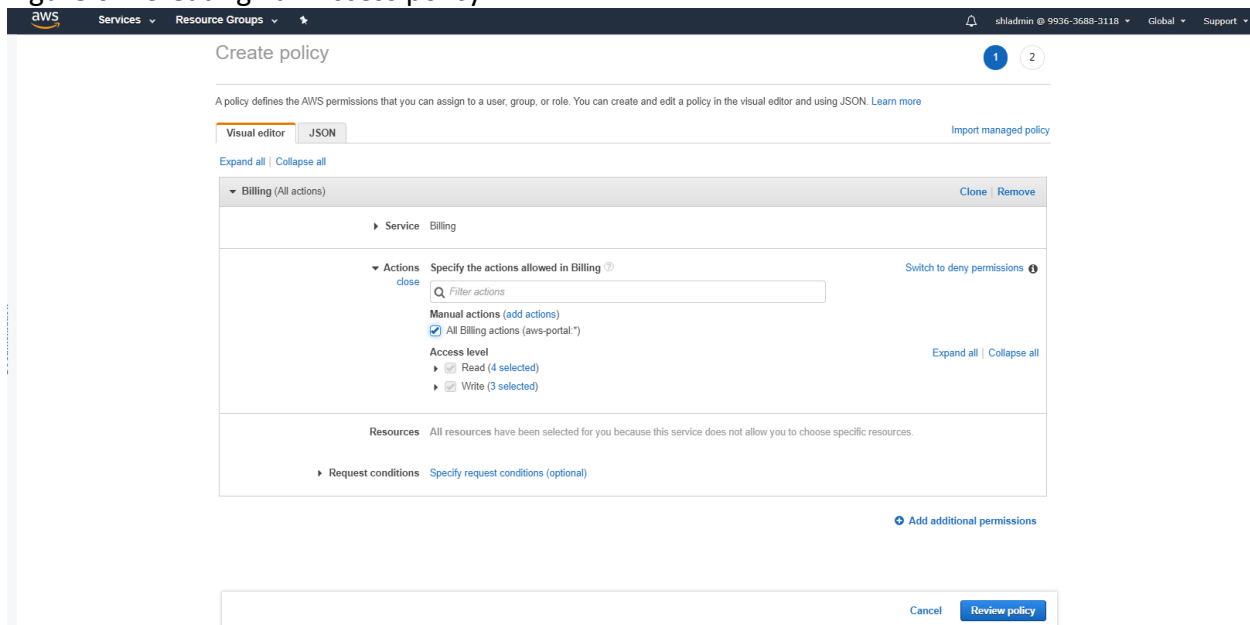
Sign out as the root user. Sign back in as Admin user

Figure 5 – Admin opens up IAM console and selects Policies



In Filter policies search box, type “Billing” to bring up Billing Policy. Open Billing Policy. Create Full Access Policy

Figure 6 – Creating Full Access policy



# How to Set up AWS CloudWatch Billing Alarms

Name the full access policy in accordance with your established naming convention.

Figure 7 – Naming the full access policy

Create policy

Review policy

Name\*

Description

Summary

Service	Access level	Resource	Request condition
Billing	Full access	All resources	None

\* Required

Cancel Previous Create policy

Click Create Policy. Policy created

Figure 8 – The full access policy created

Identity and Access Management (IAM)

o1-a01-allr-giampol-all-999-BillingFullAccess has been created.

Create policy Policy actions

Filter policies Search

Policy name	Type	Used as	Description
AdministratorAccess	Job function	Permissions policy (8), Boundary (1)	Provides full access to AWS services and resources.
AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaForBusiness services
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness resources and access to related AWS Services
AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to AlexaForBusiness services
AlexaForBusinessNetworkProfileServicePolicy	AWS managed	None	This policy enables Alexa for Business to perform automated tasks scheduled by your network profiles.
AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None	Provide access to Poly AVS devices
AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForBusiness services
AmazonAPIGatewayAdministrator	AWS managed	None	Provides full access to create/edit/delete APIs in Amazon API Gateway via the AWS Management Console.
AmazonAPIGatewayInvokeFullAccess	AWS managed	None	Provides full access to invoke APIs in Amazon API Gateway.
AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	None	Allows API Gateway to push logs to user's account.
AmazonAppStreamFullAccess	AWS managed	None	Provides full access to Amazon AppStream via the AWS Management Console.
AmazonAppStreamReadOnlyAccess	AWS managed	None	Provides read only access to Amazon AppStream via the AWS Management Console.
AmazonAppStreamServiceAccess	AWS managed	None	Default policy for Amazon AppStream service role.
AmazonAthenaFullAccess	AWS managed	None	Provide full access to Amazon Athena and scoped access to the dependencies needed to enable queryin...
AmazonChimeFullAccess	AWS managed	None	Provides full access to Amazon Chime Admin Console via the AWS Management Console.
AmazonChimeReadOnly	AWS managed	None	Provides read only access to Amazon Chime Admin Console via the AWS Management Console.
AmazonChimeServiceRolePolicy	AWS managed	None	Enables access to AWS Resources used or managed by Amazon Chime
AmazonChimeUserManagement	AWS managed	None	Provides user management access to Amazon Chime Admin Console via the AWS Management Console.

