Project Details

In this project, I am going to meet the following objectives.

1.Check CPU utilization of EC2 instance.

2.Create an alarm for CPU utilization.

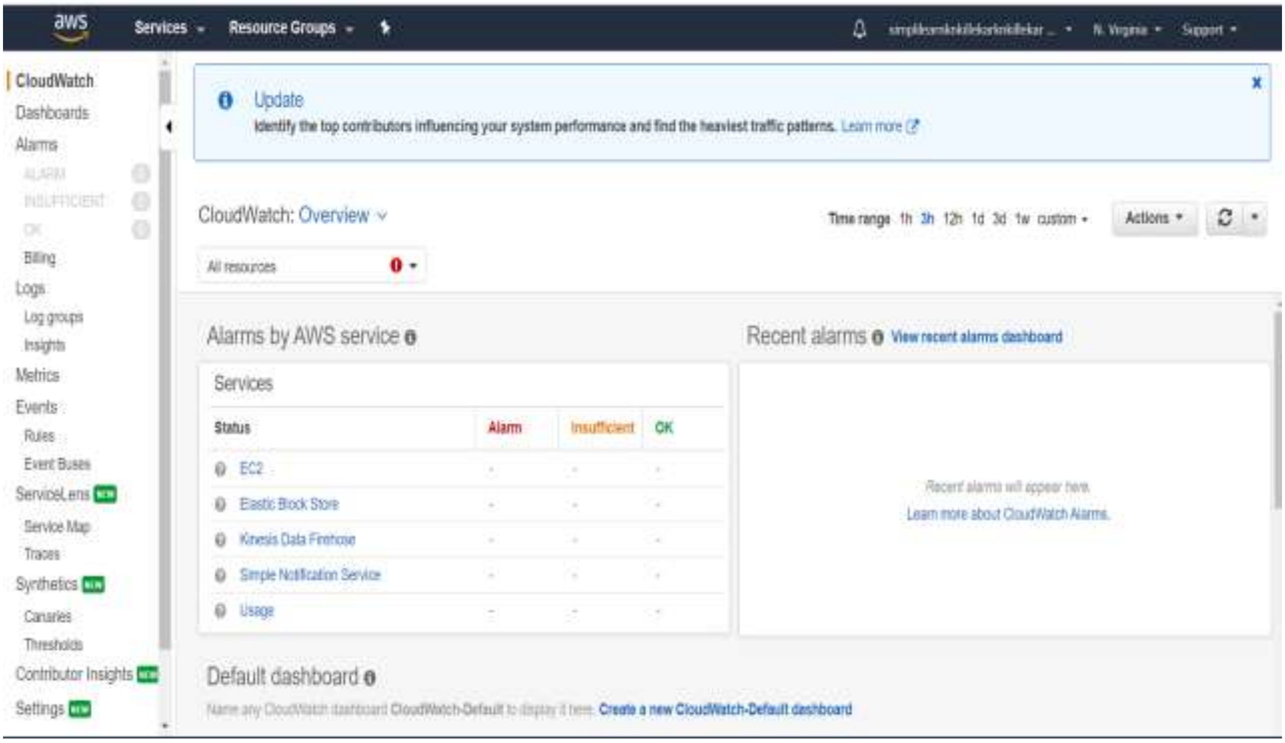
3.Create IAM user.

4.Create the IAM Administrator group and add user to IAM Administrator group.

5.Create role.

1. Check the CPU Utilization.

Step 1: Open AWS management console, click on Services. Go to Management & Governance and click on CloudWatch. Following window will appear.



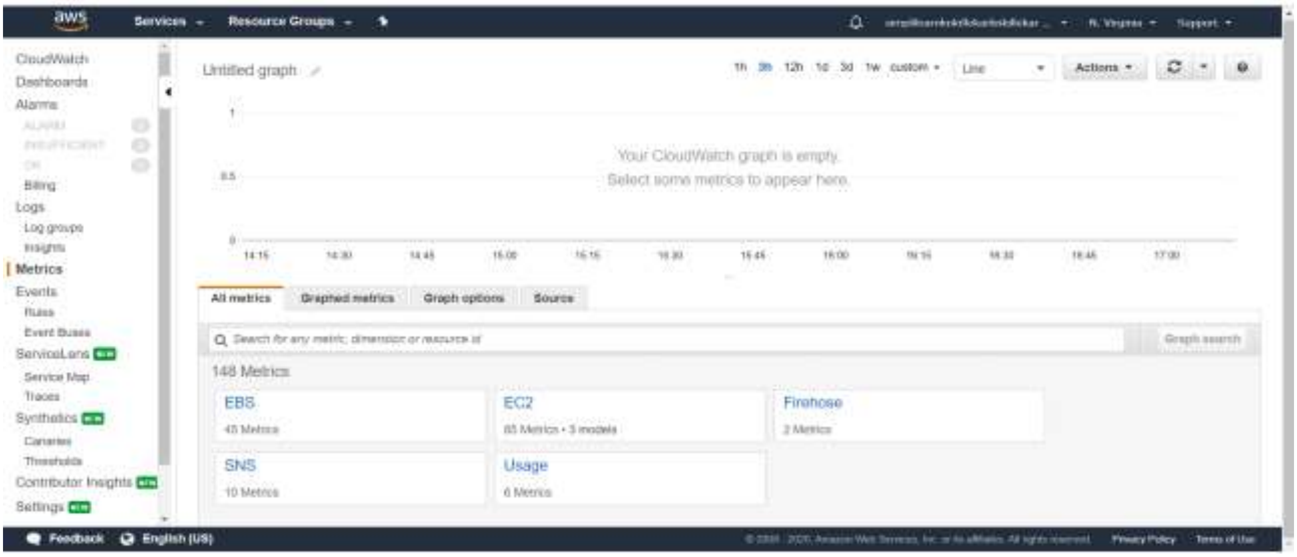
Identify the top contributors influencing your system performance and find the heaviest traffic patterns. Learn more

Status	Alarm	Insufficient	OK
EC2	-	-	-
Elastic Block Store	-	-	-
Kinesis Data Firehose	-	-	-
Simple Notification Service	-	-	-
Usage	-	-	-

Recent alarms will appear here.
Learn more about CloudWatch Alarms.

Name any CloudWatch dashboard CloudWatch-Default to display it here. Create a new CloudWatch-Default dashboard

Step 2: Next click on Metrics on left navigation pane following window will appear.



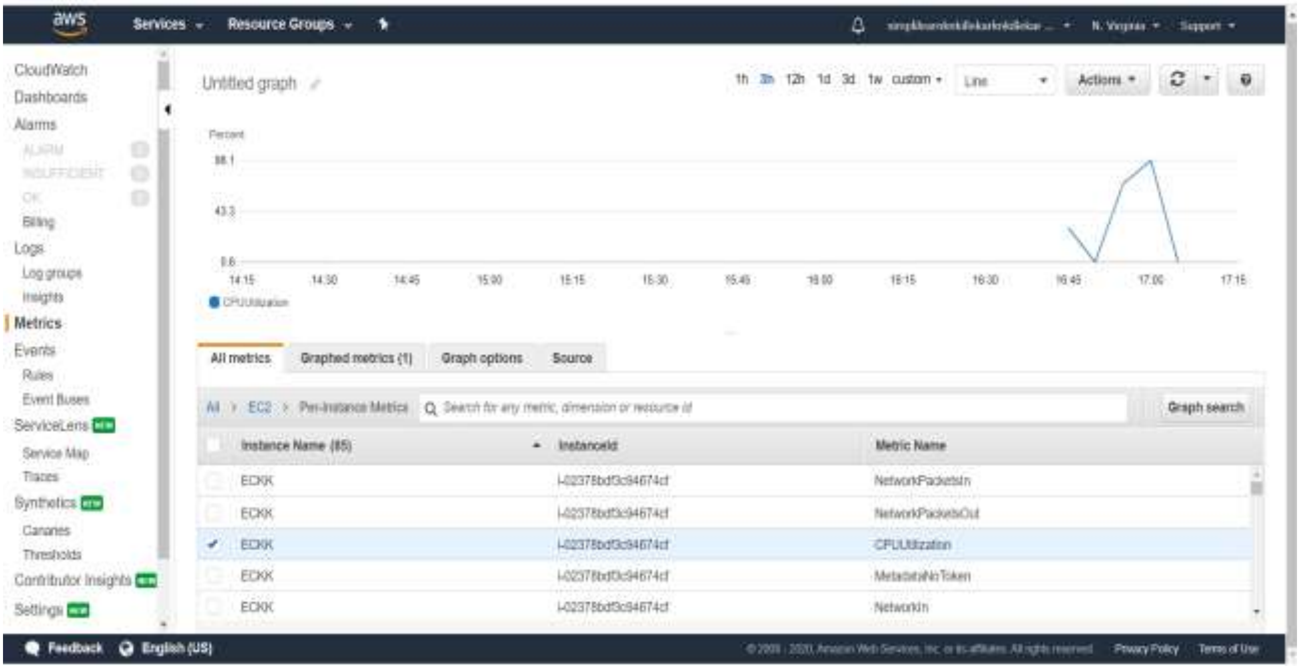
Your CloudWatch graph is empty.
Select some metrics to appear here.

Search for any metric, dimension or resource id

148 Metrics

EBS 45 Metrics	EC2 85 Metrics • 3 models	Firehose 2 Metrics
SNS 10 Metrics	Usage 6 Metrics	

Step 3: Click on EC2 and then click on Per-Instance metrics. From Per-instance metrics select Instance Name as ECKK and Metric Name as CPUUtilization which displays the graph as shown below.



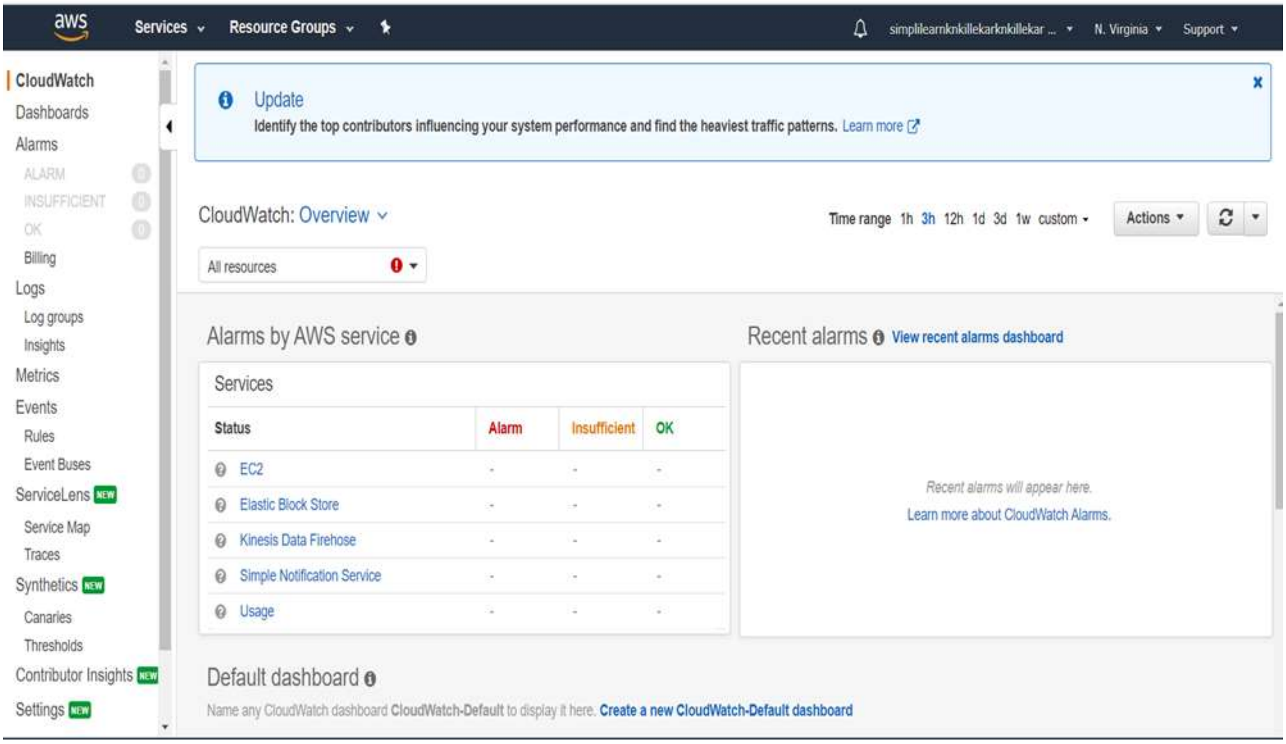
All > EC2 > Per-Instance Metrics

Search for any metric, dimension or resource id

	Instance Name (85)	InstanceId	Metric Name
□	ECKK	i-02378bdf3c94674cf	NetworkPacketsIn
□	ECKK	i-02378bdf3c94674cf	NetworkPacketsOut
✓	ECKK	i-02378bdf3c94674cf	CPUUtilization
□	ECKK	i-02378bdf3c94674cf	MetadataNoToken
□	ECKK	i-02378bdf3c94674cf	NetworkIn

2. Create an Alarm.

Step 1: Open AWS management console, click on Services. Go to Management & Governance and click on CloudWatch. Following window will appear.



