AWS IAM Mini Project — Role-Based Access Control for EC2 and S3

Author: Aryan Kaushik
Date: 2025-06-20

Objective

This mini project demonstrates how to use AWS Identity and Access Management (IAM) to create secure, role-based access for different users. We will:

- Create an IAM Group with EC2 Full Access and S3 Read-Only Access
- Create two IAM users: one EC2 admin and one S3 read-only user
- Verify the permissions by logging in with both users
- (Optional) Enable MFA for enhanced security

Tools Used

- AWS Management Console
- AWS IAM
- Amazon EC2
- Amazon S3
- Web browser (Incognito mode for testing)

Steps and Screenshots

1️⃣ Create IAM Group

Group Name: **EC2AdminS3ReadOnlyGroup**
Attached Policies:

- AmazonEC2FullAccess
- AmazonS3ReadOnlyAccess

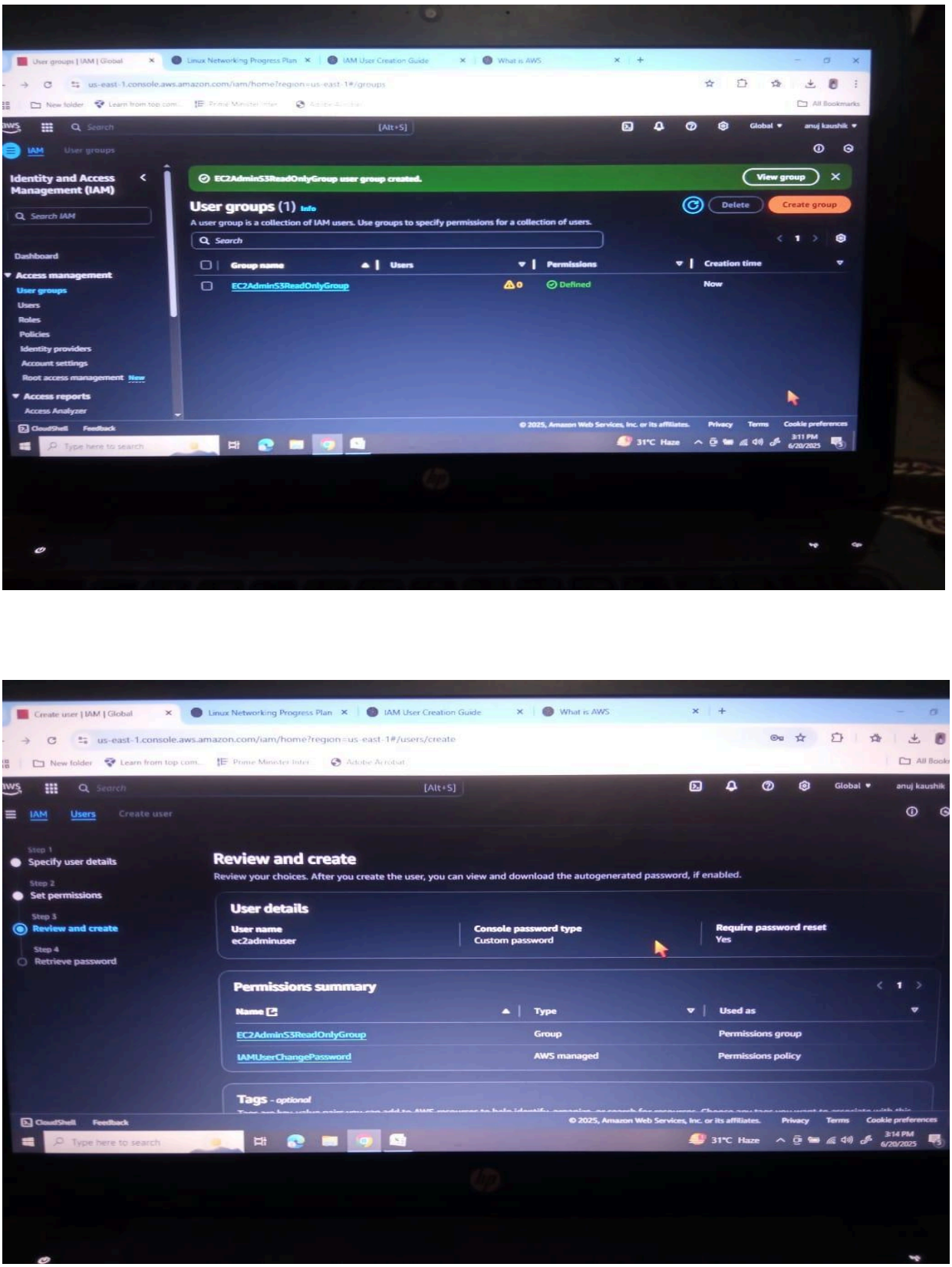
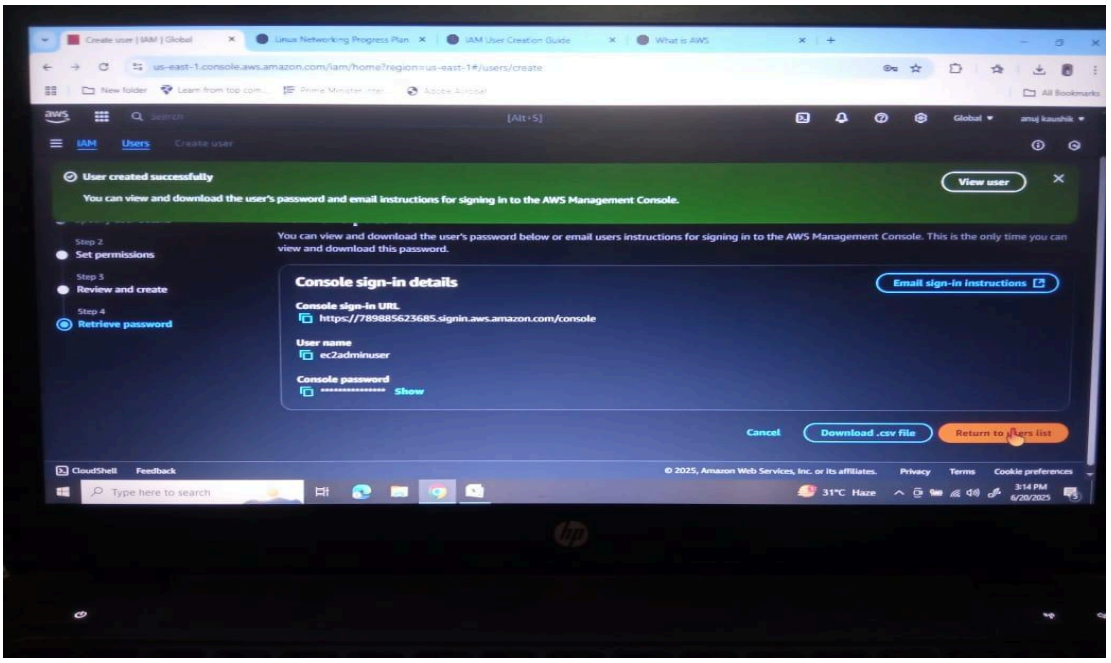


Figure 1: IAM Group creation form with attached policies

2 Create EC2 Admin User

Username: **ec2adminuser**
Access Type: Programmatic + AWS Management Console access
Group: **EC2AdminS3ReadOnlyGroup**



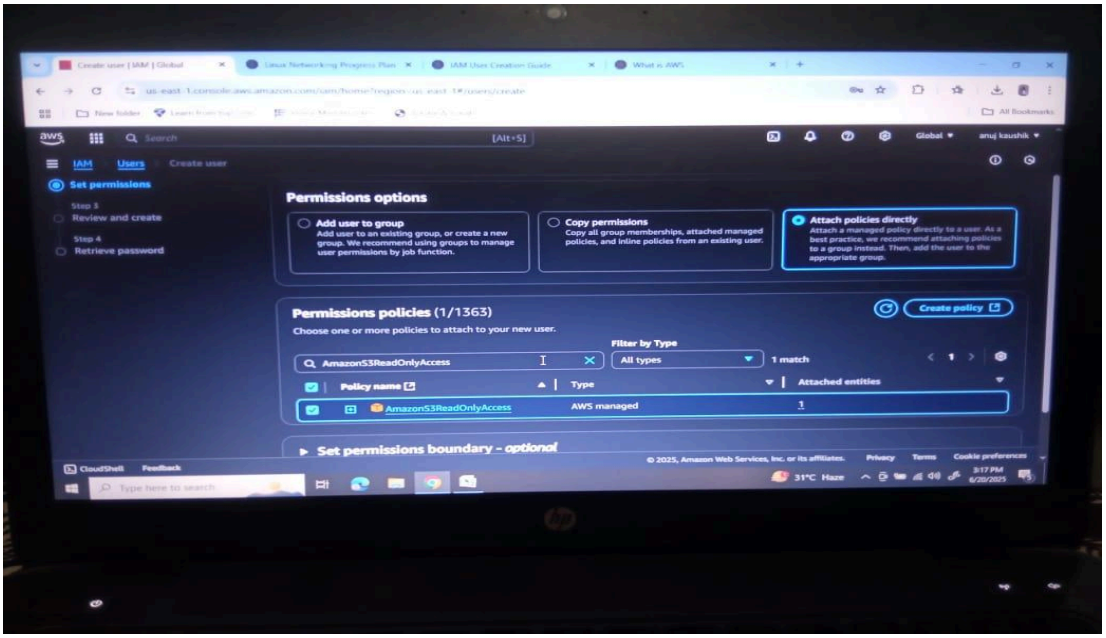


Figure 2: Add user form with username and access type

3️⃣ Create S3 Read-Only User

Username: **s3readonlyuser**
Access Type: AWS Management Console access
Policy: **AmazonS3ReadOnlyAccess**

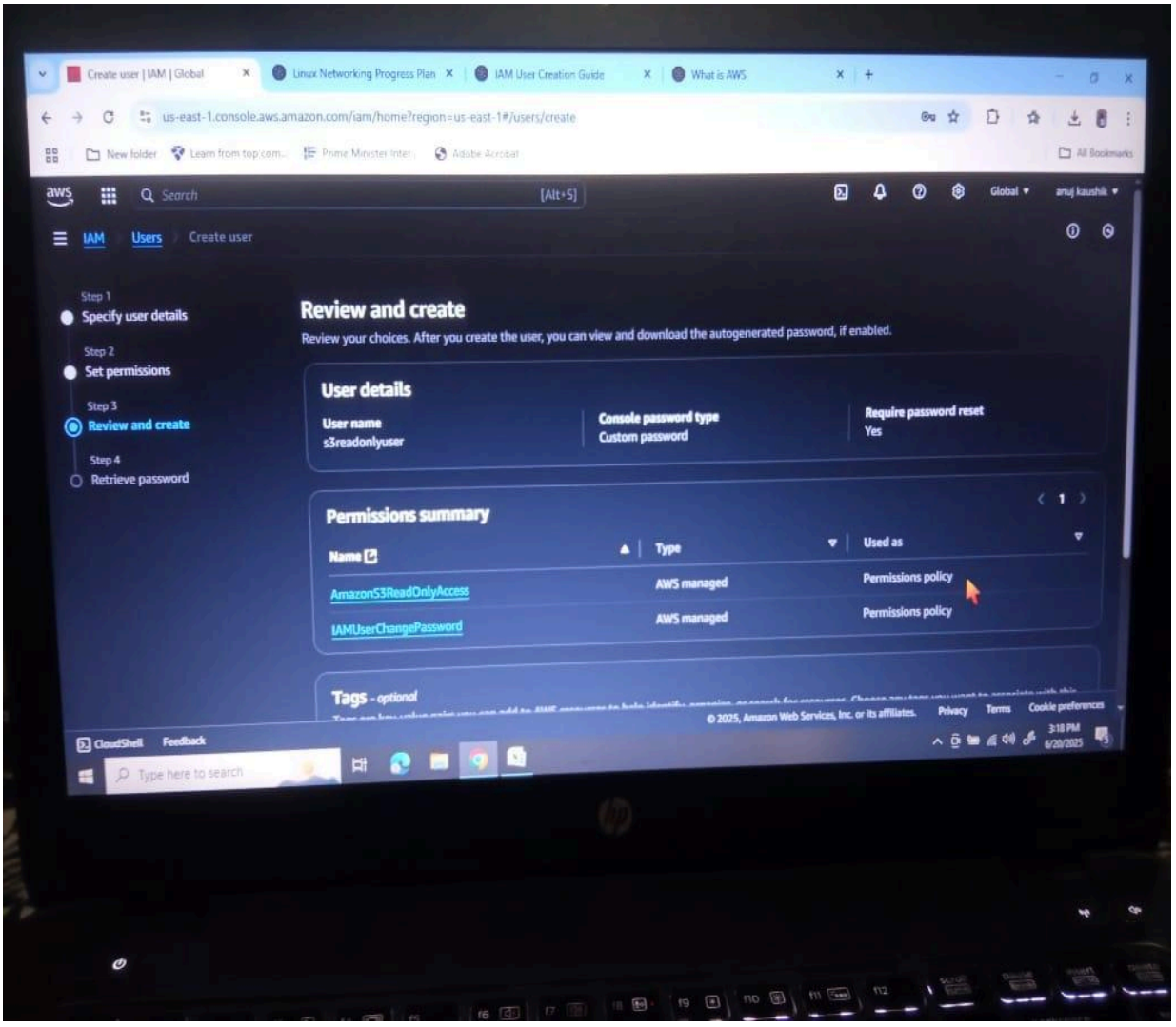


Figure 3: Policy selection screen for S3 read-only user

4️⃣ Test User Permissions

ec2adminuser:

- Access EC2 console
- Launch EC2 instance
-

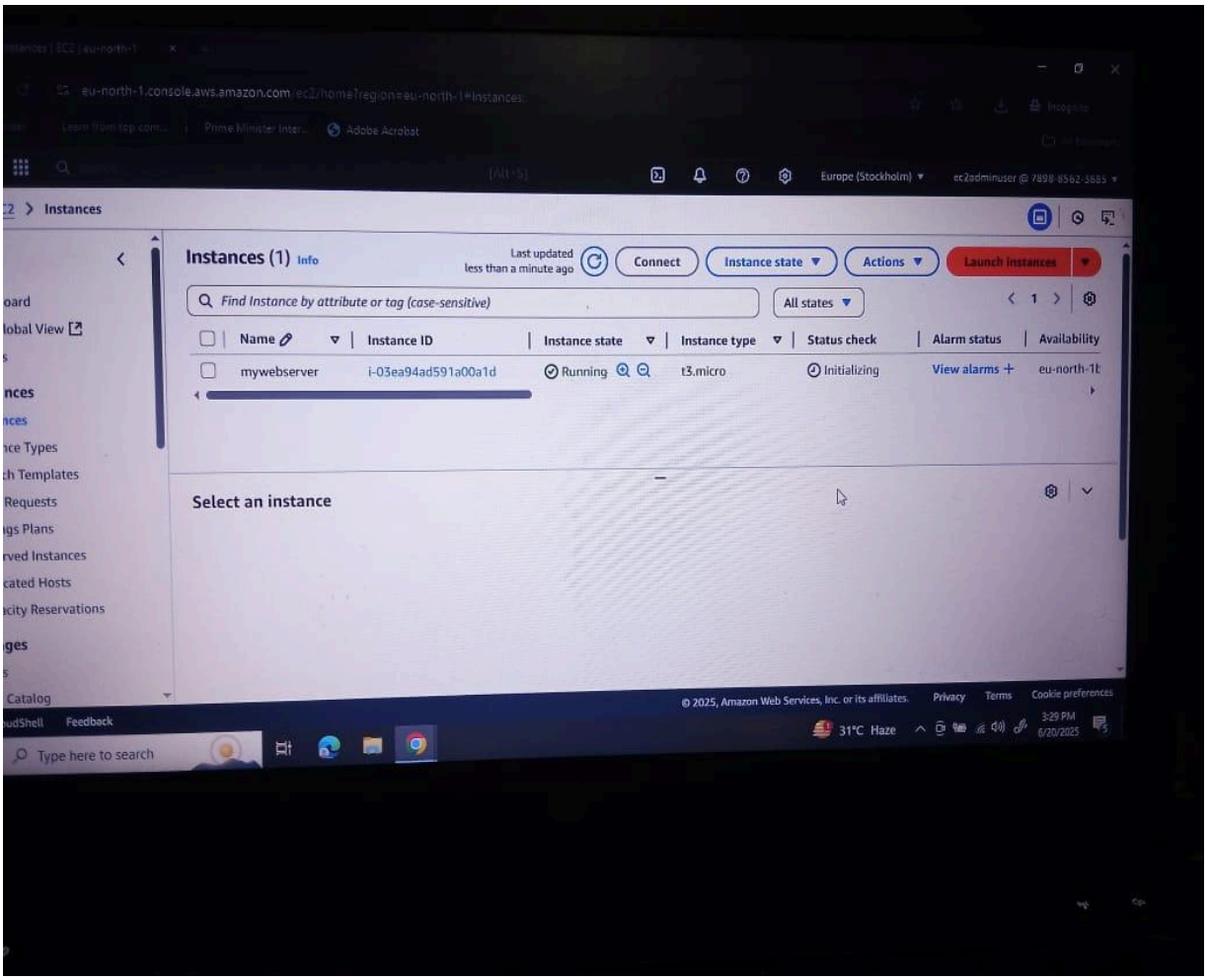


Figure 4: ec2adminuser launching EC2 instance

S3 read only user

- Access S3 console
- View bucket list
- Try to create/delete bucket (expect permission error

