

ACTIVITY 1 – IAM Users & Authentication

Objective

Understand IAM users and authentication mechanisms.

Tasks

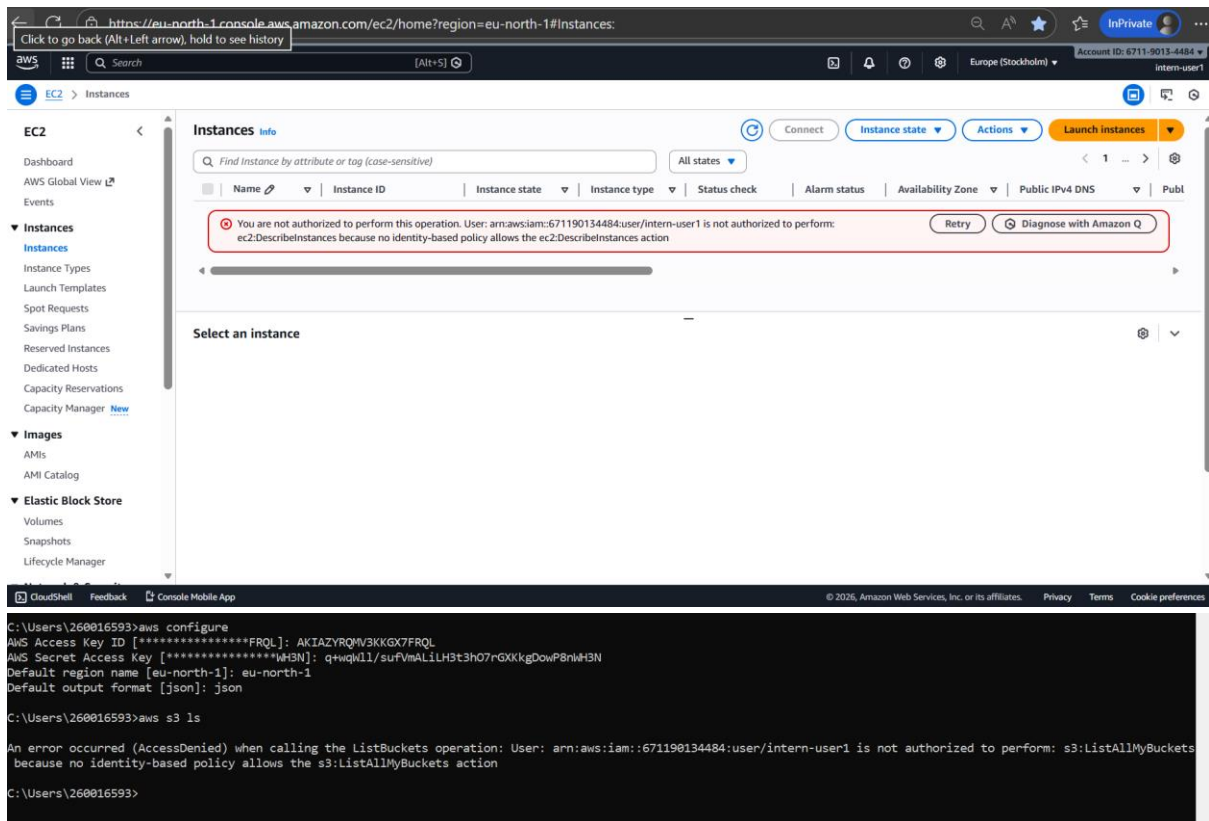
1. Create an IAM user named: intern-user1
2. Enable **AWS Management Console access**
3. Set a **custom password**
4. Log in using the IAM user and verify:
 - You cannot access S3
 - You cannot access EC2

Expected Outcome

- User exists
- Login works
- Everything shows **Access Denied**

The screenshot displays the AWS IAM console interface. The top navigation bar shows the user 'Harsh Gupta (6711-9013-4484)'. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access Management, User groups, Roles, Policies, Identity providers, Account settings, Root access management, and Temporary delegation requests. The main content area shows the details for the user 'intern-user1'. The 'Summary' section includes the ARN 'arn:aws:iam::671190134484:user/intern-user1', console access status 'Enabled without MFA', and two access keys. The 'Security credentials' tab is selected, showing the 'Console sign-in' section with a 'Console sign-in link' and a 'Console password' that was updated 7 minutes ago. The 'Last console sign-in' was 4 minutes ago.