Update

Identify the top contributors influencing your system performance and find the heaviest traffic patterns. Learn more

Alarms by AWS service

Services

Status	Alarm	Insufficient	OK
EC2	-	-	-
Elastic Block Store	-	-	-
Kinesis Data Firehose	-	-	-
Simple Notification Service	-	-	-
Usage	-	-	-

Recent alarms View recent alarms dashboard

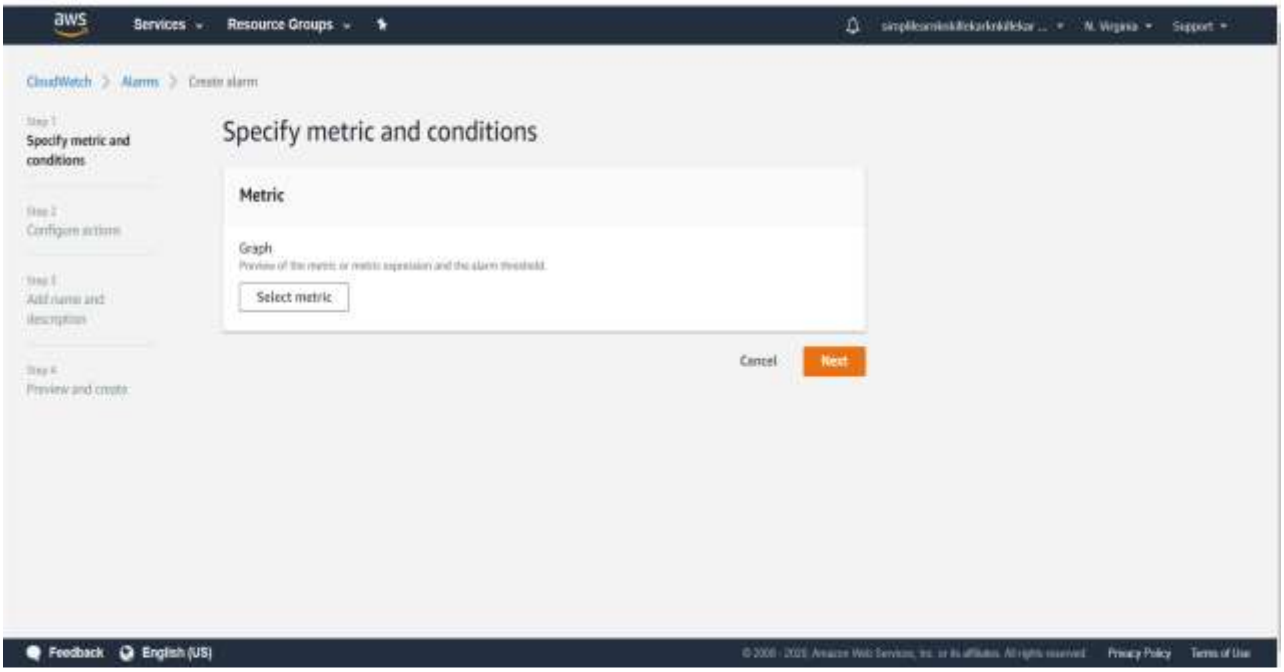
Recent alarms will appear here.

Learn more about CloudWatch Alarms.

Default dashboard

Name any CloudWatch dashboard CloudWatch-Default to display it here. Create a new CloudWatch-Default dashboard

Step 2: Next click on Alarms and then click on create alarm following window will appear.



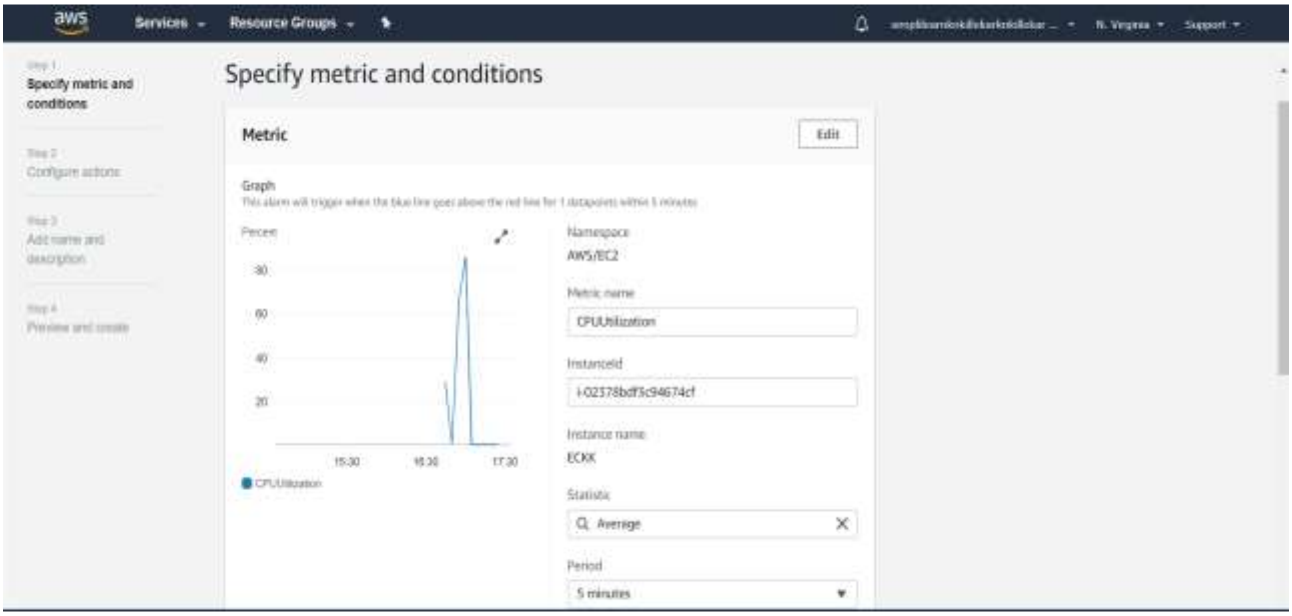
Specify metric and conditions

Metric

Graph

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

Step 3: Next click on EC2 and then click on Per-Instance metrics. From Per-instance metrics select Instance Name as ECKK and Metric Name as CPUUtilization and click on select metric following window will appear.



Specify metric and 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

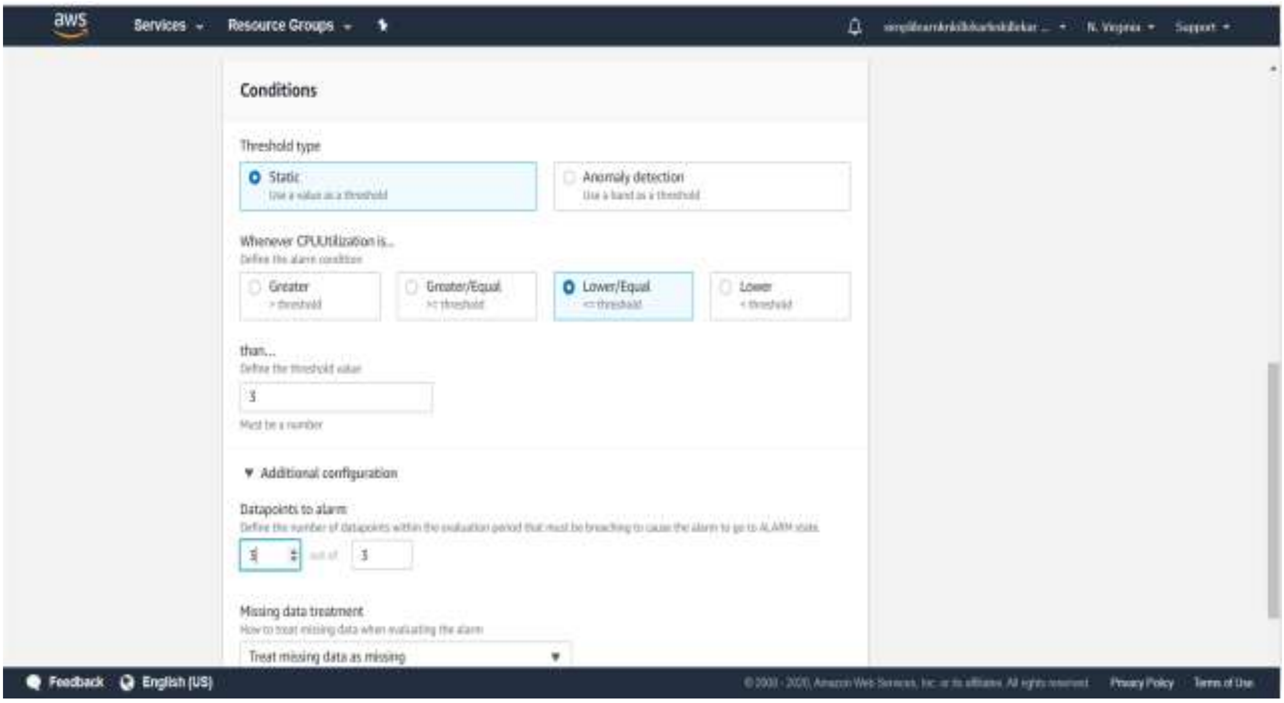
InstanceId: i-02378bdf5c94674cf

Instance name: ECKK

Statistic: Average

Period: 5 minutes

Step 4: Then set the threshold type to static ,select whenever CPUUtilization to <= threshold, threshold value=3 and datapoints to alarm=3, as shown below and 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

