

Hands-on tutorials

Deliver Content Faster with Amazon CloudFront



Deliver Content Faster with Amazon CloudFront: Hands-on tutorials

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

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	<ul style="list-style-type: none">AWS Account <div data-bbox="862 617 1507 930"><p>Note</p><p>Accounts created within the past 24 hours might not yet have access to the services required for this tutorial.</p></div> <ul style="list-style-type: none">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.

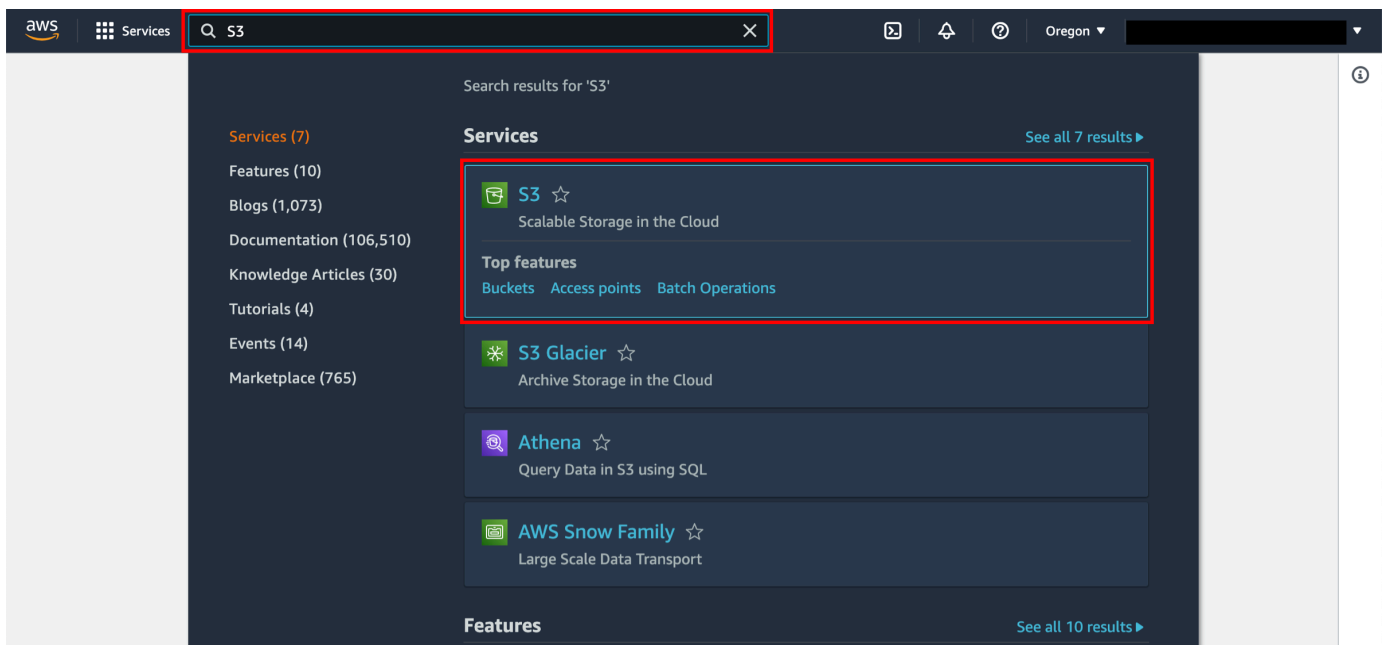
Implementation

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.