Create Read-only policy. Check “Read” under Access level

Figure 9 – Creating Read-only policy

# How to Set up AWS CloudWatch Billing Alarms

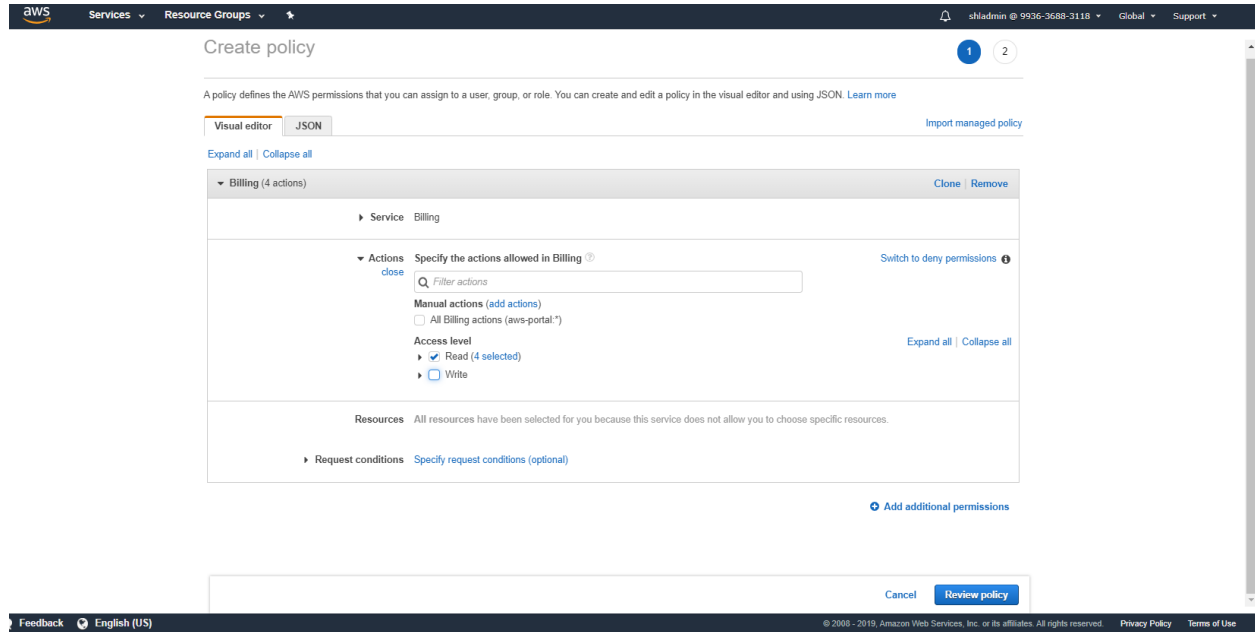
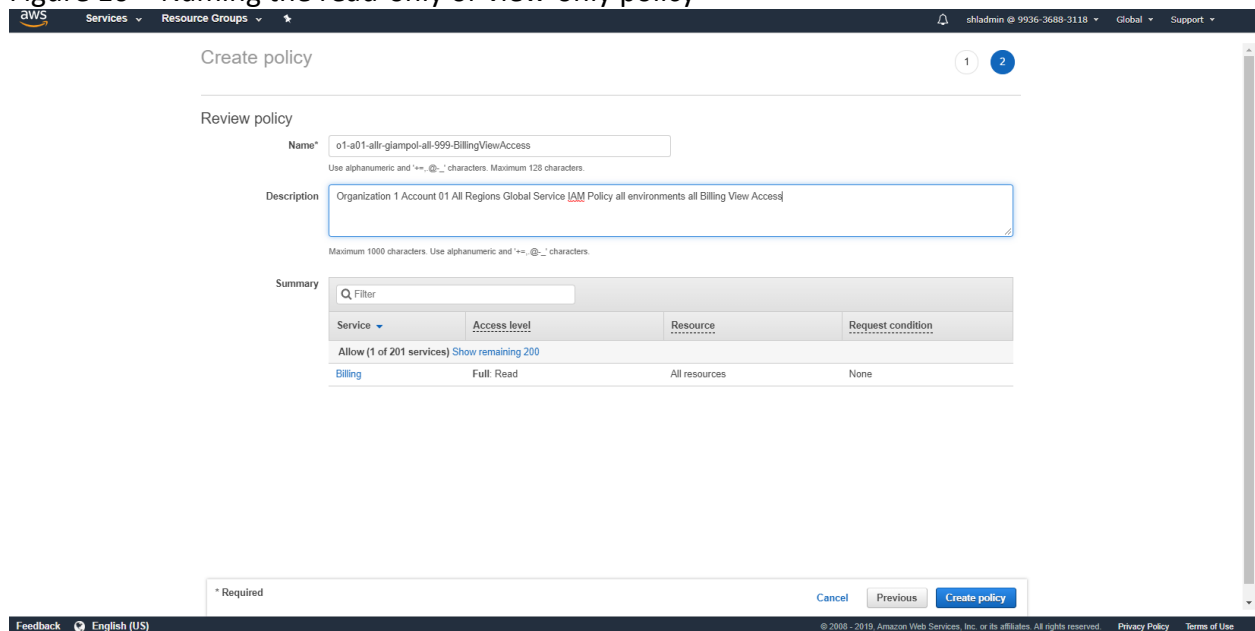


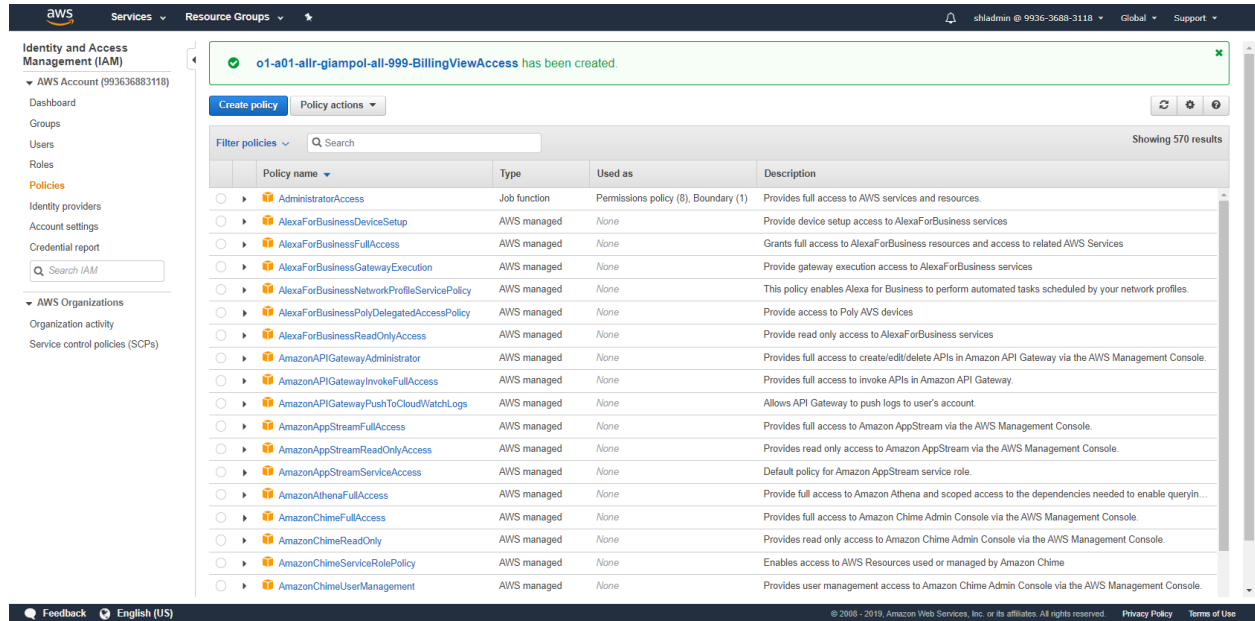
Figure 10 – Naming the read-only or view-only policy



