AWS Technical Essential
Project Document

Table of Contents

1. Introduction

Heaven Classics successfully creates an EC2 Server Instance for Windows 2012 Server. After launching the instance on the server, the next step was to monitor the operations. Monitoring is important to keep an eye on the performance of an EC2 instance. It helps gather data from all parts, and is useful for debugging failure. The monitoring team at Heaven Classics started monitoring activities using the CloudWatch Service in the AWS Management Console. The Heaven Classics support team were required to meet the following objectives:

1. Check the CPU Utilization.
2. Create an Alarm.
3. Create an IAM User.
4. Create the IAM Administrator Group, and add the user to the AdministratorGroup.
5. Create a Role

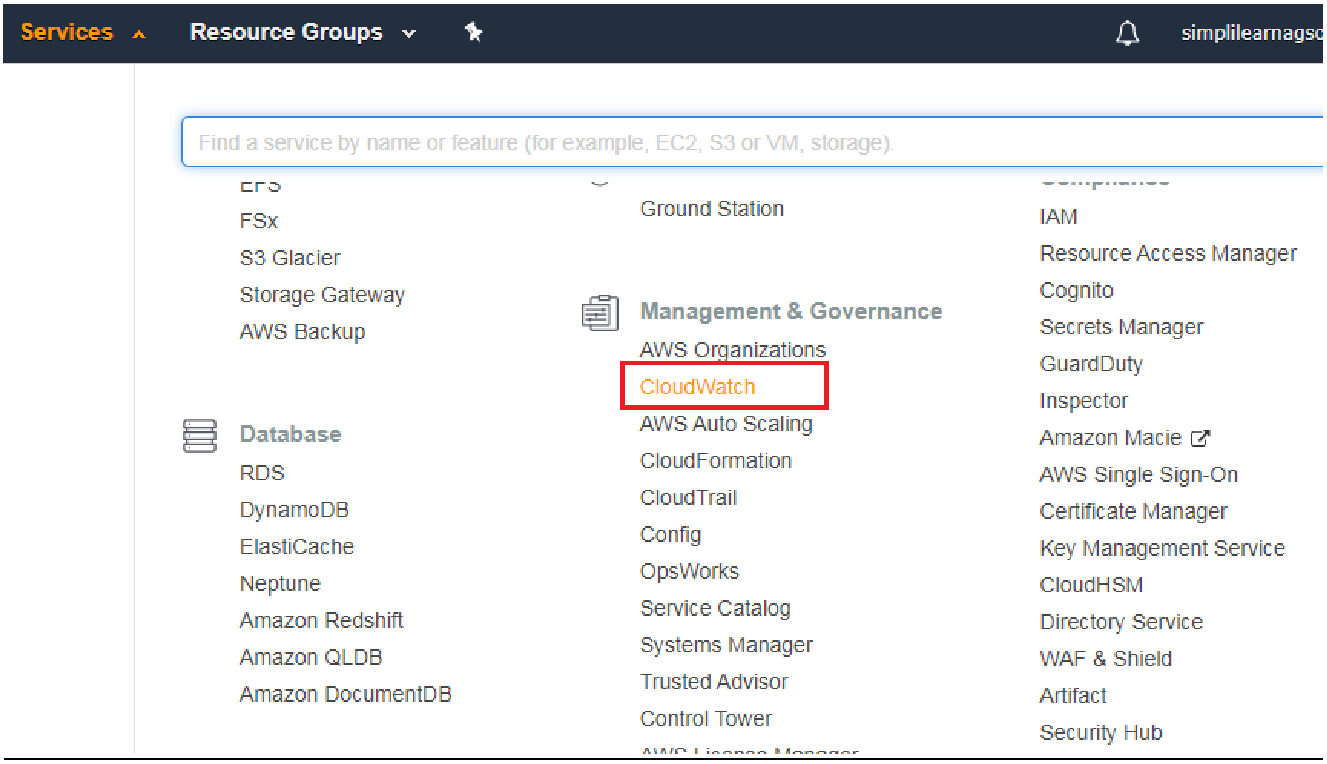
2. AWS CloudWatch Service

It is important to check and monitor CPU utilization for monitoring day to day operation. CPU utilization can be check using AWS CloudWatch Matrics and we can even create the dashboard for checking and monitoring CPU utilization. CPU utilization checkingin & monitoring using dashboard is described below:

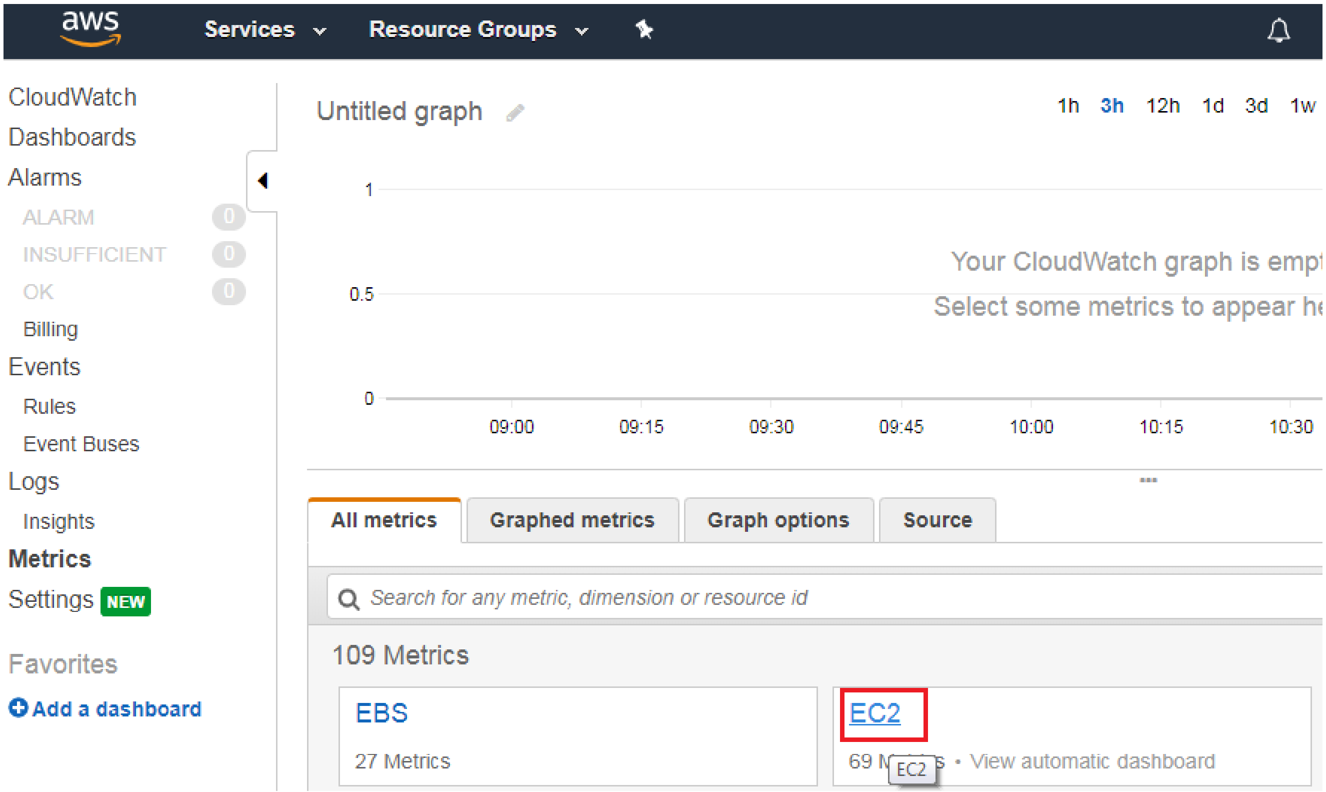
2.1 Check CPU Utilization

We have already created EC2 Windows Server 2012 EC2 instance and named it as **HeavenClassics.**

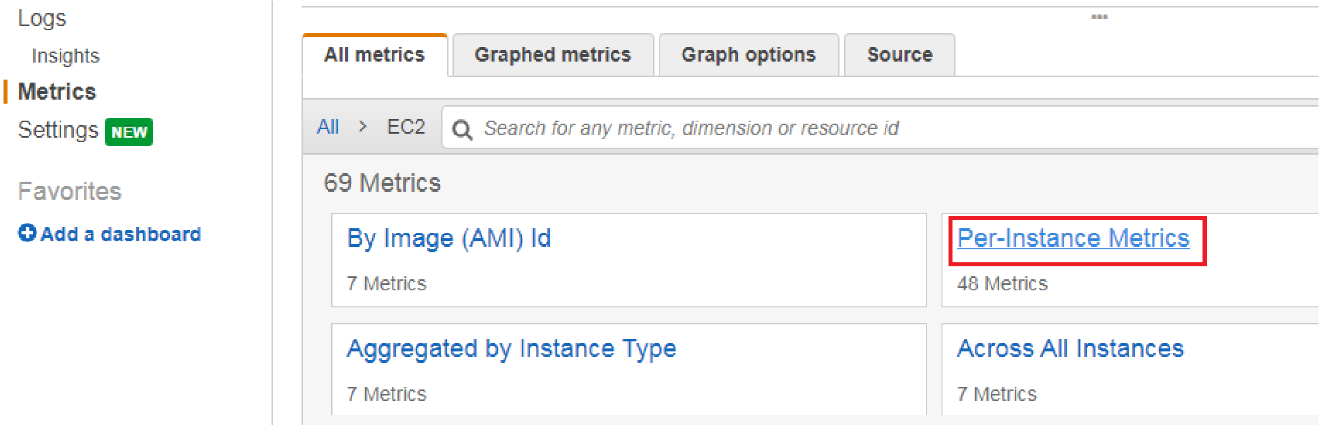
a. Open the Amazon Management Console.
b. In the AWS Management Console, locate the Amazon CloudWatch icon under the Management & Governance services. Then, click the icon to display the CloudWatch Console page.



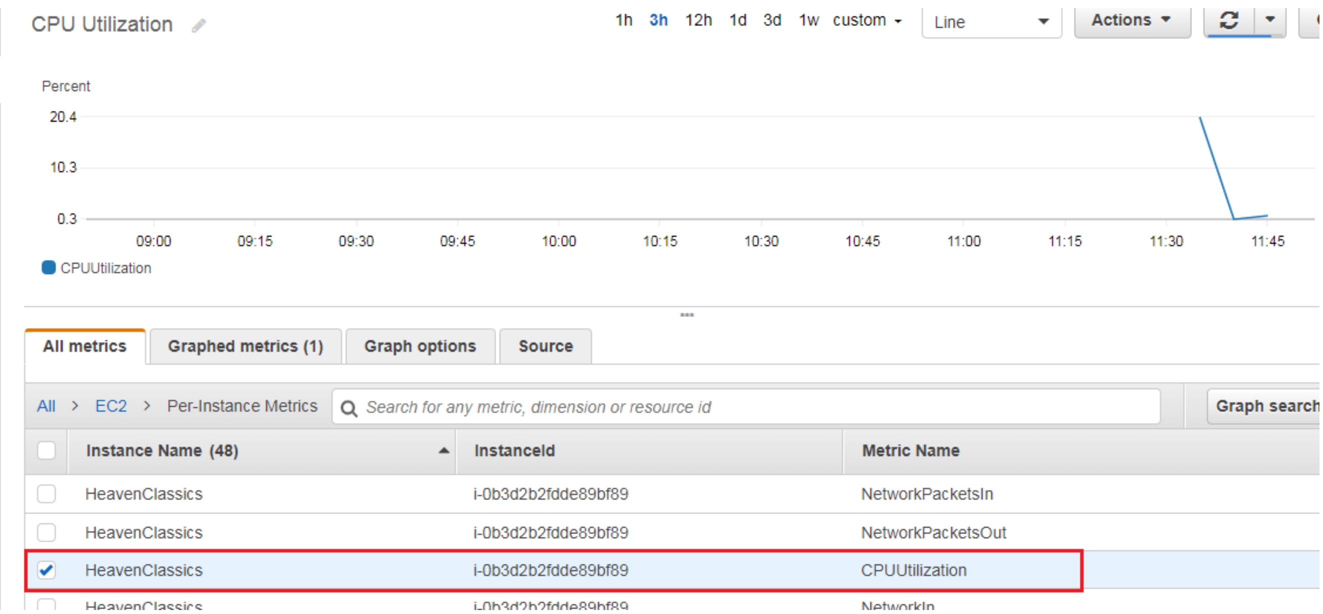
c. Under CloudWatch Console Select **Metrics then Select EC2 instance**



d. From EC2 Metrics- **Select Per-Instance Metrics**



e. Here all the instance name and metrics to check/monitor will be populated. To check CPU Utilization select instance name **HeavenClassics** with metrics CPUUtilization.



	Instance Name (48)	InstanceId	Metric Name
☐	HeavenClassics	i-0b3d2b2fdde89bf89	NetworkPacketsIn
☐	HeavenClassics	i-0b3d2b2fdde89bf89	NetworkPacketsOut
☑	HeavenClassics	i-0b3d2b2fdde89bf89	CPUUtilization
☐	HeavenClassics	i-0b3d2b2fdde89bf89	NetworkIn

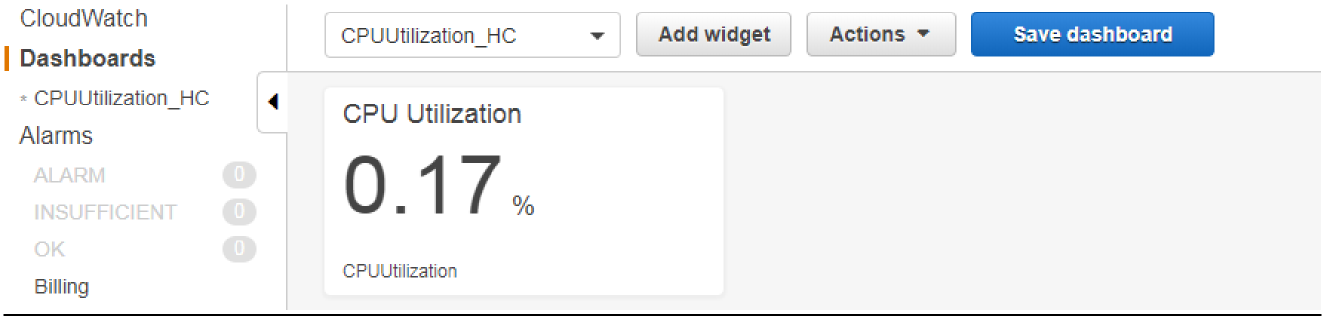
e. On selecting required metrics-CPUUtilization graph will show the CPU Utilization. This is how we can monitor CPU Utilization using CloudWatch-Metrics.