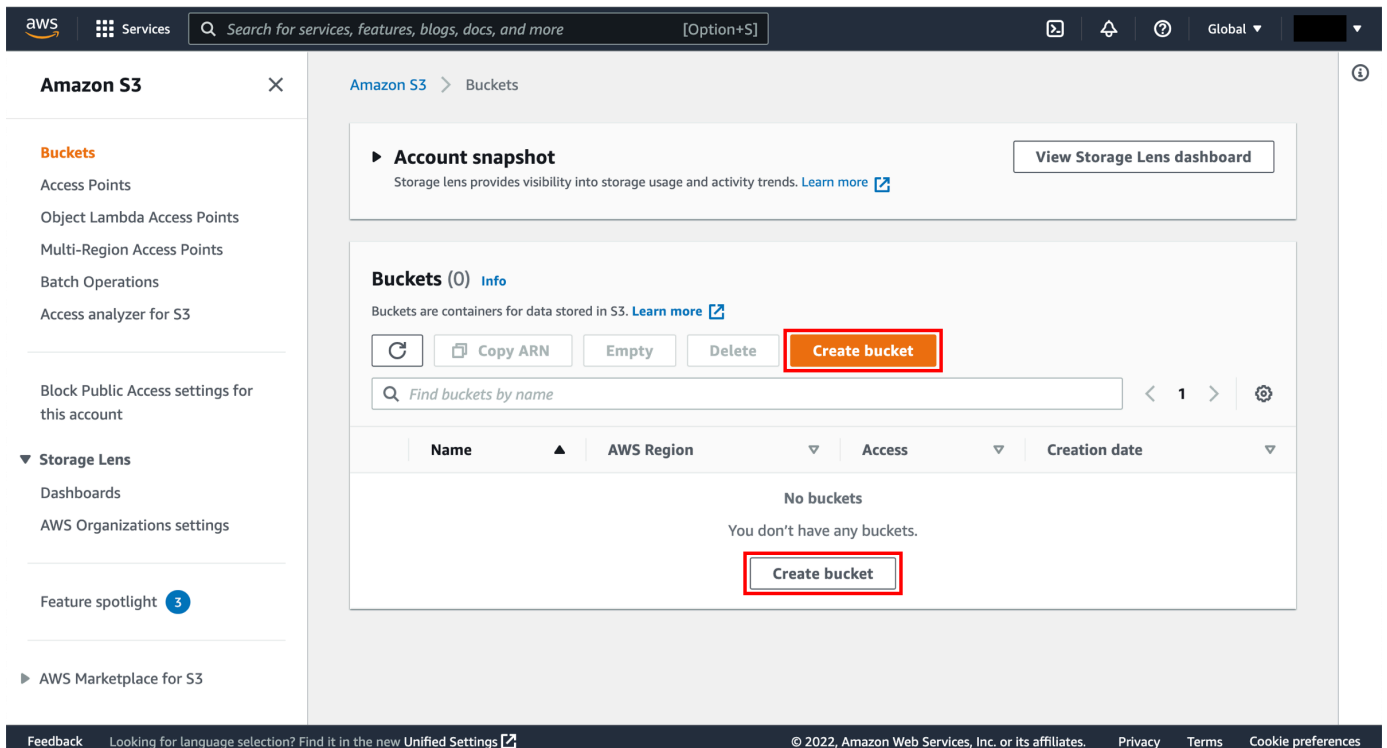


2. Create S3 bucket

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.

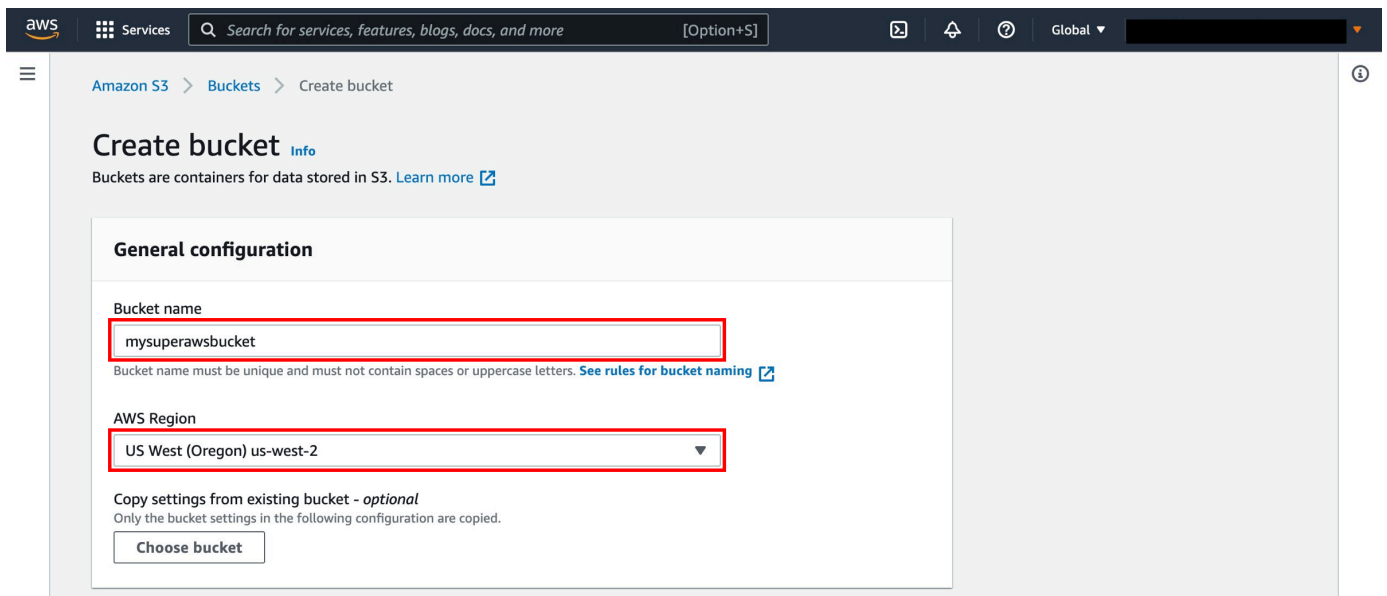
If you have already created S3 buckets, your S3 dashboard will list all the buckets you have created.



The screenshot shows the Amazon S3 console interface. On the left is a navigation sidebar with options like Buckets, Access Points, and Storage Lens. The main content area is titled 'Amazon S3 > Buckets'. It features an 'Account snapshot' section with a 'View Storage Lens dashboard' button. Below that is a 'Buckets (0) Info' section with a description and a 'Learn more' link. A row of action buttons includes 'Refresh', 'Copy ARN', 'Empty', 'Delete', and a highlighted 'Create bucket' button. A search bar 'Find buckets by name' is present. Below the search bar is a table header with columns for Name, AWS Region, Access, and Creation date. The table content shows 'No buckets' with the message 'You don't have any buckets.' and a 'Create bucket' button highlighted in red.

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.



