

## Lab 4: CS 524

In this assignment, you will learn use S3 bucket and use CDN with Cloudfront and report the results.

**ANS.**

**S3:**

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 data lakes, 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 99.99999999% (11 9's) of durability, and stores data for millions of applications for companies all around the world.

### **Bucket Policies:**

A bucket policy is a resource-based AWS Identity and Access Management (IAM) policy. You add a bucket policy to a bucket to grant other AWS accounts or IAM users access permissions for the bucket and the objects in it. Object permissions apply only to the objects that the bucket owner creates. Bucket policies use JSON-based access policy language.

### **Access control list (ACL):**

Amazon S3 access control lists (ACLs) enable you to manage access to buckets and objects. Each bucket and object has an ACL attached to it as a subresource. It defines which AWS accounts or groups are granted access and the type of access. When a request is received against a resource, Amazon S3 checks the corresponding ACL to verify that the requester has the necessary access permissions. When you create a bucket or an object, Amazon S3 creates a default ACL that grants the resource owner full control over the resource.

### **CloudFront:**

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 offers the most advanced security capabilities, including field level encryption and HTTPS support, seamlessly integrated with AWS Shield, AWS Web Application Firewall and Route 53 to protect against multiple types of attacks including network and application layer DDoS attacks. These services co-reside at edge networking locations – globally scaled and connected via the AWS network backbone – providing a more secure, performant, and available experience for your users.

CloudFront works seamlessly with any AWS origin, such as Amazon S3, Amazon EC2, Elastic Load Balancing, or with any custom HTTP origin.

**Origin:**

An origin is the location where content is stored, and from which CloudFront gets content to serve to viewers.

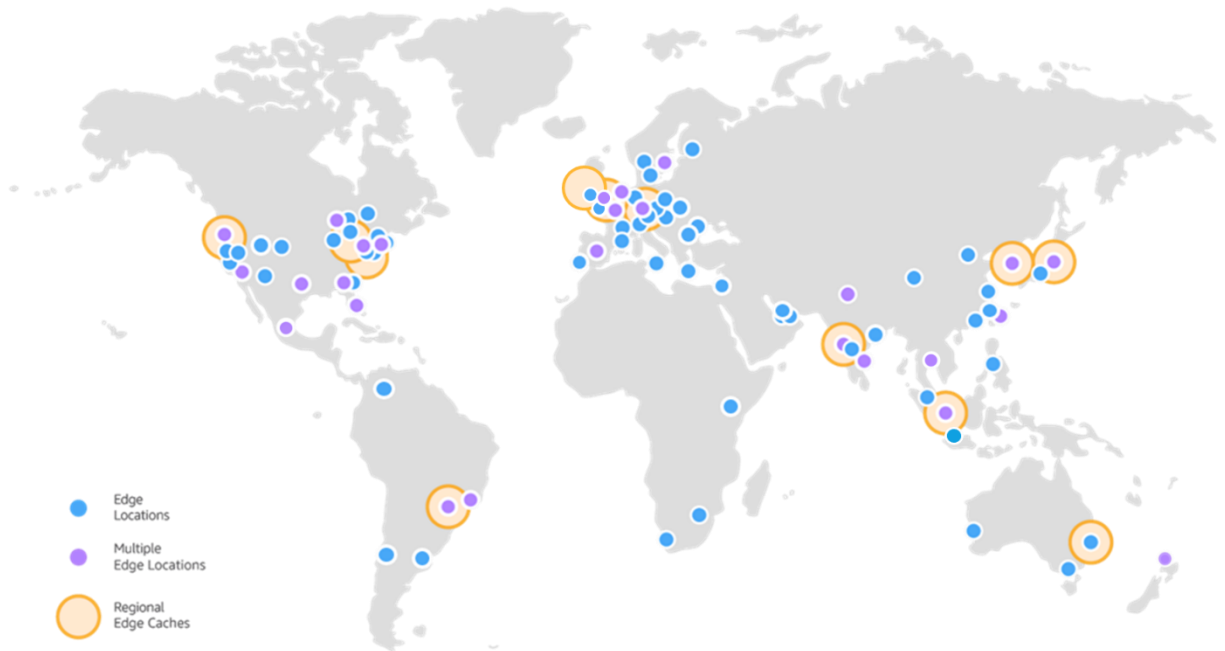
**Edge:**

CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the request is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

**Location:**

Amazon CloudFront peers with thousands of Tier 1/2/3 telecom carriers globally, is well connected with all major access networks for optimal performance and has hundreds of terabits of deployed capacity. CloudFront Edge locations are connected to the AWS Regions through the AWS network backbone - fully redundant, multiple 100GbE parallel fiber that circles the globe and links with tens of thousands of networks for improved origin fetches and dynamic content acceleration.

