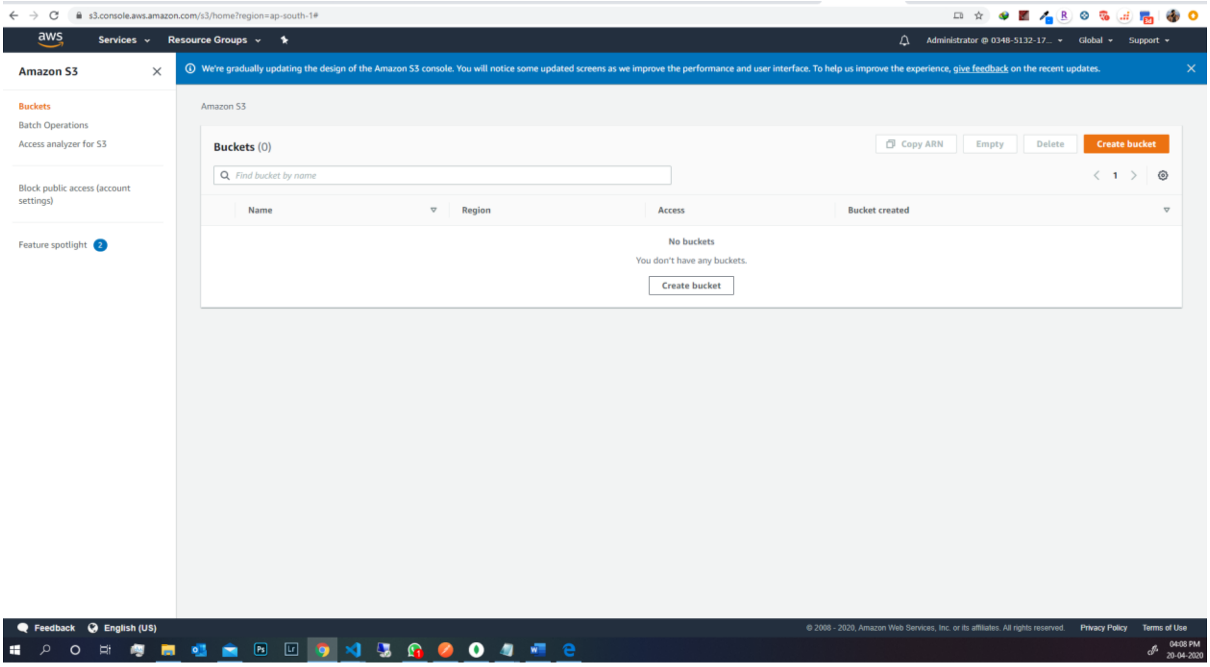
Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements. Amazon S3 is designed for 99.999999999% (11 9's) of durability, and stores data for millions of applications for companies all around the world.

Benefits:

1. Industry-leading performance, scalability, availability, and durability
2. Wide range of cost-effective storage classes
3. Unmatched security, compliance, and audit capabilities
4. Easily manage data and access controls
5. Query-in place services for analytics
6. Most supported cloud storage service

1) Create an S3 bucket

https://s3.console.aws.amazon.com/s3/home?region=ap-south-1#
Visit here and login with your iam credentials



s3.console.aws.amazon.com/s3/home?region=ap-south-1#

We're gradually updating the design of the Amazon S3 console. You will notice some updated screens as we improve the performance and user interface. To help us improve the experience, give feedback on the recent updates.

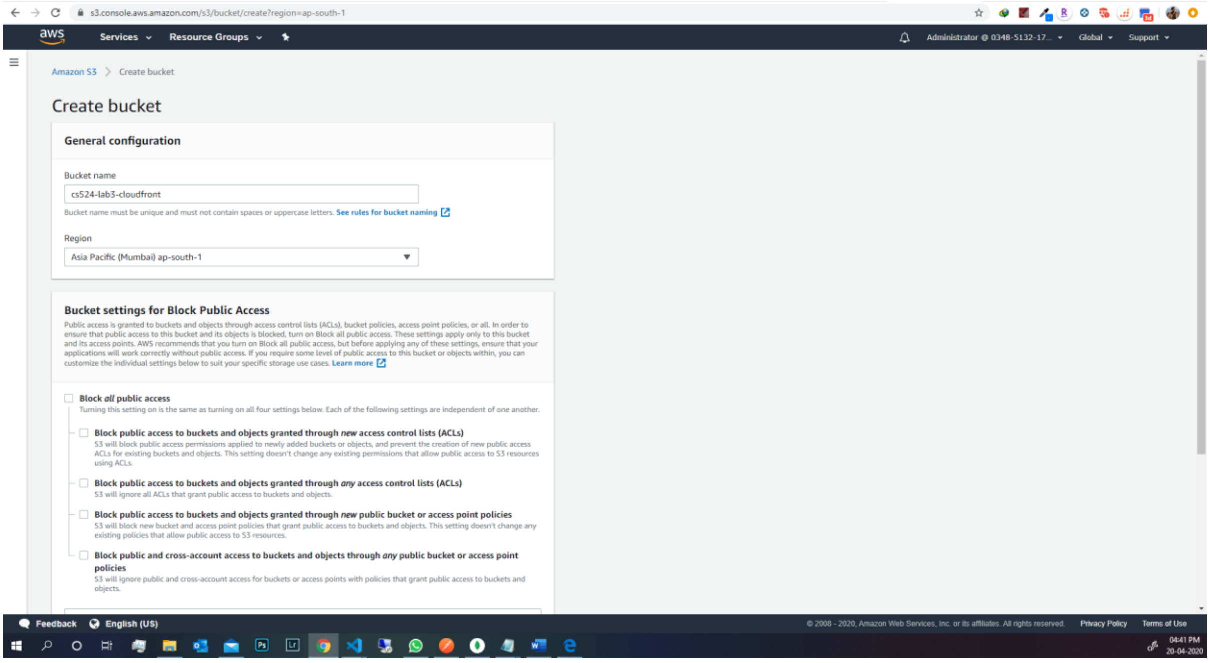
Buckets (0)

Name	Region	Access	Bucket created

No buckets

You don't have any buckets.

Uncheck “Block all public access” initially to give access to everyone


s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1
Services
Resource Groups
Administrator @ 0348-5132-17...
Global
Support
Amazon S3 > Create bucket
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
04:41 PM
20-04-2020

Create bucket

General configuration

Bucket name

cs524-lab3-cloudfront

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

Region

Asia Pacific (Mumbai) ap-south-1

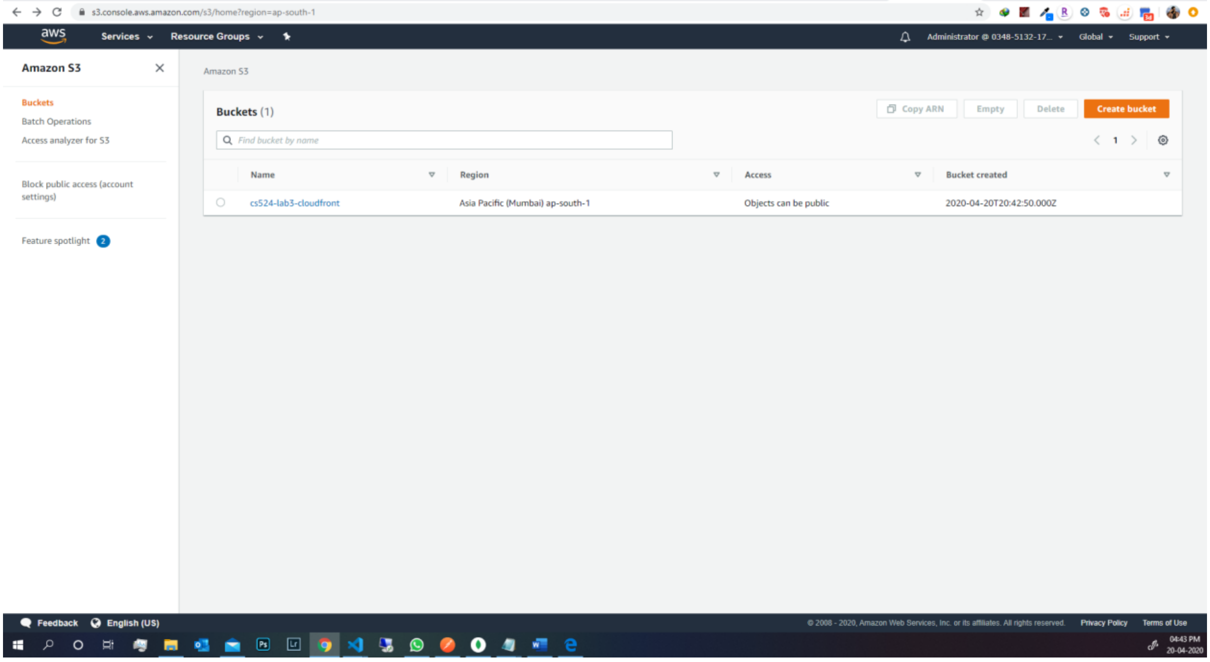
Bucket settings for Block Public Access

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.

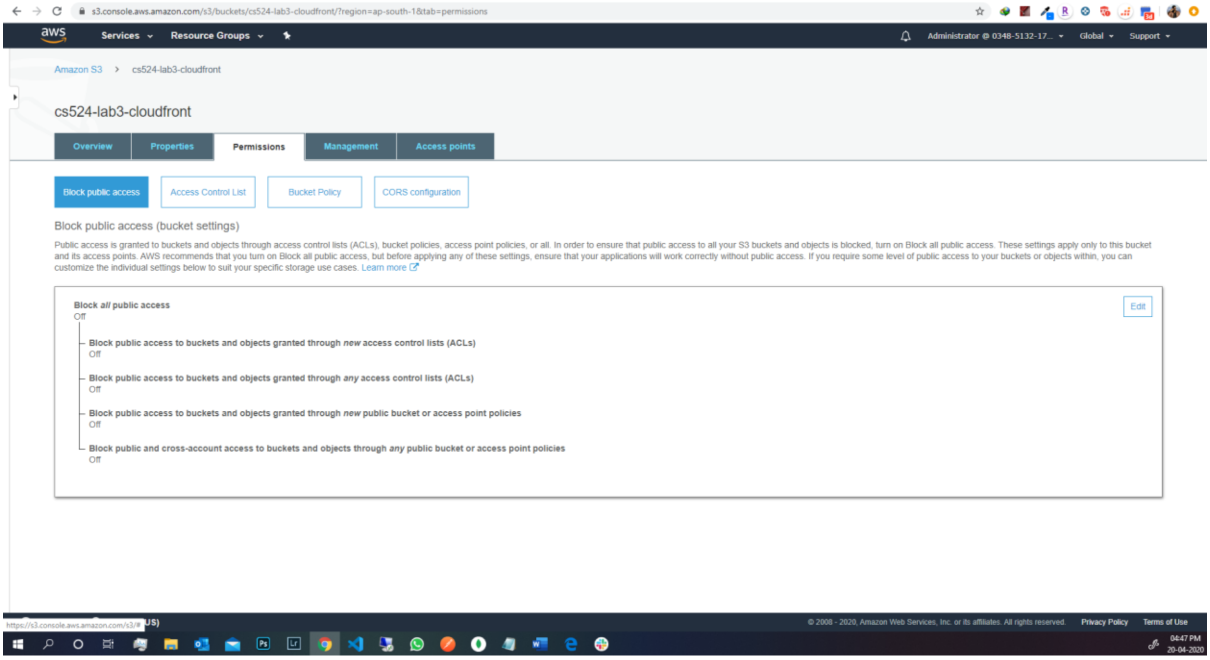
After creating the bucket you will be able to see it in your dashboard.



