

# AWS Technical Essentials Project – Server Monitoring

## DESCRIPTION

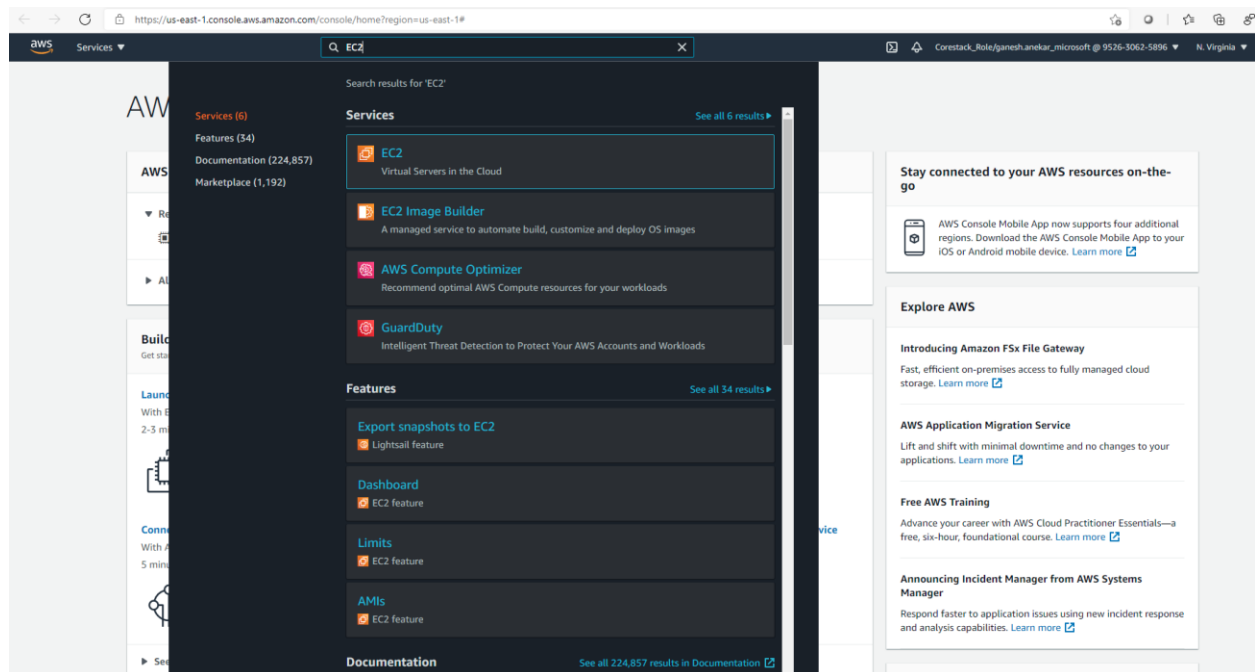
Heaven Classics successfully creates an EC2 Server Instance for Windows 2012 Server. After launching the instance on the server, the next step was to monitor the operations. Monitoring is important to keep an eye on the performance of an EC2 instance. It helps gather data from all parts and is useful 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:

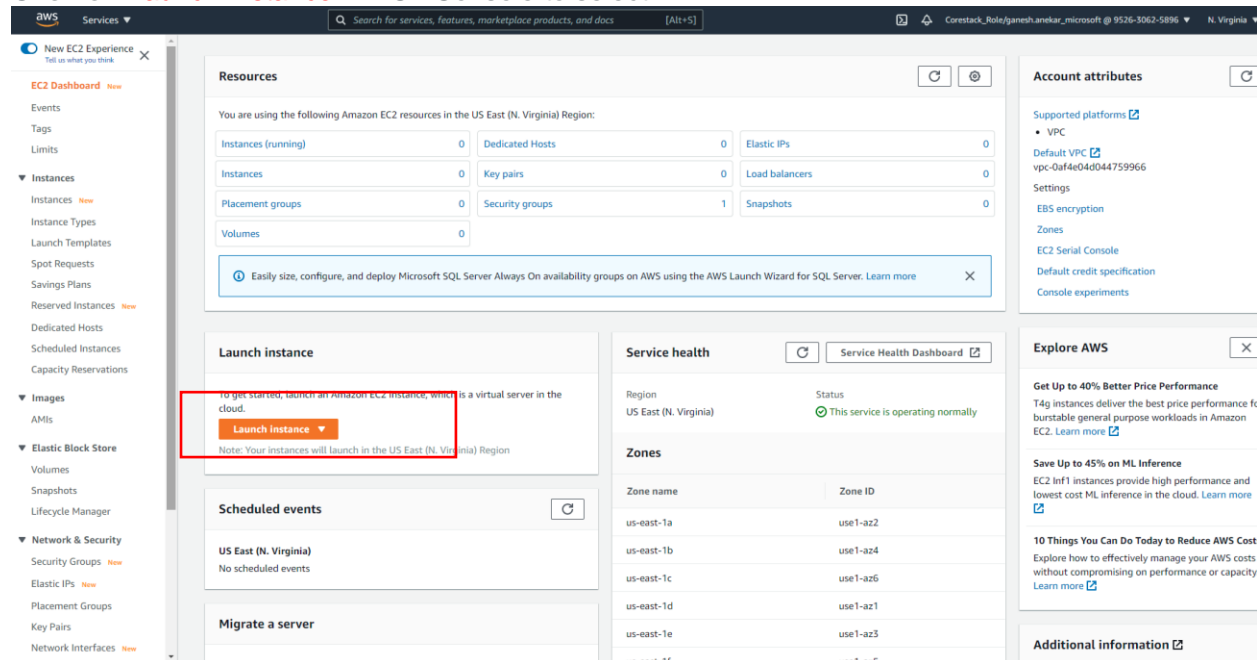
1. Check and observe the CPU utilization graph for the EC2 instance
2. Create and configure a CloudWatch alarm that sends an email notification to HCMonitor@HeavenClassics.com if the CPU utilization goes below the threshold of 3%, consecutively three times for five minutes
3. Create an IAM group named 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

## PART 1: Creating EC2 Instance for Windows 2021 Server.

Search **EC2** in AWS Console and Click on EC2 to go to EC2



## Click on **Launch Instance** in EC2 Console to select AMI



**Resources**

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

Resource	Count
Instances (running)	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.

