AWS Technical Essentials Project – Server Monitoring

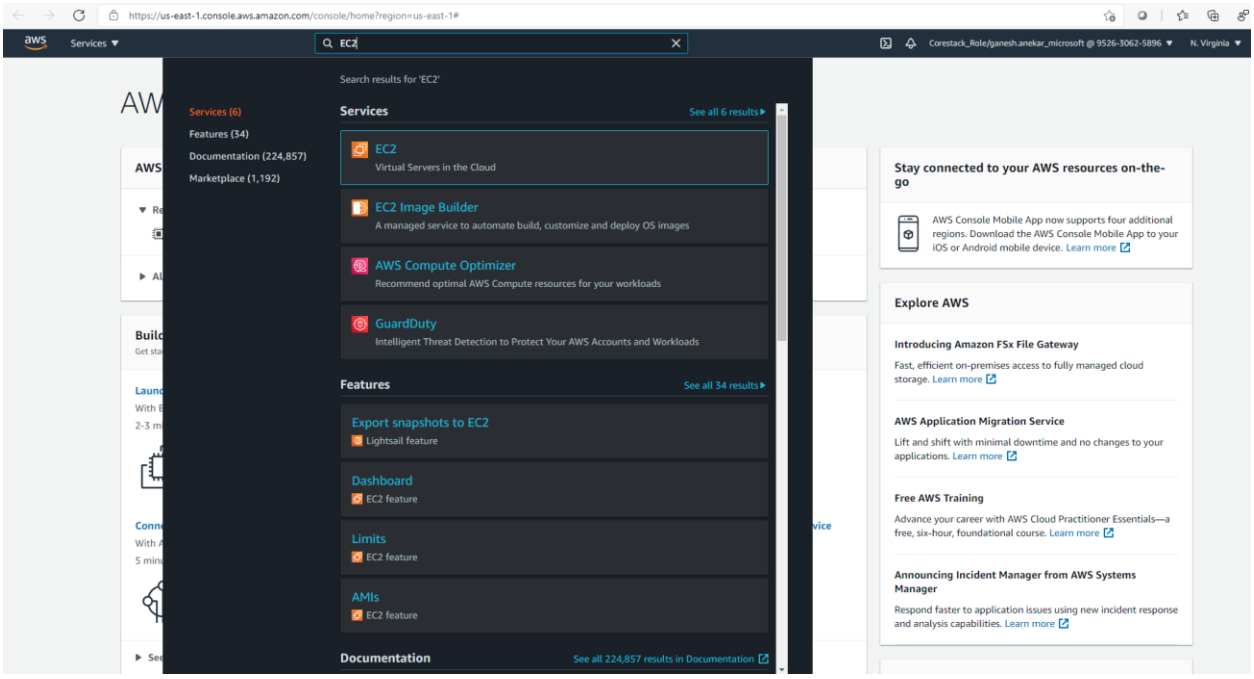
DESCRIPTION

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:

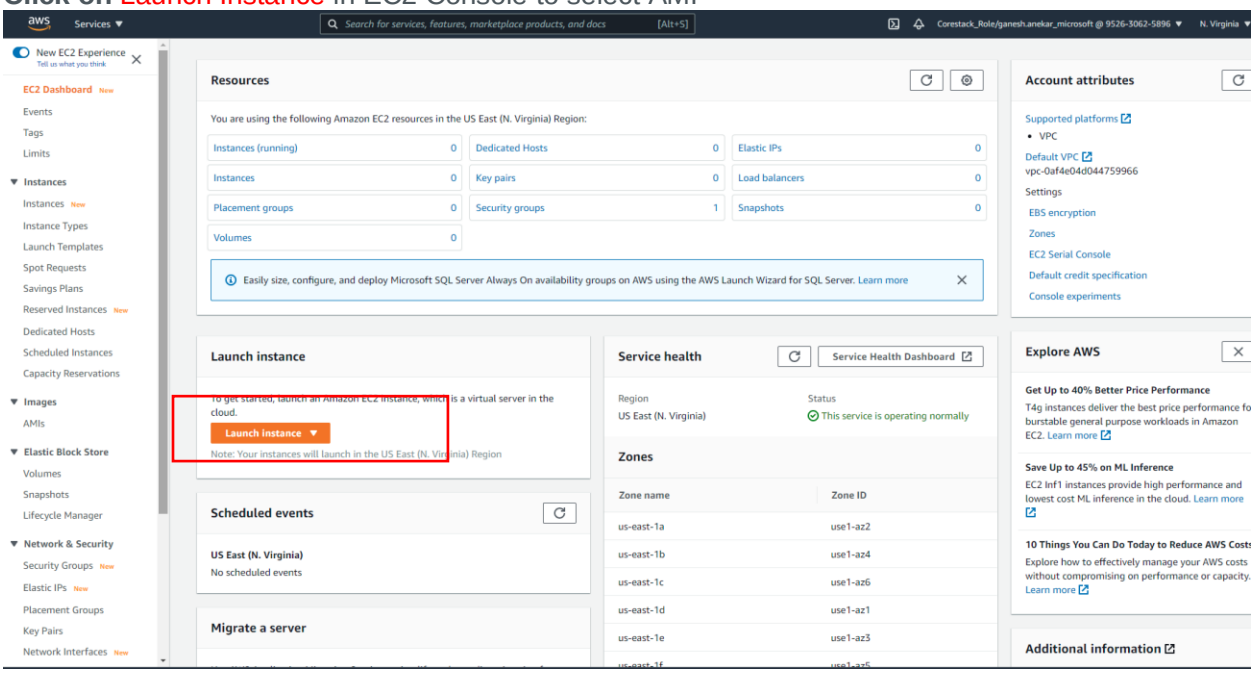
1. Check and observe the CPU utilization graph for the EC2 instance
2. Create and configure a CloudWatch alarm that sends an email notification to HCMonitor@HeavenClassics.com if the CPU utilization goes below the threshold of 3%, consecutively three times for five minutes
3. Create an IAM group named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

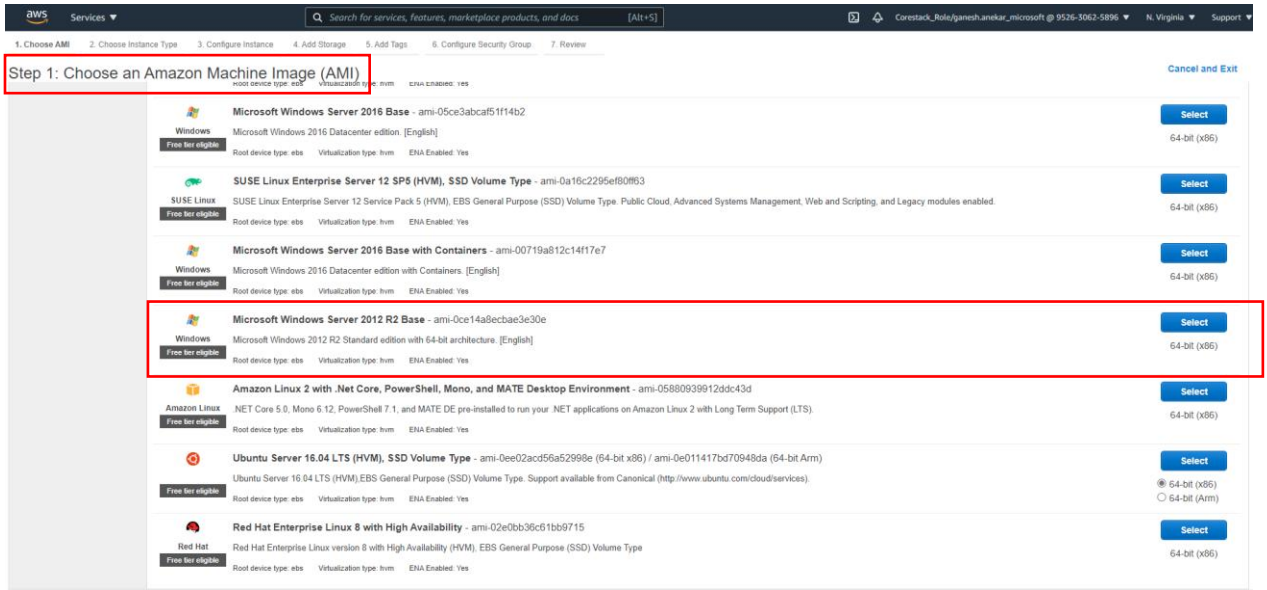
Search EC2 in AWS Console and Click on EC2 to go to EC2



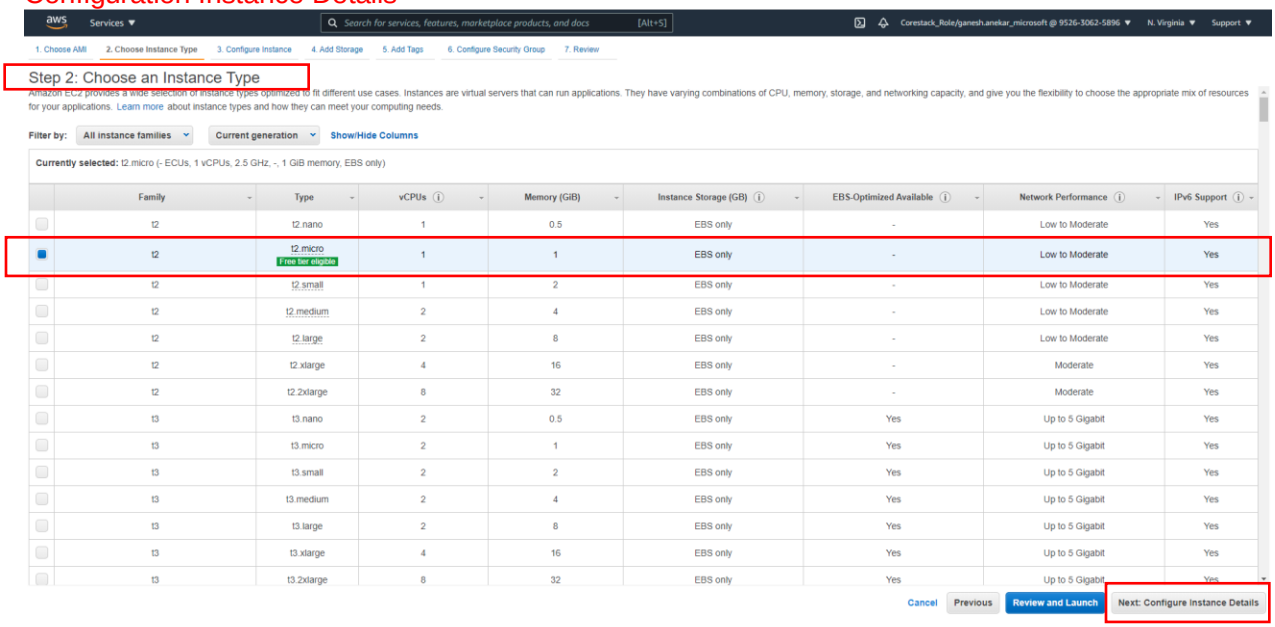
Click on Launch Instance in EC2 Console to select AMI



