






CLOUD COMPUTING

CC-1

QUESTION-3:

 Classes  New folder

 Services [Alt+S] 

 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



EU (Stockholm) eu-north-1 ▾


Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

 Classes  New folder

 Services [Alt+S] 

 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.



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 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.

 **Turning off block all public access might result in this bucket and the objects within becoming public**
AWS recommends that you turn on block all public access, unless public access is required for specific and



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 settings 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)**

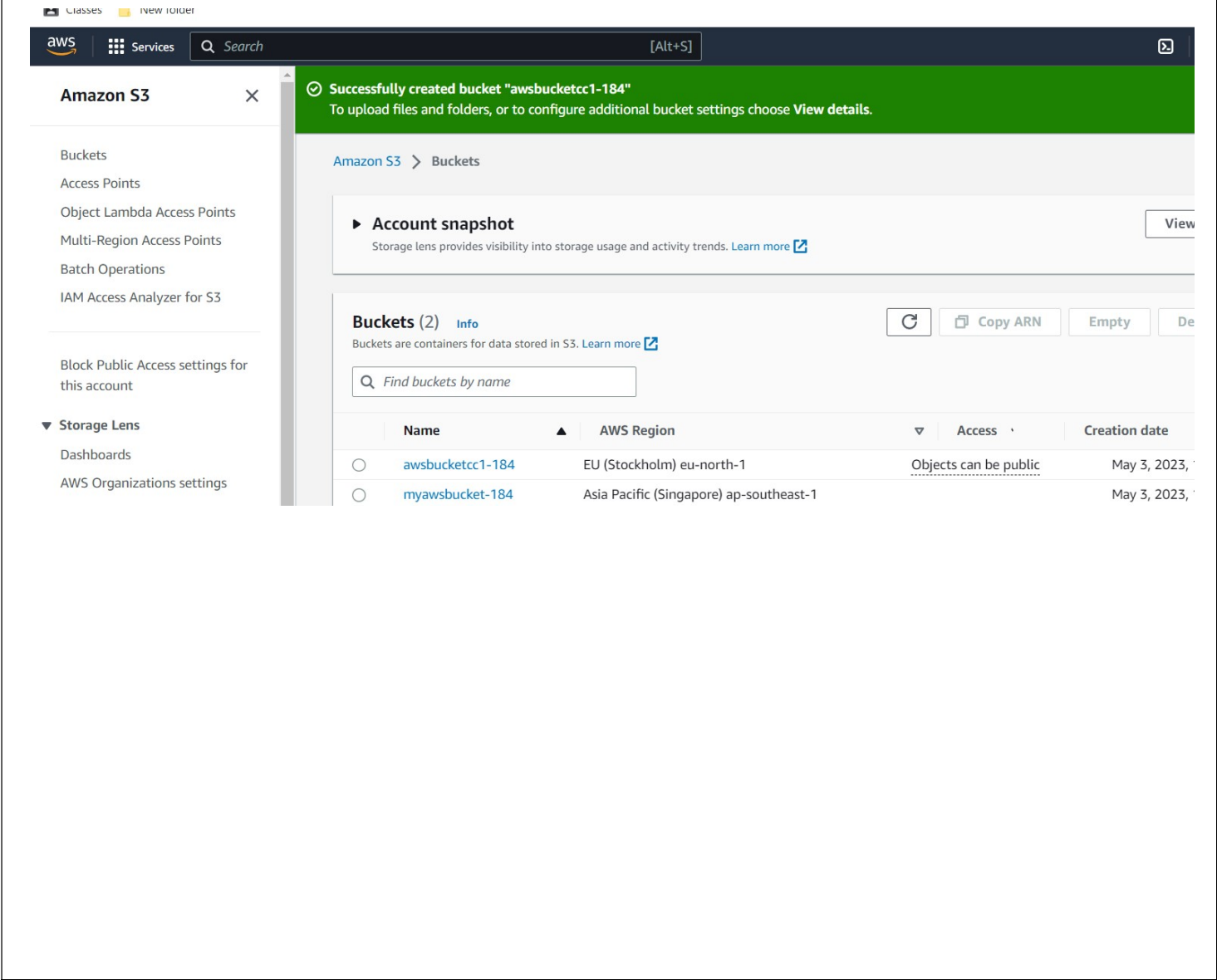
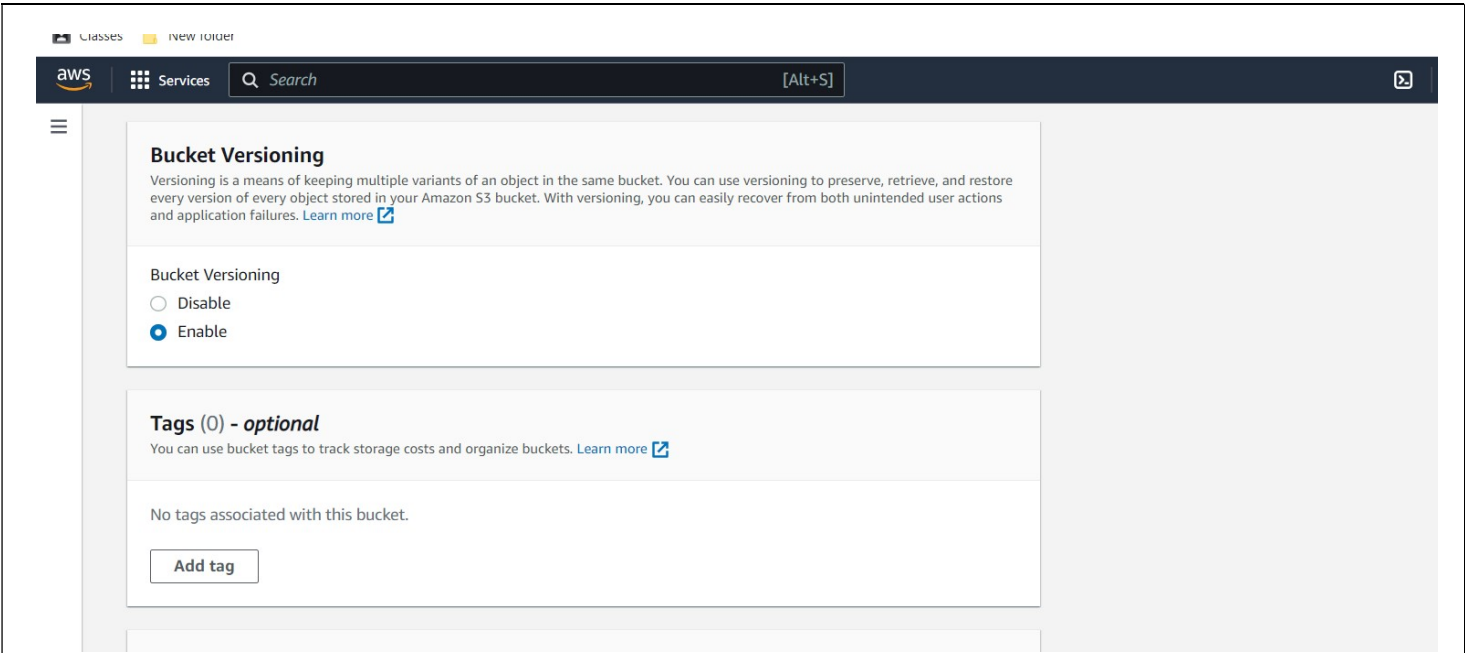
S3 will ignore all ACLs that grant public access to buckets and objects.

☐ **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.



aws

Services

Search

[Alt+S]

Upload succeeded

View details below.

Upload: status

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

Summary

Destination	Succeeded	Failed
s3://awsbucketcc1-184	✔ 1 file, 31.0 B (100.00%)	✖ 0 files, 0 B (0%)

Files and folders

Configuration

Classes

New folder

aws

Services

Search

[Alt+S]

Amazon S3 > Buckets > awsbucketcc1-184 > Accounts.txt

Accounts.txt

Info

Copy S3 URI

Download

Open

Properties

Permissions

Versions

Access control list (ACL)

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

Grantee	Object
Object owner (your AWS account)	Read
Canonical ID: bca66574237b42a1b605a3a535c8e5cbda9684a2c0164d0b10cdfcd1cd7dcf1	
Everyone (public access)	Read
Group: http://acs.amazonaws.com/groups/global/AllUsers	

aws

Services

Search

[Alt+S]

Upload succeeded

View details below.

Summary

Destination

s3://awsbucketcc1-184

Succeeded

1 file, 31.0 B (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 Total, 31.0 B)

Find by name

Meet - x | SKCET - 202 x | Google Drive x | Search resu x | SKCET x | IAM Manag x | Connect to x | EC2 Instanc x |

awsbucketcc1-184.s3.eu-north-1.amazonaws.com/Accounts.txt

Classes New folder

Hello Everyone....
I am Yamini