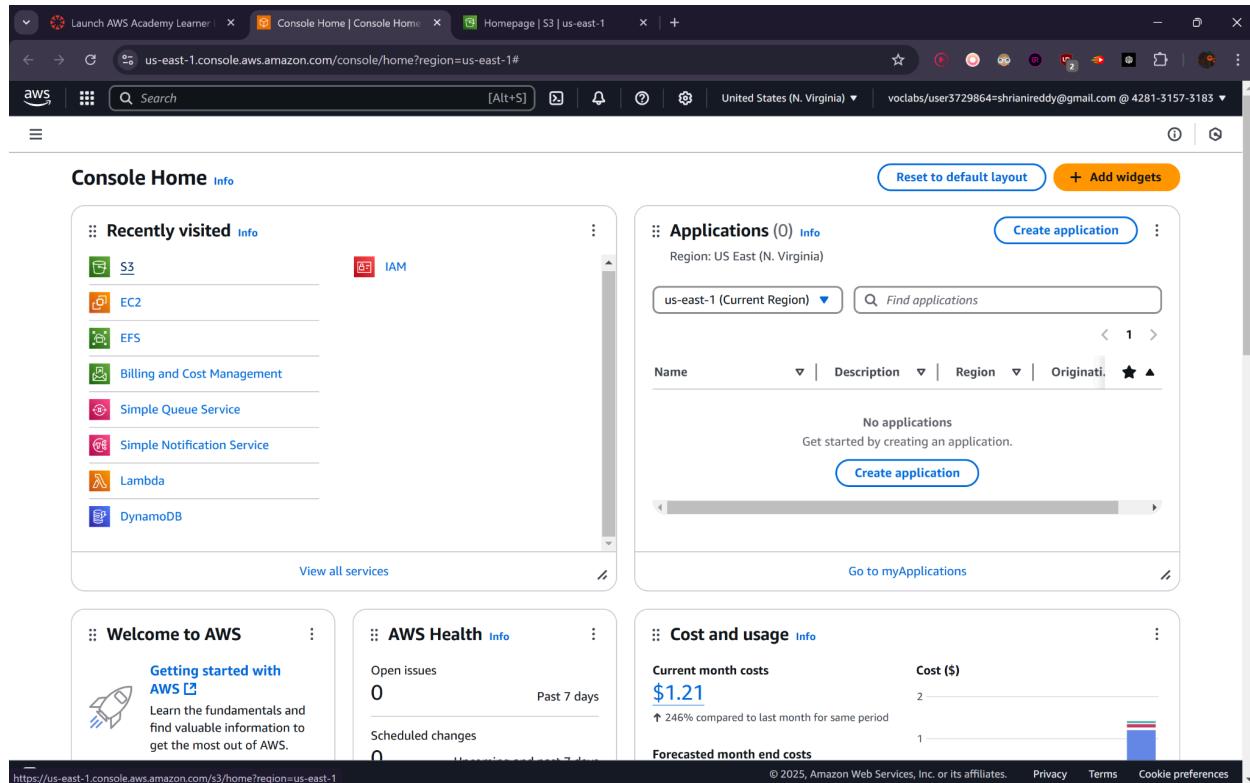


S3- Bucket and object creation and creating public access links

PUBLIC ACCESS LINK :

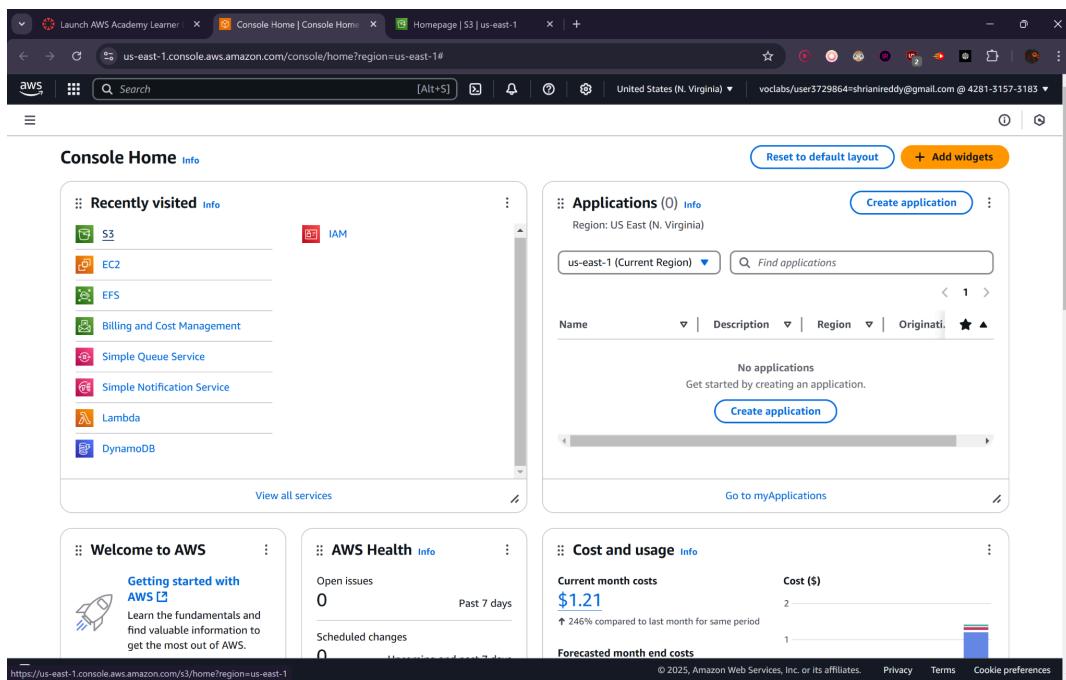
<https://052jcreations3.s3.us-east-1.amazonaws.com/it%E2%80%99s+the.png>