The screenshot shows the 'Create bucket' configuration page in the Amazon S3 console. The breadcrumb trail is 'Amazon S3 > Buckets > Create bucket'. The page title is 'Create bucket' with an 'Info' link. Below the title is a description and a 'Learn more' link. The 'General configuration' section contains two main fields: 'Bucket name' and 'AWS Region'. The 'Bucket name' field contains the text 'mysuperawsbucket' and is highlighted with a red box. Below it is a note: 'Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming'. The 'AWS Region' field is a dropdown menu showing 'US West (Oregon) us-west-2' and is also highlighted with a red box. Below these fields is a section for 'Copy settings from existing bucket - optional' with a 'Choose bucket' button.

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.

[Add tag](#)

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.

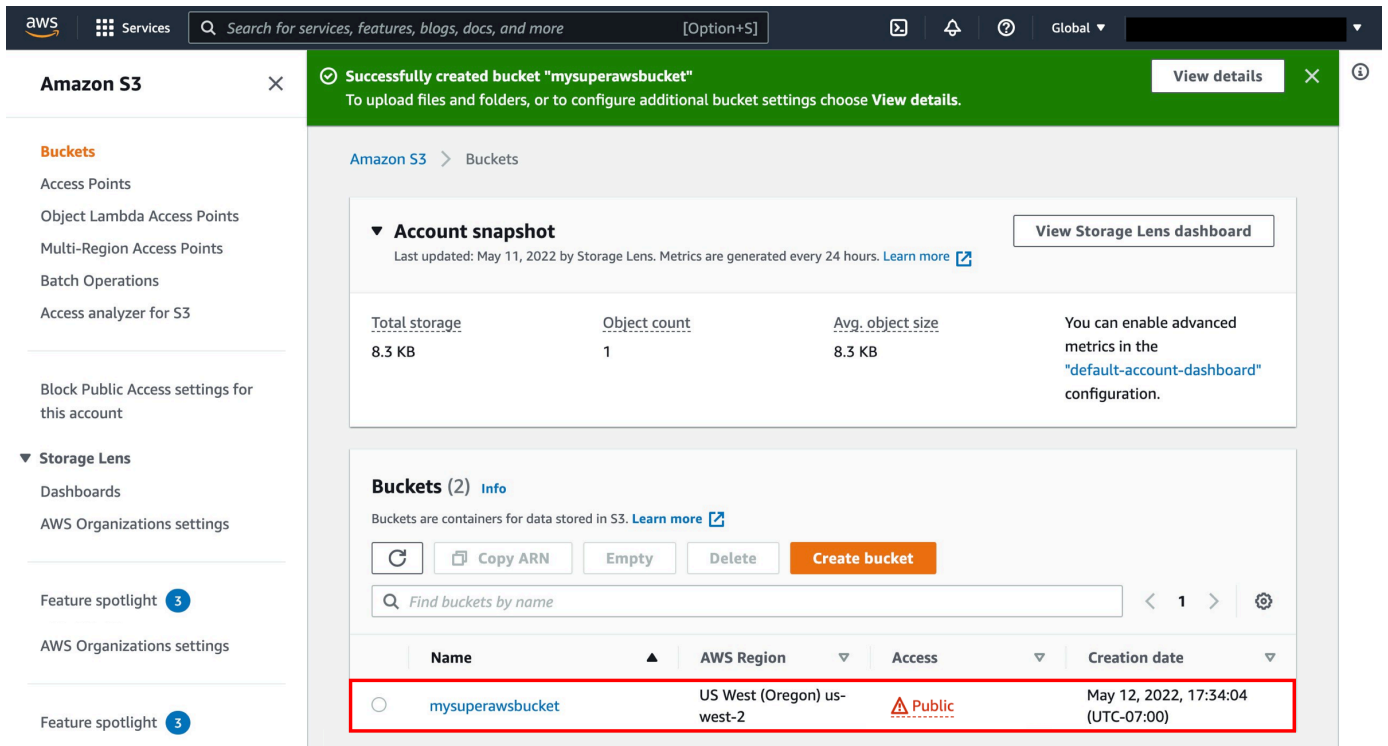
i Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Bucket Versioning.

