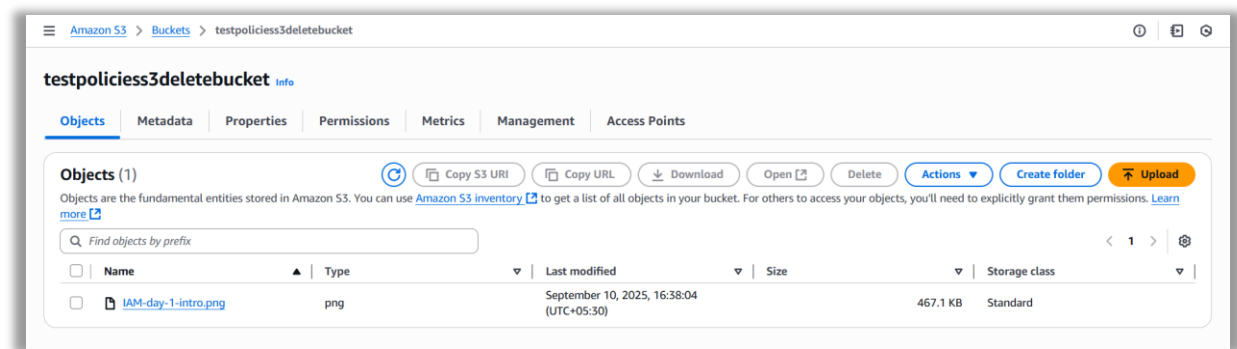
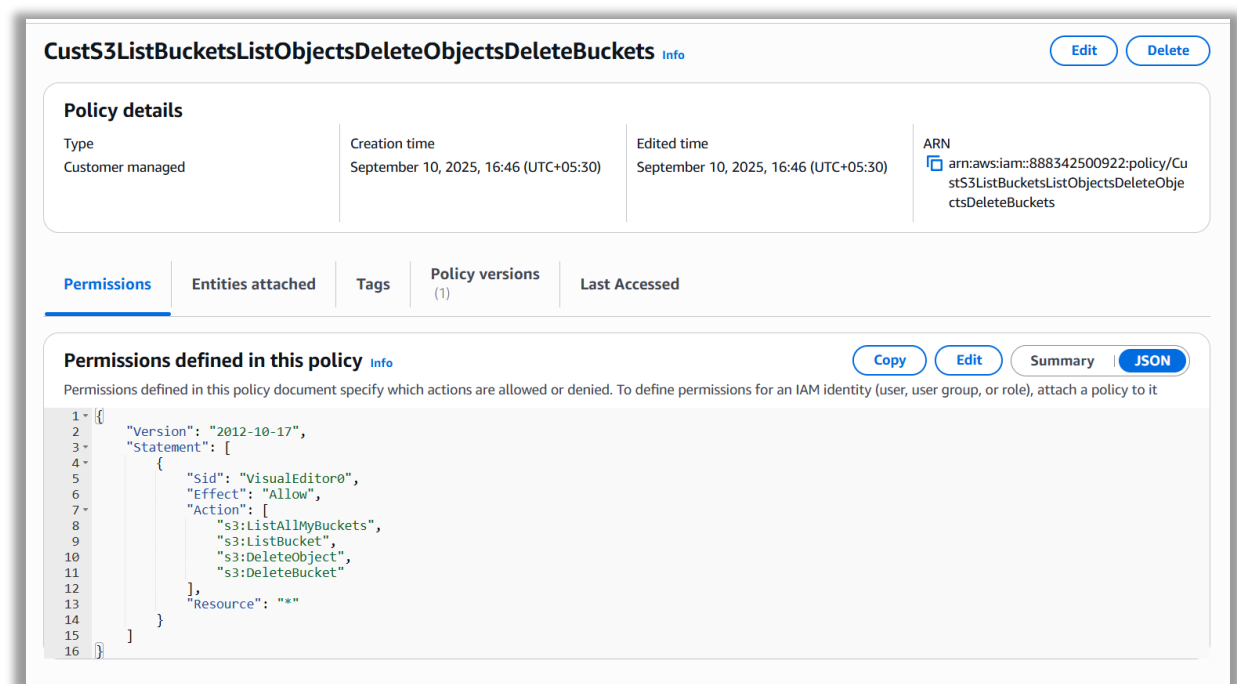


Create Bucket Object by Root



Create Delete Bucket Custom Policy



Create IAM user and attach custom policy

TestPoliciesIAMUser

Info

Delete

Summary

ARN
arn:aws:iam::888342500922:user/TestPoliciesIAMUser

Console access
Disabled

Access key 1
[Create access key](#)

Created
September 10, 2025, 16:49 (UTC+05:30)

Last console sign-in
-

Permissions

Groups

Tags

Security credentials

Last Accessed

Permissions policies (1)

Remove

Add permissions

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

Search

Filter by Type
All types

< 1 >

☐

Policy name

▲

Type

▼

Attached via

☐

[CustS3ListBucketsListObjectsDeleteObjects...](#)

Customer managed

Directly

Created Inline Policy “GetObject”