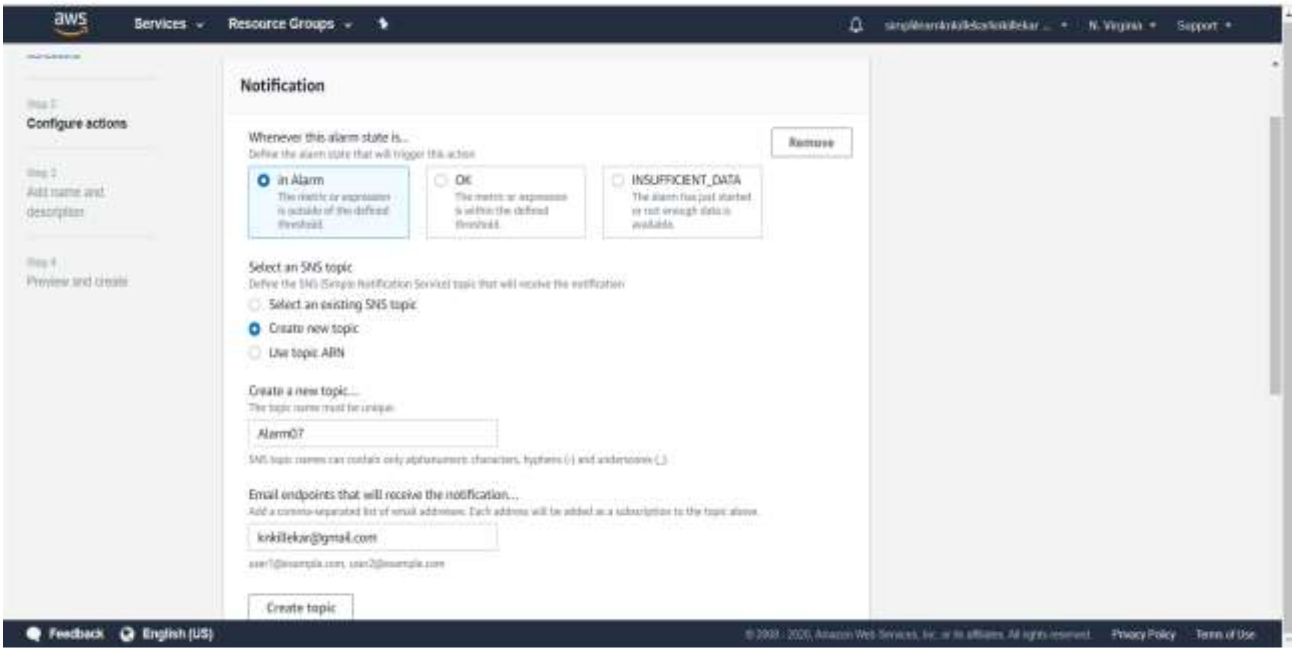
Datapoints to alarm
Define the number of datapoints within the evaluation period that must be breaching to cause the alarm to go to ALARM state.

3 out of 3

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

Treat missing data as missing

Step 5: Following window will appear and select the options as shown in the window. Create new topic as Alarm07 and Email endpoints that will receive the notification to knkillekar@gmail.com as shown below and click on 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

Create a new topic...

The topic name must be unique.

Alarm07

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

Email endpoints that will receive the notification...

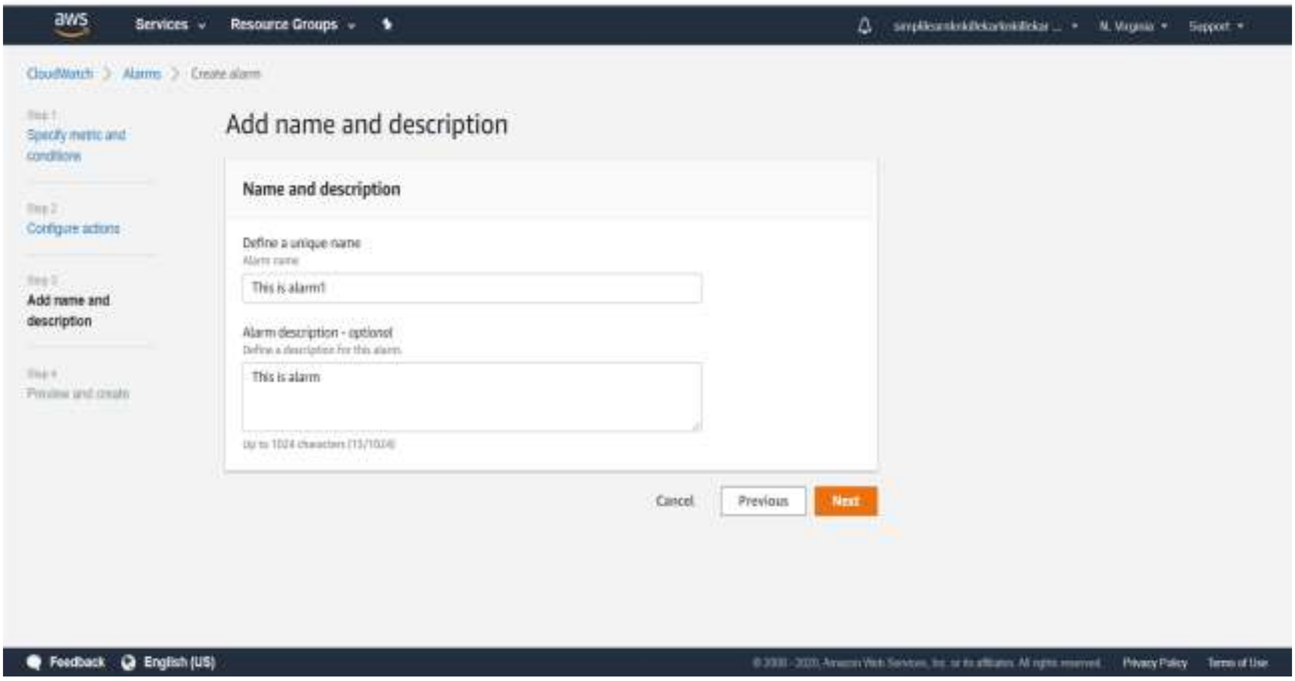
Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

knkillekar@gmail.com

user1@example.com, user2@example.com

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step 6: A window of Add name and description will appear and enter the details as shown below and click on next.



Add name and description

Name and description

Define a unique name

Alarm name

This is alarm1

Alarm description - optional

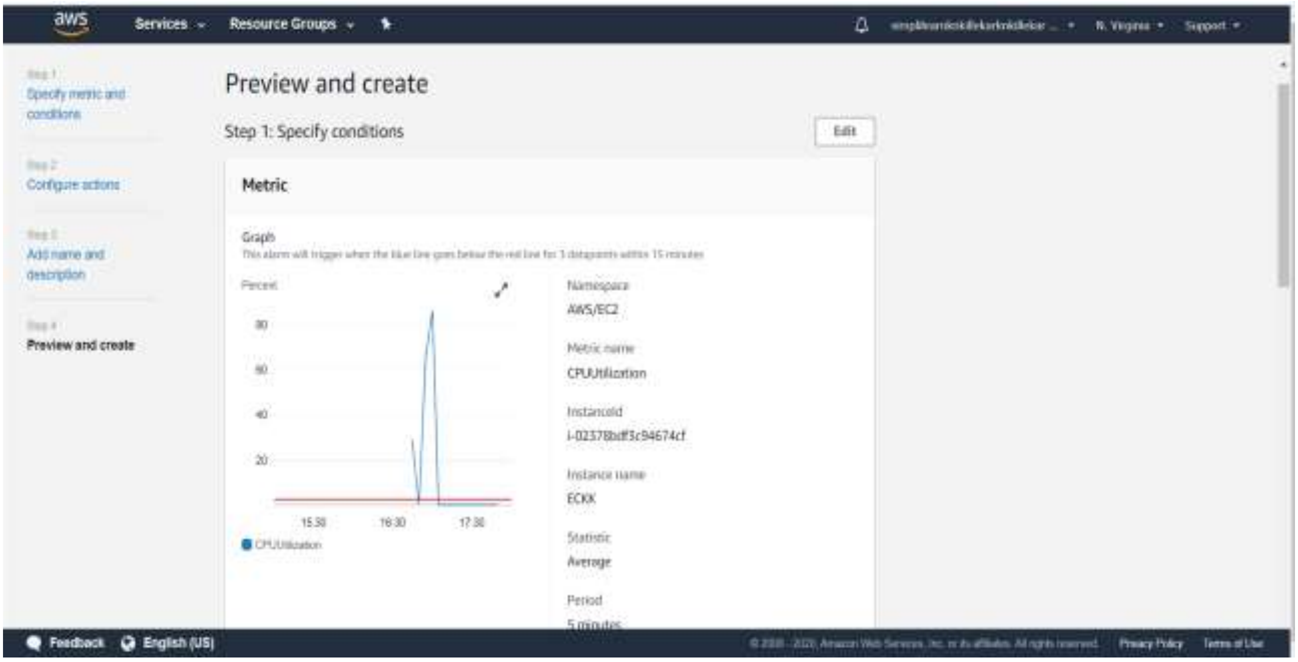
Define a description for this alarm.

This is alarm

Up to 1024 characters (13/1024)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step 7: Preview and create window will appear and click on create alarm as shown below.



Preview and create

Step 1: Specify conditions

Metric

Graph

This alarm will trigger when the blue line goes below the red line for 3 datapoints within 15 minutes