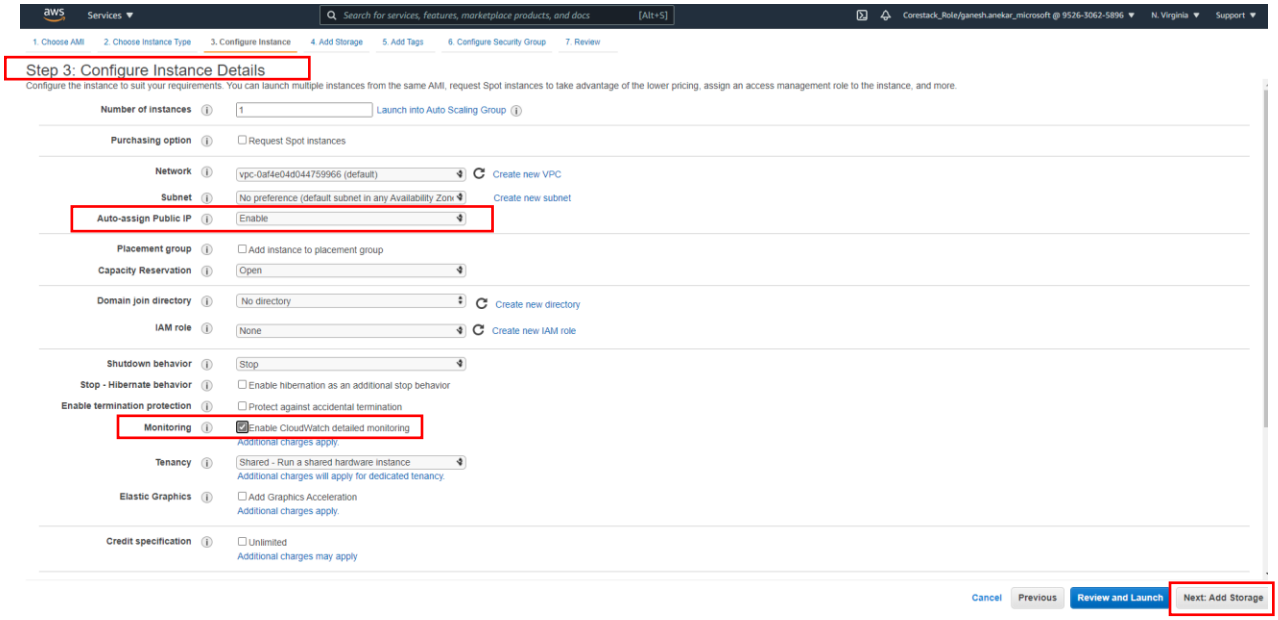
Select Microsoft Windows Server 2021 R2 Base from AMI List



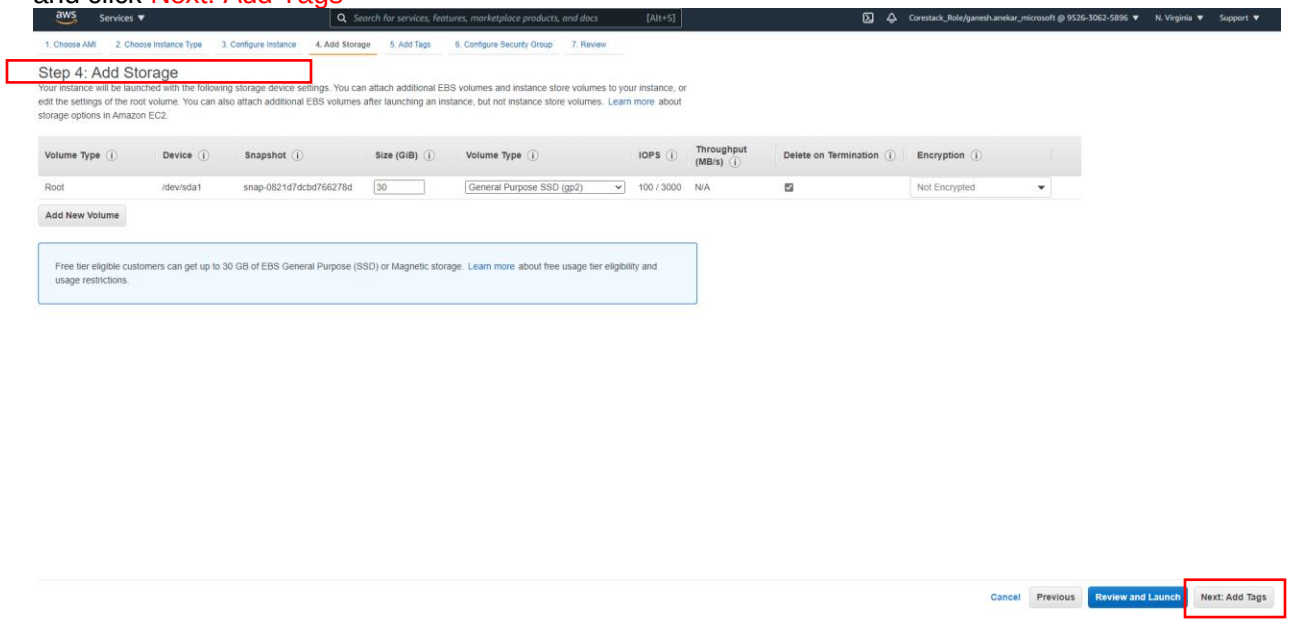
Step 2: Choose an Instance Type - Select t2.micro with 1 vCPU and 1GB Memory and Click Next Configuration Instance Details



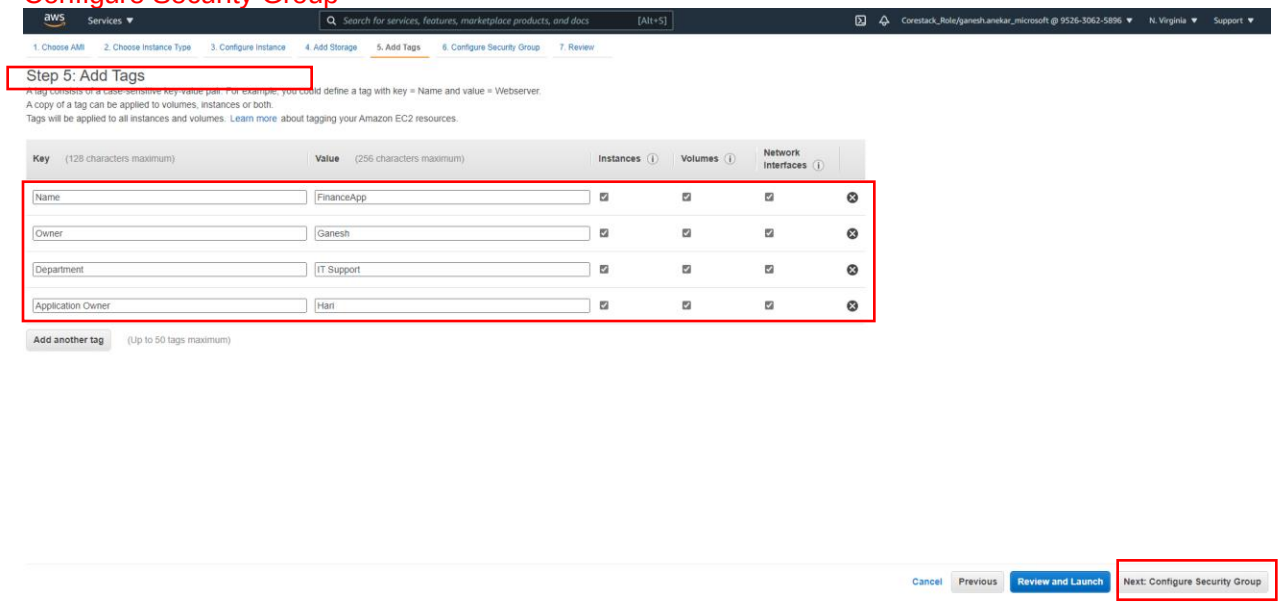
In Step 3: Configuration Instance Details - Select Enable for Auto-Assign Public IP **and also** Select Enable CloudWatch detailed Monitoring from Monitoring. Leave rest of the settings as is and **click** on Next: Add Storage



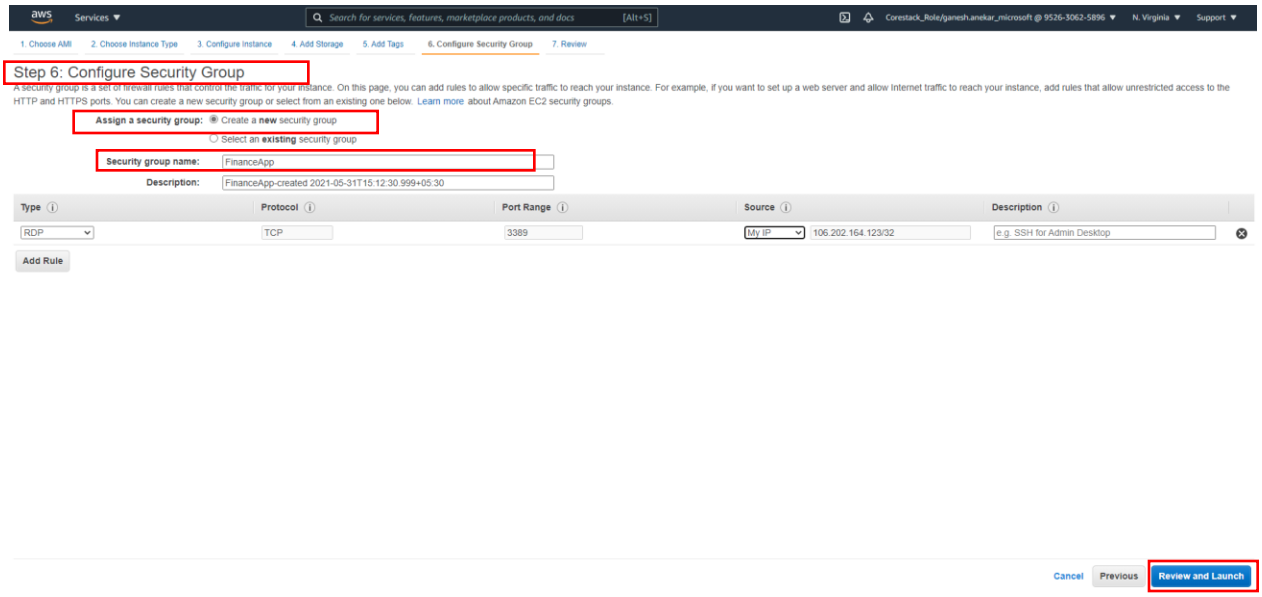
In Step 4: Add Storage - Leave the settings as is and volume type as “General Purpose SSD(gp2) and click Next: Add Tags



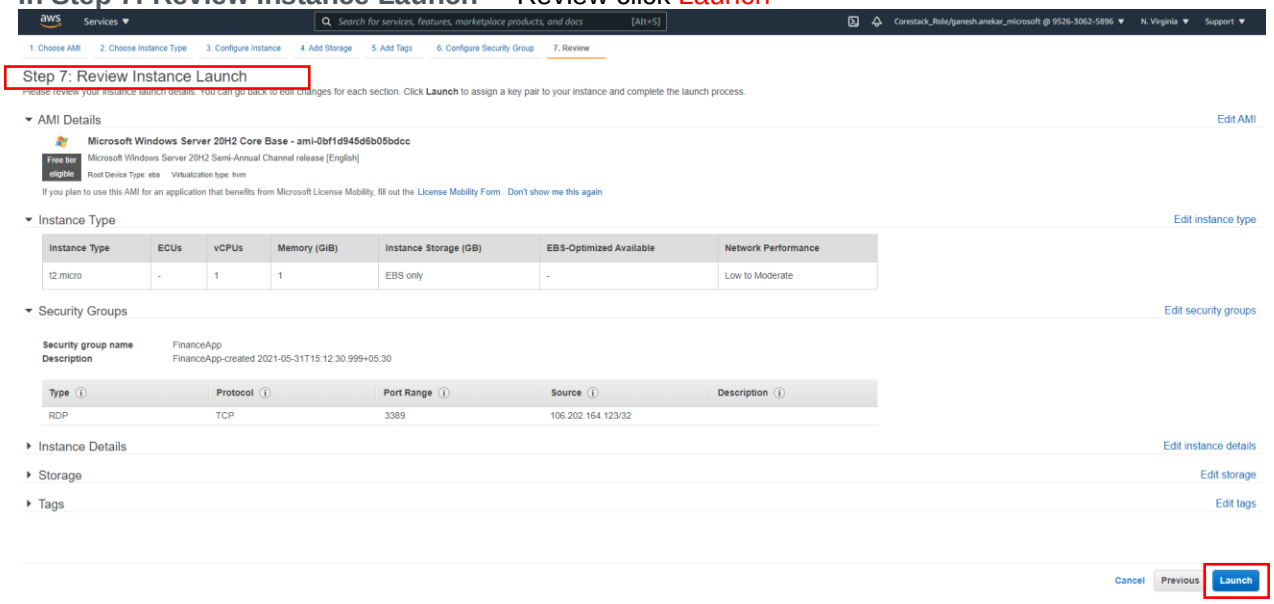
In Step 5: Add Tags – Add Owner, Department, App Team, App Team Owner and click Next: Configure Security Group



