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

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.

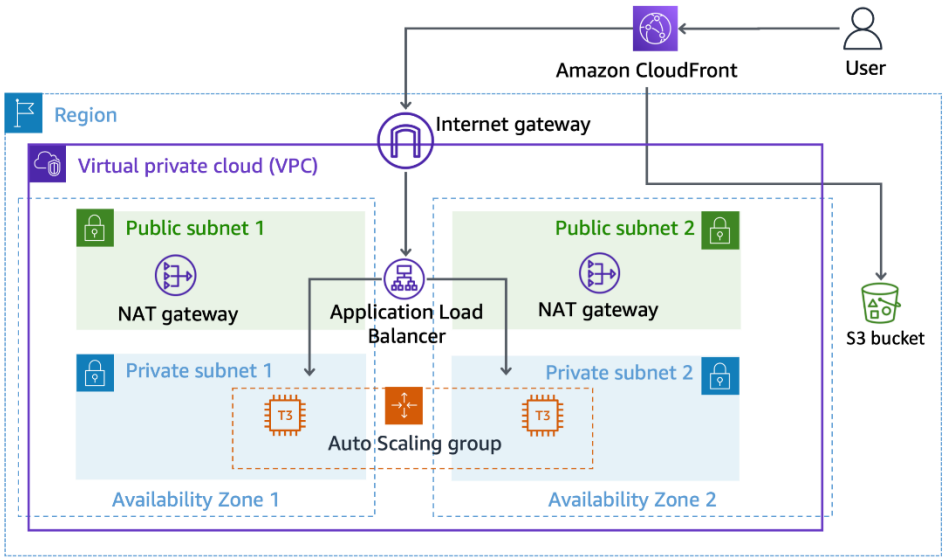


Image description: The preceding diagram depicts an environment with an Amazon VPC for secure and isolated connections between services. To decrease latency it has Amazon CloudFront to facilitate a CDN (Content-Delivery-Network) as a service for faster upload and download speeds, this connects to an 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

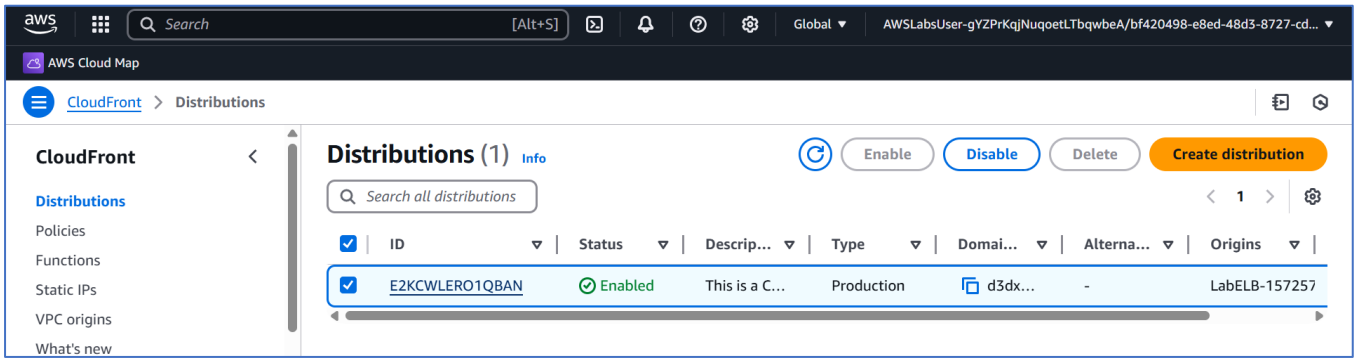
In this task, you examine the existing CloudFront distribution that was built for web server content. Before making changes to an environment, it is a good practice to understand the existing configuration. If you want to use CloudFront distributions for your personal AWS environments, you need to build 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.



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.

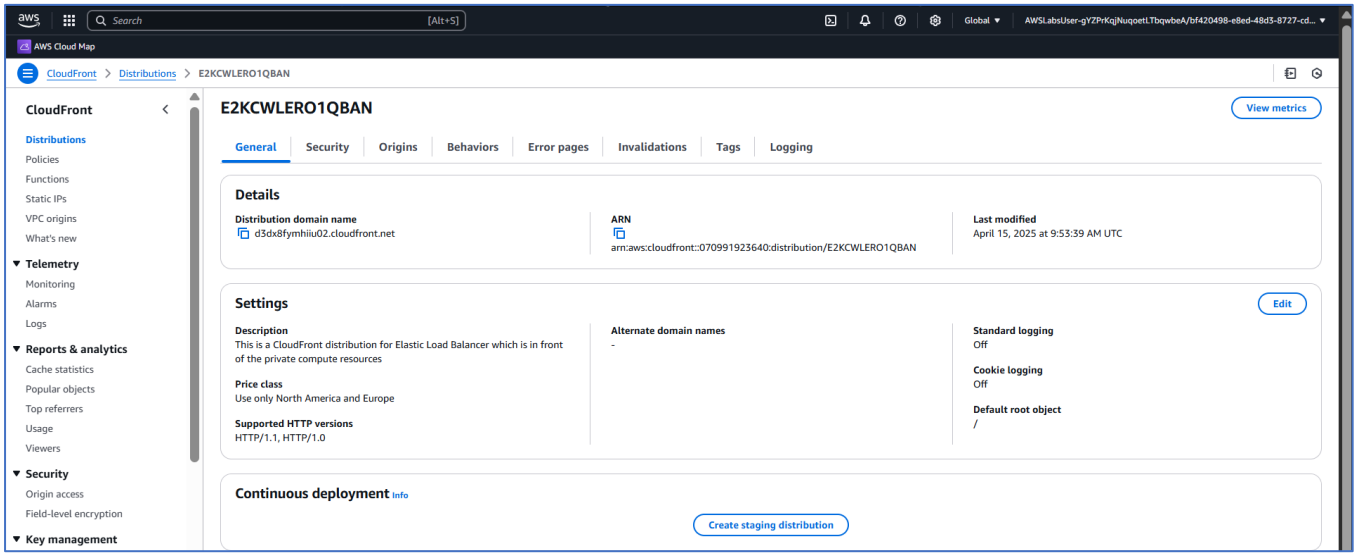
- Examine the contents of the **General** tab.

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.

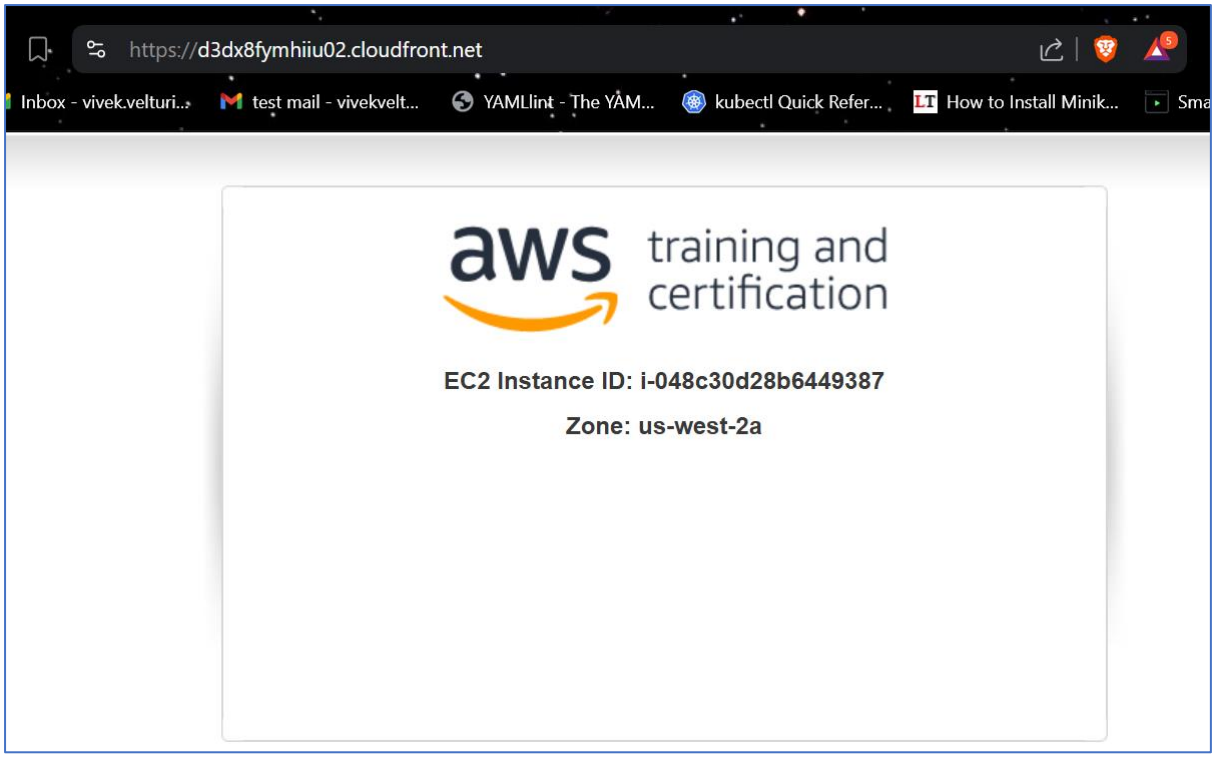
- **Copy edit:** From the **Details** section, in the **General** tab, copy the **Distribution domain name** value.

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



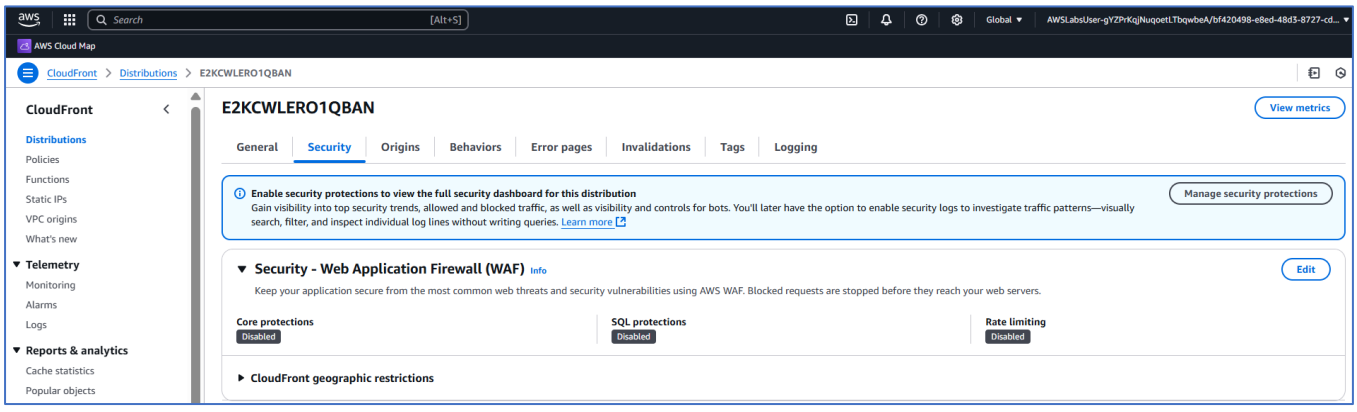
- Paste the **Distribution domain value** you copied into a new browser tab.

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.

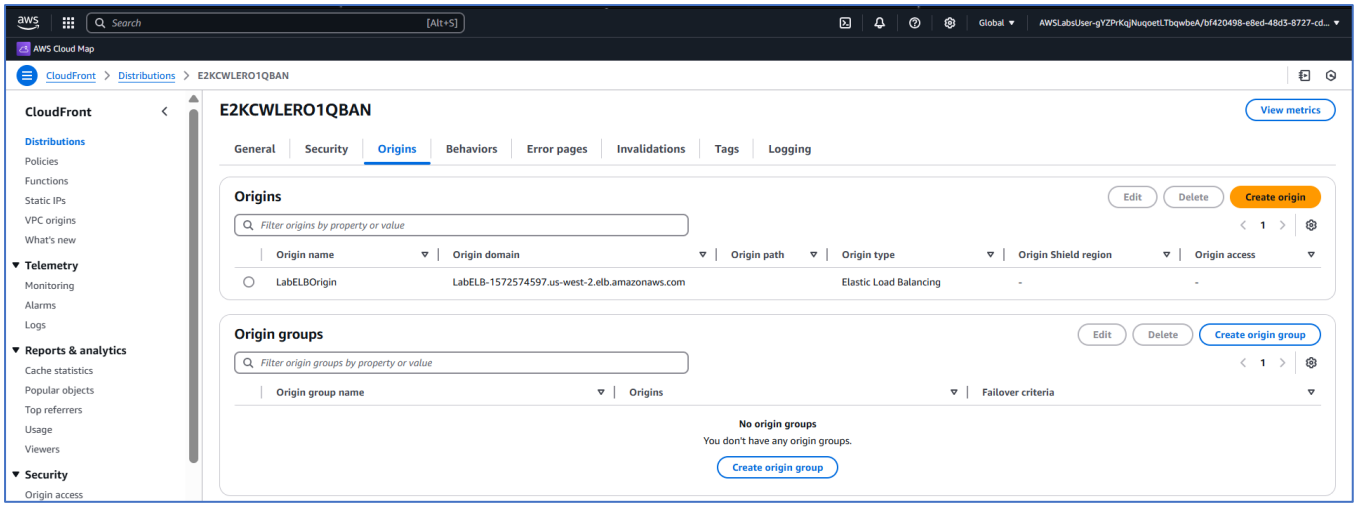
- Return to the **CloudFront** console.
- Choose the **Security** tab.



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.

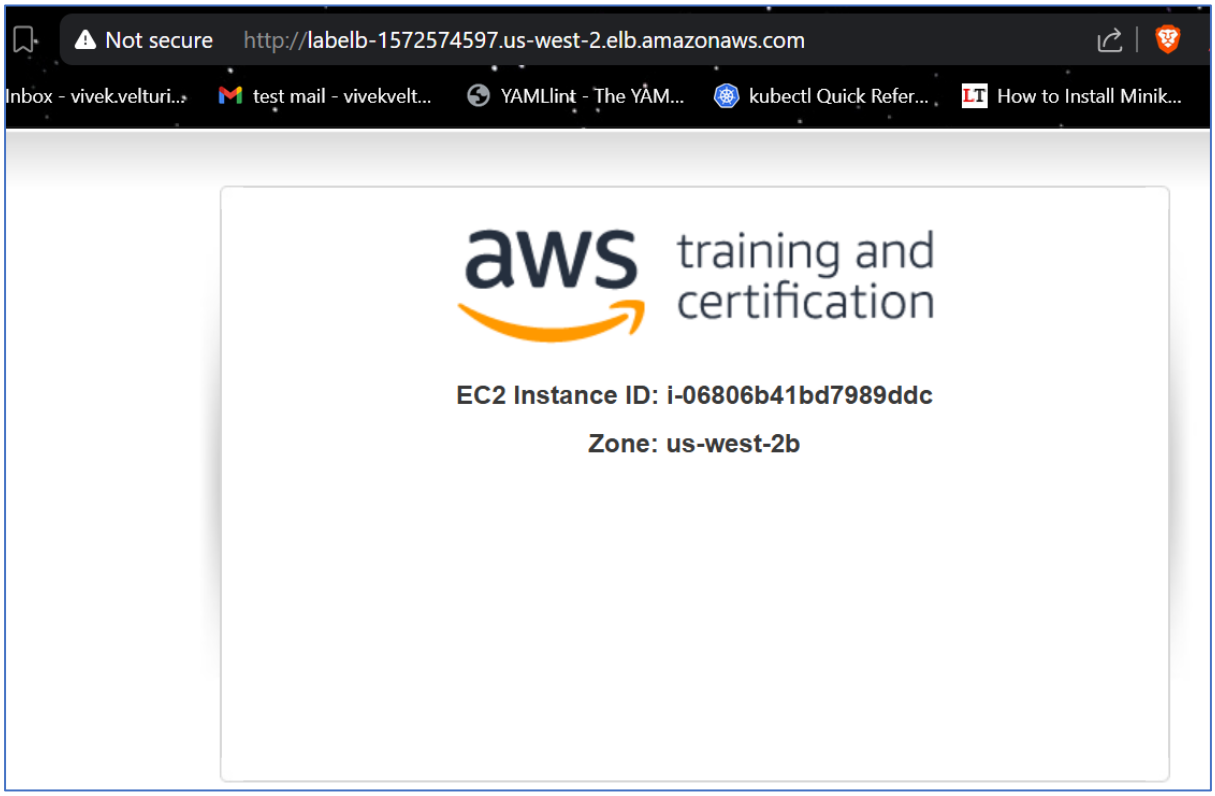


Note: The only origin currently on the distribution is an ELB load balancer. This load balancer is accepting and directing web traffic for the auto scaling web servers in its target group.

- **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.



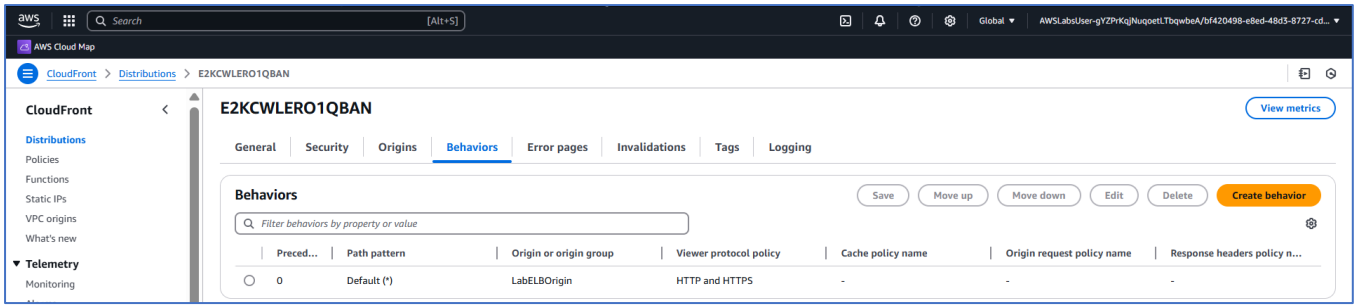
The DNS value for this distribution is also found to the left of these lab instructions under the listing *LabLoadBalancerDNS*.

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.

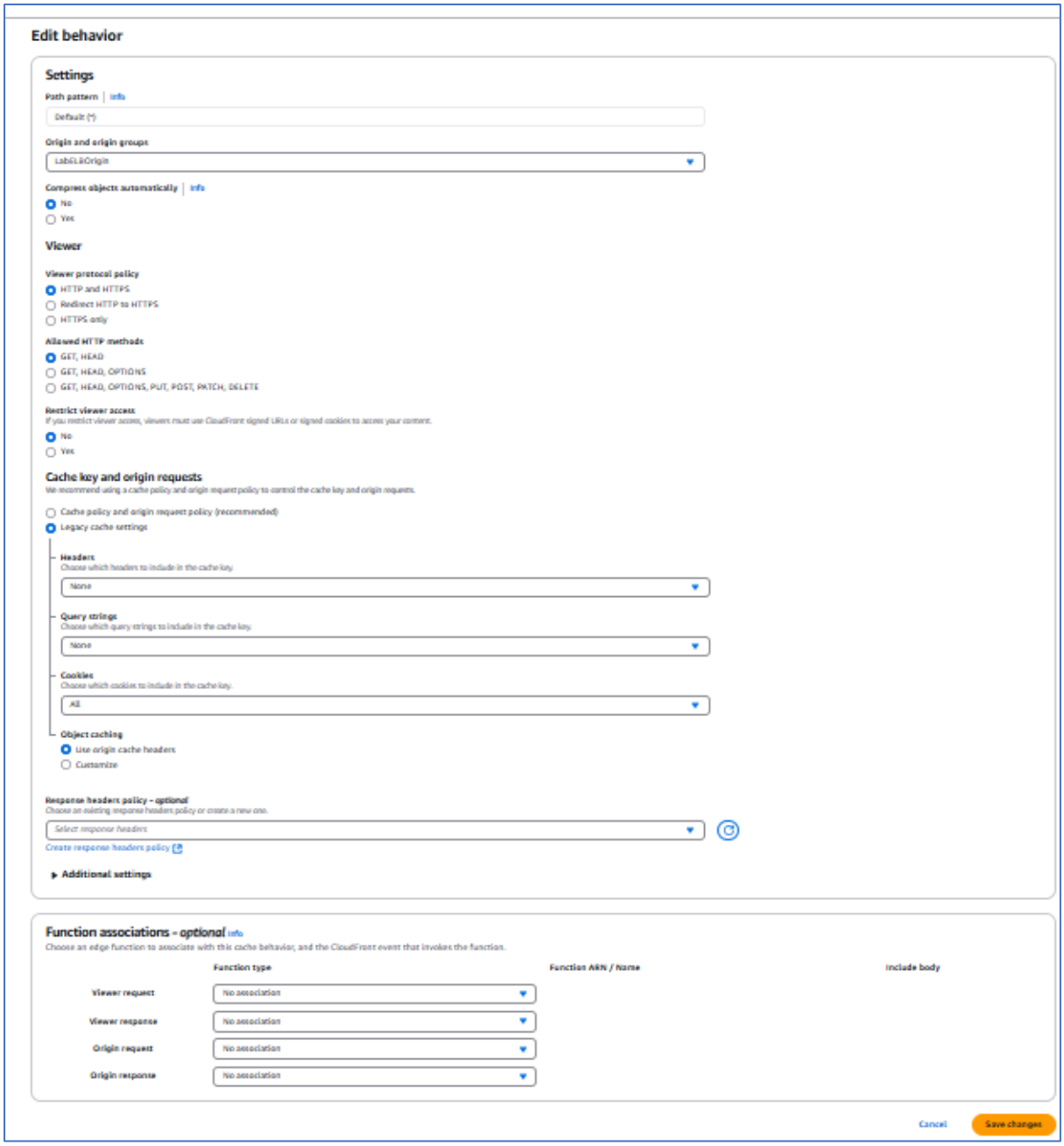


Behaviors define the actions that the CloudFront distribution takes when there is a request for content, such as which origin to serve which content, Time To Live of content in the cache, cookies, and how to handle various headers.

