

WORKING AMAZON SIMPLE STORAGE SERVICE (S3)

Amazon S3 Overview

Amazon Simple Storage Service (S3) provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web. This lab is designed to demonstrate how to interact with S3 to store, view, move and delete objects.

This lab will walk you through the following:

- Creating a bucket in S3
- Adding an object to the S3 bucket
- View the object in S3
- Move the object in S3
- Enable bucket versioning
- Delete the object and the bucket in S3

Create a Bucket in S3

Every object in Amazon S3 is stored in a bucket. Before you can store data in Amazon S3 you must create a bucket.

You are not charged for creating a bucket; you are only charged for storing objects in the bucket and for transferring objects in and out of the bucket.

1. Sign into the AWS Management Console and open the [Amazon S3 console](#)

2. Click **Create Bucket**. The **Create a Bucket** dialog box appears.

The screenshot shows the AWS 'Create bucket' dialog box. At the top, the AWS logo and 'Services' menu are visible. The breadcrumb 'Amazon S3 > Create bucket' is shown. The main heading is 'Create bucket', followed by a subtext: 'Buckets are containers for data stored in S3. [Learn more](#)'. The 'General configuration' section contains a 'Bucket name' input field with the text 'myawsbucket'. Below the input field is a note: 'Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)'. The 'Region' dropdown is set to 'EU (Frankfurt) eu-central-1'. Below the region is a section for 'Copy settings from existing bucket - optional' with a 'Choose bucket' button. The 'Bucket settings for Block Public Access' section contains text explaining that public access is granted by default and that users should turn on 'Block all public access' to restrict access, with a link to 'Learn more'.

3. Enter a bucket name in the Bucket Name field. The bucket name you choose must be unique across all existing bucket names in Amazon S3. One way to do that is to prefix your bucket names with your organization's name. Bucket names must comply with the following requirements.

Bucket names:

- Must be unique across all of Amazon S3
- Must be between 3 and 63 characters long
- Must not contain uppercase characters
- Can contain lowercase letters, numbers, periods (.) and dashes (-)
- Must start with a lowercase letter or number
- Must not contain underscores (_), end with a dash, have consecutive periods, or use dashes adjacent to periods.
- Cannot be formatted as an IP address (e.g., 10.1.1.1).

There might be additional restrictions on bucket names based on the region your bucket is in or how you intend to access the object. Once you create a bucket, you cannot change its name. In addition, the bucket name is visible in the URL that points to the objects stored in the bucket. Make sure the bucket name you choose is appropriate.

4. In the Region drop-down list box, select a region (for example `us-east-1`). Choose the us-east-1 region. Objects stored in a Region never leave that Region unless you explicitly transfer them to another Region. Click **Next**.

Create bucket

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

General configuration

Bucket name

aws-immersionday-lab-demo-bucket

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

Region

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

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

5. By default, all buckets are set to “block public access”. At this time, leave the default setting of block all public access. [Learn More](#)
6. Under Tags, click **Add tag**. Then in the Key box, type `Purpose`, and in the Value box, enter `Immersion Day`.

Tags (1) - optional

Track storage cost or other criteria by tagging your bucket. [Learn more](#)