Permissions	Groups	Tags (1)	Security credentials	Last Accessed
Console sign-in				
Console sign-in link				
https://671190134484.signin.aws.amazon.com/console				
Console password				
Updated 7 minutes ago (2026-01-27 18:55 GMT+5:30)				
Last console sign-in				
4 minutes ago (2026-01-27 18:58 GMT+5:30)				



ACTIVITY 2 – IAM Groups & Permission Inheritance

Objective

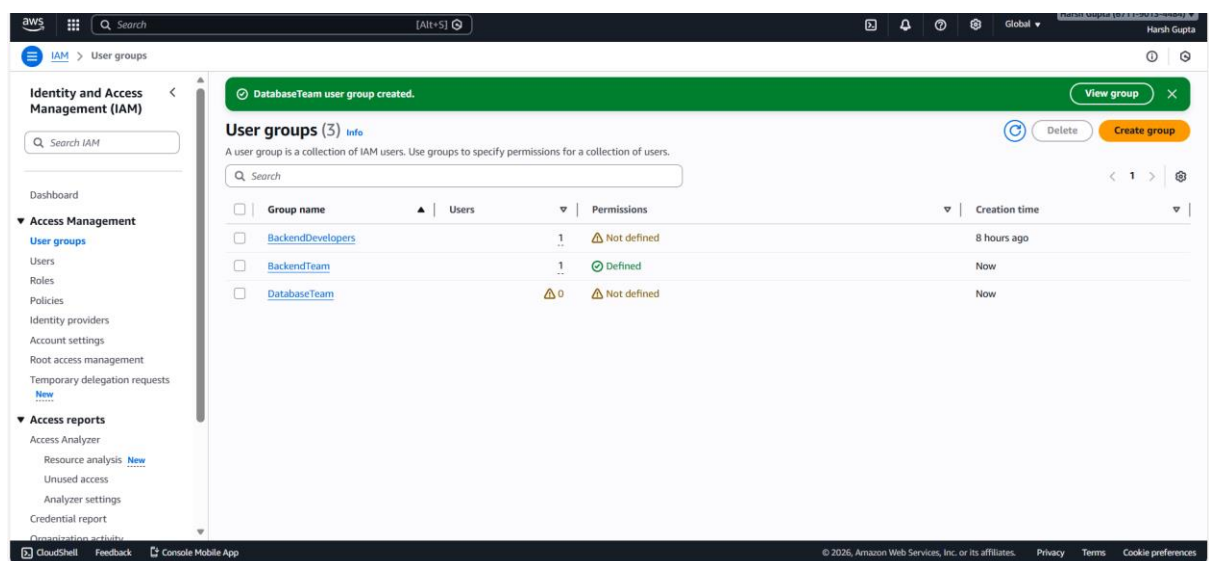
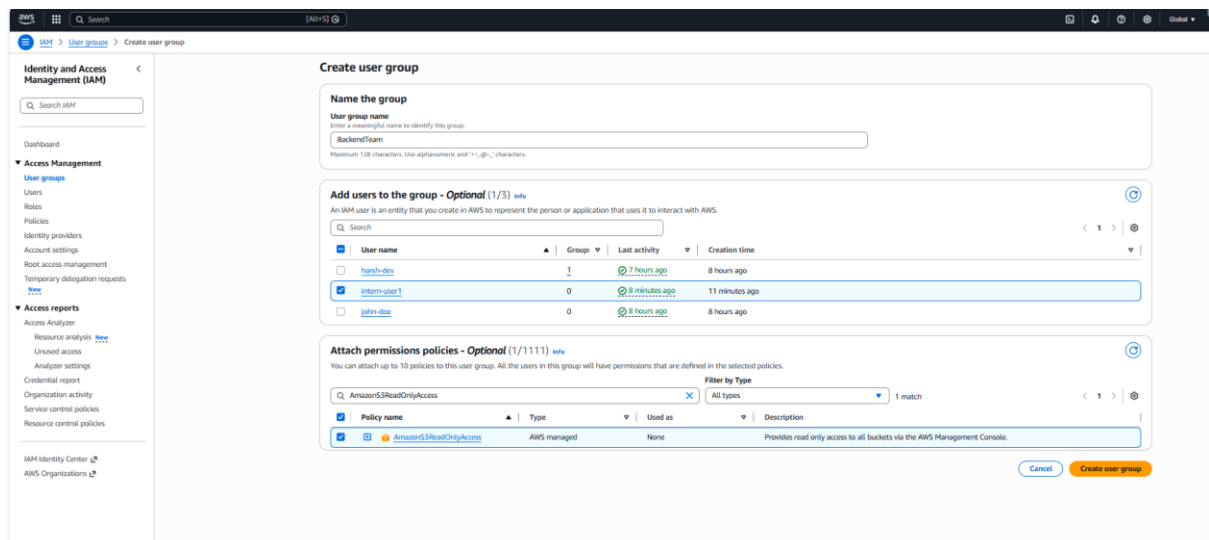
Understand why groups exist and how permissions flow.