**Launch Instance**

Note: Your instances will launch in the US East (N. Virginia) Region

**Scheduled events**

US East (N. Virginia)

No scheduled events

**Migrate a server**

**Service health**

Region: US East (N. Virginia) Status: This service is operating normally

**Zones**

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

**Account attributes**

Supported platforms

- VPC

Default VPC

vpc-0af4e04d044759966

Settings

- EBs encryption
- Zones
- EC2 Serial Console
- Default credit specification
- Console experiments

**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](#)

Save Up to 45% on ML Inference

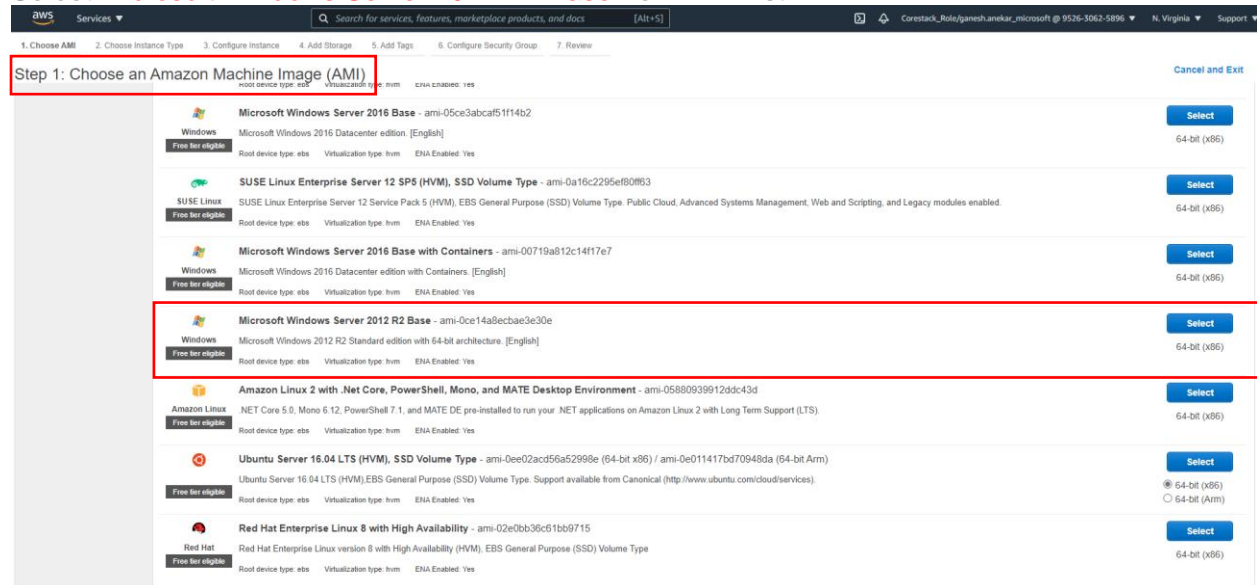
EC2 Inf1 instances provide high performance and lowest cost ML inference in the cloud. [Learn more](#)

10 Things You Can Do Today to Reduce AWS Costs

Explore how to effectively manage your AWS costs without compromising on performance or capacity. [Learn more](#)

**Additional information**

## Select **Microsoft Windows Server 2021 R2 Base** from AMI List



**Step 1: Choose an Amazon Machine Image (AMI)**

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

**Microsoft Windows Server 2021 R2 Base** - ami-0ce14a8ecbae3e30e

Microsoft Windows 2021 R2 Standard edition with 64-bit architecture. [English]

Root device type: ebs Virtualization type: hvm EHA Enabled: Yes

**Select**

64-bit (x86)

**Microsoft Windows Server 2016 Base** - ami-05ce3abca51114b2

Microsoft Windows 2016 Datacenter edition. [English]

Root device type: ebs Virtualization type: hvm EHA Enabled: Yes

**Select**

64-bit (x86)

**SUSE Linux Enterprise Server 12 SP5 (HVM), SSD Volume Type** - ami-0a16c2295ef80f63

SUSE Linux Enterprise Server 12 Service Pack 5 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.

Root device type: ebs Virtualization type: hvm EHA Enabled: Yes

**Select**

64-bit (x86)

**Microsoft Windows Server 2016 Base with Containers** - ami-00719a812c1417e7

Microsoft Windows 2016 Datacenter edition with Containers. [English]

Root device type: ebs Virtualization type: hvm EHA Enabled: Yes

**Select**

64-bit (x86)

**Amazon Linux 2 with .NET Core, PowerShell, Mono, and MATE Desktop Environment** - ami-05880939912d3c43d

.NET Core 5.0, Mono 6.12, PowerShell 7.1, and MATE DE pre-installed to run your .NET applications on Amazon Linux 2 with Long Term Support (LTS).

