

you can use this storage
to upload your data, files
objects as a secondary storage

you cannot install any operating
system in S3 bucket.
e.g. you cannot install ubuntu,
windows, redhat.

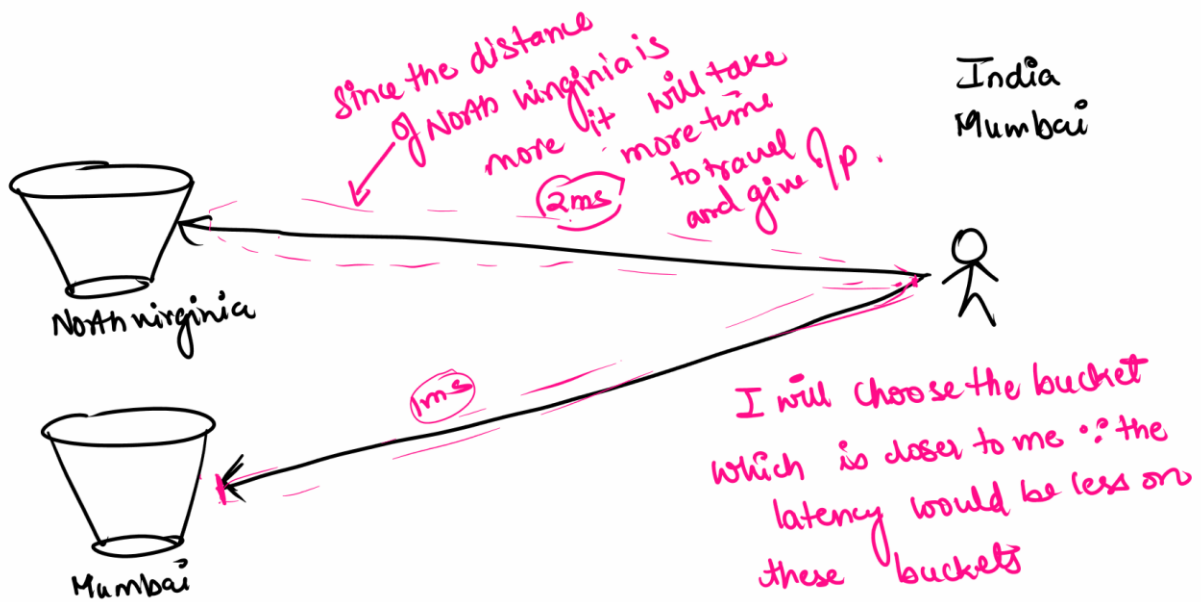
S3 → denote S3
by bucket
Simple storage
service
↓
upload any
kind of files
and
we call them
the object



size of S3 bucket = size of object

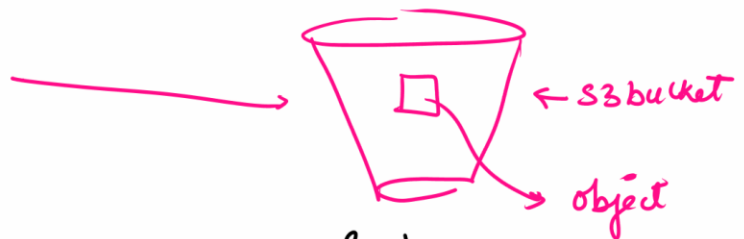
In free tier you
can upload 5GB files.





