Module 3: IAM Users Assignment

Problem Statement:

You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

Tasks To Be Performed:

1. Create 4 IAM users named "Dev1", "Dev2", "Test1", and "Test2".
2. Create 2 groups named "Dev Team" and "Ops Team".
3. Add Dev1 and Dev2 to the Dev Team.
4. Add Dev1, Test1 and Test2 to the Ops Team.

Created 4 IAM User Dev1,Dev2,Test1 & Test2

Created Two Groups Dev-Teams & Ops-Teams
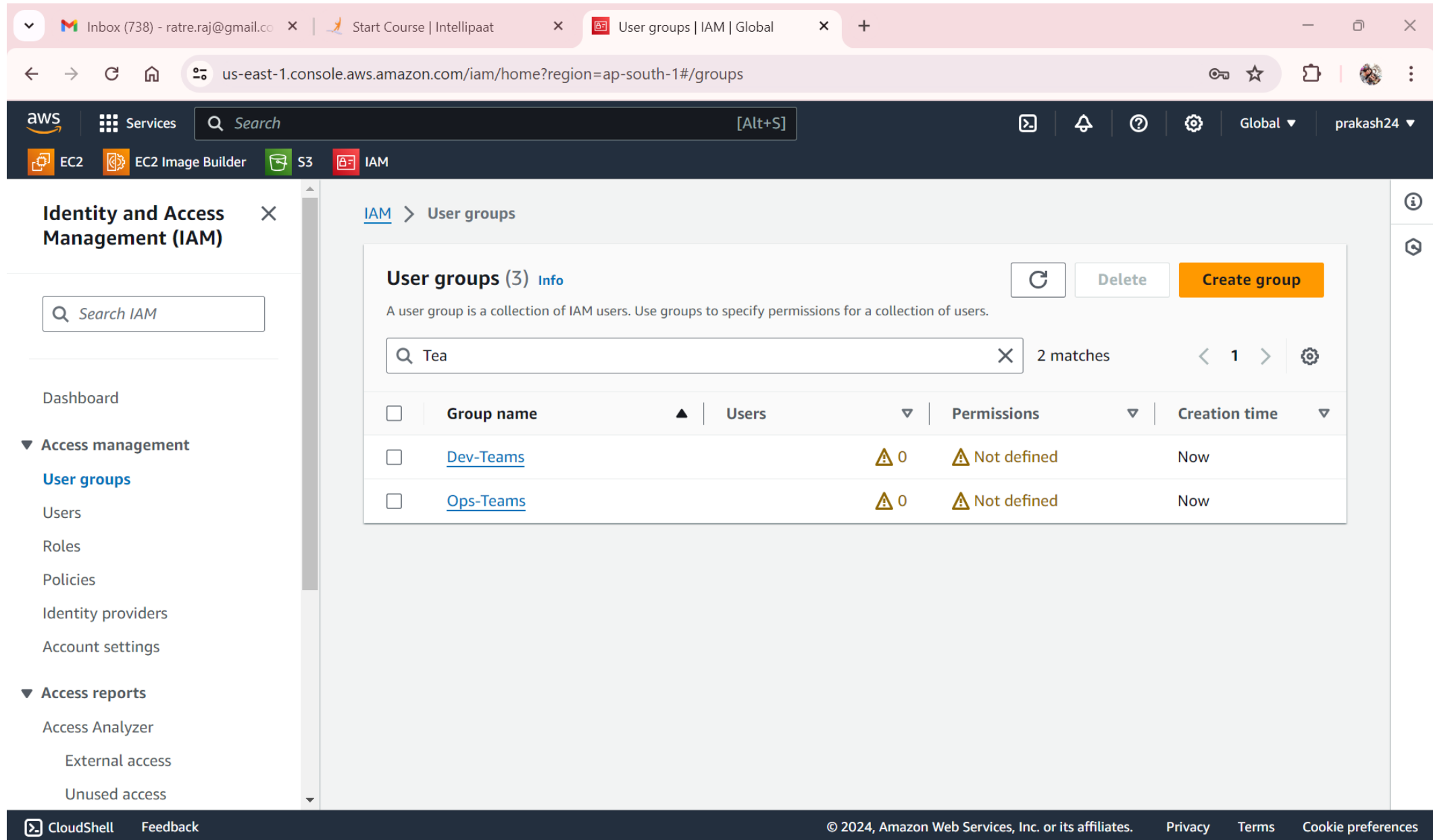
Added User Dev1 & Dev2 in Dev-Teams Group

