**Technical Essentials-Project**

**Introduction**

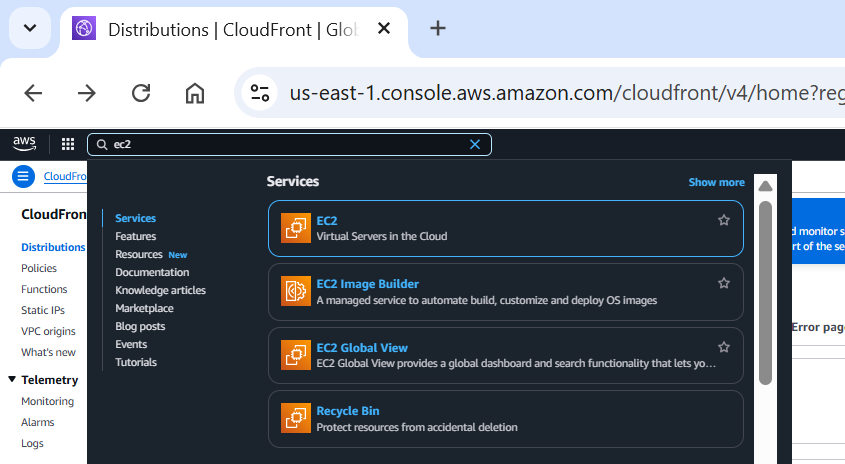
In today's cloud-driven environment, monitoring and managing cloud resources is crucial to ensuring optimal performance and security. This project focuses on monitoring an EC2 instance, configuring automated alerts, and setting up role-based access control in AWS to improve system efficiency and reliability.

The EC2 instance running requires continuous monitoring to track CPU utilization and detect potential performance issues. By leveraging AWS CloudWatch, system administrators can gain real-time insights into resource usage and set up automated alarms for proactive issue resolution. In this project, a CloudWatch alarm is configured to send an email notification to [hoodapiya18@gmail.com](mailto:hoodapiya18@gmail.com), if the CPU utilization drops below 3% for five minutes, ensuring prompt action in case of low resource usage.

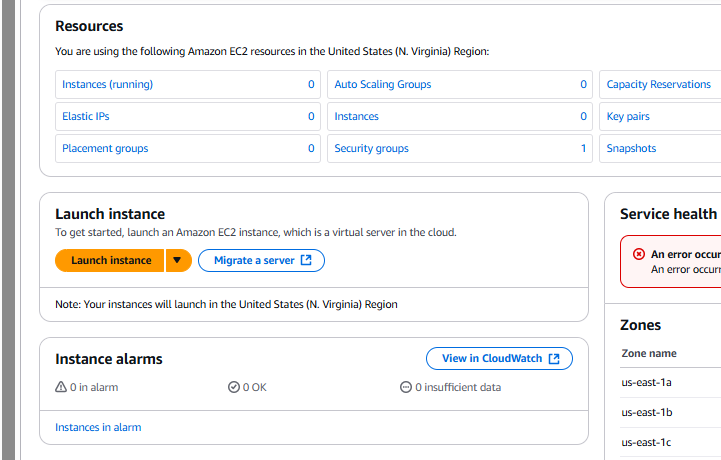
Additionally, effective access control is implemented by creating an IAM Administrator Group with full admin privileges. A new IAM user is added to this group, allowing them to manage AWS resources securely and efficiently. This structured approach enhances performance monitoring, security, and administrative control, enabling seamless cloud operations for the organization.

**Step 1: Monitor CPU Utilization Using AWS CloudWatch**

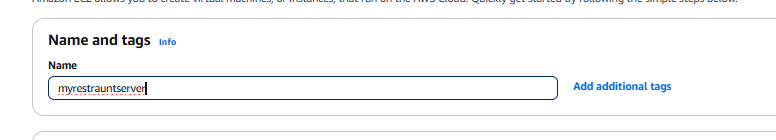
1. Navigate to **EC2 Dashboard** in the AWS Console.



1. Click **Launch Instance**.

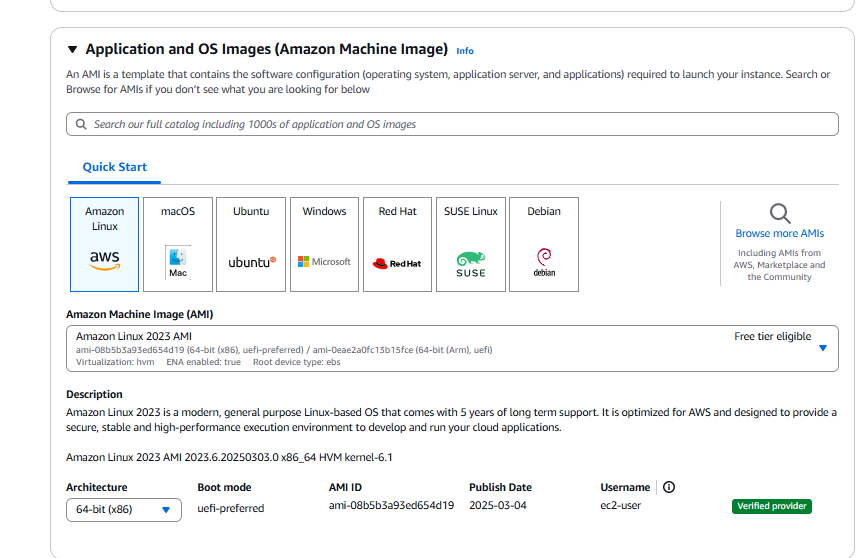


Name the instance as below:

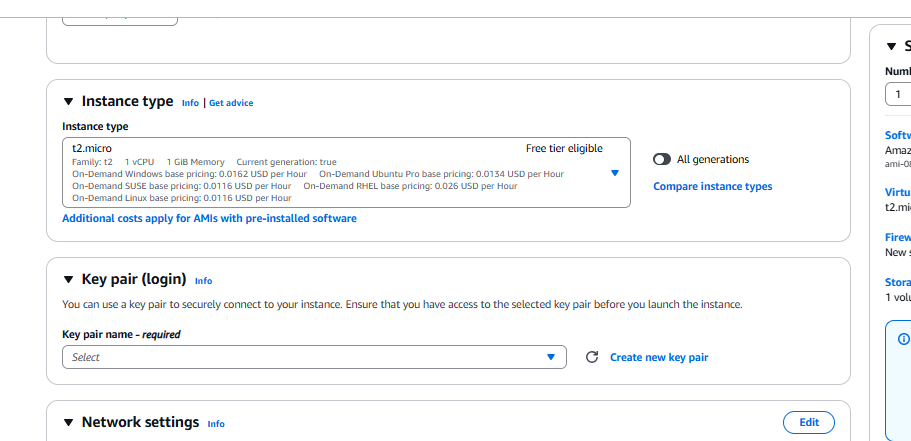


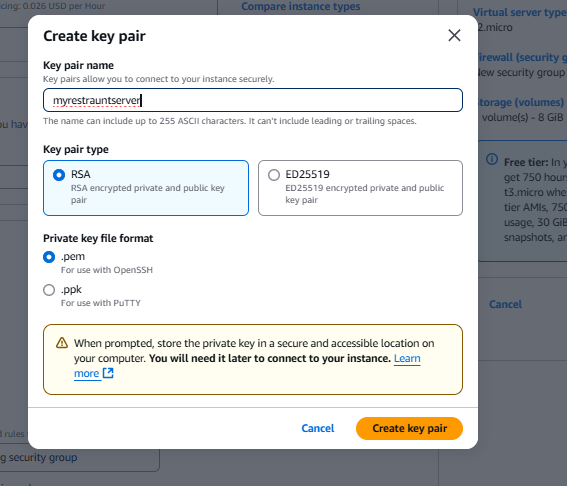
1. Choose an Amazon Machine Image (AMI) (e.g., Amazon Linux or Ubuntu).

For my project I will select Linux.

