Hands-on tutorials

Deliver Content Faster with Amazon CloudFront

Deliver Content Faster with Amazon CloudFront: Hands-on tutorials

Table of Contents

Deliver Content Faster with Amazon CloudFront ... i
Overview ... 1
Implementation ... 2
Conclusion ... 16

Deliver Content Faster with Amazon CloudFront

AWS experience	Beginner
Time to complete	10 minutes
Cost to complete	Free Tier eligible
Requires	- AWS Account **Note** Accounts created within the past 24 hours might not yet have access to the services required for this tutorial. - Recommended browser: The latest version of Chrome or Firefox
Last updated	July 1, 2022

Overview

In this tutorial, you will learn how to deliver content and decrease end-user latency of your web application using Amazon CloudFront. CloudFront speeds up content delivery by leveraging its global network of data centers, known as edge locations, to reduce delivery time by caching your content close to your end users. CloudFront fetches your content from an **origin**, such as an Amazon Simple Storage Service (Amazon S3) bucket, an Amazon Elastic Compute Cloud (Amazon EC2) instance, an Elastic Load Balancing (ELB) load balancer, or your own web server, when it's not already in an edge location. CloudFront can be used to deliver your entire website or application, including dynamic, static, streaming, and interactive content.

In the following steps, you will configure an Amazon S3 bucket as the origin and test your distribution using a web browser to ensure that your content is being delivered.

Everything done in this tutorial is free tier eligible.

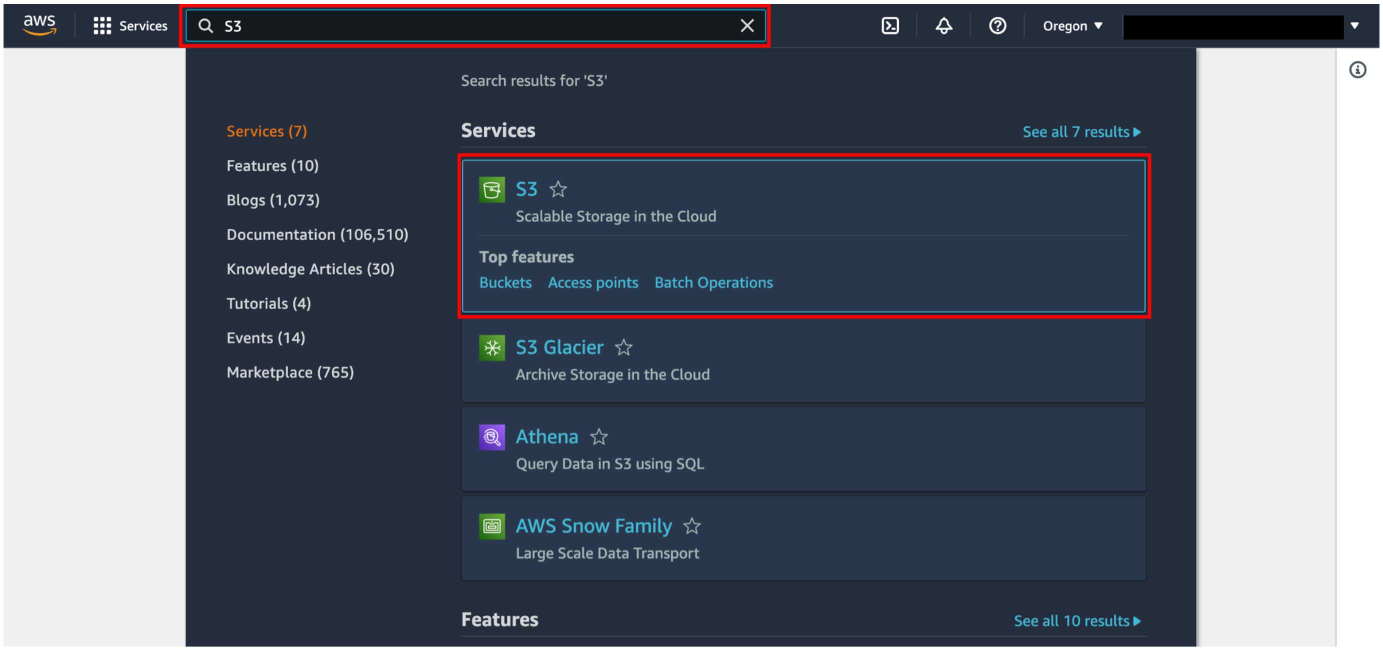
Implementation

Step 1: Prepare your content

In this step, we will upload sample static content to an Amazon S3 bucket. In later steps, we will use this bucket as a CloudFront origin. Amazon S3 is a good choice for an Amazon CloudFront origin that includes static content such as images, videos, HTML pages, .css files, and .js files. Create an HTML file.

1. Enter the Amazon S3 console

   When you click here, the AWS Management Console will open in a new browser window. Type **S3** in the search bar and select **S3** to open the console.

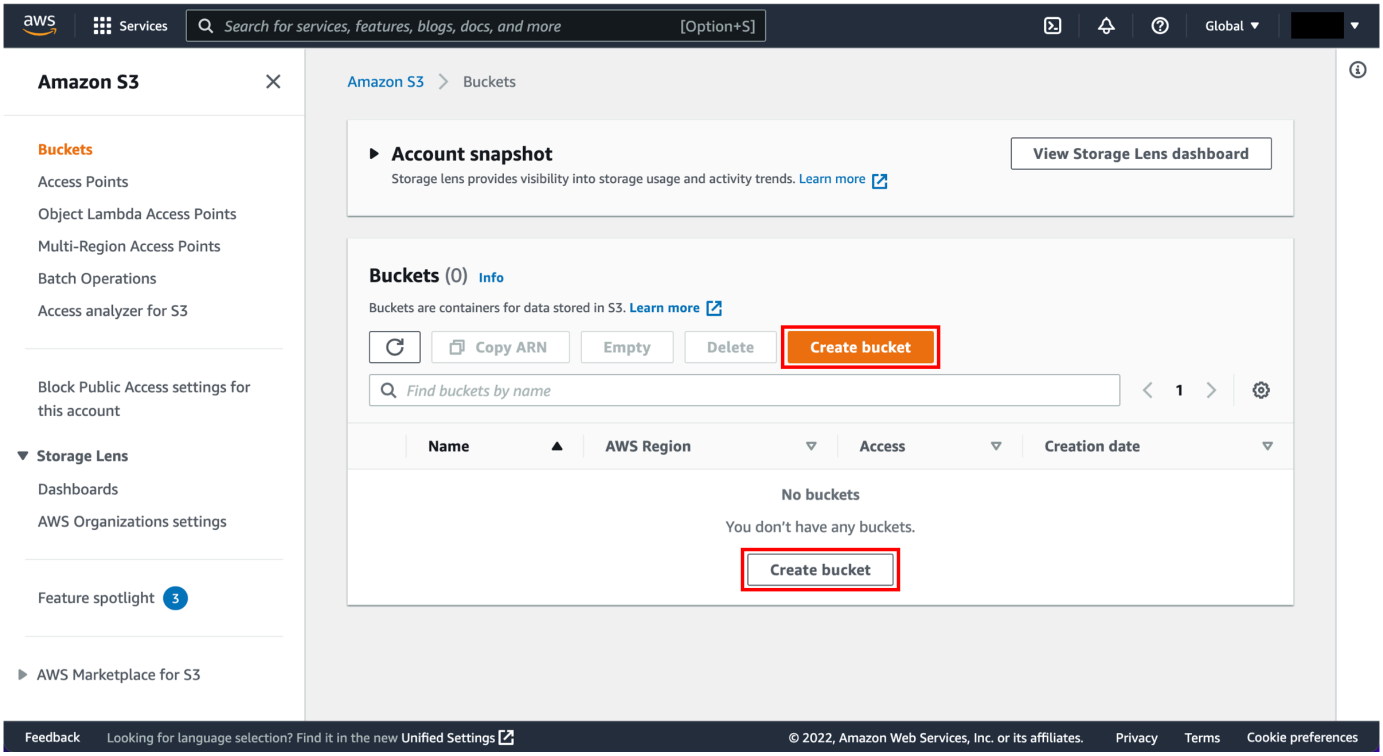


2. Create S3 bucket

   In the S3 dashboard, choose **Create bucket.**

   If this is the first time you have created a bucket, you will see a screen that looks like the image pictured here.

   If you have already created S3 buckets, your S3 dashboard will list all the buckets you have created.



Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets are containers for data stored in S3. Learn more

No buckets

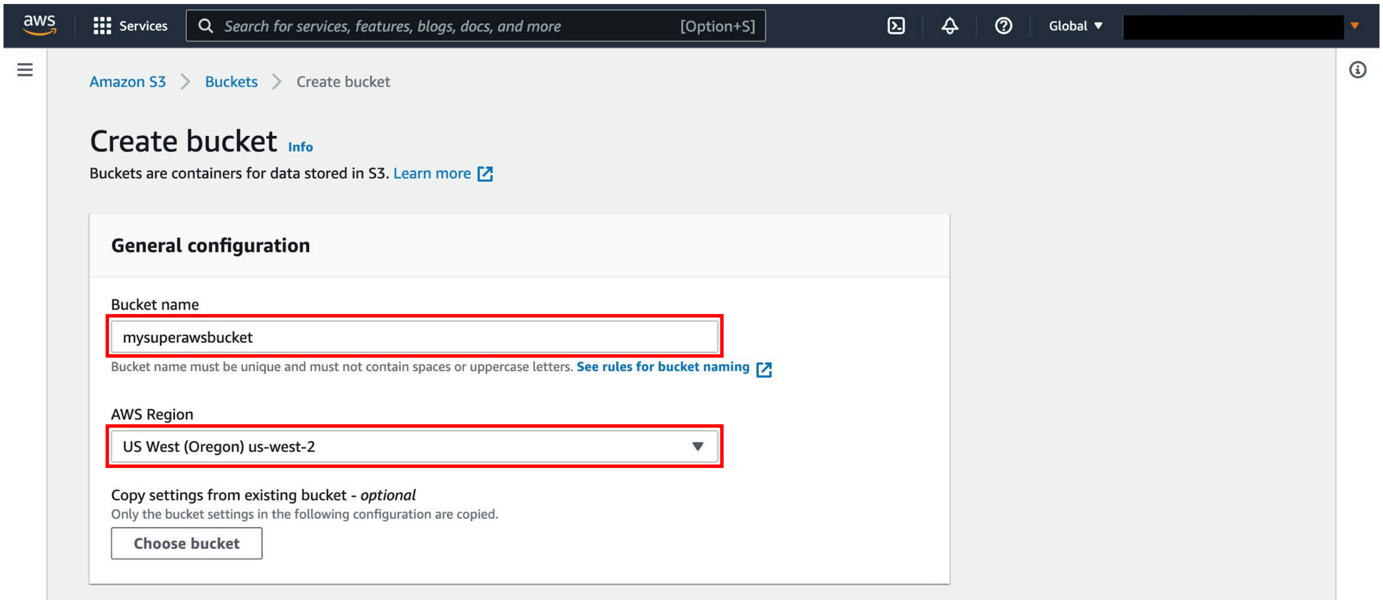
You don't have any buckets.

Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates.

3. Enter bucket name

Enter a unique bucket name. Bucket names must be unique across all existing bucket names in Amazon S3. There are a number of other restrictions on S3 bucket names as well. Then select a Region to create your bucket in.


aws
Services
Search for services, features, blogs, docs, and more
[Option+S]
Global
[redacted]
Amazon S3 > Buckets > Create bucket
Info
Choose bucket

Create bucket

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name: mysuperawsbucket

Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming

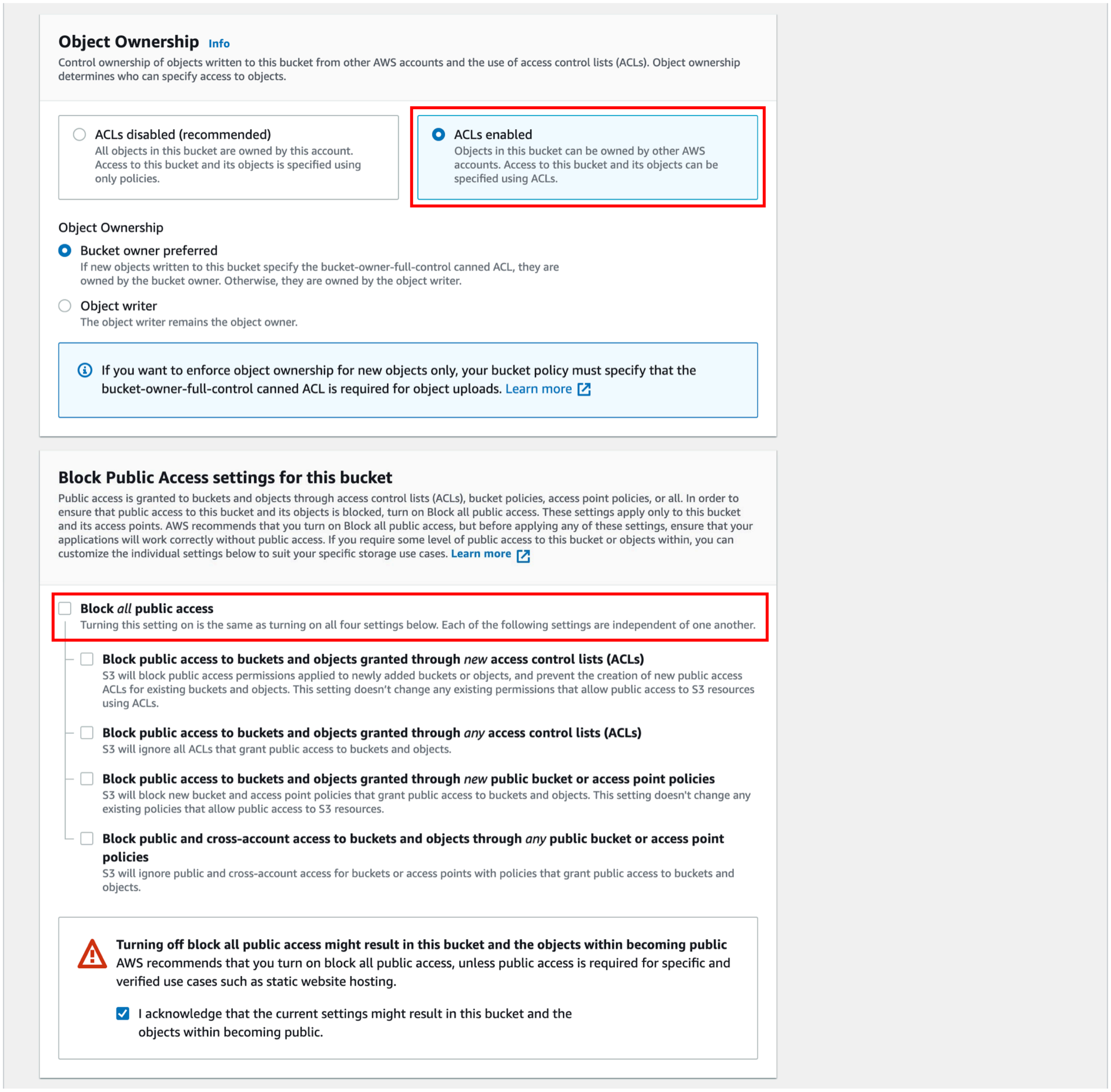
AWS Region: US West (Oregon) us-west-2

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

4. Set permission settings

You have the ability to set permission settings for your S3 bucket. By default, S3 objects are set to private. You will need to make your image publicly readable. Select **ACLs enabled** under Object Ownership, deselect “**Block all public access**” and select the checkbox **“I acknowledge that the current settings might result in this bucket and the objects within becoming public.”**



Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

○ ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

● ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership

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

○ Object writer
The object writer remains the object owner.

If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more

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.

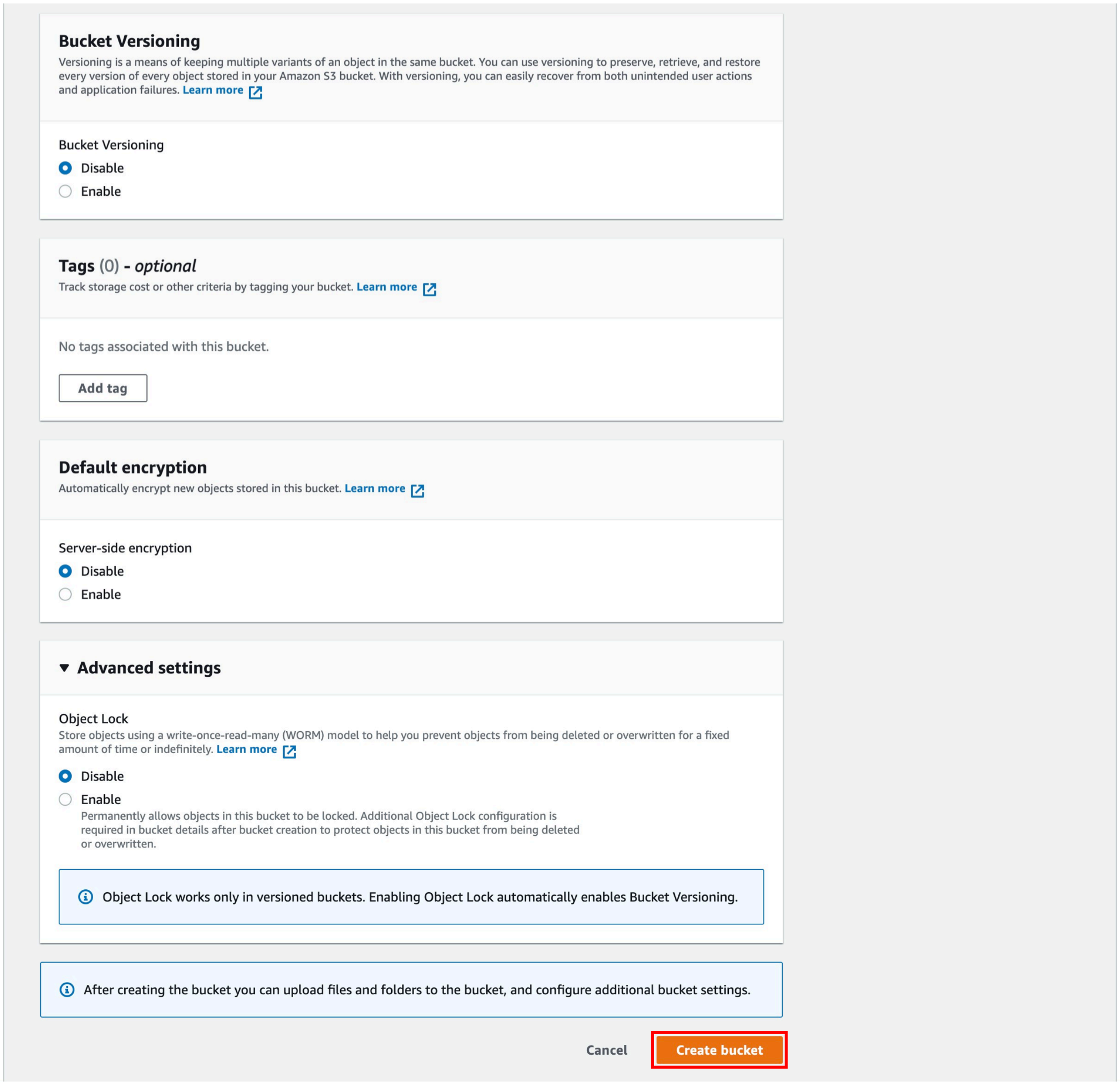
Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

