

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 shows the AWS Management Console for EC2 Instances. The URL in the browser is <https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#Instances>. The error message displayed is: "You are not authorized to perform this operation. User: arn:aws:iam::156299069152:user/intern-user1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action".

```
C:\Users\260016544>aws configure
AWS Access Key ID [*****SHAD]: AKIASIZBGQ3QB2UN5HAD
AWS Secret Access Key [*****qNCz]: fw0fgqg91FUJLeBkv9/ktdy76ily1H3rek9qNCz
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>
```

The screenshot shows the AWS IAM User details page for a user named 'intern-user1'. The left sidebar shows navigation options like 'Identity and Access Management (IAM)', 'Dashboard', and 'Access Management' (with 'Users' selected). The main content area displays the 'Summary' tab for 'intern-user1'. Key information includes:

- ARN:** arn:aws:iam::156299069152:user/intern-user1
- Console access:** Enabled without MFA
- Created:** January 27, 2026, 18:03 (UTC+05:30)
- Last console sign-in:** Today
- Access key 1:** AKIASIZBGQ3QB2UN5HAD - Active (Never used. Created today.)
- Access key 2:** Create access key

Below the summary, there are tabs for 'Permissions', 'Groups', 'Tags (1)', 'Security credentials', and 'Last Accessed'. The 'Permissions' tab is active, showing 'Permissions policies (0)' and a note: 'Permissions are defined by policies attached to the user directly or through groups.' There is a search bar, a filter dropdown set to 'All types', and pagination controls (page 1 of 1).

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)

BackendTeam Info

Summary

User group name: BackendTeam

Creation time: January 27, 2026, 19:07 (UTC+05:30)

ARN: arn:aws:iam::156299069152:group/BackendTeam

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

Search Remove Add users

Access Management

- Users
- Roles
- Policies
- Identity providers
- Account settings
- Root access management
- Temporary delegation requests
- New

Access reports

- Access Analyzer
- Resource analysis New
- Unused access
- Analyzer settings
- Credential report
- Organization activity
- Service control policies
- Resource control policies

CloudShell Feedback Console Mobile App

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

DatabaseTeam user group created.

User groups (2) Info

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	Now
DatabaseTeam	0	Not defined	Now

Search Delete Create group

CloudShell Feedback Console Mobile App

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

```
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

The screenshot shows the AWS IAM Groups page. The BackendTeam group is selected. It has two attached policies: AmazonS3ReadonlyAccess and BackendDevS3Access. The BackendDevS3Access policy is highlighted.

The screenshot shows the AWS IAM Policies page with the BackendDevS3Access policy selected for editing. The JSON editor shows the following policy:

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

```
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 ac
tion
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

The screenshot shows the AWS IAM User Groups page. A green banner at the top indicates "FrontendTeam user group created." The table below lists three user groups:

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

The screenshot shows the AWS IAM Policy Editor for the "EC2-backend-access" policy. The policy document is as follows:

```
1 "Version": "2012-10-17",
2 "Statement": [
3     {
4         "Sid": "VisualEditor0",
5         "Effect": "Allow",
6         "Action": [
7             "ec2:StartInstances",
8             "ec2:StopInstances"
9         ],
10        "Resource": "arn:aws:ec2:ap-southeast-2:156299069152:instance/1-0200457ae5f6e089a"
11    },
12    {
13        "Sid": "VisualEditor1",
14        "Effect": "Allow",
15        "Action": "ec2:DescribeInstances",
16        "Resource": "*"
17    }
18]
19
20]
```

The right side of the editor shows a "Select a statement" dropdown and a "Add new statement" button.

Instances | EC2 | ap-southeast-2

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

InPrivate intern-user1

AWS Instances

EC2 > Instances

Instances (1/6) Info

Find Instance by attribute or tag (case-sensitive)

All states

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Publ
chatapp-datab...	i-03b0809e2c42957e3	Stopped	t3.micro	You are not auth	An unexpected error occurred	ap-southeast-2b	-	-
linux-practice	i-0d6be51a1154809a4	Stopped	t3.micro	You are not auth	An unexpected error occurred	ap-southeast-2a	-	-
my-linux-pract...	i-0a16e58a8aa02a8ab	Stopped	t3.micro	You are not auth	An unexpected error occurred	ap-southeast-2a	-	-
chatapp-backend	i-020b457ae5f66b89a	Stopping	t3.micro	You are not auth	An unexpected error occurred	ap-southeast-2a	-	-
chatapp-bastion	i-0af2c8024d2be281d	Stopped	t3.micro	You are not auth	An unexpected error occurred	ap-southeast-2a	-	-

i-020b457ae5f66b89a (chatapp-backend)

Details Status and alarms Monitoring Security Networking Storage Tags

Instance summary

Instance ID: i-020b457ae5f66b89a

Public IPv4 address: -

Private IP4 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

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

CloudShell Feedback Console Mobile App