

AWS Quick Start Guide: Back Up Your Files to Amazon Simple Storage Service S3 Bucket

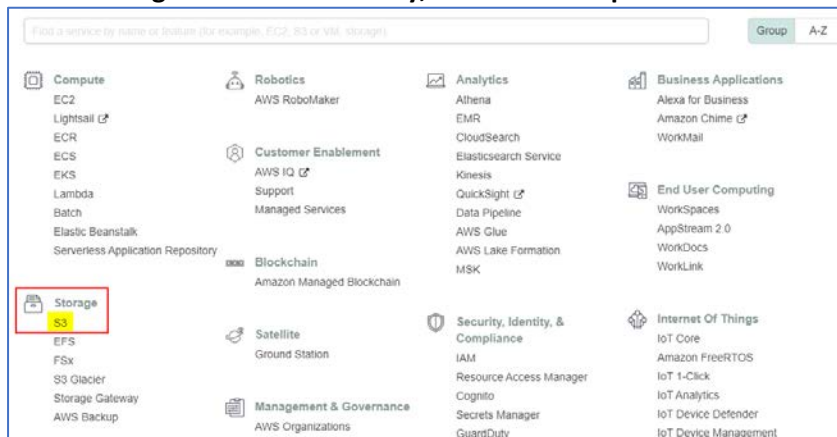
Welcome to the AWS Quick Start Guide: Back Up Your Files to Amazon Simple Storage Service. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere on the web. By completing the steps in this quick start guide, you will successfully create a new S3 bucket, add a file to it, retrieve this file, and finally delete it, all within the AWS Free Tier.

Create an Application Load Balancer

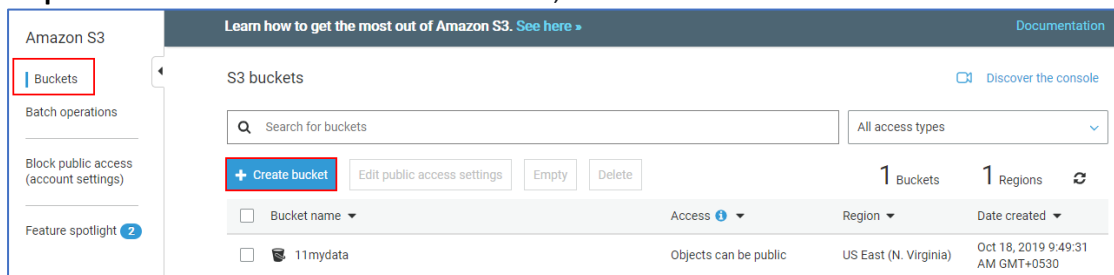
First, you need to create an Amazon S3 bucket where you will store your objects.

Step 1: Create an Amazon S3 Bucket

Under **Storage & Content Delivery**, choose **S3** to open the Amazon S3 console.