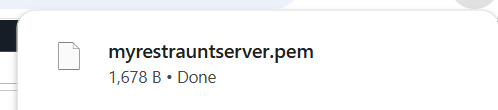


1. Select an **instance type** (e.g., t2.micro for free tier).

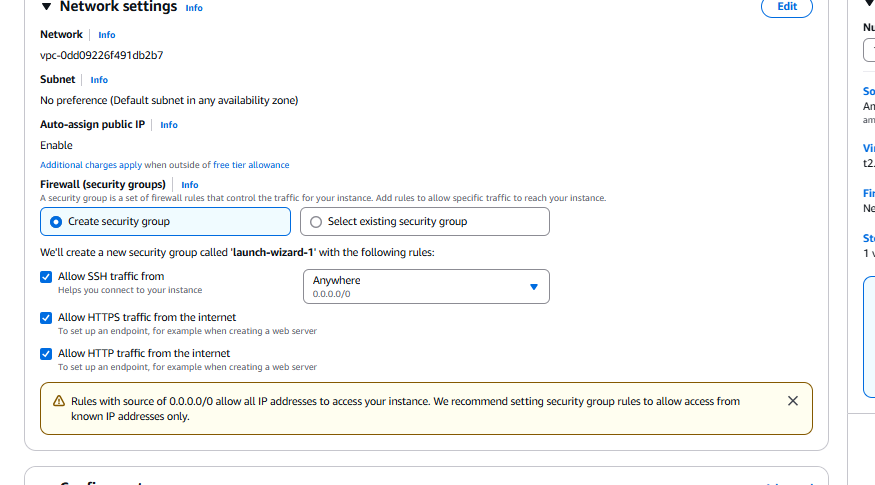




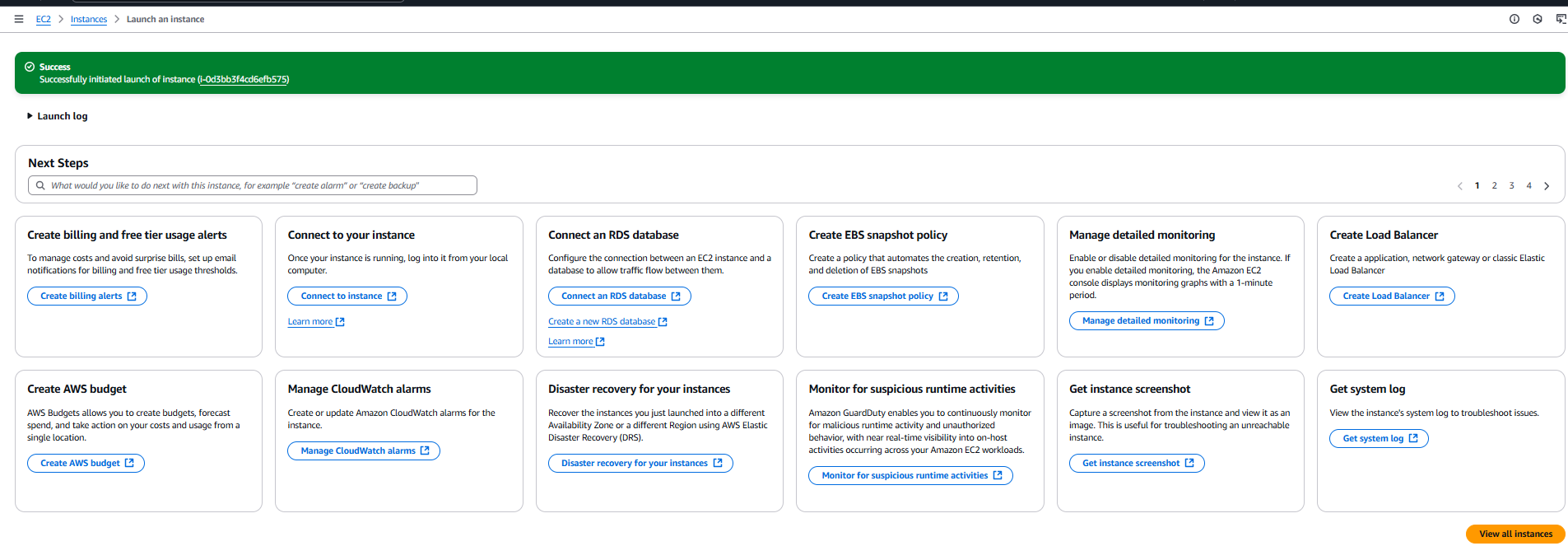
1. Configure **key pair** for SSH access.

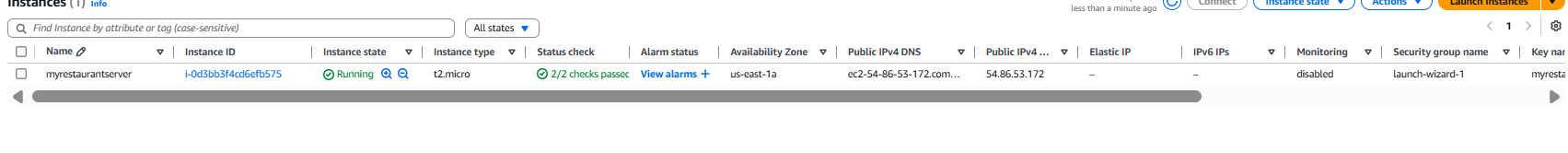


1. Allow **HTTP (port 80) and HTTPS (port 443)** in **Security Group**.

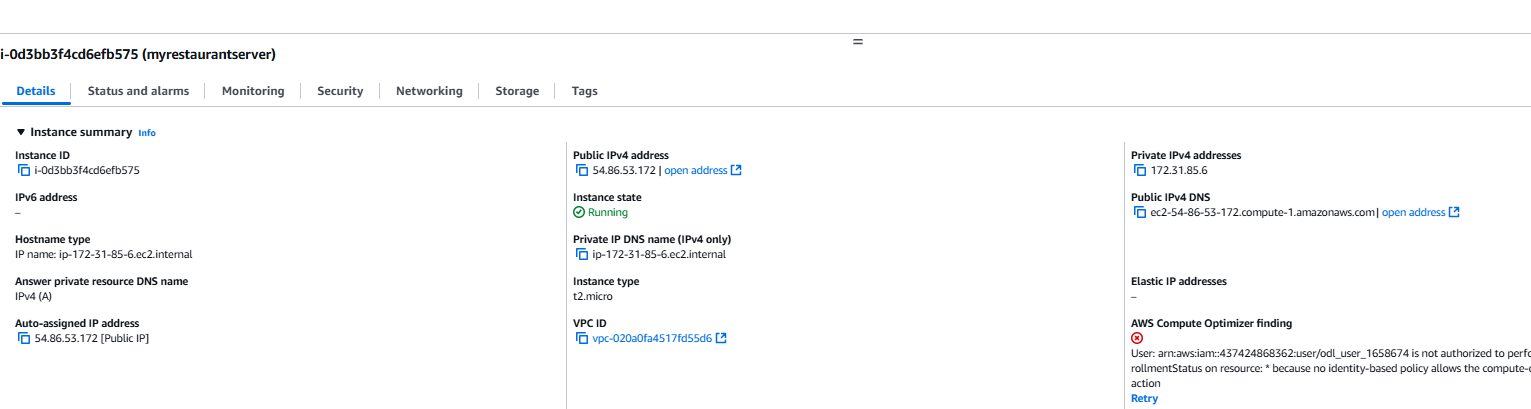


1. Click **Launch** to create instance.

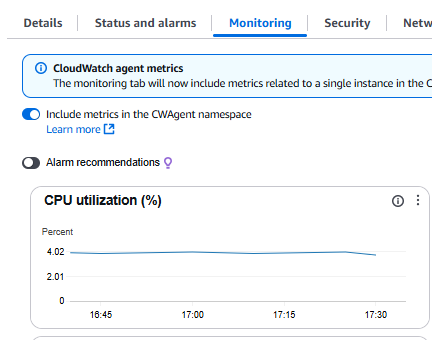


Instance created.  