Namespace
AWS/EC2

Metric name
CPUUtilization

InstanceId
i-02378bdf3c94674cf

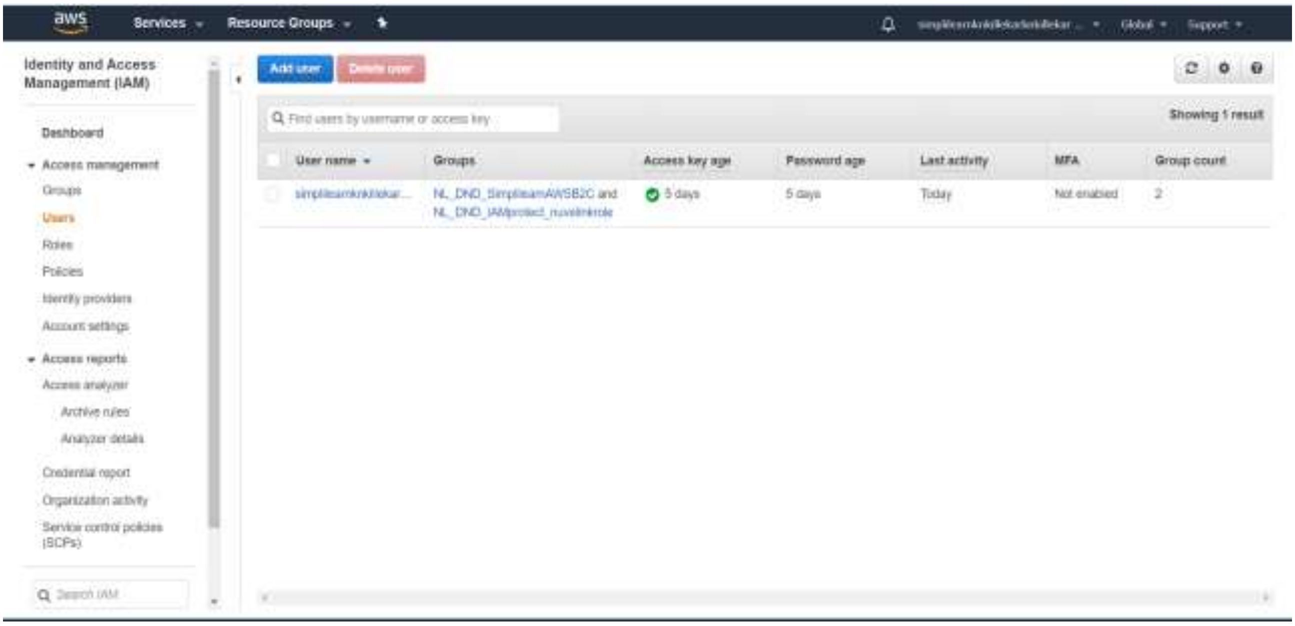
Instance name
ECKK

Statistic
Average

Period
5 minutes

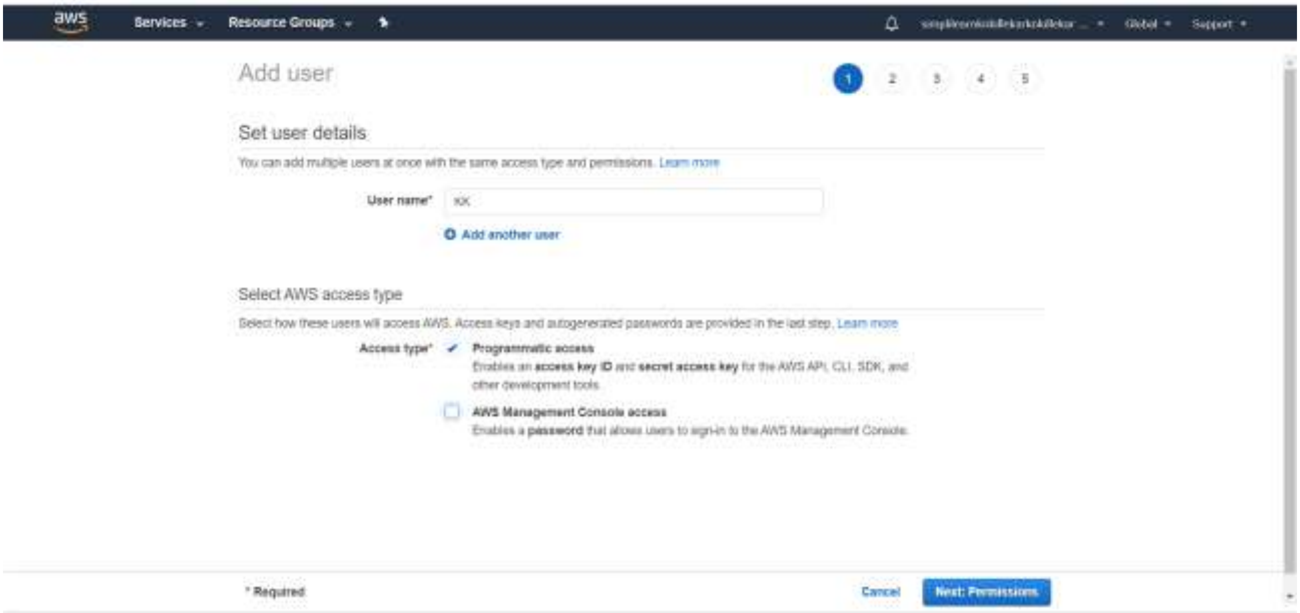
3. Create an IAM User.

Step 1: Open AWS management console, click on Services. Go to Security, Identity, & Compliance and click on IAM. Then from left navigation pane select Users option following window will appear as shown below.



User name	Groups	Access key age	Password age	Last activity	MFA	Group count
simplilearnknkilokar...	NL_DND_SimplilearnAWSB2C and NL_DND_IAMprotect_nuvelinkrole	✓ 5 days	5 days	Today	Not enabled	2

Step 2: Next click on Add user and enter the User name as "KK" and select the option Access type as "Programmatic access" as shown below and click on Next: Permissions.



Set user details

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

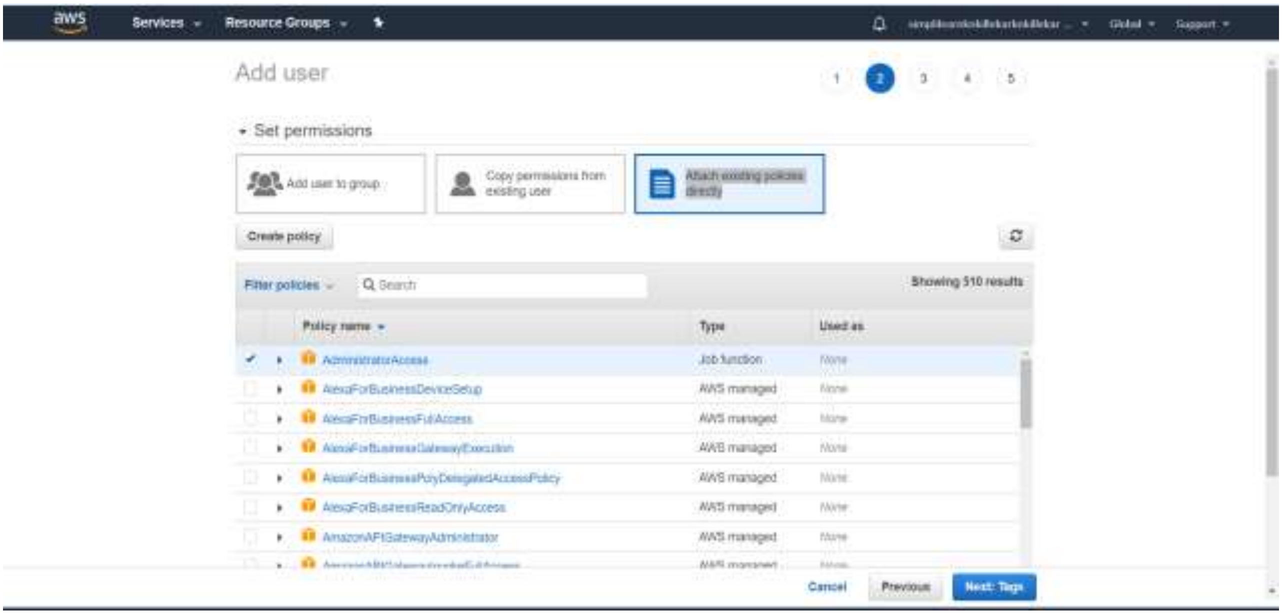
User name* KK

Select AWS access type

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

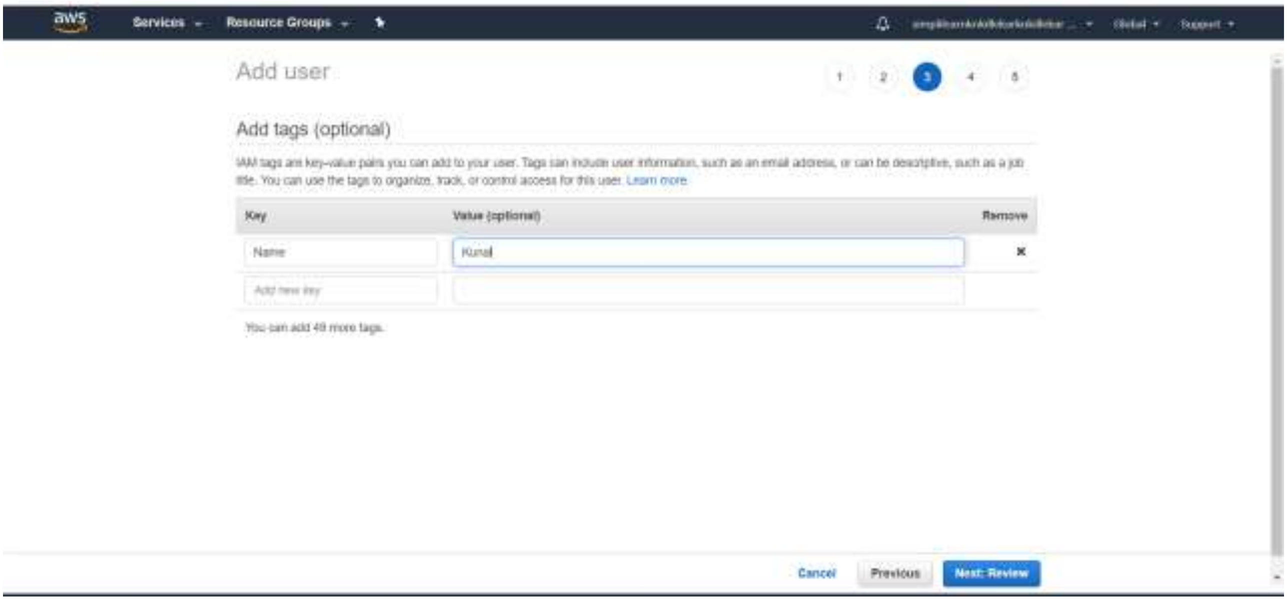
Access type*
- ☑ **Programmatic access**
  Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- □ **AWS Management Console access**
  Enables a **password** that allows users to sign-in to the AWS Management Console.

Step 3: Now set the permissions to Administrator access from Attach existing policies directly as shown below and click on Next: Tags.



	Policy name	Type	Used as
✓	AdministratorAccess	Job function	None
□	AlexaForBusinessDeviceSetup	AWS managed	None
□	AlexaForBusinessFullAccess	AWS managed	None
□	AlexaForBusinessGatewayExecution	AWS managed	None
□	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None
□	AlexaForBusinessReadOnlyAccess	AWS managed	None
□	AmazonAPIGatewayAdministrator	AWS managed	None

Step 4: Add tags to user using Key-Value pair as shown below and click on Next: Review



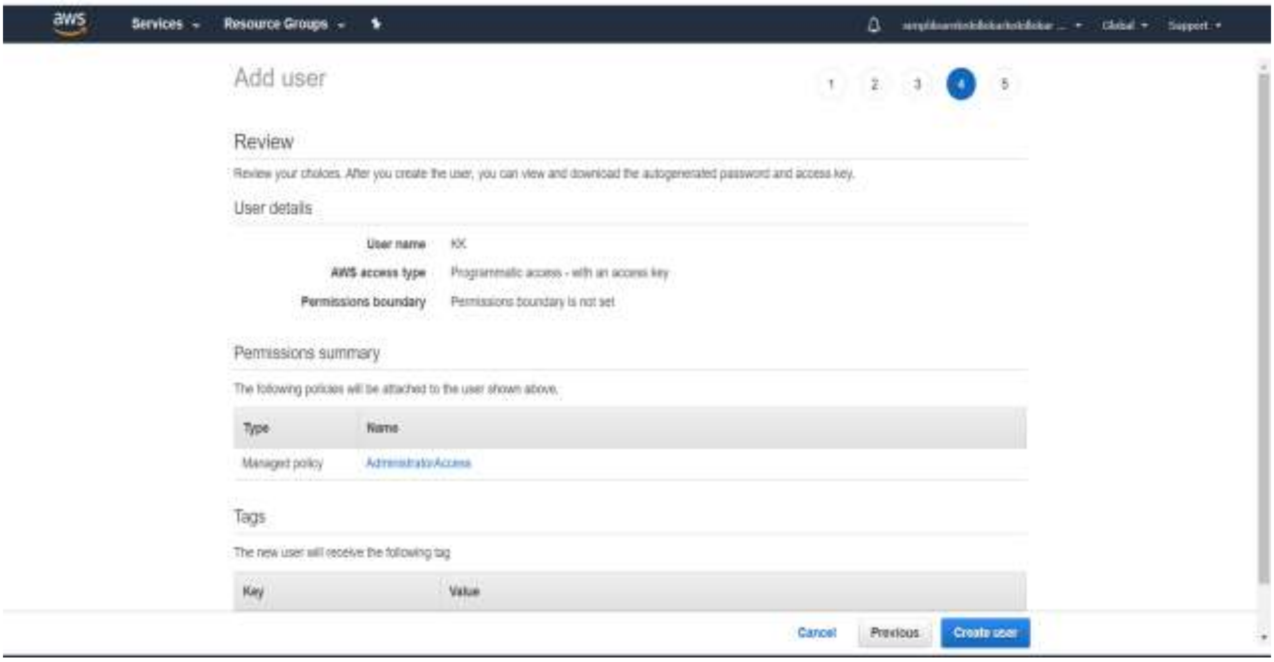
Add tags (optional)

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
Name	Kunal	✕
Add new key		

You can add 49 more tags.

Step 5: Review the user details as shown below and 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.