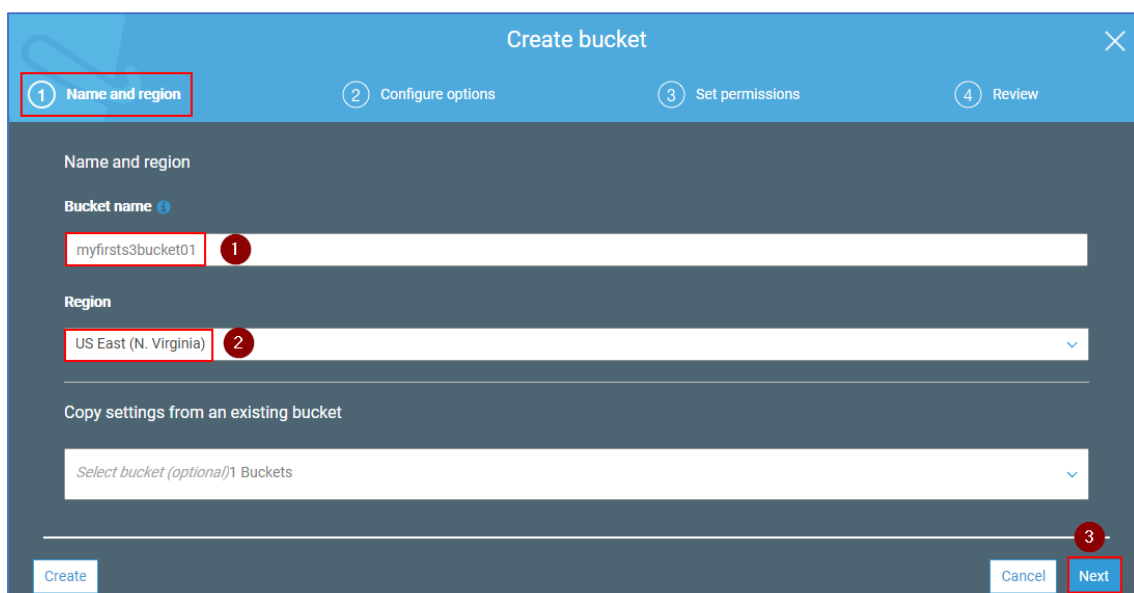


Step 2: From the Amazon S3 console dashboard, choose **Create Bucket**.



Step 3: In **Create a Bucket**, type a bucket name in **Bucket Name**.

The bucket name you choose must be globally unique across all existing bucket names in Amazon S3 (that is, across all AWS customers). For more information, see [Bucket Restrictions and Limitations](#).



Create bucket

1 Name and region

2 Configure options

3 Set permissions

4 Review

Properties

Versioning

☒ Keep all versions of an object in the same bucket. [Learn more](#)

Server access logging

☐ Log requests for access to your bucket. [Learn more](#)

Tags

You can use tags to track project costs. [Learn more](#)

Object-level logging

☐ Record object-level API activity using AWS CloudTrail for an additional cost. [See CloudTrail pricing](#) or [learn more](#)

Default encryption

☐ Automatically encrypt objects when they are stored in S3. [Learn more](#)

Advanced settings

Object lock

☐ Permanently allow objects in this bucket to be locked. [Learn more](#)

Management

CloudWatch request metrics

☐ Monitor requests in your bucket for an additional cost. [See CloudWatch pricing](#) or [learn more](#)

Previous

Next

Create bucket

1 Name and region

2 Configure options

3 Set permissions

4 Review

Note: You can grant access to specific users after you create the bucket.

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. 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. 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** Check mark this option if you want to block the 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 policies**
 S3 will block new bucket 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 policies**
 S3 will ignore public and cross-account access for buckets with policies that grant public access to buckets and objects.

Manage system permissions

Do not grant Amazon S3 Log Delivery group write access to this bucket

Do not grant Amazon S3 Log Delivery group write access to this bucket

Grant Amazon S3 Log Delivery group write access to this bucket

Select the appropriate option

Previous

Next

Create bucket

1 Name and region

2 Configure options

3 Set permissions

4 Review

Name and region

Bucket name: myfirsts3bucket007

Region: US East (N. Virginia)

Edit

Options

Versioning

Enabled

Server access logging

Disabled

Tagging

0 Tags

Object-level logging

Disabled

Default encryption

AES-256

CloudWatch request metrics

Disabled

Object lock

Disabled

Edit

Permissions

Edit

Block all public access

Off

Block public access to buckets and objects granted through new access control lists (ACLs)

Off

Block public access to buckets and objects granted through any access control lists (ACLs)

Off

Block public access to buckets and objects granted through new public bucket policies

Off

Block public and cross-account access to buckets and objects through any public bucket policies

