

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:
 - o You cannot access S3
 - o You cannot access EC2

Expected Outcome

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

The screenshot shows the AWS IAM console interface. On the left, there's a navigation sidebar with options like Dashboard, Access Management (Users, Roles, Policies, Identity providers, Account settings), and Access reports (Access Analyzer). The main area is titled "intern-user1" and shows the "Summary" tab. It includes fields for ARN (arn:aws:iam::671190134484:user/intern-user1), Console access (Enabled without MFA), and two Access keys. The "Security credentials" tab is selected, showing a "Console sign-in" section with a link to https://671190134484.signin.aws.amazon.com/console and a "Manage console access" button. At the bottom, there are links for CloudShell, Feedback, and Console Mobile App, along with copyright information and links for Privacy, Terms, and Cookie preferences.

The screenshot shows the AWS EC2 Instances page. The URL in the address bar is <https://eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#Instances>. The browser header indicates it's an InPrivate session for intern-user1 in Europe (Stockholm). A red box highlights a message: "You are not authorized to perform this operation. User: arn:aws:iam:671190134484:user/intern-user1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action". Below this, a terminal window shows AWS CLI commands and their results:

```
C:\Users\260016593>aws configure
AWS Access Key ID [*****]: AKIAZYRQWV3KKGX7FRQL
AWS Secret Access Key [*****]: q+wqj11/sufVmALiLH3t3hO7rGKkgDowP8nH3N
Default region name [eu-north-1]: eu-north-1
Default output format [json]: json

C:\Users\260016593>aws s3 ls
An error occurred (AccessDenied) when calling the ListBuckets operation: User: arn:aws:iam:671190134484:user/intern-user1 is not authorized to perform: s3>ListAllMyBuckets
because no identity-based policy allows the s3>ListAllMyBuckets action

C:\Users\260016593>
```

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:
 - o AmazonS3ReadOnlyAccess to BackendTeam
4. Login as intern-user1 and:
 - o List S3 buckets (should work)
 - o 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:use
r/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

The screenshot shows the AWS IAM User Groups page. The left sidebar is collapsed. The main content area displays the 'BackendTeam' user group. It shows a summary table with the group name, creation time (January 27, 2026, 19:07 UTC+05:30), and ARN (arn:aws:iam::671190134484:group/BackendTeam). Below the summary, there are tabs for 'Users (1)', 'Permissions', and 'Access Advisor'. The 'Permissions' tab is selected, showing a table of attached policies: 'AmazonS3ReadOnlyAccess' (AWS managed) and 'BackendTeamS3Access' (Customer managed). A 'Filter by Type' dropdown is set to 'All types'. At the bottom of the permissions section, there are buttons for 'Copy', 'Edit', 'Summary', and 'JSON'.

The screenshot shows the AWS IAM Policies page. The left sidebar is collapsed. The main content area displays the 'BackendTeamS3Access' policy. It shows a table of policy details: Type (Customer managed), Creation time (January 27, 2026, 19:37 UTC+05:30), and Edited time (January 27, 2026, 19:52 UTC+05:30). The ARN is arn:aws:iam::671190134484:policy/BackendTeamS3Access. Below the details, there are tabs for 'Permissions', 'Entities attached', 'Tags', 'Policy versions (4)', and 'Last Accessed'. The 'Permissions' tab is selected, showing a JSON representation of the policy:

```

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

```

At the bottom of the policy page, there are buttons for 'Copy', 'Edit', 'Summary', and 'JSON'.

The screenshot shows a terminal window with the following command history:

```

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 shows the AWS IAM Policies page. A success message "Policy EC2InstancePolicy created." is displayed. The policy details show it's a Customer managed policy created on January 27, 2026, at 20:12 UTC+05:30, last edited on the same date at 20:12 UTC+05:30. The ARN is listed as arn:aws:iam::671190134484:policy/EC2InstancePolicy. The "Permissions defined in this policy" section contains the following JSON code:

```
1: [ 2:   "version": "2012-10-17", 3:     "Statement": [ 4:       { 5:         "Sid": "VisualEditor0", 6:         "Effect": "Allow", 7:         "Action": "ec2:StartInstances", 8:         "ec2:StopInstances", 9:         "ec2:DescribeInstances", 10:        }, 11:        "Resource": "arn:aws:ec2:eu-north-1:671190134484:instance/i-0573e2bbe2e51c839" 12:      }, 13:      { 14:        "Sid": "VisualEditor1", 15:        "Effect": "Allow", 16:        "Action": "ec2:DescribeInstances", 17:        "Resource": "" 18:      } 19:    ] 20:  ]]
```

IAM > User groups > FrontendTeam

FrontendTeam Info

Summary

User group name: FrontendTeam | Creation time: January 27, 2026, 20:13 (UTC+05:30) | ARN: arn:aws:iam:671190134484:group/FrontendTeam

Users | 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 |
|--------------|--------|---------------|---------------|
| intern-user1 | | 1 hour ago | 1 hour ago |

CloudShell | Feedback | Console Mobile App

EC2 > Instances

Instances (8) Info

Find Instance by attribute or tag (case-sensitive)

| Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS | Publ |
|-------------------|---------------------|----------------|---------------|-------------------|-----------------|-------------------|-----------------|-------|
| chatapp-webs... | i-071784405e88dd02b | Stopped | t3.micro | You are not auth. | An unexpecte... | eu-north-1a | - | - |
| practice-backe... | i-0573e26be2e51c839 | Running | t3.micro | You are not auth. | An unexpecte... | eu-north-1a | - | - |
| practice-bastion | i-0e521e53348105ae5 | Running | t3.micro | You are not auth. | An unexpecte... | eu-north-1a | - | 13.4i |
| chatapp-datab... | i-05f4f60fe7b930c76 | Stopped | t3.micro | You are not auth. | An unexpecte... | eu-north-1b | - | - |
| chatapp-backe... | i-076172ab13d107d3 | Running | t3.micro | You are not auth. | An unexpecte... | eu-north-1b | - | - |
| linux-practice | i-0f3392aa5917e1b60 | Stopped | t3.micro | You are not auth. | An unexpecte... | eu-north-1b | - | - |
| practice-webs... | i-05ff9f5849ae99bf | Running | t3.micro | You are not auth. | An unexpecte... | eu-north-1b | - | 13.6i |
| practice-datab... | i-05c85ea5c7549489c | Running | t3.micro | You are not auth. | An unexpecte... | eu-north-1b | - | - |

Select an instance

CloudShell | Feedback | Console Mobile App

EC2 > Instances

Successfully initiated stopping of i-0573e26be2e51c839

Instances (1/8) Info

Find Instance by attribute or tag (case-sensitive)

| Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS | Publ |
|-------------------|---------------------|----------------|---------------|-------------------|-----------------|-------------------|-----------------|-------|
| chatapp-webs... | i-071784405e88dd02b | Stopped | t3.micro | You are not auth. | An unexpecte... | eu-north-1a | - | - |
| practice-backe... | i-0573e26be2e51c839 | Stopping | t3.micro | You are not auth. | An unexpecte... | eu-north-1a | - | - |
| practice-bastion | i-0e521e53348105ae5 | Running | t3.micro | You are not auth. | An unexpecte... | eu-north-1a | - | 13.4i |
| chatapp-datab... | i-05f4f60fe7b930c76 | Stopped | t3.micro | You are not auth. | An unexpecte... | eu-north-1b | - | - |
| chatapp-backe... | i-076172ab13d107d3 | Running | t3.micro | You are not auth. | An unexpecte... | eu-north-1b | - | - |
| linux-practice | i-0f3392aa5917e1b60 | Stopped | t3.micro | You are not auth. | An unexpecte... | eu-north-1b | - | - |
| practice-webs... | i-05ff9f5849ae99bf | Running | t3.micro | You are not auth. | An unexpecte... | eu-north-1b | - | 13.6i |

i-0573e26be2e51c839 (practice-backend)

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

Instance ID: i-0573e26be2e51c839

Public IPv4 address: -

Private IPv4 addresses: 10.0.177.252

CloudShell | Feedback | Console Mobile App