

Introduction to Amazon Simple Storage Service (S3)

Objectives

After completing this lab, you will know how to:

- Create a bucket in Amazon S3
- Add an object to a bucket
- Manage access permissions on an object and a bucket
- Create a bucket policy
- Use bucket versioning

Prerequisites

This lab follows the *Getting Started with Amazon Simple Storage Service (S3)* digital course.

Duration

This lab requires 60 minutes to complete.

Overview

This lab teaches you the basic feature functionality of Amazon S3 using the AWS Management Console.

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, Internet of Things (IoT) devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements. Amazon S3 is designed for 99.99999999% (11 9's) of durability and stores data for millions of applications for companies all around the world.

Start lab

1. To launch the lab, at the top of the page, choose **Start Lab**.

Caution: You must wait for the provisioned AWS services to be ready before you can continue.

2. To open the lab, choose **Open Console**.

You are automatically signed in to the AWS Management Console in a new web browser tab.

Warning: Do not change the **Region** unless instructed.

Common sign-in errors

Error: Choosing Start Lab has no effect

In some cases, certain pop-up or script blocker web browser extensions might prevent the **Start Lab** button from working as intended. If you experience an issue starting the lab:

- Add the lab domain name to your pop-up or script blocker's allow list or turn it off.

- Refresh the page and try again.

Lab Scenario

You work for a company using Amazon S3 for data storage. An application residing on an EC2 instance needs to push reporting data to an S3 bucket daily. You are tasked with creating an S3 bucket for your company to use for storing this report data. For a successful deployment, you need to ensure the EC2 instance has enough privileges to be able to upload and retrieve data from the S3 bucket. For security reasons, only the EC2 instance can write data to the S3 bucket. The files in the S3 bucket also require protection against accidental deletion. This lab follows the *Getting Started with Amazon S3 digital course*.

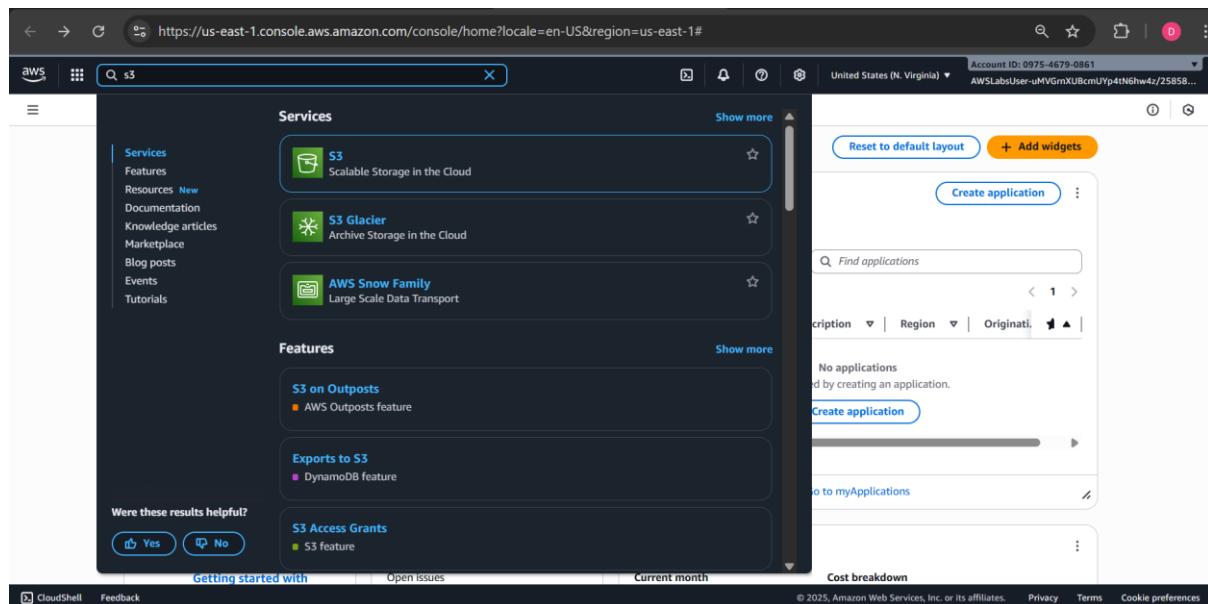
Task 1: Create a bucket

You are new to Amazon S3 and want to test the features and security of S3 as you configure the environment to hold the EC2 report data. You know that every object in Amazon S3 is stored in a bucket so creating a new bucket to hold the reports is the first thing on your task list.

In this task, you create a bucket to hold your EC2 report data and then examine the different bucket configuration options.

3. At the top-left of the AWS Management Console, on the **Services** menu choose S3.

You can also search for S3 at the top of the services menu.



4. Choose **Create bucket**

General purpose buckets (2) Info

Buckets are containers for data stored in S3.

Name	AWS Region	Creation date
awslabs-resources-krxqla59su18d-us-east-1-097546790861	US East (N. Virginia) us-east-1	October 6, 2020, 06:51:40 (UTC+05:30)
awslabs-resources-r5b3y60jjszcap-us-east-1-097546790861	US East (N. Virginia) us-east-1	October 21, 2023, 02:07:52 (UTC+05:30)

Account snapshot Info
Updated daily
[View dashboard](#)
Storage Lens provides visibility into storage usage and activity trends.

External access summary - new Info
Updated daily
External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

Caution: Bucket names must be between 3 and 63 characters long and consist of only lowercase letters, numbers, or hyphens. The bucket name must be globally unique across all of Amazon S3, regardless of account or region, and cannot be changed after the bucket is created. As you enter a bucket name, a help box displays showing any violations of the naming rules. Refer to the *Amazon S3 bucket naming rules* in the **Additional resources** section for more information.

In this lab, you will use your AWSLabUser account number in the bucket name to ensure that it is unique.

5. At the top right of the Management Console, choose the **AWSLabUser** dropdown menu.
6. Under **Account ID**, select to copy the AWSLabUser account ID to your clipboard.
7. Under the General configuration section, name your bucket: **reportbucket-<Account ID>**

Example bucket name: *reportbucket-12345678901* Replace **NUMBER** in the bucket name with a random number. This ensures that you have a unique name.

Example Bucket Name - **reportbucket-987987987987**

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 faster processing of data within a single Availability Zone.

Bucket name Info
reportbucket-097546790861

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

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.

8. In the **Object Ownership** section, configure:

- **ACLs enabled**
- **Object writer**

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.

⚠️ 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.

Object Ownership

Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

Object writer
The object writer remains the object owner.

9. Leave **Region** at its default value.

Selecting a particular region allows you to optimize latency, minimize costs, or address regulatory requirements. Objects stored in a region never leave that region unless you explicitly transfer them to another region.

10. Scroll to the bottom and choose **Create bucket**

The screenshot shows the 'Create bucket' wizard on the AWS S3 console. It includes sections for 'Default encryption' (with a note about server-side encryption being automatically applied), 'Encryption type' (radio buttons for SSE-S3, SSE-KMS, or DSSE-KMS, with SSE-S3 selected), 'Bucket Key' (radio buttons for Disable or Enable, with Enable selected), and an 'Advanced settings' link. A note at the bottom says 'After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.' At the bottom right are 'Cancel' and 'Create bucket' buttons.

Task 2: Upload an object to the bucket

Now that you have a bucket created for your report data, you are ready to work with objects. An object can be any kind of file: a text file, a photo, a video, a zip file, and so on. When you add an object to Amazon S3, you have the option of including metadata with the object and setting permissions to control access to the object.

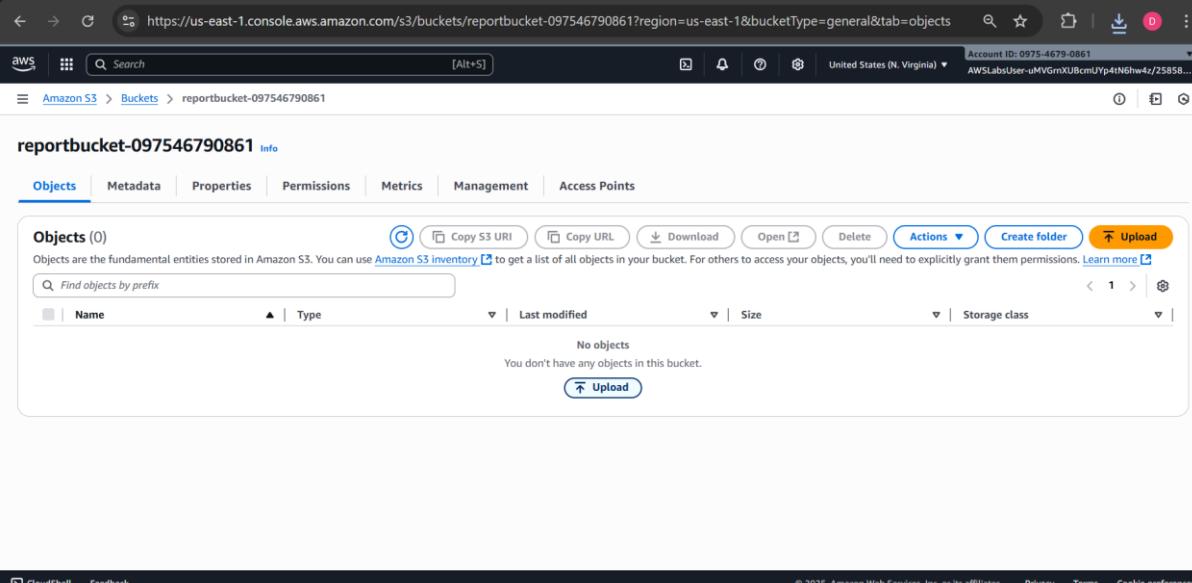
In this task you test uploading objects to your reportbucket. You have a screencapture of a daily report and want to upload this image to your S3 bucket.

11. Right-click this link [new-report.png](#), choose **Save link as**, and save the file locally.

12. In the **S3 Management Console**, find and select the bucket that starts with the name *reportbucket*.

The screenshot shows the 'Buckets' page in the AWS S3 console. A green banner at the top says 'Successfully created bucket "reportbucket-097546790861"'. Below it, the 'General purpose buckets' section lists three buckets: 'awslabs-resources-krxqqla59su18d-us-east-1-097546790861', 'awslabs-resources-r5b3y6ojjszcap-us-east-1-097546790861', and 'reportbucket-097546790861'. The last bucket is selected. To the right are sections for 'Account snapshot' (with a note about Storage Lens) and 'External access summary - new' (with a note about external access findings). At the bottom is a navigation bar with the URL 'https://us-east-1.console.aws.amazon.com/s3/buckets/reportbucket-097546790861?region=us-east-1&bucketType=general'.

