

ACTIVITY 1 – IAM Users & Authentication

Objective

Understand IAM users and authentication mechanisms.

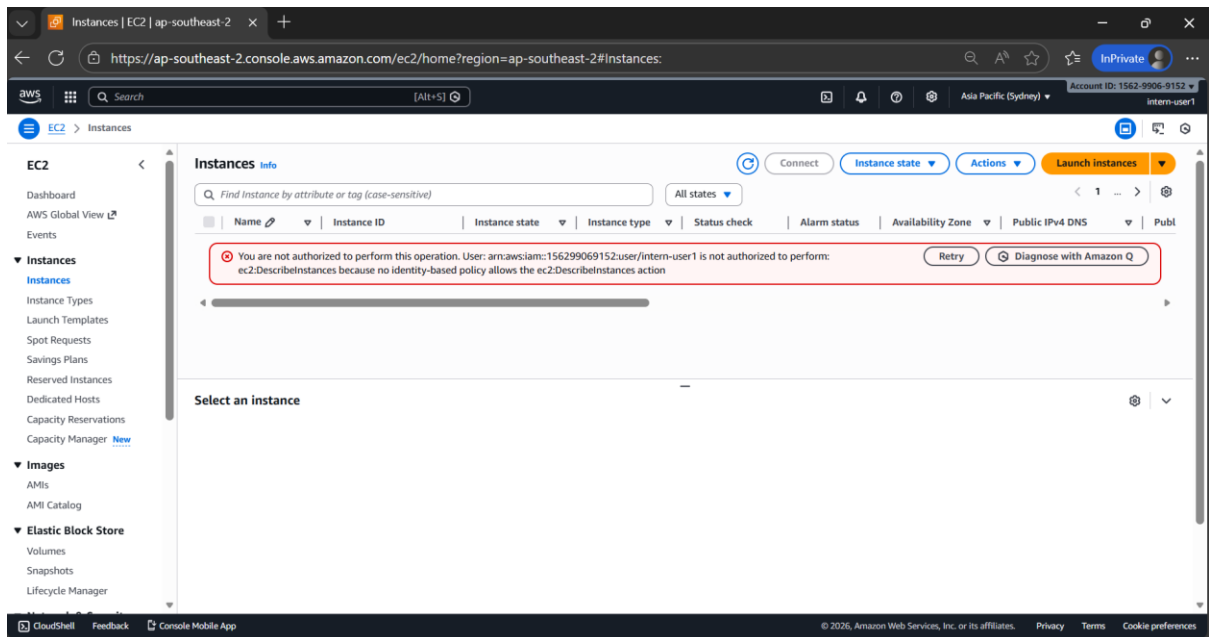
Tasks

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

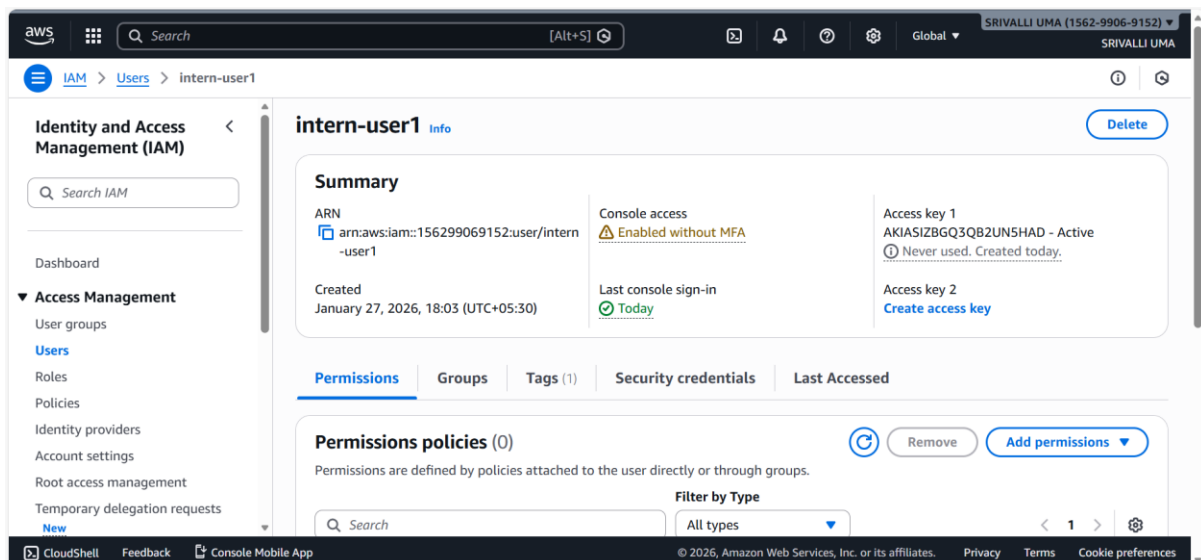
- User exists
- Login works
- Everything shows Access Denied



```
C:\Users\260016544>aws configure
AWS Access Key ID [*****5HAD]: AKIASIZBGQ3QB2UNSHAD
AWS Secret Access Key [*****qNCz]: fw9fgqc9lfUJLeBkw9/ktDY761ly1H3rek9qNCz
Default region name [ap-southeast-2]: ap-southeast-2
Default output format [JSON]: JSON

C:\Users\260016544>aws s3 ls
An error occurred (AccessDenied) when calling the ListBuckets operation: User: arn:aws:iam:156299069152:user/intern-user1 is not authorized to perform: s3:ListAllMyBuckets
because no identity-based policy allows the s3:ListAllMyBuckets action

C:\Users\260016544>
```



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)

The screenshot shows the AWS IAM console for the 'BackendTeam' user group. The left sidebar contains navigation links for Identity and Access Management (IAM), Access Management, and Access reports. The main content area displays the 'BackendTeam' group details, including a summary with the group name, creation time (January 27, 2026, 19:07 UTC+05:30), and ARN (arn:aws:iam::156299069152:group/BackendTeam). Below the summary, there is a section for 'Users in this group (1)' with a table listing the user 'intern-user1'.

User name	Groups	Last activity	Creation time
intern-user1	1	1 hour ago	1 hour ago