2.1.1 Monitor CPU Utilization using Dashboard

Using AWS CloudWatch Service we can create the dashboard to check and monitor the CPU utilization.

a. From CloudWatch service select Dashboard and select **Create Dashboard**. Enter the dashboard name as **CPUUtilization_HC**

b. Select Widget type as Number and select the EC2- **HeavenClassics** instance with **CPU utilization metrics**. This will show instant value on dashboard as below

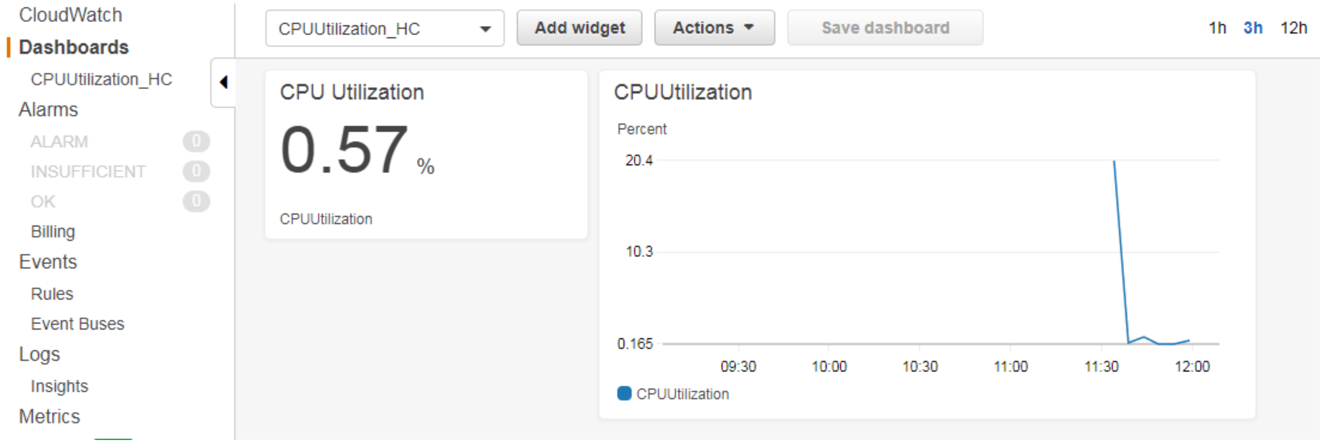


CPU Utilization

0.17 %

CPUUtilization

c. Further we can add additional widget to this dashboard to monitor CPU Utilization over time as shown below


CloudWatch

Dashboards

CPUUtilization_HC

Alarms

ALARM 0

INSUFFICIENT 0

OK 0

Billing

Events

Rules

Event Buses

Logs

Insights

Metrics

CPUUtilization_HC | Add widget | Actions | Save dashboard | 1h 3h 12h

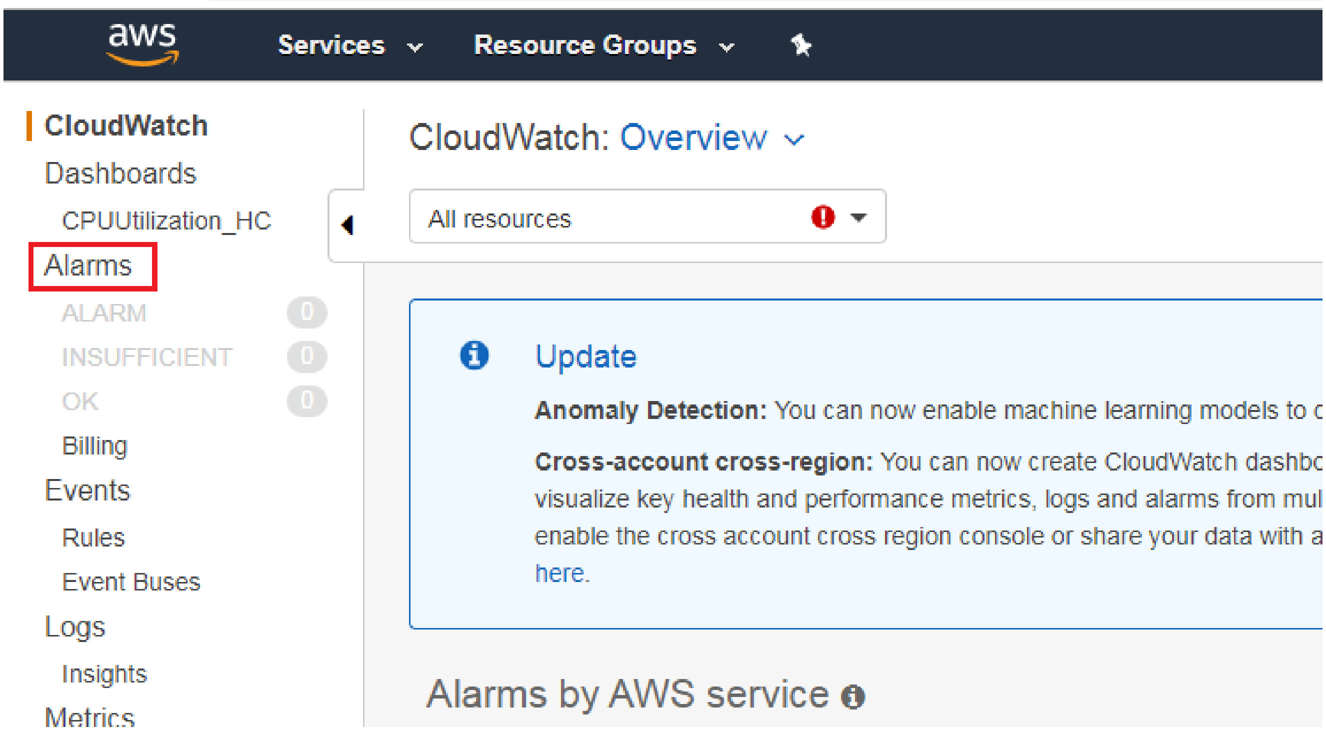
CPU Utilization

0.57 %

CPUUtilization

2.2 Alarm Creation

a. For creating alarm after specific condition occur - Under CloudWatch service select **Alarms**



CloudWatch

Dashboards

CPUUtilization_HC

Alarms

ALARM 0

INSUFFICIENT 0

OK 0

Billing

Events

Rules

Event Buses

Logs

Insights

Metrics

CloudWatch: Overview

All resources

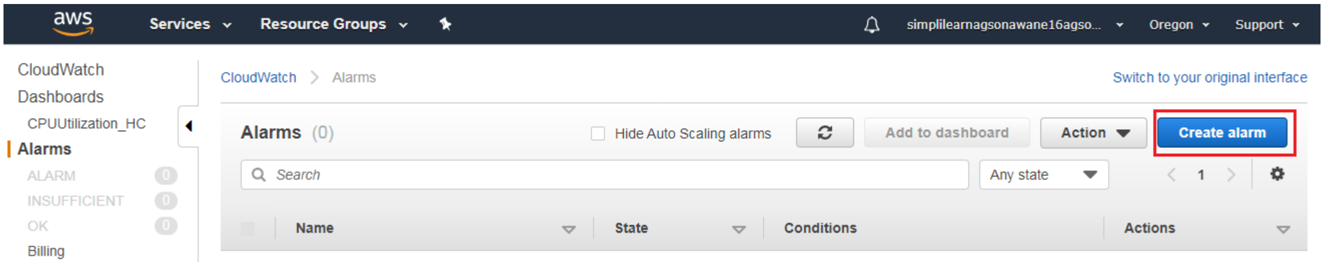
Update

Anomaly Detection: You can now enable machine learning models to c

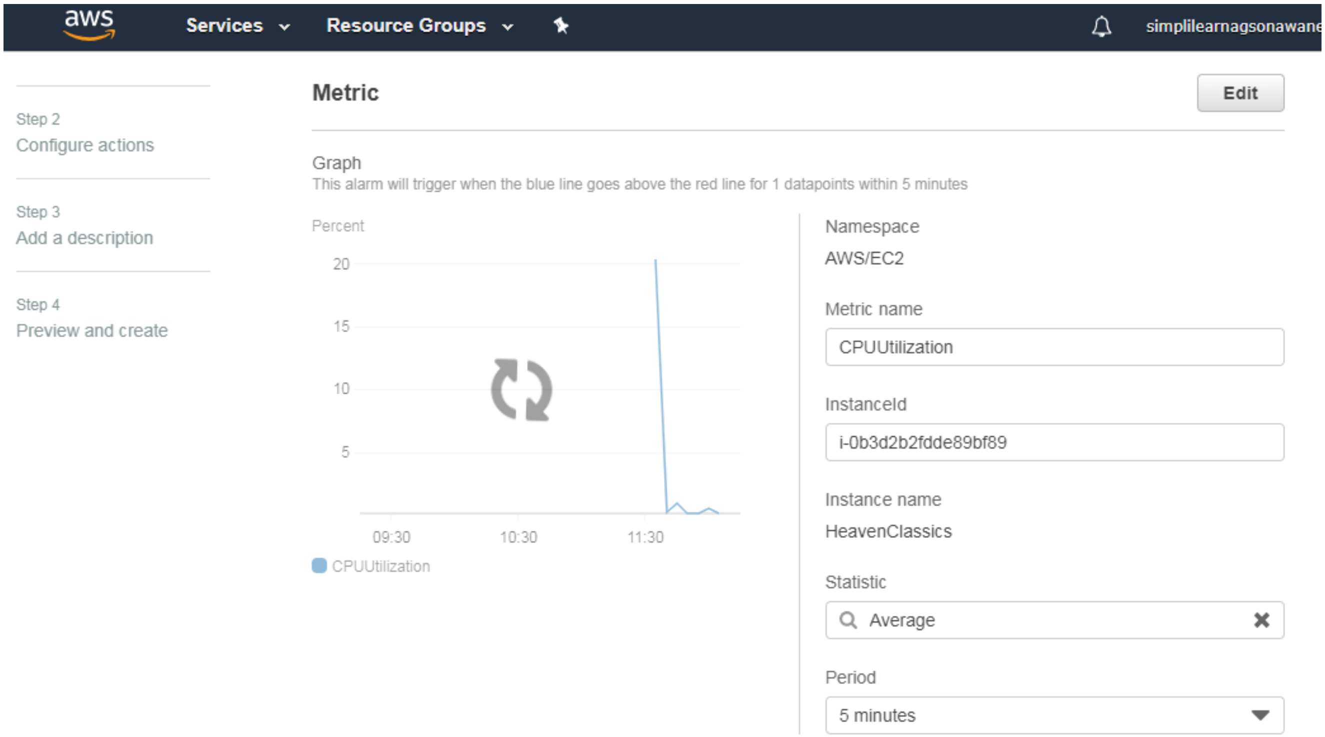
Cross-account cross-region: You can now create CloudWatch dashbc visualize key health and performance metrics, logs and alarms from mul enable the cross account cross region console or share your data with a here.

Alarms by AWS service

b. Select **Create Alarm**



c. Specify the metrics and condition to raise the alarm. Here we will create alarm for EC2-CPU Utilization



Metric

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

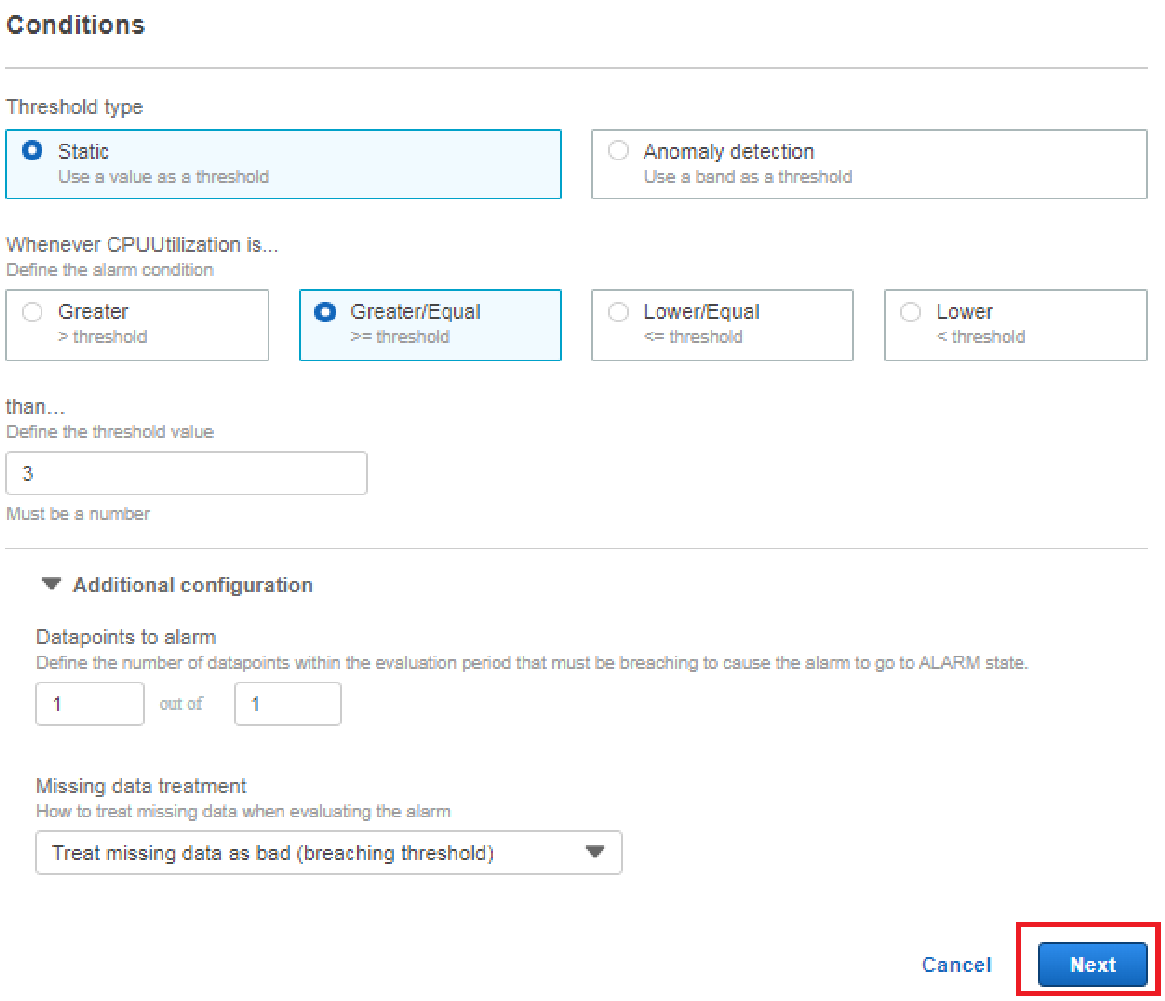
InstanceId
i-0b3d2b2fdde89bf89

Instance name
HeavenClassics

Statistic
Average

Period
5 minutes

d. Specify the condition under condition section. Here we are specifying the condition to raise the alarm as and when cpu utilization is greater than or equal to 3. After specifying the condition click on **Next.**