Key

Purpose

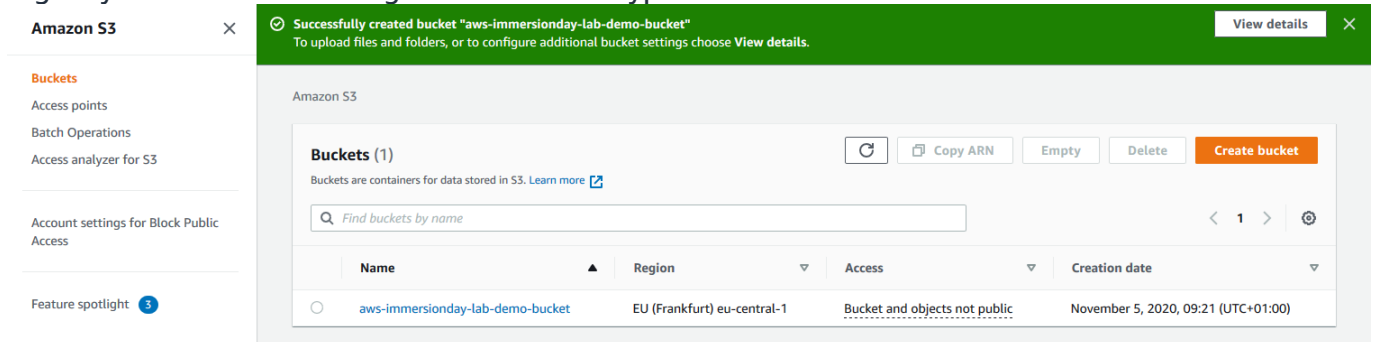
Value - optional

Immersion Day

Remove

Add tag

7. Have a good look at the other options, but leave them as default for this lab.
8. Finally, review your settings and click Create bucket. When Amazon S3 successfully creates your bucket, the console displays your empty bucket in the Buckets panel. You can also see the region your bucket is in along with the access type.



Well done – you’ve created your first bucket in Amazon S3!

Add an Object to a Bucket

Now that you’ve created a bucket, you are ready to add an object to it. An object can be any kind of file: a text file, a photo, a video and so forth. When you upload a file to Amazon S3, it is stored as an S3 object. Objects consist of the file data and metadata that describes the object. You can have an unlimited number of objects in a bucket. [Learn More](#)

1. In the Amazon S3 console, click on the name of the bucket to which you want to upload an object, and then click **Upload** in the Overview tab. You may also directly

drag and drop a file you want to upload.

Amazon S3 > aws-immersionday-lab-demo-bucket

aws-immersionday-lab-demo-bucket

Bucket overview

Region EU (Frankfurt) eu-central-1	Amazon resource name (ARN) arn:aws:s3::aws-immersionday-lab-demo-bucket	Creation date November 5, 2020, 09:21 (UTC+01:00)	Access <u>Bucket and objects not public</u>
---------------------------------------	--	--	--

Objects | Properties | Permissions | Metrics | Management | Access points

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

Objects (0)
Objects are the fundamental entities stored in Amazon S3. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Delete **Actions** ▼ **Create folder** **Upload**

Find objects by prefix

< 1 >

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

Upload

- The Upload dialogue opens (its appearance may differ slightly between different browsers), click **Add Files** to select a file to upload. A file selection dialog box opens. Select a small file to upload and click Open. The Upload dialogue shows the files and

folders you've selected to upload.

[Amazon S3](#) > [aws-immersionday-lab-demo-bucket](#) > Upload

Upload

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

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

Files and folders (1 Total, 2.5 KB)
All files and folders in this table will be uploaded.

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

☐

Name	Folder	Type	Size
awesome-logo.png	-	image/png	2.5 KB

Destination

Destination
[s3://aws-immersionday-lab-demo-bucket](#)

Bucket details

AWS Region
EU (Frankfurt) eu-central-1

Bucket Versioning
When enabled, multiple variants of an object can be stored in the bucket to easily recover from unintended user actions and application failures.
Disabled

Default encryption
When enabled, new objects stored in this bucket are automatically encrypted.
Disabled

Object Lock
When enabled, objects in this bucket might be prevented from being deleted or overwritten for a fixed amount of time or indefinitely.
Disabled

For this lab, you can choose any file or picture you have available on your laptop. Before clicking the final upload button, review the options that are available. For today's lab, we will use the default permissions. We will be using the standard storage option. To learn more about Amazon S3 storage classes [Click Here](#)

4. Click **Upload**. You can watch the progress of the upload at the top of the screen. This bar appears as soon as the upload begins. Once the object has been uploaded, you will see a confirmation message.

Upload succeeded
View details below.

Upload: status

Exit

The information below will no longer be available after you navigate away from this page.

Summary

Destination

s3://aws-immersionday-lab-demo-bucket

Succeeded

1 file, 2.5 KB (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 Total, 2.5 KB)

Find by name

< 1 >

Name	Folder	Type	Size	Status	Error
awesome-logo.png	-	image/png	2.5 KB	Succeeded	-

Good work - you have added a file to your bucket!

View an Object






Now that you've added an object to a bucket, you can try and open and view it in a browser.

By default, your Amazon S3 buckets and objects are private. To view an object using a URL, for example, <https://s3.amazonaws.com/Bucket/Object> the object must be publicly readable. Otherwise, you will need to create signed URL that includes a signature with authentication information.