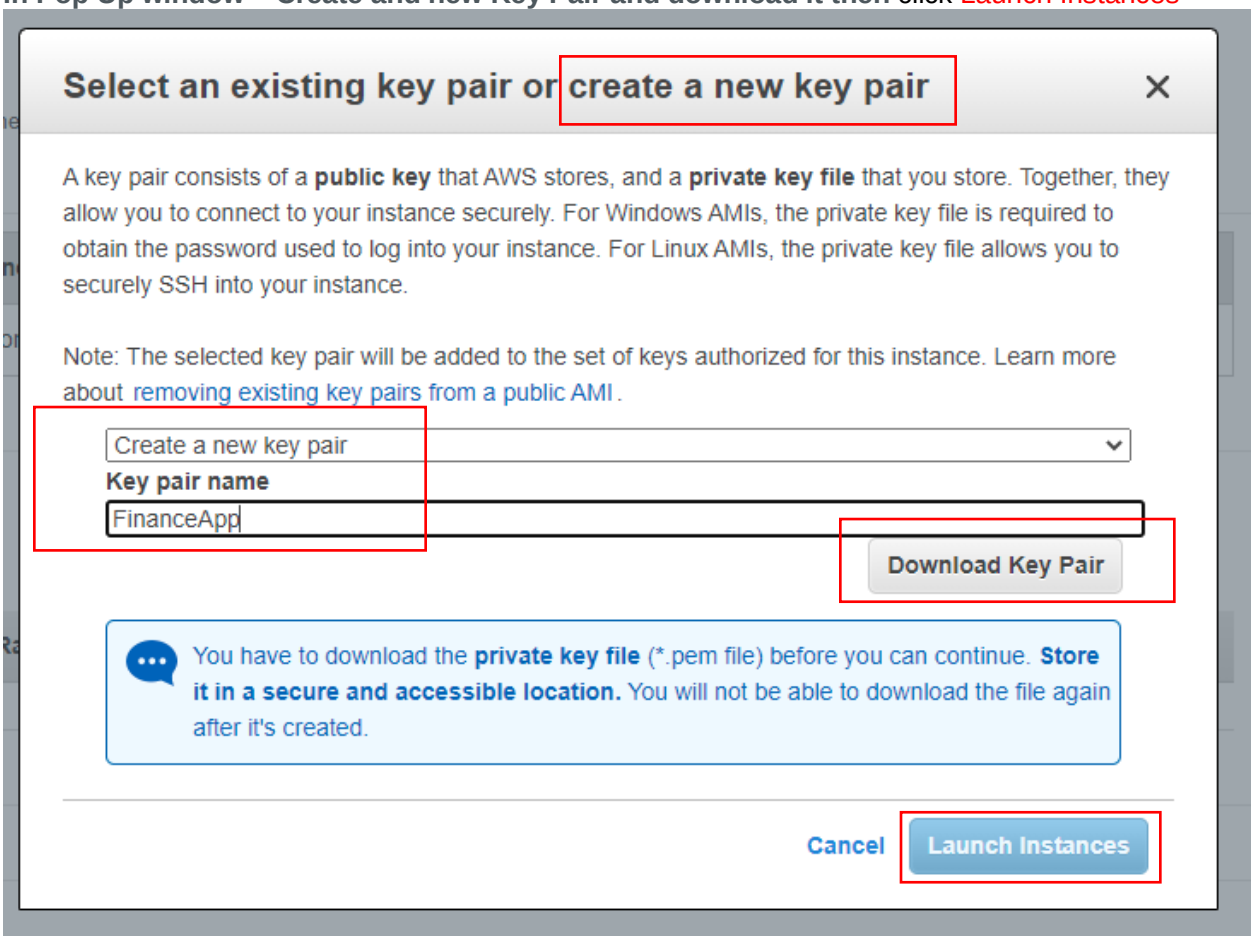
In Step 6: Configure Security Group – Create a new security Group with naming convention and click Review and Launch

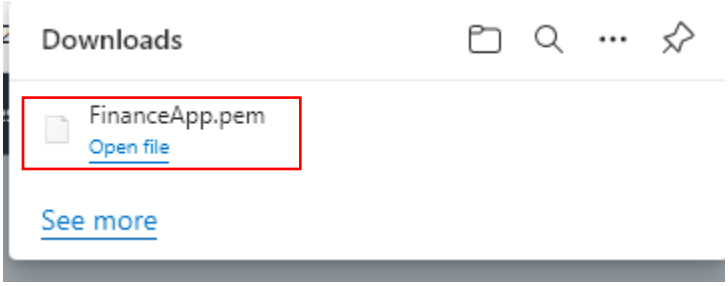


In Step 7: Review Instance Launch – Review click Launch

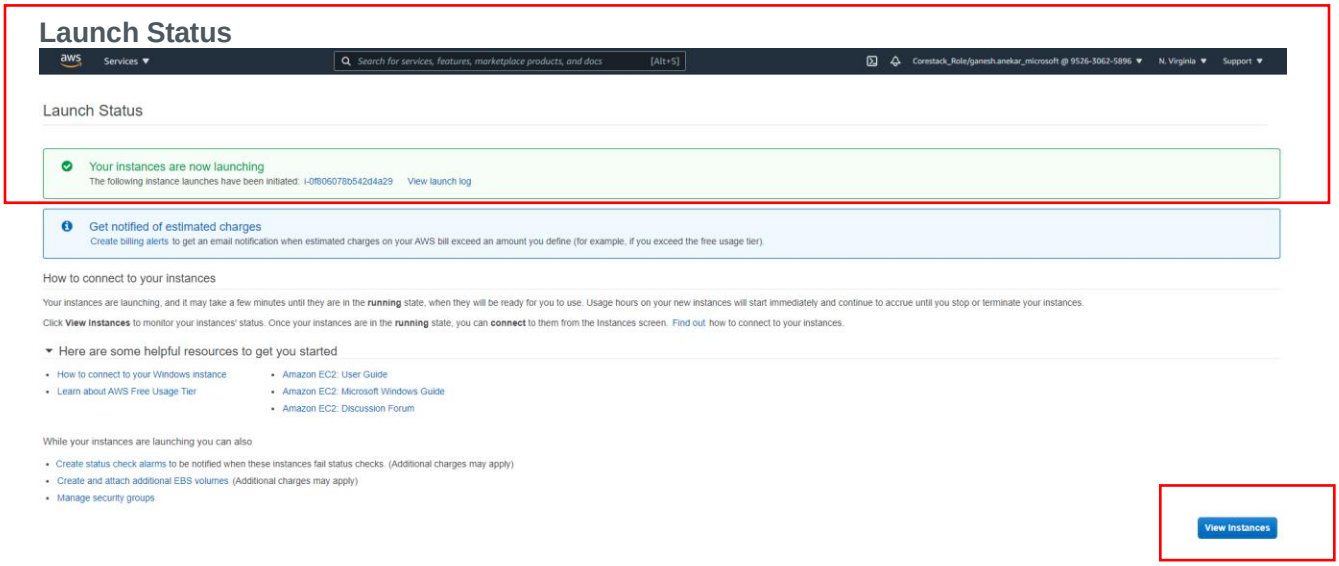


In Pop Up window – Create and new Key Pair and download it then click Launch Instances

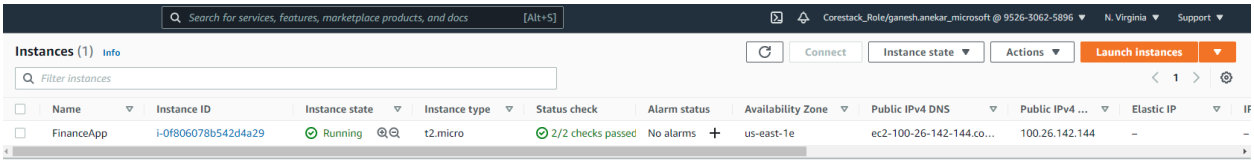




EC2 Instance is being created and now click on view instances



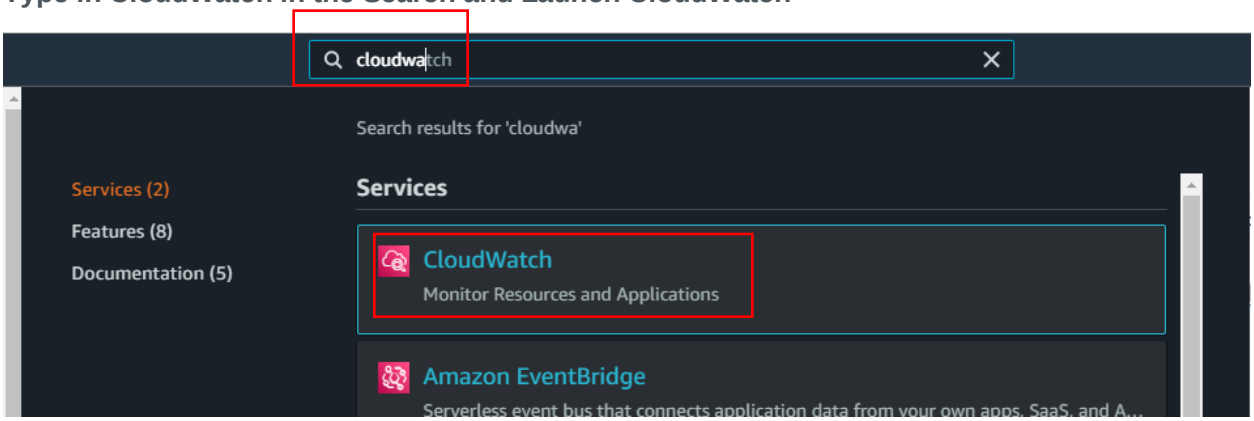
EC2 Instance is up and running.



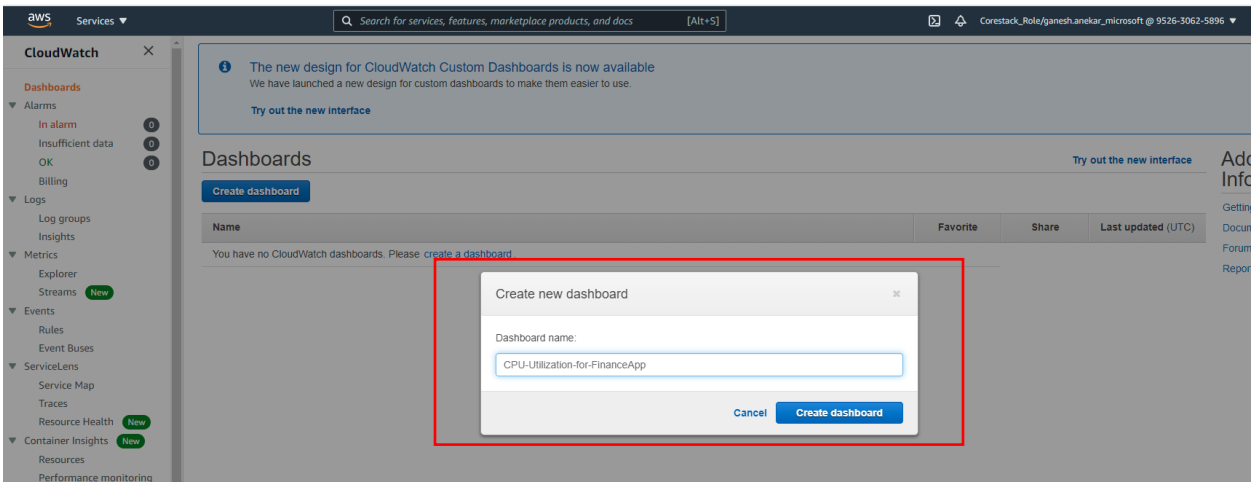
PART 2: CloudWatch Monitoring and Alarm Setup