User details

User name	KK
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

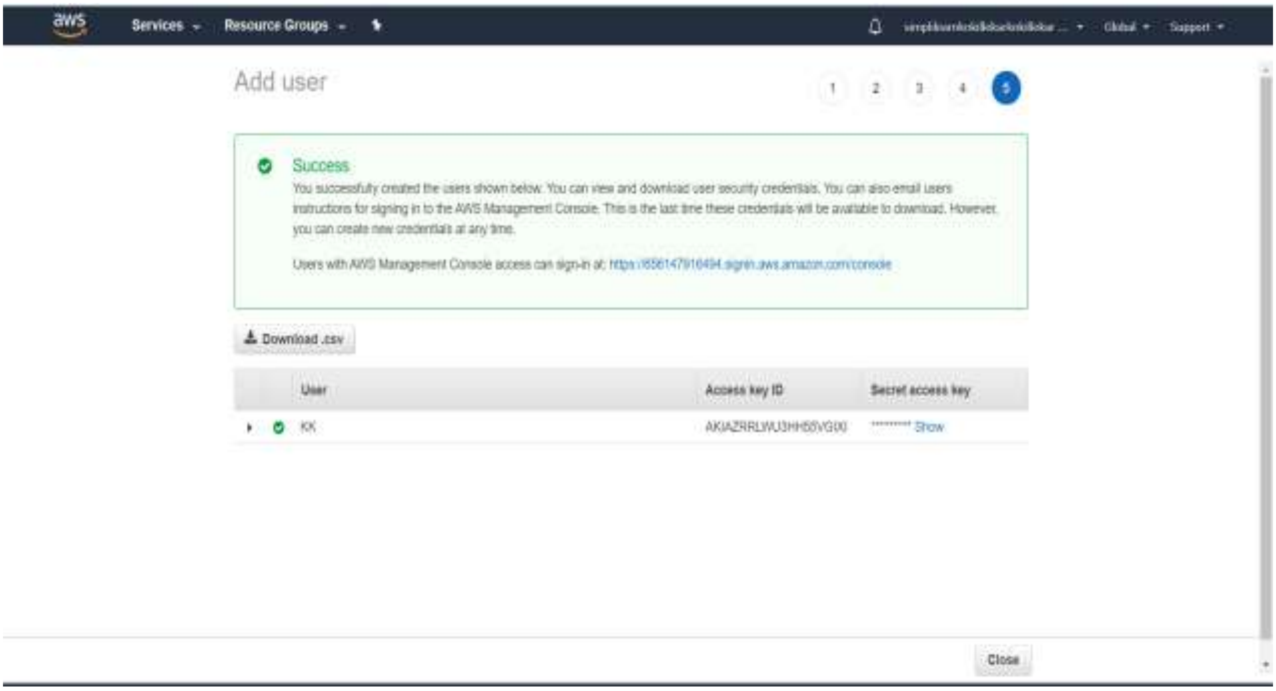
Type	Name
Managed policy	AdministratorAccess

Tags

The new user will receive the following tag

Key	Value

User is created successfully as shown below.



Add user

Success

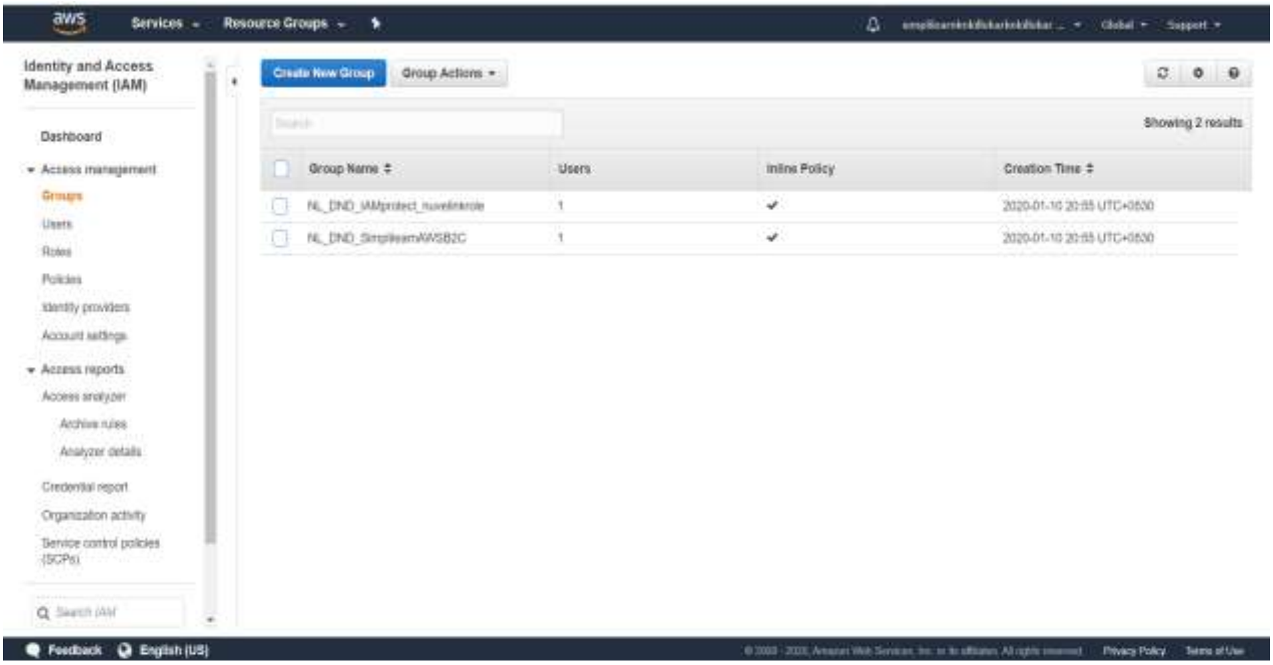
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any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

Users with AWS Management Console access can sign-in at: https://656147916494.signin.aws.amazon.com/console

	User	Access key ID	Secret access key
✓	KK	AKIAZRRLWU3HH55VGXX	********* Show

4. Create the IAM Administrator Group, and add the user to the Administrator Group.

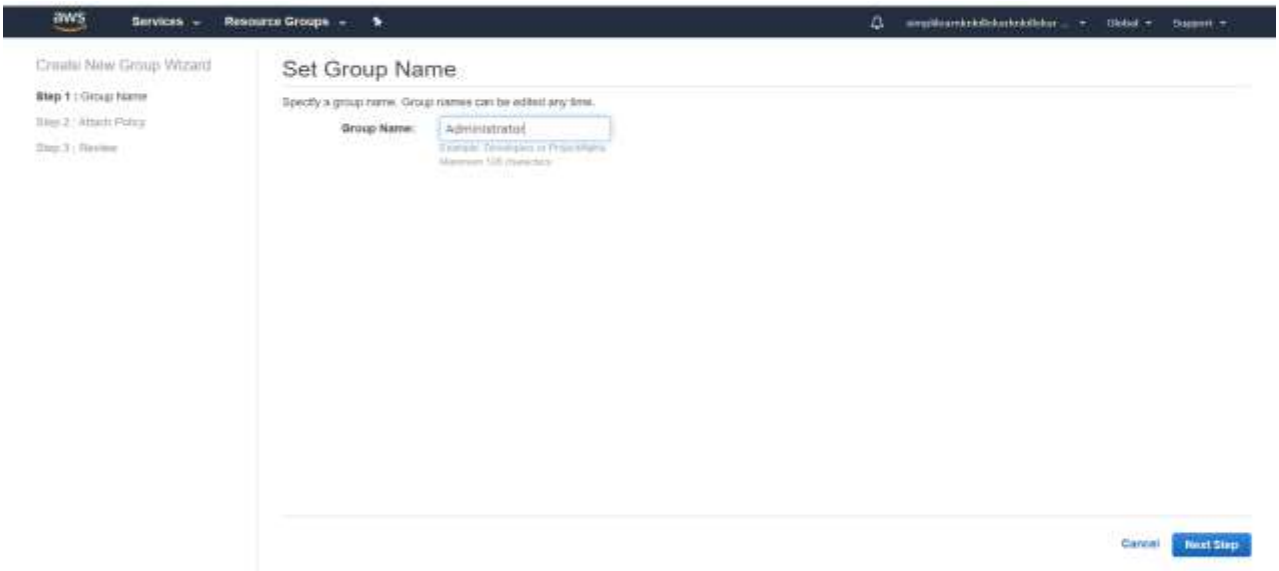
Step 1: Open AWS management console, click on Services. Go to Security, Identity, & Compliance and click on IAM. Then from left navigation pane select Groups option following window will appear as shown below.



Showing 2 results

	Group Name	Users	Inline Policy	Creation Time
□	NL_DND_IAMprotect_nuvelinkrole	1	✓	2020-01-10 20:55 UTC+0530
□	NL_DND_SimplilearnAWSB2C	1	✓	2020-01-10 20:55 UTC+0530

Step 2: Next click on create new group and set group name as "Administrator" as shown below and click on Next step.



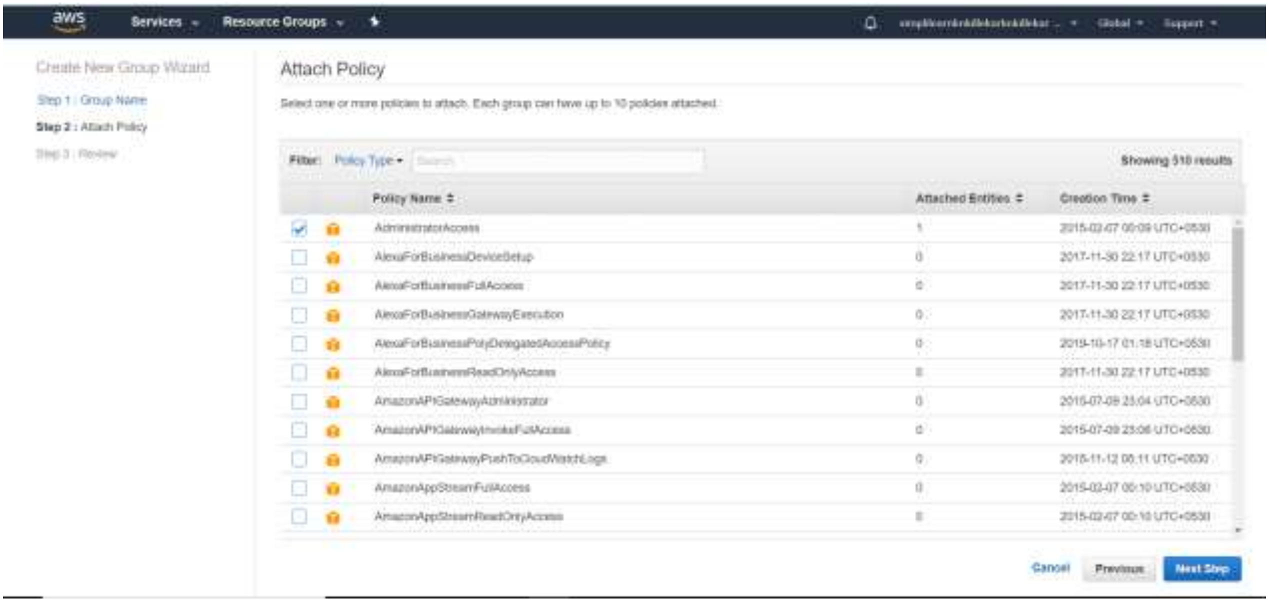
Set Group Name

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

Group Name: Administrator

Example: Developers or ProjectAlpha
Maximum 128 characters

Step 3: Now attach the policy as AdministratorAccess as shown below and click on Next step.