To deliver content to end users with lower latency, Amazon CloudFront uses a global network of 225+ Points of Presence (215+ Edge locations and 13 regional mid-tier caches) in 90 cities across 47 countries. Amazon CloudFront Edge locations are located in:



### Distribution:

When you want to use CloudFront to distribute your content, you create a distribution and choose the configuration settings you want. For example:

- Your content origin—that is, the Amazon S3 bucket, MediaPackage channel, or HTTP server from which CloudFront gets the files to distribute. You can specify any combination of up to 25 Amazon S3 buckets, channels, and/or HTTP servers as your origins.
- Access—whether you want the files to be available to everyone or restrict access to some users.
- Security—whether you want CloudFront to require users to use HTTPS to access your content.
- Cache key—which values, if any, you want to include in the cache key. The cache key uniquely identifies each file in the cache for a given distribution.
- Origin request settings—whether you want CloudFront to include HTTP headers, cookies, or query strings in requests that it sends to your origin.
- Geo-restrictions—whether you want CloudFront to prevent users in selected countries from accessing your content.
- Access logs—whether you want CloudFront to create access logs that show viewer activity.

a. Once registered for AWS, now go into AWS Console



## Sign in

☒ **Root user**

Account owner that performs tasks requiring unrestricted access. [Learn more](#)

☐ **IAM user**

User within an account that performs daily tasks. [Learn more](#)