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

5. Create the bucket

You have many useful options for your S3 bucket including Versioning, Server Access Logging, Tags, Object-level Logging and Default Encryption. We won't enable these features for this tutorial.

Select **Create bucket.**



Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning

● Disable

○ Enable

Tags (0) - *optional*

Track storage cost or other criteria by tagging your bucket. Learn more

No tags associated with this bucket.

Default encryption

Automatically encrypt new objects stored in this bucket. Learn more

Server-side encryption

● Disable

○ Enable

▼ Advanced settings

Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Learn more

● Disable

○ Enable

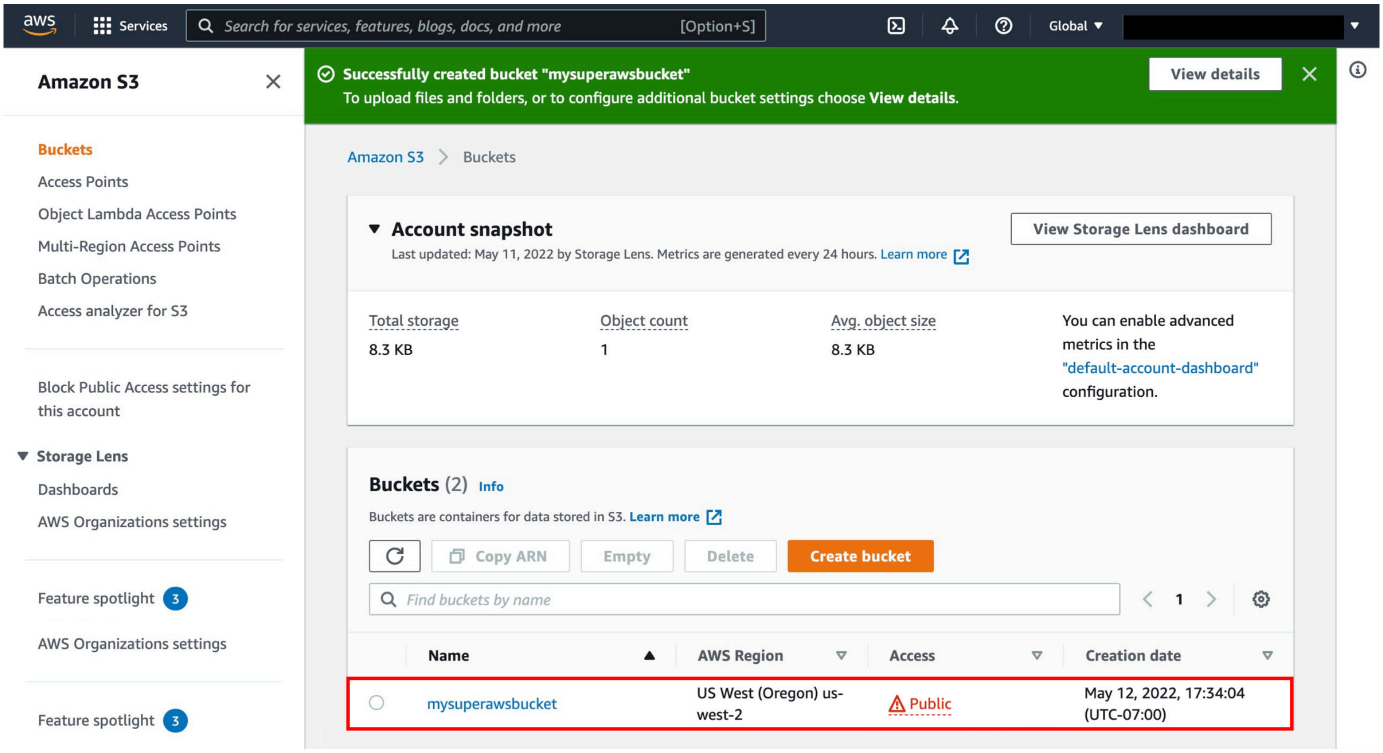
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Bucket Versioning.

After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

6. Navigate to the new bucket

You will see your new bucket in the S3 console. Click on your bucket's name to navigate to the bucket. Your bucket name will not be the same as pictured in the screenshot to the right.



Successfully created bucket "mysuperawsbucket"
To upload files and folders, or to configure additional bucket settings choose **View details**.

▼ **Account snapshot**

Last updated: May 11, 2022 by Storage Lens. Metrics are generated every 24 hours. Learn more

Total storage	Object count	Avg. object size	You can enable advanced metrics in the "default-account-dashboard" configuration.
8.3 KB	1	8.3 KB	

Buckets (2) Info

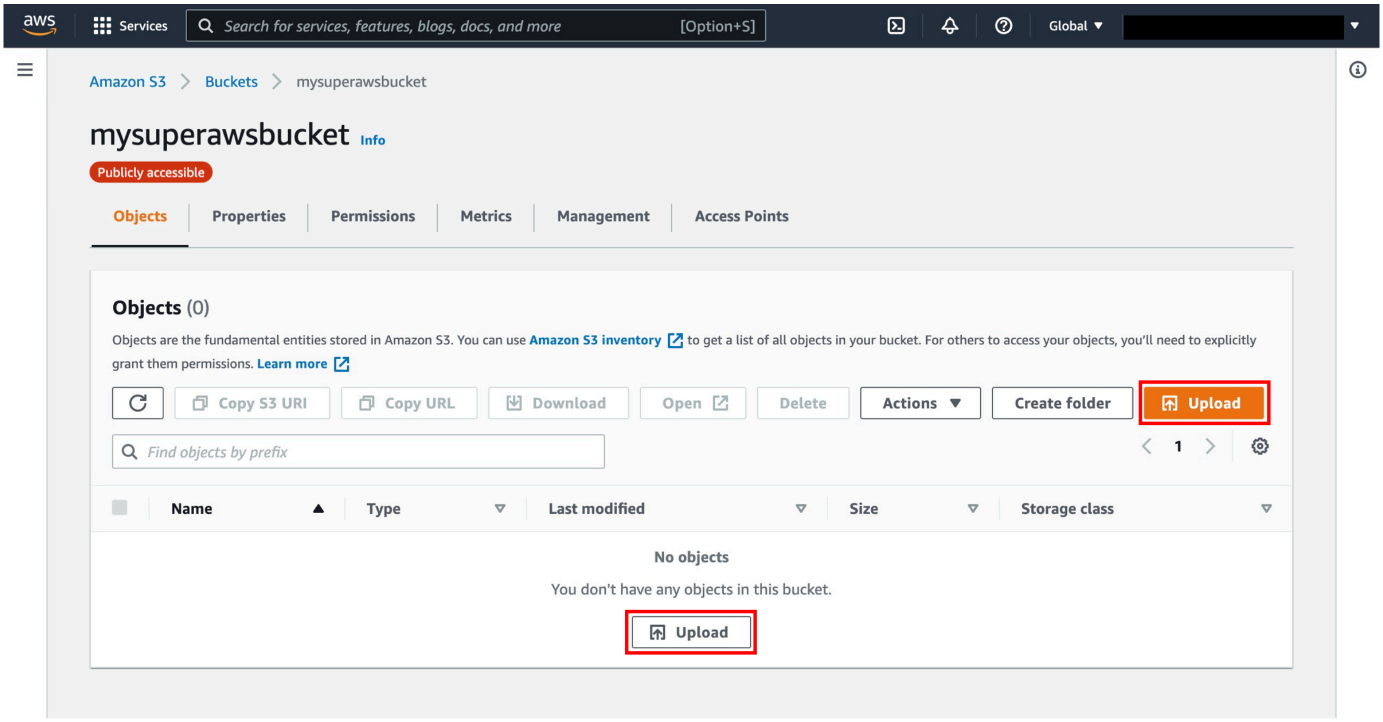
Buckets are containers for data stored in S3. Learn more

	Name ▲	AWS Region ▽	Access ▽	Creation date ▽
○	mysuperawsbucket	US West (Oregon) us-west-2	⚠ Public	May 12, 2022, 17:34:04 (UTC-07:00)

7. Select Upload

You are in your bucket's home page.