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:

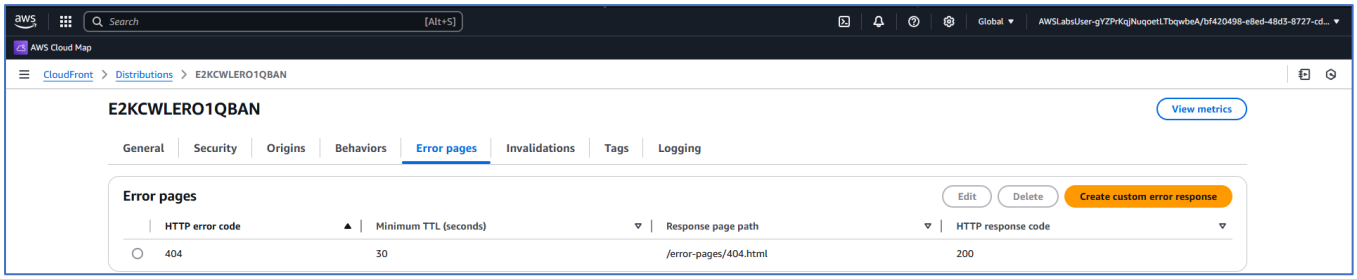
- Select the radio button in the row next to the behavior you want to modify.
- Choose **Edit**.
- Choose **Cancel** to close the page and return to the console.



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.

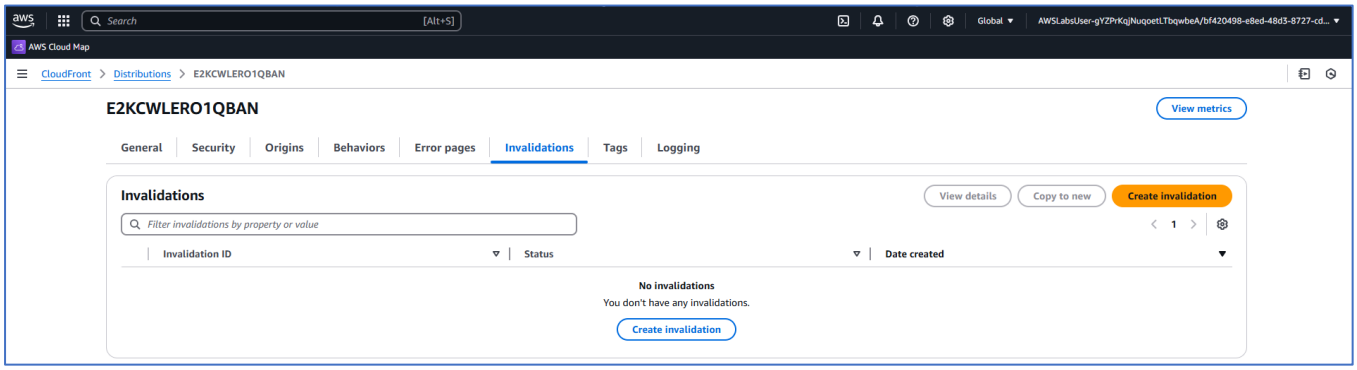
- Choose the **Error Pages** tab.

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.



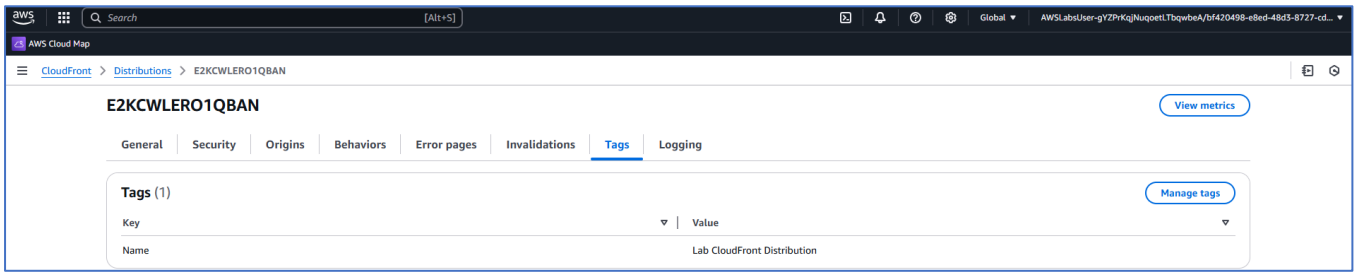
- Choose the **Invalidations** tab.

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.



- 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.



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**.

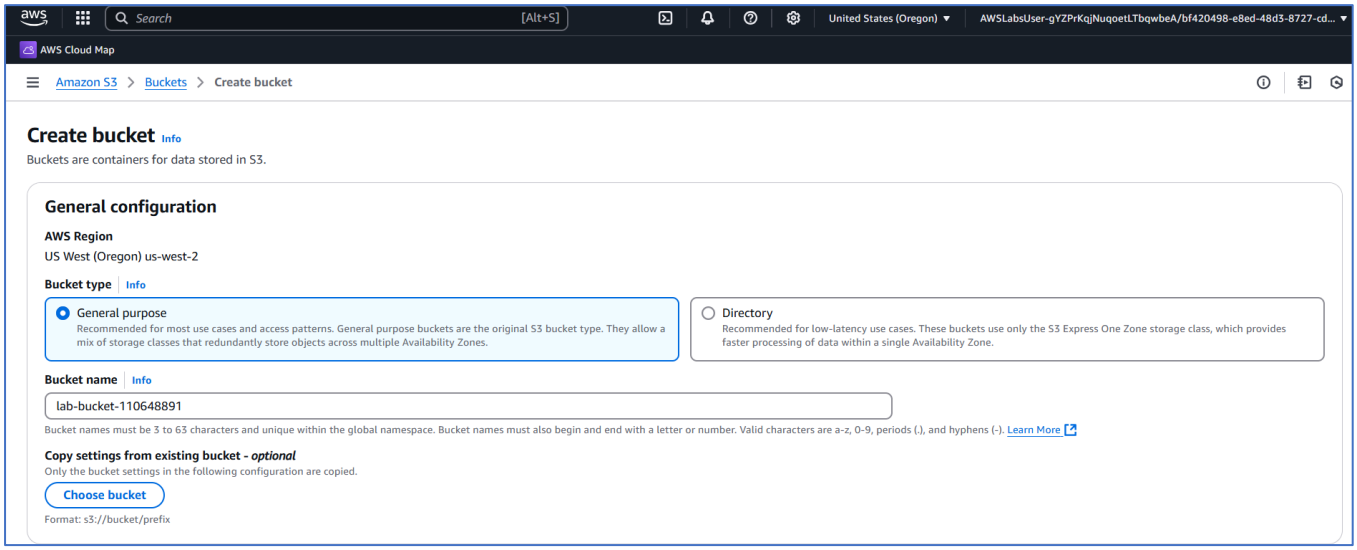
Note: If you do not find the Create bucket button, ensure you are at the correct page. Choose **Buckets** from the navigation menu located on the left side of the console.

The **Create bucket** page is displayed.

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

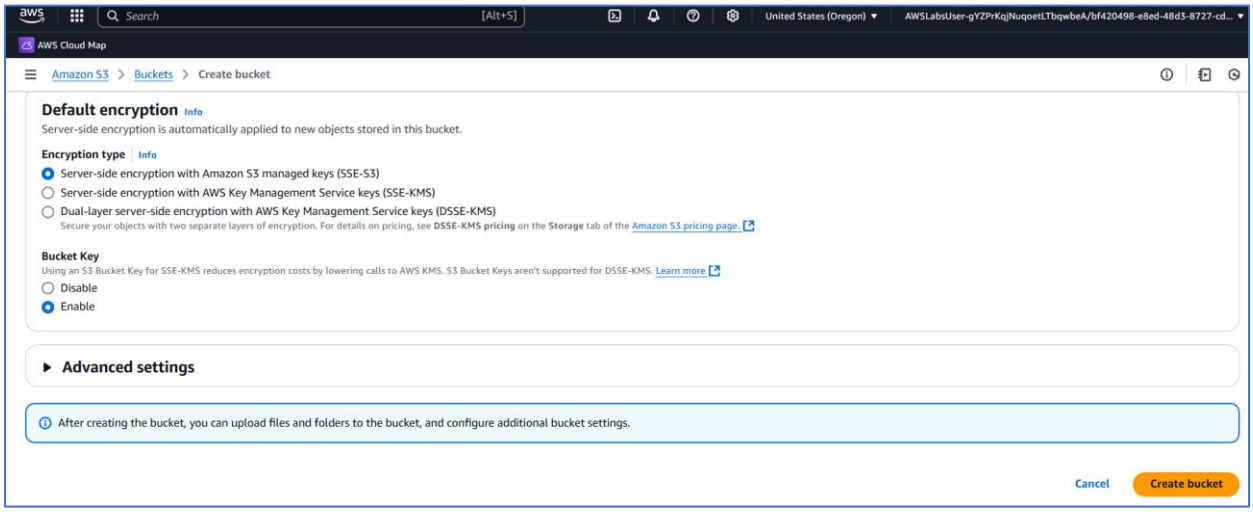
Note: To simplify the written instructions in this lab, this newly created bucket is referred to as the *LabBucket* for the remainder of the instructions.

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



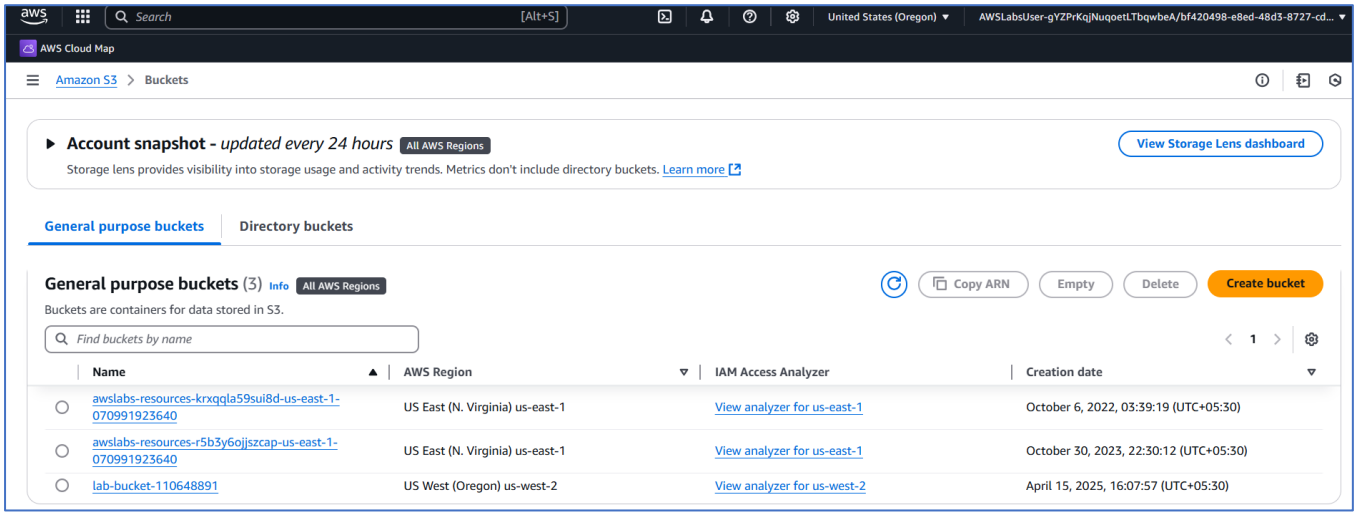
- Leave all other settings on this page as the default configurations.

- Choose **Create bucket**.



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.



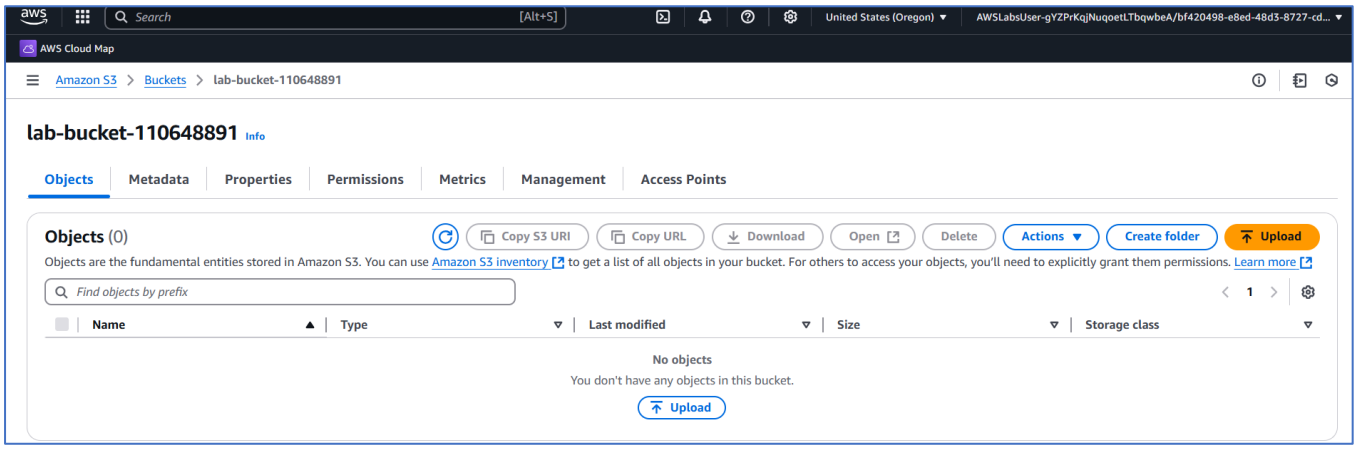
Task 3: Configure the S3 LabBucket for public access

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.

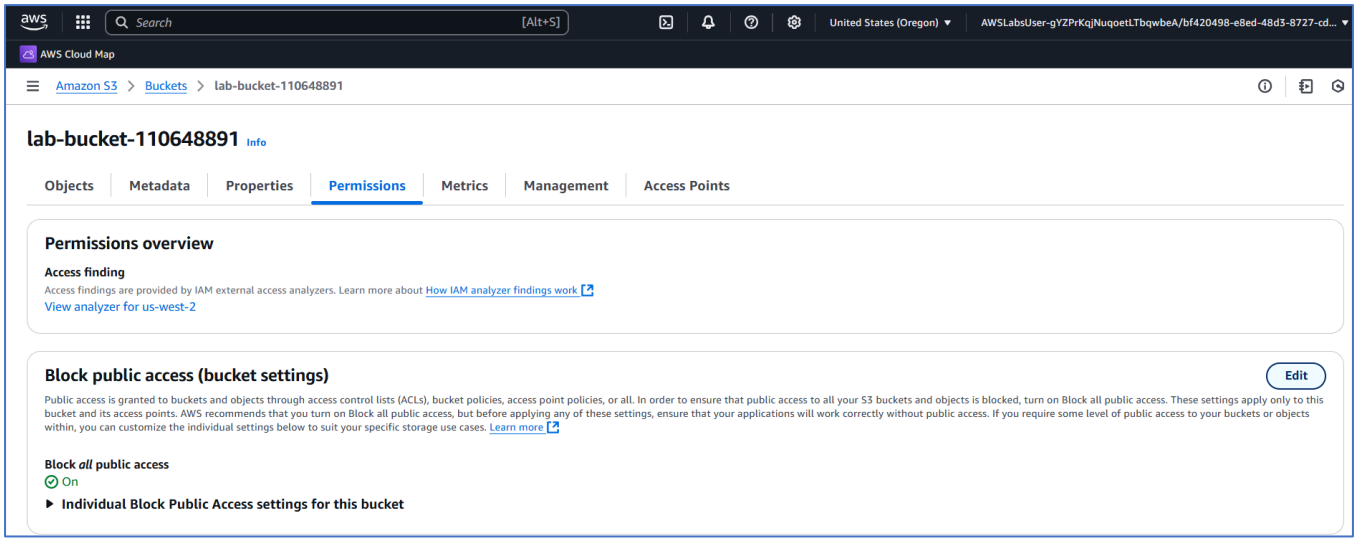
Task 3.1: Configure the LabBucket to allow public policies to be created

- 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.

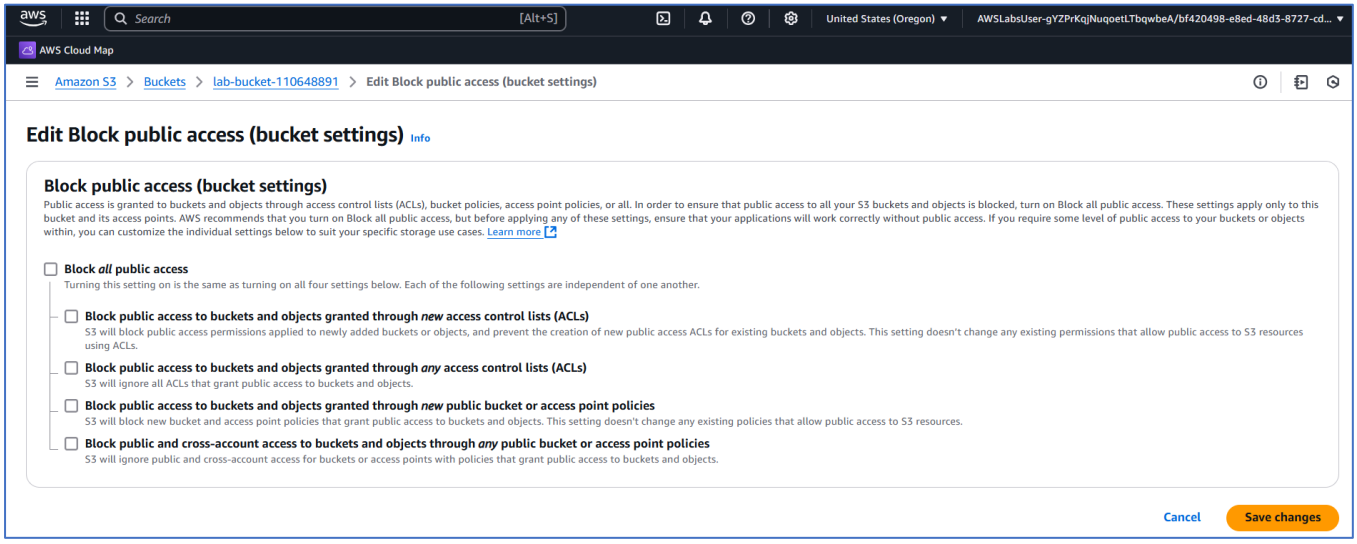


- Choose the **Permissions** tab.
- Locate the **Block public access (bucket settings)** section.
- Choose **Edit**.



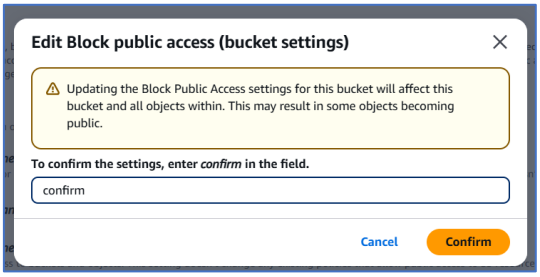
The **Edit Block public access (bucket settings)** page is displayed.

