Server Monitoring

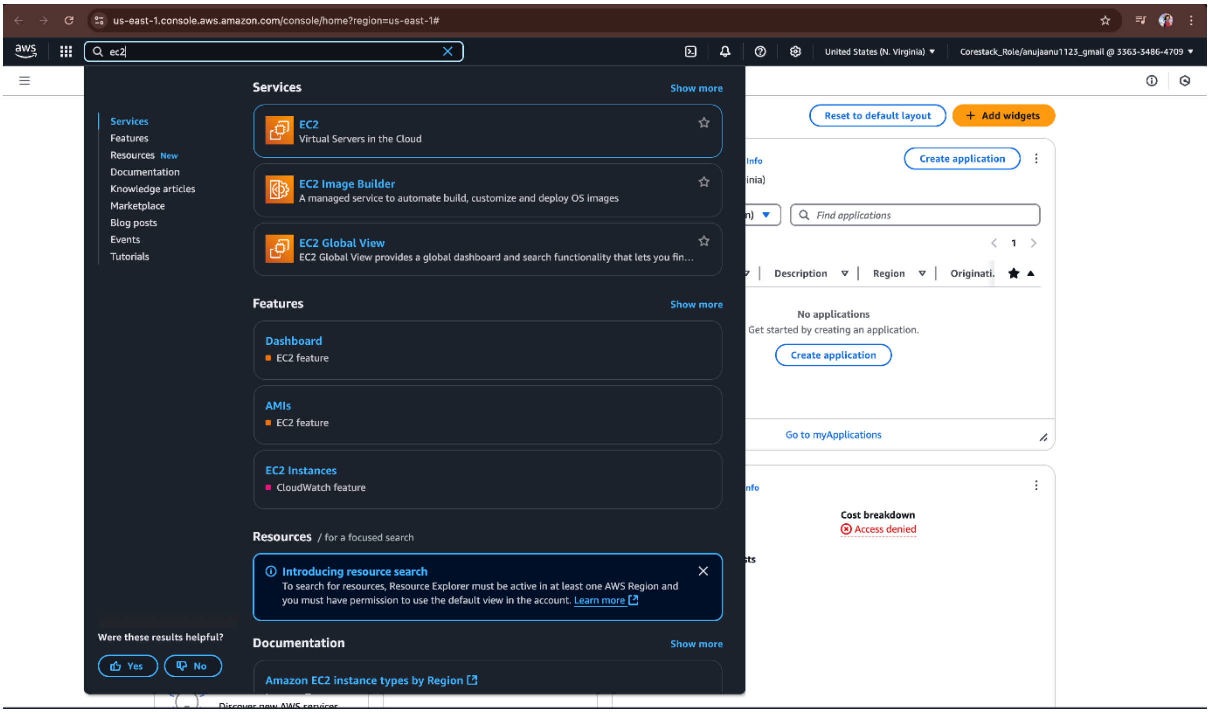
Description:

Heaven Classics successfully creates an EC2 Server Instance for Windows 2022 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 and observe the CPU utilization graph for the EC2 instance
2. Create and configure a CloudWatch alarm that sends an email notification to HCMonitor@HeavenClassics.com if the CPU utilization goes below the threshold of 3%, consecutively three times for five minutes
3. Create an IAM group named Administrator Group and attach the full administrator access policy to the group
4. Create a user for an employee of the company who requires administrator access to the company's AWS account and then add the user to the Administrator Group.

Here we are creating this requirement step by step

First we need to create a EC2 machine with the name of heaven classics so go to your amazon console and search for EC2.



EC2 — Virtual Servers in the Cloud

EC2 Image Builder — A managed service to automate build, customize and deploy OS images

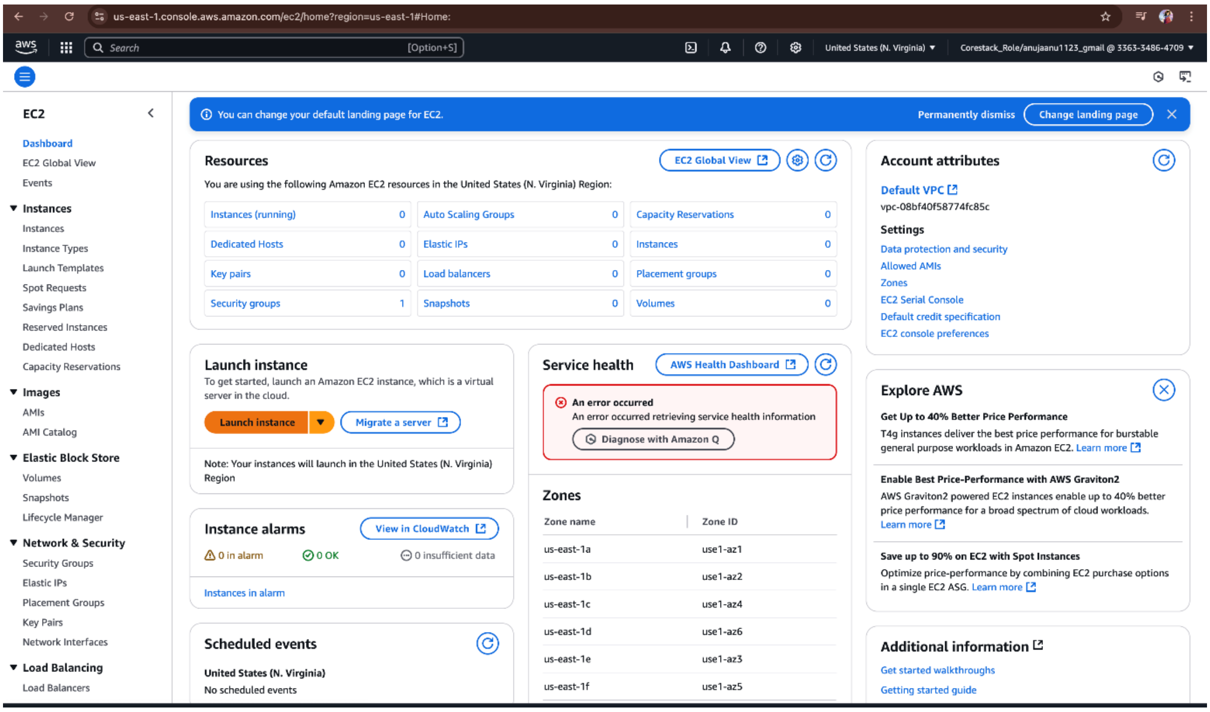
EC2 Global View — EC2 Global View provides a global dashboard and search functionality that lets you fin…

Introducing resource search: To search for resources, Resource Explorer must be active in at least one AWS Region and you must have permission to use the default view in the account. Learn more

No applications

Get started by creating an application.

And then press launch instances.



You can change your default landing page for EC2.

Resources

You are using the following Amazon EC2 resources in the United States (N. Virginia) Region:

Instances (running)	0	Auto Scaling Groups	0	Capacity Reservations	0
Dedicated Hosts	0	Elastic IPs	0	Instances	0
Key pairs	0	Load balancers	0	Placement groups	0
Security groups	1	Snapshots	0	Volumes	0

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the United States (N. Virginia) Region

Instance alarms

0 in alarm 0 OK 0 insufficient data

Scheduled events

United States (N. Virginia)

No scheduled events

Service health

An error occurred

An error occurred retrieving service health information

Zones

Zone name	Zone ID
us-east-1a	use1-az1
us-east-1b	use1-az2
us-east-1c	use1-az4
us-east-1d	use1-az6
us-east-1e	use1-az3
us-east-1f	use1-az5

Account attributes

Default VPC

vpc-08bf40f58774fc85c

Settings

Explore AWS

Get Up to 40% Better Price Performance

T4g instances deliver the best price performance for burstable general purpose workloads in Amazon EC2. Learn more

Enable Best Price-Performance with AWS Graviton2

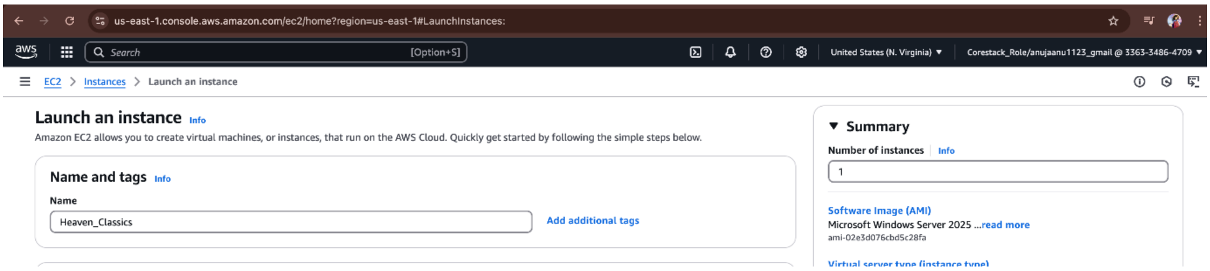
AWS Graviton2 powered EC2 instances enable up to 40% better price performance for a broad spectrum of cloud workloads. Learn more

Save up to 90% on EC2 with Spot Instances

Optimize price-performance by combining EC2 purchase options in a single EC2 ASG. Learn more

Additional information

Now we need to name our instance as heaven classics mentioned above in the description.


us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
aws
Search
[Option+S]
United States (N. Virginia) ▾
Corestack_Role/anujaanu1123_gmail @ 3363-3486-4709 ▾
EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

Heaven_Classics

Add additional tags

▼ Summary

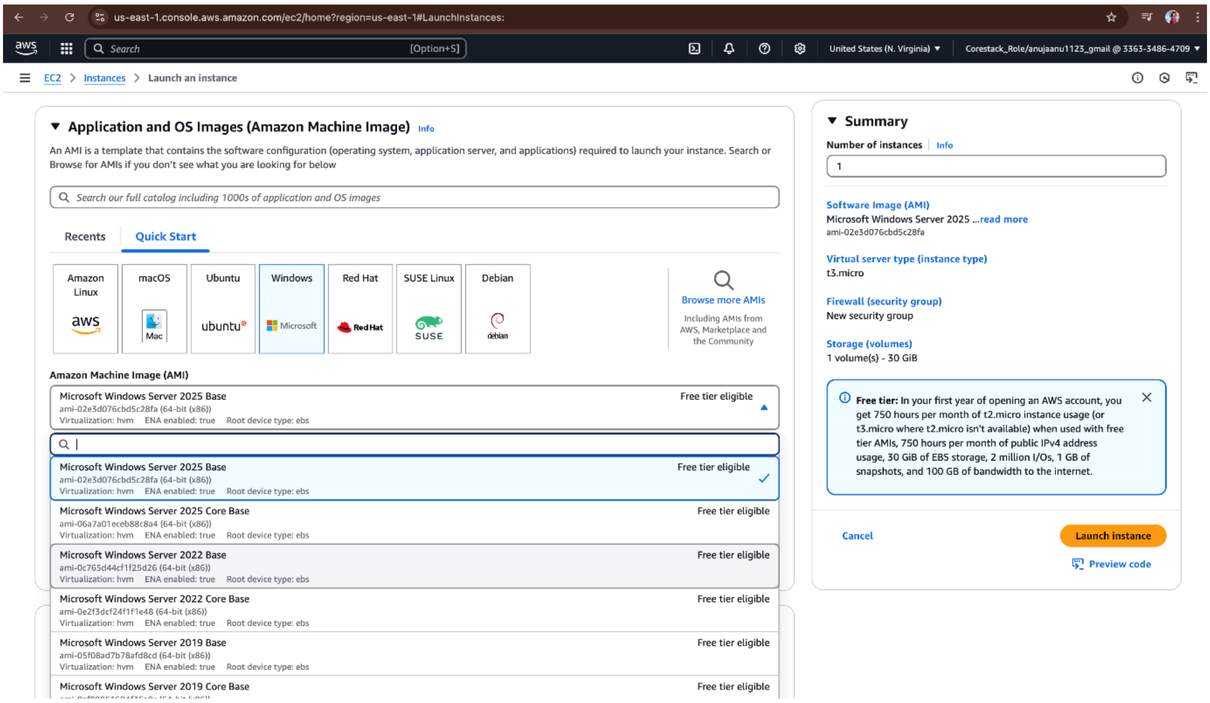
Number of instances Info

1

Software Image (AMI)
Microsoft Windows Server 2025 ...read more
ami-02e3d076cbd5c28fa

Virtual server type (instance type)

And select the windows with 2022 base in application and OS image section.


us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
aws
Search
[Option+S]
United States (N. Virginia) ▾
Corestack_Role/anujaanu1123_gmail @ 3363-3486-4709 ▾
EC2 > Instances > Launch an instance
Recents
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Debian
aws
Mac
ubuntu
Microsoft
Red Hat
SUSE
debian
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Cancel
Launch instance
Preview code

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Amazon Machine Image (AMI)

Microsoft Windows Server 2025 Base — Free tier eligible
ami-02e3d076cbd5c28fa (64-bit (x86))
Virtualization: hvm ENA enabled: true Root device type: ebs

Microsoft Windows Server 2025 Base — Free tier eligible ✓
ami-02e3d076cbd5c28fa (64-bit (x86))
Virtualization: hvm ENA enabled: true Root device type: ebs

Microsoft Windows Server 2025 Core Base — Free tier eligible
ami-06a7a01eceb88c8a4 (64-bit (x86))
Virtualization: hvm ENA enabled: true Root device type: ebs

Microsoft Windows Server 2022 Base — Free tier eligible
ami-0c765d44cf1f25d26 (64-bit (x86))
Virtualization: hvm ENA enabled: true Root device type: ebs

Microsoft Windows Server 2022 Core Base — Free tier eligible
ami-0e2f3dcf24f1f1e48 (64-bit (x86))
Virtualization: hvm ENA enabled: true Root device type: ebs

Microsoft Windows Server 2019 Base — Free tier eligible
ami-05f08ad7b78afd8cd (64-bit (x86))
Virtualization: hvm ENA enabled: true Root device type: ebs