Root device type: ebs Virtualization type: hvm EHA Enabled: Yes

**Select**

64-bit (x86)

**Ubuntu Server 16.04 LTS (HVM), SSD Volume Type** - ami-0ee02acd56a52998e (64-bit x86) / ami-0e011417bd70948da (64-bit ARM)

Ubuntu Server 16.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Root device type: ebs Virtualization type: hvm EHA Enabled: Yes

**Select**

64-bit (x86)

**Red Hat Enterprise Linux 8 with High Availability** - ami-02e0bb36c51bb9715

Red Hat Enterprise Linux version 8 with High Availability (HVM), EBS General Purpose (SSD) Volume Type

Root device type: ebs Virtualization type: hvm EHA Enabled: Yes

**Select**

64-bit (x86)

## Step 2: Choose an Instance Type - Select **t2.micro** with 1 vCPU and 1GB Memory and Click **Next Configuration Instance Details**

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

**Step 2: Choose an Instance Type**

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance families Current generation Show/Hide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro <small>Free for eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.large	2	8	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.xlarge	4	16	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.2xlarge	8	32	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous **Review and Launch** **Next: Configure Instance Details**

## In Step 3: Configuration Instance Details - Select **Enable** for **Auto-Assign Public IP** and also Select **Enable CloudWatch detailed Monitoring** from Monitoring. Leave rest of the settings as is and click on **Next: Add Storage**

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

**Step 3: Configure Instance Details**

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 [Launch into Auto Scaling Group](#)

Purchasing option: ☐ Request Spot instances

Network: vpc-0af4e04d044759966 (default) [Create new VPC](#)

Subnet: No preference (default subnet in any Availability Zone) [Create new subnet](#)

**Auto-assign Public IP: Enable**

Placement group: ☐ Add instance to placement group

Capacity Reservation: Open

Domain join directory: No directory [Create new directory](#)

IAM role: None [Create new IAM role](#)

Shutdown behavior: Stop

Stop - Hibernate behavior: ☐ Enable hibernation as an additional stop behavior

Enable termination protection: ☐ Protect against accidental termination

**Monitoring: ☒ Enable CloudWatch detailed monitoring**  
Additional charges apply

Tenancy: Shared - Run a shared hardware instance  
Additional charges will apply for dedicated tenancy.

Elastic Graphics: ☐ Add Graphics Acceleration  
Additional charges apply

Credit specification: ☐ Unlimited  
Additional charges may apply

Cancel Previous **Review and Launch** **Next: Add Storage**

## In Step 4: Add Storage - Leave the settings as is and volume type as “General Purpose SSD(gp2)” and click **Next: Add Tags**

aws Services Search for services, features, marketplace products, and docs [Alt+S] Corestack\_Rishi/ganesh.amekar\_microsoft @ 9526-3062-5896 N. Virginia Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more about storage options in Amazon EC2.](#)

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0821d7dcbd766278d	30	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more about free usage tier eligibility and usage restrictions.](#)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Tags](#)

## In Step 5: Add Tags – Add Owner, Department, App Team, App Team Owner and click **Next: Configure Security Group**

aws Services Search for services, features, marketplace products, and docs [Alt+S] Corestack\_Rishi/ganesh.amekar\_microsoft @ 9526-3062-5896 N. Virginia Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more about tagging your Amazon EC2 resources.](#)

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes	Network Interfaces
Name	FinanceApp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Owner	Ganesh	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Department	IT Support	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Application Owner	Hari	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

## In Step 6: Configure Security Group – Create a new security Group with naming convention and click **Review and Launch**

**Step 6: Configure Security Group**

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

**Assign a security group:** ☒ Create a new security group ☐ Select an existing security group

**Security group name:**

**Description:**

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	My IP 106.202.164.123/32	e.g. SSH for Admin Desktop

[Add Rule](#)


[Cancel](#) [Previous](#) [Review and Launch](#)

## In Step 7: Review Instance Launch – Review click **Launch**

**Step 7: Review Instance Launch**

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

▼ **AMI Details** [Edit AMI](#)

 **Microsoft Windows Server 20H2 Core Base - ami-0bf1d945d5b05bdcc**  
Free tier eligible Microsoft Windows Server 20H2 Semi-Annual Channel release [English]  
Root Device Type: ebs Virtualization type: hvm  
If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the [License Mobility Form](#). Don't show me this again

▼ **Instance Type** [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	-	1	1	EBS only	-	Low to Moderate

▼ **Security Groups** [Edit security groups](#)

**Security group name:** FinanceApp  
**Description:** FinanceApp-created 2021-05-31T15:12:30.999+05:30

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	106.202.164.123/32	

► **Instance Details** [Edit instance details](#)

► **Storage** [Edit storage](#)

► **Tags** [Edit tags](#)

[Cancel](#) [Previous](#) [Launch](#)

In Pop Up window – Create and new Key Pair and download it then click [Launch Instances](#)

Select an existing key pair or **create a new key pair**

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

**Key pair name**  
FinanceApp

Download Key Pair

You have to download the **private key file** (\*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel

Launch Instances

The screenshot shows a Windows File Explorer window titled "Downloads". The address bar shows the path "Downloads". The main area displays a single file named "FinanceApp.pem" with a document icon. Below the file name is a blue link that says "Open file". At the bottom of the window, there is a blue link that says "See more".

## EC2 Instance is being created and now click on view instances

**Launch Status**

Search for services, features, marketplace products, and docs [Alt+S]

Corestack\_Role/ganesh.ankar\_microsoft @ 9526-3062-5896 N. Virginia Support

Launch Status

✓ Your instances are now launching  
The following instance launches have been initiated: i-0f806078b542d4a29 View launch log

ⓘ Get notified of estimated charges  
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances. Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. Find out how to connect to your instances.

