AWS IAM ACTIVITIES

ACTIVITY 1 – IAM Users & Authentication

1. Create an IAM user named: intern-user1

2. Enable AWS Management Console access

3. Set a custom password

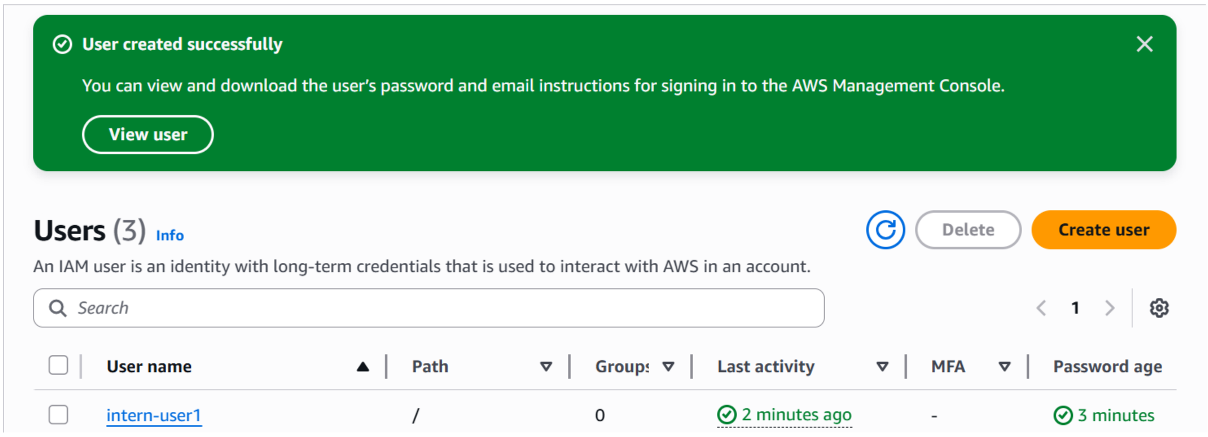
4. Log in using the IAM user and verify:

○ You cannot access S3

○ You cannot access EC2

Expected Outcome

● User exists



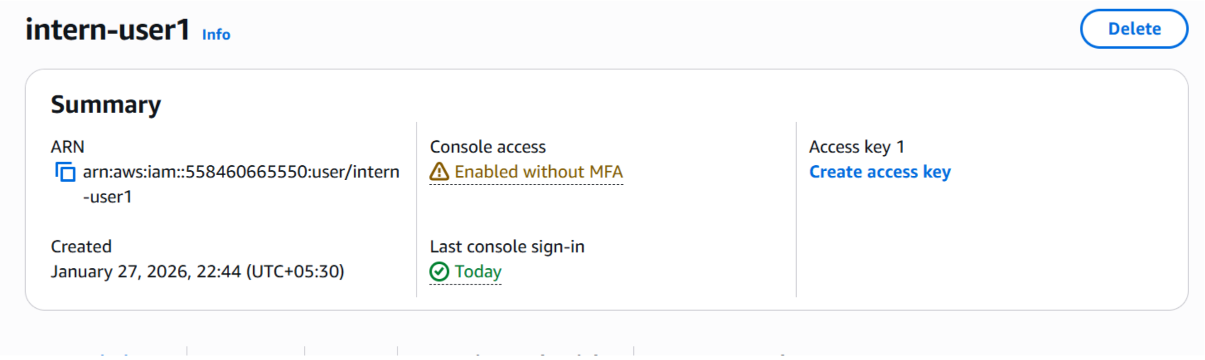
User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Users (3) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Group:	Last activity	MFA	Password age
intern-user1	/	0	✓ 2 minutes ago	-	✓ 3 minutes



intern-user1 Info

Summary

ARN
arn:aws:iam::558460665550:user/intern-user1

Created
January 27, 2026, 22:44 (UTC+05:30)