Microsoft Windows Server 2019 Core Base — Free tier eligible

▼ Summary

Number of instances Info

1

Software Image (AMI)
Microsoft Windows Server 2025 ...read more
ami-02e3d076cbd5c28fa

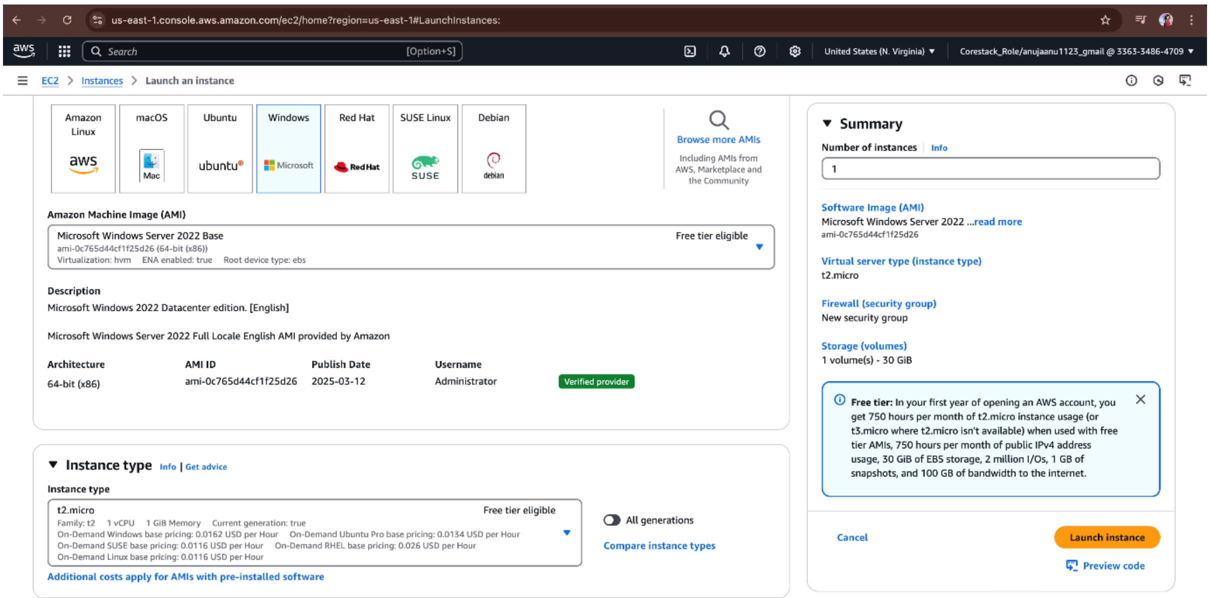
Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 30 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

And select instance type as t2.micro


us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
aws
Search
[Option+S]
United States (N. Virginia) ▾
Corestack_Role/anujaanu1123_gmail @ 3363-3486-4709 ▾
EC2 > Instances > Launch an instance
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Debian
aws
Mac
ubuntu
Microsoft
Red Hat
SUSE
debian
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Verified provider
Compare instance types
Cancel
Launch instance
Preview code

Amazon Machine Image (AMI)

Microsoft Windows Server 2022 Base — Free tier eligible
ami-0c765d44cf1f25d26 (64-bit (x86))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Microsoft Windows 2022 Datacenter edition. [English]

Microsoft Windows Server 2022 Full Locale English AMI provided by Amazon

Architecture	AMI ID	Publish Date	Username
64-bit (x86)	ami-0c765d44cf1f25d26	2025-03-12	Administrator

▼ Instance type Info | Get advice

Instance type

t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

○ All generations

Additional costs apply for AMIs with pre-installed software

▼ Summary

Number of instances Info

1

Software Image (AMI)
Microsoft Windows Server 2022 ...read more
ami-0c765d44cf1f25d26

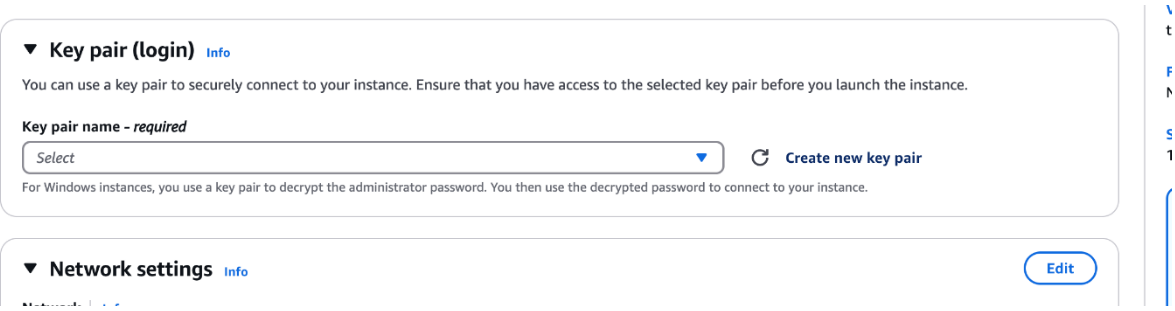
Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 30 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

And in keypair section select option as create new keypair.



Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

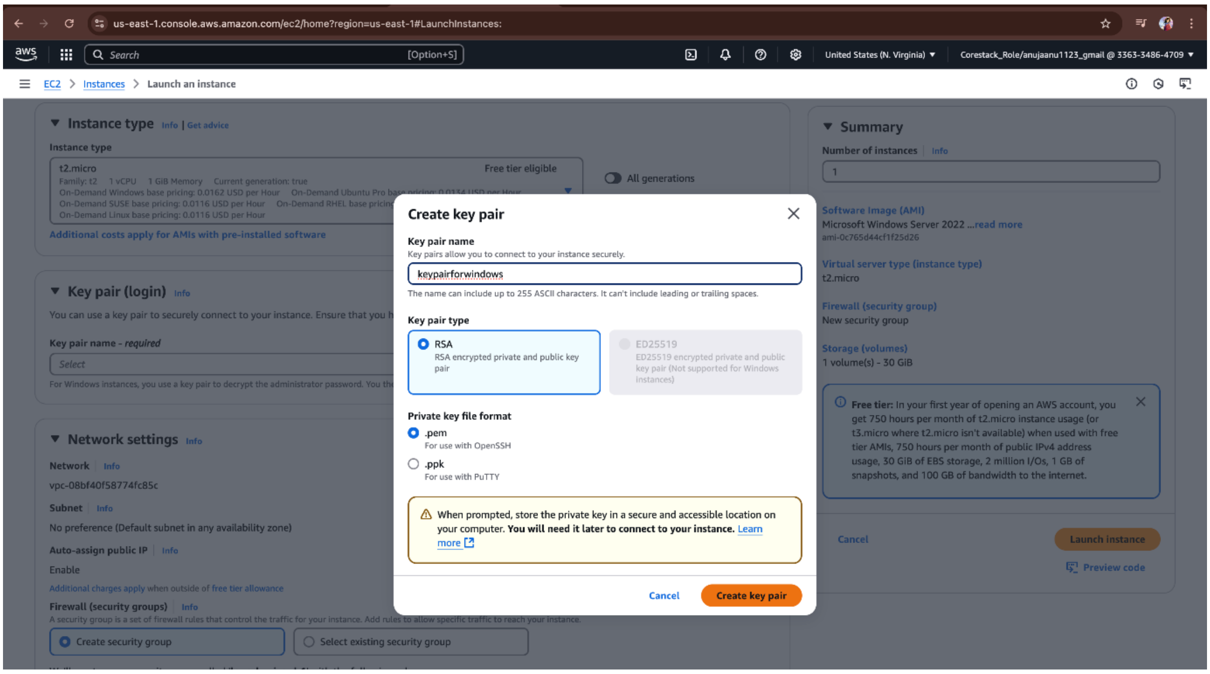
Key pair name - *required*

Select ▼   Create new key pair

For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.

Network settings Info   Edit

Then give your keypair a name and select .pem key to connect using open SSH. And click on create key pair.



us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

aws
Search [Option+S]
United States (N. Virginia) ▼
Corestack_Role/anujaanu1123_gmail @ 3363-3486-4709 ▼
EC2 > Instances > Launch an instance

Instance type Info | Get advice

Instance type

t2.micro   Free tier eligible
Family: t2   1 vCPU   1 GiB Memory   Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour   On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour   On-Demand RHEL base pricing
On-Demand Linux base pricing: 0.0116 USD per Hour

All generations

Additional costs apply for AMIs with pre-installed software

Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you h

Key pair name - *required*

Select

For Windows instances, you use a key pair to decrypt the administrator password. You the

Network settings Info

Network Info
vpc-08bf40f58774fc85c

Subnet Info
No preference (Default subnet in any availability zone)

Auto-assign public IP Info
Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group   ○ Select existing security group

Create key pair

Key pair name
Key pairs allow you to connect to your instance securely.

keypairforwindows

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

● RSA
RSA encrypted private and public key pair

○ ED25519
ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

● .pem
For use with OpenSSH

○ .ppk
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** Learn more

Cancel   Create key pair

Summary

Number of instances Info
1

Software Image (AMI)
Microsoft Windows Server 2022 ...read more
ami-0c765d44cf1f25d26

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

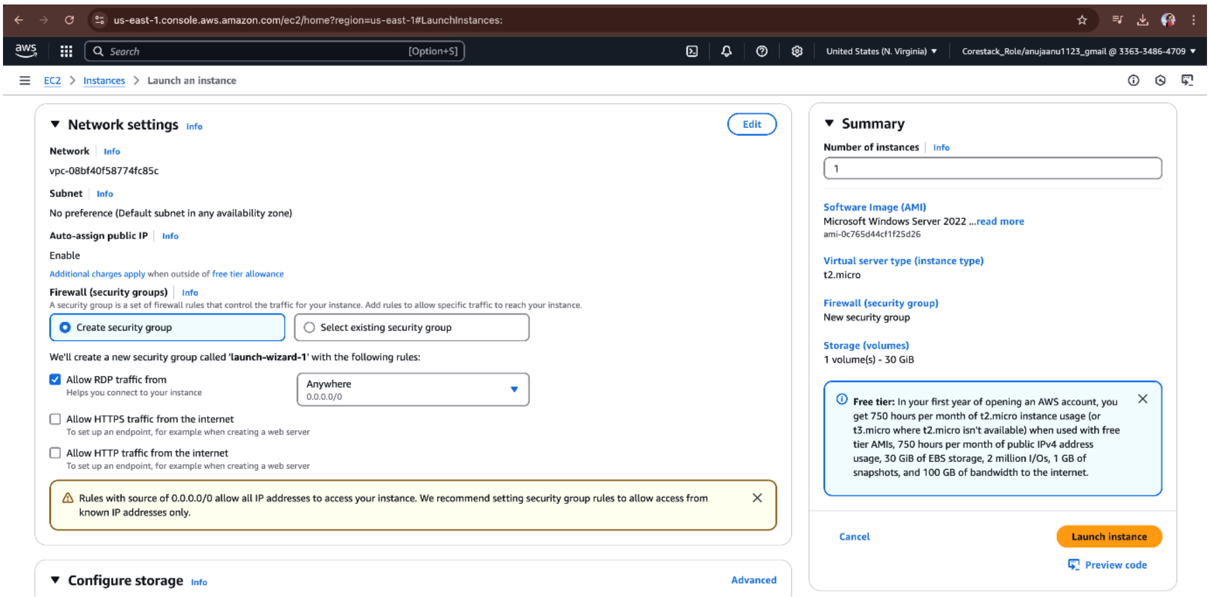
Storage (volumes)
1 volume(s) - 30 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel   Launch instance

Preview code

In network settings keep it as default and launch Instance.


us-east-1.console.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
aws
Search
[Option+S]
United States (N. Virginia) ▼
Corestack_Role/anujaanu1123_gmail @ 3363-3486-4709 ▼
EC2 > Instances > Launch an instance
Edit
Cancel
Launch instance
Preview code
Advanced

▼ Network settings Info

Network | Info

vpc-08bf40f58774fc85c

Subnet | Info

No preference (Default subnet in any availability zone)

Auto-assign public IP | Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) | Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

We'll create a new security group called '**launch-wizard-1**' with the following rules:

☑ Allow RDP traffic from — Anywhere 0.0.0.0/0
Helps you connect to your instance

☐ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

▼ Configure storage Info

▼ Summary

Number of instances | Info

1

Software Image (AMI)
Microsoft Windows Server 2022 ...read more
ami-0c765d44cf1f25d26

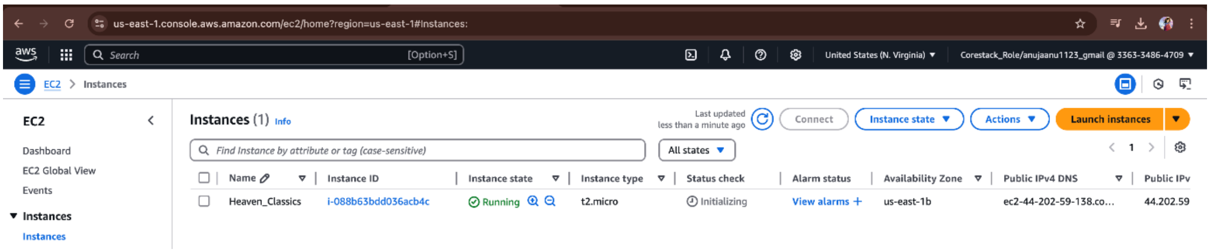
Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 30 GiB

