

Lab 6: Configure an Amazon CloudFront Distribution with an Amazon S3 Origin

© 2025 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. All trademarks are the property of their owners.

Lab overview

Amazon Web Services (AWS) solutions architects must frequently design and build secure, high-performing, resilient, efficient architectures for applications and workloads to deliver content. Amazon CloudFront is a web service that provides a cost-effective way to distribute content with low latency and high data transfer speeds. You can use CloudFront to accelerate static website content delivery, serve video on demand or live streaming video, and even run serverless code at the edge location. In this lab, you configure a CloudFront distribution in front of an Amazon Simple Storage Service (Amazon S3) bucket and secure it using origin access control (OAC) provided by CloudFront.

Objectives

After completing this lab, you should be able to do the following:

- Create an S3 bucket with default security settings.
- Configure an S3 bucket for public access.
- Add an S3 bucket as a new origin to an existing CloudFront distribution.
- Secure an S3 bucket to permit access only through the CloudFront distribution.
- Configure OAC to lock down security to an S3 bucket.
- Configure Amazon S3 resource policies for public or OAC access.

Lab Environment

The lab environment provides you with some resources to get started. There is an Auto Scaling group of EC2 instances being used as publicly accessible web servers. The web server infrastructure is deployed in an Amazon Virtual Private Cloud (Amazon VPC) and configured for multiple Availability Zones. It also uses load balancers. The lab also provides a CloudFront distribution with this load balancer as an origin.

The following diagram shows the general expected architecture you should have at the end of this lab.

During this lab, you create a new S3 bucket for the existing lab environment.

You then configure this bucket as a new, secure origin to the existing CloudFront distribution.

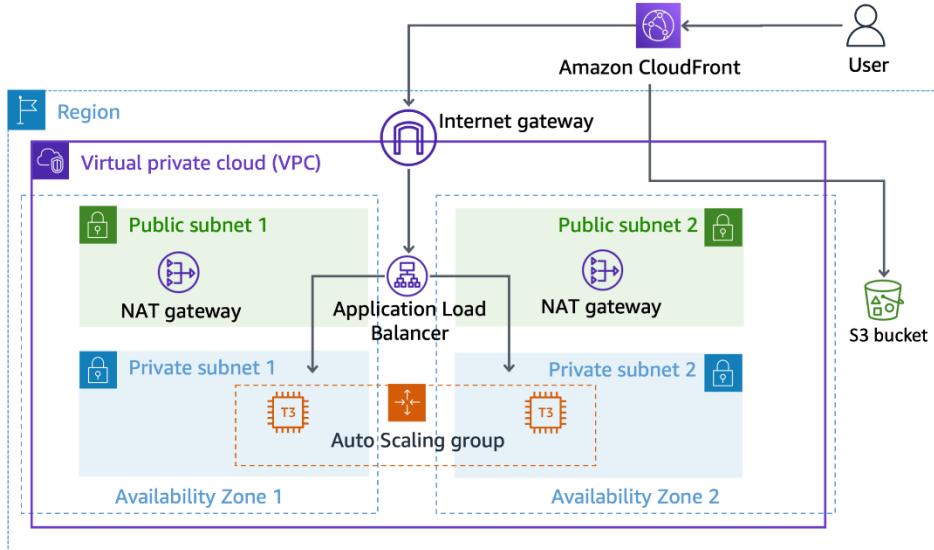


Image description: The preceding diagram depicts an environment with an Amazon VPC for secure and isolated connections between services. To decrease latency it has Amazon CloudFront to facilitate a CDN (Content-Delivery-Network) as a service for faster upload and download speeds, this connects to an InternetGateway to provide support for internet-facing applications, which is behind an Application Load Balancer which helps in distributing traffic among different instances behind an Auto-Scaling Group inside PrivateSubnets with a single NAT Gateway in each Public Subnet. It also uses Amazon S3 to provide cost effective object storage.

Services used in this lab

Amazon CloudFront

CloudFront is a content delivery web service. It integrates with other AWS products so that developers and businesses can distribute content to end users with low latency, high data transfer speeds, and no minimum usage commitments.

You can use CloudFront to deliver your entire website, including dynamic, static, streaming, and interactive content, using a global network of edge locations. CloudFront automatically routes requests for your content to the nearest edge location to deliver content with the best possible performance. CloudFront is optimized to work with other AWS services, like Amazon S3, Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB), and Amazon Route 53. CloudFront also works seamlessly with any origin server that doesn't use AWS, which stores the original, definitive versions of your files.

Amazon Simple Storage Service (Amazon S3)

Amazon S3 provides developers and information technology teams with secure, durable, highly scalable object storage. Amazon S3 has a simple web services interface to store and retrieve any amount of data from anywhere on the web.

You can use Amazon S3 alone or together with other AWS services such as Amazon EC2, Amazon Elastic Block Store (Amazon EBS), and Amazon Simple Storage Service Glacier (Amazon S3 Glacier), along with third-party storage repositories and gateways. Amazon S3 provides cost-effective object storage for a wide variety of use cases, including cloud applications, content distribution, backup and archiving, disaster recovery, and big data analytics.

Task 1: Explore the existing CloudFront distribution

In this task, you examine the existing CloudFront distribution that was built for web server content. Before making changes to an environment, it is a good practice to understand the existing configuration. If you want to use CloudFront distributions for your personal AWS environments, you need to build and configure the distribution itself first. In later tasks, you add an S3 bucket as a new origin to this CloudFront distribution.

Task 1.1: Open the CloudFront console

- If you have not already opened the console, follow the instructions in the [Start Lab](#) section to log in to the console.
- At the top of the console, in the search bar, search for and choose **CloudFront**

Task 1.2: Open the existing CloudFront distribution

- Choose the ID link for the only available distribution.

The screenshot shows the AWS CloudFront Distributions page. On the left, there's a navigation menu with 'CloudFront' selected. The main area displays a table titled 'Distributions (1)'. The table has columns for ID, Status, Description, Type, Domain Name, Alternative Domain Names, and Origins. One row is visible, showing 'E2KCWLERO1QBAN' with 'Enabled' status and 'LabELB-157257' as the origin. There are buttons for 'Enable', 'Disable', 'Delete', and 'Create distribution' at the top right of the table.

Note: If you do not find the list of distributions, ensure that you are at the correct page. Choose **Distributions** from the CloudFront navigation menu located on the left side of the console.

A page showing the details of the distribution is displayed.

Task 1.3: Explore the properties of the existing distribution

In this task, you explore each tab of the distribution to review the existing configuration. In this lab, you are not configuring this CloudFront distribution in great detail. However, it is useful to know where all of the configurations you might need for managing a CloudFront distribution are located.

- Examine the contents of the **General** tab.

This tab contains the details about the current configuration of this particular CloudFront distribution. It contains the most generally needed information about a distribution. It is also where you configure the common high-level items for the distribution, such as activating the distribution, logging, and certificate settings.

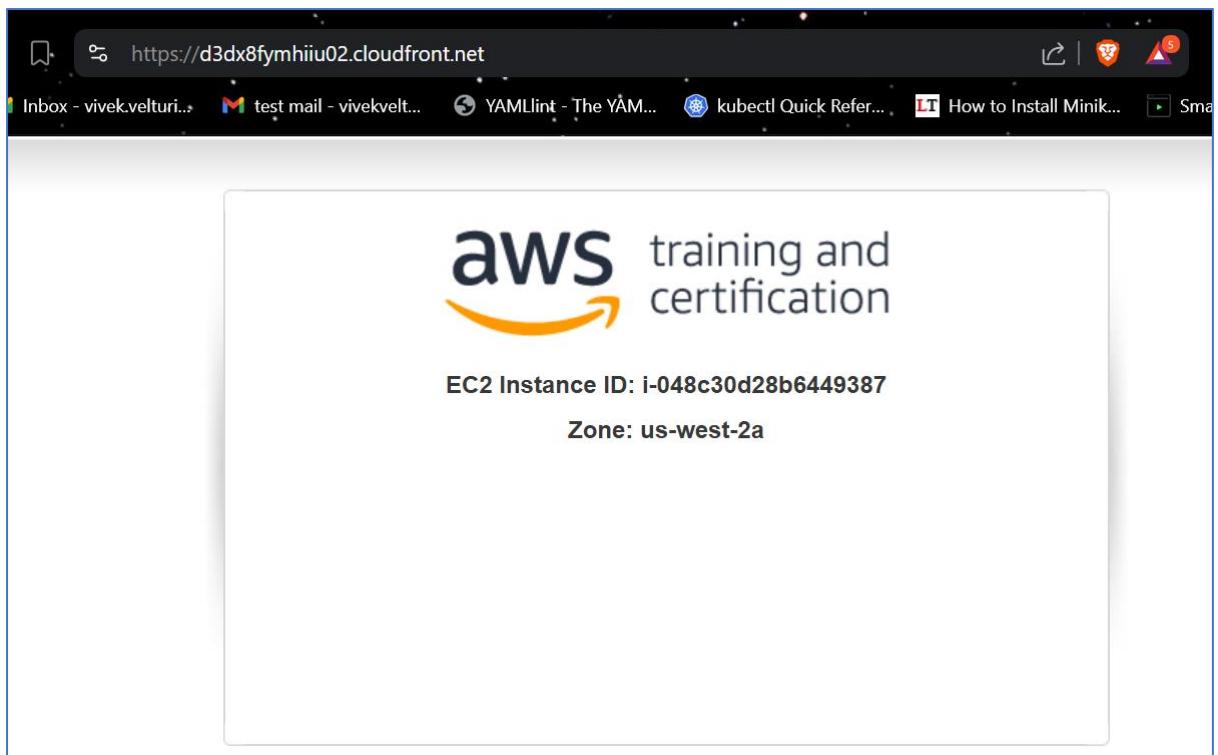
- **Copy edit:** From the **Details** section, in the **General** tab, copy the **ARN** value and save it in a text editor. You need this value for a later task.
- **Copy edit:** From the **Details** section, in the **General** tab, copy the **Distribution domain name** value.

The Distribution domain name is also found to the left of these lab instructions under the listing *LabCloudFrontDistributionDNS*.

The screenshot shows the AWS CloudFront console with the navigation bar at the top. The main area displays the 'General' tab for the distribution 'E2KCWLERO1QBAN'. The 'Details' section shows the 'Distribution domain name' as 'd5dx8fymhiu02.cloudfront.net' and the 'ARN' as 'arn:aws:cloudfront::070991923640:distribution/E2KCWLERO1QBAN'. The 'Last modified' timestamp is April 15, 2025, at 9:53:39 AM UTC. The 'Settings' section includes fields for 'Description' (a CloudFront distribution for Elastic Load Balancer), 'Price class' (Use only North America and Europe), and 'Supported HTTP versions' (HTTP/1.1, HTTP/1.0). It also lists 'Alternate domain names' and 'Standard logging' (Off). The 'Continuous deployment' section has a 'Create staging distribution' button. On the left sidebar, there are sections for Distributions, Telemetry, Reports & analytics, Security, and Key management.

- Paste the **Distribution domain value** you copied into a new browser tab.

A simple web page is loaded displaying the information of the web server from which CloudFront retrieved the content. By requesting content from the Distribution domain value for the CloudFront distribution, you are verifying that the existing cache is working.



You can close this tab.

- Return to the **CloudFront** console.
- Choose the **Security** tab.

A screenshot of the AWS CloudFront console. The left sidebar shows navigation options like 'Distributions', 'Telemetry', and 'Reports & analytics'. The main panel is titled 'E2KCWLERO1QBAN' and shows the 'Security' tab selected. It includes sections for 'Enable security protections' (with a 'Manage security protections' button), 'Security - Web Application Firewall (WAF)' (with 'Core protections', 'SQL protections', and 'Rate limiting' all set to 'Disabled'), and 'CloudFront geographic restrictions'.

This tab contains the distribution's configuration if you need to keep your application secure from the most common web threats using AWS WAF or need to prevent users in specific countries from accessing your content using geographic restrictions. These features are not configured for use in this lab.

- Choose the **Origins** tab.

This tab contains the details about the current origins that exist for this particular CloudFront distribution. It is also the area of the console you can use to configure new or existing CloudFront origins. A *CloudFront Origin* defines the location of the definitive, original version of the content that is delivered through the CloudFront distribution.

The screenshot shows the AWS CloudFront Origins page for distribution E2KCWLERO1QBAN. The left sidebar includes sections for Distributions, Telemetry, Reports & analytics, and Security. The main content area has tabs for General, Security, Origins (selected), Behaviors, Error pages, Invalidations, Tags, and Logging. The Origins section displays a table with one row:

Origin name	Origin domain	Origin path	Origin type	Origin Shield region	Origin access
LabELBOrigin	LabELB-1572574597.us-west-2.elb.amazonaws.com		Elastic Load Balancing	-	-

The Origin groups section below shows a message: "No origin groups. You don't have any origin groups." with a "Create origin group" button.

