JASVEENA-224001588

TASK 6.2P

CLOUD COMPUTING

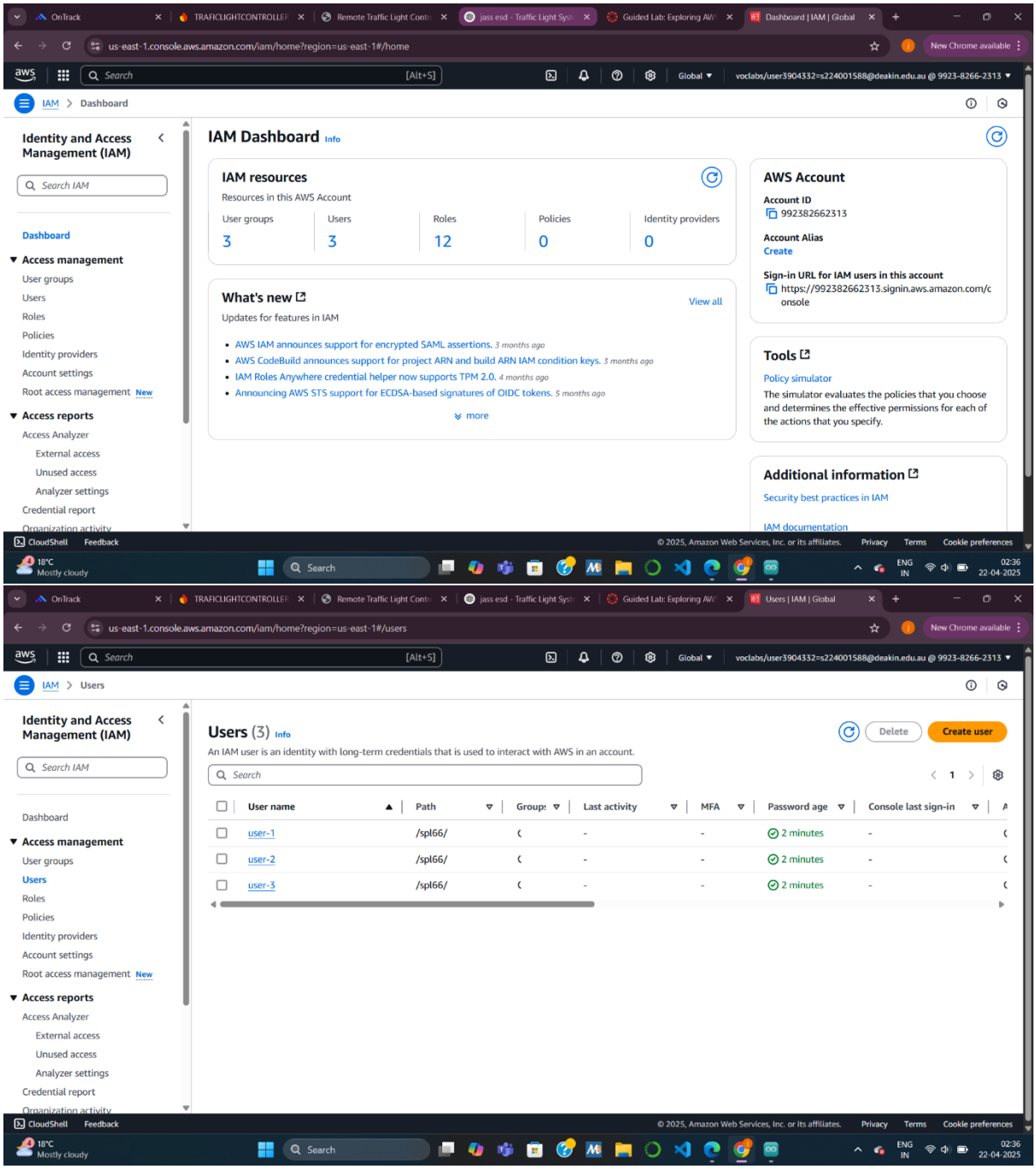
Controlling Account Access Using IAM

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

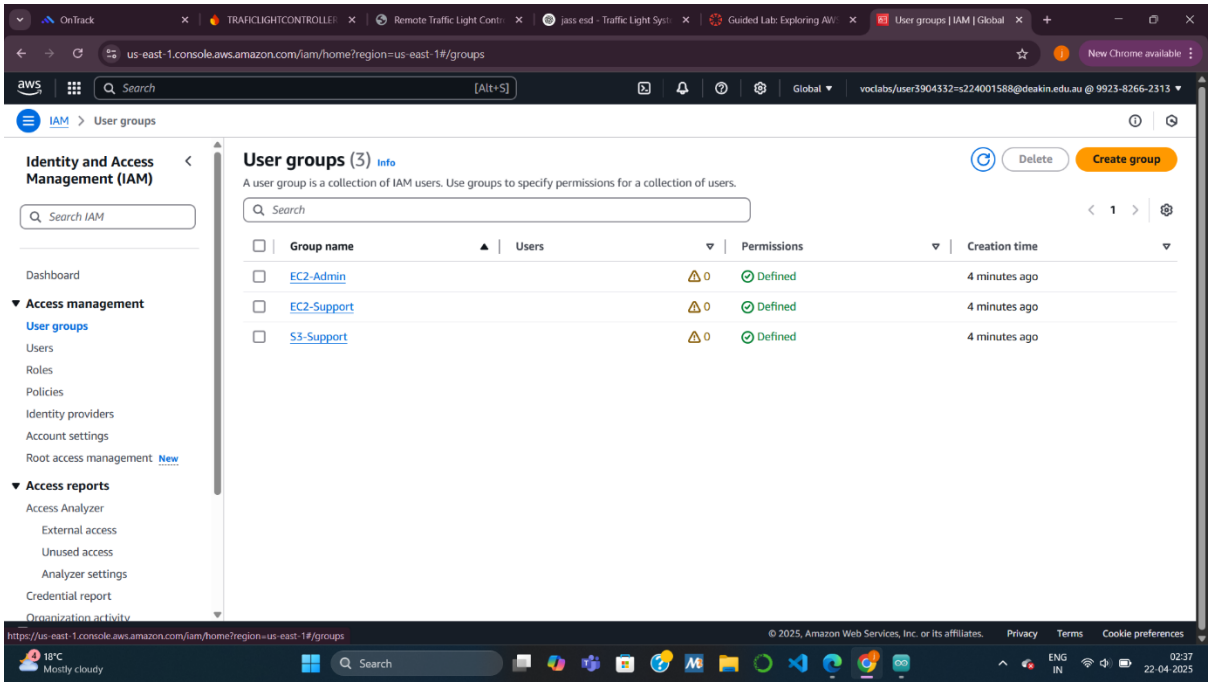
Steps:

- **Identify your current AWS Region.**
- **View the IAM users (user-1, user-2, user-3).**
- **Check the permissions, group memberships, and security credentials of each user.**
- **Inspect the pre-created groups: EC2-Admin, EC2-Support, S3-Support.**
- **Review attached policies:**
    - **AmazonEC2ReadOnlyAccess (read-only EC2 access).**
    - **AmazonS3ReadOnlyAccess (read-only S3 access).**
    - **EC2-Admin-Policy (Describe, Start, Stop EC2 instances).**

JASVEENA-224001588



JASVEENA-224001588



Task 2: Add users to groups

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

- **Add user-1 to S3-Support group.**
- **Grants read-only access to S3 buckets.**