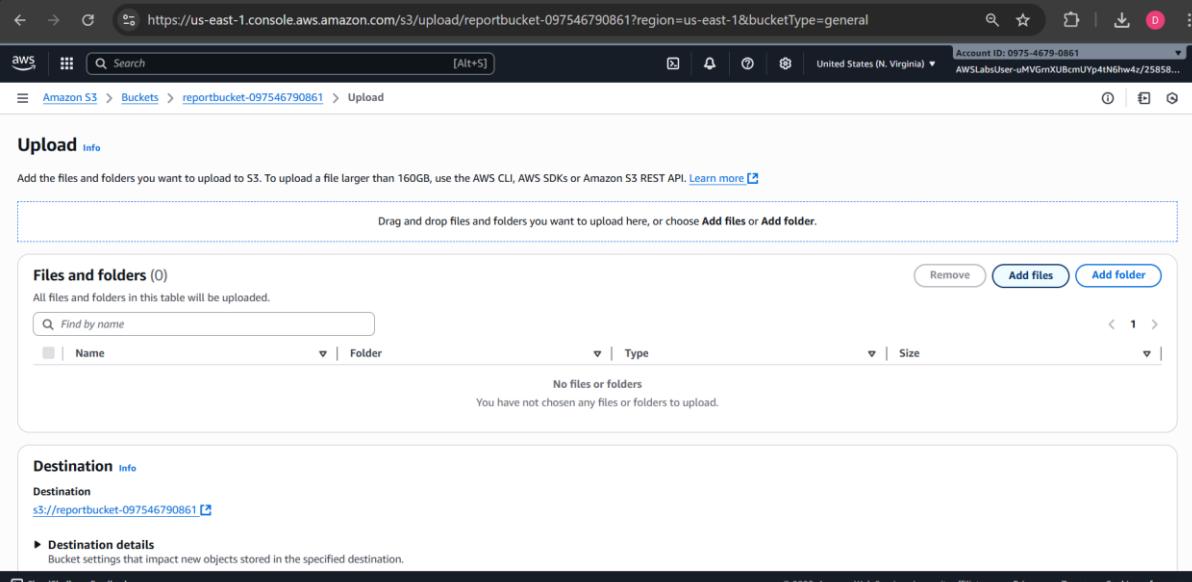
13. Choose **Upload**



The screenshot shows the AWS S3 console interface. At the top, the URL is https://us-east-1.console.aws.amazon.com/s3/buckets/reportbucket-097546790861?region=us-east-1&bucketType=general&tab=objects. The top navigation bar includes tabs for Objects, Metadata, Properties, Permissions, Metrics, Management, and Access Points. The 'Objects' tab is selected. Below the tabs, there is a search bar and a toolbar with actions like Copy S3 URI, Copy URL, Download, Open, Delete, Actions (with a dropdown arrow), Create folder, and Upload. The main content area is titled 'reportbucket-097546790861' with a blue 'info' link. It displays a message: '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.' Below this, there is a search bar labeled 'Find objects by prefix' and a table header with columns for Name, Type, Last modified, Size, and Storage class. A message 'No objects' indicates that the bucket currently contains no files. At the bottom of the table area is a large orange 'Upload' button.

This launches an upload wizard. Use this wizard to upload files either by selecting them from a file chooser or by dragging them to the S3 window.

14. Choose **Add files**



The screenshot shows the AWS S3 upload wizard. The URL is https://us-east-1.console.aws.amazon.com/s3/upload/reportbucket-097546790861?region=us-east-1&bucketType=general. The top navigation bar and tabs are identical to the previous screenshot. The main content area is titled 'Upload' with a blue 'Info' link. It contains a message: '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.' Below this is a large blue dashed rectangular area with the text 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' Underneath this area is a table titled 'Files and folders (0)' with a message 'All files and folders in this table will be uploaded.' and a search bar 'Find by name'. The table has columns for Name, Folder, Type, Size, and a 'Remove' button. A message 'No files or folders' indicates nothing has been uploaded yet. At the bottom of the table area is a large orange 'Add files' button. Below the table is a section titled 'Destination' with a blue 'Info' link. It shows the destination as 's3://reportbucket-097546790861' and a 'Destination details' section with a note about bucket settings. The bottom of the screen includes standard AWS footer links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

15. Browse to and select the **new-report.png** file that you downloaded previously.

The screenshot shows the AWS S3 console interface for uploading files to a bucket. At the top, the URL is https://us-east-1.console.aws.amazon.com/s3/upload/reportbucket-097546790861?region=us-east-1&bucketType=general. The navigation bar shows 'Amazon S3 > Buckets > reportbucket-097546790861 > Upload'. The main area is titled 'Upload' with an 'Info' link. A large text box says 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' Below it, a table lists 'Files and folders (1 total, 84.0 KB)'. The table has columns for Name, Folder, Type, and Size. One item, 'new-report.png', is listed with a size of 84.0 KB and type 'image/png'. There are 'Remove', 'Add files', and 'Add folder' buttons. A 'Destination' section shows 's3://reportbucket-097546790861' and a 'Destination details' link. The bottom of the page includes standard AWS links like CloudShell and Feedback, and a footer with copyright information.

16. Scroll down and choose **Upload**

Your file is successfully uploaded when the green bar indicating **Upload succeeded** appears.

If the file does not display in the bucket within a few seconds of uploading it, you may need to choose the refresh button at the top-right.

17. In the **Upload: status** section, choose **Close**.

The screenshot shows the AWS S3 console after the upload has completed. The URL is https://us-east-1.console.aws.amazon.com/s3/upload/reportbucket-097546790861?region=us-east-1&bucketType=general. The main area is titled 'Upload: status' with a 'Close' button. A green banner at the top says 'Upload succeeded' with a link 'For more information, see the Files and folders table.' Below it, a summary table shows 'Succeeded' (1 file, 84.0 KB, 100.00%) and 'Failed' (0 files, 0 B, 0%). The 'Files and folders' tab is selected, showing a table with one item: 'new-report.png' (image/png, 84.0 KB, Succeeded). The bottom of the page includes standard AWS links like CloudShell and Feedback, and a footer with copyright information.

Task 3: Make an object public

Security is a priority in Amazon S3. Before you configure your EC2 instance to connect to the reportbucket, you want to test the bucket and object settings for security.

In this task, you configure permissions on your bucket and your object to test accessibility.

First, you attempt to access the object to confirm that it is private by default.

18. In the reportbucket overview page, on the objects tab, locate the **new-report.png** object, and choose the **new-report.png** file name.

The new-report.png overview page opens. Notice that the navigation in the top-left updates with a link to return to the bucket overview page.

The screenshot shows the AWS S3 Object Overview page for the 'new-report.png' file. The URL in the browser is https://us-east-1.console.aws.amazon.com/s3/object/reportbucket-097546790861?region=us-east-1&bucketType=general&prefix=new-re... . The page header includes the AWS logo, search bar, and navigation links for 'Amazon S3 > Buckets > reportbucket-097546790861 > new-report.png'. The main content area has tabs for 'Properties' (selected), 'Permissions', and 'Versions'. The 'Object overview' section contains the following details:

Object overview	Properties
Owner: aws-labs-accounts+prodkiku-u1KvktTbdE7RMijhWoWe8r	S3 URI: s3://reportbucket-097546790861/new-report.png
AWS Region: US East (N. Virginia) us-east-1	Amazon Resource Name (ARN): arn:aws:s3:::reportbucket-097546790861/new-report.png
Last modified: September 14, 2025, 15:49:54 (UTC+05:30)	Entity tag (Etag): 75acf5a0dd2f6bdd67c36fa2748a1a19
Size: 84.0 KB	Object URL: https://reportbucket-097546790861.s3.us-east-1.amazonaws.com/new-report.png
Type: png	
Key: new-report.png	

At the bottom of the page, there are links for 'CloudShell', 'Feedback', and copyright information: © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences.

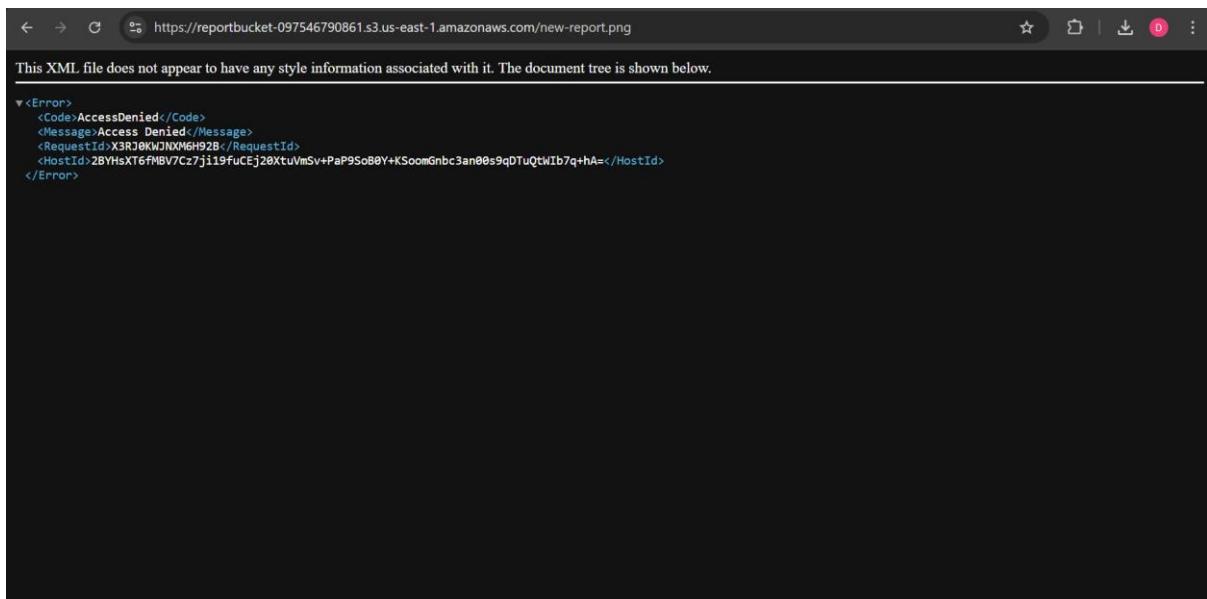
19. In the **Object overview** section, locate and copy the **Object URL** link.

The link should look similar to: <https://reportbucket987987.s3-us-west-2.amazonaws.com/new-report.png>

20. Open a new browser tab and paste the Object URL link into the address field, and then press **Enter**.

You receive an **Access Denied** error. This is because objects in Amazon S3 are private by default.