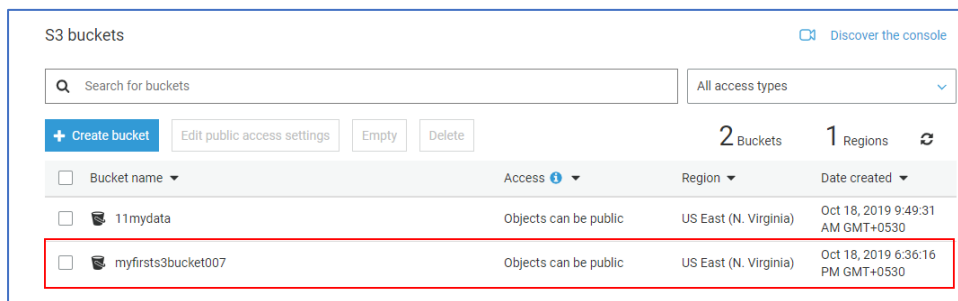
Off

System permissions

Disabled

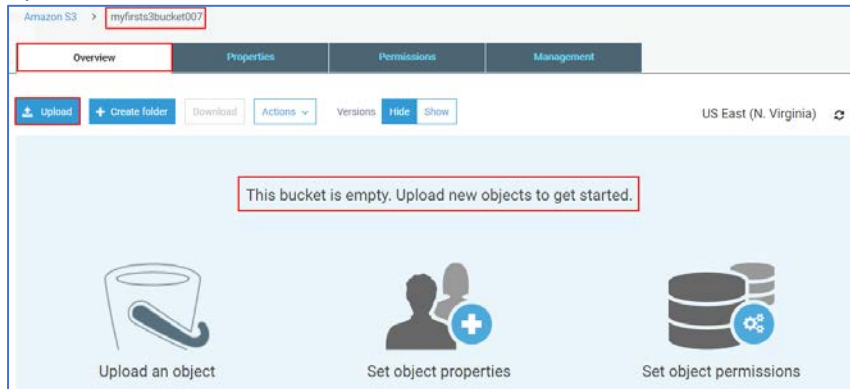
Previous

Create bucket

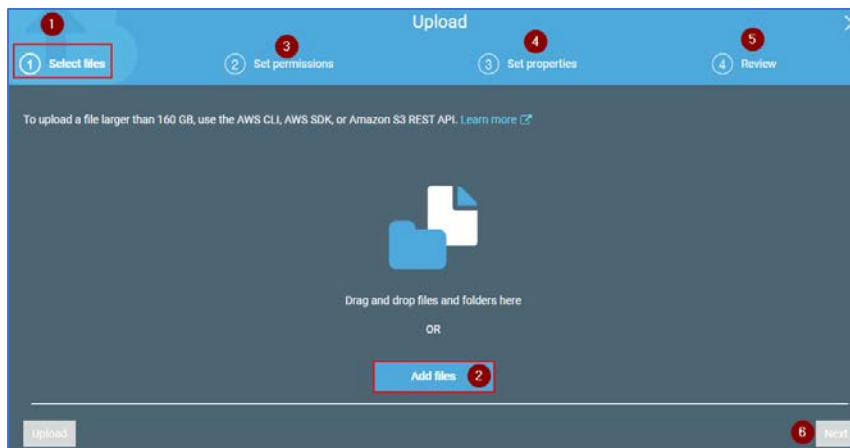


When Amazon S3 successfully creates your bucket, the console displays your empty bucket in the **Buckets** pane.

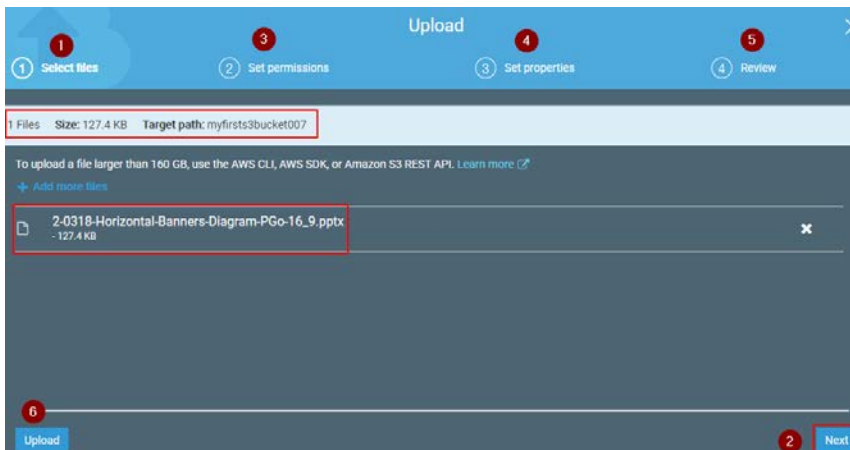
Upload a File to Your Amazon S3 Bucket



In the Amazon S3 console, choose the bucket where you want to upload an object, choose **Upload**, and then choose **Add Files**.