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

Cancel **Create bucket**

6. Navigate to the new bucket

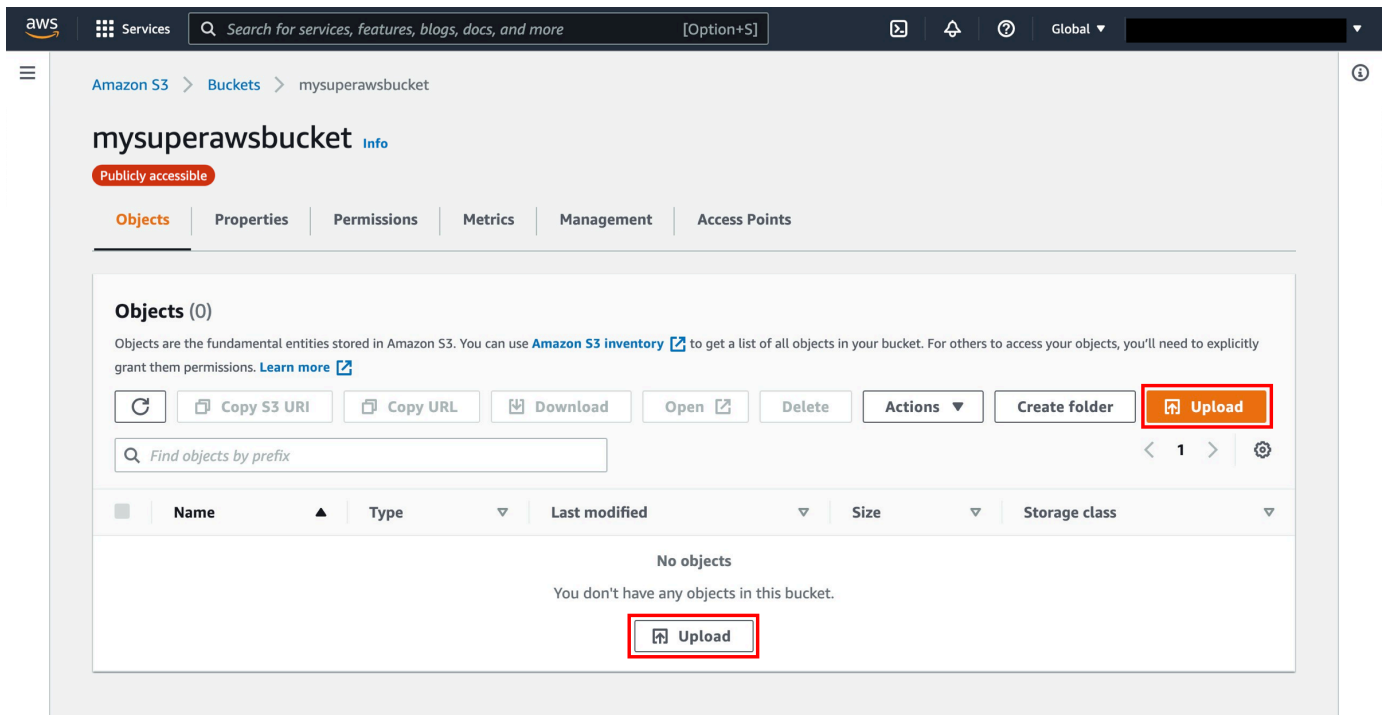
You will see your new bucket in the S3 console. Click on your bucket's name to navigate to the bucket. Your bucket name will not be the same as pictured in the screenshot to the right.



7. Select Upload

You are in your bucket's home page.

Select **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]

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) Remove **Add files** Add folder

All files and folders in this table will be uploaded.

Find by name < 1 >

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	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](#)

Info 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](#)

Warning **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.

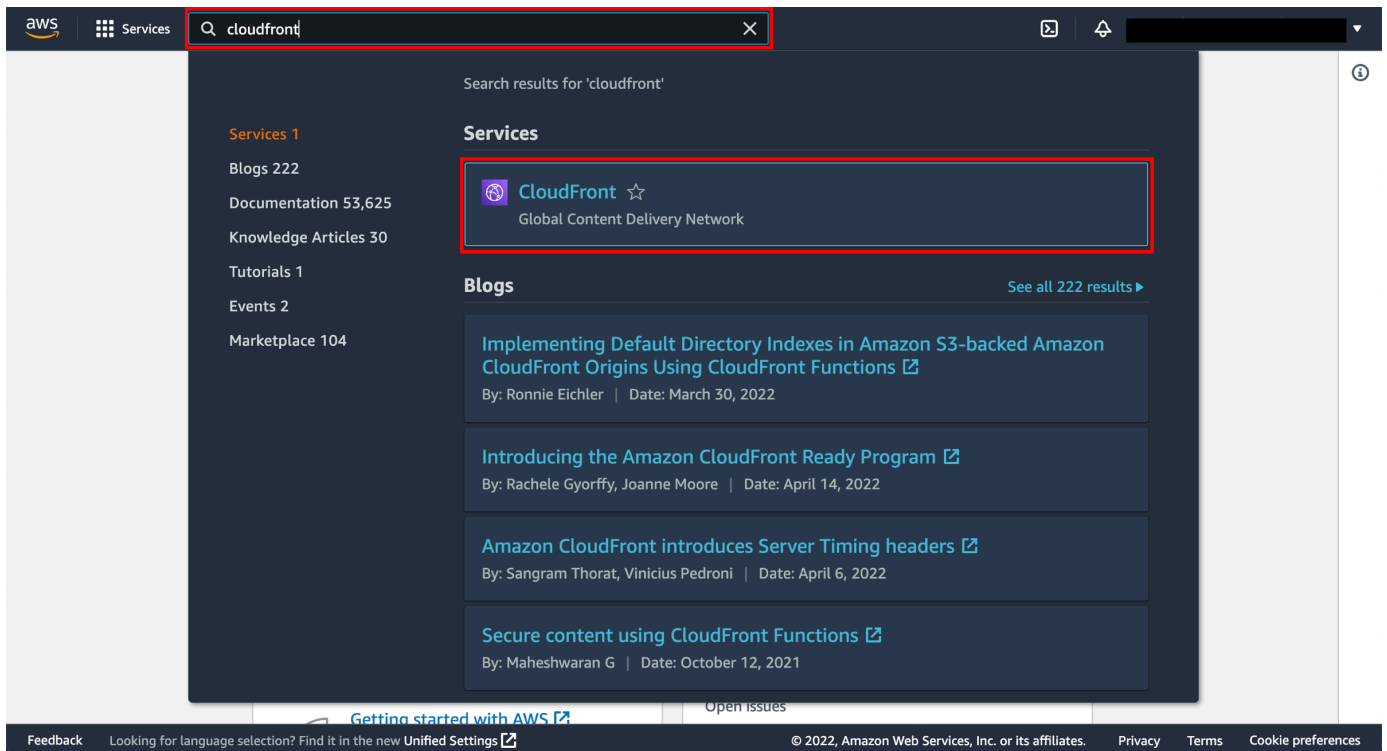
Cancel **Upload**

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.



