JASVEENA-224001588

TASK 6.2P

CLOUD COMPUTING

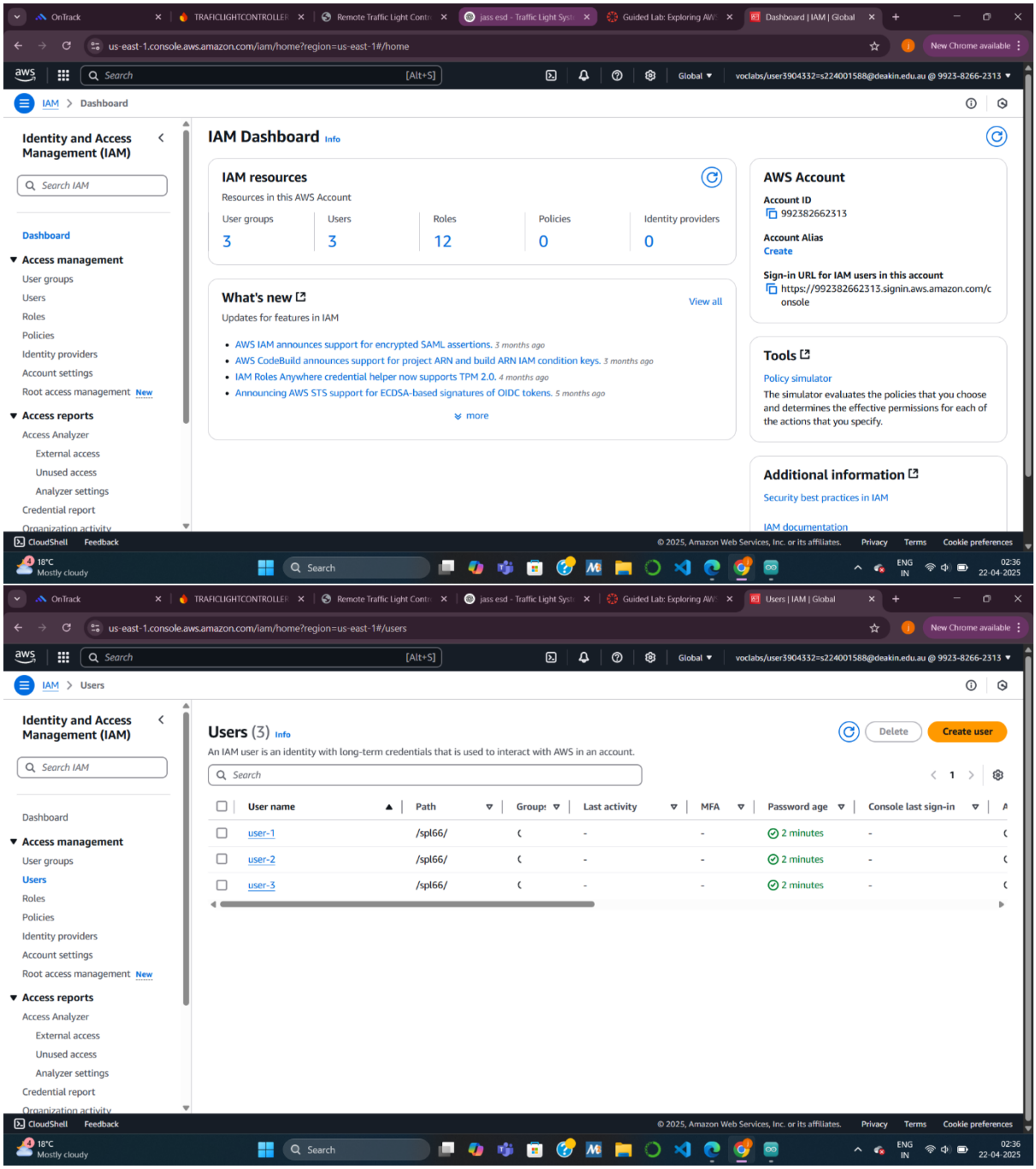
Controlling Account Access Using IAM

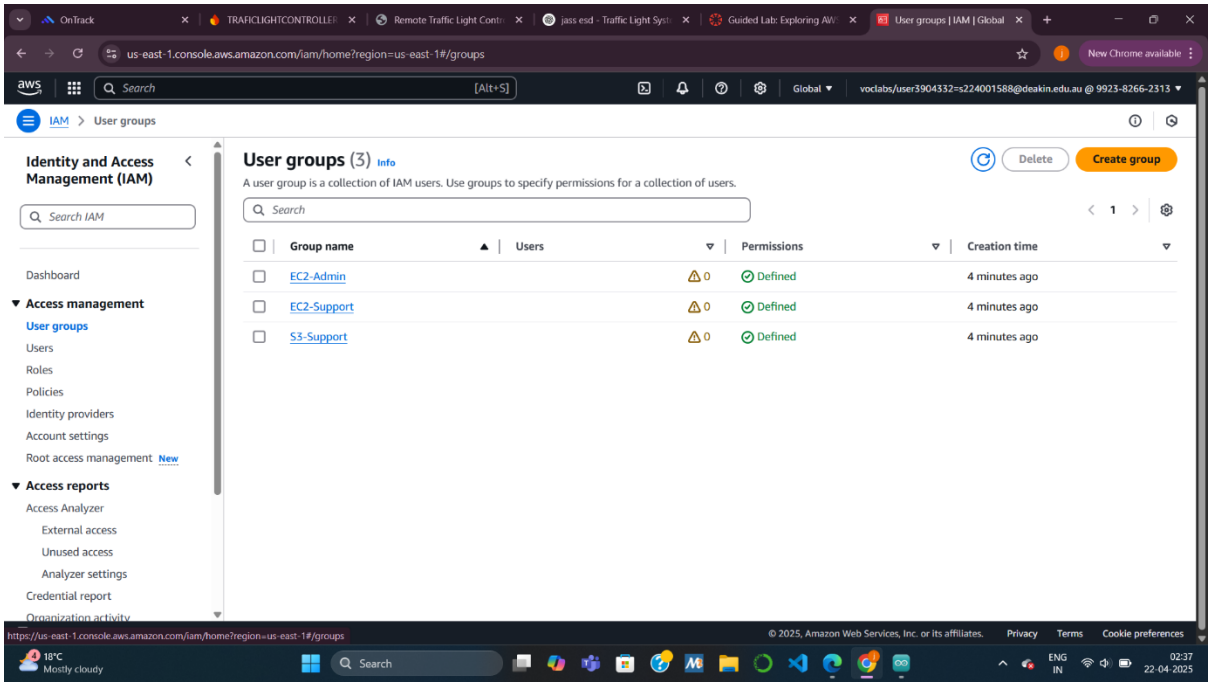
Task 1: Explore the users and groups, and inspect policies

Steps:

- **Checked the AWS Region:**
  This ensures you're operating in the correct environment because AWS resources are region-specific.
- **Explored IAM Users (user-1, user-2, user-3):**
  You inspected each user's permissions, checked if they were part of any groups, and reviewed their security credentials (such as having a console password for login).
- **Explored IAM Groups (EC2-Admin, EC2-Support, S3-Support):**
  - **Each group can have permissions via managed policies or inline policies.**
  - **Managed policies are pre-built by AWS and can be attached to many users/groups.**
  - **Inline policies are directly attached to a single group or user.**
- **Inspected Policies Attached to Groups:**
  - **EC2-Support Group: Has the AmazonEC2ReadOnlyAccess policy, allowing only viewing of EC2-related resources.**
  - **S3-Support Group: Has the AmazonS3ReadOnlyAccess policy, allowing only viewing/listing of S3 bucket contents.**
  - **EC2-Admin Group: Uses an inline policy called EC2-Admin-Policy, which allows viewing EC2 instances and the ability to start/stop them.**

JASVEENA-224001588





Task 2: Add users to groups

Task 2.1: Add user-1 to the S3-Support group

- **Why?**
  user-1 is hired as S3 support, so they need permissions to view S3 buckets and objects.
- **Action:**
  Added user-1 to the S3-Support group, which has the read-only S3 access policy.