ⓘ **Free tier:** In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

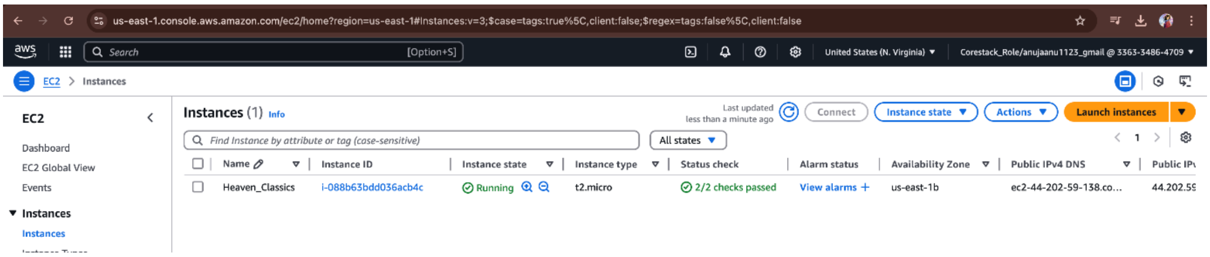
After clicking on launch instance we can see our instance is creating it will take 2 to 3 mins to create our instance.


us-east-1.console.amazon.com/ec2/home?region=us-east-1#Instances:
aws
Search
[Option+S]
United States (N. Virginia) ▼
Corestack_Role/anujaanu1123_gmail @ 3363-3486-4709 ▼
EC2 > Instances
EC2
Dashboard
EC2 Global View
Events
▼ Instances
Instances
Last updated
less than a minute ago
Connect
Instance state ▼
Actions ▼
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states ▼
1

Instances (1) Info

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv
☐	Heaven_Classics	i-088b63bdd036acb4c	Running	t2.micro	Initializing	View alarms +	us-east-1b	ec2-44-202-59-138.co...	44.202.59

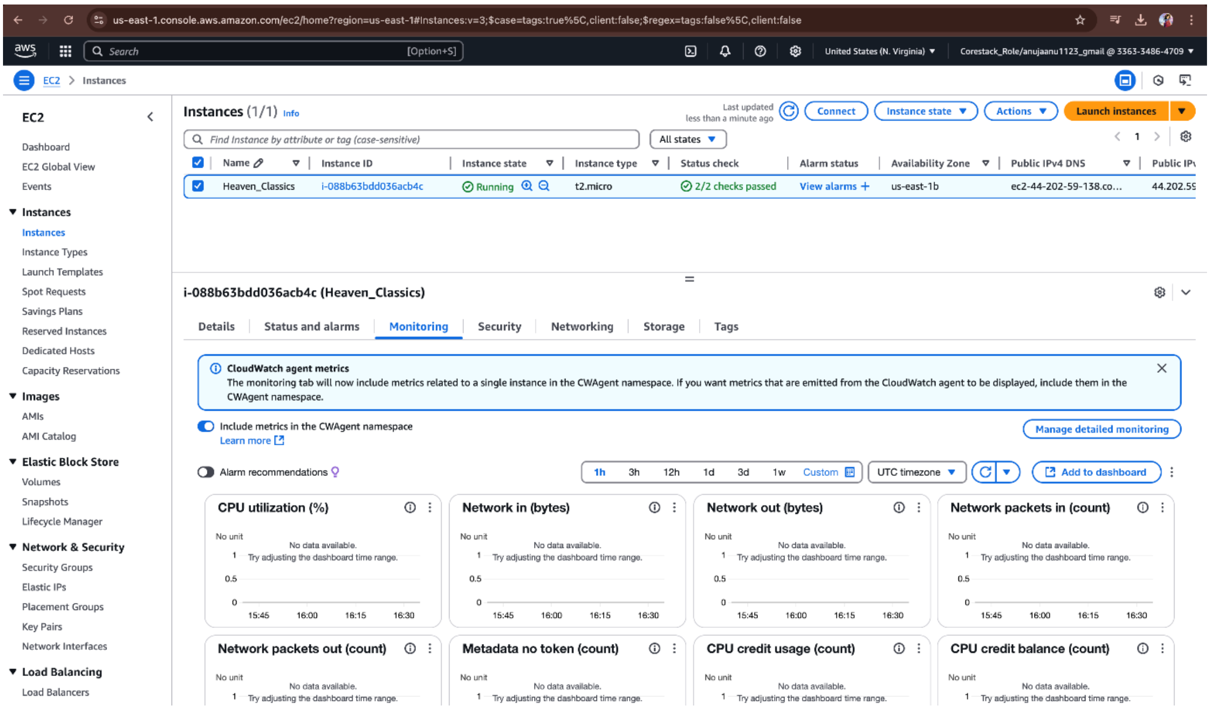
so we can see our instance is created and upon running now.


us-east-1.console.amazon.com/ec2/home?region=us-east-1#Instances:v=3;$case=tags:true%5C,client:false;$regex=tags:false%5C,client:false
aws
Search
[Option+S]
United States (N. Virginia) ▼
Corestack_Role/anujaanu1123_gmail @ 3363-3486-4709 ▼
EC2 > Instances
EC2
Dashboard
EC2 Global View
Events
▼ Instances
Instances
Last updated
less than a minute ago
Connect
Instance state ▼
Actions ▼
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states ▼
1

Instances (1) Info

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IP
☐	Heaven_Classics	i-088b63bdd036acb4c	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1b	ec2-44-202-59-138.co...	44.202.5

And the click on instance we can see down a tab called monitoring click on that you can see the CPU utilization for our EC2 instance.



Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv
Heaven_Classics	i-088b63bdd036acb4c	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1b	ec2-44-202-59-138.co...	44.202.59

i-088b63bdd036acb4c (Heaven_Classics)

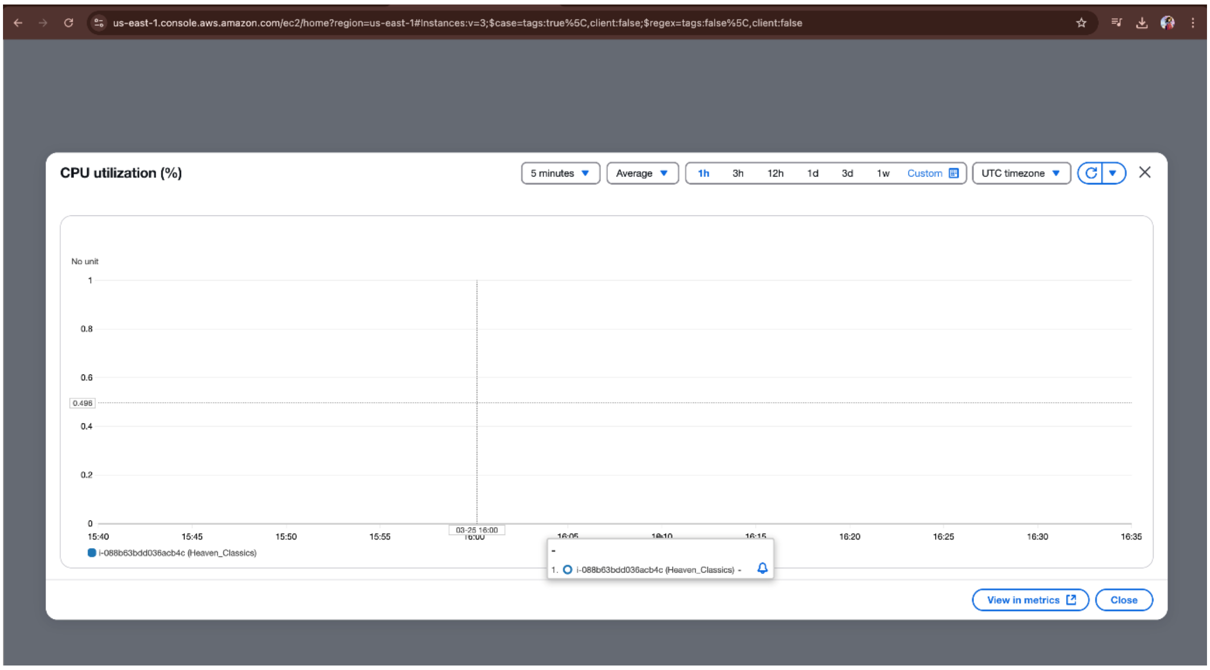
CloudWatch agent metrics
The monitoring tab will now include metrics related to a single instance in the CWAgent namespace. If you want metrics that are emitted from the CloudWatch agent to be displayed, include them in the CWAgent namespace.

Include metrics in the CWAgent namespace
Learn more

Alarm recommendations

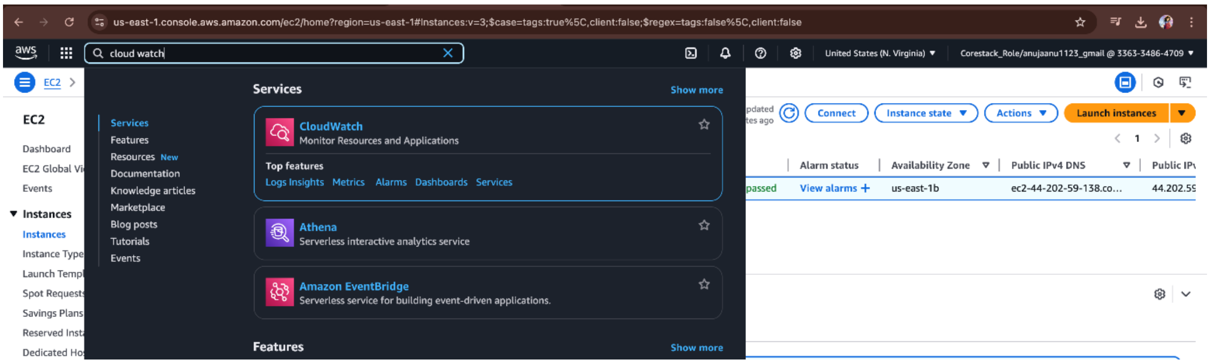
1h 3h 12h 1d 3d 1w Custom

CPU utilization (%) — No data available. Try adjusting the dashboard time range.
Network in (bytes) — No data available. Try adjusting the dashboard time range.
Network out (bytes) — No data available. Try adjusting the dashboard time range.
Network packets in (count) — No data available. Try adjusting the dashboard time range.
Network packets out (count) — No data available. Try adjusting the dashboard time range.
Metadata no token (count) — No data available. Try adjusting the dashboard time range.
CPU credit usage (count) — No data available. Try adjusting the dashboard time range.
CPU credit balance (count) — No data available. Try adjusting the dashboard time range.

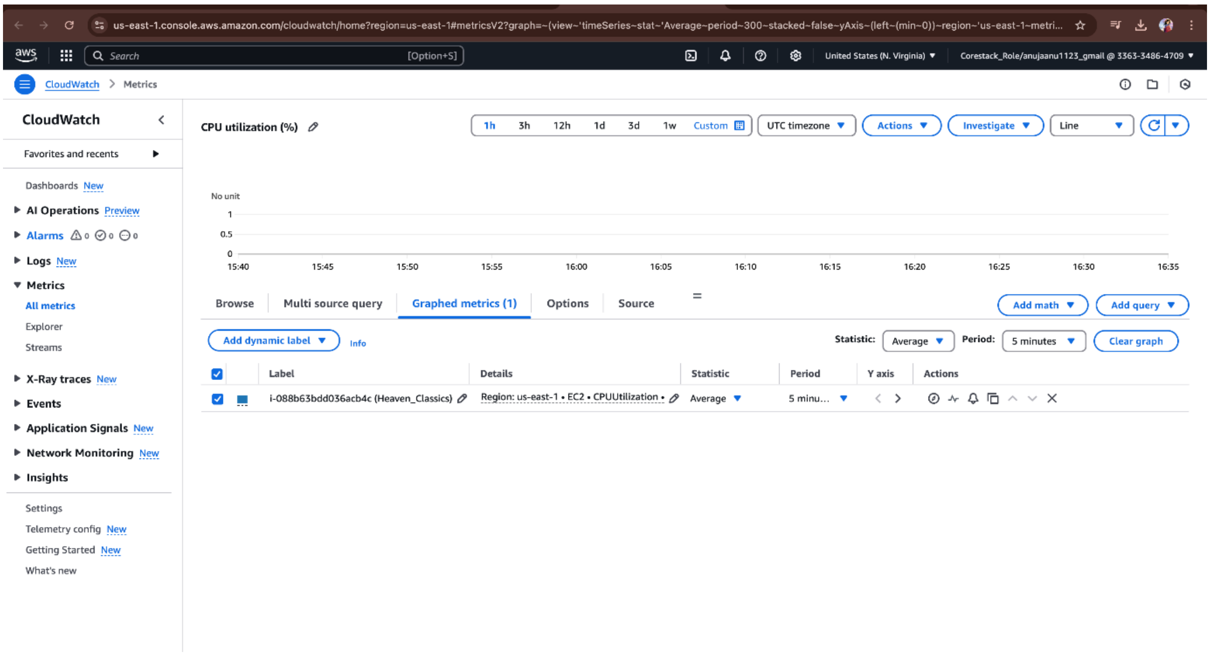

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:v=3;$case=tags:true%5C,client:false;$regex=tags:false%5C,client:false
CPU utilization (%)
5 minutes
Average
1h
3h
12h
1d
3d
1w
Custom
UTC timezone
No unit
1
0.8
0.6
0.498
0.4
0.2
0
15:40
15:45
15:50
15:55
03-25 16:00
16:05
16:10
16:15
16:20
16:25
16:30
16:35
i-088b63bdd036acb4c (Heaven_Classics)
1. i-088b63bdd036acb4c (Heaven_Classics) -
View in metrics
Close

Creating cloud watch alarm:

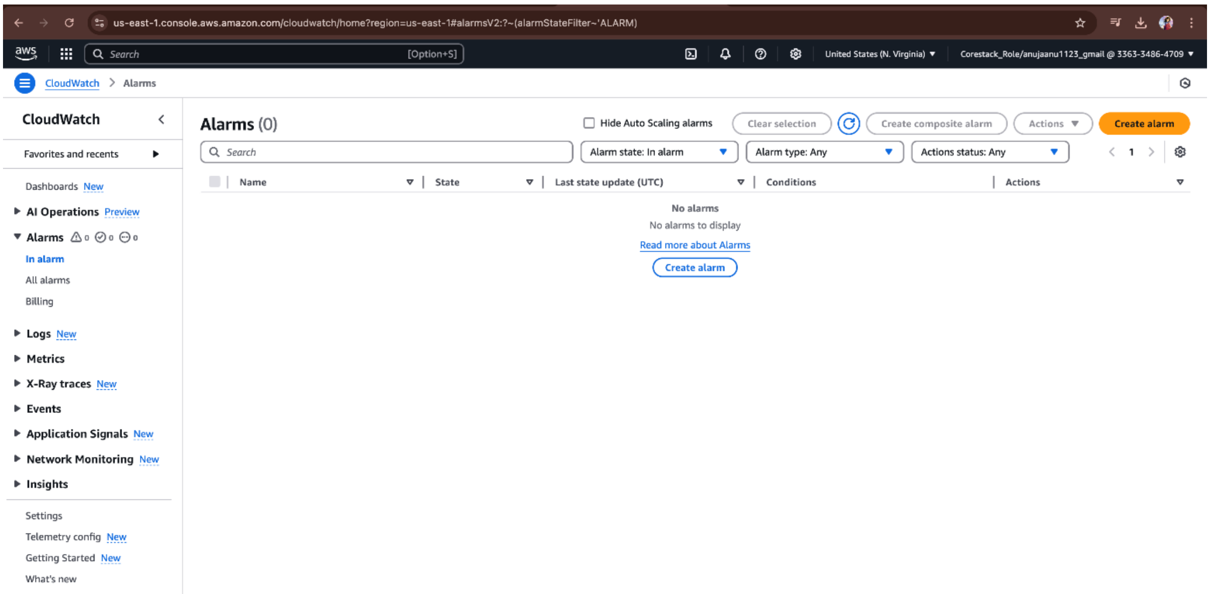
On search bar search for cloud watch. The press enter.