Select files



Set permissions

Upload

1 Select files

2 Set permissions

3 Set properties

4 Review

1 Files Size: 127.4 KB Target path: myfirsts3bucket007

Manage users

User ID

Objects

Object permissions

ashokg20(Owner)

☒ Read

☒ Read ☒ Write

×

Access for other AWS account

+ Add account

Account

Objects

Object permissions

Manage public permissions

Do not grant public read access to this object(s) (Recommended)

Upload

Previous

Next

Set properties

Upload

1 Select files

2 Set permissions

3 Set properties

4 Review

1 Files Size: 127.4 KB Target path: myfirsts3bucket007

Storage class

Choose a storage class based on your use case and access requirements. [Learn more](#) or see [Amazon S3 pricing](#)

Storage class	Designed for	Availability Zones	Min storage duration	Min billable object size	Monitoring and automation fees	Retrieval fees
<input checked="" type="radio"/> Standard	Frequently accessed data	≥ 3	-	-	-	-
<input type="radio"/> Intelligent-Tiering	Long-lived data with changing or unknown access patterns	≥ 3	30 days	-	Per-object fees apply	-
<input type="radio"/> Standard-IA	Long-lived, infrequently accessed data	≥ 3	30 days	128KB	-	Per-GB fees apply
<input type="radio"/> One Zone-IA	Long-lived, infrequently accessed, non-critical data	≥ 1	30 days	128KB	-	Per-GB fees apply
<input type="radio"/> Glacier	Archive data with retrieval times ranging from minutes to hours	≥ 3	90 days	40KB	-	Per-GB fees apply
<input type="radio"/> Glacier Deep Archive	Archive data that rarely, if ever, needs to be accessed with retrieval times in hours	≥ 3	180 days	40KB	-	Per-GB fees apply
<input type="radio"/> Reduced Redundancy (Not recommended)	Frequently accessed, non-critical data	≥ 3	-	-	-	-

Encryption

Protect data at rest by using Amazon S3 master key or by using AWS KMS master key.

☒ None ☐ Amazon S3 master-key ☐ AWS KMS master-key

Metadata

Metadata is a set of name-value pairs. You cannot modify object metadata after it is uploaded.