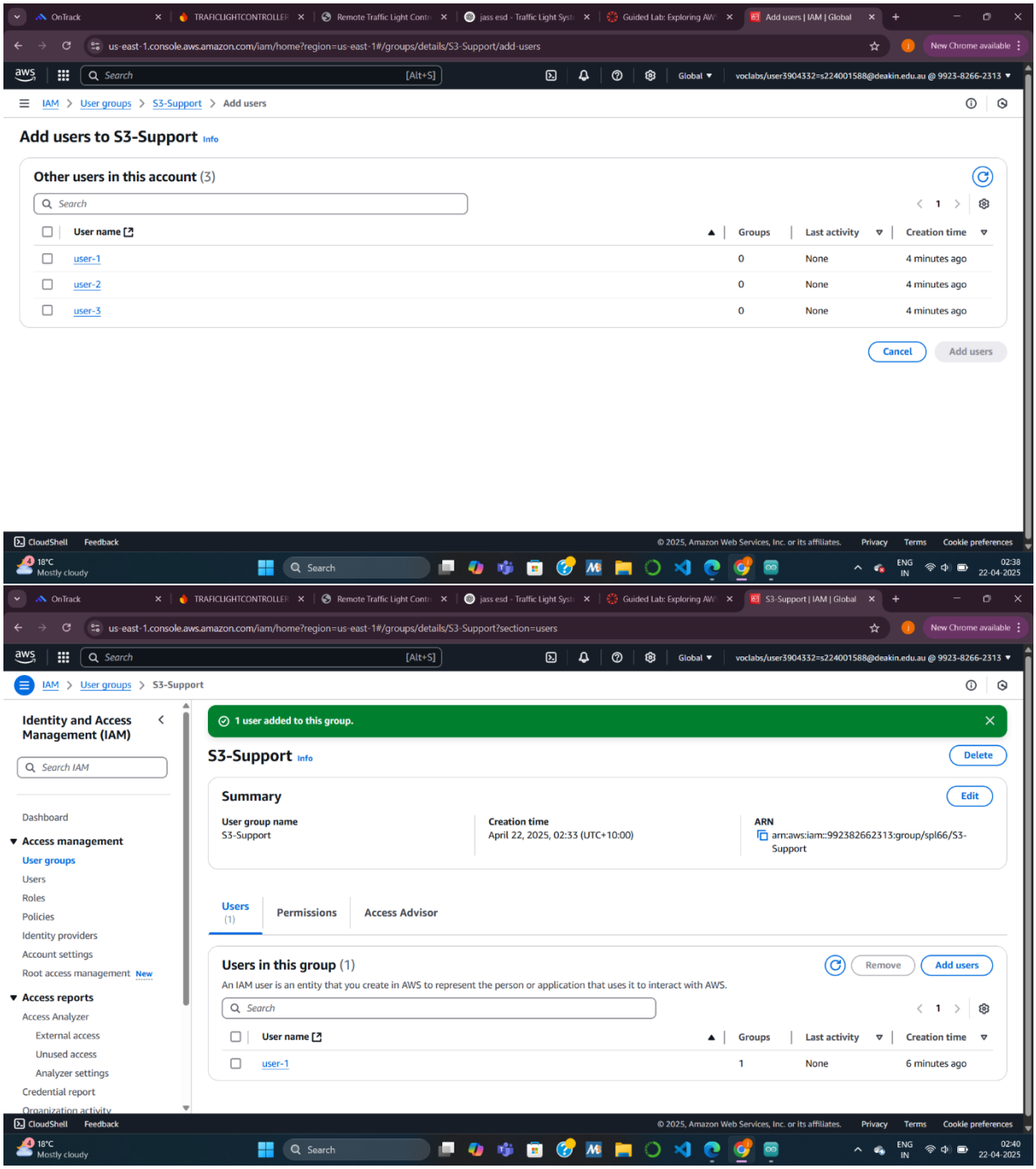
Task 2.2: Add user-2 to the EC2-Support group

- **Why?**
  user-2 is assigned to support EC2 services, so they need read-only access to EC2 resources.
- **Action:**
  Added user-2 to the EC2-Support group, which provides permission to view EC2 instances but not modify them.

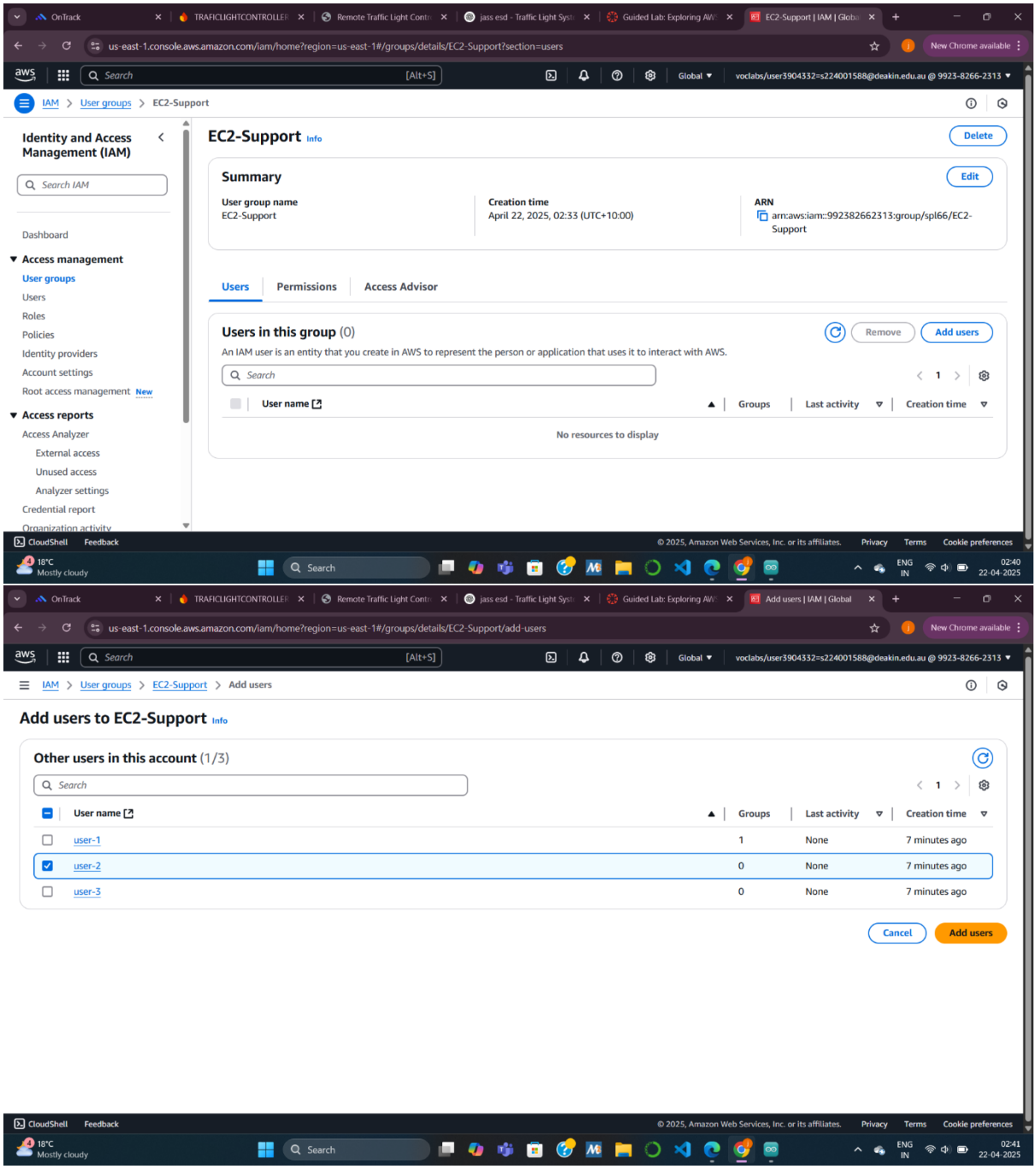
Task 2.3: Add user-3 to the EC2-Admin group

- **Why?**
  user-3 is the EC2 administrator, so they require the ability to view, start, and stop EC2 instances.
- **Action:**
  Added user-3 to the EC2-Admin group, which has an inline policy granting these permissions.