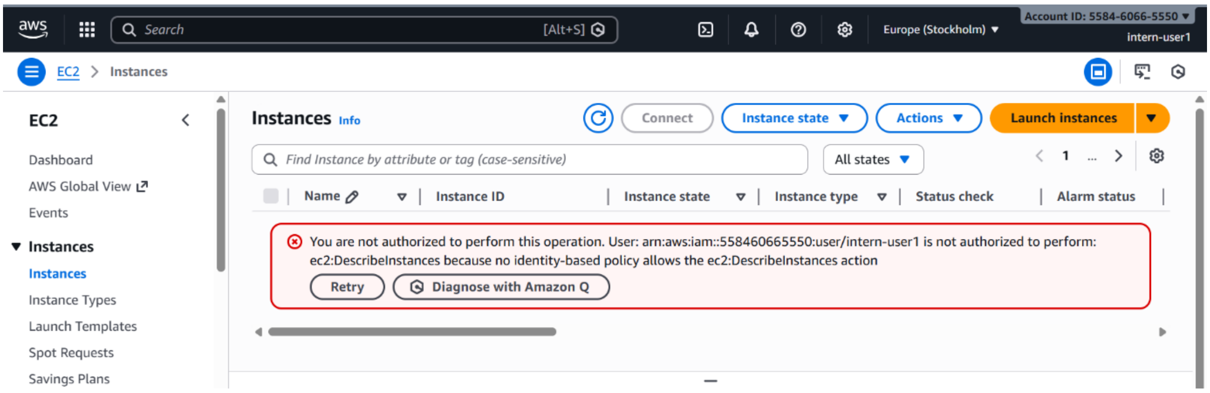
Console access
⚠ Enabled without MFA

Last console sign-in
✓ Today

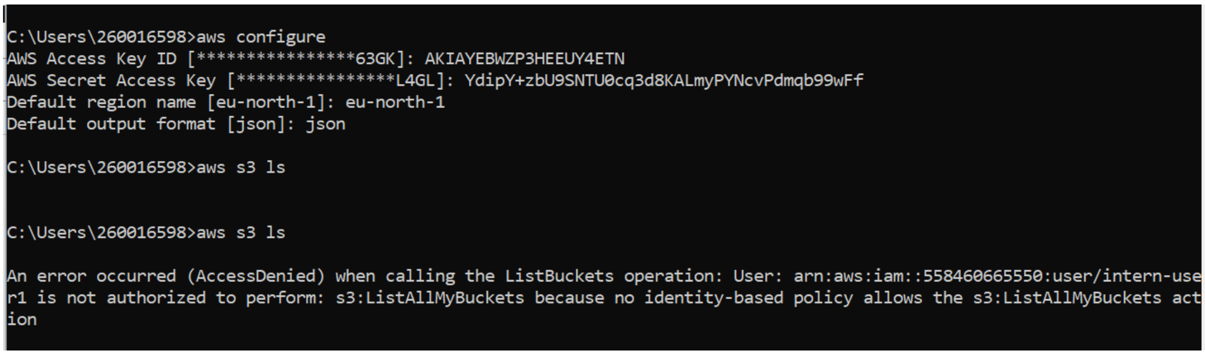
Access key 1
Create access key

● Login works

● Everything shows Access Denied



You are not authorized to perform this operation. User: arn:aws:iam::558460665550:user/intern-user1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action