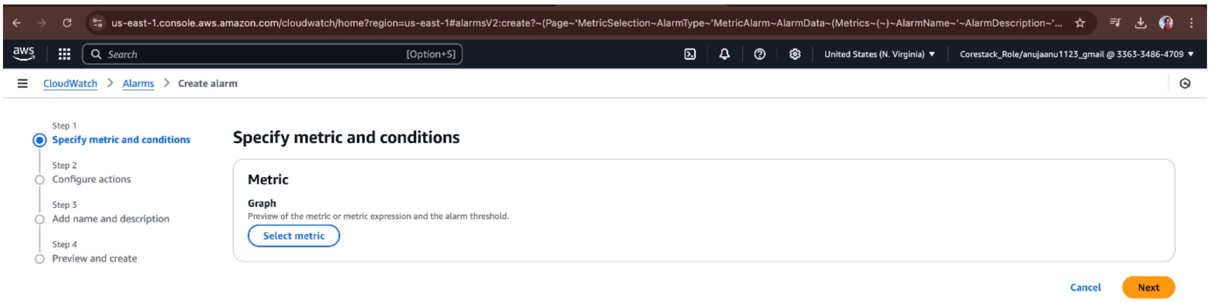
Press on Alarms then press on create alarm.



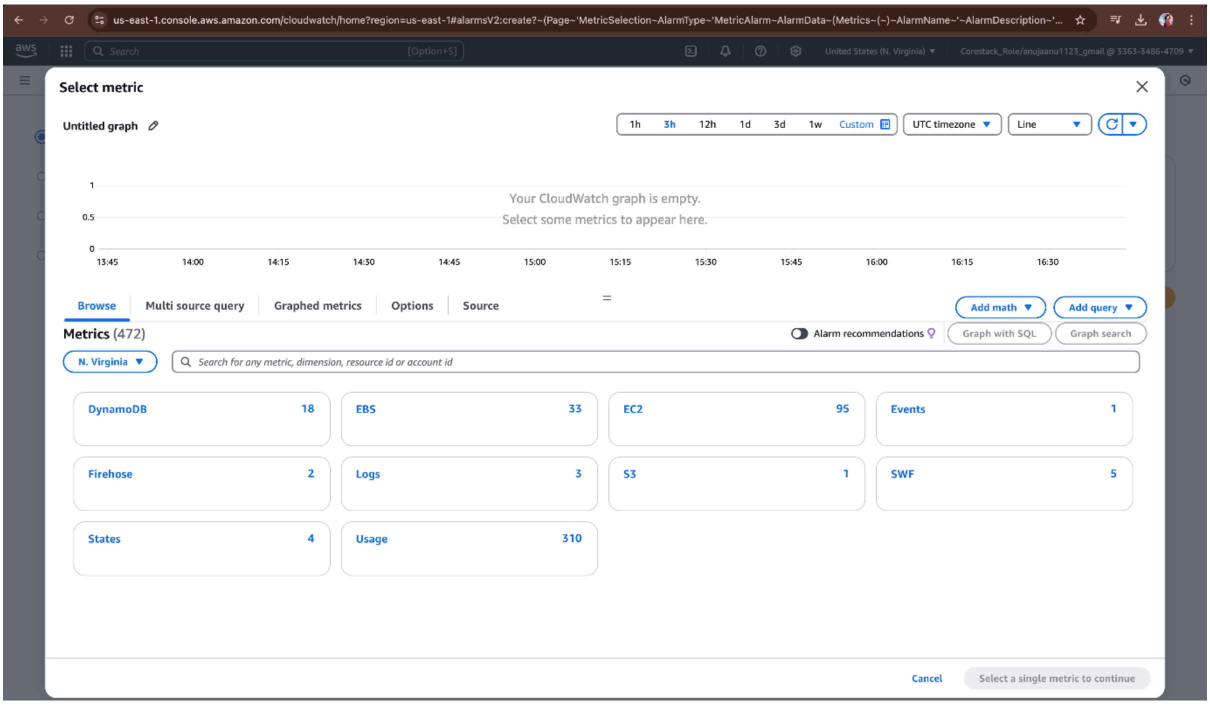
☑	Label	Details	Statistic	Period	Y axis	Actions
☑	i-088b63bdd036acb4c (Heaven_Classics)	Region: us-east-1 • EC2 • CPUUtilization •	Average	5 minu...	< >	

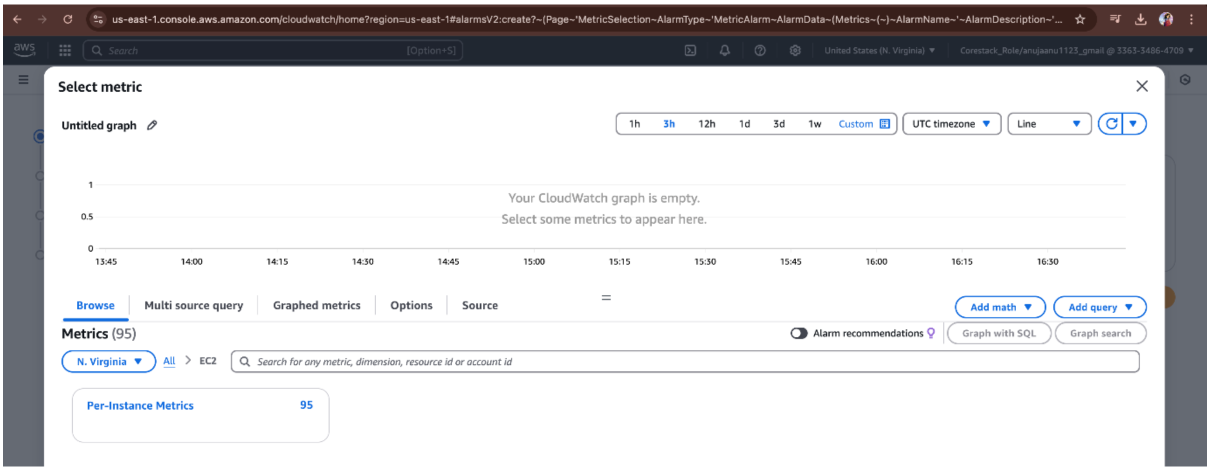


And specify the metrics and conditions and press on select metrics.

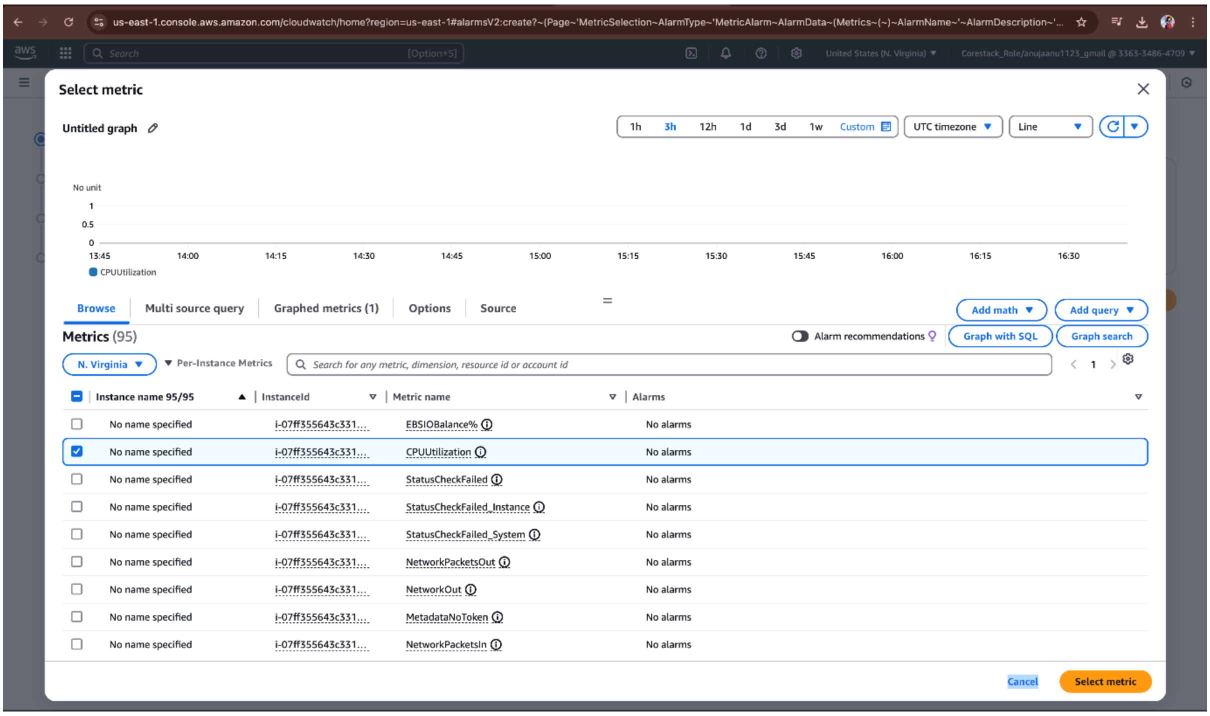

us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create?~(Page~'MetricSelection~AlarmType~'MetricAlarm~AlarmData~(Metrics~(~)~AlarmName~'~AlarmDescription~'...
Search [Option+S]
United States (N. Virginia)
Corestack_Role/anujaanu1123_gmail @ 3363-3486-4709
CloudWatch > Alarms > Create alarm
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add name and description
Step 4
Preview and create
Specify metric and conditions
Metric
Graph
Preview of the metric or metric expression and the alarm threshold.
Select metric
Cancel
Next

in select metrics select EC2





In that select metrics select CPU utilization. And press on select metrics.



us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create?~(Page~'MetricSelection~AlarmType~'MetricAlarm~AlarmData~(Metrics~(~)~AlarmName~'~AlarmDescription~'...

United States (N. Virginia) ▼   Corestack_Role/anujaanu1123_gmail @ 3363-3486-4709 ▼

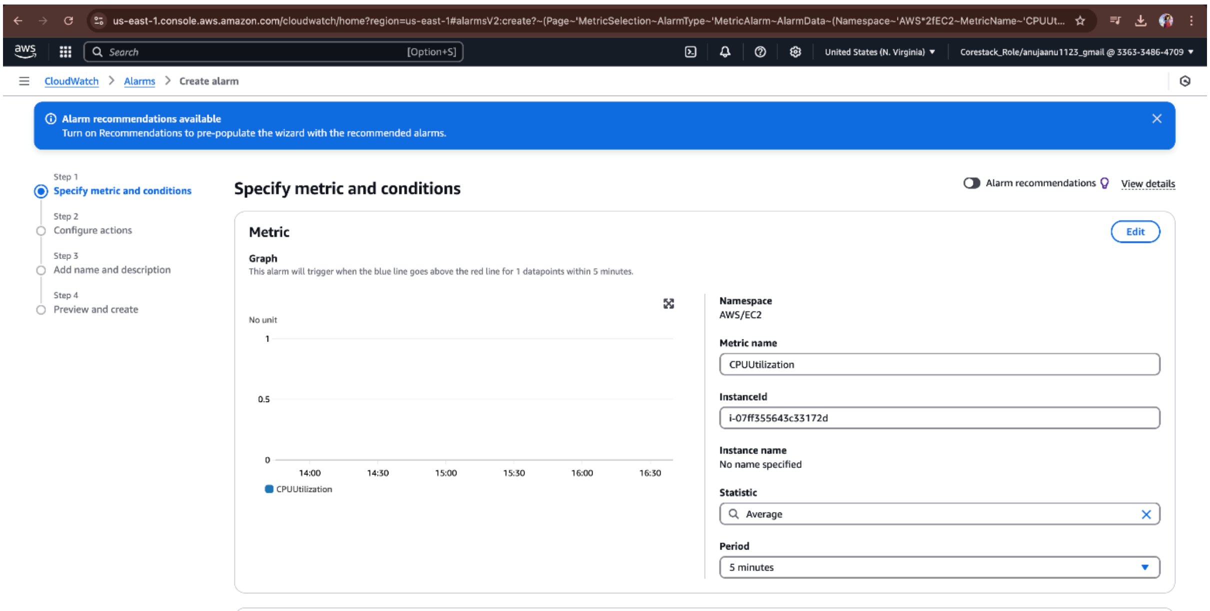
Select metric

Untitled graph

Metrics (95)

	Instance name 95/95	InstanceId	Metric name	Alarms
☐	No name specified	i-07ff355643c331...	EBSIOBalance%	No alarms
☑	No name specified	i-07ff355643c331...	CPUUtilization	No alarms
☐	No name specified	i-07ff355643c331...	StatusCheckFailed	No alarms
☐	No name specified	i-07ff355643c331...	StatusCheckFailed_Instance	No alarms
☐	No name specified	i-07ff355643c331...	StatusCheckFailed_System	No alarms
☐	No name specified	i-07ff355643c331...	NetworkPacketsOut	No alarms
☐	No name specified	i-07ff355643c331...	NetworkOut	No alarms
☐	No name specified	i-07ff355643c331...	MetadataNoToken	No alarms
☐	No name specified	i-07ff355643c331...	NetworkPacketsIn	No alarms

Then the select metrics step will look like this



us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create?~(Page~'MetricSelection~AlarmType~'MetricAlarm~AlarmData~(Namespace~'AWS*2fEC2~MetricName~'CPUUt...

