

AWS Identity and Access Management (IAM)

1. Introduction

AWS Identity and Access Management (IAM) is a critical security service in AWS that allows organizations to control access to AWS resources securely. With IAM, administrators can create users, groups, policies, and roles, assigning permissions based on the principle of least privilege, ensuring users can only access what is necessary for their job.

In this lab, we explored pre-created IAM users and groups, examined the attached managed and inline policies, assigned users to groups according to job roles, and tested their access through the IAM sign-in URL. This provides hands-on understanding of how IAM manages secure access in real AWS environments.

2. Lab Objectives

- To understand IAM user and group management.
- To explore managed and inline IAM policies.
- To assign users to appropriate groups based on business roles.
- To verify access restrictions through real-time testing using login URLs.
- To observe how permission boundaries affect AWS service access.

3. AWS IAM Key Concepts (Explanation)

a) IAM Users: IAM Users represent individual identities that can authenticate into AWS using passwords or access keys.

b) IAM Groups: IAM Groups are collections of users, allowing permissions to be assigned collectively instead of individually.

c) IAM Policies: Policies contain permission rules in JSON format which define:

- **Effect** – Allow or Deny
- **Action** – What operations are permitted (example: s3>ListBucket)
- **Resource** – Which AWS resource(s) the policy applies to (* or ARN)

Policies are of two types:

- **Managed Policy** – Prebuilt by AWS or admins, reusable across users and groups.
- **Inline Policy** – Attached directly to a single user/group for unique permission use cases.

d) IAM Roles: A temporary access identity used by services, applications, or federated users (not used in this lab but important conceptually).

4. Business Scenario Summary

User	Assigned Group	Permissions Access
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, Stop Amazon EC2 instances

5. Task-Wise Lab Explanation

Task 1: Explore Users and Groups

- Open IAM from AWS console.
- Observed three pre-created users: user-1, user-2, user-3.

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age
user-1	/spl66/	0	-	-	15 minutes	-	Active - AKIAZUCNU5Z...	15 minutes
user-2	/spl66/	0	-	-	15 minutes	-	Active - AKIAZUCNU5Z...	15 minutes
user-3	/spl66/	0	-	-	15 minutes	-	Active - AKIAZUCNU5Z...	15 minutes

- Verified that user-1 initially had no permissions and no group membership.
- Observed pre-created groups: EC2-Admin, EC2-Support, S3-Support.

Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	16 minutes ago
EC2-Support	0	Defined	16 minutes ago
S3-Support	0	Defined	16 minutes ago

Checked permissions for each group:

- EC2-Support → AmazonEC2ReadOnlyAccess (Managed Policy)
- S3-Support → AmazonS3ReadOnlyAccess (Managed Policy)
- EC2-Admin → Inline Policy allowing Describe, Start, Stop EC2 instances

Task 2: Add Users to Groups

Based on business requirements:

- Added user-1 to S3-Support

S3-Support

Summary

User group name: S3-Support

Creation time: November 18, 2025, 13:51 (UTC+05:30)

ARN: arn:aws:iam::661587816049:group/spl66/S3-Support

Users | Permissions | Access Advisor

Users in this group (0)

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
No resources to display

Groups | Last activity | Creation time

Add users

Remove

Delete

Edit

1 user added to this group.

S3-Support

Summary

User group name: S3-Support

Creation time: November 18, 2025, 13:51 (UTC+05:30)

ARN: arn:aws:iam::661587816049:group/spl66/S3-Support

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
user-1

Groups | Last activity | Creation time

Add users

Remove

Delete

Edit

- Added user-2 to EC2-Support

EC2-Support

Summary

User group name: EC2-Support

Creation time: November 18, 2025, 13:51 (UTC+05:30)

ARN: arn:aws:iam::661587816049:group/spl66/EC2-Support

Users | Permissions | Access Advisor

Users in this group (0)

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
No resources to display

Groups | Last activity | Creation time

Add users

Remove

Delete

Edit

The screenshot shows the AWS IAM User Groups page for the 'EC2-Support' group. The summary section indicates that one user has been added to the group. The 'Users' tab shows a single user named 'user-2'. The ARN of the group is listed as arn:aws:iam::661587816049:group/spl66/EC2-Support.