Note: The only origin currently on the distribution is an ELB load balancer. This load balancer is accepting and directing web traffic for the auto scaling web servers in its target group.

- **Copy edit:** Copy the load balancer's Domain Name System (DNS) value for this origin from the column labeled **Origin domain**.

Note: You can adjust the widths of most columns in the console by dragging the dividers in the header.

- Paste the DNS value for the load balancer into a new browser tab.

The screenshot shows a browser window with the URL <http://labelb-1572574597.us-west-2.elb.amazonaws.com>. The page content includes the AWS logo and the text "training and certification". Below that, it displays "EC2 Instance ID: i-06806b41bd7989ddc" and "Zone: us-west-2b". The browser toolbar at the top shows various open tabs and icons.

The DNS value for this distribution is also found to the left of these lab instructions under the listing *LabLoadBalancerDNS*.

The simple web page hosted on the EC2 instances is displayed again. This web page displays the same content that was delivered by the CloudFront distribution earlier. However, by requesting from the load balancer directly you are not using the existing CloudFront caching system. In any single request, the EC2 Instance ID displayed on the page might differ because traffic is not always routed to the same EC2 instance behind the load balancer.

This step demonstrates that the origins defined for a distribution are the locations used to retrieve novel content when a request is made to the CloudFront distribution's frontend.

You can close this tab.

- Return to the **CloudFront** console.
- Choose the **Behaviors** tab.

The screenshot shows the AWS CloudFront console with the 'Behaviors' tab selected for the distribution 'E2KCWLERO1QBAN'. The left sidebar shows navigation options like 'Distributions', 'Policies', 'Functions', 'Static IPs', 'VPC origins', and 'Telemetry'. The main area displays a table of behaviors:

Preced...	Path pattern	Origin or origin group	Viewer protocol policy	Cache policy name	Origin request policy name	Response headers policy n...
<input type="radio"/> 0	Default (*)	LabELBOOrigin	HTTP and HTTPS			

Buttons at the top right include 'Save', 'Move up', 'Move down', 'Edit', 'Delete', and 'Create behavior'.

Behaviors define the actions that the CloudFront distribution takes when there is a request for content, such as which origin to serve which content, Time To Live of content in the cache, cookies, and how to handle various headers.

This tab contains a list of current behaviors defined for the distribution. You configure new or existing behaviors here. Behaviors for the distribution are evaluated in the explicit order in which you define them on this tab.

Do the following to review or edit the configuration of any single behavior:

- Select the radio button in the row next to the behavior you want to modify.
- Choose **Edit**.
- Choose **Cancel** to close the page and return to the console.

There is only one behavior currently configured in this lab environment. The behavior accepts HTTP and HTTPS for both GET and HEAD requests to the load balancer origin.

- Choose the **Error Pages** tab.

This tab details which error page is to be returned to the user when the content requested results in an HTTP 4xx or 5xx status code. You can configure custom error pages for specific error codes here.

E2KCWLERO1QBAN

Error pages

HTTP error code	Minimum TTL (seconds)	Response page path	HTTP response code
404	30	/error-pages/404.html	200

View metrics

- Choose the **Invalidations** tab.

This tab contains the distribution's configuration for object invalidation.

Invalidated objects are removed from CloudFront edge caches.

A faster and less expensive method is to use versioned objects or directory names.

There are no invalidations configured for CloudFront distributions by default.

E2KCWLERO1QBAN

Invalidations

No invalidations
You don't have any invalidations.

Create invalidation

View details Copy to new Create invalidation

- Choose the **Tags** tab.

This tab contains the configuration for any tags applied to the distribution. You can view and edit existing tags and create new tags here. Tags help you identify and organize your distributions.

E2KCWLERO1QBAN

Tags (1)

Key	Value
Name	Lab CloudFront Distribution

Manage tags

View metrics

You have explored the existing CloudFront distribution.

Task 2: Create an S3 bucket

In this task, you create and configure a new S3 bucket. This bucket is used as a new origin for the CloudFront distribution.

- At the top of the console, in the search bar, search for and choose **S3**

- In the **Buckets** section, choose **Create bucket**.

Note: If you do not find the Create bucket button, ensure you are at the correct page. Choose **Buckets** from the navigation menu located on the left side of the console.

The **Create bucket** page is displayed.

- Type **lab-bucket-110648891** into the **Bucket name** field.

Note: To simplify the written instructions in this lab, this newly created bucket is referred to as the *LabBucket* for the remainder of the instructions.

The AWS Region should match the *PrimaryRegion* value found to the left of these lab instructions.

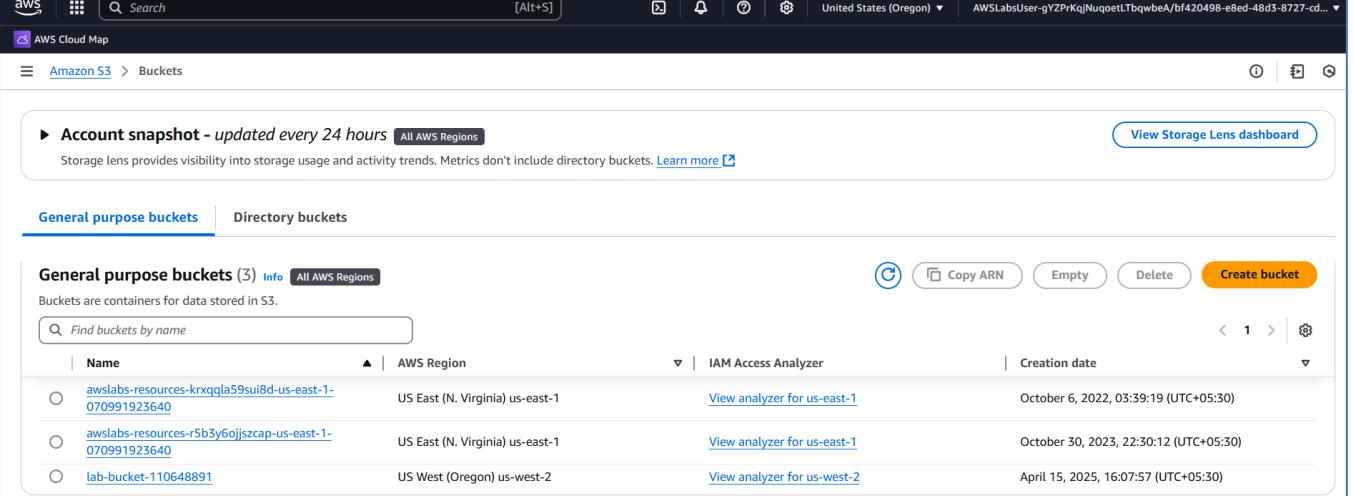
The screenshot shows the AWS S3 'Create bucket' page. The 'General configuration' section is visible. The 'Bucket name' field contains 'lab-bucket-110648891'. The 'Bucket type' dropdown is open, showing two options: 'General purpose' (selected) and 'Directory'. Below each option is a brief description. The 'General purpose' description states: '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.' The 'Directory' description states: 'Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.'

- Leave all other settings on this page as the default configurations.
- Choose **Create bucket**.

The screenshot shows the 'Default encryption' section of the 'Create bucket' page. It includes a note that server-side encryption is automatically applied to new objects stored in the bucket. The 'Encryption type' dropdown is open, showing three options: 'Server-side encryption with Amazon S3 managed keys (SSE-S3)' (selected), 'Server-side encryption with AWS Key Management Service keys (SSE-KMS)', and 'Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)'. A note below the dropdown says: 'Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#).²' The 'Bucket Key' section shows that using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. A note below says: 'Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)²'.

The Amazon S3 console is displayed. The newly created bucket is displayed among the list of all the buckets for the account.

You have created a new S3 bucket with the default configuration.



The screenshot shows the AWS S3 console with the 'Buckets' page. At the top, there's a header with the AWS logo, search bar, and navigation links. Below the header, a banner displays 'Account snapshot - updated every 24 hours' and a link to 'View Storage Lens dashboard'. The main area is titled 'General purpose buckets' with a count of 3. It includes a search bar labeled 'Find buckets by name'. A table lists three buckets:

Name	AWS Region	IAM Access Analyzer	Creation date
awslabs-resources-krxqqla59sui8d-us-east-1-070991923640	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 6, 2022, 03:39:19 (UTC+05:30)
awslabs-resources-r5b3y6ojjszcap-us-east-1-070991923640	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 30, 2023, 22:30:12 (UTC+05:30)
lab-bucket-110648891	US West (Oregon) us-west-2	View analyzer for us-west-2	April 15, 2025, 16:07:57 (UTC+05:30)

At the bottom right of the table, there are buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'.

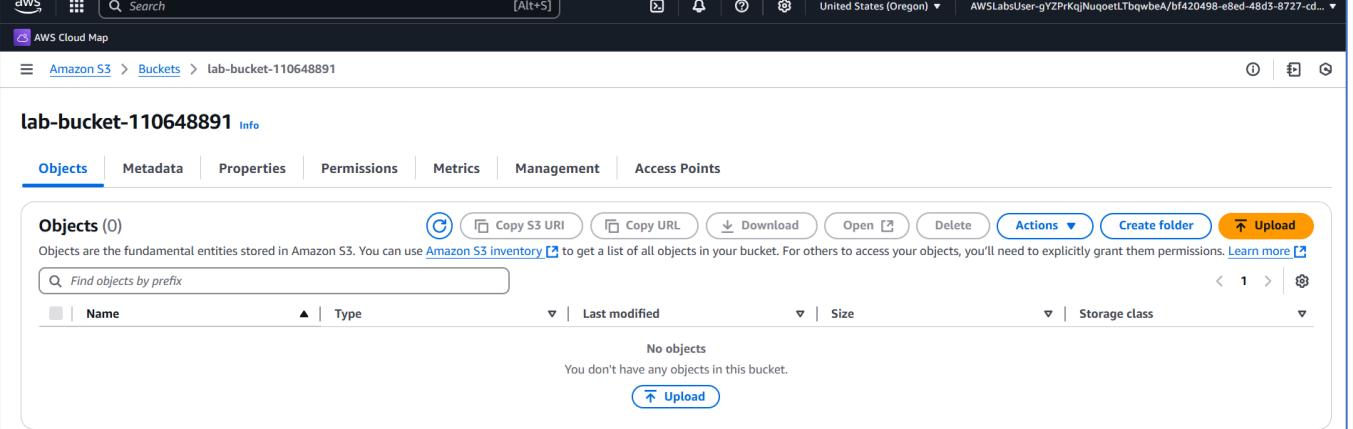
Task 3: Configure the S3 LabBucket for public access

In this task, you review the default access setting for S3 buckets. Next, you modify the permissions settings to allow public access to the bucket.

Task 3.1: Configure the LabBucket to allow public policies to be created

- Select the link for the newly created `lab-bucket-110648891` found in the **Buckets** section.

A page with all of the bucket details is displayed.



The screenshot shows the AWS S3 console with the 'Objects' tab selected for the 'lab-bucket-110648891' bucket. At the top, there's a header with the AWS logo, search bar, and navigation links. Below the header, a banner displays the bucket name and a link to 'Amazon S3 inventory'. The main area is titled 'lab-bucket-110648891' with a count of 0 objects. It includes a search bar labeled 'Find objects by prefix'. A table lists objects:

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

At the bottom right of the table, there is a 'Upload' button.

- Choose the **Permissions** tab.
- Locate the **Block public access (bucket settings)** section.
- Choose **Edit**.

The screenshot shows the AWS S3 console with the path `Amazon S3 > Buckets > lab-bucket-110648891`. The **Permissions** tab is active. In the **Block public access (bucket settings)** section, the **Block all public access** checkbox is checked (On). An **Edit** button is visible in the top right.

The **Edit Block public access (bucket settings)** page is displayed.

- Unselect **Block all public access**.
- Choose **Save Changes**.

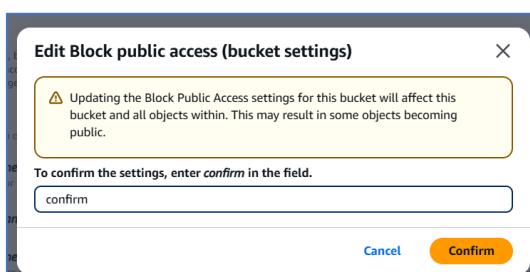
The screenshot shows the **Edit Block public access (bucket settings)** dialog. It lists several sub-options under the main **Block all public access** setting:

- Block public access to buckets and objects granted through new access control lists (ACLs)** (highlighted with a yellow box)
- 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**
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**

At the bottom, there are **Cancel** and **Save changes** buttons.