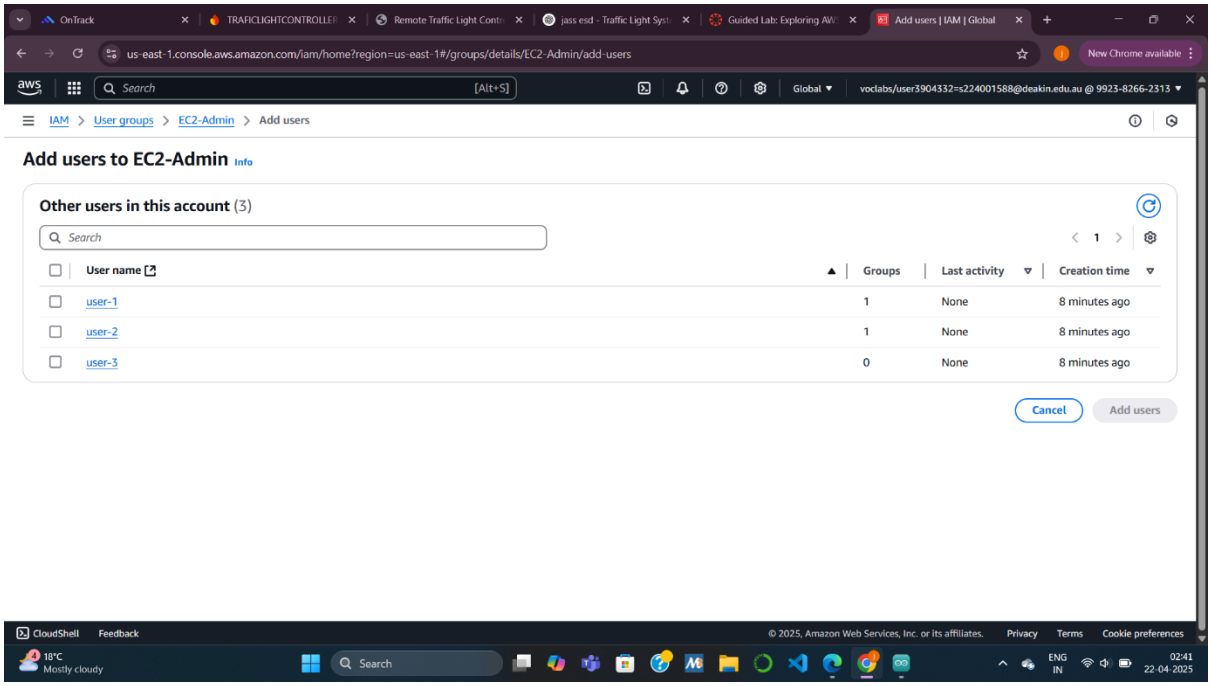
JASVEENA-224001588

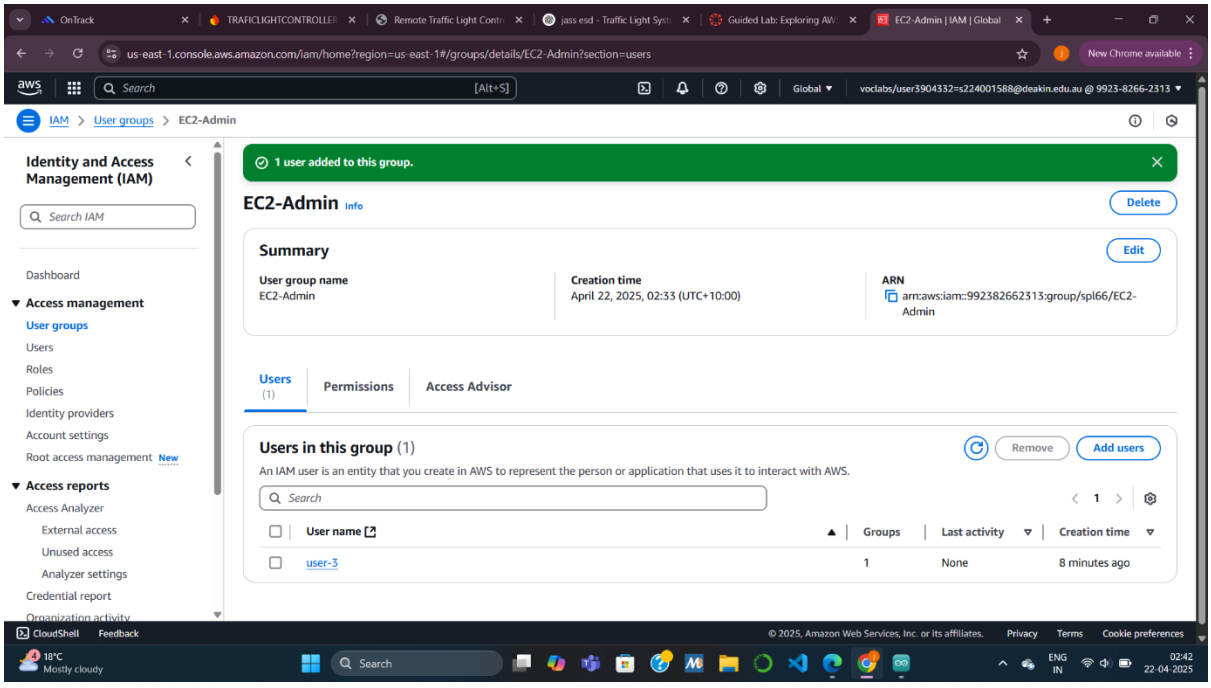


JASVEENA-224001588



JASVEENA-224001588





Task 3: Sign in and test user permissions

Task 3.1: Get the Console Sign-In URL

- **Why?**
  IAM users have a specific sign-in URL to access the AWS console.
- **Action:**
  Located and copied the IAM sign-in link, which allows you to log in as any of the IAM users created for the lab.

Task 3.2: Test user-1 permissions (S3-Support role)

- **Expected Outcome:**
  - **Can browse S3 buckets and view their contents.**
  - **Cannot access EC2 resources (gets an unauthorized error).**
- **Purpose:**
  Confirms that user-1 has only S3 read-only access through the S3-Support group.

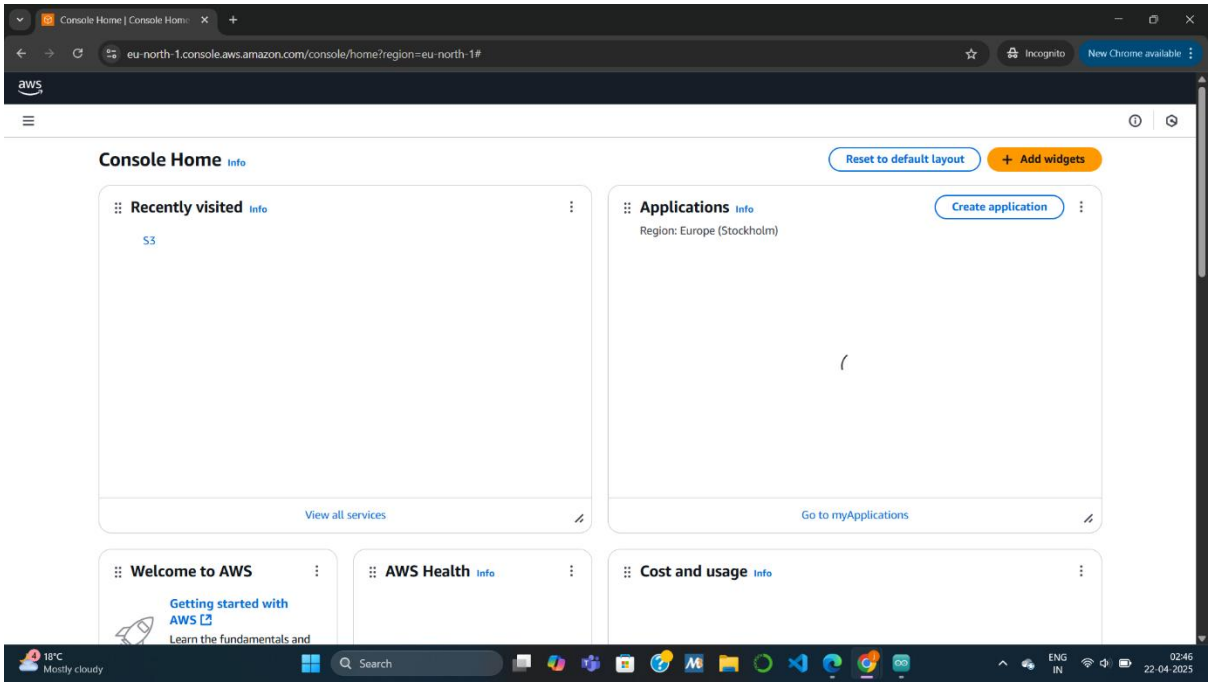
Task 3.3: Test user-2 permissions (EC2-Support role)

- **Expected Outcome:**
  - **Can view EC2 instances but cannot start/stop them.**
  - **Cannot access S3 buckets (gets a permissions error).**
- **Purpose:**
  Verifies that user-2 has read-only access to EC2 only, with no control over S3.

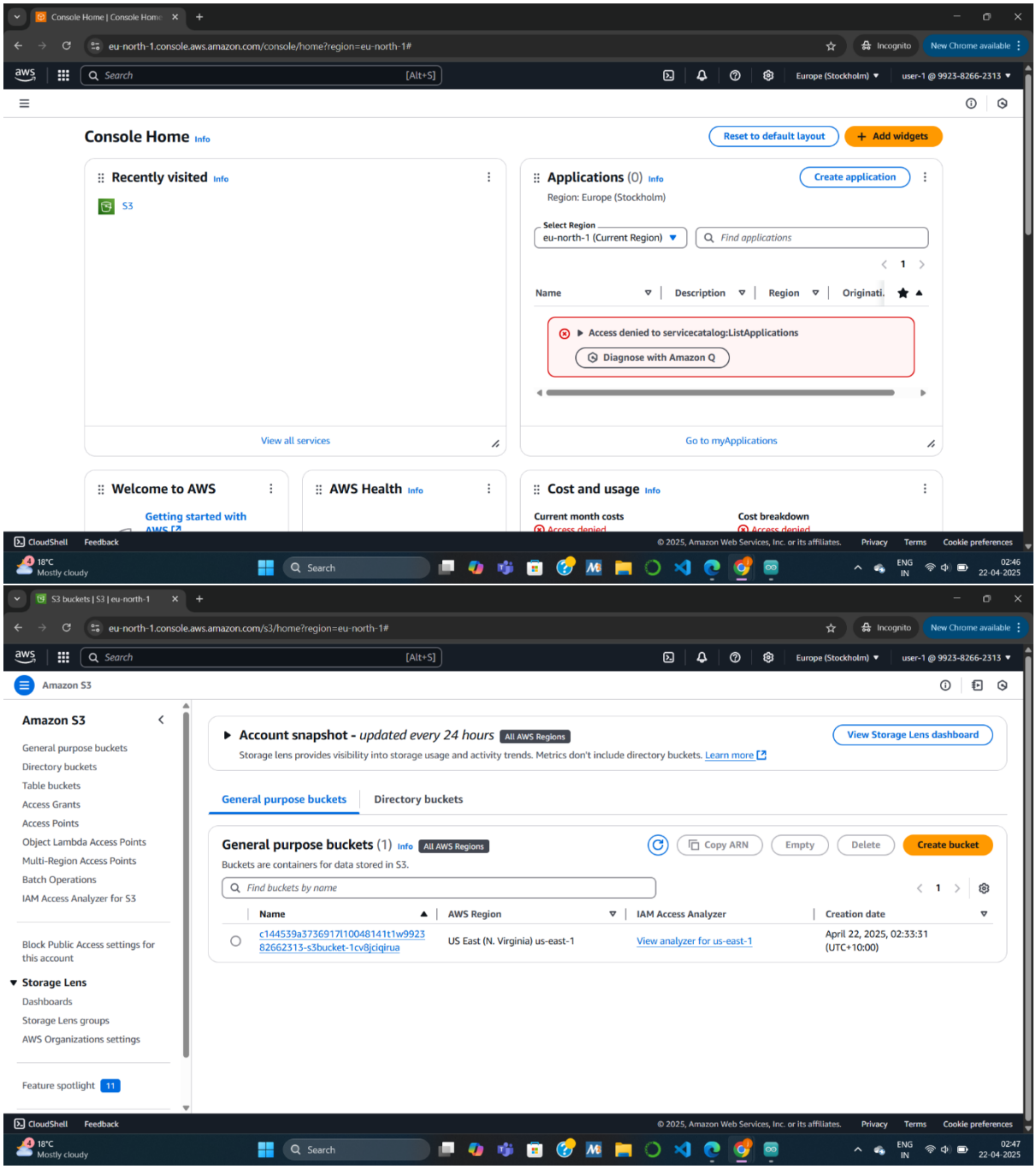
Task 3.4: Test user-3 permissions (EC2-Admin role)

- **Expected Outcome:**
  - **Can view EC2 instances.**
  - **Can start and stop EC2 instances.**
- **Purpose:**
  Confirms that user-3 has the correct administrator privileges for EC2 management.