Here are some helpful resources to get you started

- How to connect to your Windows instance
- Learn about AWS Free Usage Tier
- Amazon EC2: User Guide
- Amazon EC2: Microsoft Windows Guide
- Amazon EC2: Discussion Forum

While your instances are launching you can also

- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes. (Additional charges may apply)
- Manage security groups

**View Instances**

## EC2 Instance is up and running.

Search for services, features, marketplace products, and docs [Alt+S]

Corestack\_Role/ganesh.ankar\_microsoft @ 9526-3062-5896 N. Virginia Support

**Instances (1)** Info

Filter instances

Connect Instance state Actions Launch Instances

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IF
FinanceApp	i-0f806078b542d4a29	Running	t2.micro	2/2 checks passed	No alarms	us-east-1e	ec2-100-26-142-144.co...	100.26.142.144	-	-

## PART 2: CloudWatch Monitoring and Alarm Setup

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

## Type in CloudWatch in the Search and Launch CloudWatch

Search for services, features, marketplace products, and docs [Alt+S]

Corestack\_Role/ganesh.ankar\_microsoft @ 9526-3062-5896 N. Virginia Support

Search results for 'cloudwa'

Services (2)

Features (8)

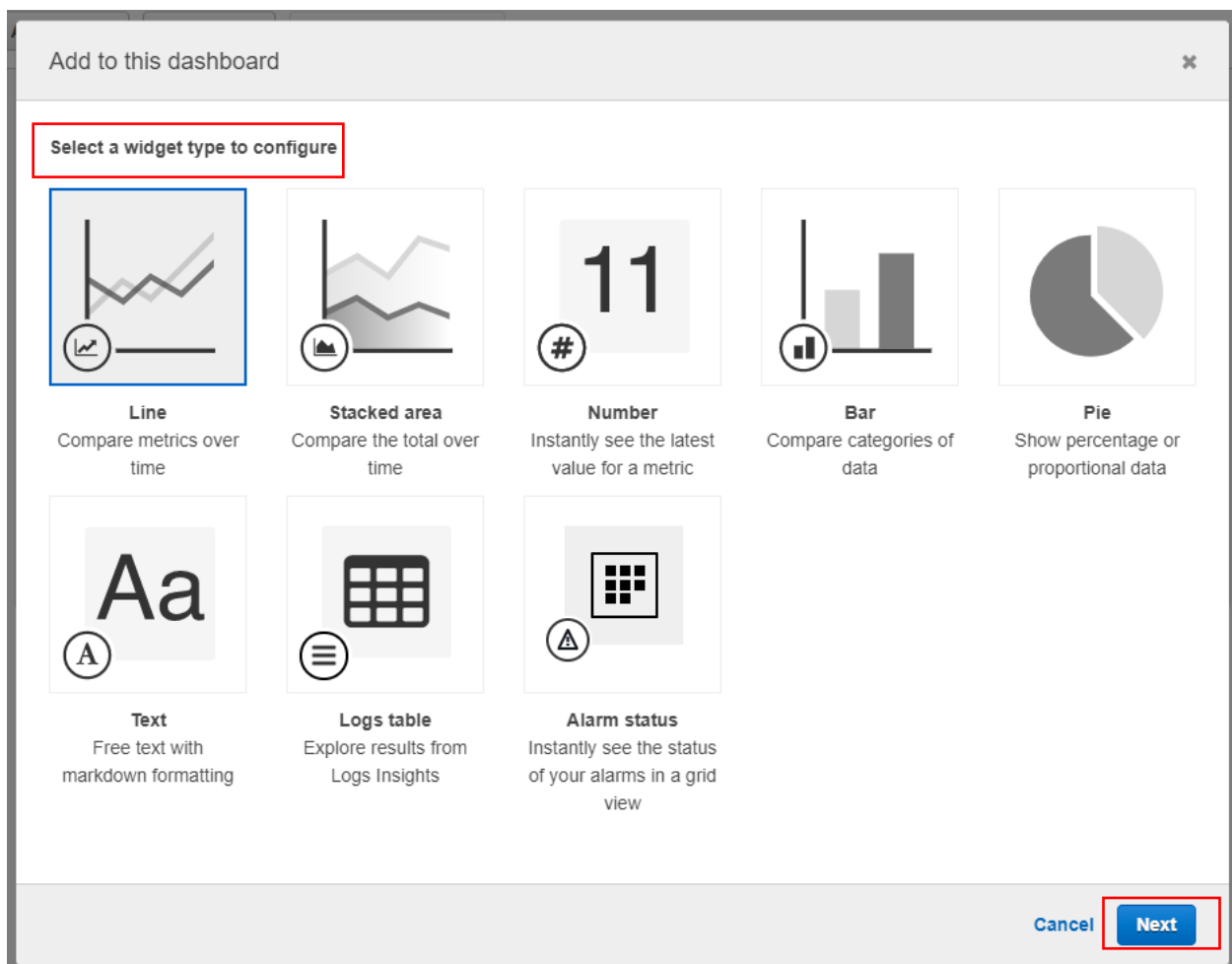
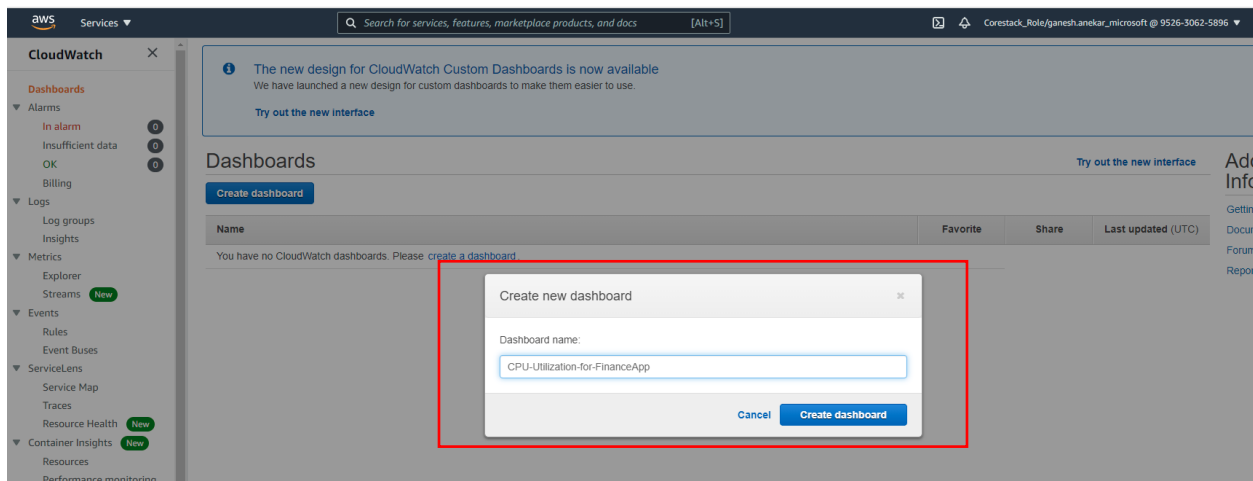
Documentation (5)