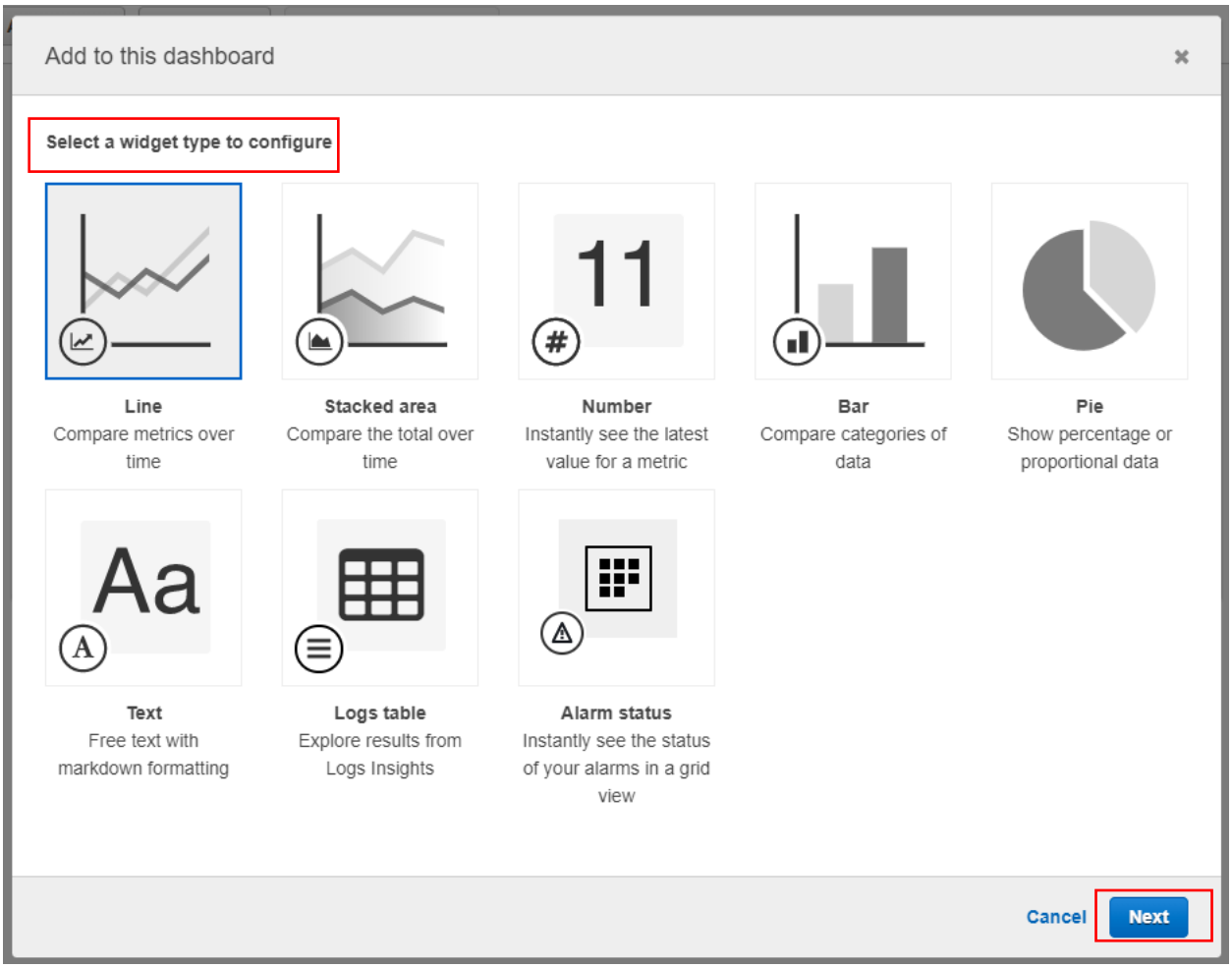
1. Check and observe the CPU utilization graph for the EC2 instance
2. Create and configure a CloudWatch alarm that sends an email notification to HCMonitor@HeavenClassics.com if the CPU utilization goes below the threshold of 3%, consecutively three times for five minutes

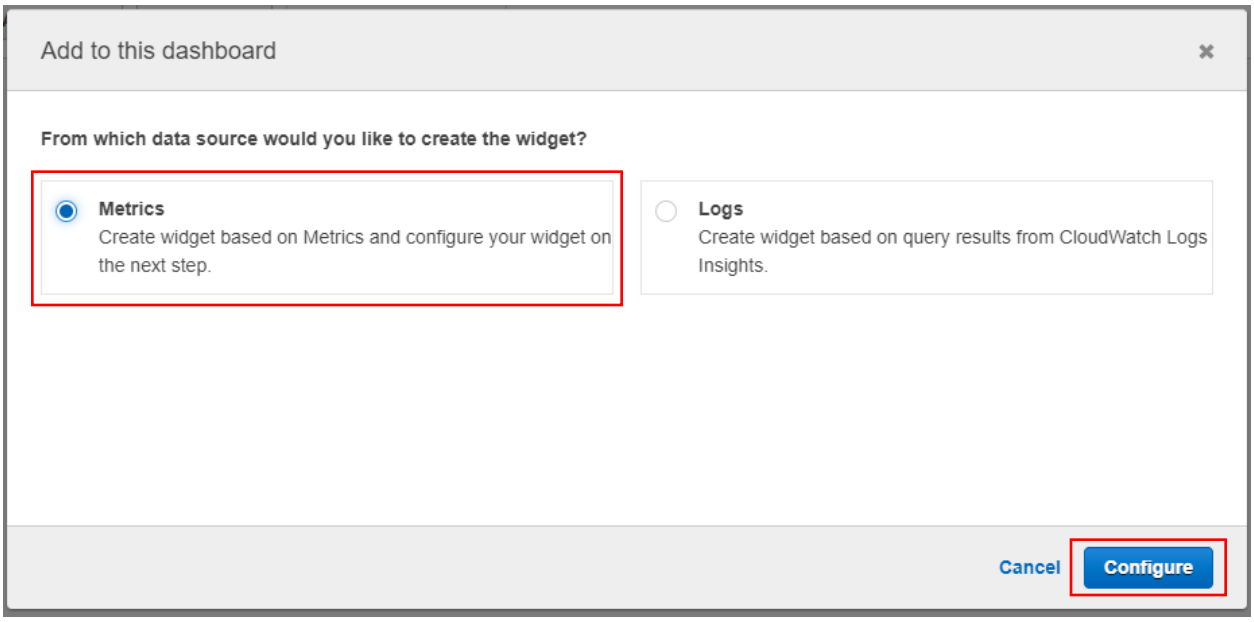
Type in CloudWatch in the Search and Launch CloudWatch



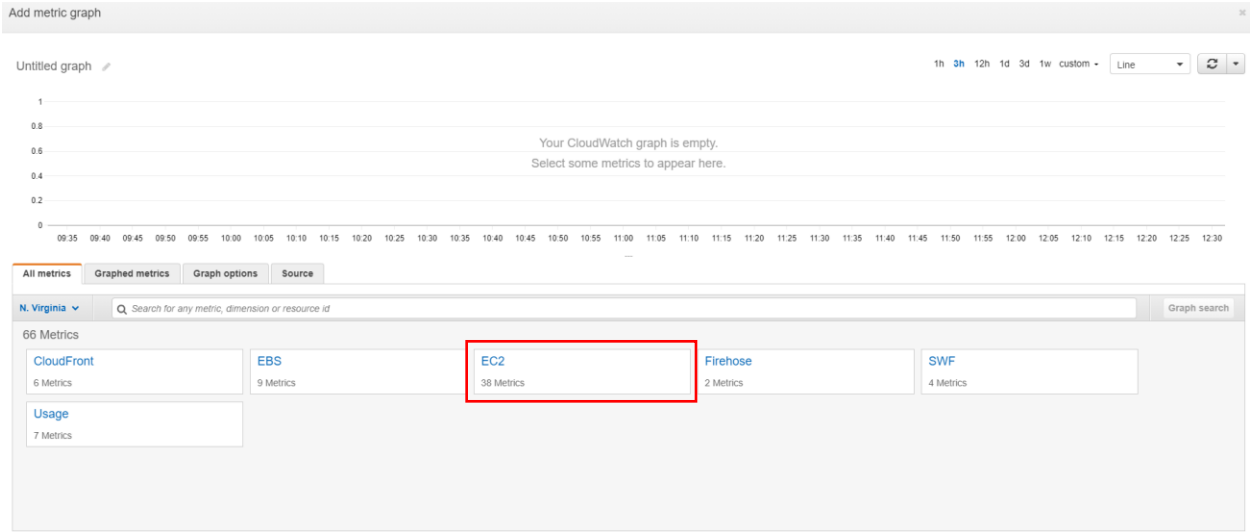
1. **Check and observe the CPU utilization graph for the EC2 instance**