Root user email address

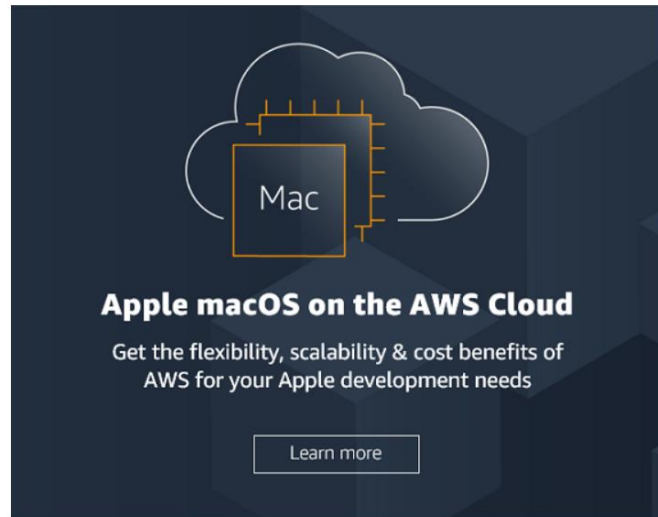
kmodi5@stevens.edu

Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

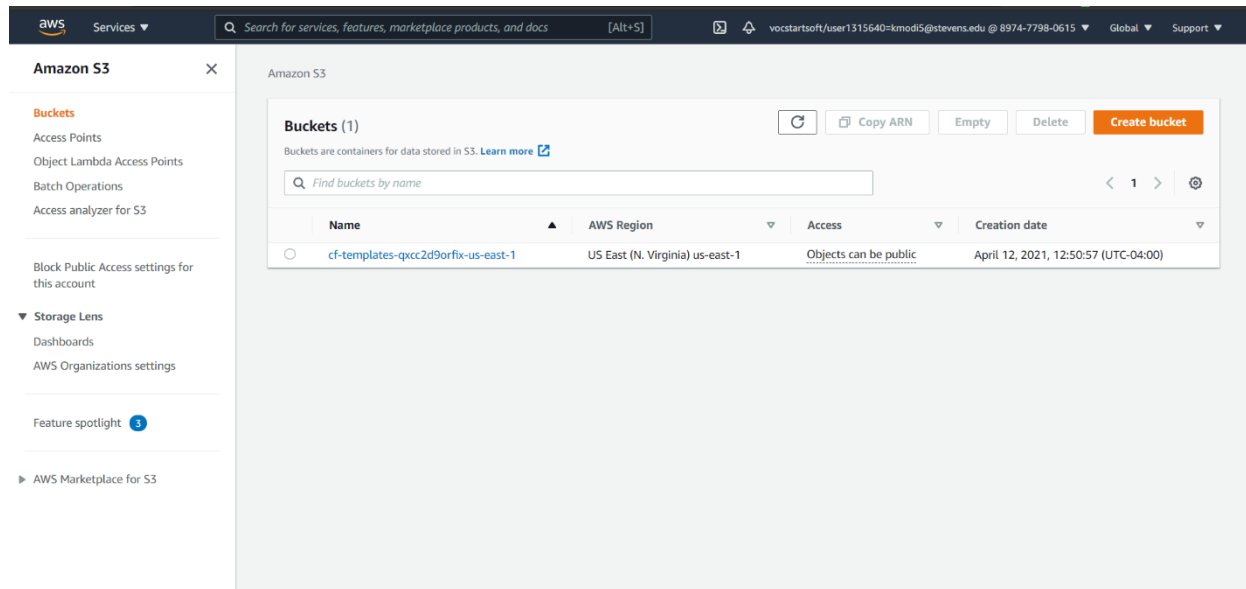
— New to AWS? —

Create a new AWS account



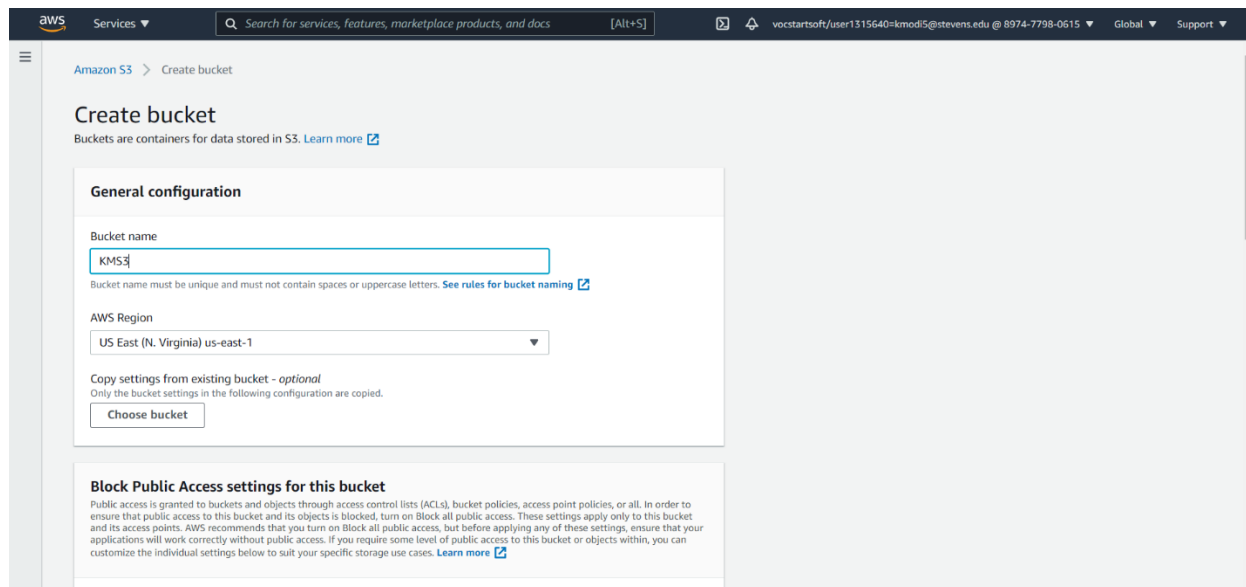
b. Go into AWS Console and Launch a S3 Bucket

### c. Create Bucket



The screenshot shows the Amazon S3 console interface. On the left, the 'Amazon S3' sidebar is visible with options like Buckets, Access Points, Object Lambda Access Points, Batch Operations, and Access analyzer for S3. The main content area is titled 'Amazon S3' and shows 'Buckets (1)'. A table lists the existing bucket: 'cf-templates-qcc2d9orfix-us-east-1' in the 'US East (N. Virginia) us-east-1' region, with 'Objects can be public' access and a creation date of 'April 12, 2021, 12:50:57 (UTC-04:00)'. Buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket' are present at the top right of the bucket list.

### d. Fill and select the requirements



The screenshot shows the 'Create bucket' wizard in the Amazon S3 console. The 'General configuration' section is active, showing a 'Bucket name' field with 'KMS3' entered. Below it, a note states: 'Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming'. The 'AWS Region' is set to 'US East (N. Virginia) us-east-1'. There is a section for 'Copy settings from existing bucket - optional' with a 'Choose bucket' button. The 'Block Public Access settings for this bucket' section is partially visible at the bottom, with a note about public access settings.

### e. Unblock all public access

aws

Services

Search for services, features, marketplace products, and docs

[Alt+S]

vocstartsoft/user1315640=kmodi5@stevens.edu @ 8974-7798-0615

Global

Support

Only the bucket settings in the following configuration are copied.

Choose bucket

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.

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

## f. Create the bucket

aws

Services

Search for services, features, marketplace products, and docs

[Alt+S]

vocstartsoft/user1315640=kmodi5@stevens.edu @ 8974-7798-0615

Global

Support

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

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

Cancel

Create bucket

g. The bucket should be ready

Amazon S3

Successfully created bucket "kms3"  
To upload files and folders, or to configure additional bucket settings choose [View details](#).