2. Create a CloudFront distribution

Select **Create a CloudFront distribution**.

The screenshot shows the Amazon CloudFront website. At the top, there's a navigation bar with the AWS logo, a search bar, and a 'Global' dropdown. The main heading is 'Amazon CloudFront' with the sub-heading 'Securely deliver content with low latency and high transfer speeds'. Below this, there's a 'Get started with CloudFront' section with a 'Create a CloudFront distribution' button. The 'Benefits and features' section is divided into four columns: 'Reduce latency', 'Improve security', 'Cut costs', and 'Customize delivery'. The 'AWS Free Tier' section lists 1 TB of data transfer out, 10,000,000 HTTP or HTTPS requests, and 2,000,000 CloudFront Function invocations. The 'Pricing (US)' section shows a table with columns for 'Usage' and 'Price'.

Usage	Price
First 1 TB data transfer free each month	
10 TB/month	\$0.085 per GB

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.

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](#)

Origin path - optional
The directory path within your origin where your content is stored. [Learn more](#)

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.

[Cancel](#)

[Previous](#)

[Next](#)

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

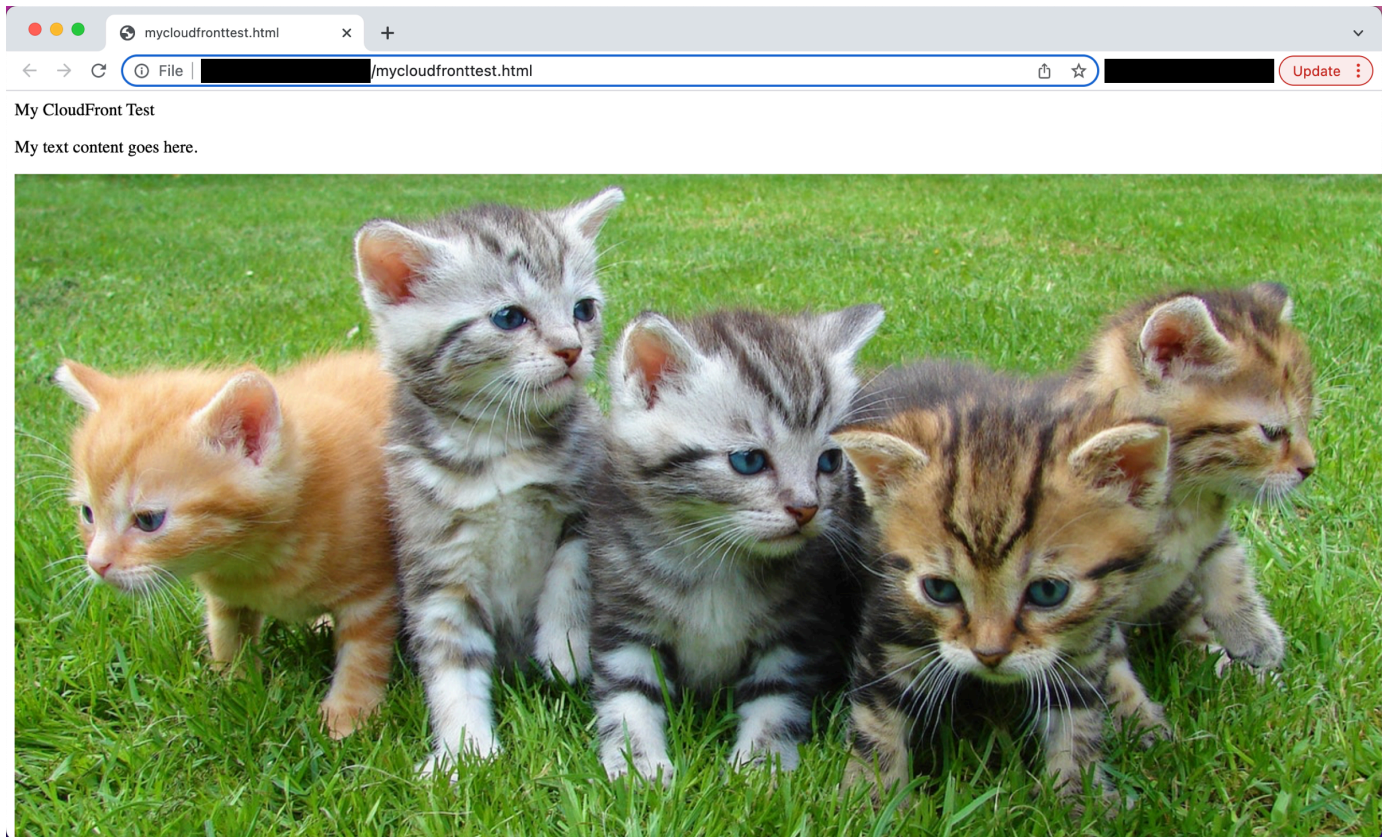
- Create an HTML file

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>
</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**.