A message window titled **Edit Block public access (bucket settings)** is displayed.

- In the message field, enter **confirm**.
- Choose **Confirm**.



You have removed the block on all public access policies for the *lab-bucket-110648891*. You are now able to create access policies for the bucket that allow for public access. The bucket is currently not public, but anyone with the appropriate permissions can grant public access to objects stored within the bucket.

Task 3.2: Configure a public read policy for the LabBucket

You now create a public object read policy for this bucket.

- On the **Permissions** tab, locate the **Bucket policy** section.
- Choose **Edit**.

The **Edit bucket policy** page is displayed.

```
Bucket policy
arn:aws:s3:::lab-bucket-110648891
Policy
Statement 1
+ Add new statement
Select a statement
+ Add new statement
Preview external access
```

- **Copy edit:** Copy and paste the **Bucket ARN** value into a text editor to save the information for later. It is a string value like *arn:aws:s3:::LabBucket* located above the *Policy* box.

The ARN value uniquely identifies this S3 bucket. You need this specific ARN value when creating bucket based policies.

- **File contents:** Copy and paste the following JSON into a text editor.

```
{
  "Version": "2012-10-17",
  "Id": "Policy1621958846486",
  "Statement": [
    {
      "Sid": "OriginalPublicReadPolicy",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ]
    }
  ]
}
```

```
        ],
        "Resource": "RESOURCE_ARN"
    }
]
```

- Replace the **RESOURCE_ARN** value in the JSON with the **Bucket ARN** value you copied in a [previous step](#) and append a `/*` to the end of the pasted **Bucket ARN** value.

By appending the `/*` wildcard to the end of the ARN, the policy definition applies to all objects located in the bucket.

Here is the example of the updated policy JSON:

```
{
    "Version": "2012-10-17",
    "Id": "Policy1621958846486",
    "Statement": [
        {
            "Sid": "OriginalPublicReadPolicy",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::lab-bucket-110648891/*"
        }
    ]
}
```

- Choose **Save changes**.

Caution: If you receive an error message at the bottom of the screen, it's probably caused by a syntax error with JSON. The policy will not save until the JSON is valid. You can expand the error message in the Amazon S3 console for more information about correcting the policy.

By using the `*` wildcard as the Principal value, *all* identities requesting the actions defined in the policy document are allowed to do so. By appending the `/*` wildcard to the allowed Resources, this policy applies to all objects located in the bucket.

Note: The policies currently applied to the bucket make the objects in this bucket publicly readable.

In later lab steps, you configure the bucket to be accessible only from the CloudFront distribution.

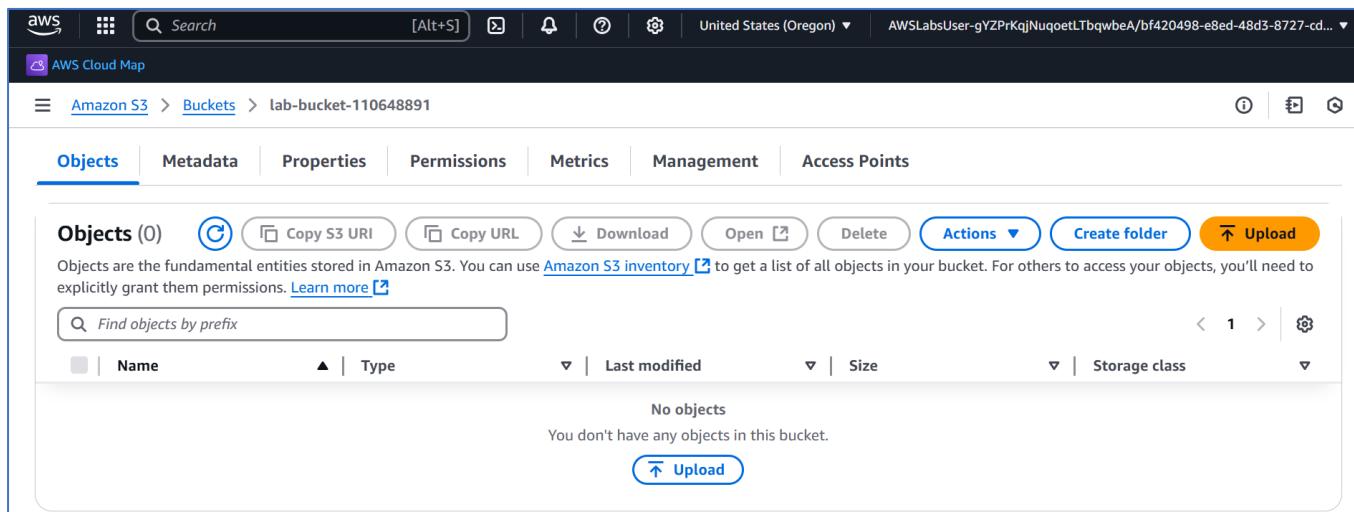
You have configured an S3 bucket for public read access.

Task 4: Upload an object into the bucket and testing public access

In this task, you upload a single object to the LabBucket. You use this object to test access in the remaining lab tasks.

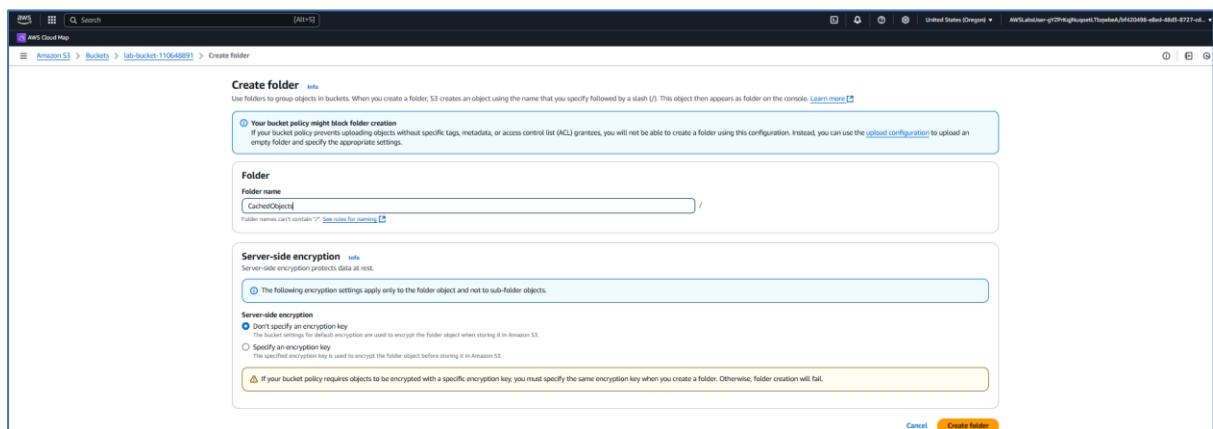
Task 4.1: Create a new folder in the bucket

- Choose the **Objects** tab.
- Choose **Create folder**.



The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with 'Search' and other account information. Below it, the 'Amazon S3 > Buckets > lab-bucket-110648891' path is visible. The main area has tabs for 'Objects', 'Metadata', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects' tab is selected. Below the tabs, there's a section for 'Objects (0)' with a 'Create folder' button highlighted. A message says 'No objects' and 'You don't have any objects in this bucket.' At the bottom right of this section is another 'Upload' button.

- Enter **CachedObjects** into the **Folder name** field.
- Leave all other settings on the page at the default values.



The screenshot shows the 'Create folder' dialog box. It has two main sections: 'Folder' and 'Server-side encryption'. In the 'Folder' section, the 'Folder name' field is filled with 'CachedObjects'. In the 'Server-side encryption' section, the 'Don't specify an encryption key' option is selected. At the bottom right of the dialog is a 'Create folder' button.

- Choose **Create folder**.

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with 'Search' and 'United States (Oregon)' information. Below it, the path 'Amazon S3 > Buckets > lab-bucket-110648891' is shown. A green success message box at the top says 'Successfully created folder "CachedObjects".' The main area is titled 'lab-bucket-110648891' with an 'Info' link. Below that, tabs for 'Objects', 'Metadata', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points' are visible. The 'Objects' tab is selected. Under 'Objects (1)', there's a single item: 'CachedObjects/' which is a 'Folder'. To the right of the object list are several actions: 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'.

Task 4.2: Upload an object to the bucket

- Download the object for these lab instructions by choosing [logo.png](#) and saving it to your local device.
- Return to the **Amazon S3** Console.
- Choose the link for the [CachedObjects/](#) folder that you created previously.
- Choose **Upload**.

The **Upload** page is displayed.

The screenshot shows the 'Upload' page in the AWS S3 console. The path in the navigation bar is 'Amazon S3 > Buckets > lab-bucket-110648891 > CachedObjects/ > Upload'. The main title is 'Upload' with an 'Info' link. Below it, a note says 'Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)'.

The 'Files and folders (0)' section has a 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder' area. Below it, a table shows 'Name' and 'Type' columns. A message says 'No files or folders' and 'You have not chosen any files or folders to upload.'

The 'Destination' section shows the URL 's3://lab-bucket-110648891/CachedObjects/'.

- Choose **Add files**.
- Choose the **logo.png** object from your local storage location.
- Choose **Upload**.

The **Upload: status** page is displayed.

A **Upload succeeded** message is displayed on top of the screen.

The screenshot shows the AWS S3 console interface. At the top, there is a green notification bar with the text "Upload succeeded" and a link to "Files and folders table". Below this, the "Summary" section shows a destination of "s3://lab-bucket-110648891/CachedObjects/" with a "Succeeded" status of "1 file, 16.0 KB (100.00%)". To the right, there is a "Failed" section showing "0 files, 0 B (0%)". Below the summary, there are two tabs: "Files and folders" (which is selected) and "Configuration". Under "Files and folders", there is a table with one row for "logo.png". The table columns include Name, Folder, Type, Size, Status, and Error. The "Status" column for "logo.png" shows "Succeeded".

Task 4.3: Test public access to an object

- Choose the [logo.png](#) link from the **Files and folders** section.

A page with details about the Amazon S3 object is displayed.

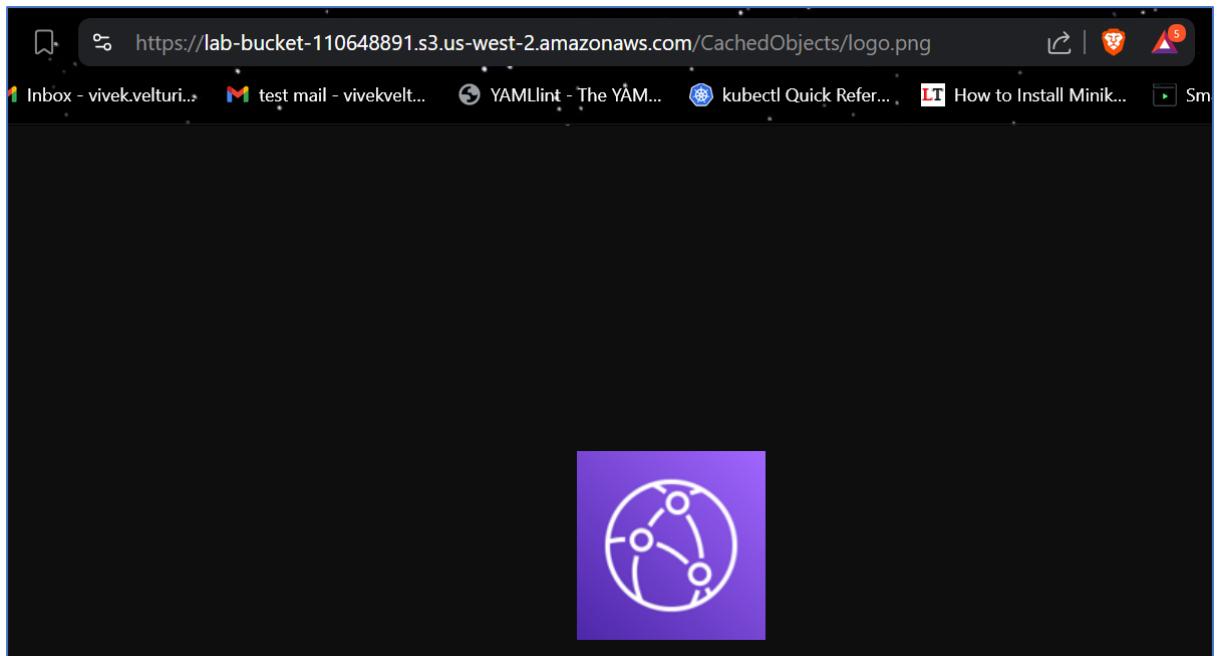
The screenshot shows the AWS S3 object details page for "logo.png". The left sidebar shows the navigation path: Amazon S3 > Buckets > lab-bucket-110648891 > CachedObjects/ > logo.png. The main content area displays the object's properties. The "Properties" tab is selected, showing the following details:

- Object overview**:
 - Owner: aws-labs-accounts+prodkiku-mAAFznTDSuvKTzbSckDqRj
 - AWS Region: US West (Oregon) us-west-2
 - Last modified: April 15, 2025, 16:31:33 (UTC+05:30)
 - Size: 16.0 KB
 - Type: png
 - Key: CachedObjects/logo.png
- S3 URI**: <s3://lab-bucket-110648891/CachedObjects/logo.png>
- Amazon Resource Name (ARN)**: <arn:aws:s3:::lab-bucket-110648891/CachedObjects/logo.png>
- Entity tag (Etag)**: <24d738d0d8206dbab4ae5de5c7a13308>
- Object URL**: <https://lab-bucket-110648891.s3.us-west-2.amazonaws.com/CachedObjects/logo.png>

- Select the link located in the **Object URL** field.