Bucket access permissions specify which users are allowed access to the objects in a bucket and which types of access they have. Object access permissions specify which users are allowed access to the object and which types of access they have. For example, one user might have only read permission, while another might have read and write permissions.

Bucket and object permissions are independent of each other.

1. Click on the name of the file you uploaded. A detail window will appear. Click on the object URL. You will receive an error message that access is denied. That is because our bucket and our object are blocked from public access.

Properties	Permissions	Versions
Object overview		
Owner ee-account+1df33532a89e4f428860dfc02e89a566		S3 URI  s3://chradavi-aws-immersionday-lab-demo-bucket/AWSomeBuilderDeck (1).pptx
AWS Region US East (N. Virginia) us-east-1		Amazon resource name (ARN)  arn:aws:s3::chradavi-aws-immersionday-lab-demo-bucket/AWSomeBuilderDeck (1).pptx
Last modified January 9, 2021, 10:19:22 (UTC-08:00)		Entity tag (Etag)  8685dc5f2aae45d037862a35a3452e21
Size 2.4 MB		Object URL  https://chradavi-aws-immersionday-lab-demo-bucket.s3.amazonaws.com/AWSomeBuilderDeck+(1).pptx
Type pptx		
Key  AWSomeBuilderDeck (1).pptx		

What happens when you click on the Object Url?

By default, your Amazon S3 buckets and objects are private. To view an object using a URL, for example, <https://s3.amazonaws.com/Bucket/Object> the object must be publicly readable. Otherwise, you will need to create signed URL that includes a signature with authentication information. You can optionally save the object locally.

It is a best practice to block public access to your buckets as they could hold sensitive data. Amazon S3 offers various layers of protection to help you implement this best practice. One such control is called **Block Public Access**. This control is available at an account level and even at bucket level. You can find more details [here](#). For the purpose of this lab, we'll allow public access and the next steps walk you through on allowing this access.

2. In the left hand pane, select "Account Settings for Block Public Access".

Amazon S3



Buckets

Access points

Batch Operations

Access analyzer for S3

Account settings for Block Public
Access

▼ Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight **2**

► AWS Marketplace for S3

3. Make sure the settings are set to off. If not click **Edit** and uncheck “Block all public access”. Click Save Changes.

Edit block public access (account settings)

Use Amazon S3 Block public access settings to control the settings that allow public access to your data.

Block public access (account 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 account-wide for all current and future buckets and 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, 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


4. Select “Buckets” from the left pane and select your S3 bucket from the list.

5. Click on the bucket name and then select **Permissions**.

Amazon S3 > aws-immersionday-lab-demo-bucket


aws-immersionday-lab-demo-bucket

Bucket overview

Region EU (Frankfurt) eu-central-1	Amazon resource name (ARN)  arn:aws:s3:::aws-immersionday-lab-demo-bucket	Creation date November 5, 2020, 09:21 (UTC+01:00)	Access <u>Bucket and objects not public</u>
---------------------------------------	---	--	--

Objects | **Properties** | **Permissions** | **Metrics** | **Management** | **Access points**

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](#) 

Edit

Block *all* public access

☒ On

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

☒ On
- Block public access to buckets and objects granted through *any* access control lists (ACLs)**

☒ On
- Block public access to buckets and objects granted through *new* public bucket or access point policies**

☒ On
- Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**

☒ On

6. Click **Edit**. Uncheck the box for Block all public access. Click **Save**.

Amazon S3 > aws-immersionday-lab-demo-bucket > Edit Block public access (bucket settings)

Edit Block public access (bucket settings)

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](#)

7. Type "confirm" in the pop-up window to confirm this change. You should see a message appears that states "Successfully edited bucket settings for Block Public Access."
8. Go back to the object in your bucket. Click on the object name and go to the **Permissions** tab.
9. Scroll down and click on **Edit**. Then select **Everyone** and **check** read object. Finally Click **Save**.

Edit access control list

Access control list (ACL)

Grant basic read/write permissions to AWS accounts. [Learn more](#)

Grantee	Objects	Object ACL
Object owner (your AWS account) Canonical ID: 81afb5e96015c3529303e5a96a71210b4d0f0f19fddf4336798e182308ccde9d	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	<input checked="" type="checkbox"/> Read	<input type="checkbox"/> Read <input type="checkbox"/> Write
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	<input type="checkbox"/> Read	<input type="checkbox"/> Read <input type="checkbox"/> Write

When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.