Tasks

1. Create two IAM groups:
BackendTeam
DatabaseTeam
2. Add intern-user1 to **BackendTeam**
3. Attach AWS managed policy:
 - AmazonS3ReadOnlyAccess to BackendTeam
4. Login as intern-user1 and:
 - List S3 buckets (should work)
 - Upload file (should fail)

Questions to Answer

- Why upload is denied?
- Where did the permission come from?



```
C:\Users\260016593>aws s3 ls
2026-01-27 11:26:24 harsh-backend-s3

C:\Users\260016593>
```

```
C:\Users\260016593>echo "Hi , Harsh" > welcome.txt
C:\Users\260016593>aws s3 cp welcome.txt s3://harsh-backend-s3/
upload failed: .\welcome.txt to s3://harsh-backend-s3/welcome.txt An error occurred (AccessDenied) when calling the PutObject operation: User: arn:aws:iam::671190134484:user/intern-user1 is not authorized to perform: s3:PutObject on resource: "arn:aws:s3:::harsh-backend-s3/welcome.txt" because no identity-based policy allows the s3:PutObject action
```

Questions to Answer

● Why upload is denied?

- The upload is denied because the AmazonS3ReadOnlyAccess policy only grants read-only permissions for S3 resources. This means intern-user1 can perform actions like:

ListBucket to see all buckets and GetObject to download objects

But write operations such as PutObject (uploading files) are not included in this policy.

● Where did the permission come from?

We attached policy attached to BackendTeam group (AmazonS3ReadOnlyAccess). So intern-user1 is a member of BackendTeam and it inherits all policies attached to that group. Therefore, intern-user1's effective permissions are exactly what BackendTeam has ie, read-only access to S3.