The picture is displayed in a browser tab.

- Inspect the URL for the object and notice it is an Amazon S3 URL.



- Close this page with the object.

You have created a folder in an S3 bucket, uploaded an object, and tested that the object can be retrieved from the S3 URL.

Task 5: Secure the bucket with Amazon CloudFront and Origin Access Control

In a previous task, you have confirmed public access to the `lab-bucket-110648891` works, but are not utilizing the CloudFront distribution for object access. In this task, you add the lab bucket as a new origin to the CloudFront distribution and make the objects in the `lab-bucket-110648891` accessible only from the CloudFront distribution.

Task 5.1: Update the bucket policy for the LabBucket

Update the bucket policy to allow read-only access from the CloudFront distribution.

- At the top of the console, in the search bar, search for and choose **S3**.
- Select the link for the `lab-bucket-110648891` found in the **Buckets** section.

A page with all of the bucket details is displayed.

- Choose the **Permissions** tab.
- Locate the **Bucket policy** section.
- Choose **Edit**.

The **Edit bucket policy** page is displayed.

- **Copy edit:** Copy and paste the **Bucket ARN** value into a text editor to save the information for later. It is a string value like `arn:aws:s3:::LabBucket` located above the *Policy* box.

The ARN value uniquely identifies this S3 bucket. You need this specific ARN value when creating bucket based policies.

- **File contents:** Copy and paste the following JSON into a text editor.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontServicePrincipalReadOnly",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "RESOURCE_ARN",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn": "CLOUDFRONT_DISTRIBUTION_ARN"
                }
            }
        }
    ]
}
```

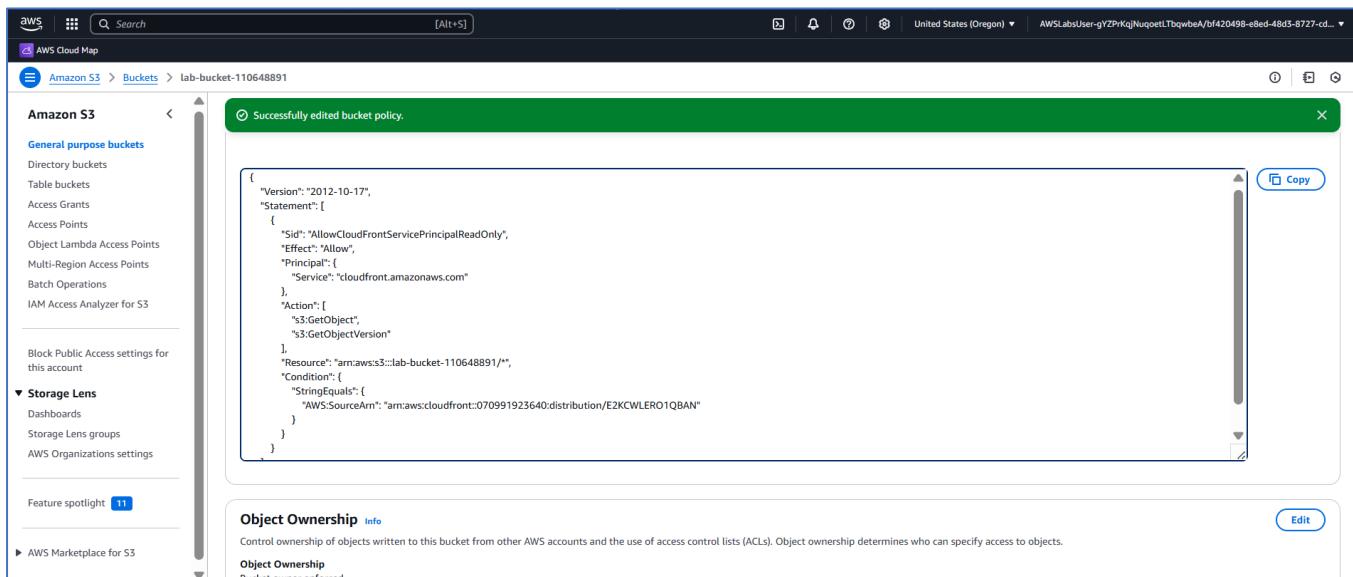
- Replace the **RESOURCE_ARN** value in the JSON with the **Bucket ARN** value you copied in a [previous step](#) and append a `/*` to the end of the pasted **Bucket ARN** value.

- Replace the **CLOUDFRONT_DISTRIBUTION_ARN** value in the JSON with the ARN value you copied in a [previous step](#).

Here is the example of the updated policy JSON:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCloudFrontServicePrincipalReadOnly",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudfront.amazonaws.com"
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::lab-bucket-110648891/*",
      "Condition": {
        "StringEquals": {
          "AWS:SourceArn": "arn:aws:cloudfront::070991923640:distribution/E2KCWLERO1QBAN"
        }
      }
    }
  ]
}
```

- Choose **Save changes**.



Task 5.2: Enable the public access blockers

- On the **Permissions** tab, locate the **Block public access (bucket settings)** section.
- Choose **Edit**.

The **Edit Block public access (bucket settings)** page is displayed.

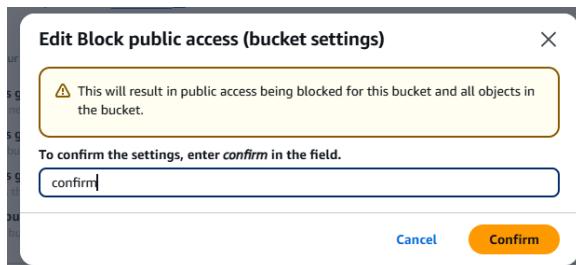
71. Select **Block all public access**.

72. Choose **Save changes**.

The screenshot shows the 'Edit Block public access (bucket settings)' page in the AWS S3 console. On the left, there's a sidebar with 'Amazon S3' and 'General purpose buckets' sections. The main area has a heading 'Edit Block public access (bucket settings)'. Underneath, it says 'Block public access (bucket settings)' and provides a detailed description. A checkbox labeled 'Block all public access' is checked. Below it are four other options with checkboxes: '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 are 'Cancel' and 'Save changes' buttons, with 'Save changes' being highlighted.

A message window titled Edit Block public access (bucket settings) is displayed.

- In the field of the message window, enter **confirm**.
- Choose **Confirm**.



A **Successfully edited Block Public Access settings for this bucket** message is displayed on top of the screen.

A page with all the bucket details is displayed.

The screenshot shows the 'lab-bucket-110648891' bucket details page in the AWS S3 console. The 'Permissions' tab is selected. In the 'Permissions overview' section, there's a note about access findings. The 'Block public access (bucket settings)' section shows that 'Block all public access' is turned 'On'. Below that, there's a link to 'Individual Block Public Access settings for this bucket'. The 'Bucket policy' section at the bottom is partially visible.

You have edited the S3 bucket policy so that the only principal allowed to read objects CloudFront distribution.

Task 5.3: Create a new origin with Origin Access Control (OAC)

In this task, you add the *lab-bucket-110648891* as a new origin to the existing CloudFront distribution.

- At the top of the console, in the search bar, search for and choose **CloudFront**.
- From the **CloudFront Distributions** page, choose the ID link for the only available distribution.

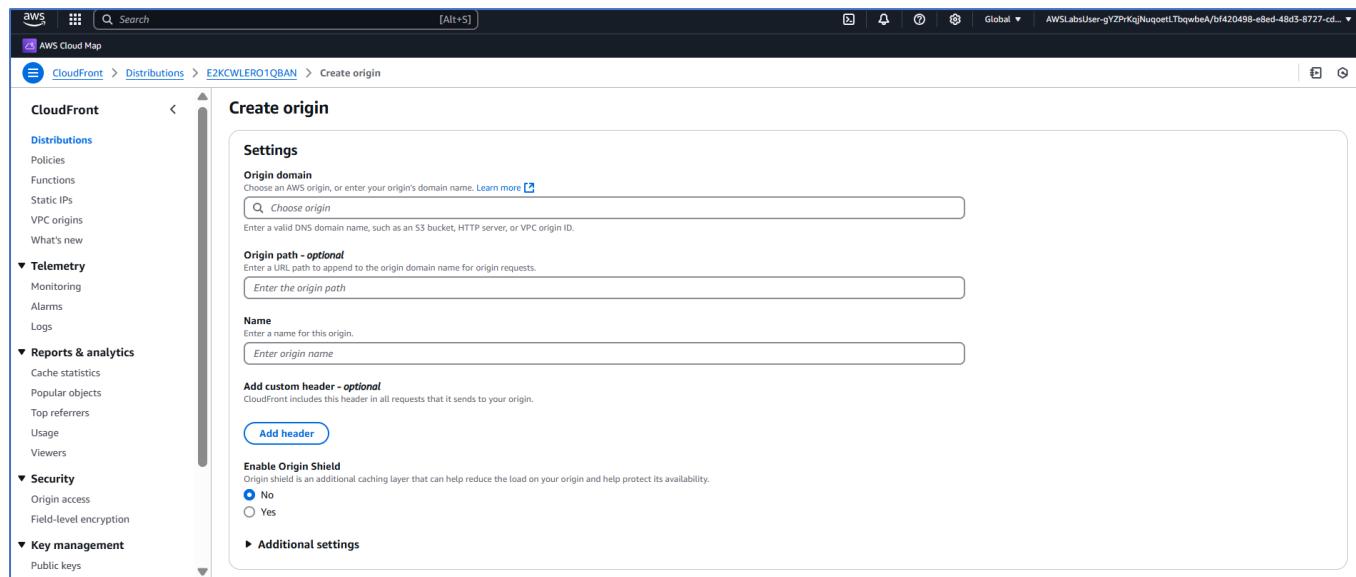
A page showing the details of the distribution is displayed.

The screenshot shows the AWS CloudFront Distributions page. On the left, there's a sidebar with options like CloudFront, Policies, Functions, Static IPs, and VPC origins. The main area has a title 'Distributions (1) Info' with a search bar. A table lists one distribution: E2KCWLERO1QBAN, which is Enabled, Production type, and uses domain d3dx8fymhiiu02.... Last modified was April 15, 2025, at 03:23. There are buttons for Enable, Disable, Delete, and Create distribution.