Select **Upload**.



mysuperawsbucket Info

Publicly accessible

Objects (0)

Objects are the fundamental entities stored in Amazon S3. You can use **Amazon S3 inventory** to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. **Learn more**

□	Name ▲	Type ▽	Last modified ▽	Size ▽	Storage class ▽

No objects

You don't have any objects in this bucket.

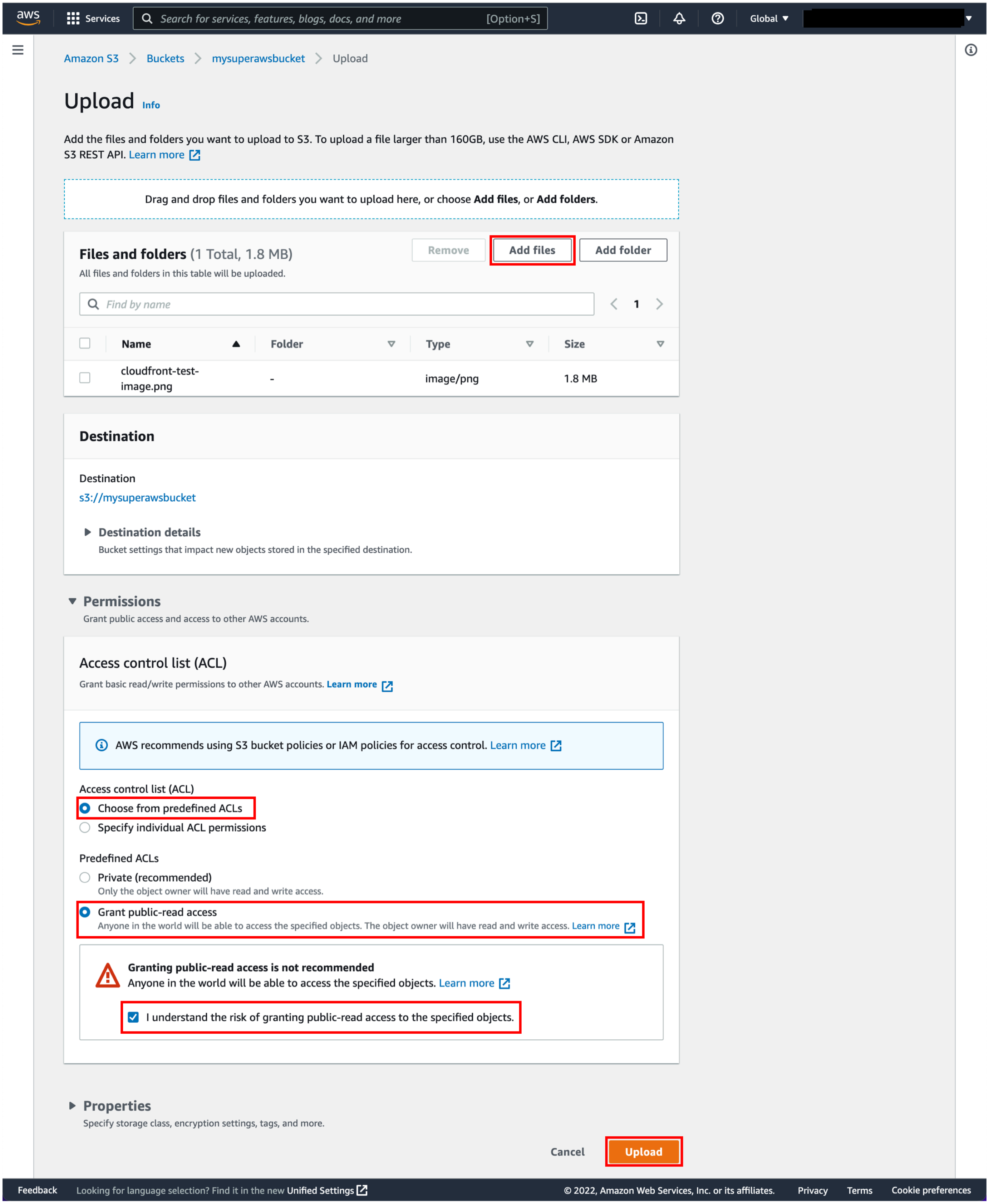
Upload

8. Upload sample content

    Upload the **cloudfront-test-image.png** file by selecting **Add files** and selecting the file **or** dragging the **cloudfront-test-image.png** file to the upload box.

    Open the **Permissions** dropdown. Select **Choose from predefined ACLs** and then select **Grant public-read access.** Select the checkbox **“I understand the risk of granting public-read access to the specified objects.”**

    Select **Upload**.



aws
Services
Search for services, features, blogs, docs, and more [Option+S]
Global
[redacted]

Amazon S3 > Buckets > mysuperawsbucket > Upload

Upload Info

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

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

Files and folders (1 Total, 1.8 MB)

All files and folders in this table will be uploaded.

□	Name	Folder	Type	Size
□	cloudfront-test-image.png	-	image/png	1.8 MB

Destination

Destination
s3://mysuperawsbucket

Destination details
Bucket settings that impact new objects stored in the specified destination.

Permissions
Grant public access and access to other AWS accounts.

Access control list (ACL)
Grant basic read/write permissions to other AWS accounts. Learn more

AWS recommends using S3 bucket policies or IAM policies for access control. Learn more

Access control list (ACL)
● Choose from predefined ACLs
○ Specify individual ACL permissions

Predefined ACLs
○ Private (recommended)
Only the object owner will have read and write access.
● Grant public-read access
Anyone in the world will be able to access the specified objects. The object owner will have read and write access. Learn more

Granting public-read access is not recommended
Anyone in the world will be able to access the specified objects. Learn more

☑ I understand the risk of granting public-read access to the specified objects.

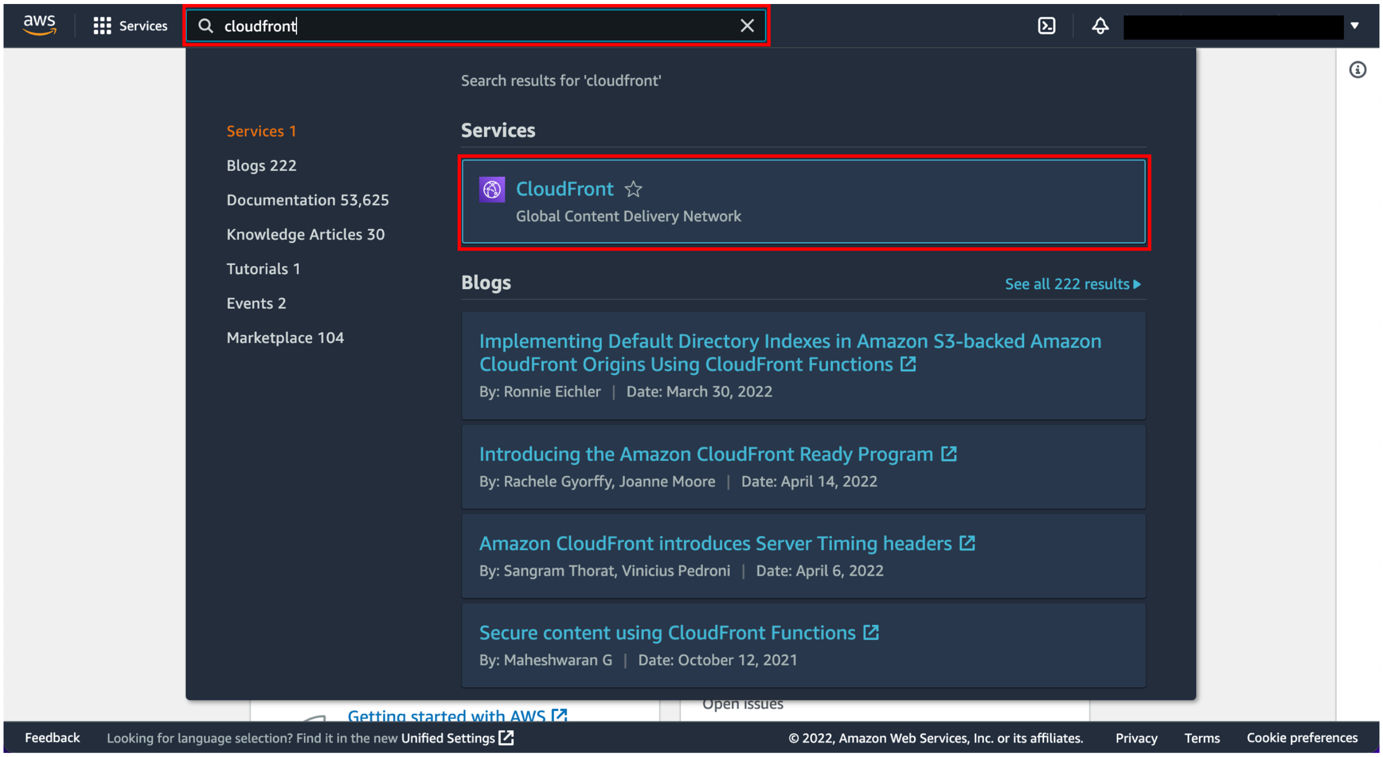
Properties
Specify storage class, encryption settings, tags, and more.