Amazon S3

**Buckets (2)**

Buckets are containers for data stored in S3. [Learn more](#)

Find buckets by name

	Name	AWS Region	Access	Creation date
<input type="radio"/>	cf-templates-qccc2d9orfix-us-east-1	US East (N. Virginia) us-east-1	Objects can be public	April 12, 2021, 12:50:57 (UTC-04:00)
<input type="radio"/>	kms3	US East (N. Virginia) us-east-1	Objects can be public	April 18, 2021, 12:06:21 (UTC-04:00)

h. Upload an object

Amazon S3

Read the S3 resources page for documentation and technical content. [Learn more](#)

**kms3**

**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](#)

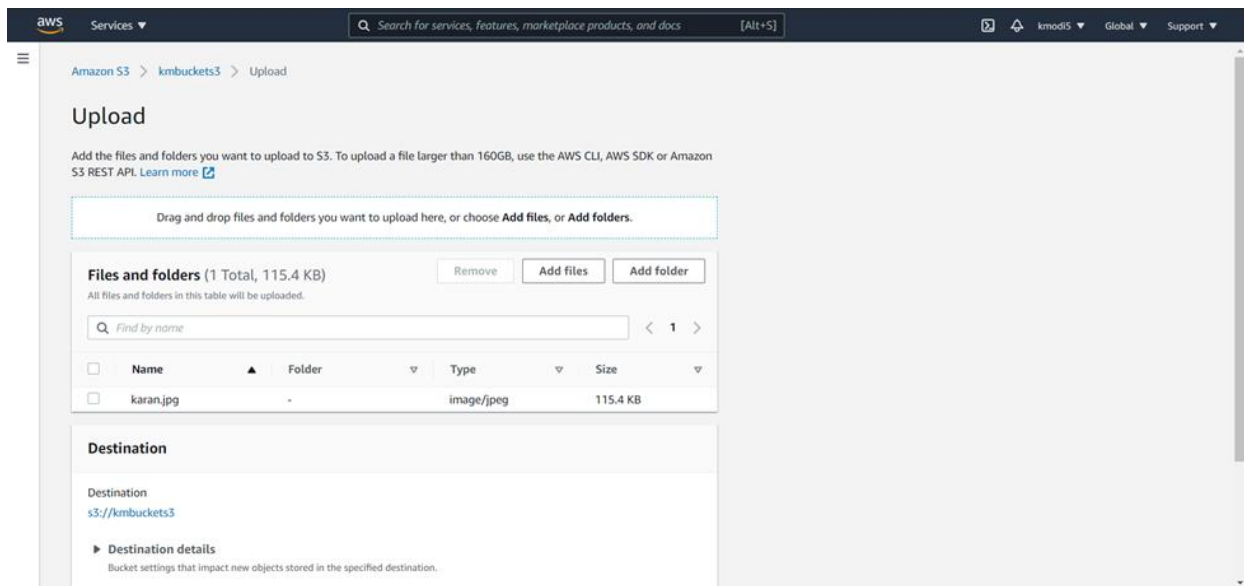
Copy URL Delete Actions Create folder Upload

Find objects by prefix

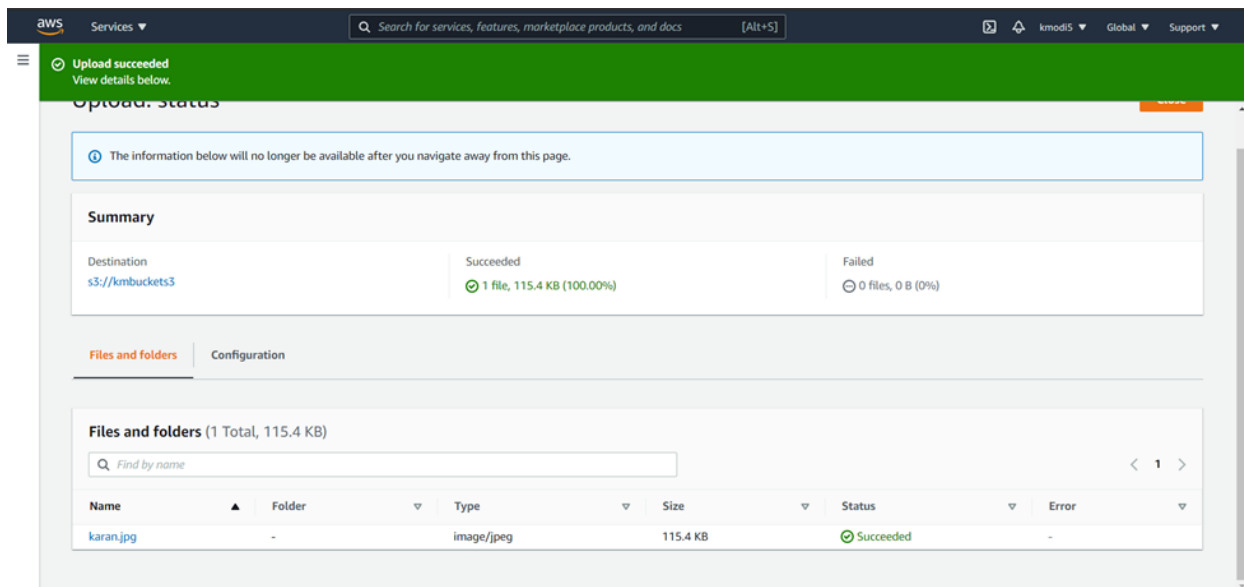
	Name	Type	Last modified	Size	Storage class
No objects You don't have any objects in this bucket.					