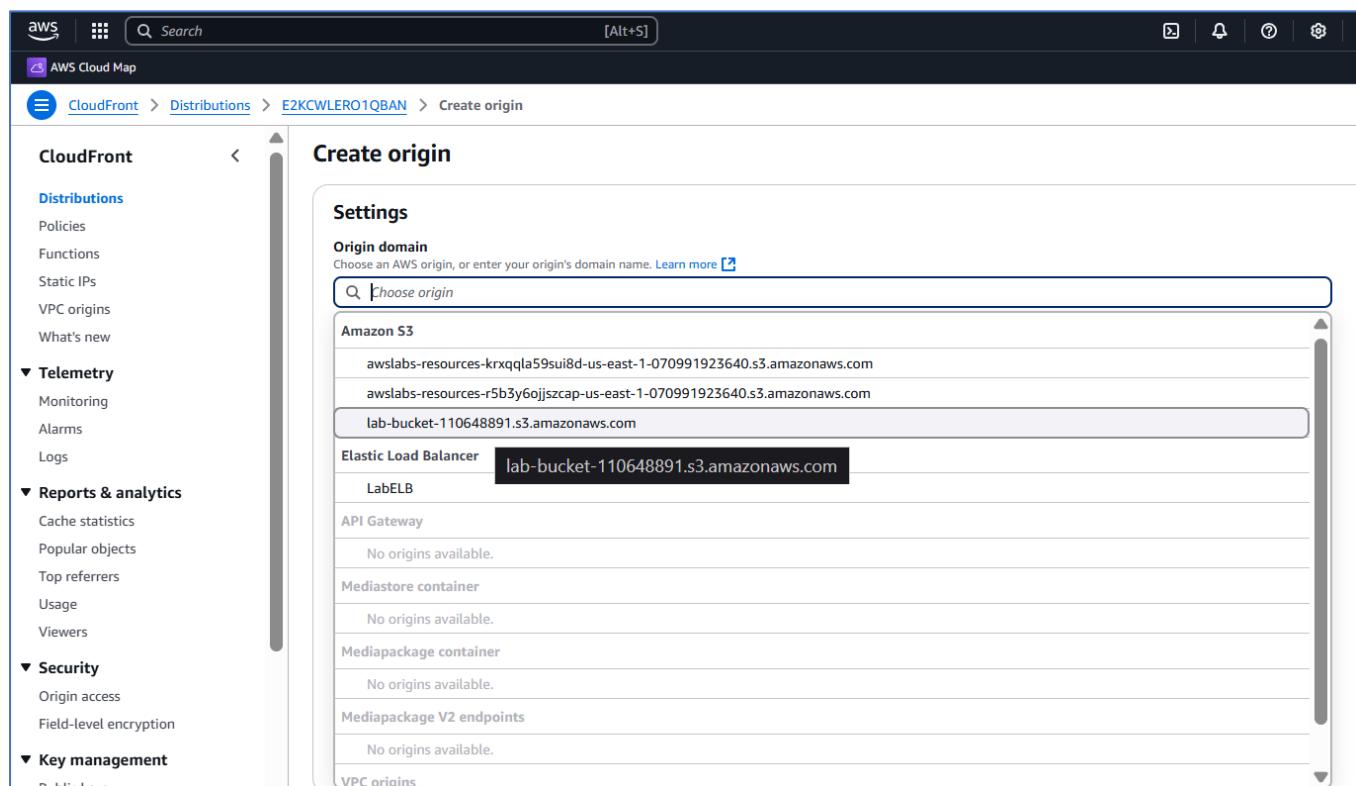
- Choose the **Origins** tab.
- Choose **Create origin**.

The screenshot shows the 'Origins' tab of the E2KCWLERO1QBAN distribution page. The sidebar includes sections for Distributions, Telemetry, Reports & analytics, and Security. The main area shows the 'Origins' section with a table for LabELBOrigin, which is an Elastic Load Balancing origin. It also shows the 'Origin groups' section, which is currently empty.

The **Create Origin** page is displayed.



- From the **Origin domain** field, choose the name of your *lab-bucket-110648891* from the **Amazon S3** section.



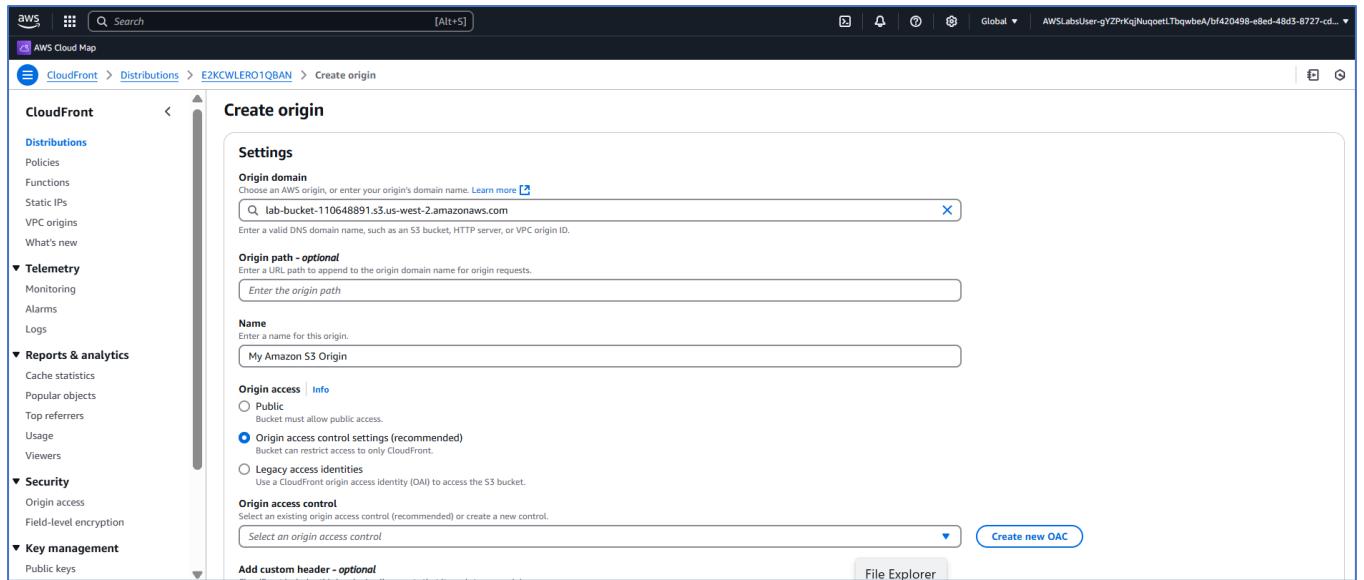
Note: Recall that the S3 bucket in this lab is never configured as a website. You have only changed the bucket policy regarding who is allowed to perform GetObject API requests against the S3 bucket into an *Allow Public* read policy.

- Leave the entry for **Origin path - optional** empty.

Note: The Origin Path field is optional and configures which directory in the origin CloudFront should forward requests to. In this lab, rather than configuring the origin

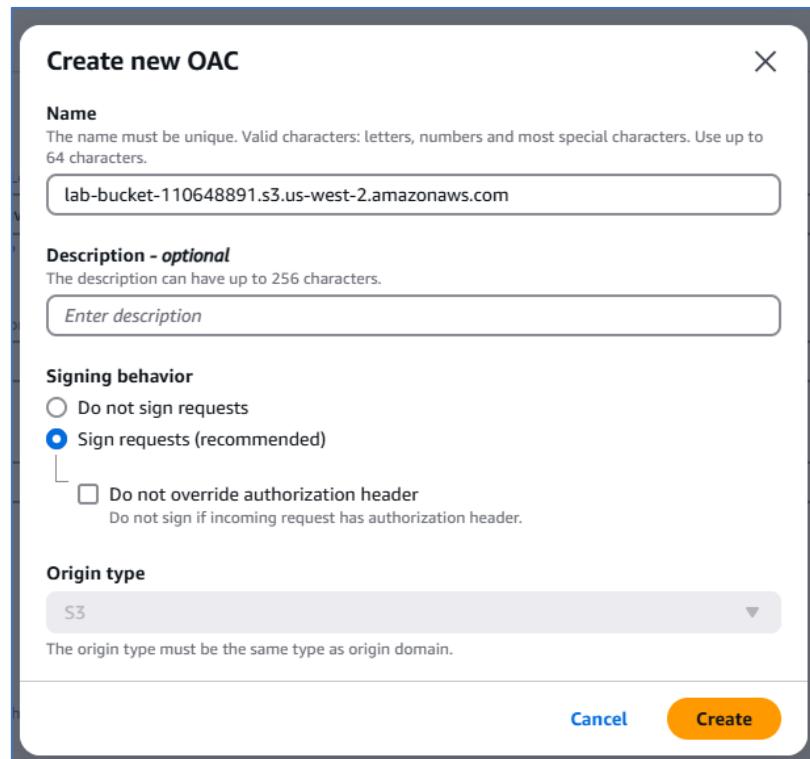
path, you leave it blank and instead configure a behavior to return only objects matching a specific pattern in the requests.

- For **Name**, enter **My Amazon S3 Origin**
- For **Origin access**, select **Origin access control settings (recommended)**.

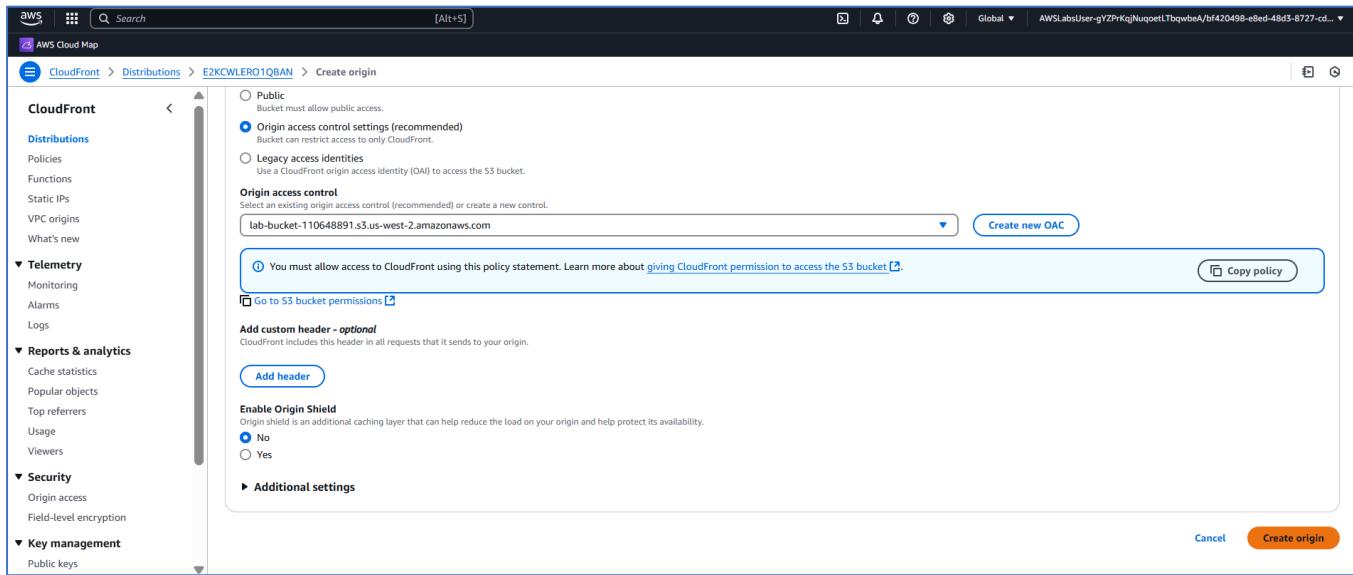


- Choose **Create new OAC**.

The console displays the **Create new OAC** message window.

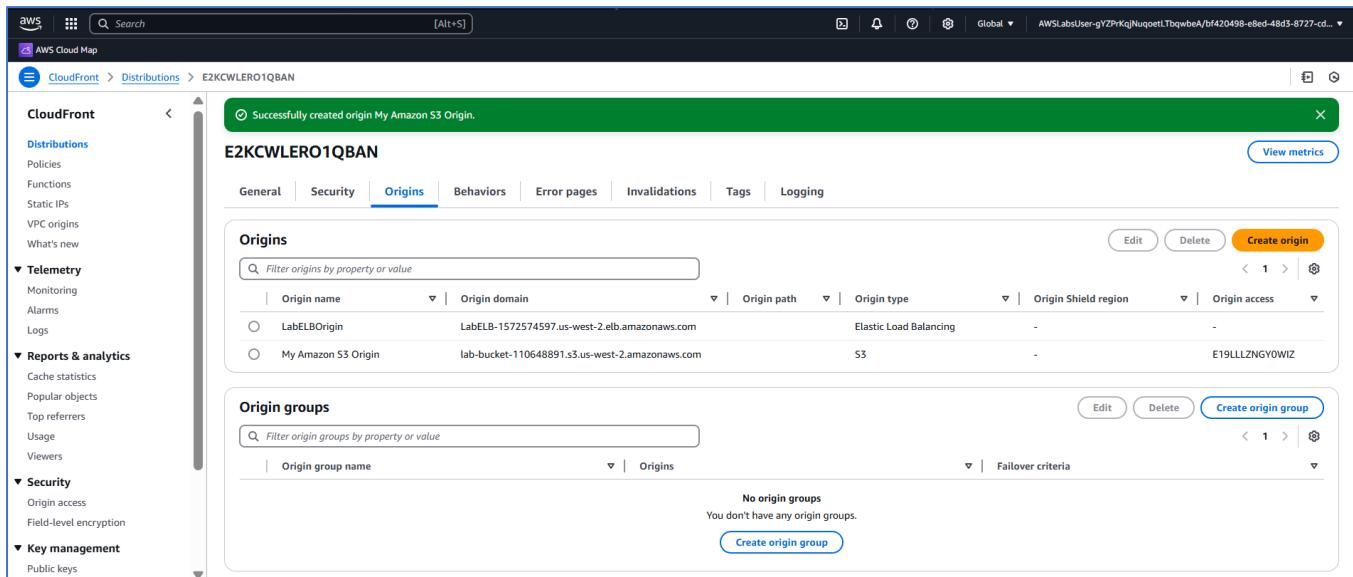


- Leave the default settings and choose **Create**.
- Choose **Create origin**.