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

3

Must be a number

▼ Additional configuration

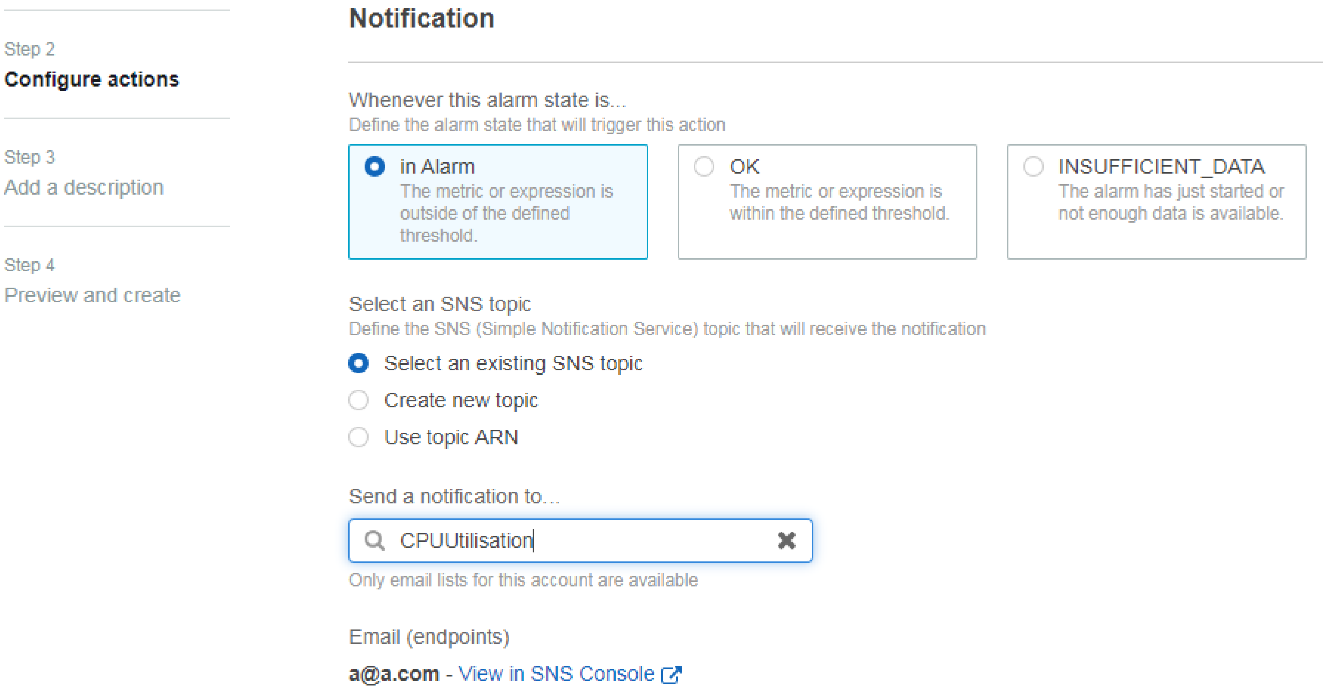
Datapoints to alarm
Define the number of datapoints within the evaluation period that must be breaching to cause the alarm to go to ALARM state.

1 out of 1

Missing data treatment
How to treat missing data when evaluating the alarm

Treat missing data as bad (breaching threshold) ▼

e. Now create the notification for this alarm. Whenever this alarm occur we need to notify to user. This can be achieve by selecting existing topic and emailID or you can create new topic with emailID list. Here we are selecting existing topic for notifying via email. After that Click **Next.**



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.

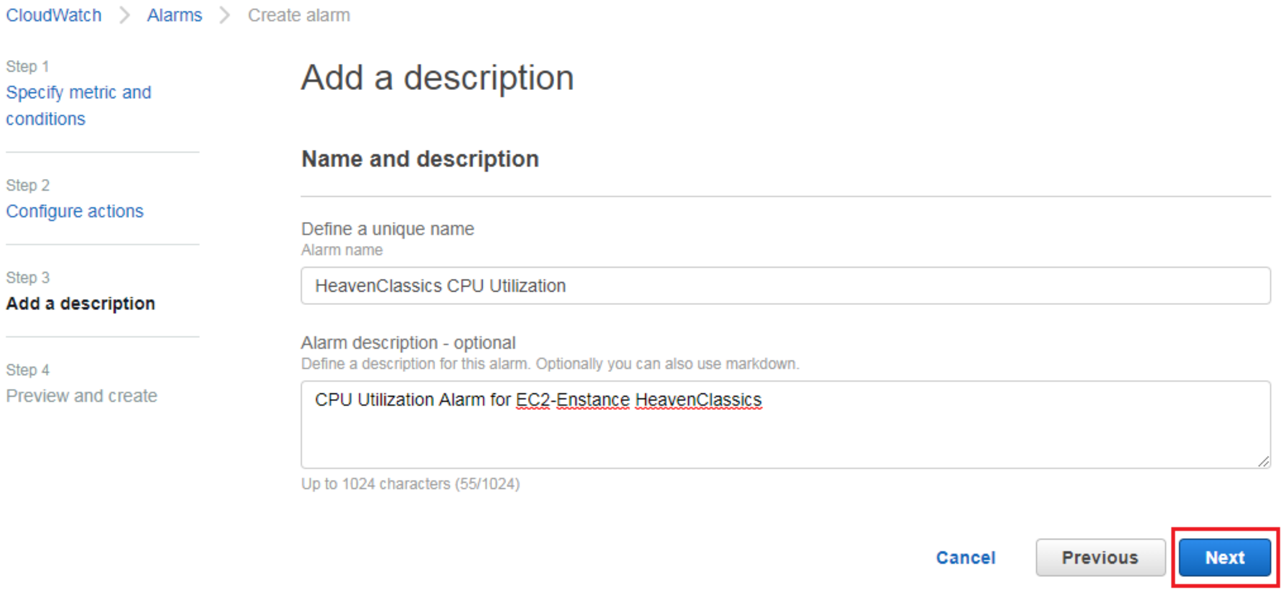
Select an SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification

● Select an existing SNS topic
○ Create new topic
○ Use topic ARN

Send a notification to...
CPUUtilisation
Only email lists for this account are available

Email (endpoints)
a@a.com - View in SNS Console

f. Provide unique Alarm Name and alarm description. Click **Next.**



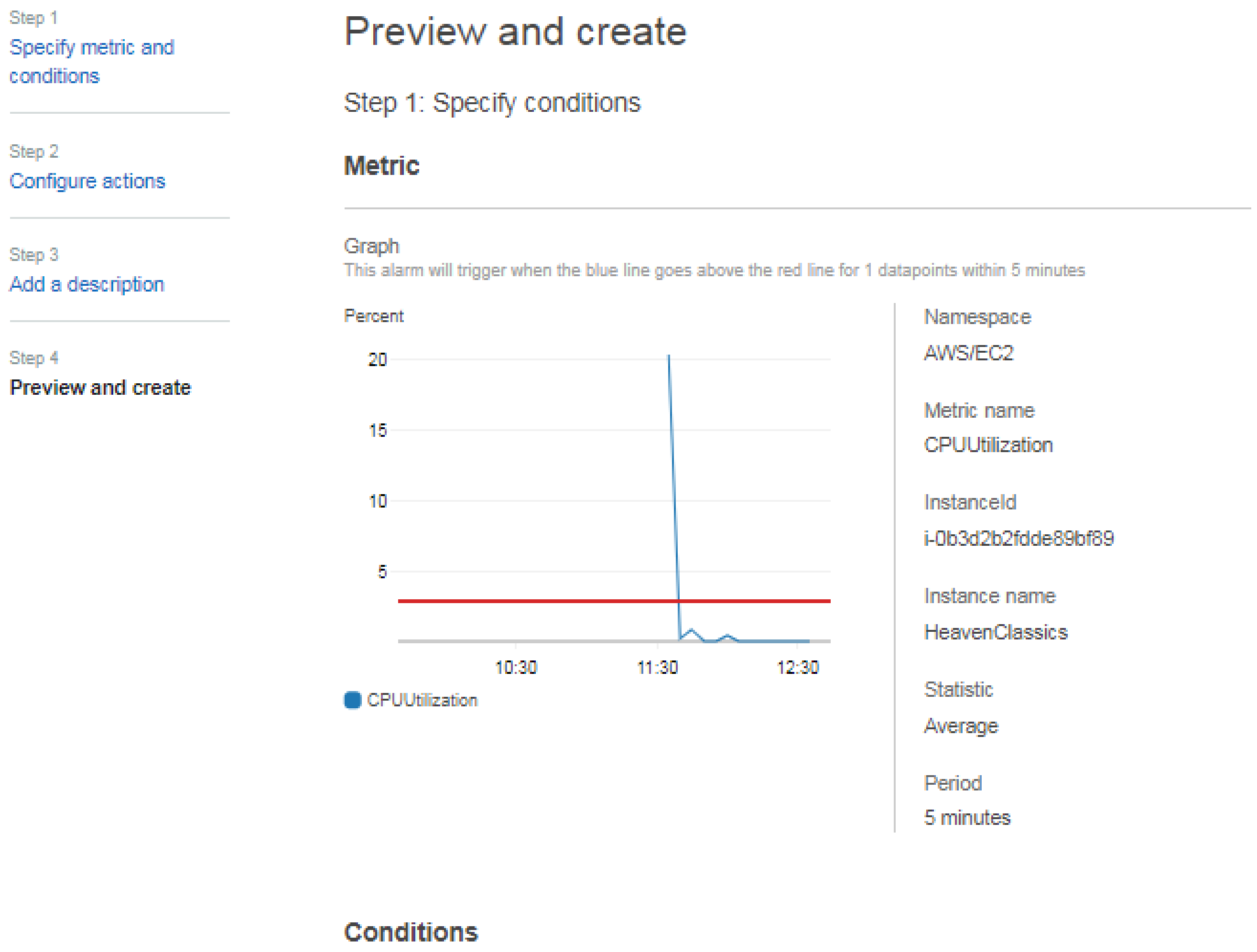
Add a description

Name and description

Define a unique name
Alarm name
HeavenClassics CPU Utilization

Alarm description - optional
Define a description for this alarm. Optionally you can also use markdown.
CPU Utilization Alarm for EC2-Enstance HeavenClassics
Up to 1024 characters (55/1024)

g. Here we can preview the alarm configuration. Verify the configuration and select **Create Alarm**



Step 1
Specify metric and conditions

Step 2
Configure actions

Step 3
Add a description

Step 4
Preview and create

Preview and create

Step 1: Specify conditions

Metric

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-0b3d2b2fdde89bf89

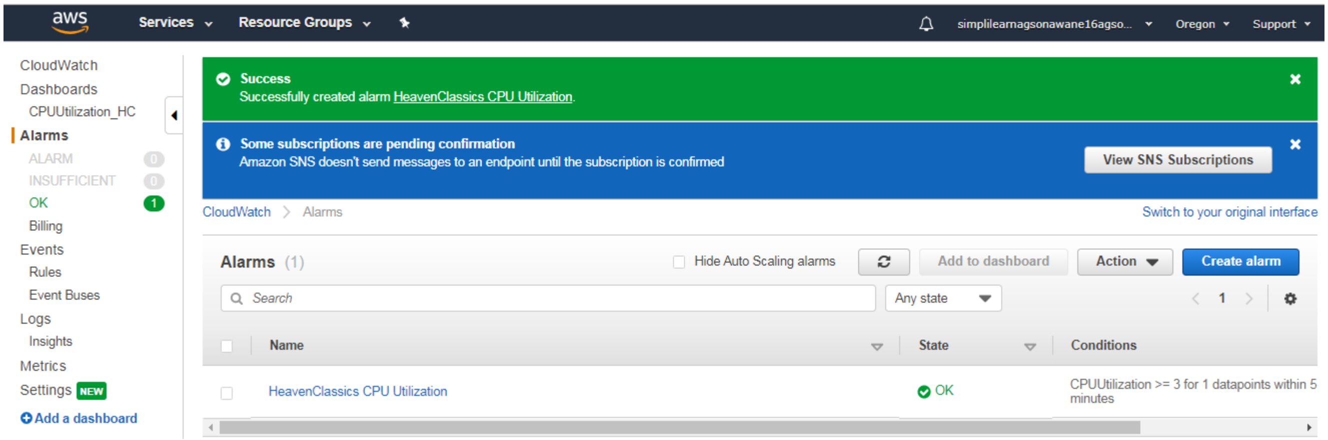
Instance name
HeavenClassics

Statistic
Average

Period
5 minutes

Conditions

h. ColudWatch Service Alarm Console will display created alarm as below.



Success
Successfully created alarm HeavenClassics CPU Utilization.

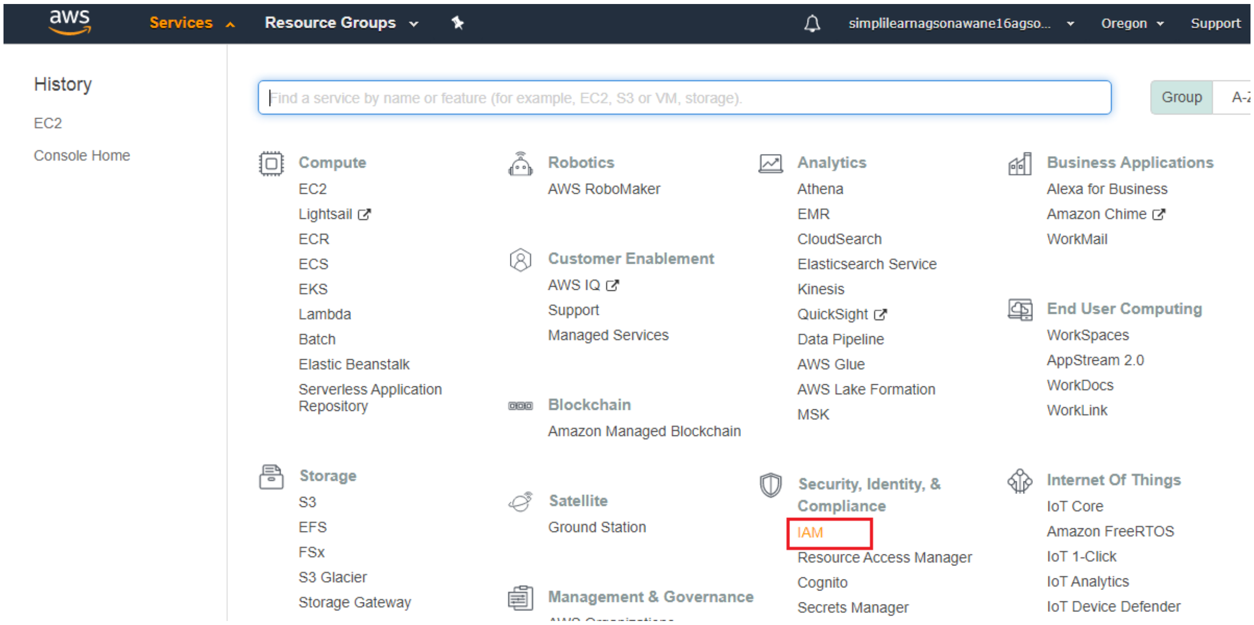
Some subscriptions are pending confirmation
Amazon SNS doesn't send messages to an endpoint until the subscription is confirmed

☐	Name	State	Conditions
☐	HeavenClassics CPU Utilization	✓ OK	CPUUtilization >= 3 for 1 datapoints within 5 minutes