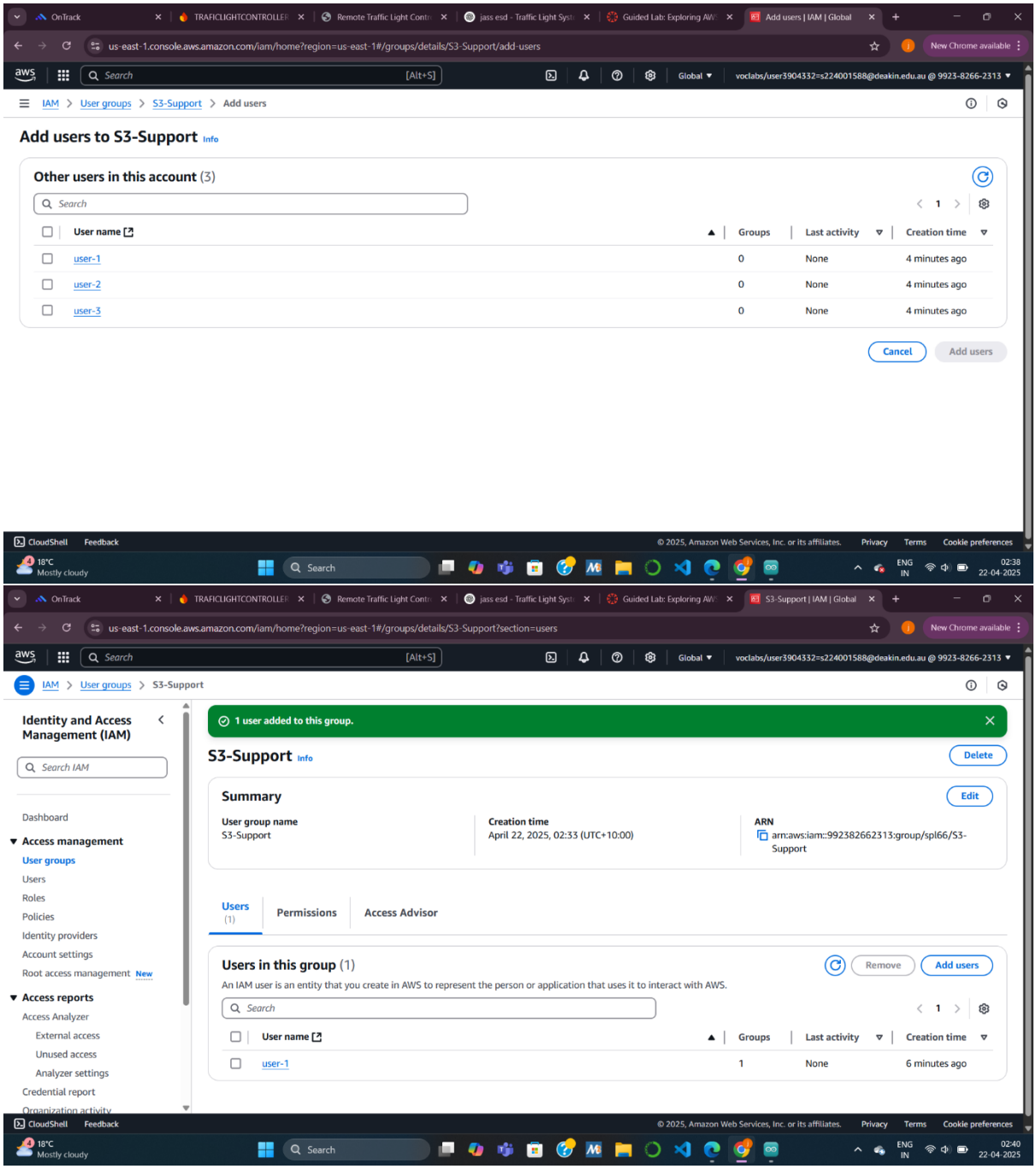
Task 2.2: Add user-2 to the EC2-Support group

- **Add user-2 to EC2-Support group.**
- **Grants read-only access to EC2 resources.**

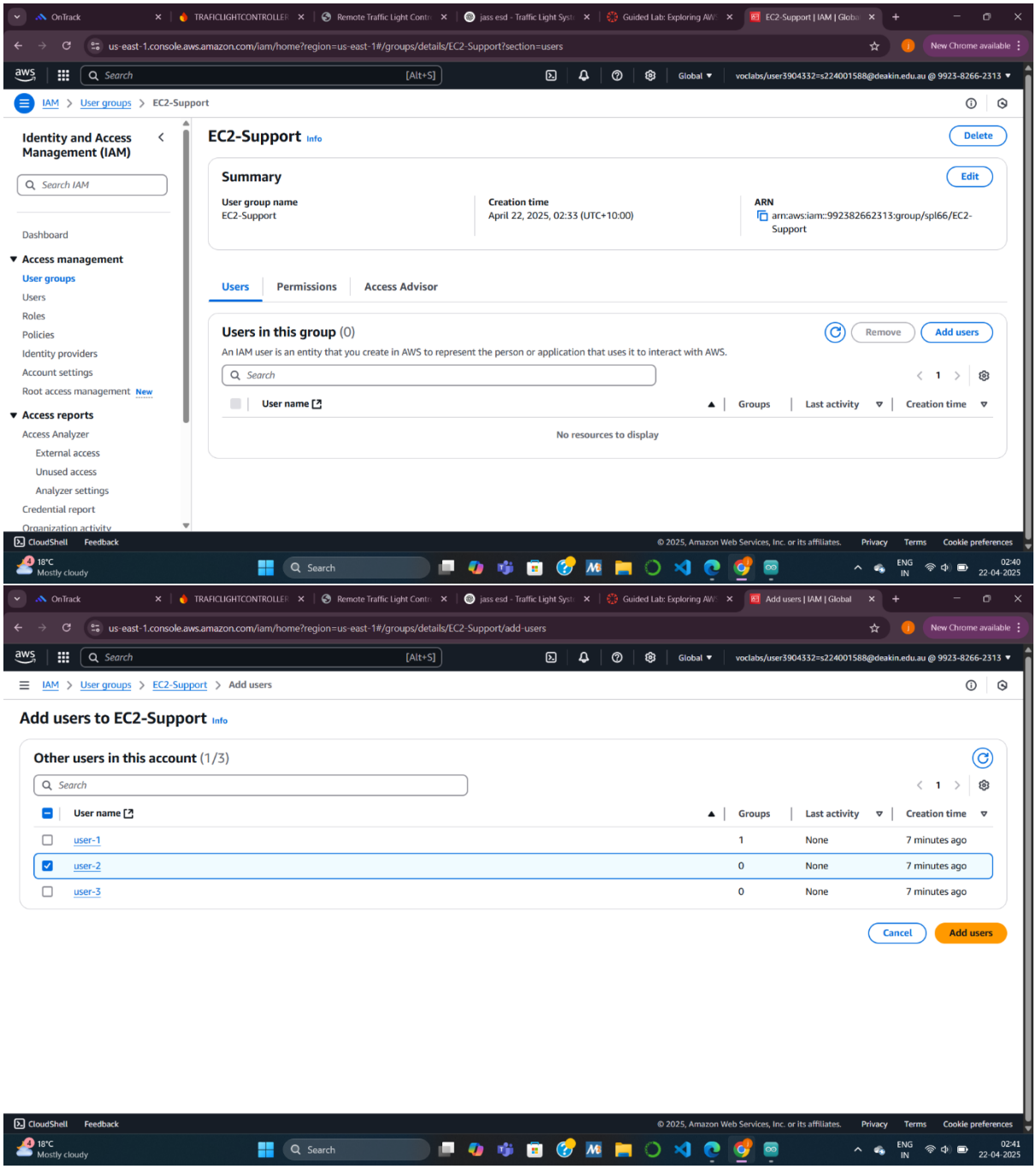
Task 2.3: Add user-3 to the EC2-Admin group