Buckets (1)

	Name	Region	Access	Bucket created
○	cs524-lab3-cloudfront	Asia Pacific (Mumbai) ap-south-1	Objects can be public	2020-04-20T20:42:50.000Z

You can open the bucket by clicking on the name and then go to permission tab to ensure that block all public access is off.


s3.console.aws.amazon.com/s3/buckets/cs524-lab3-cloudfront/?region=ap-south-1&tab=permissions
Services
Resource Groups
Administrator @ 0348-5132-17...
Global
Support
Amazon S3 > cs524-lab3-cloudfront

cs524-lab3-cloudfront

Overview
Properties
Permissions
Management
Access points
Block public access
Access Control List
Bucket Policy
CORS configuration

Block public access (bucket settings)

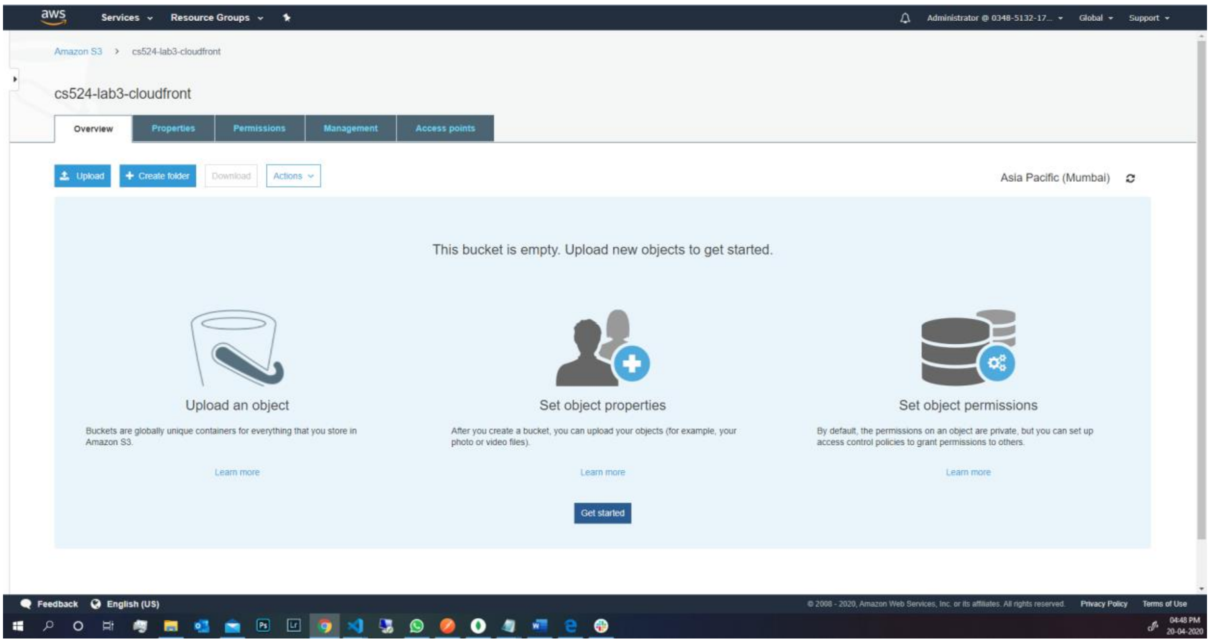
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

Block *all* public access
Off

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

Edit
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
04:47 PM
20-04-2020

Go to the overviews tab then you can upload image


Services
Resource Groups
Administrator @ 0348-5132-17...
Global
Support
Amazon S3 > cs524-lab3-cloudfront

cs524-lab3-cloudfront

This bucket is empty. Upload new objects to get started.

Upload an object

Buckets are globally unique containers for everything that you store in Amazon S3.

Learn more

Set object properties

After you create a bucket, you can upload your objects (for example, your photo or video files).

Learn more

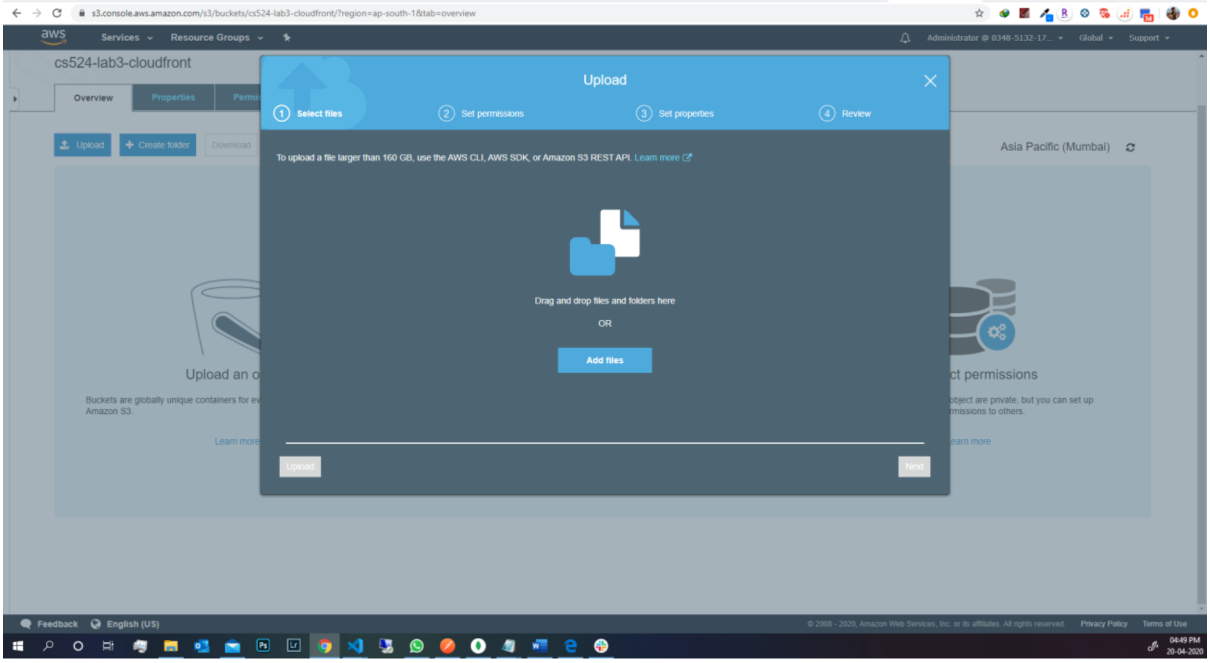
Set object permissions

By default, the permissions on an object are private, but you can set up access control policies to grant permissions to others.

Learn more

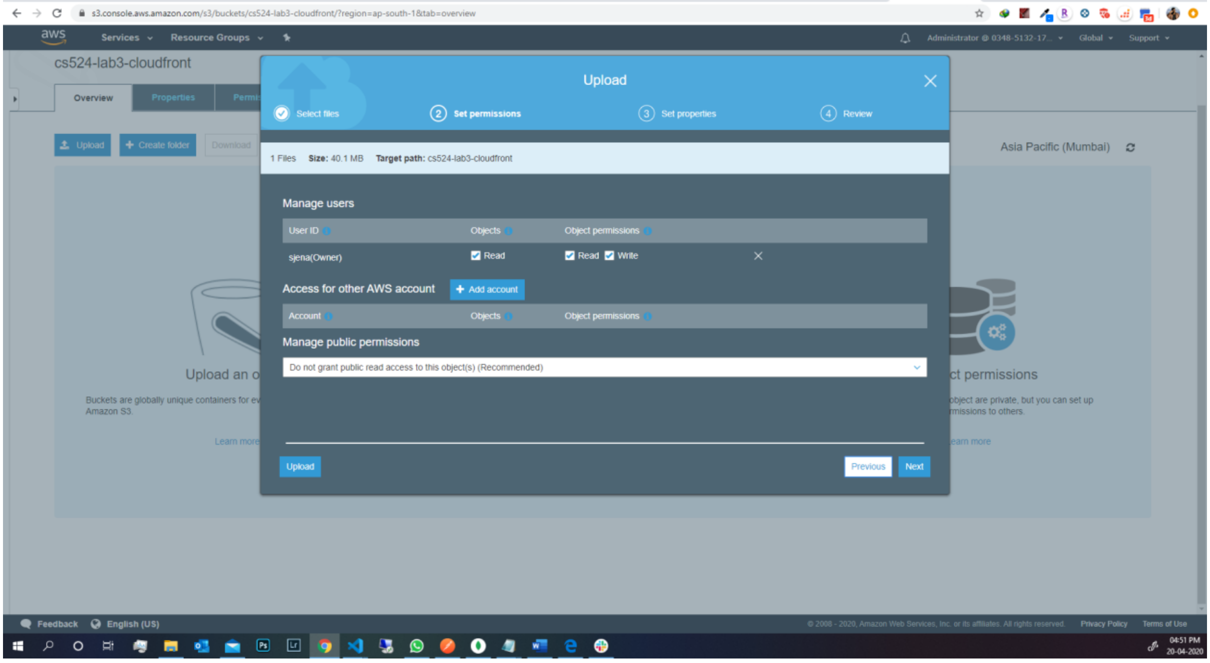
Get started
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
04:48 PM
20-04-2020

Click on upload this a dialog box appears



To upload a file larger than 160 GB, use the AWS CLI, AWS SDK, or Amazon S3 REST API. Learn more

In my case I am uploading an image (it’s a wallpaper used by tech youtuber MKBHD).



1 Files **Size:** 40.1 MB **Target path:** cs524-lab3-cloudfront

Manage users

User ID	Objects	Object permissions
sjena(Owner)	☑ Read	☑ Read ☑ Write

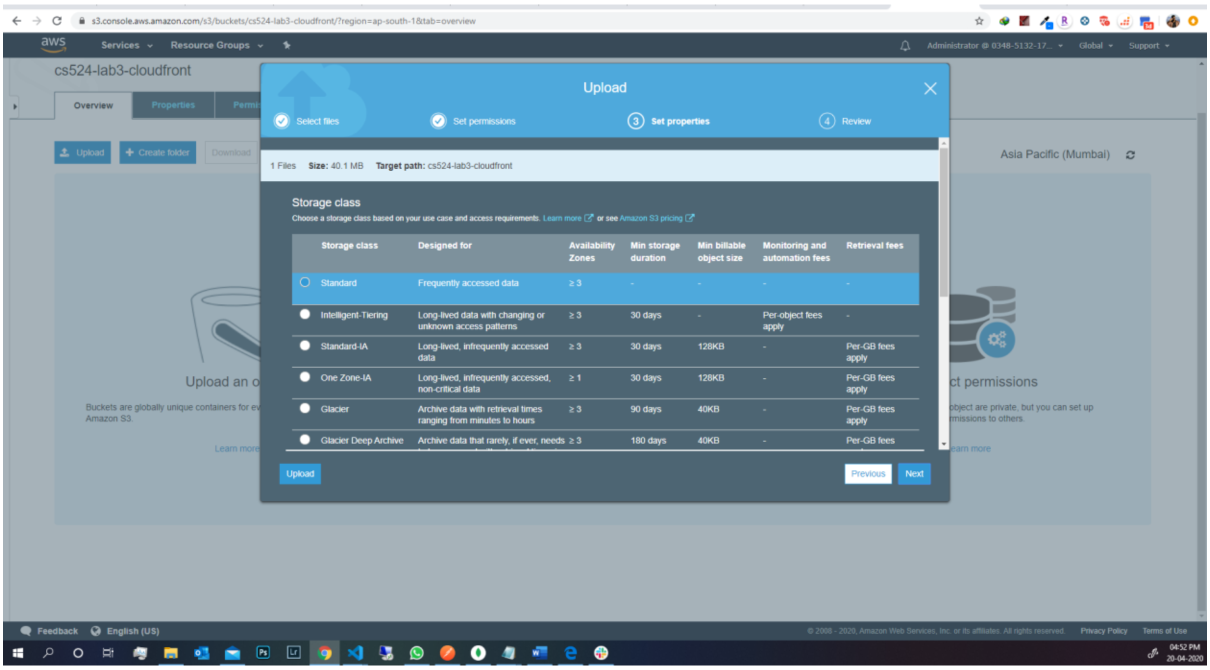
Access for other AWS account

Account	Objects	Object permissions

Manage public permissions

Do not grant public read access to this object(s) (Recommended)