United States (N. Virginia) ▼   Corestack_Role/anujaanu1123_gmail @ 3363-3486-4709 ▼

CloudWatch > Alarms > Create alarm

Alarm recommendations available
Turn on Recommendations to pre-populate the wizard with the recommended alarms.

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
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

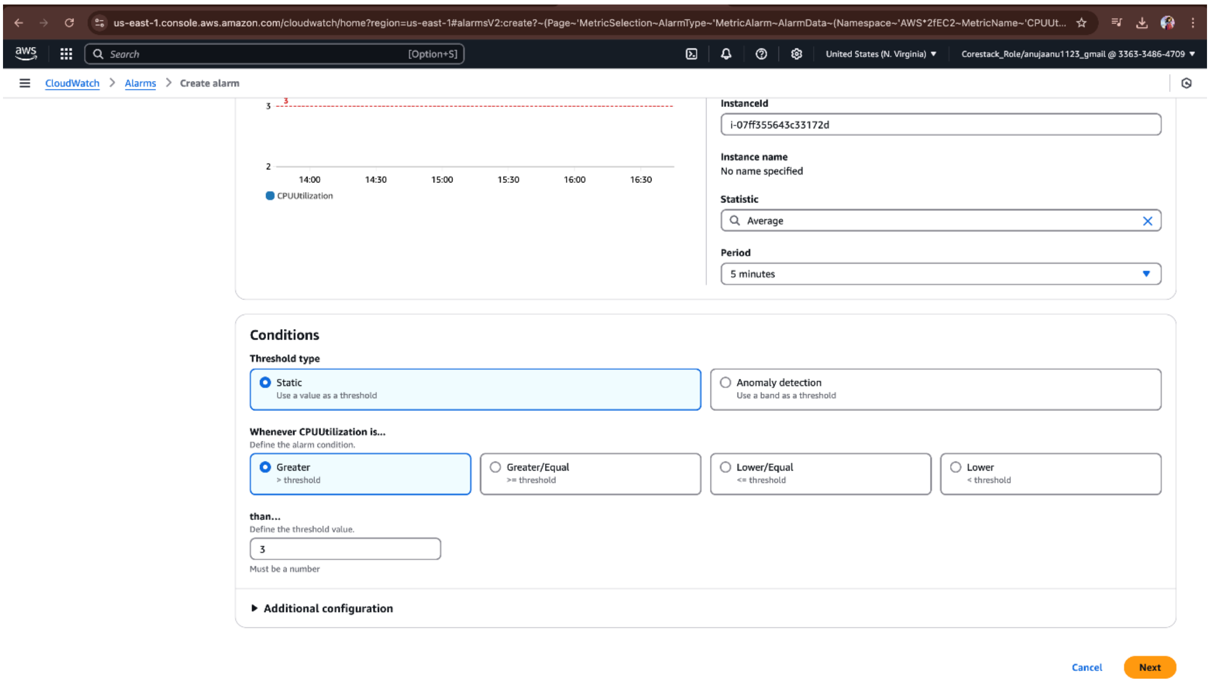
InstanceId
i-07ff355643c33172d

Instance name
No name specified

Statistic
Average

Period
5 minutes ▼

And select conditions in threshold type select static and select whenever CPU utilization is greater that 3 we need to get notification. And press next,



us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create?~(Page~'MetricSelection~AlarmType~'MetricAlarm~AlarmData~(Namespace~'AWS*2fEC2~MetricName~'CPUUt...

CloudWatch > Alarms > Create alarm

InstanceId
i-07ff355643c33172d

Instance name
No name specified

Statistic
Average

Period
5 minutes

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.

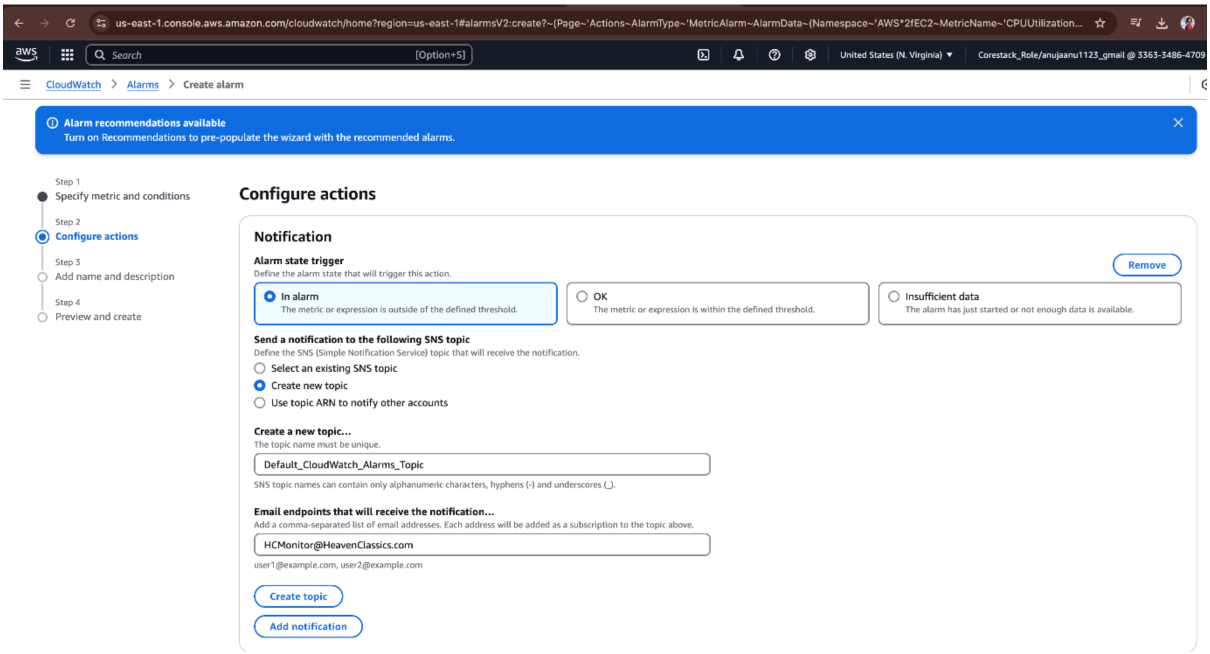
● Greater — > threshold
○ Greater/Equal — >= threshold
○ Lower/Equal — <= threshold
○ Lower — < threshold

than...
Define the threshold value.
3
Must be a number

▶ Additional configuration

Cancel Next

In configuration actions select alarm state trigger in alarm and send a notification to SNS topic select as create new topic and give alarm name and give email notification as HCMonitor@HeavenClassics.com and press on create SNS topic.



us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create?~(Page~'Actions~AlarmType~'MetricAlarm~AlarmData~(Namespace~'AWS*2fEC2~MetricName~'CPUUtilization...

CloudWatch > Alarms > Create alarm

Alarm recommendations available
Turn on Recommendations to pre-populate the wizard with the recommended alarms.

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.

Send a notification to the following 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 to notify other accounts

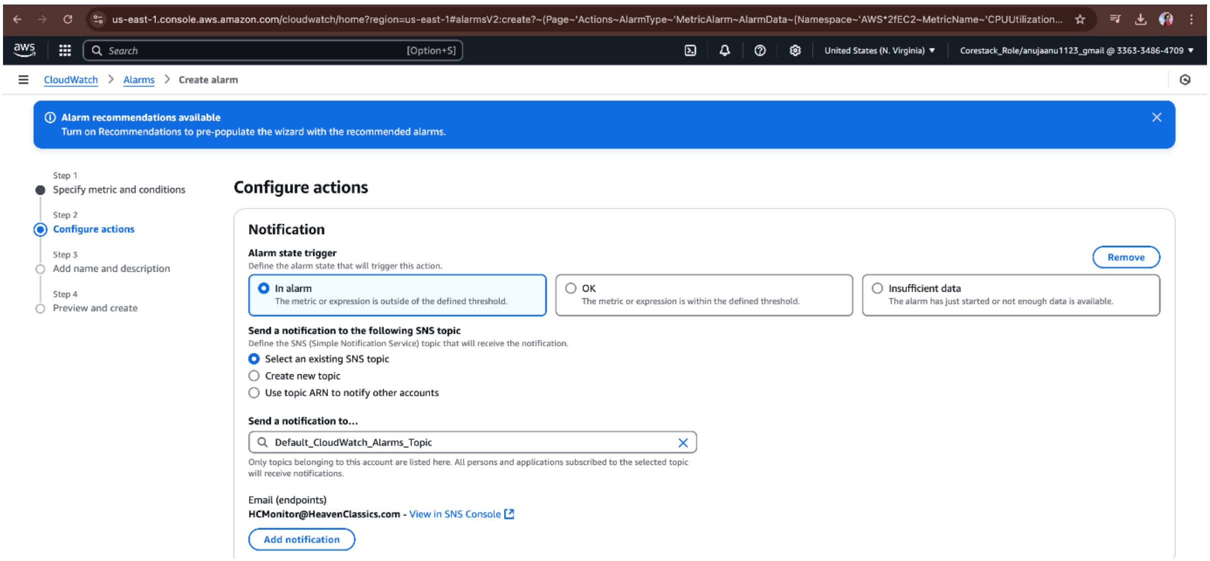
Create a new topic...
The topic name must be unique.
Default_CloudWatch_Alarms_Topic
SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).

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.
HCMonitor@HeavenClassics.com
user1@example.com, user2@example.com

Create topic

Add notification

And just review all the things and in additional configuration give datapoints to alarm as 3 why means in our description we have a condition like utilization goes below the threshold of 3%, consecutively three times for five minutes then we need to get email notification.



us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create?~(Page~'Actions~AlarmType~'MetricAlarm~AlarmData~(Namespace~'AWS*2fEC2~MetricName~'CPUUtilization...

United States (N. Virginia) ▾ Corestack_Role/anujaanu1123_gmail @ 3363-3486-4709 ▾

CloudWatch > Alarms > Create alarm

Alarm recommendations available
Turn on Recommendations to pre-populate the wizard with the recommended alarms.

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.

● In alarm
The metric or expression is outside of the defined threshold.

○ OK
The metric or expression is within the defined threshold.

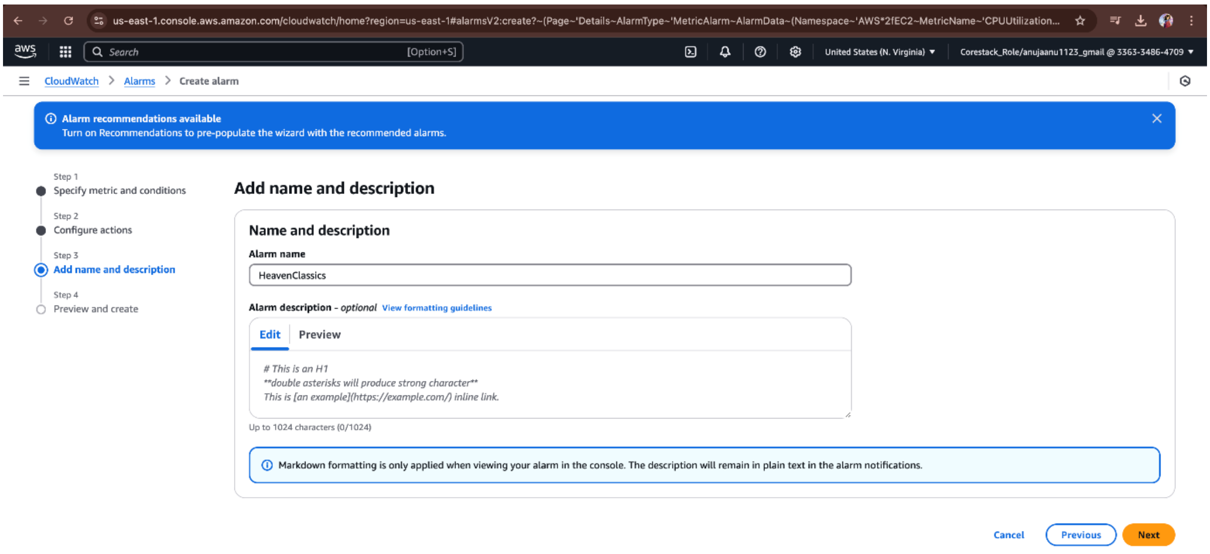
○ Insufficient data
The alarm has just started or not enough data is available.

Send a notification to the following 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 to notify other accounts

Send a notification to...
Default_CloudWatch_Alarms_Topic
Only topics belonging to this account are listed here. All persons and applications subscribed to the selected topic will receive notifications.