- **Add user-3 to EC2-Admin group.**
- **Grants permission to view, start, and stop EC2 instances.**

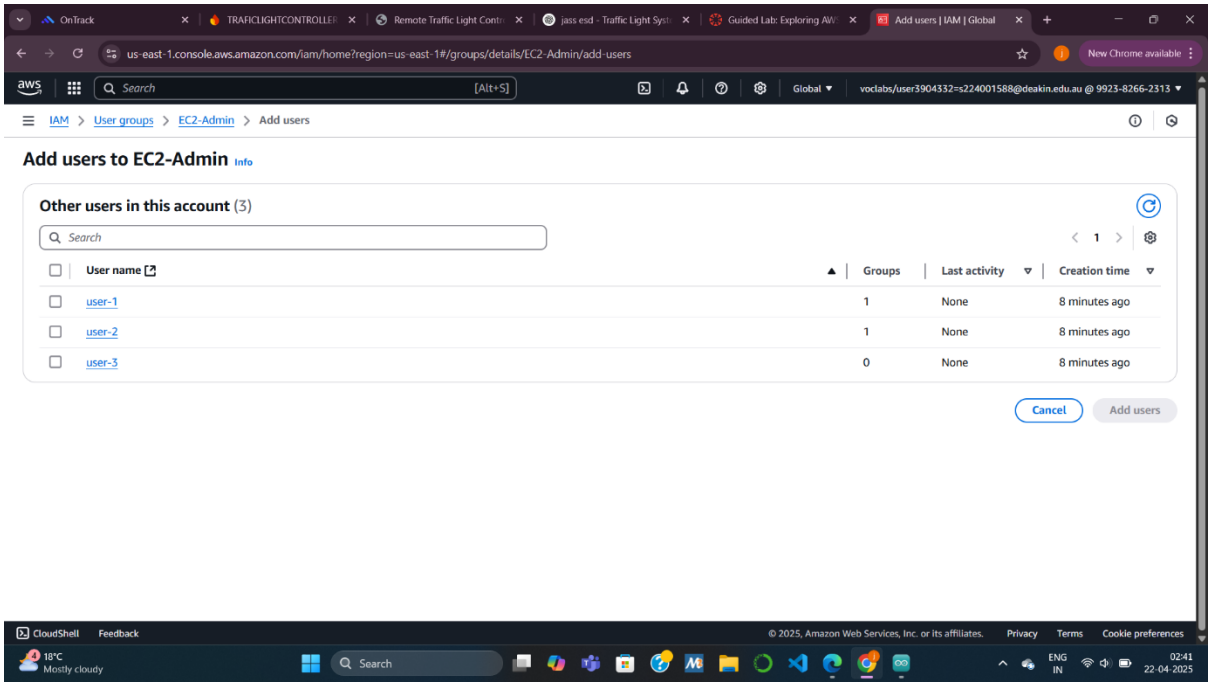
JASVEENA-224001588

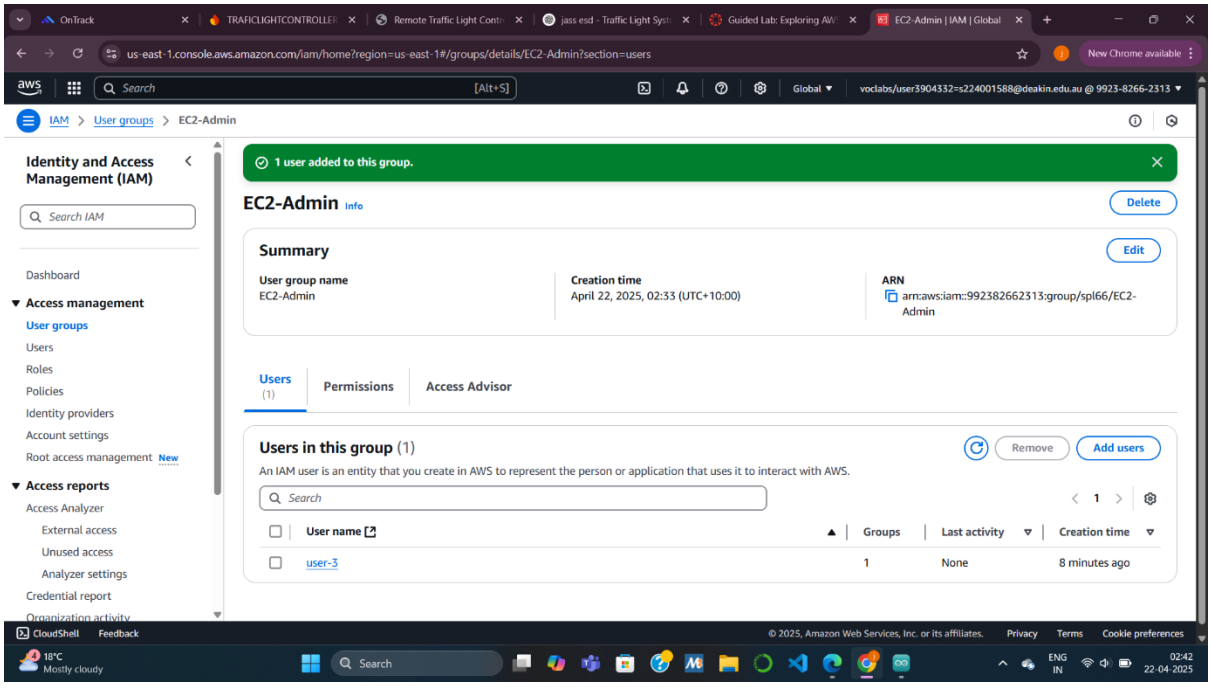


JASVEENA-224001588



JASVEENA-224001588





Task 3: Sign in and test user permissions

Task 3.1: Get the console sign-in URL

- **Locate and copy the IAM sign-in link for users.**

Task 3.2: Test user-1 permissions

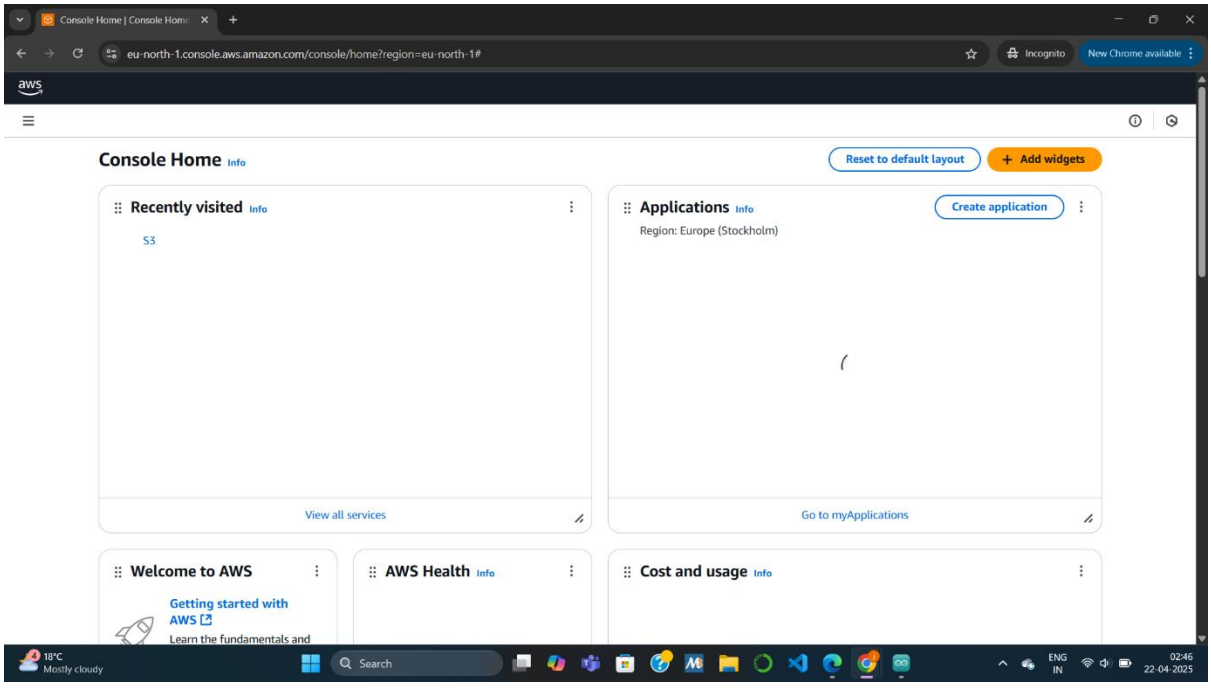
- **Sign in as user-1.**
- **Confirm they can view S3 buckets but cannot access EC2.**

Task 3.3: Test user-2 permissions

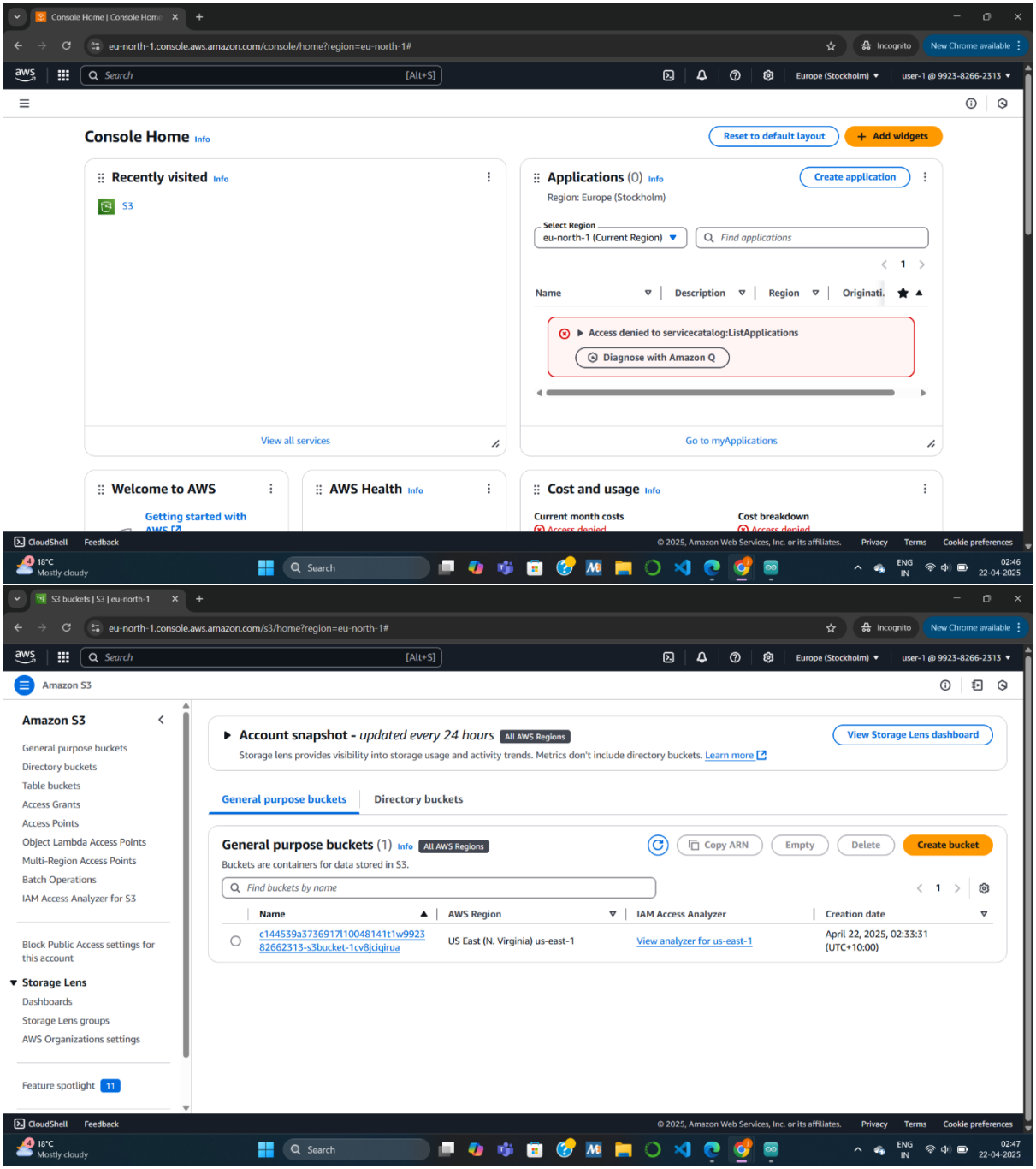
- **Sign in as user-2.**
- **Confirm they can view EC2 instances but cannot stop/start them.**
- **Confirm they cannot access S3.**

Task 3.4: Test user-3 permissions

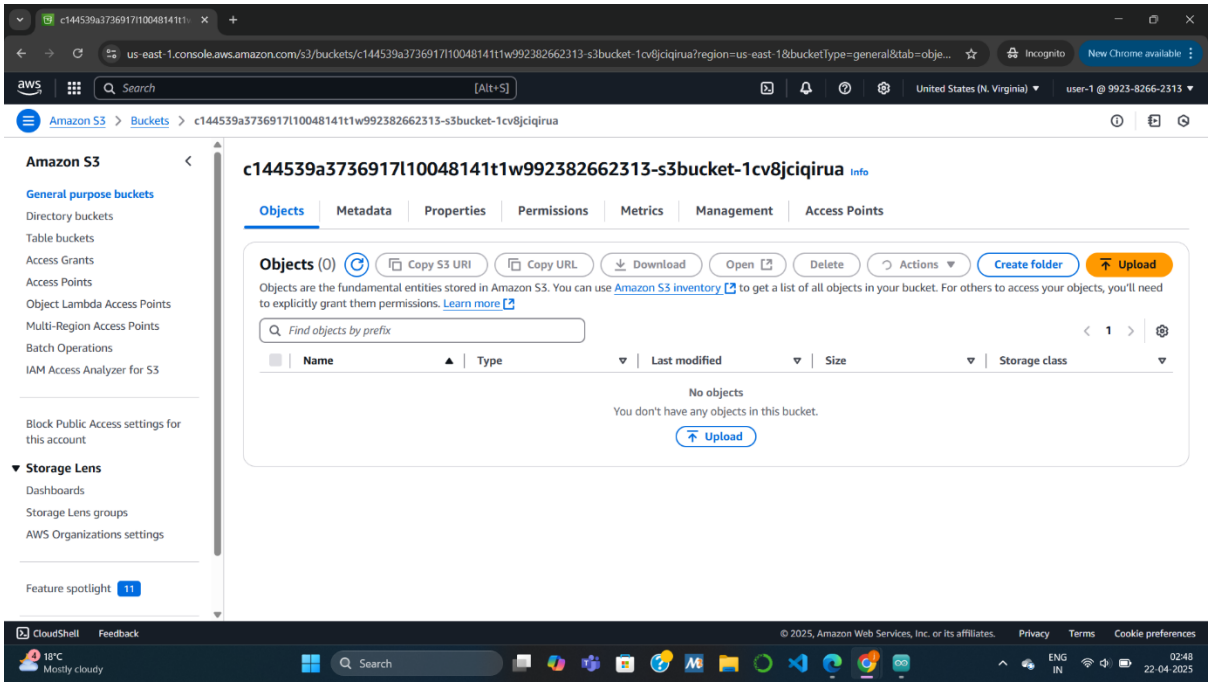
- **Sign in as user-3.**
- **Confirm they can view, stop, and start EC2 instances.**
- **Verifies that user-3 has proper admin access to EC2.**



