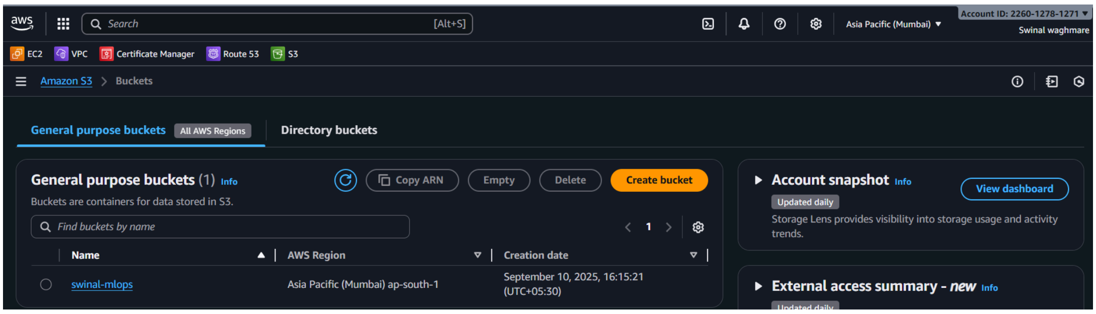
AWS IAM and S3/EC2 Policy (Task)

Date	@September 10, 2025
Multi-select	Lab-2
Status	Done

▼ 1. Create a Bucket and Upload an Object

- Log in as the **root user**.
- Create a new **S3 bucket**.



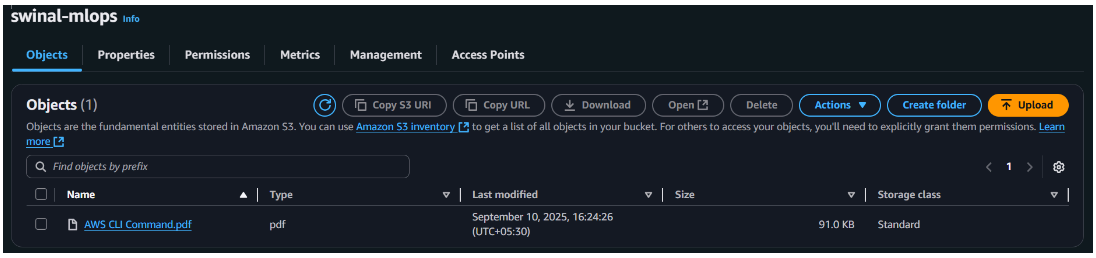
General purpose buckets (1) Info

Buckets are containers for data stored in S3.

	Name	AWS Region	Creation date
○	swinal-mlops	Asia Pacific (Mumbai) ap-south-1	September 10, 2025, 16:15:21 (UTC+05:30)

Storage Lens provides visibility into storage usage and activity trends.

- Upload an **object (file)** to the bucket.



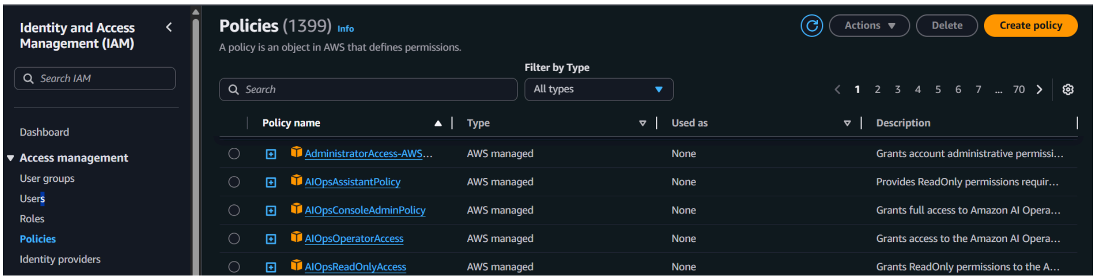
Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

☐	Name	Type	Last modified	Size	Storage class
☐	AWS CLI Command.pdf	pdf	September 10, 2025, 16:24:26 (UTC+05:30)	91.0 KB	Standard

▼ 2. Create a Custom Policy to Delete a Bucket

- Go to **IAM → Policies → Create Policy**.

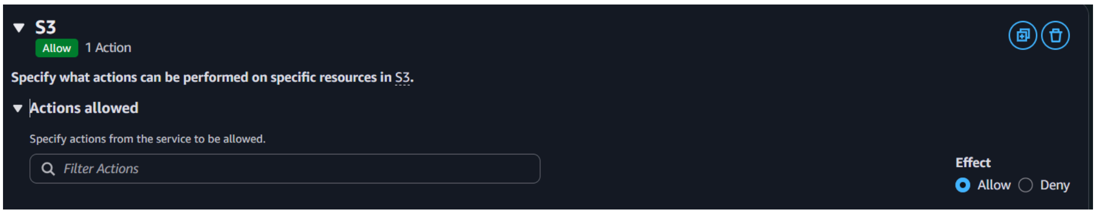


Policies (1399) Info

A policy is an object in AWS that defines permissions.

	Policy name	Type	Used as	Description
○	AdministratorAccess-AWS...	AWS managed	None	Grants account administrative permissi...
○	AIOpsAssistantPolicy	AWS managed	None	Provides ReadOnly permissions requir...
○	AIOpsConsoleAdminPolicy	AWS managed	None	Grants full access to Amazon AI Opera...
○	AIOpsOperatorAccess	AWS managed	None	Grants access to the Amazon AI Opera...
○	AIOpsReadOnlyAccess	AWS managed	None	Grants ReadOnly permissions to the A...

- Select the service **S3**.



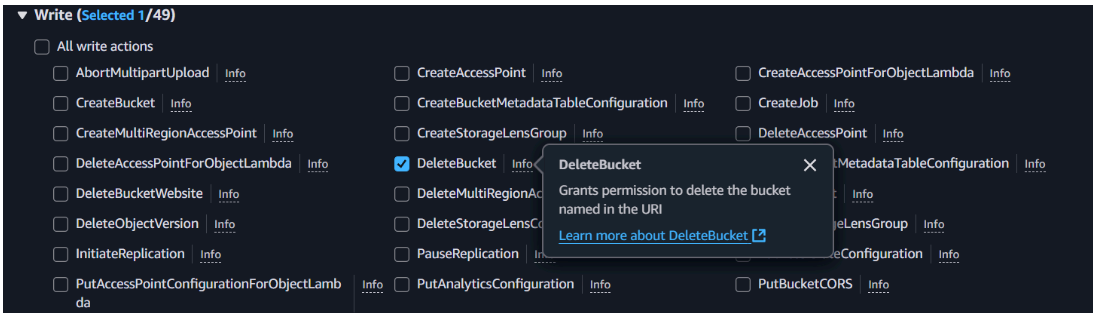
Specify what actions can be performed on specific resources in S3.

Specify actions from the service to be allowed.

Effect

● Allow ○ Deny

- Under **Actions**, choose **Write** → `DeleteBucket`.
  - This allows deleting a bucket mentioned in the resource.


▼ Write (Selected 1/49)

☐ All write actions

☐ AbortMultipartUpload Info
☐ CreateBucket Info
☐ CreateMultiRegionAccessPoint Info
☐ DeleteAccessPointForObjectLambda Info
☐ DeleteBucketWebsite Info
☐ DeleteObjectVersion Info
☐ InitiateReplication Info
☐ PutAccessPointConfigurationForObjectLambda Info

☐ CreateAccessPoint Info
☐ CreateBucketMetadataTableConfiguration Info
☐ CreateStorageLensGroup Info
☑ DeleteBucket Info
☐ DeleteMultiRegionAc
☐ DeleteStorageLensC
☐ PauseReplication In
☐ PutAnalyticsConfiguration Info

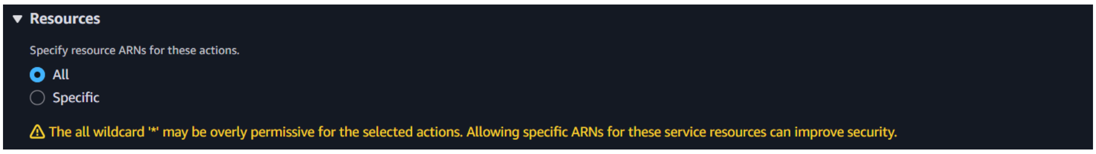
☐ CreateAccessPointForObjectLambda Info
☐ CreateJob Info
☐ DeleteAccessPoint Info
tMetadataTableConfiguration Info
Info
eLensGroup Info
eConfiguration Info
☐ PutBucketCORS Info

DeleteBucket

Grants permission to delete the bucket named in the URI

Learn more about DeleteBucket

- In **Resources**, select **All** (not restricted to one bucket).


▼ Resources

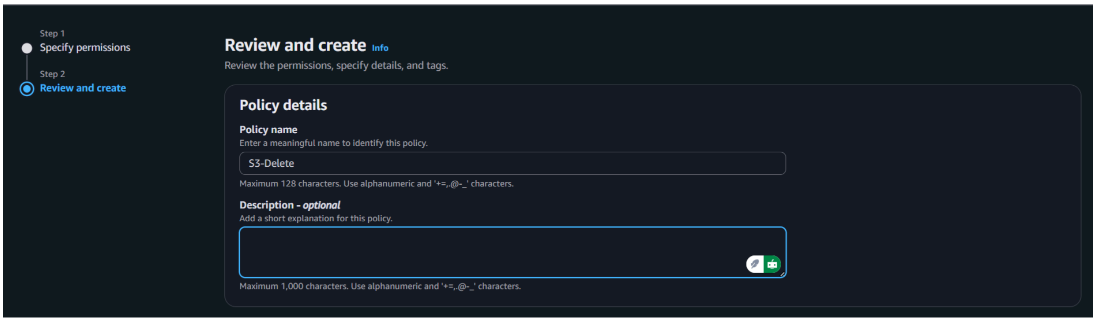
Specify resource ARNs for these actions.

● All

○ Specific

⚠ The all wildcard '*' may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

- Click **Next**, then name the policy **S3-Delete**.



Step 1
Specify permissions

Step 2
Review and create

Review and create Info

Review the permissions, specify details, and tags.

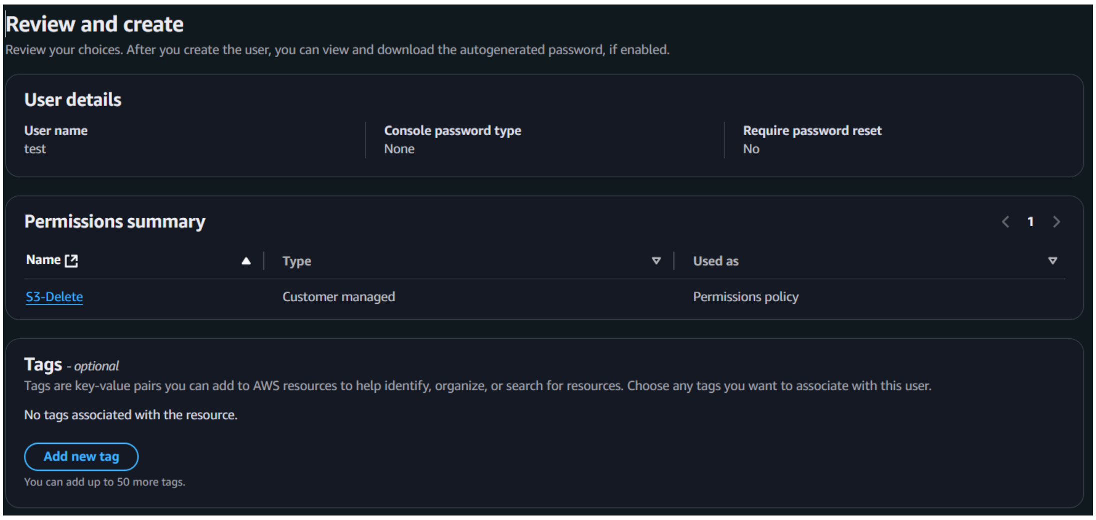
Policy details

Policy name
Enter a meaningful name to identify this policy.
S3-Delete
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

- Create a new IAM user, for example **test**.
- Attach the policy **S3-Delete** to this user.



Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Console password type	Require password reset
test	None	No

Permissions summary

Name	Type	Used as
S3-Delete	Customer managed	Permissions policy

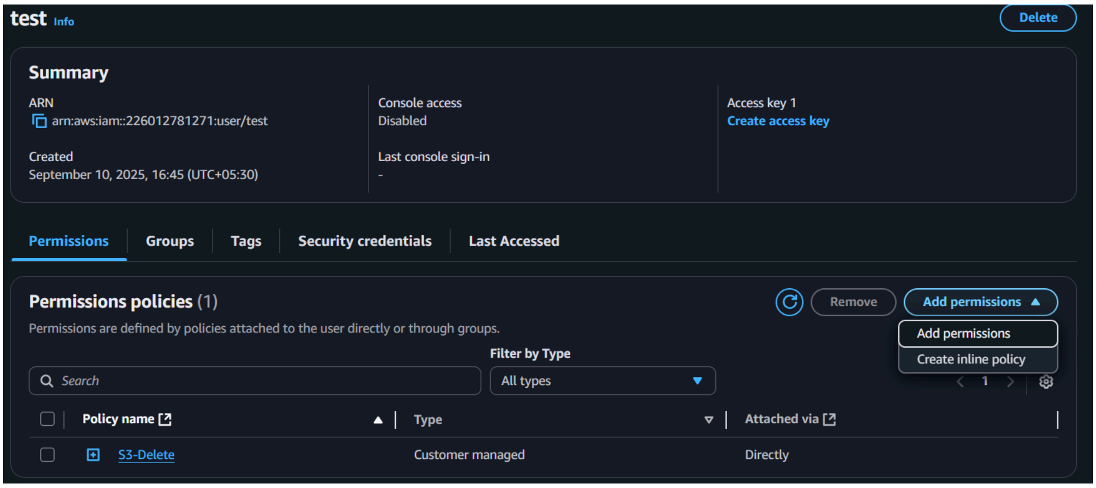
Tags - *optional*
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag
You can add up to 50 more tags.