Policy editor

Visual

JSON

Actions

1 {
2 "Version": "2012-10-17",
3 "Statement": [
4 {
5 "Sid": "VisualEditor0",
6 "Effect": "Allow",
7 "Action": "s3:GetObject",
8 "Resource": "*"
9 },
10 {
11 "Sid": "VisualEditor1",
12 "Effect": "Allow",
13 "Action": "s3:GetObject",
14 "Resource": "arn:aws:s3:::testpoliciess3deletebucket/*"
15 }
16]
17 }

Edit statement

Select a statement

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

+ Add new statement

Attached the Inline policy to IAM user

TestPoliciesIAMUser [Info](#) [Delete](#)

Summary

ARN arn:aws:iam::888342500922:user/TestPoliciesIAMUser	Console access Disabled	Access key 1 Create access key
Created September 10, 2025, 16:49 (UTC+05:30)	Last console sign-in -	

Permissions | Groups | Tags | Security credentials | Last Accessed

Permissions policies (2) [Refresh](#) [Remove](#) [Add permissions](#)

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

Search Filter by Type [All types](#) [< 1 >](#) [Settings](#)

<input type="checkbox"/>	Policy name ?	Type	Attached via ?
<input type="checkbox"/>	CustS3ListBucketsListObjectsDeleteObjects...	Customer managed	Directly
<input type="checkbox"/>	DownloadObject	Customer inline	Inline

Download Tested from Console:

testpolicieess3deletebucket [Info](#)

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

Objects (1/1) [Refresh](#) [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

<input checked="" type="checkbox"/>	Name	Type
<input checked="" type="checkbox"/>	IAM-day-1-intro.png	png

Storage class: [Standard](#)

467.1 KB

Save As dialog box: File name: [IAM-day-1-intro.png](#), Save as type: PNG Image (*.png)

List the object and s3 bucket through CLI:

```
C:\>aws s3 ls
2025-09-10 16:37:34 testpolicieess3deletebucket

C:\>aws s3 ls s3://testpolicieess3deletebucket/
2025-09-10 16:38:04      478262 IAM-day-1-intro.png

C:\>
```

Policy for create EC2 only

CustLaunchEC2Instance

Info

EditDelete

Policy details

Type

Customer managed

Creation time

September 11, 2025, 09:54 (UTC+05:30)

Edited time

September 11, 2025, 09:54 (UTC+05:30)

ARN

arn:aws:iam::888342500922:policy/CustLaunchEC2Instance

Permissions

Entities attached

Tags

Policy versions

Last Accessed

Permissions defined in this policy

Info

CopyEditSummaryJSON

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

1 {

2 "Version": "2012-10-17",

3 "Statement": [

4 {

5 "Sid": "VisualEditor0",

6 "Effect": "Allow",

7 "Action": "ec2:RunInstances",

8 "Resource": "*"

9 }

10]

11 }

Custom policy for entire S3 allow deny

One statement with few permissions – bucket list, put object, delete object

Another statement for the same policy deny permissions for entire s3

Policy editor

VisualJSONActions

1 {

2 "Version": "2012-10-17",

3 "Statement": [

4 {

5 "Sid": "AllowS3ListPutDelete",

6 "Effect": "Allow",

7 "Action": [

8 "s3:PutObject",

9 "s3:ListAllMyBuckets",

10 "s3:ListBucket",

11 "s3:DeleteObject"

12],

13 "Resource": "*"

14 },

15 {

16 "Sid": "DenyEntireS3",

17 "Effect": "Deny",

18 "Action": [

19 "s3:*"

20],

21 "Resource": "*"

22 }

23]

24 }

Edit statement

DenyEntireS3

Remove

Add actions

Choose a service

Filter services

Included

S3

Available

AI Operations

AMP

API Gateway

API Gateway V2

ARC Region switch

ARC Zonal Shift

ASC

Add a resource

Add

TestPoliciesIAMUser [Info](#)

[Delete](#)

Summary

ARN
[arn:aws:iam::888342500922:user/TestPoliciesIAMUser](#)

Console access
[Enabled without MFA](#)

Access key 1
AKIA45VKW2Y5IV6BJNFE - Active
[Used 16 hours ago. 16 hours old.](#)

Created
September 10, 2025, 16:49 (UTC+05:30)

Last console sign-in
[17 hours ago](#)

Access key 2
[Create access key](#)

Permissions

Groups

Tags
(1)

Security credentials

Last Accessed

Permissions policies (3)



[Remove](#)

[Add permissions](#) ▼

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

Filter by Type		
<input type="text" value="Search"/>	<div>All types ▼</div>	<div>< 1 > ⚙</div>
<input type="checkbox"/> Policy name ?	<input type="checkbox"/> Type	<input type="checkbox"/> Attached via ?
<input type="checkbox"/> CustPolicyEntireS3AllowDeny	Customer managed	Directly
<input type="checkbox"/> CustS3ListBucketsListObjectsDeleteObjects...	Customer managed	Directly
<input type="checkbox"/> DownloadObject	Customer inline	Inline