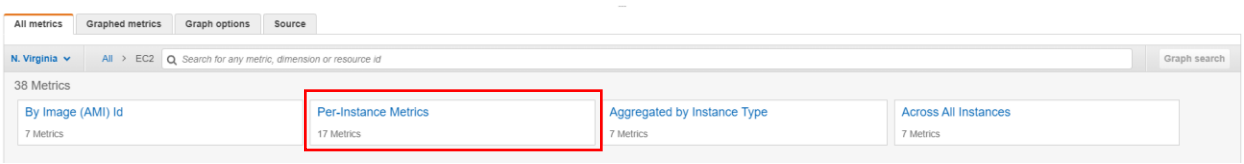




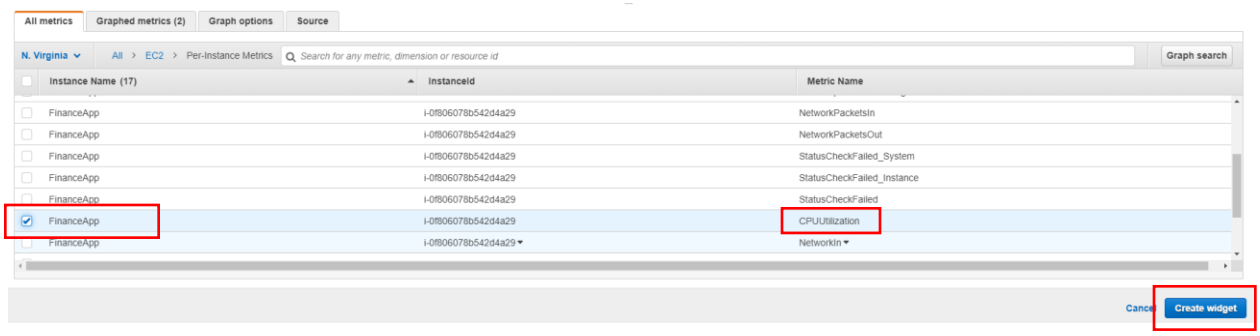
Select EC2 – 38 Metrics



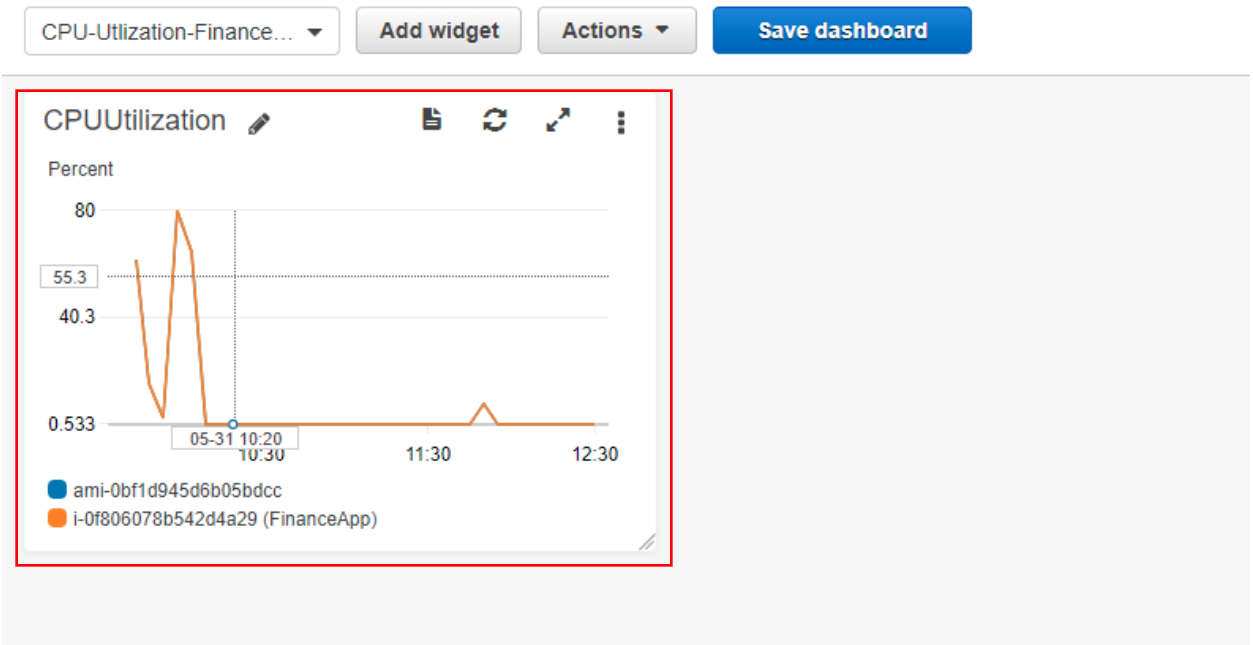
Per Instance Metrics



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

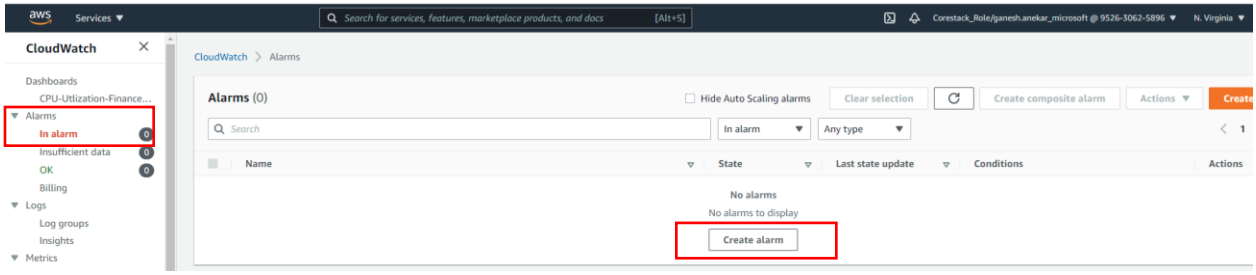


The dashboard will now have CPU Utilization as monitoring.

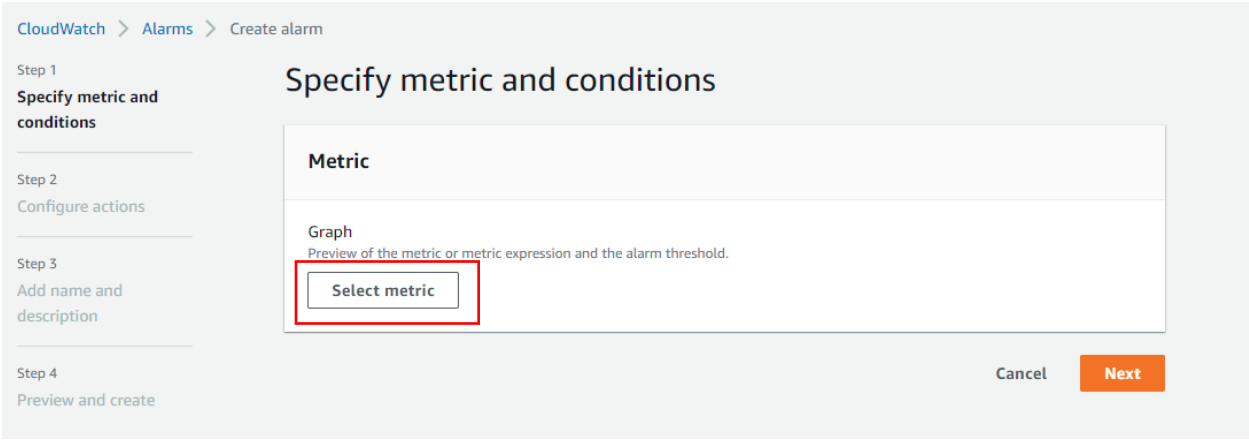


2. **Create and configure a CloudWatch alarm that sends an email notification to HCMonitor@HeavenClassics.com if the CPU utilization goes below the threshold of 3%, consecutively three times for five minutes**

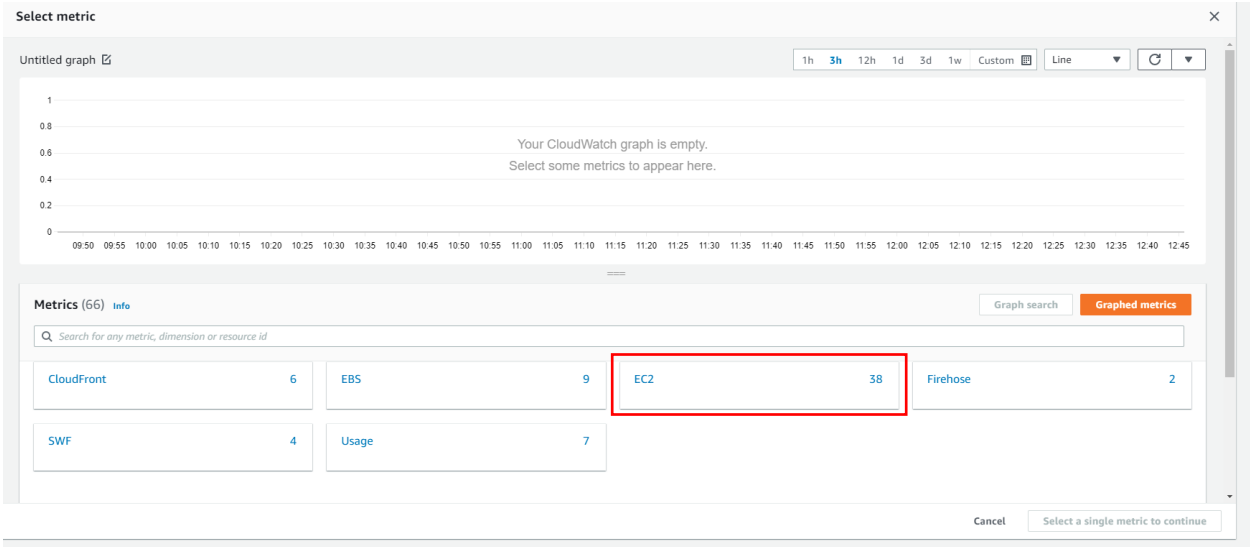
Click on **Alarms** and then **In Alarm** and then **click Create alarm**



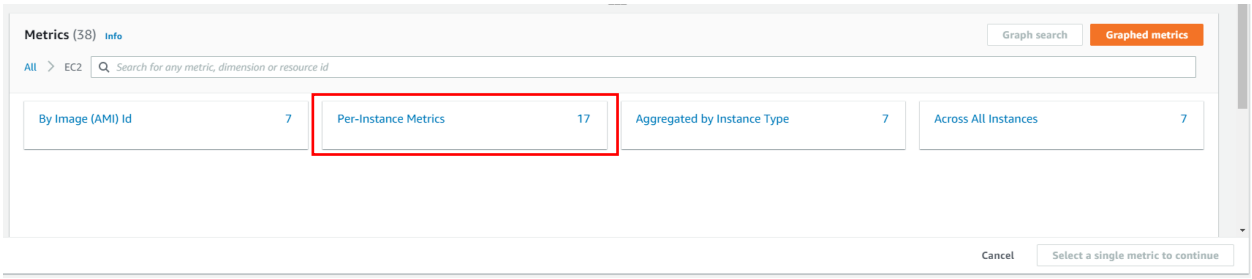
Click on **Select metric**



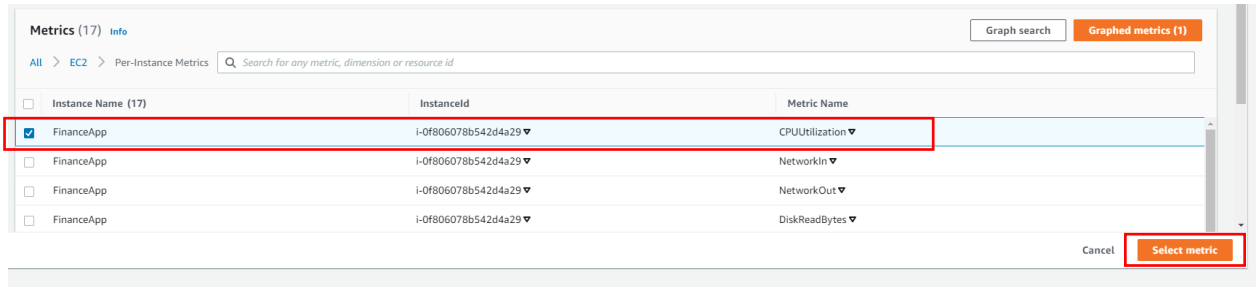
Select metric will show up like this, then click on EC2