▼ 3. Create Inline Policy to Get an Object

- Go to the user **test** → **Permissions** → **Add Permissions** → **Create Inline Policy**.



test Info

Summary

ARN
arn:aws:iam::226012781271:user/test

Created
September 10, 2025, 16:45 (UTC+05:30)

Console access
Disabled

Last console sign-in
-

Access key 1
Create access key

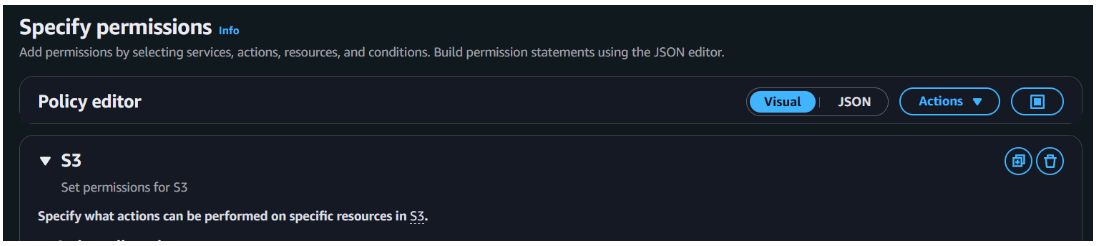
Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type
All types

□	Policy name	Type	Attached via
□	S3-Delete	Customer managed	Directly

- Select service **S3**.



Specify permissions Info

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

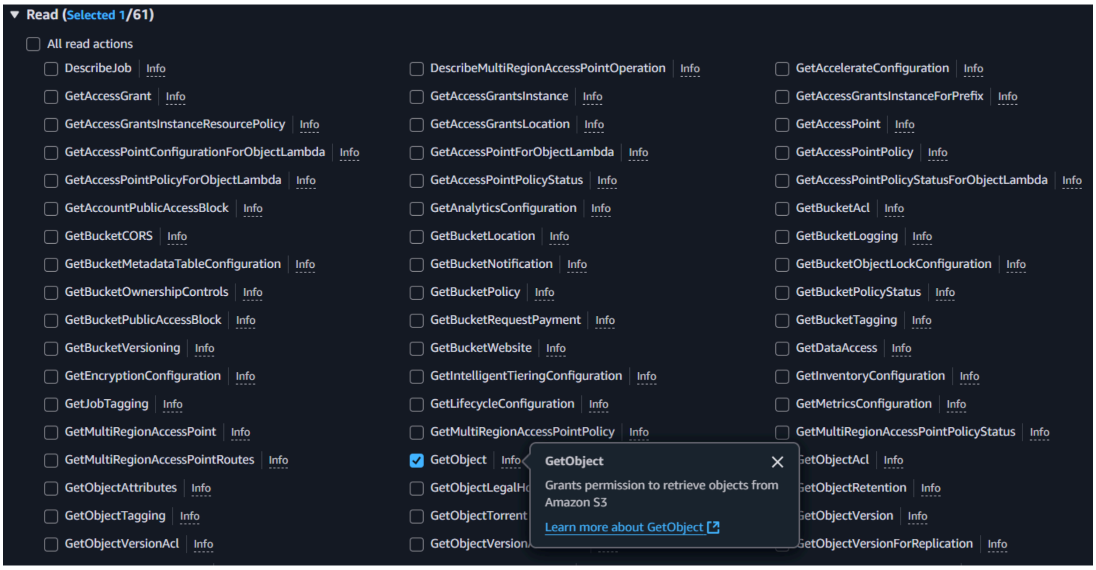
Policy editor

▼ **S3**

Set permissions for S3

Specify what actions can be performed on specific resources in S3.

- Under **Read**, select **GetObject**.



▼ **Read** (Selected 1/61)

□ All read actions

□ DescribeJob Info
□ GetAccessGrant Info
□ GetAccessGrantsInstanceResourcePolicy Info
□ GetAccessPointConfigurationForObjectLambda Info
□ GetAccessPointPolicyForObjectLambda Info
□ GetAccountPublicAccessBlock Info
□ GetBucketCORS Info
□ GetBucketMetadataTableConfiguration Info
□ GetBucketOwnershipControls Info
□ GetBucketPublicAccessBlock Info
□ GetBucketVersioning Info
□ GetEncryptionConfiguration Info
□ GetJobTagging Info
□ GetMultiRegionAccessPoint Info
□ GetMultiRegionAccessPointRoutes Info
□ GetObjectAttributes Info
□ GetObjectTagging Info
□ GetObjectVersionAcl Info

□ DescribeMultiRegionAccessPointOperation Info
□ GetAccessGrantsInstance Info
□ GetAccessGrantsLocation Info
□ GetAccessPointForObjectLambda Info
□ GetAccessPointPolicyStatus Info
□ GetAnalyticsConfiguration Info
□ GetBucketLocation Info
□ GetBucketNotification Info
□ GetBucketPolicy Info
□ GetBucketRequestPayment Info
□ GetBucketWebsite Info
□ GetIntelligentTieringConfiguration Info
□ GetLifecycleConfiguration Info
□ GetMultiRegionAccessPointPolicy Info
☑ GetObject Info
□ GetObjectLegalH
□ GetObjectTorrent
□ GetObjectVersion

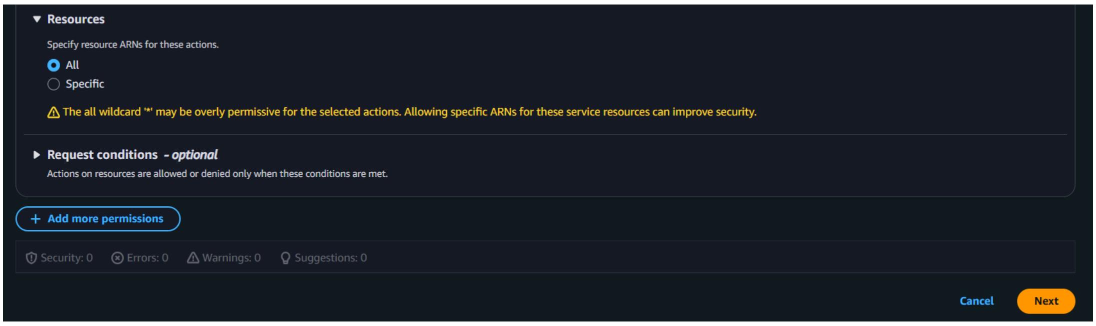
□ GetAccelerateConfiguration Info
□ GetAccessGrantsInstanceForPrefix Info
□ GetAccessPoint Info
□ GetAccessPointPolicy Info
□ GetAccessPointPolicyStatusForObjectLambda Info
□ GetBucketAcl Info
□ GetBucketLogging Info
□ GetBucketObjectLockConfiguration Info
□ GetBucketPolicyStatus Info
□ GetBucketTagging Info
□ GetDataAccess Info
□ GetInventoryConfiguration Info
□ GetMetricsConfiguration Info
□ GetMultiRegionAccessPointPolicyStatus Info
etObjectAcl Info
etObjectRetention Info
etObjectVersion Info
etObjectVersionForReplication Info

GetObject ✕

Grants permission to retrieve objects from Amazon S3

Learn more about GetObject

- In **Resources**, select **All**.



▼ **Resources**

Specify resource ARNs for these actions.

● All
○ Specific

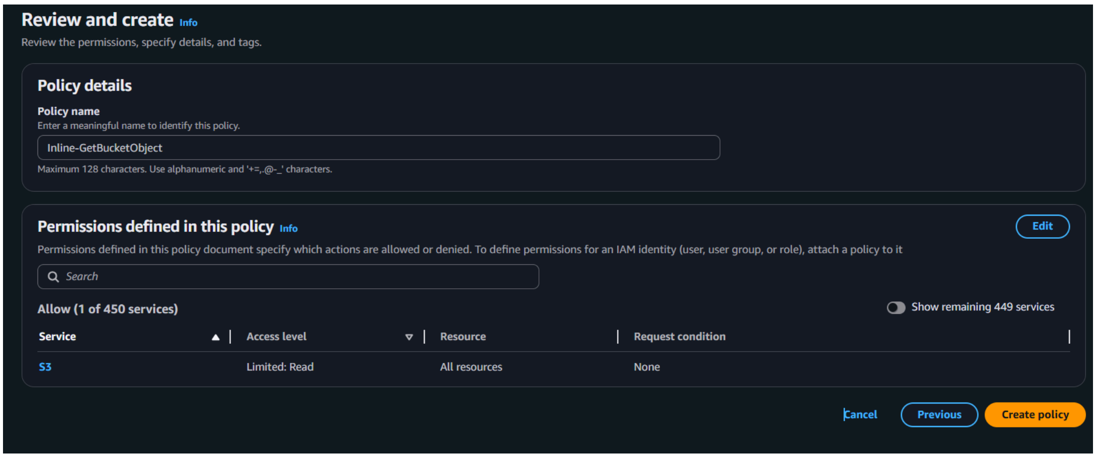
⚠ The all wildcard '*' may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

▸ **Request conditions** - *optional*

Actions on resources are allowed or denied only when these conditions are met.

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

- Name the policy `Inline-GetBucketObject` and create it.



Review and create Info

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

Inline-GetBucketObject

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Permissions defined in this policy Info

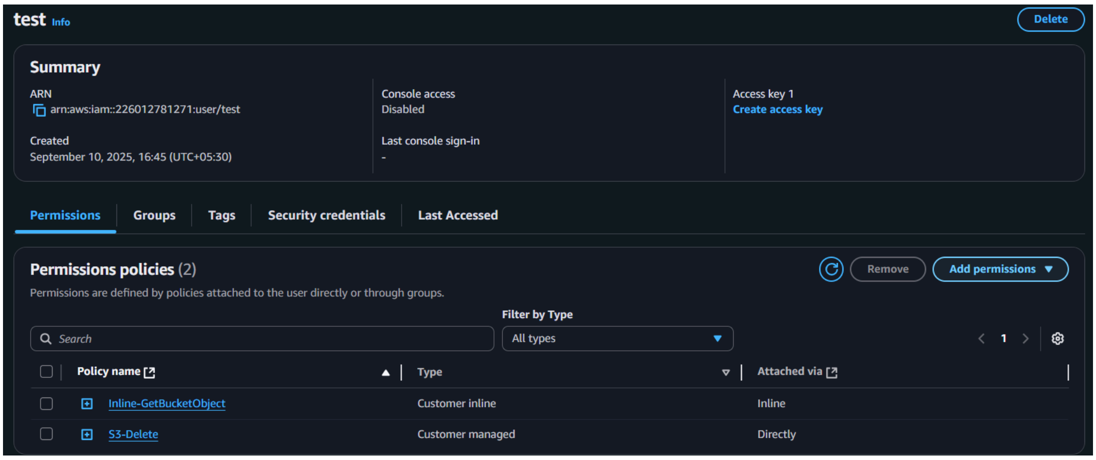
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (1 of 450 services)

Show remaining 449 services

Service	Access level	Resource	Request condition
S3	Limited: Read	All resources	None

- Now the user **test** has two policies:
    - **Customer Managed Policy →** `S3-Delete`
    - **Inline Policy →** `Inline-GetBucketObject`



test Info

Summary

ARN
arn:aws:iam::226012781271:user/test

Created
September 10, 2025, 16:45 (UTC+05:30)

Console access
Disabled

Last console sign-in
-

Access key 1
Create access key

Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

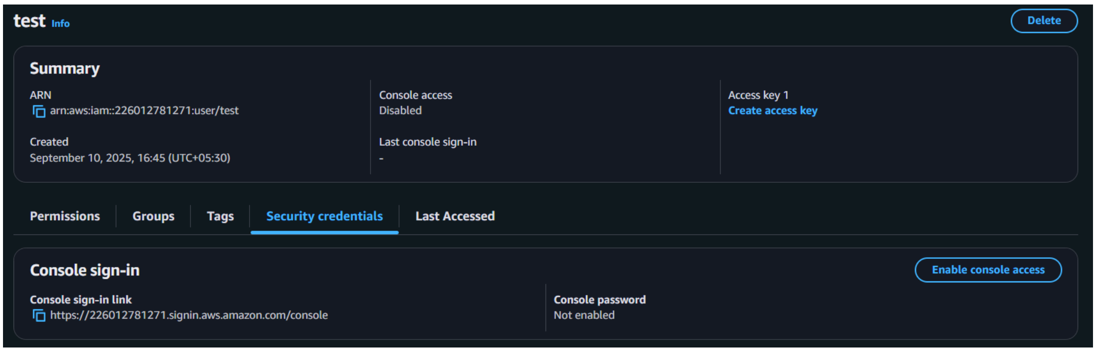
Filter by Type
All types

Policy name	Type	Attached via
Inline-GetBucketObject	Customer inline	Inline
S3-Delete	Customer managed	Directly