The screenshot shows the AWS IAM console for the 'User groups' page. A green notification banner at the top states 'DatabaseTeam user group created.' with a 'View group' button. Below the notification, there is a section for 'User groups (2)' with a table listing the groups 'BackendTeam' and 'DatabaseTeam'.

Group name	Users	Permissions	Creation time
BackendTeam	1	Defined	Now
DatabaseTeam	0	Not defined	Now

```
C:\Users\260016544>aws s3 ls
2026-01-27 19:12:03 uma-backend-s3
```

```
C:\Users\260016544>echo "Hello, world!!" > file1.txt
C:\Users\260016544>aws s3 cp file1.txt s3://uma-backend-s3/
upload failed: .\file1.txt to s3://uma-backend-s3/file1.txt An error occurred (AccessDenied) when calling the PutObject operation: User: arn:aws:iam::156299069152:user/intern-user1 is not authorized to perform: s3:PutObject on resource: "arn:aws:s3:::uma-backend-s3/file1.txt" because no identity-based policy allows the s3:PutObject action
C:\Users\260016544>
```

Questions to Answer

● Why upload is denied?

The AmazonS3ReadOnlyAccess policy only grants read-only permissions for S3 resources. But it does not include write permissions. So when the user intern-user1 tries to upload then the IAM denies the request because the permissions required is missing. To enable the upload we need to add PutObject.

● Where did the permission come from?

We attached the policy to the BackendTeam group and intern-user1 was a part of that group so the permissions for ReadOnlyAccess was enabled. So, the list buckets permission came from the AmazonS3ReadOnlyAccess policy attached to BackendTeam.

