

Cloud Storage and Management

Dakshindaya V S,

21BIT010

LAB – 3

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region

US East (N. Virginia) us-east-1

Bucket type [Info](#)

☒ General purpose

Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ Directory - New

Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)

bucketcsm

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

Object Ownership [Info](#)


Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☐ ACLs disabled (recommended)

All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☒ ACLs enabled

Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

 We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.


Object Ownership

☒ Bucket owner preferred

If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

☐ Object writer

The object writer remains the object owner.

 If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)

Amazon S3 > Buckets

Account snapshot - updated every 24 hours
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

View Storage Lens dashboard

General purpose buckets | Directory buckets

General purpose buckets (1) | Info | All AWS Regions
Buckets are containers for data stored in S3.

[Refresh](#) [Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

Find buckets by name

< 1 > ⌕

Name	AWS Region	IAM Access Analyzer	Creation date
<input type="radio"/> bucketcsm	US East (N. Virginia) us-east-1	View analyzer for us-east-1	August 16, 2024, 00:24:28 (UTC+05:30)

Amazon S3 > Buckets > bucketcsm > Upload

Upload [Info](#)

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (1 Total, 21.4 KB)

[Remove](#)

[Add files](#)

[Add folder](#)

All files and folders in this table will be uploaded.

Find by name

< 1 >

<input type="checkbox"/>	Name	Folder
<input type="checkbox"/>	451126488_7700499623395704_8673201020936562406_n....	-

Destination [Info](#)

Destination

s3://bucketcsm

Destination details

Bucket settings that impact new objects stored in the specified destination.

Permissions

Grant public access and access to other AWS accounts.

Properties

Specify storage class, encryption settings, tags, and more.

[Cancel](#)

[Upload](#)

Owner	sushant
AWS Region	US East (N. Virginia) us-east-1
Last modified	August 16, 2024, 00:25:52 (UTC+05:30)
Size	21.4 KB
Type	mp4
Key	451126488_7700499623395704_86732010209356562406_n.mp4

s3: `s3://bucketcsms/451126488_7700499623395704_8673201020936562406_n.mp4`

Amazon Resource Name (ARN)

arnaws: `arnaws:s3::bucketcsms/451126488_7700499623395704_8673201020936562406_n.mp4`

Entity tag (Etag)

etag: `S418b7541e2280c2c2a562d9a1625481`

Object URL

url: `https://bucketcsms.s3.amazonaws.com/451126488_7700499623395704_8673201020936562406_n.mp4`

The following bucket properties and object management configurations impact the behavior of this object.

Bucket Versioning

When enabled, multiple variants of an object can be stored in the bucket to easily recover from unintended user actions and application failures.

⚠ Disabled

Bucket "bucketcom" doesn't have Bucket Versioning enabled

We recommend that you enable Bucket Versioning to help protect against unintentionally overwriting or deleting objects. [Learn more](#)

Enable Bucket Versioning

Replication status

When a replication rule is applied to an object the replication status indicates the progress of the operation.

-

View replication rules

Expiration rule

You can use a lifecycle configuration to define expiration rules to schedule the removal of this object after a pre-defined time period.

-

Expiration date

The object will be permanently deleted on this date.


-

```
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>D9RN3SH9FAAMK9SH</RequestId>
  <HostId>LfcJG4joaPjBBk9eGh0+m3r5N/YH1ePzDKyy8a0vckRjesw2dF2E7MBqut30xPU30hdUejM71Cnp78T3ZK1xaA==</HostId>
</Error>
```

Block public access (bucket settings) Edit

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

 On

Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Public access is blocked because Block Public Access settings are turned on for this bucket

To determine which settings are turned on, check your Block Public Access settings for this bucket. [Learn more about using Amazon S3 Block Public Access](#)

No policy to display.

Copy

Edit Block public access (bucket settings) [Info](#)

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☐ **Block all public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**

S3 will ignore all ACLs that grant public access to buckets and objects.