###

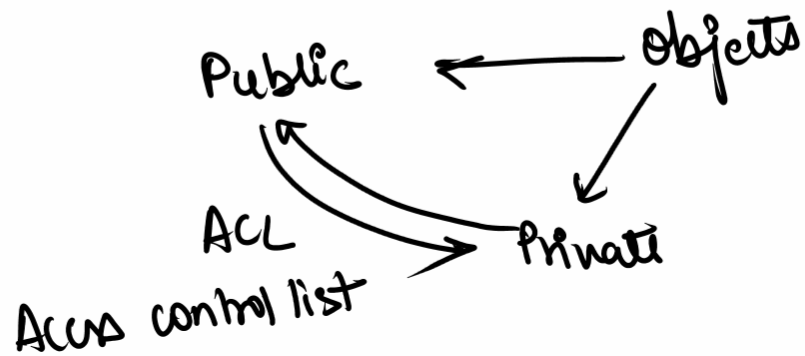
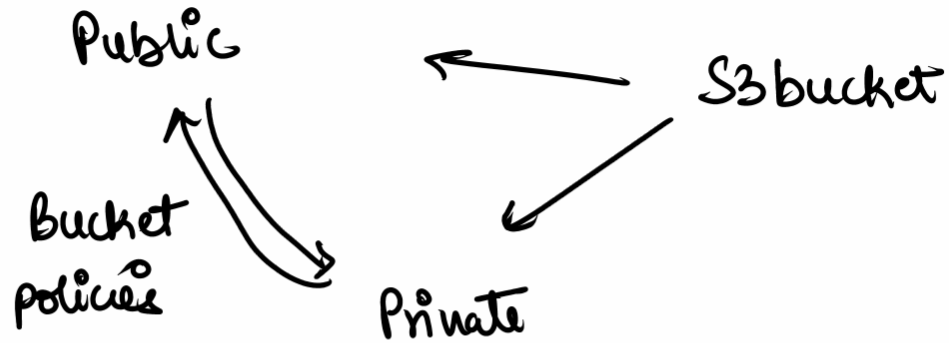
Bucket name is always globally unique.



name: Sanam

If let's say you create a bucket with the name Sanam then no one in this world would be able to create bucket with ~~name~~ same name globally.