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:

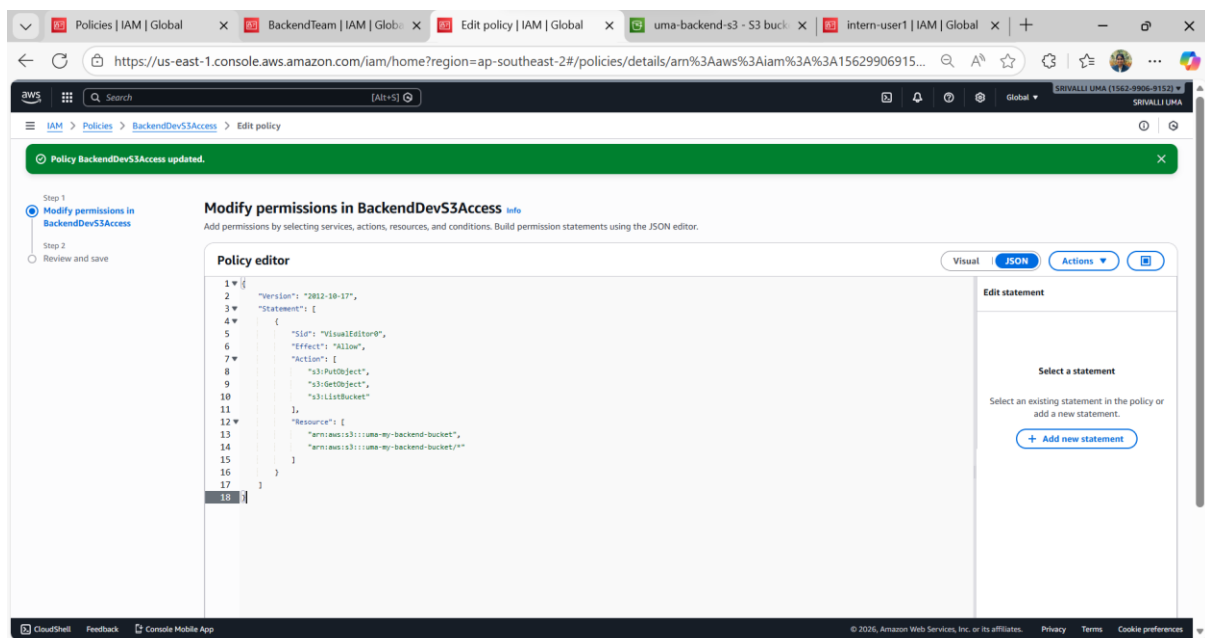
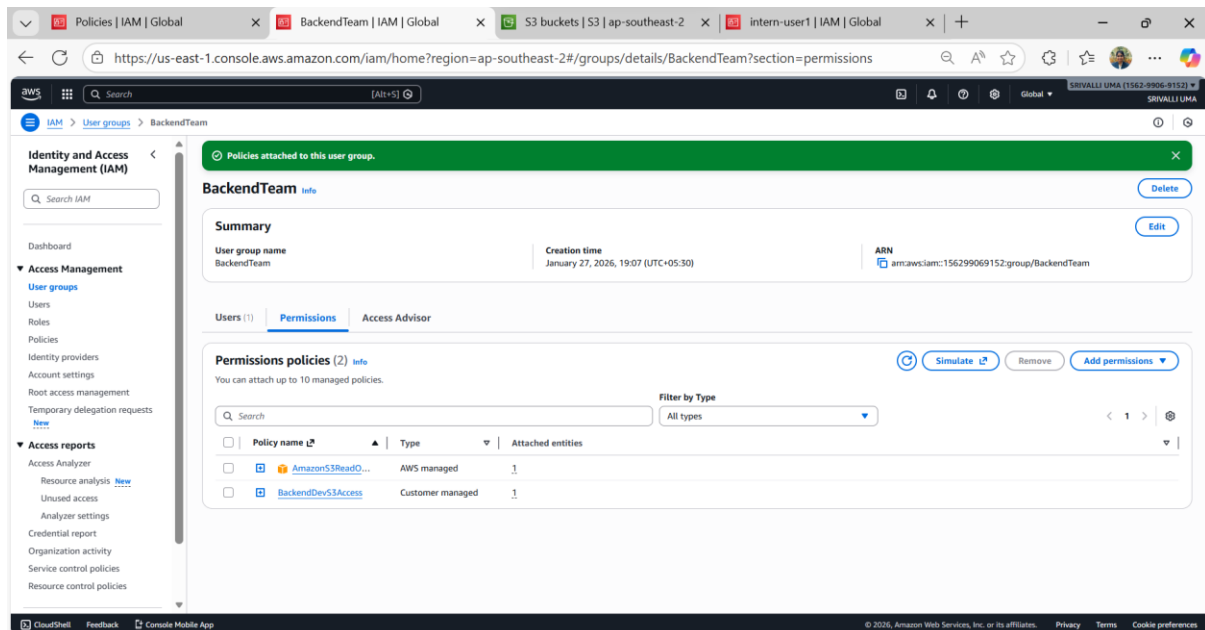
○ Upload file → allowed

