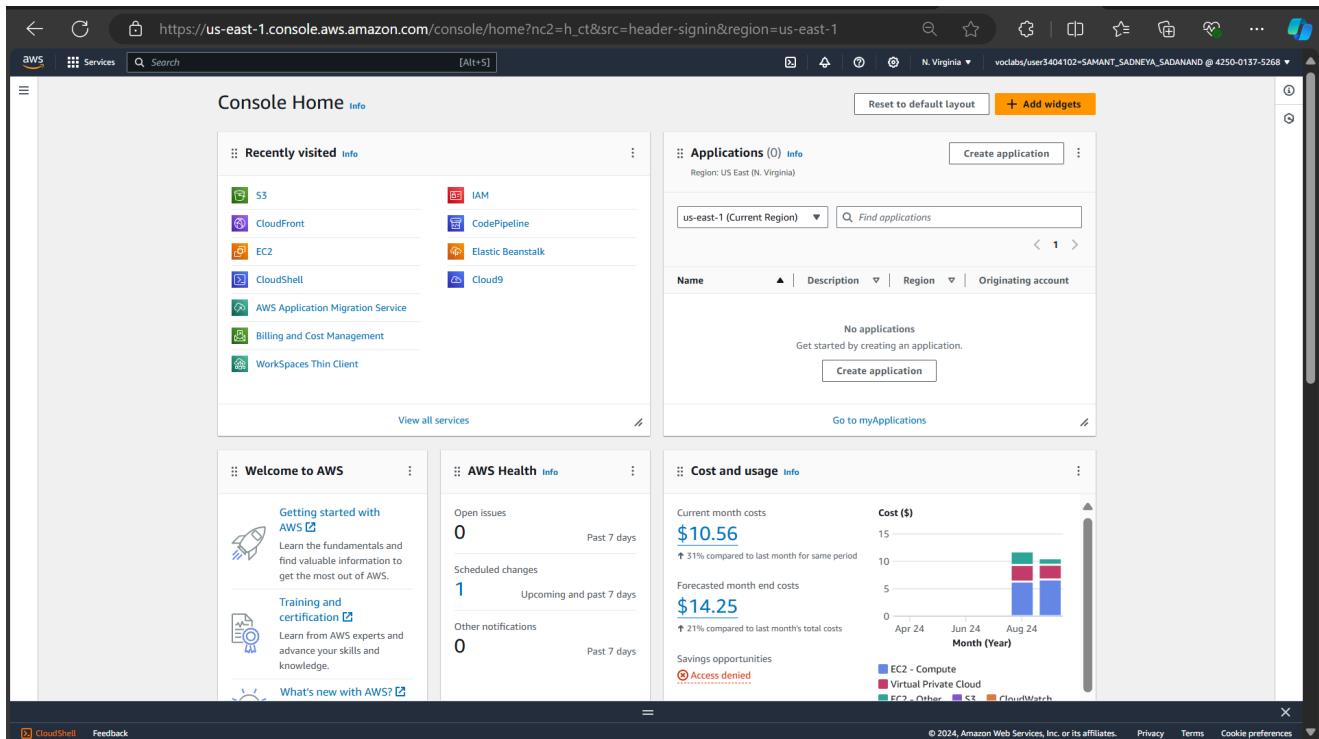


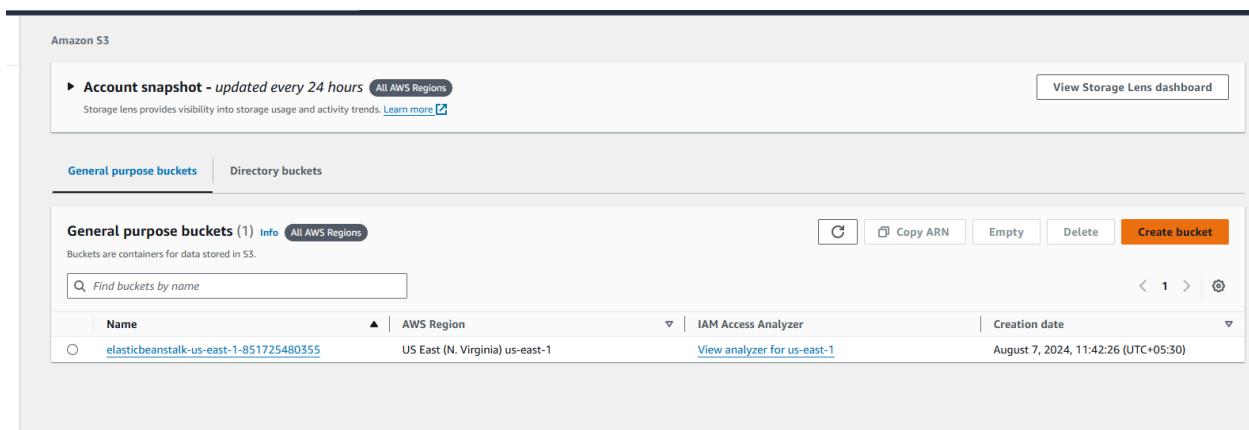
Creation of S3 bucket and to host video streaming