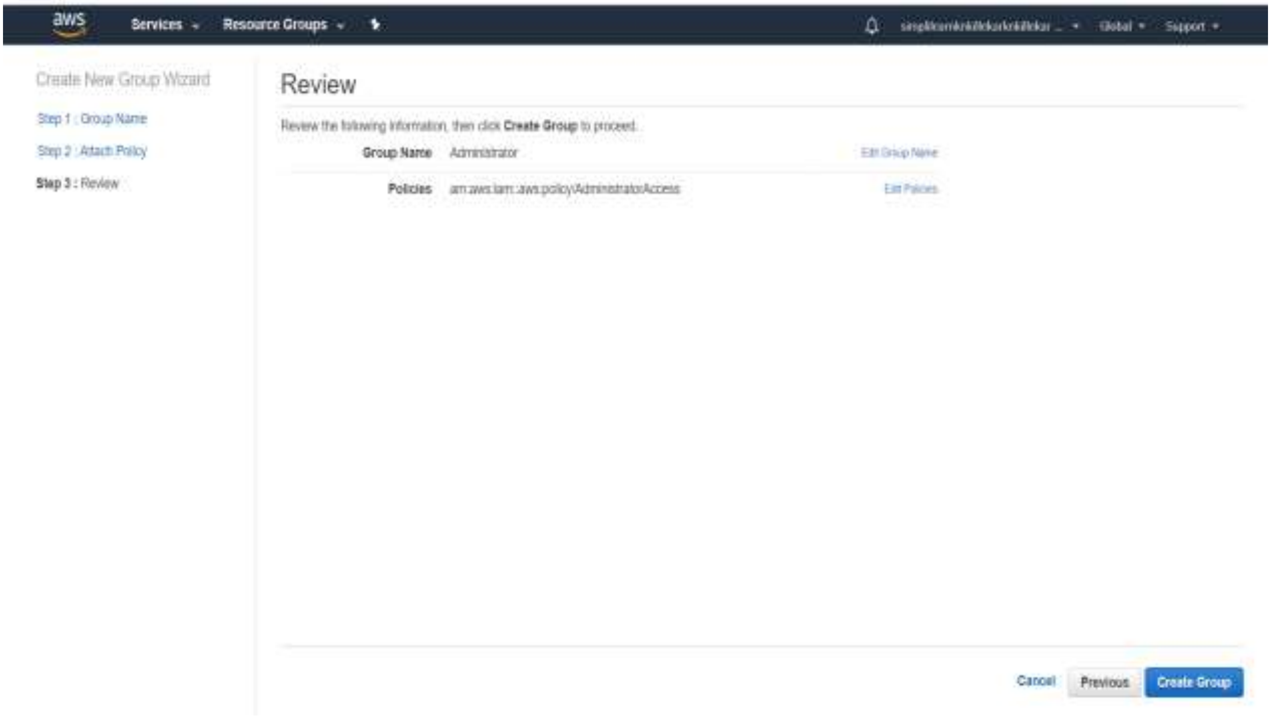


Attach Policy

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

		Policy Name	Attached Entities	Creation Time
☑		AdministratorAccess	1	2015-02-07 00:09 UTC+0530
□		AlexaForBusinessDeviceSetup	0	2017-11-30 22:17 UTC+0530
□		AlexaForBusinessFullAccess	0	2017-11-30 22:17 UTC+0530
□		AlexaForBusinessGatewayExecution	0	2017-11-30 22:17 UTC+0530
□		AlexaForBusinessPolyDelegatedAccessPolicy	0	2019-10-17 01:18 UTC+0530
□		AlexaForBusinessReadOnlyAccess	0	2017-11-30 22:17 UTC+0530
□		AmazonAPIGatewayAdministrator	0	2015-07-09 23:04 UTC+0530
□		AmazonAPIGatewayInvokeFullAccess	0	2015-07-09 23:06 UTC+0530
□		AmazonAPIGatewayPushToCloudWatchLogs	0	2015-11-12 06:11 UTC+0530
□		AmazonAppStreamFullAccess	0	2015-02-07 00:10 UTC+0530
□		AmazonAppStreamReadOnlyAccess	0	2015-02-07 00:10 UTC+0530

Step 4: Review the details of the group and click on create group.



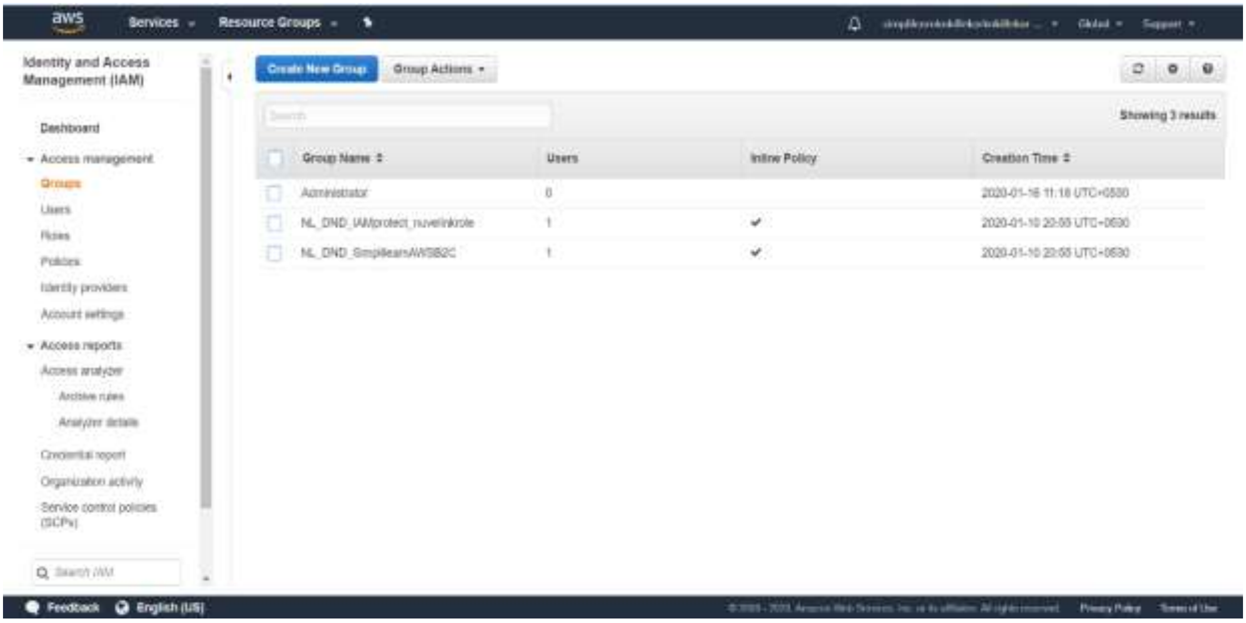
Review

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

Group Name Administrator

Policies arn:aws:iam::aws:policy/AdministratorAccess

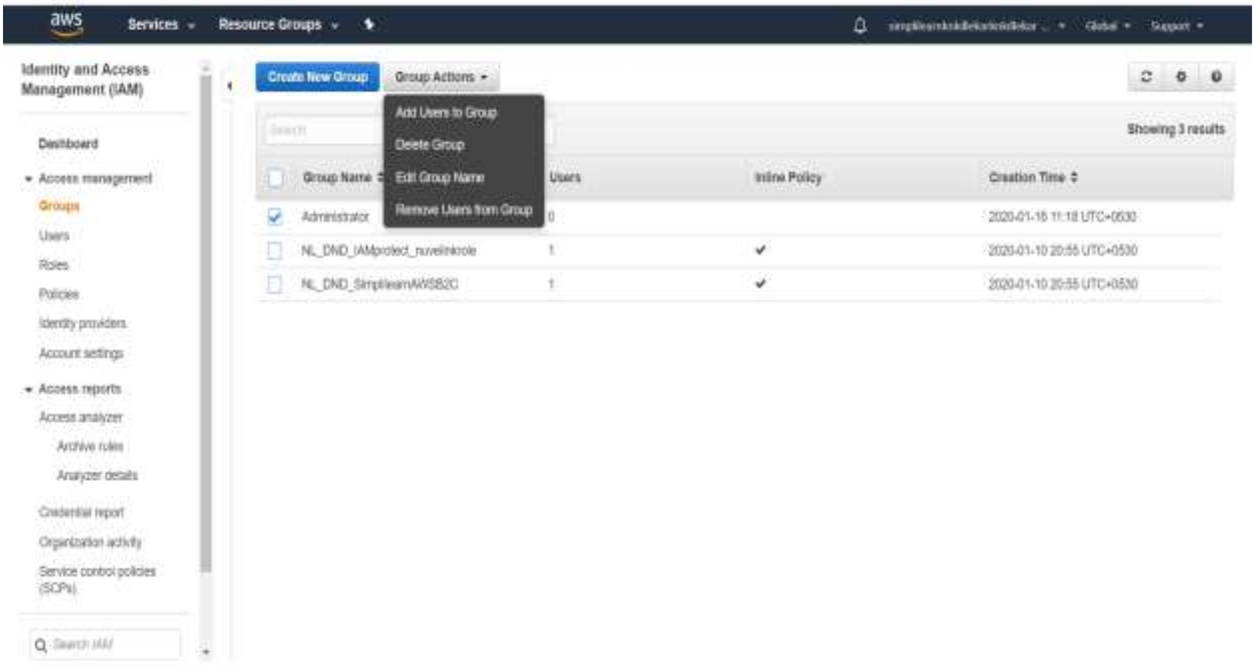
Step 5: Administrator group is created successfully as shown below.



Showing 3 results

□	Group Name	Users	Inline Policy	Creation Time
□	Administrator	0		2020-01-16 11:18 UTC+0530
□	NL_DND_IAMprotect_nuvelinkrole	1	✓	2020-01-10 20:55 UTC+0530
□	NL_DND_SimplilearnAWSB2C	1	✓	2020-01-10 20:55 UTC+0530

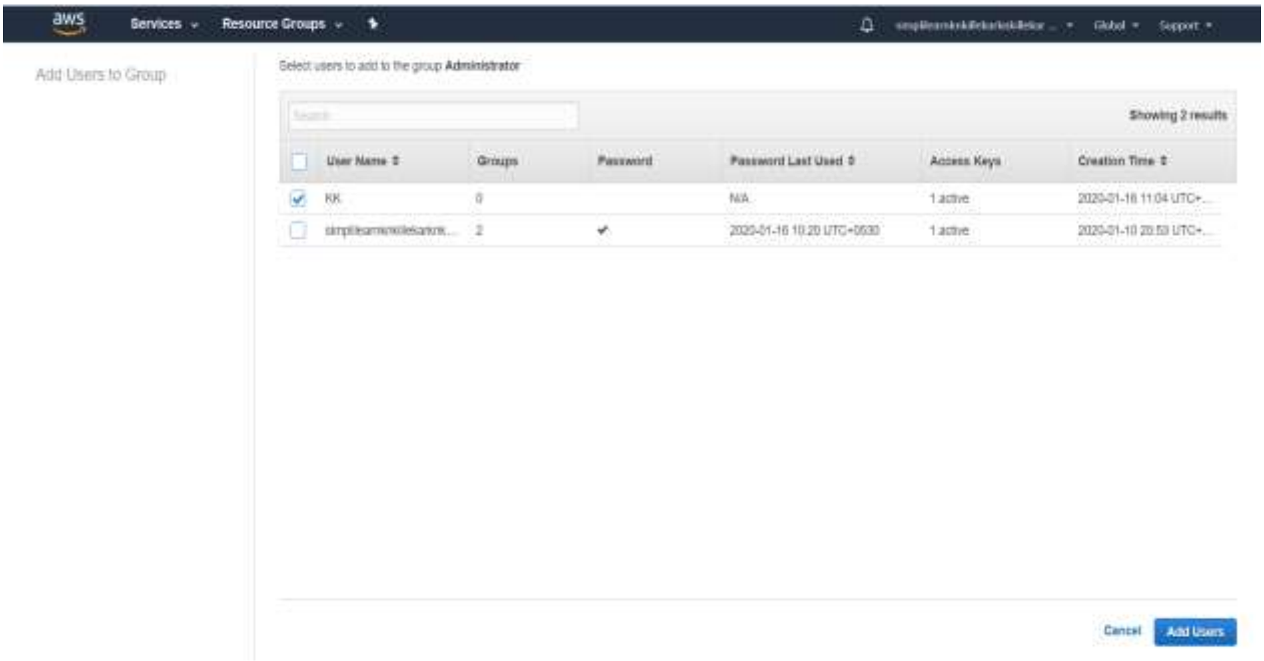
Step 6: To add users to group select the Administrator group as shown below. Then go to Group actions and select Add users to group option as shown below.