A **Successfully created origin My Amazon S3 Origin** message is displayed on top of the screen.

You can safely ignore any message like, **The S3 bucket policy needs to be updated** as you completed updating the bucket policy already.



Task 5.4: Create a new behavior for the Amazon S3 origin

In this task, you create a new behavior for the Amazon S3 origin so that the distribution has instructions for how to handle incoming requests for the origin.

- Choose the **Behaviors** tab.

The screenshot shows the AWS CloudFront Behaviors page. The distribution ID 'E2KCWLERO1QBAN' is selected. The 'Behaviors' tab is active. There is one behavior named 'Default (*)' listed. The configuration includes the 'LabELBOrigin' origin group, 'HTTP and HTTPS' viewer protocol policy, and no cache or origin request policies.

- Choose **Create behavior**.

The **Create behavior** page is displayed.

The screenshot shows the 'Create behavior' page. In the 'Settings' section, the 'Path pattern' field contains '/images'. Under 'Viewer', the 'Viewer protocol policy' is set to 'HTTP and HTTPS' and the 'Allowed HTTP methods' are 'GET, HEAD'.

- In the **Path pattern** field, enter **CachedObjects/*.**.png****

This field configures which matching patterns of object requests the origin can return. Specifically, in this behavior only .png objects stored in the *CachedObjects* folder of the Amazon S3 origin can be returned. Unless there is a behavior configured for them, all other requests to the Amazon S3 origin would result in an error being returned to the requester. Typically, users would not be requesting objects directly from the CloudFront distribution URL in this manner; instead, your frontend application would generate the correct object URL to return to the user.

- From the **Origin and origin groups** dropdown menu, choose **My Amazon S3 Origin**.
- From the **Cache key and origin requests** section, ensure **Cache policy and origin request policy (recommended)** is selected.
- From the **Cache policy** dropdown menu, ensure **CachingOptimized** is selected.

Create behavior

Settings

Path pattern [Info](#)
 [X](#)

Origin and origin groups
My Amazon S3 Origin [▼](#)

Compress objects automatically [Info](#)
 No
 Yes

Viewer

Viewer protocol policy
 HTTP and HTTPS
 Redirect HTTP to HTTPS
 HTTPS only

Allowed HTTP methods
 GET, HEAD
 GET, HEAD, OPTIONS
 GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Restrict viewer access
If you restrict viewer access, viewers must use CloudFront signed URLs or signed cookies to access your content.
 No
 Yes

Cache key and origin requests
We recommend using a cache policy and origin request policy to control the cache key and origin requests.

Cache policy and origin request policy (recommended)
 Legacy cache settings

Cache policy
Choose an existing cache policy or create a new one.

CachingOptimized
Policy with caching enabled. Supports Gzip and Brotli compression. [Recommended for S3](#) [C](#)

[Create cache policy](#) [View policy](#)

- Leave all other settings on the page at the default values.
- Choose **Create behavior**.

Cache key and origin requests
We recommend using a cache policy and origin request policy to control the cache key and origin requests.

Cache policy and origin request policy (recommended)
 Legacy cache settings

Cache policy
Choose an existing cache policy or create a new one.

CachingOptimized
Policy with caching enabled. Supports Gzip and Brotli compression. [Recommended for S3](#) [C](#)

[Create cache policy](#) [View policy](#)

Origin request policy - optional
Choose an existing origin request policy or create a new one.

Response headers policy - optional
Choose an existing response headers policy or create a new one.

Function associations - optional [Info](#)
Choose an edge function to associate with this cache behavior, and the CloudFront event that invokes the function.

Function type	Function ARN / Name	Include body
Viewer request	No association	
Viewer response	No association	
Origin request	No association	
Origin response	No association	

[Cancel](#) [Create behavior](#)

A Successfully created new cache behavior CachedObjects/*.png. message is displayed on top of the screen.

The screenshot shows the AWS CloudFront Behaviors configuration page. The distribution ID is E2KCWLERO1QBAN. The Behaviors tab is selected. There are two entries:

Behavior ID	Path pattern	Origin or origin group	Viewer protocol policy	Cache policy name	Origin request policy name	Response header
0	CachedObjects/*.png	My Amazon S3 Origin	HTTP and HTTPS	Managed-CachingOptimized	-	-
1	Default (*)	LabELBOrigin	HTTP and HTTPS	-	-	-

You have created: a new origin for the Amazon S3 bucket, an Origin Access Control, and distribution behavior on a CloudFront distribution for the objects stored in the Amazon S3 bucket for the lab.

Task 6: Test direct access to a file in the bucket using the Amazon S3 URL

In this task, you test if the object can still be directly accessed using the Amazon S3 URL.

- At the top of the console, in the search bar, search for and choose **S3**.
- Select the link for the *lab-bucket-110648891* found in the **Buckets** section.

A page with all of the bucket details is displayed.

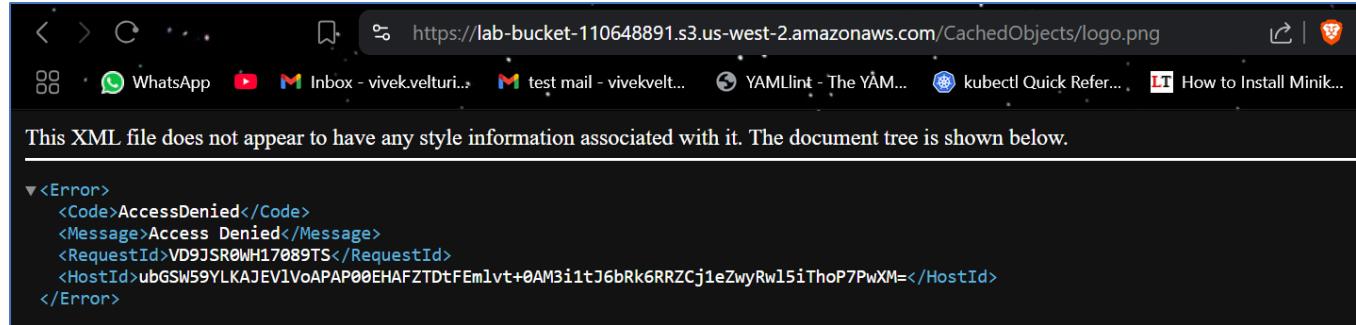
The screenshot shows the AWS S3 Bucket Details page for the bucket lab-bucket-110648891. The Objects tab is selected. There is one object listed:

Name	Type	Last modified	Size	Storage class
CachedObjects/	Folder	-	-	-

- Choose the **Objects** tab.
- Choose the link for the [CachedObjects/](#) folder.
- Choose the link for the [logo.png](#) object.
- Select the link located in the **Object URL** field.

An error message is displayed with Access denied messages. This is expected because the new bucket policy does not allow access to the object directly from Amazon S3 URLs. By denying access to S3 objects directly through Amazon S3,

users can no longer bypass the controls provided by CloudFront cache, which can include logging, behaviors, signed URLs, or signed cookies.



This screenshot shows a browser window with the URL <https://lab-bucket-110648891.s3.us-west-2.amazonaws.com/CachedObjects/logo.png>. The page content is an XML error document:

```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>VD9JSR0WH17089TS</RequestId>
<HostId>ubGSW59YLKAJEV1VoAPAP0EHAFTDtfEm1vt+0AM3i1tJ6bRk6RRZCj1eZwyRwl5iThoP7PwXM=</HostId>
</Error>
```

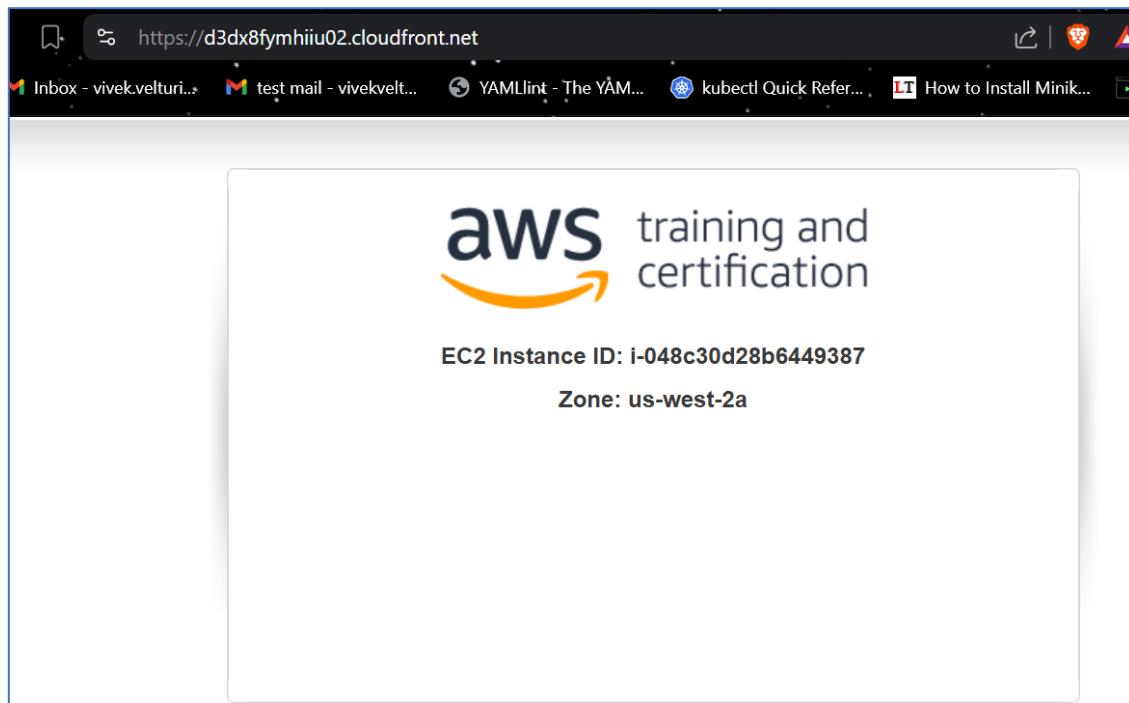
You have confirmed the object is no longer directly accessible from the Amazon S3 URL.

Task 7: Test access to the object in the bucket using the CloudFront distribution

In this task, you confirm that you can access objects in the Amazon S3 origin for the CloudFront distribution.

- **Copy edit:** Copy the CloudFront distribution's domain DNS value from the left side of these lab instructions under the listing *LabCloudFrontDistributionDNS*. (*d3dx8fymhiiu02.cloudfront.net*)
- Paste the DNS value into a new browser tab.

A simple web page is loaded displaying the information of the web server where CloudFront retrieved the content from.



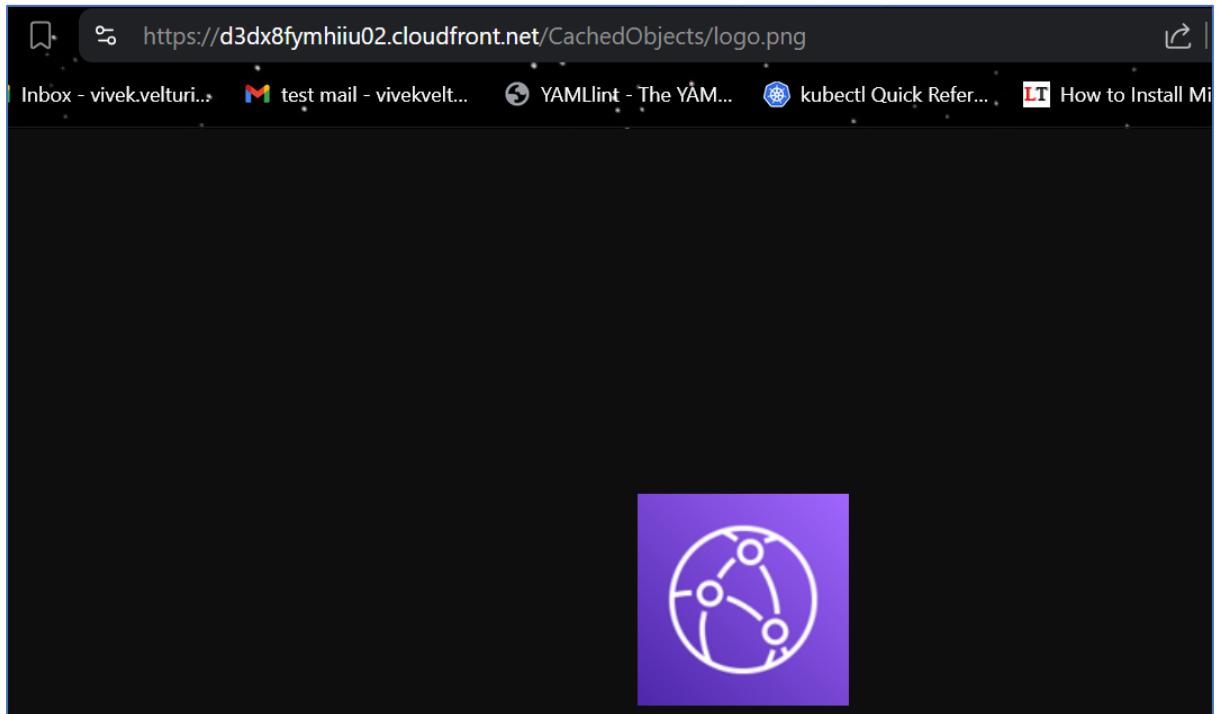
This screenshot shows a browser window with the URL <https://d3dx8fymhiiu02.cloudfront.net>. The page displays the AWS logo and the text "aws training and certification". Below that, it shows the EC2 Instance ID and Zone information:

aws training and certification

EC2 Instance ID: i-048c30d28b6449387

Zone: us-west-2a

- Append [/CachedObjects/logo.png](#) to the end of the CloudFront distribution's domain DNS and press **Enter**.