**Services**

CloudWatch  
Monitor Resources and Applications

Amazon EventBridge  
Serverless event bus that connects application data from your own apps, SaaS, and A...

## 1. Check and observe the CPU utilization graph for the EC2 instance





Add to this dashboard

From which data source would you like to create the widget?

☒

Metrics

Create widget based on Metrics and configure your widget on the next step.

☐

Logs

Create widget based on query results from CloudWatch Logs Insights.

Cancel

Configure

## Select EC2 – 38 Metrics

Add metric graph

Untitled graph

1h 3h 12h 1d 3d 1w custom Line

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

All metricsGraphed metricsGraph optionsSource

N. Virginia

Search for any metric, dimension or resource id

Graph search

66 Metrics

CloudFront

6 Metrics

EBS

9 Metrics

EC2

38 Metrics

Firehose

2 Metrics

SWF

4 Metrics

Usage

7 Metrics

## Per Instance Metrics

All metricsGraphed metricsGraph optionsSource

N. Virginia

All > EC2

Search for any metric, dimension or resource id

Graph search

38 Metrics

By Image (AMI) Id

7 Metrics

Per-Instance Metrics

17 Metrics

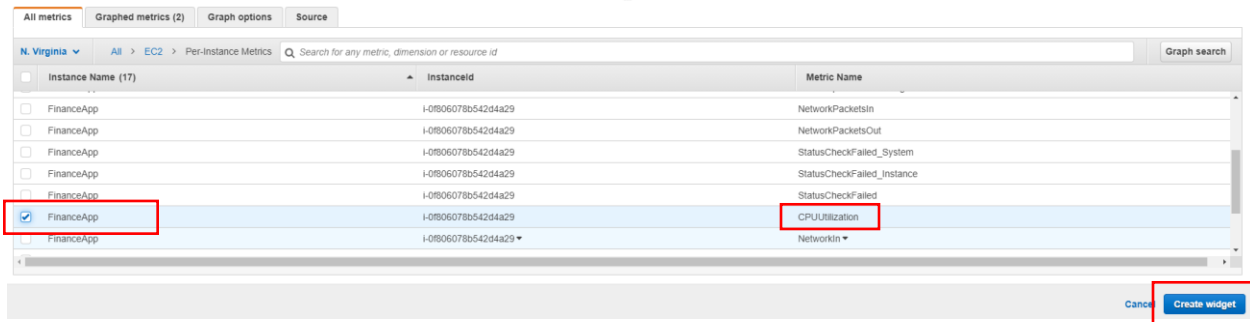
Aggregated by Instance Type

7 Metrics

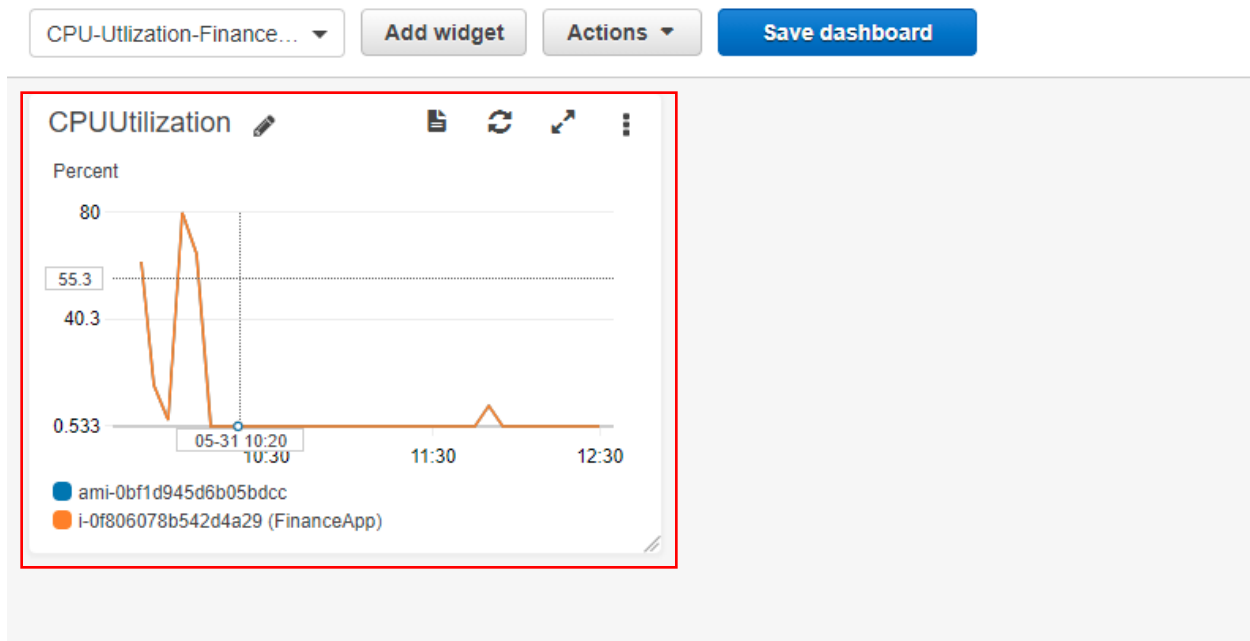
Across All Instances

7 Metrics

Select Instance Name as **FinanceApp** and Metric Name as **CPUUtilization** and Click **Create Widget**