Start your AWS LAB



The screenshot shows the AWS Console Home page. The top navigation bar includes tabs for Launch AWS Academy Learner, Console Home, and Homepage. The URL in the address bar is <https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1#>. The sidebar on the left lists recently visited services: S3, IAM, EC2, EFS, Billing and Cost Management, Simple Queue Service, Simple Notification Service, Lambda, and DynamoDB. Below this is a "View all services" link. The main content area contains several cards: "Welcome to AWS" (Getting started with AWS), "AWS Health" (Open issues 0, Past 7 days), "Cost and usage" (Current month costs \$1.21, Forecasted month end costs), and "Applications" (0). A "Create application" button is visible. The bottom of the page includes links for Privacy, Terms, and Cookie preferences.

From the dashboard , select s3.



This screenshot is identical to the one above, but the S3 icon in the "Recently visited" sidebar is highlighted with a blue border, indicating it is the selected service. The rest of the interface and content are the same as the first screenshot.

Name your bucket , The name should be all small character with no special characters and must be a unique name.

General configuration

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

Bucket type 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.

Bucket name 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.

Object Ownership
Bucket owner enforced

Bucket is successfully created

Successfully created bucket "052jcreations3"
To upload files and folders, or to configure additional bucket settings, choose View details. **View details**

Account snapshot - updated every 24 hours All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [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.

Name	AWS Region	IAM Access Analyzer	Creation date
052jcreations3	US East (N. Virginia) us-east-1	View analyzer for us-east-1	February 17, 2025, 10:20:17 (UTC+05:30)

Create bucket

Upload an image

The screenshot shows the AWS S3 upload status page. At the top, there's a summary section with a note: "After you navigate away from this page, the following information is no longer available." Below this is a "Summary" section with two boxes: "Succeeded" (1 file, 11.5 MB (100.00%)) and "Failed" (0 files, 0 B (0%)). There are tabs for "Files and folders" and "Configuration". Under "Files and folders", a table lists one file: "it's the.png" (image/png, 11.5 MB, Status: Succeeded). The URL in the browser bar is `us-east-1.console.aws.amazon.com/s3/upload/052jcreations3?region=us-east-1&bucketType=general`.

Try to access the public link , we see that public acces is blocked

The screenshot shows a browser window displaying an XML error response. The message reads: "This XML file does not appear to have any style information associated with it. The document tree is shown below." Below this, the XML error code is shown:

```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied.</Message>
<RequestId>RJXQH3N59BYGWf2</RequestId>
<HostId>fa/Rp+D14BwYFHR/NMTlJHA/Ef3ElWrTGyahhRvVpPqTTycGgC0xtkxty0AffWkxXbx2rLbM4Jk=</HostId>
```

Click on edit public access in the bucket permissions and turn off block public access.

052jcreations3 [Info](#)

Objects | Metadata | 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)

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

Edit

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](#)

Edit **Delete**

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](#).

The access is updated.

Amazon S3

General purpose buckets

- Directory buckets
- Table buckets
- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight [\[1\]](#)

