Lab 1: Introduction to AWS Identity and Access Management (IAM)

Objective

The objective of this lab is to gain hands-on experience with AWS Identity and Access Management (IAM) by exploring how users, groups, and policies are used to control access to AWS resources. The lab demonstrates role-based access control by assigning permissions through IAM groups and validating access by logging in as different users. This helps reinforce the principle of least privilege and foundational cloud security concepts.

Key AWS services and concepts covered:

- AWS Identity and Access Management (IAM)
- IAM Users and User Groups
- Managed Policies and Inline Policies
- Role-Based Access Control (RBAC)
- AWS Management Console access using IAM credentials

Scenario

An organization is expanding its use of Amazon Web Services and relies heavily on Amazon EC2 and Amazon S3. As new employees join, they require controlled access to cloud resources based on their job roles. To maintain security and operational efficiency, permissions must be managed centrally using IAM groups instead of assigning permissions individually.

In this lab scenario, three IAM users are created and assigned distinct responsibilities. One user provides read-only support for Amazon S3, another provides read-only support for Amazon EC2, and a third user acts as an EC2 administrator with permissions to view, start, and stop EC2 instances. The expected outcome is that each user can access only the AWS services and actions permitted by their assigned IAM group and policies.

Working Methodology

Task 1: Exploring IAM Users, Groups, and Policies

The IAM console was accessed to review pre-created IAM users and user groups. Each user was examined to verify permissions, group membership, and security credentials. IAM group policies were analyzed to understand the difference between managed policies and inline policies and how they define access to AWS services.

Observations:

- Users had no permissions unless assigned through groups.
- Managed policies provided reusable permission sets, while inline policies were specific to individual groups.

Task 2: Assigning Users to IAM Groups

Users were assigned to IAM groups based on their job roles. User-1 was added to the S3-Support group, user-2 to the EC2-Support group, and user-3 to the EC2-Admin group. This ensured that permissions were inherited automatically through group policies rather than assigned individually.

Completed Actions:

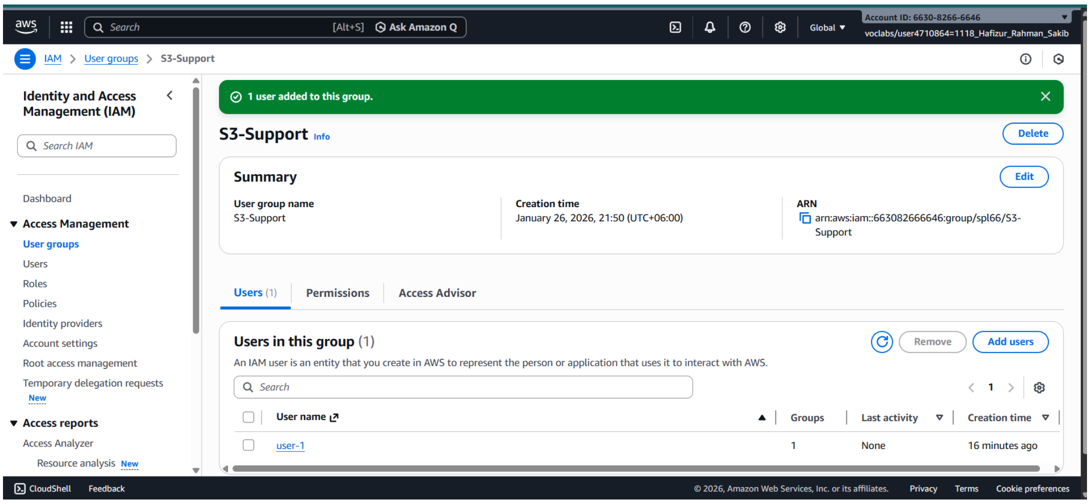
- Task 2a: Added user-1 to S3-Support group
- Task 2b: Added user-2 to EC2-Support group
- Task 2c: Added user-3 to EC2-Admin group

Observations:

- Each group correctly showed one assigned user.
- Minor authorization warnings appeared due to lab restrictions but did not affect completion.

Added user-1 to S3-Support group

This screenshot shows user-1 being successfully added to the S3-Support IAM group. By assigning this group membership, user-1 inherits read-only permissions for Amazon S3 through the attached managed policy. This confirms the correct implementation of role-based access control.



1 user added to this group.

S3-Support

Summary

User group name: S3-Support

Creation time: January 26, 2026, 21:50 (UTC+06:00)

ARN: arn:aws:iam::663082666646:group/spl66/S3-Support

Users in this group (1)

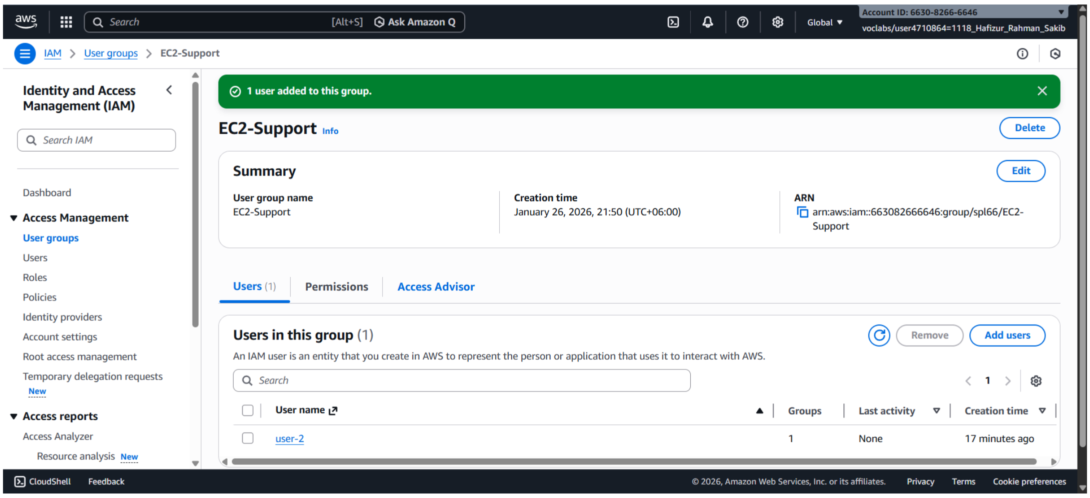
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

User name	Groups	Last activity	Creation time
user-1	1	None	16 minutes ago

Figure 1: Added user-1 to S3-Support group

Added user-2 to EC2-Support group

This image illustrates the assignment of user-2 to the EC2-Support group. The group provides read-only access to Amazon EC2 resources, allowing the user to view instance details without making modifications. This step ensures operational support access without administrative privileges.



1 user added to this group.

EC2-Support

Summary

User group name: EC2-Support

Creation time: January 26, 2026, 21:50 (UTC+06:00)

ARN: arn:aws:iam::663082666646:group/spl66/EC2-Support

Users in this group (1)

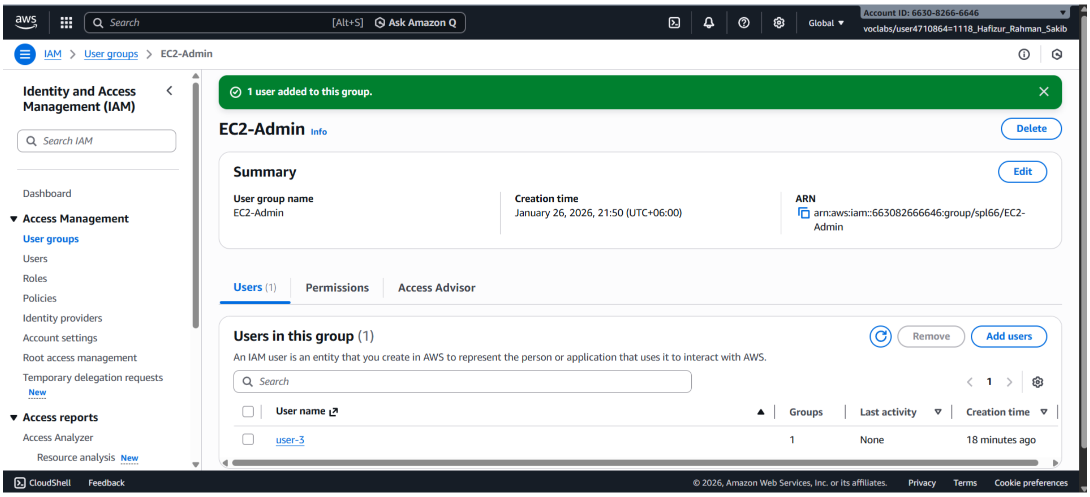
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

User name	Groups	Last activity	Creation time
user-2	1	None	17 minutes ago

Figure 2: Added user-2 to EC2-Support group

Added user-3 to EC2-Admin group

This screenshot confirms that user-3 was added to the EC2-Admin group. The inline policy attached to this group allows starting and stopping EC2 instances in addition to viewing them. This assignment grants administrator-level permissions required for instance management.



1 user added to this group.

EC2-Admin

Summary

User group name
EC2-Admin

Creation time
January 26, 2026, 21:50 (UTC+06:00)

ARN
arn:aws:iam::663082666646:group/spl66/EC2-Admin

Users (1) | Permissions | Access Advisor

Users in this group (1)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

User name	Groups	Last activity	Creation time
user-3	1	None	18 minutes ago

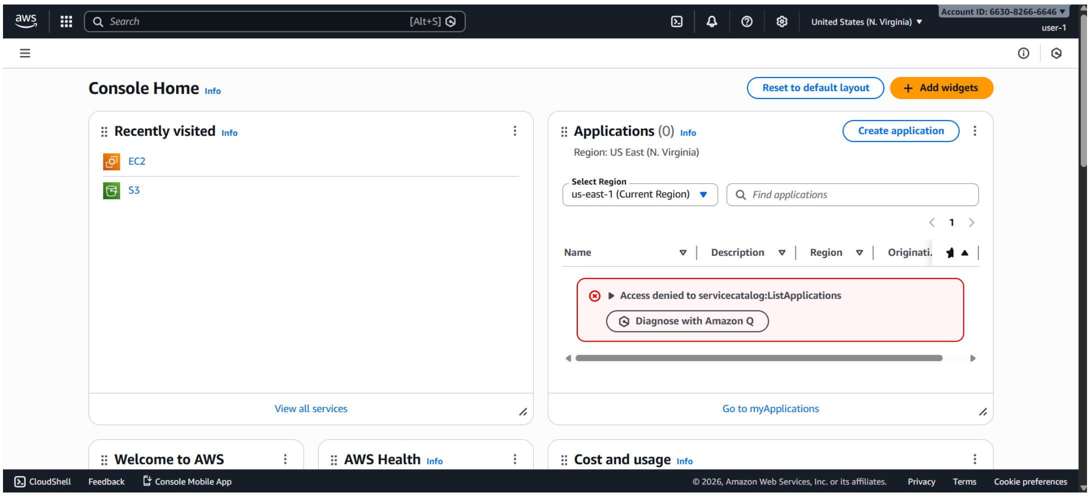
Figure 3: Added user-3 to EC2-Admin group

Task 3: User Login and Permission Validation

Each IAM user logged in using the IAM sign-in URL in a private browser session to validate permissions. User-1 successfully accessed Amazon S3 but was denied access to EC2. User-2 could view EC2 instances but was unable to stop them and had no access to S3. User-3 successfully stopped an EC2 instance, confirming administrator-level permissions.

user-1 logged in

This screenshot shows a successful login by user-1 using the IAM sign-in URL. The user was able to access Amazon S3 resources, confirming that the S3-Support permissions were correctly applied. Access to unauthorized services was restricted as expected.



Console Home

Recently visited
EC2
S3

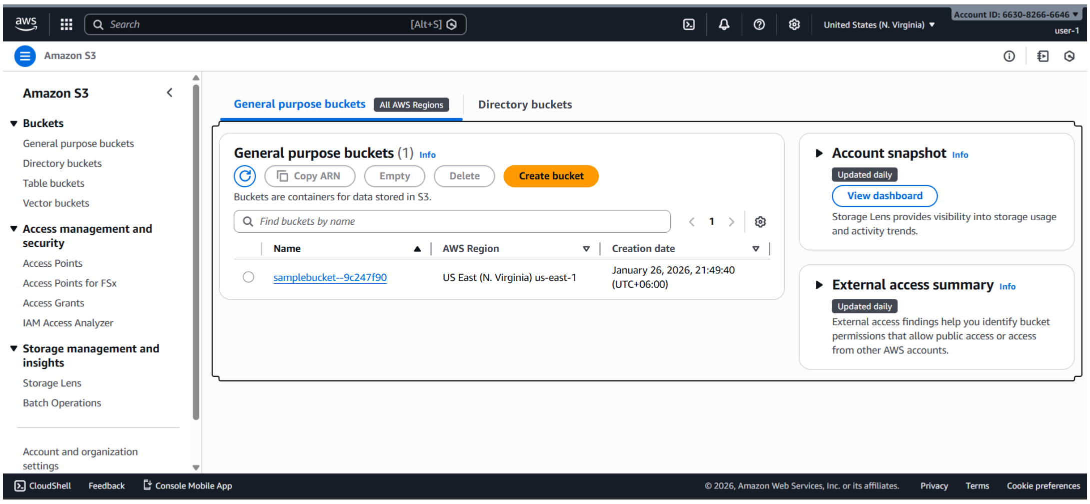
Applications (0)
Region: US East (N. Virginia)
Select Region: us-east-1 (Current Region)