☐ **Block public access to buckets and objects granted through new public bucket or access point policies**

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Cancel

Save changes

Edit Block public access (bucket settings)



Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.

To confirm the settings, enter *confirm* in the field.

Cancel

Confirm

bucketcsm

Info

- Objects
- Properties
- Permissions
- Metrics
- Management
- Access Points

Permissions overview

Access finding

Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#).

[View analyzer for us-east-1](#)

Block public access (bucket settings)

Edit

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

Off

Individual Block Public Access settings for this bucket

Bucket policy

Edit

Delete

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

No policy to display.





Copy


Edit access control list

Info

Access control list (ACL)

Grant basic read/write permissions to AWS accounts. [Learn more](#)

Grantee	Objects	Object ACL
Object owner (your AWS account) Canonical ID: 575dff92146c1f6ee29bd0 16c9b7d97ff8fe3aee016f51998 ab1e34fcc99d6b5	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	<input checked="" type="checkbox"/>  Read	<input checked="" type="checkbox"/>  Read <input type="checkbox"/> Write
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	<input checked="" type="checkbox"/>  Read	<input checked="" type="checkbox"/>  Read <input type="checkbox"/> Write

 When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.
[Learn more](#)


☒ I understand the effects of these changes on this object.

Access for other AWS accounts

No other AWS accounts associated with the resource.

Add grantee

Specified objects


Name	Type	Last modified	Size
 451126488_7700499623395704_8673201020936562406_n.mp4	mp4	August 16, 2024, 00:25:52 (UTC+05:30)	21.4 KB

Storage class

Amazon S3 offers a range of storage classes designed for different use cases. [Learn more](#) or see [Amazon S3 pricing](#)

	Storage class	Designed for	Availability Zones	Min storage duration	Min object size
<input type="radio"/>	Standard	Frequently accessed data (more than once a month) with milliseconds access	≥ 3	-	-
<input type="radio"/>	Intelligent-Tiering	Data with changing or unknown access patterns	≥ 3	-	-
<input type="radio"/>	Standard-IA	Infrequently accessed data (once a month) with milliseconds access	≥ 3	30 days	1
<input type="radio"/>	One Zone-IA	Recreatable, infrequently accessed data (once a month) stored in a single Availability Zone with milliseconds access	1	30 days	1
<input type="radio"/>	Glacier Instant Retrieval	Long-lived archive data accessed once a quarter with instant retrieval in milliseconds	≥ 3	90 days	1
<input checked="" type="radio"/>	Glacier Flexible Retrieval (formerly Glacier)	Long-lived archive data accessed once a year with retrieval of minutes to hours	≥ 3	90 days	-
<input type="radio"/>	Glacier Deep Archive	Long-lived archive data accessed less than once a year with retrieval of hours	≥ 3	180 days	-
<input type="radio"/>	Reduced redundancy	Noncritical, frequently accessed data with milliseconds access (not recommended as S3 Standard is more cost effective)	≥ 3	-	-

Specified objects

Name	Type	Last modified
 451126488_7700499623395704_8673201020936562406_n.mp4	mp4	August 16, 2024, 00:25:52 (U

Successfully edited storage class
View details below

Edit storage class: status

Close

The information below will no longer be available after you navigate away from this page.

Summary

Source

s3://bucketcsm

Successfully edited

1 object, 21.4 KB

Failed to edit

0 objects

Failed to edit

Configuration

Failed to edit (0)

Find objects by name

Name	Folder	Type	Last modified	Size	Error
No failed edits.					

Amazon S3

Buckets

bucketcsm

bucketcsm

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (1)

Copy

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

Name	Type	Last modified	Size	Storage class
<div><div>451126488_7700499623395704_867320102093</div><div>6562406_n.mp4</div></div> <div>mp4</div>		August 16, 2024, 00:40:56 (UTC+05:30)	21.4 KB	Glacier Flexible Retrieval (formerly Glacier)