1. Click on the **Monitoring** tab.



1. Locate **CPU Utilization** and observe the graph.



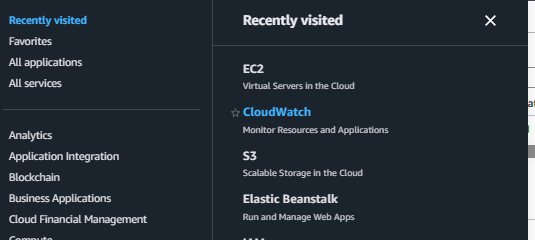
**Now, you can track the performance of the EC2 instance.**

**Step 2: Create a CloudWatch Alarm for Low CPU Utilization**

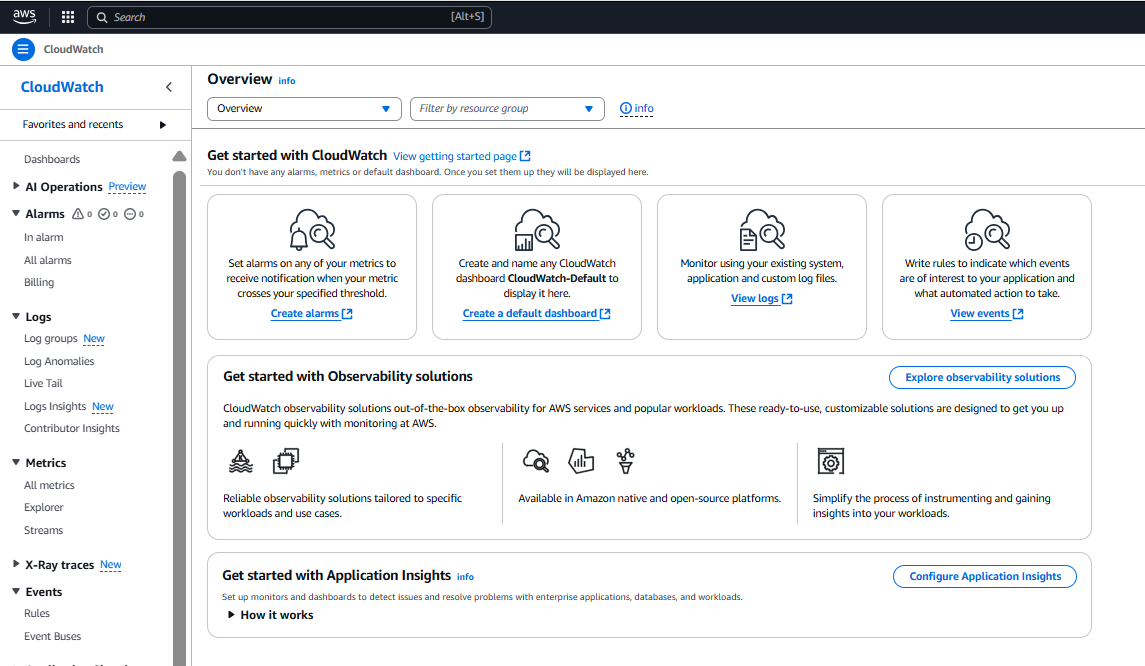
The goal is to **send an email notification** when CPU utilization **falls below 3% for three consecutive times in 5 minutes**.

**2.1 Open AWS CloudWatch**

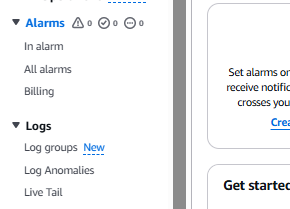
1. Go to **AWS Management Console**.



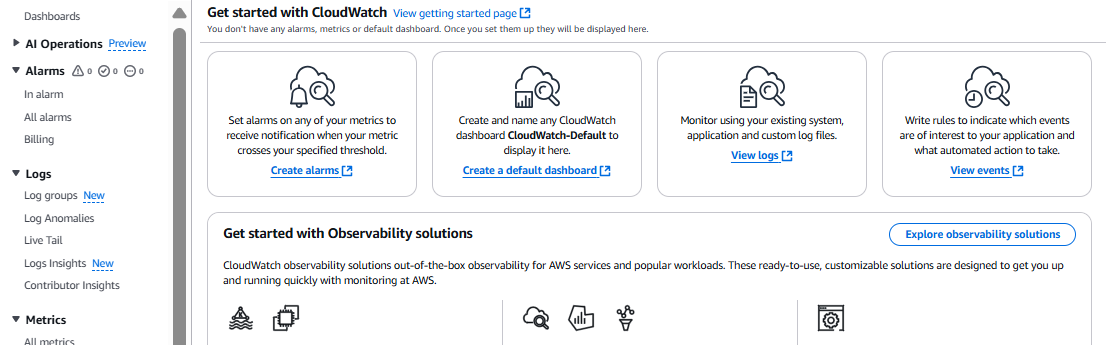
1. Navigate to **CloudWatch**.



1. In the left menu, select **Alarms**.

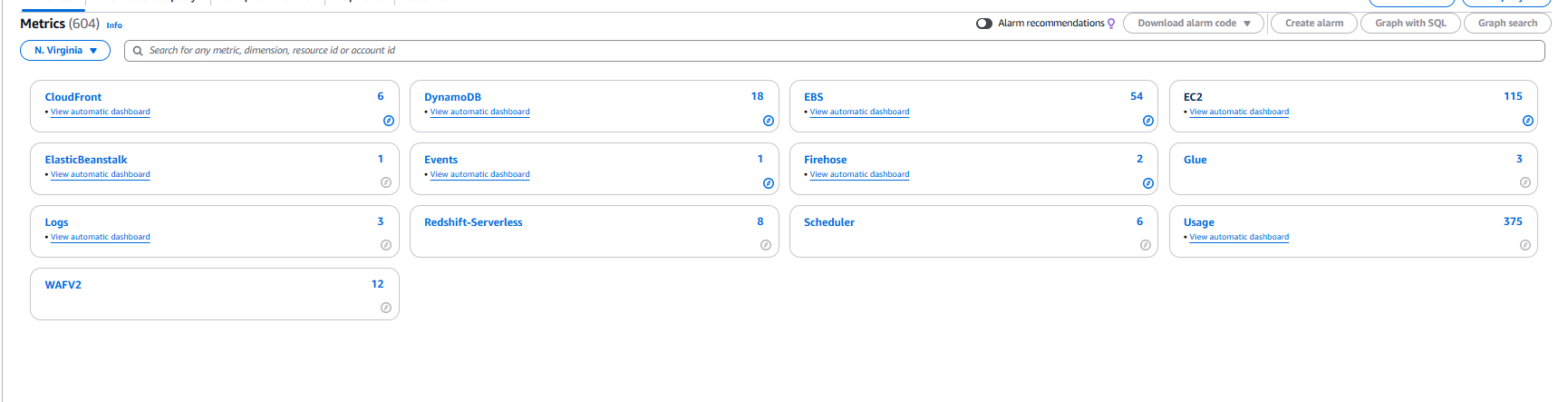


1. Click **Create Alarm**.

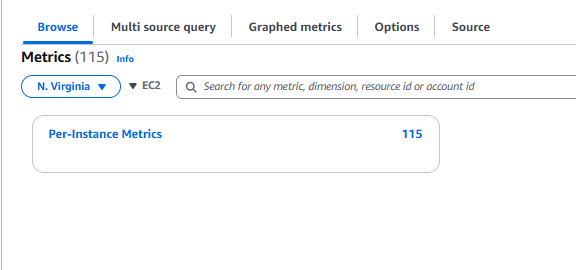


**2.2 Set Up the Alarm Condition**

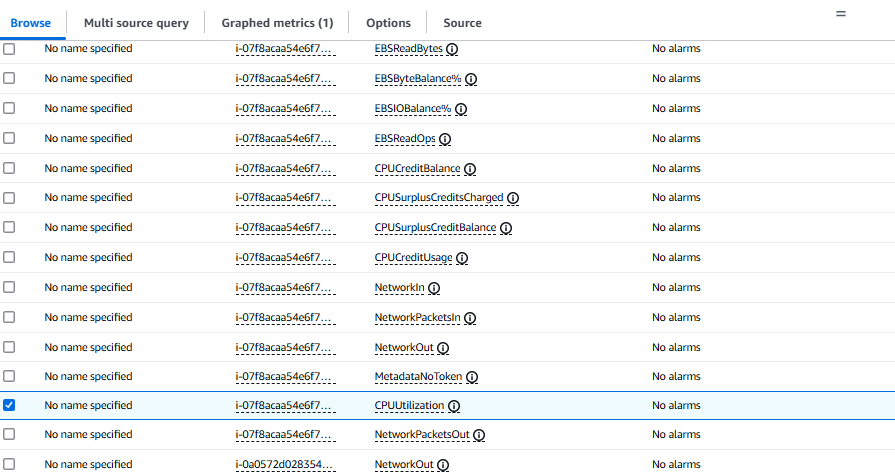
1. Click **Select Metric** → **EC2 Metrics**.