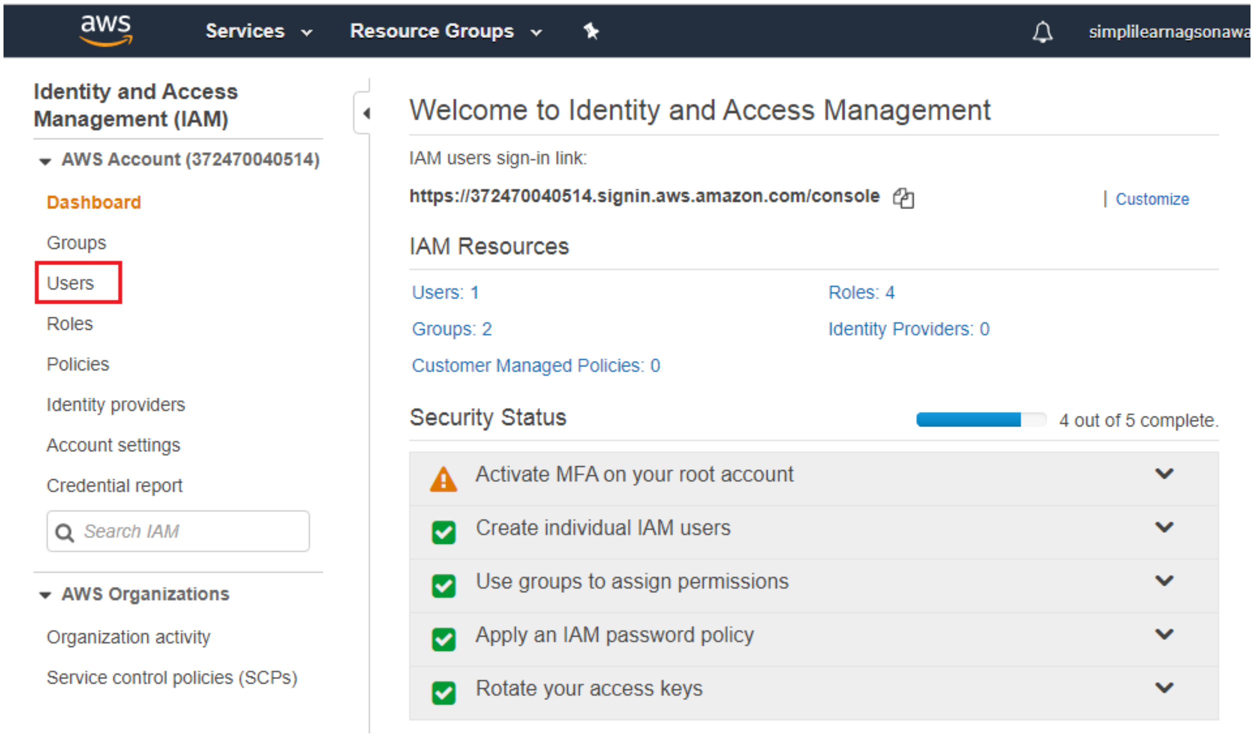
2.3 IAM User Creation

a. Open the Amazon Management Console.

b. In the AWS Management Console, locate the IAM service icon under the Security, Identity & Compliance. Then, click the IAM icon to display the IAM Console page as shown below.



c. Under Identity and Access Management console click **USER**



Welcome to Identity and Access Management

IAM users sign-in link:

https://372470040514.signin.aws.amazon.com/console

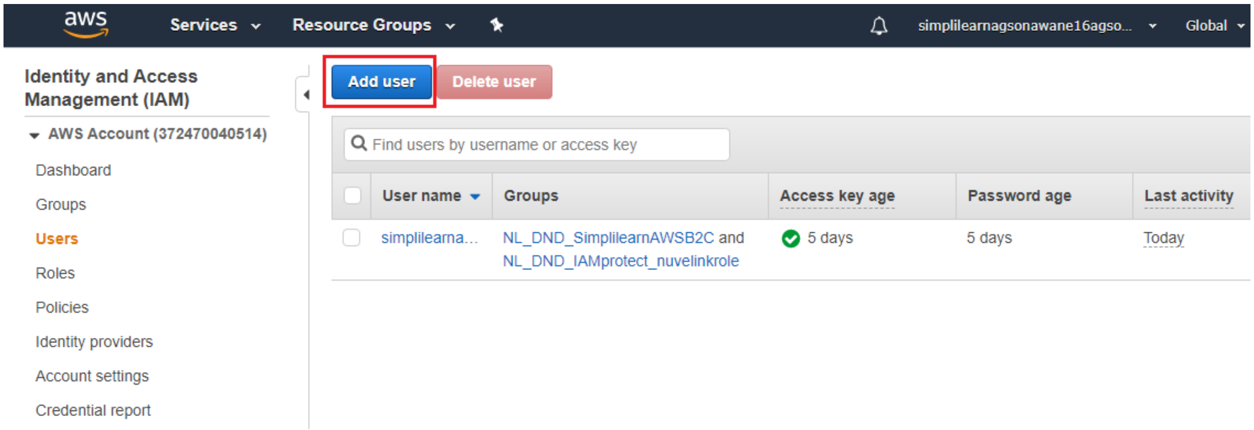
IAM Resources

Users: 1
Groups: 2
Customer Managed Policies: 0
Roles: 4
Identity Providers: 0

Security Status 4 out of 5 complete.

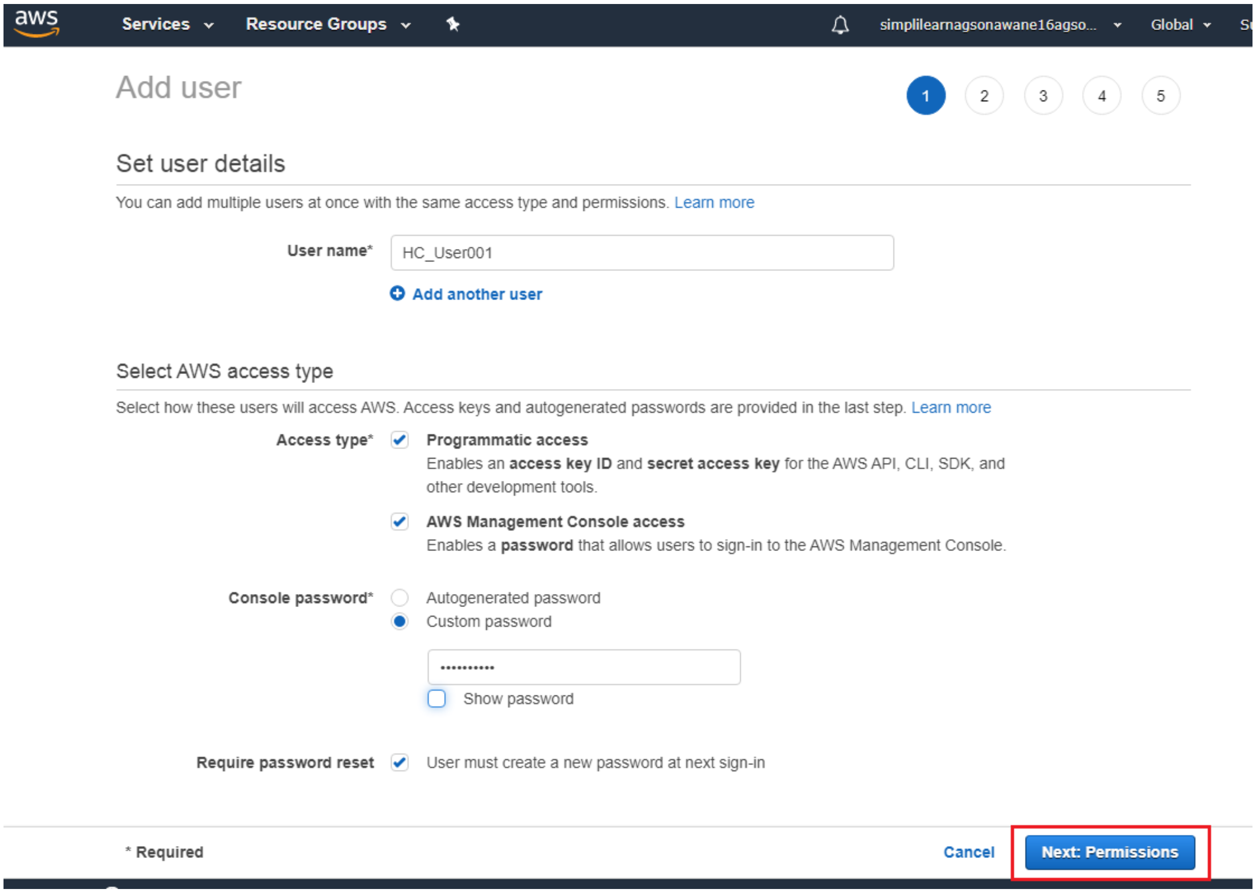
- Activate MFA on your root account
- ✓ Create individual IAM users
- ✓ Use groups to assign permissions
- ✓ Apply an IAM password policy
- ✓ Rotate your access keys

d. Click on **ADD USER**



□	User name	Groups	Access key age	Password age	Last activity
□	simplilearna...	NL_DND_SimplilearnAWSB2C and NL_DND_IAMprotect_nuvelinkrole	✓ 5 days	5 days	Today

e. Under Add user section, provide User Name, Access Type. In this project we are creating user with name "HC_User001" and then click on **Next Permission**



Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* HC_User001

Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

Access type* ☑ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☑ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

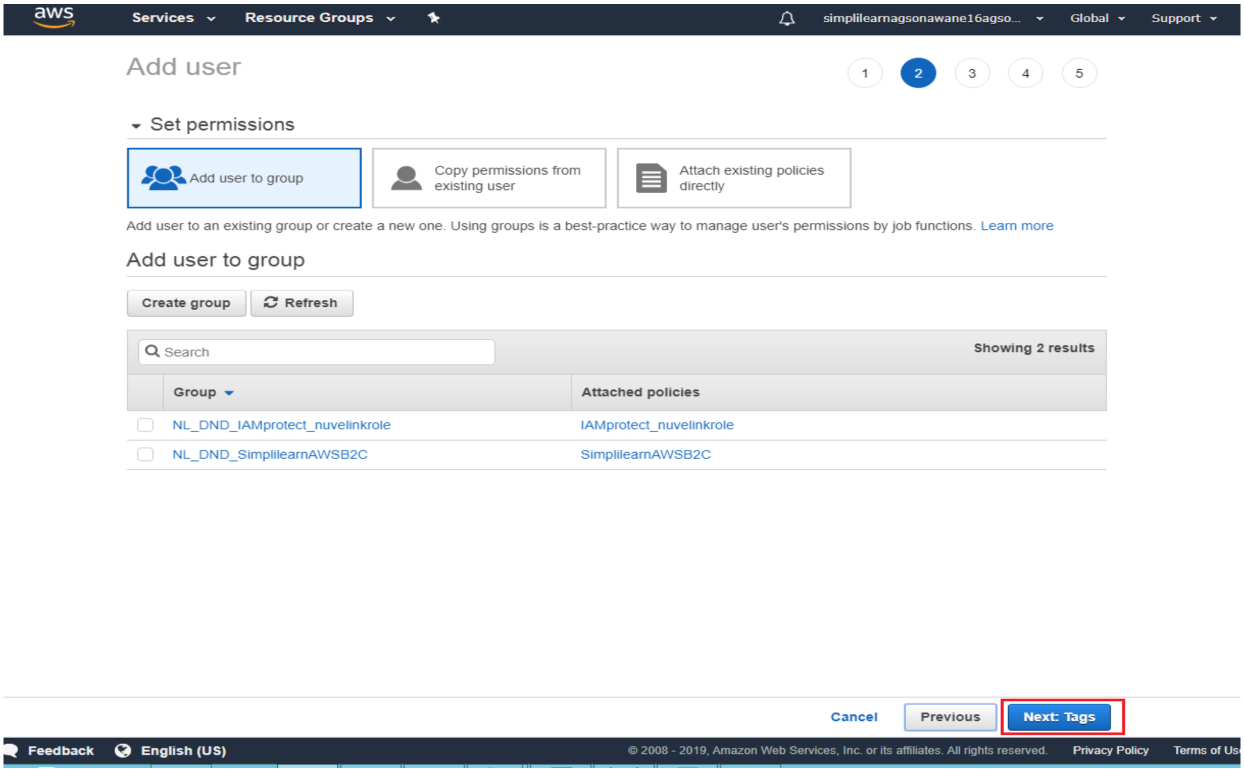
Console password* ○ Autogenerated password
● Custom password

••••••••••
□ Show password

Require password reset ☑ User must create a new password at next sign-in

* Required

f. Under set permission section, we can add user to existing group or even we can create the new group for this user. Or simply attach existing policy directly to this user. After that click on **Next Tag**



Add user

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

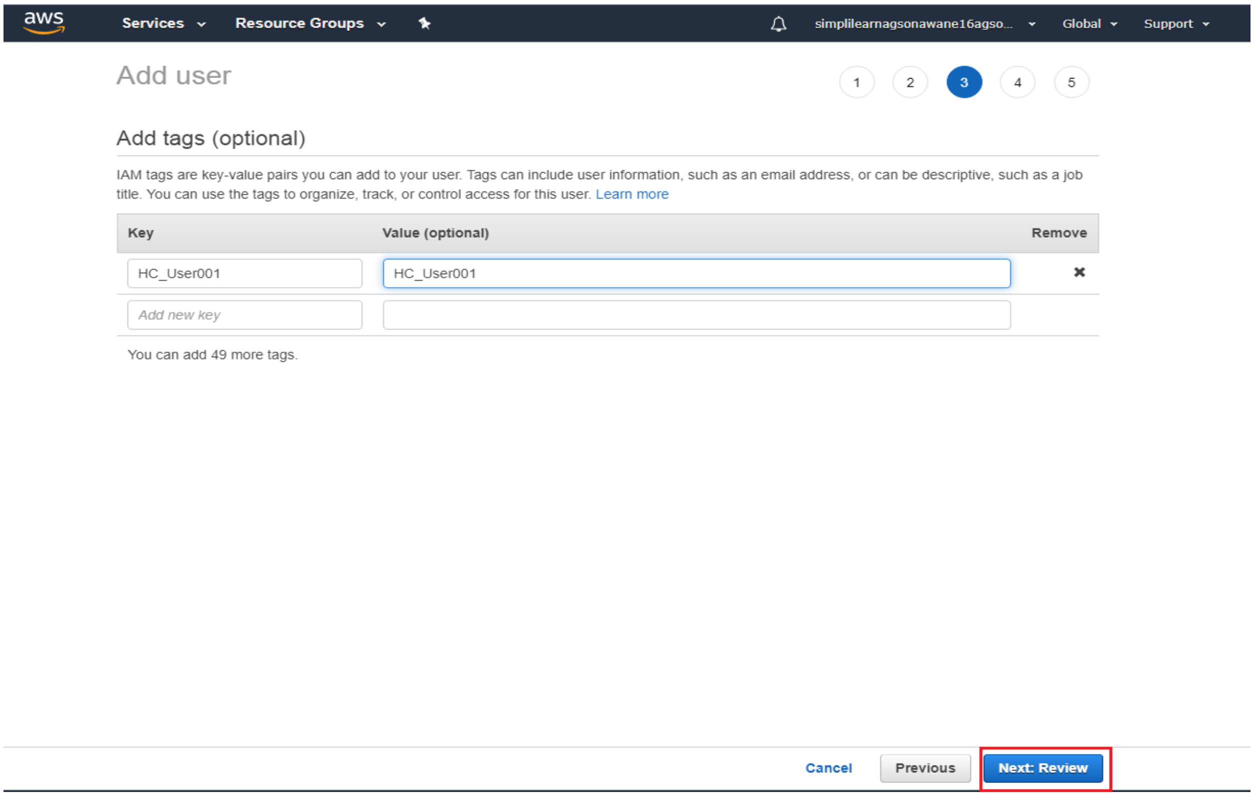
Add user to group

Showing 2 results

	Group	Attached policies
□	NL_DND_IAMprotect_nuvelinkrole	IAMprotect_nuvelinkrole
□	NL_DND_SimplilearnAWSB2C	SimplilearnAWSB2C

© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

g. Under tag section provide key and value. Click on **Review**



Add user

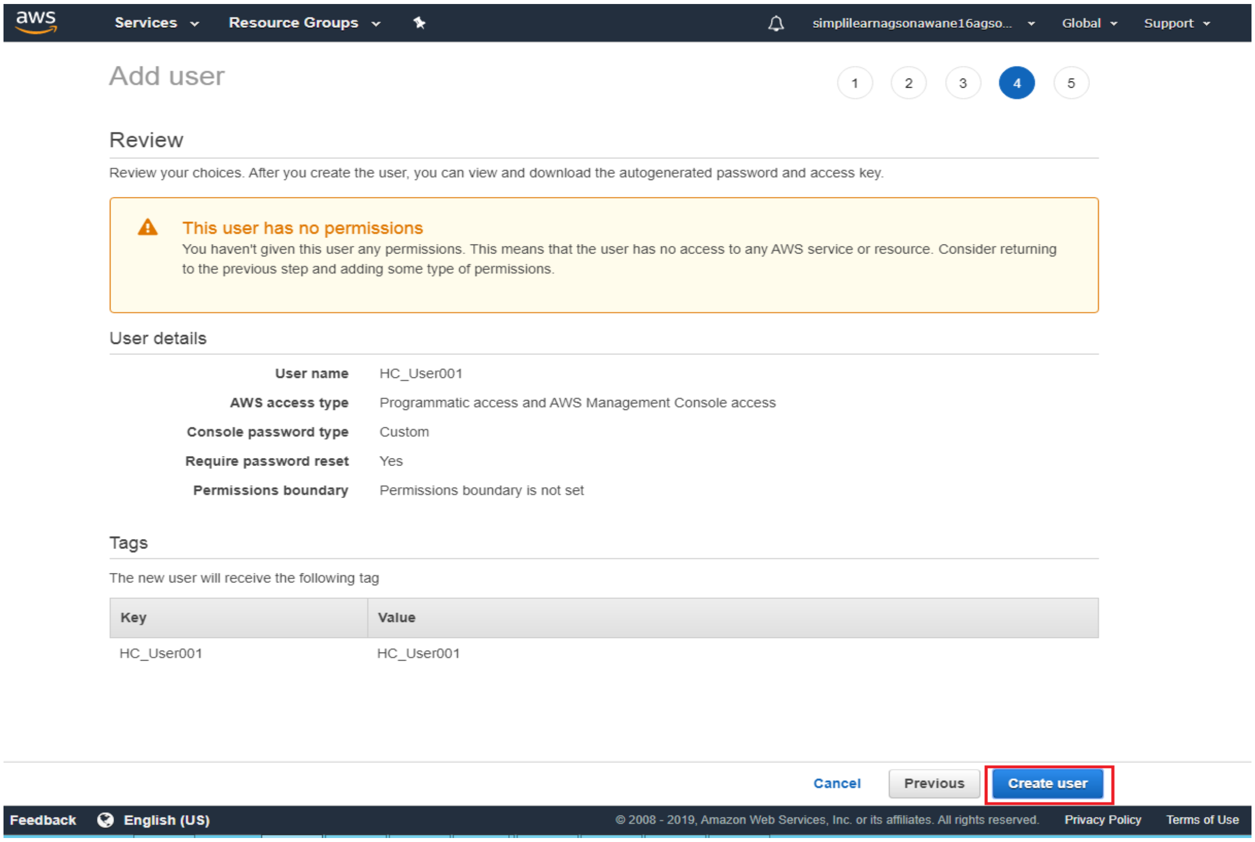
Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. Learn more

Key	Value (optional)	Remove
HC_User001	HC_User001	✖
Add new key		

You can add 49 more tags.

h. Under Review section review the user setting. Click on **Create User**



Add user

Review

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

This user has no permissions

You haven't given this user any permissions. This means that the user has no access to any AWS service or resource. Consider returning to the previous step and adding some type of permissions.

User details

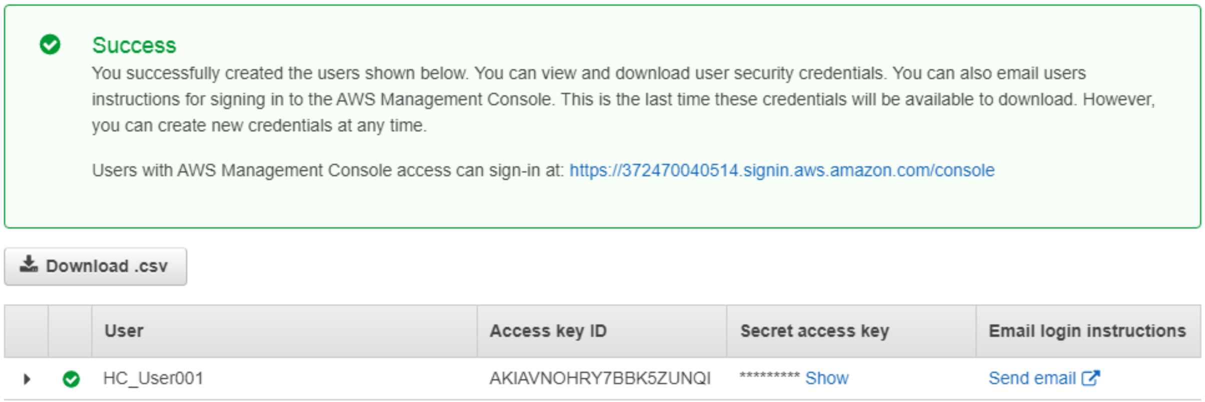
User name	HC_User001
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Tags

The new user will receive the following tag

Key	Value
HC_User001	HC_User001

i. This will display user created section.

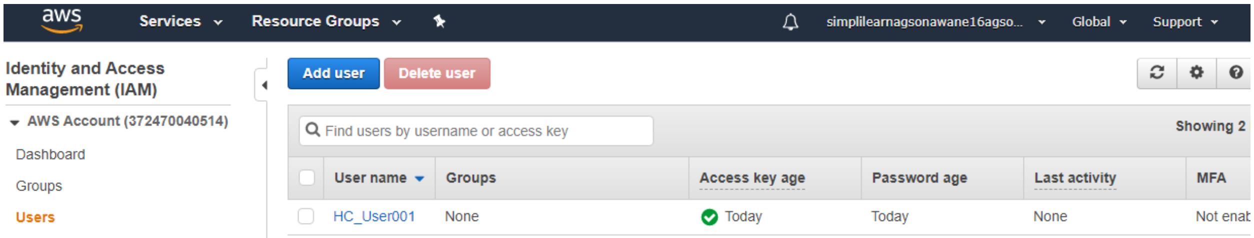


Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://372470040514.signin.aws.amazon.com/console

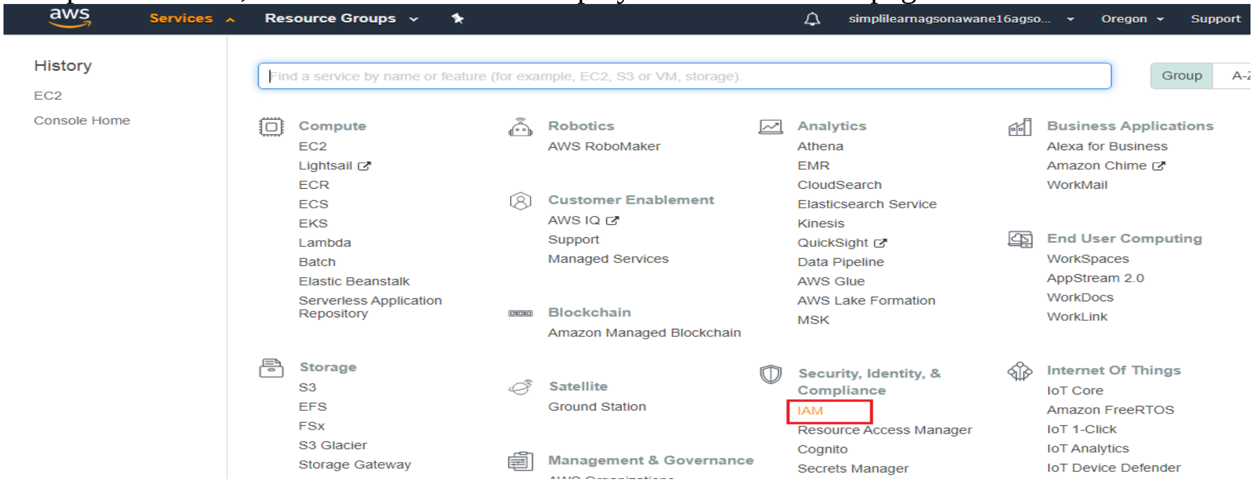
		User	Access key ID	Secret access key	Email login instructions
▸	✓	HC_User001	AKIAVNOHRY7BBK5ZUNQI	********* Show	Send email


aws
Services
Resource Groups
simplilearnagsonawane16agso...
Global
Support
Identity and Access Management (IAM)
AWS Account (372470040514)
Dashboard
Groups
Users
Add user
Delete user
Find users by username or access key
Showing 2

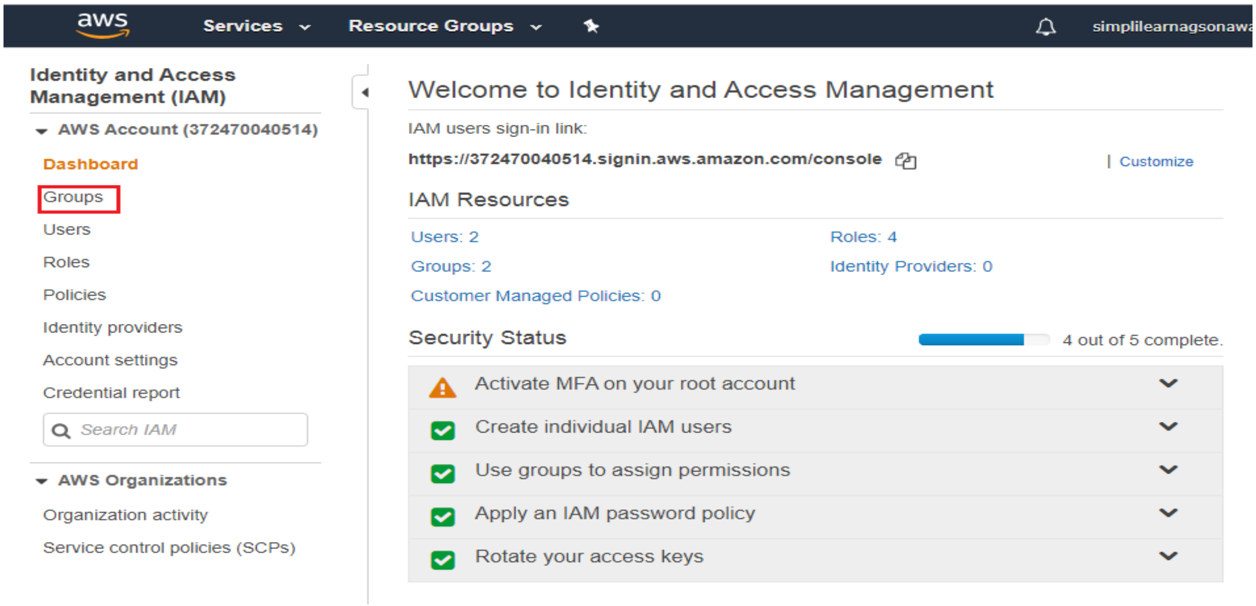
□	User name	Groups	Access key age	Password age	Last activity	MFA
□	HC_User001	None	✓ Today	Today	None	Not enal

2.4 IAM Administrator Group Creation

a. In the AWS Management Console, locate the IAM service icon under the Security, Identity & Compliance. Then, click the IAM icon to display the IAM Console page as shown below.



b. Under Identity and Access Management console click **Groups**



Welcome to Identity and Access Management

IAM users sign-in link:

https://372470040514.signin.aws.amazon.com/console

Customize

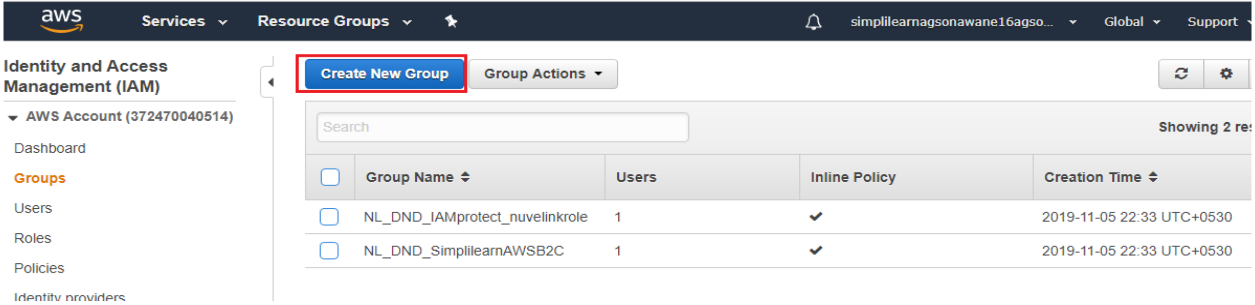
IAM Resources

Users: 2 | Roles: 4
Groups: 2 | Identity Providers: 0
Customer Managed Policies: 0

Security Status — 4 out of 5 complete.