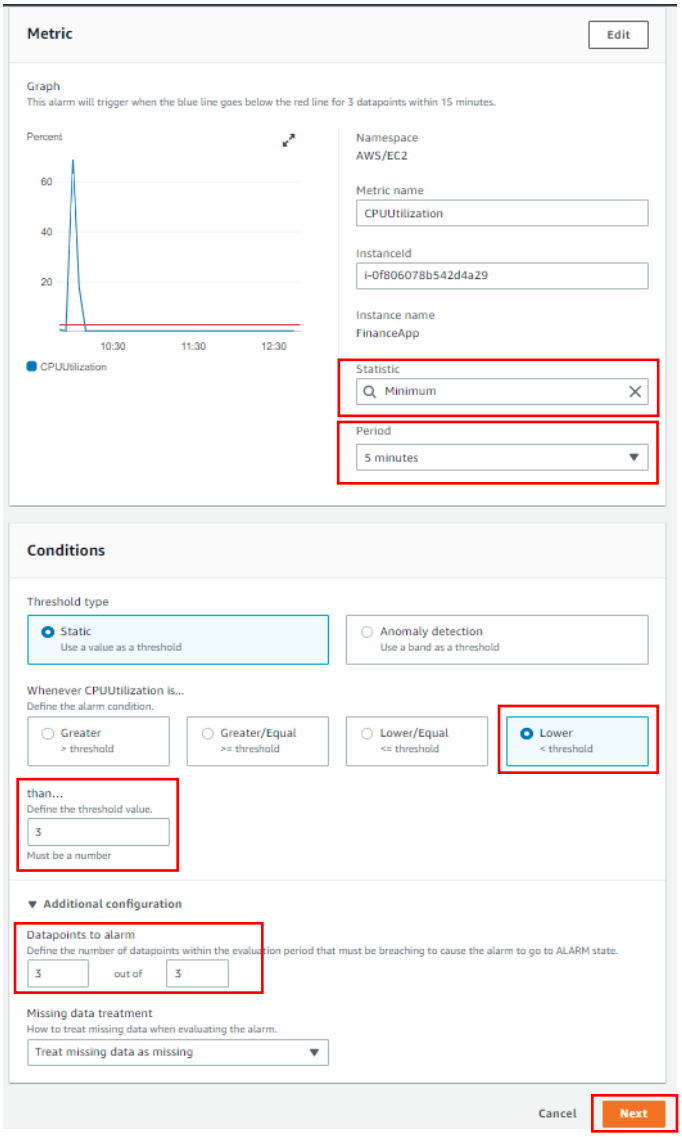
In EC2, Select **Per-Instance Metrics**



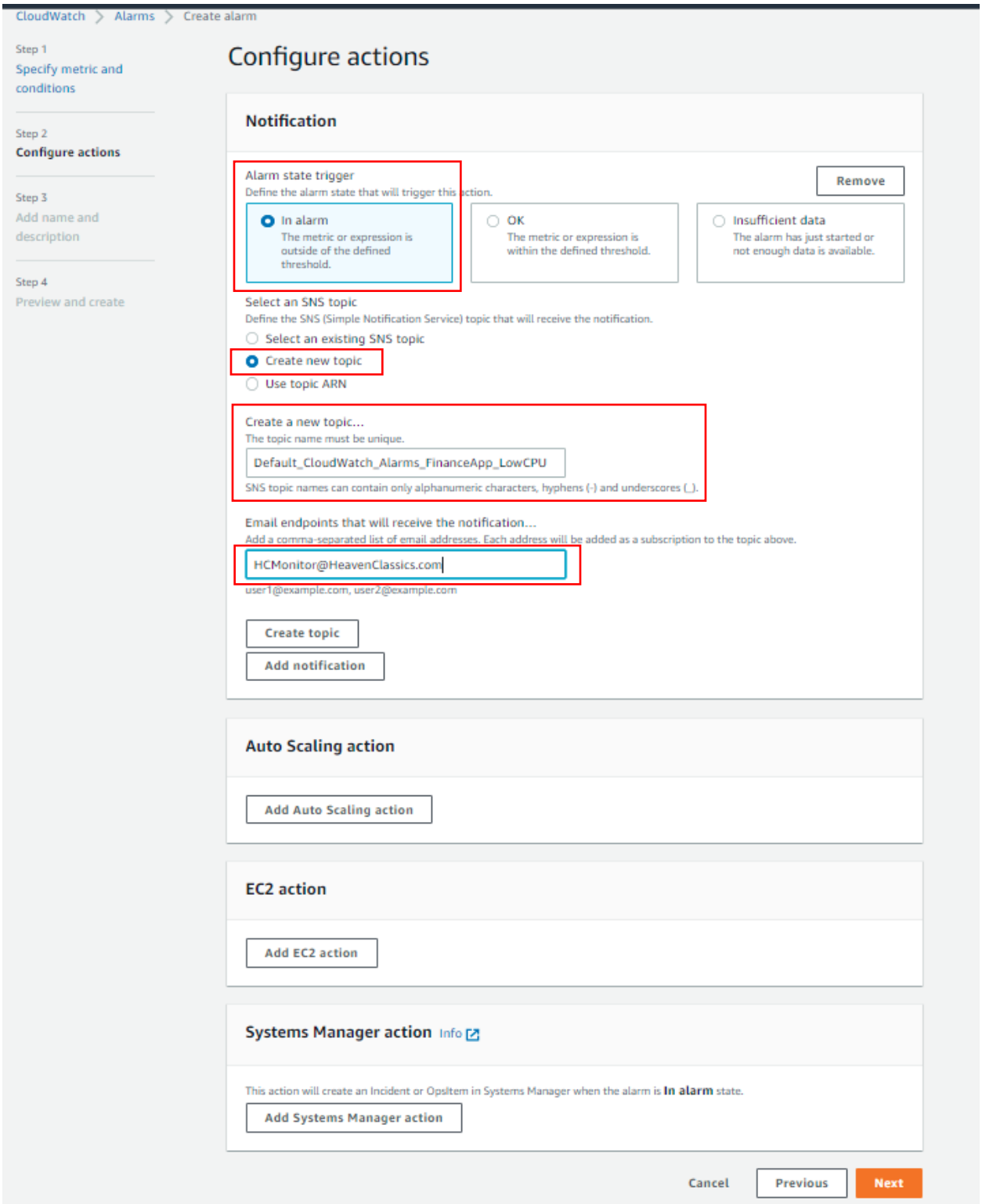
In Per-Instance Metrics, Select **FinanceApp** and **CPUUtilization** and then click "**Select metric**"



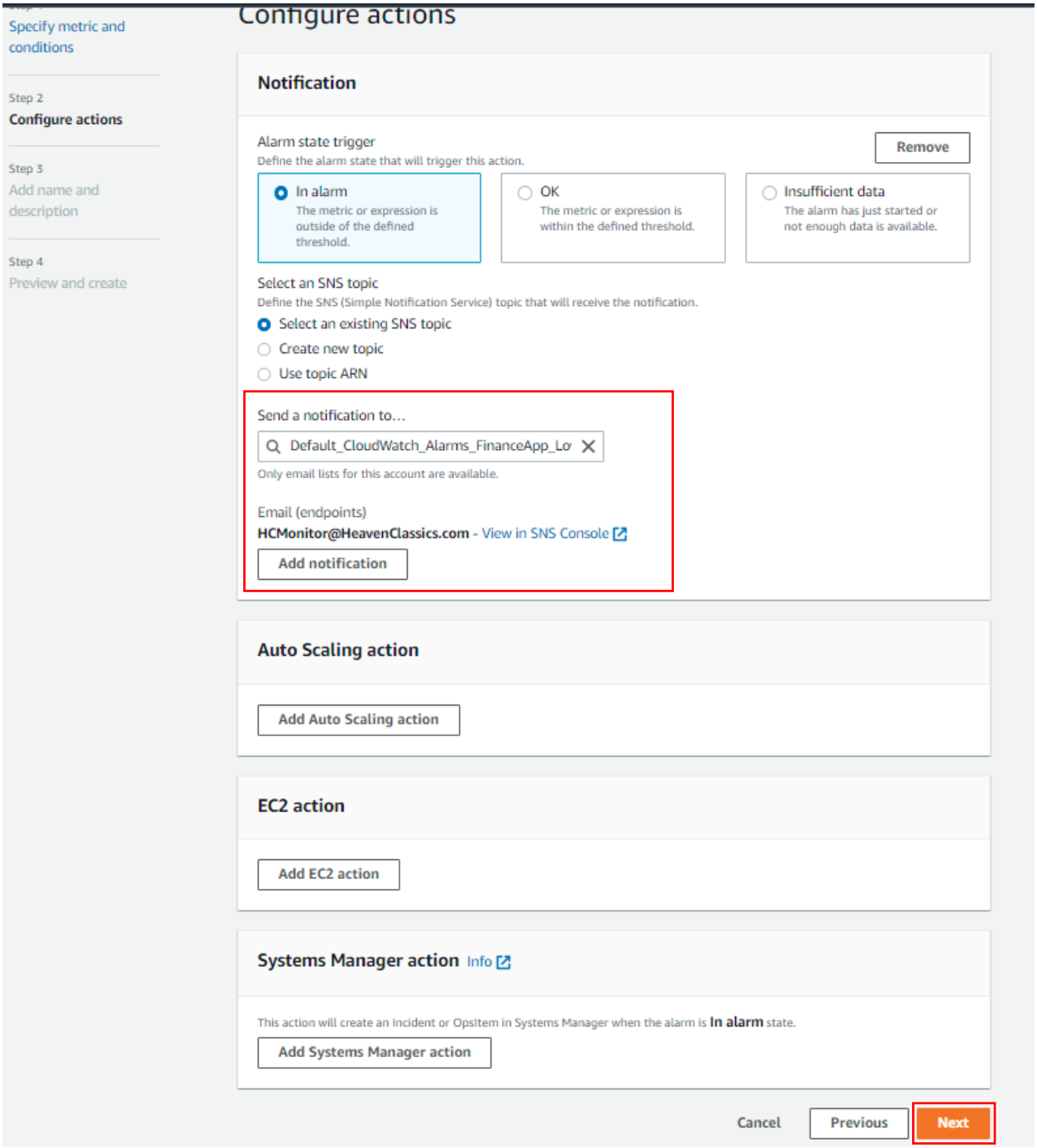
In the metric window, select **Statics**: **Minimum**, **Period**: **5 Minutes, Threshold Type**: **Static,** In Alarm Condition: Select **Lower** than define threshold **Value: 3** then select **3 instances** as datapoint click **Next**



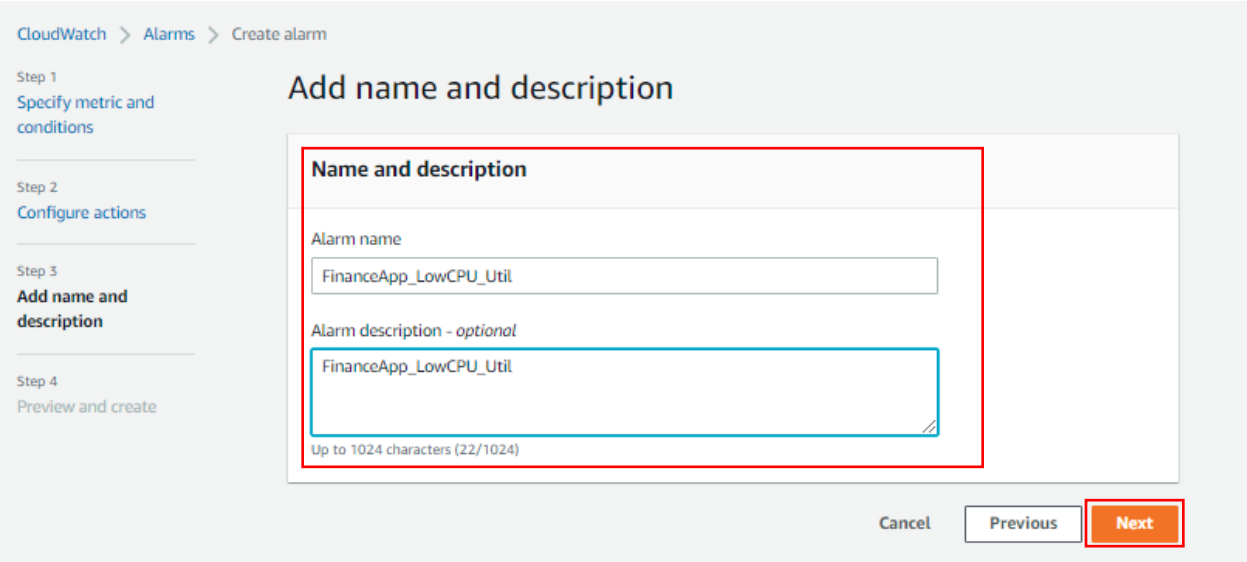
In Configure Actions, select **Alarm state trigger** then **create new topic**, **email** and then click on **Create Topic**



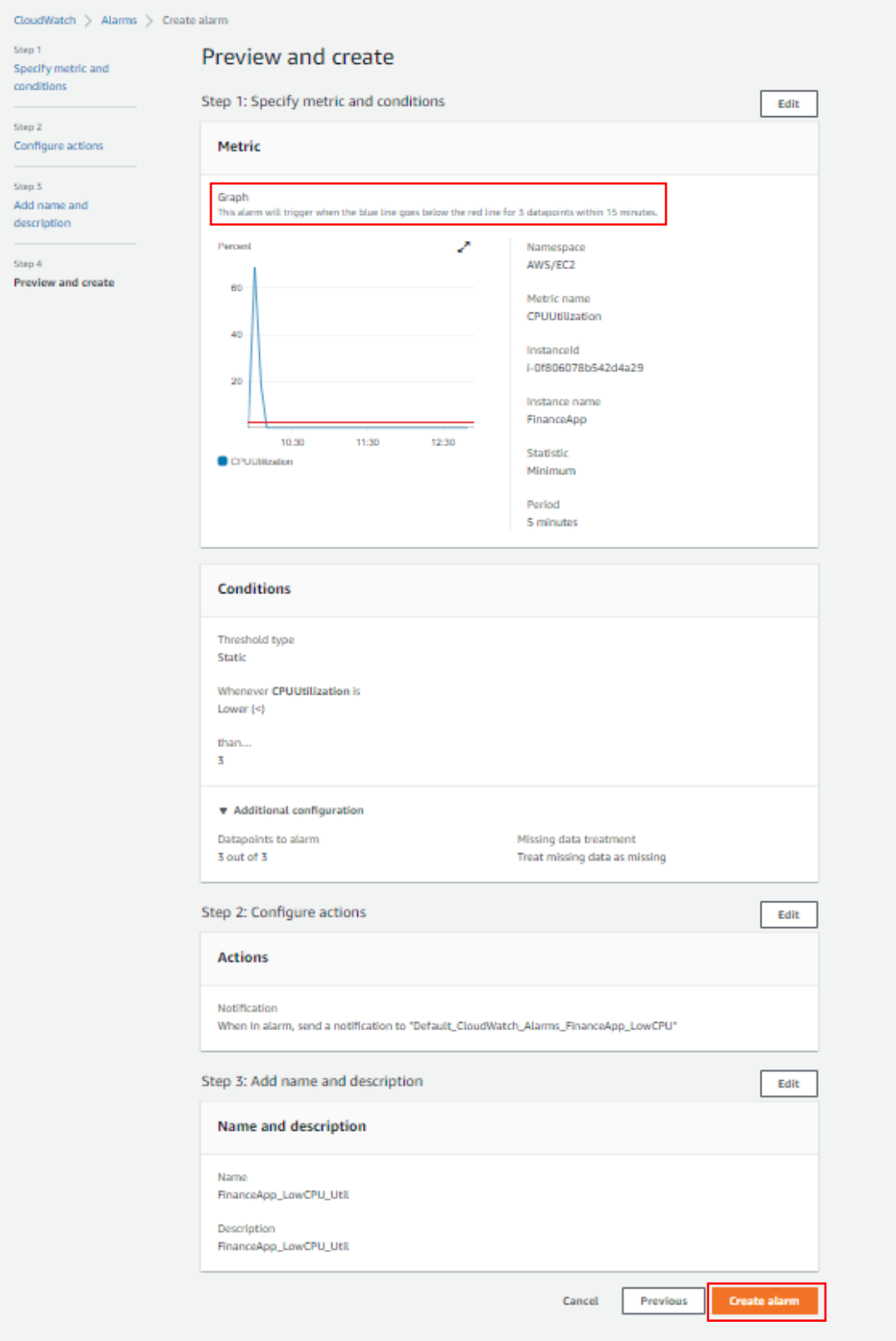
Once SNS topic is created, it will show like below, now will click **Next**



