Department of Computer Science & Engineering
Premier University.

CSE 482: Contemporary Course of Computer Science Laboratory.

Introduction to AWS Identity and Access Management (IAM): Managing User Access and Permissions.

Submitted By:

Name	**Sajjad Hosen Emon**
ID	0222310005101105
Section	C
Semester	7th
Submission Date	26/01/2026

Remarks

Objectives

The main purpose of this laboratory exercise was to develop practical understanding of AWS Identity and Access Management (IAM) by configuring and managing user permissions using groups and policies. This lab emphasized the secure implementation of role-based access control by applying the principle of least privilege, ensuring that users receive only the permissions required for their assigned responsibilities.

Through this experiment, the following AWS concepts and services were explored:

1. Creation and management of IAM users, groups, and permission policies
2. Practical application of the Principle of Least Privilege
3. Use of the IAM sign-in URL for individual user authentication
4. Verification of access permissions for Amazon S3 and Amazon EC2 services
5. Implementation of group-based permission control using JSON policy documents

Scenario

An organization is gradually increasing its dependency on Amazon Web Services to support its operational needs. Amazon EC2 is being used to handle computing workloads, while Amazon S3 serves as the primary storage solution. To ensure system security and prevent unauthorized access, permissions must be assigned strictly based on individual job responsibilities.

In this environment, three IAM users (user-1, user-2, and user-3) are pre-configured without any default permissions. Additionally, three IAM groups are available, each attached with specific access policies: S3-Support, which provides read-only access to Amazon S3; EC2-Support, which allows read-only access to Amazon EC2 resources; and EC2-Admin, which grants permission to view, start, and stop EC2 instances.

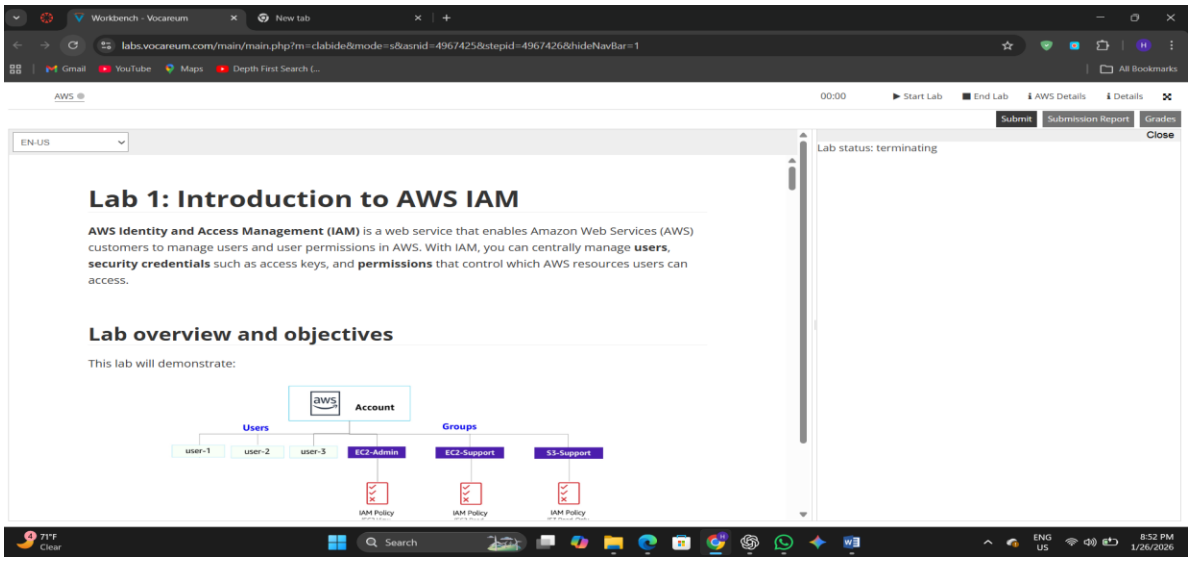
The objective is to place each user into the appropriate group and then validate the assigned permissions by signing in as each user and performing actions on Amazon S3 and Amazon EC2. Successful completion of this task confirms that users can access only the resources permitted by their assigned group, effectively demonstrating secure, role-based access control within AWS.