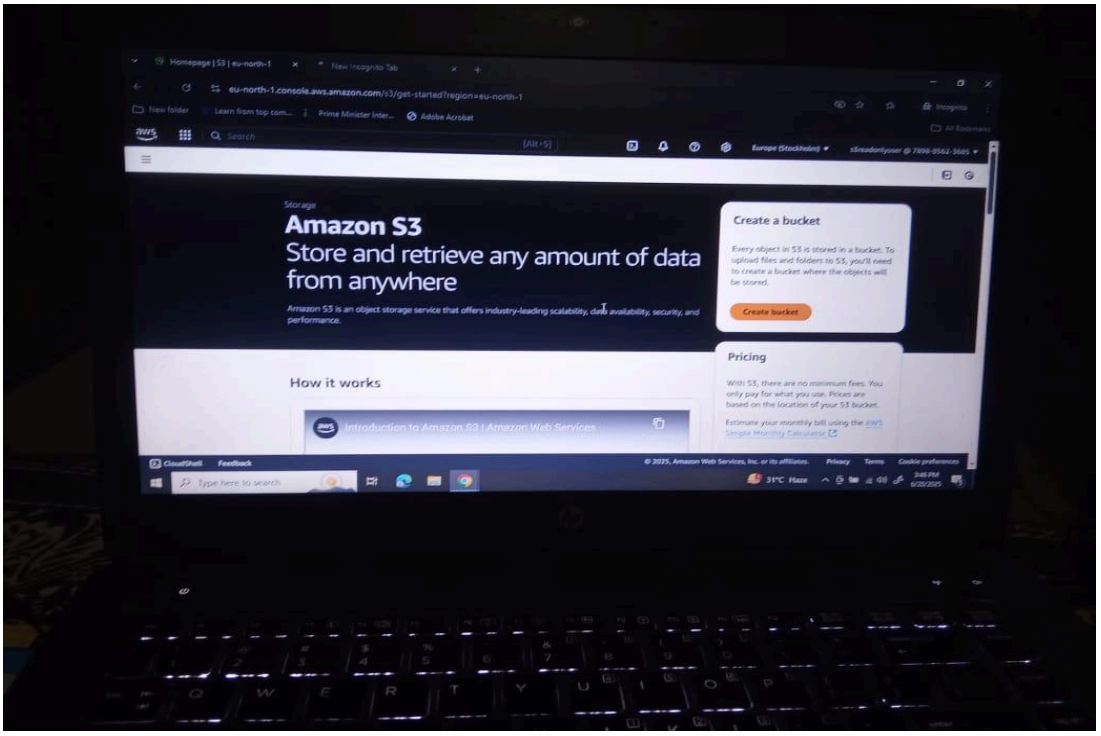


Figure 5: s3 read only user viewing bucket list

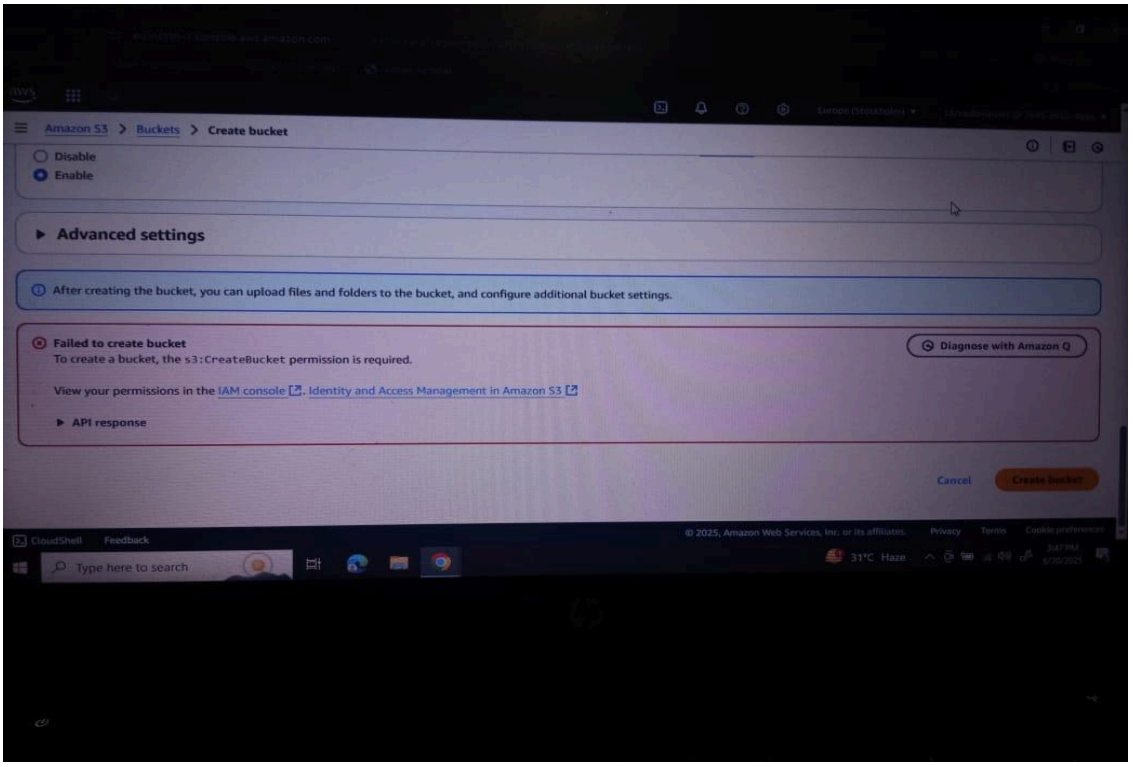