Cancel
Upload
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Step 2: Enter the CloudFront console

1. Open the CloudFront console

   When you click here, the AWS Management Console will open in a new browser tab. Type **CloudFront** in the search bar and select **CloudFront** to open the console.



Search results for 'cloudfront'

Services

CloudFront
Global Content Delivery Network

Blogs See all 222 results

Implementing Default Directory Indexes in Amazon S3-backed Amazon CloudFront Origins Using CloudFront Functions
By: Ronnie Eichler | Date: March 30, 2022

Introducing the Amazon CloudFront Ready Program
By: Rachele Gyorffy, Joanne Moore | Date: April 14, 2022

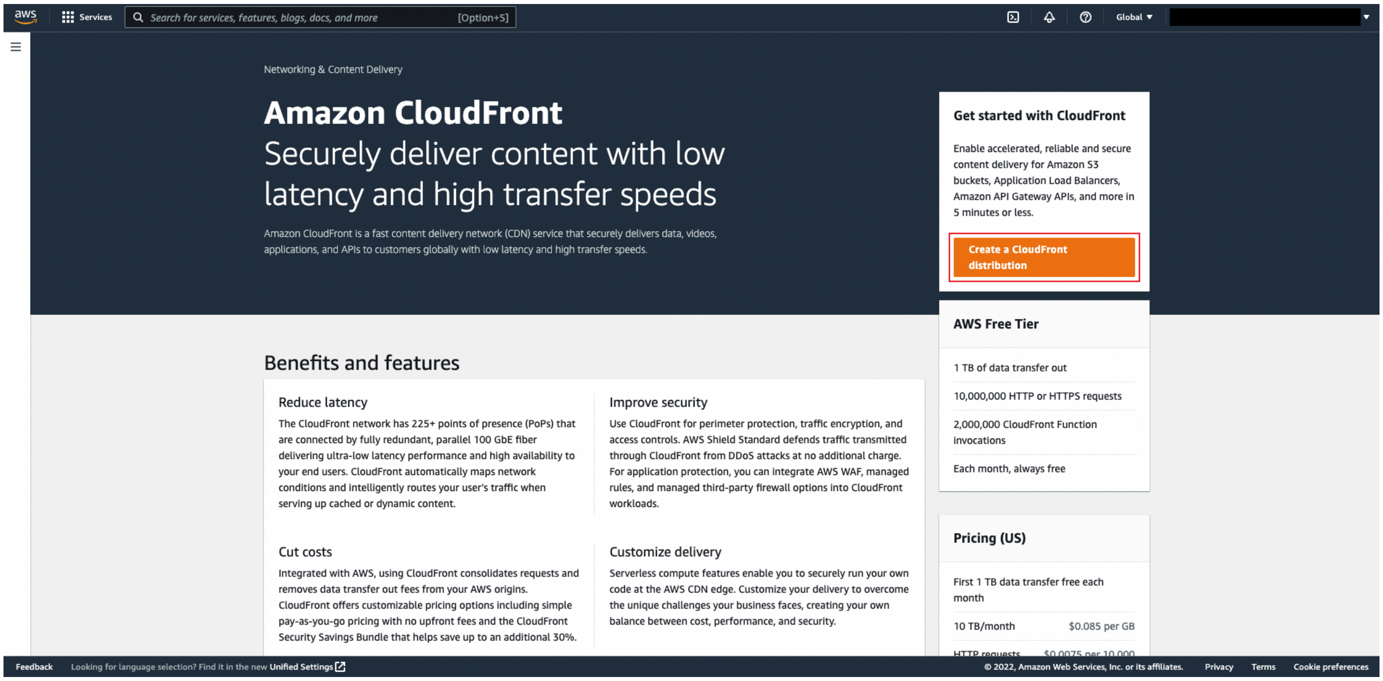
Amazon CloudFront introduces Server Timing headers
By: Sangram Thorat, Vinicius Pedroni | Date: April 6, 2022

Secure content using CloudFront Functions
By: Maheshwaran G | Date: October 12, 2021

© 2022, Amazon Web Services, Inc. or its affiliates.

2. Create a CloudFront distribution

   Select **Create a CloudFront distribution.**


aws
Services
Search for services, features, blogs, docs, and more [Option+S]
Global
[redacted]
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Networking & Content Delivery

Amazon CloudFront

Securely deliver content with low latency and high transfer speeds

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds.

Get started with CloudFront

Enable accelerated, reliable and secure content delivery for Amazon S3 buckets, Application Load Balancers, Amazon API Gateway APIs, and more in 5 minutes or less.

Create a CloudFront distribution

Benefits and features

Reduce latency

The CloudFront network has 225+ points of presence (PoPs) that are connected by fully redundant, parallel 100 GbE fiber delivering ultra-low latency performance and high availability to your end users. CloudFront automatically maps network conditions and intelligently routes your user's traffic when serving up cached or dynamic content.

Improve security

Use CloudFront for perimeter protection, traffic encryption, and access controls. AWS Shield Standard defends traffic transmitted through CloudFront from DDoS attacks at no additional charge. For application protection, you can integrate AWS WAF, managed rules, and managed third-party firewall options into CloudFront workloads.

Cut costs

Integrated with AWS, using CloudFront consolidates requests and removes data transfer out fees from your AWS origins. CloudFront offers customizable pricing options including simple pay-as-you-go pricing with no upfront fees and the CloudFront Security Savings Bundle that helps save up to an additional 30%.

Customize delivery

Serverless compute features enable you to securely run your own code at the AWS CDN edge. Customize your delivery to overcome the unique challenges your business faces, creating your own balance between cost, performance, and security.

AWS Free Tier

1 TB of data transfer out

10,000,000 HTTP or HTTPS requests

2,000,000 CloudFront Function invocations

Each month, always free

Pricing (US)

First 1 TB data transfer free each month

10 TB/month	$0.085 per GB
HTTP requests	$0.0075 per 10,000

Step 3: Configure a Standard distribution

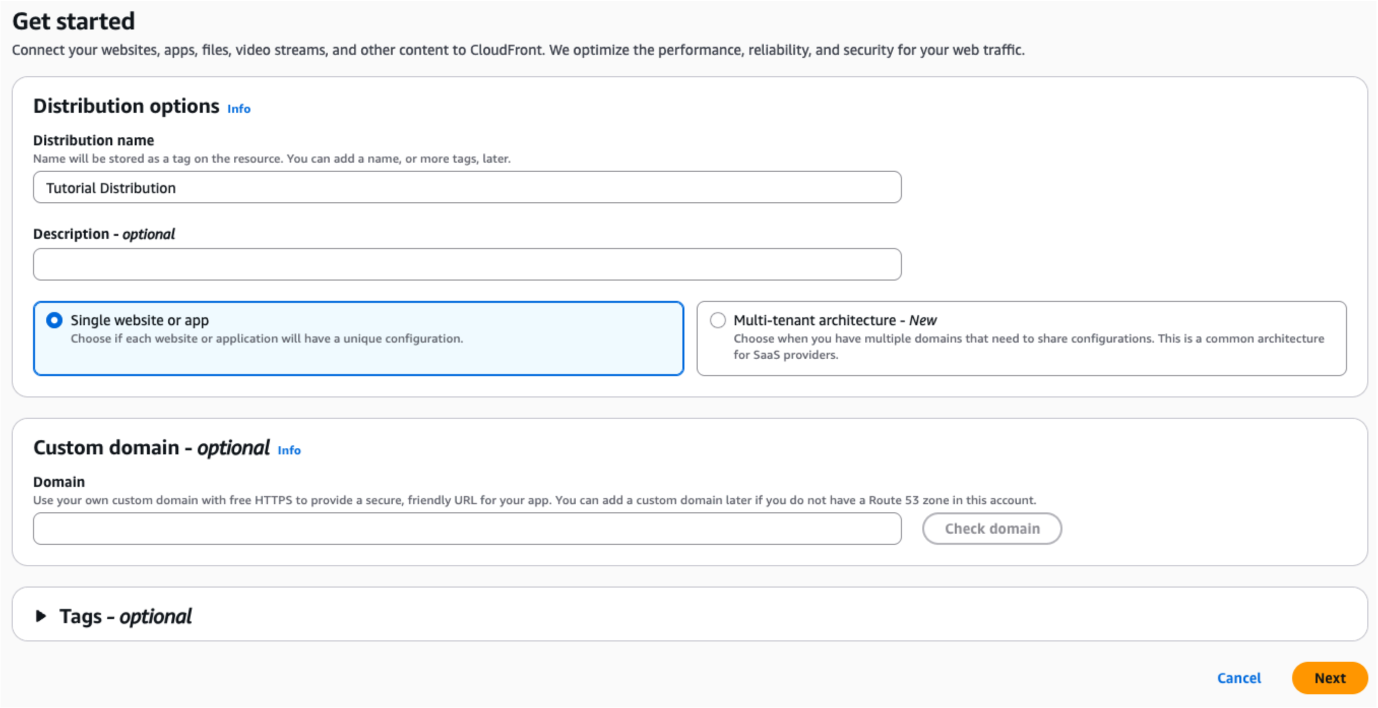
1. Get Started

   Connect your websites, apps, files, video streams, and other content to CloudFront. We optimize the performance, reliability, and security for your web traffic.