Now that you've confirmed the default security of S3 is private, you want to test how to make the object publicly accessible.



21. Keep the browser with the Access Denied error open and return to the web browser tab with the **S3 Management Console**.
22. You should still be on the **new-report.png** Object overview tab.
23. Choose the **Object actions** button and **Make public using ACL**, which will be the last item in the list.

The screenshot shows the AWS S3 Object Overview page for the file 'new-report.png'. The object details include:

- Properties:** Owner: aws-labs-accounts+prodkiku-u1KvktTbdE7RMjhWoWe8r, AWS Region: US East (N. Virginia) us-east-1, Last modified: September 14, 2025, 15:49:54 (UTC+05:30), Size: 84.0 KB, Type: png, Key: new-report.png.
- Object URI:** s3://reportbucket-097546790861/new-report.png
- Amazon Resource Name (ARN):** arn:aws:s3:::reportbucket-097546790861/new-report.png
- Entity tag (Etag):** 7Sacf5a0dd2f6bdd67c36fa2748a1a19
- Object URL:** https://reportbucket-097546790861.s3.us-east-1.amazonaws.com/new-report.png

The 'Object actions' dropdown menu is open, listing various actions such as Copy, Move, Initiate restore, Query with S3 Select, Edit actions, Rename object, Edit storage class, Edit server-side encryption, Edit metadata, Edit tags, and Make public using ACL. The 'Make public using ACL' option is highlighted.

Make public Info

The make public action enables public read access in the object access control list (ACL) settings. [Learn more](#)

ⓘ 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](#)

⚠ When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.

Specified objects

Name	Type	Last modified	Size
new-report.png	png	September 14, 2025, 15:49:54 (UTC+05:30)	84.0 KB

[Cancel](#) [Make public](#)

Notice the warning **Public access is blocked because Block Public Access settings are turned on for this bucket**. This error displays because this bucket is configured not to allow public access. The bucket settings override any permissions applied to individual objects. If you want the object to viewable by the general public, you need to turn off Block Public Access (BPA).

24. Choose **Make public** and read the warning at the top of the window indicating that it “Failed to edit public access” again this is due to BPA being enabled.

Failed to edit public access
For more information, see the Error column in the Failed to edit table below.

Make public: status

ⓘ 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](#)

ⓘ After you navigate away from this page, the following information is no longer available.

Summary

Source	Successfully edited public access	Failed to edit public access
s3://reportbucket-097546790861	0 objects	1 object, 84.0 KB

[Close](#)

Failed to edit public access [Configuration](#)

Failed to edit public access (1 object, 84.0 KB)

Name	Folder	Type	Last modified	Size	Error
new-report.png		png	September 14, 2025, 15:49:54 (UTC+05:30)	84.0 KB	

25. Choose **Close** to return to the object overview.
26. Use the navigation at the top to go back to the main reportbucket overview page.
27. Choose the **Permissions** tab.

The screenshot shows the AWS S3 Bucket Permissions overview page. At the top, there are tabs for Objects, Metadata, Properties, **Permissions**, Metrics, Management, and Access Points. The Permissions tab is selected. Below the tabs, there's a section titled "Permissions overview" with a sub-section "Access finding". It says "Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#)". There's also a link to "View analyzer for us-east-1". The main content area has a section titled "Block public access (bucket settings)". It shows that "Block all public access" is turned "On". There's a link to "Individual Block Public Access settings for this bucket". Below this, there's a "Bucket policy" section with "Edit" and "Delete" buttons. At the bottom, there are links for CloudShell and Feedback, and standard footer links for Privacy, Terms, and Cookie preferences.

24. Under **Block public access (bucket settings)**, choose **Edit** to change the settings.

The screenshot shows the "Edit Block public access (bucket settings)" configuration page. At the top, it says "Edit Block public access (bucket settings) [Info](#)". Below that is a section titled "Block public access (bucket settings)" with a detailed description of what it does. There are several checkboxes for different settings: "Block all public access" (which is checked), "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.

25. Deselect the **Block all public access** option, and then leave all other options deselected.

The screenshot shows the 'Edit Block public access (bucket settings)' page. The 'Block all public access' checkbox is unchecked. Below it, several other checkboxes for different access control mechanisms are also unchecked. At the bottom right, there are 'Cancel' and 'Save changes' buttons.

Notice that all of the individual options remain deselected. When deselecting all public access, you must then select the individual options that apply to your situation and security objectives. Both ACLs and bucket policies are used later in the lab, so they all remain deselected in this task. In a production environment, it is recommended to use the least permissive settings possible. Refer to the Amazon S3 block public access link in the *Additional Resources* section at the end of the lab for more information.

30. Choose **Save changes**

31. A dialogue box opens asking you to confirm your changes. Type confirm in the field, and then choose **Confirm**

The screenshot shows a confirmation dialog box titled 'Edit Block public access (bucket settings)'. It contains a message: 'Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.' Below this is a text input field with the word 'confirm' typed into it. At the bottom of the dialog are 'Cancel' and 'Confirm' buttons. The background shows the 'Edit Block public access (bucket settings)' page with the 'Block all public access' checkbox still unchecked.

A **Successfully edited bucket settings for Block Public Access** message displays at the top of the window.

The screenshot shows the 'Permissions' tab of the AWS S3 bucket configuration. A green success message at the top states: 'Successfully edited Block Public Access settings for this bucket.' Below it, the 'Block public access (bucket settings)' section is visible, showing that 'Block all public access' is currently off. The 'Edit' button is highlighted. The 'Bucket policy' section is also partially visible.

32. Choose the Objects tab.

The screenshot shows the 'Objects' tab of the AWS S3 bucket. It lists a single object named 'new-report.png' with a size of 84.0 KB and a storage class of Standard. The object was last modified on September 14, 2025, at 15:49:54 (UTC+05:30). The 'Actions' dropdown menu is open, showing options like Copy S3 URI, Copy URL, Download, Open, Delete, Create folder, and Upload.

33. Choose the new-report.png file name.

The screenshot shows the properties of the 'new-report.png' object. The 'Properties' tab is selected. Key details include:

- Object overview**: Owner is 'aws-labs-accounts-prodkiu-u1KvtTbdE7RMijhWoWe8r', AWS Region is 'US East (N. Virginia) us-east-1', Last modified is 'September 14, 2025, 15:49:54 (UTC+05:30)', Size is '84.0 KB', Type is 'png', and Key is 'new-report.png'.
- S3 URI**: <https://reportbucket-097546790861.s3.us-east-1.amazonaws.com/new-report.png>
- Amazon Resource Name (ARN)**: [arn:aws:s3::reportbucket-097546790861/new-report.png](#)
- Entity tag (Etag)**: [75acf5a0dd2f6bdd67c36fa2748a1a19](#)
- Object URL**: <https://reportbucket-097546790861.s3.us-east-1.amazonaws.com/new-report.png>

34. On the new-report.png overview page, choose the **Object actions** button and select **Make public using ACL**.

The screenshot shows the AWS S3 console interface. A file named 'new-report.png' is selected. The 'Object overview' section displays details such as Owner, AWS Region, Last modified, Size, Type, and Key. The 'Object actions' dropdown menu is open, listing options like Copy, Move, Initiate restore, Query with S3 Select, Edit actions, Rename object, Edit storage class, Edit server-side encryption, Edit metadata, Edit tags, and 'Make public using ACL'. The 'Make public using ACL' option is highlighted.

Notice the warning: **When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.** This is designed to remind you that if you make the object public then everyone in the world will be able to read the object.

The screenshot shows the 'Make public' dialog box. It contains a warning message: '⚠ When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.' Below this, a table lists the 'Specified objects' with one item: 'new-report.png'. The table includes columns for Name, Type, Last modified, and Size. At the bottom right of the dialog are 'Cancel' and 'Make public' buttons.

35. Choose **Make public** and you should see the green banner **Successfully edited public access** at the top of the window.

The screenshot shows the AWS S3 Management Console interface. At the top, there is a green banner with the text "Successfully edited public access" and "View details below." Below the banner, the title "Make public: status" is displayed. A message states: "After you navigate away from this page, the following information is no longer available." Under the "Summary" section, it shows "Source: s3://reportbucket-097546790861" and two status boxes: "Successfully edited public access" (1 object, 84.0 KB) and "Failed to edit public access" (0 objects). Below this, there are tabs for "Failed to edit public access" (selected) and "Configuration". Under "Failed to edit public access", there is a table header with columns: Name, Type, Last modified, Size, and Error. The table body is empty, showing "No objects failed to edit". At the bottom of the page, there are links for CloudShell, Feedback, and copyright information: "© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".

35. Choose **Close** to return to the object overview.

37. Return to the other browser tab that displayed **Access Denied** for the new-report.png and refresh the page.

The screenshot shows a Microsoft Excel spreadsheet titled "sample-report". The data is presented in a table with the following columns: Service, Operation, UsageType, Resource, StartTime, EndTime, and UsageValue. The data rows are as follows:

	A	B	C	D	E	F	G
1	Service	Operation	UsageType	Resource	StartTime	EndTime	UsageValue
2	AmazonS3	HeadBucket	USW2-C3DataTransfer-Out-Bytes	lab-test-bucket-77	10/31/2020 0:00	12/31/2020 11:59	15309
3	AmazonS3	PutObject	USW2-C3DataTransfer-In-Bytes	admin-test-77	10/31/2020 0:00	12/31/2020 11:59	19032
4	AmazonS3	HeadBucket	USW2-Requests-Tier2	admin-test-77	10/31/2020 0:00	12/31/2020 11:59	128
5	AmazonS3	PutObjectForReplication	USV1-Request-SIA-Tier1	mybucket-98765	10/31/2020 0:00	12/31/2020 11:59	56888
6	AmazonS3	GetObjectFor Replication	USV1-USW2-AWS-In-Bytes	mybucket-98766	10/31/2020 0:00	12/31/2020 11:59	254587
7	AmazonS3	GetObjectFor Replication	USW2-C3DataTransfer-Out-Bytes	mybucket-98767	10/31/2020 0:00	12/31/2020 11:59	235
8	AmazonS3	HeadBucket	USW2-C3DataTransfer-In-Bytes	mybucket-98768	10/31/2020 0:00	12/31/2020 11:59	25589
9	AmazonS3	PutObject	USW2-Requests-Tier2	mybucket-98769	10/31/2020 0:00	12/31/2020 11:59	2348
10	AmazonS3	PutObjectForReplication	USV1-Request-SIA-Tier1	mybucket-98770	10/31/2020 0:00	12/31/2020 11:59	15309
11	AmazonS3	GetObjectFor Replication	USV1-USW2-AWS-In-Bytes	mybucket-98771	10/31/2020 0:00	12/31/2020 11:59	19032
12	AmazonS3	GetObjectFor Replication	USW2-C3DataTransfer-Out-Bytes	lab-example-bucket	10/31/2020 0:00	12/31/2020 11:59	128
13	AmazonS3	HeadBucket	USW2-C3DataTransfer-In-Bytes	lab-example-bucket	10/31/2020 0:00	12/31/2020 11:59	56888
14	AmazonS3	PutObject	USW2-Requests-Tier2	lab-example-bucket	10/31/2020 0:00	12/31/2020 11:59	254587
15	AmazonS3	PutObjectForReplication	USV1-Request-SIA-Tier1	lab-example-bucket	10/31/2020 0:00	12/31/2020 11:59	235
16	AmazonS3	GetObjectFor Replication	USV1-USW2-AWS-In-Bytes	lab-example-bucket	10/31/2020 0:00	12/31/2020 11:59	25589
17							
18							

The new-report.png now displays properly because it is publicly accessible.