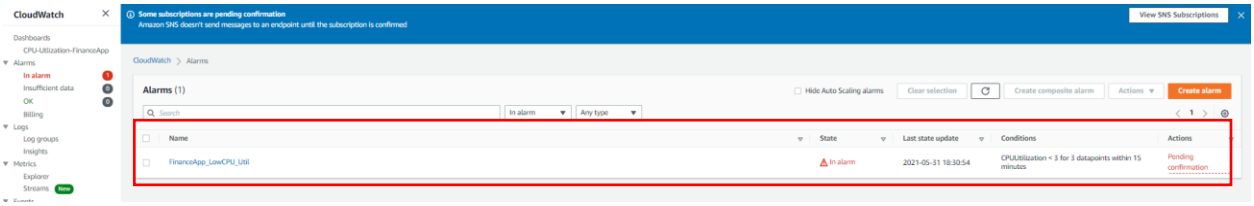
Add name and description for the Alarm and click **Next**



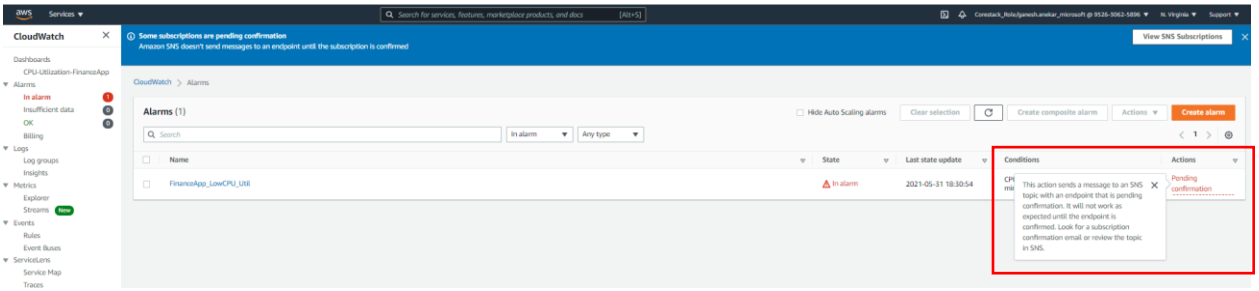
Preview and Create Alarm



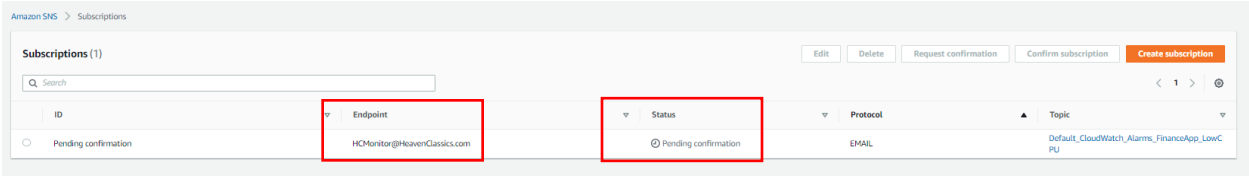
In Alarm dashboard, we can now see the Alarm is created by name **FinanceApp_LowCPU_Util**



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



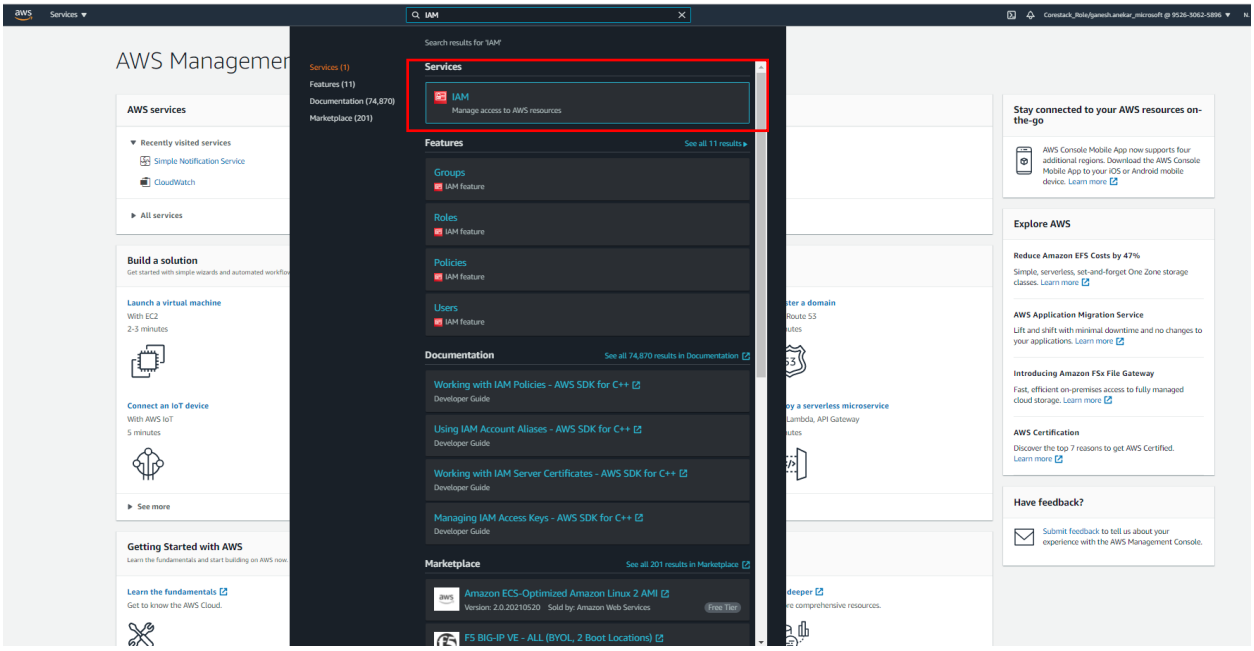
In SNS subscription view, it shows below as Endpoint as pending confirmation.



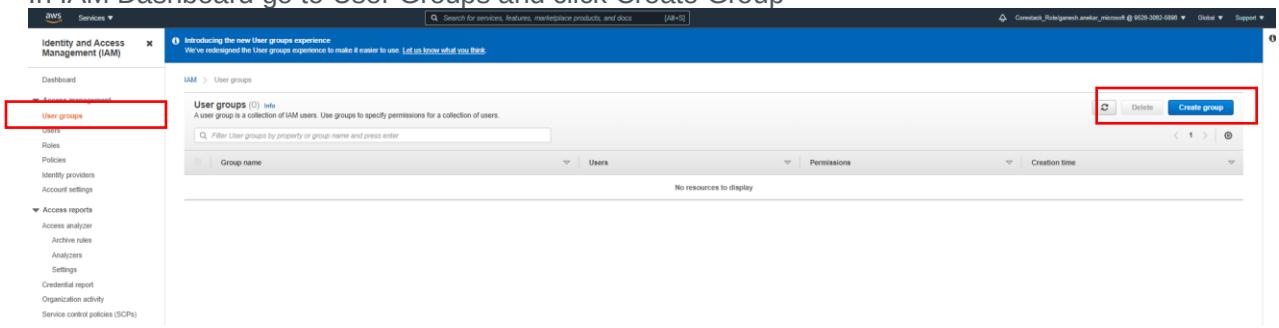
PART 3: Create IAM Group

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

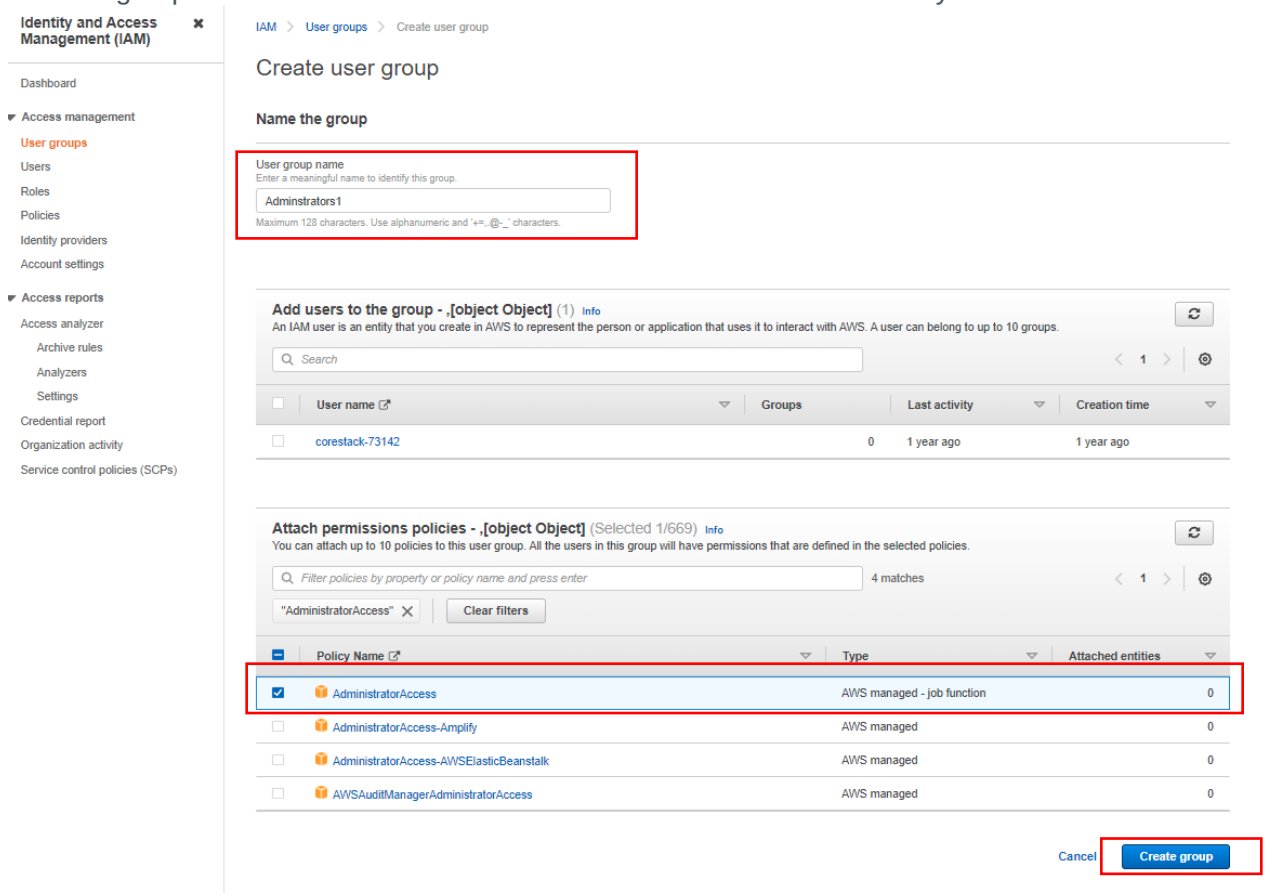
In AWS Management console, search **IAM** and select **IAM**