○ Delete file → denied

Expected Outcome

● Fine-grained access

● No admin permissions



```
C:\Users\260016544>aws s3 cp fileA.txt s3://uma-my-backend-bucket/
upload: .\fileA.txt to s3://uma-my-backend-bucket/fileA.txt

C:\Users\260016544>aws s3 rm s3://uma-my-backend-bucket/fileA.txt
delete failed: s3://uma-my-backend-bucket/fileA.txt An error occurred (AccessDenied) when calling the DeleteObject operation: User: arn:aws:iam::156299069152:user/intern-user1 is not authorized to perform: s3:DeleteObject on resource: "arn:aws:s3:::uma-my-backend-bucket/fileA.txt" because no identity-based policy allows the s3:DeleteObject action

C:\Users\260016544>
```

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

FrontendTeam user group created.

User groups (3)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Group name	Users	Permissions	Creation time
BackendTeam	1	Defined	1 hour ago
DatabaseTeam	0	Not defined	1 hour ago
FrontendTeam	0	Defined	Now

Modify permissions in EC2-backend-access

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

```
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:ap-southeast-2:156299069152:instance/i-0280457ae5f66089a"
12    },
13    {
14      "Sid": "VisualEditor1",
15      "Effect": "Allow",
16      "Action": "ec2:DescribeInstances",
17      "Resource": "*"
18    }
19  ]
20 }
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

Instances | EC2 | ap-southeast-2

https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#instances:

aws

Search

[Alt+S]

Asia Pacific (Sydney)

Account ID: 1562-9906-9152

intern-user1

EC2 > Instances

EC2

Dashboard

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Capacity Manager [New](#)

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Instances (1/6) [Info](#)

All states

Connect

Instance state

Actions

Launch instances

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Publ
<input type="checkbox"/>	chatapp-datab...	i-03b0809e2c42957e3	Stopped	t3.micro	You are not auth	An unexpecte	ap-southeast-2b	-	-
<input type="checkbox"/>	linux-practice	i-0d6be51a1154809a4	Stopped	t3.micro	You are not auth	An unexpecte	ap-southeast-2a	-	-
<input type="checkbox"/>	my-linux-pract...	i-0a16e68a8aa02a8ab	Stopped	t3.micro	You are not auth	An unexpecte	ap-southeast-2a	-	-
<input checked="" type="checkbox"/>	chatapp-backe...	i-020b457ae5f66b89a	Stopping	t3.micro	You are not auth	An unexpecte	ap-southeast-2a	-	-
<input type="checkbox"/>	chatapp-bastion	i-0af2c8024d2be281d	Stopped	t3.micro	You are not auth	An unexpecte	ap-southeast-2a	-	-

i-020b457ae5f66b89a (chatapp-backend)

Details

Status and alarms

Monitoring

Security

Networking

Storage

Tags

▼ Instance summary [Info](#)

Instance ID

i-020b457ae5f66b89a

Public IPv4 address

-

Private IPv4 addresses

10.0.174.64

IPV6 address

-

Instance state

Stopping

Public DNS

-

Hostname type

IP name: ip-10-0-174-64.ap-southeast-2.compute.internal

Private IP DNS name (IPv4 only)

ip-10-0-174-64.ap-southeast-2.compute.internal

CloudShell

Feedback

Console Mobile App

© 2026, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)