38. Close the web browser tab that displays your new-report.png image and return to the tab with the Amazon S3 Management Console.

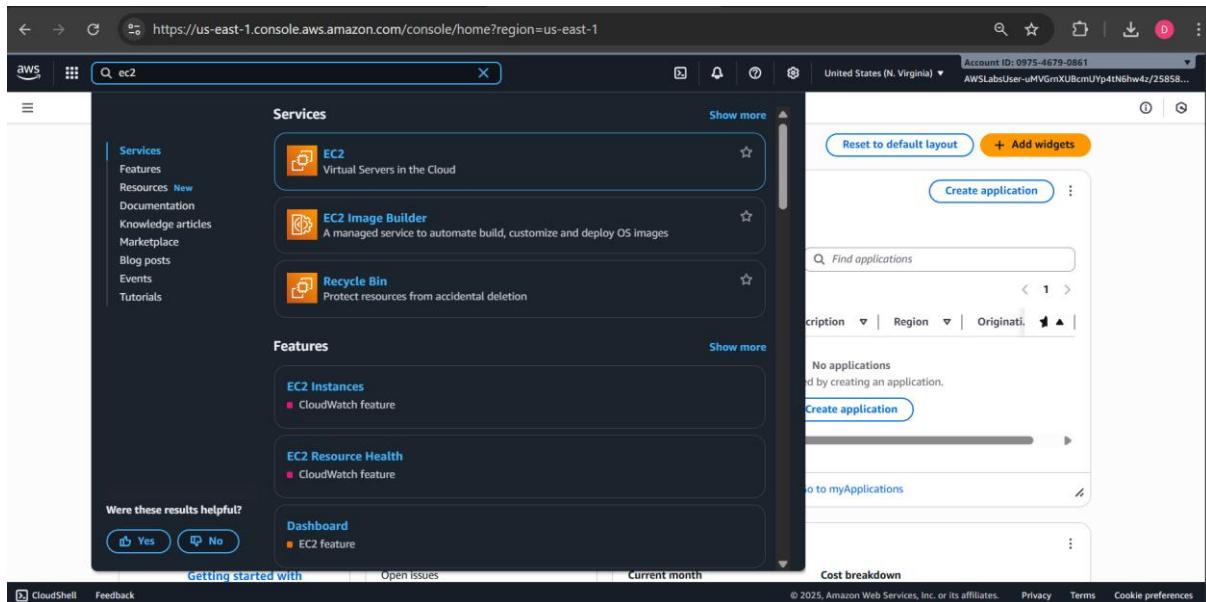
In this example, you granted read access to just one specific object. If you wish to grant access to the entire bucket, you need to use a bucket policy, which is covered later in this lab.

In the next task, you work with your EC2 instance to confirm connectivity to the S3 bucket.

In this task, you connect to your Amazon Elastic Compute Cloud (Amazon EC2) instance to test connectivity and security to the S3 reportbucket.

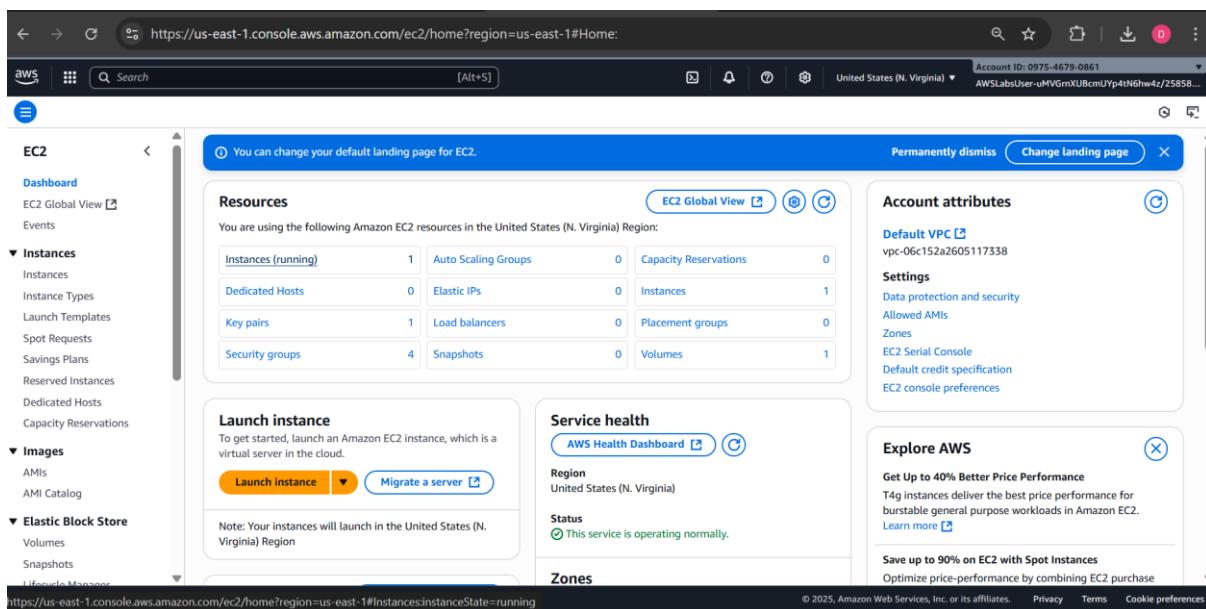
You should already be logged into the AWS Management Console. If not, follow the steps in the Start Lab section to log in to the AWS Management Console.

39. On the **Services** menu, choose **EC2**.



The screenshot shows the AWS Management Console Services menu. The EC2 service is selected and highlighted with a blue border. Other options like EC2 Image Builder and Recycle Bin are also listed. To the right, there's a preview window for the EC2 service showing a 'Create application' button and a search bar for 'Find applications'. The URL in the browser is https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1.

40. On the **EC2 Dashboard**, under the **Resources** section, choose **Instances (running)**.



The screenshot shows the EC2 Dashboard. Under the 'Resources' section, 'Instances (running)' is selected, showing 1 instance. Other resources listed include Auto Scaling Groups (0), Capacity Reservations (0), Dedicated Hosts (0), Elastic IPs (0), Instances (1), Key pairs (1), Load balancers (0), Placement groups (0), Security groups (4), Snapshots (0), and Volumes (1). To the right, there are sections for 'Account attributes' (Default VPC, Settings, Explore AWS), 'Service health' (AWS Health Dashboard, Region: United States (N. Virginia), Status: This service is operating normally), and 'Zones' (Regions: United States (N. Virginia)). The URL in the browser is https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#InstancesInstanceState=running.

41. Select **Bastion Host** and choose **Connect**

The screenshot shows the AWS EC2 Instances page. On the left sidebar, under the 'Instances' section, there is a single item labeled 'Bastion Host'. The main content area displays the details for this instance, including its ID (i-08db8e47b878b8dab), state (Running), type (t5.micro), and various status metrics. A 'Connect' button is visible at the top right of the instance card.

42. In the **Connect to instance** window:

- For Connection method, select **Session Manager**.

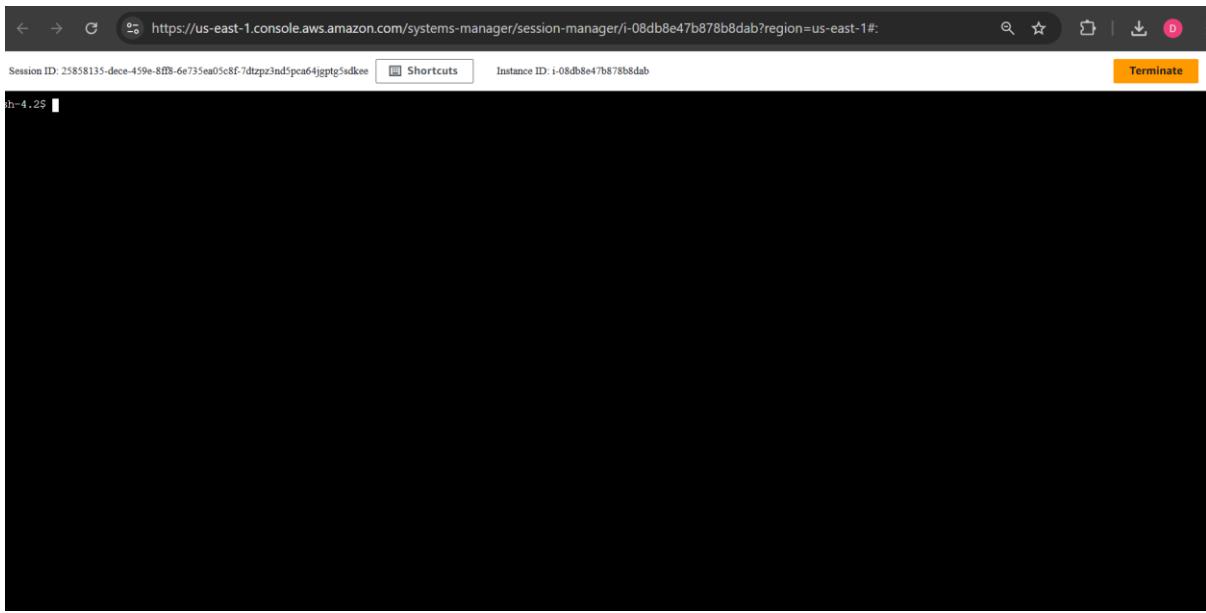
Session Manager enables you to connect to the bastion host instance without the need for specific ports to be open on your firewall or Amazon Virtual Private Cloud (Amazon VPC) security group. Refer to *AWS Systems Manager Session Manager* in the *Additional resources* section at the end of this lab for more information.