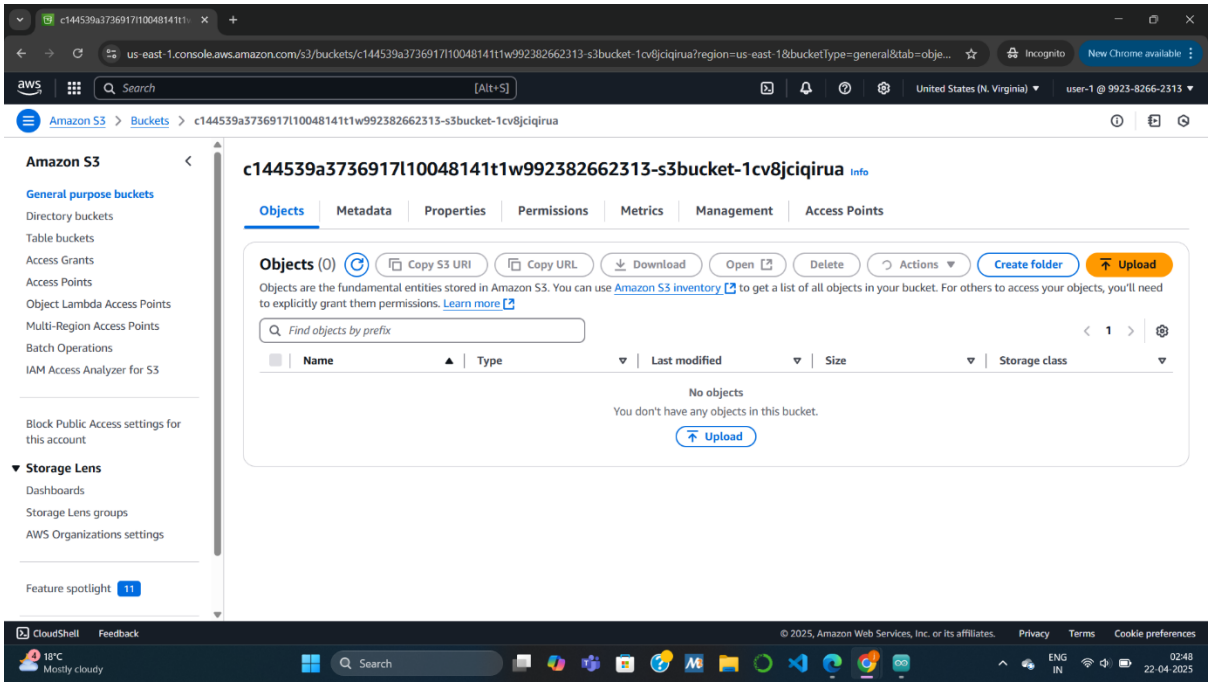
JASVEENA-224001588



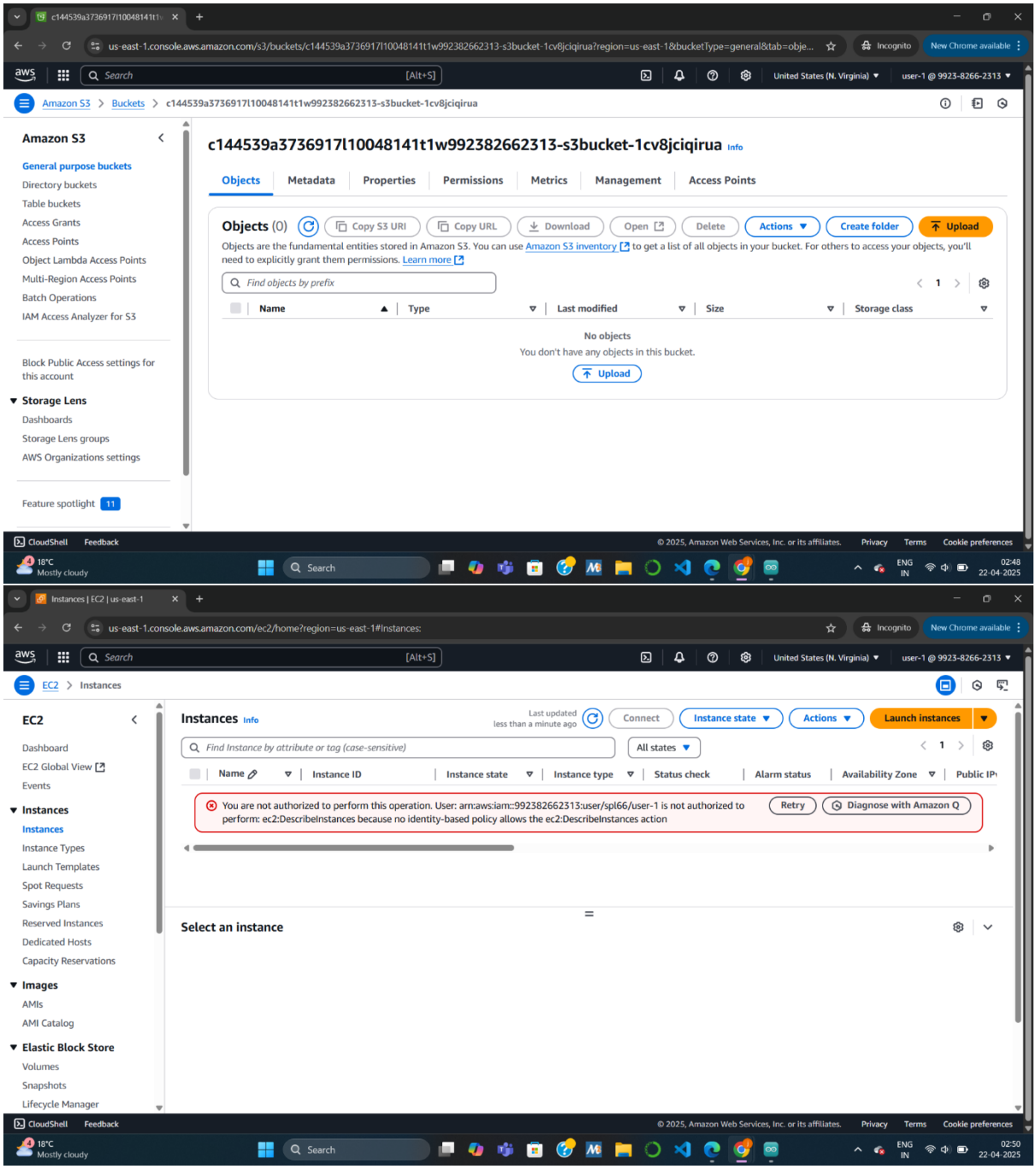
JASVEENA-224001588



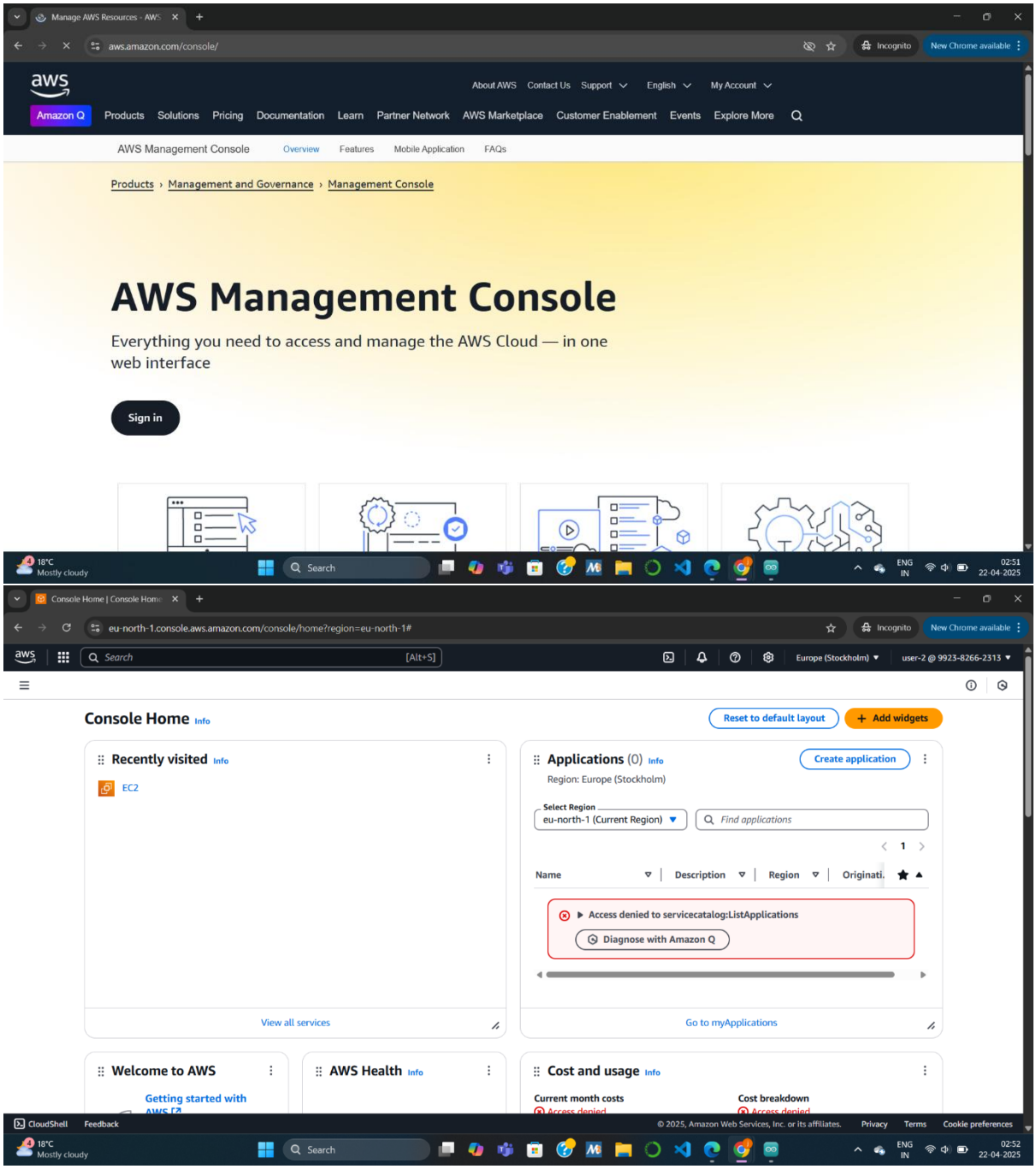
JASVEENA-224001588