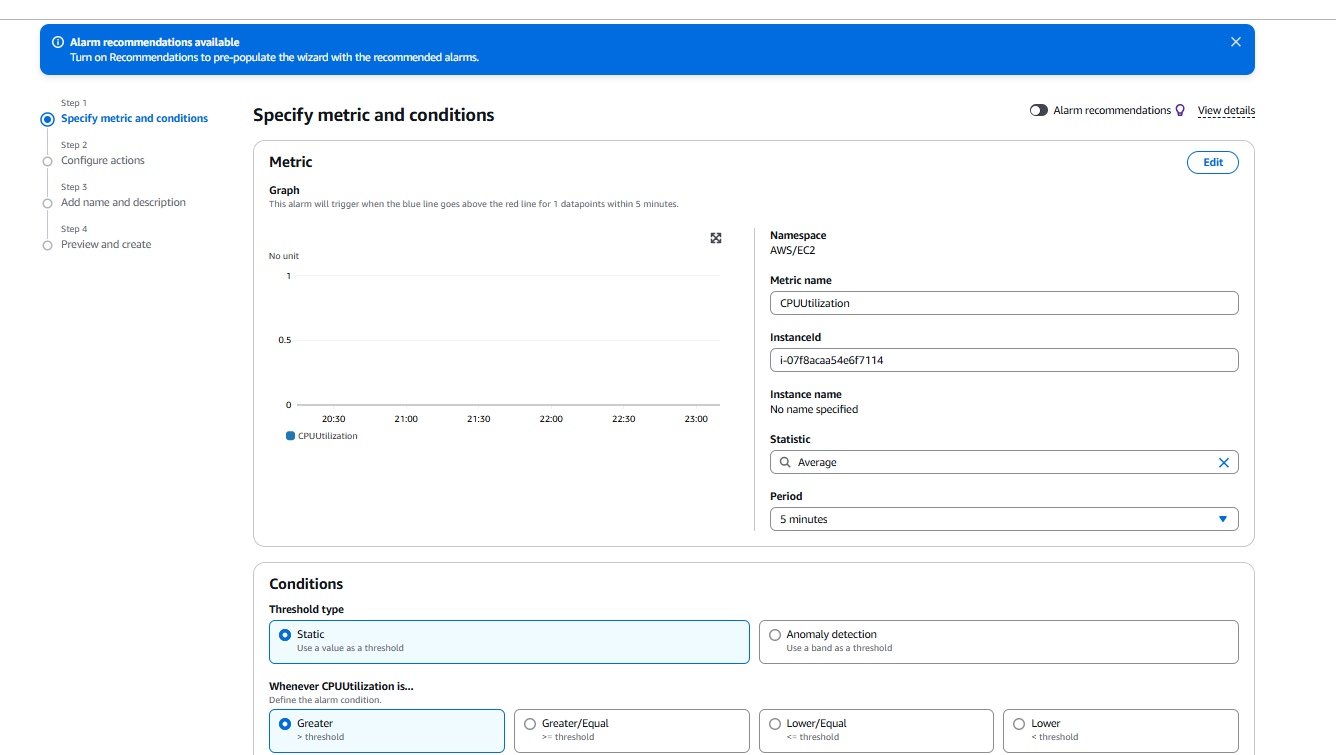
1. Select **Per-Instance Metrics**.



1. Choose **CPUUtilization** for your **EC2 instance**.

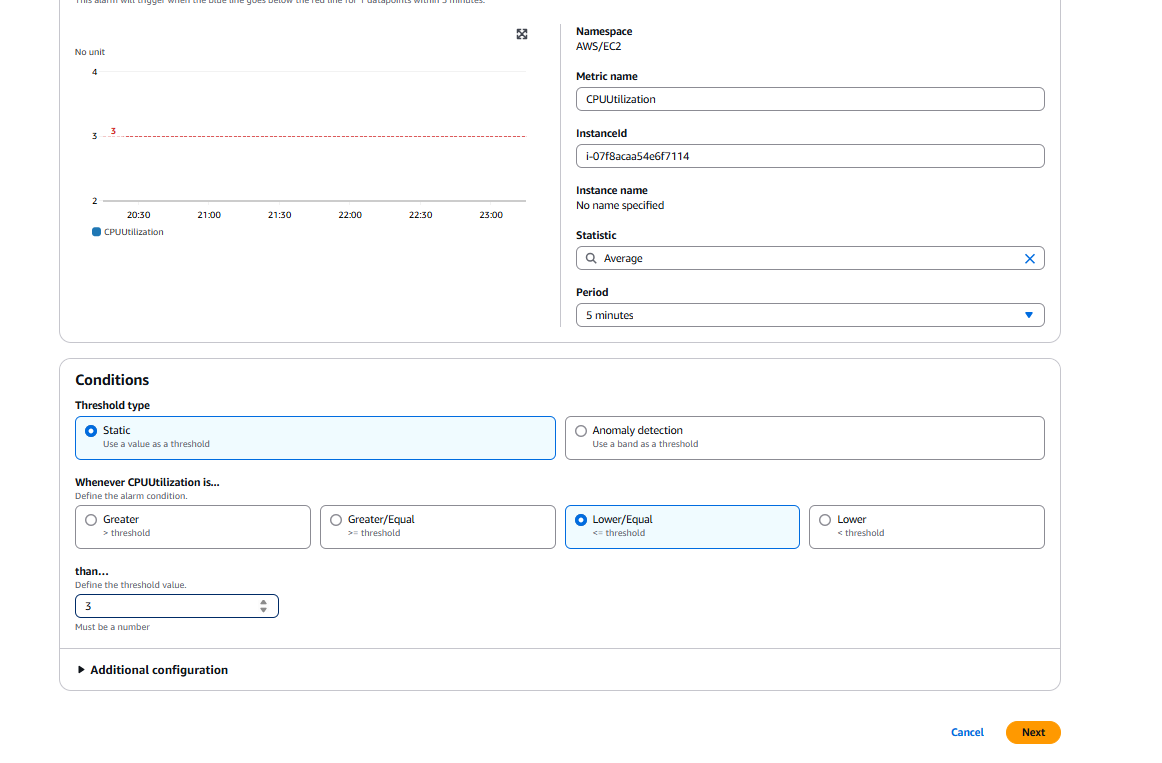


1. Click **Select metric**.

Create metrics.  