4. Test Permissions (Console and CLI)

Enable Console Access

- Go to **User → test → Security Credentials**.



test Info

Summary

ARN
arn:aws:iam::226012781271:user/test

Created
September 10, 2025, 16:45 (UTC+05:30)

Console access
Disabled

Last console sign-in
-

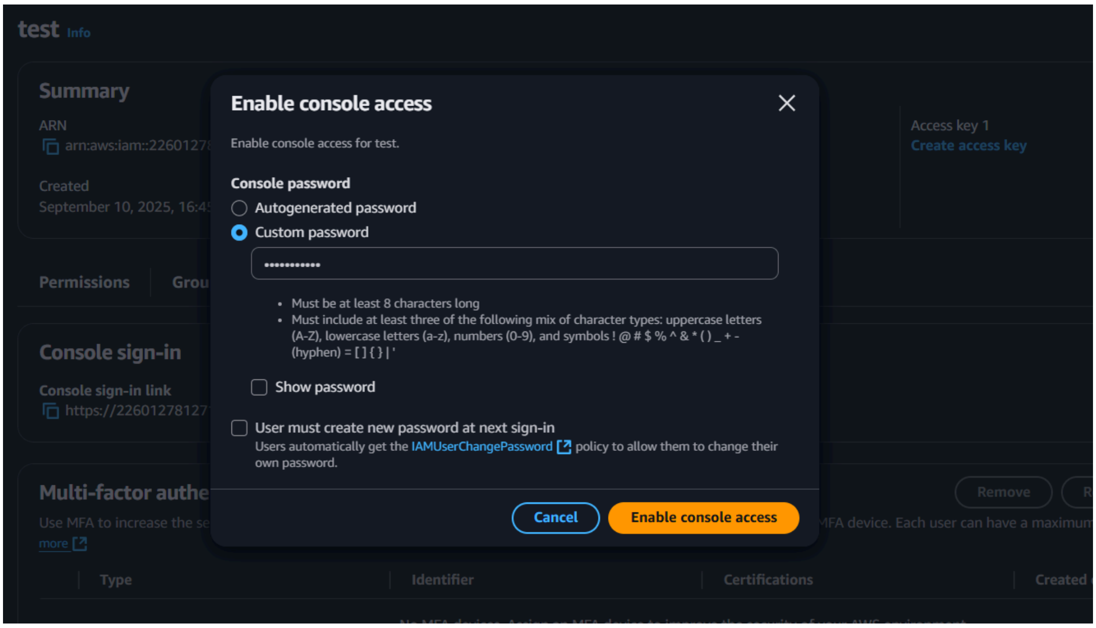
Access key 1
Create access key

Console sign-in

Console sign-in link
https://226012781271.signin.aws.amazon.com/console

Console password
Not enabled

- Enable **Console Access** and set a **custom password**.



Enable console access

Enable console access for test.

Console password

○ Autogenerated password

● Custom password

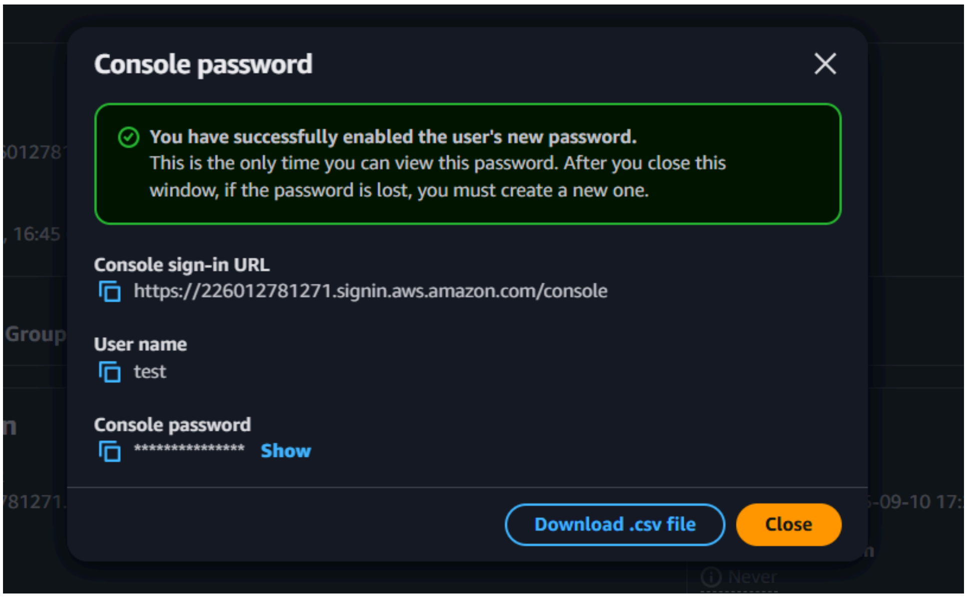
•••••••••••

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ Show password

□ User must create new password at next sign-in

Users automatically get the IAMUserChangePassword policy to allow them to change their own password.



Console password

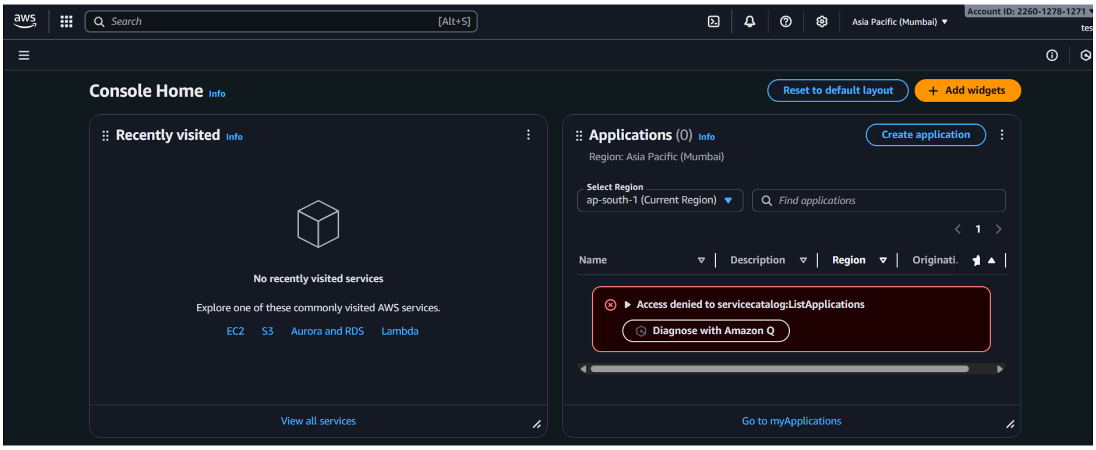
✓ You have successfully enabled the user's new password.
This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.

Console sign-in URL: https://226012781271.signin.aws.amazon.com/console

User name: test

Console password: *************** Show

- Log in using these credentials.



No recently visited services

Explore one of these commonly visited AWS services.

EC2 S3 Aurora and RDS Lambda

Region: Asia Pacific (Mumbai)

Select Region: ap-south-1 (Current Region)

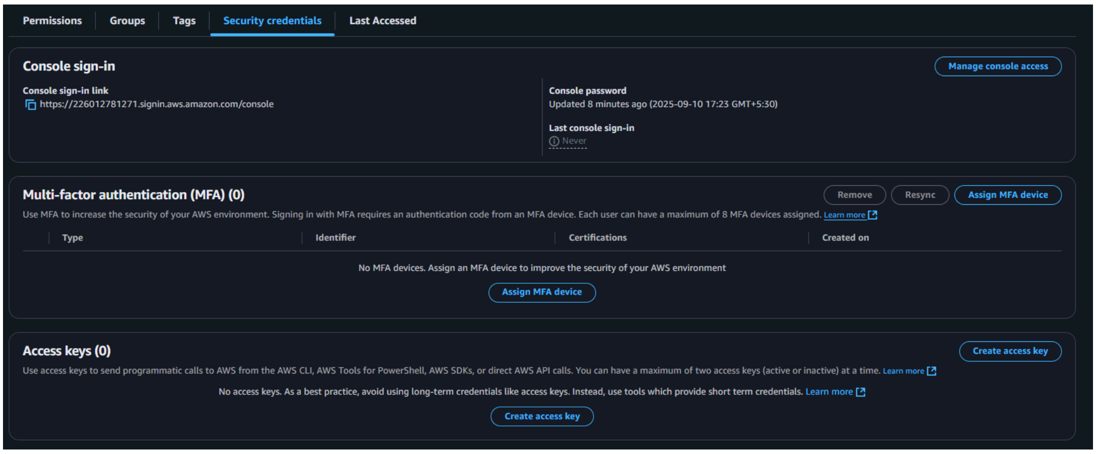
Find applications

Name	Description	Region	Originati.

Access denied to servicecatalog:ListApplications

Enable CLI Access

- Go to **User → test → Security Credentials**.



Console sign-in

Console sign-in link
https://226012781271.signin.aws.amazon.com/console

Console password
Updated 8 minutes ago (2025-09-10 17:23 GMT+5:30)

Last console sign-in
Never

Multi-factor authentication (MFA) (0)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

Type	Identifier	Certifications	Created on

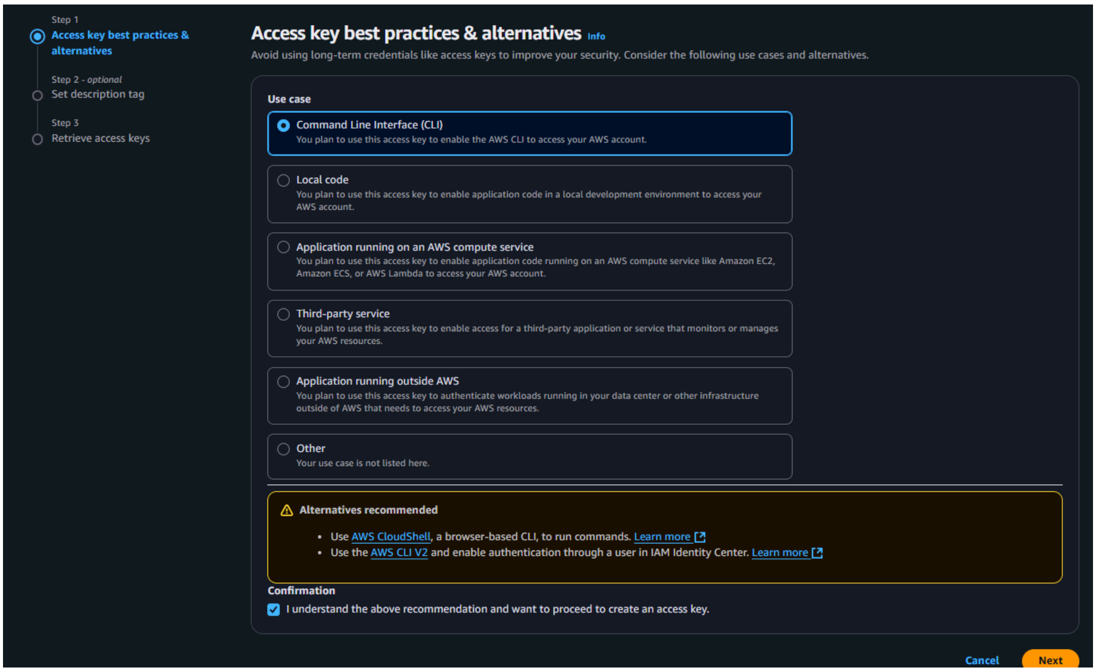
No MFA devices. Assign an MFA device to improve the security of your AWS environment

Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more

No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. Learn more

- Create an **Access Key** (for CLI use).


Step 1
● Access key best practices & alternatives

Step 2 - *optional*
○ Set description tag

Step 3
○ Retrieve access keys

Access key best practices & alternatives Info

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Use case

● Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.

○ Local code
You plan to use this access key to enable application code in a local development environment to access your AWS account.

○ Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

○ Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

○ Application running outside AWS
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.

○ Other
Your use case is not listed here.