Added Test1 & Test2 user to Group Ops-Teams

Module 3: IAM Policies Assignment

Problem Statement:

You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

Tasks To Be Performed:

1. Create policy number 1 which lets the users to:
   a. Access S3 completely
   b. Only create EC2 instances
   c. Full access to RDS

2. Create a policy number 2 which allows the users to:
   a. Access CloudWatch and billing completely
   b. Can only list EC2 and S3 resources

3. Attach policy number 1 to the Dev Team from task 1
4. Attach policy number 2 to Ops Team from task 1

Policy Number 1

Step 2

Review and create

Policy details

Policy name
Enter a meaningful name to identify this policy.

```
number1
```

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

Description - *optional*
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

Permissions defined in this policy Info   Edit

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (3 of 420 services)   ⬤ Show remaining 417 services

Service ▲	Access level ▽	Resource	Request condition
EC2	Limited: List, Write	All resources	None
RDS	Full access	All resources	None
S3	Full access	All resources	None

Policy Number 2

number2 Info

Edit | Delete

Policy details

Type	Creation time	Edited time	ARN
Customer managed	July 23, 2024, 08:42 (UTC+05:30)	July 23, 2024, 08:42 (UTC+05:30)	arn:aws:iam::654654393526:policy/number2

Permissions | Entities attached | Tags | Policy versions (1) | Access Advisor

Permissions defined in this policy Info

Edit | **Summary** | JSON

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

Allow (4 of 420 services)

Show remaining 416 services

Service ▲	Access level ▽	Resource	Request condition
Billing	Full access	All resources	None
CloudWatch	Full access	All resources	None
EC2	Limited: List	All resources	None
S3	Full: List	All resources	None