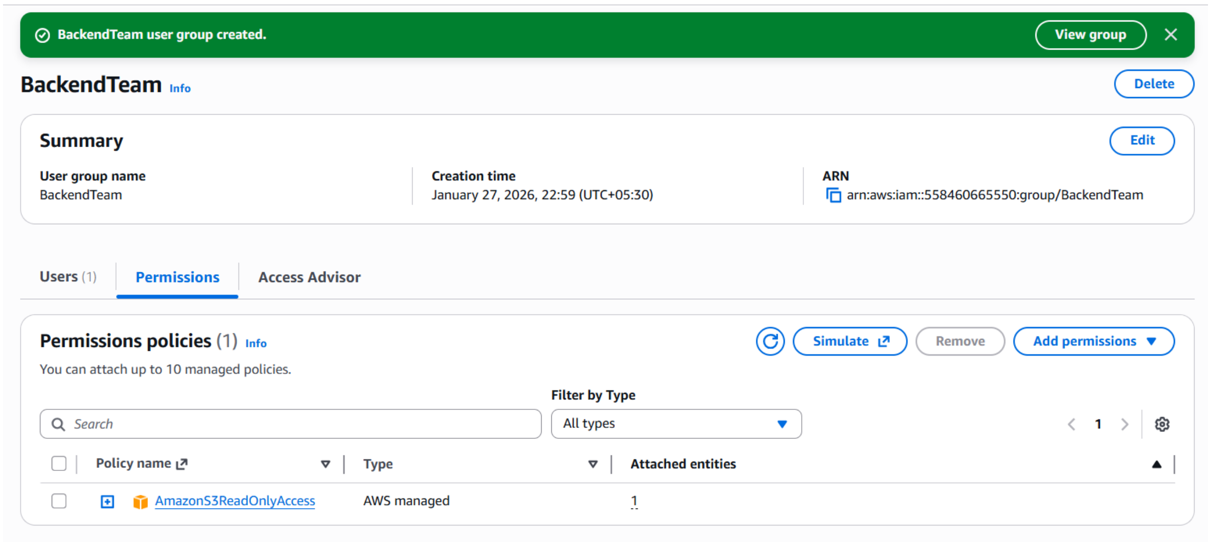


```
C:\Users\260016598>aws configure
AWS Access Key ID [****************63GK]: AKIAYEBWZP3HEEUY4ETN
AWS Secret Access Key [****************L4GL]: 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
Default region name [eu-north-1]: eu-north-1
Default output format [json]: json

C:\Users\260016598>aws s3 ls


C:\Users\260016598>aws s3 ls

An error occurred (AccessDenied) when calling the ListBuckets operation: User: arn:aws:iam::558460665550:user/intern-use
r1 is not authorized to perform: s3:ListAllMyBuckets because no identity-based policy allows the s3:ListAllMyBuckets act
ion
```

ACTIVITY 2 – IAM Groups & Permission Inheritance

Tasks

1. Create two IAM groups:
   BackendTeam, DatabaseTeam
2. Add intern-user1 to BackendTeam
3. Attach AWS managed policy:
   ○ AmazonS3ReadOnlyAccess to BackendTeam



BackendTeam user group created.

Summary

User group name: BackendTeam

Creation time: January 27, 2026, 22:59 (UTC+05:30)

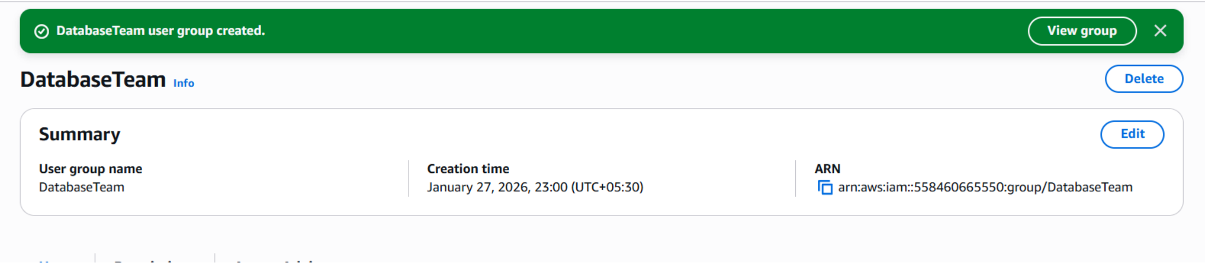
ARN: arn:aws:iam::558460665550:group/BackendTeam

Permissions policies (1) Info

You can attach up to 10 managed policies.

Filter by Type

Policy name	Type	Attached entities
AmazonS3ReadOnlyAccess	AWS managed	1



DatabaseTeam user group created.

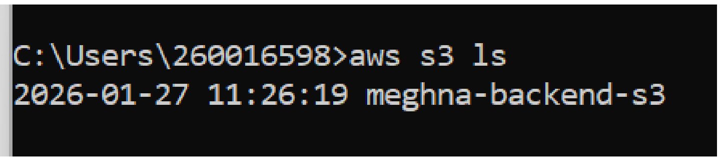
Summary

User group name: DatabaseTeam

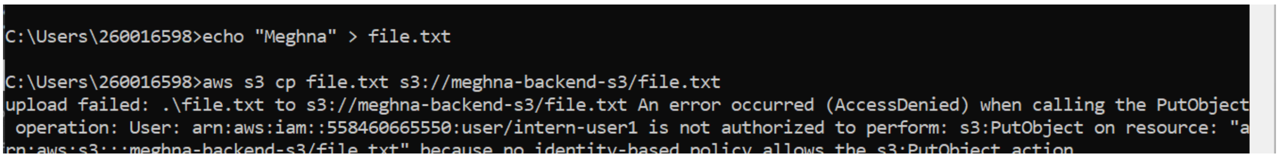
Creation time: January 27, 2026, 23:00 (UTC+05:30)

ARN: arn:aws:iam::558460665550:group/DatabaseTeam

4. Login as intern-user1 and:
   ○ List S3 buckets (should work)
   ○ Upload file (should fail)



```
C:\Users\260016598>aws s3 ls
2026-01-27 11:26:19 meghna-backend-s3
```



```
C:\Users\260016598>echo "Meghna" > file.txt

C:\Users\260016598>aws s3 cp file.txt s3://meghna-backend-s3/file.txt
upload failed: .\file.txt to s3://meghna-backend-s3/file.txt An error occurred (AccessDenied) when calling the PutObject
 operation: User: arn:aws:iam::558460665550:user/intern-user1 is not authorized to perform: s3:PutObject on resource: "a
rn:aws:s3:::meghna-backend-s3/file.txt" because no identity-based policy allows the s3:PutObject action
```

Questions to Answer:

● **Why upload is denied?**

Since we have used AmazonS3ReadOnlyAccess policy for the group, it only grants read permissions for the s3 buckets. Other permissions are not included. For intern-user1 to be able to upload files and do other operations we need to enable other policies.

● Where did the permission come from?

intern-user1 is a part of BackendTeam user group, and we attached the AmazonS3ReadOnlyAccess policy for the BackendTeam group. So, the permission to list all buckets came from there.

ACTIVITY 3 – Custom Policy Using Visual Editor

Scenario:

Backend team needs:

● Read & write objects in one specific S3 bucket

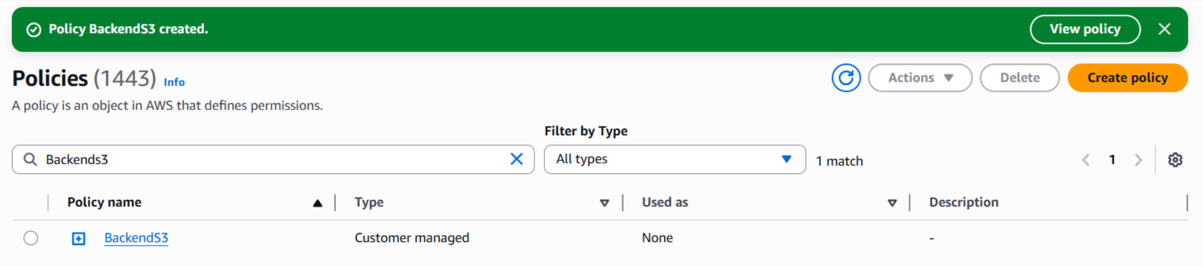
● No delete permission

Tasks

1. Create a policy using Visual Editor
2. Service: S3
3. Allow:

○ GetObject ○ PutObject ○ ListBucket

4. Restrict access to: my-backend-bucket



Policy BackendS3 created.

Policies (1443)

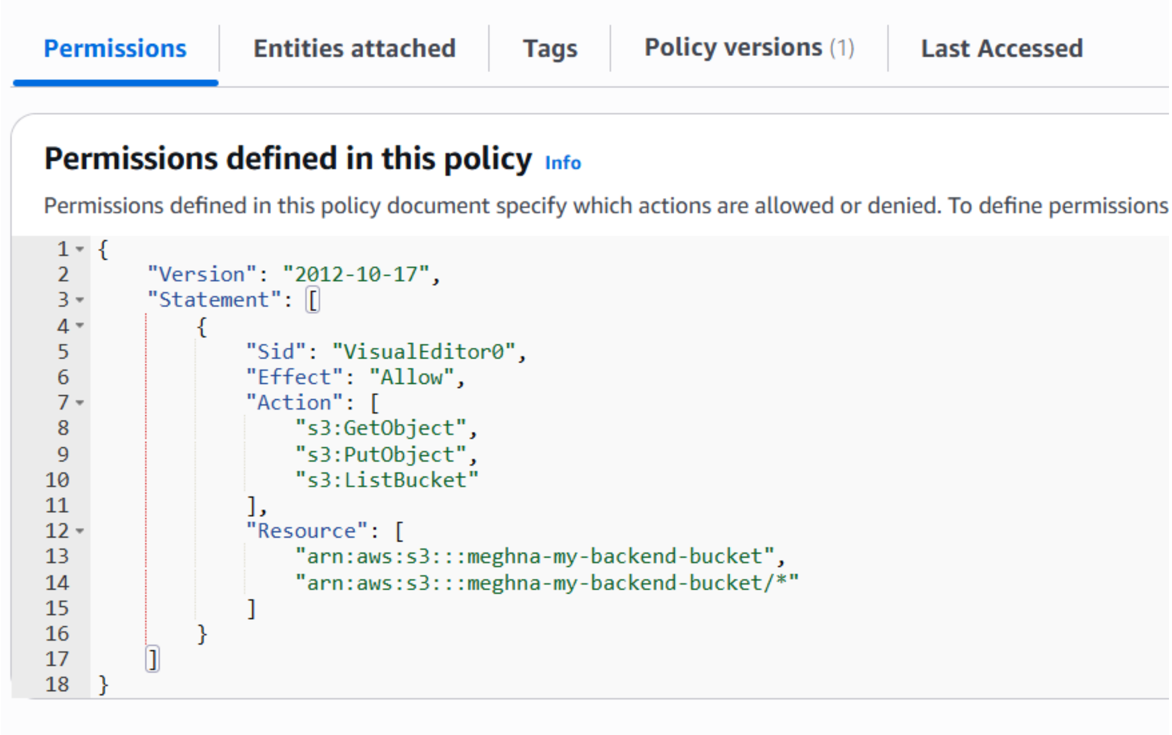
A policy is an object in AWS that defines permissions.

Filter by Type: All types

Backends3

1 match

Policy name	Type	Used as	Description
BackendS3	Customer managed	None	-

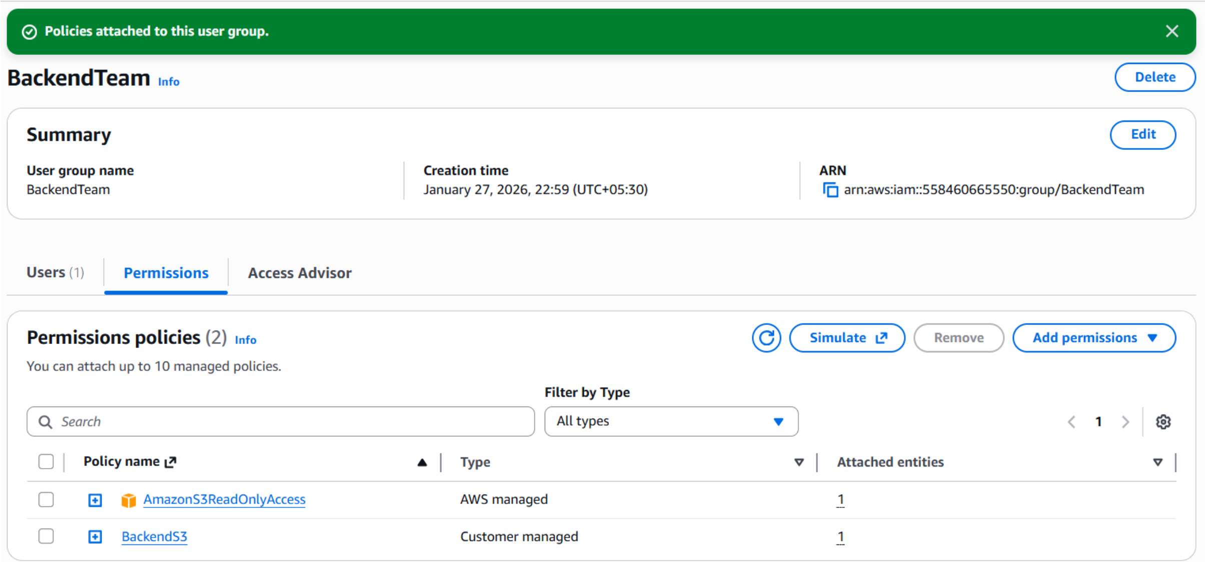


Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::meghna-my-backend-bucket",
                "arn:aws:s3:::meghna-my-backend-bucket/*"
            ]
        }
    ]
}
```

5. Attach policy to BackendTeam



Policies attached to this user group.

BackendTeam Info

Summary

User group name	Creation time	ARN
BackendTeam	January 27, 2026, 22:59 (UTC+05:30)	arn:aws:iam::558460665550:group/BackendTeam

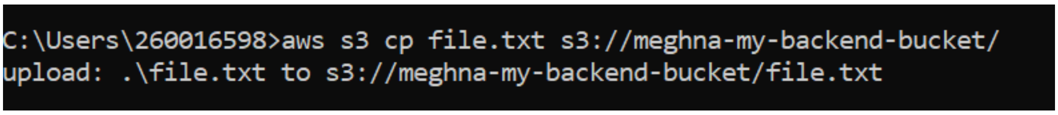
Permissions policies (2) Info

You can attach up to 10 managed policies.

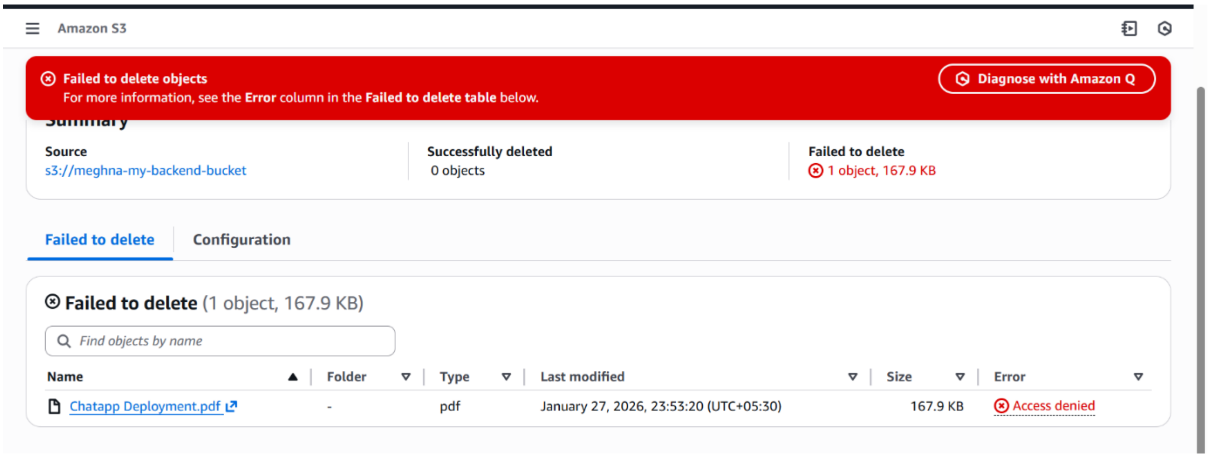
Filter by Type: All types

□	Policy name	Type	Attached entities
□	AmazonS3ReadOnlyAccess	AWS managed	1
□	BackendS3	Customer managed	1

6. Test: ○ Upload file → allowed ○ Delete file → denied



```
C:\Users\260016598>aws s3 cp file.txt s3://meghna-my-backend-bucket/
upload: .\file.txt to s3://meghna-my-backend-bucket/file.txt
```



Failed to delete objects
For more information, see the **Error** column in the **Failed to delete table** below.

Source	Successfully deleted	Failed to delete
s3://meghna-my-backend-bucket	0 objects	1 object, 167.9 KB

Failed to delete (1 object, 167.9 KB)

Name	Folder	Type	Last modified	Size	Error
Chatapp Deployment.pdf	-	pdf	January 27, 2026, 23:53:20 (UTC+05:30)	167.9 KB	Access denied

ACTIVITY 4 – Custom Policy Using JSON Editor

Scenario

Frontend team can:

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

Tasks

1. Create a policy using JSON editor

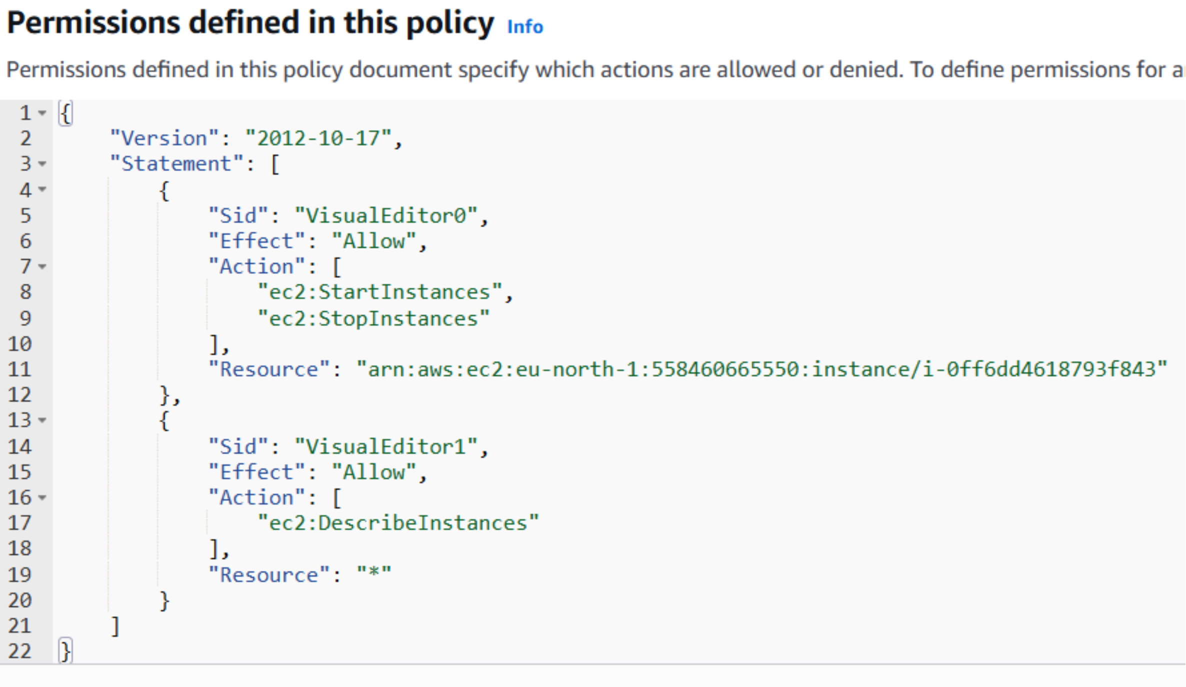
2. Allow actions:

○ ec2: StartInstances

○ ec2: StopInstances

○ ec2: DescribeInstances

3. Restrict resource to: One specific EC2 instance ARN



Permissions defined in this policy Info

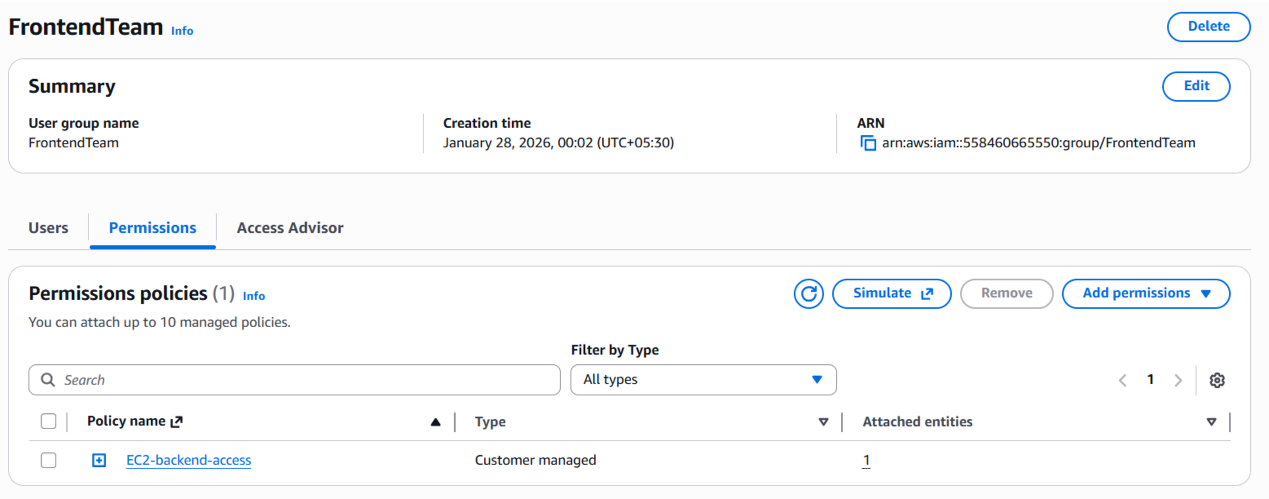
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for a

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "arn:aws:ec2:eu-north-1:558460665550:instance/i-0ff6dd4618793f843"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