Showing 3 results

□	Group Name	Users	Inline Policy	Creation Time
☑	Administrator	0		2020-01-16 11:18 UTC+0530
□	NL_DND_IAMprotect_nuvelinkrole	1	✓	2020-01-10 20:55 UTC+0530
□	NL_DND_SimplilearnAWSB2C	1	✓	2020-01-10 20:55 UTC+0530

Step 7: Now select the user as “KK” as shown below and click on Add users.

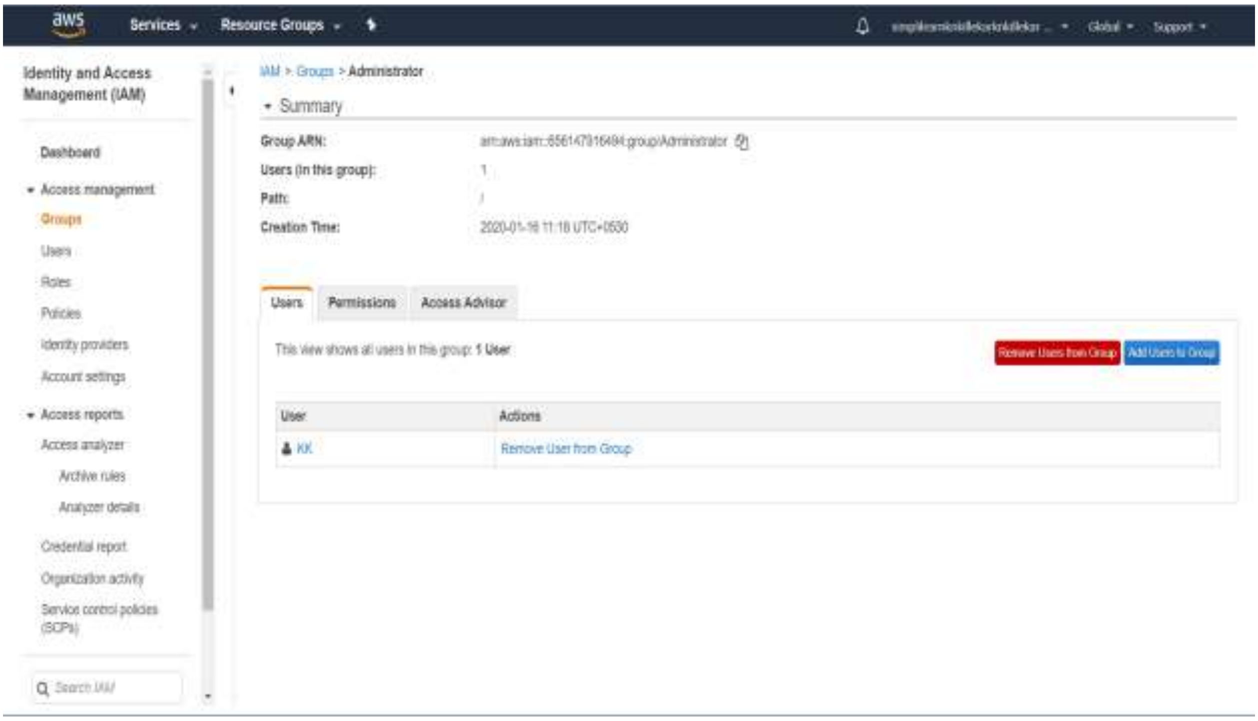


Select users to add to the group **Administrator**

Showing 2 results

□	User Name ⇕	Groups	Password	Password Last Used ⇕	Access Keys	Creation Time ⇕
☑	KK	0		N/A	1 active	2020-01-16 11:04 UTC+...
□	simplilearnkrkkllekarkrk...	2	✓	2020-01-16 10:20 UTC+0530	1 active	2020-01-10 20:53 UTC+...

Step 8: User is added to the group successfully as shown below.



IAM > Groups > Administrator

Summary

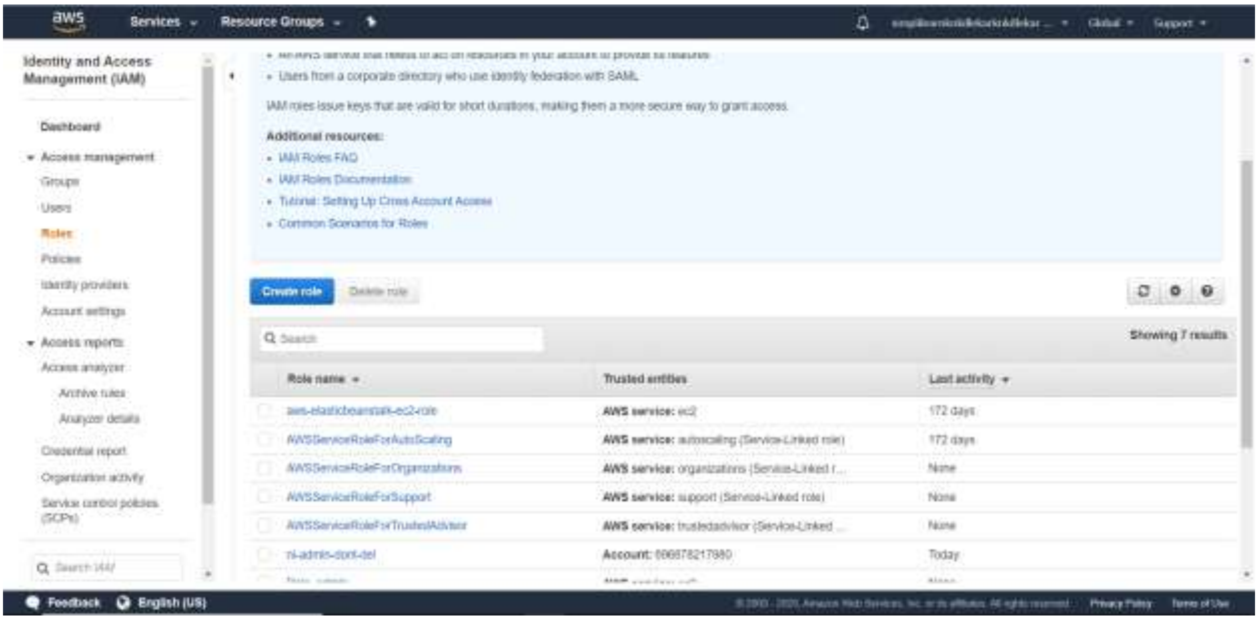
Group ARN:	arn:aws:iam::656147916494:group/Administrator
Users (in this group):	1
Path:	/
Creation Time:	2020-01-16 11:18 UTC+0530

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

User	Actions
KK	Remove User from Group

5. Create a Role.

Step 1: Open AWS management console, click on Services. Go to Security, Identity, & Compliance and click on IAM. Then from left navigation pane select Roles option following window will appear as shown below.



- 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.

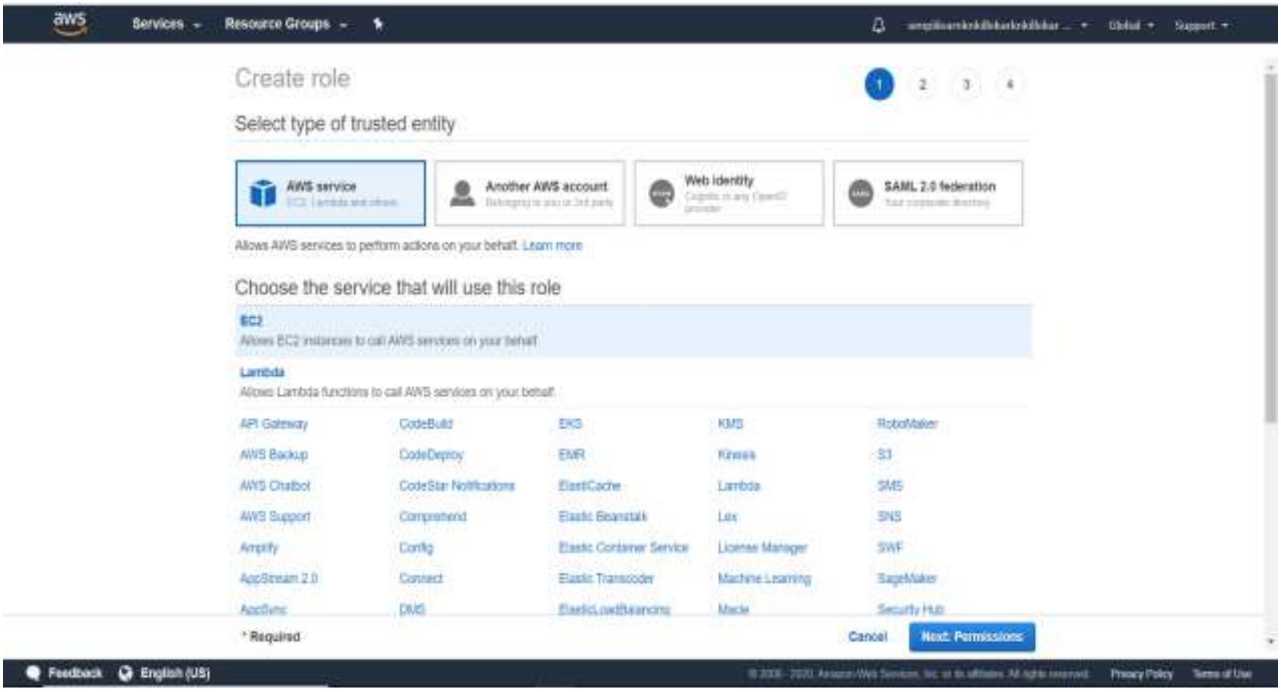
Additional resources:

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

Showing 7 results

Role name	Trusted entities	Last activity
aws-elasticbeanstalk-ec2-role	**AWS service:** ec2	172 days
AWSServiceRoleForAutoScaling	**AWS service:** autoscaling (Service-Linked role)	172 days
AWSServiceRoleForOrganizations	**AWS service:** organizations (Service-Linked r...	None
AWSServiceRoleForSupport	**AWS service:** support (Service-Linked role)	None
AWSServiceRoleForTrustedAdvisor	**AWS service:** trustedadvisor (Service-Linked ...	None
nl-admin-dont-del	**Account:** 898878217880	Today

Step 2: Next click on create role and select the type of trusted entity as EC2 as shown below and click on Next: permissions.