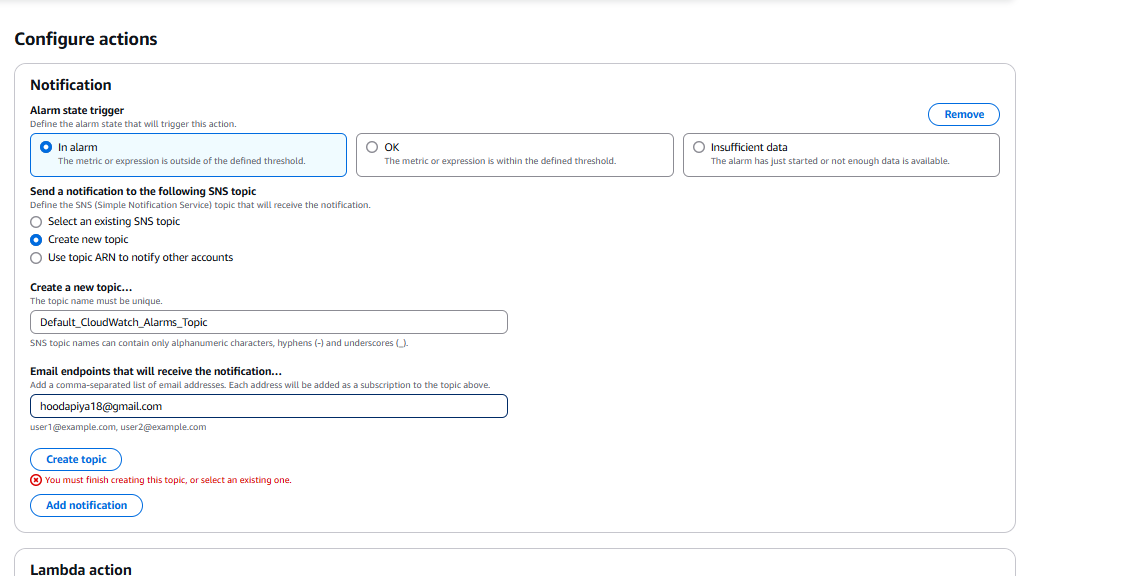
**2.3 Define the Threshold Condition**

1. Under **Threshold Type**, select **Static**.
2. Set **Threshold Value** to **3%**.
3. Select **Alarm Condition**:
   * **Whenever CPU utilization is below 3%**.
   * **For three consecutive periods of 5 minutes each**.

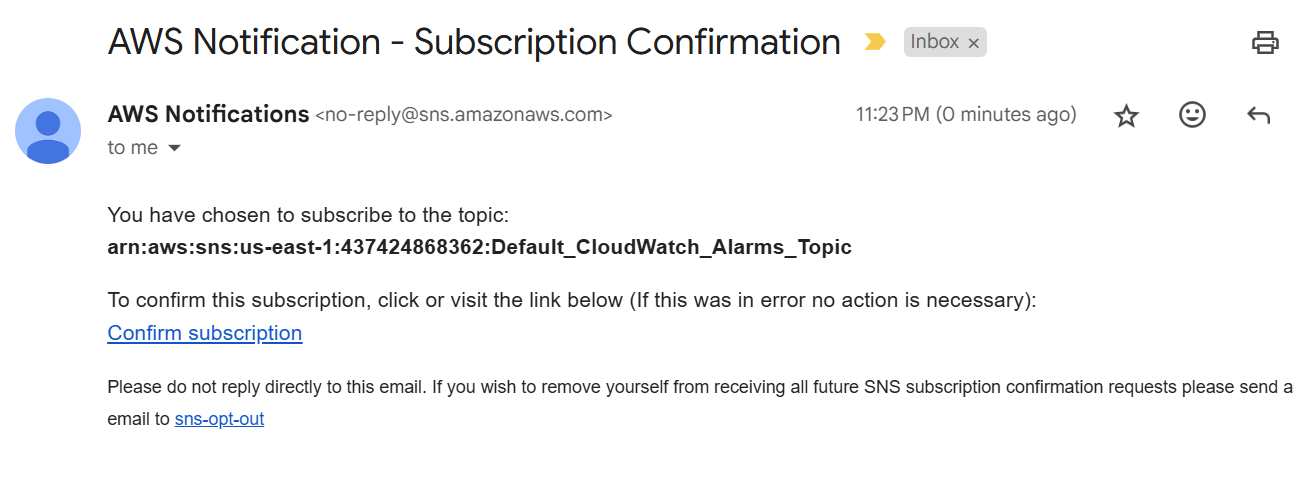


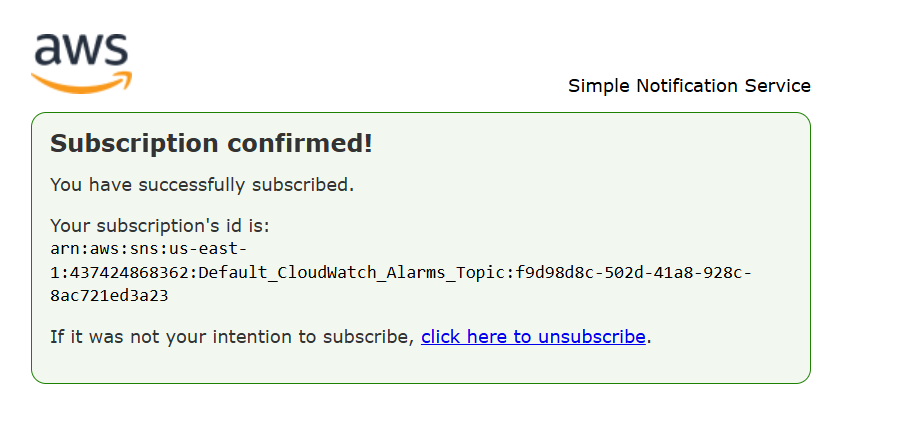
**2.4 Configure the Alarm Action**

1. Under **Notification**, select **Create New SNS Topic**.
2. Name it **HCMonitorTopic**.
3. Enter the email [(hoodapiya18@gmail.com) -as](mailto:(hoodapiya18@gmail.com)%20-as) [HCMonitor@HeavenClassics.com](mailto:HCMonitor@HeavenClassics.com) is imaginary)



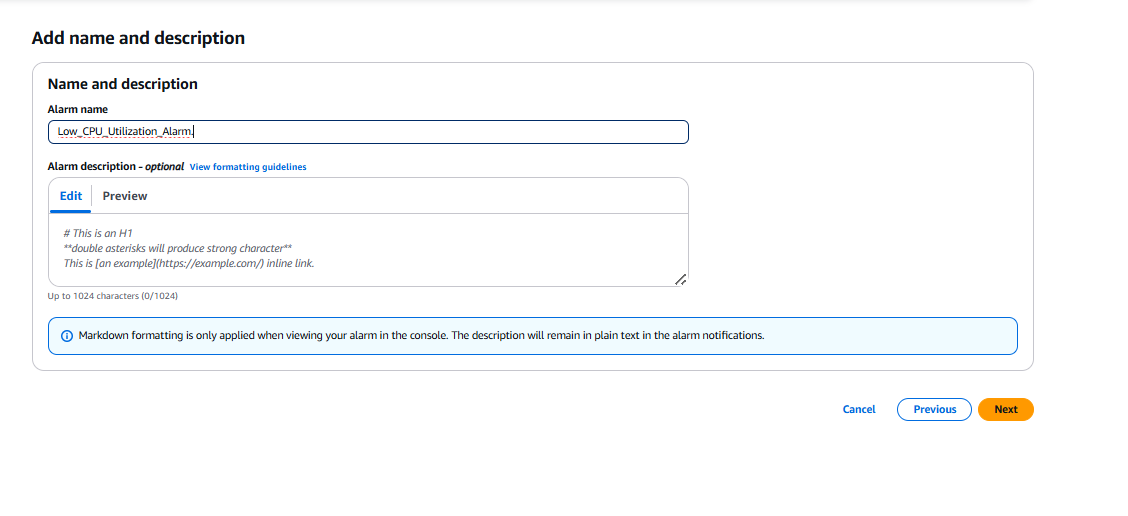
1. Click **Create topic**.
2. **Check your email inbox** and **confirm the SNS subscription**.