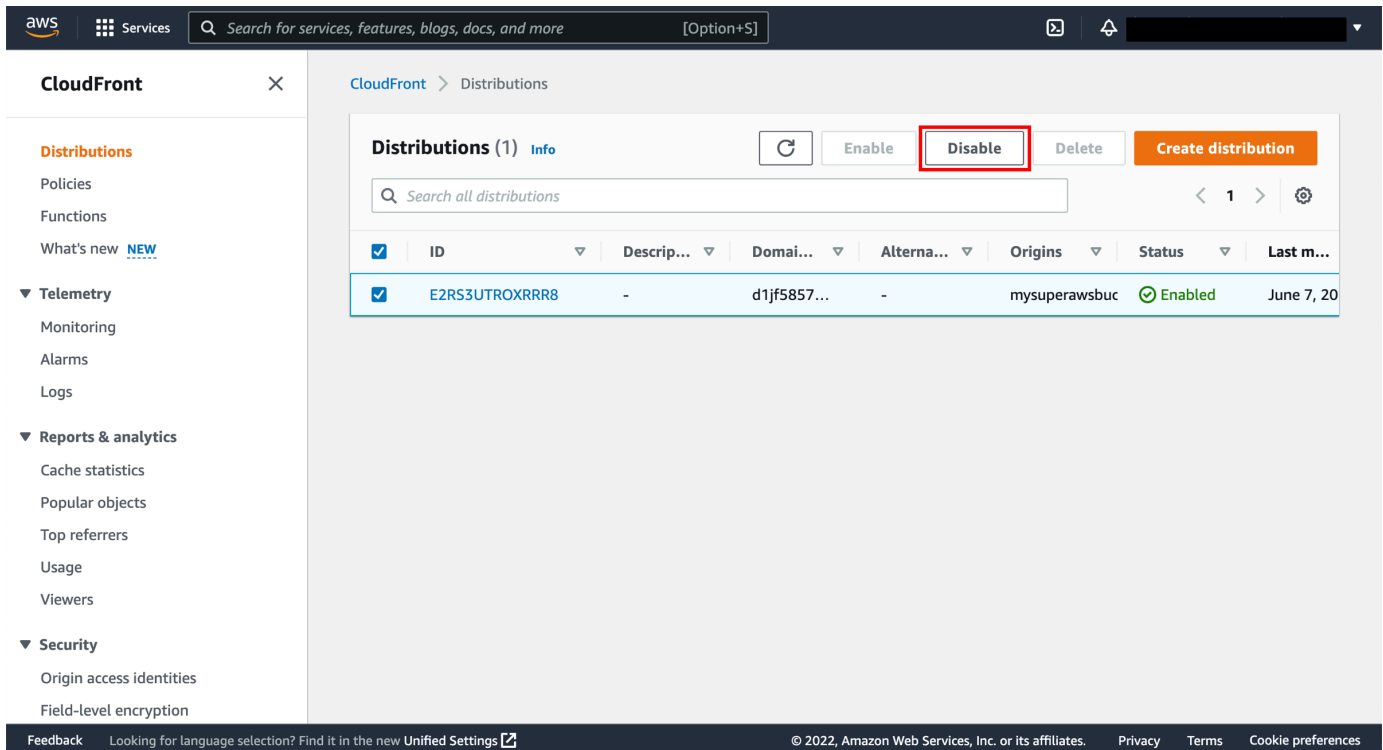
Open your HTML file in a web browser to verify that the link works.



(Optional) Disable and delete your distribution

1. Select the distribution to disable

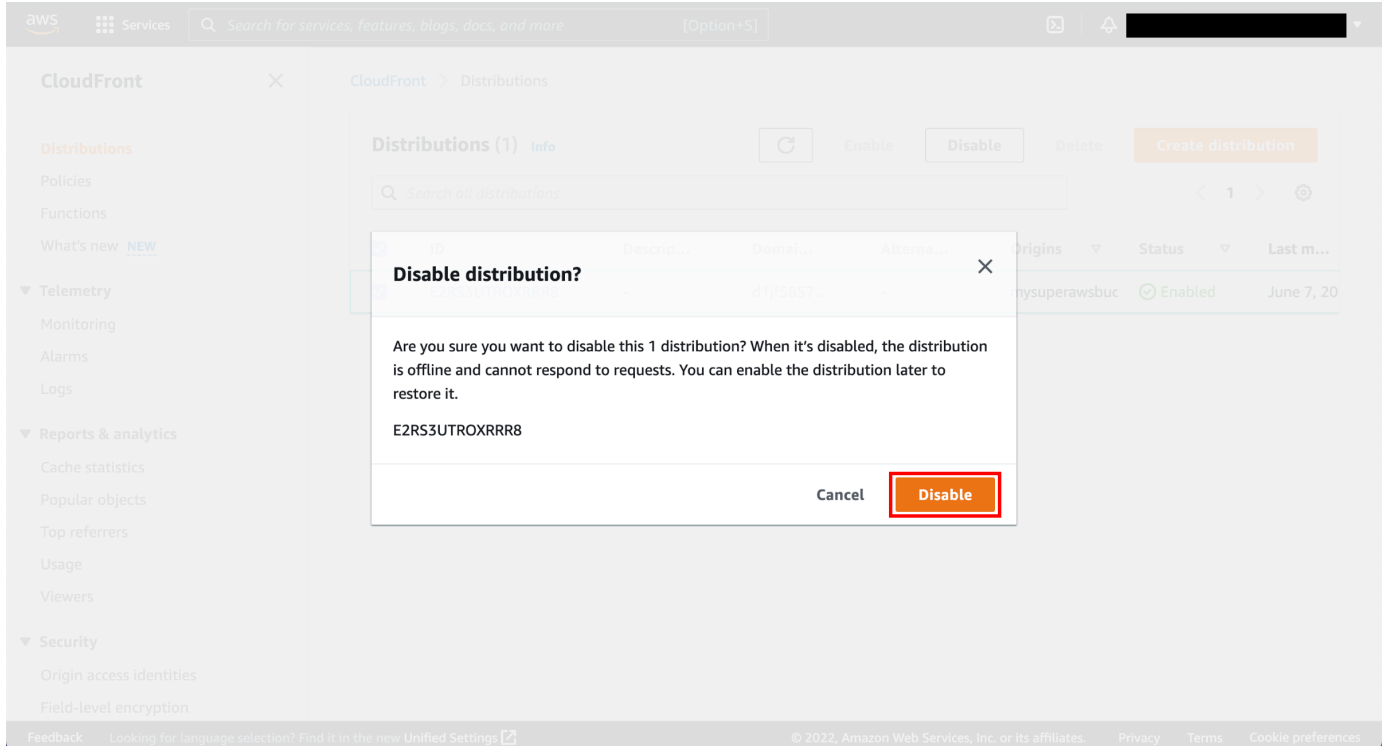
Select the checkbox next to the distribution you created and choose **Disable**.