Create role

Select type of trusted entity

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

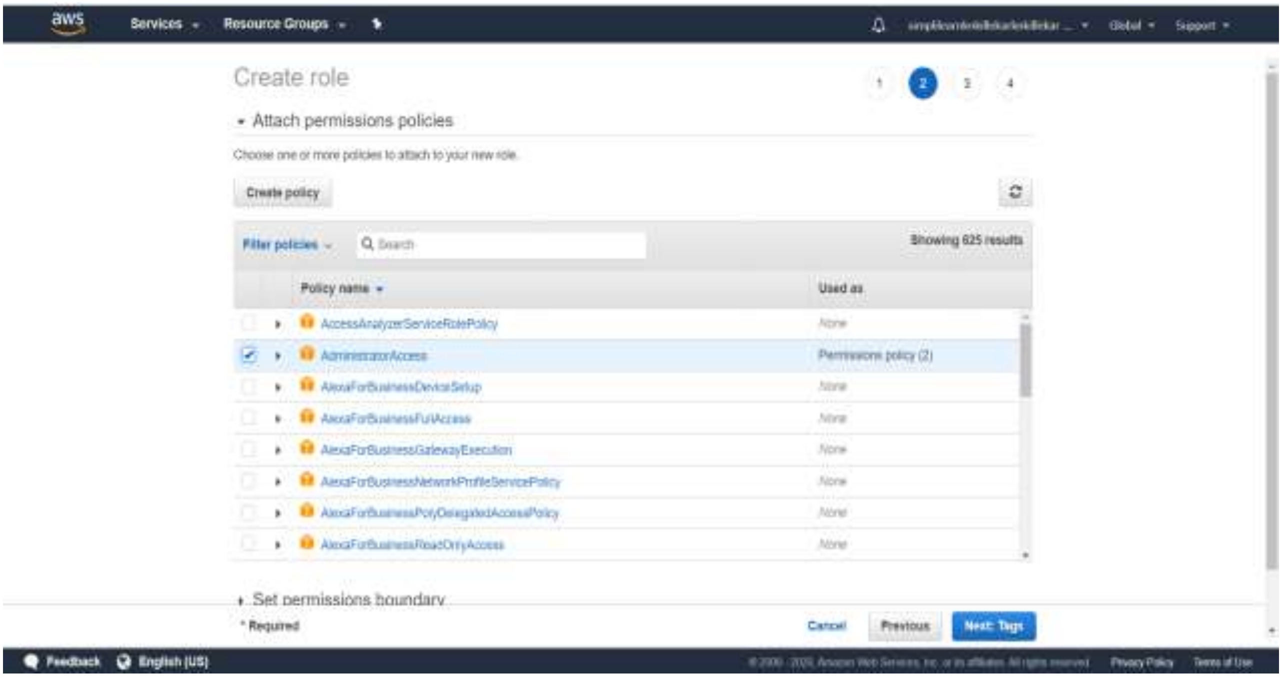
Choose the service that will use this role

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

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

* Required

Step 3: Attach policy to the role as Administrator Access as shown below and click on Next: Tags.



Create role

Attach permissions policies

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

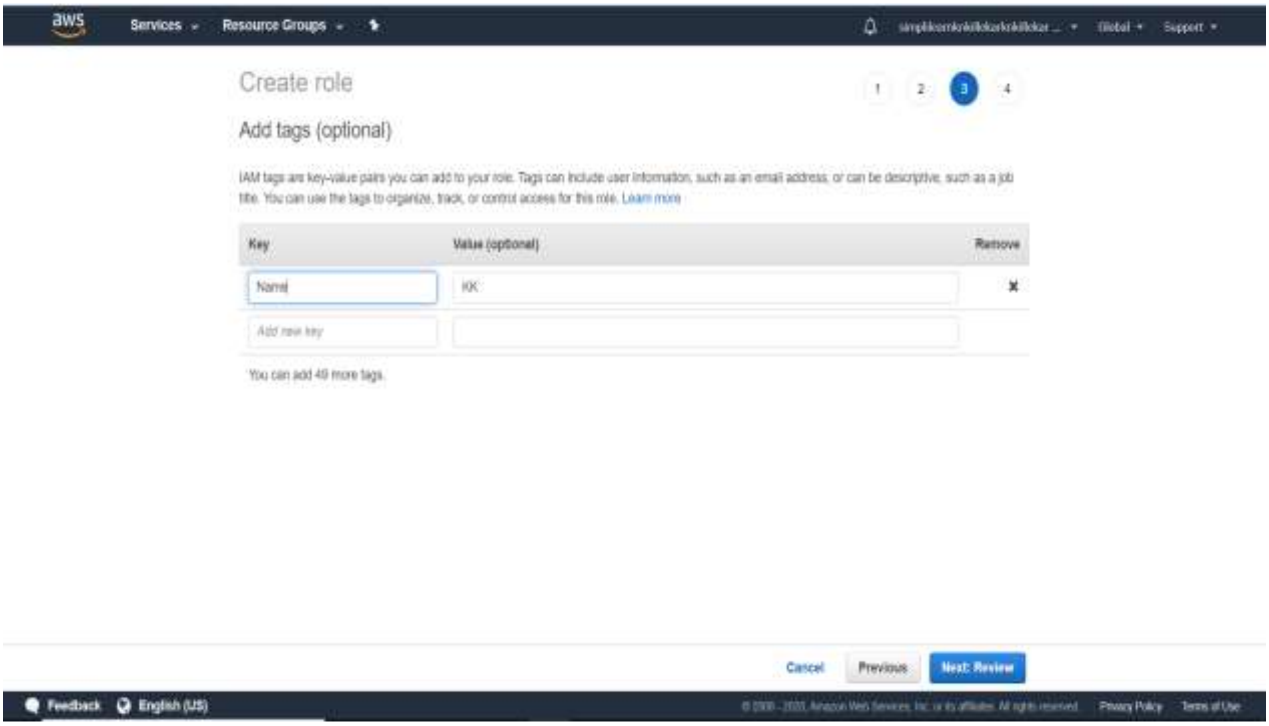
Showing 625 results

	Policy name	Used as
□	AccessAnalyzerServiceRolePolicy	None
☑	AdministratorAccess	Permissions policy (2)
□	AlexaForBusinessDeviceSetup	None
□	AlexaForBusinessFullAccess	None
□	AlexaForBusinessGatewayExecution	None
□	AlexaForBusinessNetworkProfileServicePolicy	None
□	AlexaForBusinessPolyDelegatedAccessPolicy	None
□	AlexaForBusinessReadOnlyAccess	None

Set permissions boundary

* Required

Step 4: Now add tags to the role as shown below and click on Next: Review.



Create role

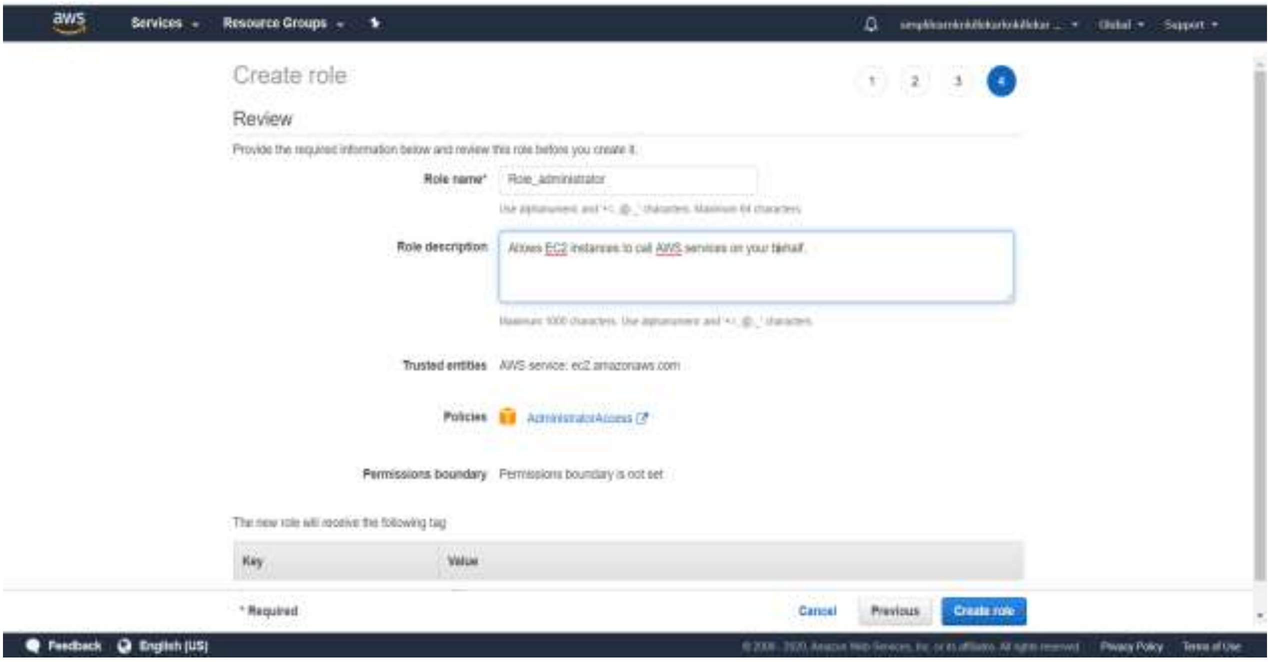
Add tags (optional)

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
Name	KK	✖
Add new key		

You can add 49 more tags.

Step 5: In review section enter the role name as “Role_administrator” as shown below and click on 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

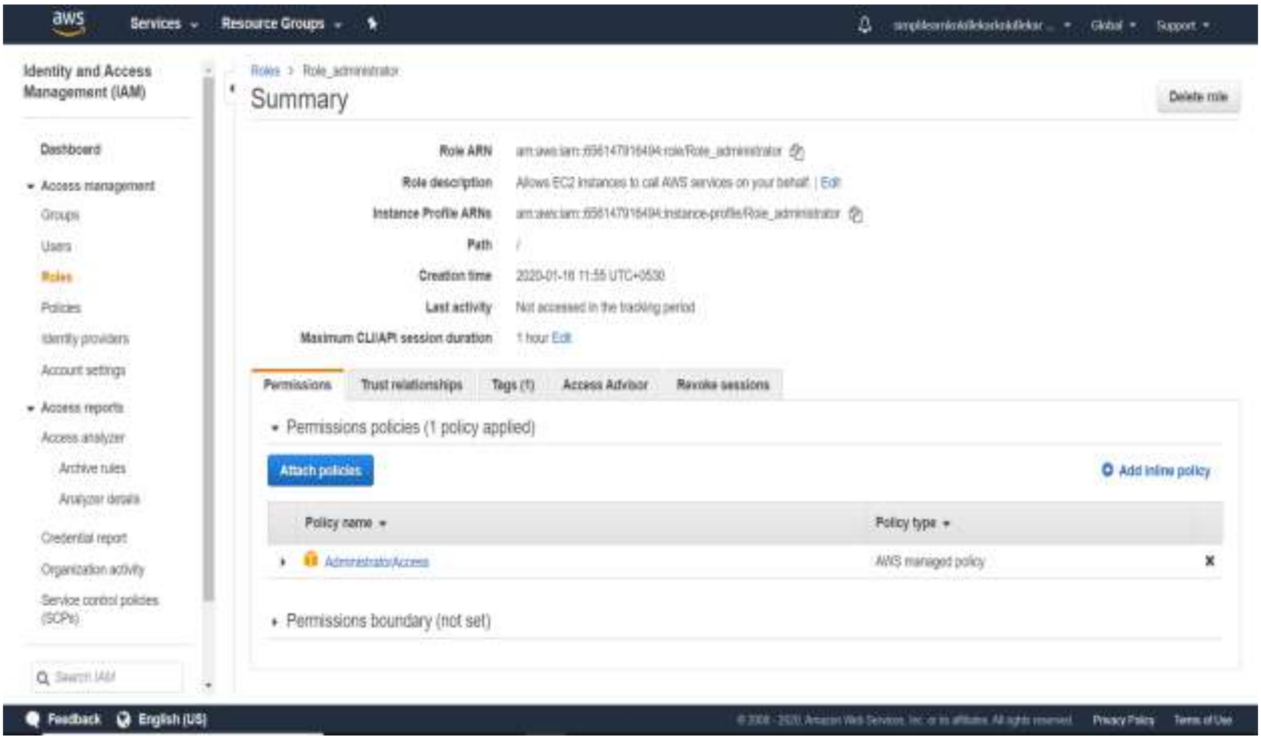
Permissions boundary Permissions boundary is not set

The new role will receive the following tag

Key	Value

* Required

Step 6: Role is created successfully as shown below.



Roles > Role_administrator

Summary

Role ARN arn:aws:iam::656147916494:role/Role_administrator

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

Instance Profile ARNs arn:aws:iam::656147916494:instance-profile/Role_administrator

Path /

Creation time 2020-01-16 11:55 UTC+0530

Last activity Not accessed in the tracking period

Maximum CLI/API session duration 1 hour Edit

Permissions policies (1 policy applied)

Policy name	Policy type
AdministratorAccess	AWS managed policy

Permissions boundary (not set)