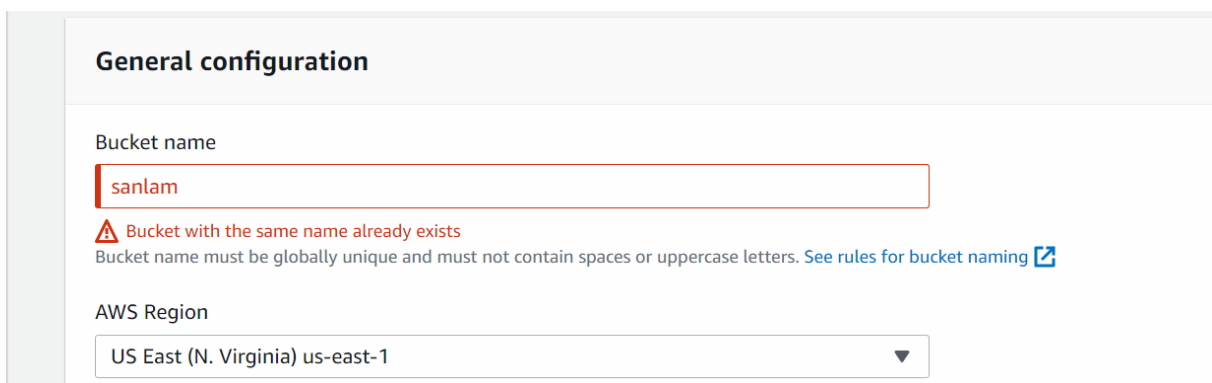
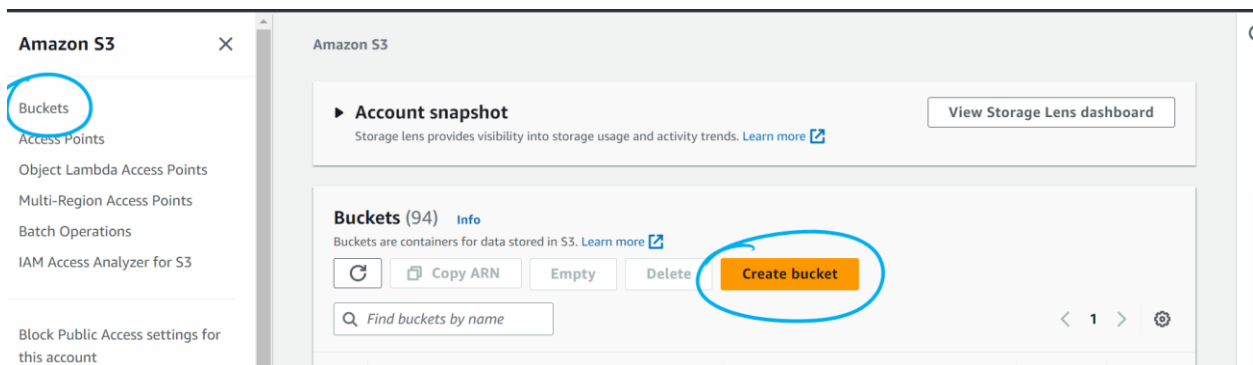
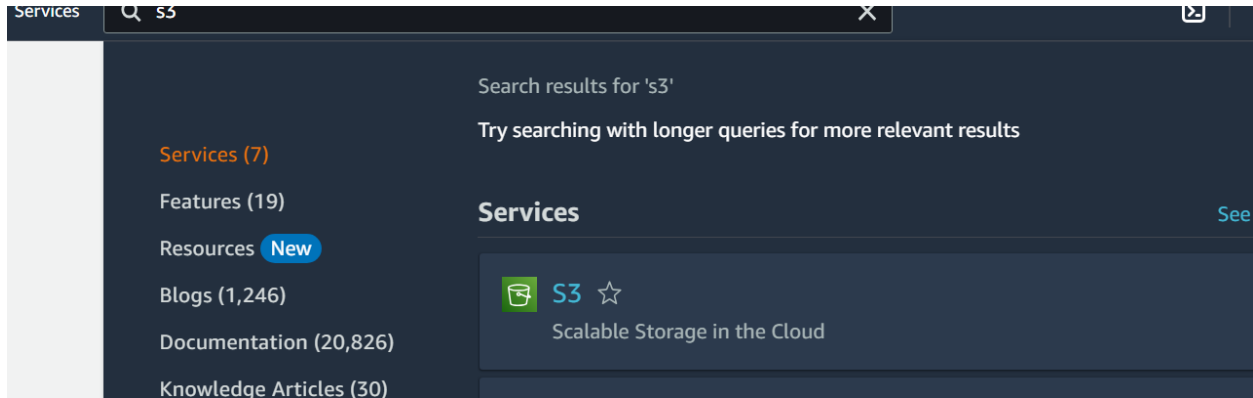
##



##

Bucket →	Public	Bucket → Private
Object → <u>Public</u>	yes, we would be able to access object	No, object is not accessible even if object is public then ^{also} object will not be accessible <i>Intact object cannot be made public in bucket</i>
Object - Private	No, since object is private we cannot access the object	No, since bucket & object is private we cannot access object

##



(since name is globally unique we cannot create a bucket with the name Sanlam because someone might have created the bucket with same name)

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

Asia Pacific (Mumbai) ap-south-1

Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

Choose bucket

Where the bucket would be created

Services Search [Alt+S] Global SamjayGarer

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](#)

Then you will not be able to connect the object to public

You will be able to connect the object to public. By default the object is uploaded as private

aws Services Search [Alt+S] Global SamjayGare

Block Public Access settings for this bucket

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 this bucket and its 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 this bucket 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 permission 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.

yes, Block all acms => Private bucket
If you deselect, then the public bucket would be created

- ☒ **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.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☒ Disable
☐ Enable

Tags (0) - optional

To prevent accidental deletion we use Bucket versioning. It is same like Recycle bin of our windows!