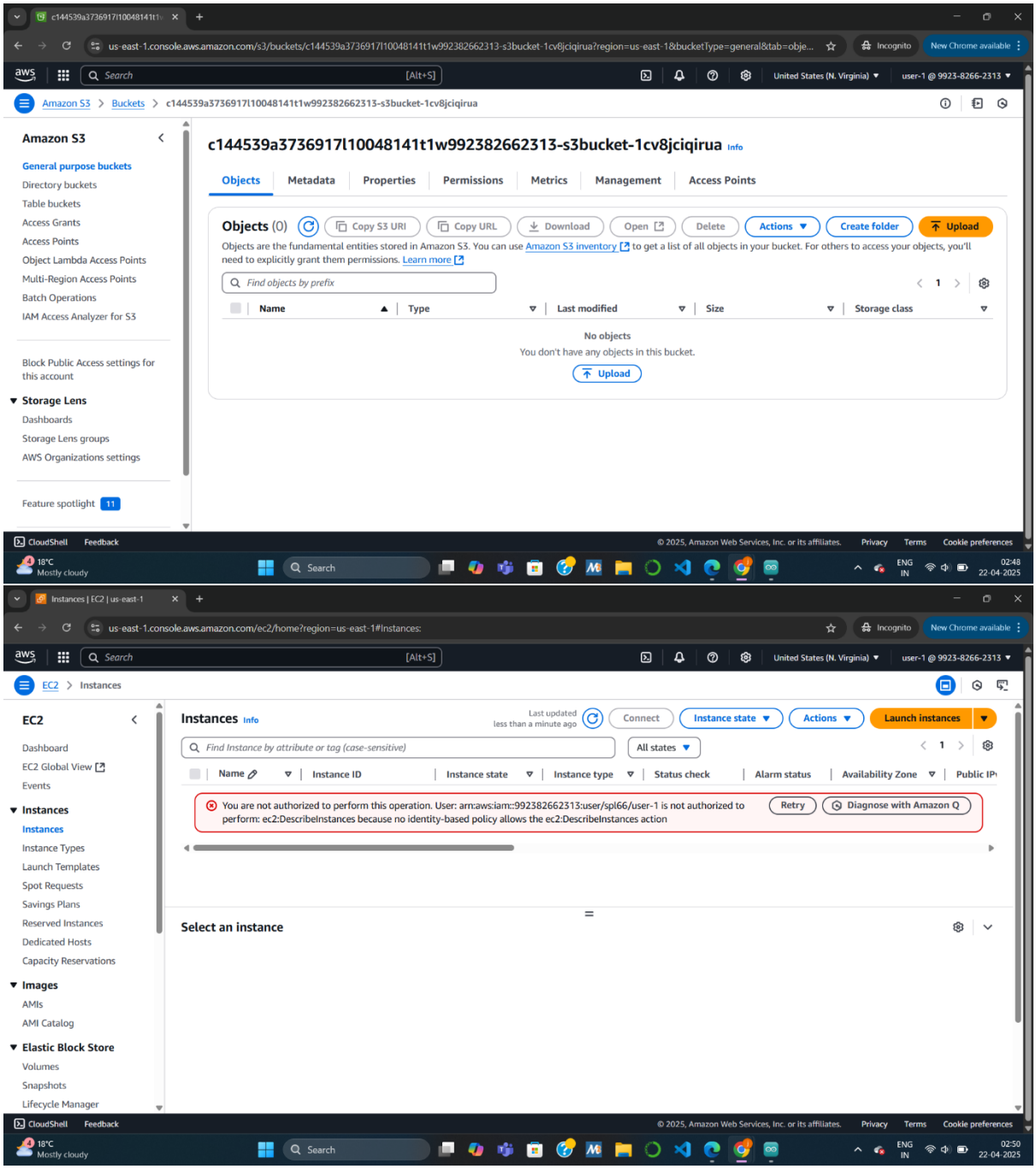
JASVEENA-224001588



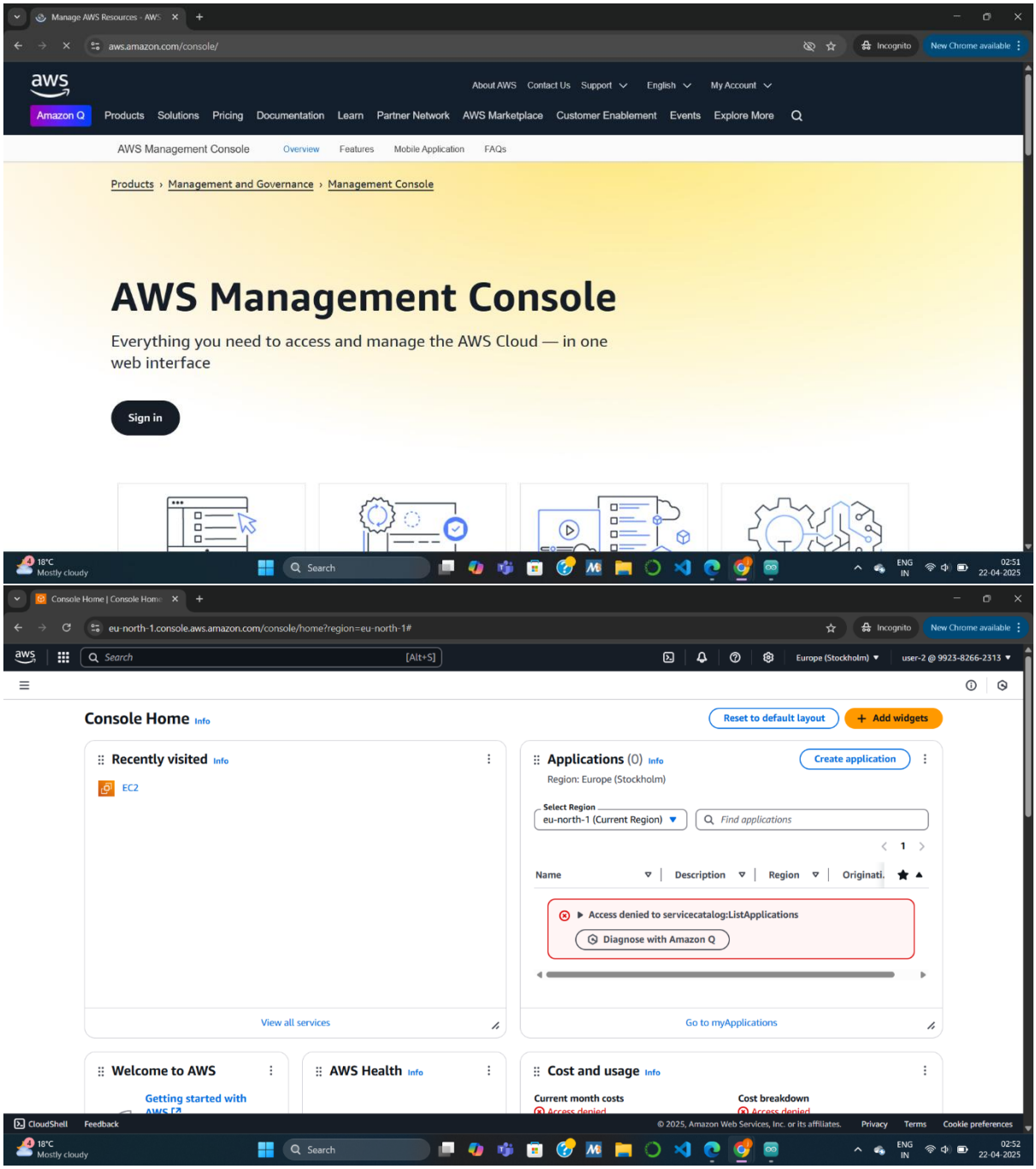
JASVEENA-224001588