Click Create policy

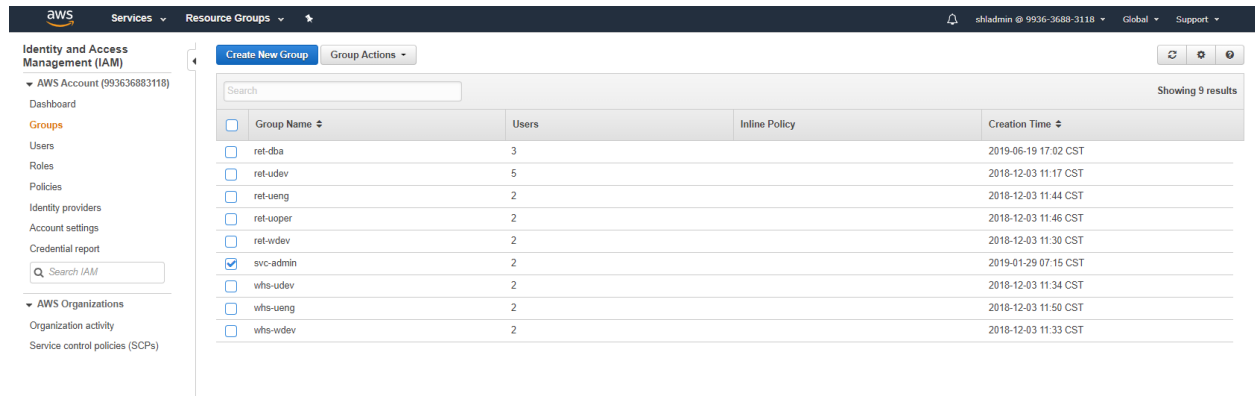
Figure 11 – The view-only policy created

# How to Set up AWS CloudWatch Billing Alarms



Select Admin group svc-admins

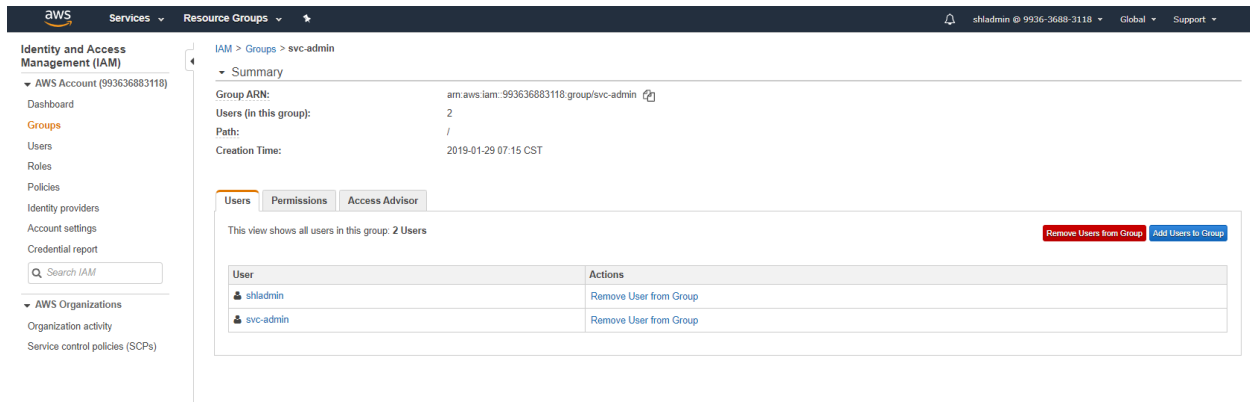
Figure 12 – Admin Group svc-admins selected



Open up Admin group svc-admins.

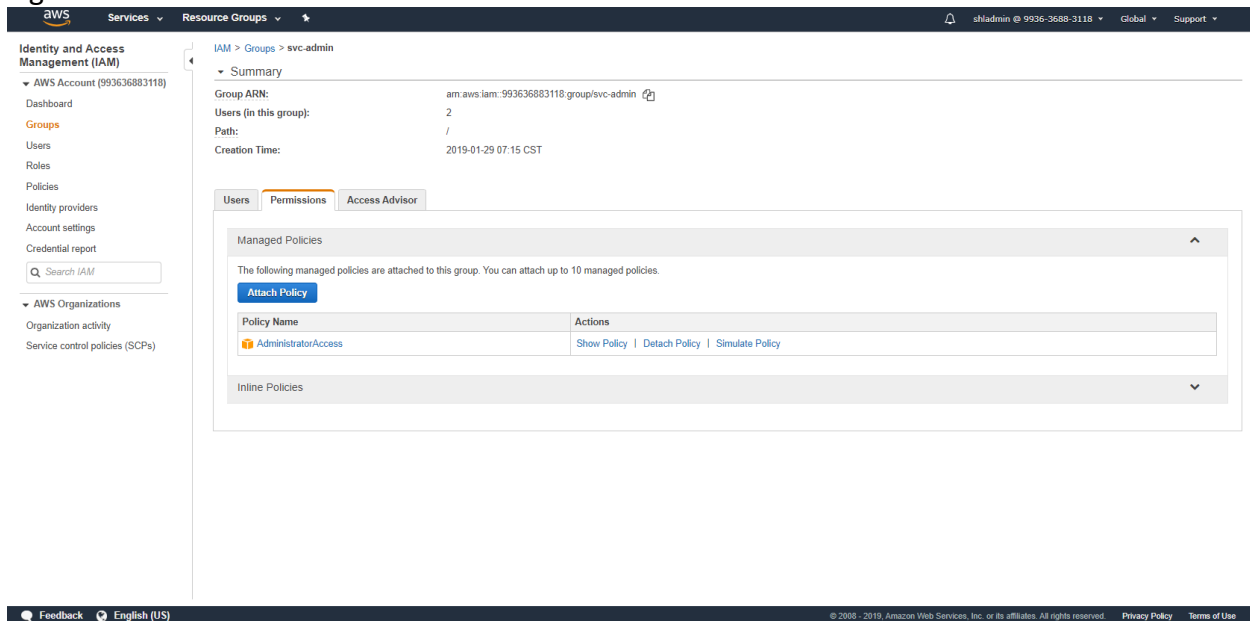
# How to Set up AWS CloudWatch Billing Alarms