User	In Group	Permissions
user-1	S3-Support	Read-Only access to Amazon S3
user-2	EC2-Support	Read-Only access to Amazon EC2
user-3	EC2-Admin	View, Start and Stop Amazon EC2 instances

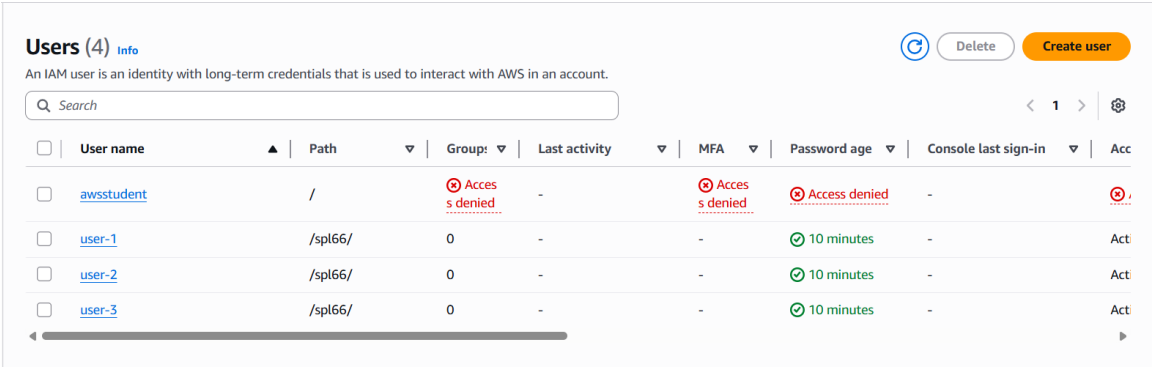
Work Procedure

1. The lab session was initiated by clicking the Start Lab option at the top of the interface.

2. The session timer was carefully monitored, and the lab was refreshed by clicking Start Lab again before the timer reached zero to avoid session expiration.
3. The lab environment was considered ready once the indicator next to the AWS link turned green.
4. The AWS Management Console was opened by clicking the provided AWS link located at the upper-left corner. Browser pop-ups were enabled when necessary.
5. For better navigation, the AWS Console tab was arranged side-by-side with the lab instructions.

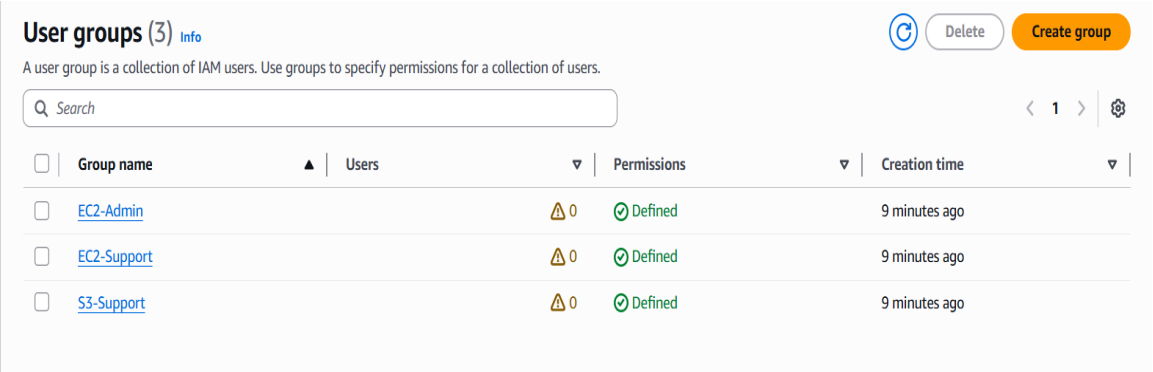


6. Within the AWS Console, the search bar located to the right of the Services menu was used.
7. The keyword IAM was entered in the search box, and the IAM service was selected to access the IAM console.
8. From the left navigation panel, the Users option was selected.
9. The list of pre-created IAM users was observed, which included:
   a) user-1
   b) user-2
   c) user-3