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



us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create?~(Page~'Details~AlarmType~'MetricAlarm~AlarmData~(Namespace~'AWS*2fEC2~MetricName~'CPUUtilization...

United States (N. Virginia) ▾ Corestack_Role/anujaanu1123_gmail @ 3363-3486-4709 ▾

CloudWatch > Alarms > Create alarm

Alarm recommendations available
Turn on Recommendations to pre-populate the wizard with the recommended alarms.

Step 1
Specify metric and conditions

Step 2
Configure actions

Step 3
Add name and description

Step 4
Preview and create

Add name and description

Name and description

Alarm name
HeavenClassics

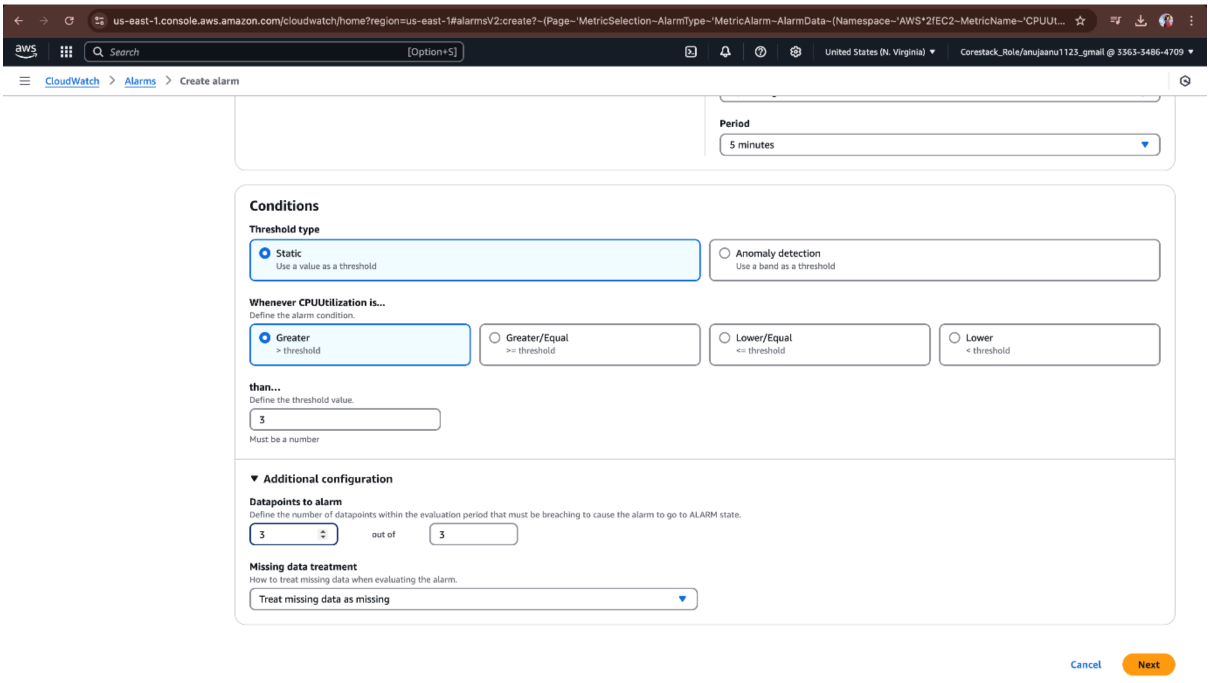
Alarm description - *optional* View formatting guidelines

Edit Preview

# This is an H1
double asterisks will produce strong character
This is [an example](https://example.com/) inline link.

Up to 1024 characters (0/1024)

Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.



us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create?~(Page~'MetricSelection~AlarmType~'MetricAlarm~AlarmData~(Namespace~'AWS*2fEC2~MetricName~'CPUUt...

United States (N. Virginia) ▾ Corestack_Role/anujaanu1123_gmail @ 3363-3486-4709 ▾

CloudWatch > Alarms > Create alarm

Period
5 minutes

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

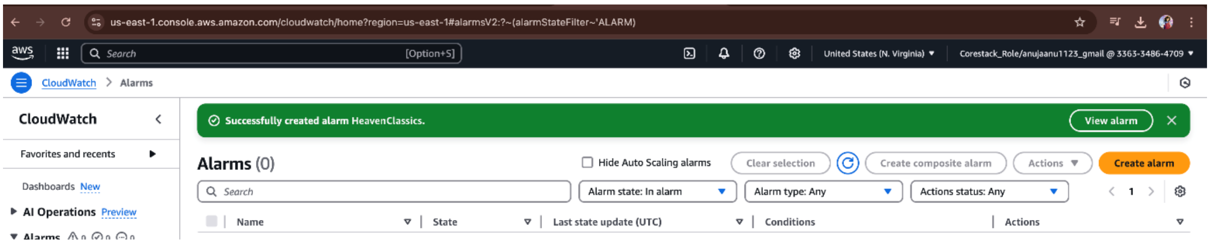
than...
Define the threshold value.
3
Must be a number

▼ **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

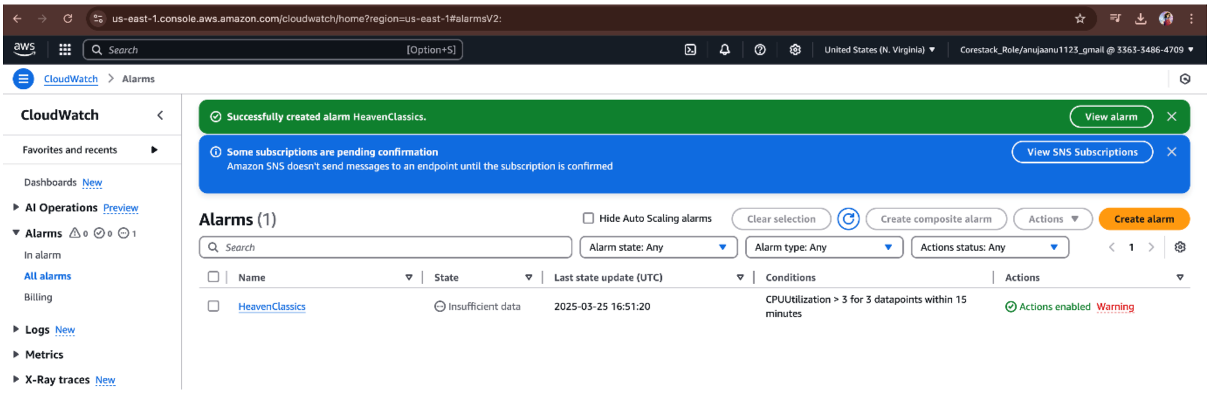
Missing data treatment
How to treat missing data when evaluating the alarm.
Treat missing data as missing

And finally press on create alarm.



Successfully created alarm HeavenClassics.

Then you need to verify your email then your SNS topic will be active.



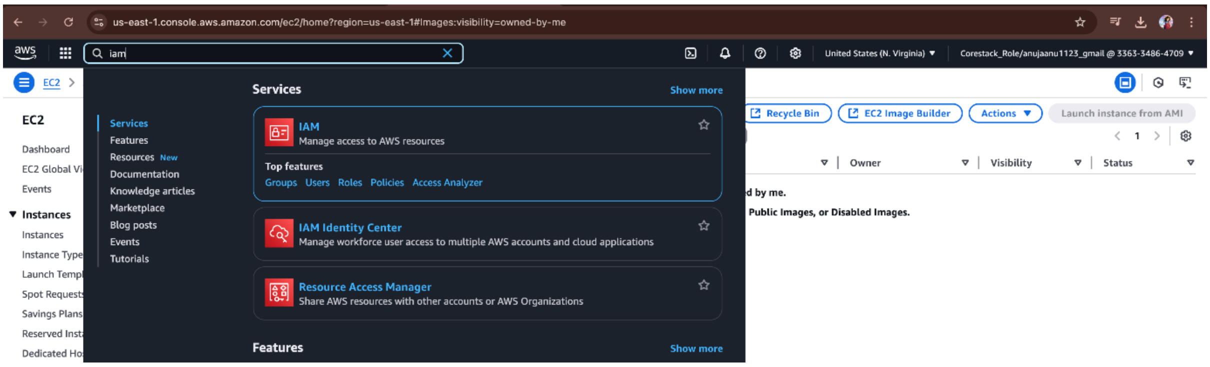
Successfully created alarm HeavenClassics.

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

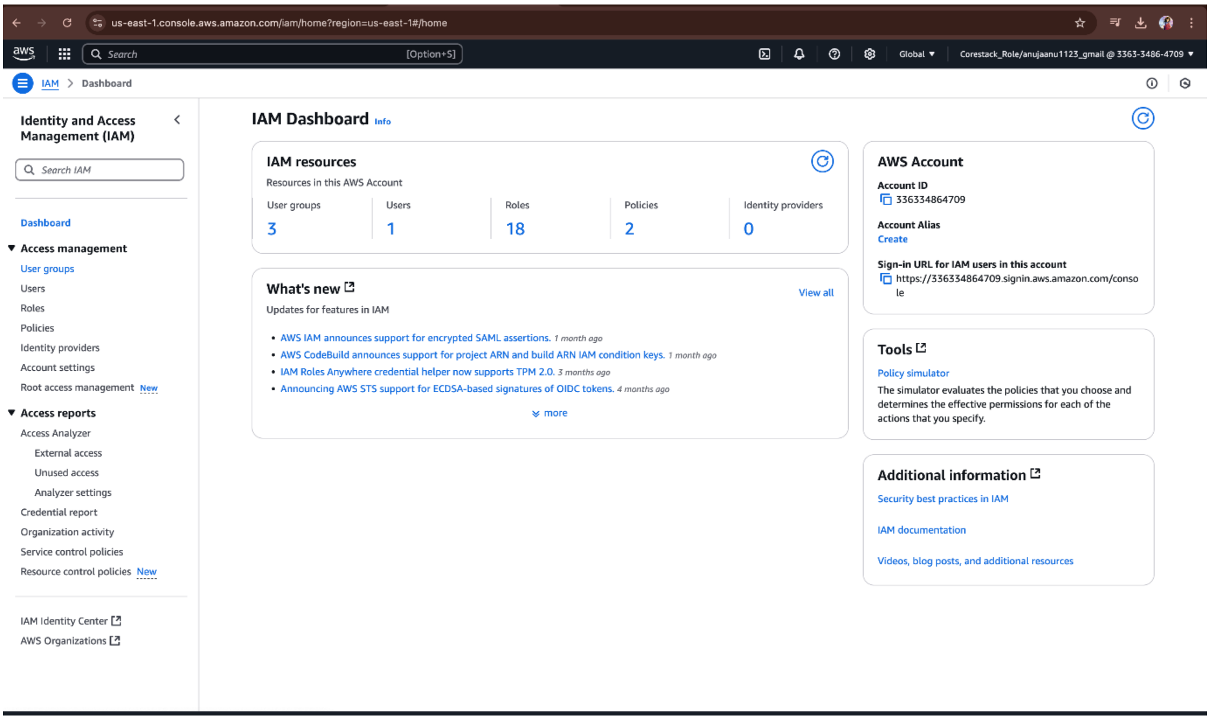
Name	State	Last state update (UTC)	Conditions	Actions
HeavenClassics	Insufficient data	2025-03-25 16:51:20	CPUUtilization > 3 for 3 datapoints within 15 minutes	Actions enabled Warning

Creating a group and giving administrator access to new user in the group:

Open AWS console and click on IAM (Identity and access management) in search bar



Click on user group and create a new group.



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/home

Search [Option+S] Global ▾ Corestack_Role/anujaanu1123_gmail @ 3363-3486-4709 ▾

IAM > Dashboard

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New

▼ Access reports

Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New

IAM Identity Center
AWS Organizations

IAM Dashboard Info

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
3	1	18	2	0

What's new

Updates for features in IAM

View all

- AWS IAM announces support for encrypted SAML assertions. *1 month ago*
- AWS CodeBuild announces support for project ARN and build ARN IAM condition keys. *1 month ago*
- IAM Roles Anywhere credential helper now supports TPM 2.0. *3 months ago*
- Announcing AWS STS support for ECDSA-based signatures of OIDC tokens. *4 months ago*

more

AWS Account

Account ID
336334864709

Account Alias
Create

Sign-in URL for IAM users in this account
https://336334864709.signin.aws.amazon.com/console

Tools

Policy simulator

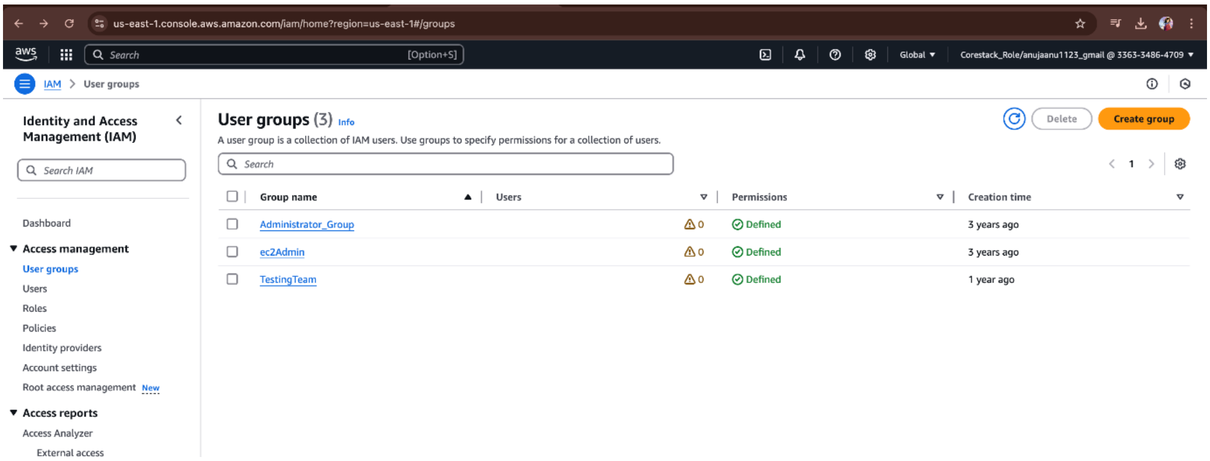
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