Figure 13 – Admin group svc-admins with Users tab showing two users



Select Permissions tab

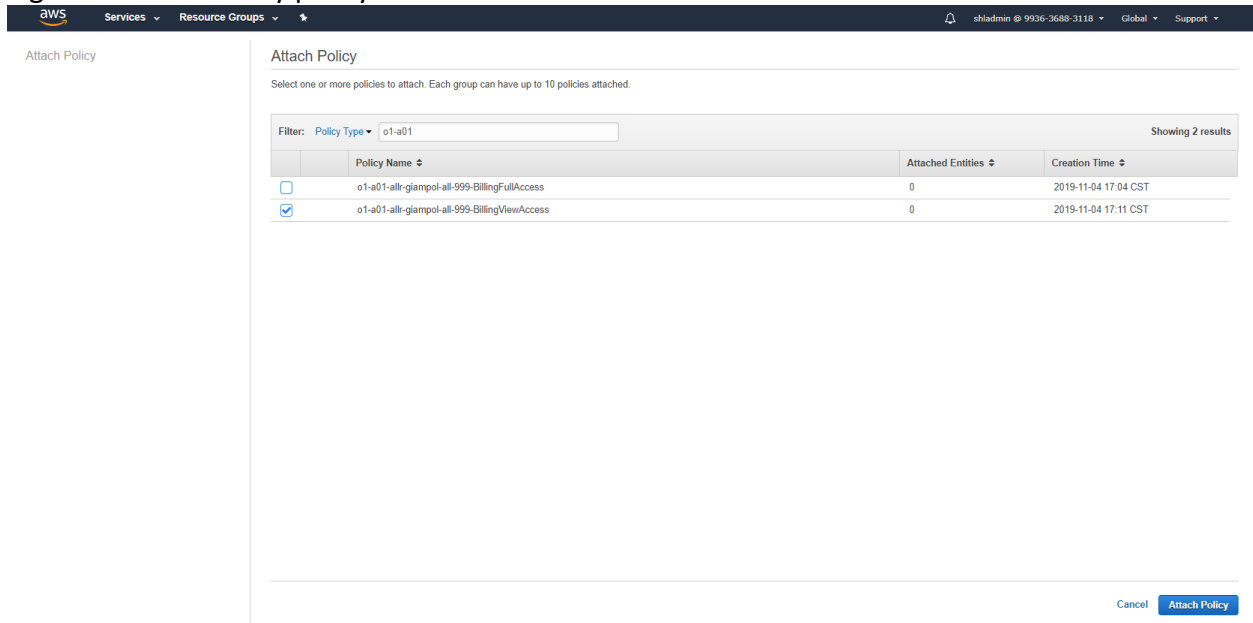
Figure 14 – Permissions tab



Locate the created billing information access policies by using Filer search box. Two policies show up. Select View-only policy.

# How to Set up AWS CloudWatch Billing Alarms

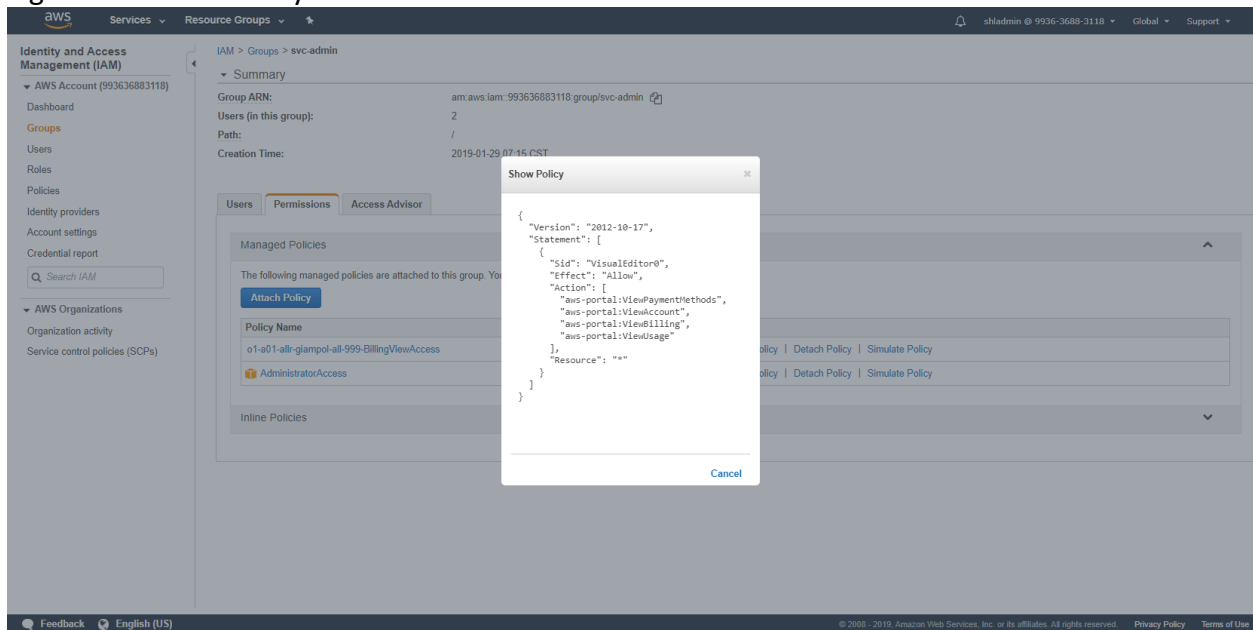
Figure 15 – View-only policy selected for it to be attached



Click Attach policy

View Policy (optional)

