**Placement Empowerment Program**

***Cloud Computing and DevOps Centre***

**Set Up IAM Roles and Permissions:**Create an IAM role on your cloud platform. Assign the role to your VM to restrict/allow specific actions.

Name: Mathimalar.P Department : ADS



**Introduction and Overview**..

IAM (Identity and Access Management) roles in cloud platforms like AWS allow virtual machines (VMs) to securely interact with cloud services without requiring manual access credentials. By assigning an IAM role to a VM, permissions can be managed efficiently, ensuring only authorized actions are allowed.

**Objective**

 Create an IAM role with specific permissions.

 Attach the IAM role to a VM instance (EC2 in AWS).

 Ensure secure and restricted access to cloud resources.

 Verify the role’s effect by attempting allowed and denied actions.

Importance

 **Enhanced Security** – Eliminates the need for storing access keys.

 **Granular Access Control** – Restricts actions to only what's necessary.

 **Automated Credential Management** – AWS handles temporary credentials securely.

 **Scalability** – Easily assign roles to multiple VMs without manual configuration.

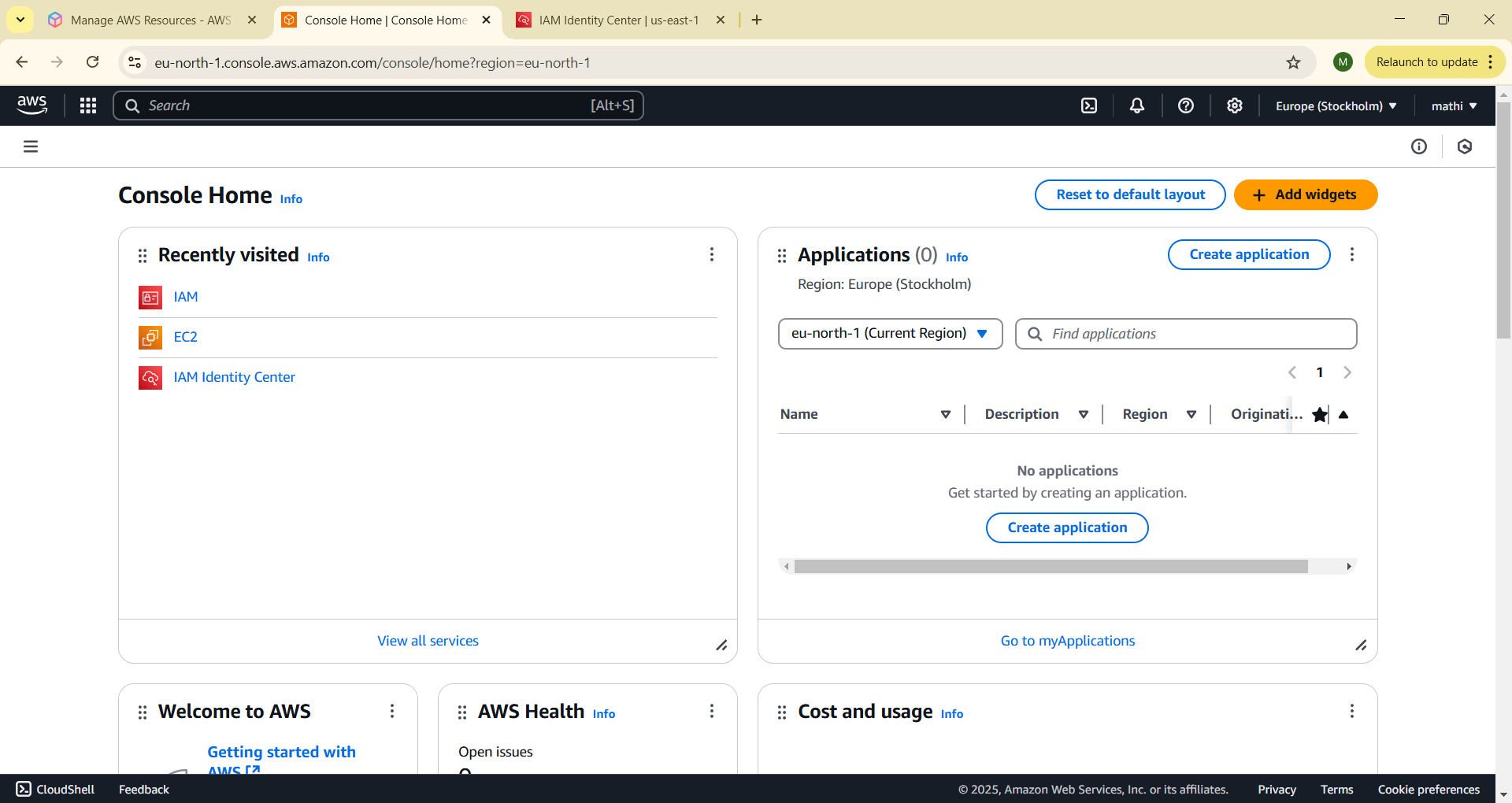
**Step-by-Step Overview**

Step 1:

Step 1:

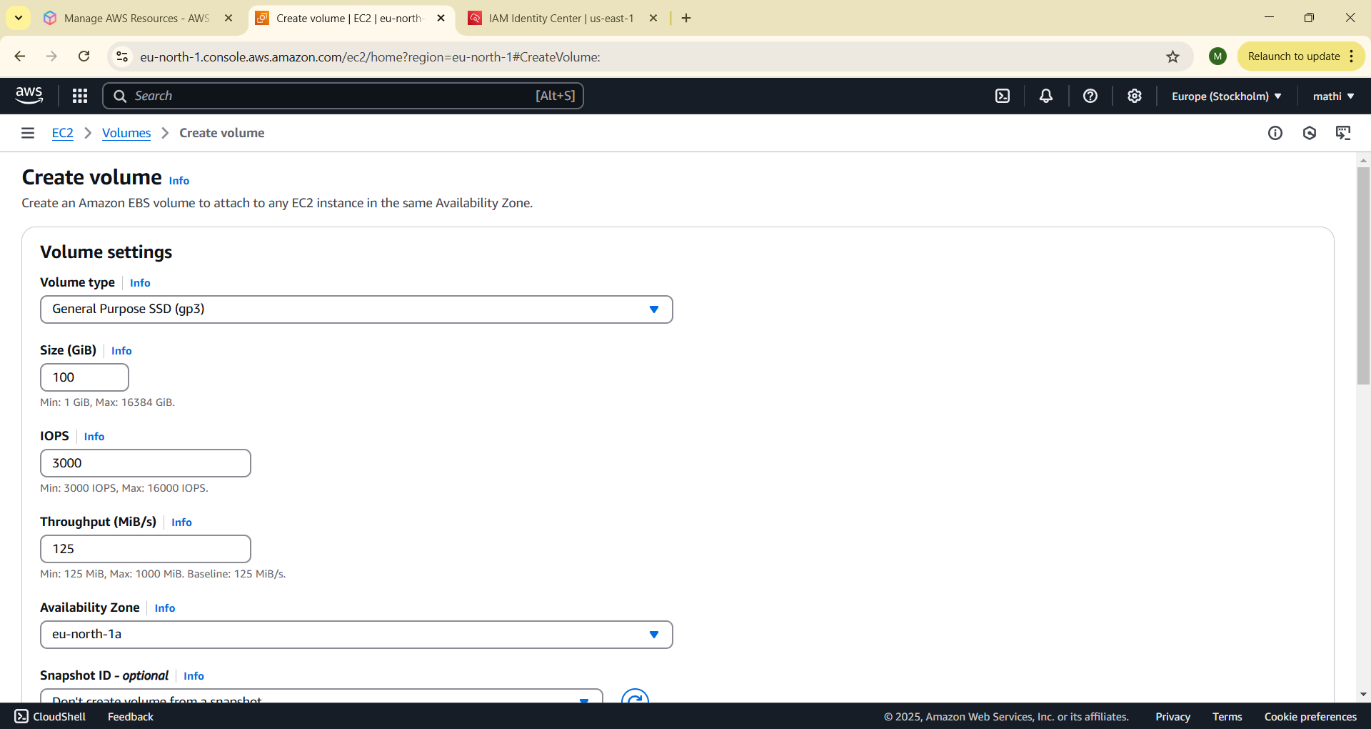
1. Go to AWS Management Console.