Click next then choose storage class as standard



Upload

✓ Select files ✓ Set permissions (3) Set properties (4) Review

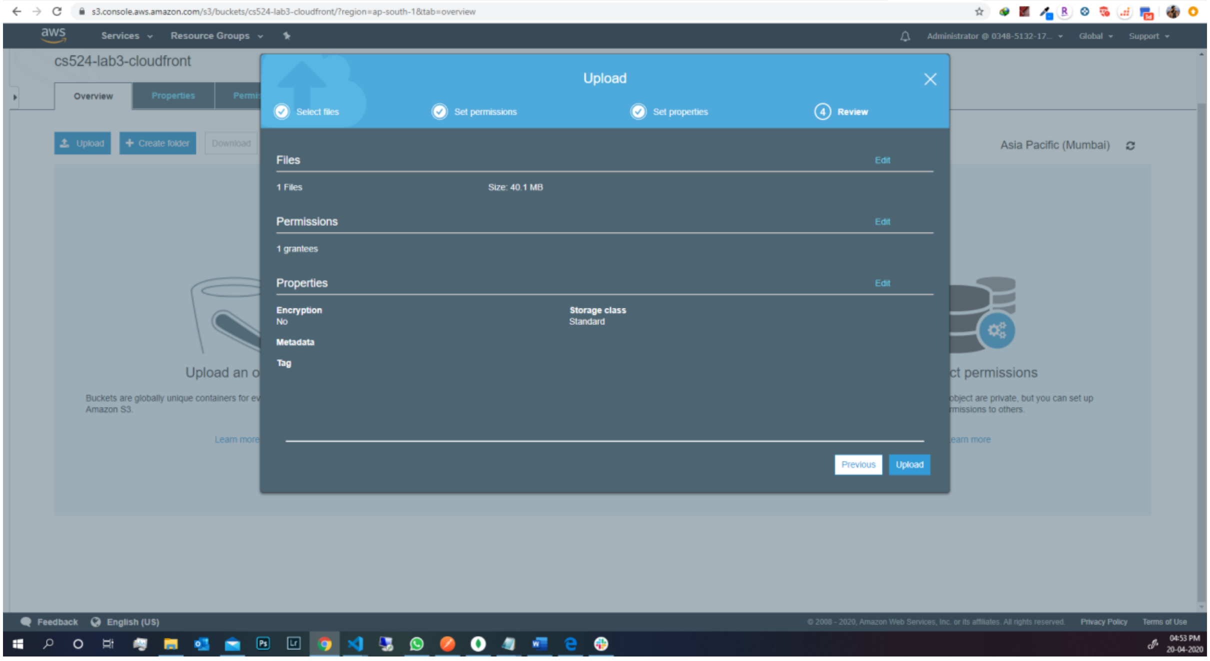
1 Files **Size:** 40.1 MB **Target path:** cs524-lab3-cloudfront

Storage class

Choose a storage class based on your use case and access requirements. Learn more or see Amazon S3 pricing

	Storage class	Designed for	Availability Zones	Min storage duration	Min billable object size	Monitoring and automation fees	Retrieval fees
○	Standard	Frequently accessed data	≥ 3	-	-	-	-
●	Intelligent-Tiering	Long-lived data with changing or unknown access patterns	≥ 3	30 days	-	Per-object fees apply	-
●	Standard-IA	Long-lived, infrequently accessed data	≥ 3	30 days	128KB	-	Per-GB fees apply
●	One Zone-IA	Long-lived, infrequently accessed, non-critical data	≥ 1	30 days	128KB	-	Per-GB fees apply
●	Glacier	Archive data with retrieval times ranging from minutes to hours	≥ 3	90 days	40KB	-	Per-GB fees apply
●	Glacier Deep Archive	Archive data that rarely, if ever, needs	≥ 3	180 days	40KB	-	Per-GB fees

This is the final step



Upload

✓ Select files ✓ Set permissions ✓ Set properties (4) Review

Files — Edit

1 Files Size: 40.1 MB

Permissions — Edit

1 grantees

Properties — Edit

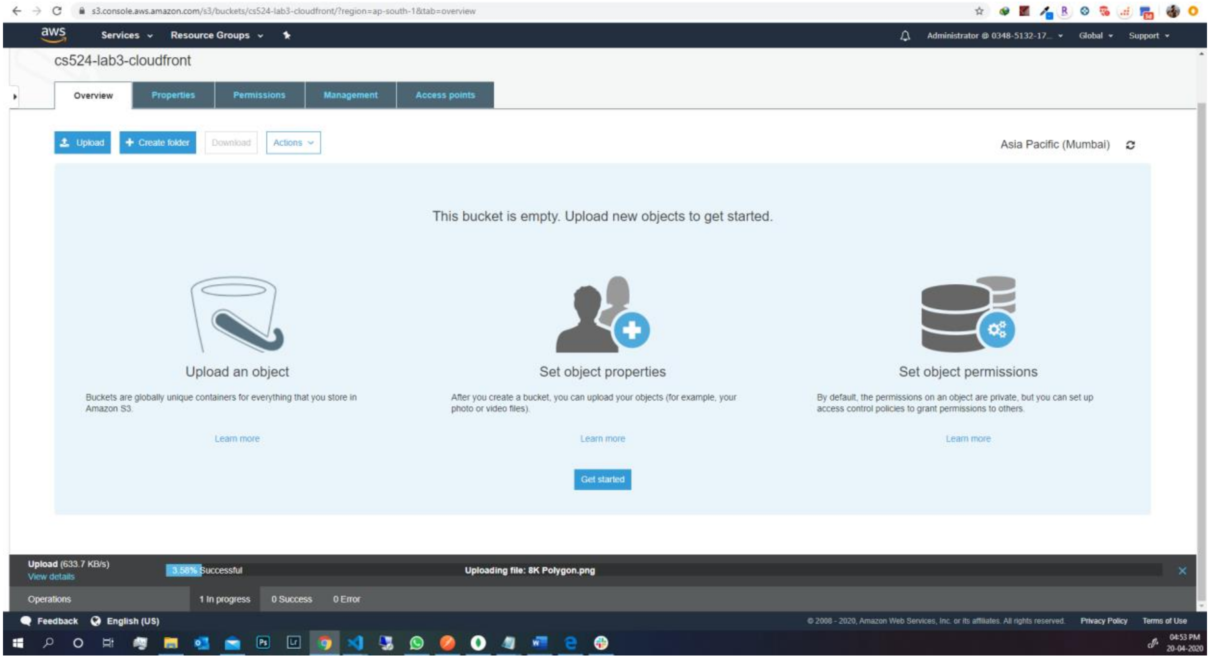
Encryption
No

Storage class
Standard

Metadata

Tag

Click upload to finish uploading



This bucket is empty. Upload new objects to get started.

Upload an object

Buckets are globally unique containers for everything that you store in Amazon S3.

Set object properties

After you create a bucket, you can upload your objects (for example, your photo or video files).

Set object permissions

By default, the permissions on an object are private, but you can set up access control policies to grant permissions to others.

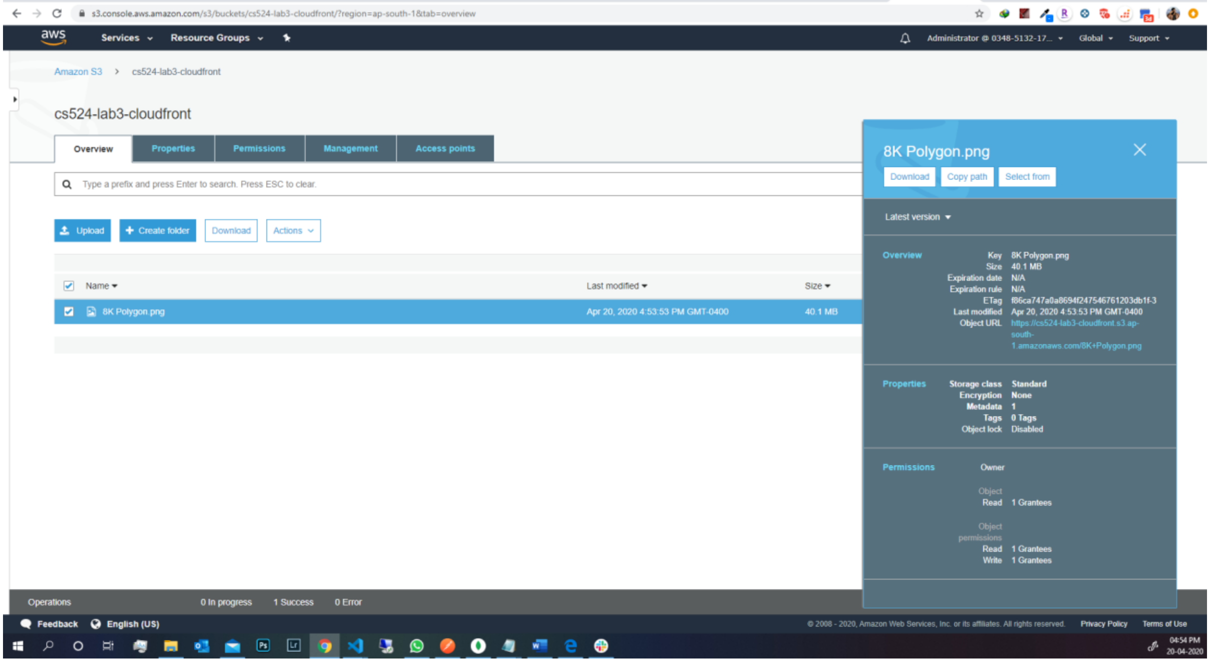
Upload (633.7 KB/s)
View details
3.58% Successful
Uploading file: 8K Polygon.png

Operations 1 In progress 0 Success 0 Error

Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
04:53 PM
20-04-2020

You can see the upload status in the bottom of the page

Once the upload is finished, click on the file name and you can copy the object url from the right hand portion of the page and access it independently.



s3.console.aws.amazon.com/s3/buckets/cs524-lab3-cloudfront/?region=ap-south-1&tab=overview
Services
Resource Groups
Administrator @ 0348-5132-17...
Global
Support
Amazon S3 > cs524-lab3-cloudfront
cs524-lab3-cloudfront
Overview
Properties
Permissions
Management
Access points
Type a prefix and press Enter to search. Press ESC to clear.
Upload
Create folder
Download
Actions

☑ Name	Last modified	Size
☑ 8K Polygon.png	Apr 20, 2020 4:53:53 PM GMT-0400	40.1 MB