[Learn more](#)

☒ I understand the effects of these changes on this object.

Instead of doing that you can also use the **Make public** button on the Overview tab as a shortcut.

- Click on the **Overview** tab. Scroll down and click on the Object URL. You should now be able to see your object.

Good job – you have retrieved your object from S3 via the web!

Move an Object

Now that you have added an object to a bucket and viewed it, you might like to move the object to a different bucket or folder. In this example, we will use the move operation to move one or more objects from one bucket to another bucket.

1. In the Amazon S3 console, create another bucket. Follow the same instructions you did earlier.
2. Select the first bucket you created. Under the **Permissions** tab, enable **Block all public access**. Follow the same instructions as earlier, instead this time, you will check the box to block all public access. Now the two buckets will have the same configuration.
3. Select the object(s) you want to move by clicking the selection box to their left.
4. Once you have selected your file, click on the **Actions** button, and then click **Move**

Amazon S3 > aws-immersionday-lab-demo-bucket

aws-immersionday-lab-demo-bucket

Bucket overview

Region	Amazon resource name (ARN)	Creation date	Access
EU (Frankfurt) eu-central-1	arn:aws:s3:::aws-immersionday-lab-demo-bucket	November 5, 2020, 09:21 (UTC+01:00)	<u>Bucket and objects not public</u>

Objects | Properties | Permissions | Metrics | Management | Access points

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

Objects (1)

Objects are the fundamental entities stored in Amazon S3. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Delete **Actions** **Create folder** **Upload**

Find objects by prefix


<input checked="" type="checkbox"/>	Name	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	awesome-l	November 5, 2020, 09:49 (UTC+01:00)	2.5 KB	Standard

- Open
- Calculate total size
- Copy
- Move**
- Initiate restore
- Query with S3 Select
- Download actions**
- Download
- Download as
- Edit actions**
- Rename object
- Edit storage class
- Edit server-side encryption
- Edit metadata
- Edit tags
- Make public


5. Select the bucket you created above, to which you want to move the object. Then Select Choose. Verify the information is correct. Then select Move.

Amazon S3 > aws-immersionday-lab-demo-bucket > Move

Move



- This action creates a copy of the object with updated settings and a new last-modified date in the specified location, and then deletes the original object.
- This action applies to all objects within the specified folders (prefixes). Objects added to these folders while the action is in progress might be affected.
- Copied objects will not retain the Object Lock settings from the original objects.
- Objects encrypted with customer-provided encryption keys (SSE-C) will fail to be copied using the S3 console. To copy objects encrypted with SSE-C, use the AWS CLI, AWS SDK, or the Amazon S3 REST API.

[Learn more](#) 


Destination

Destination

Browse S3

Format: s3://bucket/prefix/

Destination bucket details

AWS Region EU (Frankfurt) eu-central-1	Default encryption When enabled, new objects stored in this bucket are automatically encrypted. Disabled
Bucket Versioning When enabled, multiple variants of an object can be stored in the bucket to easily recover from unintended user actions and application failures.  Disabled	Object Lock When enabled, objects in this bucket might be prevented from being deleted or overwritten for a fixed amount of time or indefinitely. Disabled

When you move an object across buckets the previously set object permissions will persist by default. The bucket permissions will however change the object permissions accordingly.

You can verify that you original bucket is now empty. The file will be in the new bucket.

Congratulations - you have now moved an object between buckets.

Enable Bucket Versioning

If you want to add new version of the object to the same bucket but want to retain the old version, you can turn on bucket versioning.

1. In the S3 Console, click on the link representing the bucket you created, and then select the **Properties** tab.

The screenshot shows the AWS S3 console interface for a bucket's Properties tab. At the top, there are navigation tabs: Objects, Properties (selected), Permissions, Metrics, Management, and Access points. The main content area is divided into several sections:

- Bucket Versioning:** A section with a description of versioning and a 'Learn more' link. Below the description is an 'Edit' button. The status is 'Bucket Versioning Disabled'.
- Tags (1):** A section with a description and a 'Learn more' link. To the right is an 'Edit' button. Below is a table with two columns: 'Key' and 'Value'. The table contains one row: 'Purpose' and 'Immersion Day'.
- Default encryption:** A section with a description and a 'Learn more' link. To the right is an 'Edit' button. The status is 'Default encryption Disabled'.
- Server access logging:** A section with a description and a 'Learn more' link. To the right is an 'Edit' button. The status is 'Server access logging Disabled'.
- AWS CloudTrail data events:** A partially visible section at the bottom with a 'Configure in CloudTrail' link.