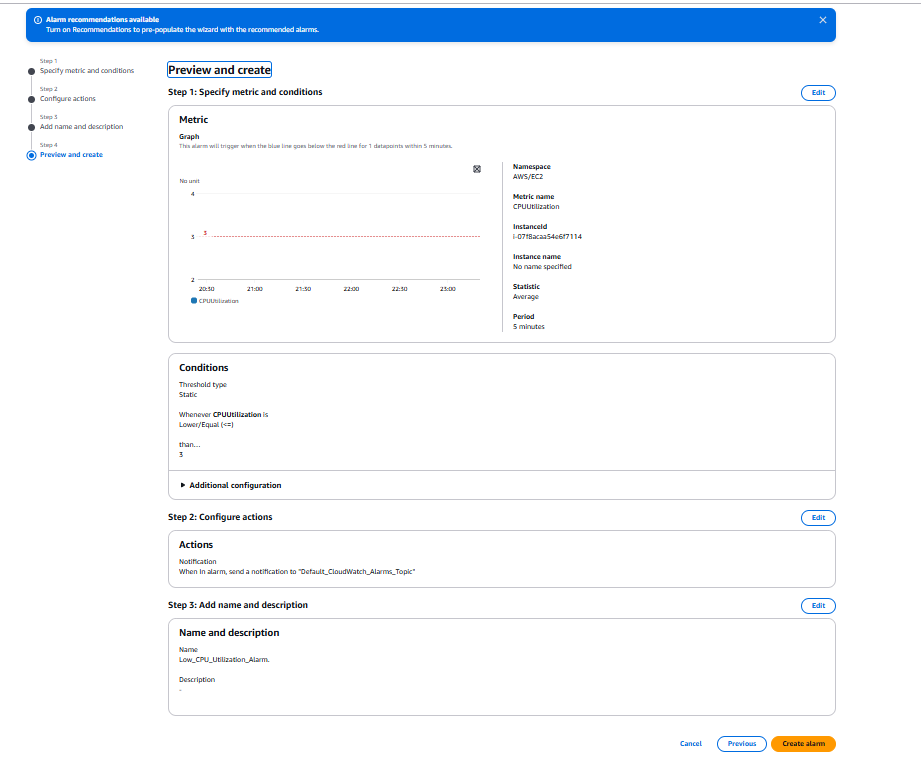




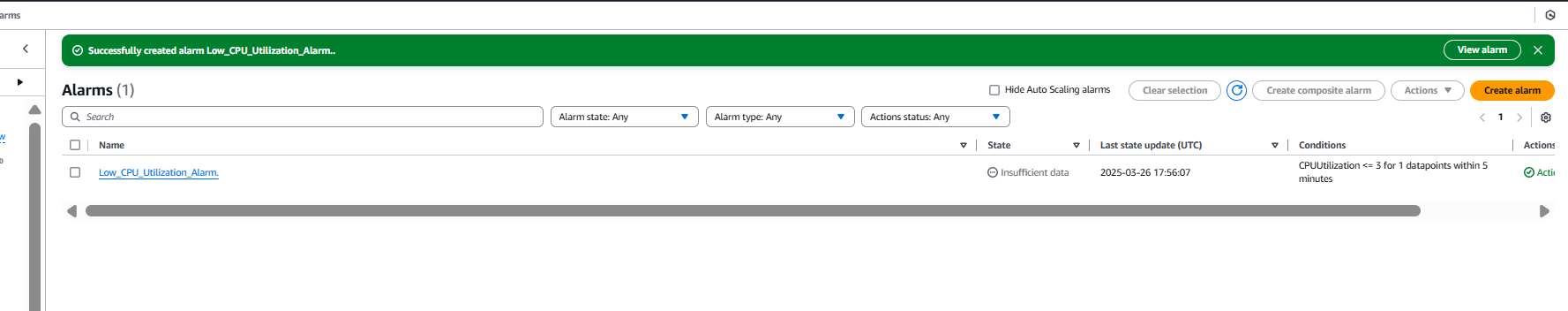
**2.5 Finalize and Create the Alarm**

1. Name the alarm **Low\_CPU\_Utilization\_Alarm**.



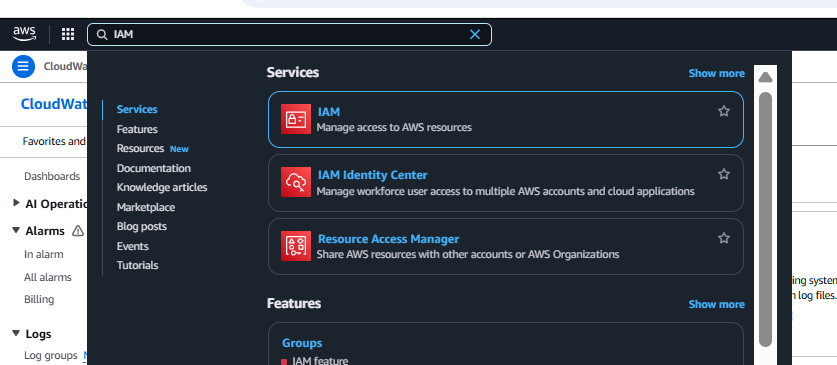
1. Click **Create Alarm**.
2. 

**Now, an email alert will be sent if CPU utilization falls below 3% for 5 minutes.**

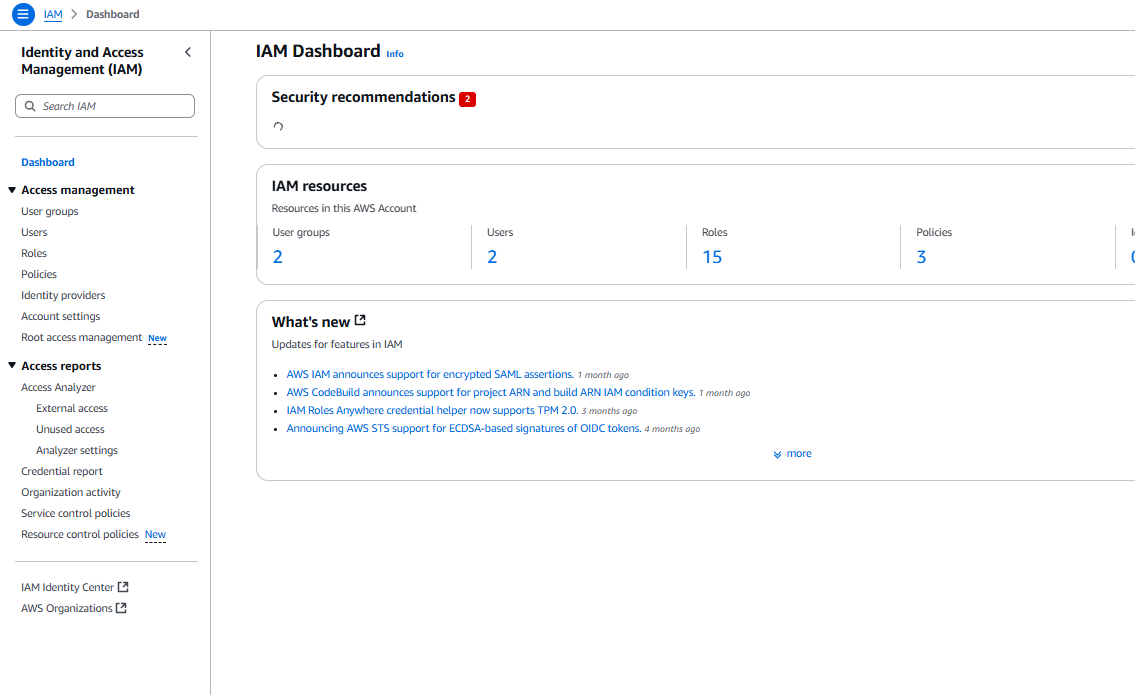


**Step 3: Create an IAM Group for Administrators**

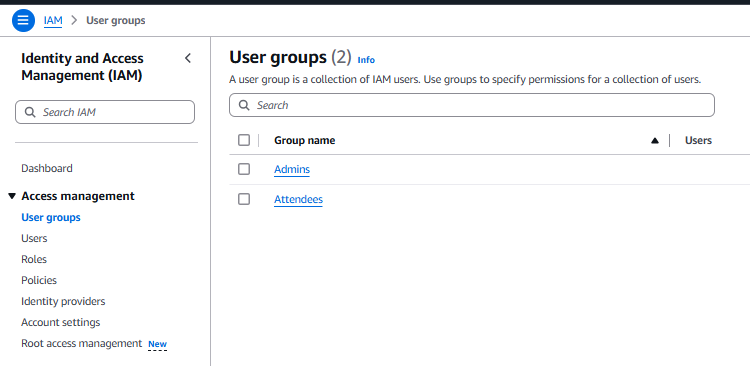
1. Go to **AWS Management Console**.