Create bucket

sanlam657

Info

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (0)

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](#)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

< 1 >

Name

▲

Type

▼

Last modified

▼

Size

▼

Storage class

No objects

Upload any image

sanlam657

Info

Objects

Properties

Permissions

Metrics

Management

Access Points

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](#)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

< 1 >

Name

▲

Type

▼

Last modified

▼

Size

▼

Storage class

▼

printable-maze.jpg

jpg

June 7, 2023, 17:09:43 (UTC+05:30)

113.3 KB

Standard

aws console.aws.amazon.com/s3/object/sanlam657/?region=ap-south-1&prefix=printable-maze.jpg

Services Search [Alt+S]

Object details for `s3://sanlam657/printable-maze.jpg`

Amazon Resource Name (ARN)
`arn:aws:s3:::sanlam657/printable-maze.jpg`

Entity tag (Etag)
`8b5caf031eef1dcf2aa41031a2be0a2b`

Object URL
`https://sanlam657.s3.ap-south-1.amazonaws.com/printable-maze.jpg`

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

Bucket properties | Management configurations

Copy the object url and paste the url in the browser

sanlam657.s3.ap-south-1.amazonaws.com/printable-maze.jpg

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>WW4PTV30R6V2NWPX</RequestId>
  <HostId>91YyvfSnnj8V08jqsPQ9EvYiuGWNBJPPk2f3IvPpSBLPCzb6gsk7Re+3Rk7F1F0SxqtQ2V1CAFs=</HostId>
</Error>
```








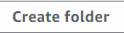

Why ? because our bucket is private and object is also private




Lets first make bucket public:


sanlam657 [Info](#)[Objects](#) | [Properties](#) | [Permissions](#) | [Metrics](#) | [Management](#) | [Access Points](#)

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](#)

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

 1  

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	 printable-maze.jpg	jpg	June 7, 2023, 17:09:43 (UTC+05:30)	113.3 KB	Standard

Permissions overview

Access

Bucket and objects not public

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](#)

[Edit](#)

Block all public access

 On

► Individual Block Public Access settings for this bucket

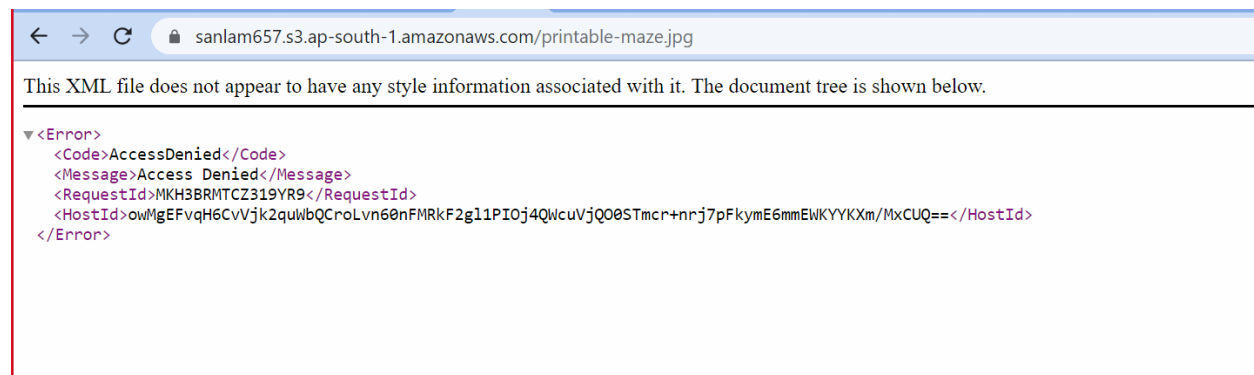
ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will 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**

Bucket is now public ...lets again see if I can access the object or not



My object is still not accessible

Since my object is private I cannot access the object

Lets make object public

Amazon S3 > Buckets > sanlam657 > printable-maze.jpg

printable-maze.jpg

Info

Copy S3 URI

Download

Open

Object actions

Properties

Permissions

Versions

Object overview

Owner

c1af66ddea31602a7cd8822dcc0b2172a51af576fc039e686ac68f99b15f7e7a

AWS Region

Asia Pacific (Mumbai) ap-south-1

Last modified

June 7, 2023, 17:00:43 (UTC+05:30)

S3 URI

s3://sanlam657/printable-maze.jpg

Amazon Resource Name (ARN)

arn:aws:s3:::sanlam657/printable-maze.jpg

Entity tag (Etag)

5125-6231-6416-14234-211-2-21

Amazon S3 > Buckets > sanlam657 > printable-maze.jpg

printable-maze.jpg

Info

Copy S3 URI

Download

Open

Object actions

Properties

Permissions

Versions

Access control list (ACL)


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




Edit

Grantee	Object	Object ACL
<div>Object owner (your AWS account)</div> <div>Canonical ID: c1af66ddea31602a7cd8822dcc0b2172a51af576fc039e686ac68f99b15f7e7a</div>	Read	Read, Write
<div>Everyone (public access)</div> <div>Group: http://acs.amazonaws.com/groups/global/AllUsers</div>	-	-
<div>Authenticated users group (anyone with an AWS account)</div>	-	-

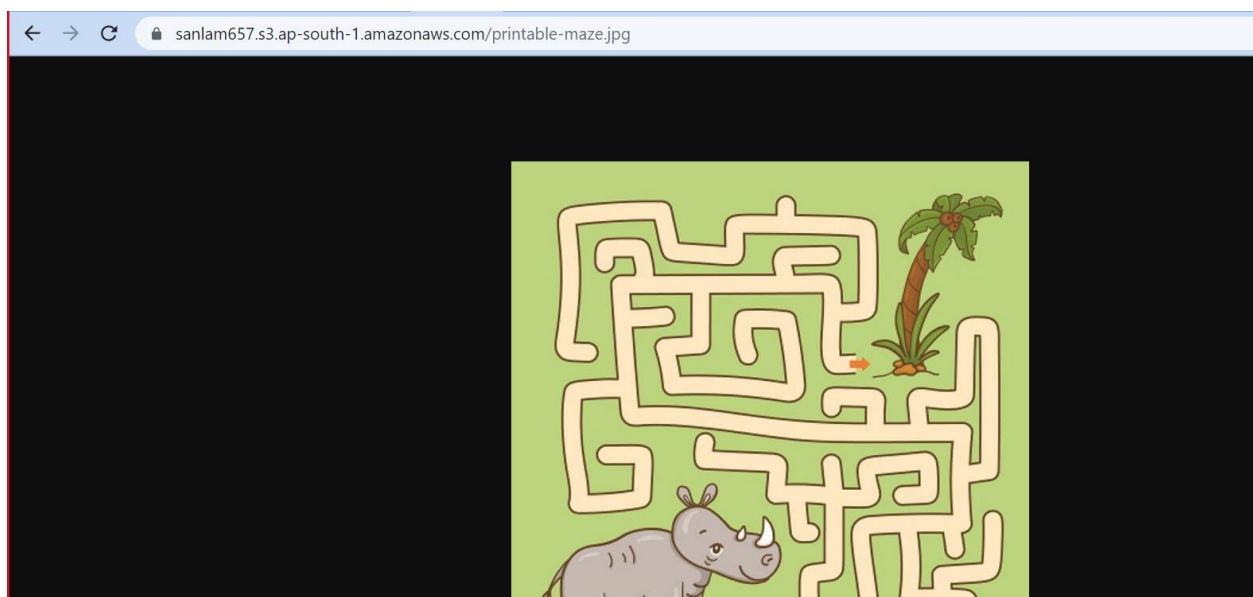
Edit access control list [Info](#)

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:  c1af66ddea31602a7cd8822dcc0b2172a51af576fc039e686ac68f99b15f7e7a	<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 type="checkbox"/> Read <input type="checkbox"/> Write
Authenticated users group	<input type="checkbox"/> Read	<input type="checkbox"/> Read

Save



Object is now accessible