- Added user-3 to EC2-Admin

The screenshot shows the AWS IAM User Groups page for the 'EC2-Admin' group. The summary section indicates that no users have been added to the group. The 'Users' tab shows a search bar and a note stating 'No resources to display'. The ARN of the group is listed as arn:aws:iam::661587816049:group/spl66/EC2-Admin.

The screenshot shows the AWS IAM User Groups page for the 'EC2-Admin' group again. This time, it displays a message indicating that one user has been added to the group. The 'Users' tab shows a single user named 'user-3'. The ARN of the group is listed as arn:aws:iam::661587816049:group/spl66/EC2-Admin.

Finally verified that each group displayed 1 assigned user.

Task 3: Sign-In and Permissions Testing

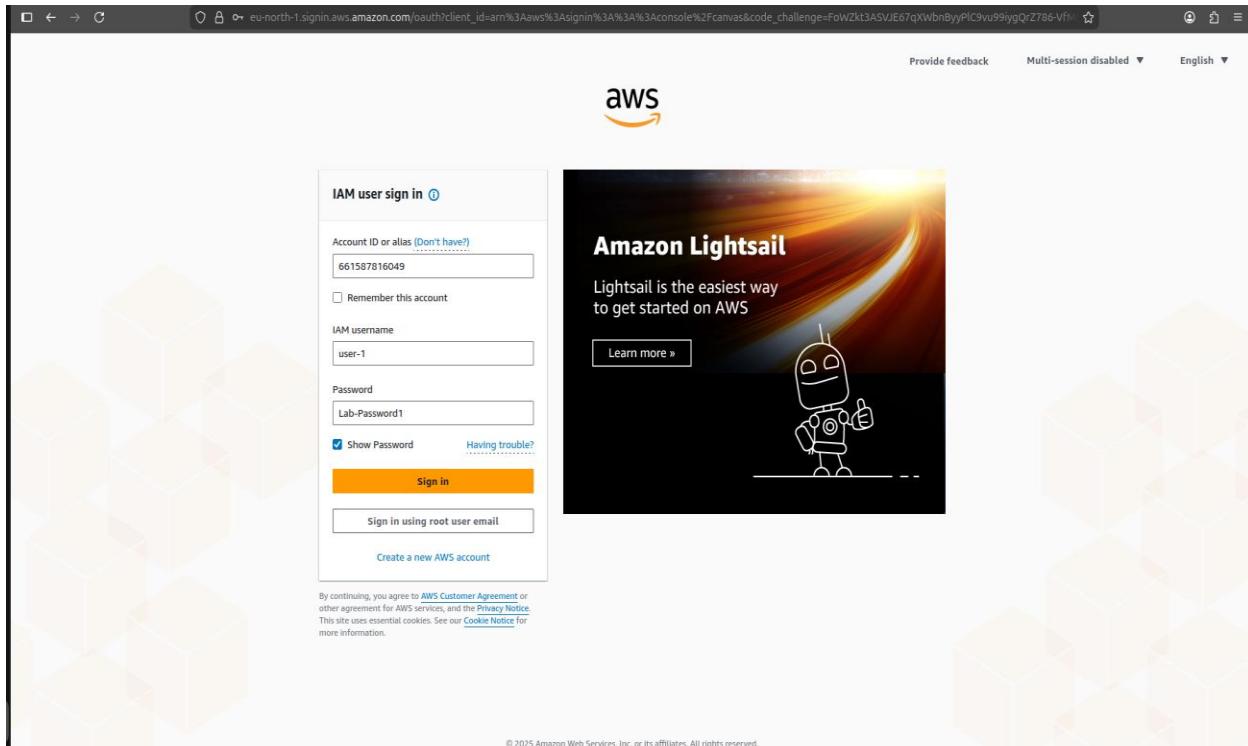
- In the navigation pane on the left, choose the Dashboard. On the right side, a Sign-in URL for IAM users in this account is displayed. The sign-in link shown in the lab environment was: <https://661587816049.signin.aws.amazon.com/console>