Attaching Policy Number 1 to Dev-Teams

Attaching Policy Number 2 to Ops-Teams
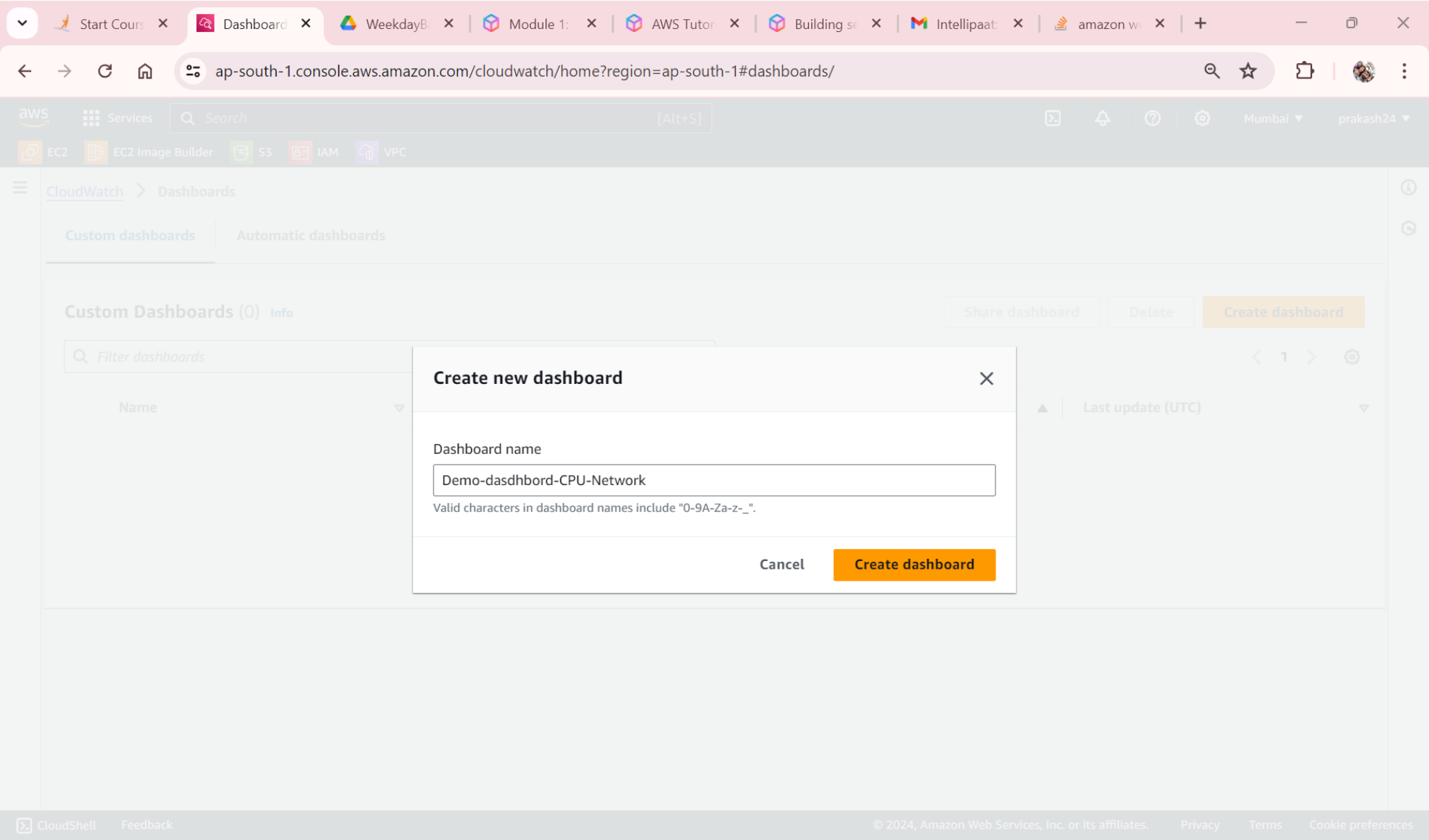
Module 3: IAM Roles Assignment

Problem Statement:

You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

Tasks To Be Performed:

1. Create a role which only lets user1 and user2 from task 1 to have complete access to VPCs and DynamoDB.
2. Login into user1 and shift to the role to test out the feature.

Created a IAM Role having VPC Full access & DynamoDB Full Access

Adding Test1 & Test2 User to trust policy so use can access as role

Login as Test1 user

Switched as Assigned Role

User Can access the VPC Dashboard

User Can access the DynamoDB

Module 3: CloudWatch Dashboard Assignment

Problem Statement:

You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users. Also, you will be monitoring the machines created by these users for any errors or misconfigurations.

Tasks To Be Performed:

1. Create a dashboard which lets you check the CPU utilization and networking for a particular EC2 instance.

Cloudwatch dashboard creation Step 1

Adding metric to dashboard

Demo Instance for cloudwatch dashboard

CPU & Network utilization of demo-ec2
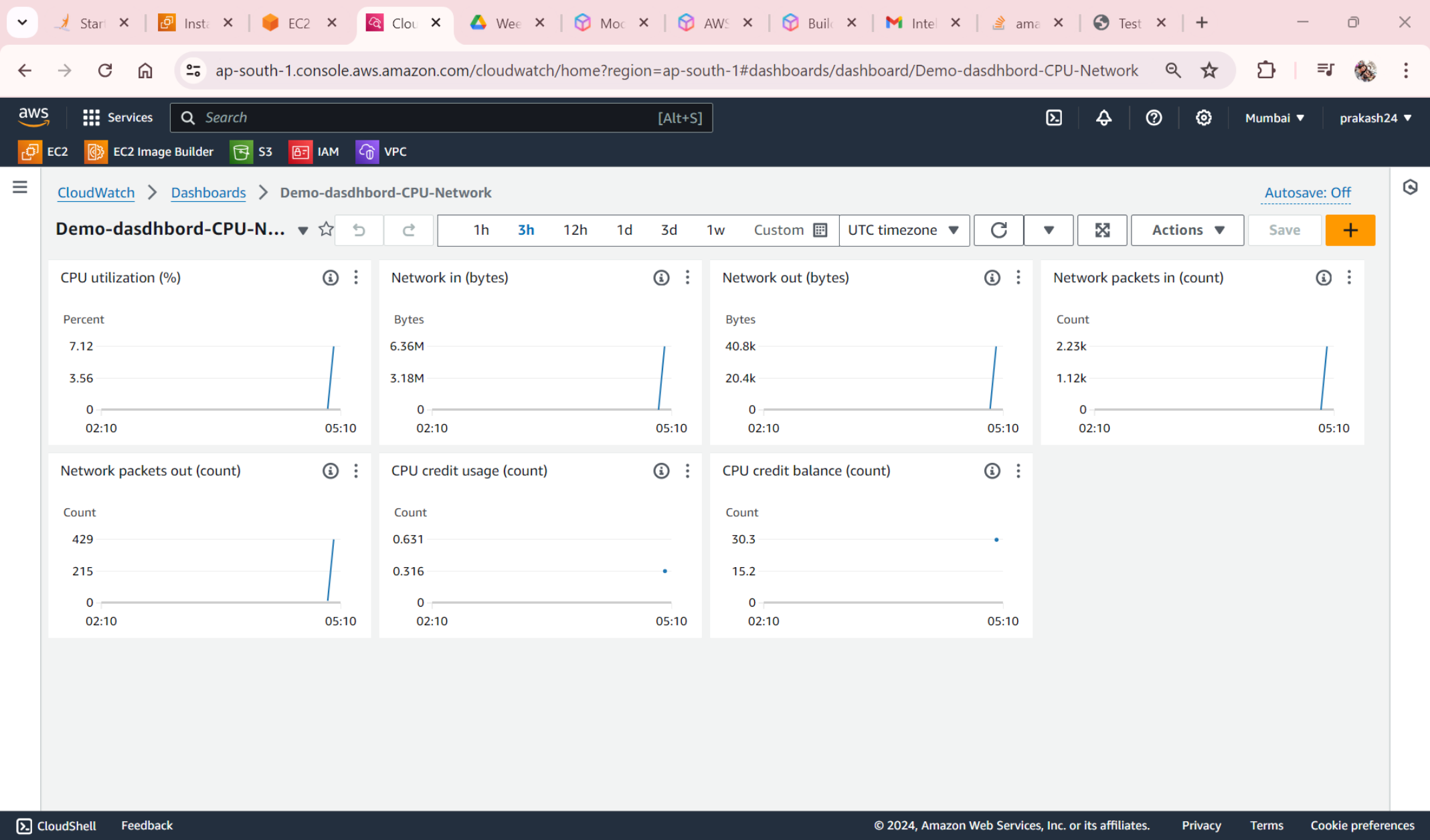
Module 3: CloudWatch Alarms Assignment

Problem Statement:

You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users. Also, you will be monitoring the machines created by these users for any errors or misconfigurations.

Tasks To Be Performed:

1. Create a CloudWatch billing alarm which goes off when the estimated charges go above $500.
2. Create a CloudWatch alarm which goes off to an Alarm state when the CPU utilization of an EC2 instance goes above 65%. Also add an SNS topic so that it notifies the person when the threshold is crossed.

Alarm Creation Step 1

Metric Selection for alarm creation

Step 1 of alarm creation

EstimatedCharges

Maximum

Period

6 hours

Conditions

Threshold type

- ● Static
  Use a value as a threshold

- ○ Anomaly detection
  Use a band as a threshold

Whenever EstimatedCharges is...
Define the alarm condition.

- ● Greater
  \> threshold

- ○ Greater/Equal
  \>= threshold

- ○ Lower/Equal
  <= threshold

- ○ Lower
  < threshold

than...
Define the threshold value.

500   USD

Must be a number

▶ Additional configuration

Cancel   Next

Step 2 of alarm creation

A CloudWatch billing alarm which goes off when the estimated charges go above $500

A CloudWatch alarm which goes off to an Alarm state when the CPU utilization of an EC2 instance goes above 65%. Also add an SNS