Upload

i. Upload a file in our case, an image

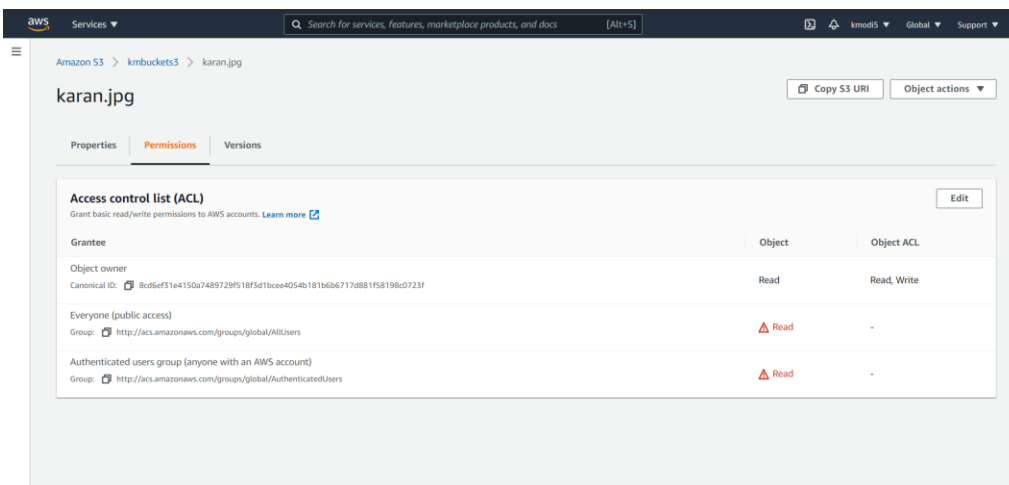
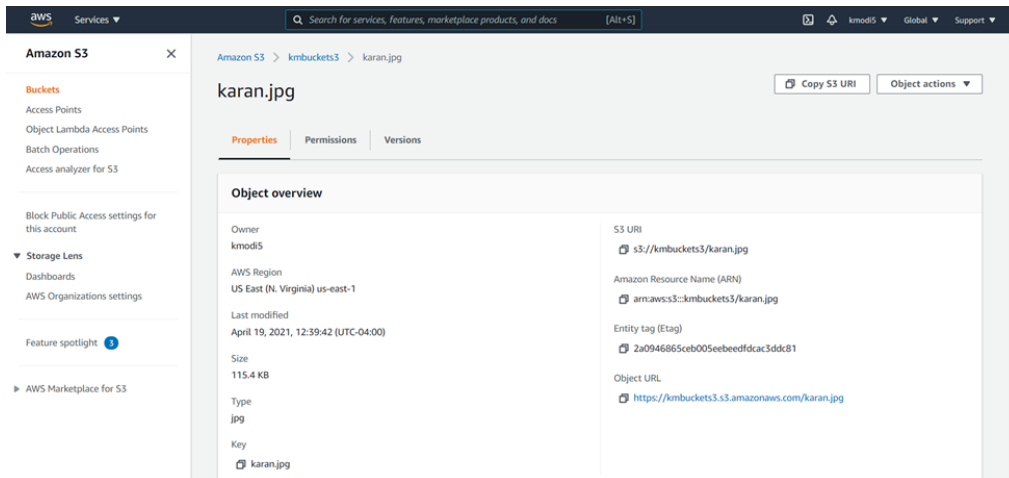


j. Check if it succeeded uploading the file

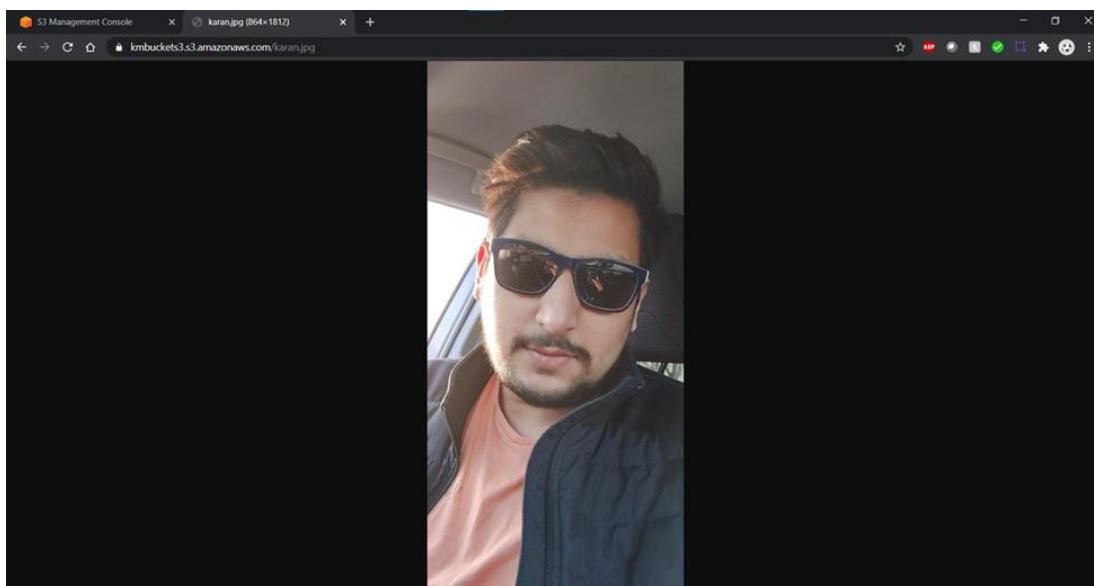


k. Give the read access for public( if required)

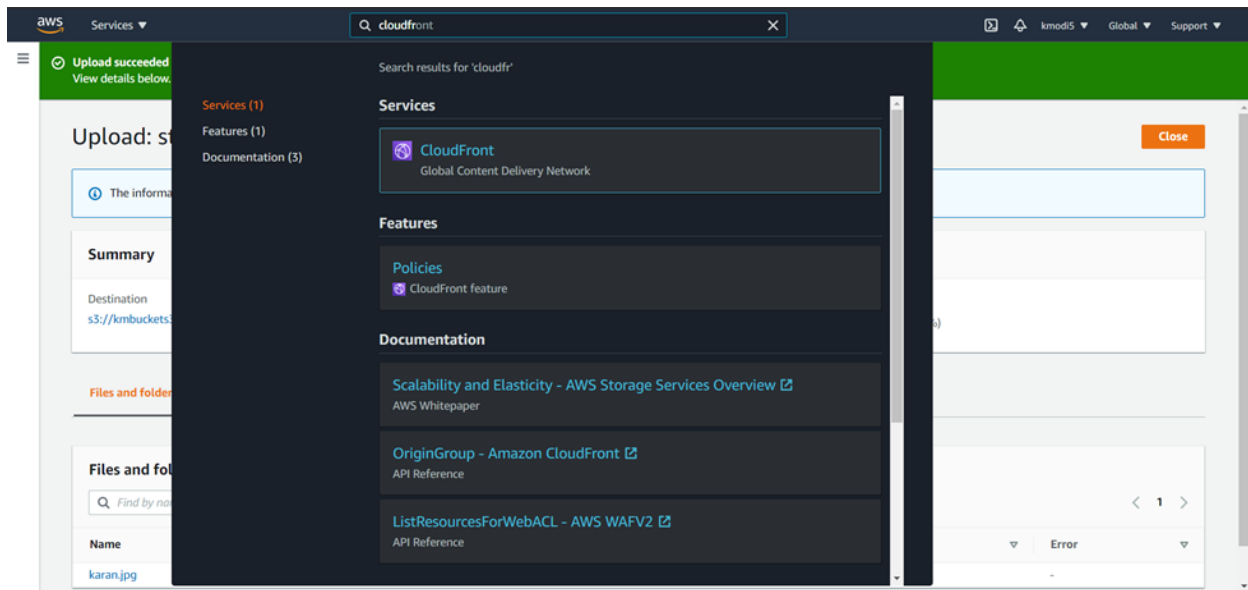




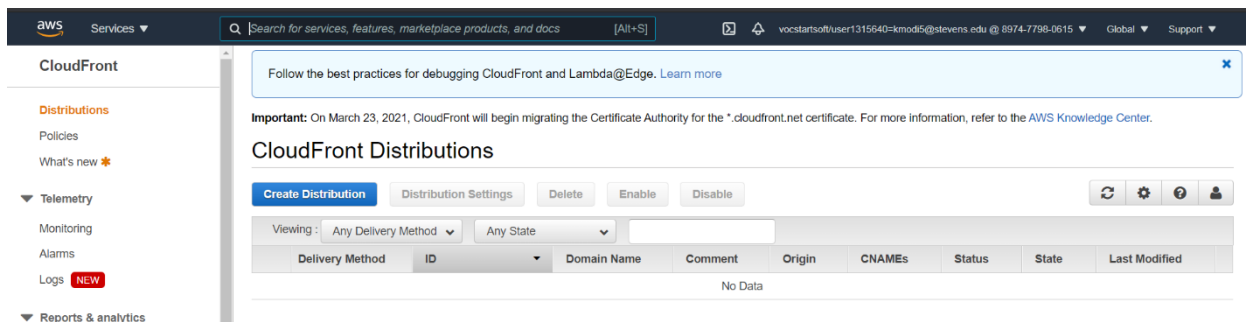
- I. Access the object using the URL: <https://kmbuckets3.s3.amazonaws.com/karan.jpg>