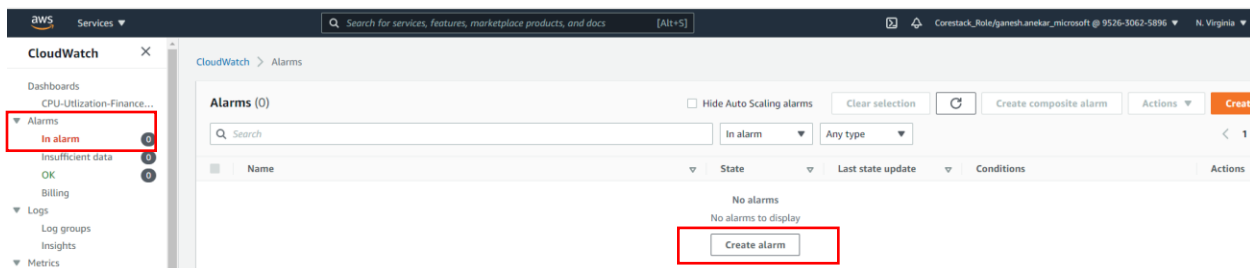


The dashboard will now have CPU Utilization as monitoring.



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

Click on **Alarms** and then **In Alarm** and then click **Create alarm**



Click on **Select metric**

CloudWatch > Alarms > Create alarm

Step 1  
**Specify metric and conditions**

Step 2  
Configure actions

Step 3  
Add name and description

Step 4  
Preview and create

## Specify metric and conditions

**Metric**

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

Select metric

Cancel Next

Select metric will show up like this, then click on EC2

Select metric

Untitled graph

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

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

Metrics (66) Info

Graph search Graphed metrics

Search for any metric, dimension or resource id

CloudFront 6	EBS 9	<b>EC2 38</b>	Firehose 2
SWF 4	Usage 7		

Cancel Select a single metric to continue

In EC2, Select **Per-Instance Metrics**

Metrics (38) Info

Graph search Graphed metrics

All > EC2 Search for any metric, dimension or resource id

By Image (AMI) Id 7	<b>Per-Instance Metrics 17</b>	Aggregated by Instance Type 7	Across All Instances 7
---------------------	--------------------------------	-------------------------------	------------------------

Cancel Select a single metric to continue

In Per-Instance Metrics, Select **FinanceApp** and **CPUUtilization** and then click “Select metric”

Metrics (17) Info Graph search Graphed metrics (1)

All > EC2 > Per-Instance Metrics

<input type="checkbox"/>	Instance Name (17)	Instance Id	Metric Name
<input checked="" type="checkbox"/>	FinanceApp	i-0f806078b542d4a29 ▼	CPUUtilization ▼
<input type="checkbox"/>	FinanceApp	i-0f806078b542d4a29 ▼	NetworkIn ▼
<input type="checkbox"/>	FinanceApp	i-0f806078b542d4a29 ▼	NetworkOut ▼
<input type="checkbox"/>	FinanceApp	i-0f806078b542d4a29 ▼	DiskReadBytes ▼

Cancel Select metric

In the metric window, select **Statics**: Minimum, **Period**: 5 Minutes, **Threshold Type**: Static, In Alarm Condition: Select **Lower** than define threshold **Value**: 3 then select **3 instances** as datapoint click **Next**

Metric Edit

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

Percent

■ CPUUtilization

Namespace  
AWS/EC2

Metric name  
CPUUtilization

Instance Id  
i-0f806078b542d4a29

Instance name  
FinanceApp

Statistic

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.  
  
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.  
 out of

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

Cancel Next

In Configure Actions, select **Alarm state trigger** then **create new topic, email** and then click on **Create Topic**

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

## 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.

[Remove](#)

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

☐ Select an existing SNS topic

☒ Create new topic

☐ Use topic ARN

Create a new topic...  
The topic name must be unique.

Default\_CloudWatch\_Alarms\_FinanceApp\_LowCPU

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](#)

### Auto Scaling action

[Add Auto Scaling action](#)

### EC2 action

[Add EC2 action](#)

### Systems Manager action [Info](#)

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

[Add Systems Manager action](#)

[Cancel](#) [Previous](#) [Next](#)

Once SNS topic is created, it will show like below, now will click **Next**

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.

Remove

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

☒ Select an existing SNS topic

☐ Create new topic

☐ Use topic ARN

Send a notification to...

X

Only email lists for this account are available.

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

Add notification

### Auto Scaling action

Add Auto Scaling action

### EC2 action

Add EC2 action

### Systems Manager action

 Info  

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

Add Systems Manager action

Cancel

Previous

Next

Add name and description for the Alarm and click **Next**

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

## Add name and description

**Name and description**

Alarm name

Alarm description - *optional*

Up to 1024 characters (22/1024)

Cancel Previous **Next**

## Preview and Create Alarm

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


### Preview and create

Step 1: Specify metric and conditions

Graph

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

Percent



Namespace

AWS/EC2

Metric name

CPUUtilization

InstanceId

i-0f806078b542d4a29

Instance name

FinanceApp

Statistic

Minimum

Period

5 minutes

Conditions

Threshold type

Static

Whenever **CPUUtilization** is

Lower (<)

than...