1. Creation of S3 Bucket



The screenshot shows the AWS Console Home page. In the top left, under 'Recently visited' services, 'S3' is listed. Other services like IAM, CloudFront, EC2, and CloudWatch are also visible. To the right, there's a section for 'Applications' which is currently empty. Below these, the 'Welcome to AWS' section provides links for getting started with AWS, training and certification, and what's new with AWS. On the far right, there's a 'Cost and usage' dashboard showing current month costs of \$10.56 and forecasted month end costs of \$14.25, along with a bar chart of cost distribution over time.

1. Go to AWS academy and search for S3 bucket. Then click on it there you will get a button to click to create a bucket.



The screenshot shows the 'General purpose buckets' section of the Amazon S3 console. It displays one bucket named 'elasticbeanstalk-us-east-1-851725480355'. The bucket details include its name, AWS Region (US East (N. Virginia)), IAM Access Analyzer (with a link to 'View analyzer for us-east-1'), and Creation date (August 7, 2024, 11:42:26 (UTC+05:30)). There are buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'.

2. Give your bucket a unique name to your bucket. Here I have given the name "video-storage-streaming". There is no other changes made in general configuration.

Amazon S3 > Buckets > Create bucket

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
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

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.

Format: s3://bucket/prefix

3. Also There is no changes in object ownership and keep block public access on.

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.

Object Ownership
Bucket owner enforced

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 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.

4. Then Enable Bucket Versioning. After that enable Default encryption also.

AWS Services Search [Alt+S] N. Virginia v volcabs/user5404102-SAMANT_SADNEYA_SADANAND @ 4250-0137-5268

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
 Enable

Tags - optional (0)
You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

Default encryption [Info](#)
Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)

- Server-side encryption with Amazon S3 managed keys (SSE-S3)
- Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#).

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

- Disable
- Enable

Advanced settings

Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

- Disable
- Enable
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

Info Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Versioning.

Info After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

5.Do not Enable Advanced Settings.Keep it disabled by default.

6.After clicking confirm this , “video-storage-streaming” named bucket got created.

[Amazon S3](#) > [Buckets](#) > video-storage-streaming

video-storage-streaming [Info](#)

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

Objects (0) [Info](#)

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

Name	Type	Last modified	Size	Storage class
No objects You don't have any objects in this bucket.				

[Upload](#)

7.Click on the upload button

2. Uploading A video

1. Then you can drag and drop your video .mp4 file or you can add it by using Add files.

The screenshot shows the AWS S3 'Upload' interface. At the top, the navigation path is 'Amazon S3 > Buckets > video-storage-streaming > Upload'. Below this, there's a large dashed blue box labeled 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' To the right of this box, there are three buttons: 'Remove', 'Add files', and 'Add folder'. Below this section, a table titled 'Files and folders (1 Total, 172.4 MB)' lists the file '3214448-uhd_3840_2160_25fps.mp4'. There are 'Remove', 'Add files', and 'Add folder' buttons above the table. A search bar labeled 'Find by name' is present. The 'Destination' section shows the destination as 's3://video-storage-streaming'. It includes sections for 'Destination details', 'Permissions', and 'Properties'. At the bottom right are 'Cancel' and 'Upload' buttons, with 'Upload' being orange.

2. Then click on the upload button. Then check the status of the video file whether it is uploaded successfully or not.

The screenshot shows the AWS S3 'Upload: status' page. The URL in the browser is 'https://us-east-1.console.aws.amazon.com/s3/upload/video-storage-streaming?region=us-east-1&bucketType=ge...'. The main message is 'Upload succeeded' with a link to 'View details below.'. Below this, there's a summary table:

Destination	Succeeded	Failed
s3://video-storage-streaming	1 file, 172.4 MB (100.00%)	0 files, 0 B (0%)

Below the summary, there are tabs for 'Files and folders' (selected) and 'Configuration'. The 'Files and folders' tab shows a table with one item:

Files and folders (1 Total, 172.4 MB)						
Find by name						
Name	Folder	Type	Size	Status	Error	
3214448-uh...	-	video/mp4	172.4 MB	Succeeded	-	

3. Thus, the video got uploaded successfully.

The screenshot shows the AWS S3 console. In the top navigation bar, 'Amazon S3' and 'Buckets' are selected. The main page displays the bucket 'video-storage-streaming'. Below the bucket name, there are tabs for 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects' tab is active, showing a table with one item: '3214448-uhd_3840_2160_25fps.mp4'. The table includes columns for Name, Type, Last modified, Size, and Storage class. The file is an mp4 file, last modified on September 23, 2024, at 19:58:12 (UTC+05:30), with a size of 172.4 MB and a Standard storage class. At the bottom right of the table, there is an orange 'Upload' button.