### m. Launch the Cloudfront



### n. Create a Distribution List



aws

Services

Search for services, features, marketplace products, and docs

[Alt+S]

Global

Support

CloudFront

Distributions

Policies

What's new

Telemetry

Monitoring

Alarms

Logs

Reports & analytics

Cache statistics

Popular objects

Top referers

Usage

Viewers

Security

Origin access identity

Field-level encryption

Key management

Follow the best practices for debugging CloudFront and Lambda@Edge. [Learn more](#)

Amazon CloudFront - Get 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](#))

Create Distribution

aws

Services

Search for services, features, marketplace products, and docs

[Alt+S]

Global

Support

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

Cancel

- o. Select the Origin Domain Name, origin access identity and create the Distribution

Services

Search for services, features, marketplace products, and docs

[Alt+S]

kmod5

Global

Support

Step 1: Select delivery method

Step 2: Create distribution

Create Distribution

Origin Settings

Origin Domain Name

kmbuckets3.s3.amazonaws.com

Origin Path

/karan.jpg

Enable Origin Shield

☐ Yes

☒ No

Origin ID

S3-kmbuckets3/karan.jpg

Restrict Bucket Access

☒ Yes

☐ No

Origin Access Identity

☒ Create a New Identity

☐ Use an Existing Identity

Comment

access-identity-kmbuckets3.s3.amazona

Grant Read Permissions on Bucket

☐ Yes, Update Bucket Policy

☒ No, I Will Update Permissions

Origin Connection Attempts

3

Origin Connection Timeout

10

Origin Custom Headers

Header Name

Value

Default Cache Behavior Settings

Services

Search for services, features, marketplace products, and docs

[Alt+S]

kmod5

Global

Support

Step 1: Select delivery method

Step 2: Create distribution

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 and origin request settings

☐ Use a cache policy and origin request policy

☒ Use legacy cache settings

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

aws

Services ▾

Search for services, features, marketplace products, and docs

[Alt+S]

🔍

🔔

kmod5 ▾

Global ▾

Support ▾

Step 1: Select delivery method

Step 2: Create distribution

### Distribution Settings

Price Class

Use All Edge Locations (Best Performance) ▾

?

AWS WAF Web ACL

None ▾

?

Alternate Domain Names (CNAMEs)

?

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://d1111111abc0def8.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.

?

Request or Import a Certificate with ACM

[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

?

Standard Logging

☐ On

?

Step 1: Select delivery method  
Step 2: Create distribution

Request or import a Certificate with ACM

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  ⓘ

Standard Logging ☐ On ☒ Off ⓘ

S3 Bucket for Logs  ⓘ

Log Prefix  ⓘ

Cookie Logging ☐ On ☒ Off ⓘ

Enable IPv6 ☒ ⓘ  
[Learn more](#)

Comment  ⓘ

Distribution State ☒ Enabled ☐ Disabled ⓘ

Cancel Back Create Distribution

p. Now check if the cloudfront distribution is deployed

Best practices to optimize Lambda@Edge with CloudFront. [Learn more](#)

Important: On March 23, 2021, CloudFront will begin migrating the Certificate Authority for the \*.cloudfront.net certificate. For more information, refer to the [AWS Knowledge Center](#).

### CloudFront Distributions

Create Distribution Distribution Settings Delete Enable Disable

Viewing: Any Delivery Method Any State << < Viewing 1 of 1 Items > >>

	Delivery Method	ID	Domain Name	Comment	Origin	CNAMEs	Status	State	Last Modified
<input type="checkbox"/>	Web	EJN4ZINKP8OIA	d2yqcow3m8hbi7.clo	-	kmbuckets3:	-	In Progress	Enabled	2021-04-19 12:52 UT

<< < Viewing 1 of 1 Items > >>

Enable new real-time metrics for better visibility of your traffic. [Learn more](#)

**Important:** On March 23, 2021, CloudFront will begin migrating the Certificate Authority for the \*.cloudfront.net certificate. For more information, refer to the [AWS Knowledge Center](#).