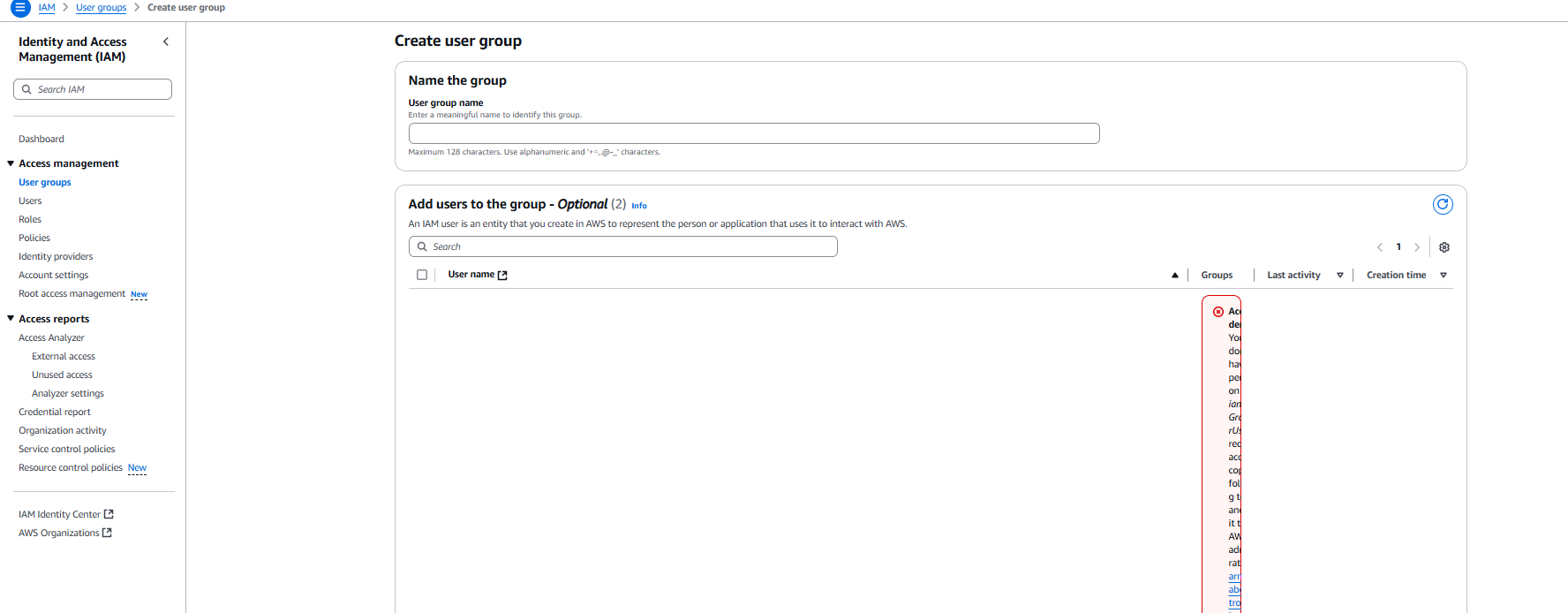
1. Navigate to **IAM (Identity & Access Management)**.



1. In the left menu, select **User Groups**.

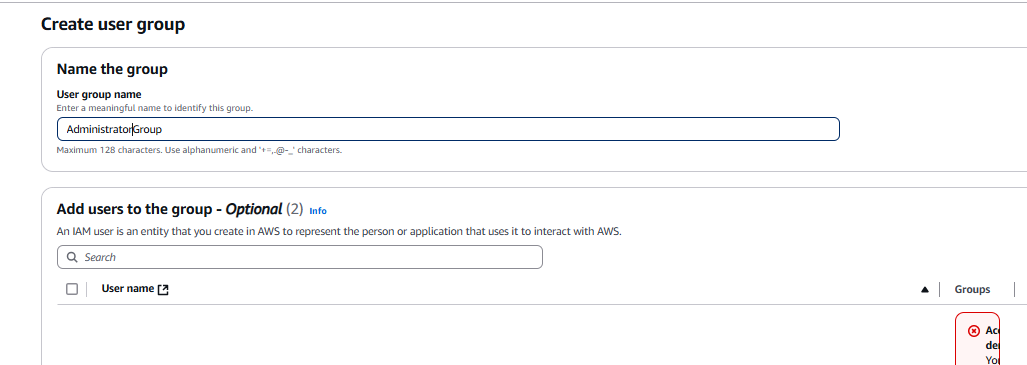


1. Click **Create Group**.

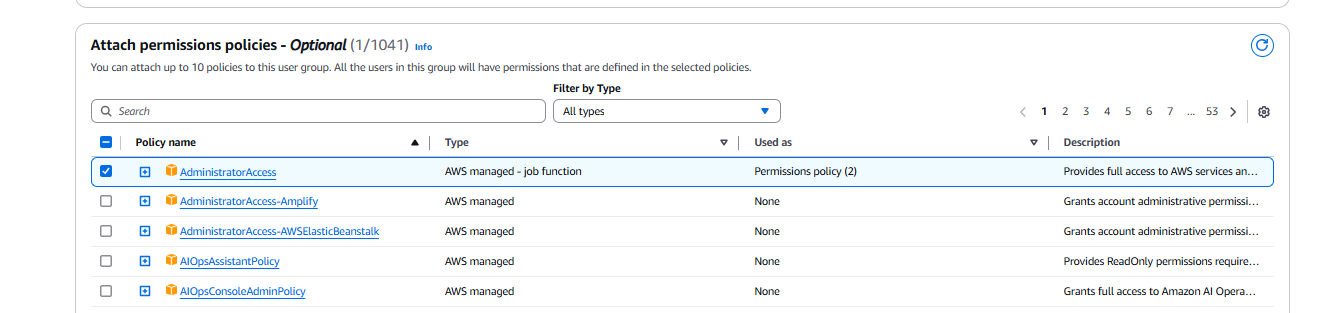


**3.1 Configure the IAM Group**

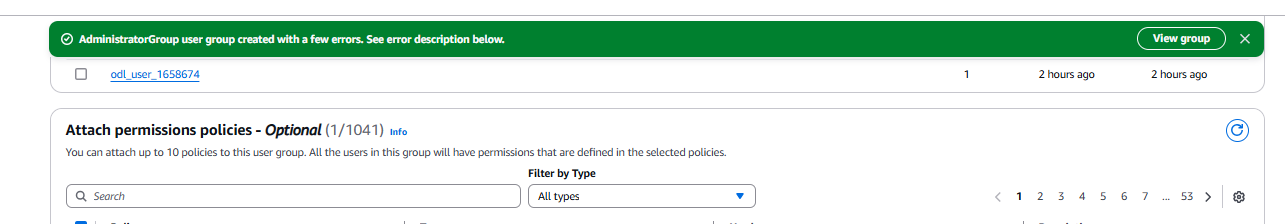
1. **Enter Group Name**: Administrator-Group.



1. For permissions In the search bar, type AdministratorAccess and Check the box for **AdministratorAccess policy**.



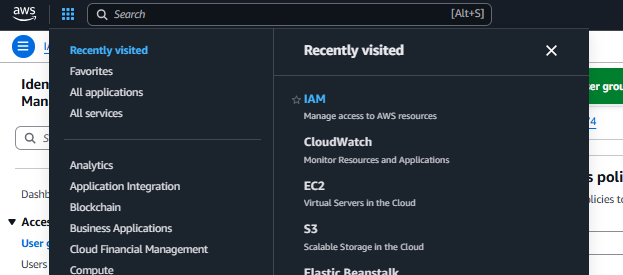
1. Click **Next** → **Create Group**.