Figure 6: s3 read only user permission error while trying to create bucket

5 Enable MFA (Optional)

MFA enabled for **ec2adminuser**

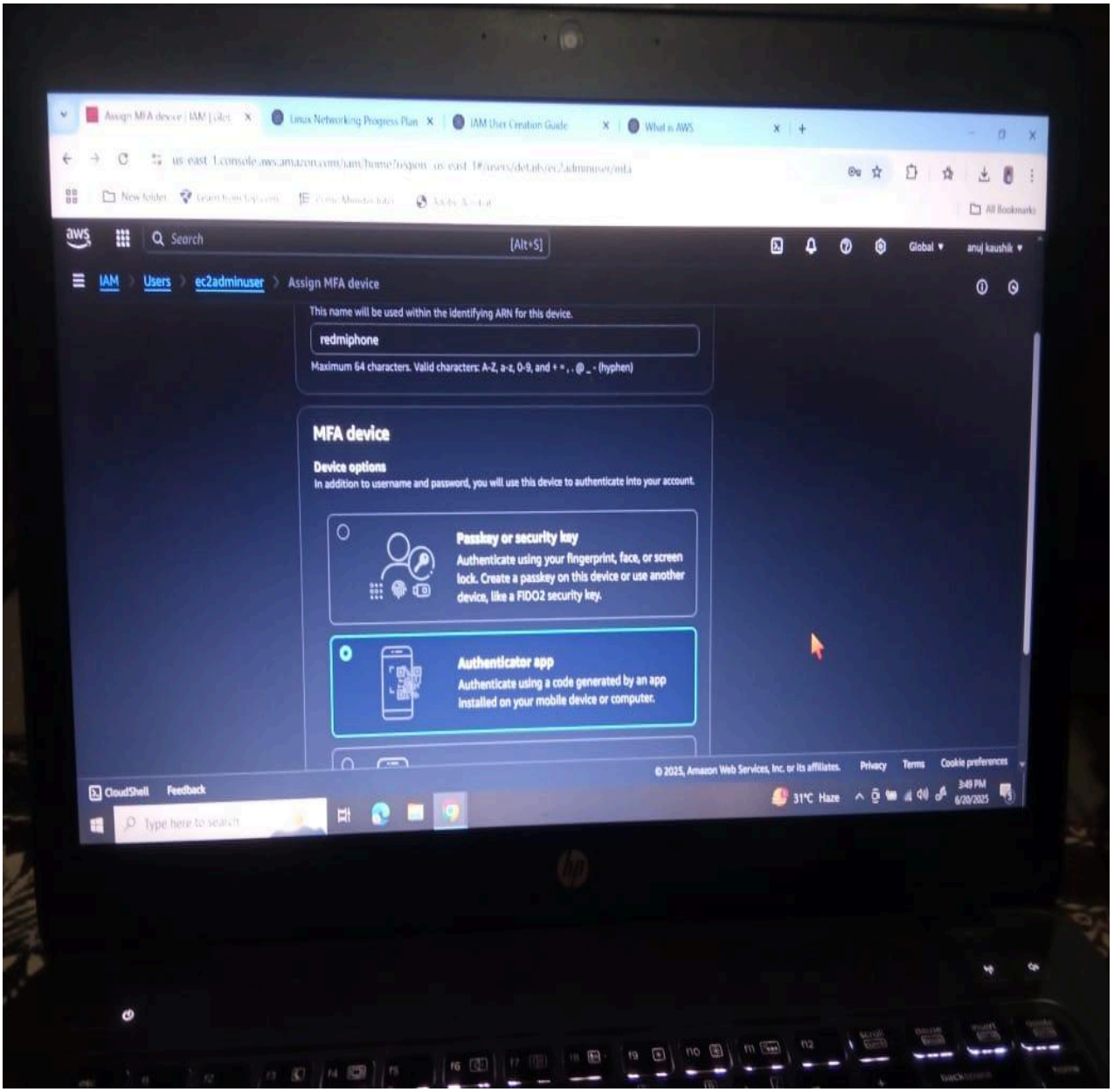
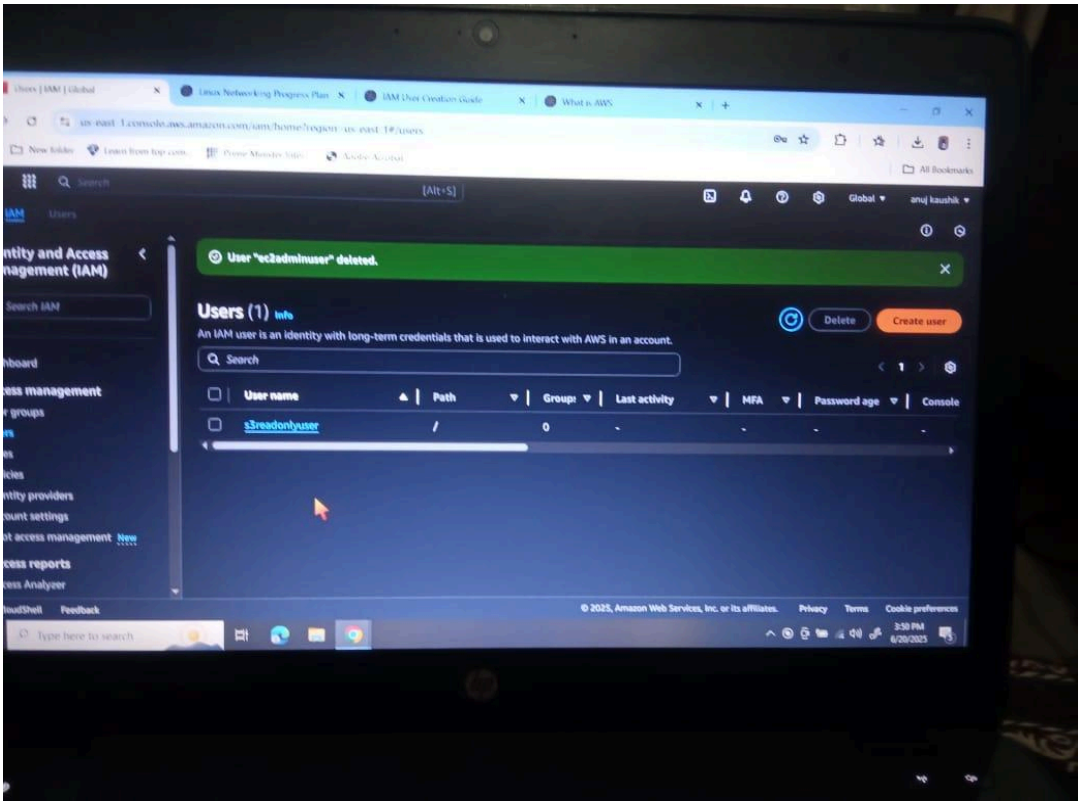