8K Polygon.png

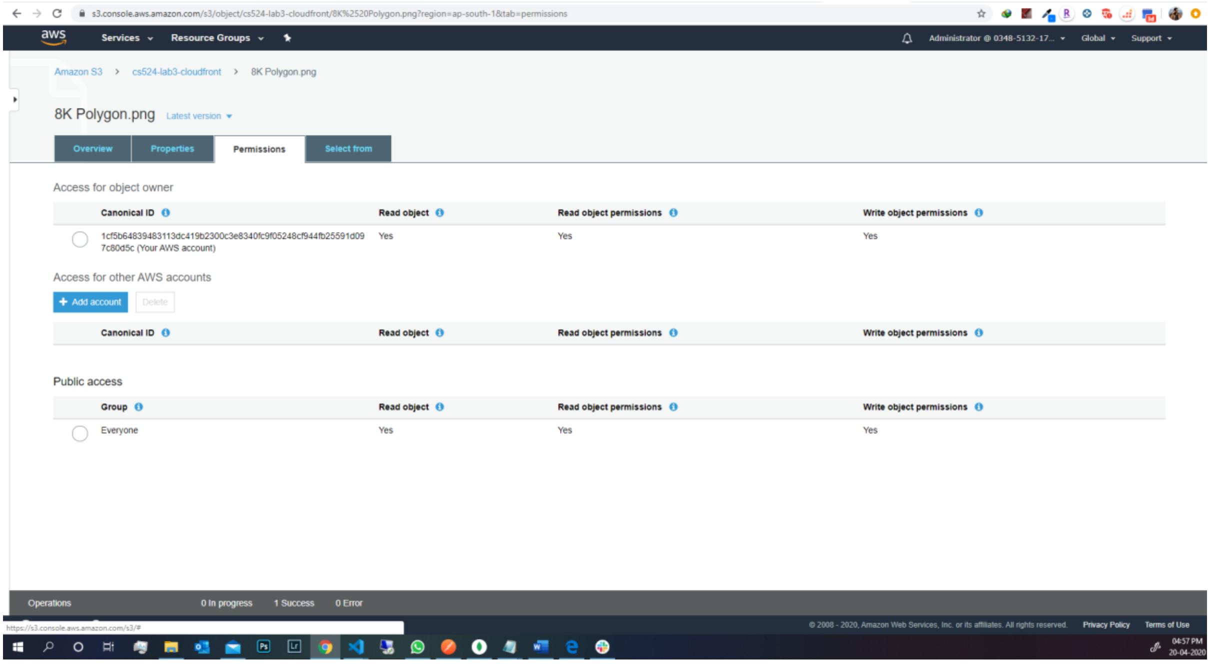
Download
Copy path
Select from
Latest version

Overview	Key	8K Polygon.png
	Size	40.1 MB
	Expiration date	N/A
	Expiration rule	N/A
	ETag	f86ca747a0a8694f247546761203db1f-3
	Last modified	Apr 20, 2020 4:53:53 PM GMT-0400
	Object URL	https://cs524-lab3-cloudfront.s3.ap-south-1.amazonaws.com/8K+Polygon.png
Properties	Storage class	Standard
	Encryption	None
	Metadata	1
	Tags	0 Tags
	Object lock	Disabled
Permissions	Owner	
	Object Read	1 Grantees
	Object permissions Read	1 Grantees
	Write	1 Grantees

Operations 0 In progress 1 Success 0 Error

Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
04:54 PM
20-04-2020

Go to overview and click on make public then you can access it from the URL.



8K Polygon.png

Access for object owner

	Canonical ID	Read object	Read object permissions	Write object permissions
○	1cf5b64839483113dc419b2300c3e8340fc9f05248cf944fb25591d09 7c80d5c (Your AWS account)	Yes	Yes	Yes

Access for other AWS accounts

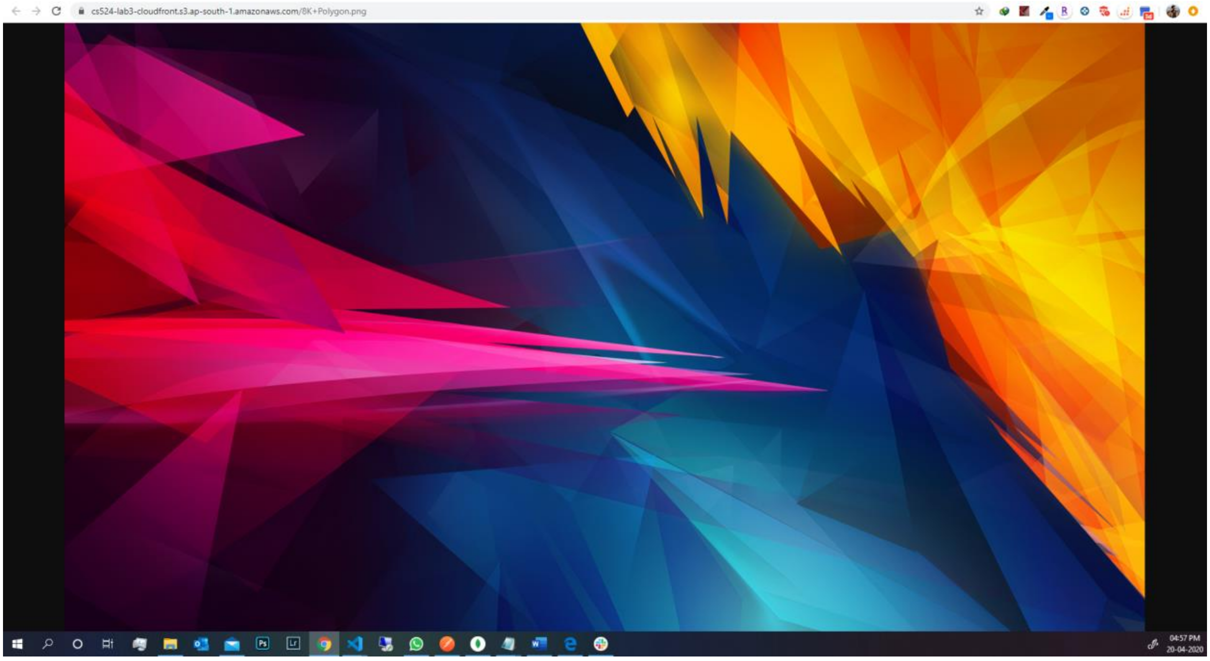
Canonical ID	Read object	Read object permissions	Write object permissions

Public access

	Group	Read object	Read object permissions	Write object permissions
○	Everyone	Yes	Yes	Yes

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Accessing the image form the url (https://cs524-lab3-cloudfront.s3.ap-south-1.amazonaws.com/8K+Polygon.png)


cs524-lab3-cloudfront.s3.ap-south-1.amazonaws.com/8K+Polygon.png
04:57 PM
20-04-2020

2) Create a Web Distribution in Cloud Front.

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. CloudFront is integrated with AWS – both physical locations that are directly connected to the AWS global infrastructure, as well as other AWS services. CloudFront works seamlessly with services including AWS Shield for DDoS mitigation, Amazon S3, Elastic Load

Balancing or Amazon EC2 as origins for your applications, and Lambda@Edge to run custom code closer to customers' users and to customize the user experience. Lastly, if you use AWS origins such as Amazon S3, Amazon EC2 or Elastic Load Balancing, you don't pay for any data transferred between these services and CloudFront.

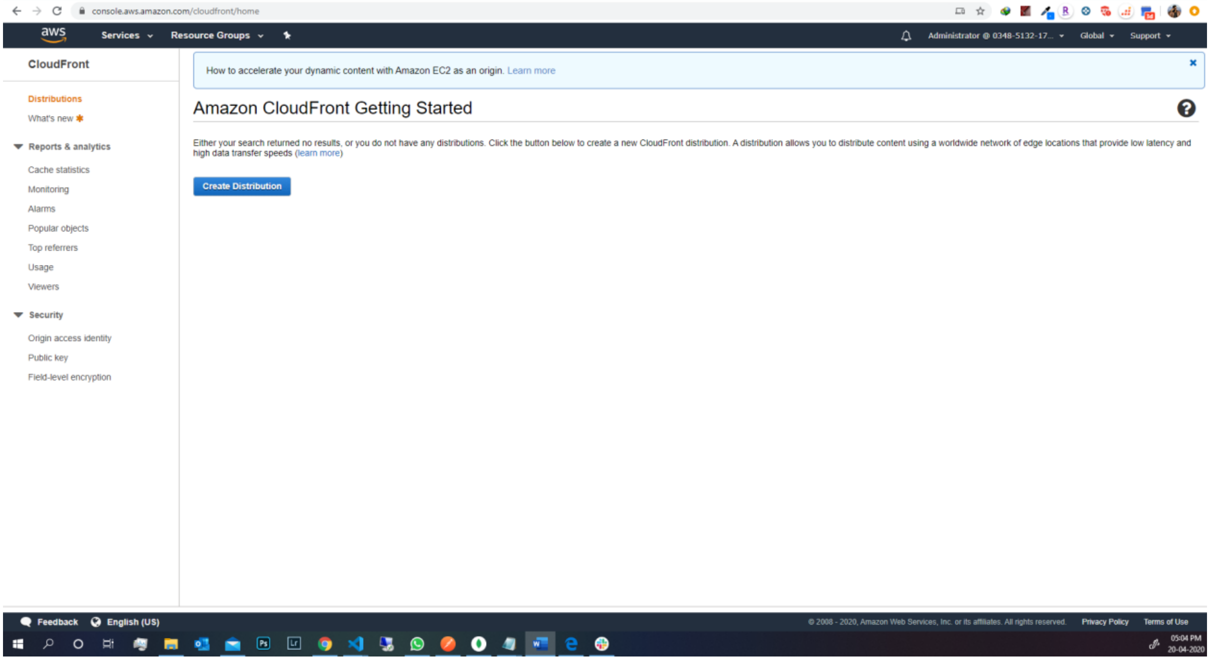
You can get started with the Content Delivery Network in minutes, using the same AWS tools that you're already familiar with: APIs, AWS Management Console, AWS CloudFormation, CLIs, and SDKs. Amazon's CDN offers a simple, pay-as-you-go pricing model with no upfront fees or required long-term contracts, and support for the CDN is included in your existing AWS Support subscription.

Benefits:

1. Fast & global
2. Security at the Edge
3. Highly Programmable
4. Deep integration with AWS

Steps to execute the assignment.

Visit the cloudfront home page from the url (https://console.aws.amazon.com/cloudfront/home)

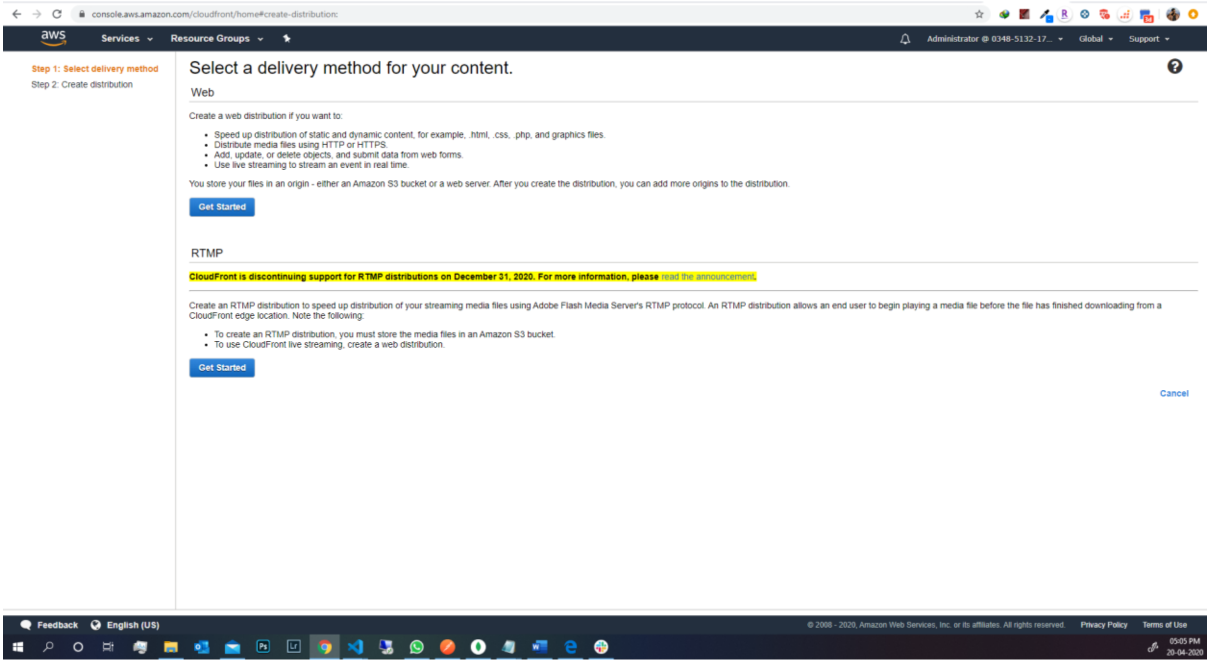


How to accelerate your dynamic content with Amazon EC2 as an origin. Learn more

Amazon CloudFront Getting Started

Either your search returned no results, or you do not have any distributions. Click the button below to create a new CloudFront distribution. A distribution allows you to distribute content using a worldwide network of edge locations that provide low latency and high data transfer speeds (learn more)

Click on Create Distribution



console.aws.amazon.com/cloudfront/home#create-distribution:
aws
Services
Resource Groups
Administrator @ 0348-5132-17...
Global
Support
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
05:05 PM
20-04-2020

Step 1: Select delivery method
Step 2: Create distribution

Select a delivery method for your content.