4. Then Click on Permissions and then off the block public access.i.e providing public access .

The screenshot shows the 'Edit Block public access (bucket settings)' page. The URL in the browser is 'Amazon S3 > Buckets > video-storage-streaming > Edit Block public access (bucket settings)'. The page title is 'Edit Block public access (bucket settings)'. Below the title, there is a section titled 'Block public access (bucket settings)' with a sub-section 'Block all public access'. A note states: 'Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.' There are four checkboxes under this section: 'Block public access to buckets and objects granted through new access control lists (ACLs)', 'Block public access to buckets and objects granted through any access control lists (ACLs)', 'Block public access to buckets and objects granted through new public bucket or access point policies', and 'Block public and cross-account access to buckets and objects through any public bucket or access point policies'. At the bottom right, there are 'Cancel' and 'Save changes' buttons, with 'Save changes' being highlighted in orange.

Then Click on save changes.

5. Then again go to permissions of the project and look at Access Control List (ACL) whether it has read write access to it. See in the below diagram it has list, write, read properties.

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: 02755ae775ac14219b8f635cc3162e1c98cfba254869f7505c142bb69b2d72d0	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	-	-

Then go to S3 main page and click the video that you uploaded and then inside the properties you will get the link click on it but it shows access denied.

```

<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>1DZTDNXK37NW2FB</RequestId>
  <HostId>pIYNbPuiVyqaQaU5aQLlsM0PQ6E4GHnzUPaPTzKds8oEYZ09Nx0uuUUbCq/LwefEqnHjbUHVDLrcD5M/ZIPUQ==</HostId>
</Error>