The screenshot shows the 'Connect to instance' window for the Bastion Host instance. The 'Session Manager' tab is selected. A message at the top encourages users to move towards zero standing privileges by requiring operators to request access before connecting to instances. Below this, a section titled 'Session Manager usage:' provides instructions on how to use Session Manager. At the bottom right, there are 'Cancel' and 'Connect' buttons.

43. Choose **Connect**

A new browser tab or window opens with a connection to the bastion host instance.

You are now connected to the EC2 instance that holds the reporting application. Because Session Manager uses https port 443, it does not require you to open SSH port 22 to the outside world, you are satisfied with this security feature. Now you want to see how EC2 interacts with your S3 bucket.



44. In the bastion host session, enter the following command to change to home directory (/home/ssm-user):

```
cd ~
```

The output returns you to the command prompt.

45. Enter the following command to verify you are in the home directory:

```
pwd
```

The output should be:

```
/home/ssm-user
```

You are now in the ssm-user's home directory where you will run all of the commands in this lab.

46. Enter the following command to list all of your S3 buckets.

```
aws s3 ls
```

The output should look similar to this:

```
2020-11-11 22:27:28 ql-cf-templates-1603924046-5d95cf473a39fe4e-us-west-2
```

```
2020-11-11 22:27:49 qltrail-lab-59350-1603924067
```

```
2020-11-11 22:34:46 reportbucket987987
```

You see the reportbucket you created as well as lab auto-generated buckets.

Note: During the creating of the lab environment, both an Instance Profile (which defines who you are for authentication) and a Role (which defines what you can do after you authenticate), have been automatically added for the EC2 instance to allow the EC2 instance to list the S3 buckets and objects.

47. Enter the following command to list all objects in your reportbucket. Remember to change the number at the end of the reportbucket name, to match the name of the bucket you created.

```
aws s3 ls s3://reportbucket(NUMBER)
```

The command looks similar to this: **aws s3 ls s3://reportbucket987987**

The output should look like this:

```
2020-11-11 15:46:34    86065 new-report.png
```

There is currently just one object in your bucket called new-report.png.

48. Type the following to change directories into the reports directory.

```
cd reports
```

The output returns you to the command prompt.

49. Type the following to list the contents of the directory.

```
ls
```

The output shows some files created in your reports directory to test the application.

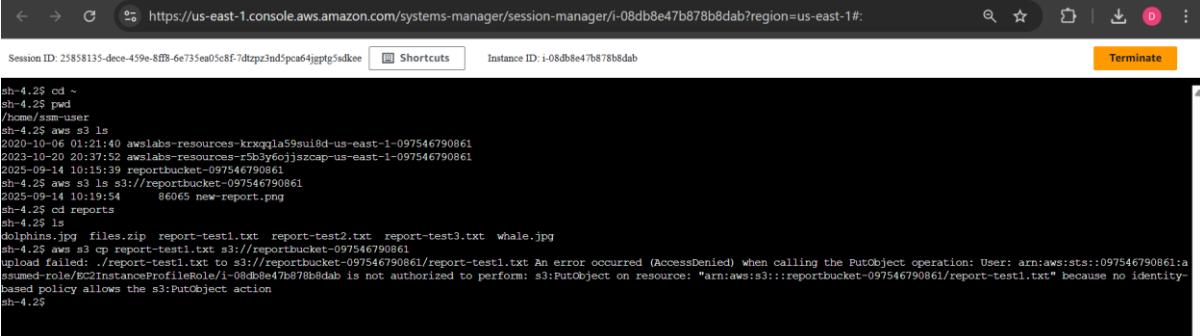
```
dolphins.jpg files.zip report-test.txt report-test1.txt report-test2.txt report-test3.txt whale.jpg
```

50. Type the following to see if you can copy a file to the S3 bucket.

```
aws s3 cp report-test1.txt s3://reportbucket(NUMBER)
```

The command looks similar to this: **aws s3 cp report-test1.txt s3://reportbucket987987**

The output indicates an error **upload failed**. This is because we have read-only rights to the bucket and do not have the permissions to perform the PutObject operation.



A screenshot of a web browser window showing an AWS Systems Manager session terminal. The URL is https://us-east-1.console.aws.amazon.com/systems-manager/session-manager/i-08db8e47b878b8dab?region=us-east-1#. The terminal session ID is i-08db8e47b878b8dab. The terminal window shows a command-line interface with the following history:

```
sh-4.2$ cd ~  
sh-4.2$ pwd  
/home/ssm-user  
sh-4.2$ aws s3 ls  
2020-10-06 01:21:40 awslogs-resources-krxqqla59sui8d-us-east-1-097546790861  
2023-10-20 20:37:52 awslogs-resources-r53y6ojjszcap-us-east-1-097546790861  
2025-09-14 10:15:39 reportbucket-097546790861  
sh-4.2$ aws s3 ls s3://reportbucket-097546790861  
2025-09-14 10:19:54    86065 new-report.png  
sh-4.2$ cd reports  
sh-4.2$ ls  
dolphins.jpg files.zip report-test1.txt report-test2.txt report-test3.txt whale.jpg  
sh-4.2$ aws s3 cp report-test1.txt s3://reportbucket-097546790861  
upload failed: /report-test1.txt to s3://reportbucket-097546790861/report-test1.txt An error occurred (AccessDenied) when calling the PutObject operation: User: arn:aws:sts::097546790861:assumed-role/EC2InstanceProfileRole/-08db8e47b878b8dab is not authorized to perform: s3:PutObject on resource: "arn:aws:s3:::reportbucket-097546790861/report-test1.txt" because no identity-based policy allows the s3:PutObject action.  
sh-4.2$
```

51. Leave this window open and go back to the AWS Console tab.

In the next task you create a bucket policy to add the PutOperation.

Task 5: Create a bucket policy

A bucket policy is a set of permissions associated with an S3 bucket. It is used to control access to an entire bucket or to specific directories within a bucket.

In this task, you use the AWS Policy Generator to create a bucket policy to enable read and write access from the EC2 instance to the bucket to ensure your reporting application can successfully write to S3.

52. Right-click this link [sample-file.txt](#), choose **Save link as**, and save the file locally.

53. Return to the AWS Management Console, go to the **Services** menu and select **S3**.

54. In the **S3 Management Console** tab, select the name of your bucket.

The screenshot shows the AWS S3 Management Console interface. On the left, there's a sidebar with navigation links like 'General purpose buckets', 'Directory buckets', 'Table buckets', etc. The main area is titled 'General purpose buckets' and shows a list of three buckets:

Name	AWS Region	Creation date
awslabs-resources-krrqqja59ui8d-us-east-1-097546790861	US East (N. Virginia) us-east-1	October 6, 2020, 06:51:40 (UTC+05:30)
awslabs-resources-r5b3y6ojjszcap-us-east-1-097546790861	US East (N. Virginia) us-east-1	October 21, 2023, 02:07:52 (UTC+05:30)
reportbucket-097546790861	US East (N. Virginia) us-east-1	September 14, 2025, 15:45:39 (UTC+05:30)

On the right, there are two informational boxes: 'Account snapshot' and 'External access summary - new'. The bottom of the screen includes standard AWS footer links like CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

The screenshot shows the AWS S3 console interface. The URL in the address bar is <https://us-east-1.console.aws.amazon.com/s3/buckets/reportbucket-097546790861?region=us-east-1&tab=objects&bucketType=general>. The page title is "reportbucket-097546790861 Info". On the left sidebar, under "General purpose buckets", there are links for Directory buckets, Table buckets, Vector buckets, Access Grants, Access Points (General Purpose Buckets, Fsx file systems), Access Points (Directory Buckets), Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and IAM Access Analyzer for S3. Below this, there is a link to "Block Public Access settings for this account". Under "Storage Lens", there are links for Dashboards, Storage Lens groups, and AWS Organizations settings. At the bottom of the sidebar, there are "CloudShell" and "Feedback" buttons. The main content area shows the "Objects" tab selected. There is one object listed: "new-report.png" (Type: png, Last modified: September 14, 2025, 15:49:54 (UTC+05:30), Size: 84.0 KB, Storage class: Standard). There are buttons for Actions (with a dropdown arrow), Create folder, and Upload.

55. Choose **Upload** and use the same upload process as in the previous task to upload the **sample-file.txt**.

The screenshot shows the AWS S3 console interface, identical to the previous one but with two objects now listed in the "Objects" table. The URL in the address bar is <https://us-east-1.console.aws.amazon.com/s3/buckets/reportbucket-097546790861?region=us-east-1&tab=objects&bucketType=general>. The page title is "reportbucket-097546790861 Info". The main content area shows the "Objects" tab selected. There are two objects listed: "new-report.png" (Type: png, Last modified: September 14, 2025, 15:49:54 (UTC+05:30), Size: 84.0 KB, Storage class: Standard) and "sample-file.txt" (Type: txt, Last modified: September 14, 2025, 16:35:32 (UTC+05:30), Size: 113.0 B, Storage class: Standard). There are buttons for Actions (with a dropdown arrow), Create folder, and Upload.

56. Choose the **sample-file.txt** file name. The sample-file.txt overview page opens.

The screenshot shows the AWS S3 Object Overview page for the file 'sample-file.txt'. The left sidebar has tabs for 'Properties', 'Permissions', and 'Versions', with 'Properties' selected. The main area is titled 'Object overview' and contains the following details:

Owner	aws-labs-accounts+prodkiku-u1KvktTbdE7RMijhWoWe8r
AWS Region	US East (N. Virginia) us-east-1
Last modified	September 14, 2025, 16:35:32 (UTC+05:30)
Size	113.0 B
Type	txt
Key	sample-file.txt

On the right side, there are links for 'S3 URI' (s3://reportbucket-097546790861/sample-file.txt), 'Amazon Resource Name (ARN)' (arn:aws:s3:::reportbucket-097546790861/sample-file.txt), 'Entity tag (etag)' (4a0b2a536384728d06b8a9c5ceae0581), and 'Object URL' (<https://reportbucket-097546790861.s3.us-east-1.amazonaws.com/sample-file.txt>). At the bottom of the page, there are links for 'CloudShell', 'Feedback', and copyright information: '© 2025, Amazon Web Services, Inc. or its affiliates.' and 'Cookie preferences'.

57. Under the Object overview section, locate and copy the **Object URL** link.

58. In a new browser tab, paste the link into the address field, and then press **Enter**.

Once again, **Access Denied** will be displayed. You need to configure a bucket policy to grant access to *all* objects in the bucket without having to specify permissions on each object individually.