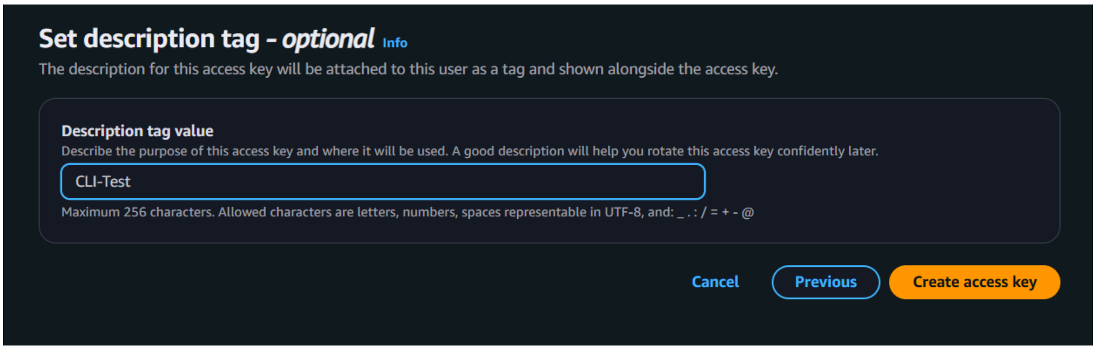
⚠ Alternatives recommended

- Use AWS CloudShell, a browser-based CLI, to run commands. Learn more
- Use the AWS CLI V2 and enable authentication through a user in IAM Identity Center. Learn more

Confirmation

☑ I understand the above recommendation and want to proceed to create an access key.

- Give some description tag like `CLI-Test` then click on `Create access key`



Set description tag - *optional* Info

The description for this access key will be attached to this user as a tag and shown alongside the access key.

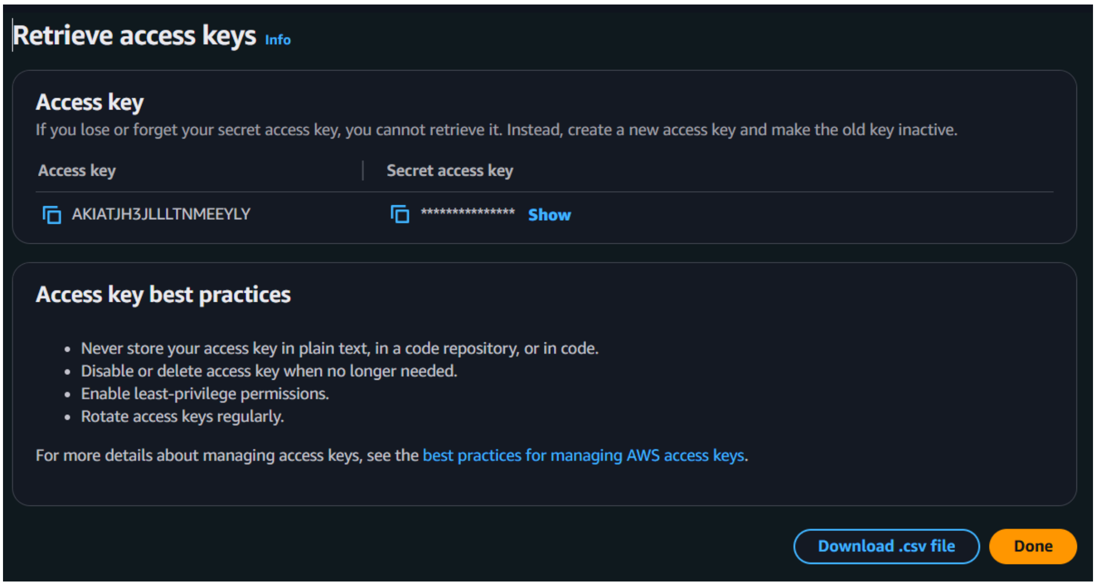
Description tag value

Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.

CLI-Test

Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . : / = + - @

- Download the `.csv` file with keys.



Retrieve access keys Info

Access key

If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIATJH3JLLLTNMEEYLY	*************** Show

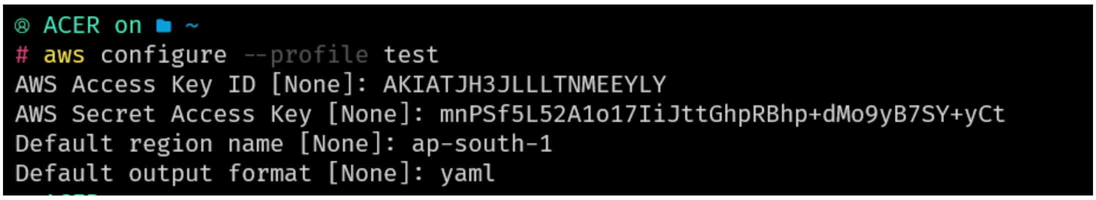
Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the best practices for managing AWS access keys.

- Configure AWS CLI for this user:

```
aws configure --profile test
```

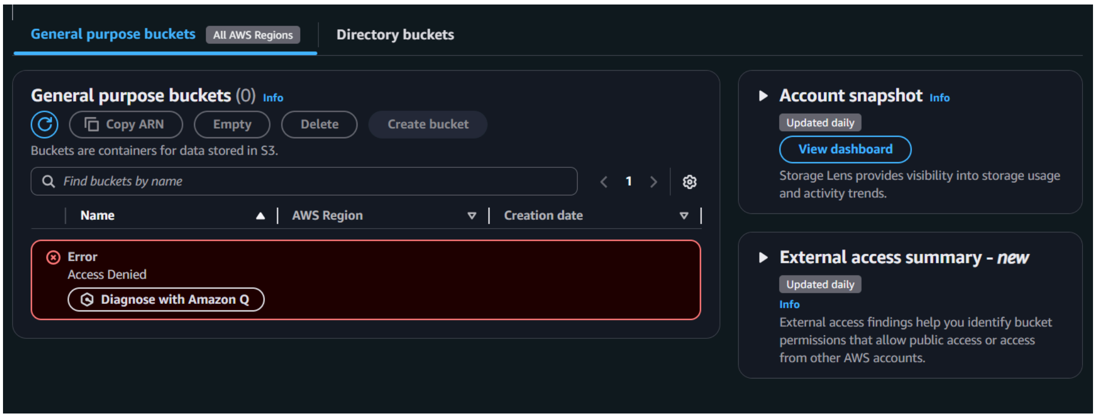


```
@ ACER on ~
# aws configure --profile test
AWS Access Key ID [None]: AKIATJH3JLLLTNMEEYLY
AWS Secret Access Key [None]: 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
Default region name [None]: ap-south-1
Default output format [None]: yaml
```

5. List Buckets (Missing Permission Fix)

Now, let’s try to access the policies we created earlier: `GetObject` (inline) and `DeleteBucket` (custom policy).

- As we can see, we cannot access the bucket from either the console or the terminal because we have not created a policy to list the buckets.



General purpose buckets (0) Info

Buckets are containers for data stored in S3.

Name	AWS Region	Creation date

Error
Access Denied
Diagnose with Amazon Q

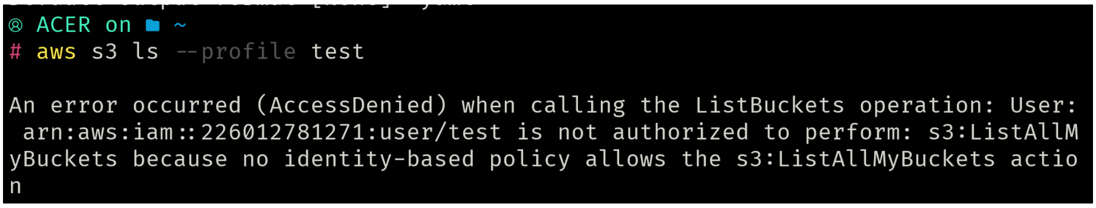
Account snapshot Info

Storage Lens provides visibility into storage usage and activity trends.

External access summary - *new*

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

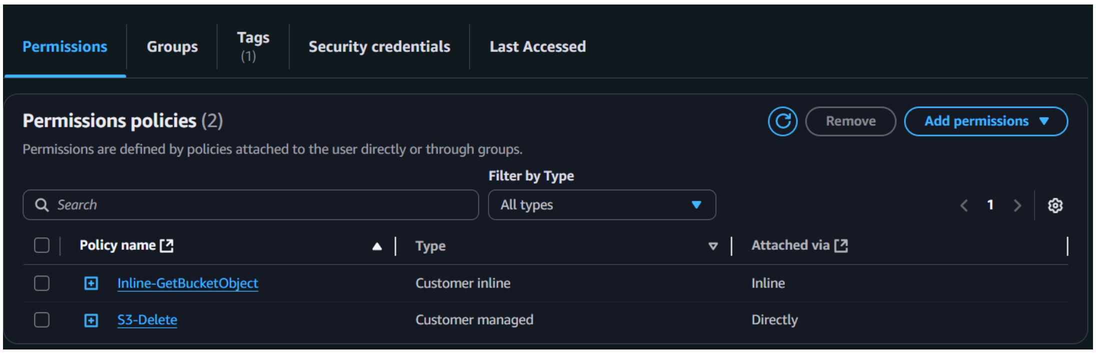
```
aws s3 ls --profile test
```



```
⊗ ACER on 🖿 ~
# aws s3 ls --profile test

An error occurred (AccessDenied) when calling the ListBuckets operation: User:
 arn:aws:iam::226012781271:user/test is not authorized to perform: s3:ListAllM
yBuckets because no identity-based policy allows the s3:ListAllMyBuckets actio
n
```

- So first, we need to give this user a **Bucket List Policy**. For that, we go inside the **Permissions** tab and click on **Add permissions** for the `test` user.

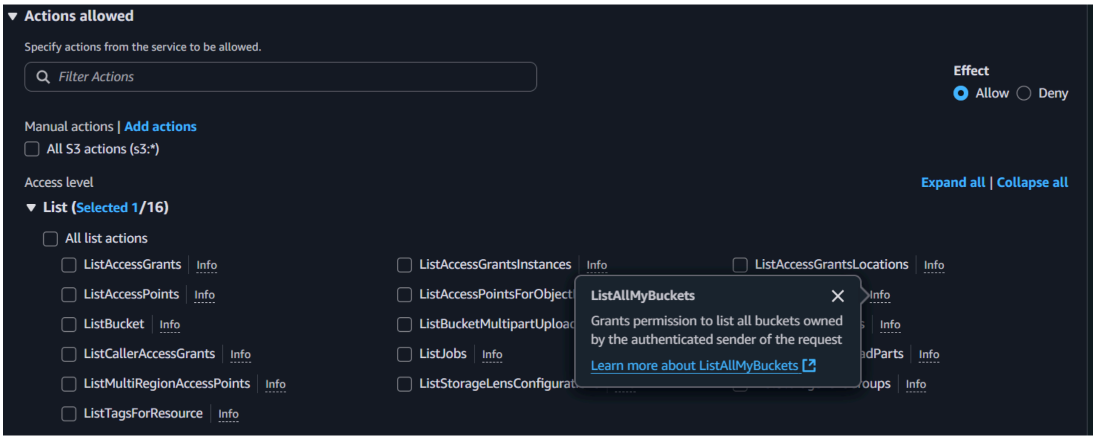


Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

□	Policy name	Type	Attached via
□	Inline-GetBucketObject	Customer inline	Inline
□	S3-Delete	Customer managed	Directly

- Here also, we are going to create an **inline policy** for S3 where the action will be `ListAllMyBuckets` and the resource will be `*`. We'll give this policy the name `S3BucketList`.



Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Effect: ● Allow ○ Deny

Manual actions | Add actions

□ All S3 actions (s3:*)

Access level

Expand all | Collapse all

List (Selected 1/16)

□ All list actions

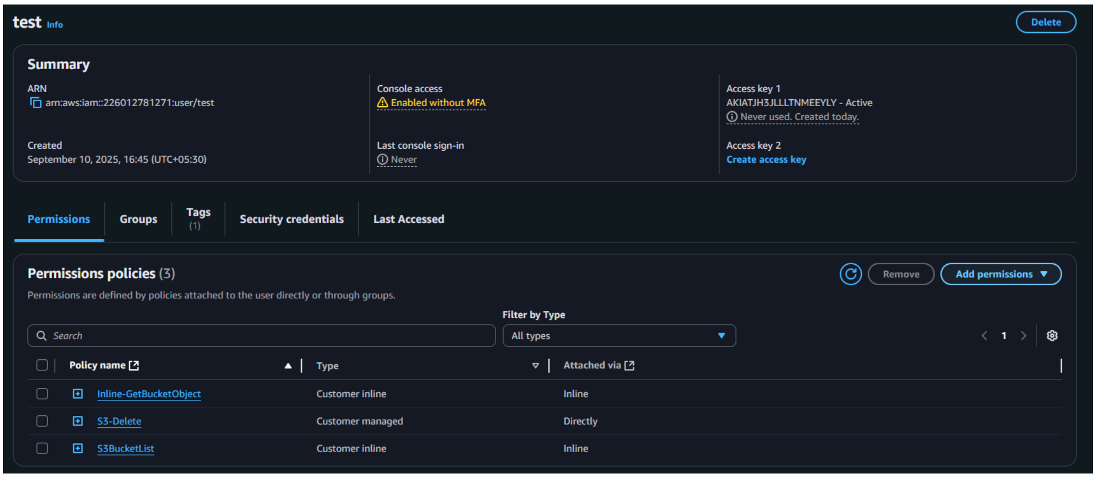
□ ListAccessGrants Info	□ ListAccessGrantsInstances Info	□ ListAccessGrantsLocations Info
□ ListAccessPoints Info	□ ListAccessPointsForObject	Info
□ ListBucket Info	□ ListBucketMultipartUploa	Info
□ ListCallerAccessGrants Info	□ ListJobs Info	adParts Info
□ ListMultiRegionAccessPoints Info	□ ListStorageLensConfigurat	oups Info
□ ListTagsForResource Info		

ListAllMyBuckets

Grants permission to list all buckets owned by the authenticated sender of the request

Learn more about ListAllMyBuckets

- As you can see, we have added this `S3BucketList` policy to the user `test`.



test Info

Delete

Summary

ARN
arn:aws:iam::226012781271:user/test

Created
September 10, 2025, 16:45 (UTC+05:30)

Console access
⚠ Enabled without MFA

Last console sign-in
Never

Access key 1
AKIATJH3JLLLTNMEEYLY - Active
Never used. Created today.