The browser makes a request to the CloudFront distribution and the object is returned from the Amazon S3 origin.

Hint: If the CloudFront URL redirects you to the Amazon S3 URL, or if the object isn't immediately available, the CloudFront distribution might still be updating from your recent changes. Return to the CloudFront console. Select **Distributions** from the navigation menu. Confirm that the Status column is **Enabled** and the Last modified column has a timestamp. You need to wait for this before testing the new origin and behavior. After you have confirmed the status of the distribution, wait a few minutes and try this task again.

You have confirmed that the object is returned from a CloudFront request.

Task 8: Replicate an S3 bucket across AWS Regions

Cross-Region replication is a feature of Amazon S3 that allows for automatic copying of your data from one bucket to another bucket located in a different AWS Region. It is a useful feature for disaster recovery. After the cross-Region replication feature is enabled for a bucket, every *new* object that you currently have read permissions for, which is created in the source bucket, is replicated into the destination bucket you define. This means that objects replicated to the destination bucket have the same names. Objects encrypted using an Amazon S3 managed encryption key are encrypted in the same manner as their source bucket.

To perform *Cross-Region replication*, you must enable object versioning for both the source and destination buckets. To maintain good data orderliness with versioning

enabled, you can deploy lifecycle policies to automatically archive objects to Amazon S3 Glacier or to delete the objects.

Task 8.1: Enable versioning on your source bucket

- Return to the browser tab open to the AWS Management Console.
- At the top of the console, in the search bar, search for and choose **S3**.
- Select the link for the **lab-bucket-110648891** found in the **Buckets** section.

A page with all the bucket details is displayed.

The screenshot shows the AWS S3 Bucket Details page for the bucket 'lab-bucket-110648891'. The left sidebar lists various S3 features like General purpose buckets, Directory buckets, Table buckets, etc. The main content area has tabs for Objects, Metadata, Properties, Permissions, Metrics, Management, and Access Points. The 'Objects' tab is active, showing a single object named 'CachedObjects/'. Below the table, there's a note about using Amazon S3 inventory to get a list of all objects in the bucket. The 'Properties' tab is highlighted in blue, indicating it's selected.

- Select the **Properties** tab.
- Locate the **Bucket Versioning** section.
- Choose **Edit**.

The **Edit Bucket Versioning** page is displayed.

- Select **Enable** for **Bucket Versioning**.
- Choose **Save changes**.

The screenshot shows the 'Edit Bucket Versioning' page for the 'lab-bucket-110648891'. The left sidebar includes 'Block Public Access settings for this account' and 'Storage Lens'. The main content area has a 'Bucket Versioning' section with a note explaining its purpose. It shows two radio buttons: 'Suspend' (unchecked) and 'Enable' (checked). A callout box points to a note: 'After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.' At the bottom right are 'Cancel' and 'Save changes' buttons.

Task 8.2: Create a destination bucket for cross-Region replication

- From the Amazon S3 navigation menu, choose **Buckets**.

- At the top of the screen, choose the drop-down next to the region you are in and choose the **SecondaryRegion** value (**us-east-1**)

This navigates you to the **SecondaryRegion** to create the bucket.

- Choose **Create bucket**.

The **Create bucket** page is displayed.

- In the **Bucket name** field, enter a unique bucket name (***optionalbucket-1992***).

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 One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name Info
optionalbucket-1992

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

- In the **Block Public Access settings for this bucket** section, unselect **Block all public access**.
- In the warning message, select **I acknowledge that the current settings might result in this bucket and the objects within becoming public**.

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- Block public access to buckets and objects granted through new access control lists (ACLS)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLS)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

⚠ Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Caution: You do not need to have public access enabled for your personal buckets to use the cross-Region replication feature. It is enabled in this lab so that you can quickly test if objects are replicated and retrievable using the Amazon S3 URL.

- For Bucket Versioning, select **Enable**.

The screenshot shows the 'Bucket Versioning' section of the 'Create bucket' page. 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.' Below this, there are two radio buttons: 'Disable' and 'Enable'. The 'Enable' button is selected and highlighted in blue.

- Choose **Create bucket**.

The screenshot shows the 'Default encryption' and 'Advanced settings' sections of the 'Create bucket' page. In the 'Default encryption' section, it says 'Server-side encryption is automatically applied to new objects stored in this bucket.' and lists three options: 'Server-side encryption with Amazon S3 managed keys (SSE-S3)' (selected), 'Server-side encryption with AWS Key Management Service keys (SSE-KMS)', and 'Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)'. In the 'Bucket Key' section, it says 'Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS.' and lists 'Disable' and 'Enable' options, with 'Enable' selected. The 'Advanced settings' section is collapsed. 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.

The **Amazon S3 console** is displayed.

The screenshot shows the 'Buckets' page. A green success message box says 'Successfully created bucket "optionalbucket-1992". To upload files and folders, or to configure additional bucket settings, choose View details.' Below this, there are tabs for 'General purpose buckets' (selected) and 'Directory buckets'. A search bar and filter buttons ('All AWS Regions') are at the top. A table lists four buckets: 'awslabs-resources-krxqqla59sui8d-us-east-1-070991923640', 'awslabs-resources-r5b3y6ojjszcap-us-east-1-070991923640', 'lab-bucket-110648891', and 'optionalbucket-1992'. Each row includes columns for Name, AWS Region, IAM Access Analyzer (with a 'View analyzer' link), and Creation date.

Name	AWS Region	IAM Access Analyzer	Creation date
awslabs-resources-krxqqla59sui8d-us-east-1-070991923640	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 6, 2022, 03:39:19 (UTC+05:30)
awslabs-resources-r5b3y6ojjszcap-us-east-1-070991923640	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 30, 2023, 22:30:12 (UTC+05:30)
lab-bucket-110648891	US West (Oregon) us-west-2	View analyzer for us-west-2	April 15, 2025, 16:07:57 (UTC+05:30)
optionalbucket-1992	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 15, 2025, 18:06:06 (UTC+05:30)

The newly created bucket is displayed among the list of all the buckets for the account.

Note: To simplify the narrative in this lab, this newly created bucket is referred to as the *optionalbucket-1992* in the remainder of instructions.

Task 8.3: Configure a public read policy for the new destination bucket

You now create a public object read policy for this bucket. You use the public read policy in this lab to demonstrate during the lab time that objects are replicated and retrievable using the Amazon S3 URL. It is not recommended for most use cases to use bucket policies which allow for public access.

- From the Amazon S3 navigation menu, choose **Buckets**.
- Choose the link for the *optionalbucket-1992* from the list of buckets.
- Choose the **Permissions** tab.
- Locate the **Bucket policy** section.
- Choose **Edit**.

The **Edit bucket policy** page is displayed.

- Copy edit:** Copy and paste the **Bucket ARN** value into a text editor to save the information for later. It is a string value like *arn:aws:s3:::LabBucket* located above the *Policy* box. (**arn:aws:s3:::optionalbucket-1992**)

The ARN value uniquely identifies this S3 bucket. You need this specific ARN value when creating bucket-based policies.

- File contents:** Copy and paste the following JSON into a text editor:

```
{
    "Version": "2012-10-17",
    "Id": "Policy1621958846486",
    "Statement": [
        {
            "Sid": "OriginalPublicReadPolicy",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "RESOURCE_ARN"
        }
    ]
}
```

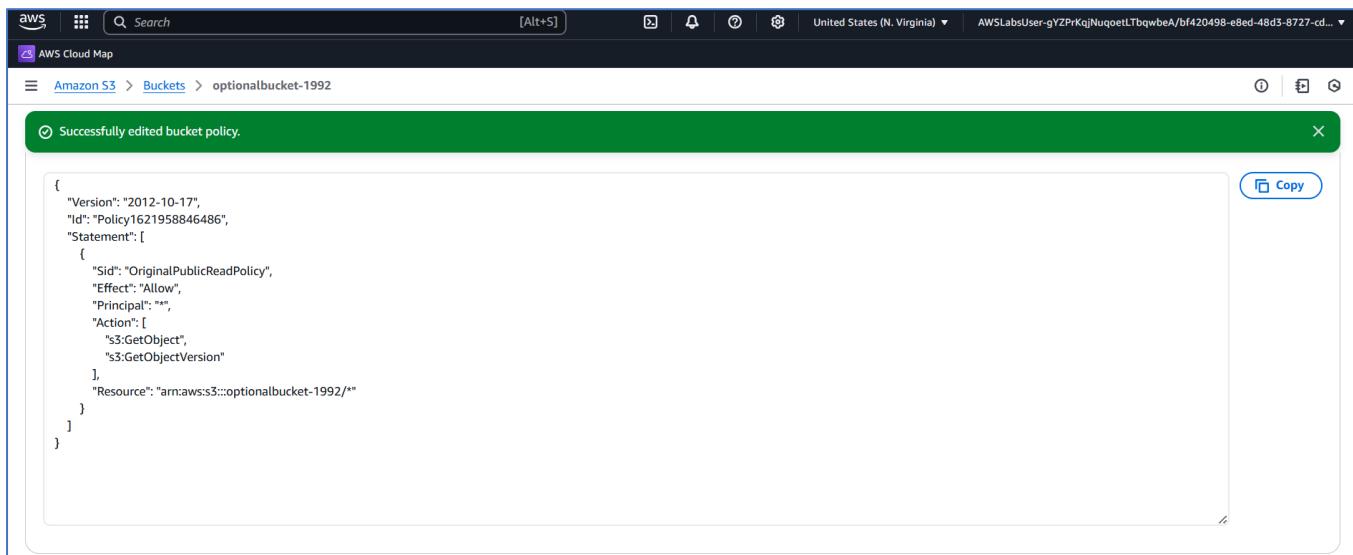
- Replace the **RESOURCE_ARN** value in the JSON with the **Bucket ARN** value you copied in a [previous step](#) and append a `/*` to the end of the pasted **Bucket ARN** value.

Here is the example of the updated policy JSON:

```
{
  "Version": "2012-10-17",
  "Id": "Policy1621958846486",
  "Statement": [
    {
      "Sid": "OriginalPublicReadPolicy",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::optionalbucket-1992/*"
    }
  ]
}
```

- Choose **Save changes**.

The **bucket details** page is displayed.



Note: The policies currently applied to the bucket make the objects in this bucket publicly readable.

Task 8.4: Create a replication rule

- From the Amazon S3 navigation menu, choose **Buckets**.
- In the **Buckets** section, choose the link for the *lab-bucket-110648891*.
- Choose the **Management** tab.

- Locate the **Replication rules** section.
- Choose **Create replication rule**.

The **Create replication rule** page is displayed.

- In the **Replication rule name** field, enter **MyCrossRegionReplication**
- Verify that *lab-bucket-110648891* is set for **Source bucket name**. If it is not, then you chose the incorrect bucket before choosing the replication rules.
- In the **Choose a rule scope** section, select **Apply to all objects in the bucket**.

Create replication rule Info

Replication rule configuration

Replication rule name
MyCrossRegionReplication
Up to 255 characters. In order to be able to use CloudWatch metrics to monitor the progress of your replication rule, the replication rule name must only contain English characters.

Status
Choose whether the rule will be enabled or disabled when created.
 Enabled
 Disabled

Priority
The priority value resolves conflicts that occur when an object is eligible for replication under multiple rules to the same destination. The rule is added to the configuration at the highest priority and the priority can be changed on the replication rules table.
0

Source bucket

Source bucket name
lab-bucket-110648891

Source Region
US West (Oregon) us-west-2

Choose a rule scope
 Limit the scope of this rule using one or more filters
 Apply to all objects in the bucket

- Locate the **Destination** section.
- Choose **Browse S3**.