2. Enter your username and password to log in



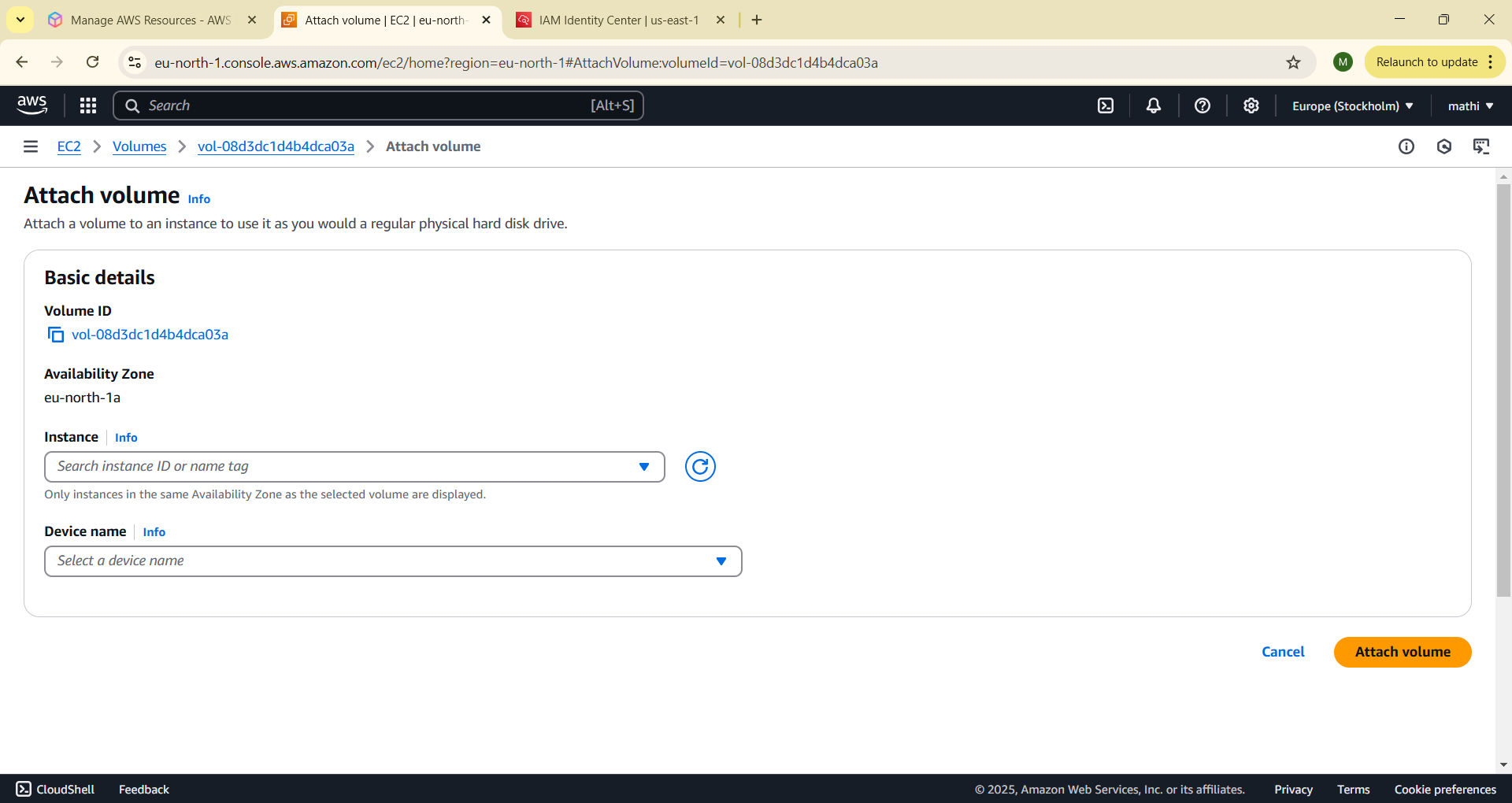
Step 2:

On the EC2 Dashboard, click on Launch Instances and enter a name for your instance (e.g., "My Monitoring Instance"). Leave other settings as default and Click Launch Instance.