Web

Create a web distribution if you want to:

- Speed up distribution of static and dynamic content, for example, .html, .css, .php, and graphics files.
- Distribute media files using HTTP or HTTPS.
- Add, update, or delete objects, and submit data from web forms.
- Use live streaming to stream an event in real time.

You store your files in an origin - either an Amazon S3 bucket or a web server. After you create the distribution, you can add more origins to the distribution.

Get Started

RTMP

CloudFront is discontinuing support for RTMP distributions on December 31, 2020. For more information, please read the announcement.

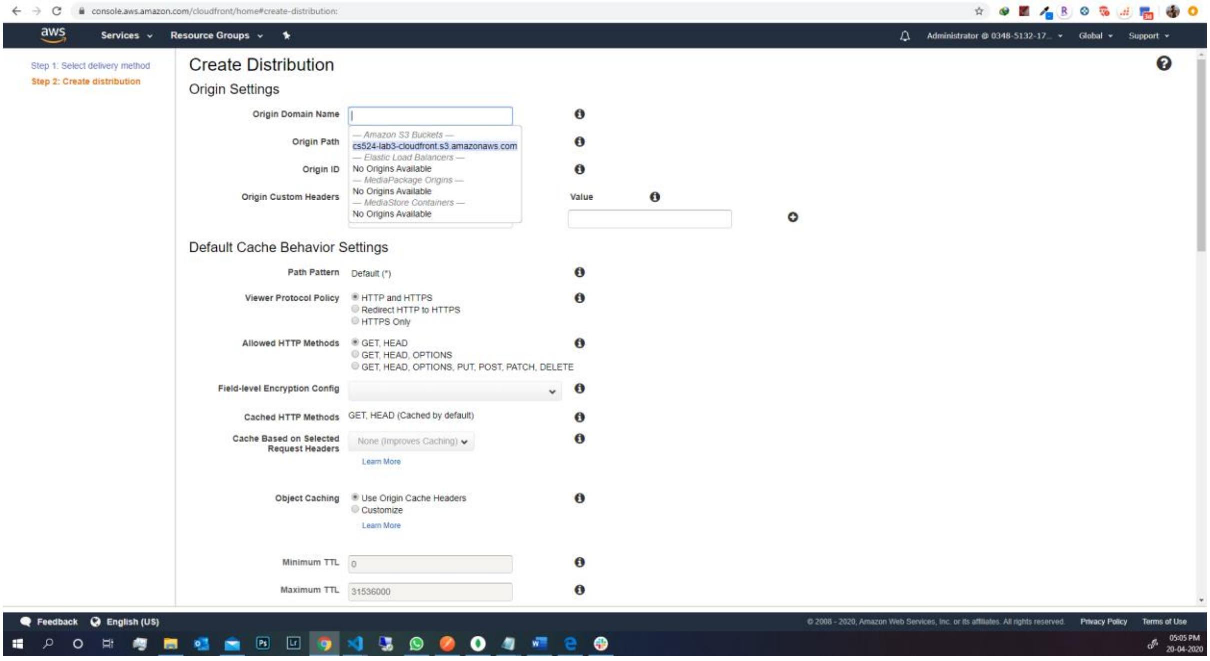
Create an RTMP distribution to speed up distribution of your streaming media files using Adobe Flash Media Server's RTMP protocol. An RTMP distribution allows an end user to begin playing a media file before the file has finished downloading from a CloudFront edge location. Note the following:

- To create an RTMP distribution, you must store the media files in an Amazon S3 bucket.
- To use CloudFront live streaming, create a web distribution.

Get Started

Cancel

Click on Get started button below Web. Under Origin domain name select the S3 bucket which we just created.



console.aws.amazon.com/cloudfront/home#create-distribution:
aws
Services
Resource Groups
Administrator @ 0348-5132-17...
Global
Support
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
05:05 PM
20-04-2020

Step 1: Select delivery method
Step 2: Create distribution

Create Distribution

Origin Settings

Origin Domain Name |
— Amazon S3 Buckets —
cs524-lab3-cloudfront.s3.amazonaws.com
— Elastic Load Balancers —
No Origins Available
— MediaPackage Origins —
No Origins Available
— MediaStore Containers —
No Origins Available

Origin Path

Origin ID

Origin Custom Headers — Value

Default Cache Behavior Settings

Path Pattern: Default (*)

Viewer Protocol Policy: ● HTTP and HTTPS ○ Redirect HTTP to HTTPS ○ HTTPS Only

Allowed HTTP Methods: ● GET, HEAD ○ GET, HEAD, OPTIONS ○ GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Field-level Encryption Config

Cached HTTP Methods: GET, HEAD (Cached by default)

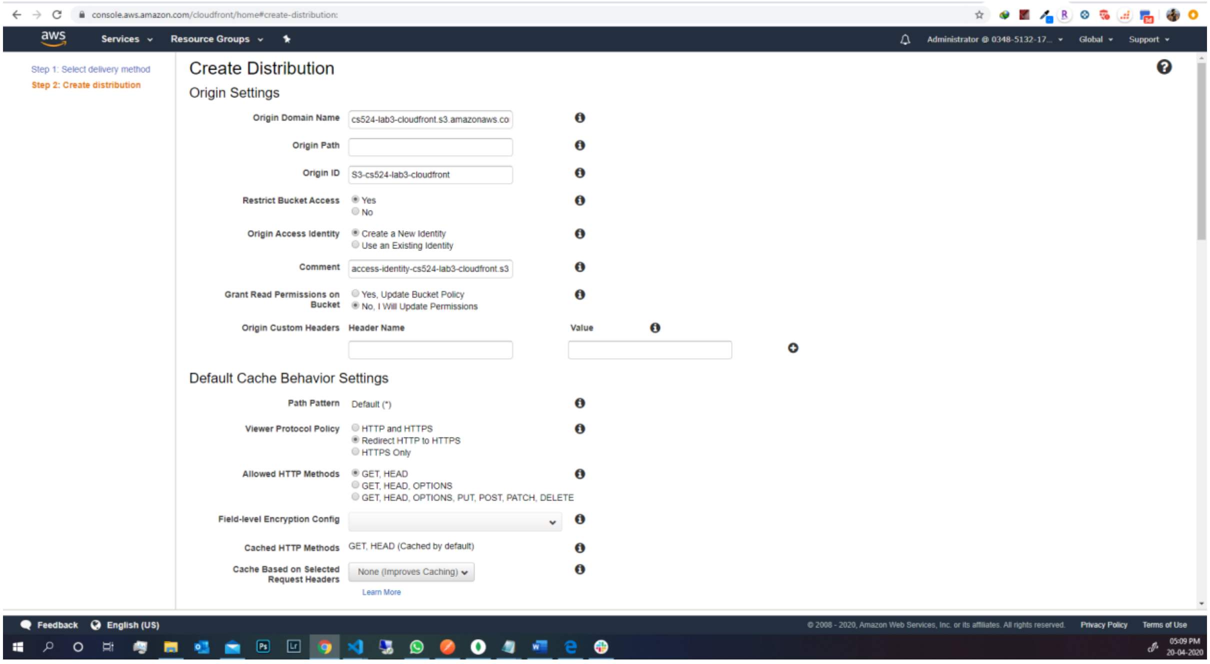
Cache Based on Selected Request Headers: None (Improves Caching)
Learn More

Object Caching: ● Use Origin Cache Headers ○ Customize
Learn More

Minimum TTL: 0

Maximum TTL: 31536000

We need to create a new identity so that we can block public access in S3 bucket and only allow cloudfront to access the same.


console.aws.amazon.com/cloudfront/home#create-distribution:
aws
Services
Resource Groups
Administrator @ 0348-5132-17...
Global
Support
Step 1: Select delivery method
Step 2: Create distribution

Create Distribution

Origin Settings

Origin Domain Name: cs524-lab3-cloudfront.s3.amazonaws.co

Origin Path:

Origin ID: S3-cs524-lab3-cloudfront

Restrict Bucket Access: ● Yes ○ No

Origin Access Identity: ● Create a New Identity ○ Use an Existing Identity

Comment: access-identity-cs524-lab3-cloudfront.s3

Grant Read Permissions on Bucket: ○ Yes, Update Bucket Policy ● No, I Will Update Permissions

Origin Custom Headers: Header Name / Value

Default Cache Behavior Settings

Path Pattern: Default (*)

Viewer Protocol Policy: ○ HTTP and HTTPS ● Redirect HTTP to HTTPS ○ HTTPS Only

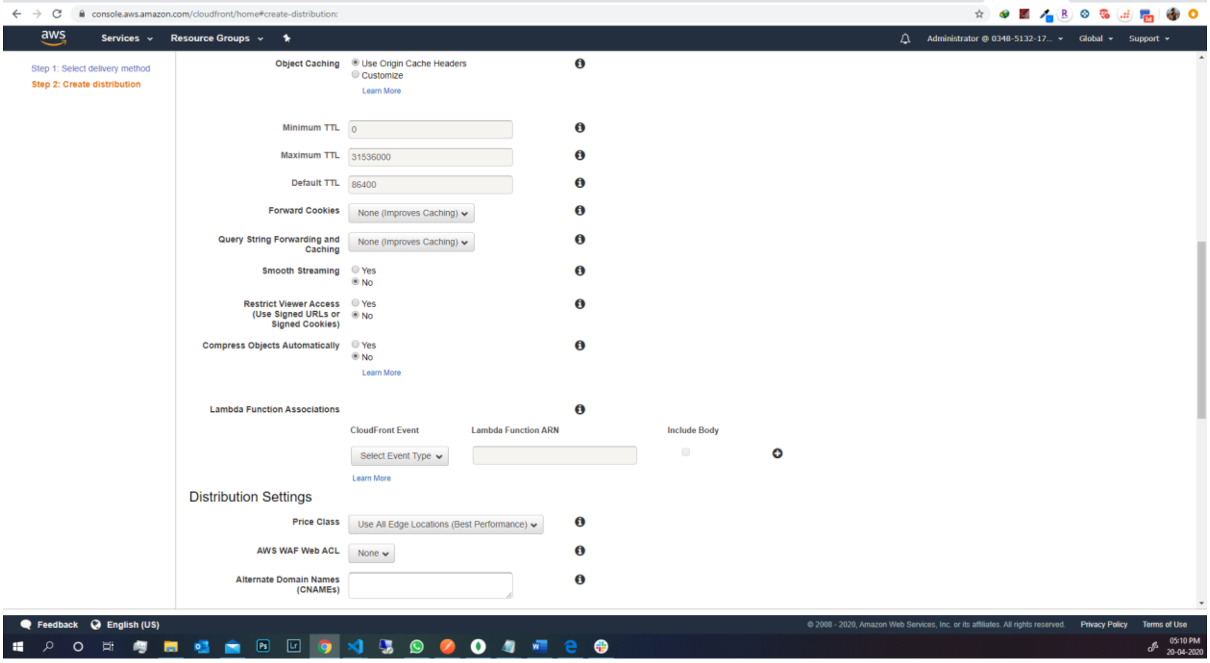
Allowed HTTP Methods: ● GET, HEAD ○ GET, HEAD, OPTIONS ○ GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Field-level Encryption Config:

Cached HTTP Methods: GET, HEAD (Cached by default)

Cache Based on Selected Request Headers: None (Improves Caching)

Learn More
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
05:09 PM
20-04-2020


console.aws.amazon.com/cloudfront/home#create-distribution:
aws
Services
Resource Groups
Administrator @ 0348-5132-17...
Global
Support
Step 1: Select delivery method
Step 2: Create distribution