► AWS Marketplace for S3

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**

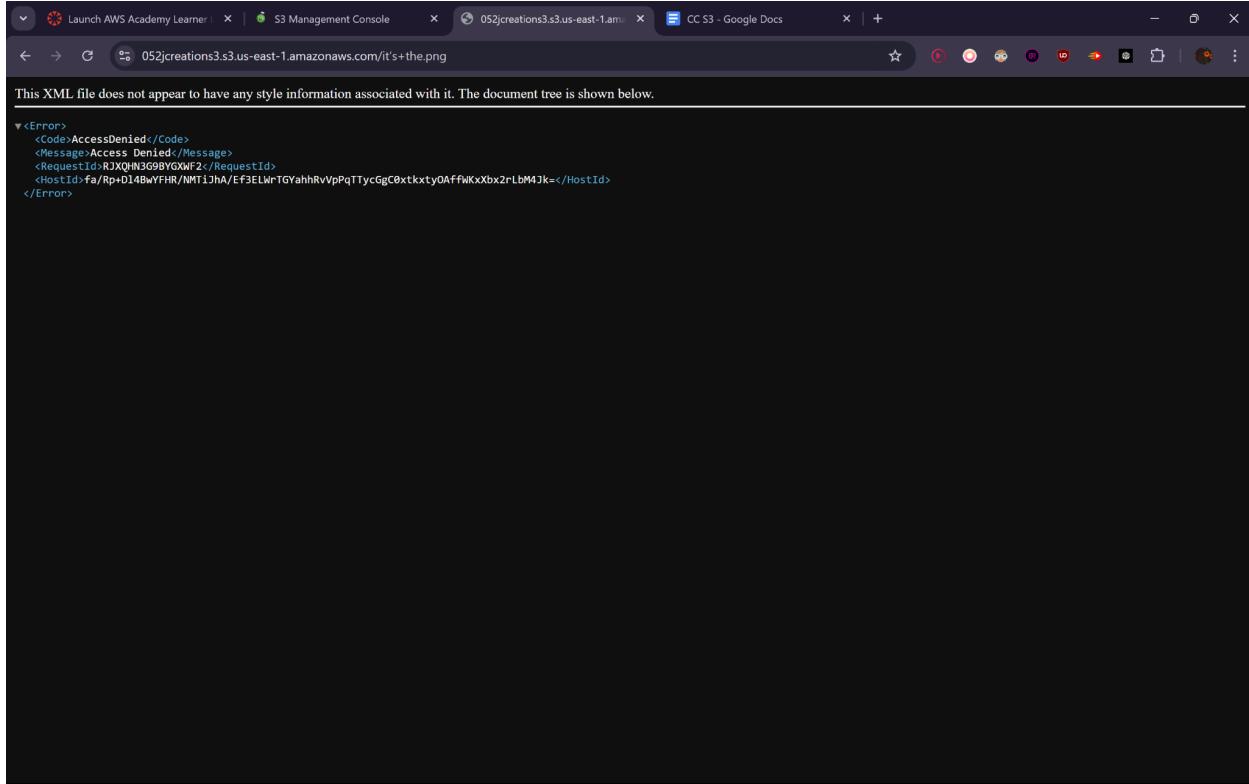
Edit the Object ownership. And select enable ACL

The screenshot shows the 'Edit Object Ownership' page in the AWS S3 console. On the left, there's a sidebar with navigation links like 'Amazon S3', 'General purpose buckets', 'Storage Lens', and 'AWS Marketplace for S3'. The main content area is titled 'Edit Object Ownership' and contains a 'Object Ownership' section. It explains that control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). It highlights two options: 'ACLs disabled (recommended)' and 'ACLs enabled'. The 'ACLs enabled' option is selected and highlighted with a blue border. A note below it states: '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.' Another note below that says: 'Enabling ACLs turns off the bucket owner enforced setting for Object Ownership. Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.' There's also a checkbox for acknowledging that ACLs will be restored.

Edit the access control list , select all options under everyone public

The screenshot shows the 'Edit access control list (ACL)' page in the AWS S3 console. The left sidebar includes 'Amazon S3', 'General purpose buckets', 'Storage Lens', and 'AWS Marketplace for S3'. The main area displays the ACL configuration for a specific object. It lists four groups: 'Canonical ID', 'Everyone (public access)', 'Authenticated users group (anyone with an AWS account)', and 'S3 log delivery group'. Under 'Everyone (public access)', both 'List' and 'Write' checkboxes are checked. Under 'Authenticated users group', 'List' is checked and 'Write' is unchecked. Under 'S3 log delivery group', both 'List' and 'Write' are unchecked. A note at the bottom of this section says: 'When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access the objects in this bucket.' Below this is a section for 'Access for other AWS accounts' which states 'No other AWS accounts associated with the resource.' At the bottom right are 'Cancel' and 'Save changes' buttons.

Even if we check the public link now , the link is still not accessible as we have only changed bucket level



Edit the object level access control and select everything under everyone , and save changes

A screenshot of the AWS S3 Edit access control list (ACL) interface. The URL in the address bar is "us-east-1.console.aws.amazon.com/s3/buckets/052jcreations3/object/edit_acl?region=us-east-1&bucketType=general&prefix=it's+the...". The main section shows the Access control list (ACL) configuration. It lists grants for the Object owner (your AWS account), Everyone (public access), and Authenticated users group. For each grantee, it shows checkboxes for Read and Write permissions. The "Everyone" grant has both Read and Write checkboxes checked. The "Authenticated users group" grant has both Read and Write checkboxes unchecked. A warning message at the bottom states: "When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object." Below this, there are two checkboxes: "I understand the effects of these changes on this object." and "You must select the check box to continue." At the bottom, there is an "Add grantee" button.

Now the link is publicly accessible