Additional information

Security best practices in IAM

IAM documentation

Videos, blog posts, and additional resources



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/groups

Search [Option+S] Global ▾ Corestack_Role/anujaanu1123_gmail @ 3363-3486-4709 ▾

IAM > User groups

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New

▼ Access reports

Access Analyzer
External access

User groups (3) Info

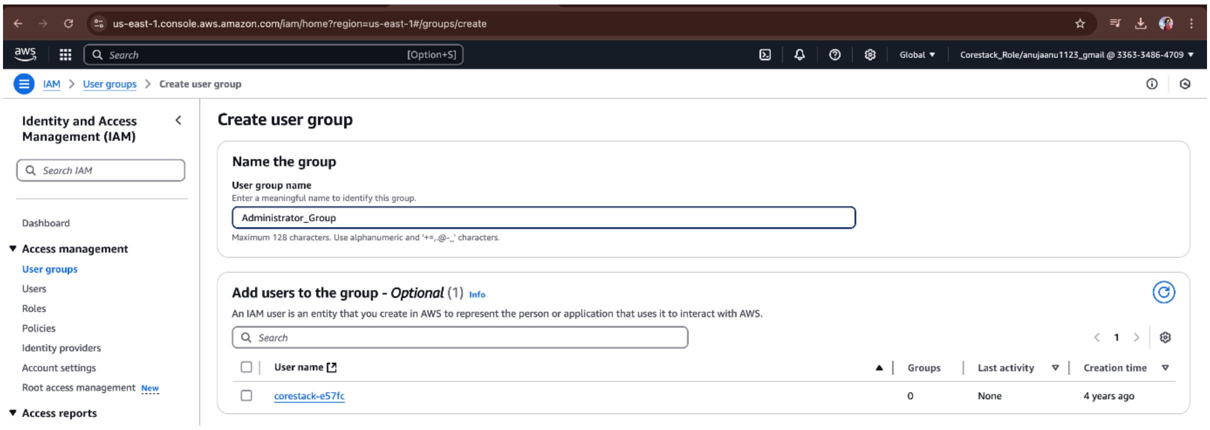
Delete Create group

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Search

□	Group name ▲	Users	Permissions	Creation time
□	Administrator_Group	⚠ 0	✓ Defined	3 years ago
□	ec2Admin	⚠ 0	✓ Defined	3 years ago
□	TestingTeam	⚠ 0	✓ Defined	1 year ago

And a name to your group.



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/groups/create

Search [Option+S] Global ▾ Corestack_Role/anujaanu1123_gmail @ 3363-3486-4709 ▾

IAM > User groups > Create user group

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New

▼ Access reports

Create user group

Name the group

User group name
Enter a meaningful name to identify this group.

Administrator_Group

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

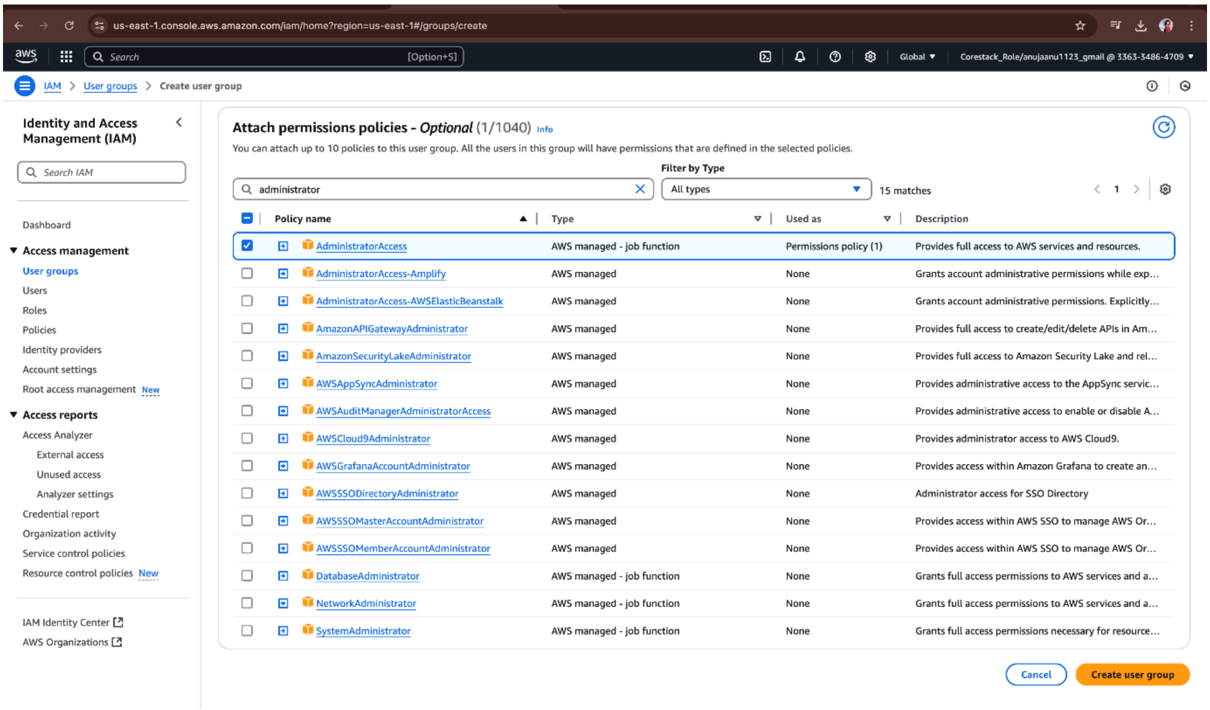
Add users to the group - *Optional* (1) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search

□	User name ▲	Groups	Last activity	Creation time
□	corestack-e57fc	0	None	4 years ago

And in attach permission column attach permission as Administrator access it will grant full administrator access. Then click on create group.



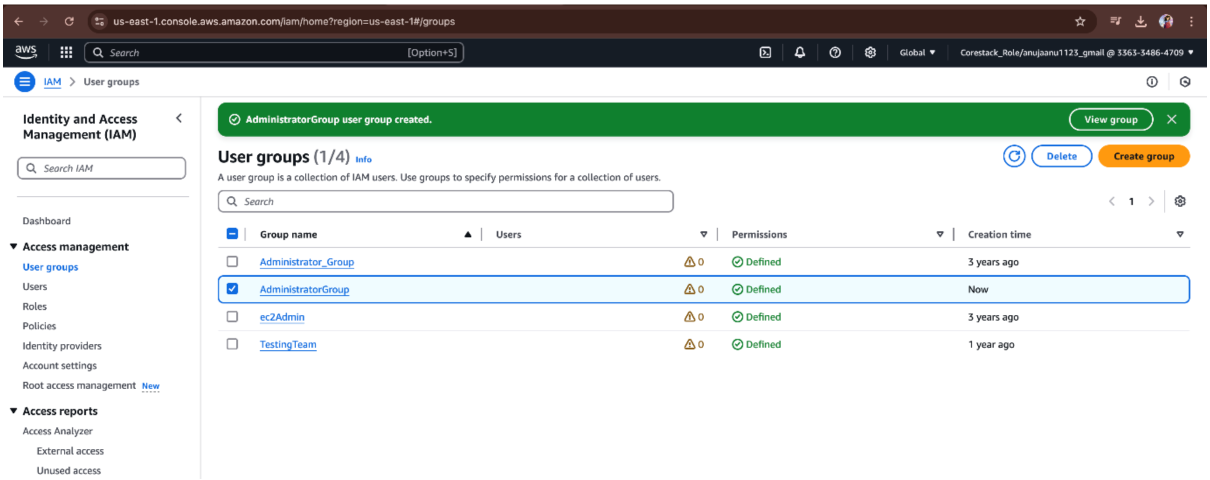
Attach permissions policies - *Optional* (1/1040) Info

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.

Search: administrator | Filter by Type: All types | 15 matches

	Policy name	Type	Used as	Description
☑	AdministratorAccess	AWS managed - job function	Permissions policy (1)	Provides full access to AWS services and resources.
□	AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissions while exp...
□	AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permissions. Explicitly...
□	AmazonAPIGatewayAdministrator	AWS managed	None	Provides full access to create/edit/delete APIs in Am...
□	AmazonSecurityLakeAdministrator	AWS managed	None	Provides full access to Amazon Security Lake and rel...
□	AWSAppSyncAdministrator	AWS managed	None	Provides administrative access to the AppSync servic...
□	AWSAuditManagerAdministratorAccess	AWS managed	None	Provides administrative access to enable or disable A...
□	AWSCloud9Administrator	AWS managed	None	Provides administrator access to AWS Cloud9.
□	AWSGrafanaAccountAdministrator	AWS managed	None	Provides access within Amazon Grafana to create an...
□	AWSSSODirectoryAdministrator	AWS managed	None	Administrator access for SSO Directory
□	AWSSSOMasterAccountAdministrator	AWS managed	None	Provides access within AWS SSO to manage AWS Or...
□	AWSSSOMemberAccountAdministrator	AWS managed	None	Provides access within AWS SSO to manage AWS Or...
□	DatabaseAdministrator	AWS managed - job function	None	Grants full access permissions to AWS services and a...
□	NetworkAdministrator	AWS managed - job function	None	Grants full access permissions to AWS services and a...
□	SystemAdministrator	AWS managed - job function	None	Grants full access permissions necessary for resource...

It will create a new group. Now we need to create a user and need to attach in that group.



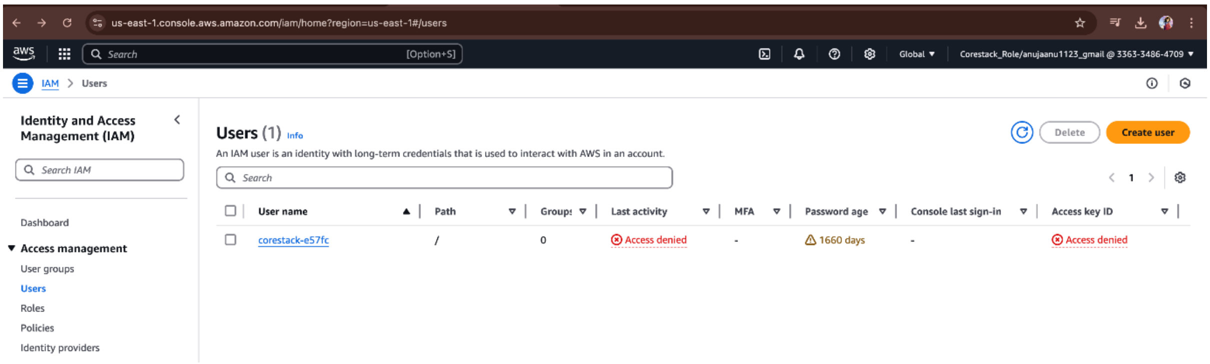
AdministratorGroup user group created.

User groups (1/4) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

	Group name	Users	Permissions	Creation time
□	Administrator_Group	⚠ 0	✓ Defined	3 years ago
☑	AdministratorGroup	⚠ 0	✓ Defined	Now
□	ec2Admin	⚠ 0	✓ Defined	3 years ago
□	TestingTeam	⚠ 0	✓ Defined	1 year ago

click on user and create user.

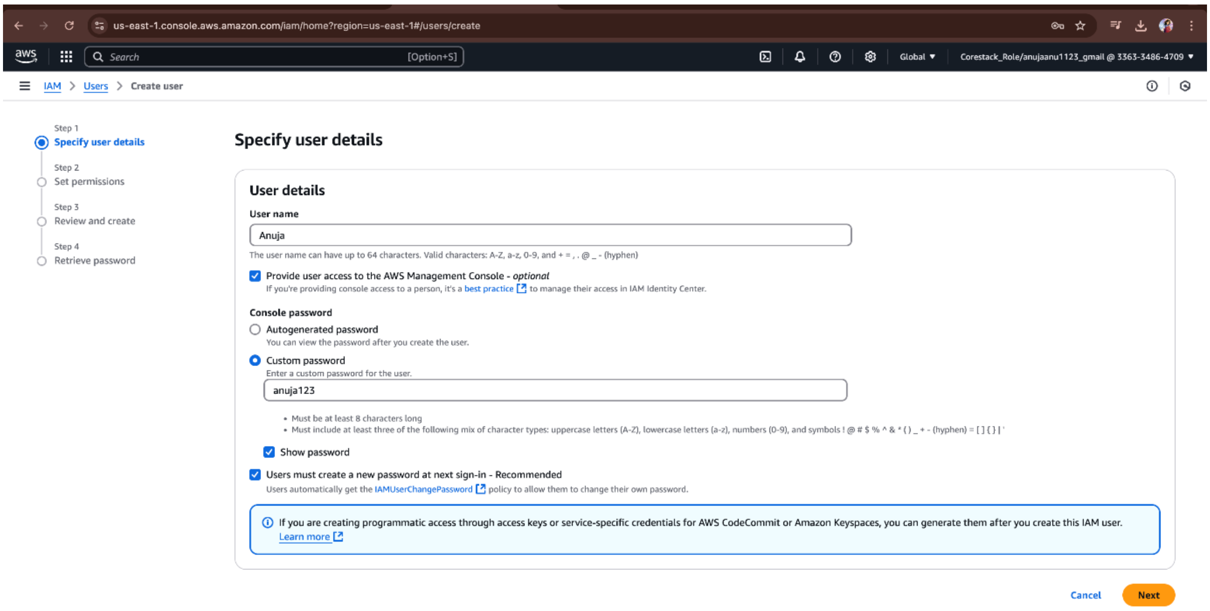

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users

Users (1) Info

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

□	User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID
□	corestack-e57fc	/	0	Access denied	-	1660 days	-	Access denied

Now we need to specify the user details like name and password after that press on next.


us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create

Specify user details

User details

User name: Anuja

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.