Object Caching: ● Use Origin Cache Headers ○ Customize

Minimum TTL: 0

Maximum TTL: 31536000

Default TTL: 86400

Forward Cookies: None (Improves Caching)

Query String Forwarding and Caching: None (Improves Caching)

Smooth Streaming: ○ Yes ● No

Restrict Viewer Access (Use Signed URLs or Signed Cookies): ○ Yes ● No

Compress Objects Automatically: ○ Yes ● No

Lambda Function Associations

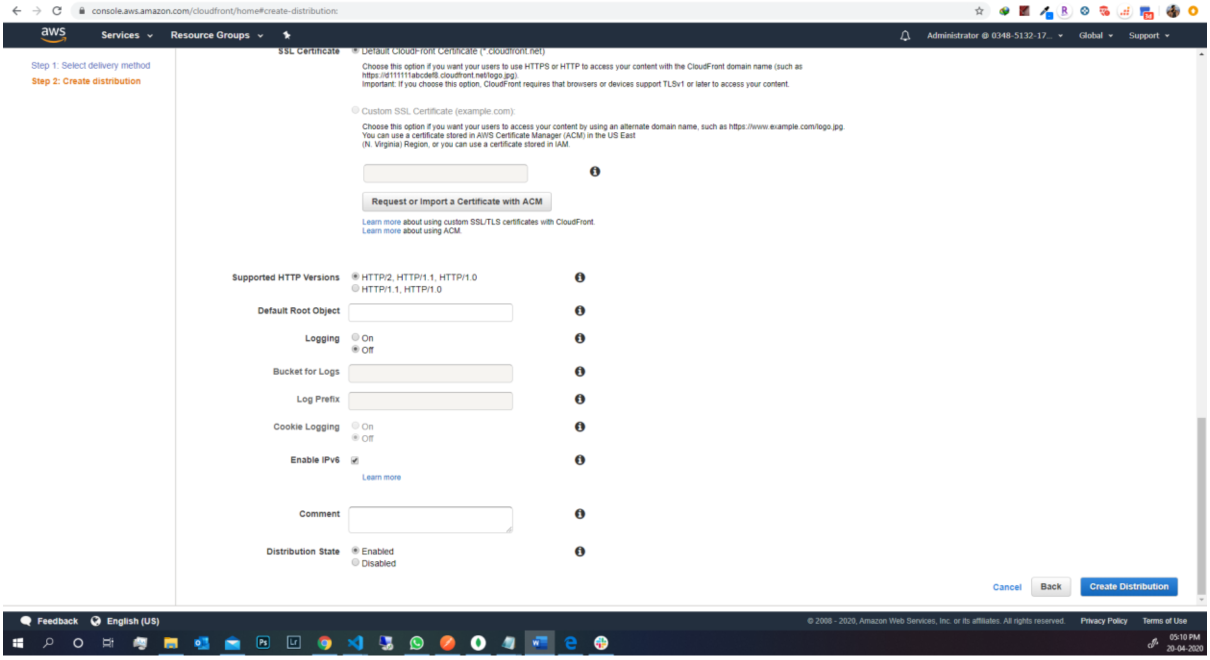
CloudFront Event	Lambda Function ARN	Include Body
Select Event Type		□

Distribution Settings

Price Class: Use All Edge Locations (Best Performance)

AWS WAF Web ACL: None

Alternate Domain Names (CNAMEs):



console.aws.amazon.com/cloudfront/home#create-distribution:
aws
Services
Resource Groups
Administrator @ 0348-5132-17...
Global
Support
Step 1: Select delivery method
Step 2: Create distribution
Request or Import a Certificate with ACM
Cancel
Back
Create Distribution
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
05:10 PM
20-04-2020

SSL Certificate ● Default CloudFront Certificate (*.cloudfront.net)

Choose this option if you want your users to use HTTPS or HTTP to access your content with the CloudFront domain name (such as https://d111111abcdef8.cloudfront.net/logo.jpg).
Important: If you choose this option, CloudFront requires that browsers or devices support TLSv1 or later to access your content.

○ Custom SSL Certificate (example.com):

Choose this option if you want your users to access your content by using an alternate domain name, such as https://www.example.com/logo.jpg.
You can use a certificate stored in AWS Certificate Manager (ACM) in the US East
(N. Virginia) Region, or you can use a certificate stored in IAM.

Learn more about using custom SSL/TLS certificates with CloudFront.
Learn more about using ACM.

Supported HTTP Versions ● HTTP/2, HTTP/1.1, HTTP/1.0 ○ HTTP/1.1, HTTP/1.0

Default Root Object

Logging ○ On ● Off

Bucket for Logs

Log Prefix

Cookie Logging ○ On ● Off

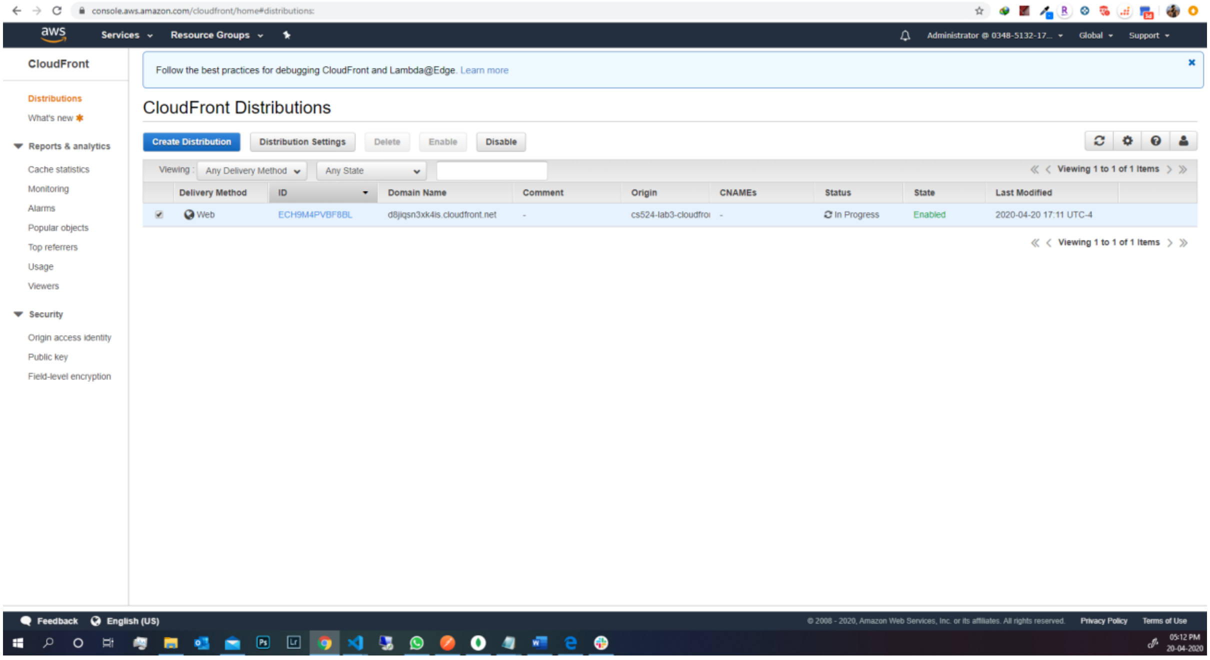
Enable IPv6 ☑
Learn more

Comment

Distribution State ● Enabled ○ Disabled

Finally click on create distribution. To finish the creation

You can now see the distribution is getting created.

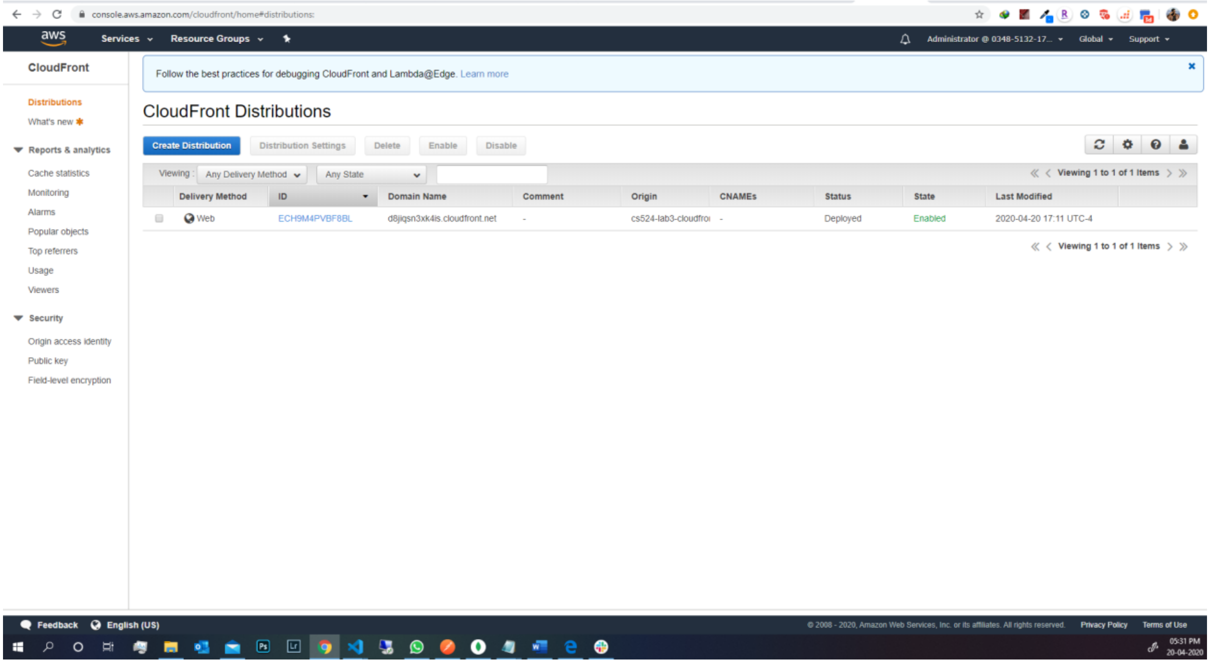


Follow the best practices for debugging CloudFront and Lambda@Edge. Learn more

CloudFront Distributions

	Delivery Method	ID	Domain Name	Comment	Origin	CNAMEs	Status	State	Last Modified
☑	Web	ECH9M4PVBF8BL	d8jiqsn3xk4is.cloudfront.net	-	cs524-lab3-cloudfro	-	In Progress	Enabled	2020-04-20 17:11 UTC-4

Now we can see that the status of the cloudfront has been changed to deployed.

