

1 – Bucket Creation

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

Account snapshot - updated every 24 hours All AWS Regions

[View Storage Lens dashboard](#)

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

General purpose buckets

Directory buckets

General purpose buckets (1) All AWS Regions

Copy ARN

Empty

Delete

Create bucket

Buckets are containers for data stored in S3.

Find buckets by name

< 1 >

Name	AWS Region	IAM Access Analyzer	Creation date
sagemaker-us-east-1-254050731868	US East (N. Virginia) us-east-1	View analyzer for us-east-1	May 11, 2022, 21:52:04 (UTC-05:00)

Amazon S3 > Buckets > Create bucket

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.

Directory

Recommended for low-latency use cases. Express One Zone storage class, which is available in a single Availability Zone.

Bucket name

static-webpage-project

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

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.

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 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.

static-webpage-project [Info](#)

Objects

Metadata - Preview

Properties

Permissions

Metrics

Management

Access Points

Actions

Create folder

Upload

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

< 1 >







	Name		Type		Last modified		Size		Storage class	
No objects										
You don't have any objects in this bucket.										
<div> Upload</div>										



2 – Upload Files

static-webpage-project [Info](#)

[Objects](#) | [Metadata - Preview](#) | [Properties](#) | [Permissions](#) | [Metrics](#) | [Management](#) | [Access Points](#)

Objects (0) [Info](#)

      [Actions](#) [Create folder](#)

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](#)


Name

Type

Last modified


Size

Storage class

< 1 > 

No objects

You don't have any objects in this bucket.



Upload [Info](#)

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (0)

All files and folders in this table will be uploaded.

[Remove](#)[Add files](#)[Add folder](#)

< 1 >

Name

Folder

Type

Size

No files or folders

You have not chosen any files or folders to upload.

Files and folders (1633 total, 20.8 MB)

All files and folders in this table will be uploaded.

[Remove](#)[Add files](#)[Add folder](#)

< 1 2 3 4 5 6 7 ... 164 >

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	udacity-starter-website.zip	code/	application/x-zip-compressed	6.2 MB
<input type="checkbox"/>	.DS_Store	code/vendor/	-	6.0 KB
<input type="checkbox"/>	jquery.js	code/vendor/jquery/	text/javascript	265.4 KB
<input type="checkbox"/>	jquery.min.js	code/vendor/jquery/	text/javascript	84.9 KB
<input type="checkbox"/>	jquery.min.map	code/vendor/jquery/	text/plain	129.3 KB
<input type="checkbox"/>	jquery.slim.js	code/vendor/jquery/	text/javascript	213.8 KB
<input type="checkbox"/>	jquery.slim.min.js	code/vendor/jquery/	text/javascript	68.3 KB
<input type="checkbox"/>	jquery.slim.min.map	code/vendor/jquery/	text/plain	102.9 KB

Destination [Info](#)

Destination

[s3://static-webpage-project](#)

► Destination details

Bucket settings that impact new objects stored in the specified destination.

► Permissions

Grant public access and access to other AWS accounts.

► Properties

Specify storage class, encryption settings, tags, and more.

[Cancel](#)[Upload](#) 

3 – Secure Bucket

static-webpage-project [Info](#)

Objects | Metadata - Preview | 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)

[Edit](#)

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

 OFF

► Individual Block Public Access settings for this bucket

Bucket policy

[Edit](#)

[Delete](#)

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](#)

No policy to display.


 Copy

Edit bucket policy [Info](#)

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies do [more](#)

Bucket ARN

 `arn:aws:s3:::static-webpage-project`

Policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "AddPerm",  
6       "Effect": "Allow",  
7       "Principal": "*",  
8       "Action": "s3:GetObject",  
9       "Resource": "arn:aws:s3:::static-webpage-project/*"  
10    }  
11  ]  
12 }
```

4 – Configure Bucket

static-webpage-project [Info](#)

Objects Metadata - Preview **Properties** Permissions Metrics

Bucket overview

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

Amazon Resource Name (ARN)
[arn:aws:s3::static-webpage-project](#)

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both [more](#)

Bucket Versioning
Disabled

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

Tags (0)

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

Key	Value
-----	-------

Edit static website hosting [Info](#)

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

☐ Disable

☒ Enable

Hosting type

☒ Host a static website

Use the bucket endpoint as the web address. [Learn more](#)

☐ Redirect requests for an object

Redirect requests to another bucket or domain. [Learn more](#)

i For your customers to access content at the website endpoint, you must make all your content publicly accessible. Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#)

Index document

Specify the home or default page of the website.

index.html

Error document - optional

This is returned when an error occurs.

error.html

Redirection rules - optional

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

Static website hosting

Edit

Use this bucket to host a website or redirect requests. [Learn more](#)

i We recommend using AWS Amplify Hosting for static website hosting

Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about [Amplify Hosting](#) or [View your existing Amplify apps](#)

Create Amplify app

S3 static website hosting

Enabled

Hosting type

Bucket hosting

Bucket website endpoint

When you configure your bucket as a static website, the website is available at the Amazon Region-specific website endpoint of the bucket. [Learn more](#)

<http://static-webpage-project.s3-website-us-east-1.amazonaws.com>

5 – Distribute Website

Networking & Content Delivery

Amazon CloudFront

Securely deliver content with low latency and high transfer speeds

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds.

Get started with CloudFront

Enable accelerated, reliable and secure content delivery for Amazon S3 buckets, Application Load Balancers, Amazon API Gateway APIs, and more in 5 minutes or less.

Create a CloudFront distribution

Settings

Origin domain

Choose an AWS origin, or enter your origin's domain name. [Learn more](#)

static-webpage-project.s3-website-us-east-1.amazonaws.com

Enter a valid DNS domain name, such as an S3 bucket, HTTP server, or VPC origin ID.

Protocol

- ☒ HTTP only
- ☐ HTTPS only
- ☐ Match viewer

HTTP port

Enter your origin's HTTP port. The default is port 80.

80

Origin path - optional

Enter a URL path to append to the origin domain name for origin requests.

Enter the origin path

Name

Enter a name for this origin.

static-webpage-project.s3.us-east-1.amazonaws.com

Add custom header - optional

CloudFront includes this header in all requests that it sends to your origin.

Add header

Enable Origin Shield

Origin shield is an additional caching layer that can help reduce the load on your origin and help protect its availability.

- ☒ No
- ☐ Yes

Edit behavior

Settings

Path pattern

Default (*)

Origin and origin groups

static-webpage-project.s3.us-east-1.amazonaws.com

Compress objects automatically

- ☐ No
- ☒ Yes

Viewer

Viewer protocol policy

- ☐ HTTP and HTTPS
- ☒ Redirect HTTP to HTTPS
- ☐ HTTPS only

Allowed HTTP methods

- ☒ GET, HEAD
- ☐ GET, HEAD, OPTIONS
- ☐ GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Restrict viewer access

If you restrict viewer access, viewers must use CloudFront signed URLs or signed cookies to access your content.

- ☒ No

Domain name	Alterna...	Origins	Status	Last modified
d1l25st2d6lho4.cloudfront.net	-	static-webpage	Enabled	January 19, 2025 at 7:25:49 AM UTC

6 – Access Website