   Under Distribution Options, enter a **Distribution name** for the standard distribution and optionally provide a description.

   Make sure you select **Single website or app.**

   For the purpose of this tutorial we will skip the **Custom domain** and **Tags** setup. Leave both of these optional fields blank.



Get started

Connect your websites, apps, files, video streams, and other content to CloudFront. We optimize the performance, reliability, and security for your web traffic.

Distribution options Info

Distribution name

Name will be stored as a tag on the resource. You can add a name, or more tags, later.

Tutorial Distribution

Description - *optional*

● Single website or app
Choose if each website or application will have a unique configuration.

○ Multi-tenant architecture - *New*
Choose when you have multiple domains that need to share configurations. This is a common architecture for SaaS providers.

Custom domain - *optional* Info

Domain

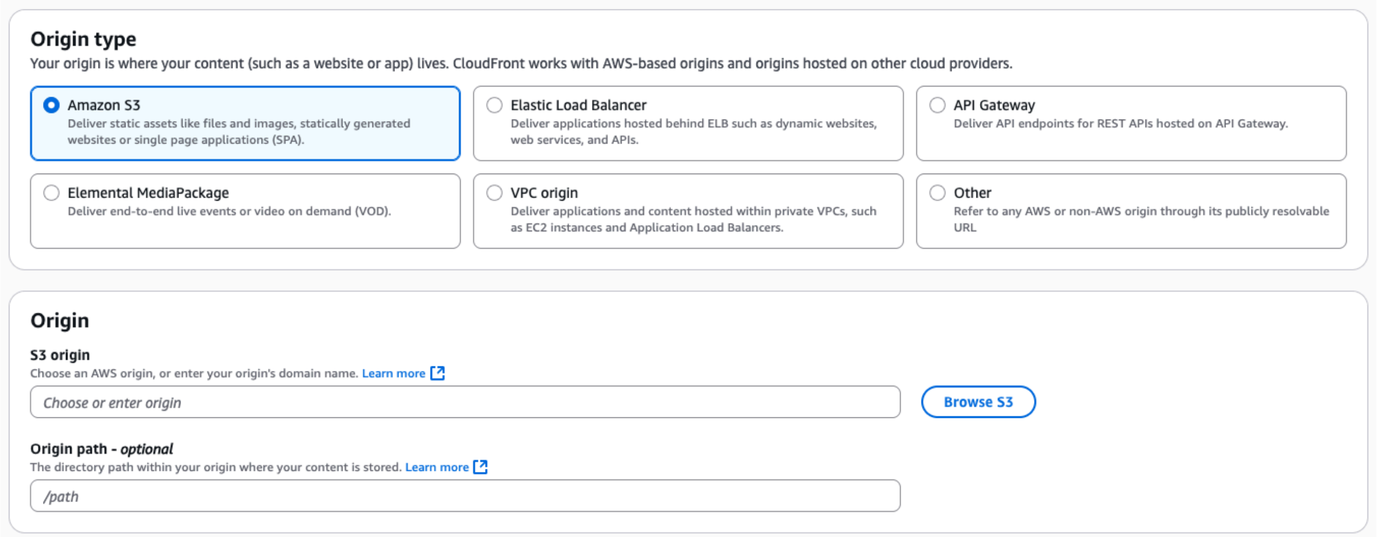
Use your own custom domain with free HTTPS to provide a secure, friendly URL for your app. You can add a custom domain later if you do not have a Route 53 zone in this account.

▶ Tags - *optional*

2. Specify Origin

Under Origin type, select **Amazon S3** (which should be the default value). Under the Origin section, click the **Browse S3** button and select the name of the S3 bucket you stored the cloudfront-test-image.png in.

You can leave the rest of the settings on this page unchanged. This will setup your distribution with the correct settings for caching content from S3 automatically.



Origin type

Your origin is where your content (such as a website or app) lives. CloudFront works with AWS-based origins and origins hosted on other cloud providers.

● Amazon S3
Deliver static assets like files and images, statically generated websites or single page applications (SPA).

○ Elastic Load Balancer
Deliver applications hosted behind ELB such as dynamic websites, web services, and APIs.

○ API Gateway
Deliver API endpoints for REST APIs hosted on API Gateway.

○ Elemental MediaPackage
Deliver end-to-end live events or video on demand (VOD).

○ VPC origin
Deliver applications and content hosted within private VPCs, such as EC2 instances and Application Load Balancers.

○ Other
Refer to any AWS or non-AWS origin through its publicly resolvable URL

Origin

S3 origin

Choose an AWS origin, or enter your origin's domain name. Learn more

Choose or enter origin

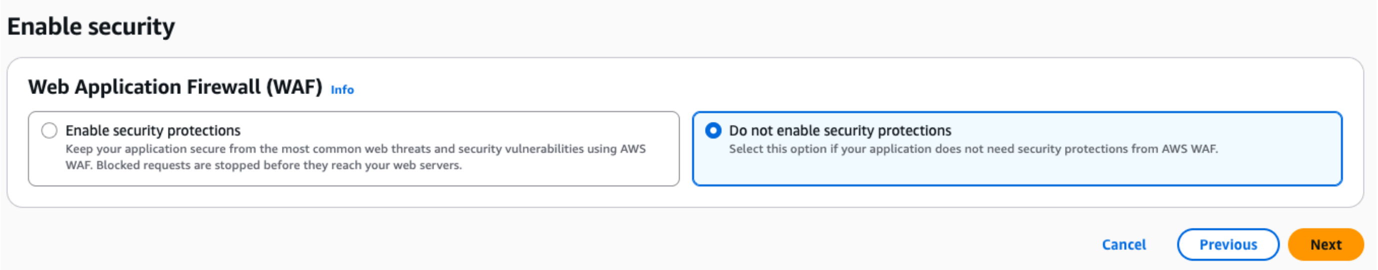
Origin path - *optional*

The directory path within your origin where your content is stored. Learn more

/path

3. Enable Security

For the purposes of this tutorial we will choose **Do not enable security protections**. It is highly recommended to enable security protections for non-tutorial workloads which you will keep running on CloudFront.



Enable security

Web Application Firewall (WAF) Info

○ Enable security protections
Keep your application secure from the most common web threats and security vulnerabilities using AWS WAF. Blocked requests are stopped before they reach your web servers.

● Do not enable security protections
Select this option if your application does not need security protections from AWS WAF.

Step 4: Review Your Changes

- Review your changes to ensure everything is setup correctly and then click **Create Distribution.**

  After CloudFront creates your distribution, the value of the **Status** column for your distribution will change from **Deploying** to the date and time that the distribution is deployed.

> **Note**
>
> This can take a few minutes to complete.