ACTIVITY 3 – Custom Policy Using Visual Editor

Objective

Create a **least-privilege custom policy**

Scenario

Backend team needs:

- Read & write objects in **one specific S3 bucket**
- No delete permission

Tasks

1. Create a policy using **Visual Editor**
2. Service: **S3**
3. Allow:
 - GetObject
 - PutObject
 - ListBucket
4. Restrict access to:
my-backend-bucket
5. Attach policy to **BackendTeam**
6. Test:
 - Upload file → allowed
 - Delete file → denied

BackendTeam Summary

- User group name: BackendTeam
- Creation time: January 27, 2026, 19:07 (UTC+05:30)
- ARN: arn:aws:iam::671190134484:group/BackendTeam

Permissions policies (2)

Policy name	Type	Attached entities
AmazonS3ReadOnlyAccess	AWS managed	1
BackendTeamS3Access	Customer managed	1

BackendTeamS3Access Policy details

- Type: Customer managed
- Creation time: January 27, 2026, 19:37 (UTC+05:30)
- Edited time: January 27, 2026, 19:52 (UTC+05:30)
- ARN: arn:aws:iam::671190134484:policy/BackendTeamS3Access

Permissions defined in this policy

```

1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Sid": "VisualEditor0",
6-       "Effect": "Allow",
7-       "Action": [
8-         "s3:PutObject",
9-         "s3:ListBucket",
10-      ],
11-       "Resource": [
12-         "arn:aws:s3:::harsh-backend-bucket",
13-         "arn:aws:s3:::harsh-backend-bucket/*"
14-       ]
15-     }
16-   ]
17- }
18-

```

Terminal Output:

```

C:\Users\260016593>aws s3 cp welcome.txt s3://harsh-backend-bucket/
upload: .\welcome.txt to s3://harsh-backend-bucket/welcome.txt

C:\Users\260016593>aws s3 rm s3://harsh-backend-bucket/welcome.txt
delete failed: s3://harsh-backend-bucket/welcome.txt An error occurred (AccessDenied) when calling the DeleteObject operation: User: arn:aws:iam::671190134484:user/intern-user1 is not authorized to perform: s3:DeleteObject on resource: "arn:aws:s3:::harsh-backend-bucket/welcome.txt" because no identity-based policy allows the s3:DeleteObject action

```

ACTIVITY 4 – Custom Policy Using JSON Editor

Objective

Understand IAM policy JSON structure.

Scenario

Frontend team can:

- Start/Stop only **one EC2 instance**
- Cannot access other instances

Tasks

1. Create a policy using **JSON editor**
2. Allow actions:
 - ec2:StartInstances
 - ec2:StopInstances
 - ec2:DescribeInstances
3. Restrict resource to:
One specific EC2 instance ARN
4. Create group:
FrontendTeam
5. Attach policy
6. Test by logging in as frontend user