10. The summary page of user-1 was opened, and the Groups tab was selected to verify group membership.
    a) It was confirmed that user-1 was not assigned to any group at this stage.
11. The Security credentials tab was then accessed to review authentication settings.
    a) It was verified that a console login password had been assigned to user-1.

12. From the left navigation panel, the User groups option was selected.
13. The available IAM groups were displayed as follows:
    a) EC2-Admin
    b) EC2-Support
    c) S3-Support



Business Scenario

For the remaining part of this laboratory exercise, the focus was placed on configuring IAM users and groups to support a realistic business environment. The organization is increasingly utilizing Amazon Web Services, with extensive use of Amazon EC2 instances for computing operations and Amazon S3 for data storage. To maintain security and proper access control, permissions must be assigned to employees strictly based on their job roles.

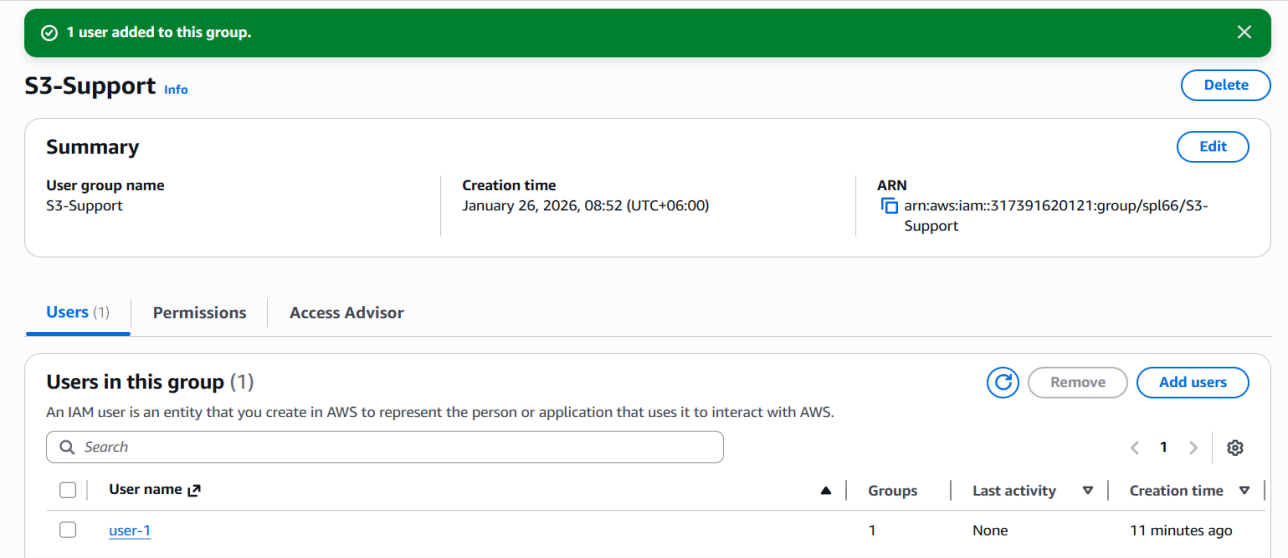
To achieve this, specific group-based access permissions were defined as follows:

User	Assigned Group	Permissions
user-1	S3-Support	Read-only access to Amazon S3
user-2	EC2-Support	Read-only access to Amazon EC2
user-3	EC2-Admin	Permission to view, start, and stop Amazon EC2 instances

Task 1: Assign user-1 to the S3-Support Group

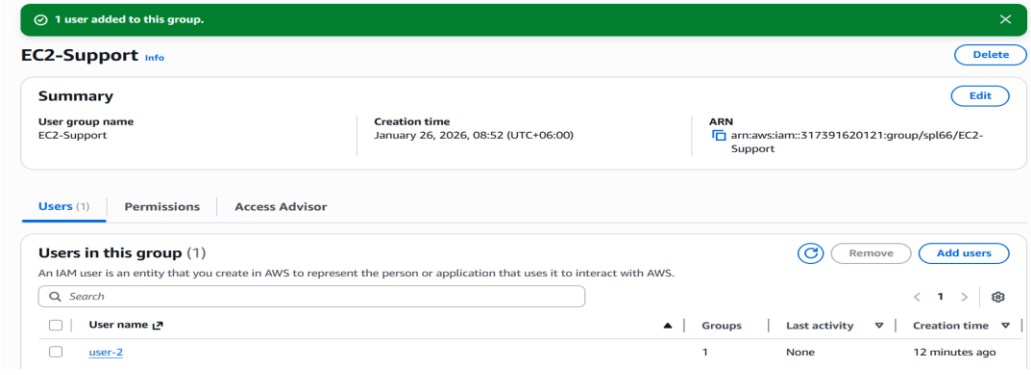
1. From the left navigation panel of the IAM console, the User groups option was selected.
2. The S3-Support group was opened by clicking its name.
3. The Users tab was accessed to manage group members.
4. The Add users option was selected.
5. In the *Add users to S3-Support* window:
   a) user-1 was selected from the user list.
   b) The Add users button was clicked to complete the assignment.

6. The Users tab was reviewed to confirm that user-1 had been successfully added to the S3-Support group.



Task 2: Assign user-2 to the EC2-Support Group

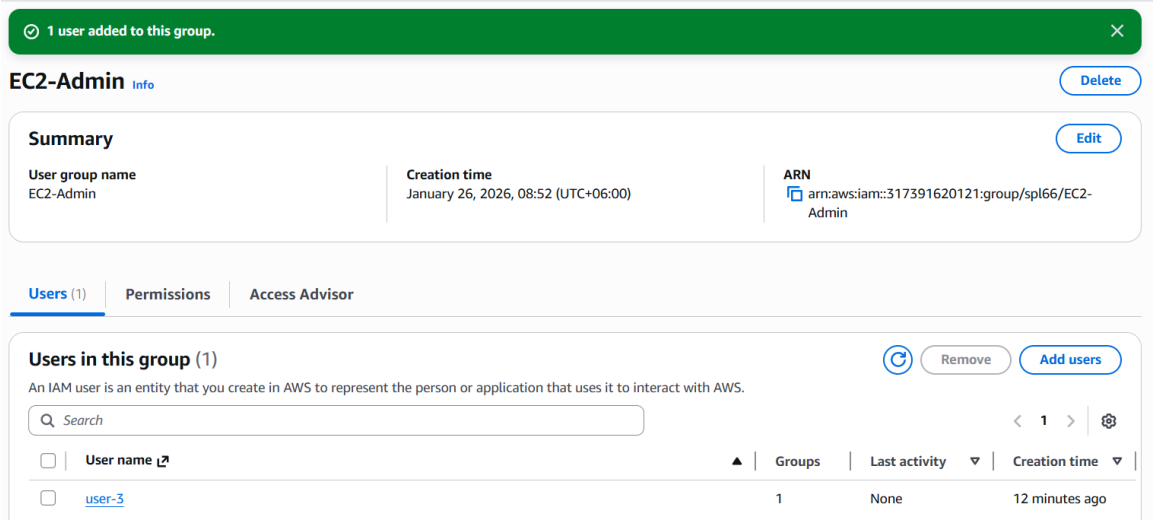
1. The User groups section was accessed from the left navigation panel.
2. The EC2-Support group was selected.
3. The Users tab was opened.
4. The Add users option was chosen.
5. In the *Add users to EC2-Support* window:
   a) user-2 was selected.
   b) The Add users button was clicked to confirm the selection.
6. Verification was performed in the Users tab to ensure that user-2 was now a member of the EC2-Support group.



Task 3: Assign user-3 to the EC2-Admin Group

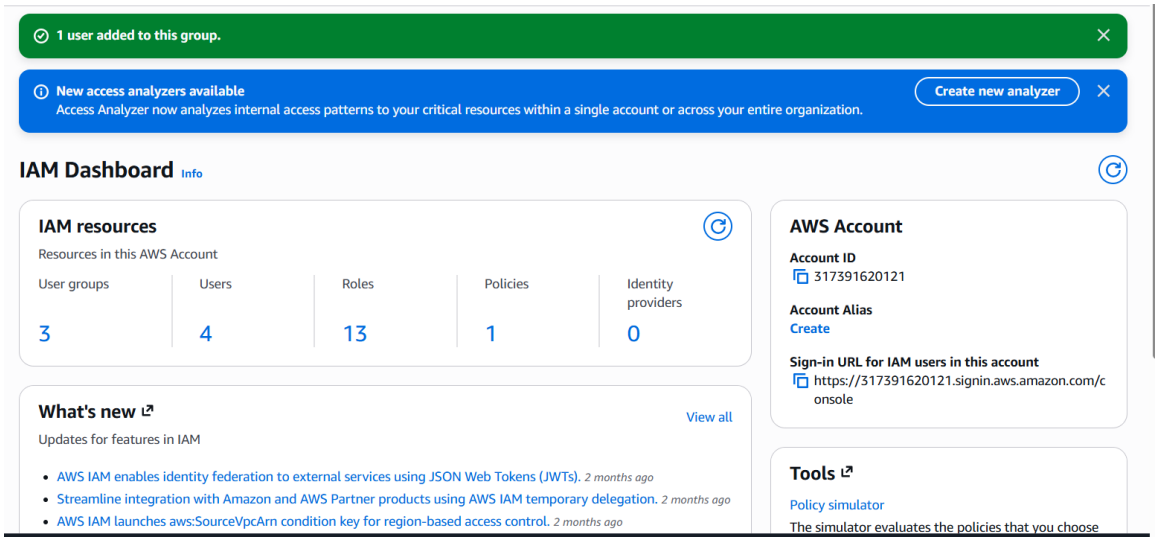
1. From the IAM console, the User groups option was selected.

2. The EC2-Admin group was opened.
3. The Users tab was accessed.
4. The Add users option was selected.
5. In the *Add users to EC2-Admin* window:
   a) user-3 was selected from the list.
   b) The Add users button was clicked to finalize the assignment.
6. The Users tab was checked to confirm that user-3 had been successfully added to the EC2-Admin group.
7. After verification, the interface was returned to the User groups list.



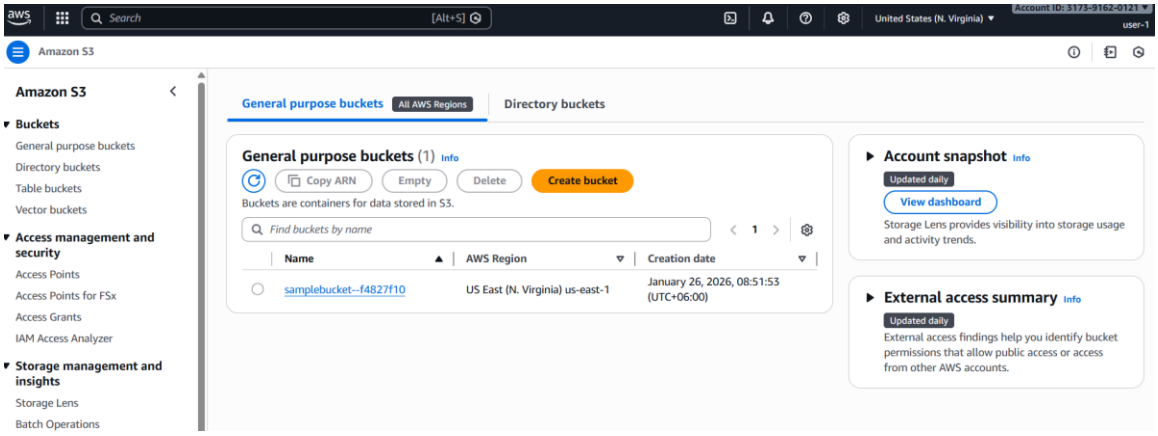
Task 4: Verifying User Access via IAM Sign-in URL