Step 5: Create a distribution

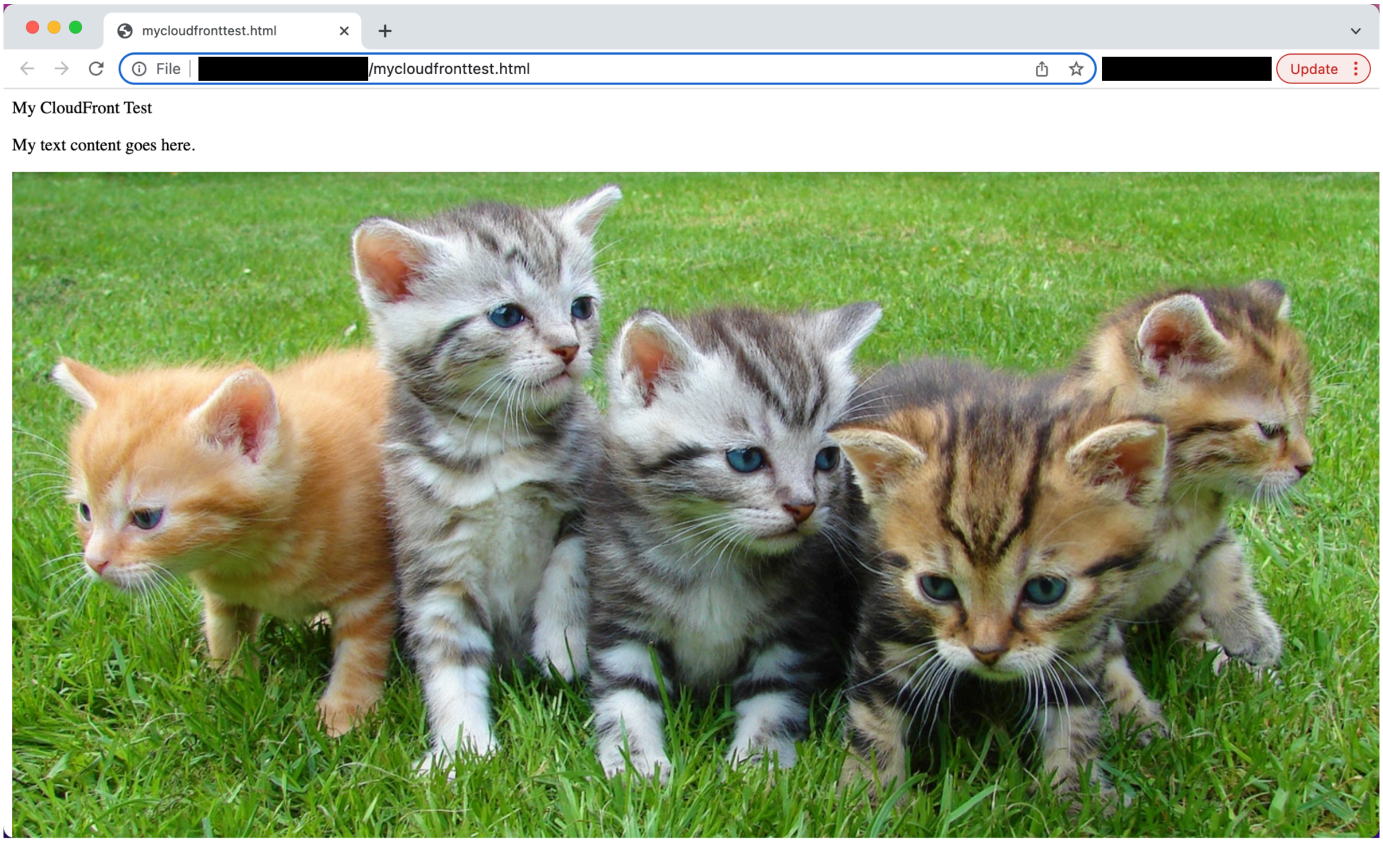
- Create an HTML file

  Open a text editor on your computer. Copy and paste the following HTML code:

```
<html>
<head>My CloudFront Test</head>
<body>
<p>My text content goes here.</p>
<p><img src="http://domain name/object name" alt="my test image">
</body>
</html>
```

- Replace **domain name** with the domain name that CloudFront assigned to your distribution, such as **d111111abcdef8.cloudfront.net**.
- Replace **object name** with the name of your image file in the Amazon S3 bucket - in our case, **cloudfront-test-image.png.**
- Save the text in a file as **mycloudfronttest.html**.

Open your HTML file in a web browser to verify that the link works.



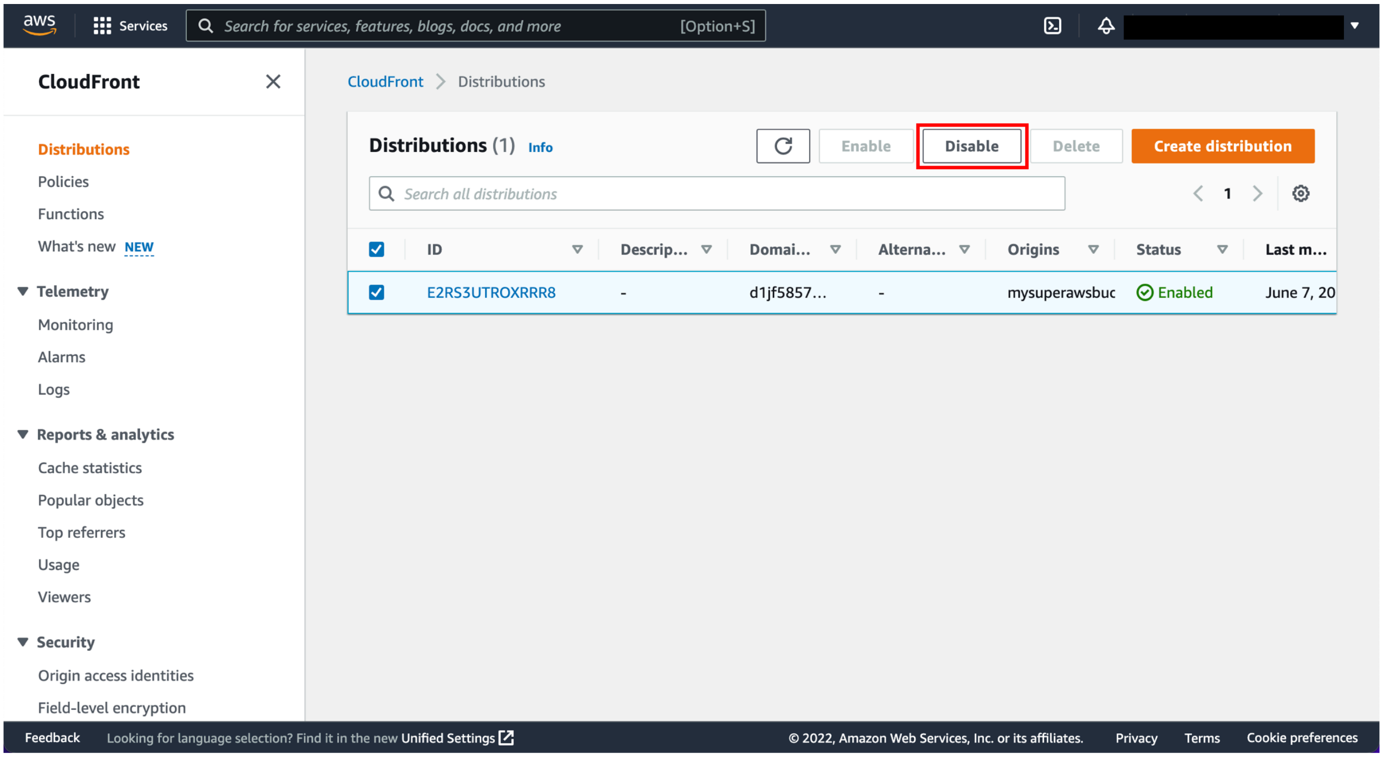
My CloudFront Test

My text content goes here.

(Optional) Disable and delete your distribution

1. Select the distribution to disable

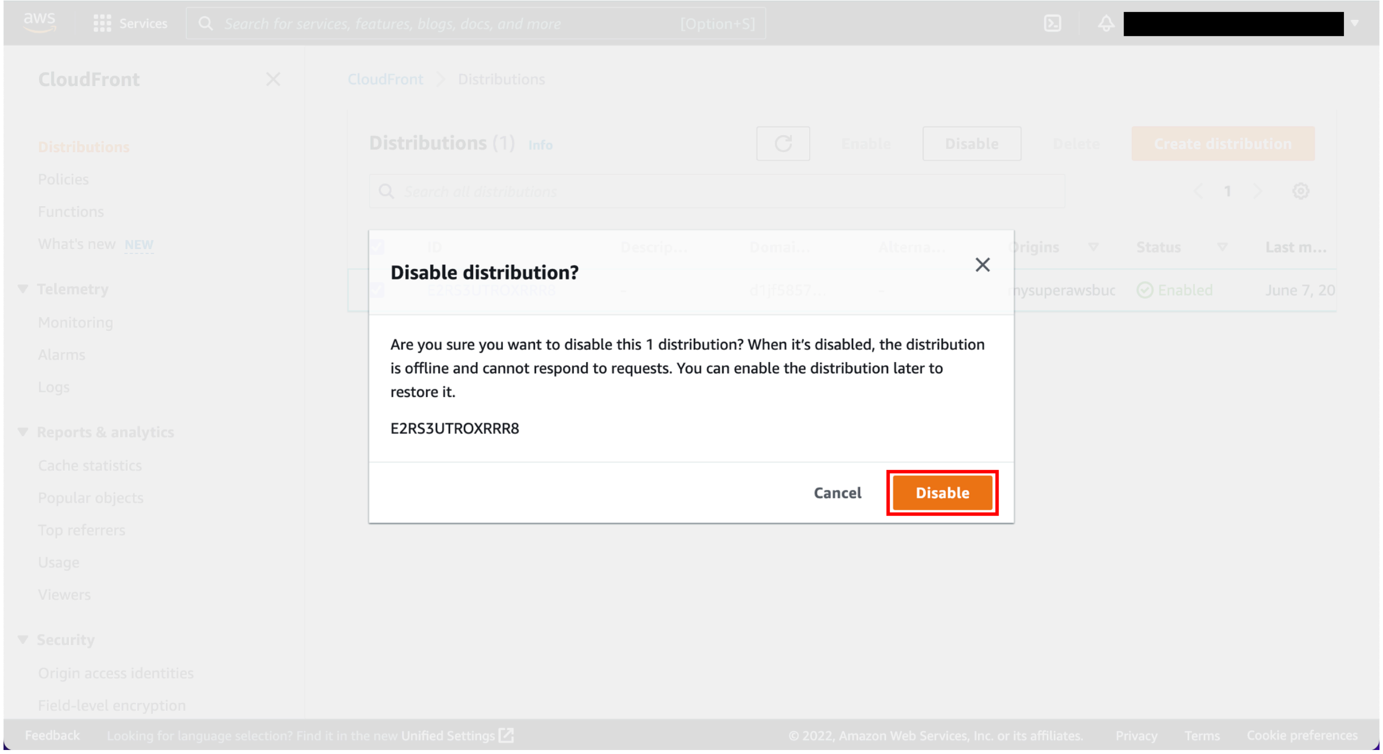
   Select the checkbox next to the distribution you created and choose **Disable**.