Expected Outcome

- Only one EC2 visible & controllable

The screenshot displays the AWS IAM console interface. On the left, the navigation menu includes sections for Identity and Access Management (IAM), Access Management, and Access reports. The main content area shows the details for a policy named 'EC2InstancePolicy'. A green banner at the top indicates 'Policy EC2InstancePolicy created.' Below this, the 'Policy details' section shows the policy type as 'Customer managed', creation and editing times as 'January 27, 2026, 20:12 (UTC+05:30)', and the ARN as 'arn:aws:iam:671190134484:policy/EC2InstancePolicy'. The 'Permissions' tab is selected, showing the 'Permissions defined in this policy' section. The JSON policy document is displayed, defining permissions for 'VisualEditor0' and 'VisualEditor1' to perform 'ec2:StartInstances', 'ec2:StopInstances', and 'ec2:DescribeInstances' on a specific EC2 instance resource. The bottom of the console shows the URL 'https://eu-north-1.console.aws.amazon.com/console/home?region=eu-nort...' and the footer with copyright information for Amazon Web Services, Inc.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": [
8         "ec2:StartInstances",
9         "ec2:StopInstances"
10      ],
11       "Resource": "arn:aws:ec2:eu-north-1:671190134484:instance/i-0573e26be2e51c839"
12     },
13     {
14       "Sid": "VisualEditor1",
15       "Effect": "Allow",
16       "Action": "ec2:DescribeInstances",
17       "Resource": "*"
18     }
19   ]
20 }
```

Search

[Alt+S]

Ask Amazon Q

Global

Harsh Gupta (6711-9013-4484)

Identity and Access Management (IAM)

Search IAM

Dashboard

Access Management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Temporary delegation requests

Access reports

Access Analyzer

Resource analysis

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Resource control policies

FrontendTeam

Summary

User group name

FrontendTeam

Creation time

January 27, 2026, 20:13 (UTC+05:30)

ARN

arn:aws:iam::671190134484:group/FrontendTeam

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.

Search

User name

intern-user1

Groups

Last activity

Creation time

1 hour ago

1 hour ago

CloudShell

Feedback

Console Mobile App

© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Search

[Alt+S]

Europe (Stockholm)

Account ID: 6711-9013-4484

intern-user1

EC2

Instances

Dashboard

AWS Global View

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Capacity Manager

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Instances (8)

Find instance by attribute or tag (case-sensitive)

All states

Connect

Instance state

Actions

Launch instances

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv6 DNS
chatapp-webs...	i-071784405e88d402b	Stopped	t3.micro	You are not auth	An unexpected	eu-north-1a	-	-
practice-backe...	i-0573e26be2e51c839	Running	t3.micro	You are not auth	An unexpected	eu-north-1a	-	-
practice-bastion	i-0e321e53348105ae5	Running	t3.micro	You are not auth	An unexpected	eu-north-1a	-	13.4i
chatapp-datab...	i-05f4f60fe7b930c76	Stopped	t3.micro	You are not auth	An unexpected	eu-north-1b	-	-
chatapp-backe...	i-07617f2ab13d107d3	Running	t3.micro	You are not auth	An unexpected	eu-north-1b	-	-
linux-practice	i-0f3392aa5917e1b60	Stopped	t3.micro	You are not auth	An unexpected	eu-north-1b	-	-
practice-webs...	i-05f9f584f9ae99bf	Running	t3.micro	You are not auth	An unexpected	eu-north-1b	-	13.6i
practice-datab...	i-05c85ea5c7549489c	Running	t3.micro	You are not auth	An unexpected	eu-north-1b	-	-

Select an instance

CloudShell

Feedback

Console Mobile App

© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Search

[Alt+S]

Europe (Stockholm)

Account ID: 6711-9013-4484

intern-user1

EC2

Instances

Dashboard

AWS Global View

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Capacity Manager

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Instances (1/8)

Find instance by attribute or tag (case-sensitive)

All states

Connect

Instance state

Actions

Launch instances

Successfully initiated stopping of i-0573e26be2e51c839

Notifications 2 0 1 0 0 0

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv6 DNS
chatapp-webs...	i-071784405e88d402b	Stopped	t3.micro	You are not auth	An unexpected	eu-north-1a	-	-
practice-backe...	i-0573e26be2e51c839	Stopping	t3.micro	You are not auth	An unexpected	eu-north-1a	-	-
practice-bastion	i-0e321e53348105ae5	Running	t3.micro	You are not auth	An unexpected	eu-north-1a	-	13.4i
chatapp-datab...	i-05f4f60fe7b930c76	Stopped	t3.micro	You are not auth	An unexpected	eu-north-1b	-	-
chatapp-backe...	i-07617f2ab13d107d3	Running	t3.micro	You are not auth	An unexpected	eu-north-1b	-	-
linux-practice	i-0f3392aa5917e1b60	Stopped	t3.micro	You are not auth	An unexpected	eu-north-1b	-	-
practice-webs...	i-05f9f584f9ae99bf	Running	t3.micro	You are not auth	An unexpected	eu-north-1b	-	13.6i

i-0573e26be2e51c839 (practice-backend)

Details

Status and alarms

Monitoring

Security

Networking

Storage

Tags

Instance summary

Instance ID

i-0573e26be2e51c839

Public IPv4 address

-

Private IPv4 addresses

10.0.177.252

CloudShell

Feedback

Console Mobile App

© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences