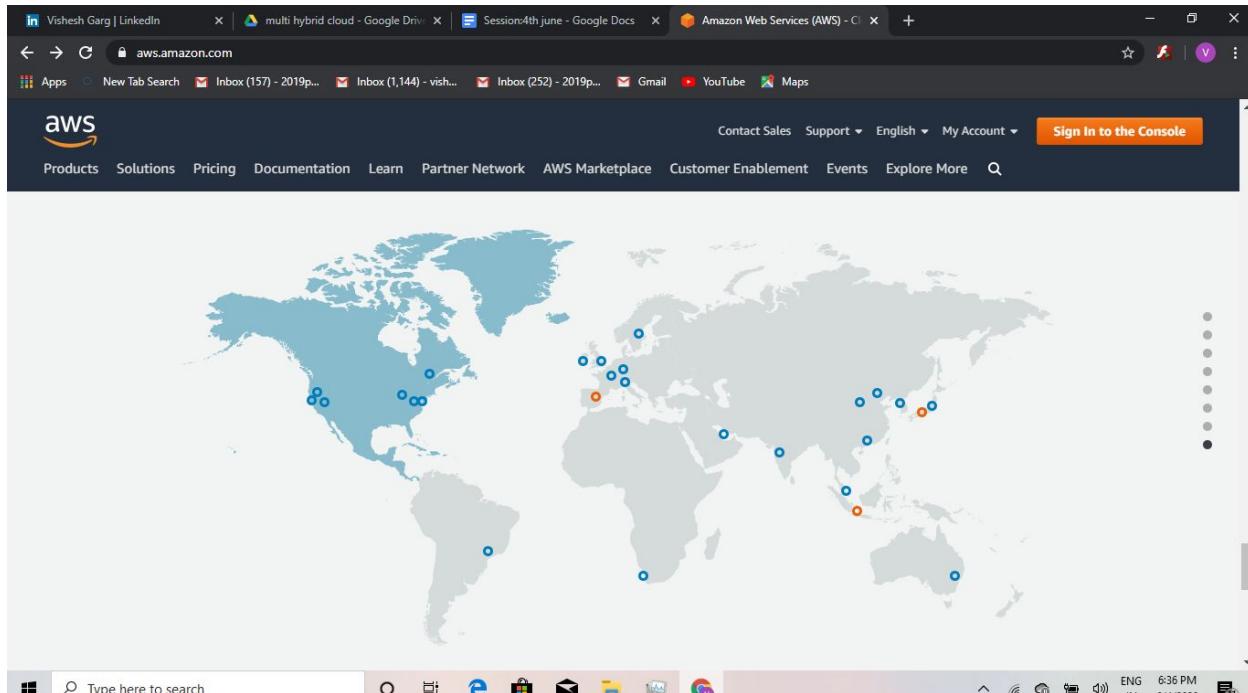
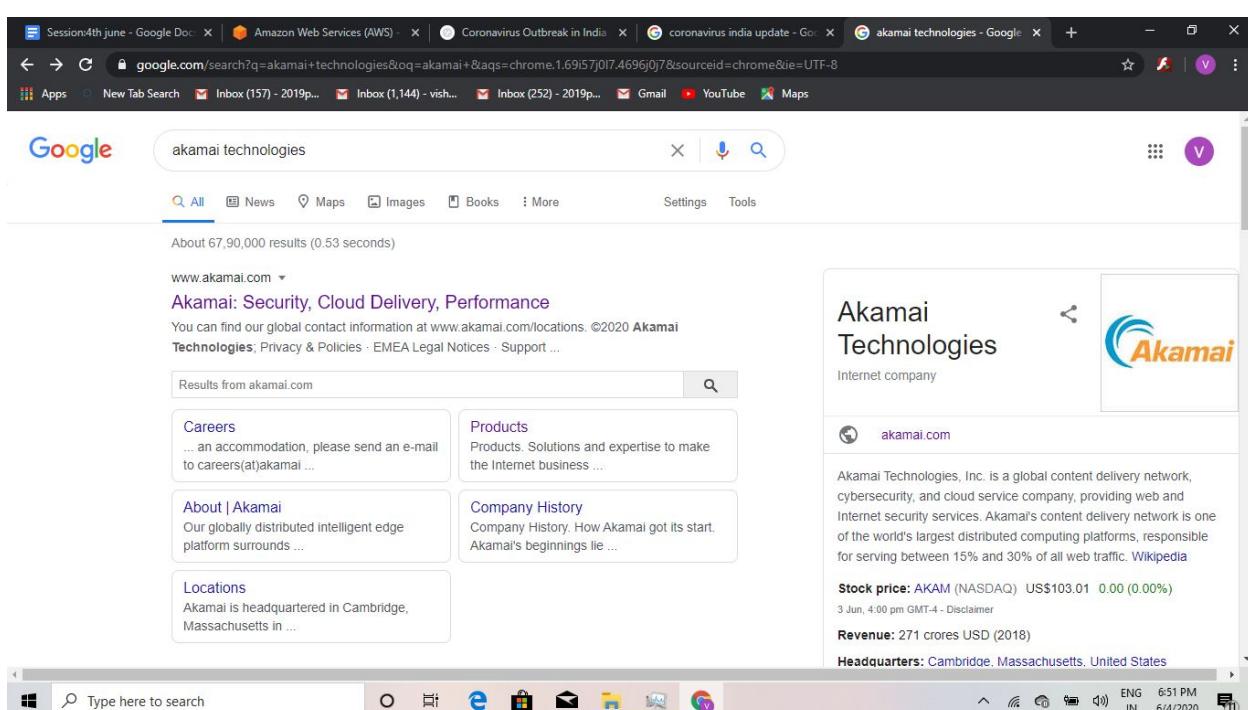


# Session:4th june



The screenshot shows the AWS homepage with a world map in the center. The map is light gray with several blue and orange dots scattered across it, representing AWS data centers or regions. The AWS logo is at the top left, and a navigation bar with links like 'Products', 'Solutions', 'Pricing', etc., is at the top right. A 'Sign In to the Console' button is also visible.

The screenshot shows a Google search results page for "akamai technologies". The search bar at the top contains the query. Below the search bar, there are several search filters: All, News, Maps, Images, Books, More, Settings, and Tools. The main search results area shows a snippet from the official Akamai website. To the right of the search results, there is a sidebar with the Akamai Technologies logo, a brief description as an "Internet company", and links to their website and stock information. The status bar at the bottom indicates the time as 6:51 PM and the date as 6/4/2020.

S3 Management Console

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

visheshgargavi Global Support Documentation

Amazon S3

Buckets Batch operations Access analyzer for S3 Block public access (account settings) Feature spotlight

We've updated the console

S3 buckets

+ Create

Operations 0 In progress 1 Success 0 Error

Feedback English (US)

Type here to search

Events 0 Active notifications Versioning Disabled MFA delete Disabled Logging Disabled Static web hosting Disabled Tags 0 Tags Requester pays Disabled Object lock Disabled Server acceleration Disabled

Owner vishesh8199 Block public access Enabled Bucket policy No Access control list 1 Grantees Privacy Policy Terms of Use

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

7:31 PM 6/4/2020

**Edit block public access settings for selected buckets**

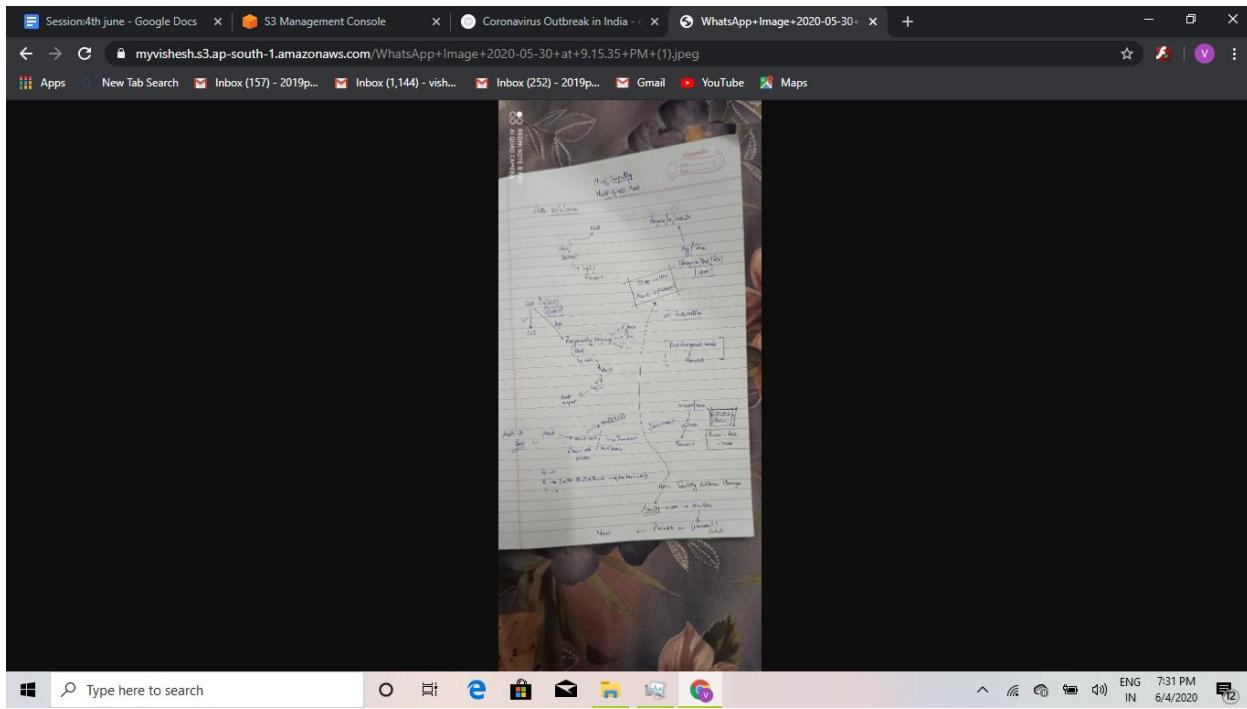
Updating the Amazon S3 block public access settings affects all selected buckets. This may result in some buckets and objects becoming public.

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

confirm

Cancel Confirm

The screenshot shows the AWS S3 Management Console interface. A modal dialog box is open in the center, titled "Edit block public access settings for selected buckets". Inside the dialog, there is a warning message: "Updating the Amazon S3 block public access settings affects all selected buckets. This may result in some buckets and objects becoming public." Below this message is a text input field containing the word "confirm". At the bottom of the dialog are two buttons: "Cancel" and "Confirm". The background of the main S3 console shows a list of buckets and various configuration settings for the account, such as "Events 0 Active notifications", "Versioning Disabled", and "Logging Disabled". The overall theme is the standard AWS dark blue color scheme.



Screenshot of the AWS S3 Management Console showing the details of a file named "WhatsApp+Image+2020-05-30+at+9.15.35+PM+(1).jpeg".

**Owner:** ee5a3a6e97b45047a93b9a3100ec1daeb1dd15bfff6a8eac799e72367ce39541b

**Last modified:** Jun 4, 2020 7:30:52 PM GMT+0530

**Etag:** 6973ec59c248aea82b13cc8b25e58f28

**Storage class:** Standard

**Server-side encryption:** None

**Size:** 91.3 KB

**Key:** WhatsApp Image 2020-05-30 at 9.15.35 PM (1).jpeg

**Object URL:** [https://myvishesh.s3.ap-south-1.amazonaws.com/WhatsApp+Image+2020-05-30+at+9.15.35+PM+\(1\).jpeg](https://myvishesh.s3.ap-south-1.amazonaws.com/WhatsApp+Image+2020-05-30+at+9.15.35+PM+(1).jpeg)

For static content using ssh /https then click on web

For live streaming eg. netflix use RTMP

The screenshot shows the AWS Management Console with the Services menu open. The left sidebar lists services like S3, CloudFront, and EC2. The main pane displays a grid of service icons and names under categories such as Media Services, Mobile, AR & VR, Machine Learning, and Application Integration.

Services listed in the main pane include:

- Media Services: Application Discovery Service, Database Migration Service, Server Migration Service, AWS Transfer Family, Snowball, DataSync.
- Mobile: Elastic Transcoder, Kinesis Video Streams, MediaConnect, MediaConvert, MediaLive, MediaPackage, MediaStore.
- AR & VR: AWS Amplify, Mobile Hub, AWS AppSync, Device Farm.
- Machine Learning: Amazon SageMaker, Amazon CodeGuru, Amazon Comprehend, Amazon Forecast, Amazon Fraud Detector, Amazon Kendra.
- Application Integration: Step Functions, Amazon AppFlow, Amazon EventBridge, Amazon MQ, Simple Notification Service.

The screenshot shows the AWS CloudFront Management console. The left sidebar has sections for CloudFront, Distributions, Reports & analytics, and Security. The main pane displays a message about accelerating dynamic content with Amazon EC2 as an origin, followed by a "Create Distribution" button and a note about creating a new distribution.

Message in the main pane:

How to accelerate your dynamic content with Amazon EC2 as an origin. [Learn more](#)

Note below the message:

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](#))

Buttons and links:

- Create Distribution
- Feedback
- English (US)

Session/4th june - Google Docs X AWS CloudFront Management C X Coronavirus Outbreak in India - X WhatsApp+Image+2020-05-30+ X +

← → ⌂ console.aws.amazon.com/cloudfront/home?region=ap-south-1#create-distribution:

Apps New Tab Search Inbox (157) - 2019p... Inbox (1,144) - vish... Inbox (252) - 2019p... Gmail YouTube Maps

aws Services Resource Groups

Select a delivery method for your content.

Step 1: Select delivery method

Step 2: Create distribution

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

Feedback English (US)

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Type here to search

8 e M 7:35 PM 6/4/2020 ENG IN

The screenshot shows the AWS CloudFront Management console with the URL `console.aws.amazon.com/cloudfront/home?region=ap-south-1#create-distribution`. The page is titled "Create Distribution" and is currently on "Step 2: Create distribution".

**Origin Settings**

- Origin Domain Name: `mvvishesh.s3.amazonaws.com`
- Origin Path: `/`
- Origin ID: `S3-mvvishesh`
- Restrict Bucket Access:  No

**Default Cache Behavior Settings**

- Path Pattern: Default (\*)
- Viewer Protocol Policy:  HTTP and HTTPS
- Allowed HTTP Methods:  GET, HEAD

At the bottom of the page, there is a "Feedback" link, a search bar, and a status bar indicating "ENG IN 7:38 PM 6/4/2020".

For restrict bucket access

for unique url any1 can open images if yes then make it public else no

The screenshot shows the AWS S3 Management Console interface. The top navigation bar includes tabs for Session:4th june - Google Doc, AWS CloudFront Management, Coronavirus Outbreak in India, WhatsApp+Image+2020-05-30, and S3 Management Console. The main content area displays the properties of an S3 object named "WhatsApp Image 2020-05-30 at 9.15.33 PM (1).jpeg". The "Properties" tab is active. The "Permissions" section shows the following:

- Access for object owner:** A table with one row for the canonical ID "ee5a3a6e97b45047a93b9a3100ec1daeb1dd 15bf6a8eac799e72367ce39541b (Your AWS account)". Under "Read object", the value is "Yes". Under "Read object permissions", the value is "Yes".
- Access for other AWS accounts:** A table with one row for the canonical ID "Everyone". Under "Read object", the value is "Yes". Under "Read object permissions", the value is "-".
- Public access:** A table with one row for the group "Everyone". Under "Read object", the value is "Yes". Under "Read object permissions", the value is "-".

A modal dialog box titled "Everyone" is overlaid on the page. It contains the following information:

- Warning:** This object has public access. Everyone has access to one or all of the following: read this object, read and write permissions.
- Access to the object:**  Read object
- Access to this object's ACL:**  Read object permissions

At the bottom of the modal are "Cancel" and "Save" buttons.

The browser status bar at the bottom shows: Feedback, English (US), Search here, and system icons including battery level, signal strength, and date/time (7:42 PM, 6/4/2020).

Screenshot of the AWS S3 Management Console showing object permissions for a file named "WhatsApp+Image+2020-05-30+at+9.15.35+PM+(1).jpeg".

The main interface shows three tabs: Overview, Properties (selected), Permissions, and Select from.