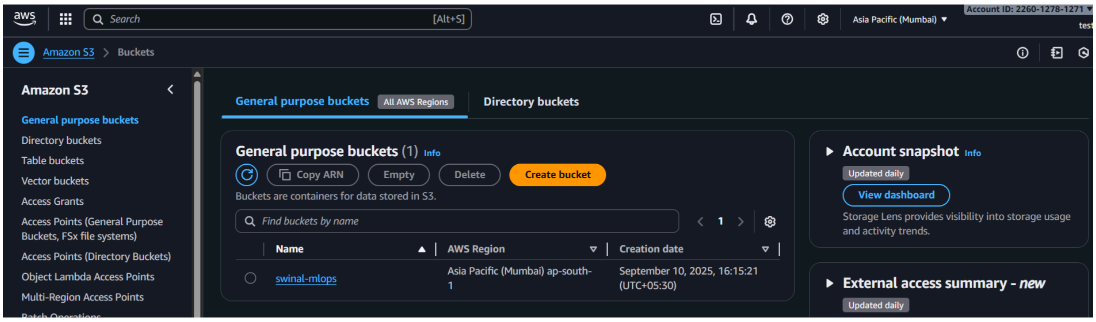
Access key 2
Create access key

Permissions policies (3)

Permissions are defined by policies attached to the user directly or through groups.

Policy name	Type	Attached via
Inline-GetBucketObject	Customer inline	Inline
S3-Delete	Customer managed	Directly
S3BucketList	Customer inline	Inline

- Now, let's try to access the S3 bucket from both the console and CLI. We can see that the user `test` is now able to access the `mlops-swinal` bucket.



General purpose buckets (1) Info

Buckets are containers for data stored in S3.

Name	AWS Region	Creation date
swinal-mlops	Asia Pacific (Mumbai) ap-south-1	September 10, 2025, 16:15:21 (UTC+05:30)

Account snapshot Info

Updated daily

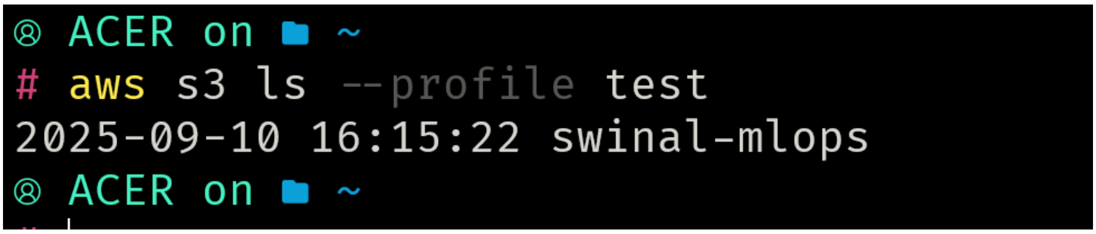
View dashboard

Storage Lens provides visibility into storage usage and activity trends.

External access summary - *new*

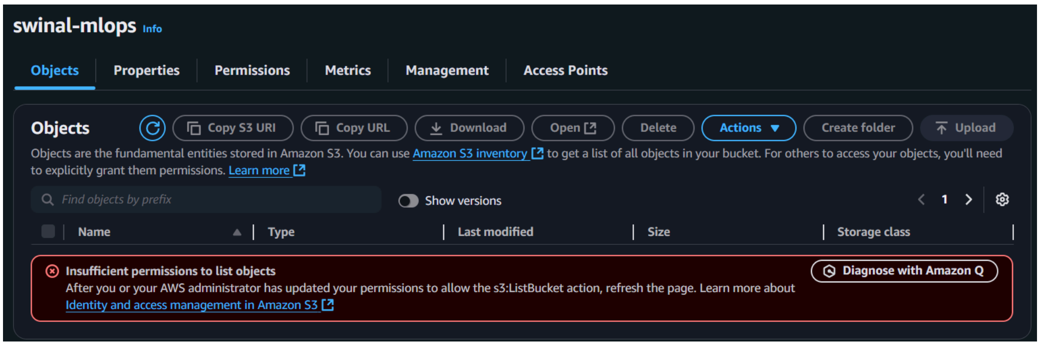
Updated daily

```
aws s3 ls --profile test
```



```
ACER on ~
# aws s3 ls --profile test
2025-09-10 16:15:22 swinal-mlops
ACER on ~
```

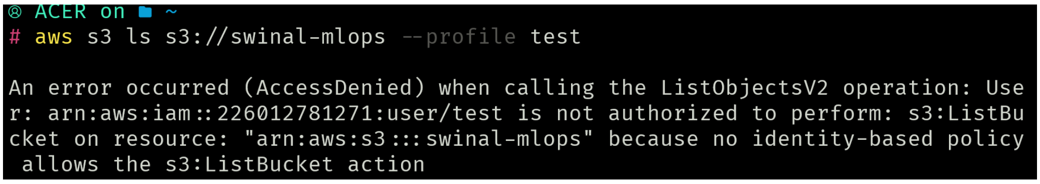
- Next, let’s try to get the objects from this bucket using both the console and CLI. We already created an inline policy for this: `inline-GetBucketObject`.
  - However, we encounter another error because we haven’t granted permission to list the objects inside the bucket. So, we need to create another inline policy.



Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Insufficient permissions to list objects
After you or your AWS administrator has updated your permissions to allow the s3:ListBucket action, refresh the page. Learn more about Identity and access management in Amazon S3

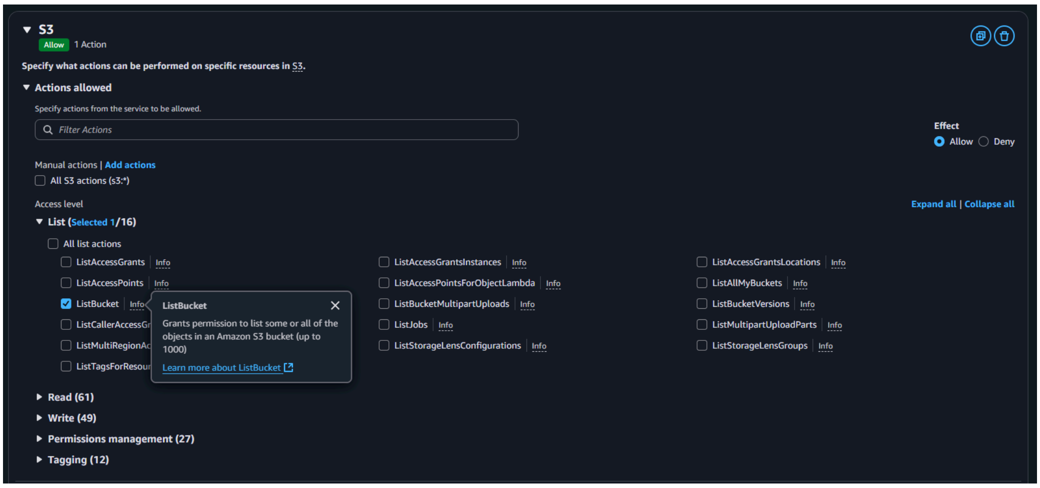
```
aws s3 ls s3://swinal-mlops --profile test
```



```
ACER on ~
# aws s3 ls s3://swinal-mlops --profile test

An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Use
r: arn:aws:iam::226012781271:user/test is not authorized to perform: s3:ListBu
cket on resource: "arn:aws:s3:::swinal-mlops" because no identity-based policy
 allows the s3:ListBucket action
```

  - We’ll create an inline policy that grants the `ListBucket` action, which allows the user to list all the objects inside the bucket. The resource will be `*`.



S3

Allow 1 Action

Specify what actions can be performed on specific resources in S3.

Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Effect

● Allow ○ Deny

Manual actions | Add actions

□ All S3 actions (s3:*)

Access level

Expand all | Collapse all

List (Selected 1/16)

□ All list actions

□ ListAccessGrants Info	□ ListAccessGrantsInstances Info	□ ListAccessGrantsLocations Info
□ ListAccessPoints Info	□ ListAccessPointsForObjectLambda Info	□ ListAllMyBuckets Info
☑ ListBucket Info	□ ListBucketMultipartUploads Info	□ ListBucketVersions Info
□ ListCallerAccessGr	□ ListJobs Info	□ ListMultipartUploadParts Info
□ ListMultiRegionAc	□ ListStorageLensConfigurations Info	□ ListStorageLensGroups Info
□ ListTagsForResour		

ListBucket

Grants permission to list some or all of the objects in an Amazon S3 bucket (up to 1000)

Learn more about ListBucket

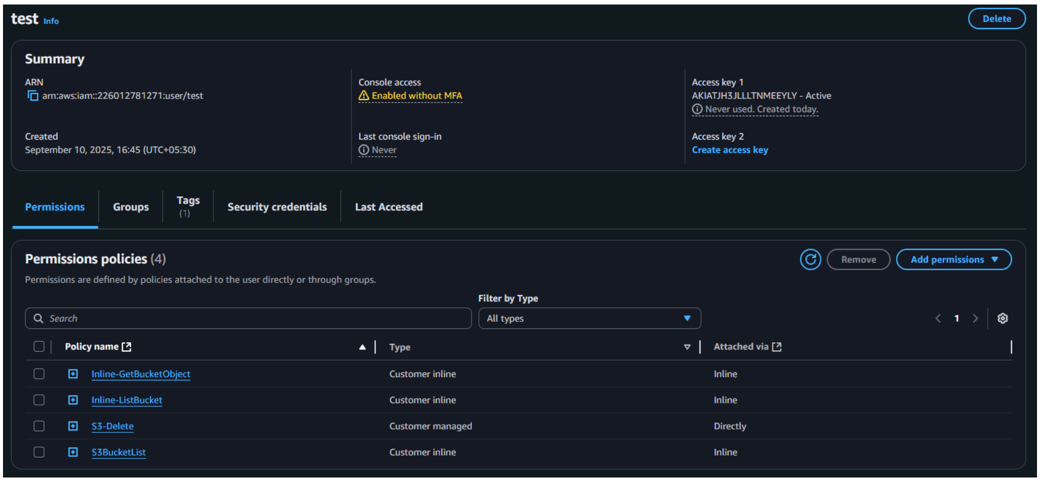
Read (61)

Write (49)

Permissions management (27)

Tagging (12)

- Let's name this policy Inline-ListBucket. Once created, this policy gets attached to the user test.



test Info

Delete

Summary

ARN
arn:aws:iam::226012781271:user/test

Created
September 10, 2025, 16:45 (UTC+05:30)

Console access
Enabled without MFA

Last console sign-in
Never

Access key 1
AKIATJH3JLLLTNMEEYLY - Active
Never used. Created today.

Access key 2
Create access key

Permissions | Groups | Tags (1) | Security credentials | Last Accessed

Permissions policies (4)

Remove | Add permissions

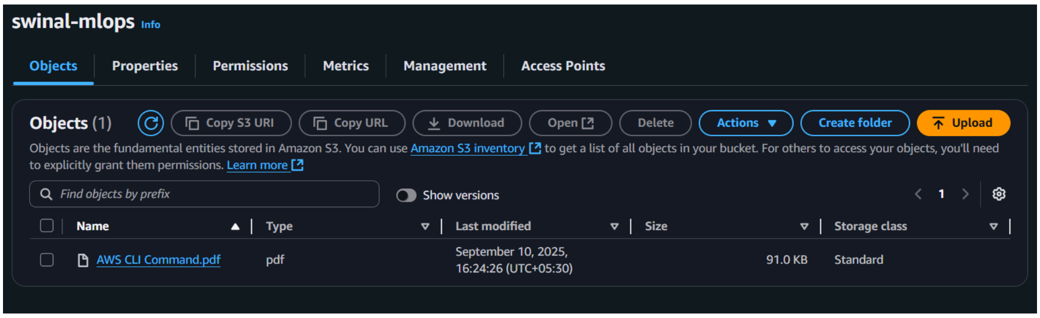
Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: All types

Search

Policy name	Type	Attached via
Inline-GetBucketObject	Customer inline	Inline
Inline-ListBucket	Customer inline	Inline
S3-Delete	Customer managed	Directly
S3BucketList	Customer inline	Inline

- Now, let's test it again in the console and CLI. The user can successfully list the objects inside the bucket.



swinal-mlops Info

Objects | Properties | Permissions | Metrics | Management | Access Points

Objects (1)

Copy S3 URI | Copy URL | Download | Open | Delete | Actions | Create folder | Upload

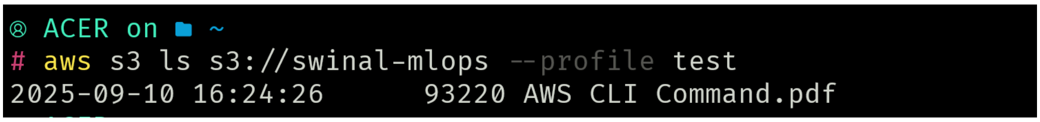
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Find objects by prefix

Show versions

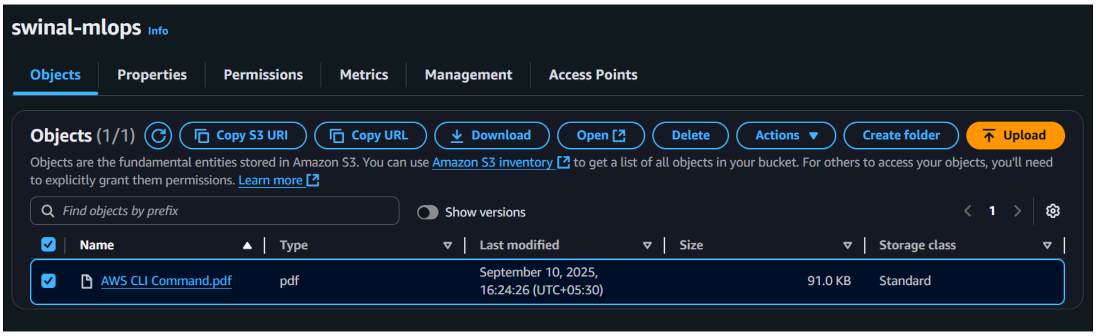
Name	Type	Last modified	Size	Storage class
AWS CLI Command.pdf	pdf	September 10, 2025, 16:24:26 (UTC+05:30)	91.0 KB	Standard

```
aws s3 ls s3://swinal-mlops --profile test
```



```
ACER on  ~
# aws s3 ls s3://swinal-mlops --profile test
2025-09-10 16:24:26      93220 AWS CLI Command.pdf
```

- The **GetObject** inline policy allows the user to download objects.

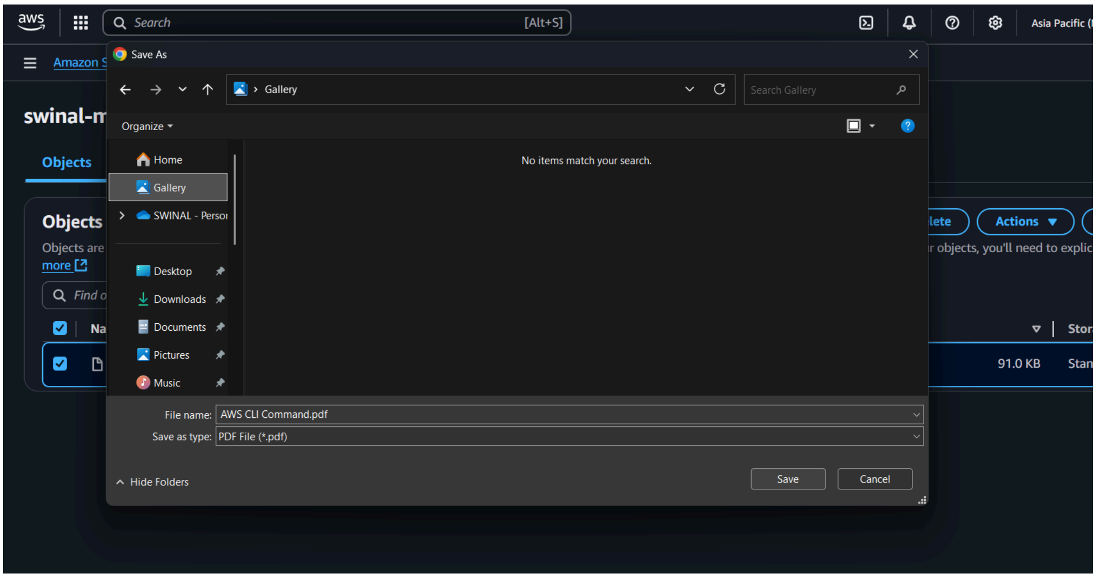


swinal-mlops Info

Objects (1/1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

☑	Name	Type	Last modified	Size	Storage class
☑	AWS CLI Command.pdf	pdf	September 10, 2025, 16:24:26 (UTC+05:30)	91.0 KB	Standard

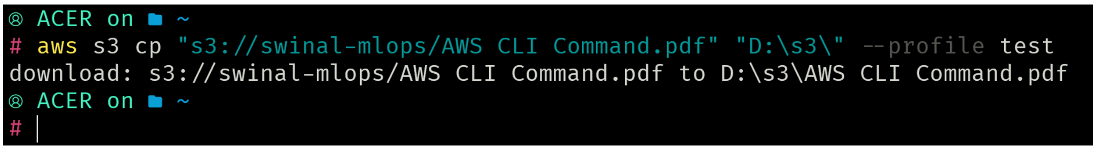


No items match your search.

File name: AWS CLI Command.pdf

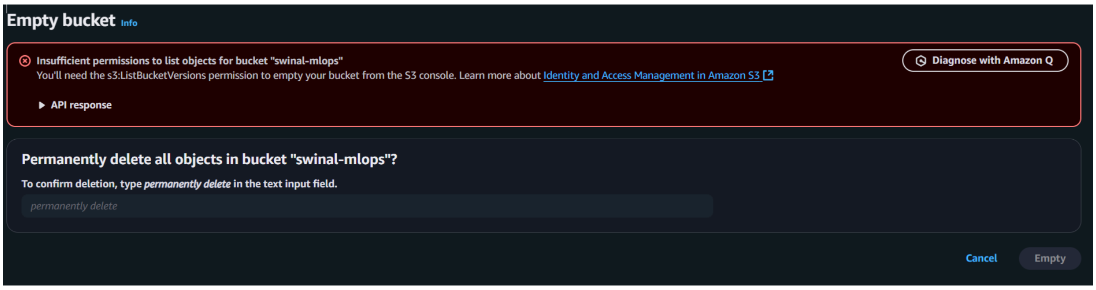
Save as type: PDF File (*.pdf)

```
aws s3 cp "s3://swinal-mlops/AWS CLI Command.pdf" "D:\s3\" --profile test
```



```
ACER on  ~
# aws s3 cp "s3://swinal-mlops/AWS CLI Command.pdf" "D:\s3\" --profile test
download: s3://swinal-mlops/AWS CLI Command.pdf to D:\s3\AWS CLI Command.pdf
ACER on  ~
# |
```

- Next, let's try to delete the bucket. Before deleting a bucket, it must be emptied first. Since we don't have permission to delete objects, we need another inline policy.



Empty bucket Info

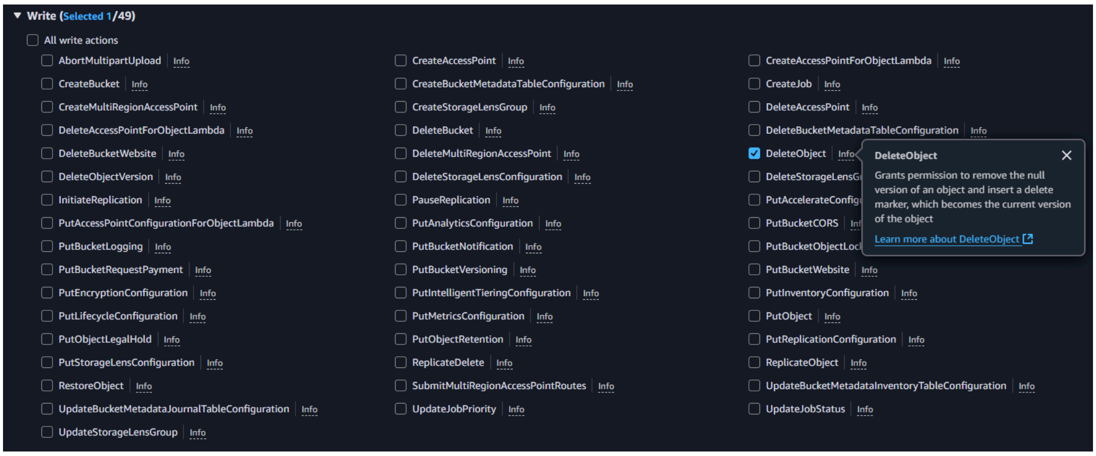
Insufficient permissions to list objects for bucket "swinal-mlops"
You'll need the s3:ListBucketVersions permission to empty your bucket from the S3 console. Learn more about Identity and Access Management in Amazon S3

Permanently delete all objects in bucket "swinal-mlops"?

To confirm deletion, type *permanently delete* in the text input field.

- We'll create an inline policy with the following permissions: `DeleteObject` , `DeleteBucketVersion` , and `ListBucketVersions` . The resource will be `*` , and the policy will be named `Inline-DeleteObject` .

> 💡 This all i achieved by just try and error.



▼ Write (Selected 1/49)

☐ All write actions

☐ AbortMultipartUpload
☐ CreateBucket
☐ CreateMultiRegionAccessPoint
☐ DeleteAccessPointForObjectLambda
☐ DeleteBucketWebsite
☐ DeleteObjectVersion
☐ InitiateReplication
☐ PutAccessPointConfigurationForObjectLambda
☐ PutBucketLogging
☐ PutBucketRequestPayment
☐ PutEncryptionConfiguration
☐ PutLifecycleConfiguration
☐ PutObjectLegalHold
☐ PutStorageLensConfiguration
☐ RestoreObject
☐ UpdateBucketMetadataJournalTableConfiguration
☐ UpdateStorageLensGroup

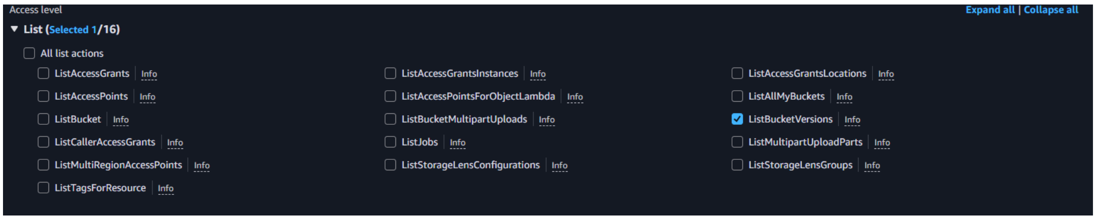
☐ CreateAccessPoint
☐ CreateBucketMetadataTableConfiguration
☐ CreateStorageLensGroup
☐ DeleteBucket
☐ DeleteMultiRegionAccessPoint
☐ DeleteStorageLensConfiguration
☐ PauseReplication
☐ PutAnalyticsConfiguration
☐ PutBucketNotification
☐ PutBucketVersioning
☐ PutIntelligentTieringConfiguration
☐ PutMetricsConfiguration
☐ PutObjectRetention
☐ ReplicateDelete
☐ SubmitMultiRegionAccessPointRoutes
☐ UpdateJobPriority

☐ CreateAccessPointForObjectLambda
☐ CreateJob
☐ DeleteAccessPoint
☐ DeleteBucketMetadataTableConfiguration
☑ DeleteObject
☐ DeleteStorageLensG
☐ PutAccelerateConfig
☐ PutBucketCORS
☐ PutBucketObjectLoc
☐ PutBucketWebsite
☐ PutInventoryConfiguration
☐ PutObject
☐ PutReplicationConfiguration
☐ ReplicateObject
☐ UpdateBucketMetadataInventoryTableConfiguration
☐ UpdateJobStatus

DeleteObject

Grants permission to remove the null version of an object and insert a delete marker, which becomes the current version of the object

Learn more about DeleteObject



Access level

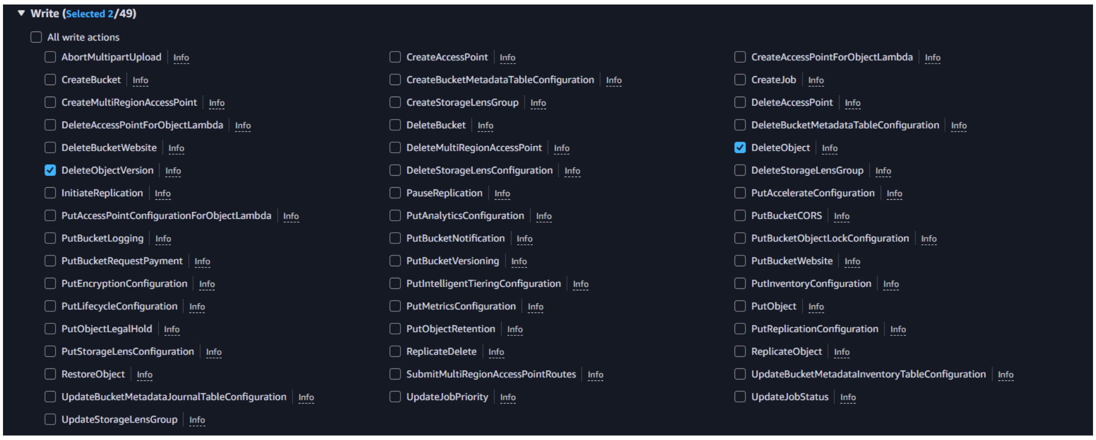
▼ List (Selected 1/16)