Access denied to servicecatalog:ListApplications

Figure 4: user-1 logged in

user-1 logged in

This image further demonstrates user-1 navigating the AWS Management Console. It reinforces that the user could only access permitted services and was restricted from accessing Amazon EC2. This validates correct enforcement of IAM policies.



General purpose buckets (1) Info

Buckets are containers for data stored in S3.

Name	AWS Region	Creation date
samplebucket--9c247f90	US East (N. Virginia) us-east-1	January 26, 2026, 21:49:40 (UTC+06:00)

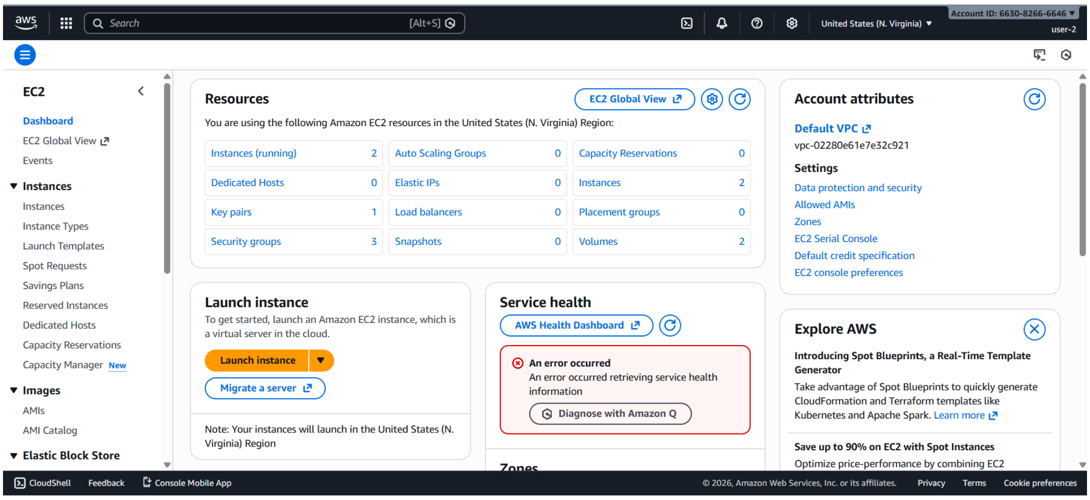
Storage Lens provides visibility into storage usage and activity trends.

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

Figure 5: user-1 logged in

user-2 logged in

This screenshot displays a successful login by user-2. The user was able to view EC2 instances due to read-only EC2 permissions. However, modification actions were restricted, maintaining security boundaries.



Resources

You are using the following Amazon EC2 resources in the United States (N. Virginia) Region:

Instances (running)	2	Auto Scaling Groups	0	Capacity Reservations	0
Dedicated Hosts	0	Elastic IPs	0	Instances	2
Key pairs	1	Load balancers	0	Placement groups	0
Security groups	3	Snapshots	0	Volumes	2

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the United States (N. Virginia) Region

Service health

An error occurred
An error occurred retrieving service health information

Account attributes

Default VPC
vpc-02280e61e7e32c921

Settings
Data protection and security
Allowed AMIs
Zones
EC2 Serial Console
Default credit specification
EC2 console preferences