3

▼ Additional configuration

Datapoints to alarm

3 out of 3

Missing data treatment

Treat missing data as missing

Step 2: Configure actions

Actions

Notification

When in alarm, send a notification to "Default\_CloudWatch\_Alarms\_FinanceApp\_LowCPU"

Step 3: Add name and description

Name and description

Name

FinanceApp\_LowCPU\_Util

Description

FinanceApp\_LowCPU\_Util

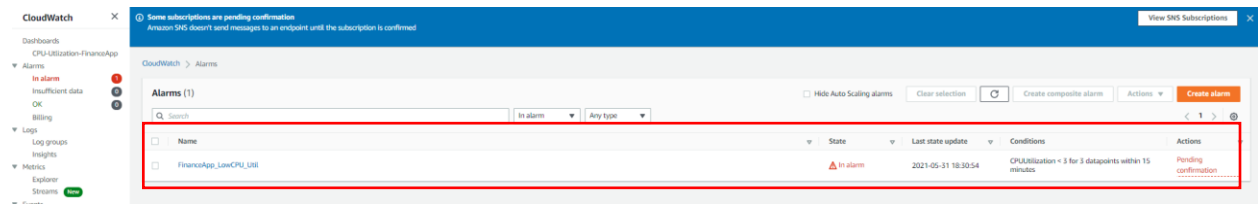
Cancel

Previous

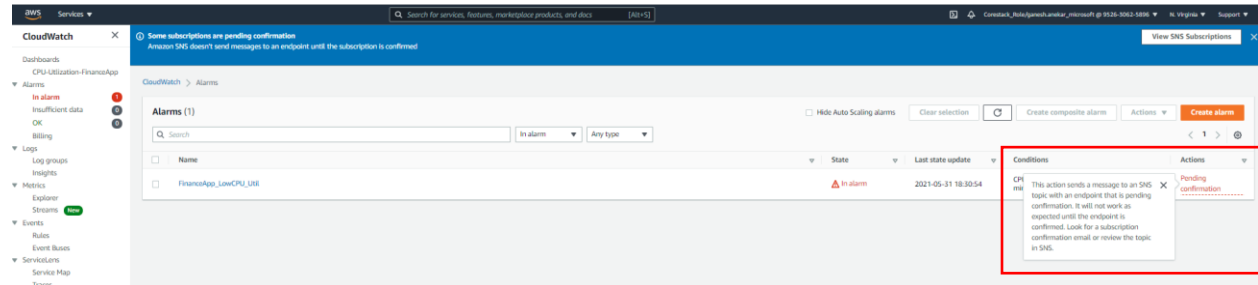
Create alarm



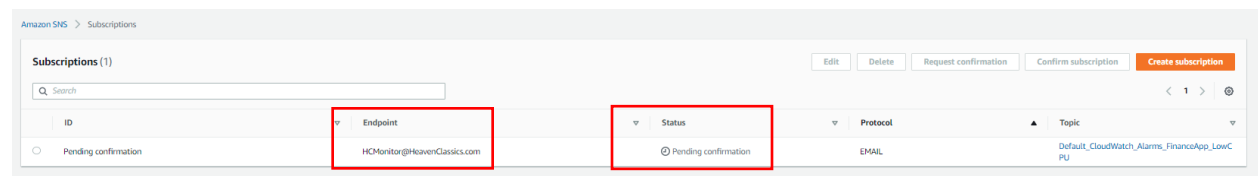
In Alarm dashboard, we can now see the Alarm is created by name **FinanceApp\_LowCPU\_Util**



The Alarm shows pending confirmation for the Alarm as the **Email Endpoint needs to be confirmed**.



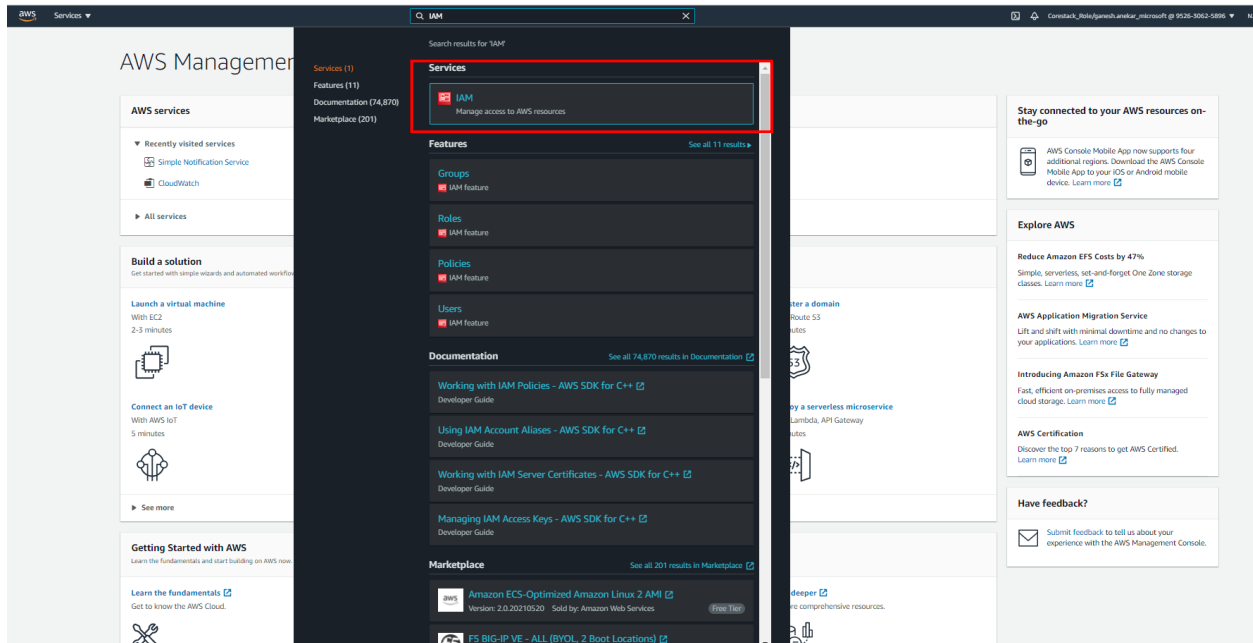
In SNS subscription view, it shows below as Endpoint as pending confirmation.