```

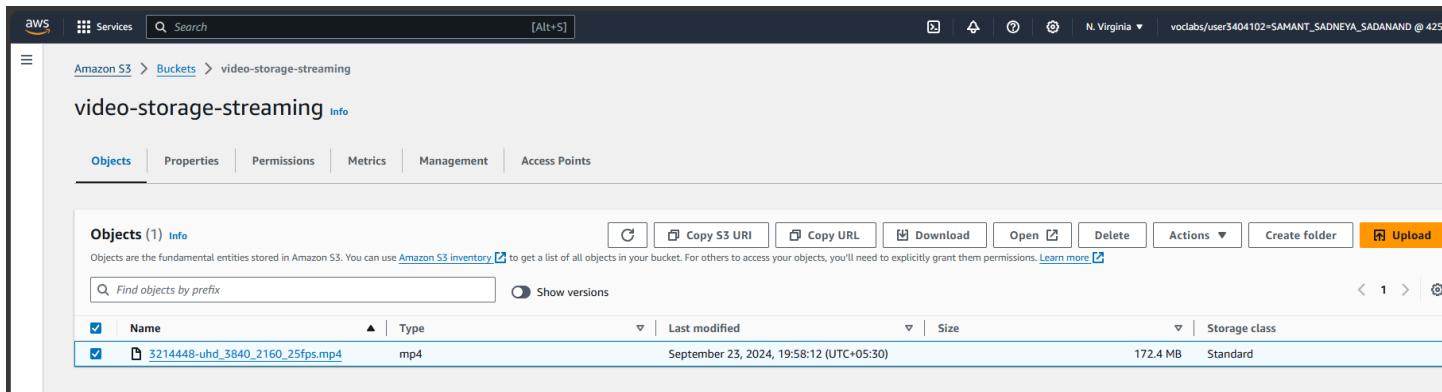
6. Thus we need to update the bucket policy by using the following code. In this click on Edit button and then add script for adding the code for bucket-policy.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": "s3:GetObject",  
      "Resource": "arn:aws:s3:::video-storage-streaming/*"  
    }  
  ]  
}
```

The screenshot shows the AWS Management Console interface for editing a bucket policy. The top navigation bar includes the AWS logo, Services, a search bar, and a keyboard shortcut [Alt+S]. Below the navigation is a breadcrumb trail: Amazon S3 > Buckets > video-storage-streaming > Edit bucket policy. The main content area is titled 'Edit bucket policy' with a 'Info' link. A sub-section titled 'Bucket policy' contains a note about bucket policies being written in JSON and providing access to objects in the bucket. It also mentions that bucket policies don't apply to objects owned by other accounts, with a 'Learn more' link. Below this is a 'Bucket ARN' field containing 'arn:aws:s3:::video-storage-streaming'. The 'Policy' section displays the JSON policy code, which is identical to the one provided in the text above. The JSON code is numbered from 1 to 12. Line 12 is highlighted with a dark gray background, indicating it is the current line of focus or selection.

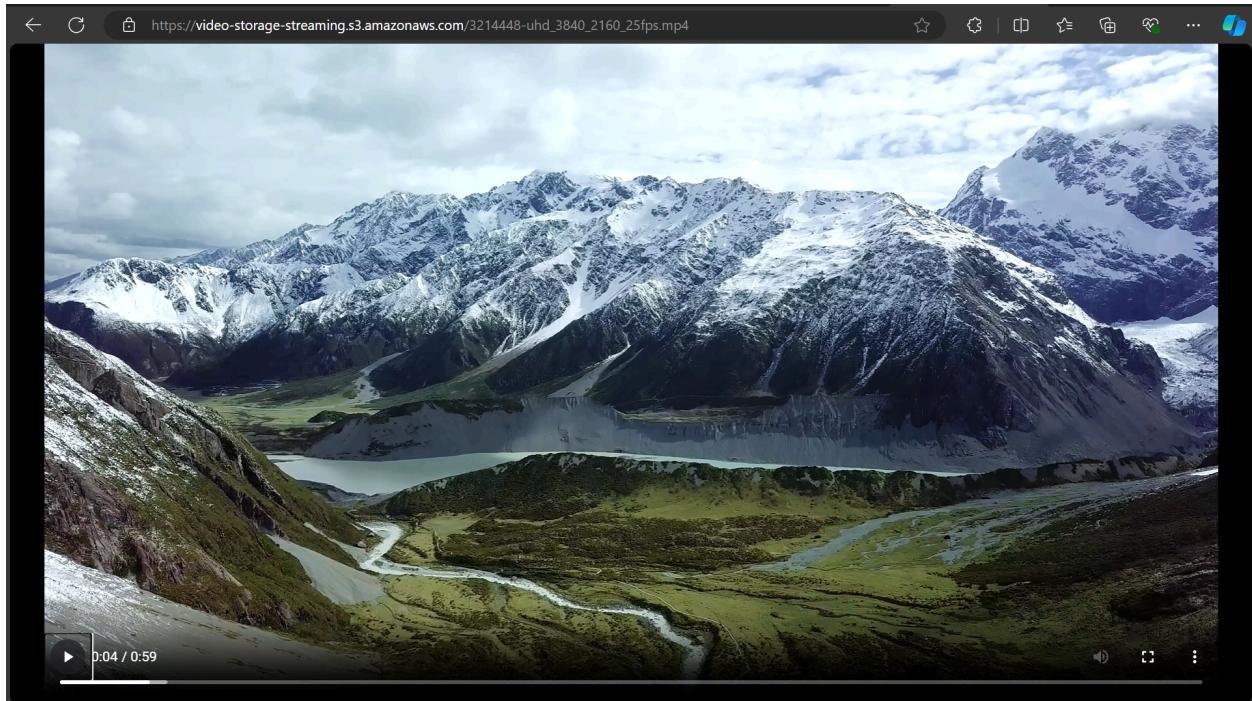
```
1▼ {  
2  "Version": "2012-10-17",  
3▼  "Statement": [  
4▼    {  
5      "Effect": "Allow",  
6      "Principal": "*",  
7      "Action": "s3:GetObject",  
8      "Resource": "arn:aws:s3:::video-storage-streaming/*"  
9    }  
10  ]  
11 }  
12 |
```

7. Go back on S3 main page then refresh the page.



The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with 'Services' and a search bar. Below it, the path 'Amazon S3 > Buckets > video-storage-streaming' is shown. The main area is titled 'video-storage-streaming' with a 'Info' link. A horizontal menu bar below the title includes 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects' tab is selected. A table below shows one object: '3214448-uhd_3840_2160_25fps.mp4'. The table has columns for Name, Type, Last modified, Size, and Storage class. The file is an MP4 type, was last modified on September 23, 2024, at 19:58:12 UTC+05:30, is 172.4 MB in size, and is stored in the Standard storage class. There are buttons for 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', and 'Create folder'.

8. Then go to S3 main page and click the video that you uploaded and then inside the properties you will get the link click on it video-storage-streaming.s3.amazonaws.com/3214448-uhd_3840_2160_25fps.mp4 (Like this) copy this link and paste it on a new tab. Now you can see the video you have uploaded.



Thus Video Stream Hosted Using S3 bucket Successfully.