Explore AWS

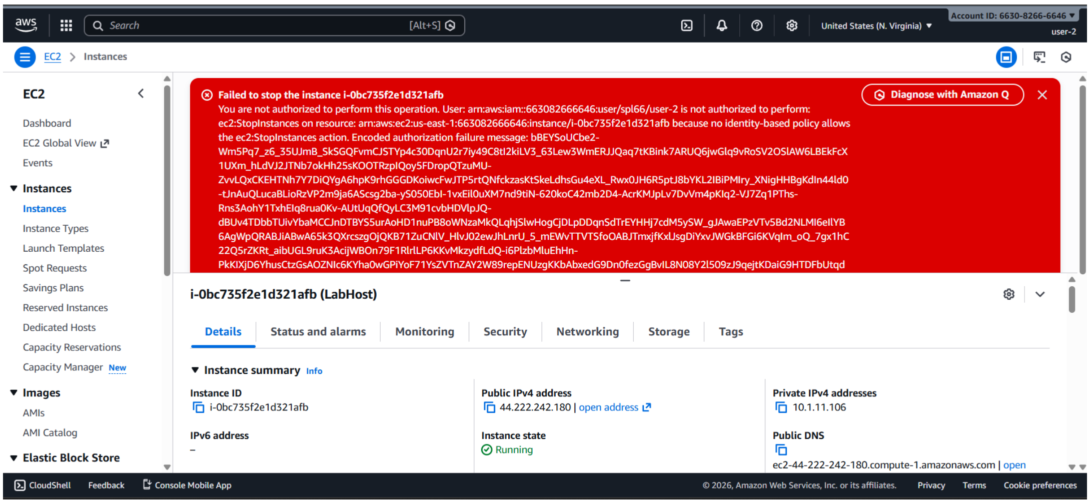
Introducing Spot Blueprints, a Real-Time Template Generator
Take advantage of Spot Blueprints to quickly generate CloudFormation and Terraform templates like Kubernetes and Apache Spark. Learn more

Save up to 90% on EC2 with Spot Instances
Optimize price-performance by combining EC2

Figure 6: user-2 logged in

user-2 ec2 stop instance attempt failed

This image captures the failed attempt by user-2 to stop an EC2 instance. The error message confirms that the read-only EC2 policy prevented the action. This demonstrates effective enforcement of permission limitations.



```
Failed to stop the instance i-0bc735f2e1d321afb
You are not authorized to perform this operation. User: arn:aws:iam::663082666646:user/spl66/user-2 is not authorized to perform:
ec2:StopInstances on resource: arn:aws:ec2:us-east-1:663082666646:instance/i-0bc735f2e1d321afb because no identity-based policy allows
the ec2:StopInstances action. Encoded authorization failure message: bBEYSoUCbe2-
Wm5Pq7_z6_35UJmB_SkSGQFvmCJSTYp4c30DqnU2r7iy49C8tI2kiLV3_63Lew3WmERJJQaq7tKBink7ARUQ6jwGlq9vRoSV2OSlAW6LBEkFcX
1UXm_hLdVJ2JTNb7okHh25sKOOTRzpIQoy5FDropQTzuMU-
ZvvLQxCKEHTNh7Y7DiQYgA6hpK9rhGGGDKoiwcFwJTP5rtQNfckzasKtSkeLdhsGu4eXL_Rwx0JH6R5ptJ8bYKL2IBiPMIry_XNigHHBgKdIn44ld0
-tJnAuQLucaBLioRzVP2m9ja6AScsg2ba-yS050EbI-1vxEil0uXM7nd9tiN-620koC42mb2D4-AcrKMJpLv7DvVm4pKIq2-VJ7Zq1PThs-
Rns3AohY1TxhEIq8rua0Kv-AUtUqQfQyLC3M91cvbHDVlpJQ-
dBUv4TDbbTUivYbaMCCJnDTBYS5urAoHD1nuPB8oWNzaMkQLqhjSlwHogCjDLpDDqnSdTrEYHHj7cdM5ySW_gJAwaEPzVTv5Bd2NLMI6eIlYB
6AgWpQRABJiABwA65k3QXrcszgOjQKB71ZuCNlV_HlvJ02ewJhLnrU_5_mEWvTTVTSfoOABJTmxjfKxlJsgDiYxvJWGkBFGi6KVqIm_oQ_7gx1hC
22Q5rZKRt_aibUGL9ruK3AcijWBOn79F1RlrlLP6KKvMkzydfLdQ-i6PlzbMluEhHn-
PkKIXjD6YhusCtzGsAOZNIc6KYha0wGPiYoF71YsZVTnZAY2W89repENUzgKKbAbxedG9Dn0fezGgBvIL8N08Y2l509zJ9qejtKDaiG9HTDFbUtqd
```

i-0bc735f2e1d321afb (LabHost)