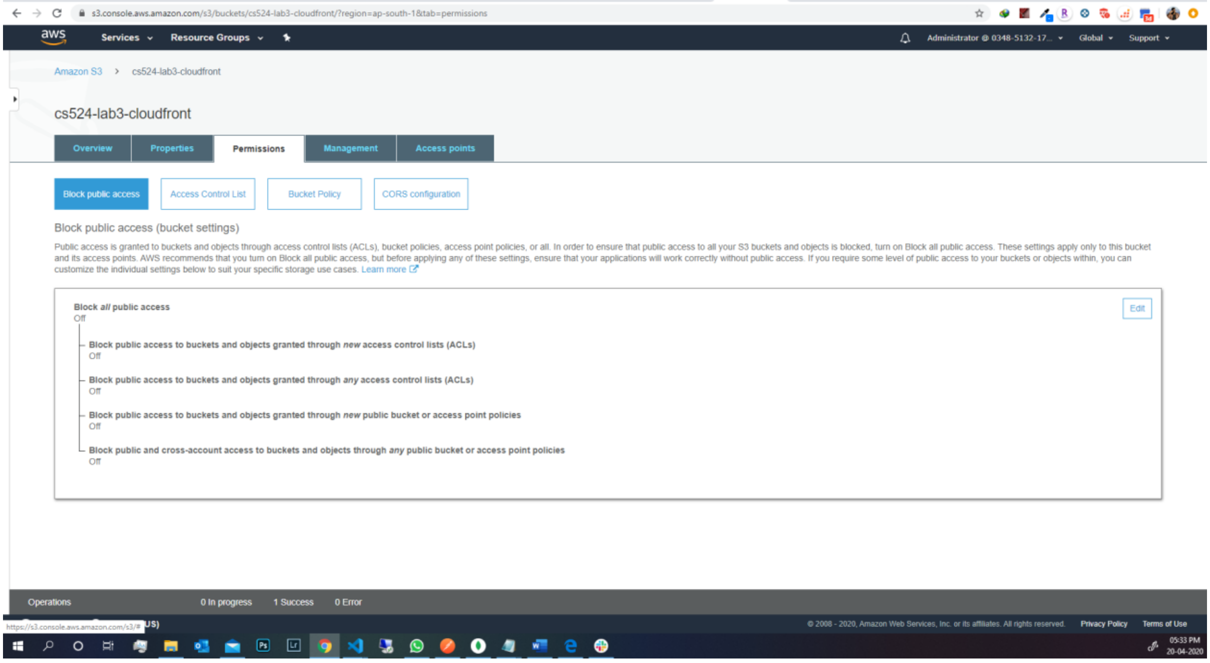


Follow the best practices for debugging CloudFront and Lambda@Edge. Learn more

CloudFront Distributions

	Delivery Method	ID	Domain Name	Comment	Origin	CNAMEs	Status	State	Last Modified
□	Web	ECH9M4PVBF8BL	d8jiqsn3xk4is.cloudfront.net	-	cs524-lab3-cloudfro	-	Deployed	Enabled	2020-04-20 17:11 UTC-4

We need to go back to s3 now to disable



cs524-lab3-cloudfront

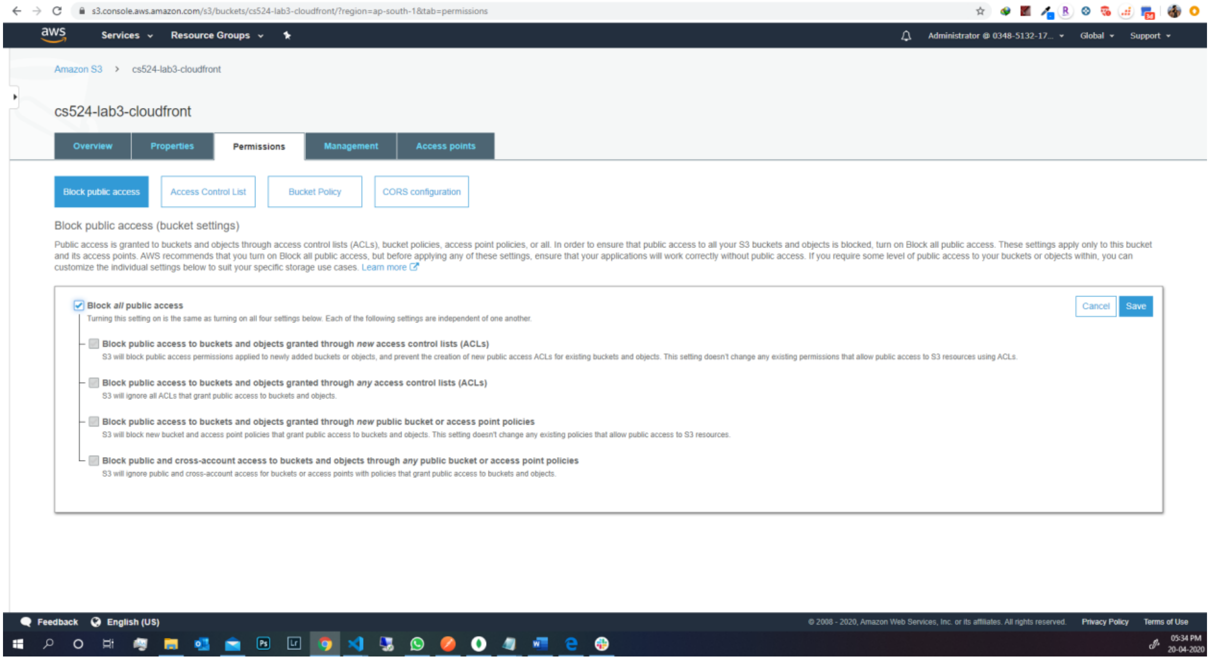
Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

Block *all* public access
Off

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

Click on block public access after clicking edit and click on save.



s3.console.aws.amazon.com/s3/buckets/cs524-lab3-cloudfront/?region=ap-south-1&tab=permissions
aws
Services
Resource Groups
Administrator @ 0348-5132-17...
Global
Support
Amazon S3 > cs524-lab3-cloudfront
Overview
Properties
Permissions
Management
Access points
Block public access
Access Control List
Bucket Policy
CORS configuration
Cancel
Save
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
05:34 PM
20-04-2020

cs524-lab3-cloudfront

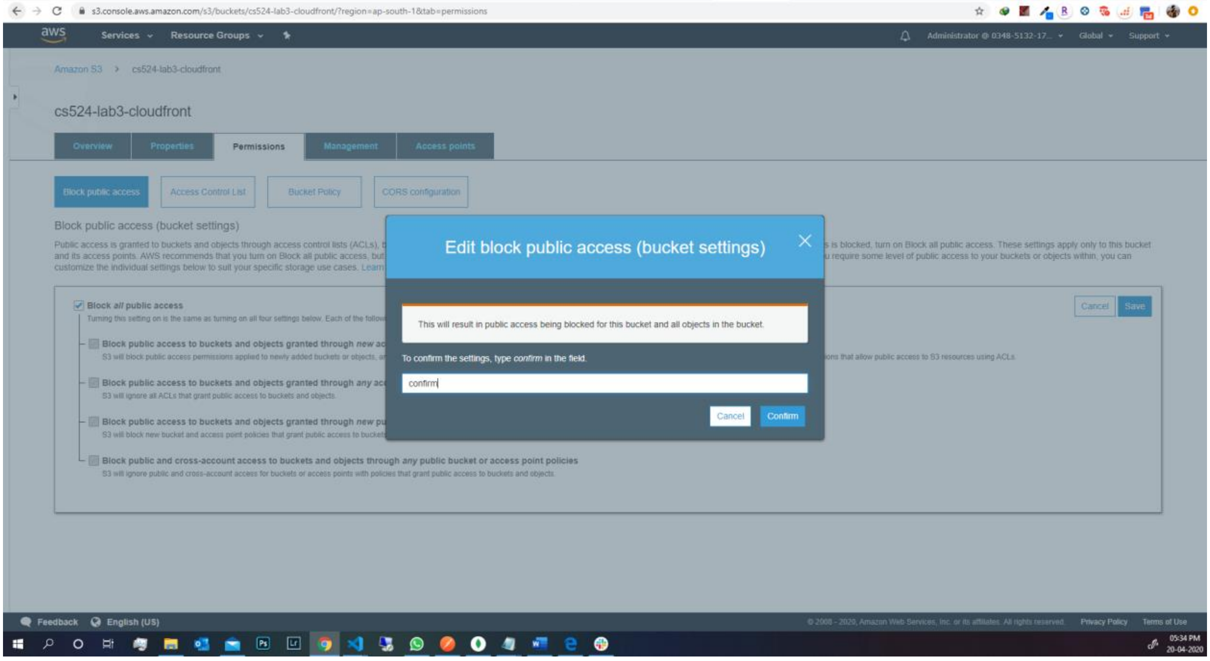
Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets 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.

You will be prompted with the dialog to type confirm in order to block public access.



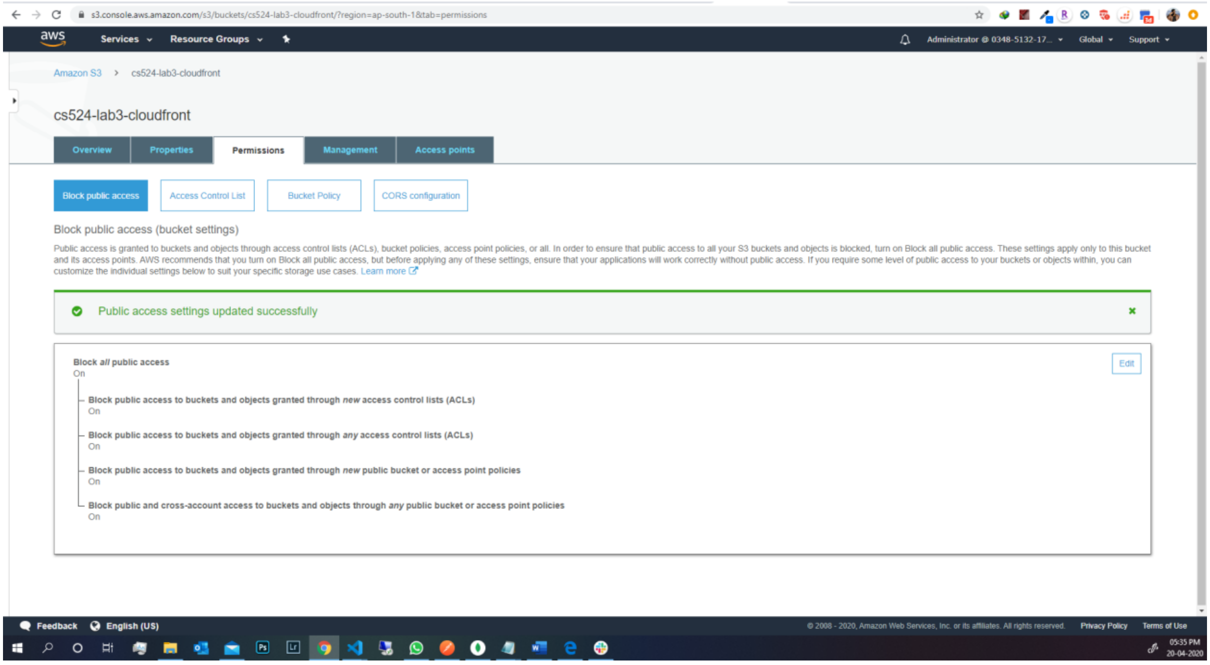
Edit block public access (bucket settings)

This will result in public access being blocked for this bucket and all objects in the bucket.