Destination

You can replicate objects across buckets in different AWS Regions (Cross-Region Replication) or you can replicate objects across buckets in the same AWS Region (Same-Region Replication). You can also specify a different bucket for each rule in the configuration. [Learn more](#) or see [Amazon S3 pricing](#).

Choose a bucket in this account
 Specify a bucket in another account

Bucket name
Choose the bucket that will receive replicated objects.
 Browse S3

Destination Region
-

- Select the **optionalbucket-1992**.
- Select **Choose path**.

Choose a bucket

S3 Buckets

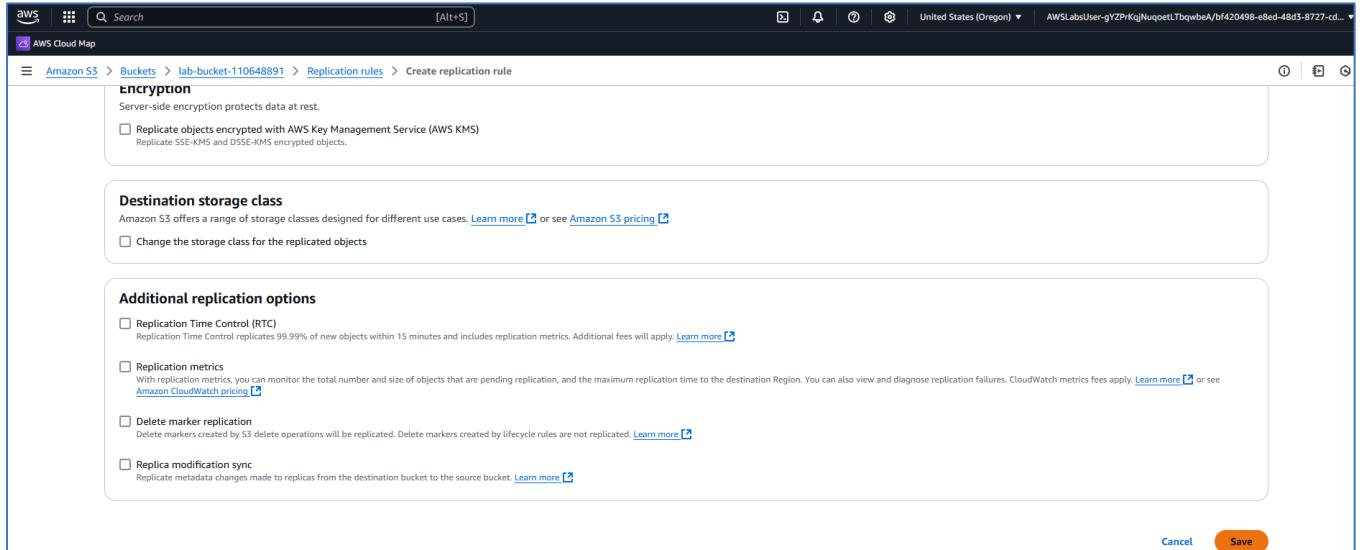
Buckets (1/4)

Name	AWS Region
awslabs-resources-krxqlq59su8d-us-east-1-070991923640	US East (N. Virginia) us-east-1
awslabs-resources-r5b3y6ojjszcap-us-east-1-070991923640	US East (N. Virginia) us-east-1
lab-bucket-110648891	US West (Oregon) us-west-2
optionalbucket-1992	US East (N. Virginia) us-east-1

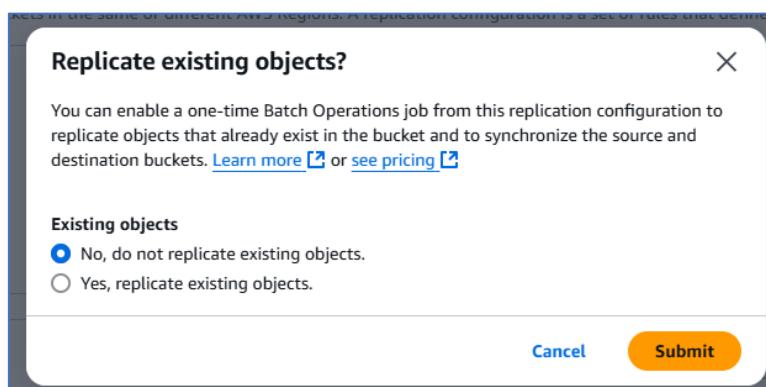
Choose path

- Locate the **IAM Role** section.

- Select **Create new role**.
- Leave all other options as their default selection.
- Choose **Save**.



- If the Replicate existing objects window is displayed, select **No, do not replicate existing objects** then choose **Submit**.



The **Replication rules** page for the *lab-bucket-110648891* is displayed.

A **Replication configuration successfully updated** If changes to the configuration aren't displayed, choose the refresh button. Changes apply only to new objects. To replicate existing objects with this configuration, choose **Create replication job**. message is displayed on top of the screen.

All newly created objects in the *lab-bucket-110648891* are replicated into the DestinationBucket.

Note: It is possible to replicate existing objects between buckets, but that is beyond the scope of this lab. You can find more information about this topic in the document linked in the Appendix section.

Task 8.5: Verify object replication

- From the Amazon S3 navigation menu, choose **Buckets**. You might need to expand the menu by choosing the menu icon.
- In the **Buckets** section, choose the link for the *lab-bucket-110648891*.
- Download the object for these lab instructions by right-clicking [logo2.png](#) and saving it to your local device.
- Return to the **Amazon S3** console.
- Choose the link for the [CachedObjects/](#) folder.

Note: If you do not find the **CachedObjects** folder, choose **Buckets** from the navigation menu located on the left side of the console. Then choose the link for the *lab-bucket-110648891* from the list. Finally, choose the **Objects** tab to ensure that you are at the correct page.

- Choose **Upload**.

The **Upload** page is displayed.

The screenshot shows the AWS S3 'Upload' page. At the top, there's a header with the AWS logo, search bar, and account information ('United States (Oregon) AWSLabsUser-gY2PrKqjNuqoetLTbqwbea/bf420498-e8ed-48d3-8727-cd...'). Below the header, the breadcrumb navigation shows 'Amazon S3 > Buckets > lab-bucket-110648891 > CachedObjects/ > Upload'. The main content area has three main sections: 'Upload Info' (with a note about file size limits), 'Files and folders (0)' (empty table with columns for Name, Folder, Type, and Size), and 'Destination Info' (specifying the destination as 's3://lab-bucket-110648891/CachedObjects/'). There's also a 'Permissions' section.

- Choose **Add files**.
- Choose the **logo2.png** object from your local storage location.
- Choose **Upload**.

The **Upload: status** page is displayed.

A **Upload succeeded** message is displayed on top of the screen.

The screenshot shows the 'Upload: status' page. A prominent green banner at the top says 'Upload succeeded' with a link to 'See more information'. Below this, the title 'Upload: status' is shown with a note that the information will be lost after navigating away. The 'Summary' section shows the destination 's3://lab-bucket-110648891/CachedObjects/' and a table with two rows: 'Succeeded' (1 file, 13.9 KB (100.00%)) and 'Failed' (0 files, 0 B (0%)). The 'Files and folders' section shows a table with one entry: 'logo2.png' (image/png, 13.9 KB, Status: Succeeded).

- Choose the link for the **logo2.png** from the **Files and folders** section.

A page with details about the Amazon S3 object is displayed.

The screenshot shows the AWS S3 Object Properties page for an object named 'logo2.png'. The object was last modified on April 15, 2025, at 18:32:46 UTC+05:50. It has a size of 13.9 kB and is of type png. The key is 'CachedObjects/logo2.png'. The 'Object management overview' section indicates that replication status is 'PENDING' and refreshes periodically until it changes to 'COMPLETED'. The 'Bucket properties' section shows that Bucket Versioning is enabled. The 'Management configurations' section shows that replication rules are pending completion.

- In the **Object management overview** section, examine *Replication status* and refresh the page periodically until it changes from *PENDING* to *COMPLETED*.

This screenshot shows the 'Object management overview' page for the same object. It highlights the 'Bucket properties' section, which shows that Bucket Versioning is enabled. The 'Management configurations' section shows replication rules pending completion and an expiration rule scheduled for April 15, 2025.

- From the Amazon S3 navigation menu, select **Buckets**.
- In the **Buckets** section, choose the link for the *optionalbucket-1992*.

A page with all the bucket details is displayed.

The screenshot shows the 'optionalbucket-1992' bucket details. The left sidebar lists 'General purpose buckets' such as Directory buckets, Table buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and IAM Access Analyzer for S3. The main content area shows one object named 'CachedObjects/'. The object was last modified on April 15, 2025, at 18:32:46 UTC+05:50, and its storage class is Standard.

- Choose the link for the *CachedObjects/* folder.
- Choose the link for the *logo2.png*.

A page with details about the Amazon S3 object is displayed.

The screenshot shows the AWS S3 console. The left sidebar shows 'Amazon S3' with 'General purpose buckets' expanded, listing 'Directory buckets', 'Table buckets', 'Access Grants', 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', and 'IAM Access Analyzer for S3'. Below this is a section for 'Block Public Access settings for this account'. Under 'Storage Lens', 'Dashboards', 'Storage Lens groups', and 'AWS Organizations settings' are listed. The main content area shows the details for an object named 'logo2.png' in the bucket 'optionalbucket-1992'. The 'Properties' tab is selected. The 'Object overview' section contains the following information:

Key	Value
Owner	aws-labs-accounts+prodkiku-mAAFznTDSuvKTzbSckDqRJ
AWS Region	US East (N. Virginia) us-east-1
Last modified	April 15, 2025, 18:32:46 (UTC+05:30)
Size	13.9 KB
Type	png
Key	CachedObjects/logo2.png

Below the properties are buttons for 'Copy S3 URI', 'Download', 'Open', and 'Object actions'.

- In the **Object management overview** section, examine *Replication Status*. It displays **REPLICA**.

The screenshot shows the 'Object management overview' page for the same object. The left sidebar is identical to the previous screenshot. The main content area shows the following details:

Key	Value
Bucket	optionalbucket-1992
Key	CachedObjects/logo2.png

The 'Object management overview' section includes a note: 'The following bucket properties and object management configurations impact the behavior of this object.' It then splits into two columns: 'Bucket properties' and 'Management configurations'.

Bucket properties:

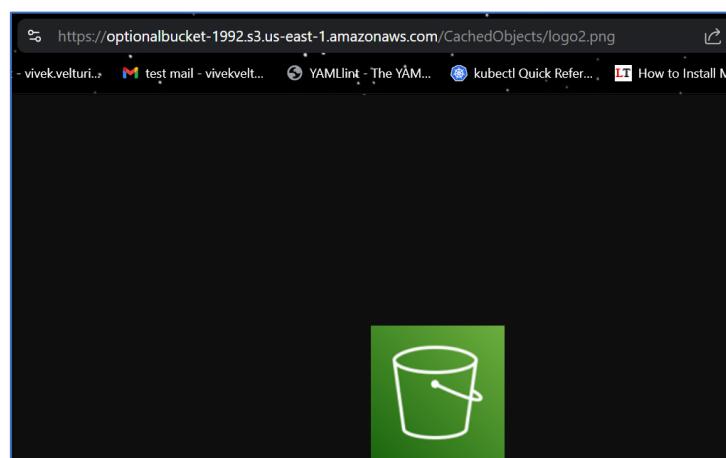
- Bucket Versioning:** When enabled, multiple variants of an object can be stored in the bucket to easily recover from unintended user actions and application failures. Status: Enabled.

Management configurations:

- Replication status:** When a replication rule is applied to an object, the replication status indicates the progress of the operation. Status: REPLICA. Link: View replication rules.
- Expiration rule:** You can use a lifecycle configuration to define expiration rules to schedule the removal of this object after a pre-defined time period. -
- Expiration date:** The object will be made noncurrent and generate a delete marker on this date. -

- Choose the link located in the **Object URL** field.

The picture is displayed in a browser tab.



You have completed setting up cross-Region replication for all new objects uploaded into the *lab-bucket-110648891*.

Conclusion

You now have successfully done the following:

- Created an S3 bucket with default security settings.
- Configured an S3 bucket for public access.
- Added an S3 bucket as a new origin to an existing CloudFront distribution.
- Secured an S3 bucket to allow access only through the CloudFront distribution.
- Configured OAC to lock down security to an S3 bucket.
- Configured Amazon S3 resource policies for public or OAC access.