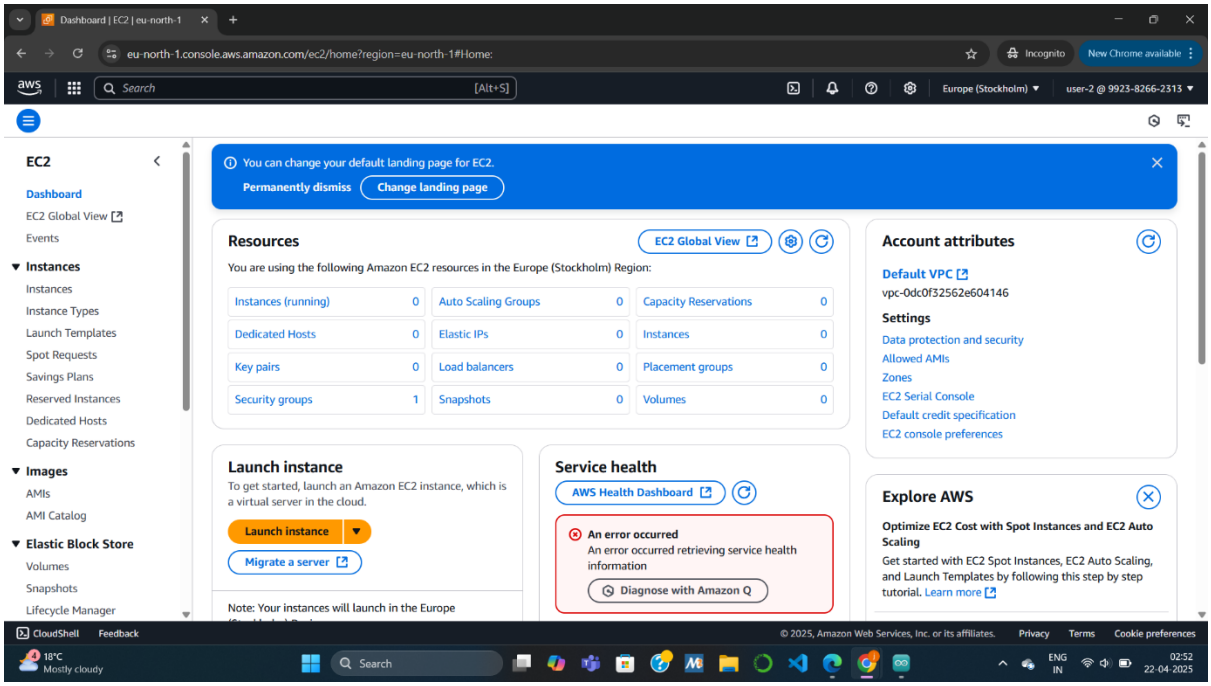
JASVEENA-224001588



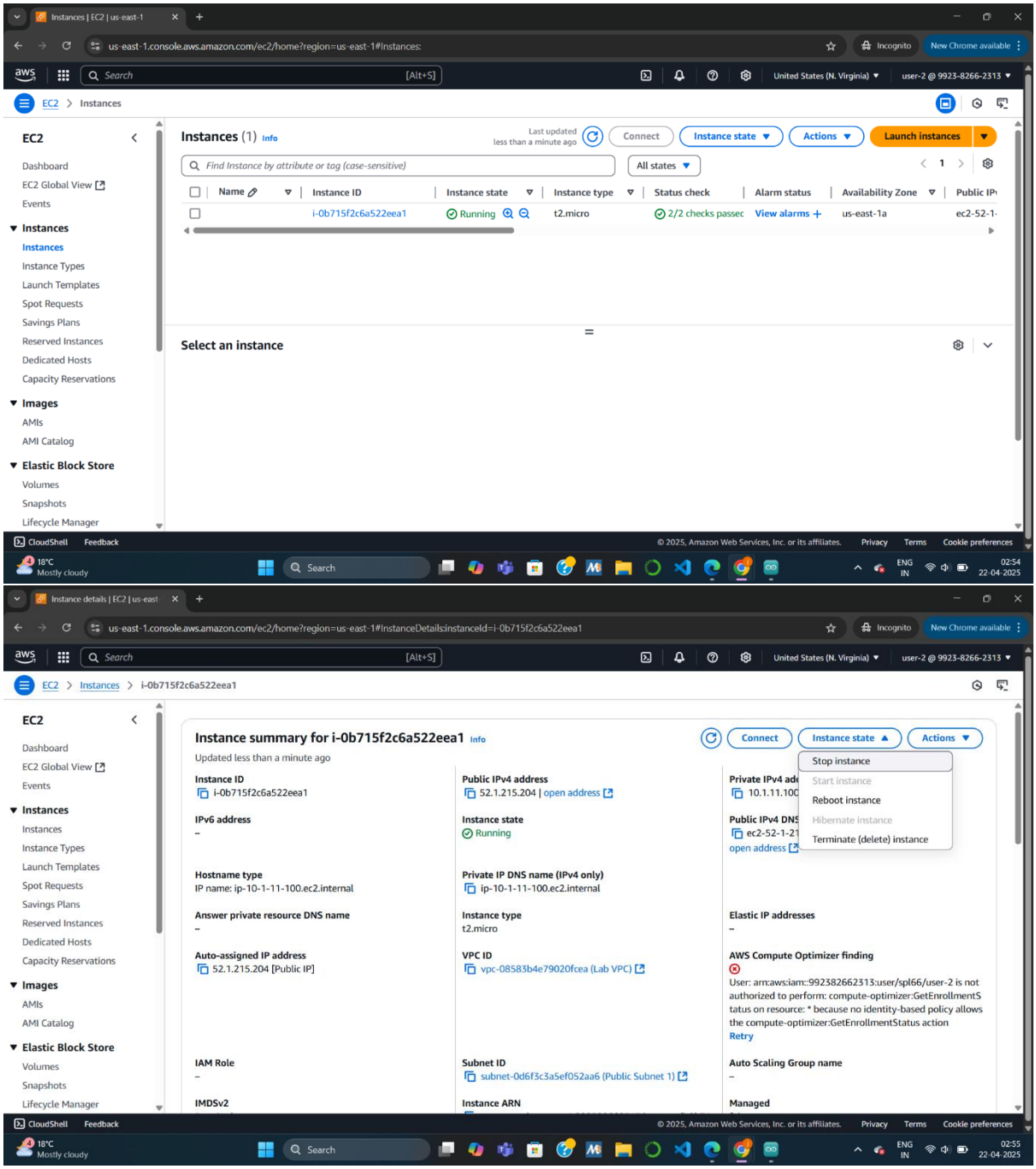
JASVEENA-224001588



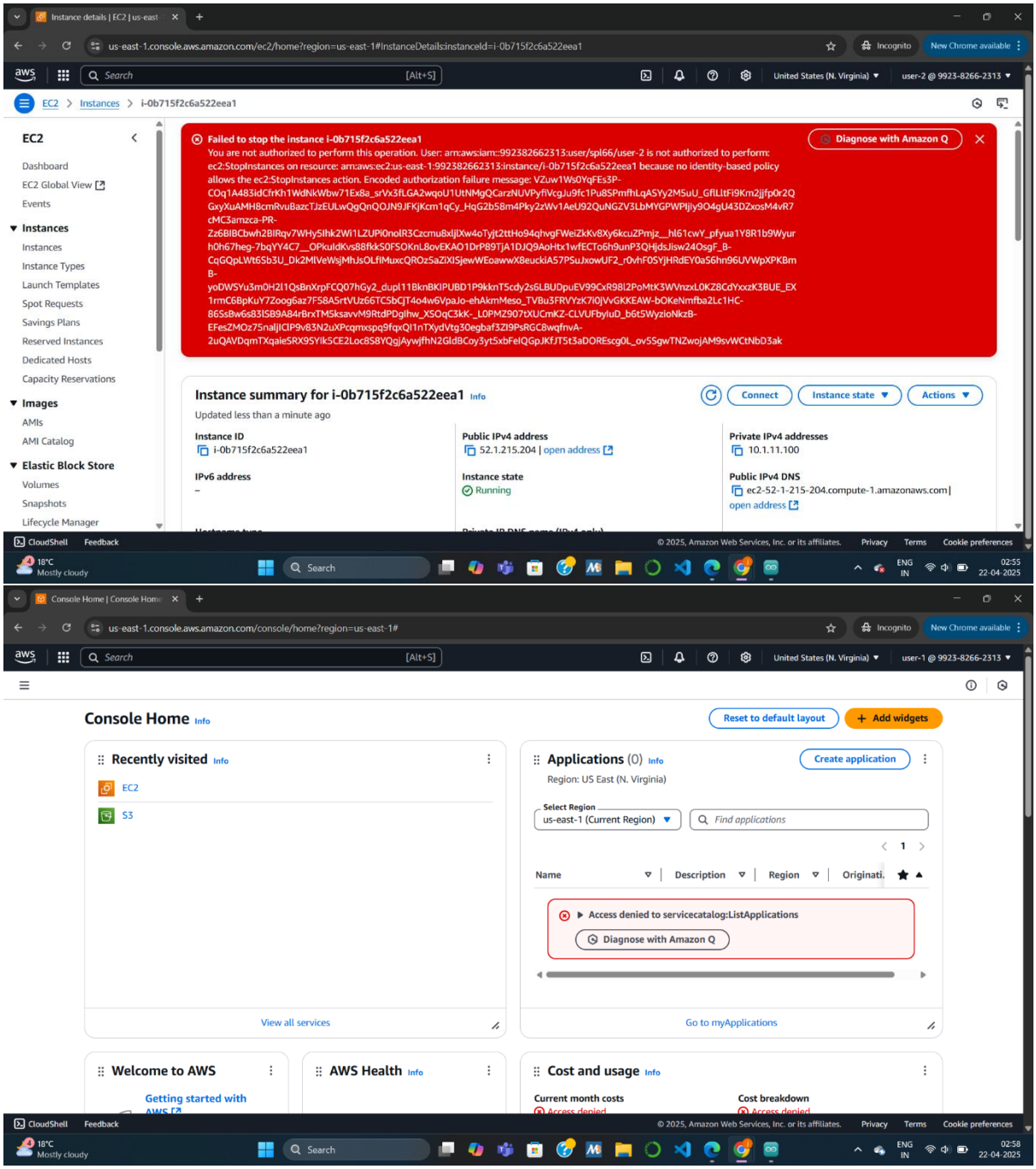