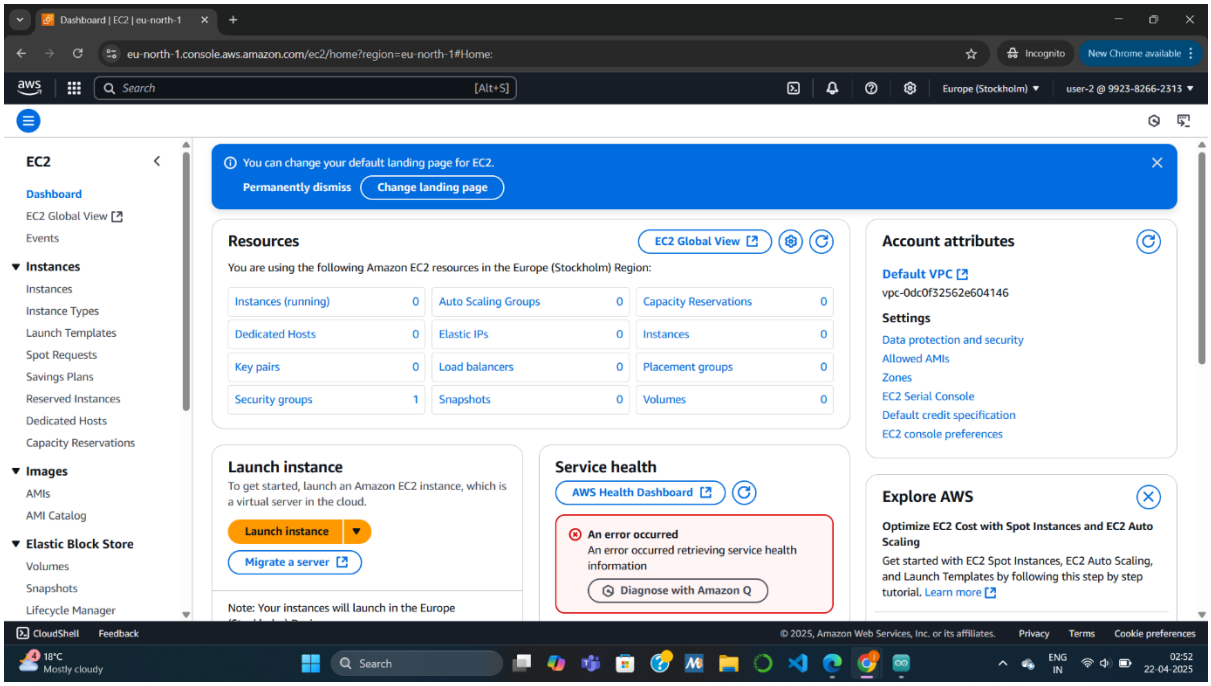
JASVEENA-224001588



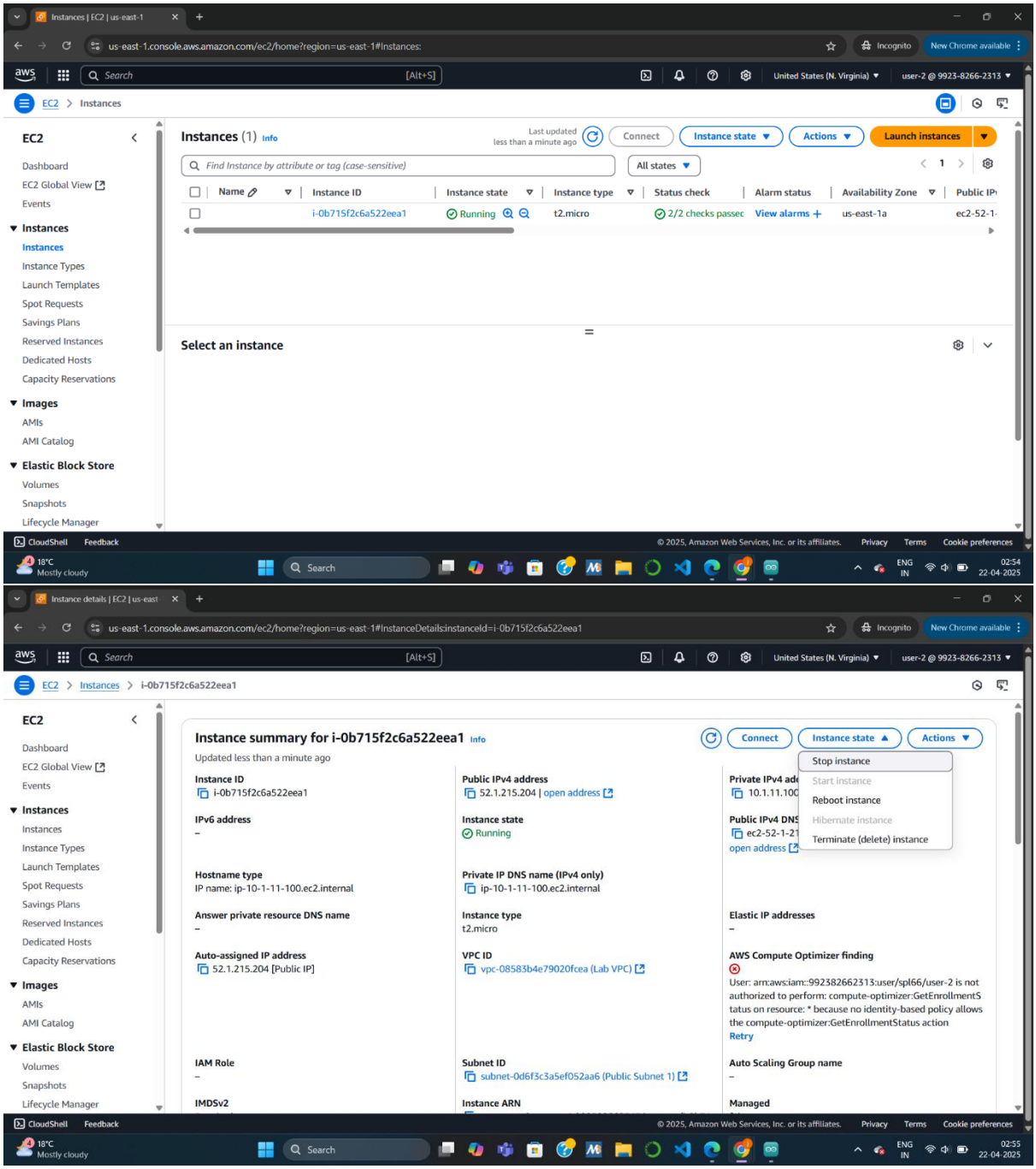
JASVEENA-224001588



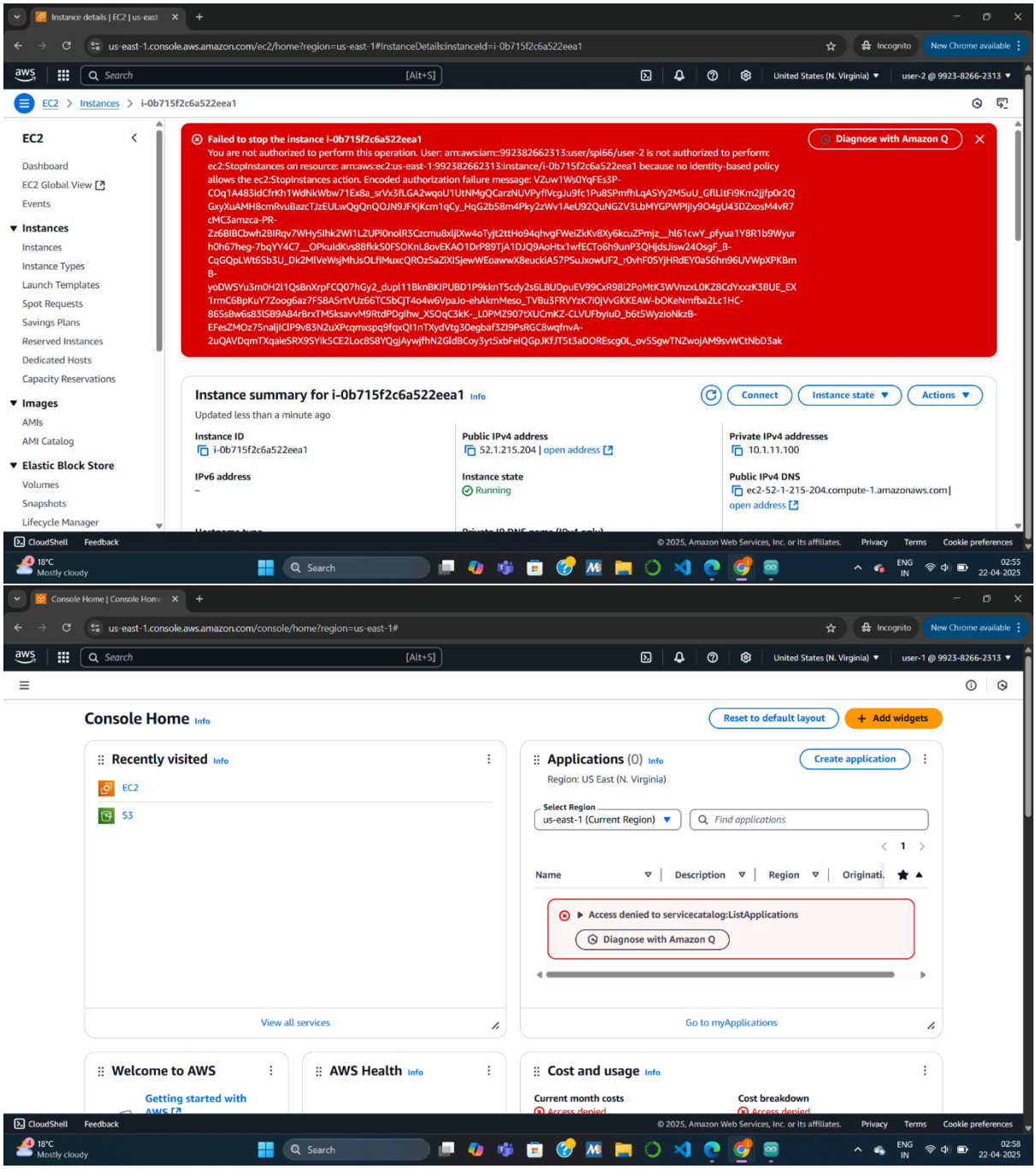
JASVEENA-224001588



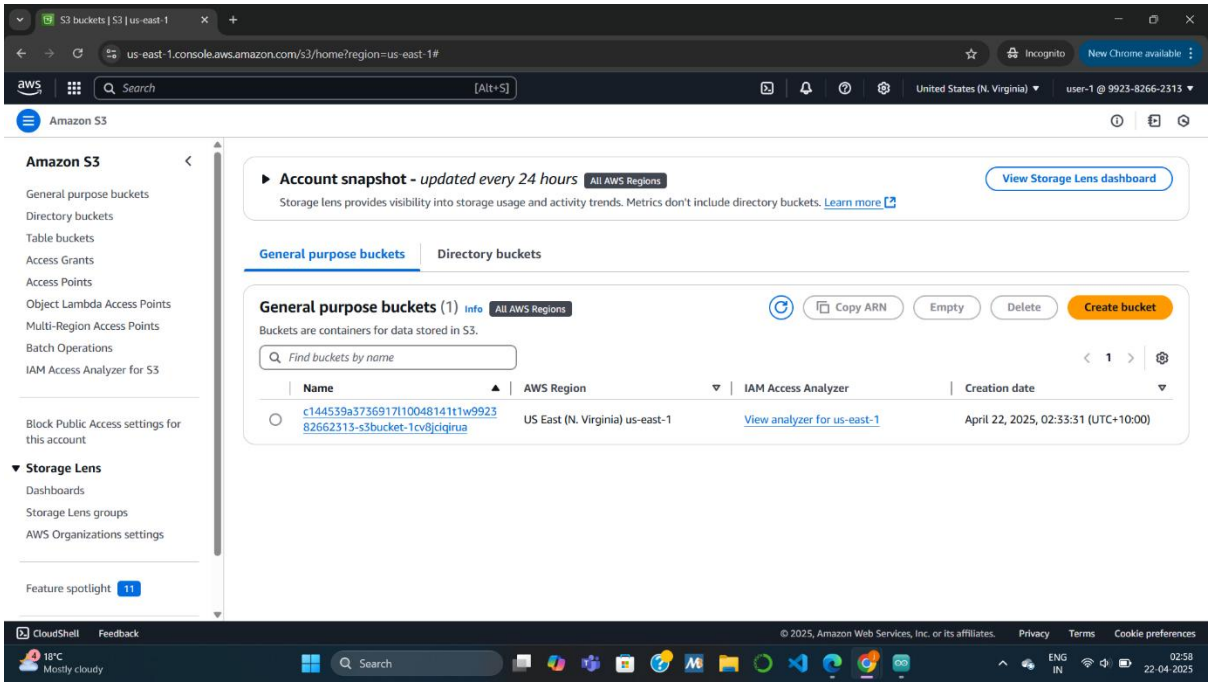