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



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

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



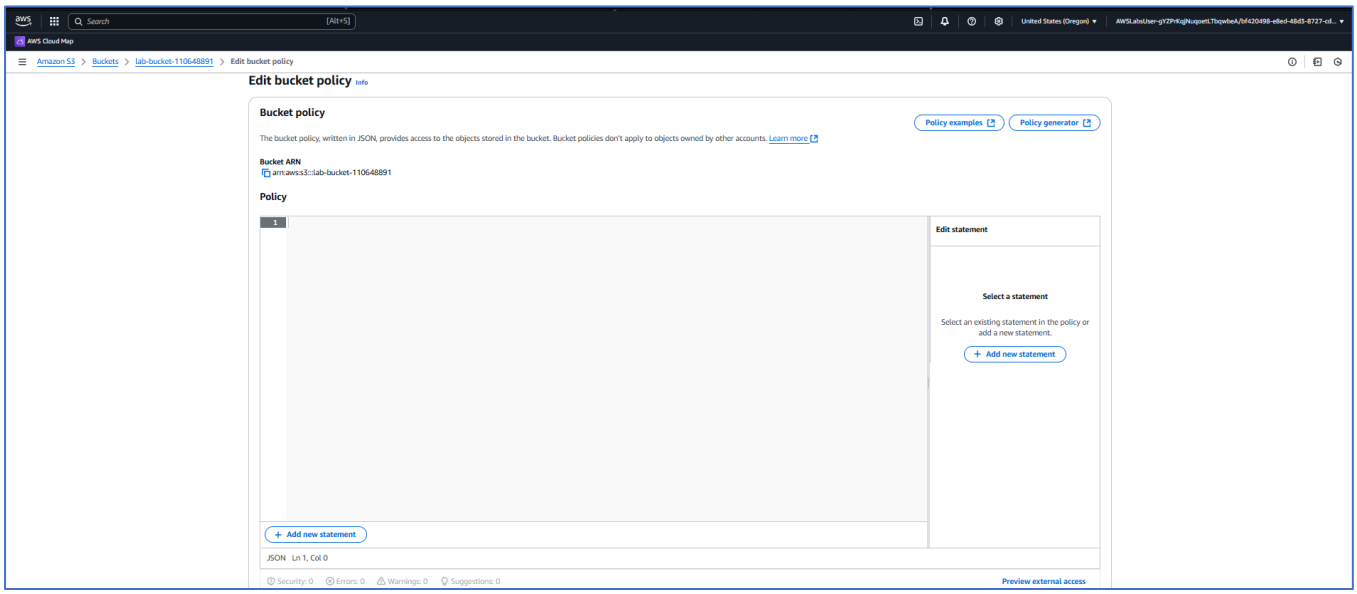
You have removed the block on all public access policies for the *lab-bucket-110648891*. You are now able to create access policies for the bucket that allow for public access. The bucket is currently not public, but anyone with the appropriate permissions can grant public access to objects stored within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



- **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.

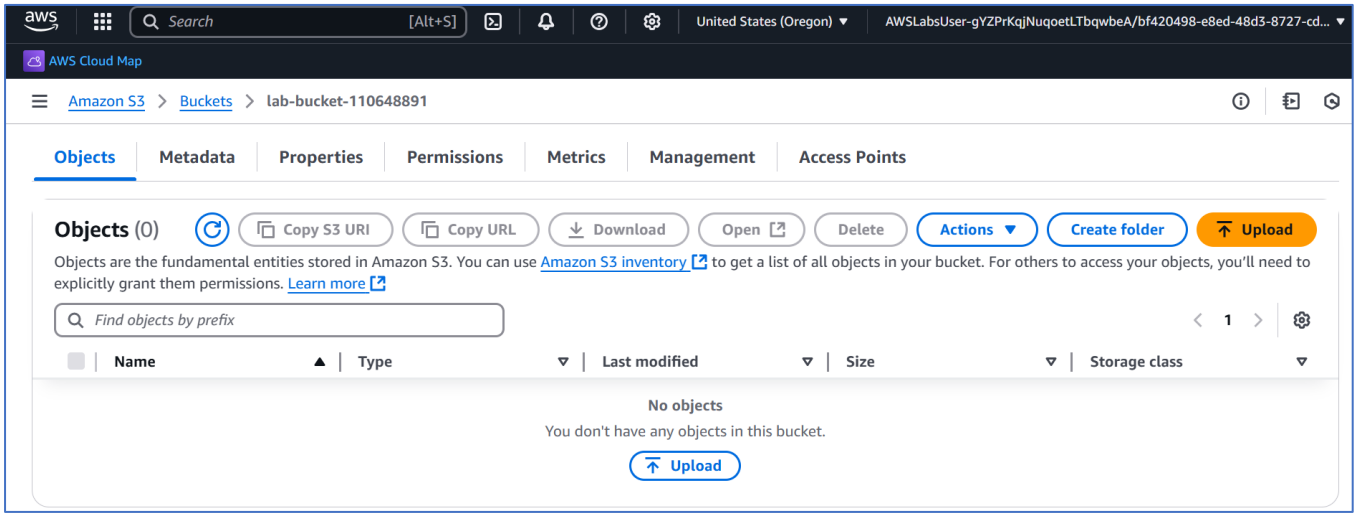
You have configured an S3 bucket for public read access.

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

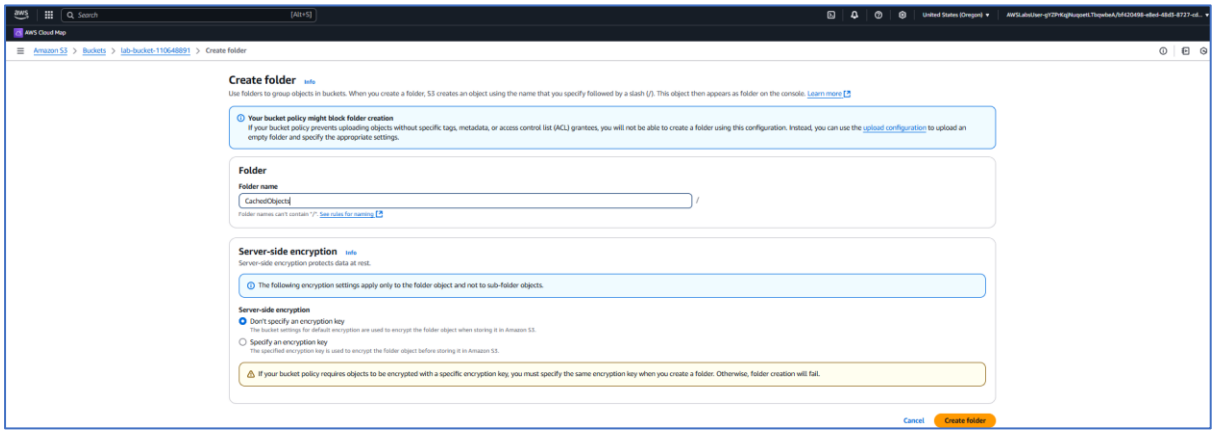
In this task, you upload a single object to the LabBucket. You use this object to test access in the remaining lab tasks.

Task 4.1: Create a new folder in the bucket

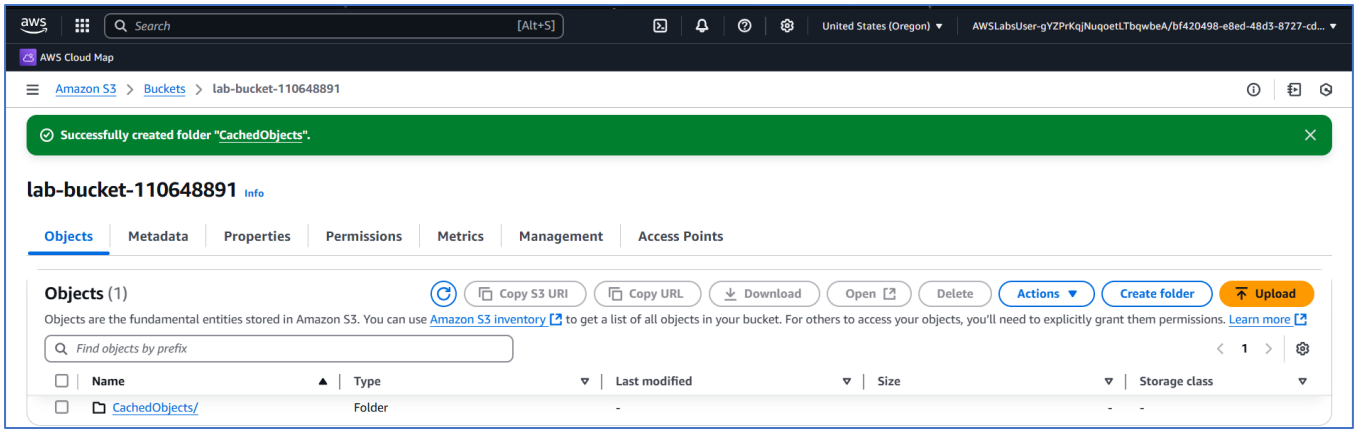
- Choose the **Objects** tab.
- Choose **Create folder**.



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



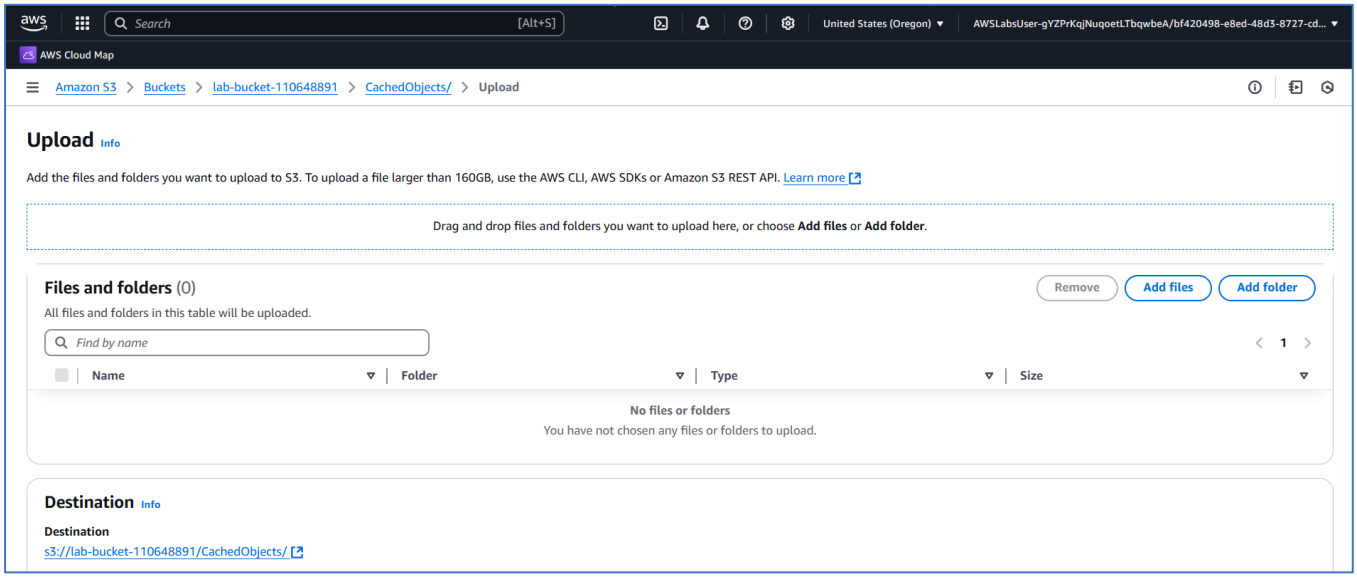
- Choose **Create folder**.



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**.

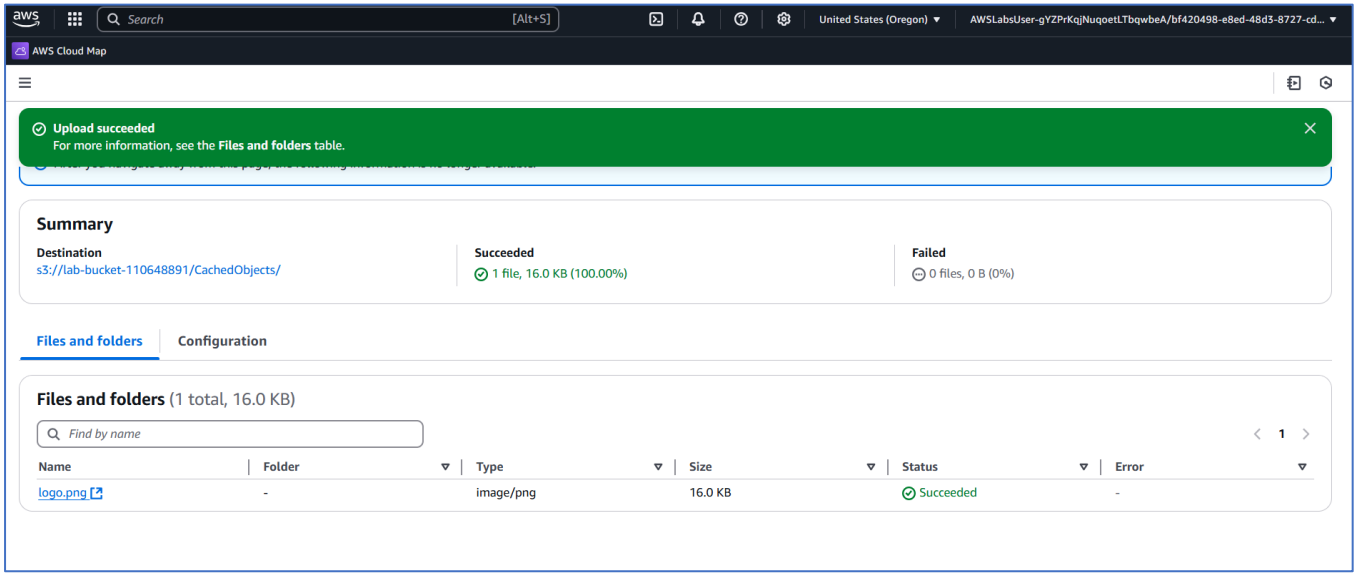
The **Upload** page is displayed.



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

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

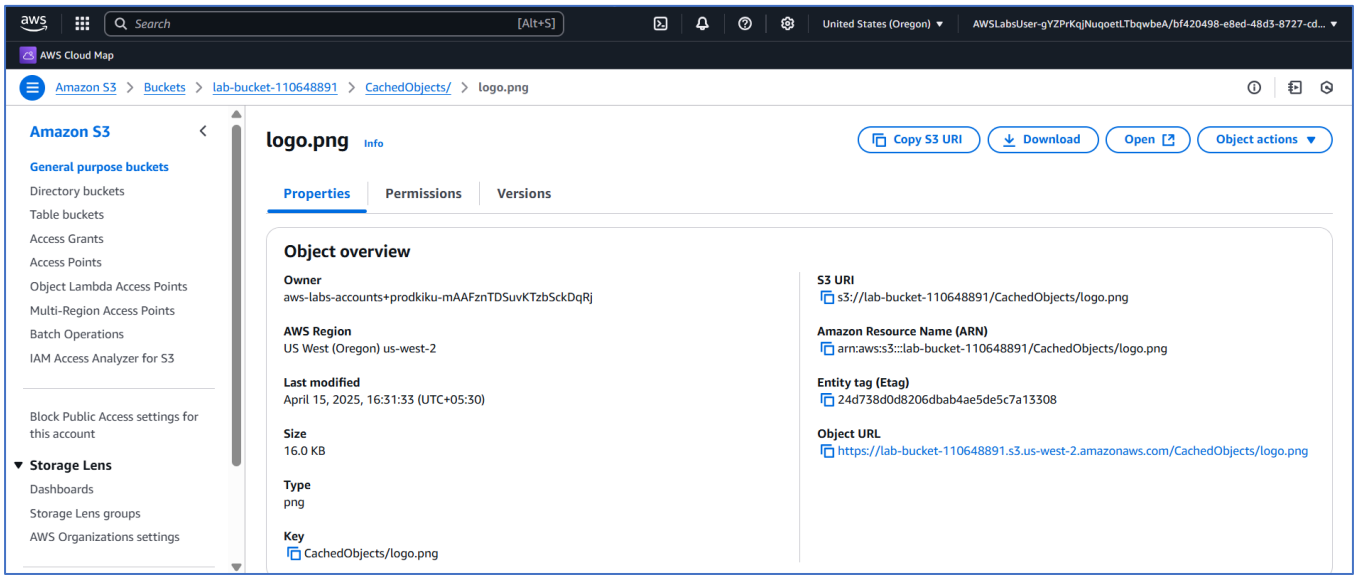
A **Upload succeeded** message is displayed on top of the screen.



Task 4.3: Test public access to an object

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

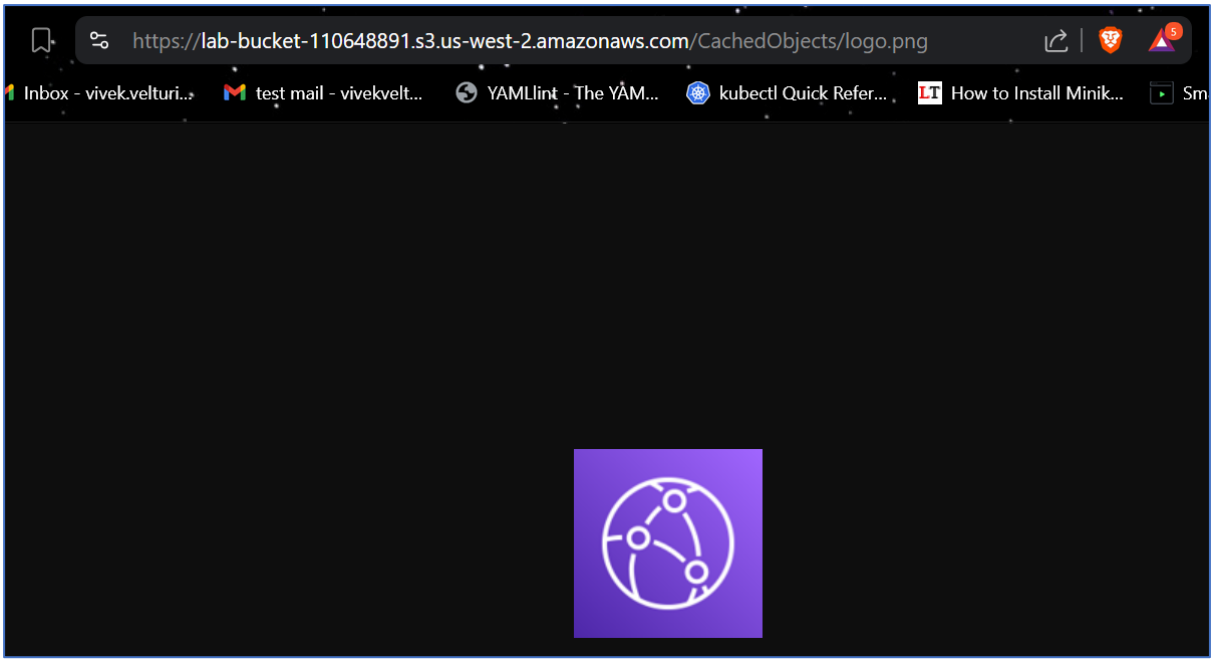
A page with details about the Amazon S3 object is displayed.



- 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.