JASVEENA-224001588



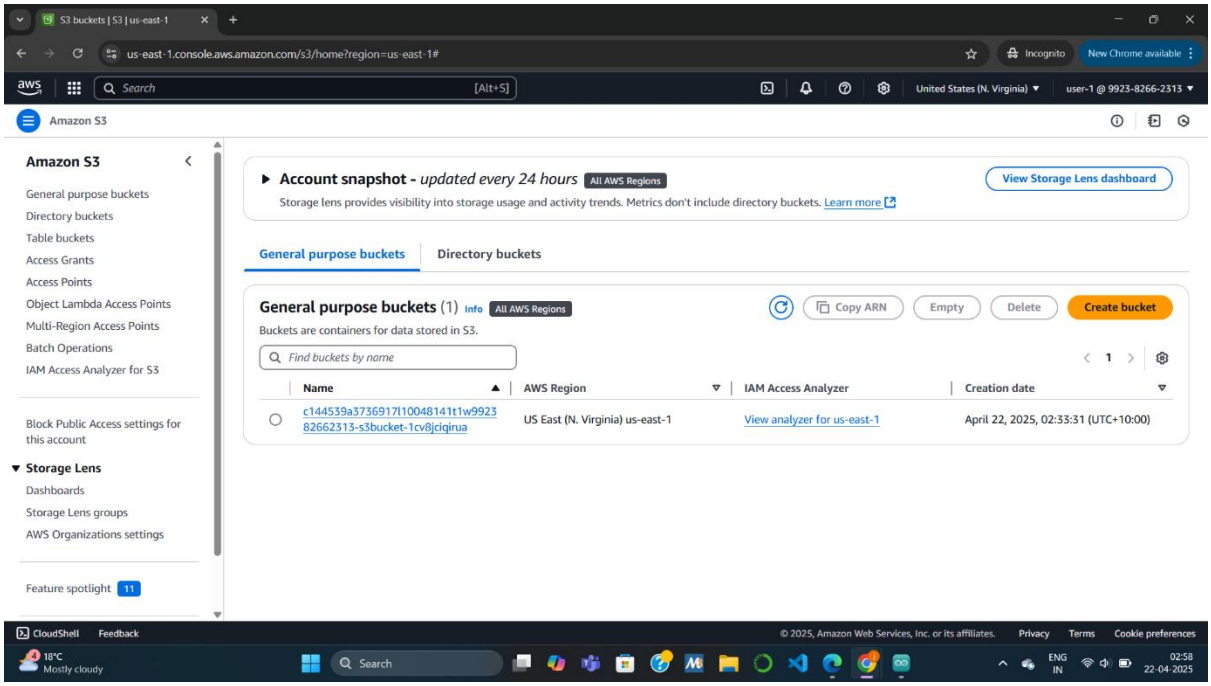
JASVEENA-224001588



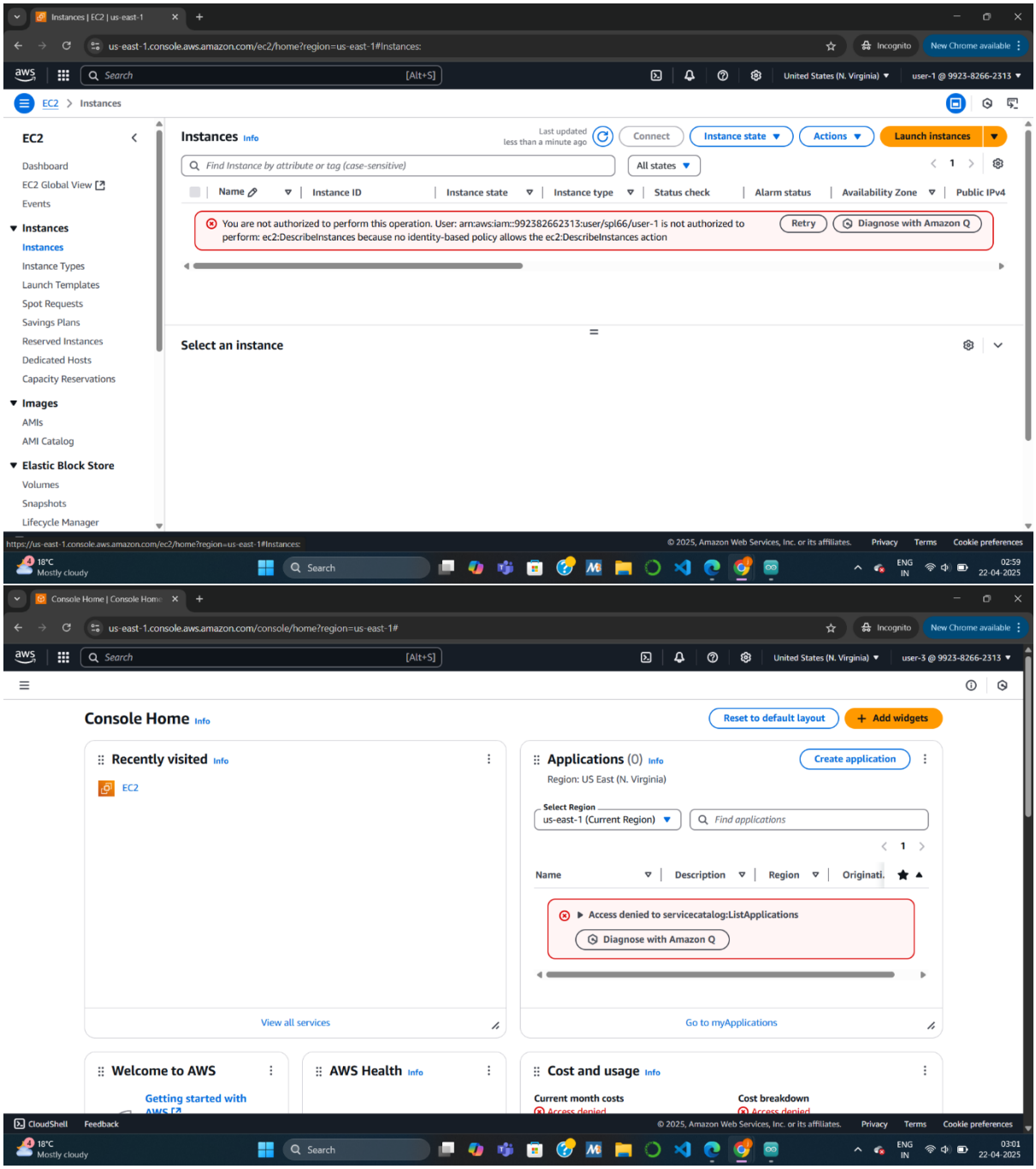