☑	ID	Descrip...	Domai...	Alterna...	Origins	Status	Last m...
☑	E2RS3UTROXRRR8	-	d1jf5857...	-	mysuperawsbuc	✓ Enabled	June 7, 20

2. Confirm disabling the distribution

You will be asked to confirm. Choose **Disable**.



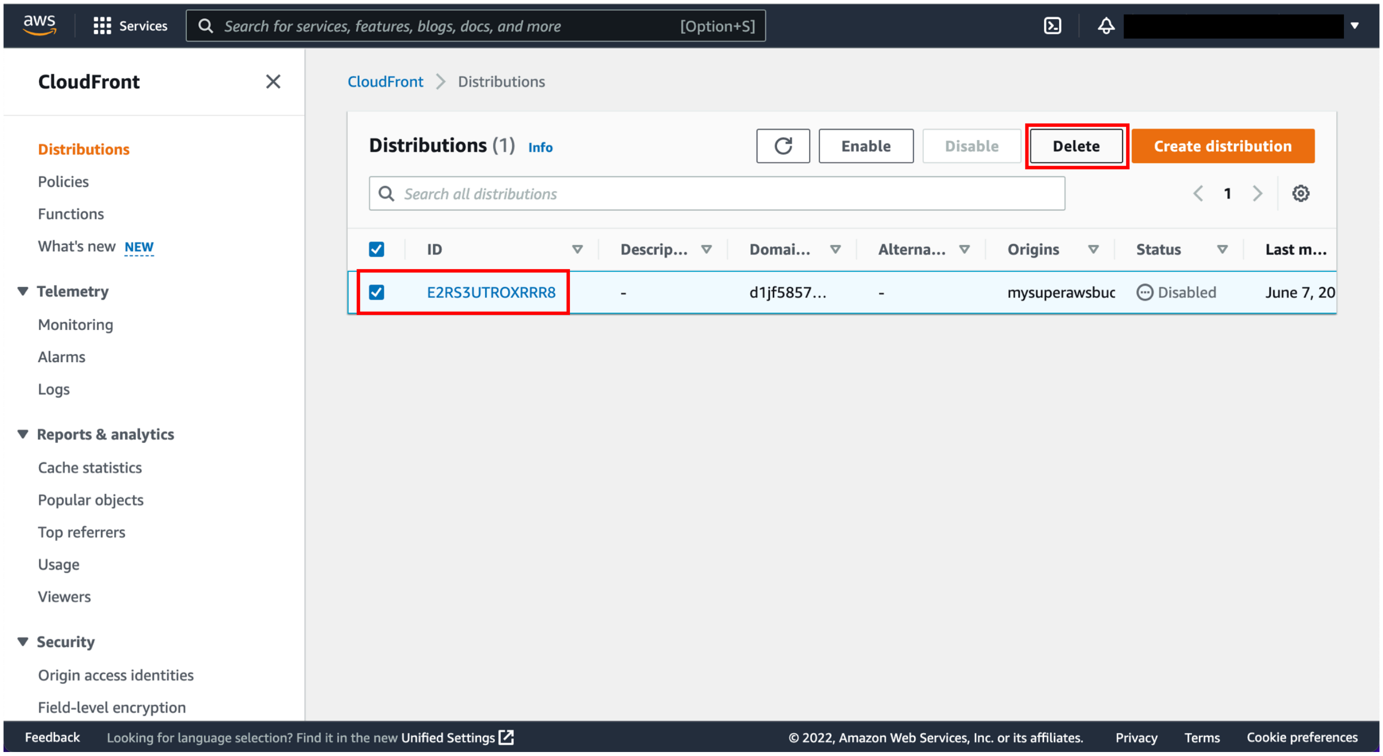
Disable distribution?

Are you sure you want to disable this 1 distribution? When it's disabled, the distribution is offline and cannot respond to requests. You can enable the distribution later to restore it.

E2RS3UTROXRRR8

3. Select the distribution to delete

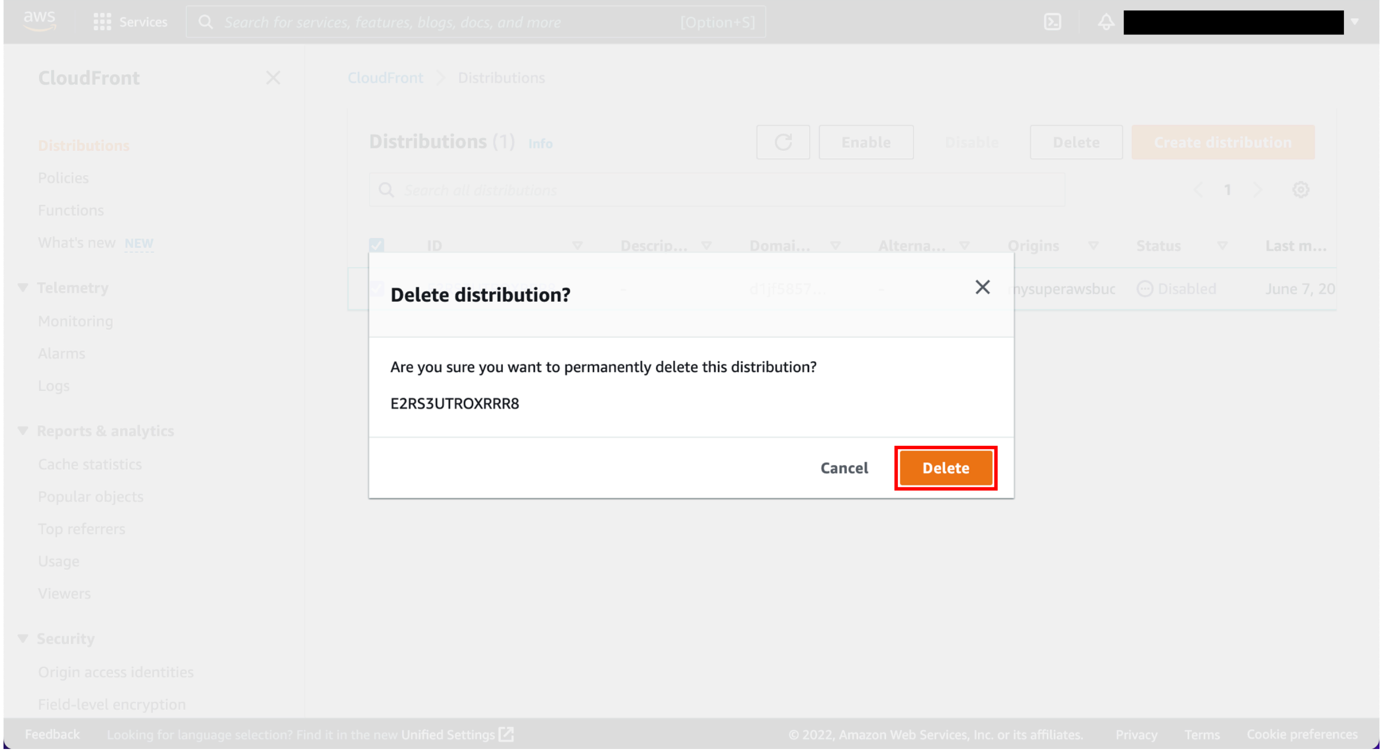
Select the checkbox next to the distribution you created and choose **Delete.**



☑	ID	Descrip…	Domai…	Alterna…	Origins	Status	Last m…
☑	E2RS3UTROXRRR8	-	d1jf5857…	-	mysuperawsbuc	Disabled	June 7, 20

4. Confirm deleting the distribution

You will be asked to confirm. Choose **Delete**.



Are you sure you want to permanently delete this distribution?

E2RS3UTROXRRR8

Conclusion

You created your first Amazon CloudFront web distribution and delivered a piece of static content hosted in the cloud through Amazon S3. With a few configuration changes, you can use CloudFront to deliver dynamic content, live events such as a meeting, conference, or concert, in real time over HTTP or HTTPS. Use Amazon Cloudfront to speed delivery of your entire website or application, including dynamic, static, streaming, and interactive content.