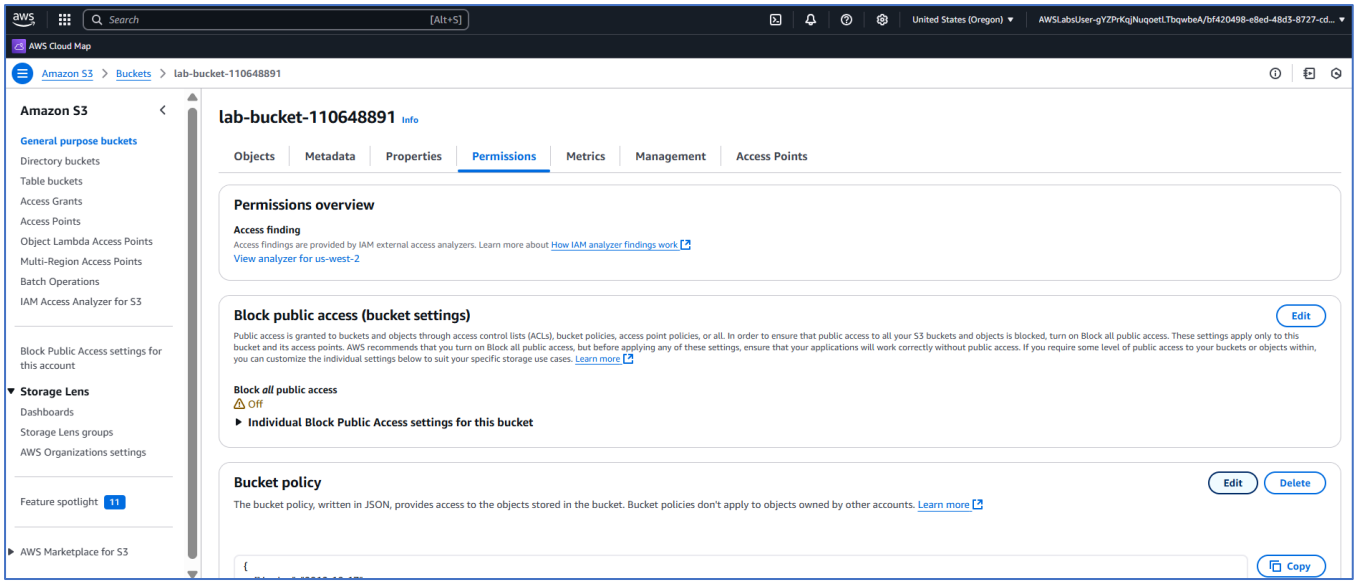
Task 5.1: Update the bucket policy for the LabBucket

