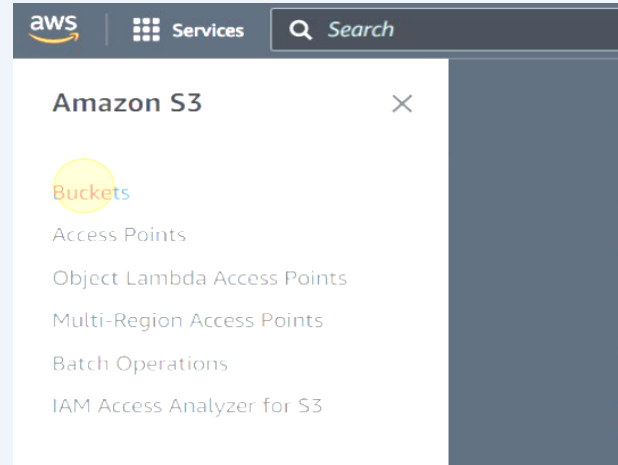


CREATE A PUBLIC BUCKET IN AWS.UPLOAD A FILE AND GIVE THE NECESSARY PERMISSION TO CHECK WHETHER THE FILE URL IS WORKING OR NOT.

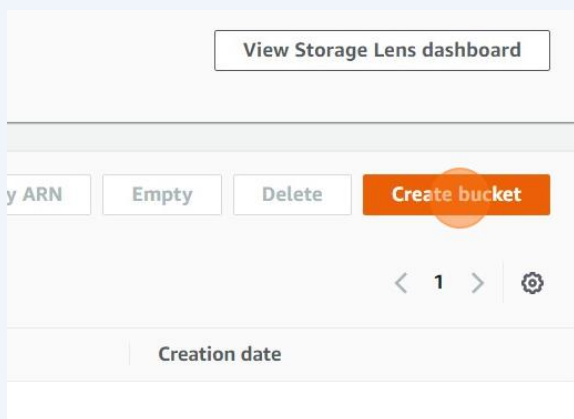
1. Visit aws.amazon.com and Sign in. Click on the search field and type "s3" in the search field and select S3



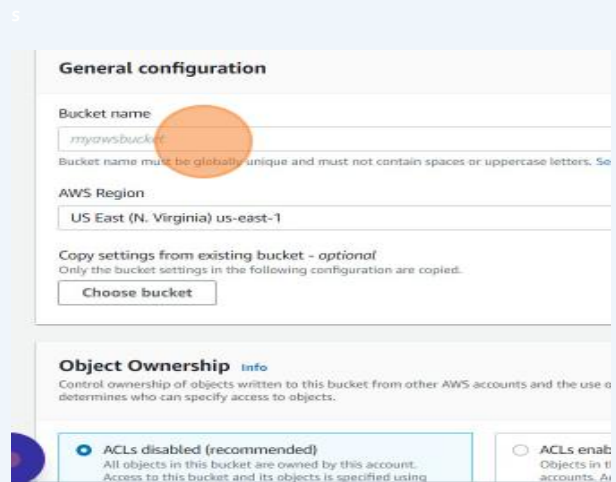
2. Click on "Buckets"



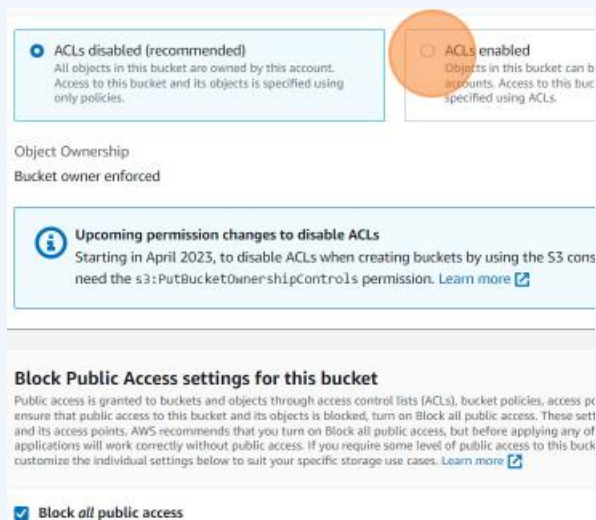
3. Click on "Create Bucket"



4. Click the "Bucket name" field and type "hiteshpublicbucket".



5. Select ACLs enabled and uncheck "Block all public access"



The screenshot shows the 'Access Control List (ACL)' settings for a bucket. There are two radio buttons: 'ACLs disabled (recommended)' and 'ACLs enabled'. The 'ACLs enabled' option is selected and highlighted with an orange circle. Below this, the 'Object Ownership' is set to 'Bucket owner enforced'. A blue information box states: 'Upcoming permission changes to disable ACLs. Starting in April 2023, to disable ACLs when creating buckets by using the S3 console, you need the s3:PutBucketOwnershipControls permission. Learn more'. At the bottom, under 'Block Public Access settings for this bucket', the checkbox for 'Block all public access' is checked.

☒ 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 accounts. Access to this bucket and its objects is specified using ACLs.

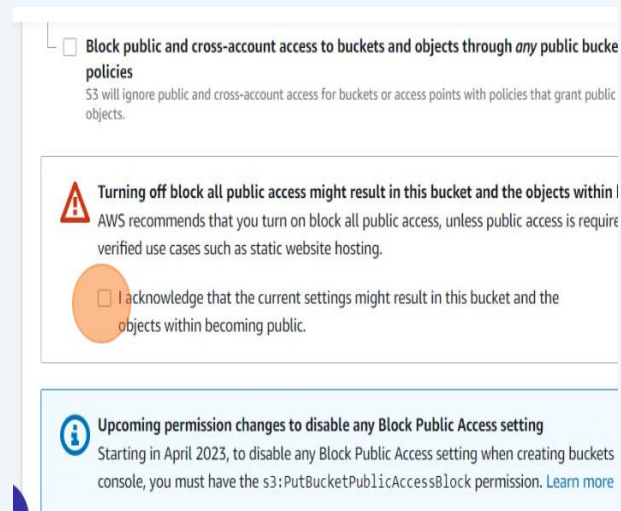
Object Ownership
Bucket owner enforced

Upcoming permission changes to disable ACLs
Starting in April 2023, to disable ACLs when creating buckets by using the S3 console, you need the `s3:PutBucketOwnershipControls` permission. [Learn more](#)

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, and IAM permissions. To ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings and their access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, you must first turn on Block all public access. If you require some level of public access to this bucket, you must first turn on Block all public access. [Learn more](#)

☒ Block all public access

6. Click on this check box



The screenshot shows the 'Block Public Access' settings. The checkbox 'Block public and cross-account access to buckets and objects through any public bucket policies' is checked and highlighted with an orange circle. Below it, a warning message states: '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 verified use cases such as static website hosting.' Another checkbox 'I acknowledge that the current settings might result in this bucket and the objects within becoming public.' is also checked and highlighted with an orange circle. At the bottom, a blue information box states: 'Upcoming permission changes to disable any Block Public Access setting. Starting in April 2023, to disable any Block Public Access setting when creating buckets in the console, you must have the s3:PutBucketPublicAccessBlock permission. Learn more'.

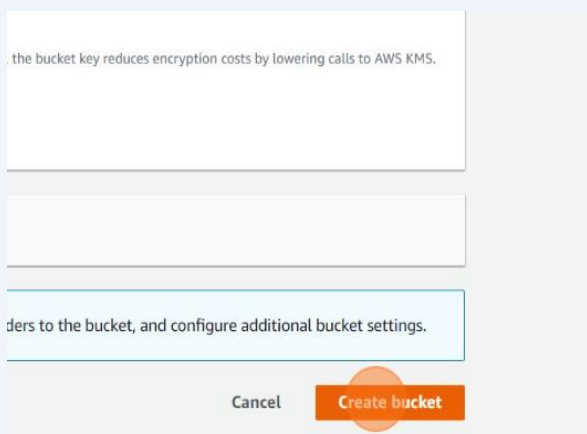
☒ Block public and cross-account access to buckets and objects through any public bucket policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access.

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 verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Upcoming permission changes to disable any Block Public Access setting
Starting in April 2023, to disable any Block Public Access setting when creating buckets in the console, you must have the `s3:PutBucketPublicAccessBlock` permission. [Learn more](#)

7. Click on "Create bucket"



The screenshot shows the 'Create bucket' dialog. The 'Bucket name' field is empty. The 'AWS Region' dropdown is set to 'US East (N. Virginia)'. The 'Encryption' section is expanded, showing 'Server-side encryption with Amazon S3-managed keys' selected. The 'Block Public Access' section is also expanded, showing 'Block all public access' checked. At the bottom, there are 'Cancel' and 'Create bucket' buttons. The 'Create bucket' button is highlighted with an orange circle.

the bucket key reduces encryption costs by lowering calls to AWS KMS.

Bucket name

AWS Region

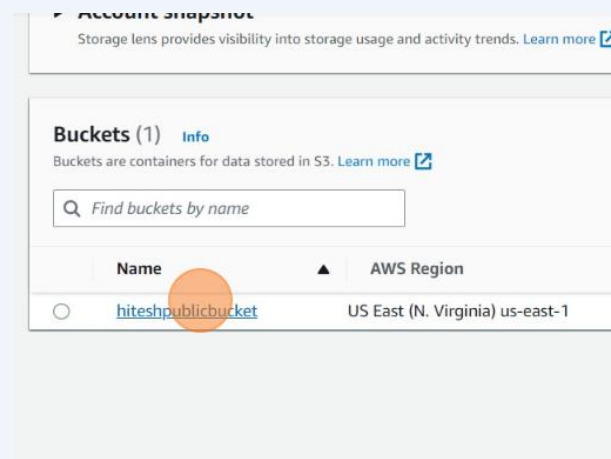
Server-side encryption with Amazon S3-managed keys

Block Public Access

Block all public access

Cancel Create bucket

8. Click on "hiteshpublicbucket"



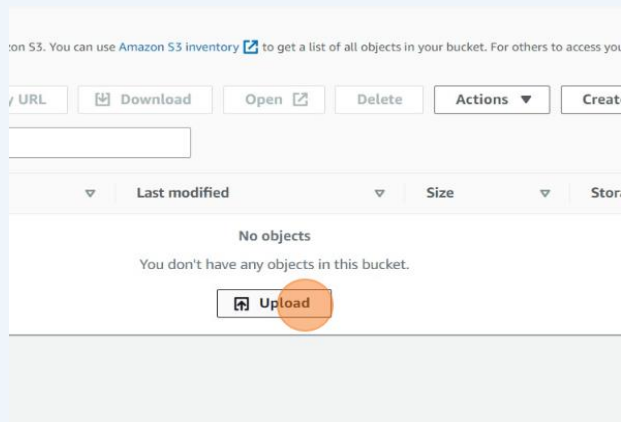
The screenshot shows the 'Buckets' list in the AWS S3 console. The table has two columns: 'Name' and 'AWS Region'. The first row shows a bucket named 'hiteshpublicbucket' in the 'US East (N. Virginia) us-east-1' region. The bucket name is highlighted with an orange circle.

Buckets (1) [Info](#)
Buckets are containers for data stored in S3. [Learn more](#)

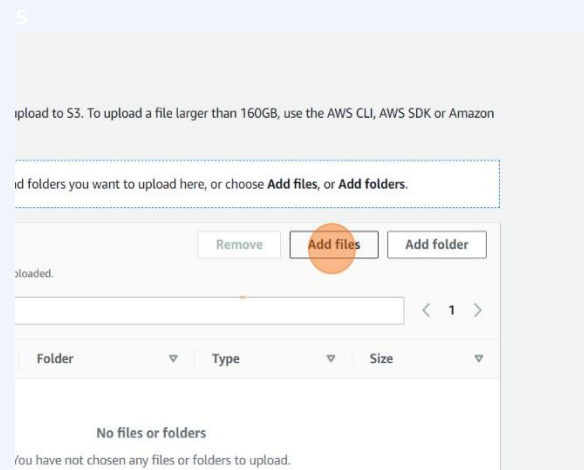
Find buckets by name

Name	AWS Region
hiteshpublicbucket	US East (N. Virginia) us-east-1

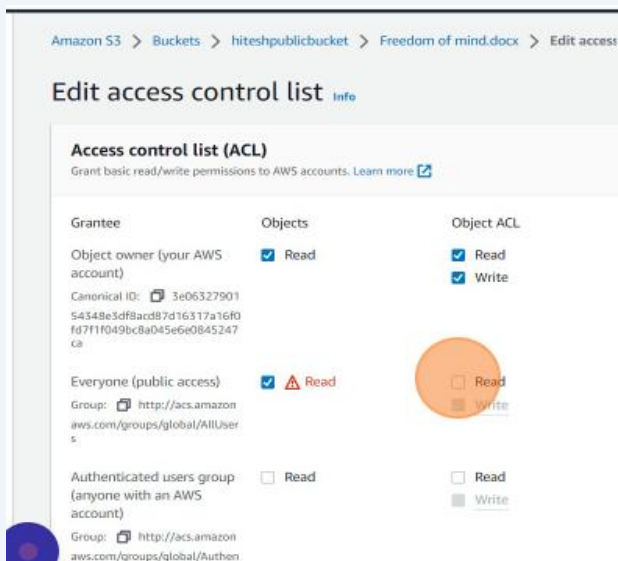
9. Click on “Upload”



10. Add files and folders which you want to upload and click upload

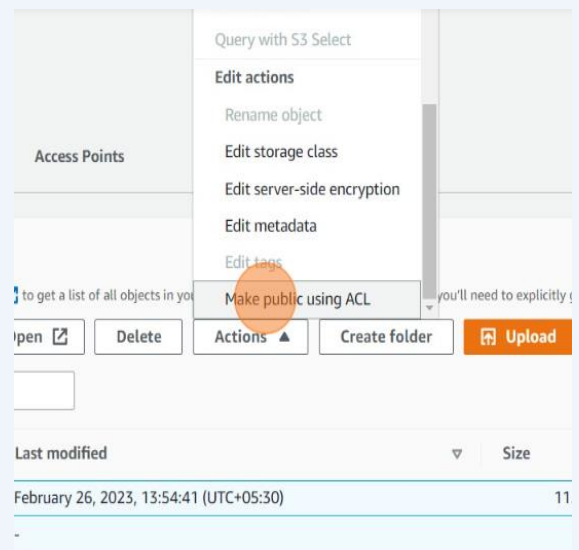


11. You may click the filename and then go to permission and select edit and allow everyone to access the file. Acknowledge and then save changes.



or

12. Select the file click “Action”. Click on “Make public using ACL” and then click on make public.



13. Now the file is accessible through both the object URL and the presigned URL.