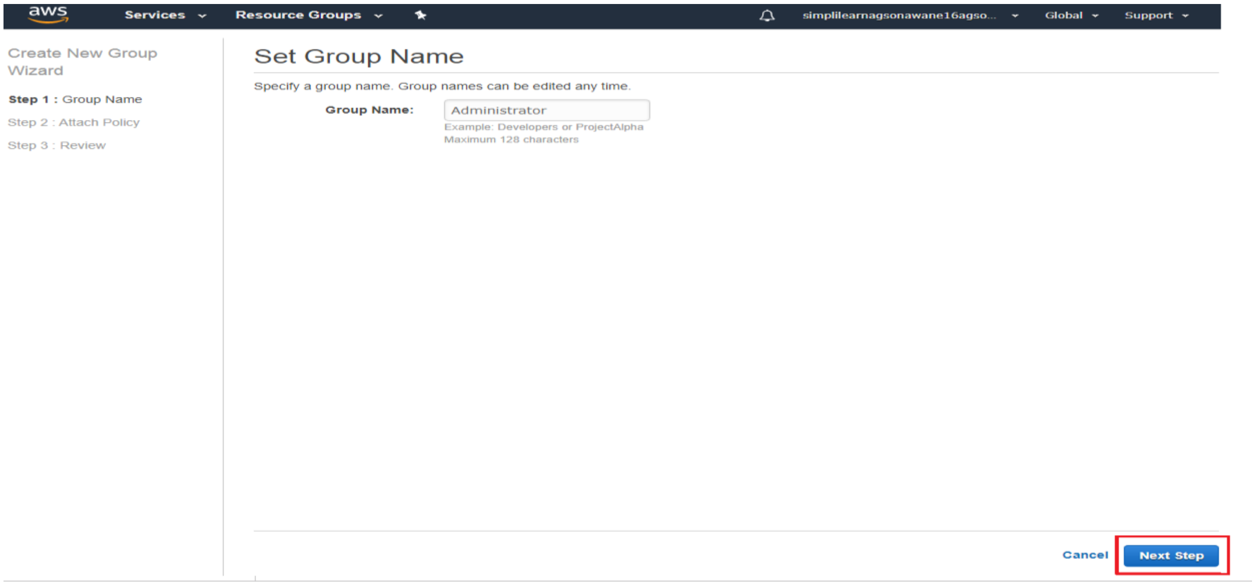
- Activate MFA on your root account
- ✓ Create individual IAM users
- ✓ Use groups to assign permissions
- ✓ Apply an IAM password policy
- ✓ Rotate your access keys

c. Under Gropus section click on **Create New Group**



☐	Group Name	Users	Inline Policy	Creation Time
☐	NL_DND_IAMprotect_nuvelinkrole	1	✓	2019-11-05 22:33 UTC+0530
☐	NL_DND_SimplilearnAWSB2C	1	✓	2019-11-05 22:33 UTC+0530

d. Under Create New Grou wizard, set the new group name. Here we are giving group name as "Administrator". Click on **Next Step.**



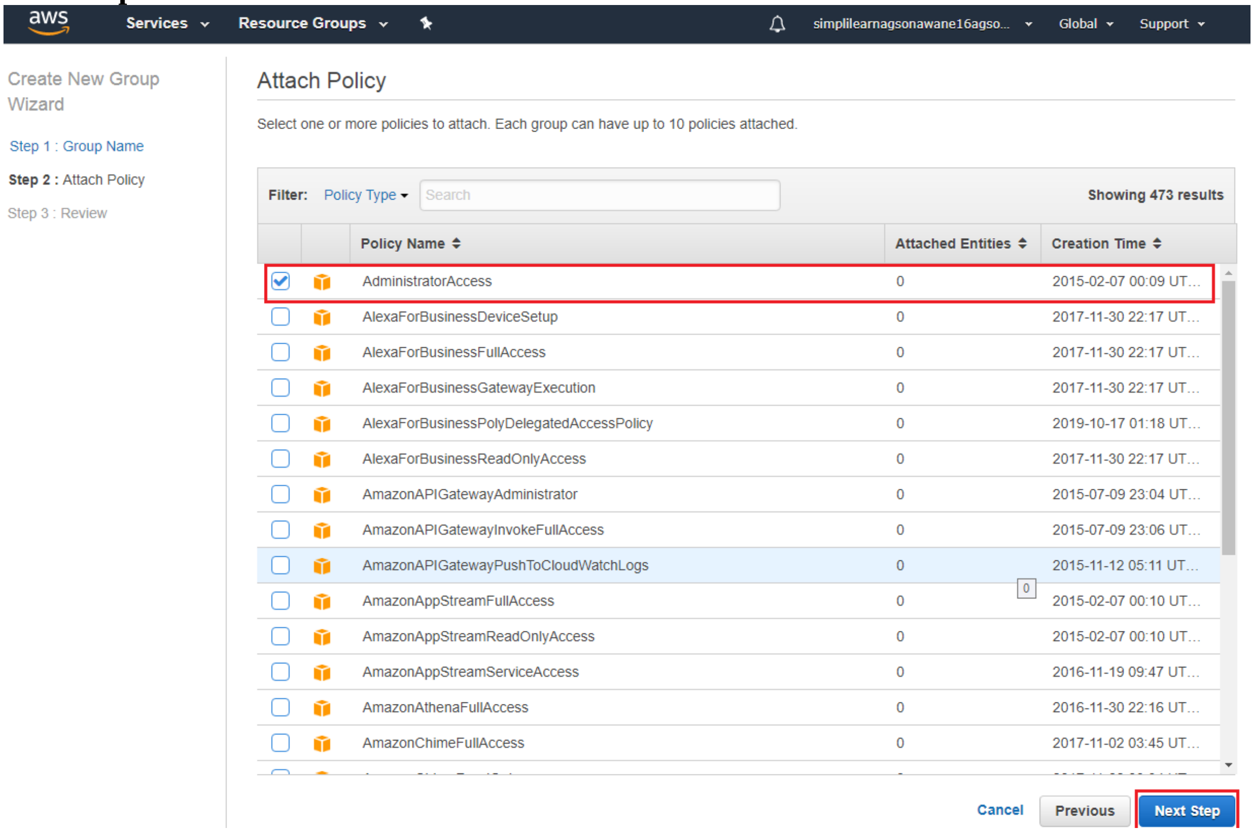
Set Group Name

Specify a group name. Group names can be edited any time.

Group Name: Administrator

Example: Developers or ProjectAlpha
Maximum 128 characters

e. Under attach polciy, select the policy which we need to assign to this gropu. Here we are creating Administrator group hence we have selected the Administrator policy. After selecting policy click **Next Step**



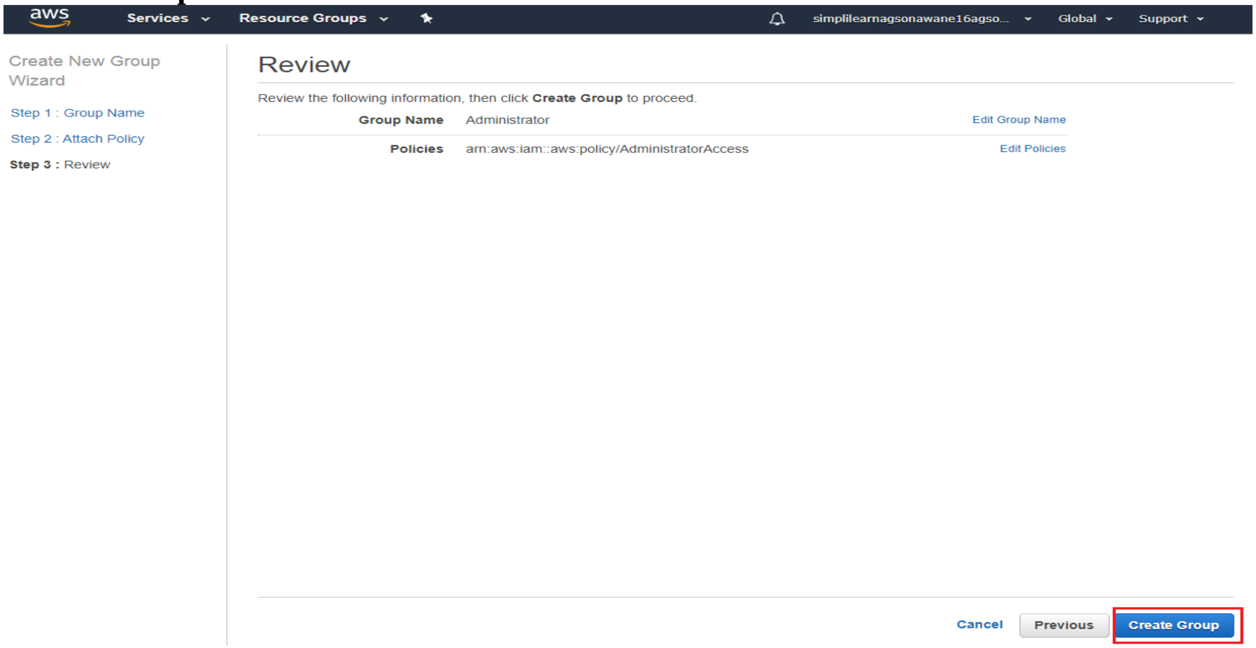
Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Showing 473 results

	Policy Name	Attached Entities	Creation Time
☑	AdministratorAccess	0	2015-02-07 00:09 UT...
□	AlexaForBusinessDeviceSetup	0	2017-11-30 22:17 UT...
□	AlexaForBusinessFullAccess	0	2017-11-30 22:17 UT...
□	AlexaForBusinessGatewayExecution	0	2017-11-30 22:17 UT...
□	AlexaForBusinessPolyDelegatedAccessPolicy	0	2019-10-17 01:18 UT...
□	AlexaForBusinessReadOnlyAccess	0	2017-11-30 22:17 UT...
□	AmazonAPIGatewayAdministrator	0	2015-07-09 23:04 UT...
□	AmazonAPIGatewayInvokeFullAccess	0	2015-07-09 23:06 UT...
□	AmazonAPIGatewayPushToCloudWatchLogs	0	2015-11-12 05:11 UT...
□	AmazonAppStreamFullAccess	0	2015-02-07 00:10 UT...
□	AmazonAppStreamReadOnlyAccess	0	2015-02-07 00:10 UT...
□	AmazonAppStreamServiceAccess	0	2016-11-19 09:47 UT...
□	AmazonAthenaFullAccess	0	2016-11-30 22:16 UT...
□	AmazonChimeFullAccess	0	2017-11-02 03:45 UT...

f. Under Create New group, Review section - review the group name and policies, then click on **Create Group.**

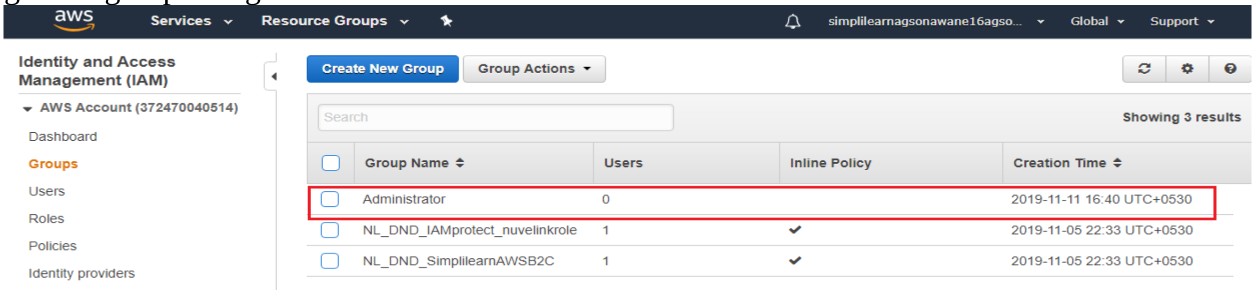


Review

Review the following information, then click **Create Group** to proceed.

Group Name	Administrator
Policies	arn:aws:iam::aws:policy/AdministratorAccess

g. New group will get created and will be shown under user section as below.

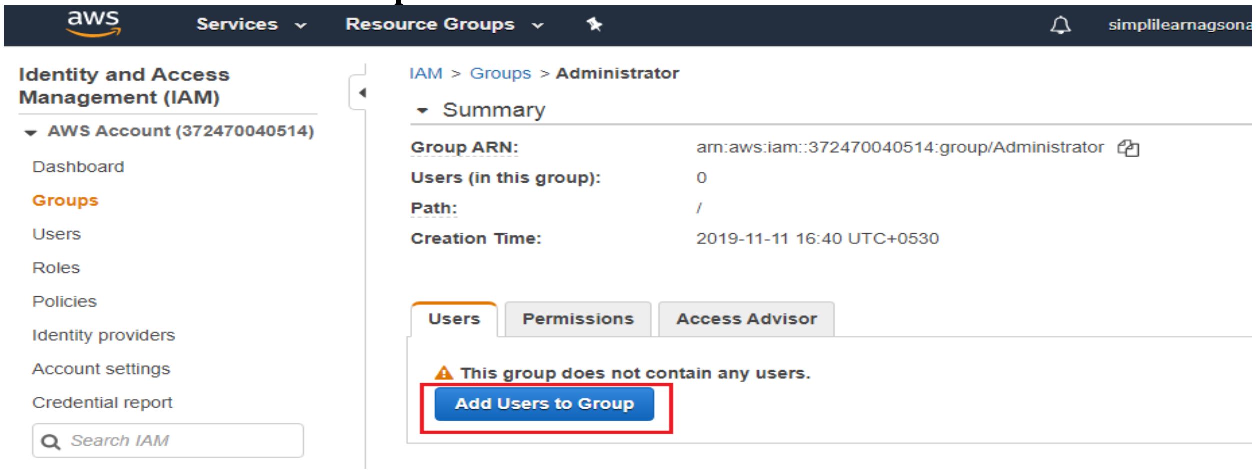


Showing 3 results

□	Group Name	Users	Inline Policy	Creation Time
□	Administrator	0		2019-11-11 16:40 UTC+0530
□	NL_DND_IAMprotect_nuvelinkrole	1	✓	2019-11-05 22:33 UTC+0530
□	NL_DND_SimplilearnAWSB2C	1	✓	2019-11-05 22:33 UTC+0530

2.4.1 Adding User to IAM Administrator Group

a. To Add user to IAM Administrator group, select the Administrator Group from IAM User console, then select **Add User to Group**

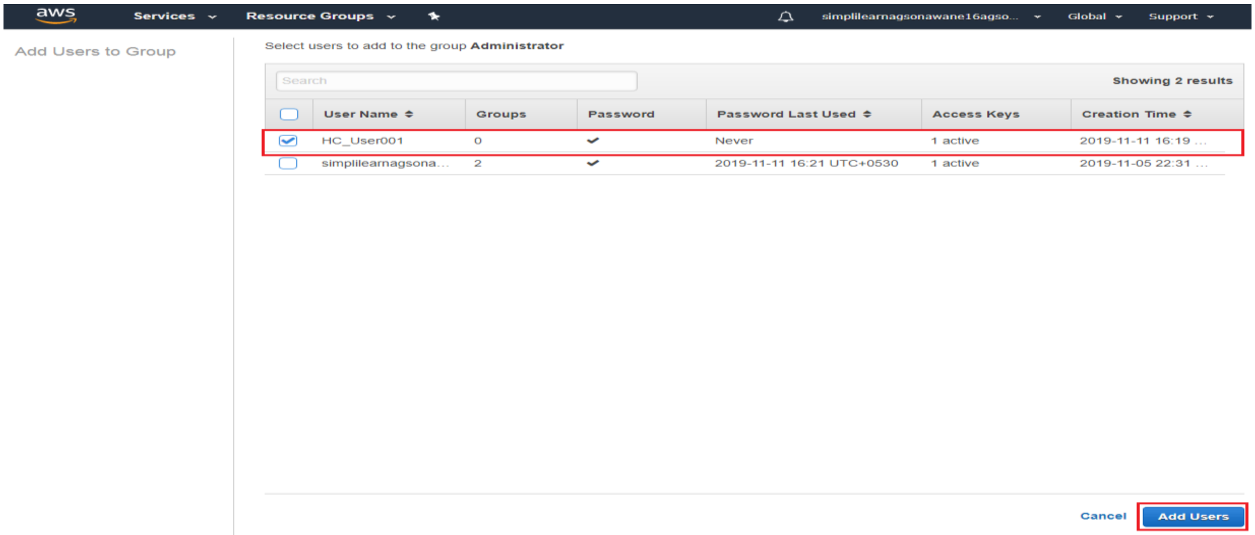


Summary

Group ARN:	arn:aws:iam::372470040514:group/Administrator
Users (in this group):	0
Path:	/
Creation Time:	2019-11-11 16:40 UTC+0530

⚠ This group does not contain any users.

b. To add the user in this group, select the user which we have created earlier i.e. HC_User001 and then click on Add User.