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"
            }
        }
    }
}
```

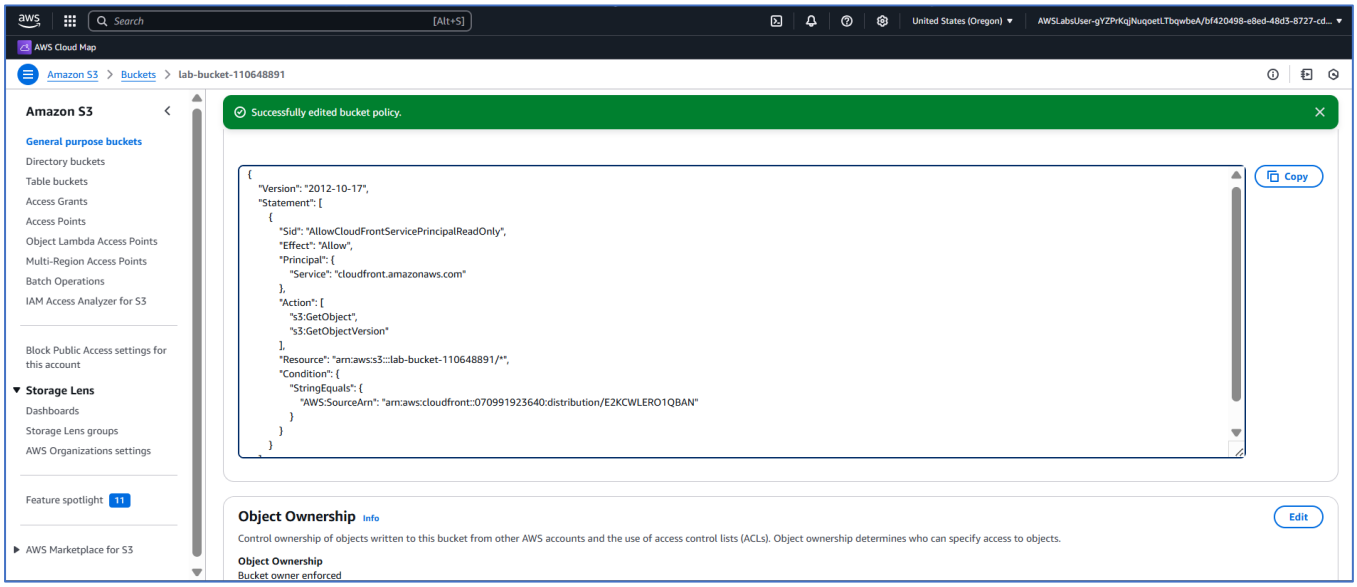
- Replace the **RESOURCE_ARN** value in the JSON with the **Bucket ARN** value you copied in a previous step and append a `/*` to the end of the pasted **Bucket ARN** value.

- 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**.



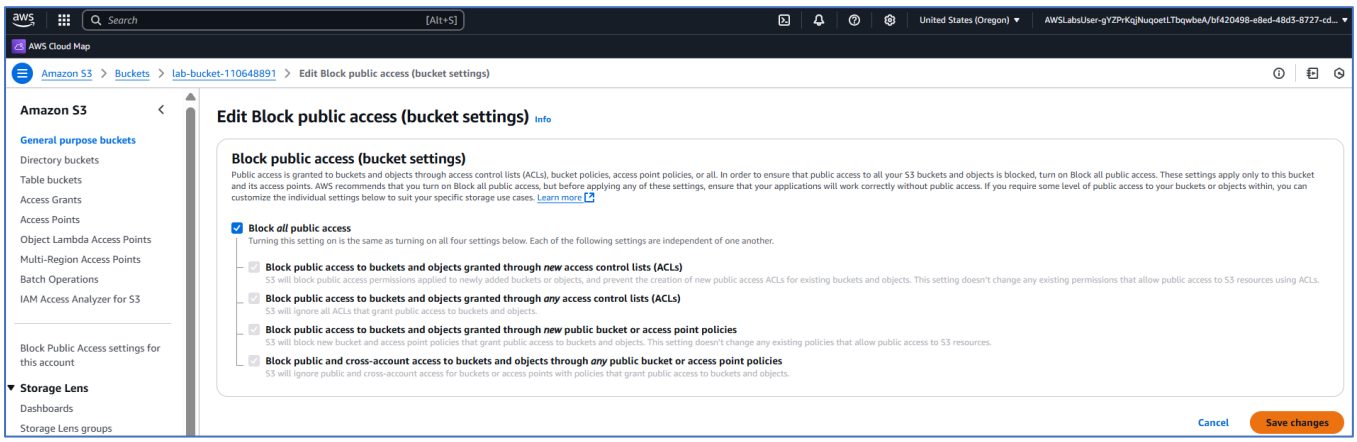
Task 5.2: Enable the public access blockers

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

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

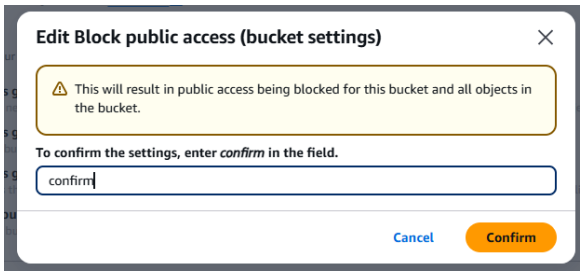
71. Select **Block *all* public access**.

72. Choose **Save changes**.



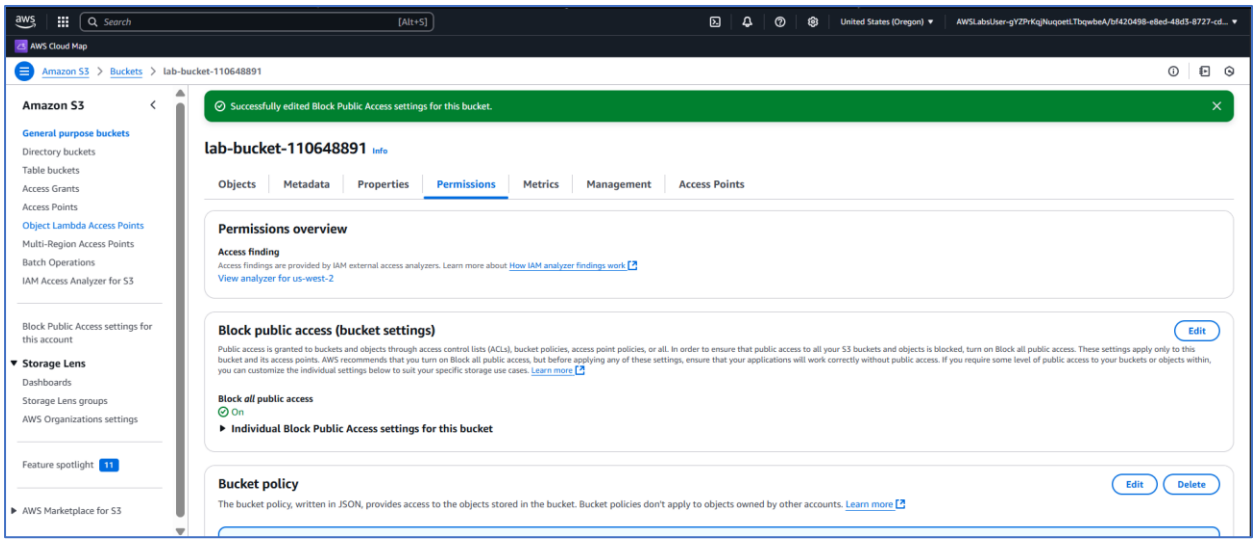
A message window titled Edit Block public access (bucket settings) is displayed.

- 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.



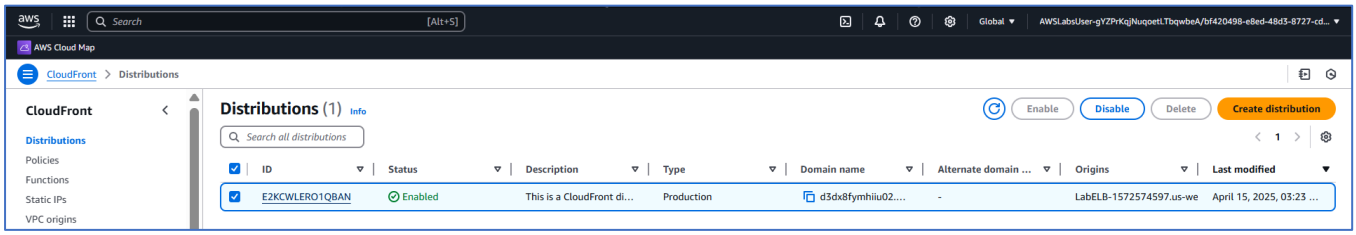
You have edited the S3 bucket policy so that the only principal allowed to read objects CloudFront distribution.

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

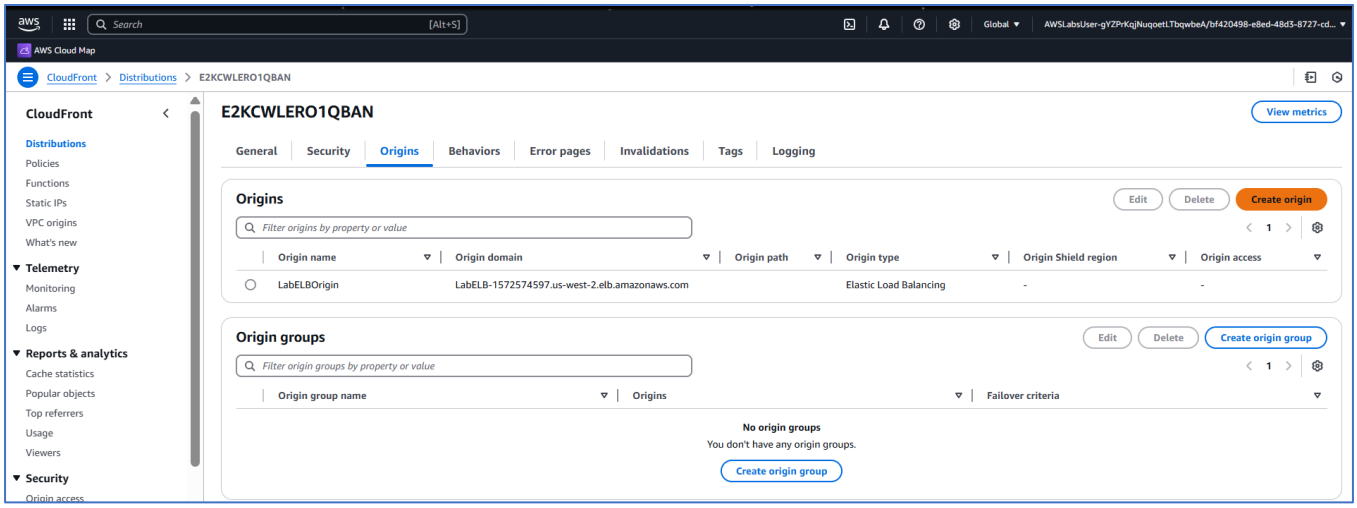
In this task, you add the *lab-bucket-110648891* as a new origin to the existing CloudFront distribution.

- 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.

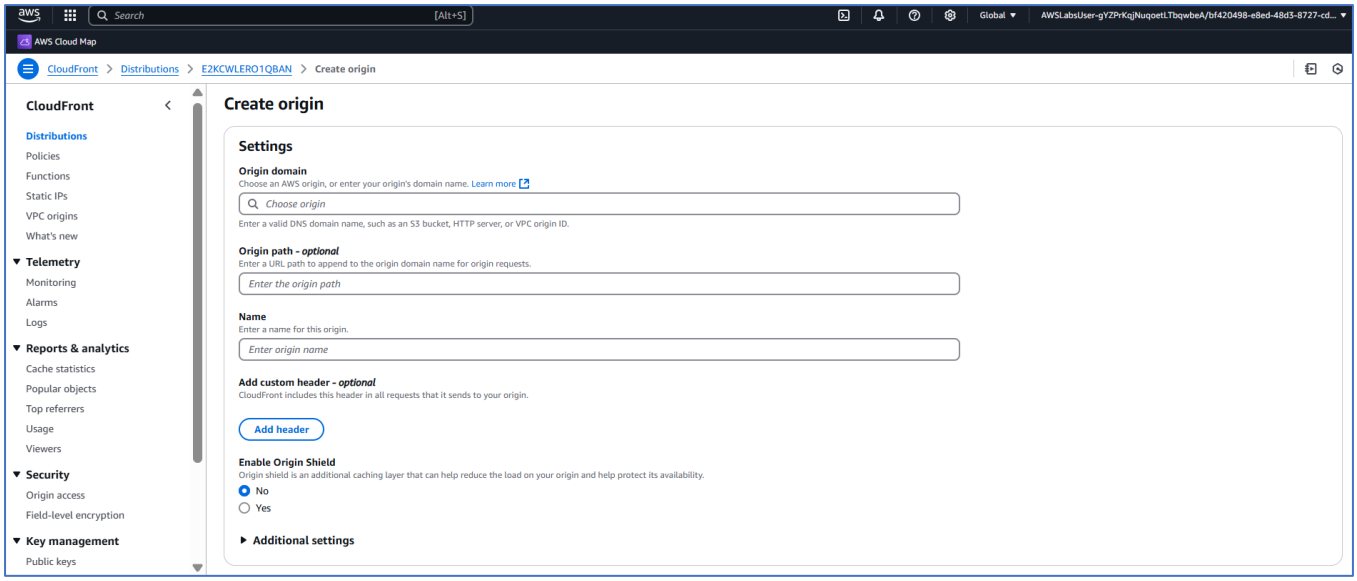
A page showing the details of the distribution is displayed.



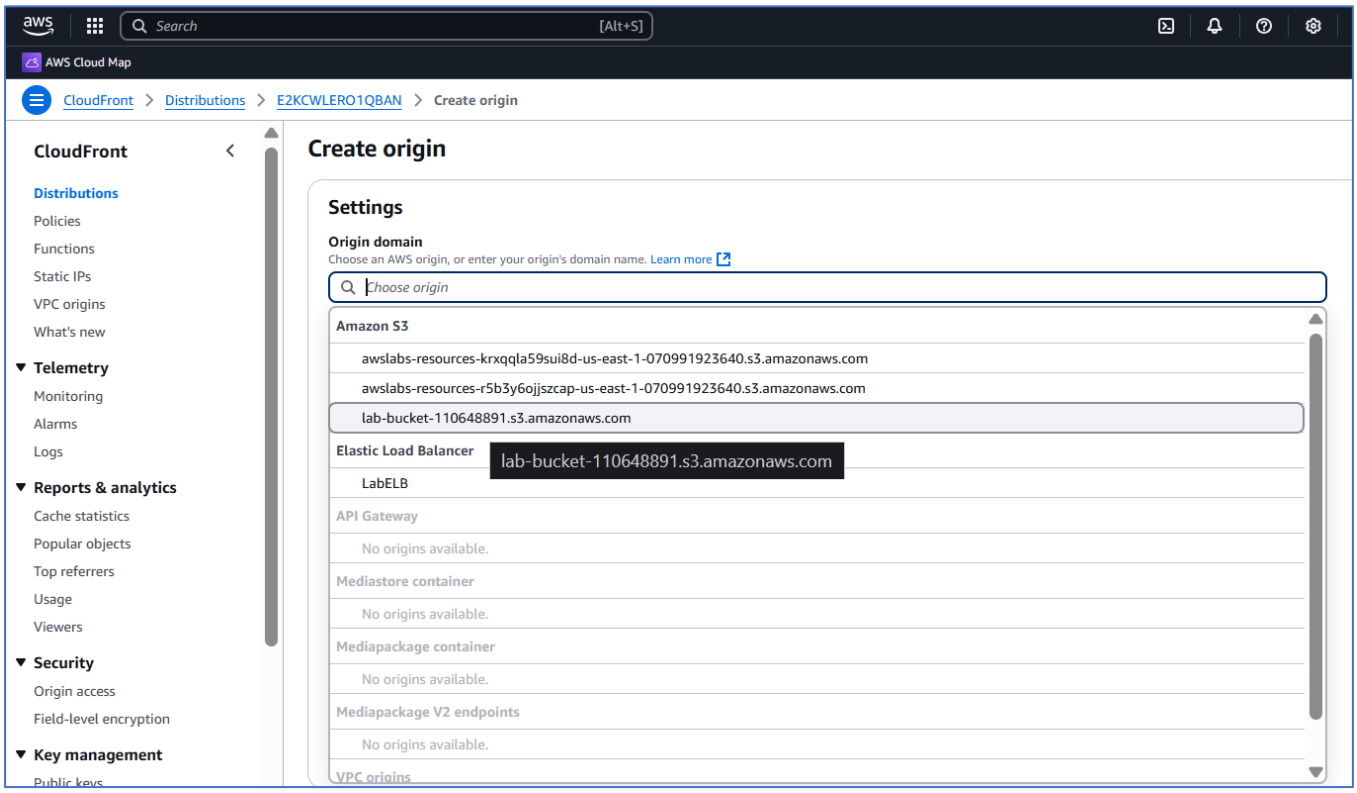
- Choose the **Origins** tab.
- Choose **Create origin**.



The **Create Origin** page is displayed.



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



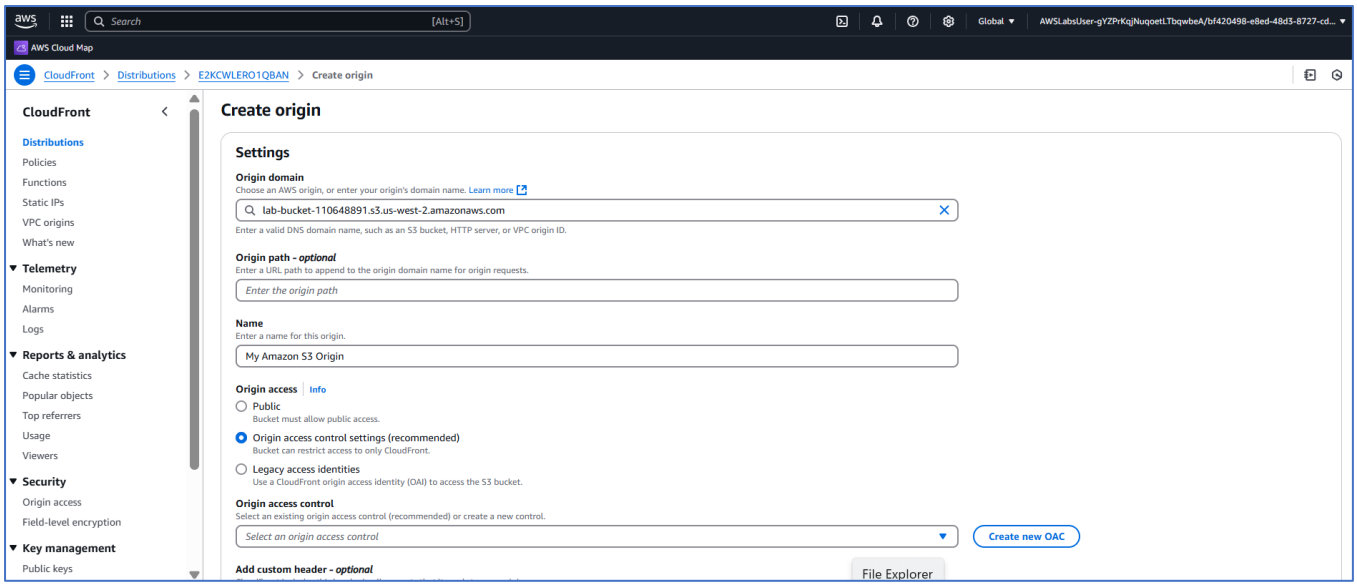
Note: Recall that the S3 bucket in this lab is never configured as a website. You have only changed the bucket policy regarding who is allowed to perform GetObject API requests against the S3 bucket into an *Allow Public* read policy.

- 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

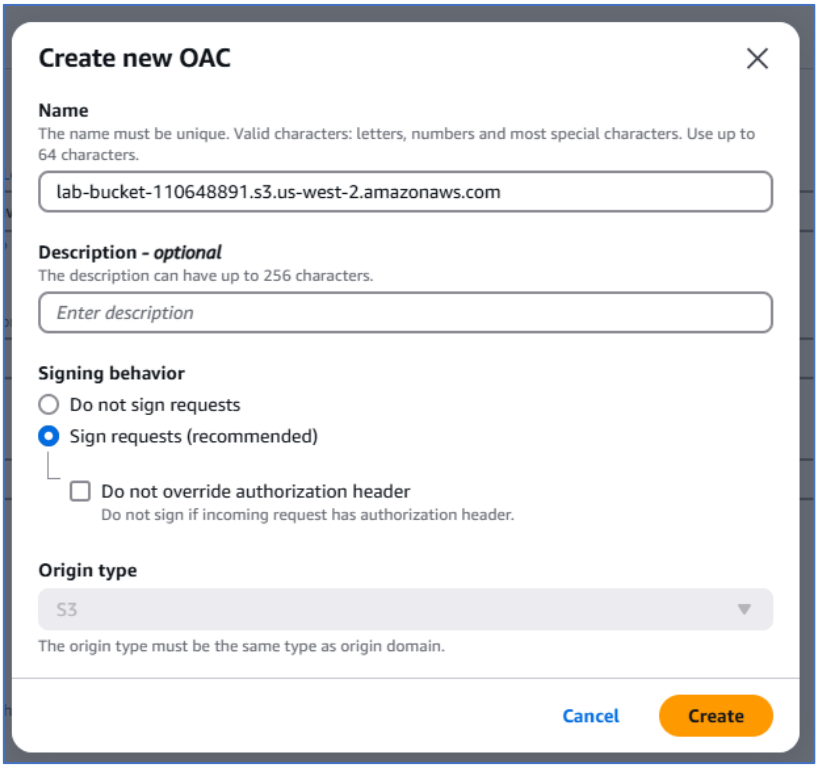
path, you leave it blank and instead configure a behavior to return only objects matching a specific pattern in the requests.

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

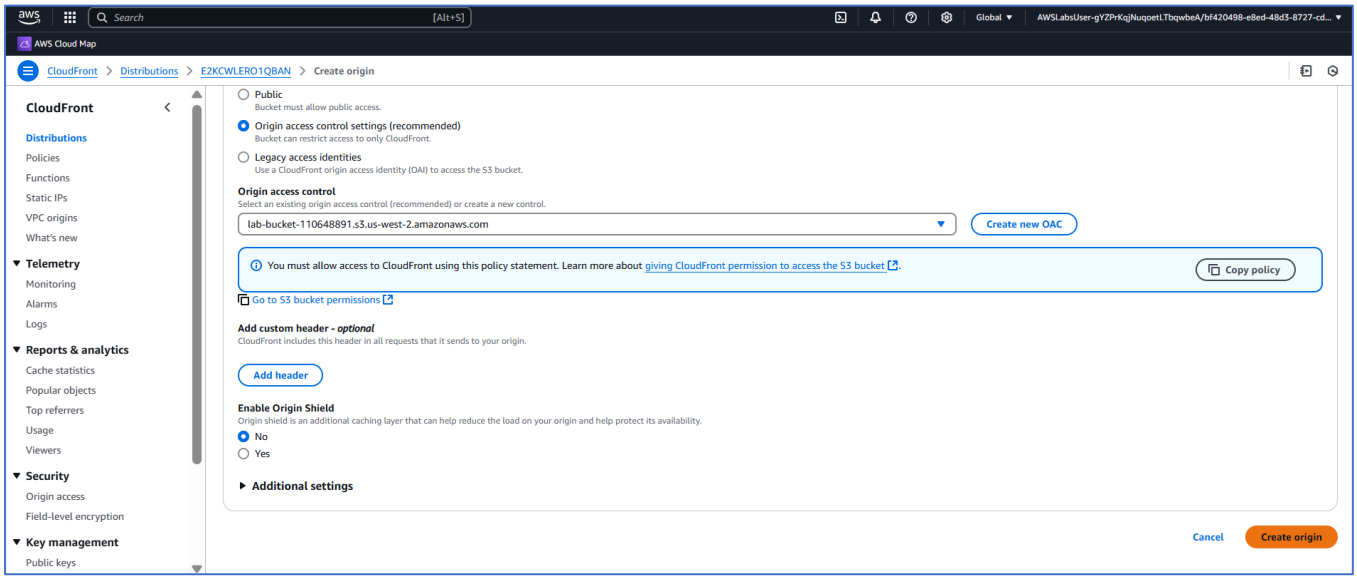


- Choose **Create new OAC**.

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

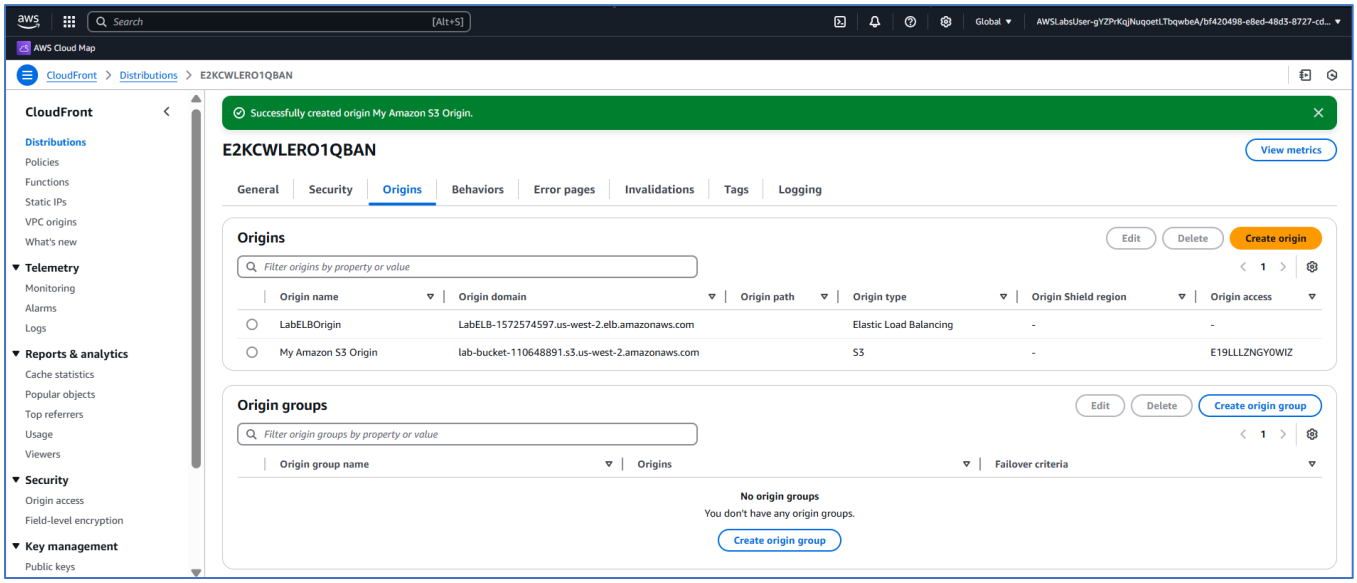


- Leave the default settings and choose **Create**.
- Choose **Create origin**.



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

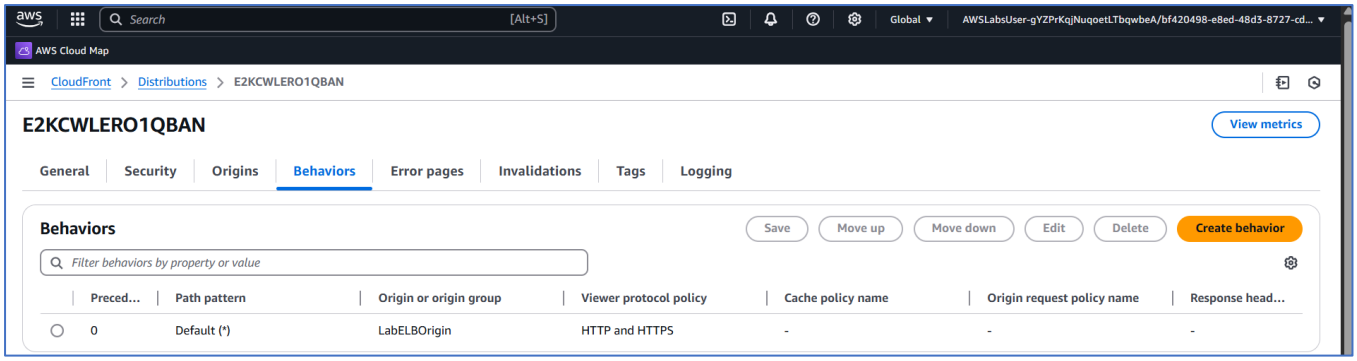
You can safely ignore any message like, **The S3 bucket policy needs to be updated** as you completed updating the bucket policy already.



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

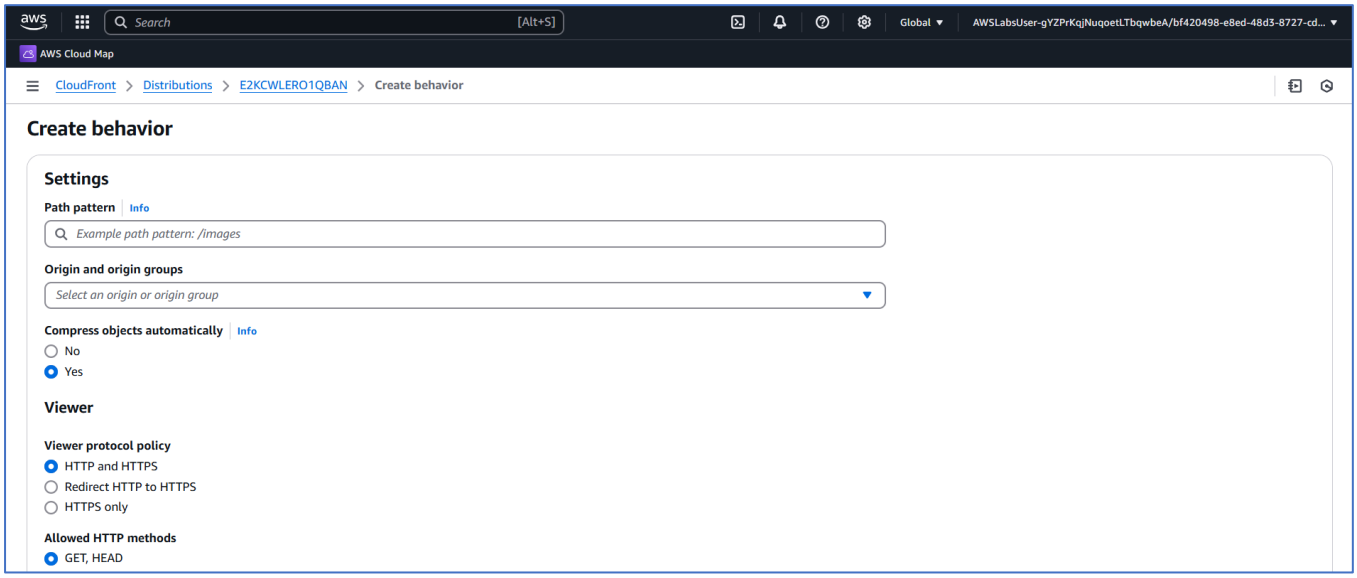
In this task, you create a new behavior for the Amazon S3 origin so that the distribution has instructions for how to handle incoming requests for the origin.

- Choose the **Behaviors** tab.



- Choose **Create behavior**.

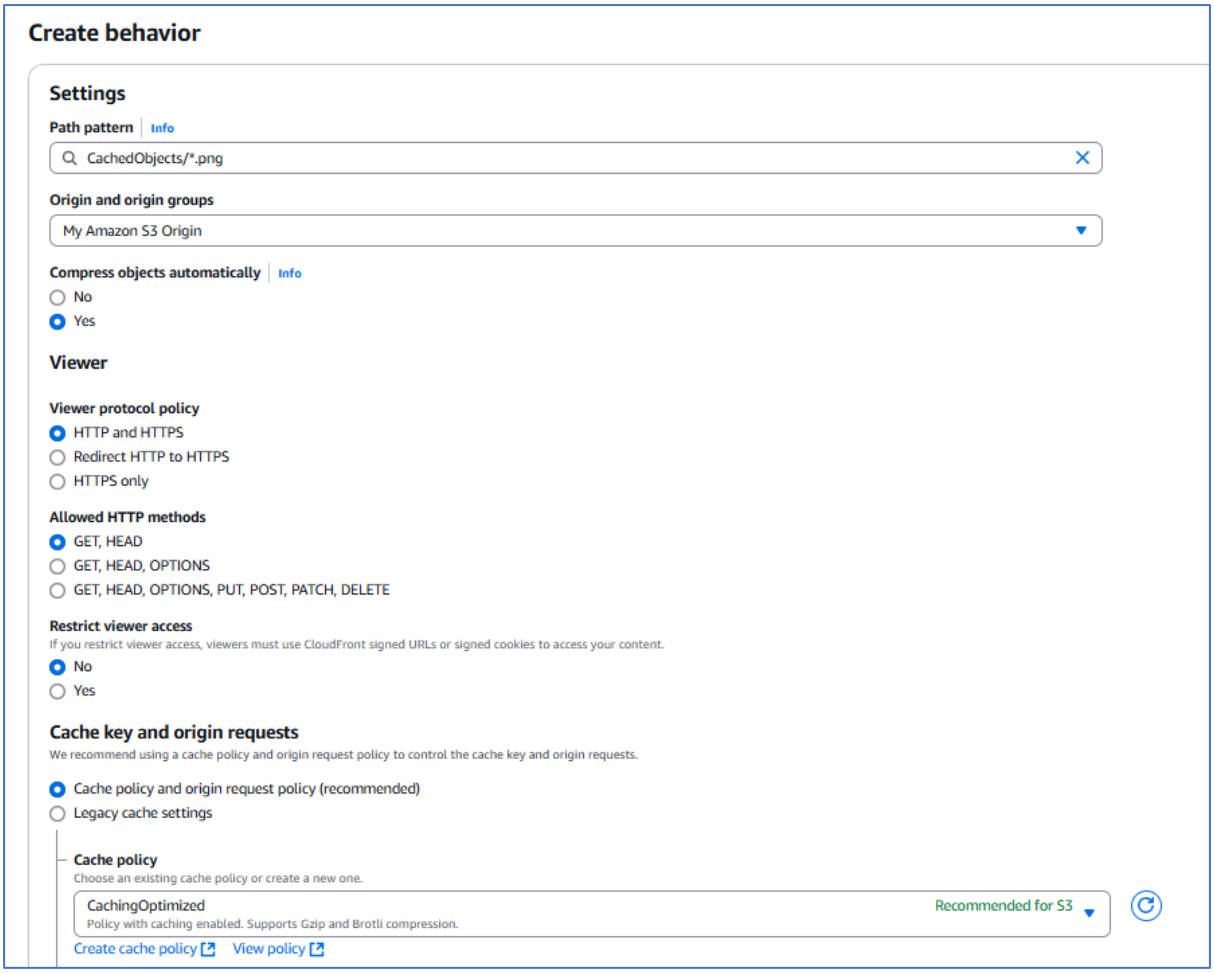
The **Create behavior** page is displayed.



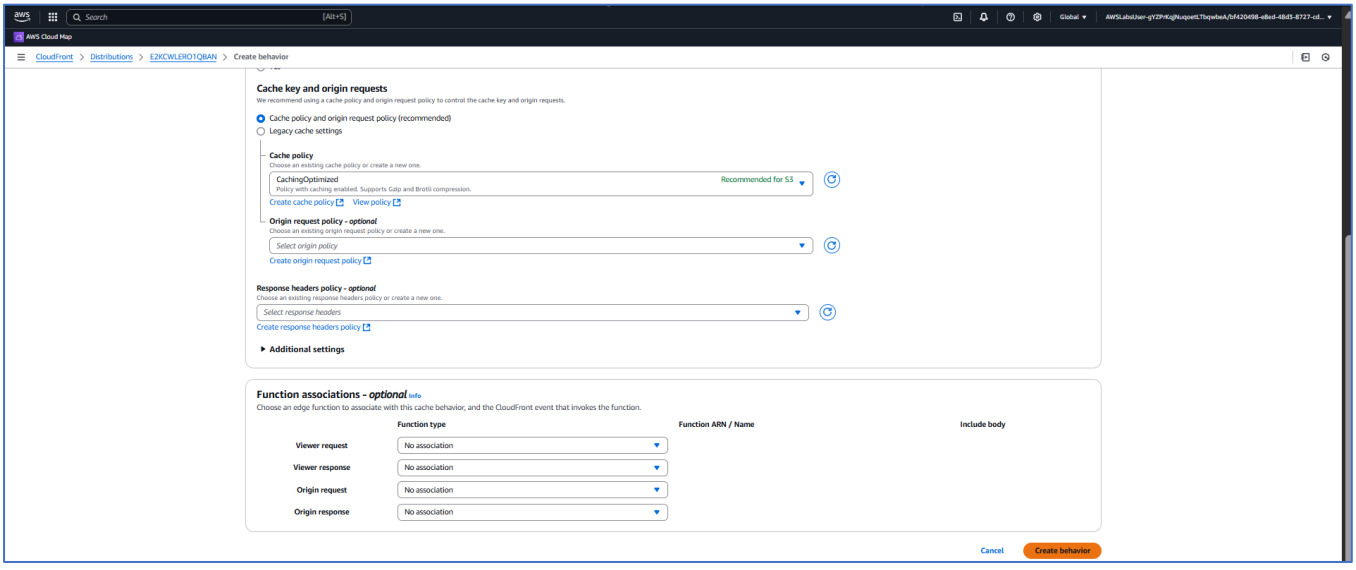
- In the **Path pattern** field, enter `CachedObjects/*.png`

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.

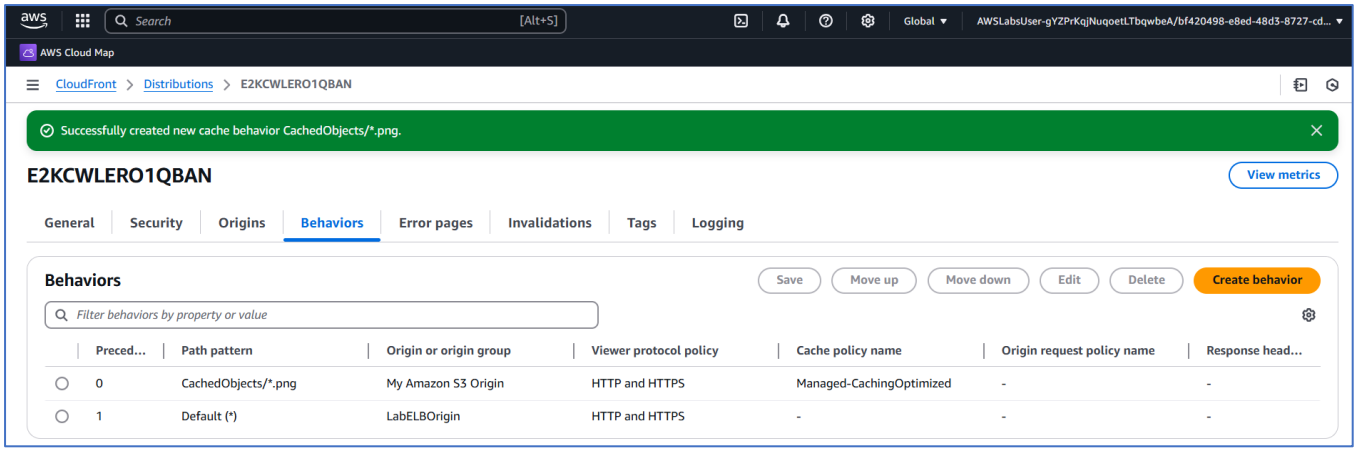
- From the **Origin and origin groups** dropdown menu, choose **My Amazon S3 Origin**.
- From the **Cache key and origin requests** section, ensure **Cache policy and origin request policy (recommended)** is selected.
- From the **Cache policy** dropdown menu, ensure **CachingOptimized** is selected.



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



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



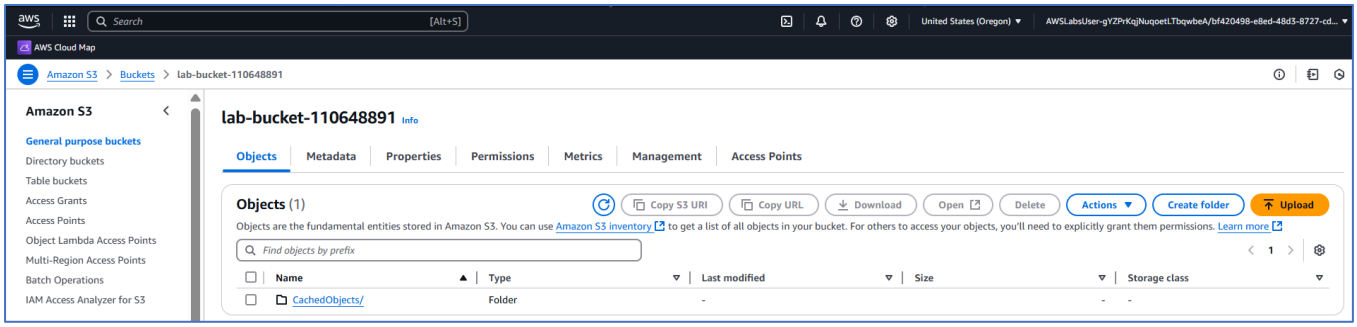
You have created: a new origin for the Amazon S3 bucket, an Origin Access Control, and distribution behavior on a CloudFront distribution for the objects stored in the Amazon S3 bucket for the lab.

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.

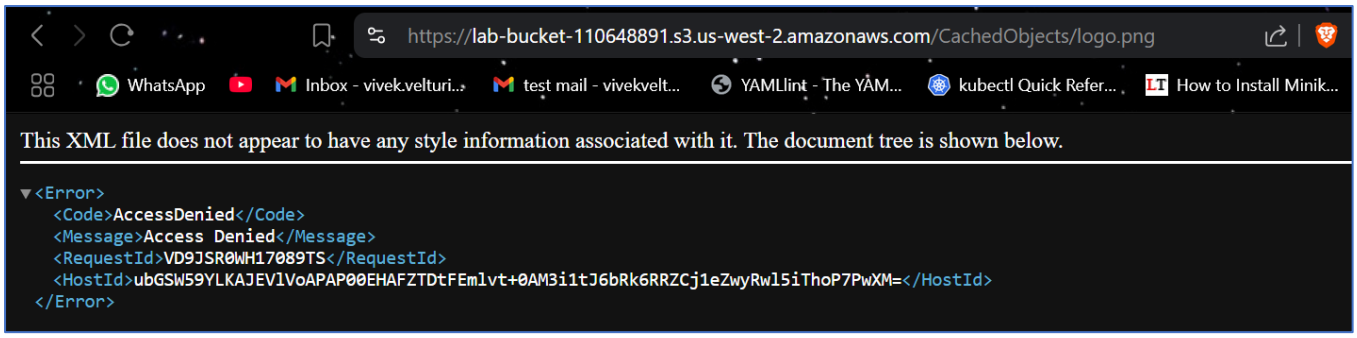
A page with all of the bucket details is displayed.



- 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.



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

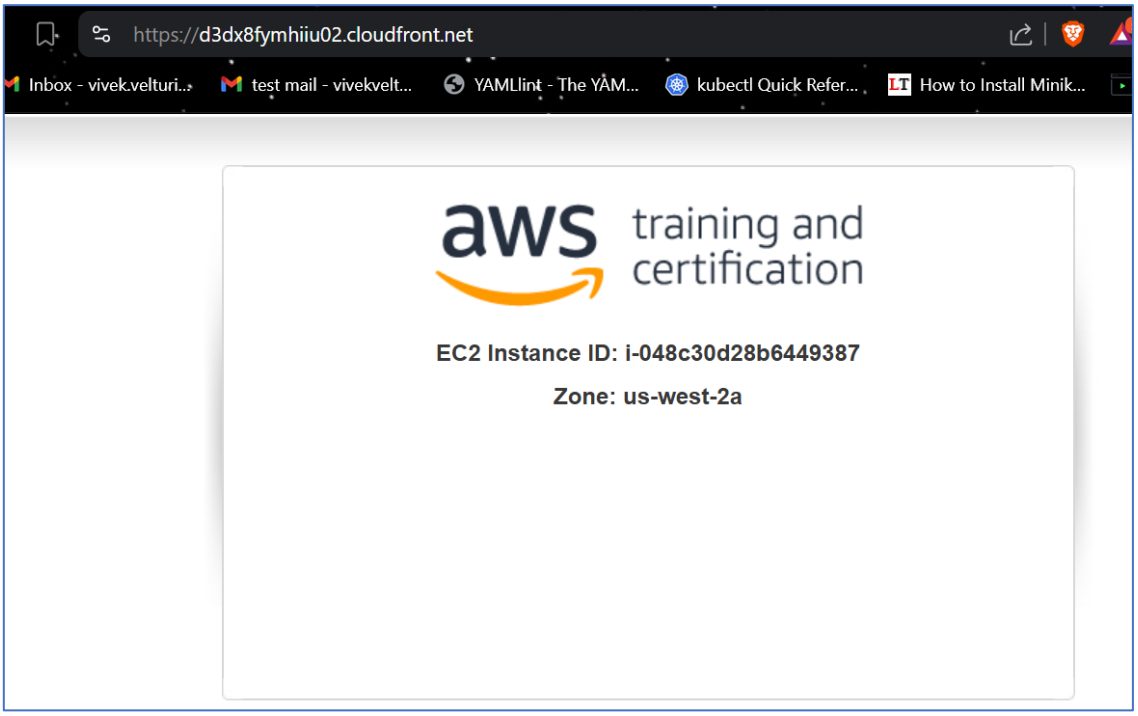
Task 7: Test access to the object in the bucket using the CloudFront distribution

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

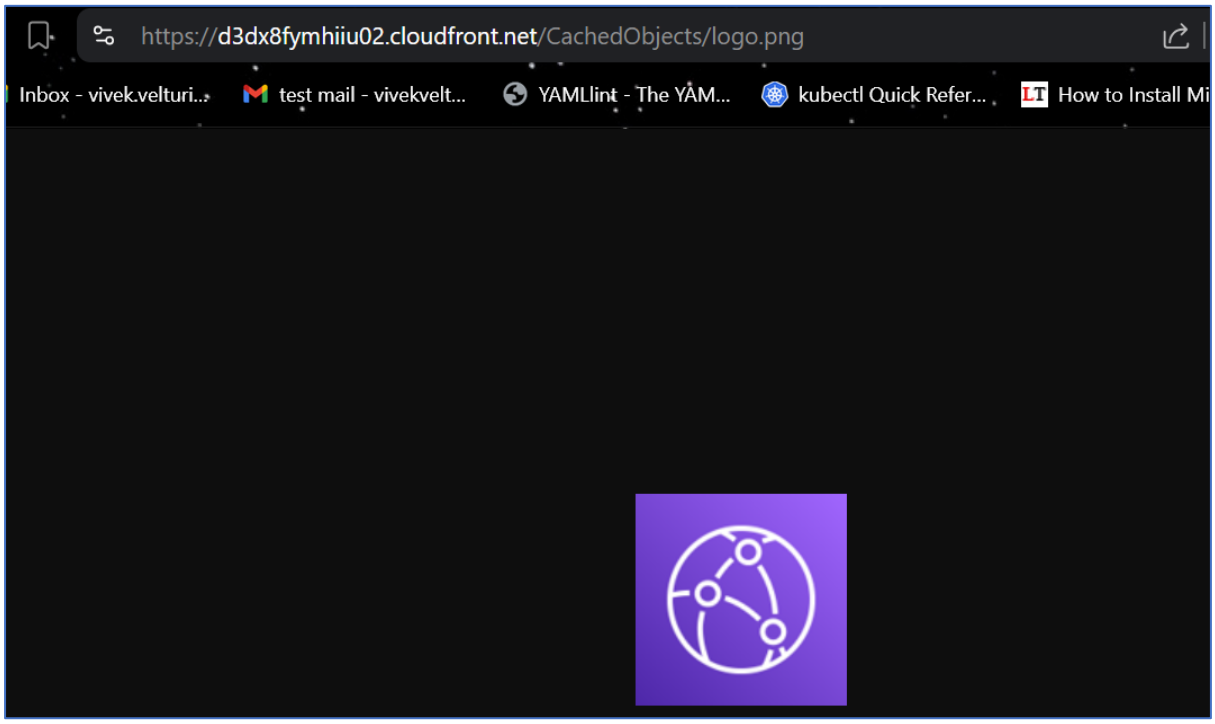
- **Copy edit:** Copy the CloudFront distribution's domain DNS value from the left side of these lab instructions under the listing *LabCloudFrontDistributionDNS*. ***(d3dx8fymhiiu02.cloudfront.net)***

- 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.



- 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.

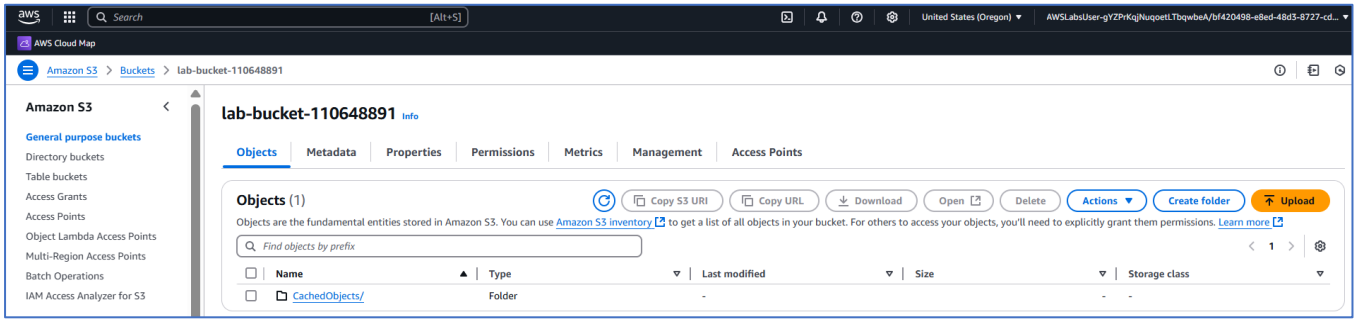
To perform *Cross-Region replication*, you must enable object versioning for both the source and destination buckets. To maintain good data orderliness with versioning

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.

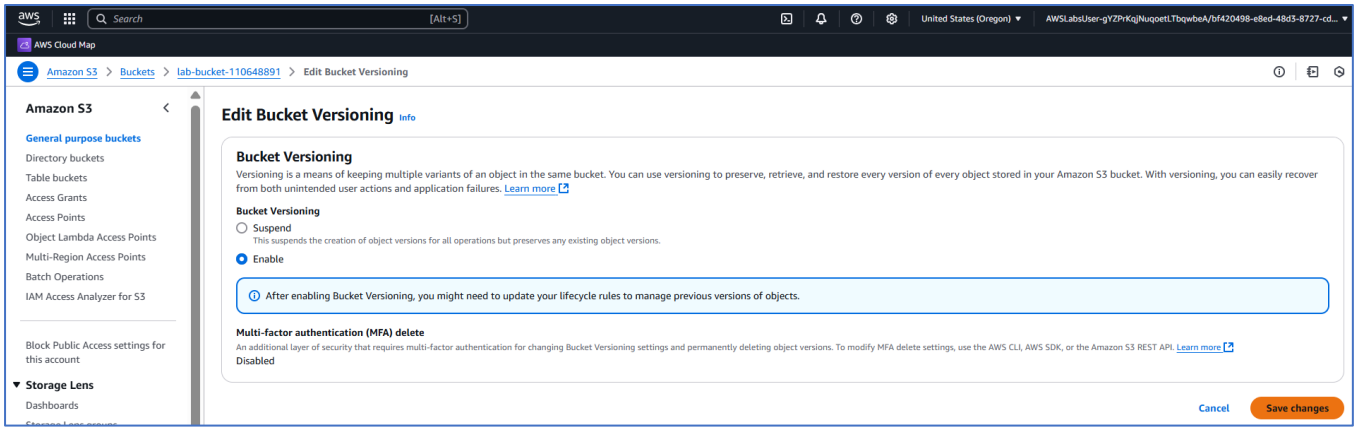
A page with all the bucket details is displayed.



- 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**.



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

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

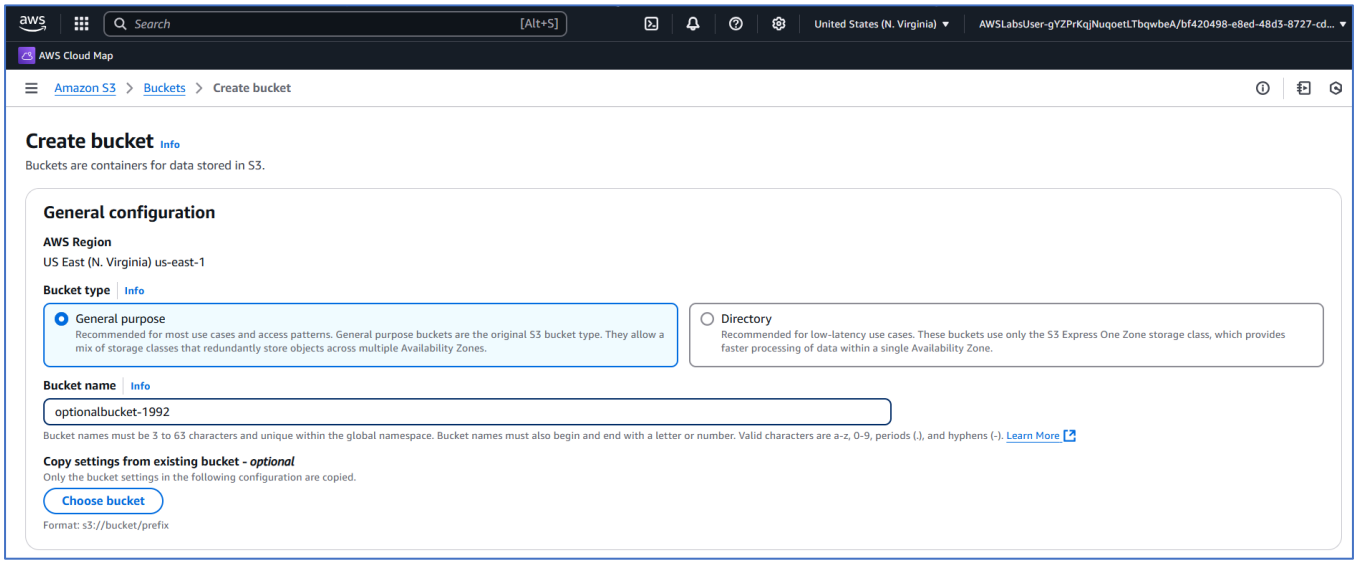
- At the top of the screen, choose the drop-down next to the region you are in and choose the **SecondaryRegion** value **(us-east-1)**

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

- Choose **Create bucket**.

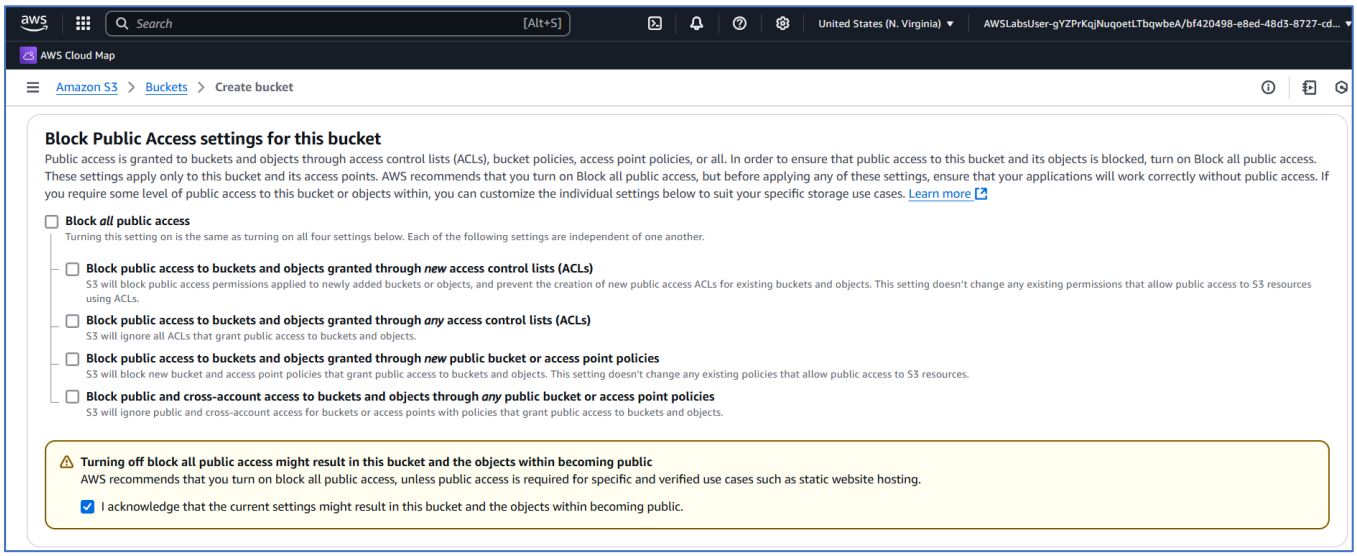
The **Create bucket** page is displayed.

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



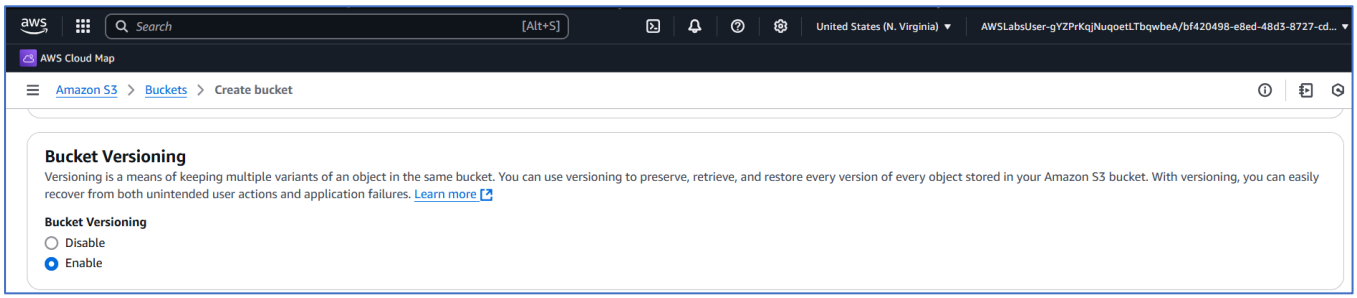
- In the **Block Public Access settings for this bucket** section, unselect **Block all public access**.

- In the warning message, select **I acknowledge that the current settings might result in this bucket and the objects within becoming public**.

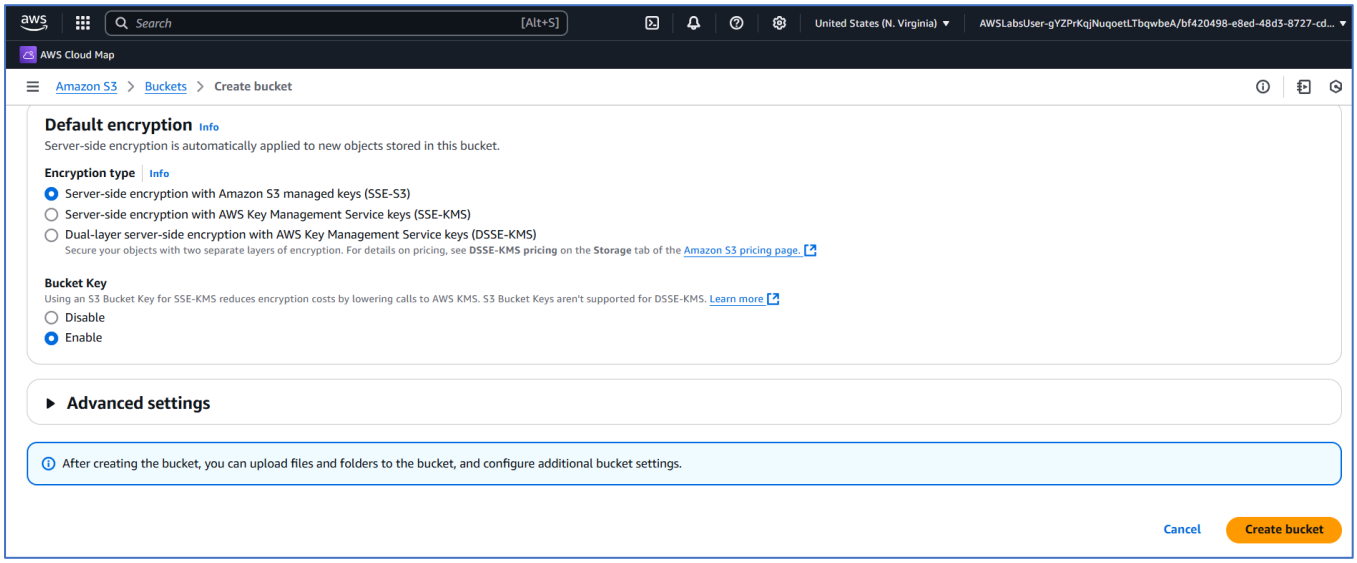


Caution: You do not need to have public access enabled for your personal buckets to use the cross-Region replication feature. It is enabled in this lab so that you can quickly test if objects are replicated and retrievable using the Amazon S3 URL.

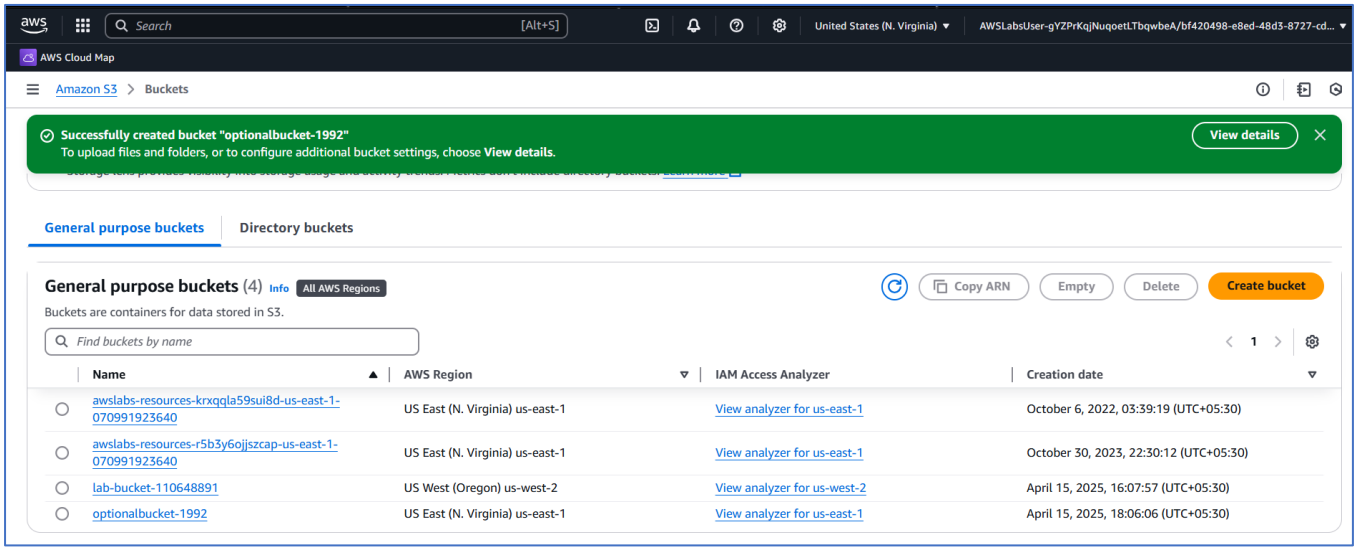
- For **Bucket Versioning**, select **Enable**.



- Choose **Create bucket**.



The **Amazon S3 console** is displayed.



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"
        }
    ]
}
```