The screenshot shows the AWS CloudFront console interface. The left sidebar contains navigation options: Distributions, Policies, Functions, What's new, Telemetry, Reports & analytics, and Security. The main content area displays the 'Distributions (1)' page. At the top, there are buttons for 'Enable', 'Disable' (highlighted with a red box), and 'Delete', along with a 'Create distribution' button. Below these is a search bar and a table of distributions. The table has columns for 'ID', 'Description', 'Domain', 'Alternate', 'Origins', 'Status', and 'Last modified'. One distribution is listed with ID 'E2RS3UTROXRRR8', status 'Enabled', and last modified 'June 7, 20...'. The footer contains feedback links and copyright information for Amazon Web Services, Inc. or its affiliates.

2. Confirm disabling the distribution

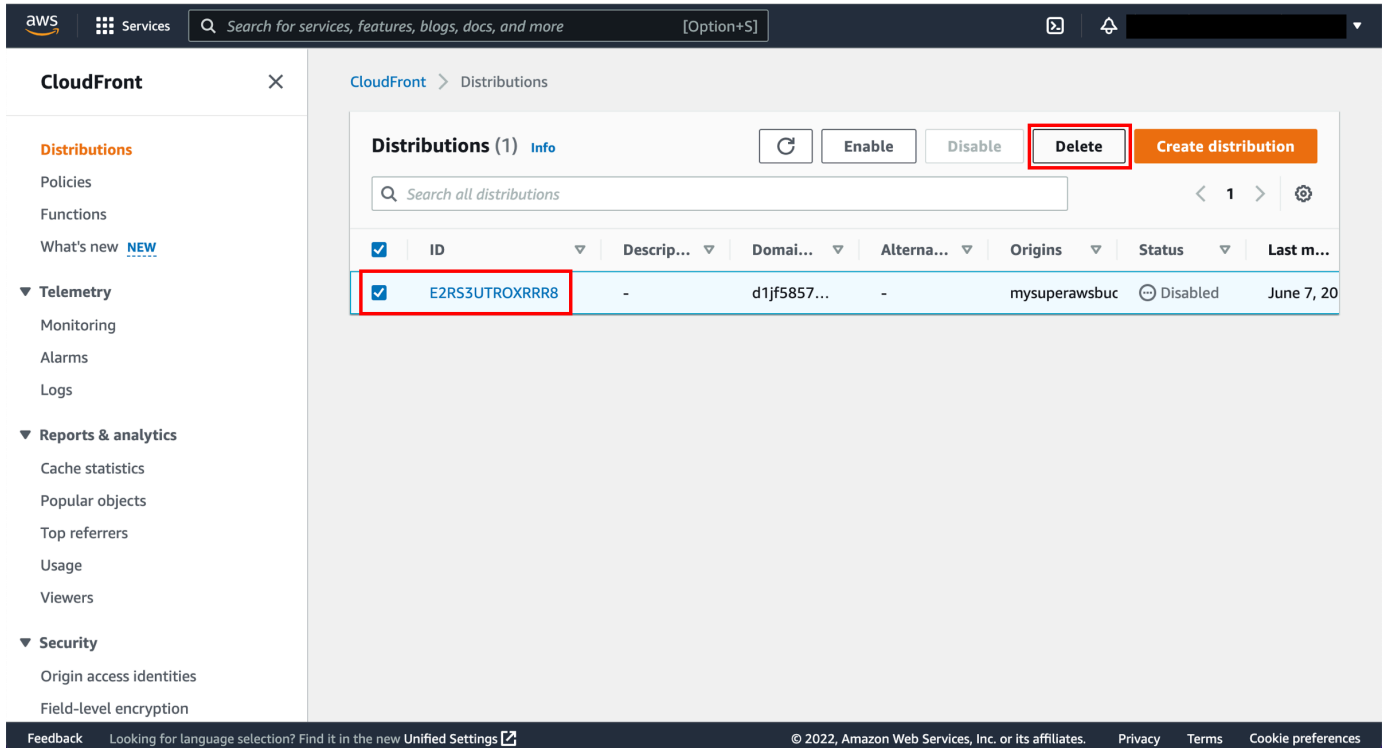
You will be asked to confirm. Choose **Disable**.