JASVEENA-224001588



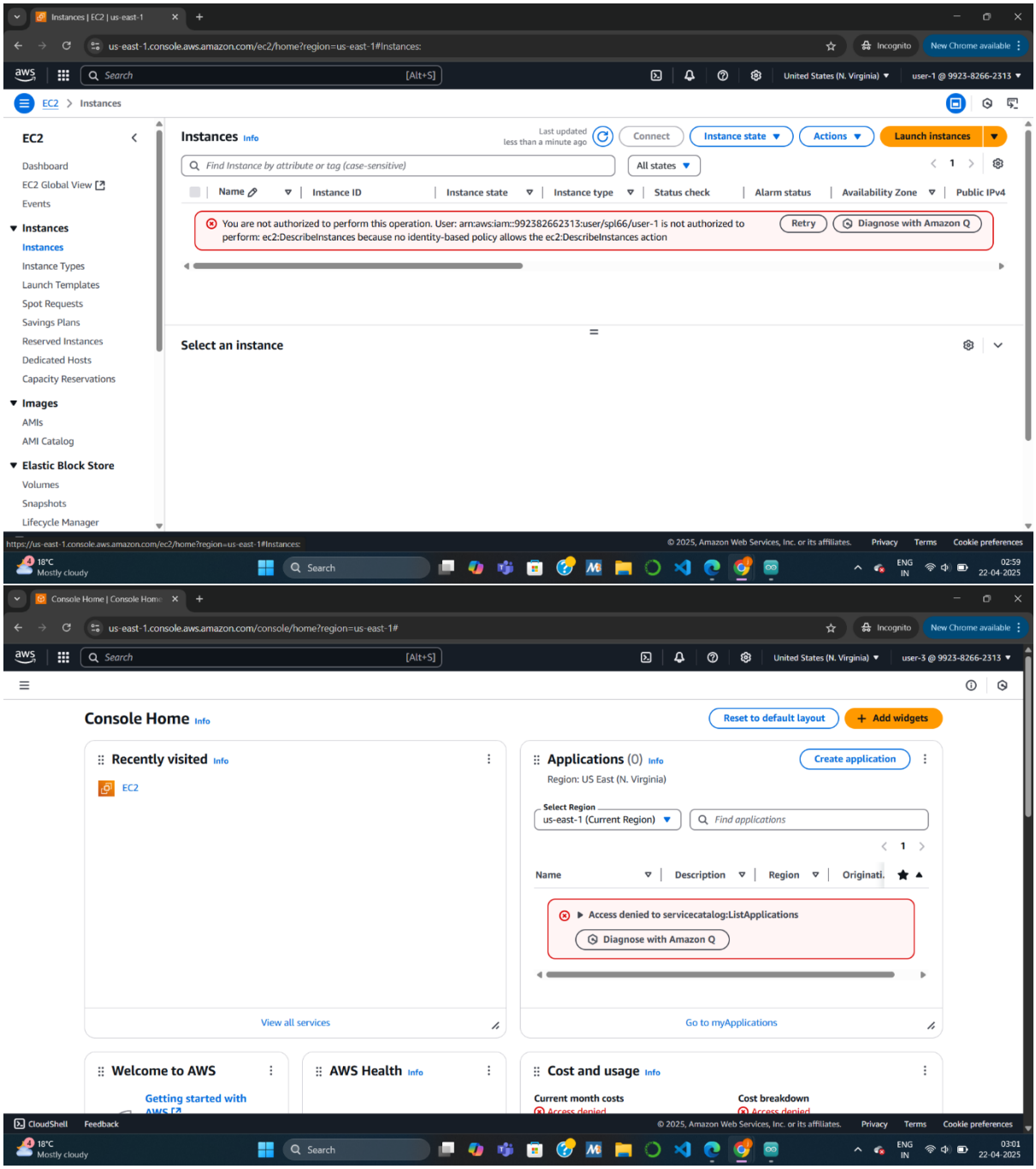
JASVEENA-224001588



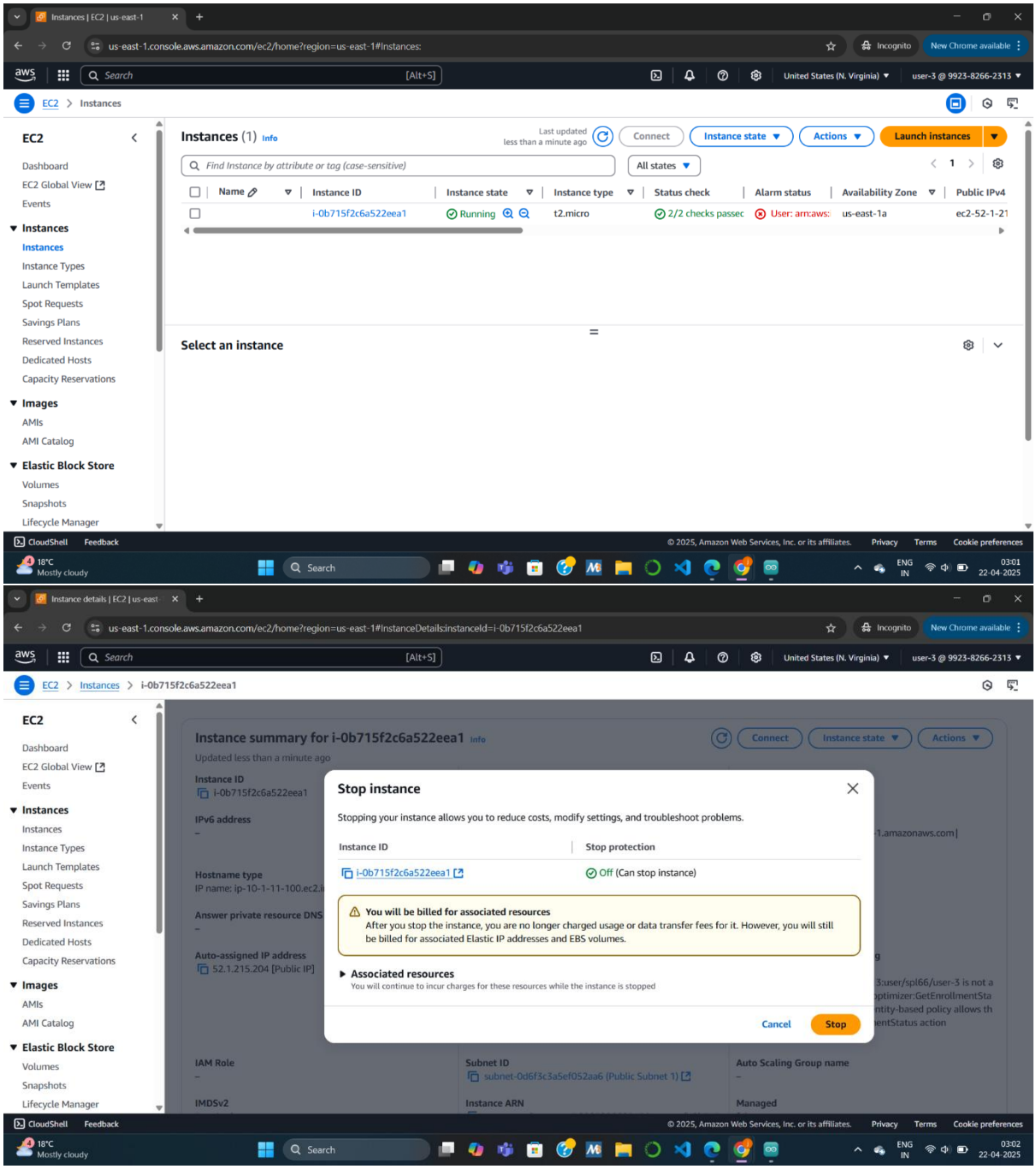
JASVEENA-224001588



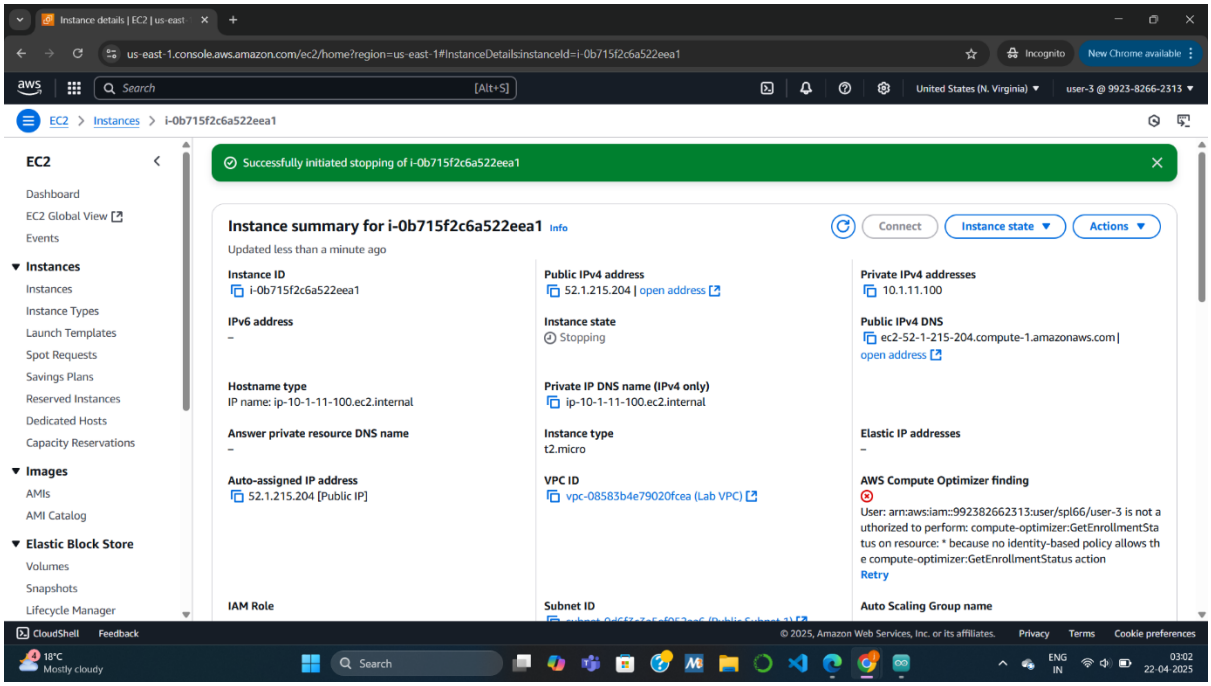