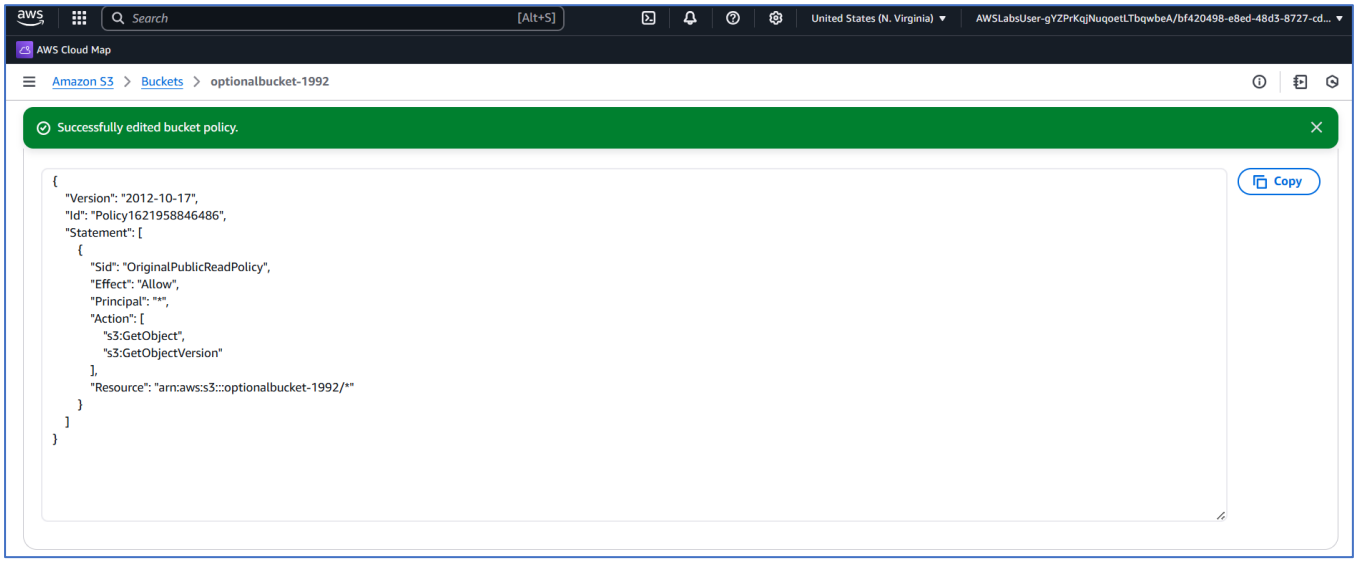
- Replace the **RESOURCE_ARN** value in the JSON with the **Bucket ARN** value you copied in a previous step and append a `/*` to the end of the pasted **Bucket ARN** value.