1. From the IAM console, the Dashboard option was selected from the left navigation panel.
2. On the right side of the dashboard, the IAM user sign-in URL was copied: https://317391620121.signin.aws.amazon.com/console



3. The copied URL was pasted into a text editor for temporary reference.

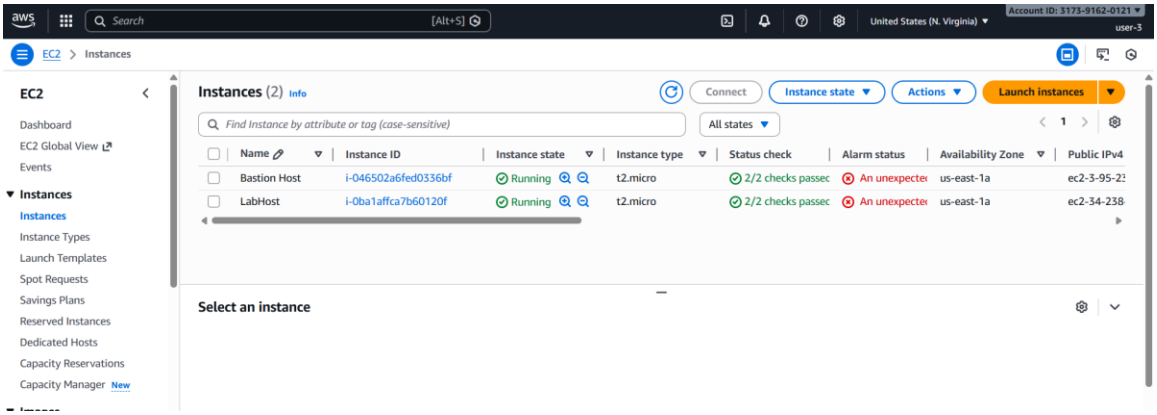
4. A private or incognito browser window was opened based on the browser in use:
   a) Firefox → Menu bar → *New Private Window*
   b) Chrome → Three dots (⋮) → *New Incognito Window*
   c) Microsoft Edge → Three dots (⋮) → *New InPrivate Window*
   d) Internet Explorer → Tools → *InPrivate Browsing*
5. The IAM sign-in URL was then pasted into the address bar of the private/incognito window and loaded by pressing Enter.
6. The system was logged in using the following credentials:
   a) IAM user name: user-1
   b) Password: Lab-Password1



7. After successful login, Amazon S3 was searched from the AWS service search bar and the S3 console was opened.
8. The existing S3 bucket was selected and its contents were reviewed.
   a) It was confirmed that user-1 could view the bucket and its contents, as the user belongs to the S3-Support group.
   b) It was observed that the bucket did not contain any objects.
9. Next, Amazon EC2 was searched and the EC2 console was opened to verify EC2 access.
   a) This step was performed to test whether user-1 had permission to access EC2 services.
10. From the EC2 console, the Instances option was selected from the left navigation panel.
    a) A system message appeared stating: "You are not authorized to perform this operation."
    b) This result confirmed that user-1 does not have any permissions to access Amazon EC2 resources, which aligns with the assigned S3-Support role.
11. After completing the access verification, the user was signed out of the AWS Management Console:
    a) The user-1 account name was selected from the top-right corner of the console.
    b) The Sign Out option was chosen to safely end the session.