59. Keep this browser tab open, but return to the tab with the **S3 Management Console**.

60. Go to **Services > IAM > Roles**.

The screenshot shows the AWS IAM Roles list. The left sidebar has sections for 'Identity and Access Management (IAM)', 'Access management', 'Access reports', and 'CloudWatch Metrics Insights'. The 'Roles' section is expanded, showing a list of 26 roles. The columns in the list are 'Role name', 'Trusted entities', and 'Last activity'. The roles listed include:

Role name	Trusted entities	Last activity
aws-codedstar-service-role	AWS Service: codestar	-
aws-opsworks-cm-service-role	AWS Service: opsworks-cm	-
aws-opsworks-ec2-role	AWS Service: ec2	-
AWSCloudFormationStackSetExecutionRole	Account: 180005829642	-
AWSLabs-LabFunction-LabAdmin-v1-BeuZgQuaVhM	AWS Service: lambda	-
AWSLabs-LabFunction-LabAdmin-v2-BqztPLLHXkv	AWS Service: lambda	-
AWSLabs-LabFunction-ReadOnly-v1-iFlpBUZaZF	AWS Service: lambda	-
AWSLabs-LabFunction-ReadOnly-v2-mADAxixmnT	AWS Service: lambda	-
AWSLabs-Provisioner-v1-DwAEawsNCww	Account: 684652433853	-
AWSLabs-Provisioner-v2-CJDTNhCaQDT	Account: 684652433853	-
AWSLabs-Reaper-v1-BggBBwvMBCww	Account: 230749523606, and 1 more	-
AWSLabs-Report-Processor-v1-DhoSE-0Tdu	AWS Service: globalprod-reporterbu	-

At the bottom of the page, there are links for 'CloudShell', 'Feedback', and copyright information: '© 2025, Amazon Web Services, Inc. or its affiliates.' and 'Cookie preferences'.

61. In the Search field type **EC2InstanceProfileRole** This is the Role that the EC2 instance uses to connect to S3.

The screenshot shows the AWS IAM Roles page with a search bar at the top containing "EC2InstanceProfileRole". Below the search bar, there is a table with one result: "EC2InstanceProfileRole". The table has columns for "Role name", "Trusted entities", and "Last activity". The "Role name" column shows "EC2InstanceProfileRole", the "Trusted entities" column shows "AWS Service: ec2", and the "Last activity" column shows "10 minutes ago". There are "Delete" and "Create role" buttons at the top right of the table.

62. Select **EC2InstanceProfileRole**. On the Summary page, copy the **Role ARN** to a text file to be used in a later step.

It should look similar to this: **arn:aws:iam::596123517671:role/EC2InstanceProfileRole**

The screenshot shows the AWS IAM Role details page for "EC2InstanceProfileRole". The "Summary" section includes fields for "Creation date" (September 14, 2025, 13:59 (UTC+05:30)), "Last activity" (4 minutes ago), "Maximum session duration" (1 hour), and "Instance profile ARN" (arn:aws:iam::097546790861:instance-profile/EC2InstanceProfile). A green message bubble says "ARN copied". The "Permissions" tab is selected, showing "Permissions policies (3)". The table lists three policies: "AmazonSSMManagedInstanceCore" (AWS managed, 1 attached entity) and "ReadOnlyAccess" (AWS managed - job function, 5 attached entities). There are "Simulate", "Remove", and "Add permissions" buttons at the top of the permissions table.

63. Choose Services , S3 and return to the S3 Management Console.

The screenshot shows the AWS S3 Management Console. On the left, there's a sidebar with options like General purpose buckets, Directory buckets, Table buckets, Vector buckets, Access Grants, Access Points (General Purpose Buckets, FSx file systems), Access Points (Directory Buckets), Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, and Block Public Access settings for this account. Below that is a Storage Lens section with Dashboards, Storage Lens groups, and AWS Organizations settings. The main area is titled "General purpose buckets (3) Info". It has buttons for Copy ARN, Empty, Delete, and Create bucket. A note says "Buckets are containers for data stored in S3." Below is a table with columns Name, AWS Region, and Creation date. Three buckets are listed:

Name	AWS Region	Creation date
awslabs-resources-097546790861	US East (N. Virginia) us-east-1	October 6, 2020, 06:51:40 (UTC+05:30)
awslabs-resources-r5b3y6ojiszcap-us-east-1-097546790861	US East (N. Virginia) us-east-1	October 21, 2023, 02:07:52 (UTC+05:30)
reportbucket-097546790861	US East (N. Virginia) us-east-1	September 14, 2025, 15:45:39 (UTC+05:30)

On the right, there are two boxes: "Account snapshot" (updated daily) and "External access summary - new" (updated daily). The "Account snapshot" box says "Storage Lens provides visibility into storage usage and activity trends." The "External access summary" box says "External access findings help you identify bucket permissions that allow public access or access from other AWS accounts."

64. Choose the reportbucket.

You should see the two objects you uploaded. If not, navigate back to your bucket so that you see the list of objects you have uploaded.

The screenshot shows the AWS S3 Management Console with the path "Amazon S3 > Buckets > reportbucket-097546790861". The sidebar is identical to the previous screenshot. The main area is titled "reportbucket-097546790861 Info". It has tabs for Objects, Metadata, Properties, Permissions, Metrics, Management, and Access Points. The "Objects" tab is selected. It shows a table with two objects:

Name	Type	Last modified	Size	Storage class
new-report.png	png	September 14, 2025, 15:49:54 (UTC+05:30)	84.0 KB	Standard
sample-file.txt	txt	September 14, 2025, 16:35:32 (UTC+05:30)	113.0 B	Standard

65. Choose the Permissions tab.

The screenshot shows the AWS S3 console with the URL <https://us-east-1.console.aws.amazon.com/s3/buckets/reportbucket-097546790861?region=us-east-1&tab=permissions&bucketType=gen...>. The 'Permissions' tab is active. On the left sidebar, under 'Amazon S3', there's a 'General purpose buckets' section with various options like Directory buckets, Table buckets, Vector buckets, Access Grants, Access Points (General Purpose Buckets, FSx file systems), Access Points (Directory Buckets), Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and IAM Access Analyzer for S3. Below that is a 'Block Public Access settings for this account' section. Under 'Storage Lens', there are Dashboards, Storage Lens groups, and AWS Organizations settings. At the bottom of the sidebar are CloudShell and Feedback links. The main content area has tabs for Objects, Metadata, Properties, Permissions (which is selected), Metrics, Management, and Access Points. The 'Permissions' section contains a 'Permissions overview' box with 'Access finding' information and a 'View analyzer for us-east-1' link. Below that is a 'Block public access (bucket settings)' box with a note about public access being granted through ACLs, bucket policies, and access point policies. It shows 'Block all public access' is off and has a link to 'Individual Block Public Access settings for this bucket'. The 'Bucket policy' section shows 'No policy to display.' with 'Edit' and 'Delete' buttons. At the bottom right of the main content area are links for 'Edit', 'Delete', 'Copy', and 'CloudShell'. The footer includes copyright information and links for Privacy, Terms, and Cookie preferences.

66. In the **Permissions** tab, scroll to the Bucket Policy section, choose **Edit**

A blank **Bucket policy editor** is displayed. Bucket policies can be created manually, or they can be created with the assistance of the **AWS Policy generator**.

The screenshot shows the 'Edit bucket policy' page with the URL <https://us-east-1.console.aws.amazon.com/s3/bucket/reportbucket-097546790861/property/policy/edit?region=us-east-1&bucketType=gen...>. The left sidebar is identical to the previous screenshot. The main content area has a title 'Edit bucket policy' with an 'Info' link. Below it is a 'Bucket policy' section with a note about the policy being written in JSON and applying to objects in the bucket. A 'Bucket ARN' field contains 'arn:aws:s3:::reportbucket-097546790861'. The 'Policy' section shows a single statement labeled '1'. To the right, there are buttons for 'Policy examples' and 'Policy generator'. A 'Select a statement' section with a note to add a new statement is also visible. At the bottom right of the main content area are links for 'Edit statement', 'Select a statement', and '+ Add new statement'. The footer includes copyright information and links for Privacy, Terms, and Cookie preferences.

Amazon Resource Names (ARN)s uniquely identify AWS resources across all of AWS. Each section of the ARN is separated by a ":" and represents a specific piece of the path to the specified resource. The sections can vary slightly depending on the service being referenced, but generally follows this format:

`arn:partition:service:region:account-id:resource`

Amazon S3 does not require region or account-id parameters in ARNs, so those sections are left blank. However, the ":" to separate the sections is still used, so it looks similar to `arn:aws:s3:::reportbucket987987`

Refer to the Amazon Resource Names (ARNs) and AWS Service Namespaces documentation link in the *Additional Resources* section at the end of the lab for more information.

67. Copy the Bucket ARN to a text file to be used in a later step.

It is displayed below the **Policy examples** and **Policy generator** buttons.

It looks like this:

Bucket ARN

arn:aws:s3:::reportbucket987987

68. Choose **Policy generator**

A new web browser tab will open with the AWS Policy Generator.

AWS policies use the JSON format, and are used to configure granular permissions for AWS services. While you can write the policy in JSON manually, the AWS Policy Generator allows you to create it using a friendly web interface.

In the AWS Policy Generator window:

- For **Select Type of Policy**, select **S3 Bucket Policy**.
- For **Effect**, select **Allow**.
- For **Principal**, paste the **EC2InstanceProfileRole ARN** that you copied to a text file in a previous step.
- For **AWS Service**, keep the default setting of **Amazon S3**.
- For **Actions**, select **PutObject** and **GetObject**

The get *GetObject* action grants permission for objects to be retrieved from Amazon S3. Refer to the Additional Resources section at the end of the lab for links to more information about the actions available for use in Amazon S3 policies.

- **Amazon Resource Name (ARN):** Paste the Bucket ARN that you previously copied.
- At the end of the ARN, append /*

The ARN should look similar to: **arn:aws:s3:::reportbucket987987/***

An Amazon Resource Name (ARN) is a standard way to refer to resources within AWS. In this case, the ARN is referring to your S3 bucket. Adding /* to the end of the bucket name allows the policy to apply to all objects *within* the bucket.

Step 1: Select policy type
A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Type of Policy
 S3 Bucket Policy

Step 2: Add statement(s)
A statement is the formal description of a single permission. See [a description of elements](#) that you can use in statements.

Effect
 Allow
 Deny

Principal

Use a comma to separate multiple values.

Actions
 All Actions ("*")
--Select Actions--

Actions
 All Actions ("*")
--Select Actions--

Amazon Resource Name (ARN)
 All Resources ("*")

ARN should follow the following format: arn:aws:s3:::\${BucketName}/\${KeyName}. Use a comma to separate multiple values.