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with navigation links like 'Identity and Access Management (IAM)', 'Access management', 'Access reports', and 'AWS Organizations'. The main area has a 'IAM Dashboard' card with statistics: 3 User groups, 4 Users, 13 Roles, 1 Policies, and 0 Identity providers. Below it is a 'What's new' section with a list of recent changes. To the right, there's an 'AWS Account' summary with the Account ID (661587816049) and a 'Sign-in URL for IAM users in this account' link: <https://661587816049.signin.aws.amazon.com/console>. There are also sections for 'Tools' (Policy simulator) and 'Additional information' (Security best practices in IAM).

- This link can be used to sign-in to the AWS Account you are currently using. Copy the Sign-in URL for IAM users in this account to a text editor. Open a private (Incognito) window.

The screenshot shows a Firefox browser window with a dark theme. The address bar shows the URL: <https://661587816049.signin.aws.amazon.com/console>. A modal window titled 'Next-level privacy on mobile' is open, featuring an image of a smartphone and the text: 'Firefox Focus clears your history every time while blocking ads and trackers.' It includes a 'Download Firefox Focus' button. Below the modal, there's a note: 'Firefox clears your search and browsing history when you close all private windows, but this doesn't make you anonymous.' with a 'Learn more' link.

Logged in as user-1



Successfully accessed S3 and viewed bucket list (read-only)

Amazon S3

General purpose buckets [All AWS Regions](#) | Directory buckets

General purpose buckets (1/1) [Info](#)

Buckets are containers for data stored in S3.

Name	AWS Region	Creation date
samplebucket--7a82d9c0	US East (N. Virginia) us-east-1	November 18, 2025, 13:50:51 (UTC+05:50)

[Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

Account snapshot [Info](#)

Updated daily

Storage Lens provides visibility into storage usage and activity trends.

External access summary - new [Info](#)

Updated daily

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

Amazon S3

- General purpose buckets
- Directory buckets
- Table buckets
- Vector buckets
- Access Grants
- Access Points (General Purpose Buckets, FSx file systems)
- Access Points (Directory Buckets)
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight: [11](#)

AWS Marketplace for S3

Tried accessing EC2 but received "not authorized" error

Screenshot of the AWS EC2 Instances page. The URL is us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances. The account ID is 6615-8781-6049, and the region is United States (N. Virginia). The user is 'user-1'. A red box highlights an error message: 'You are not authorized to perform this operation. User: arn:aws:iam::661587816049:user/spl66/user-1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action'. The left sidebar shows navigation links for EC2, Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Capacity Manager, Images, AMIs, AM Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security, Security Groups, Elastic IPs, Placement Groups, and Key Pairs.

Logged in as user-2

Screenshot of the AWS IAM user sign-in page. The URL is eu-north-1.sigin.aws.amazon.com/auth/client_id-arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=F6mdsXbbNXJmbdjWDaSoKSGQkdxgHzmo-ydellA. The page includes a 'Provide feedback' link, 'Multi-session disabled' indicator, and an 'English' language dropdown. The main form fields are: Account ID or alias (661587816049), Remember this account (unchecked), IAM username (user-2), Password (Lab-Password2), Show Password (checked), Having trouble? (link), Sign in (button), and Sign in using root user email (link). Below the form is a note about AWS Customer Agreement and Privacy Notice, and a link to the Cookie Notice. To the right is an advertisement for Amazon Lightsail with the text 'Lightsail is the easiest way to get started on AWS' and a 'Learn more' button. The bottom of the page shows a copyright notice for 2025 Amazon Web Services, Inc. and a transfer status bar: 'Transferring data from eu-north-1.sigin.aws.amazon.com...'.