Step 3:

Go to the EC2 Dashboard in the AWS Console. In the left menu, click Volumes under Elastic Block Store (EBS). Click Create Volume.

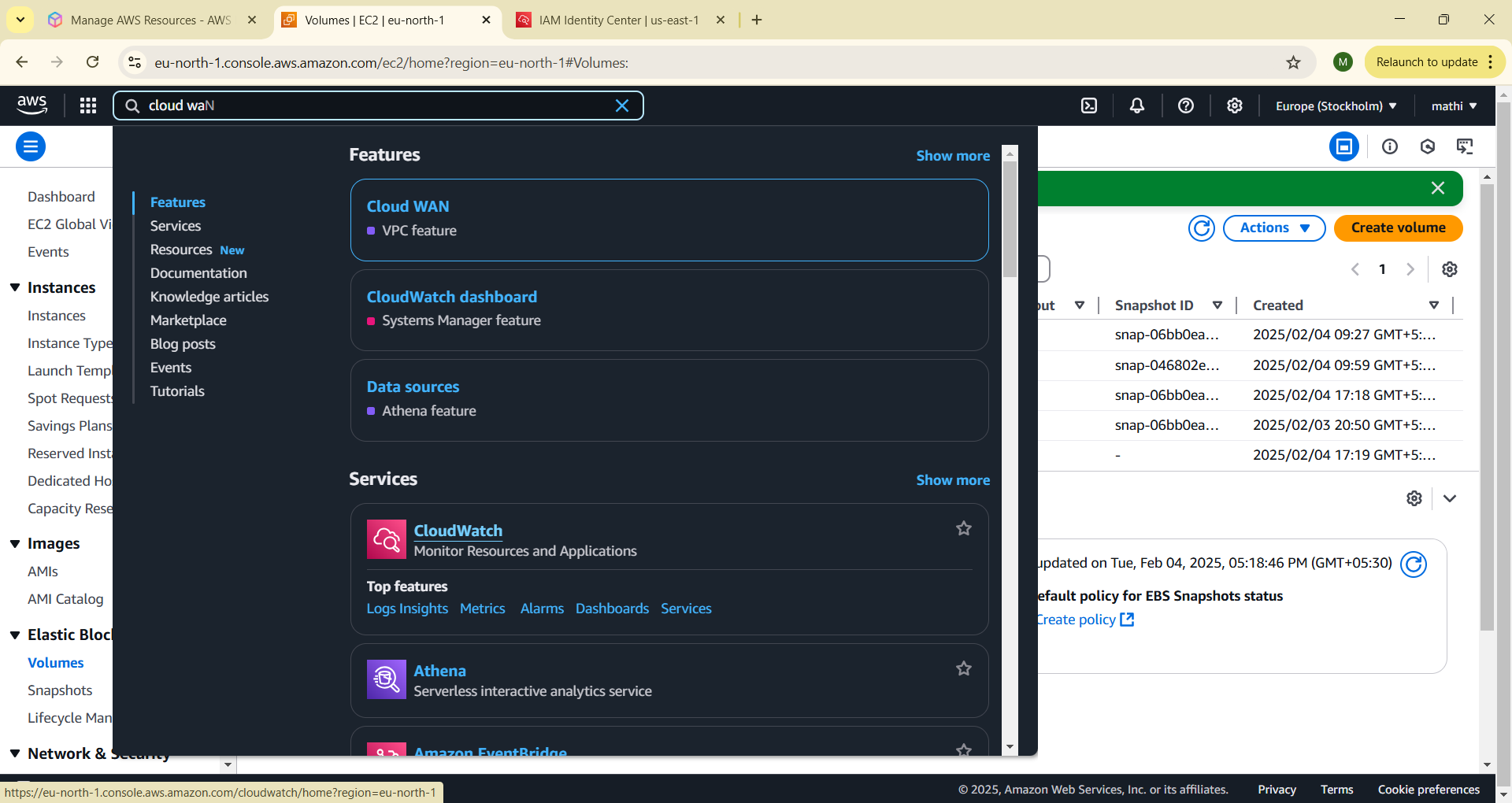


Step 4:

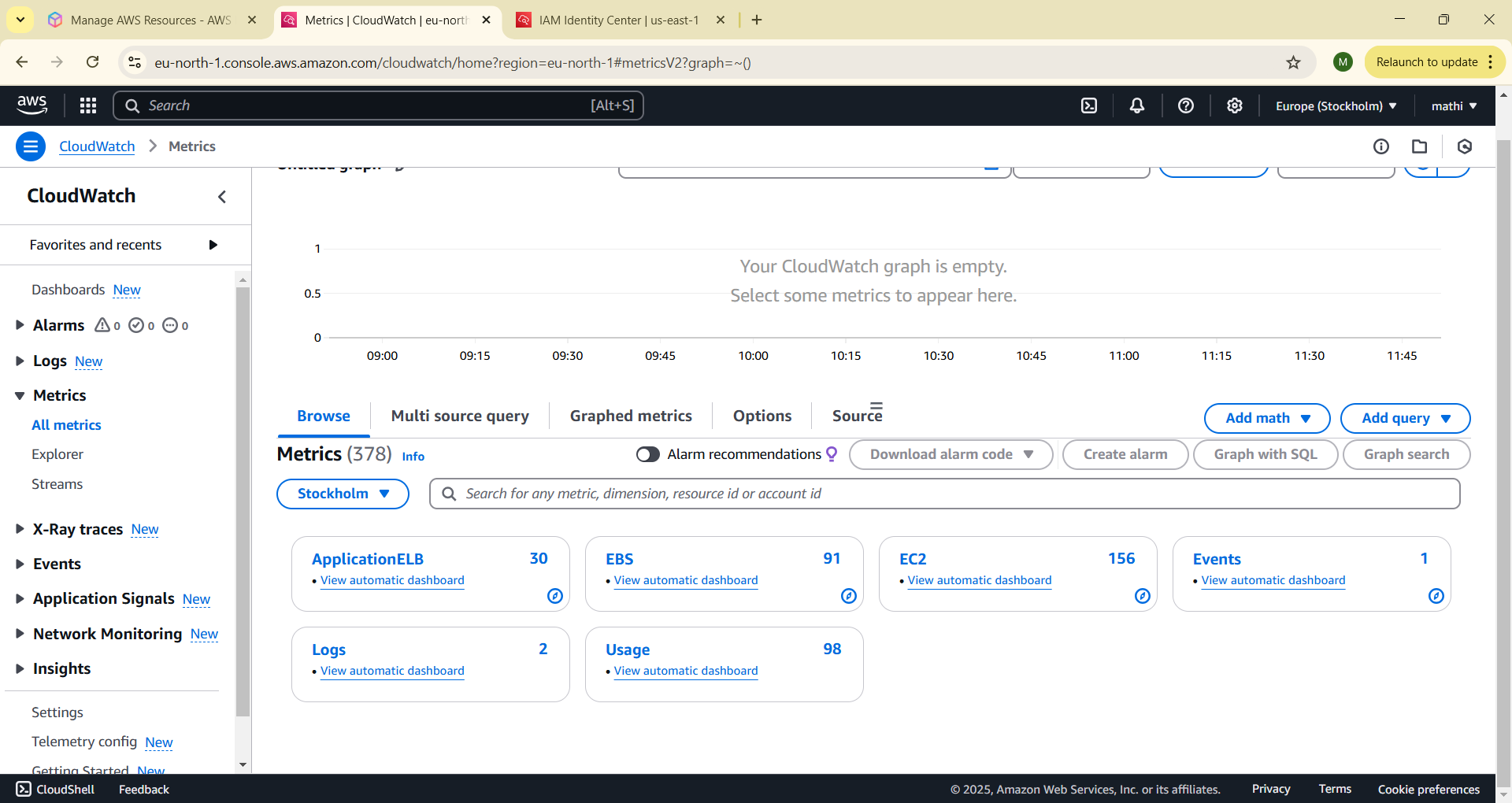
Once created, go to your Volumes list, select the newly created volume, and click Actions > Attach Volume.