JASVEENA-224001588



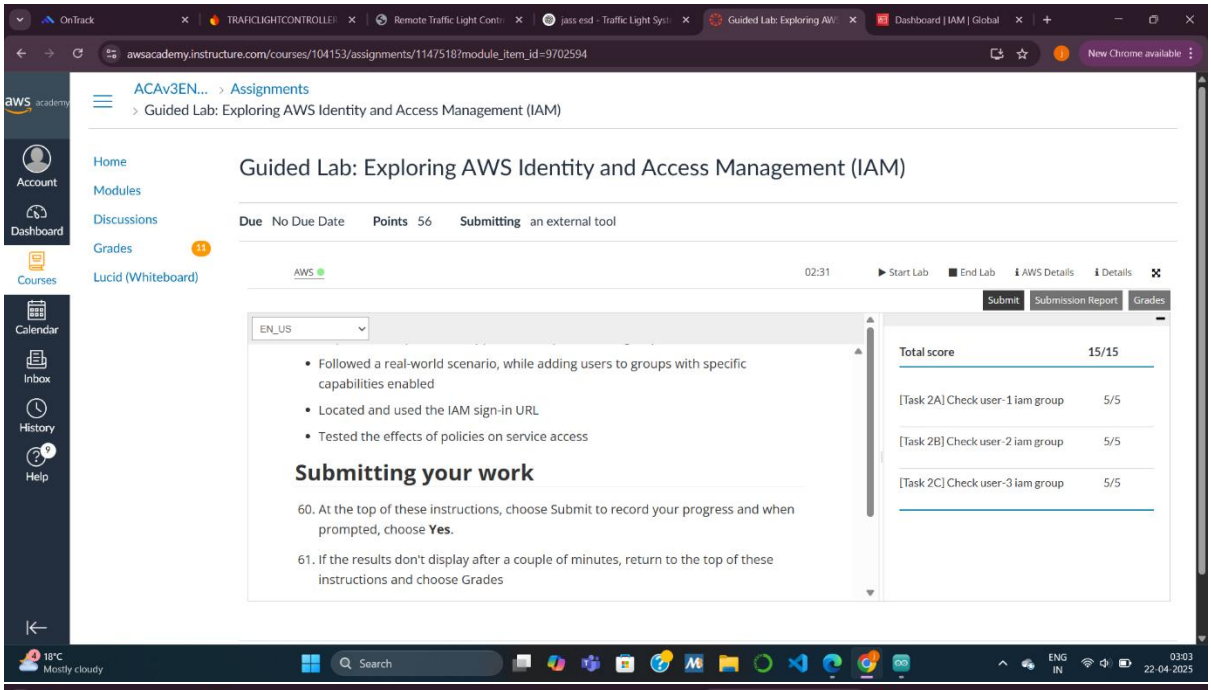
JASVEENA-224001588

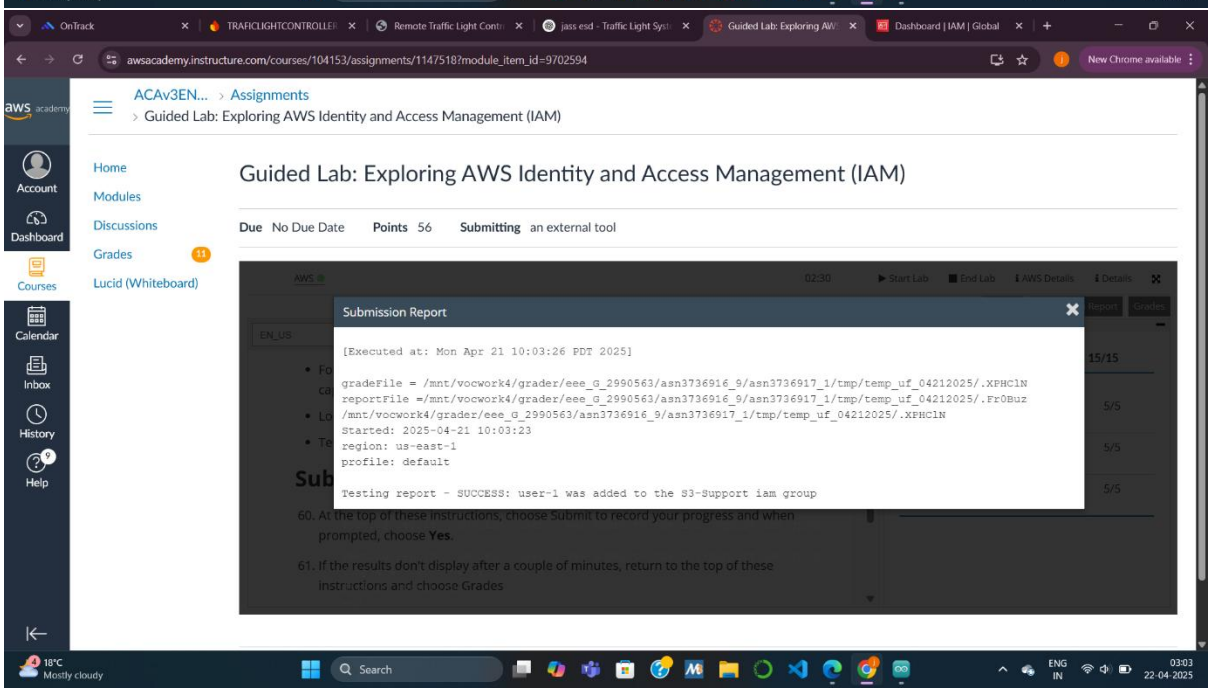


JASVEENA-224001588



JASVEENA-224001588





KNOWLEDGE CHECK :

JASVEENA-224001588