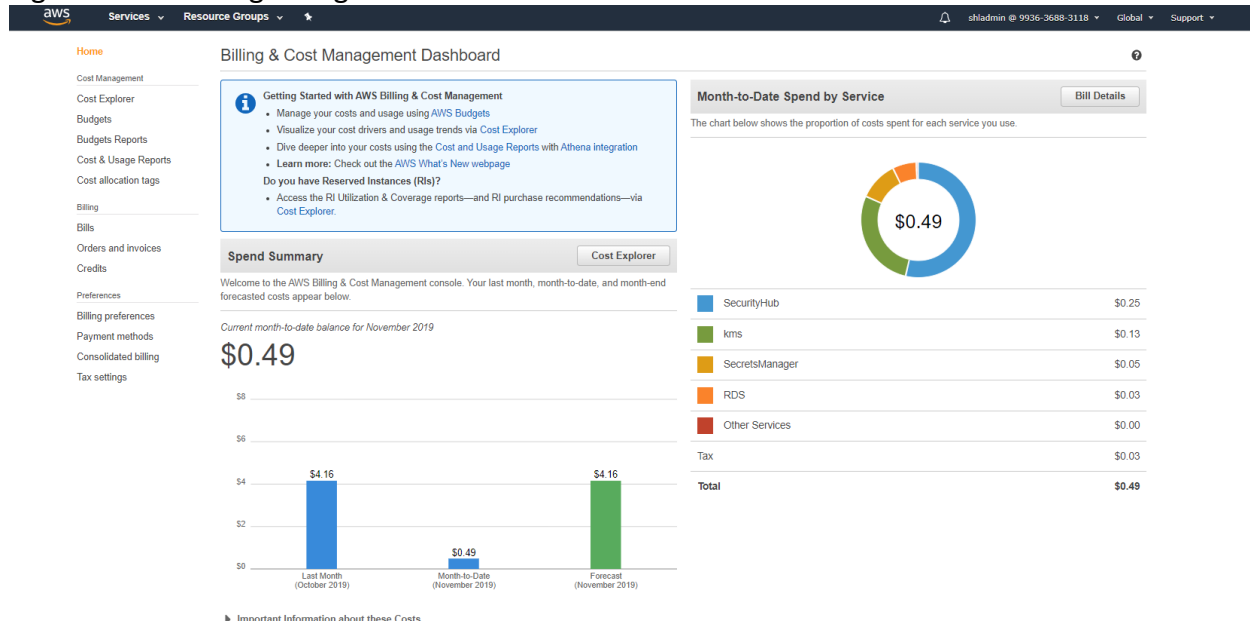
Figure 16 – View Policy



Verify that Admin user shladmin can access and view billing information

# How to Set up AWS CloudWatch Billing Alarms

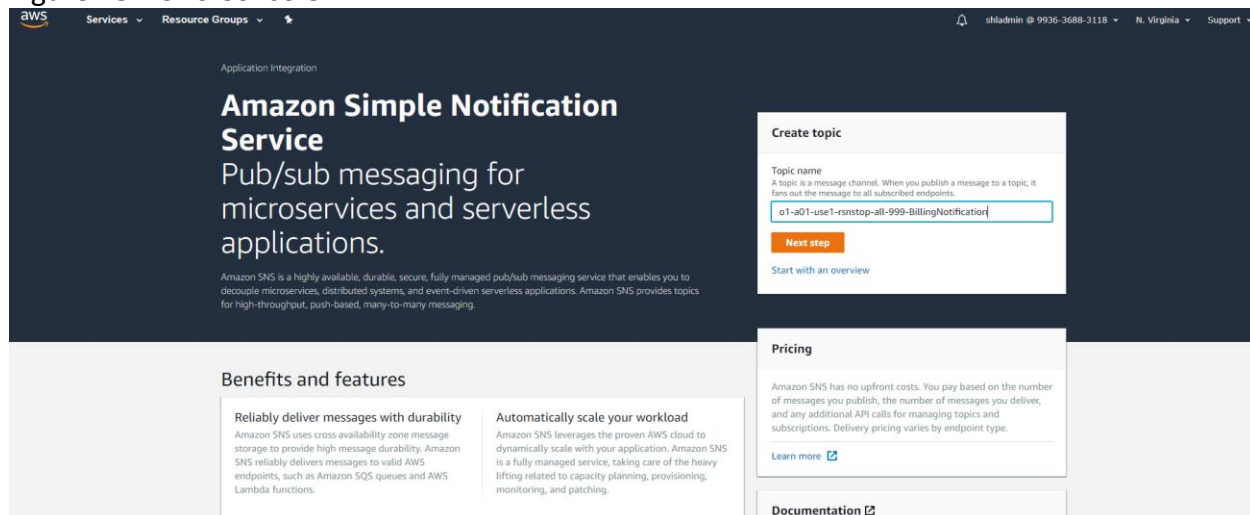
Figure 17 – Viewing billing information



## Step 4 – Creating SNS topic

Create SNS Topic for BA. Open up SNS Console. Name a new SNS topic per your naming convention

Figure 18 – SNS Console



# How to Set up AWS CloudWatch Billing Alarms

Figure 19 – Creating SNS topic (continued)

The screenshot shows the 'Create topic' page in the AWS Management Console. The left sidebar contains the 'Amazon SNS' menu with options for Dashboard, Topics, Subscriptions, and Mobile. The main content area is titled 'Create topic' and includes several sections: 'Details' with fields for 'Name' and 'Display name - optional', both containing the value 'o1-a01-use1-rsntop-all-999-BillingNotification'; 'Encryption - optional'; 'Access policy - optional'; 'Delivery retry policy (HTTP/S) - optional'; 'Delivery status logging - optional'; and 'Tags - optional' with a table for adding tags. At the bottom right are 'Cancel' and 'Create topic' buttons.

Amazon SNS > Topics > Create topic

### Create topic

**Details**

Name  
o1-a01-use1-rsntop-all-999-BillingNotification  
Maximum 256 characters. Can include alphanumeric characters, hyphens (-) and underscores (\_).

Display name - optional  
To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message. [Info](#)  
o1-a01-use1-rsntop-all-999-BillingNotification  
Maximum 100 characters, including hyphens (-) and underscores (\_).

► **Encryption - optional**  
Amazon SNS provides in-transit encryption by default. Enabling server-side encryption adds at-rest encryption to your topic. [Info](#)

► **Access policy - optional**  
This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic. [Info](#)

► **Delivery retry policy (HTTP/S) - optional**  
The policy defines how Amazon SNS retries failed deliveries to HTTP/S endpoints. To modify the default settings, expand this section. [Info](#)

► **Delivery status logging - optional**  
These settings configure the logging of message delivery status to CloudWatch Logs. [Info](#)

▼ **Tags - optional**  
A tag is a metadata label that you can assign to an Amazon SNS topic. Each tag consists of a key and an optional value. You can use tags to search and filter your topics and track your costs. [Learn more](#)

Key	Value - optional	
Q Name	Q o1-a01-use1-rsntop-all-999-BillingNotific	X Remove tag

Add tag

Cancel Create topic

Click Create topic. SNS topic created

Figure 20 – SNS topic created

The screenshot shows the 'Topic o1-a01-use1-rsntop-all-999-BillingNotification created successfully.' message at the top. Below it, the 'o1-a01-use1-rsntop-all-999-BillingNotification' topic page is displayed. The 'Details' section shows the Name, Display name, ARN, and Topic owner. The 'Subscriptions' section shows a table with columns for ID, Endpoint, Status, and Protocol, and a 'Create subscription' button.

Amazon SNS > Topics > o1-a01-use1-rsntop-all-999-BillingNotification

### o1-a01-use1-rsntop-all-999-BillingNotification

Edit Delete Publish message

**Details**

Name o1-a01-use1-rsntop-all-999-BillingNotification	Display name o1-a01-use1-rsntop-all-999-BillingNotification
ARN arn:aws:sns:us-east-1:993636883118:o1-a01-use1-rsntop-all-999-BillingNotification	Topic owner 993636883118

**Subscriptions (0)** Edit Delete Request confirmation Confirm subscription Create subscription

Q Search

ID	Endpoint	Status	Protocol
No subscriptions found You don't have any subscriptions to this topic.			

Create subscription



# How to Set up AWS CloudWatch Billing Alarms

## Step 5 – Creating Subscription

Figure 21 – Creating subscription

The screenshot shows the 'Create subscription' page in the AWS console. The page has a dark header with the AWS logo and navigation tabs for 'Services' and 'Resource Groups'. Below the header, the breadcrumb trail is 'Amazon SNS > Subscriptions > Create subscription'. The main content area is titled 'Create subscription' and contains a form with the following fields:

- Details**
  - Topic ARN**: A text input field containing 'arn:aws:sns:us-east-1:993636883118:o1-a1'.
  - Protocol**: A dropdown menu with 'Email' selected.
  - Endpoint**: A text input field containing 'tony.shen@live.com'.
- Subscription filter policy - optional**: A section with a link to 'info'.