JASVEENA-224001588



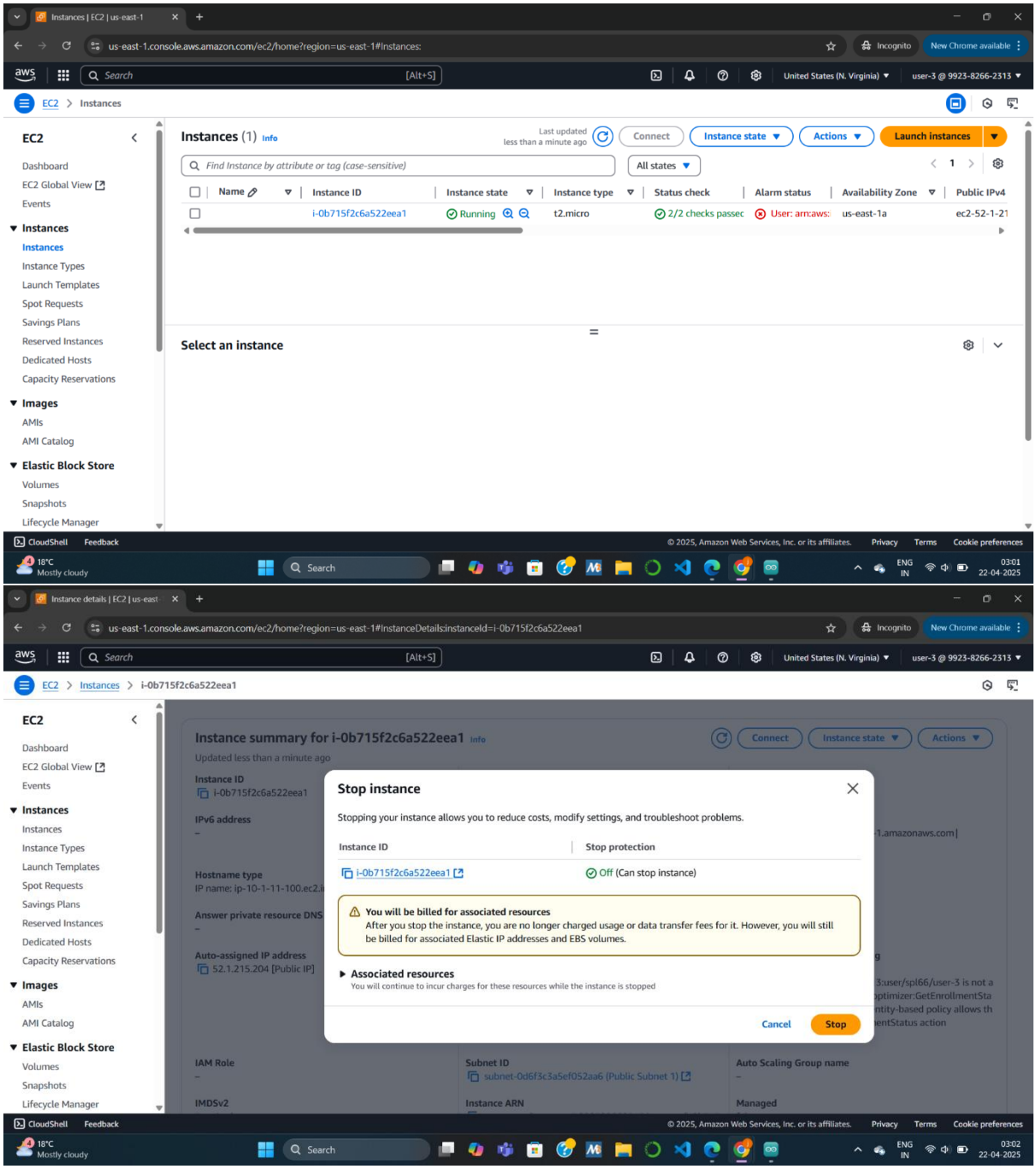
JASVEENA-224001588



JASVEENA-224001588



JASVEENA-224001588



JASVEENA-224001588