Task 5: Sign in as user-2 and Verify Access Permissions

1. The IAM user sign-in URL was pasted into the address bar of the private/incognito browser window and loaded by pressing Enter.
2. The system was logged in using the following credentials:
   - IAM user name: user-2
   - Password: Lab-Password2
3. After successful login, Amazon EC2 was searched from the AWS service search bar and the EC2 console was opened.
4. From the left navigation panel, the Instances option was selected.
   - The available EC2 instance was visible, indicating read-only access.
   - If no instance was displayed, the Region selector at the top-right corner was checked and adjusted to the appropriate region (for example, N. Virginia).



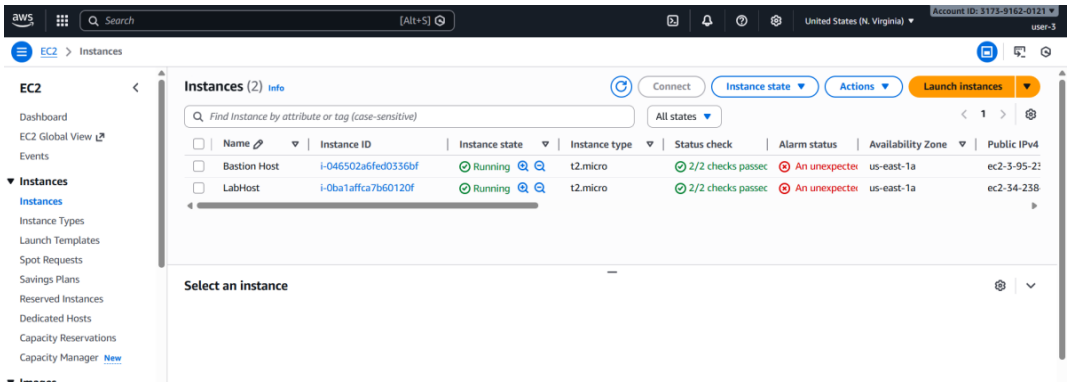
5. The EC2 instance named LabHost was selected.
   - An attempt was made to stop the instance; however, an error message appeared stating "You are not authorized to perform this operation."
   - The error message was closed by clicking the X icon.
   - This behavior confirmed that user-2 has view-only permissions for Amazon EC2.
6. Next, Amazon S3 was searched and the S3 console was opened.
   - A message was displayed indicating "You don't have permissions to list buckets."
   - This confirmed that user-2 does not have any permissions for Amazon S3.
7. After completing the permission verification, the user was signed out of the AWS Management Console:
   - The user-2 account name was selected from the top-right corner.
   - The Sign Out option was chosen to end the session.

Task 6: Sign in as user-3 (EC2 Administrator) and Stop an EC2 Instance

1. The IAM user sign-in URL was pasted into the address bar of the private/incognito browser window and opened by pressing Enter.

- If the URL was not available in the clipboard, it was retrieved from the previously saved text editor.

2. The system was logged in using the following credentials:
   - IAM user name: user-3
   - Password: Lab-Password3
3. After successful authentication, Amazon EC2 was searched from the AWS service search bar and the EC2 console was opened.
4. From the left navigation panel, the Instances option was selected.
5. The EC2 instance named LabHost was chosen.
   - If the instance was not visible, the Region selector in the top-right corner was checked and set to the appropriate region (for example, N. Virginia).
6. From the Instance state menu, the Stop instance option was selected.
7. In the Stop Instance confirmation window, the Stop button was clicked.
   - The instance transitioned into the stopping state and was successfully shut down.



8. After completing the task, the private/incognito browser window was closed.
9. The lab was then submitted through the lab interface.
10. A successful submission confirmation message was displayed after the report submission.
11.