Figure 7: MFA setup confirmation

6 Clean-Up

Deleted users and group after testing to avoid unnecessary cost



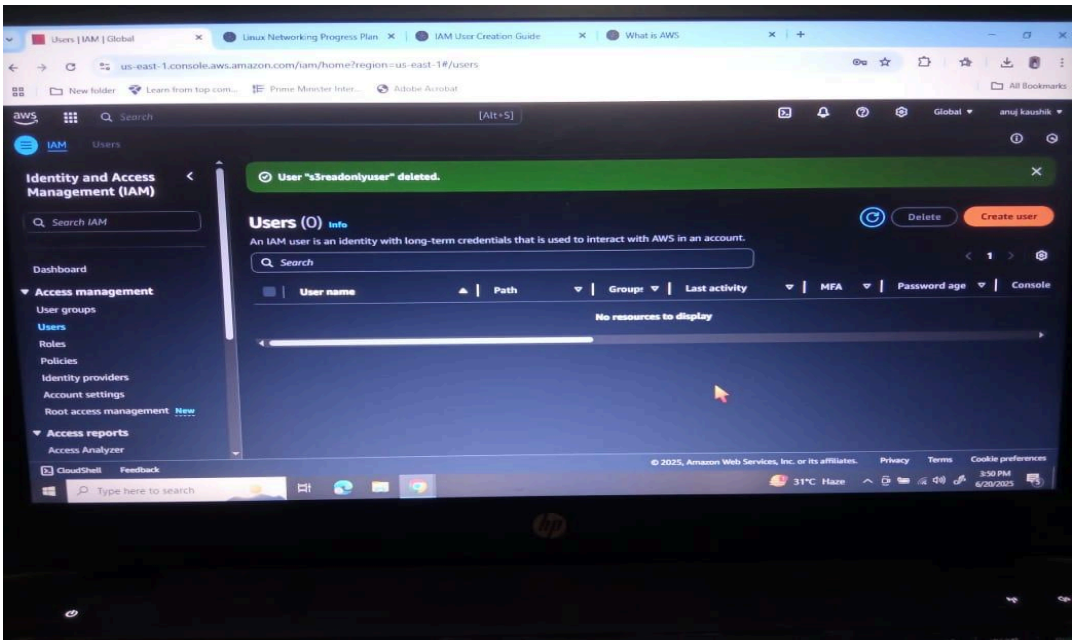


Figure 8: User delete confirmation

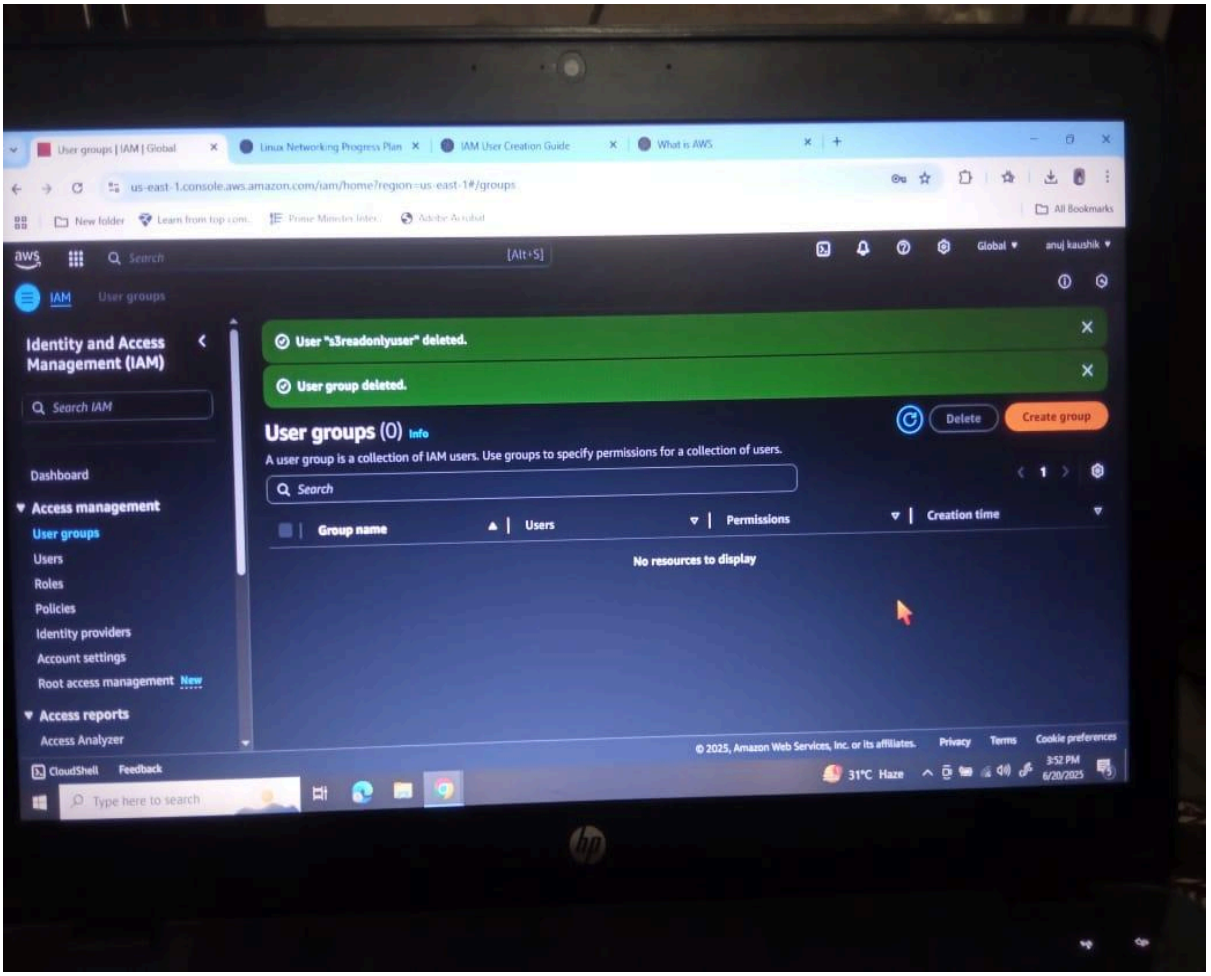


Figure 9: Group delete confirmation

Conclusion

This project successfully implemented role-based access control using AWS IAM. Two users were created with distinct permissions:

- An EC2 admin with full control over EC2
- An S3 read-only user with limited S3 access

Permissions were tested, and optional MFA was enabled to add an extra layer of security. This project demonstrates good IAM practices for managing cloud infrastructure securely.