Successfully viewed EC2 instance (read-only)

Instances (2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
LabHost	i-0678558a9257a3d57	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-100-24-119-163.co...	100.24.119.163	-
Bastion Host	i-071650efde8907a8a	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-44-200-160-192.co...	44.200.160.192	-

Select an instance

Attempted to stop EC2 instance but got permission denied

Instances (1/2) Info

Name	Instance ID	Public IPv4 address	Private IPv4 addresses
i-0678558a9257a3d57 (LabHost)	i-0678558a9257a3d57	100.24.119.163 open address	10.1.11.152

Details **Status and alarms** **Monitoring** **Security** **Networking** **Storage** **Tags**

Instance summary

Instance ID	Public IPv4 address
i-0678558a9257a3d57	100.24.119.163 open address
IPv6 address	Instance state
-	Running
Hostname type	Private IP DNS name (IPv4 only)
IP name: ip-10-1-11-152.ec2.internal	ip-10-1-11-152.ec2.internal
Answer private resource DNS name	Instance type
-	t2.micro
	Private IPv4 addresses
	Public DNS
	EC2 instance
	Elastic IP addresses
	-

Tried accessing S3 but was denied

Screenshot of the AWS S3 Bucket creation page:

The URL is us-east-1.console.aws.amazon.com/s3/bucket/create?region=us-east-1

Default encryption (Info): Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type (Info): Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the Storage tab of the [Amazon S3 pricing page](#).

- Server-side encryption with Amazon S3 managed keys (SSE-S3)
- Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Bucket Key: Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

- Disable
- Enable

Advanced settings

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Failed to create bucket: To create a bucket, the `s3:CreateBucket` permission is required. [View your permissions](#) in the [IAM console](#). [Identity and Access Management in Amazon S3](#)

[Diagnose with Amazon Q](#)

[Cancel](#) [Create bucket](#)

Logged in as user-3

Screenshot of the IAM user sign-in page:

The URL is eu-north-1.sigin.aws.amazon.com/auth/client_id=arn%3aws%3asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=J0t65dxdmU9gfEhaZ3wsdVjDYLZGe8OHQsglm

IAM user sign in

Account ID or alias (Don't have?):

Remember this account

IAM username:

Password:

Show Password [Having trouble?](#)

[Sign in](#)

[Sign in using root user email](#)

[Create a new AWS account](#)

By continuing, you agree to [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

Provide feedback Multi-session disabled English

Amazon Lightsail: Lightsail is the easiest way to get started on AWS. [Learn more](#)

© 2025 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Accessed EC2 and successfully stopped the LabHost instance

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with sections like EC2, Dashboard, EC2 Global View, Events, Instances, Images, Elastic Block Store, Network & Security, and Key Pairs. The main area displays two instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 IP	Elastic IP
LabHost	i-0678558a9257a3d57	Stopping	t2.micro	2/2 checks passed	User: arn:aws:	us-east-1a	ec2-100-24-119-163.co...	100.24.119.163	-
Bastion Host	i-071650eefed8907a8a	Running	t2.micro	2/2 checks passed	User: arn:aws:	us-east-1a	ec2-44-200-160-192.co...	44.200.160.192	-

A green banner at the top says "Successfully initiated stopping of i-0678558a9257a3d57". Below the table, there's a detailed view for the LabHost instance:

i-0678558a9257a3d57 (LabHost)

Details (selected) | Status and alarms | Monitoring | Security | Networking | Storage | Tags

Instance summary

Instance ID	I-0678558a9257a3d57	Public IPv4 address	100.24.119.163 open address
IPv6 address	-	Instance state	Stopping
Hostname type	IP name: ip-10-1-11-152.ec2.internal	Private IP DNS name (IPv4 only)	ip-10-1-11-152.ec2.internal
Answer private resource DNS name	-	Instance type	t2.micro
		Private IPv4 addresses	10.1.11.152
		Public DNS	ec2-100-24-119-163.compute-1.amazonaws.com open address
		Elastic IP addresses	-

Permissions worked as per admin role design

6. Conclusion

Through this lab, we successfully learned how IAM enables secure access control in AWS environments. We explored and analyzed IAM users, groups, and policies, assigned users to groups based on job roles, and verified permission restrictions by testing actions in AWS Management Console.

This demonstrates how IAM enforces secure, role-based access, ensuring every individual has only the required level of access, maintaining security and operational integrity.