☐ All list actions

☐ ListAccessGrants
☐ ListAccessPoints
☐ ListBucket
☐ ListCallerAccessGrants
☐ ListMultiRegionAccessPoints
☐ ListTagsForResource

☐ ListAccessGrantsInstances
☐ ListAccessPointsForObjectLambda
☐ ListBucketMultipartUploads
☐ ListJobs
☐ ListStorageLensConfigurations

☐ ListAccessGrantsLocations
☐ ListAllMyBuckets
☑ ListBucketVersions
☐ ListMultipartUploadParts
☐ ListStorageLensGroups



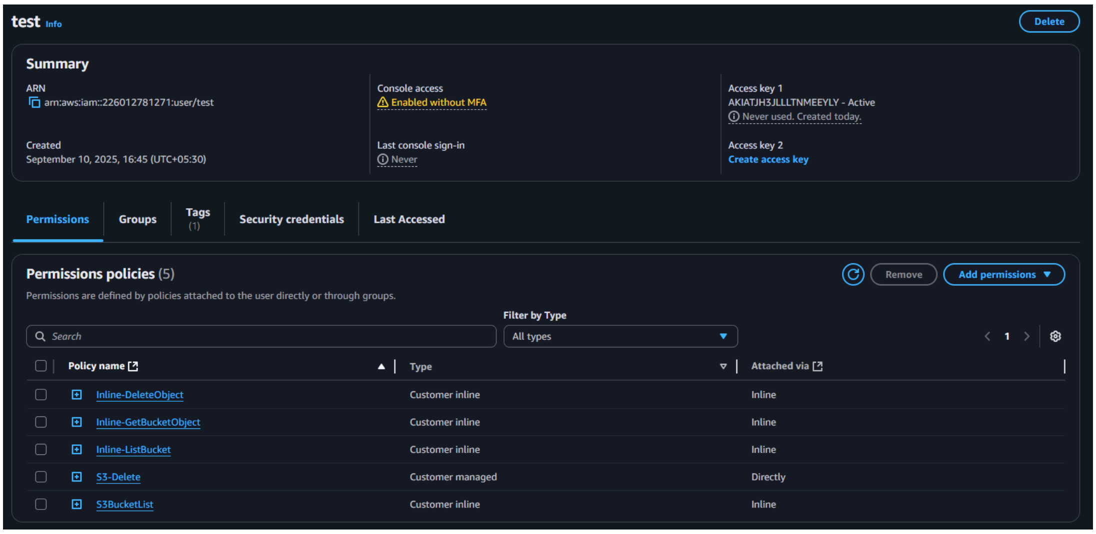
▼ Write (Selected 2/49)

☐ All write actions

☐ AbortMultipartUpload
☐ CreateBucket
☐ CreateMultiRegionAccessPoint
☐ DeleteAccessPointForObjectLambda
☐ DeleteBucketWebsite
☑ DeleteObjectVersion
☐ InitiateReplication
☐ PutAccessPointConfigurationForObjectLambda
☐ PutBucketLogging
☐ PutBucketRequestPayment
☐ PutEncryptionConfiguration
☐ PutLifecycleConfiguration
☐ PutObjectLegalHold
☐ PutStorageLensConfiguration
☐ RestoreObject
☐ UpdateBucketMetadataJournalTableConfiguration
☐ UpdateStorageLensGroup

☐ CreateAccessPoint
☐ CreateBucketMetadataTableConfiguration
☐ CreateStorageLensGroup
☐ DeleteBucket
☐ DeleteMultiRegionAccessPoint
☐ DeleteStorageLensConfiguration
☐ PauseReplication
☐ PutAnalyticsConfiguration
☐ PutBucketNotification
☐ PutBucketVersioning
☐ PutIntelligentTieringConfiguration
☐ PutMetricsConfiguration
☐ PutObjectRetention
☐ ReplicateDelete
☐ SubmitMultiRegionAccessPointRoutes
☐ UpdateJobPriority

☐ CreateAccessPointForObjectLambda
☐ CreateJob
☐ DeleteAccessPoint
☐ DeleteBucketMetadataTableConfiguration
☑ DeleteObject
☐ DeleteStorageLensGroup
☐ PutAccelerateConfiguration
☐ PutBucketCORS
☐ PutBucketObjectLockConfiguration
☐ PutBucketWebsite
☐ PutInventoryConfiguration
☐ PutObject
☐ PutReplicationConfiguration
☐ ReplicateObject
☐ UpdateBucketMetadataInventoryTableConfiguration
☐ UpdateJobStatus



test Info

Summary

ARN
arn:aws:iam::226012781271:user/test

Created
September 10, 2025, 16:45 (UTC+05:30)

Console access
⚠ Enabled without MFA

Last console sign-in
Never

Access key 1
AKIATJH3JLLLTNMEEYLY - Active
Never used. Created today.

Access key 2
Create access key

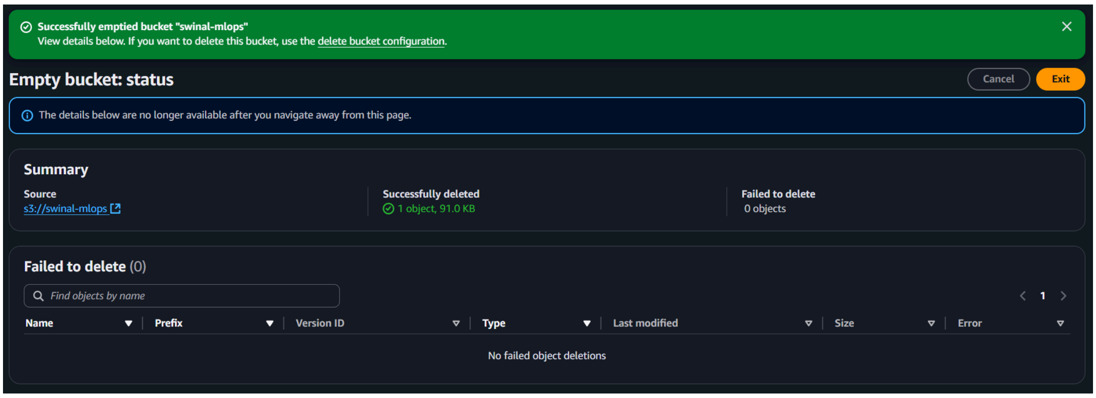
Permissions policies (5)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: All types

Policy name	Type	Attached via
Inline-DeleteObject	Customer inline	Inline
Inline-GetBucketObject	Customer inline	Inline
Inline-ListBucket	Customer inline	Inline
S3-Delete	Customer managed	Directly
S3BucketList	Customer inline	Inline

- After attaching the policy, we can now empty the bucket and delete it using both the console and CLI:



Successfully emptied bucket "swinal-mlops"
View details below. If you want to delete this bucket, use the delete bucket configuration.

Empty bucket: status

The details below are no longer available after you navigate away from this page.

Summary

Source
s3://swinal-mlops

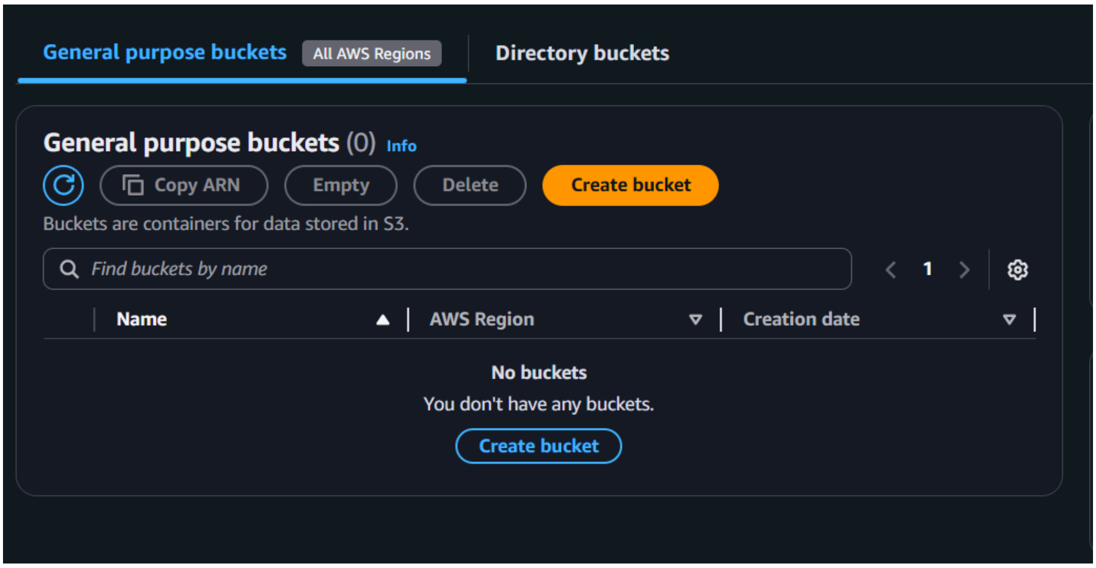
Successfully deleted
1 object, 91.0 KB

Failed to delete
0 objects

Failed to delete (0)

Name	Prefix	Version ID	Type	Last modified	Size	Error

No failed object deletions



General purpose buckets (0) Info

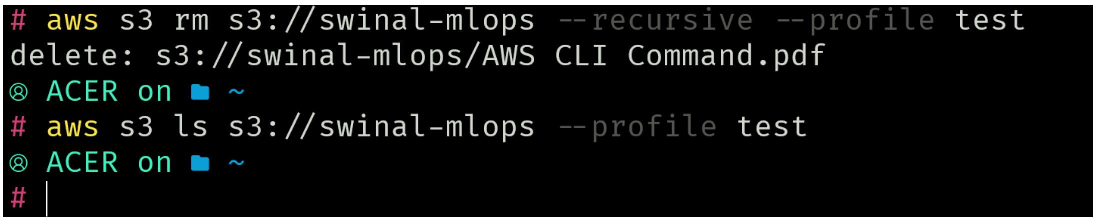
Buckets are containers for data stored in S3.

Name	AWS Region	Creation date

No buckets

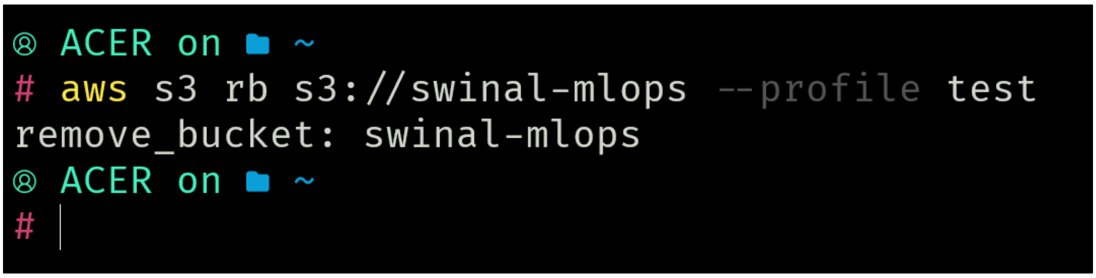
You don't have any buckets.

```
aws s3 rm s3://swinal-mlops --recursive --profile test
```



```
# aws s3 rm s3://swinal-mlops --recursive --profile test
delete: s3://swinal-mlops/AWS CLI Command.pdf
@ ACER on 🖿 ~
# aws s3 ls s3://swinal-mlops --profile test
@ ACER on 🖿 ~
#
```

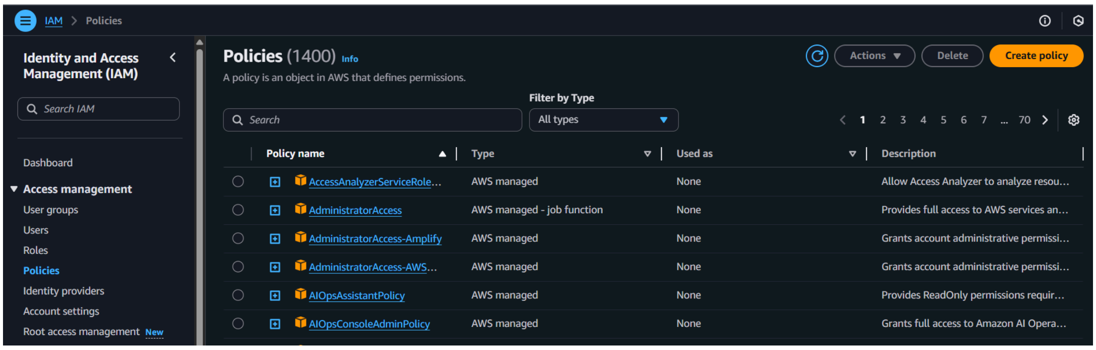
```
aws s3 rb s3://swinal-mlops --profile test
```



```
@ ACER on 🖿 ~
# aws s3 rb s3://swinal-mlops --profile test
remove_bucket: swinal-mlops
@ ACER on 🖿 ~
#
```

▼ 6. Create policy for ec2 creation only not full access

- Now, let's create a custom policy for EC2 instance creation. Go to **Policies → Create Policy**, and this time we'll use the **JSON editor**:



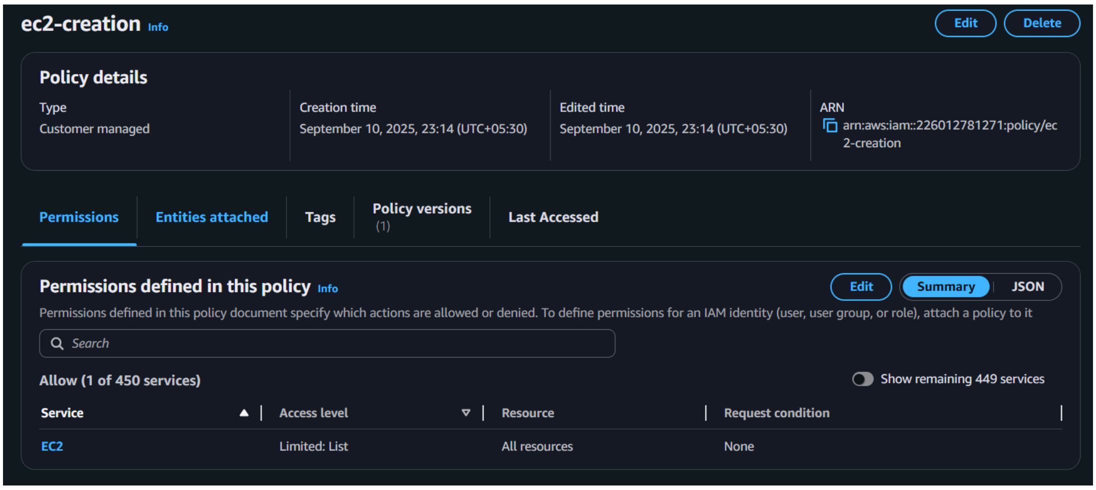
Policies (1400) Info

A policy is an object in AWS that defines permissions.