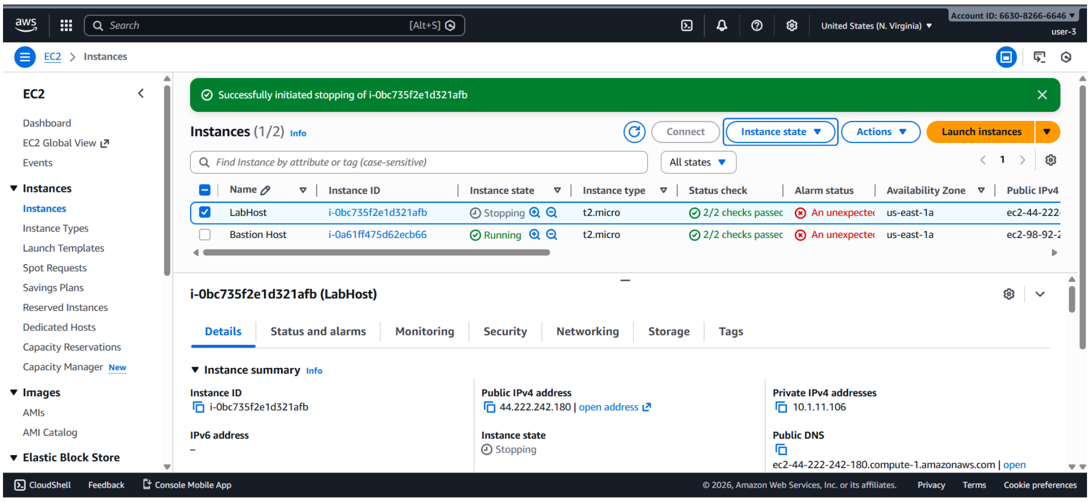
Instance summary Info

Instance ID: i-0bc735f2e1d321afb
Public IPv4 address: 44.222.242.180 | open address
Private IPv4 addresses: 10.1.11.106
IPv6 address: –
Instance state: Running
Public DNS: ec2-44-222-242-180.compute-1.amazonaws.com | open

Figure 7: user-2 ec2 stop instance attempt failed

user-3 ec2 stop instance attempt successful

This screenshot shows user-3 successfully stopping an EC2 instance. The successful action confirms that EC2 administrative permissions were correctly assigned. This validates that the EC2-Admin group allows instance management operations.



Successfully initiated stopping of i-0bc735f2e1d321afb

Instances (1/2) Info

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
☑	LabHost	i-0bc735f2e1d321afb	Stopping	t2.micro	2/2 checks passec	An unexpecte	us-east-1a	ec2-44-222-
□	Bastion Host	i-0a61ff475d62ecb66	Running	t2.micro	2/2 checks passec	An unexpecte	us-east-1a	ec2-98-92-2

i-0bc735f2e1d321afb (LabHost)

Instance summary Info

Instance ID: i-0bc735f2e1d321afb
Public IPv4 address: 44.222.242.180 | open address
Private IPv4 addresses: 10.1.11.106
IPv6 address: –
Instance state: Stopping
Public DNS: ec2-44-222-242-180.compute-1.amazonaws.com | open

Figure 8: user-3 ec2 stop instance attempt successful

Results Summary

All lab tasks were completed successfully and verified through the lab grading system. The final score achieved was **40/40**, confirming correct configuration of IAM users, groups, and permissions.

- Task 2a–2c: User-to-group assignments completed successfully
- Task 3a–3e: User login and permission testing completed successfully

Conclusion

This lab provided practical exposure to AWS Identity and Access Management and demonstrated how access to cloud resources can be securely controlled using users, groups, and policies. Assigning permissions through IAM groups simplified management and ensured adherence to the principle of least privilege. Successfully validating permissions through multiple user logins reinforced the importance of testing access controls. Overall, the lab strengthened foundational knowledge of cloud security and access management, which is essential for designing secure and scalable AWS environments.