At the bottom of the form, there are two buttons: 'Cancel' and 'Create subscription'.

Click Create subscription

Figure 25 – Subscription created, pending confirmation

The screenshot shows the AWS console after a subscription has been created. A green banner at the top of the main content area states: 'Subscription to o1-a01-use1-rsntop-all-999-BillingNotification created successfully. The ARN of the subscription is arn:aws:sns:us-east-1:993636883118:o1-a01-use1-rsntop-all-999-BillingNotification:4f879992-0a54-437f-95f2-bfbc74449977.' Below the banner, the breadcrumb trail is 'Amazon SNS > Topics > o1-a01-use1-rsntop-all-999-BillingNotification > Subscription: 4f879992-0a54-437f-95f2-bfbc74449977'. The main content area is titled 'Subscription: 4f879992-0a54-437f-95f2-bfbc74449977' and contains a 'Details' section with the following information:

- ARN**: arn:aws:sns:us-east-1:993636883118:o1-a01-use1-rsntop-all-999-BillingNotification:4f879992-0a54-437f-95f2-bfbc74449977
- Endpoint**: tony.shen@live.com
- Topic**: o1-a01-use1-rsntop-all-999-BillingNotification
- Status**: Pending confirmation
- Protocol**: EMAIL

Below the details section, there is a 'Subscription filter policy' section. It states: 'No filter policy configured for this subscription. To apply a filter policy, edit this subscription.' and includes an 'Edit' button.

Click to confirm when receiving the confirmation email

# How to Set up AWS CloudWatch Billing Alarms

Figure 26 – SNS subscription confirmation email received, click to confirm

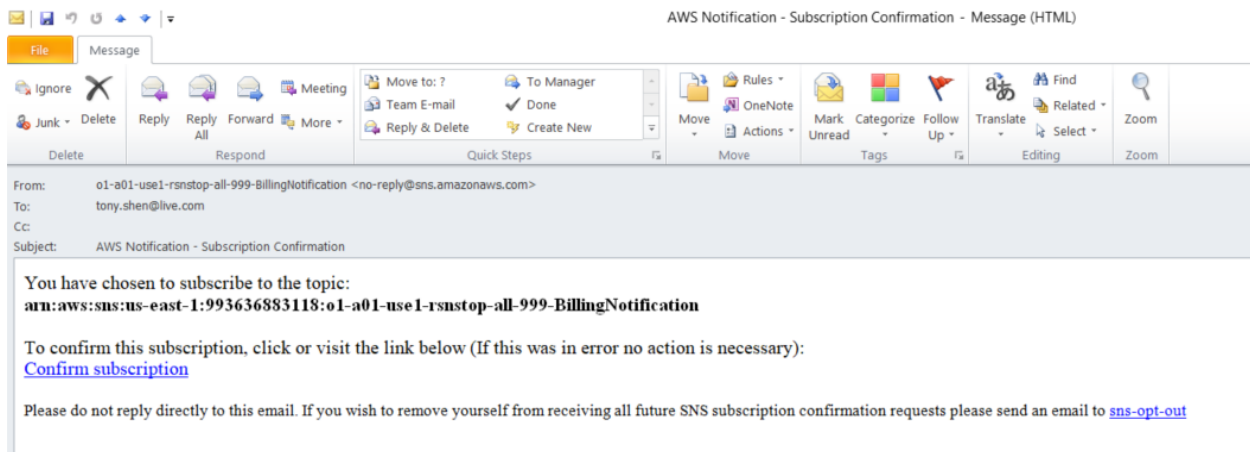
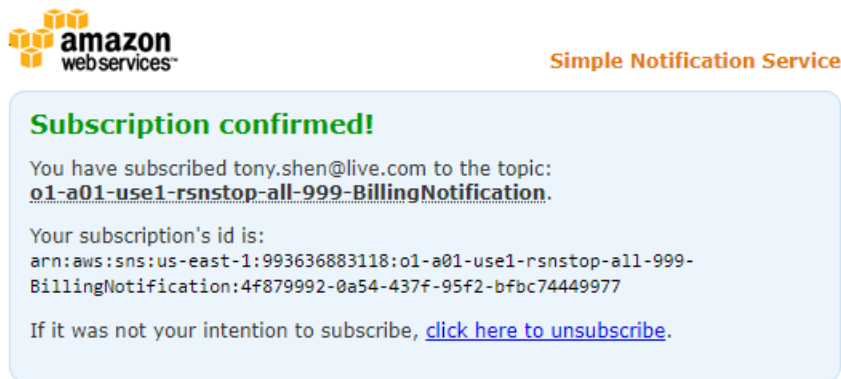
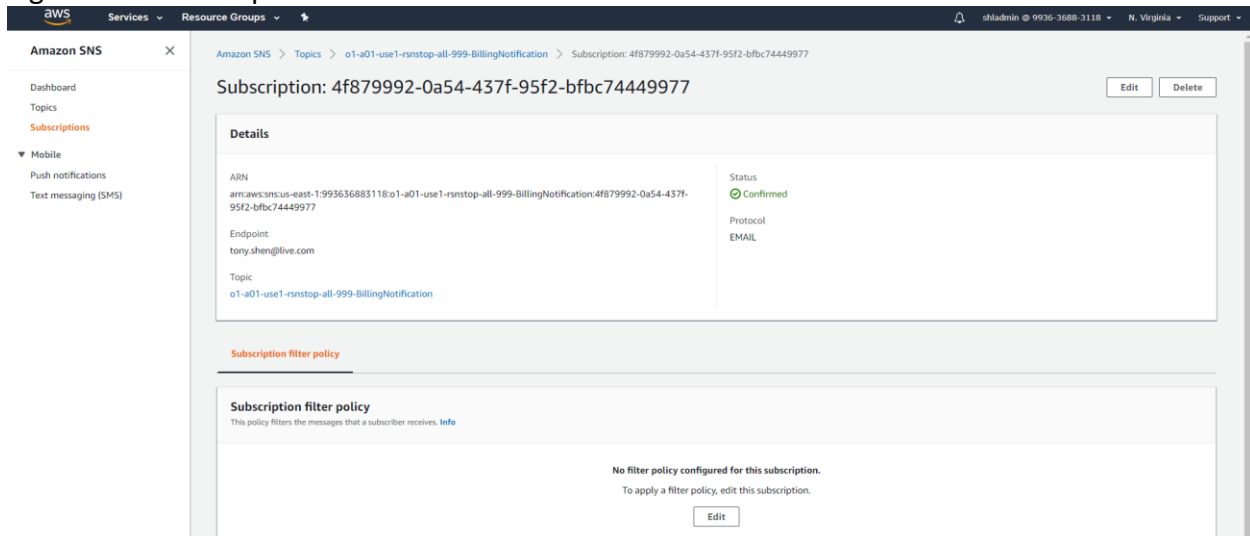