In IAM Dashboard go to User Groups and click Create Group

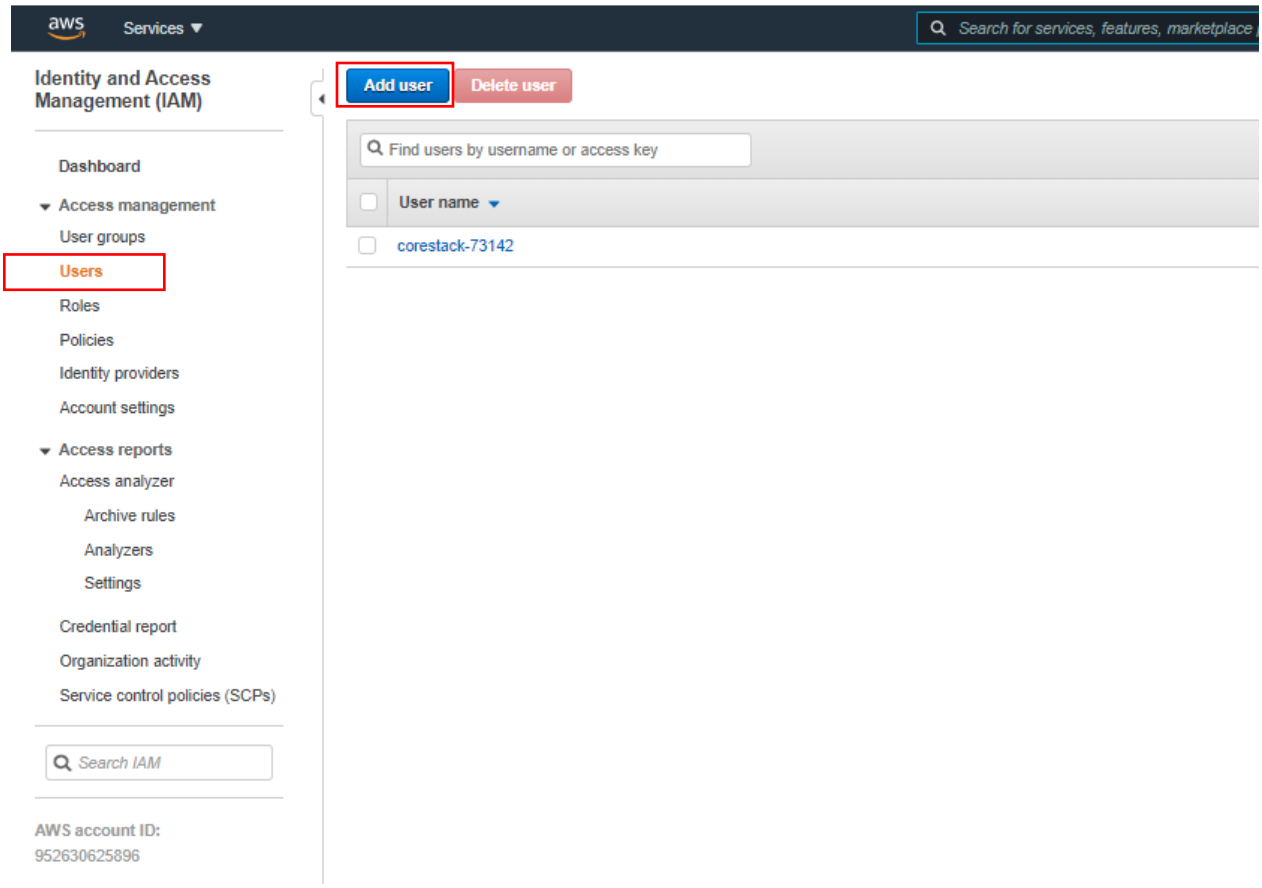


Created group called **Administrators1** – With **AdministratorAccess** Policy



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



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

Add user

1 2 3 4 5

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.

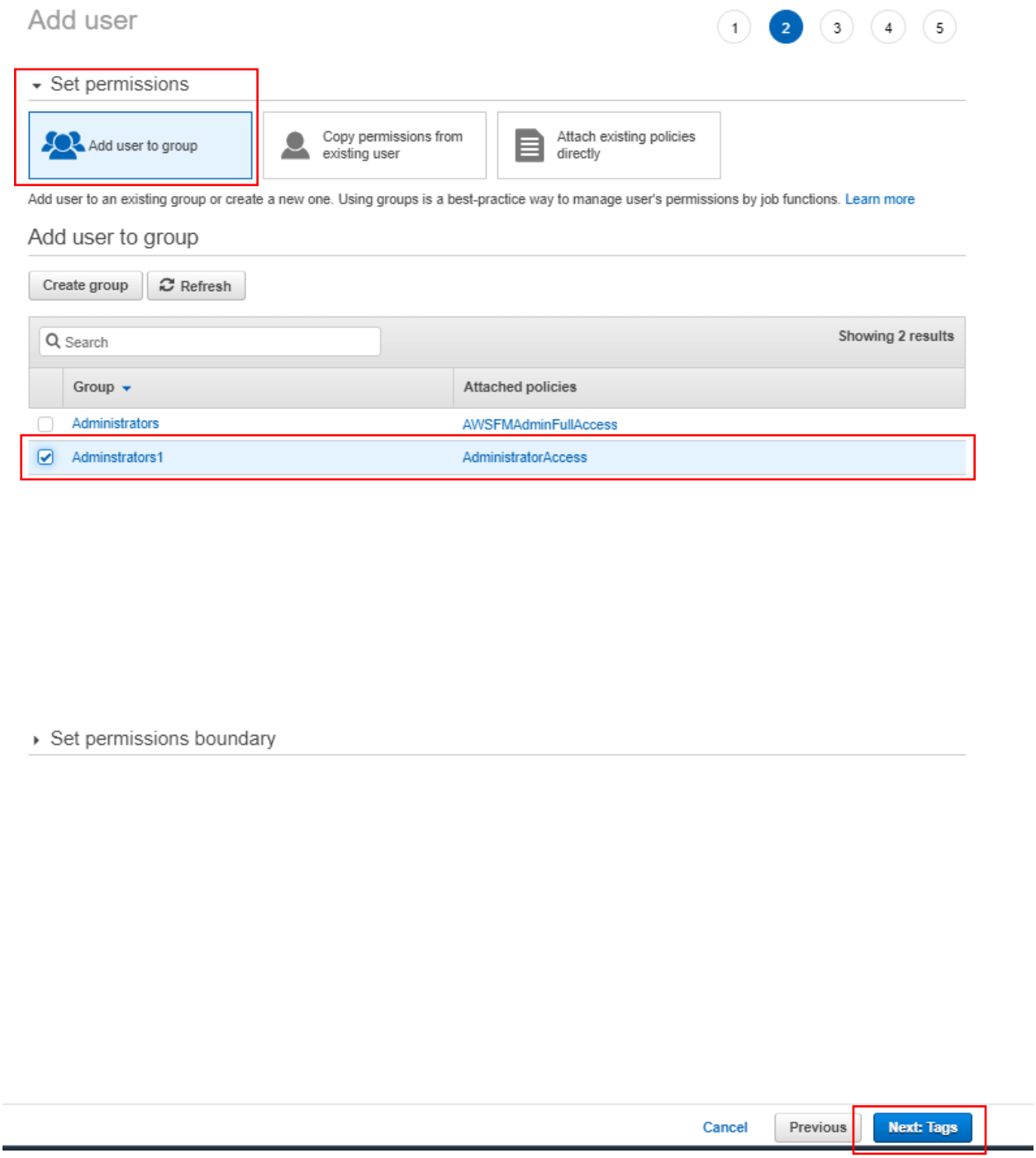
Console password* Autogenerated password
Custom password

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.

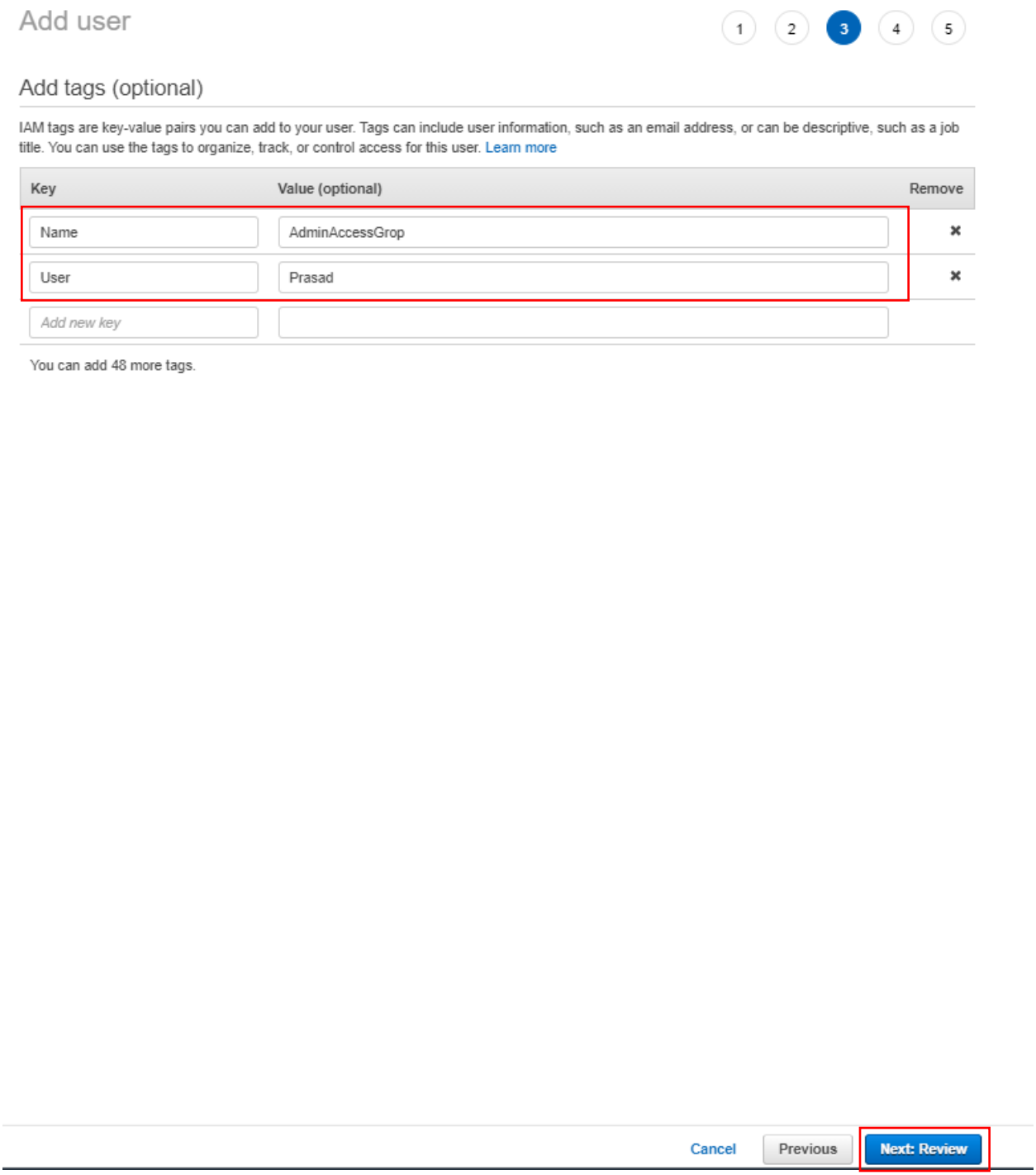
* Required

Cancel Next: Permissions

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



Added Tags and clicked **Next: Review**



Add user **Review Screen** and **Create User**

Add user

1 2 3 4 5

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	Adminstrators1
Managed policy	IAMUserChangePassword

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.**