Submission Report

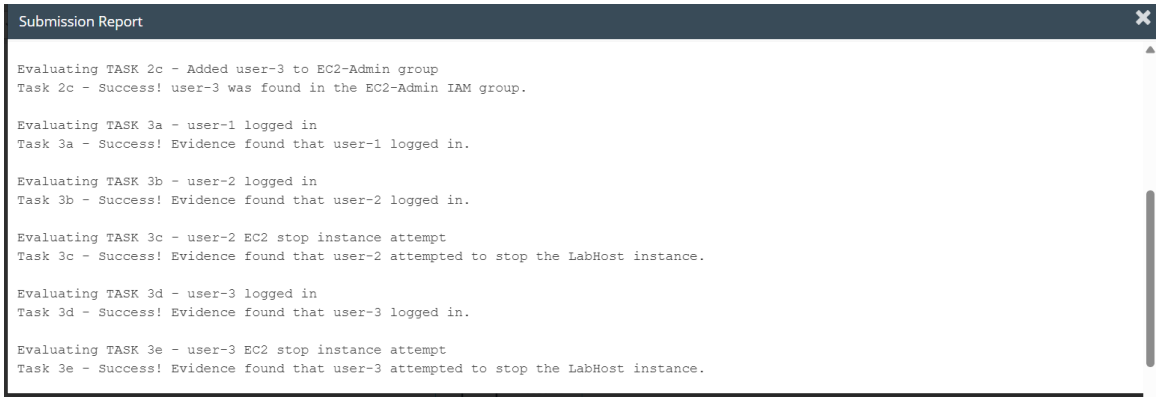
```
[Executed at: Mon Jan 19 1:30:38 PST 2026]

gradeFile = /mnt/vocwork5/grader/eee_G_2692329/asn4967425_1/asn4967426_1/tmp/temp_uf_01192026/.vn75jmr0r8omffRylsk
reportFile =/mnt/vocwork5/grader/eee_G_2692329/asn4967425_1/asn4967426_1/tmp/temp_uf_01192026/.5om0t1uv2hed9hAWZEA
/mnt/vocwork5/grader/eee_G_2692329/asn4967425_1/asn4967426_1/tmp/temp_uf_01192026/.vn75jmr0r8omffRylsk
Started: 2026-01-19 01:30:29
region: us-east-1
profile: default

Evaluating TASK 2a - Added user-1 to S3-Support group
Task 2a - Success! user-1 was found in the S3-Support IAM group.

Evaluating TASK 2b - Added user-2 to EC2-Support group
Task 2b - Success! user-2 was found in the EC2-Support IAM group.

Evaluating TASK 2c - Added user-3 to EC2-Admin group
Task 2c - Success! user-3 was found in the EC2-Admin IAM group.
```



12. Total Score

Total score	40/40
TASK 2a - Added user-1 to S3-Support group	5/5
TASK 2b - Added user-2 to EC2-Support group	5/5
TASK 2c - Added user-3 to EC2-Admin group	5/5
TASK 3a - user-1 logged in	5/5
TASK 3b - user-2 logged in	5/5
TASK 3c - user-2 ec2 stop instance attempt	5/5
TASK 3d - user-3 logged in	5/5
TASK 3e - user-3 EC2 stop instance attempt	5/5

13. Finally, the lab session was closed.

Conclusion

In this lab, we learned how AWS Identity and Access Management (IAM) helps control access to different cloud resources in a secure way. At the beginning, the pre-created IAM users and groups were reviewed, and it was observed that users had no permissions until they were assigned to specific groups. When user-1 was added to the S3-Support group, the user was able to view Amazon S3 buckets. Similarly, user-2 received read-only access to Amazon EC2 by being added to the EC2-Support group. On the other hand, user-3, as a member of the EC2-Admin group, was able to manage EC2 instances by viewing, starting, and stopping them.

Throughout the lab, we also practiced signing in using the IAM user sign-in URL and tested permissions in private browser sessions. This helped us clearly understand how IAM policies control what actions a user can or cannot perform. Overall, this lab showed how group-based access control makes cloud environments more secure by giving each user only the access they need. The experience closely reflects real-world scenarios where proper permission management is essential for balancing usability and security in cloud systems.