Policy name	Type	Used as	Description
AccessAnalyzerServiceRole...	AWS managed	None	Allow Access Analyzer to analyze resou...
AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissi...
AdministratorAccess-AWS...	AWS managed	None	Grants account administrative permissi...
AIOpsAssistantPolicy	AWS managed	None	Provides ReadOnly permissions requir...
AIOpsConsoleAdminPolicy	AWS managed	None	Grants full access to Amazon AI Opera...

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RunInstances",
        "ec2:CreateTags",
        "ec2:DescribeVolumes"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

- We’ll name this policy `ec2-creation` and attach it to the user `test`.



ec2-creation Info

Policy details

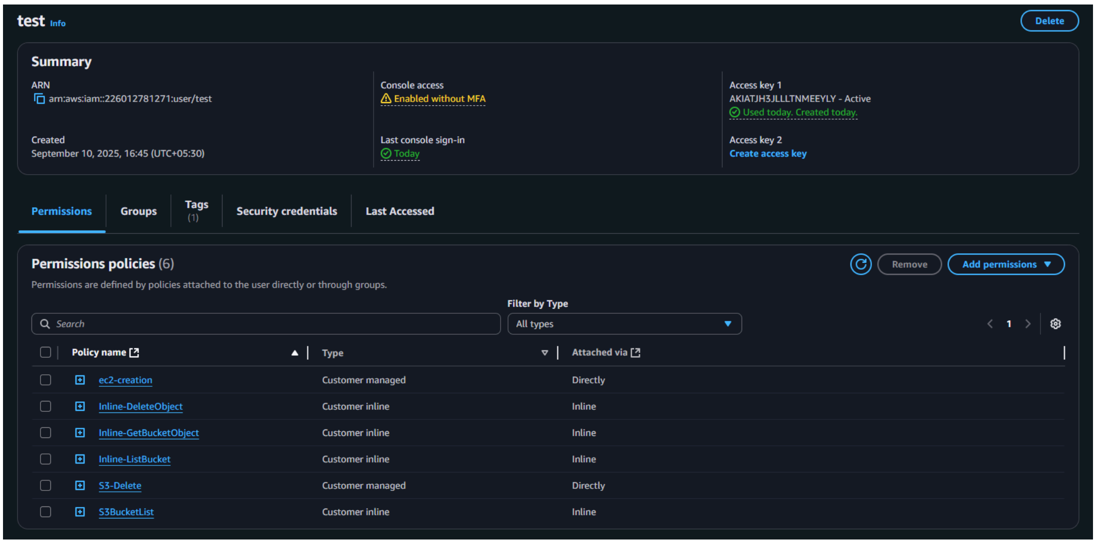
Type	Creation time	Edited time	ARN
Customer managed	September 10, 2025, 23:14 (UTC+05:30)	September 10, 2025, 23:14 (UTC+05:30)	arn:aws:iam::226012781271:policy/ec2-creation

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (1 of 450 services)

Service	Access level	Resource	Request condition
EC2	Limited: List	All resources	None



test Info

Summary

ARN
arn:aws:iam::226012781271:user/test

Created
September 10, 2025, 16:45 (UTC+05:30)

Console access
⚠ Enabled without MFA

Last console sign-in
✓ Today

Access key 1
AKIATJH3JLLLTNMEEYLY - Active
✓ Used today. Created today.

Access key 2
Create access key

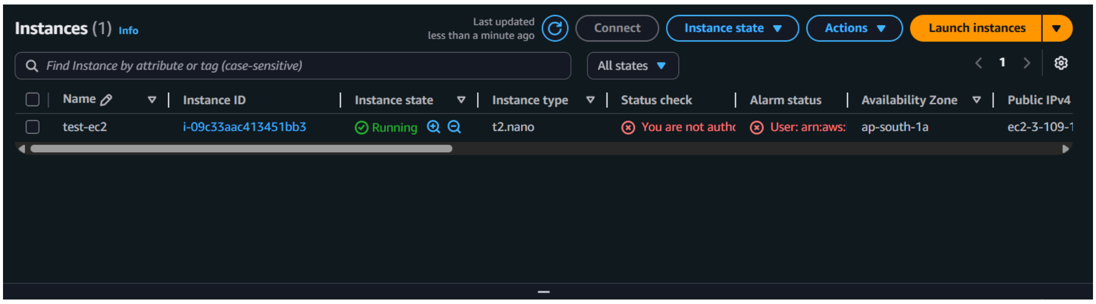
Permissions policies (6)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: All types

Policy name	Type	Attached via
ec2-creation	Customer managed	Directly
Inline-DeleteObject	Customer inline	Inline
Inline-GetBucketObject	Customer inline	Inline
Inline-ListBucket	Customer inline	Inline
S3-Delete	Customer managed	Directly
S3BucketList	Customer inline	Inline

- The user can now successfully launch an EC2 instance.



Instances (1) Info

Last updated less than a minute ago

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
test-ec2	i-09c33aac413451bb3	Running	t2.nano	You are not authc	User: arn:aws:	ap-south-1a	ec2-3-109-1

7. Create Policy with Mixed Permissions

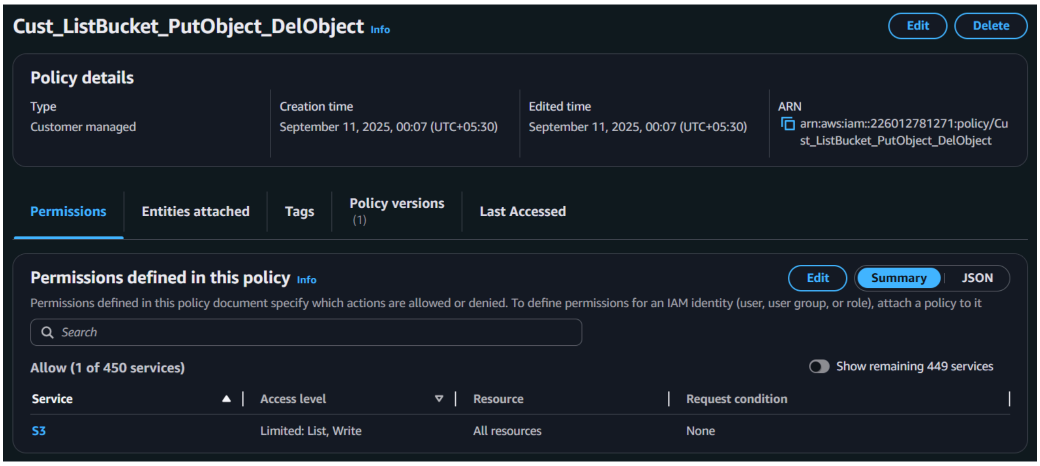
1. **Allow Bucket List, PutObject, and DeleteObject**

    - So we are creating a custom policy using json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "*"
```

```
            ]
        }
    ]
}
```

- This policy is named `Cust_ListBucket_PutObject_DelObject`.



Cust_ListBucket_PutObject_DelObject Info

Policy details

Type	Creation time	Edited time	ARN
Customer managed	September 11, 2025, 00:07 (UTC+05:30)	September 11, 2025, 00:07 (UTC+05:30)	arn:aws:iam::226012781271:policy/Cust_ListBucket_PutObject_DelObject

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

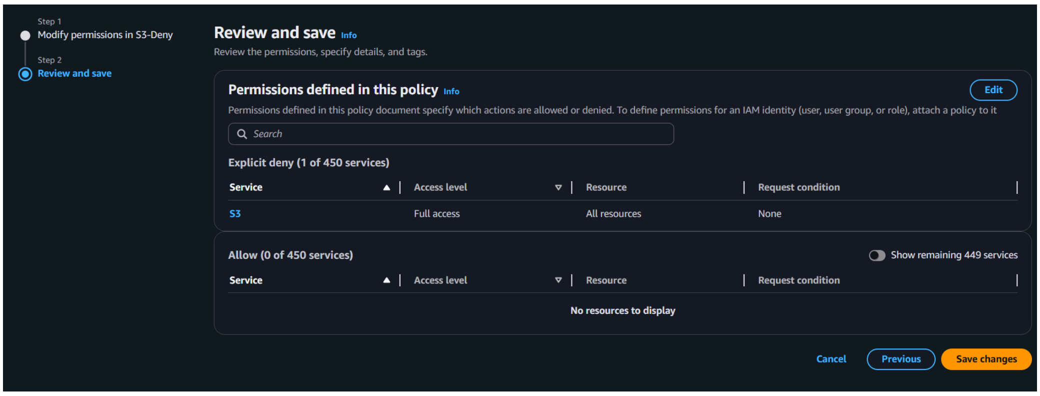
Allow (1 of 450 services)

Service	Access level	Resource	Request condition
S3	Limited: List, Write	All resources	None

2. Deny All S3 Permissions (using Inline Policy)

- Now lets give deny permission for S3 using `inline policy`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```



Review and save Info

Review the permissions, specify details, and tags.

Permissions defined in this policy Info

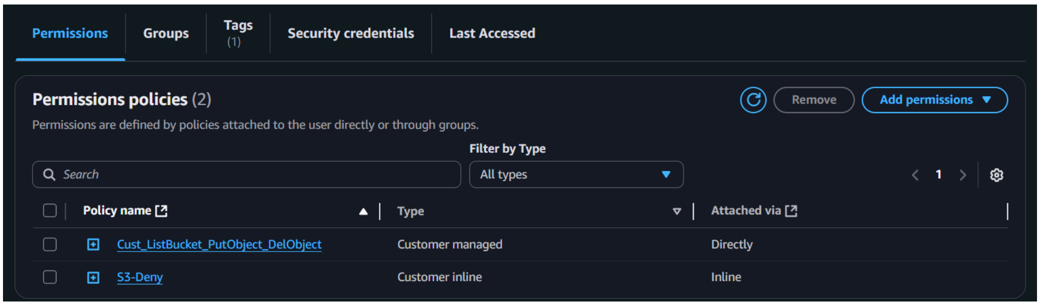
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Explicit deny (1 of 450 services)

Service	Access level	Resource	Request condition
S3	Full access	All resources	None

Allow (0 of 450 services)

Service	Access level	Resource	Request condition
No resources to display			



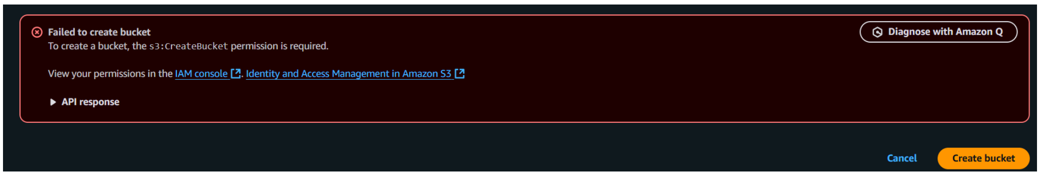
Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: All types

□	Policy name	Type	Attached via
□	Cust_ListBucket_PutObject_DelObject	Customer managed	Directly
□	S3-Deny	Customer inline	Inline

- After creating this deny policy and attaching it, when we try to access or create an S3 bucket, we get an **Access Denied** error (as expected).



Failed to create bucket

To create a bucket, the `s3:CreateBucket` permission is required.

View your permissions in the IAM console. Identity and Access Management in Amazon S3