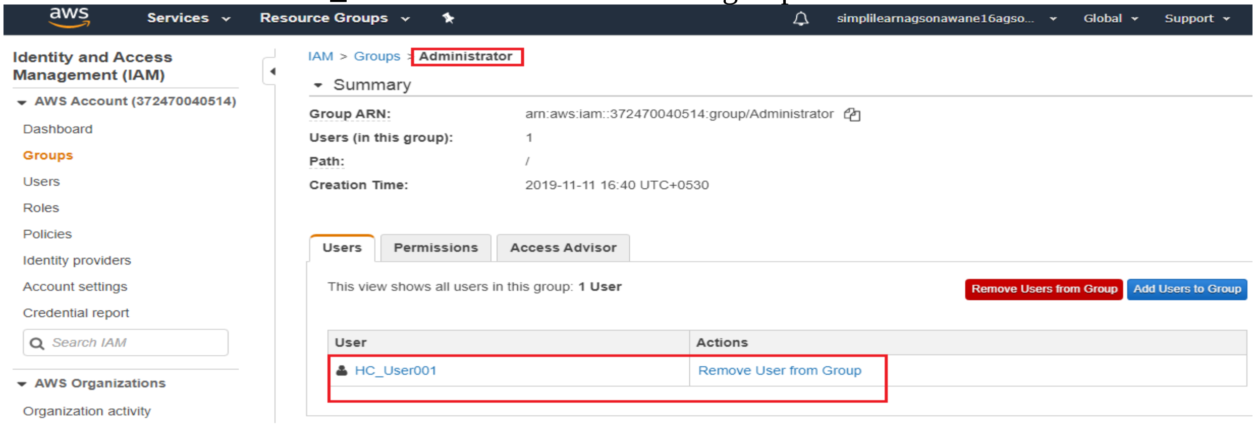


Select users to add to the group **Administrator**

Showing 2 results

	User Name	Groups	Password	Password Last Used	Access Keys	Creation Time
☑	HC_User001	0	✓	Never	1 active	2019-11-11 16:19 ...
□	simplilearnagsona...	2	✓	2019-11-11 16:21 UTC+0530	1 active	2019-11-05 22:31 ...

c. This will add user "HC_User001" in "Administrator" group as shown below.



Summary

Group ARN: arn:aws:iam::372470040514:group/Administrator

Users (in this group): 1

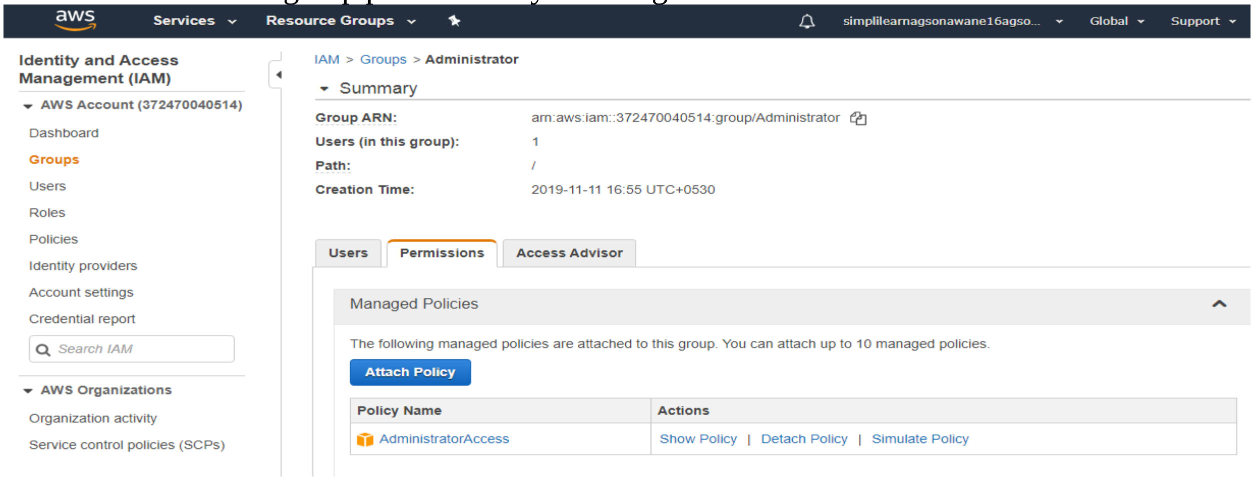
Path: /

Creation Time: 2019-11-11 16:40 UTC+0530

This view shows all users in this group: **1 User**

User	Actions
HC_User001	Remove User from Group

d. We can review the group permission by selecting Permission tab.



Summary

Group ARN: arn:aws:iam::372470040514:group/Administrator

Users (in this group): 1

Path: /

Creation Time: 2019-11-11 16:55 UTC+0530

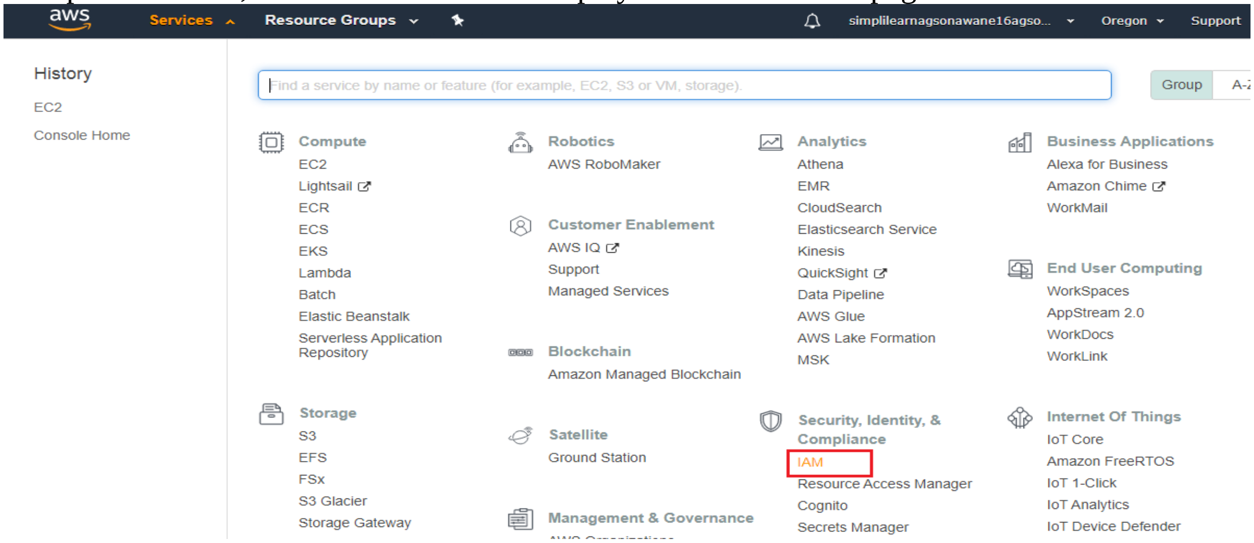
Managed Policies

The following managed policies are attached to this group. You can attach up to 10 managed policies.

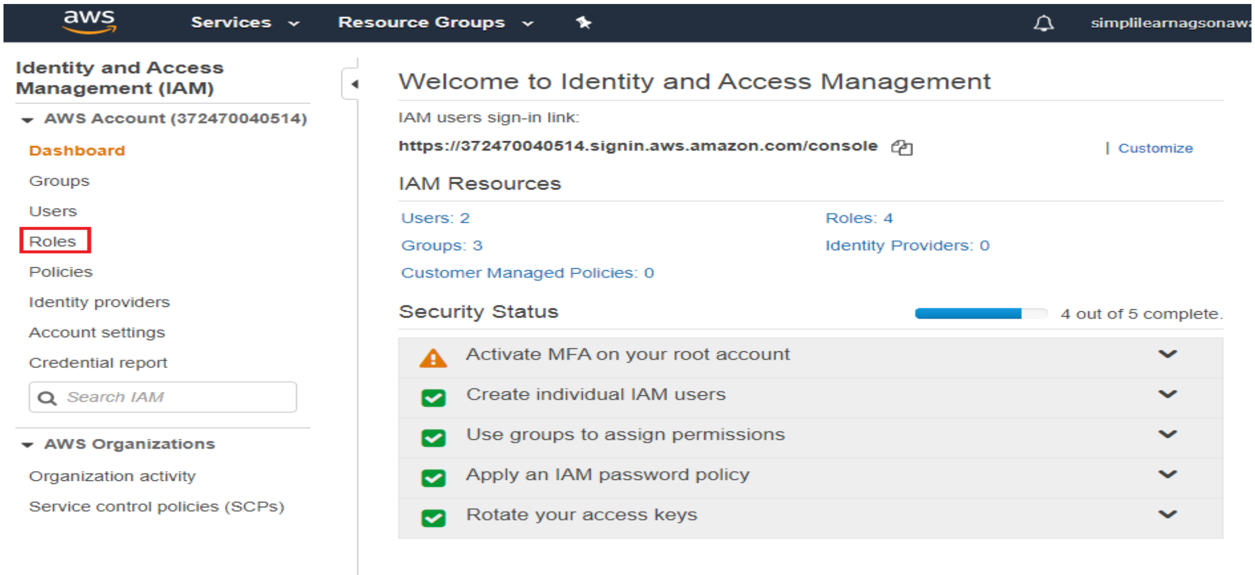
Policy Name	Actions
AdministratorAccess	Show Policy | Detach Policy | Simulate Policy

2.5 Role Creation

a. In the AWS Management Console, locate the IAM service icon under the Security, Identity & Compliance. Then, click the IAM icon to display the IAM Console page as shown below.



b. Under Identity and Access Management console click **Roles**



Welcome to Identity and Access Management

IAM users sign-in link:

https://372470040514.signin.aws.amazon.com/console | Customize

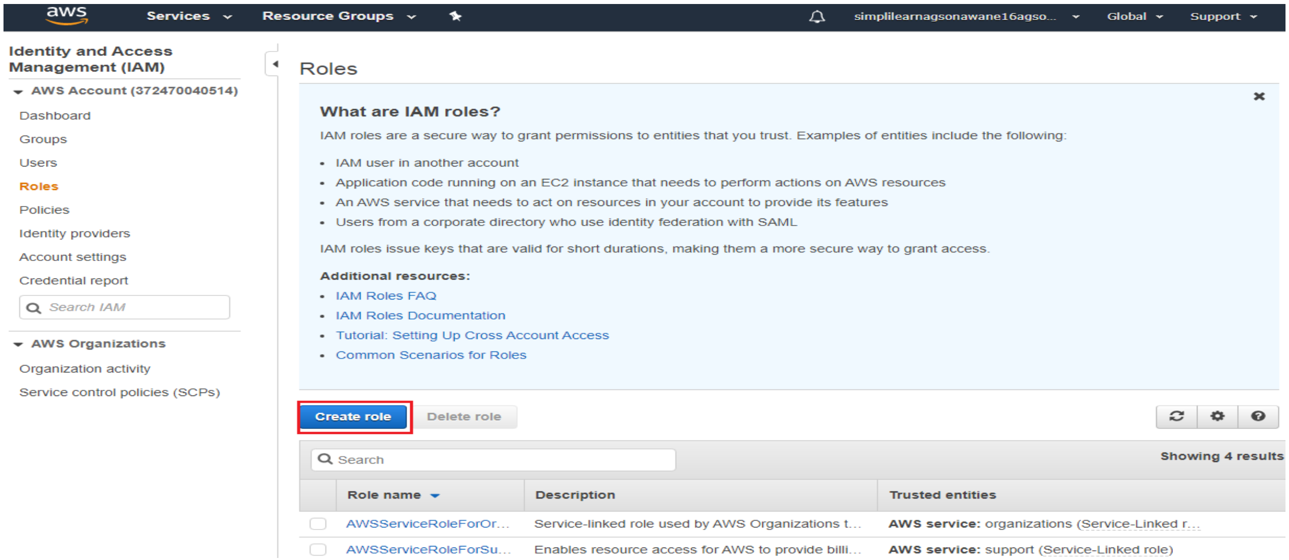
IAM Resources

Users: 2	Roles: 4
Groups: 3	Identity Providers: 0
Customer Managed Policies: 0	

Security Status 4 out of 5 complete.

- ⚠ Activate MFA on your root account
- ✓ Create individual IAM users
- ✓ Use groups to assign permissions
- ✓ Apply an IAM password policy
- ✓ Rotate your access keys

c. Under IAM Role section, click on Create Role



Roles

What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

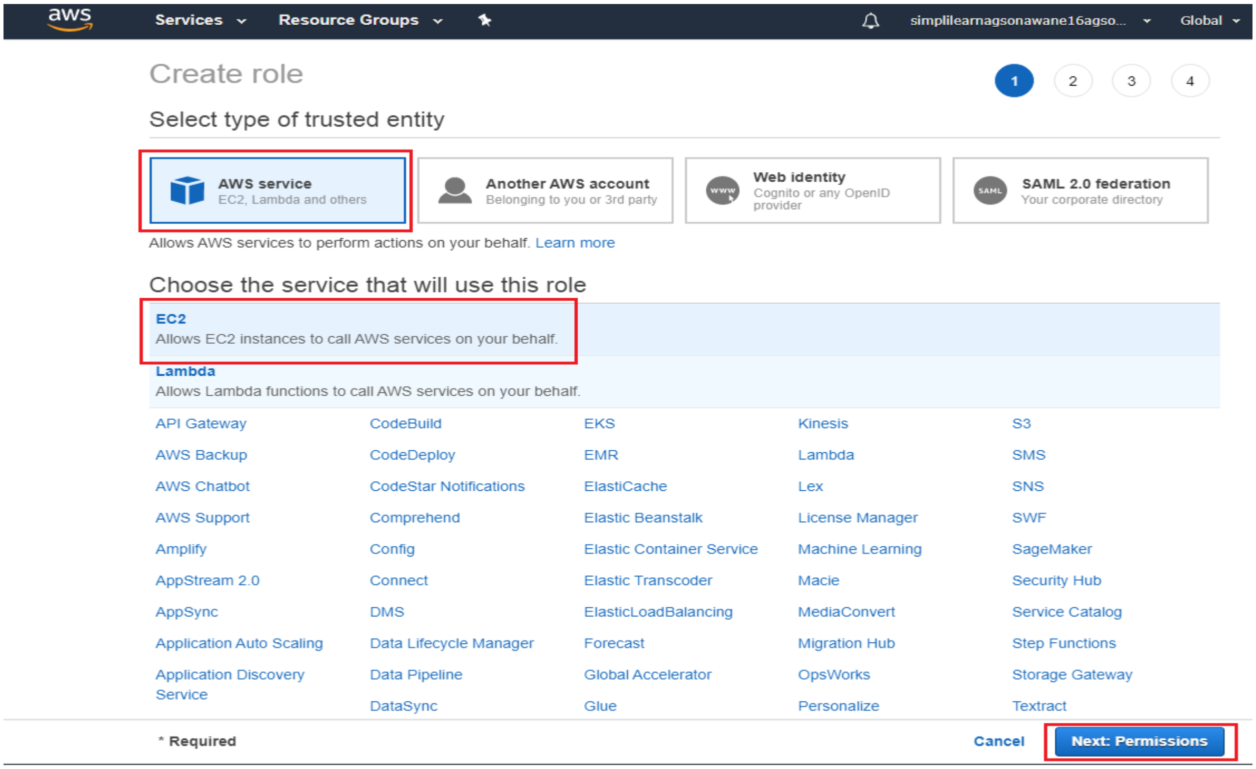
IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