► Add conditions (optional)

Add Statement

69. Choose **Add Statement**. The details of the statement you configured are added to a table below the button. You can add multiple statements to a policy.

Actions
 All Actions ("*")
--Select Actions--

Amazon Resource Name (ARN)
 All Resources ("*")

ARN should follow the following format: arn:aws:s3:::\${BucketName}/\${KeyName}. Use a comma to separate multiple values.

► Add conditions (optional)

Add Statement

Statements added (1)
You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource(s)	Condition(s)	Remove
arn:aws:iam::097546790861:role/EC2InstanceProfileRole	Allow	s3:PutObject s3:GetObject	arn:aws:s3:::reportbucket-097546790861/*	None	Remove

Step 3: Generate policy

70. Choose **Generate Policy**.

A new window is displayed showing the generated policy in JSON format. It should look similar to:

```
{  
  "Version": "2012-10-17",  
  "Id": "Policy1604361694227",  
  "Statement": [  
    {  
      "Sid": "Stmt1604361692117",  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": "arn:aws:iam::416159072693:role/EC2InstanceProfileRole"  
      },  
      "Action": [  
        "s3:GetObject",  
        "s3:PutObject"  
      ],  
      "Resource": "arn:aws:s3:::reportbucket987987/*"  
    }  
}
```

The screenshot shows the AWS Policy Generator interface at <https://awspolicygen.s3.amazonaws.com/policygen.html>. The main area displays a JSON policy document:

```

1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Sid": "Statement1",
6        "Effect": "Allow",
7        "Principal": {
8          "AWS": "arn:aws:iam::097546790861:role/EC2InstanceProfileRole"
9        },
10       "Action": [
11         "s3:PutObject",
12         "s3:GetObject"
13       ],
14       "Resource": "arn:aws:s3:::reportbucket-097546790861/*"
15     }
16   ]
17 }

```

Below the code editor, a note reads: "This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is, and your use is in compliance with all applicable terms and conditions. This AWS Policy Generator does not modify the policy you are generating." At the bottom right are "Close" and "Copy Policy" buttons.

Confirm that /* appears after your bucket name as shown in the Resource line in the sample above.

71. Copy the policy you created to your clipboard.

72. Close the web browser tab and return to the tab with the Bucket policy editor.

73. Paste the bucket policy you created into the **Bucket policy editor**.

74. Choose **Save changes**

The screenshot shows the AWS S3 Bucket Properties page for the bucket "reportbucket-097546790861". The "Edit bucket policy" section is open, displaying the JSON policy you copied earlier:

```

1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Sid": "Statement1",
6        "Effect": "Allow",
7        "Principal": {
8          "AWS": "arn:aws:iam::097546790861:role/EC2InstanceProfileRole"
9        },
10       "Action": [
11         "s3:PutObject",
12         "s3:GetObject"
13       ],
14       "Resource": "arn:aws:s3:::reportbucket-097546790861/*"
15     }
16   ]
17 }

```

To the right of the policy editor, there are buttons for "Edit statement" and "Select a statement". Below these buttons is a link to "Add new statement".

75. Return to the AWS Systems Manager (SSM) window. If your session has timed out, reconnect to the SSM using the steps from earlier in the lab.

76. Type the following to verify you are in the /home/ssm-user/reports directory.

```
pwd
```

The output should be:

```
/home/ssm-user/reports
```

77. Enter the following command to list all objects in your reportbucket. Replace NUMBER with the number you used to create your bucket.

```
aws s3 ls s3://reportbucket(NUMBER)
```

The command should look similar to this: **aws s3 ls s3://reportbucket987987**

The output should look similar to this:

```
sh-4.2$ aws s3 ls s3://reportbucket987987
```

```
2020-11-02 23:20:27    86065 new-report.png
```

```
2020-11-02 23:57:03    90 sample-file.txt
```

78. Type the following to list the contents of the reports directory.

```
ls
```

The output returns a list of files.

79. Type the following to try coping the report-test1.txt file to the s3 bucket.

```
aws s3 cp report-test1.txt s3://reportbucket(NUMBER)
```

The command should look like this: **aws s3 cp report-test1.txt s3://reportbucket987987**

The output returns the following:

```
upload: ./report-test1.txt to s3://reportbucket987987/report-test1.txt
```

80. Type the following to see if the file successfully uploaded to S3.

```
aws s3 ls s3://reportbucket(NUMBER)
```

The output should look similar to this:

```
2020-11-11 18:20:23    86065 new-report.png
```

```
2020-11-11 18:32:18    31 report-test1.txt
```

```
2020-11-11 18:20:22    90 sample-file.txt
```

You have successfully uploaded (PutObject) a file from the EC2 instance to your S3 bucket.

81. Now type the following command to retrieve (GetObject) a file from S3 to the EC2 Instance.

The output should look similar to this:

```
download: s3://reportbucket987987/sample-file.txt to ./sample-file.txt
```

82. Type the following to see if the file is now in the /reports directory.

```
ls
```

The output should look similar to this:

```
dolphins.jpg files.zip report-test1.txt report-test2.txt report-test3.txt sample-file.txt
```

You now see the sample-file.txt in your file list. Congratulations! You have successfully uploaded and retrieved a file from EC2 to the S3 bucket.

83. Return to the browser tab that displayed the **Access Denied** for the **sample-file.txt** and refresh the page.

The page still displays an error message because the Bucket Policy only gave rights to the principal called EC2InstanceProfileRole.



84. Next, on your own, go back to the policy generator and add another statement to the bucket policy allowing EVERYONE (*), Read access (GetObject). Take a moment to generate this policy which allows both the EC2InstanceProfileRole to have access to the bucket while giving EVERYONE access to read the objects via the browser.

85. To test if your policy works, go to your browser with the Access Denied error and refresh it. If you can read the text, then congratulations! Your policy was successful.

If not, look at the policy below for help. The modified policy should look like the policy listed below. Notice that there are TWO statements, one with the EC2InstanceProfileRole and one where the Principal is "*" for everyone.

If you had trouble generating the policy on your own, you can copy the policy below and paste it into the BucketPolicy Editor. Remember to replace the existing EC2InstanceProfileRole ARN in the policy below with the EC2InstanceProfileRole ARN you copied in an earlier step. Ensure that the /* appears at the end of the Bucket ARN. See the last line of the file as an example.

```
{
```

```
  "Version": "2012-10-17",
```

```
  "Id": "Policy1604428844058",
```

```
"Statement": [  
    {  
        "Sid": "Stmt1604428821481",  
        "Effect": "Allow",  
        "Principal": {  
            "AWS": "arn:aws:iam::285058481724:role/EC2InstanceProfileRole"  
        },  
        "Action": [  
            "s3:GetObject",  
            "s3:PutObject"  
        ],  
        "Resource": "arn:aws:s3:::reportbucket987987/*"  
    },  
    {  
        "Sid": "Stmt1604428842806",  
        "Effect": "Allow",  
        "Principal": "*",  
        "Action": "s3:GetObject",  
        "Resource": "arn:aws:s3:::reportbucket987987/*"  
    }  
]
```

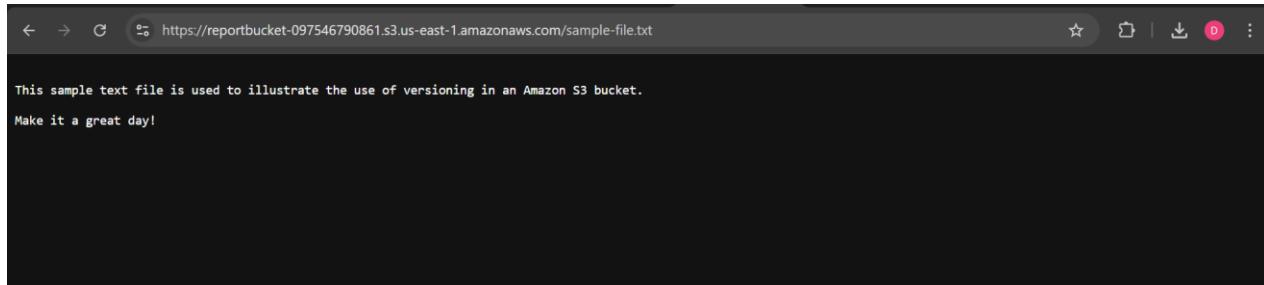
Mine:

```
{  
    "Version": "2012-10-17",  
    "Id": "Policy1604428844058",
```

```
"Statement": [  
    {  
        "Sid": "Statement1",  
        "Effect": "Allow",  
        "Principal": {  
            "AWS": "arn:aws:iam::097546790861:role/EC2InstanceProfileRole"  
        },  
        "Action": [  
            "s3:GetObject",  
            "s3:PutObject"  
        ],  
        "Resource": "arn:aws:s3:::reportbucket-097546790861/*"  
    },  
    {  
        "Sid": "Statement1",  
        "Effect": "Allow",  
        "Principal": "*",  
        "Action": "s3:GetObject",  
        "Resource": "arn:aws:s3:::reportbucket-097546790861/*"  
    }  
]
```

86. Leave the tab open with the sample-file.txt displayed. You will return to this tab in the next task.

In this task you created a bucket policy to allow specific access rights to your bucket. In the next section you explore how to keep copies of files to prevent against accidental deletion.



Task 6: Explore 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.

For auditing and compliance reasons you need to enable versionsing on your reportbucket. Versioning should protect the reports in the reportbucket against accidental deletion. You are curious to see if this works as advertised. In this task, you enable versioning and test the feature by uploading a modified version of the sample-file.txt file from the previous task.

87. You should be on the S3 bucket Permissions tab from the previous task. If you are not, choose the link to the bucket at the top-left of the screen to return to the bucket Overview page.

88. On the reportbucket overview page, choose the **Properties** tab.

A screenshot of the AWS S3 Bucket Properties page for the bucket 'reportbucket-097546790861'. The 'Properties' tab is selected. The page displays the following information:

- Bucket overview:** AWS Region: US East (N. Virginia) us-east-1; ARN: arn:aws:s3:::reportbucket-097546790861; Creation date: September 14, 2025, 15:45:39 (UTC+05:30)
- Bucket Versioning:** Status: Disabled. A note states: "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." A 'Learn more' link is provided.
- Multi-factor authentication (MFA) delete:** Status: Disabled. A note states: "An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API." A 'Learn more' link is provided.
- Tags (0):** A note states: "You can use bucket tags to track storage costs and organize buckets." A 'Learn more' link is provided.

The left sidebar shows the bucket's general purpose buckets and storage lens settings.

