

1. Create users and attach custom policy for delete bucket.

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Users (1) Info

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

Search

1

<input type="checkbox"/>	User name	Path	Group	Last activity	MFA	Password age	Console
<input type="checkbox"/>	user-test	/	0	-	-	3 minutes	-

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/user-test/permissions-policies

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Permissions policies (2)

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

Filter by Type

Search

All types

<input type="checkbox"/>	Policy name	Type	Attached via
<input type="checkbox"/>	deleteBucket	Customer managed	Directly
<input type="checkbox"/>	IAMUserChangePassword	AWS managed	Directly

Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#)

eu-north-1.console.aws.amazon.com/s3/buckets?region=eu-north-1

Amazon S3

General purpose buckets

Directory buckets

Table buckets

Vector buckets

Access Grants

Access Points (General Purpose Buckets, FSx file systems)

Access Points (Directory Buckets)

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

General purpose buckets (2) Info

Buckets are containers for data stored in S3.

Find buckets by name

<input type="radio"/>	Name	AWS Region	Creation date
<input type="radio"/>	ms3buckettt	US East (N. Virginia) us-east-1	September 10, 2025, 14:53:02 (UTC+05:30)
<input type="radio"/>	ryteuwyiywui	US East (N. Virginia) us-east-1	September 10, 2025, 14:53:26 (UTC+05:30)

Account snapshot

Updated daily

Storage Lens provides visibility into storage usage and activity trends.

View dashboard

External access summary - new

Updated daily

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

S3 buckets | S3 | us-east-1

New Incognito tab

us-east-1.console.aws.amazon.com/s3/home?region=us-east-1

Incognito

All Bookmarks

aws

Search

[Alt+S]

United States (N. Virginia)

Account ID: 8765-9443-8092

user-test

Amazon S3

Successfully deleted bucket "rytewuyiywiwi"

General purpose bucketsAll AWS RegionsDirectory buckets

General purpose buckets (1) Info

Copy ARN

Empty

Delete

Create bucket

Buckets are containers for data stored in S3.

Find buckets by name

< 1 >

Name	AWS Region	Creation date
ms3buckettt	US East (N. Virginia) us-east-1	September 10, 2025, 14:53:02 (UTC+05:30)

Account snapshot Info

Updated daily

View dashboard

Storage Lens provides visibility into storage usage and activity trends.

External access summary - new Info

Updated daily

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

CloudShellFeedback

© 2025, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

Delete bucket - S3 bucket ms3

New Incognito tab

us-east-1.console.aws.amazon.com/s3/bucket/ms3buckettt/delete?region=us-east-1#

Incognito

All Bookmarks

aws

Search

[Alt+S]

United States (N. Virginia)

Account ID: 8765-9443-8092

user-test

Amazon S3 > Buckets > ms3buckettt > Delete bucket

Bucket names are unique. If you delete a bucket, another AWS user can use the name.

- If this bucket is used with a Multi-Region Access Point in an external account, initiate failover before deleting the bucket.
- If this bucket is used with an access point in an external account, the requests made through those access points will fail after you delete this bucket.

Learn more

Delete bucket "ms3buckettt"?

To confirm deletion, enter the name of the bucket in the text input field.

ms3buckettt

You don't have permission to delete bucket "ms3buckettt"

After you or your AWS admin has updated your IAM permissions to allow s3:DeleteBucket, choose **delete bucket**. Learn more about [Identity and Access Management in Amazon S3](#)

If you have the s3:DeleteBucket permission in your IAM user policy and you cannot delete a bucket, the bucket policy might include a deny statement for s3:DeleteBucket. Before you can delete the bucket, you must delete the deny s3:DeleteBucket statement or delete the bucket policy.

API response

Diagnose with Amazon Q

CloudShellFeedback

© 2025, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

2. Create Inline policy to get object to same user

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/user-test?section=permissions

Policy getObject created.

Permissions policies (3)

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

Filter by Type: All types

<input type="checkbox"/>	Policy name	Type	Attached via
<input type="checkbox"/>	deleteBucket	Customer managed	Directly
<input type="checkbox"/>	getObject	Customer inline	Inline
<input type="checkbox"/>	IAMUserChangePassword	AWS managed	Directly

Permissions boundary (not set)

us-east-1.console.aws.amazon.com/s3/buckets/ms3bucketttt?region=us-east-1&buckettype=general&tab=objects

Amazon S3 > Buckets > ms3bucketttt

ms3bucketttt Info

Objects (1)

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: ☐

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	user.csv	csv	September 10, 2025, 15:32:24 (UTC+05:30)	115.0 B	Standard

3. Create policy for create EC2

2 "Version": "2012-10-17",
3 "Statement": [
4 {
5 "Sid": "Statement1",
6 "Effect": "Allow",
7 "Action": [
8 "ec2:DescribeInstances",
9 "ec2:DescribeSecurityGroups",
10 "ec2:DescribeVpcs",
11 "ec2:DescribeSubnets",
12 "ec2:RunInstances",
13 "ec2:DescribeKeyPairs",
14 "ec2:CreateKeyPair",
15 "ec2:DescribeImages",
16 "ec2:CreateTags",
17 "ec2:CreateSecurityGroup",
18 "ec2:DescribeSecurityGroupRules",
19 "ec2:GetSecurityGroupsForVpc"
20],
21 "Resource": [
22 "*"]
23 }]
24]

Edit statement

Select a statement

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

+ Add new statement

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

Success
Successfully initiated launch of instance (i-0e7959e873d3dec9d)

Launch log

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"

Create billing usage alerts

Connect to your instance

Connect an RDS database

You don't have permission to see the color for this account

Account ID
8765-9443-8092

IAM user
user-test

Account
Organization
Service Quotas
Billing and Cost Management
Security credentials

Turn on multi-session support

Switch role

Sign out

Amazon Linux 2023

https://aws.amazon.com/linux/amazon-linux-2023

ec2-user@ip-172-31-16-137 ~]\$

i-0e7959e873d3dec9d (test)

PublicIPs: 13.220.117.82 PrivateIPs: 172.31.16.137

4. Create policy one statement give few permissions like bucket list, put object, delete object another statement for the same policy give deny permissions for entire s3