## CloudFront Distributions

[Create Distribution](#) [Distribution Settings](#) [Delete](#) [Enable](#) [Disable](#)

Viewing: Any Delivery Method Any State

	Delivery Method	ID	Domain Name	Comment	Origin	CNAMEs	Status	State	Last Modified
<input type="checkbox"/>	Web	EJN4ZINKP8OIA	d2yqcow3m8hbi7.clo	-	kmbuckets3:	-	Deployed	Enabled	2021-04-19 15:13 UT
<input type="checkbox"/>	Web	EXVD7RXJ0TJ39	d24vmx0t4t8c4m.clo	-	kmbuckets3:	-	In Progress	Enabled	2021-04-19 15:47 UT

Viewing 1 to 2 of 2 Items

### q. Disable public access to S3 bucket and allow only

Amazon S3 > kmbuckets3

## kmbuckets3

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

### Permissions overview

Access  
Objects can be public

### 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](#)

[Edit](#)

**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

Amazon S3 > kmbuckets3 > Edit Block public access (bucket settings)

## Edit Block public access (bucket settings)

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 in this pane

☐ Block public access to the S3 with block public access policies

☐ Block public access to the S3 with public access point policies

☐ Block public access to the S3 with public access point policies

☐ Block public and request access to buckets and objects through any public bucket or access point policies

☐ Block public and request access to buckets and objects through any public bucket or access point policies

[Cancel](#) [Save settings](#)

### Edit Block public access (bucket settings)

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

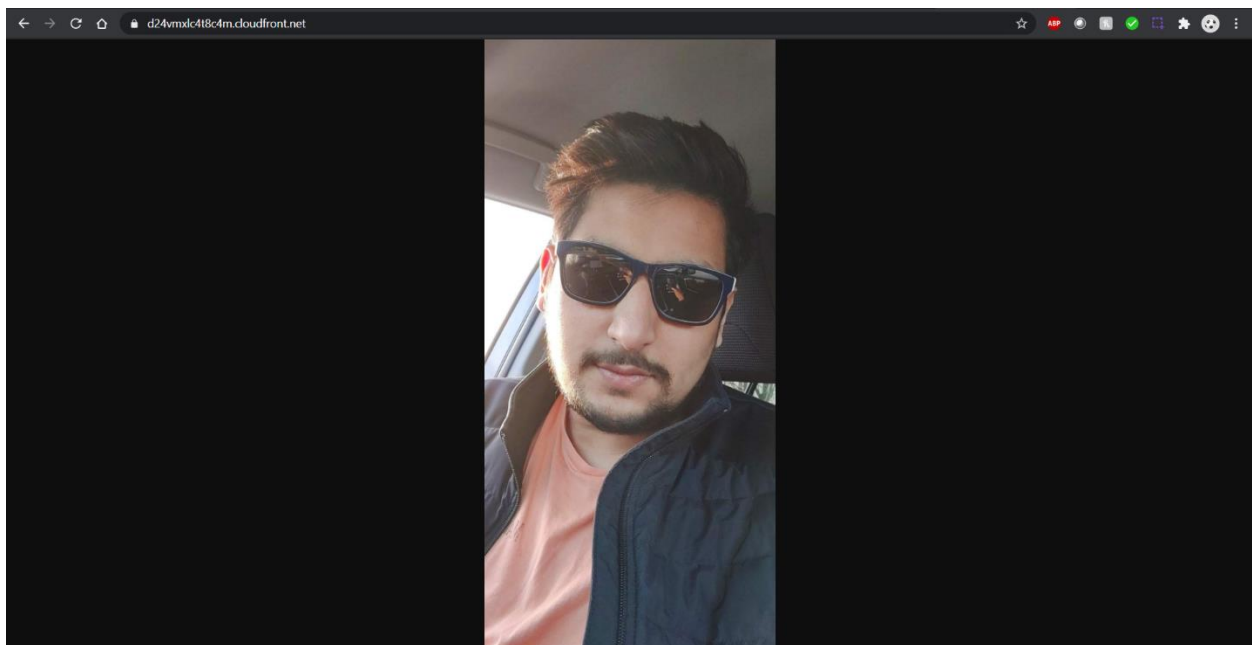
To confirm the settings, enter confirm in the field.

[Cancel](#) [Confirm](#)

- r. Since we revoked public access the object can't be retrieved for public access



- s. Cloud front URL: <https://d24vmxlc4t8c4m.cloudfront.net/>  
Using cloudfront to access the bucket object which is now saved in different locations for best performance (like cache in very close to the CPU!)



We can conclude that CDN allows fast, efficient, durable, and reliable access to our files from any geographical location as seen with the above example compared to our S3 bucket object.

A content delivery network (CDN) refers to a geographically distributed group of servers which work together to provide fast delivery of Internet content.

A CDN allows for the quick transfer of assets needed for loading Internet content including HTML pages, javascript files, stylesheets, images, and videos. The popularity of CDN services continues to grow, and today the majority of web traffic is served through CDNs, including traffic from major sites like Facebook, Netflix, and Amazon.

We can see various benefits from CDN and according to my observations it would be:

- a. Quick access at all times( low latency)



- b. Reliable storage (distributed copies at different locations)
- c. Guaranteed Service at different Geographical Locations (Asia, Americas. Europe etc)
- d. Durable file service that the file isn't lost/corrupted (redundancy)
- e. Would provide better bandwidth and with it security due to the distributed nature(DDOS)
- f. We can use this information at different locations gauge demand and for analytics
- g.