Additional resources:

- IAM Roles FAQ
- IAM Roles Documentation
- Tutorial: Setting Up Cross Account Access
- Common Scenarios for Roles

	Role name	Description	Trusted entities
□	AWSServiceRoleForOr...	Service-linked role used by AWS Organizations t...	**AWS service:** organizations (Service-Linked r...
□	AWSServiceRoleForSu...	Enables resource access for AWS to provide billi...	**AWS service:** support (Service-Linked role)

d. Under Create Role section, select type of trusted entity- "AWS Service" and choose the service that will use this role. Here we have selected EC2 service. Then click on **Next Permissions.**



Create role

Select type of trusted entity

- **AWS service** EC2, Lambda and others
- **Another AWS account** Belonging to you or 3rd party
- **Web identity** Cognito or any OpenID provider
- **SAML 2.0 federation** Your corporate directory

Allows AWS services to perform actions on your behalf. Learn more

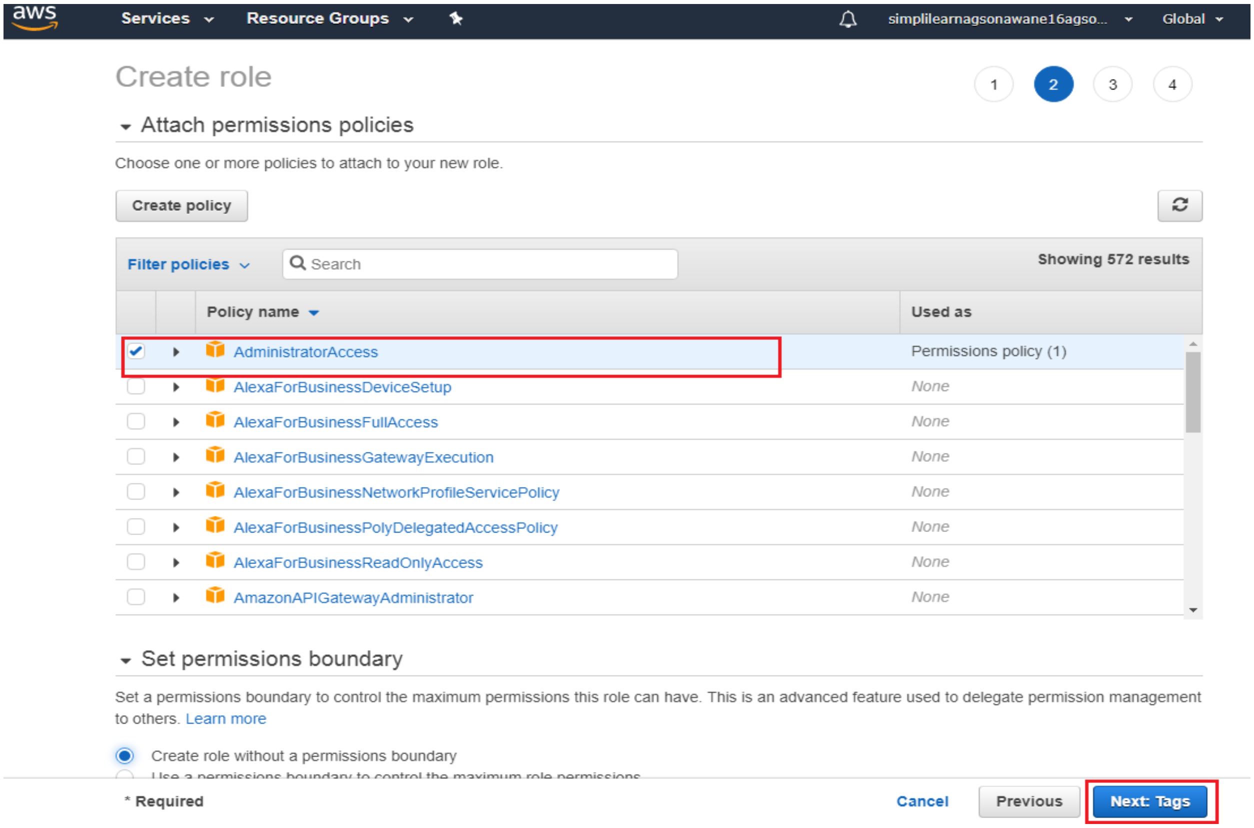
Choose the service that will use this role

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

API Gateway
AWS Backup
AWS Chatbot
AWS Support
Amplify
AppStream 2.0
AppSync
Application Auto Scaling
Application Discovery Service
CodeBuild
CodeDeploy
CodeStar Notifications
Comprehend
Config
Connect
DMS
Data Lifecycle Manager
Data Pipeline
DataSync
EKS
EMR
ElastiCache
Elastic Beanstalk
Elastic Container Service
Elastic Transcoder
ElasticLoadBalancing
Forecast
Global Accelerator
Glue
Kinesis
Lambda
Lex
License Manager
Machine Learning
Macie
MediaConvert
Migration Hub
OpsWorks
Personalize
S3
SMS
SNS
SWF
SageMaker
Security Hub
Service Catalog
Step Functions
Storage Gateway
Textract

e. Under Cerate role section, select the policy which need to assign tot his role. Here we have selected Administrator policy. Them Click **Next Tags**



Create role

Attach permissions policies

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

Showing 572 results

		Policy name	Used as
☑	▸	AdministratorAccess	Permissions policy (1)
□	▸	AlexaForBusinessDeviceSetup	None
□	▸	AlexaForBusinessFullAccess	None
□	▸	AlexaForBusinessGatewayExecution	None
□	▸	AlexaForBusinessNetworkProfileServicePolicy	None
□	▸	AlexaForBusinessPolyDelegatedAccessPolicy	None
□	▸	AlexaForBusinessReadOnlyAccess	None
□	▸	AmazonAPIGatewayAdministrator	None

Set permissions boundary

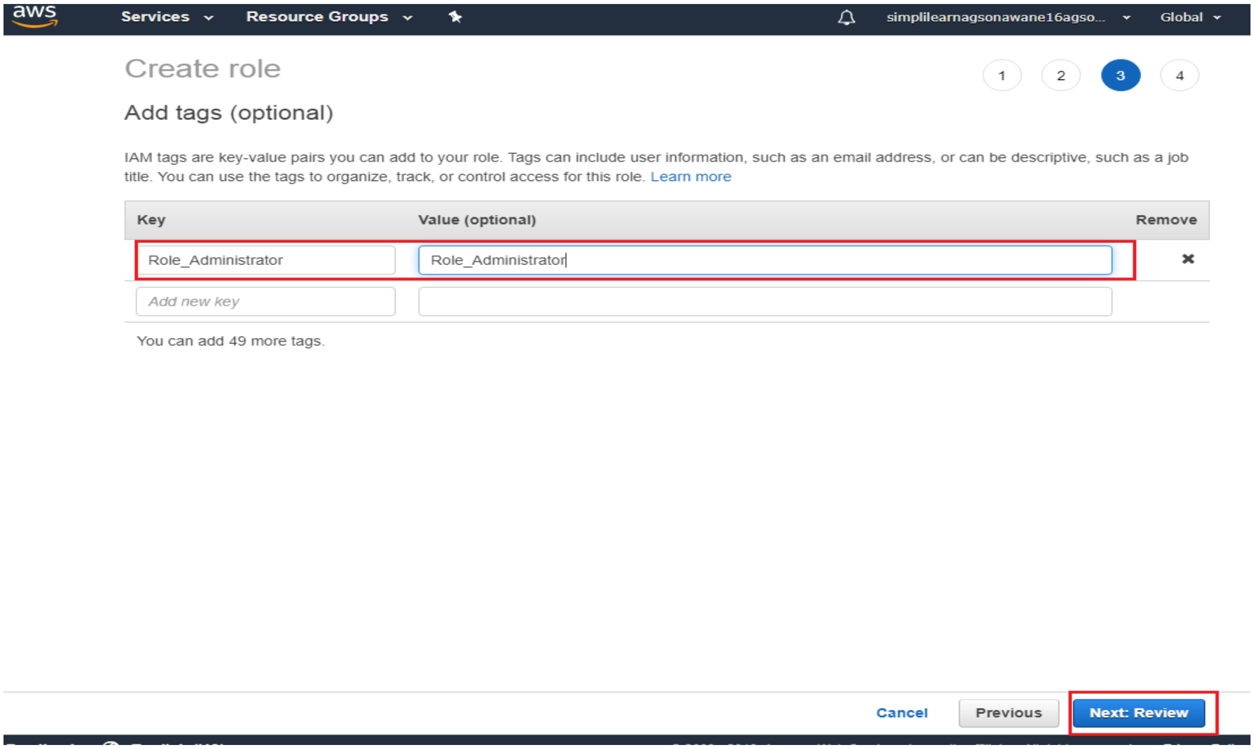
Set a permissions boundary to control the maximum permissions this role can have. This is an advanced feature used to delegate permission management to others. Learn more

● Create role without a permissions boundary

○ Use a permissions boundary to control the maximum role permissions

* Required

f. Under Create Role- Add tag section, enter key and value. Click on **Next:Review.**



Create role

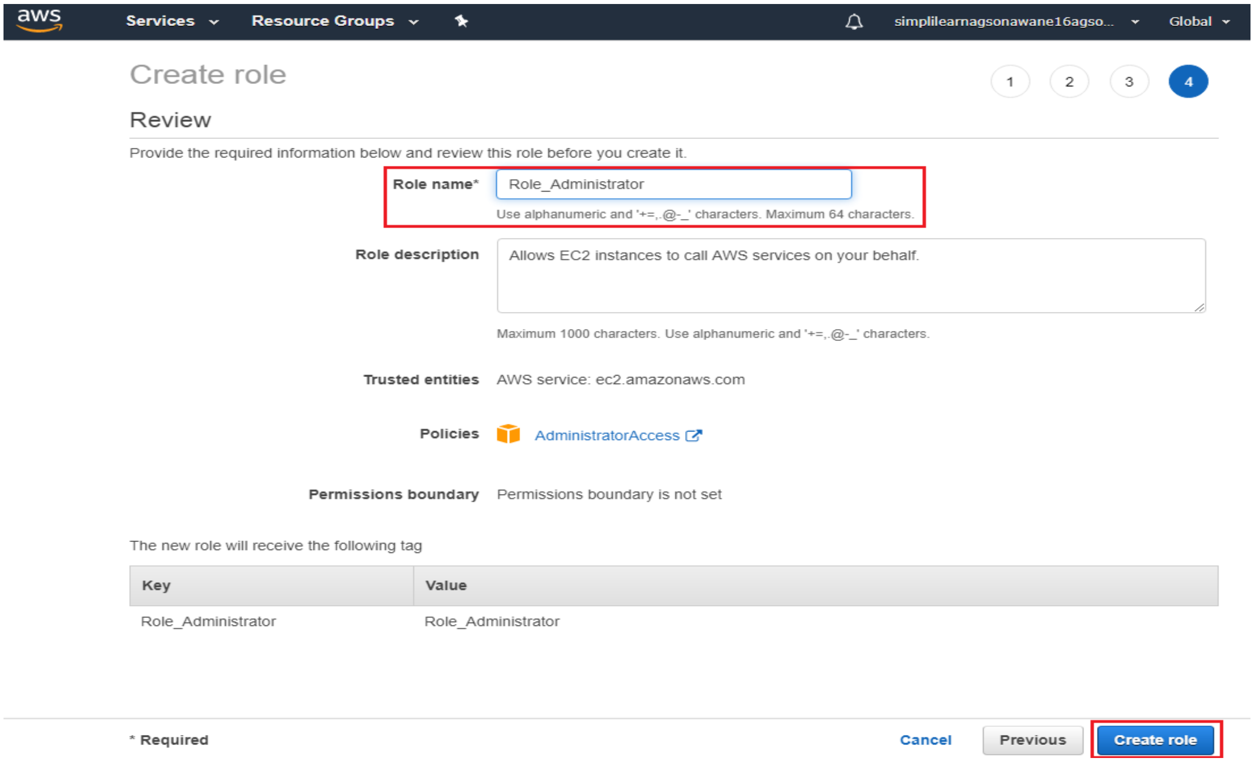
Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. Learn more

Key	Value (optional)	Remove
Role_Administrator	Role_Administrator	✖
Add new key		

You can add 49 more tags.

g. Under Create Role-Review section, review the role configuration. Tehn select Create role.



Create role

Review

Provide the required information below and review this role before you create it.

Role name* Role_Administrator

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

Role description Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies AdministratorAccess

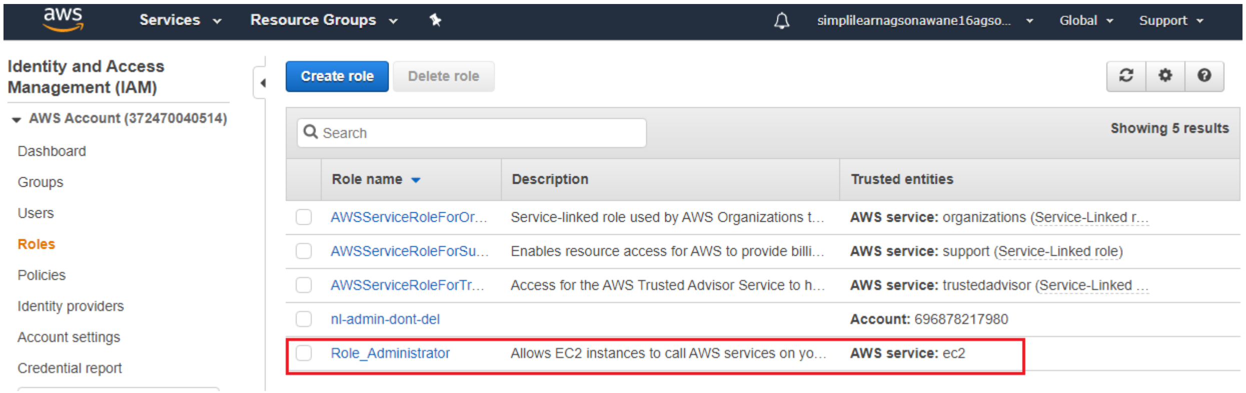
Permissions boundary Permissions boundary is not set

The new role will receive the following tag

Key	Value
Role_Administrator	Role_Administrator

* Required

h. Newly Create role will be shown on Role console.



Showing 5 results

	Role name	Description	Trusted entities
□	AWSServiceRoleForOr...	Service-linked role used by AWS Organizations t...	**AWS service:** organizations (Service-Linked r...
□	AWSServiceRoleForSu...	Enables resource access for AWS to provide billi...	**AWS service:** support (Service-Linked role)
□	AWSServiceRoleForTr...	Access for the AWS Trusted Advisor Service to h...	**AWS service:** trustedadvisor (Service-Linked ...
□	nl-admin-dont-del		**Account:** 696878217980
□	Role_Administrator	Allows EC2 instances to call AWS services on yo...	**AWS service:** ec2