The screenshot shows the same AWS CloudFront console interface as above, but with a modal dialog box open in the center. The dialog box is titled 'Disable distribution?' and contains the following text: '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.' Below the text, the distribution ID 'E2RS3UTROXRRR8' is displayed. At the bottom of the dialog, there are two buttons: 'Cancel' and 'Disable' (highlighted with a red box). The background of the console is dimmed.

3. Select the distribution to delete

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

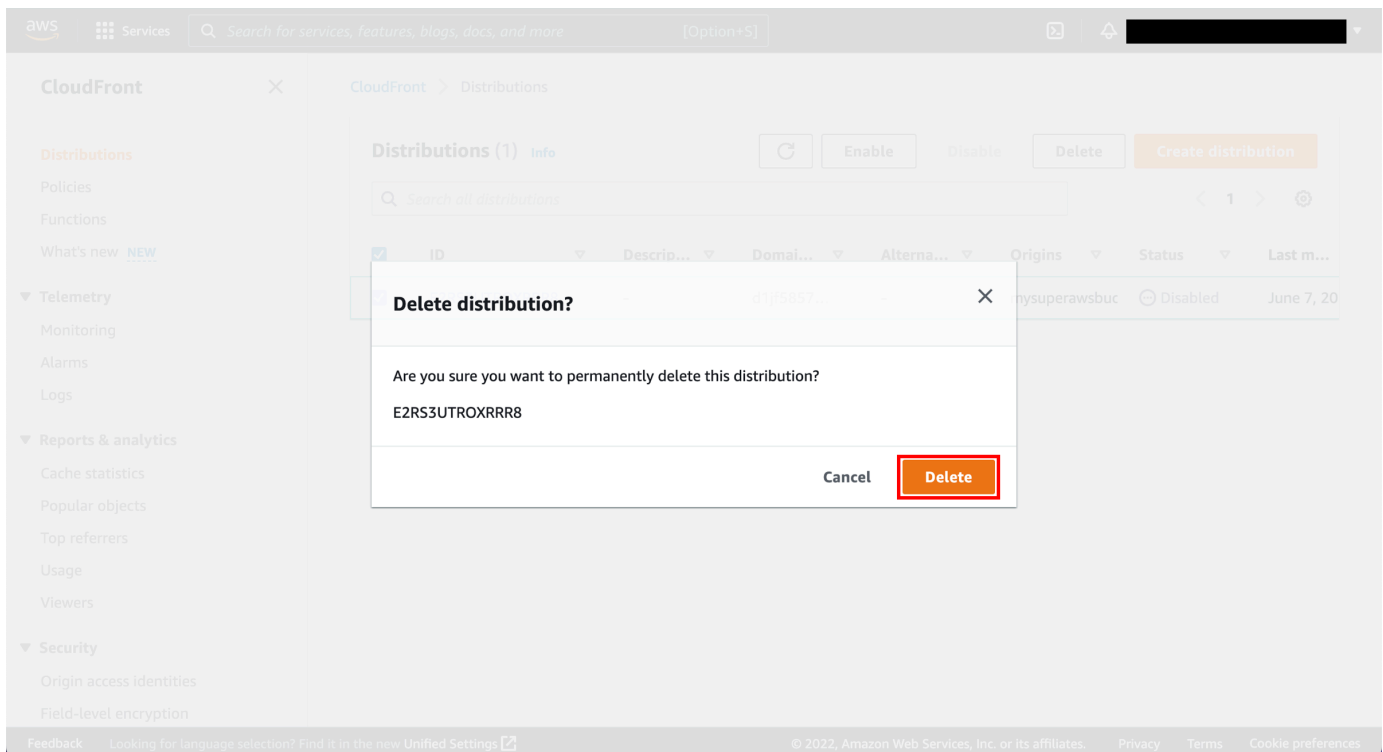


The screenshot shows the AWS CloudFront console interface. The left sidebar contains navigation options: Distributions, Policies, Functions, What's new, Telemetry, Reports & analytics, and Security. The main content area displays the 'Distributions (1)' page with a search bar and a table of distributions. The 'Delete' button is highlighted with a red box, and the checkbox next to the distribution ID 'E2RS3UTROXRRR8' is also highlighted with a red box.

<input checked="" type="checkbox"/>	ID	Descrip...	Domai...	Alterna...	Origins	Status	Last m...
<input checked="" type="checkbox"/>	E2RS3UTROXRRR8	-	d1jf5857...	-	mysuperawsbuc	Disabled	June 7, 20

4. Confirm deleting the distribution

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



The screenshot shows the AWS CloudFront console interface with a confirmation dialog box open. The dialog box asks 'Are you sure you want to permanently delete this distribution?' and displays the distribution ID 'E2RS3UTROXRRR8'. The 'Delete' button is highlighted with a red box.

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.