Header

Value

Select a key

Save

Clear

Tag

Add tags to search, organize and manage access

Key

Value

Key

Value

Save

Clear

Upload

Previous

Next

Review and upload done

Upload

1 Select files

2 Set permissions

3 Set properties

4 Review

Files

1 Files Size: 127.4 KB

Permissions

1 grantees

Properties

Encryption No Storage class Standard

Metadata

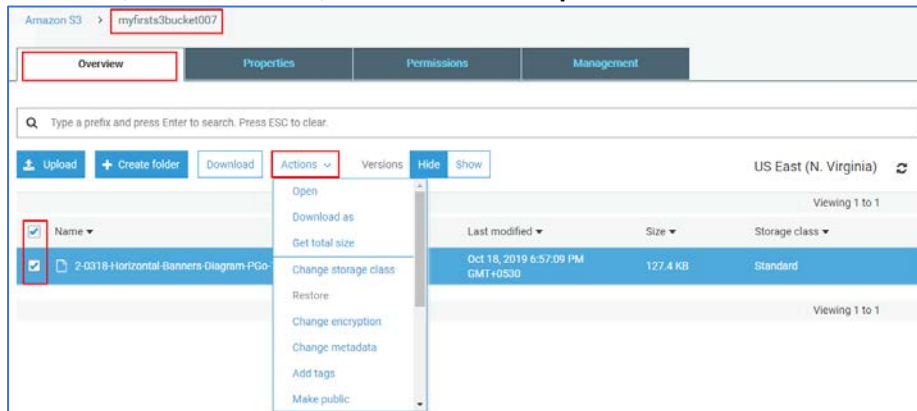
Tag

Previous

Upload

Retrieve a File from Your Amazon S3 Bucket

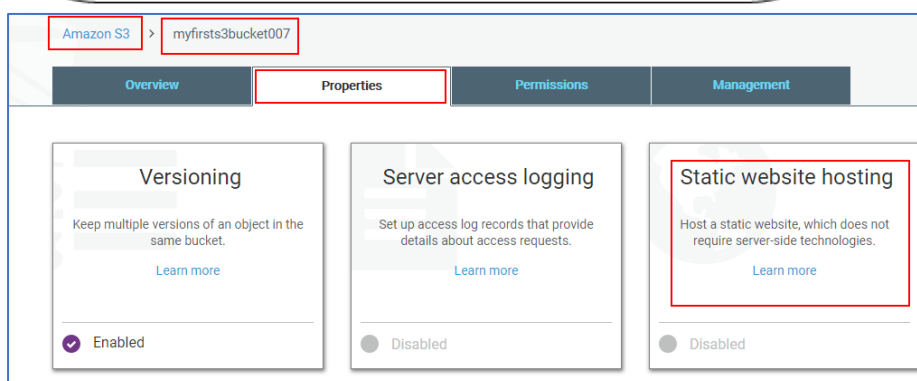
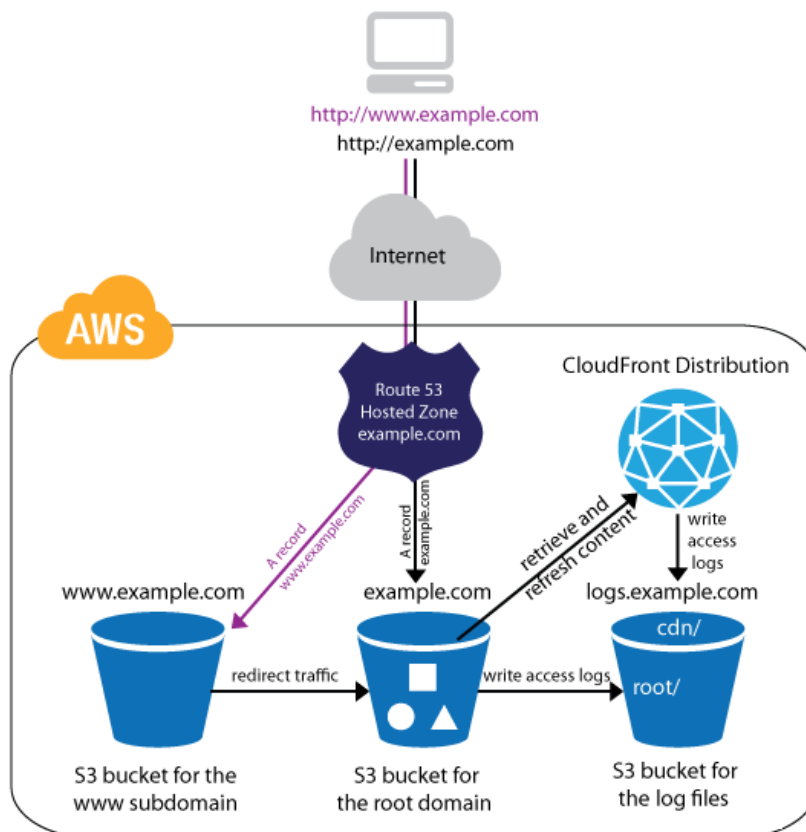
In the Amazon S3 console, choose your S3 bucket, choose the file that you want to open or download, choose **Actions**, and then choose **Open** or **Download**.



Configuring Your S3 Bucket for Static Website Hosting

You can host a static website on Amazon S3. On a static website, individual webpages include static content. They might also contain client-side scripts. By contrast, a dynamic website relies on server-side processing, including server-side scripts such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting. AWS also has resources for hosting dynamic websites. To learn more about website hosting on AWS

<https://docs.aws.amazon.com/AmazonS3/latest/dev/website-hosting-custom-domain-walkthrough.html>



- Click into your bucket.
- Click the “Properties” section.
- Click the “Static website hosting” option.
- Select “Use this bucket to host a website”.
- Enter “index.html” as the Index document.

Static website hosting

Endpoint : `http://myfirsts3bucket007.s3-website-us-east-1.amazonaws.com`

☒ Use this bucket to host a website [Learn more](#)

Index document [i](#)

`index.html`

Error document [i](#)

`error.html`

Redirection rules (optional) [i](#)

☐ Redirect requests [Learn more](#)

☐ Disable website hosting

Disabled

Cancel Save

This quick start guide includes the following topics:

- **Step 1: Create an Amazon S3 Bucket**
- **Step 2: Upload a File to Your Amazon S3 Bucket**
- **Step 3: Retrieve a File from Your Amazon S3 Bucket**
- **Step 4: Delete a File From Your Amazon S3 Bucket**

For more information about Amazon S3, see the [Amazon Simple Storage Service Documentation](#).