Console password

○ Autogenerated password
You can view the password after you create the user.

● Custom password
Enter a custom password for the user.

anuja123

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

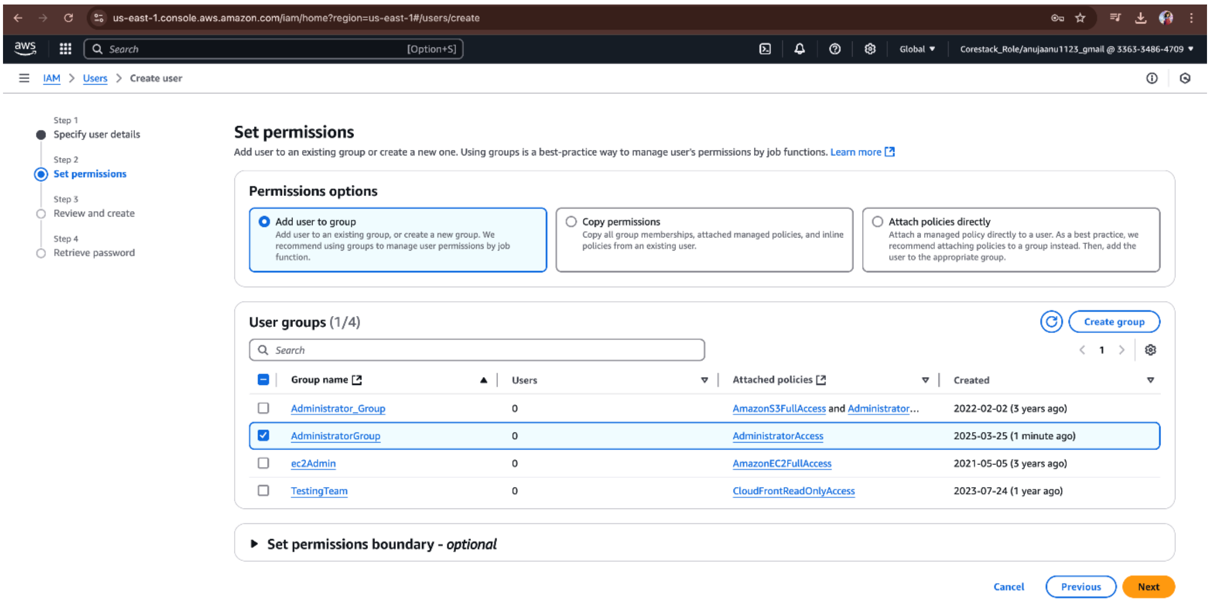
☑ Show password

☑ Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more

In set permission select add user to group and select your group name which you need to add this user.

By adding in that group our user will also get all the permissions which are there applicable for the group. And then press next.



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create

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.

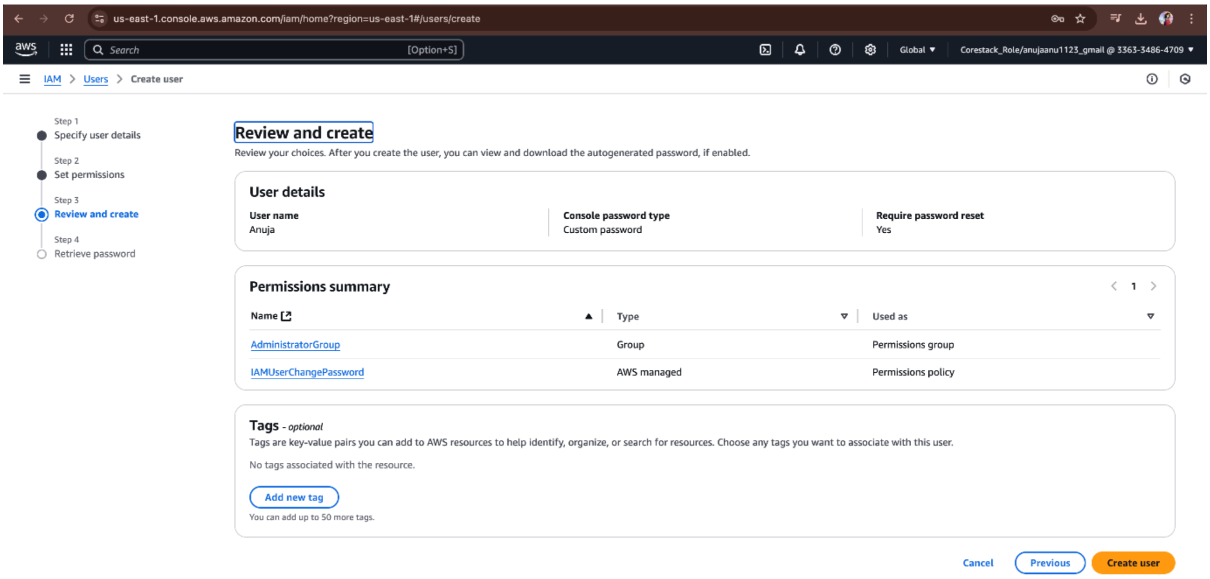
○ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1/4)

	Group name	Users	Attached policies	Created
□	Administrator_Group	0	AmazonS3FullAccess and Administrator...	2022-02-02 (3 years ago)
☑	AdministratorGroup	0	AdministratorAccess	2025-03-25 (1 minute ago)
□	ec2Admin	0	AmazonEC2FullAccess	2021-05-05 (3 years ago)
□	TestingTeam	0	CloudFrontReadOnlyAccess	2023-07-24 (1 year ago)

▶ Set permissions boundary - *optional*

Review and create the user.



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create

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
Anuja	Custom password	Yes

Permissions summary

Name	Type	Used as
AdministratorGroup	Group	Permissions group
IAMUserChangePassword	AWS managed	Permissions policy

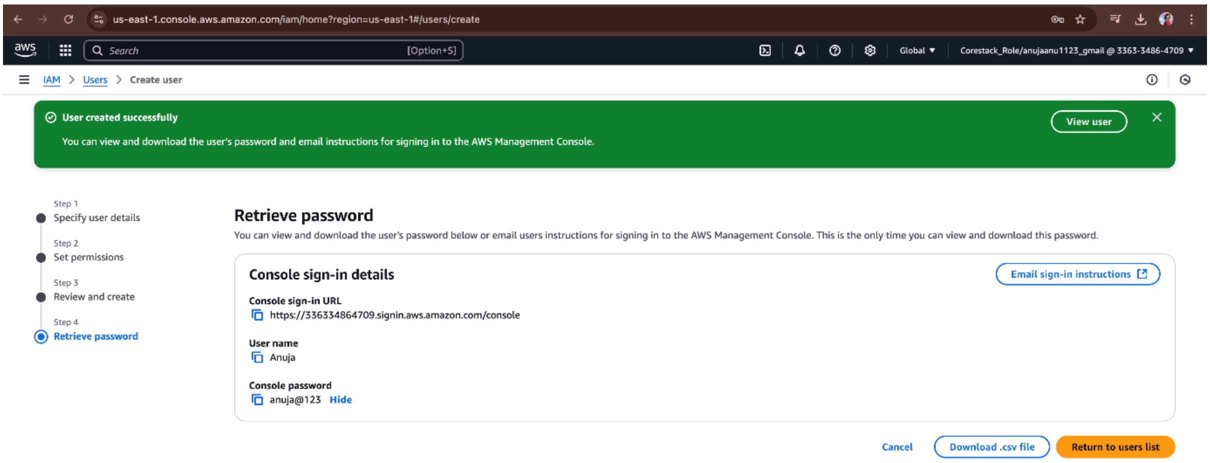
Tags - *optional*

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

You can add up to 50 more tags.

After that your user name and password will visible please remember them.



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create
Search [Option+S]
Global
Corestack_Role/anujaanu1123_gmail @ 3363-3486-4709
IAM > Users > Create user
View user
Email sign-in instructions
Cancel
Download .csv file
Return to users list

User created successfully

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

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Retrieve password

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

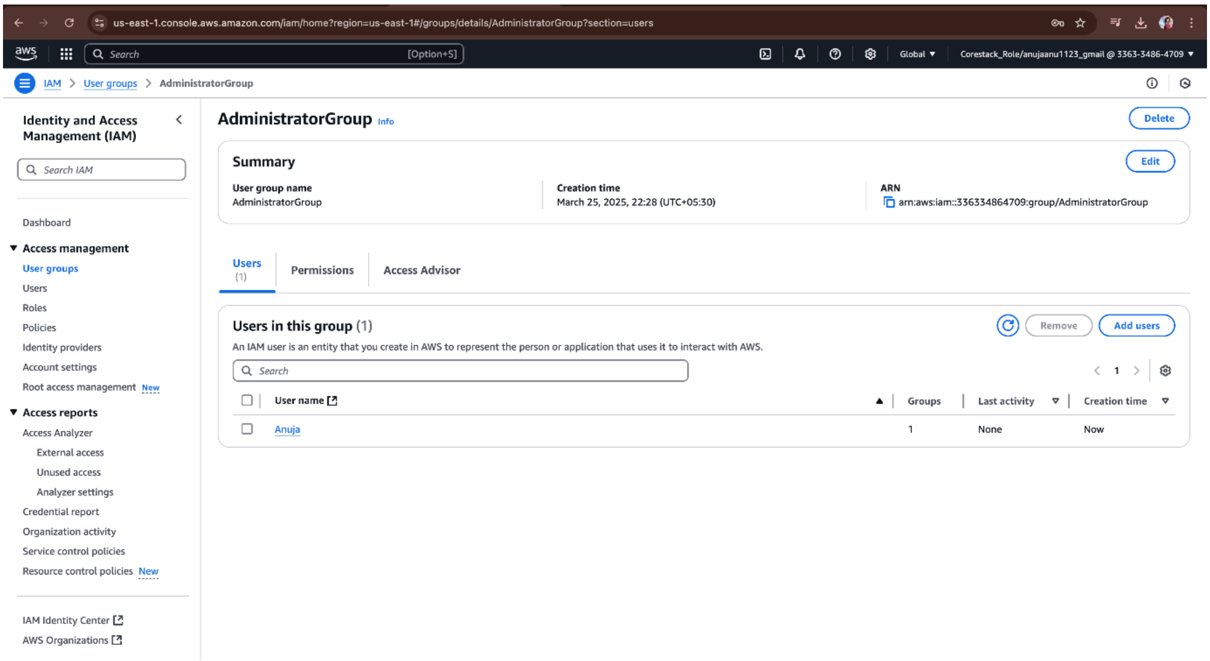
Console sign-in details

Console sign-in URL
https://336334864709.signin.aws.amazon.com/console

User name
Anuja

Console password
anuja@123 Hide

Finally you can able to see your user in the created and having administrator access.



AdministratorGroup

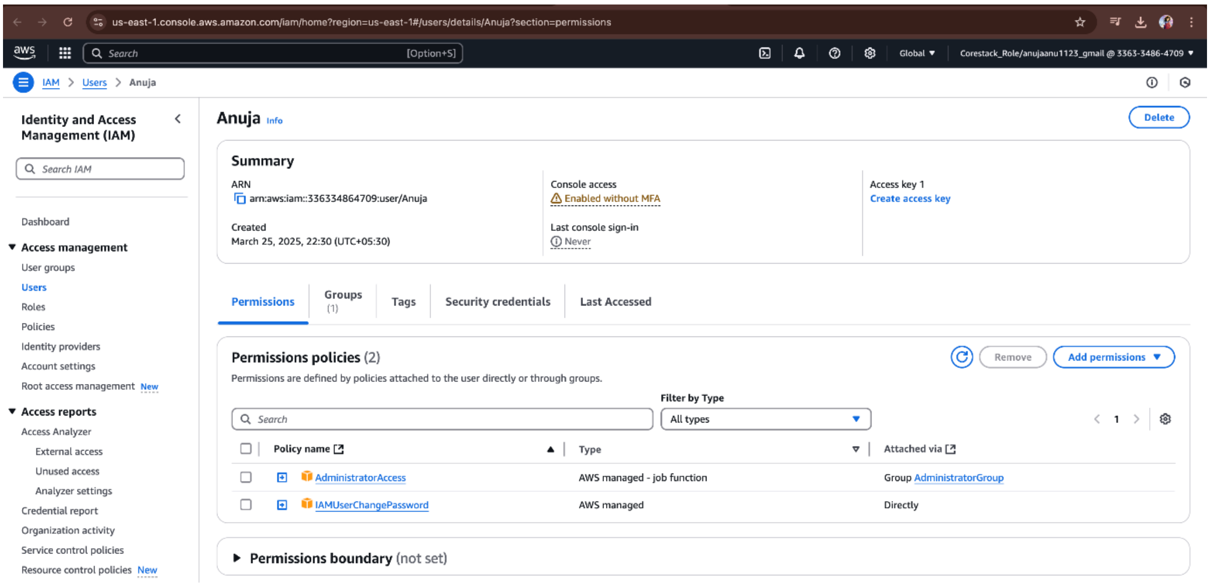
Summary

User group name	Creation time	ARN
AdministratorGroup	March 25, 2025, 22:28 (UTC+05:30)	arn:aws:iam::336334864709:group/AdministratorGroup

Users in this group (1)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

□	User name	Groups	Last activity	Creation time
□	Anuja	1	None	Now



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/Anuja?section=permissions

Identity and Access Management (IAM)

Anuja Info

Summary

ARN
arn:aws:iam::336334864709:user/Anuja

Created
March 25, 2025, 22:30 (UTC+05:30)

Console access
⚠ Enabled without MFA

Last console sign-in
Never

Access key 1
Create access key

Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: All types

□	Policy name	Type	Attached via
□	AdministratorAccess	AWS managed - job function	Group AdministratorGroup
□	IAMUserChangePassword	AWS managed	Directly

▶ **Permissions boundary** (not set)