Figure 27 – Subscription confirmed



Verify in SNS Console the subscription is confirmed as well

Figure 28 – Subscription confirmed in SNS Console

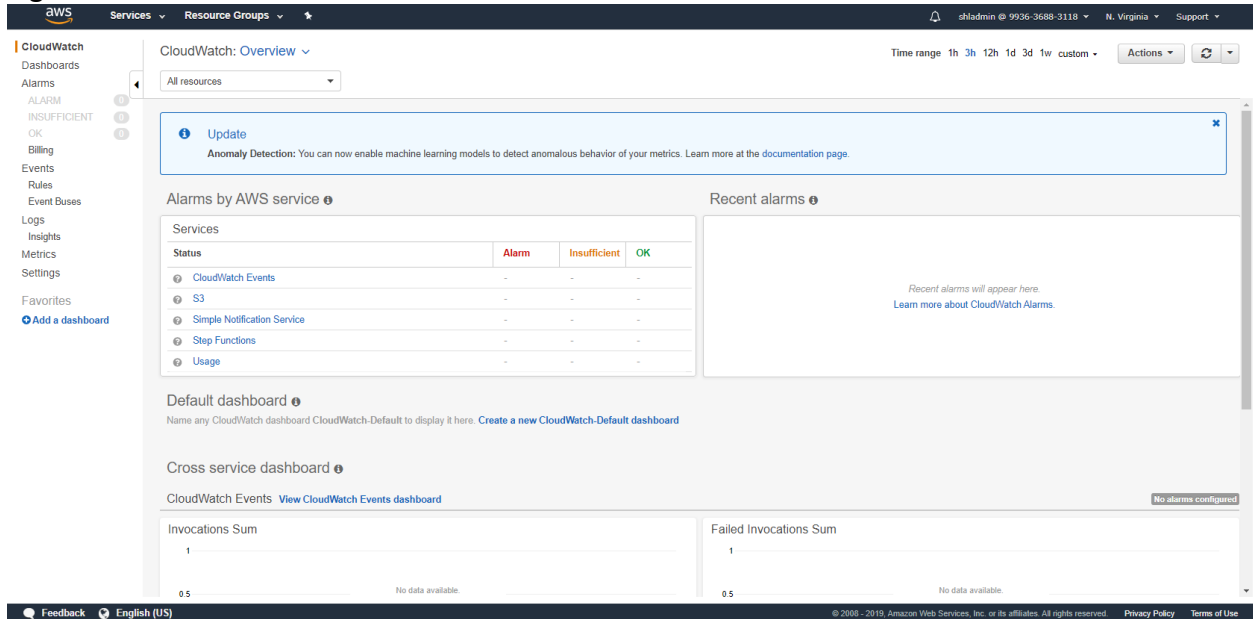


# How to Set up AWS CloudWatch Billing Alarms

## Step 6 – Creating CloudWatch Alarm

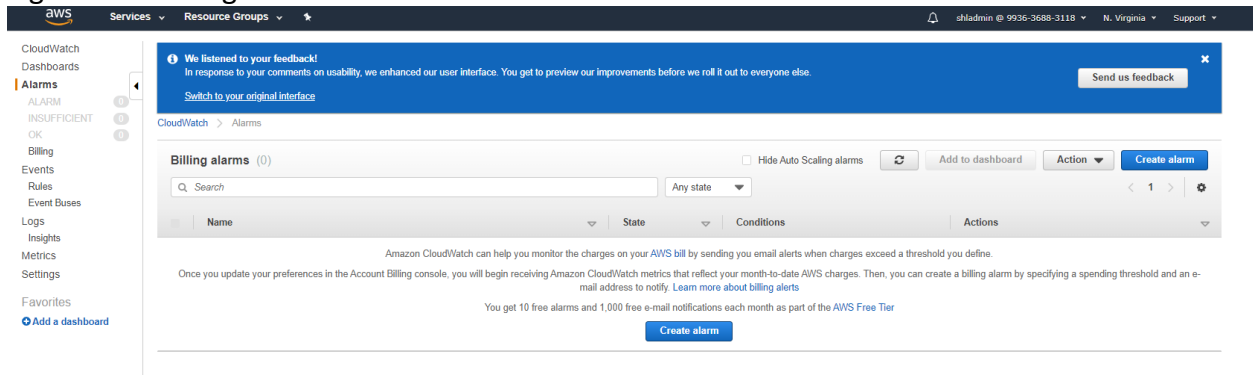
Open up CloudWatch Console.

Figure 29 – CloudWatch Console



Click Billing in Navigation Pane

Figure 30 – Billing alarms



Click Create alarm. Specify metric and conditions

# How to Set up AWS CloudWatch Billing Alarms

Figure 31 – Specify metric and conditions

aws

Services

Resource Groups

★

CloudWatch > Alarms > Create alarm

Step 1  
Specify metric and conditions

Step 2  
Configure actions

Step 3  
Add a description

Step 4  
Preview and create

Specify metric and conditions

Edit

Metric

Graph

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

11

10.5

10

9.5

9

10/29

10/31

11/01

11/03

No data available

Try adjusting the dashboard time range.

o1-a01-use1-rcwmet-all-999-BillingEstimatedCharges

Namespace

AWS/Billing

Metric name

o1-a01-use1-rcwmet-all-999-BillingEstimatedCharges

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 o1-a01-use1-rcwmet-all-999-BillingEstimatedCharges is...

Define the alarm condition

Greater

> threshold

Greater/Equal

>= threshold

Lower/Equal

<= threshold

Lower

< threshold

than...

Define the threshold value

10

USD

Must be a number

Additional configuration

Cancel

Next

Configure actions

# How to Set up AWS CloudWatch Billing Alarms

Figure 32 – Configuring actions

aws

Services

Resource Groups

★

CloudWatch > Alarms > Create alarm

Step 1

Specify metric and conditions

Step 2

Configure actions

Step 3

Add a description

Step 4

Preview and create

## Configure actions

### Notification

Whenever this alarm state is...  
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.