To confirm the settings, type *confirm* in the field.

confirm

After clicking confirm, the settings got saved.


s3.console.aws.amazon.com/s3/buckets/cs524-lab3-cloudfront/?region=ap-south-1&tab=permissions
aws
Services
Resource Groups
Administrator @ 0348-5132-17...
Global
Support
Amazon S3 > cs524-lab3-cloudfront
Overview
Properties
Permissions
Management
Access points
Block public access
Access Control List
Bucket Policy
CORS configuration
Edit
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
05:35 PM
20-04-2020

cs524-lab3-cloudfront

Block public access (bucket settings)

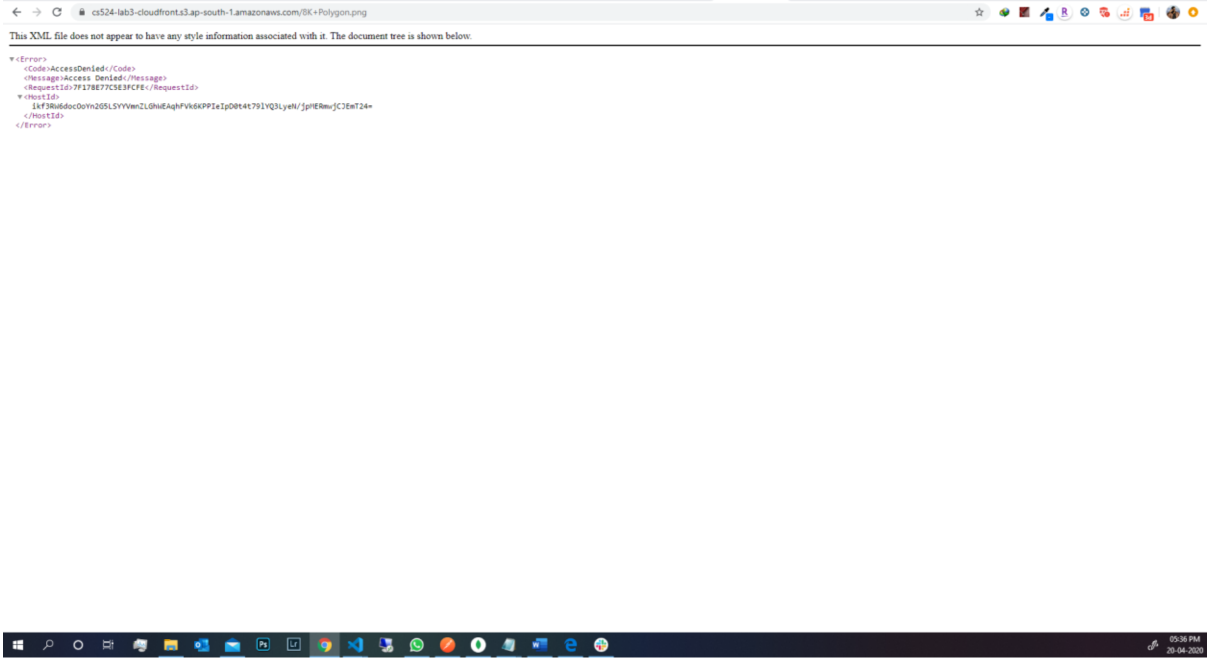
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

Public access settings updated successfully

Block *all* public access
On

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

Now when you try to open the image from the url (https://cs524-lab3-cloudfront.s3.ap-south-1.amazonaws.com/8K+Polygon.png) you will get an error

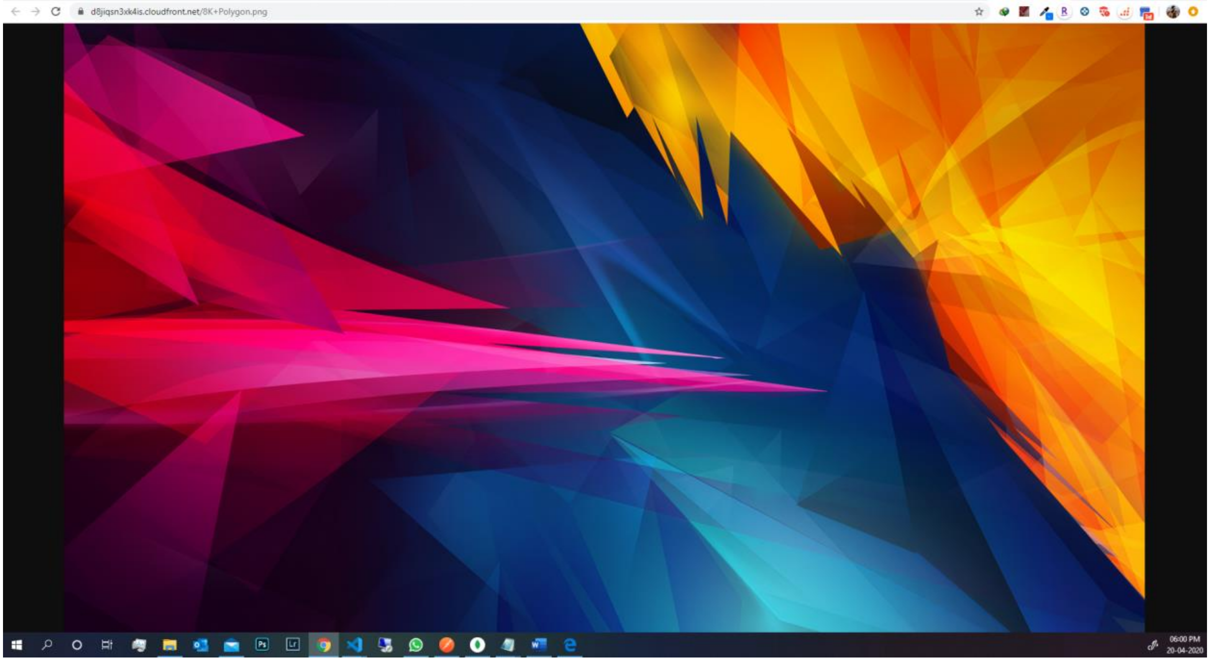

cs524-lab3-cloudfront.s3.ap-south-1.amazonaws.com/8K+Polygon.png
05:36 PM
20-04-2020

This XML file does not appear to have any style information associated with it. The document tree is shown below.

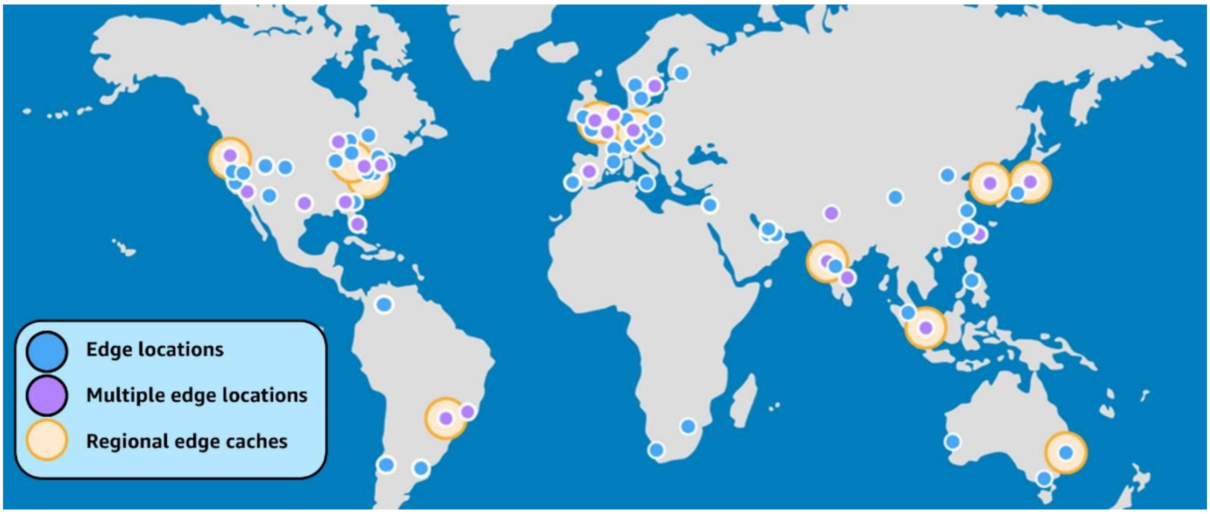
```
▼<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>7F178E77C5E3FCFE</RequestId>
 ▼<HostId>
    ikf3RW6docOoYn2G5LSYYVmnZLGhWEAqhFVk6KPPIeIpD0t4t79lYQ3LyeN/jpMERmwjCJEmT24=
   </HostId>
 </Error>
```

This can now be accessed from cloud front by entering the domain name of the cloudfront we just deployed followed by the Origin path(/8K+Polygon.png) It takes close to 10 – 15 mins to get deployed. Keep calm until then.

https://d8jiqsn3xk4is.cloudfront.net/8K+Polygon.png



When I had created the cloudfront, the server was in Mumbai location so the first time, I tried to access the resource, it was a bit slow since it is in the other side of the globe. But after requesting it once, it gets cached in the local edge location and starts loading blazing fast. In the image below we can see edge locations & regional edge cache.



Benefits of using CDN:

1. **Load on the server will decrease drastically.**
2. **Content delivery becomes faster.**
3. **We can easily segment our audience.**
4. **There will be negligible network latency and packet drops.**
5. **High UP times & Less Down times.**
6. **Your data is safe and secure.**

7. **You don’t have to worry of any natural calamity and your service will be always UP & running.**

Few of the settings that we used. Help documentation from aws.

Origin Settings

When you create or update a distribution, you provide information about one or more locations—known as origins—where you store the original versions of your web content. CloudFront gets your web content from your origins and serves it to viewers via a world-wide network of edge servers. Each origin is either an Amazon S3 bucket or an HTTP server, for example, a web server.

For the current maximum number of origins that you can create for a distribution, or to request a higher quota (formerly known as limit), see General Quotas on Web Distributions.

Origin Path

If you want CloudFront to request your content from a directory in your AWS resource or your custom origin, enter the directory path, beginning with a slash (/). CloudFront appends the directory path to the value of **Origin Domain Name**, for example, **cf-origin.example.com/production/images**. Do not add a slash (/) at the end of the path.

For example, suppose you've specified the following values for your distribution:

- **Origin Domain Name** – An Amazon S3 bucket named **myawsbucket**
- **Origin Path** – **/production**
- **Alternate Domain Names (CNAMEs)** – **example.com**

When a user enters **example.com/index.html** in a browser, CloudFront sends a request to Amazon S3 for **myawsbucket/production/index.html**.

When a user enters **example.com/acme/index.html** in a browser, CloudFront sends a request to Amazon S3 for **myawsbucket/production/acme/index.html**.

Origin ID

A string that uniquely distinguishes this origin or origin group in this distribution. If you create cache behaviors in addition to the default cache behavior, you use the ID that you specify here to identify the origin or origin group that you want CloudFront to route a request to when the request matches the path pattern for that cache behavior.

For more information, see the following:

- **Origins that you can specify:** Using CloudFront Origin Groups
- **Creating origin groups:** Creating an Origin Group
- **Working with cache behaviors:** Cache Behavior Settings

Restrict Bucket Access

Note

Applies only to Amazon S3 bucket origins (except if configured as website endpoints).

Choose **Yes** if you want to require users to access objects in an Amazon S3 bucket by using only CloudFront URLs, not by using Amazon S3 URLs. Then specify additional values.

Choose **No** if you want users to be able to access objects by using either CloudFront URLs or Amazon S3 URLs.

For more information, see Restricting Access to Amazon S3 Content by Using an Origin Access Identity.

For information about how to require users to access objects on a custom origin by using only CloudFront URLs, see Restricting Access to Files on Custom Origins.

Origin Access Identity

Note

Applies only to Amazon S3 bucket origins (except if configured as website endpoints).

If you chose **Yes** for **Restrict Bucket Access**, choose whether to create a new origin access identity or use an existing one that is associated with your AWS account. If you already have an origin access identity, we recommend that you reuse it to simplify maintenance. For more information about origin access identities, see Restricting Access to Amazon S3 Content by Using an Origin Access Identity.

Comment for New Identity

Note

Applies only to Amazon S3 bucket origins (except if configured as website endpoints).

If you chose **Create a New Identity** for **Origin Access Identity**, enter a comment that identifies the new origin access identity. CloudFront creates the origin access identity when you create this distribution.

Your Identities

Note

Applies only to Amazon S3 bucket origins (except if configured as website endpoints).

If you chose **Use an Existing Identity** for **Origin Access Identity**, choose the origin access identity that you want to use. You cannot use an origin access identity that is associated with another AWS account.

Grant Read Permissions on Bucket

Note

Applies only to Amazon S3 bucket origins (except if configured as website endpoints).

If you want CloudFront to automatically grant the origin access identity the permission to read objects in your Amazon S3 bucket, choose **Yes, Update Bucket Policy**.

Important

If you choose **Yes, Update Bucket Policy**, CloudFront updates the bucket policy to grant the specified origin access identity the permission to read objects in your bucket. However, CloudFront does not remove existing permissions in the bucket policy or permissions on individual objects. If users currently have permission to access the objects in your bucket using Amazon S3 URLs, they will still have that permission after CloudFront updates your bucket policy. To view or change the existing bucket policy and the existing permissions on the objects in your bucket, use a method provided by Amazon S3. For more information, see Granting the OAI Permission to Read Files in Your Amazon S3 Bucket.

If you want to update permissions manually, for example, if you want to update ACLs on your objects instead of updating bucket permissions, choose **No, I will Update Permissions**.