Step 5:

On the AWS Console homepage, look for the search bar at the top. Type CloudWatch in the search bar and press Enter. From the search results, click on CloudWatch



Step 6: In the CloudWatch dashboard, look at the left-hand menu. Click on Metrics. Under Browse, click on EC2

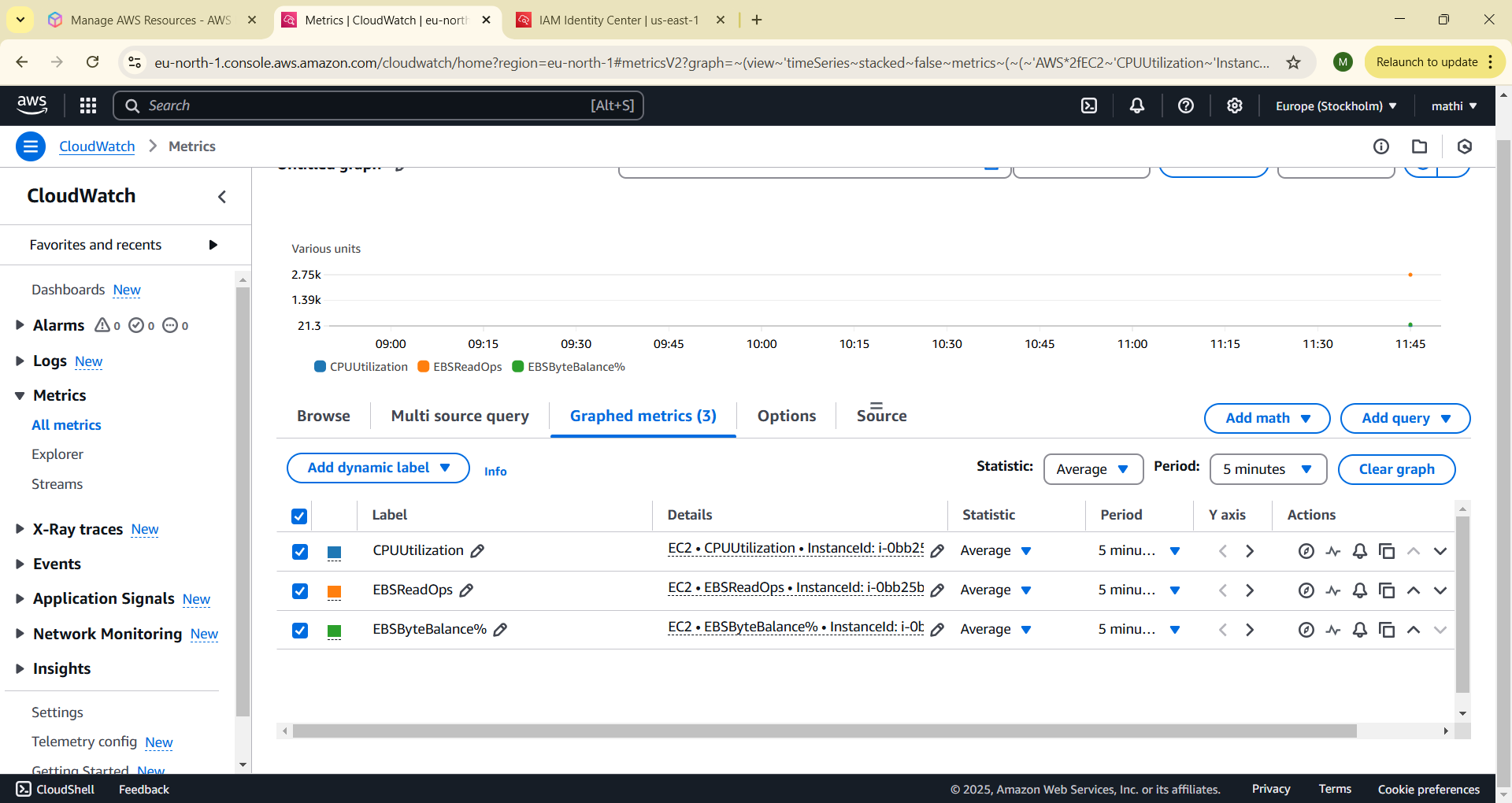
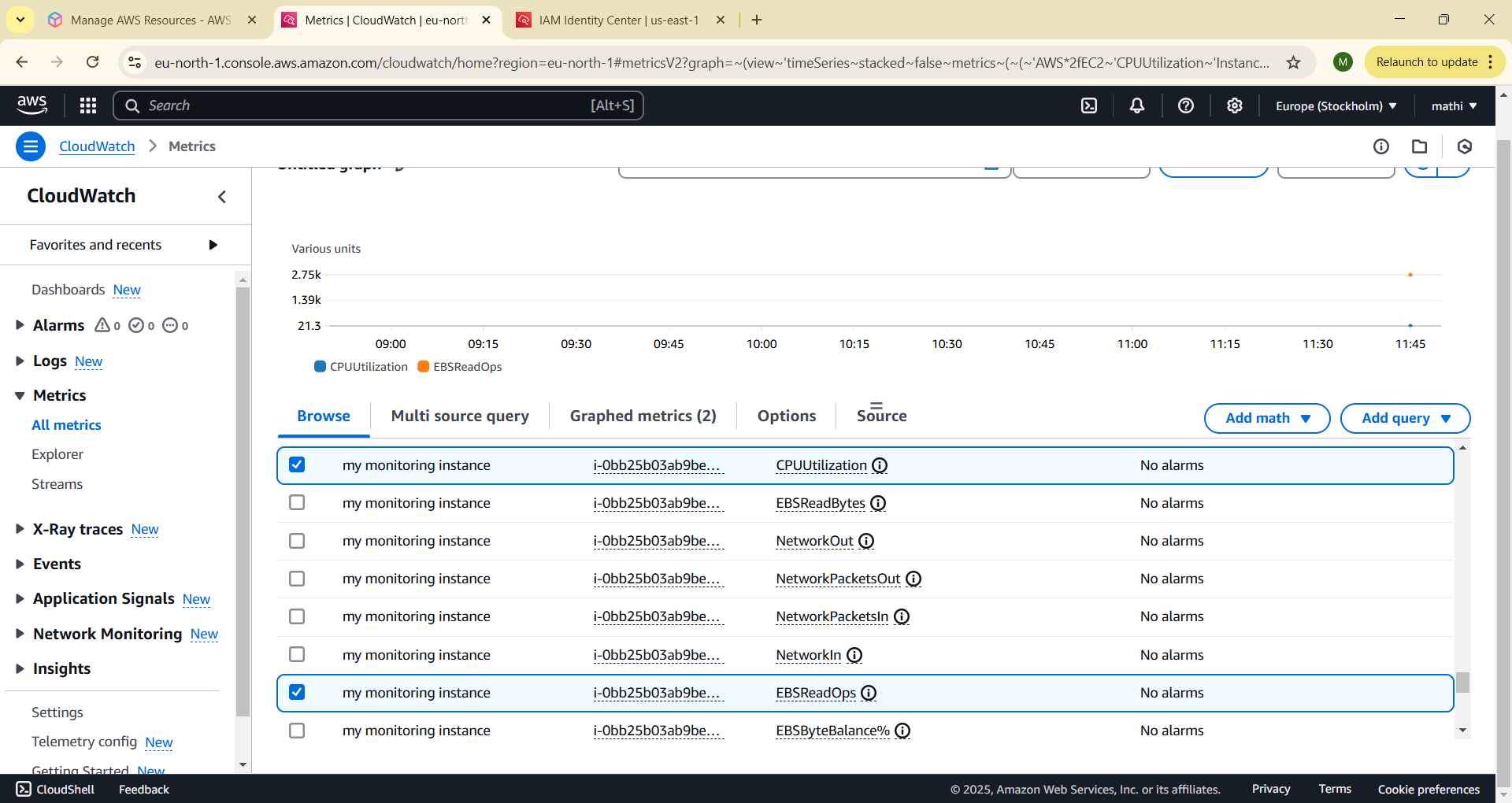


Then click on the Per-Instance Metrics.

Step 7:

You should now see a list of metrics for all your EC2 instances, such as: CPUUtilization (CPU usage) DiskReadOps / DiskWriteOps (Disk I/O) Identify the specific EC2 instance you want to monitor (it will be listed by its instance ID).

Click on the metrics associated with your instance To view detail click Graphed metrics



**Expected Outcome**

 **Secure Access** – No need to store long-term credentials.

 **Granular Control** – Only necessary permissions are granted to the VM.

 **Automated Credential Management** – AWS provides temporary credentials dynamically.

 **Successful Verification** – Running AWS CLI commands confirms the role’s functionality.