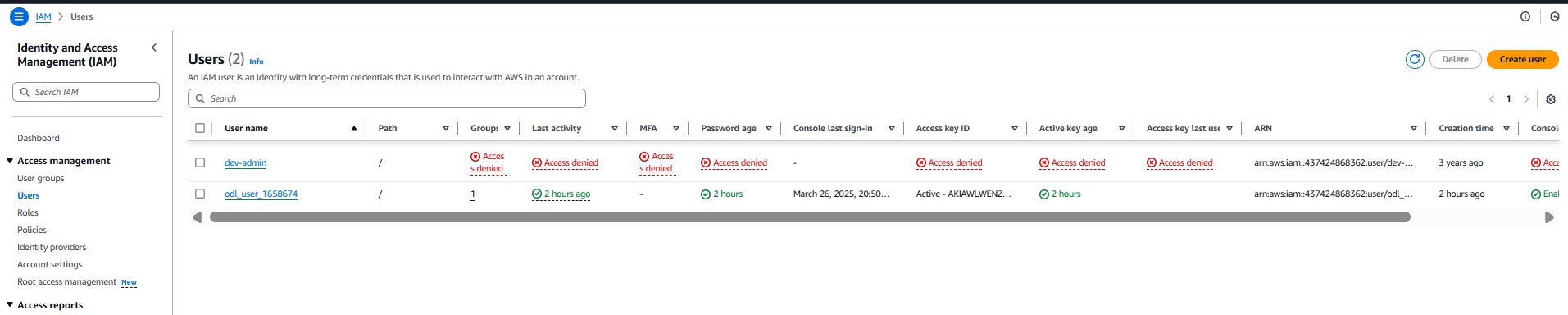
**Now, the "Administrator-Group" has full admin permissions.**

**Step 4: Create an IAM User and Add Them to the Administrator Group**

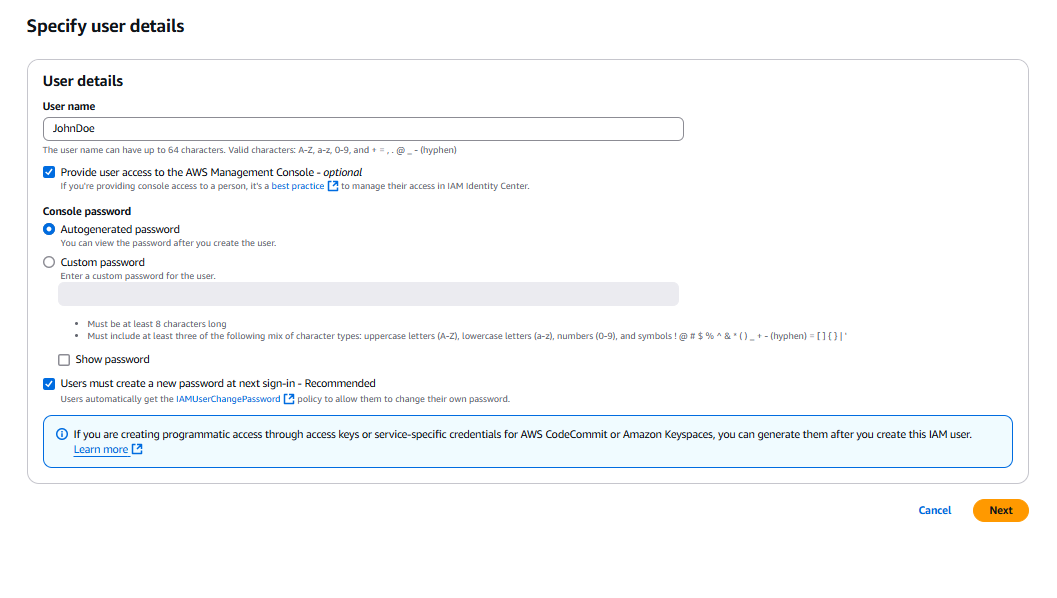
1. Go to **AWS IAM Console**.



1. In the left menu, click **Users**.

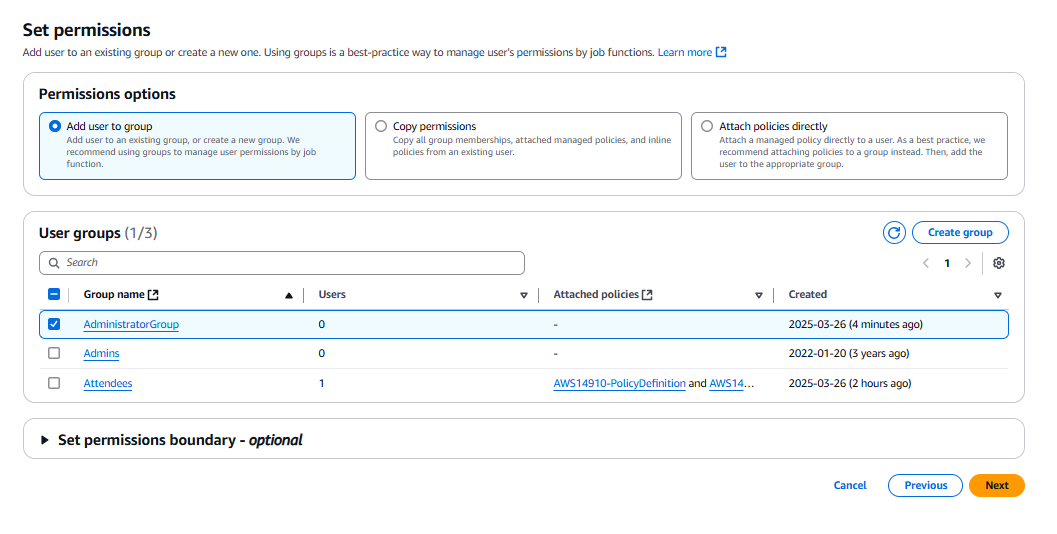


1. Click **Create User**.
2. **Username**: JohnDoe
3. Select **Provide user access to AWS Management Console**.
4. Choose **"Autogenerated password"**.

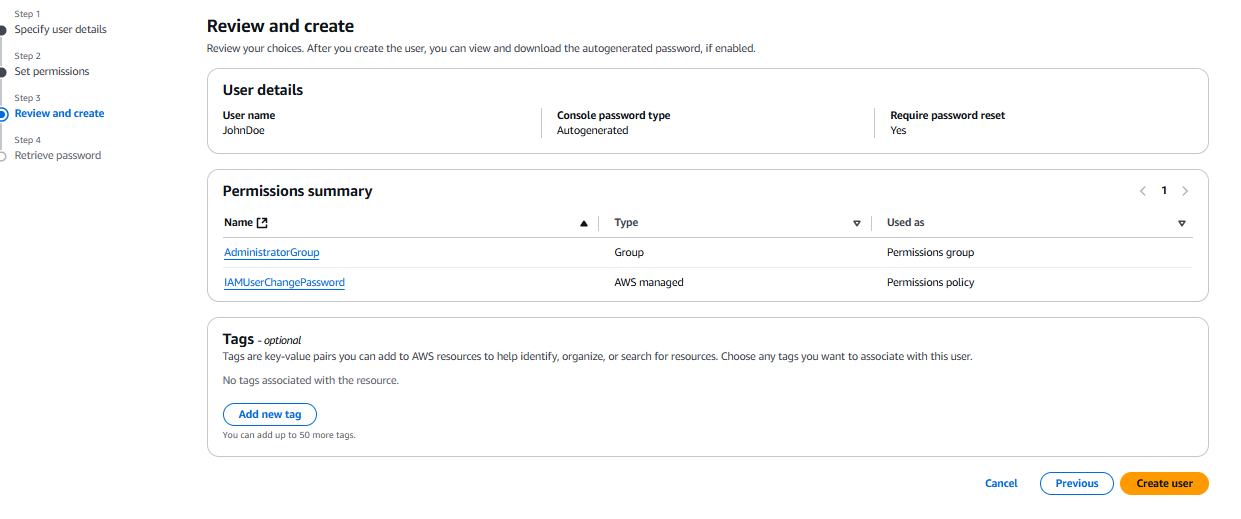


**4.2 Assign User to Administrator Group**

1. Click **Next: Permissions**.
2. Select **Add User to Group**.
3. Choose **Administrator-Group**.



1. Click **Next** → **Create User**.



**The user "JohnDoe" is now part of the Administrator Group and has full access to AWS.**