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**.

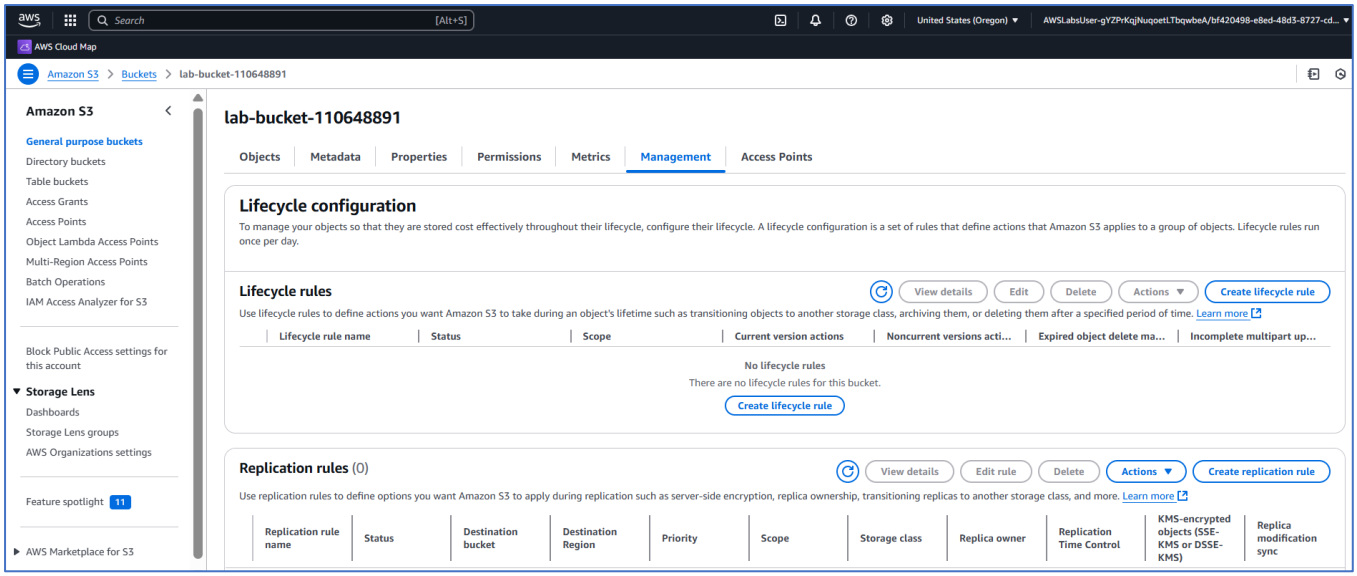
The **bucket details** page is displayed.



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

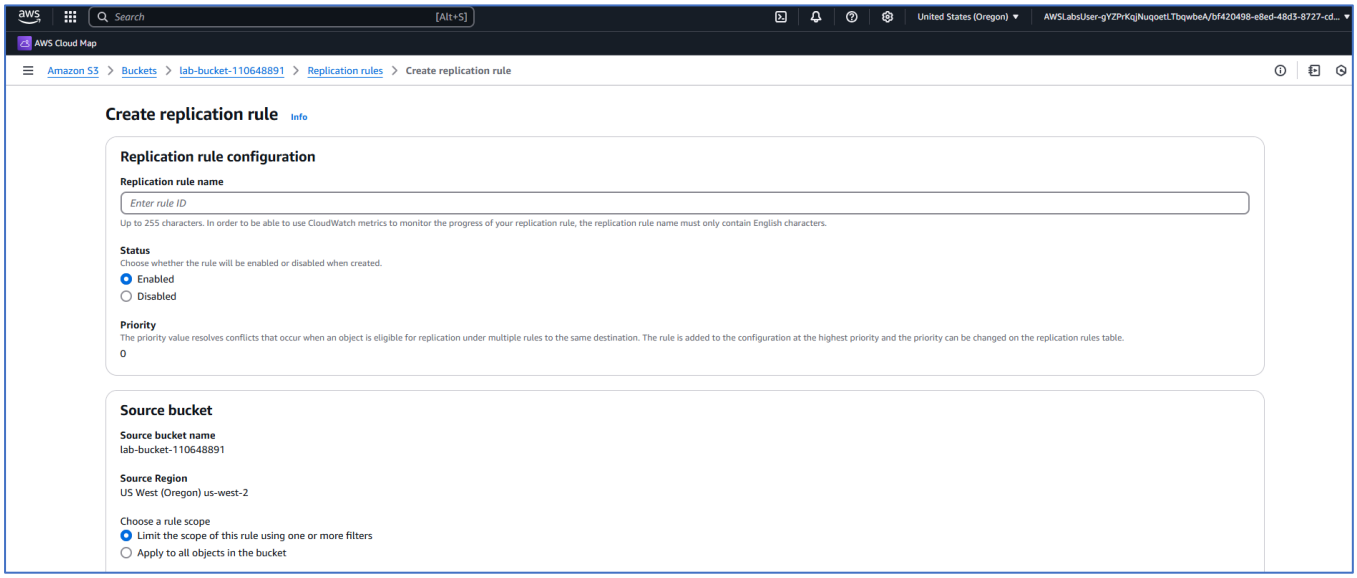
Task 8.4: Create a replication rule

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

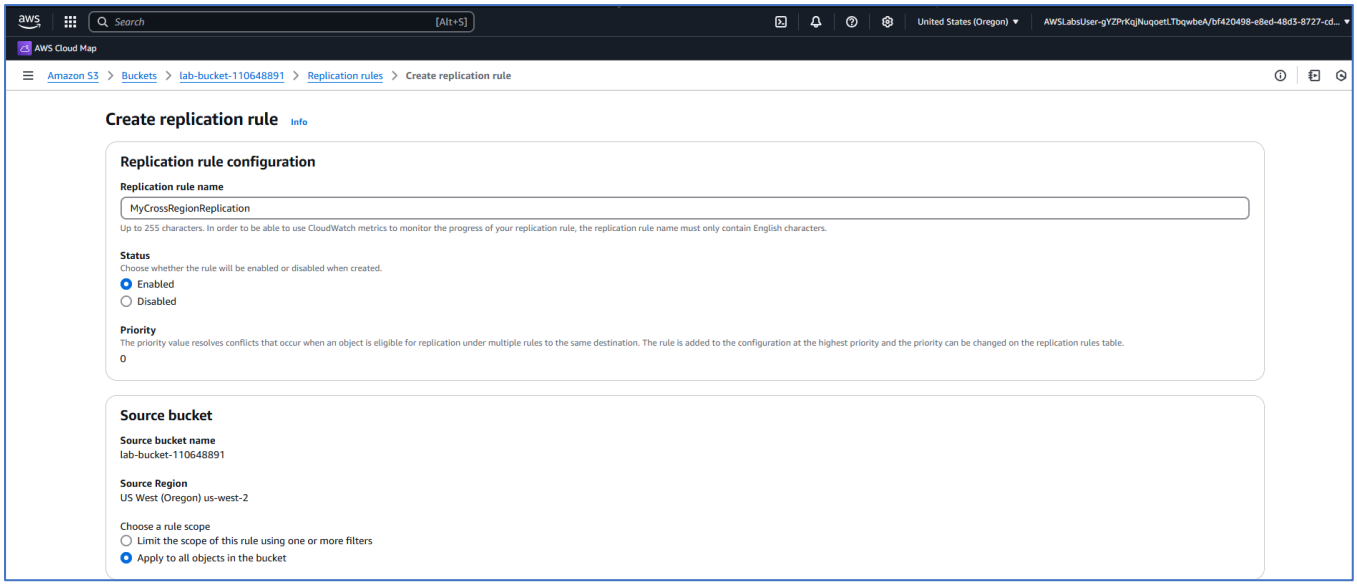


- Locate the **Replication rules** section.
- Choose **Create replication rule**.

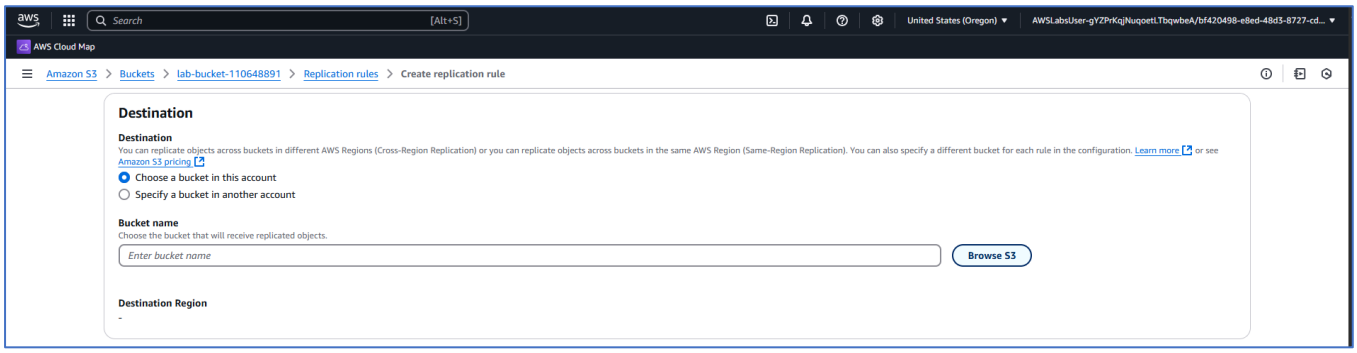
The **Create replication rule** page is displayed.



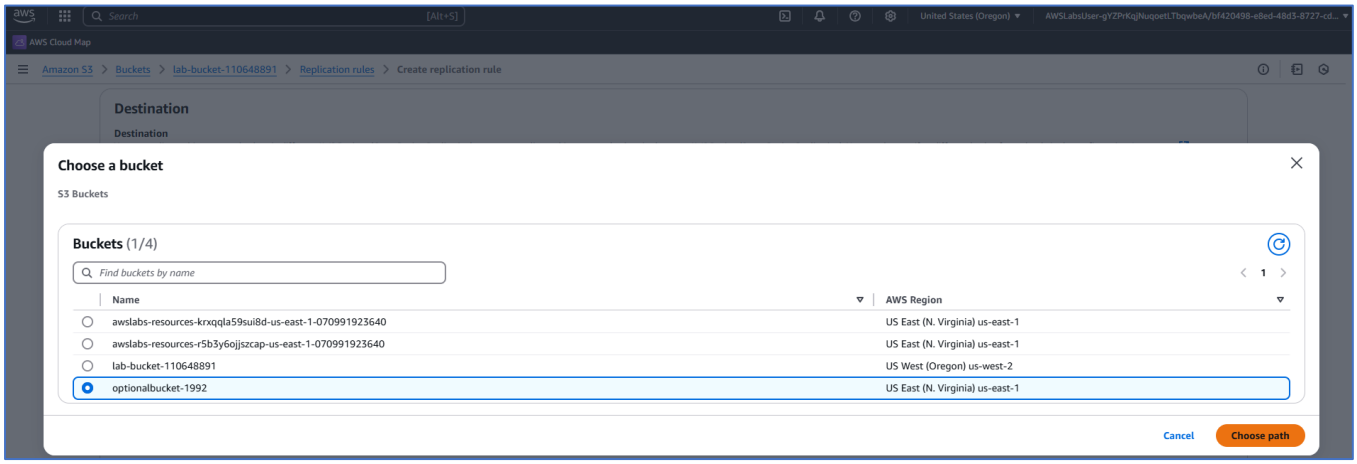
- In the **Replication rule name** field, enter `MyCrossRegionReplication`
- Verify that *lab-bucket-110648891* is set for **Source bucket name**. If it is not, then you chose the incorrect bucket before choosing the replication rules.
- In the **Choose a rule scope** section, select **Apply to all objects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



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

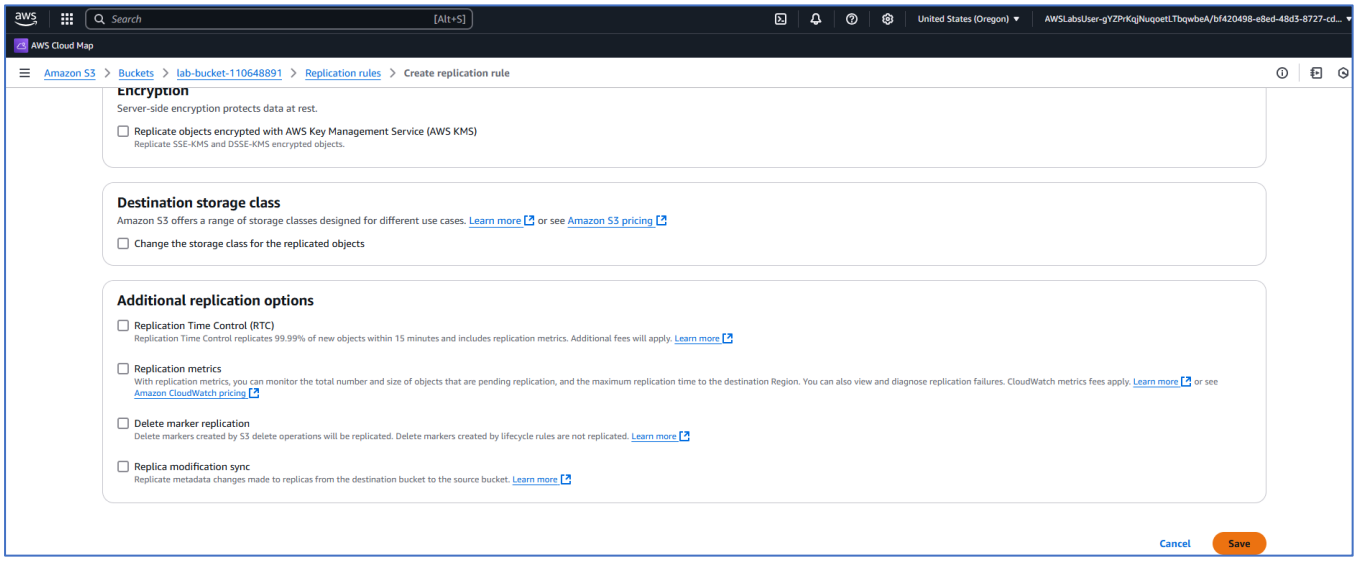


- Select the *optionalbucket-1992* .
- Select **Choose path**.