87. Under the **Bucket Versioning** section, choose **Edit**

90. Select **Enable** and then choose **Save changes**

The screenshot shows the 'Edit Bucket Versioning' page in the AWS S3 console. On the left, there's a sidebar with 'Amazon S3' navigation. Under 'General purpose buckets', 'reportbucket-097546790861' is selected. The main content area is titled 'Edit Bucket Versioning'. It contains a 'Bucket Versioning' section with two options: 'Suspend' (radio button is unselected) and 'Enable' (radio button is selected). A note below says: 'After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.' Another section, 'Multi-factor authentication (MFA) delete', is shown with a note: 'An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API.' Below these sections are 'Cancel' and 'Save changes' buttons.

Versioning is enabled for an entire bucket and all objects within the bucket. It cannot be enabled for individual objects.

There are also cost considerations when enabling versioning. Refer to the Additional Resources section at the end of the lab for links to more information.

91. Right-click this link and save the text file to your computer **using the same name as the text file in the previous task: [sample-file.txt](#)**.

While this file has the same name as the previous file, it contains new text.

92. In the S3 Management Console, on the reportbucket, choose the **Objects** tab.

The screenshot shows the 'Objects' tab in the 'reportbucket-097546790861' bucket. The sidebar on the left shows the bucket's general properties. The main area lists two objects: 'new-report.png' (Type: png, Last modified: September 14, 2025, 15:49:54 (UTC+05:30), Size: 84.0 KB, Storage class: Standard) and 'sample-file.txt' (Type: txt, Last modified: September 14, 2025, 16:35:32 (UTC+05:30), Size: 113.0 B, Storage class: Standard). There are buttons for Actions, Create folder, and Upload at the top of the object list. A search bar and filters for Name, Type, Last modified, Size, and Storage class are available.

Under the **Objects** section look for **Show versions**.

93. Choose **Upload** and use the same upload process in the previous task to upload the new sample-file.txt file.

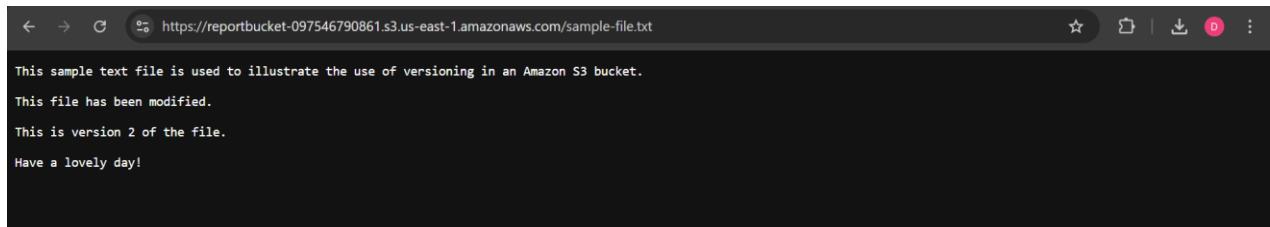
94. Go to the browser tab that has the contents of the sample-file.txt file.

95. Make a note of the contents on the page, then refresh the page.

Notice new lines of text appear.

Amazon S3 always returns the *latest version* of an object if a version is not otherwise specified.

You can also obtain a list of available versions in the S3 Management Console.



96. Close the web browser tab with the contents of the text file.

97. In the S3 Management Console, choose the **sample-file.txt** file name. The sample-file.txt overview page opens.

A screenshot of the AWS S3 Management Console. The left sidebar shows the navigation path: Amazon S3 > Buckets > reportbucket-097546790861 > sample-file.txt. The main content area displays the "sample-file.txt" object details. The "Properties" tab is selected. Key details shown include:

- Object overview**:
 - Owner**: aws-labs-accounts+prodkiku-u1KvktTbdE7RMijhWoWe8r
 - AWS Region**: US East (N. Virginia) us-east-1
 - Last modified**: September 14, 2025, 17:22:27 (UTC+05:30)
 - Size**: 171.0 B
 - Type**: txt
 - Key**: sample-file.txt
- S3 URI**: <https://reportbucket-097546790861.s3.us-east-1.amazonaws.com/sample-file.txt>
- Amazon Resource Name (ARN)**: arn:aws:s3:::reportbucket-097546790861/sample-file.txt
- Entity tag (Etag)**: 32d17db8e4e888af4e0965bd55afec4e
- Object URL**: <https://reportbucket-097546790861.s3.us-east-1.amazonaws.com/sample-file.txt>

98. Choose the **Versions** tab and then select the bottom version which reads **null** (Note: This is **not** the latest version).

Version ID	Type	Last modified	Size	Storage class
PgJDKyMk8QYVcPl_WvsIQv...	txt	September 14, 2025, 17:22:27 (U...)	171.0 B	Standard
<input checked="" type="checkbox"/> null	txt	September 14, 2025, 16:35:32 (U...)	113.0 B	Standard

99. Select **Open**.

You should now see the original version of the file using the S3 Management Console.

However, if you try to access the older version of the sample-file.txt file using the object URL link, you will receive an access denied message. This is expected because the bucket policy you created in the previous task only allows permission to access the latest version of the object. In order to access a previous version of the object, you need to update your bucket policy to include the “**s3:GetObjectVersion**” permission. Below is an example bucket policy with the additional “**s3:GetObjectVersion**” action added that allows you to access the older version using the link. You do not need to update your bucket policy with this example to complete this lab. You can try to do this on your own after you complete the task.

```
{  
  "Id": "Policy1557511288767",  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "Stmt1557511286634",  
      "Action": [  
        "s3:GetObject",  
        "s3:GetObjectVersion"  
      ],  
      "Resource": "arn:aws:s3:::reportbucket-097546790861/*",  
      "Condition": {"StringLike": {"aws:Requester": "AWSLabsUser-uMVgnXU#cmJYp4tNShw4z/25858..."}},  
      "Effect": "Allow"  
    }  
  ]  
}
```

```

"s3:GetObjectVersion"
],
"Effect": "Allow",
"Resource": "arn:aws:s3:::mybucket45647467/*",
"Principal": "*"
}
]
}

```

100. Return to the **AWS Management Console** tab and choose the link for the bucket name at the top-left to return to the bucket Objects tab.

101. Locate the **Show versions** option and toggle the button to on to show the versions.

Now you can view the available versions of each object and identify which version is the latest. Notice the **new-report.png** object only has one version and the version ID is **null**. This is because the object was uploaded before versioning was enabled on this bucket.

Also notice that you can now choose the version name link to navigate directly to that version of the object in the console.

102. Next to **Show versions** toggle the button to off to return to the default object view.

103. Select the checkbox to the left of the **sample-file.txt**.

104. With the object selected, choose **Delete**

105. The **Delete objects** window appears.

106. At the bottom, in the **Delete objects?** section you must type the word delete to confirm deletion of the object. Type **delete** and choose the **Delete objects** button.

107. Choose **Close** to return to the bucket overview.

The sample-file.txt object is no longer displayed in the bucket. However, if the object is deleted by mistake, versioning can be used to recover it.

108. Locate the **Show versions** option and toggle the button to on to show the versions.

Notice that the sample-file.txt object is displayed again, but the most recent version is a **Delete marker**. The two previous versions are listed as well. If versioning has been enabled on the bucket, objects are not immediately deleted. Instead, Amazon S3 inserts a delete marker, which becomes the current object version. The previous versions of the object are not removed. Refer to the Additional Resources section at the end of the lab for links to more information about versioning.

109. Select the checkbox to the left of the version of the sample-file.txt object with the **Delete marker**.
110. With the object selected, choose **Delete**
111. The **Delete objects** window appears.
112. At the bottom in the **Permanently delete objects?** section you must type the word permanently delete to confirm deletion of the object. Type **permanently delete** and choose the **Delete objects** button.
113. Choose **Close** to return to the bucket overview.
114. Next to **Show versions** toggle the button to off to return to the default object view.

Notice that the sample-file.txt object has been restored to the bucket. Removing the delete marker has effectively restored the object to its previous state. Refer to the Additional Resources section at the end of the lab for links to more information about undeleting S3 objects.

Next, you delete a specific version of the object.

115. To delete a specific version of the object, locate the **Show versions** option and toggle the button to on to show the versions.

You should see two versions of the *sample-file.txt* object.

116. Select the checkbox to the left of the latest version of the **sample-file.txt** object.
117. With the object selected, choose **Delete**.
118. The **Delete objects** window appears.
119. At the bottom in the **Permanently delete objects?** section type **permanently delete** and choose the **Delete objects** button.
120. Choose **Close** to return to the bucket overview.

Notice that there is now only one version of the sample-file.txt file. When deleting a specific version of an object no delete marker is created. The object is permanently deleted. Refer to the Additional Resources section at the end of the lab for links to more information about deleting object versions in Amazon S3.

121. Next to **Show versions** toggle the button to off to return to the default object view.
122. Choose the **sample-file.txt** file name. The sample-file.txt overview page opens.
123. Copy the **Object URL** link displayed at the bottom of the window.
124. In a new browser tab, paste the link into the address field, and then press **Enter**.

The text of the original version of the sample-file.txt object is displayed.

Summary:

You have successfully created an S3 bucket for your company to use to store report data from your EC2 Instance. You created a bucket policy to allow for the EC2 Instance to PutObjects and GetObject from the reportbucket and you successfully tested uploading and downloading files from the EC2 instance to test the bucket policy. You have enabled versioning on the S3 bucket to protect against accidental object deletion. You have successfully completed the configuration for your EC2 reportbucket. Congratulations!

Conclusion

You have successfully learned how to:

- Create a bucket in Amazon S3
- Add an object to your bucket
- Manage access permissions on an object
- Create a bucket policy
- Use bucket versioning

End lab

Follow these steps to close the console and end your lab.

125. Return to the **AWS Management Console**.
126. At the upper-right corner of the page, choose **AWSLabsUser**, and then choose **Sign out**.
127. Choose **End Lab** and then confirm that you want to end your lab.

Additional resources

- [Amazon S3](#)
- [Amazon S3 training](#)
- [Editing Object Permissions](#)
- [Amazon S3 bucket naming rules](#)
- [Amazon S3 block public access](#)
- [Amazon Resource Names \(ARNs\) and AWS Service Namespaces documentation](#)
- [AWS JSON Policy Elements documentation](#)
- [Actions, Resources, and Condition Keys for Amazon S3](#)
- [Amazon S3 Versioning](#)
- [Undelete objects in Amazon S3](#)
- [Deleting object versions in Amazon S3](#)
- [Amazon S3 Versioning cost considerations](#)
- [AWS Systems Manager Session Manager](#) For more information about AWS Training and Certification, see <https://aws.amazon.com/training/>.