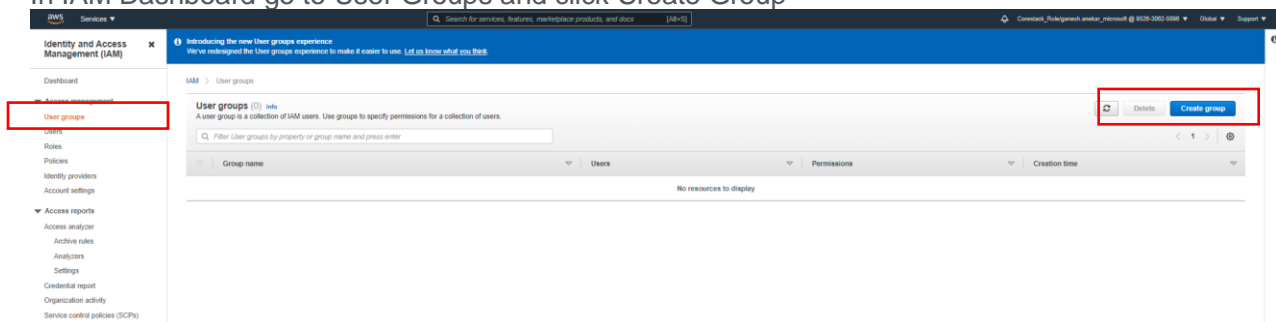
## PART 3: Create IAM Group

1. Create an IAM group named Administrator Group and attach the full administrator access policy to the group

In AWS Management console, search **IAM** and select **IAM**



In IAM Dashboard go to User Groups and click Create Group



Created group called **Administrators1** – With **AdministratorAccess** Policy

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

IAM > User groups > Create user group

Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

Administrators1

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

Add users to the group - [object Object] (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. A user can belong to up to 10 groups.

Search

< 1 > ⚙

☐

User name ↗

Groups

Last activity

Creation time

☐

corestack-73142

0

1 year ago

1 year ago

Attach permissions policies - [object Object] (Selected 1/669) 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.

Filter policies by property or policy name and press enter

4 matches

< 1 > ⚙

AdministratorAccess X Clear filters

☒

AdministratorAccess

AWS managed - job function

0

☐ AdministratorAccess-Amplify

☐ AdministratorAccess-AWSElasticBeanstalk

☐ AWSAuditManagerAdministratorAccess

AWS managed

AWS managed

AWS managed

0

0

0

Cancel

Create group

2. 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

Go to Users and click on Add User

The screenshot displays the AWS Identity and Access Management (IAM) console. The top navigation bar includes the AWS logo, a 'Services' dropdown, and a search bar. The left-hand navigation pane is titled 'Identity and Access Management (IAM)' and contains a sidebar menu. In this menu, 'Users' is highlighted with a red box. The main content area features a header with 'Add user' (highlighted with a red box) and 'Delete user' buttons. Below this is a search bar labeled 'Find users by username or access key'. A table lists users, with one entry 'corestack-73142' visible. The bottom of the console shows the 'AWS account ID: 952630625896'.

aws Services ▾ Search for services, features, marketplace

Identity and Access Management (IAM)

Dashboard

▼ Access management

User groups

**Users**

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Q Search IAM

AWS account ID:  
952630625896

Add user Delete user

Q Find users by username or access key

☐ User name ▾

☐ corestack-73142

Created Employee User – Prasad with following information and clicked **Next: Permissions**

## Add user



### Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name\* Prasad

[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

- Require password reset ☒ User must create a new password at next sign-in  
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

\* Required

[Cancel](#)


[Next: Permissions](#)


Added Prasad User into Administrators1 Group who has full Admin Permissions and clicked **Next:Tags**


Add user

12345

▼ Set permissions

 Add user to group

 Copy permissions from existing user

 Attach existing policies directly

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

Create groupRefresh

Q Search

Showing 2 results

Group ▼	Attached policies
<input type="checkbox"/> Administrators	AWSFMAdminFullAccess
<input checked="" type="checkbox"/> Administrators1	AdministratorAccess

► Set permissions boundary

CancelPreviousNext: Tags

Added Tags and clicked **Next: 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
<input type="text" value="Name"/>	<input type="text" value="AdminAccessGrop"/>	✕
<input type="text" value="User"/>	<input type="text" value="Prasad"/>	✕
<input type="text" value="Add new key"/>	<input type="text"/>	

You can add 48 more tags.

[Cancel](#)

[Previous](#)

[Next: Review](#)

## Add user **Review Screen** and **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	Prasad
AWS access type	AWS Management Console access - with a password
Console password type	Autogenerated
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

#### Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	<a href="#">Administrators1</a>
Managed policy	<a href="#">IAMUserChangePassword</a>

#### Tags

The new user will receive the following tags

Key	Value
Name	AdminAccessGrop
User	Prasad

[Cancel](#)[Previous](#)[Create user](#)



User **Prasad** is created and part of **Administrators group**.

## Add user

1 2 3 4 5



### 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://952630625896.signin.aws.amazon.com/console>

Download .csv

	User	Password	Email login instructions
▶	✓ Prasad	***** <a href="#">Show</a>	<a href="#">Send email</a>