Remove

### 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

### Send a notification to...

o1-a01-use1-rsntop-all-999-BillingNot

✕

Only email lists for this account are available

### Email (endpoints)

tony.shen@live.com - [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

Cancel

Previous

Next

# How to Set up AWS CloudWatch Billing Alarms

Figure 33 – Add alarm description

The screenshot shows the AWS CloudWatch console interface for creating a new alarm. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and a star icon. The breadcrumb trail is 'CloudWatch > Alarms > Create alarm'. On the left, a sidebar lists four steps: 'Step 1: Specify metric and conditions', 'Step 2: Configure actions', 'Step 3: Add a description' (which is highlighted), and 'Step 4: Preview and create'. The main content area is titled 'Add a description' and contains a section 'Name and description'. Under 'Define a unique name', the 'Alarm name' field is populated with 'o1-a01-use1-rciwalm-all-999-BillingEstimatedCharge'. Below this, the 'Alarm description - optional' section has a text area containing 'Organization 1 Account 01 N.Virginia Region CloudWatch Alarm All Environments All Billing Estimated Charge 6 hour period exceeding \$10 USD'. A character count at the bottom of the text area indicates 'Up to 1024 characters (138/1024)'. At the bottom right of the form are three buttons: 'Cancel', 'Previous', and 'Next'.

Give a unique name per your naming convention. Click Next

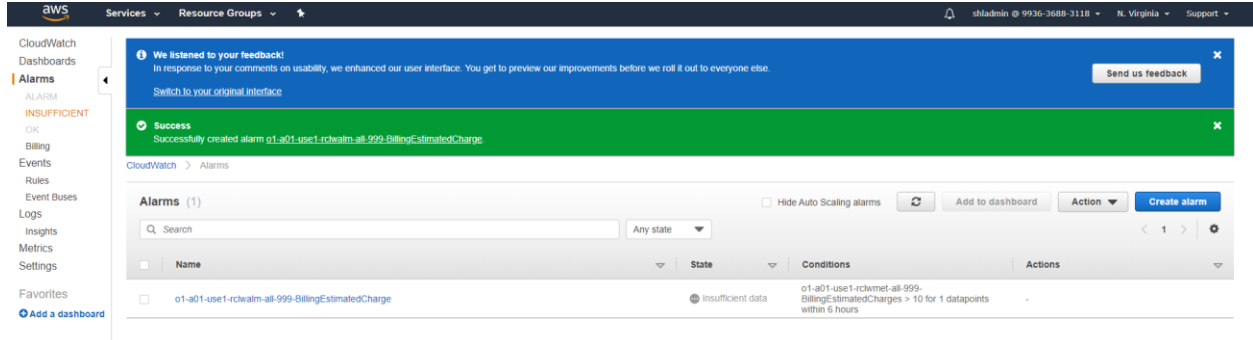
Figure 34 – Creating alarm

This screenshot displays the 'Creating alarm' step in the AWS CloudWatch console. The top navigation bar is identical to Figure 33. The breadcrumb trail is 'Greater (>) > than... > 10'. The main content area shows 'Step 2: Configure actions' with an 'Edit' button. Below this is the 'Actions' section, which includes a 'Notification' field with the value 'When in Alarm, send a notification to "o1-a01-use1-rsntop-all-999-BillingNotification"'. Further down, 'Step 3: Add a description' is shown with an 'Edit' button. The 'Name and description' section contains a table with two columns: 'Name' and 'Description'. The 'Name' column contains 'o1-a01-use1-rciwalm-all-999-BillingEstimatedCharge' and the 'Description' column contains 'Organization 1 Account 01 N.Virginia Region CloudWatch Alarm All Environments All Billing Estimated Charge 6 hour period exceeding \$10 USD'. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Create alarm'.

# How to Set up AWS CloudWatch Billing Alarms

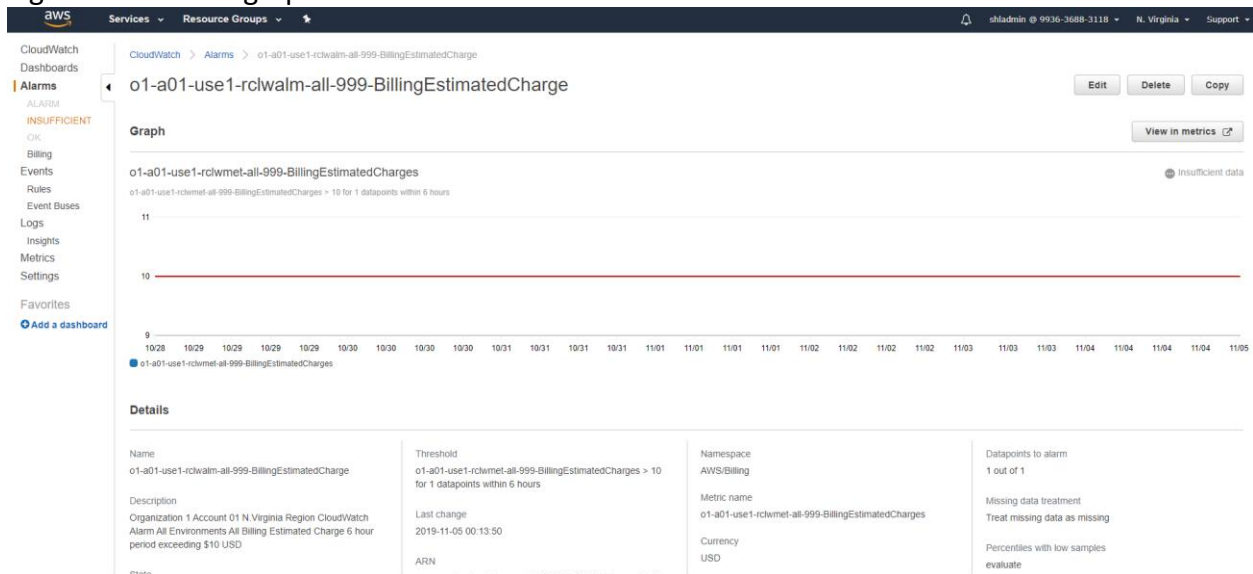
Click Create alarm  
Alarm created

Figure 35 – Alarm created



Select and open the newly created alarm and verify the details

Figure 36 – Alarm graph



CloudWatch BA setup is thus completed. This BA will send billing alert emails to BA recipient when billing estimated charge exceeds \$10 in a 6-hour period.

## Summary

In order to minimize your AWS cost and maximize your returns, you need to closely monitor your billing. Using CloudWatch to keep watching AWS estimated charges regularly is one way to save money. Billing monitoring helps raising your AWS usage efficiency by bringing your attention to unnecessary usages so you can reduce them. Billing monitoring also helps you in identifying incorrect charges and engaging AWS timely for them to investigate and remove

## How to Set up AWS CloudWatch Billing Alarms

---

those charges. Considering how vast and complex AWS services and their pricing models are, incorrect billings from AWS do occur, and such occurrences are not uncommon, though unintentional by AWS. What was introduced in this article offers you a way to do both in keeping your AWS cost down.

### References

[AWS CloudWatch User Guide](#)

[AWS SNS User Guide](#)

[AWS IAM User Guide](#)