4. Create group: FrontendTeam

5. Attach policy

6. Test by logging in as frontend user



FrontendTeam Info

Summary

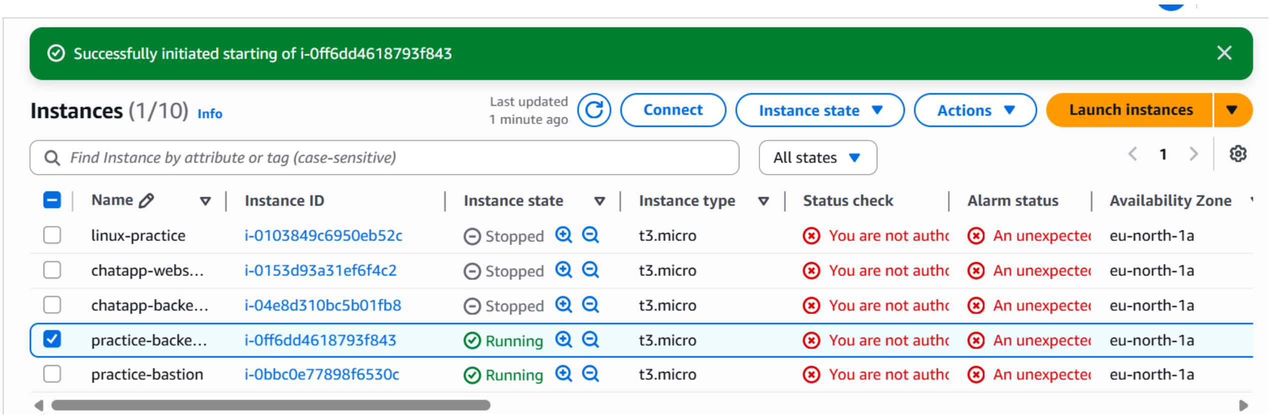
User group name	Creation time	ARN
FrontendTeam	January 28, 2026, 00:02 (UTC+05:30)	arn:aws:iam::558460665550:group/FrontendTeam

Permissions policies (1) Info

You can attach up to 10 managed policies.

Filter by Type: All types

□	Policy name	Type	Attached entities
□	EC2-backend-access	Customer managed	1



Successfully initiated starting of i-0ff6dd4618793f843

Instances (1/10) Info

Last updated
1 minute ago

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
□	linux-practice	i-0103849c6950eb52c	Stopped	t3.micro	You are not autho	An unexpecte	eu-north-1a
□	chatapp-webs…	i-0153d93a31ef6f4c2	Stopped	t3.micro	You are not autho	An unexpecte	eu-north-1a
□	chatapp-backe…	i-04e8d310bc5b01fb8	Stopped	t3.micro	You are not autho	An unexpecte	eu-north-1a
☑	practice-backe…	i-0ff6dd4618793f843	Running	t3.micro	You are not autho	An unexpecte	eu-north-1a
□	practice-bastion	i-0bbc0e77898f6530c	Running	t3.micro	You are not autho	An unexpecte	eu-north-1a