2. Click on **Edit** next to **Bucket versioning**, select **Enable** and then click **Save changes**.
3. Choose an object that you are able to edit on your computer, and upload it using the steps from the Add an Object to a Bucket section above.
4. Now open the original file on your computer and edit it, saving the updated version under the **same file name**.
5. Upload this updated file to the S3 bucket in the same way as before.
6. Now click on the object's link in the S3 bucket and click on **Versions** tab.

This shows the different versions of the object in the bucket. You can click on the **download** icon next to each version of the object to download that version.

Well done - you have now uploaded 2 different version of the same document.

Delete an Object and Bucket

You've added an object to a bucket, viewed it, and moved it. Now, you can delete it and the bucket it's in. If you no longer need to store the objects you uploaded and moved while going through this lab, you should delete them so you do not incur further charges on those objects.

1. In the Amazon S3 console, click on the link representing the bucket containing the object(s) you want to delete. Then select the object(s).
2. Click the **Delete** button. To confirm the action in the **Delete objects** dialogue, type "delete" and click **Delete objects**.

The screenshot shows the Amazon S3 console interface for a bucket. The 'Objects' tab is selected. A dashed box at the top says 'Drag and drop files and folders you want to upload here, or choose Upload.' Below this, the 'Objects (1)' section shows a single object, 'awesome.txt', with a size of 9.0 B and a storage class of 'Standard'. The object is selected with a checkbox. The 'List versions' toggle is turned off. The 'Delete' button is visible.

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	awesome.txt	txt	November 5, 2020, 10:34 (UTC+01:00)	9.0 B	Standard

3. If you deleted one or more objects from a bucket in which versioning is enabled, select the **List versions** option to see that the older versions of the deleted objects still exist.


The screenshot shows the Amazon S3 console interface for a bucket with versioning enabled. The 'List versions' toggle is turned on. The 'Delete' button is visible. The table below shows three versions of the object 'awesome.txt'.

<input type="checkbox"/>	Name	Type	Version ID	Last modified	Size	Storage class
<input type="checkbox"/>	awesome.txt	Delete marker	zmf0HEalaJnqq9RPXurAjGCKcIneN11k	November 5, 2020, 10:39 (UTC+01:00)	0 B	-
<input type="checkbox"/>	awesome.txt	txt	vgjEKEj7bhKKqBIV8.nYFaDmBbT3iYl	November 5, 2020, 10:34 (UTC+01:00)	9.0 B	Standard
<input type="checkbox"/>	awesome.txt	txt	0w3tVJ53v6wNhhvYjpGHNnrj.aRlMC9EH	November 5, 2020, 10:34 (UTC+01:00)	5.0 B	Standard


4. You can then select the checkboxes for the older versions of the objects, click **Delete** to delete the older versions.
5. Navigate back to the S3 console and select the bucket you want to delete (not the link to its right), and at the top of the page, click **Delete**. Confirm the deletion by typing its name verbatim at the Delete bucket prompt.

Amazon S3 > aws-immersionday-lab-demo-bucket > Delete bucket

Delete bucket



- Deleting a bucket cannot be undone.
- Bucket names are unique. If you delete a bucket, another AWS user can use the name.

[Learn more](#) 

Delete bucket aws-immersionday-lab-demo-bucket

To confirm deletion, type the name of the bucket.

Cancel **Delete bucket**

To delete a bucket, you must first delete all of the objects in it. If you haven't deleted all of the objects in your bucket, do that now.

Well done, your bucket is now deleted!

Conclusion

In this lab you have learned the basic operations to manage the lifecycle of an S3 object. First, you created a bucket, which is the logical container of objects. Then by uploading, viewing, moving an object, and enabling versioning, you learned the basic operations of the object itself. Finally, you learned how to delete both an object and a bucket.

You could continue exploring more [features of S3](#)