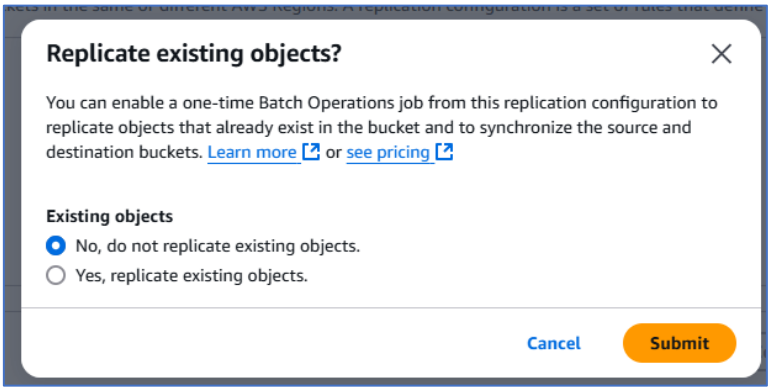


- Locate the **IAM Role** section.

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

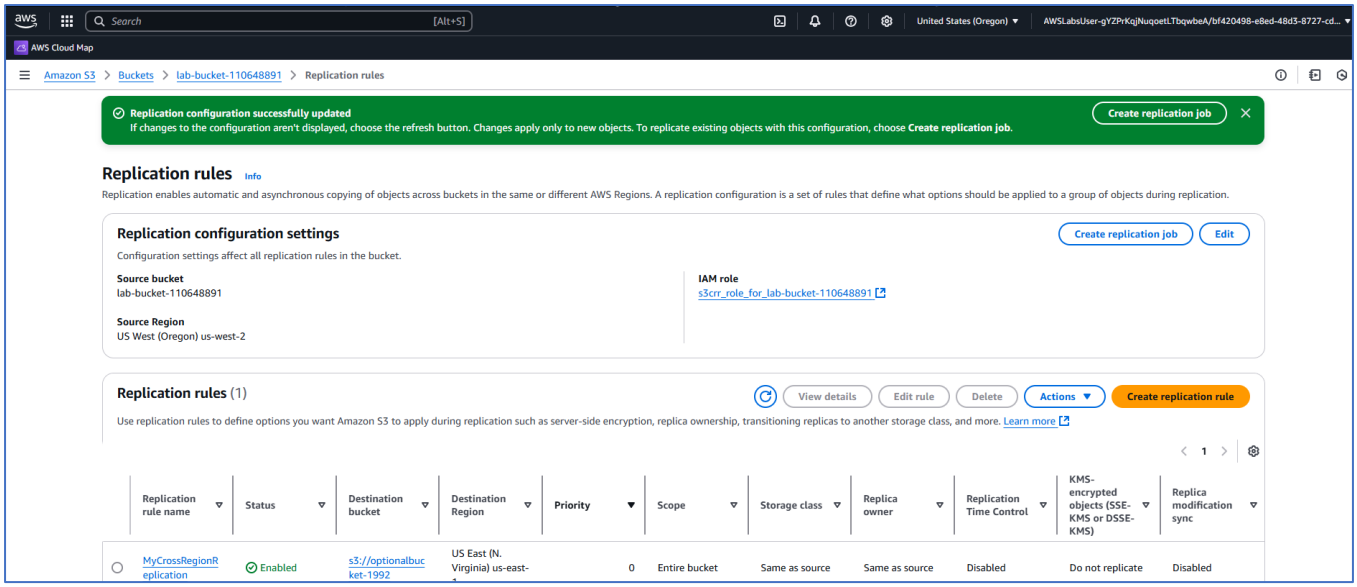


- If the Replicate existing objects window is displayed, select **No, do not replicate existing objects** then choose **Submit**.



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.

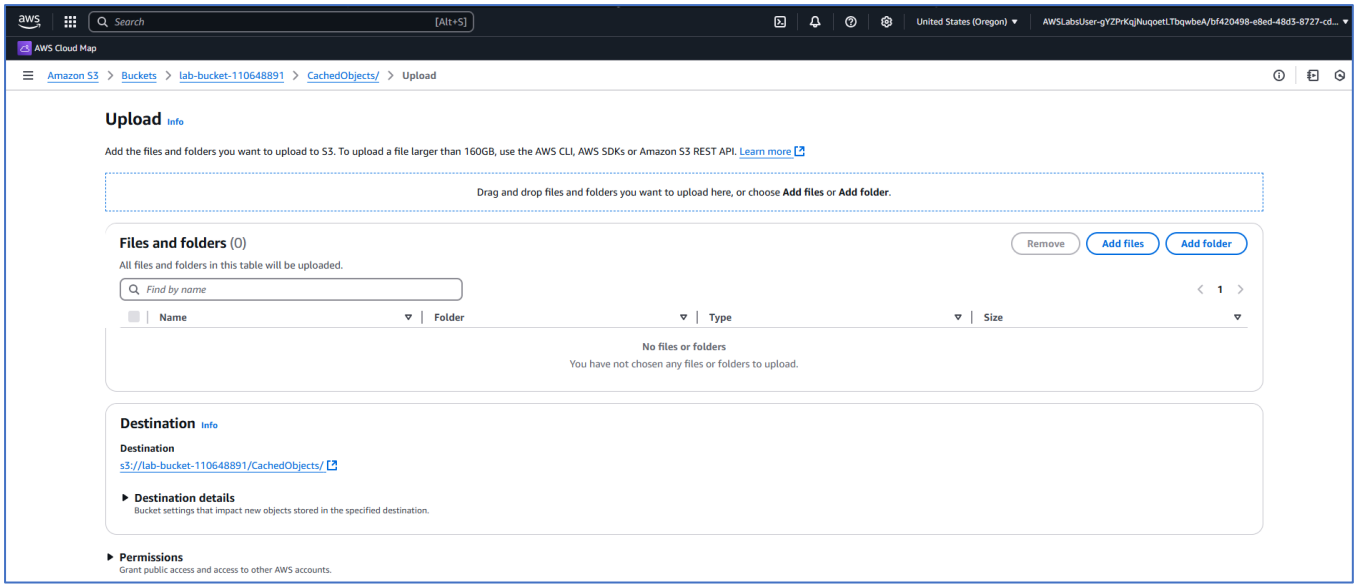
Task 8.5: Verify object replication

- 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**.

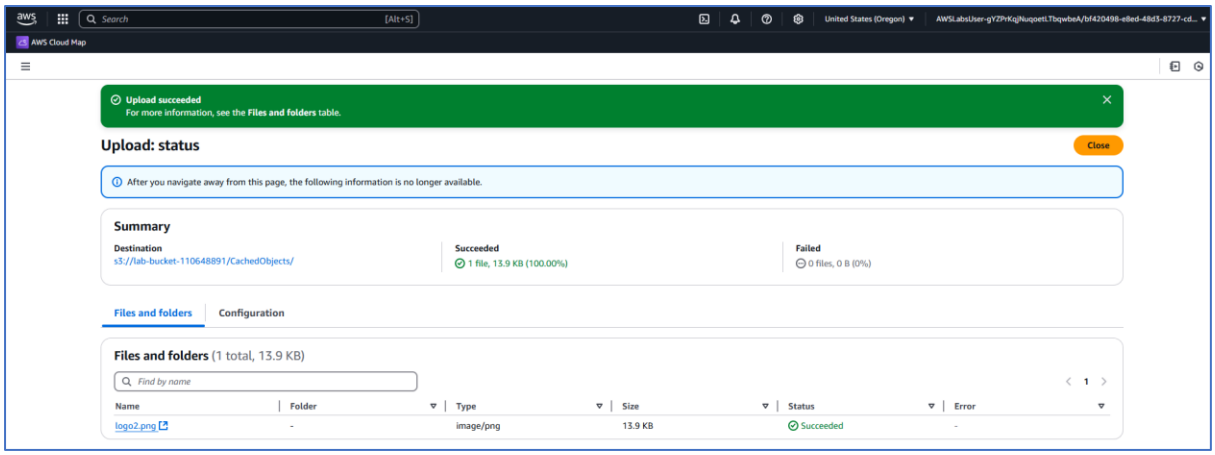
The **Upload** page is displayed.



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

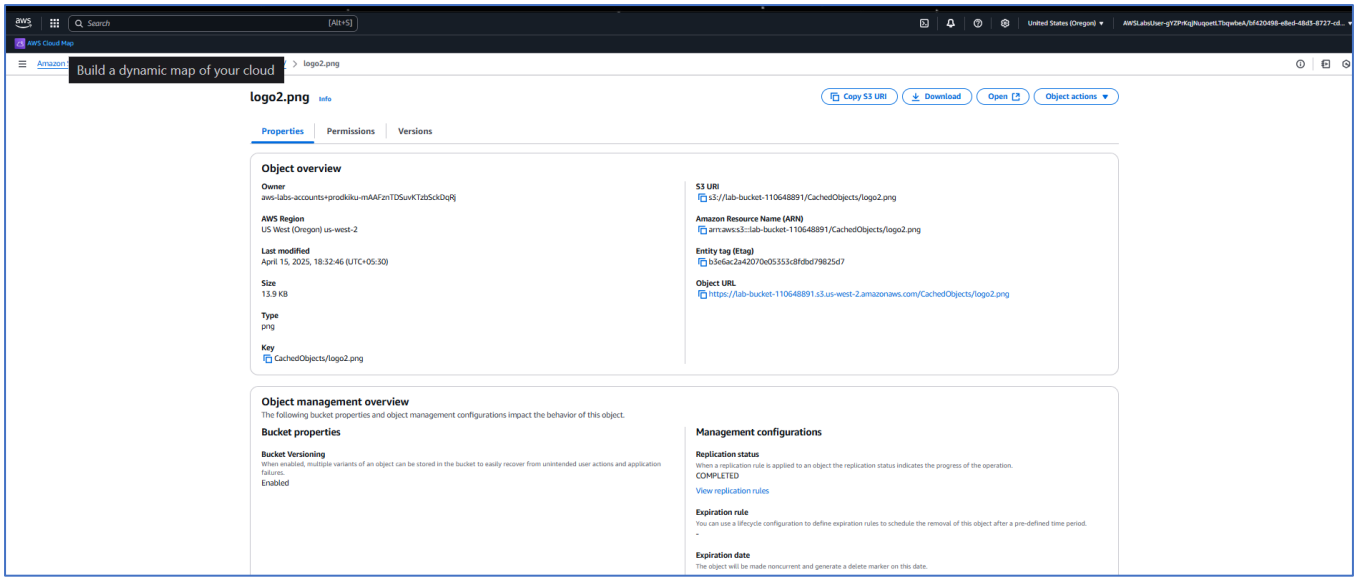
The **Upload: status** page is displayed.

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

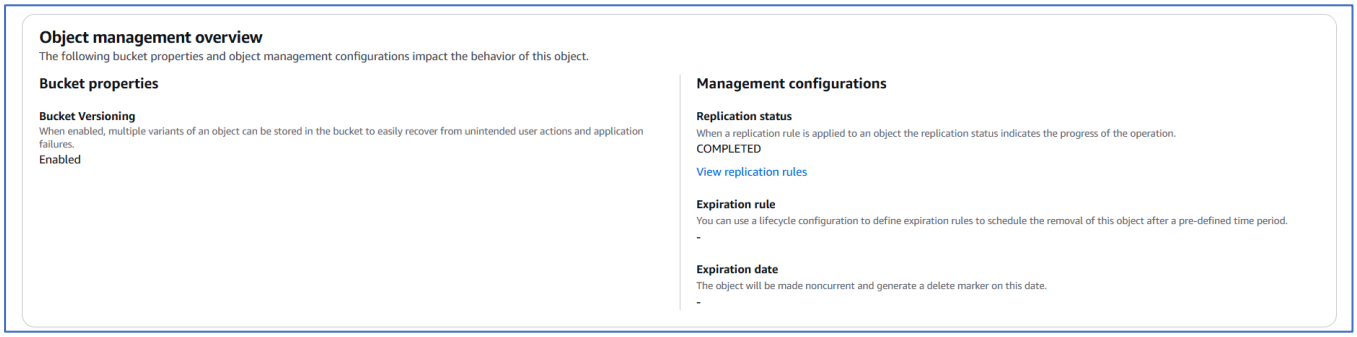


- Choose the link for the logo2.png from the **Files and folders** section.

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

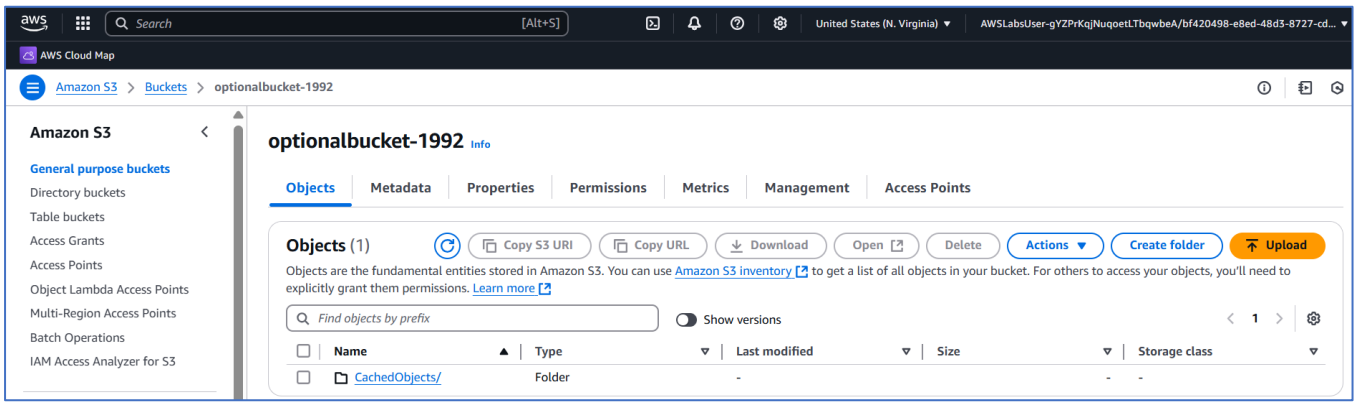


- In the **Object management overview** section, examine *Replication status* and refresh the page periodically until it changes from *PENDING* to *COMPLETED*.



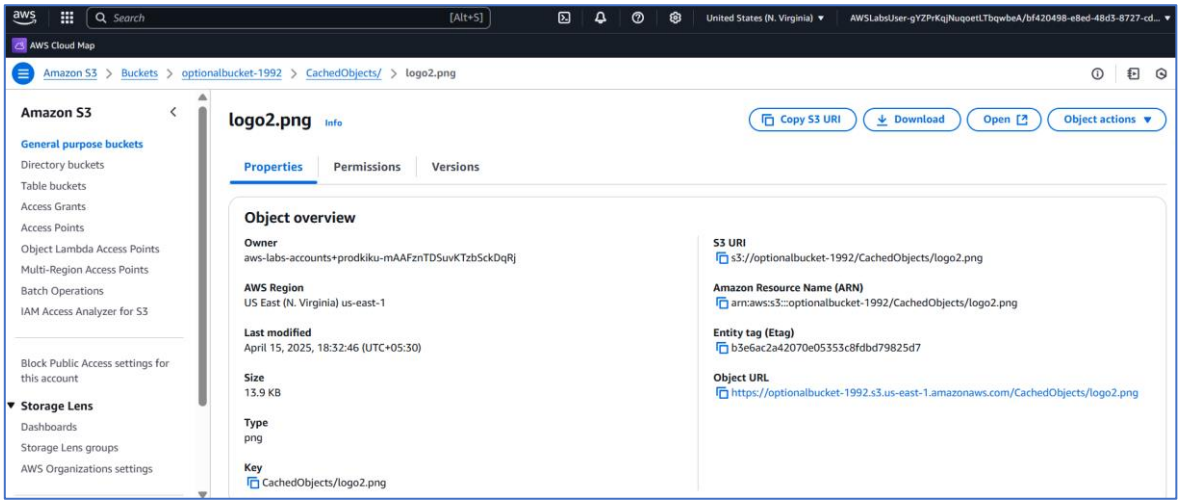
- From the Amazon S3 navigation menu, select **Buckets**.
- In the **Buckets** section, choose the link for the *optionalbucket-1992* .

A page with all the bucket details is displayed.

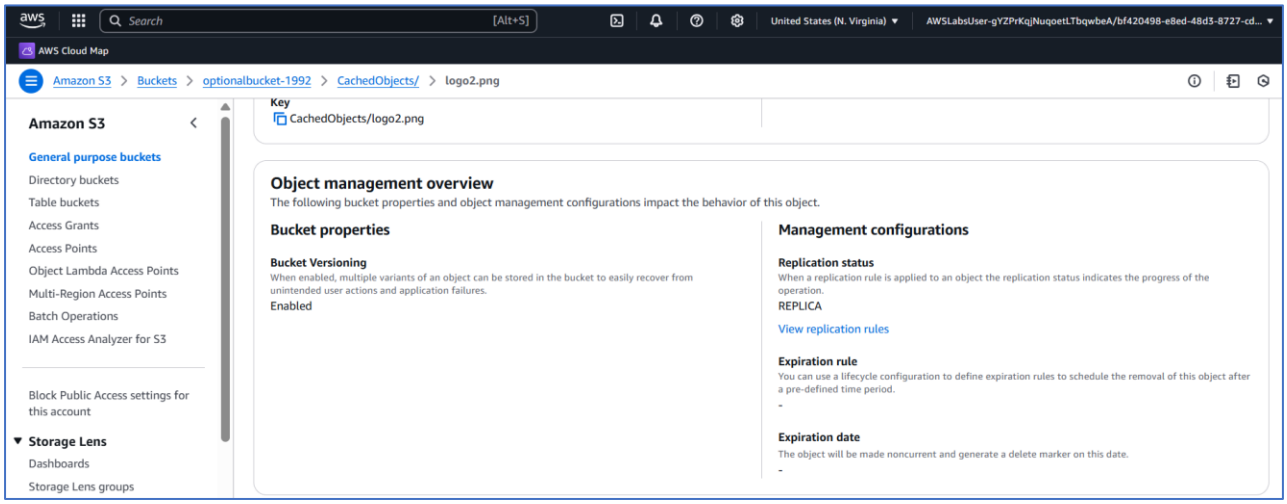


- Choose the link for the CachedObjects/ folder.
- Choose the link for the logo2.png.

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

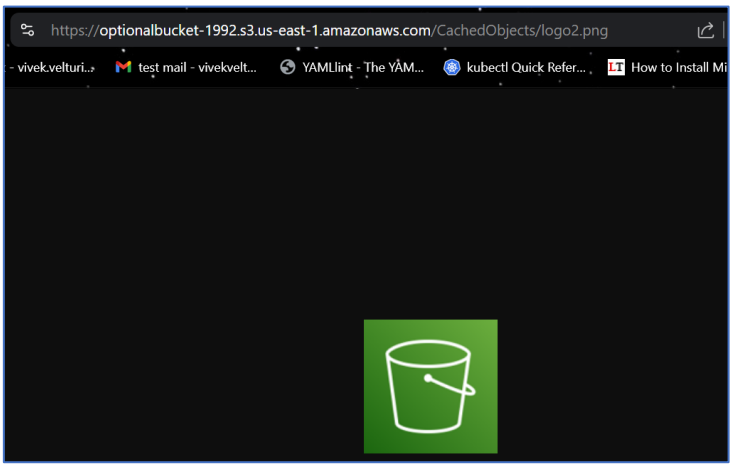


- In the **Object management overview** section, examine *Replication Status*. It displays **REPLICA**.



- 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.