**Access for object owner:**

Canonical ID	Read object	Read object permissions
ee5a6e97b45047a93b9a3100ec1daeb1dd 15bff6a0eac799e72367ce39541b (Your AWS account)	Yes	Yes

**Access for other AWS accounts:**

+ Add account    Delete

Canonical ID	Read object	Read object permissions

**Public access:**

Group	Read object	Read object permissions
Everyone	Yes	-

A modal dialog box titled "Everyone" is open, displaying the following message:

**This object has public access**  
 Everyone has access to one or all of the following:  
 read this object, read and write permissions.

Access to the object:  
 Read object

Access to this object's ACL:  
 Read object permissions

Cancel    Save

Screenshot of a browser window showing the URL: [https://myvishesh.s3.ap-south-1.amazonaws.com/WhatsApp+Image+2020-05-30+at+9.15.35+PM+\(1\).jpeg](https://myvishesh.s3.ap-south-1.amazonaws.com/WhatsApp+Image+2020-05-30+at+9.15.35+PM+(1).jpeg).

The page content is as follows:

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>444292BA39CAE15</RequestId>
<HostId>CuHEV0d1zrGNGGSVPBxfQhvRYJETRH9U96otXgd/ojabGD13hon3/eLo8kRh5apQ0nkt40kQ=</HostId>
</Error>
```

Screenshot of a Windows taskbar showing the same URL: [https://myvishesh.s3.ap-south-1.amazonaws.com/WhatsApp+Image+2020-05-30+at+9.15.35+PM+\(1\).jpeg](https://myvishesh.s3.ap-south-1.amazonaws.com/WhatsApp+Image+2020-05-30+at+9.15.35+PM+(1).jpeg).

Go to edit and block all

The screenshot shows the AWS S3 Management Console interface. The top navigation bar includes tabs for Session/4th June - Google Doc, AWS CloudFront Management, S3 Management Console, Coronavirus Outbreak in India, and a link to myvishesh.s3.ap-south-1. The main content area displays the 'myvishesh' bucket. A search bar at the top says 'Type a prefix and press Enter to search. Press ESC to clear.' Below it are buttons for Upload, Create folder, Download, and Actions. The region is set to Asia Pacific (Mumbai). The table lists one object:

Name	Last modified	Size	Storage class
WhatsApp Image 2020-05-30 at 9.15.35 PM (1).jpeg	Jun 4, 2020 7:30:52 PM GMT+0530	91.3 KB	Standard

The screenshot shows the AWS S3 Management Console interface, specifically the 'Permissions' tab for the 'myvishesh' bucket. The title is 'Block public access (bucket settings)'. A note states: '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.' Below this is a 'Learn more' link.

The configuration form includes a 'Block all public access' checkbox, which is checked. This setting is described as turning on all four settings below. The other settings are:

- 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.

At the bottom right are 'Cancel' and 'Save' buttons.

This screenshot is identical to the one above, showing the 'Block public access (bucket settings)' configuration page for the 'myvishesh' bucket. The interface, settings, and notes are the same.

Session:4th june - Google Doc x AWS CloudFront Management x S3 Management Console x Coronavirus Outbreak in India x https://myvishesh.s3.ap-south-1.amazonaws.com/region=ap-south-1&tab=permissions

Apps New Tab Search Gmail Inbox (157) - 2019p... Gmail Inbox (1,144) - vish... Gmail Inbox (252) - 2019p... Gmail YouTube Maps

AWS Services Resource Groups

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.

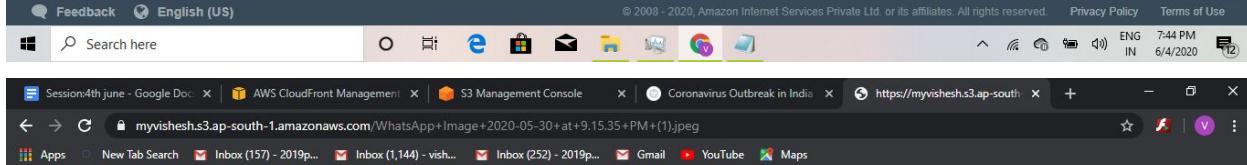
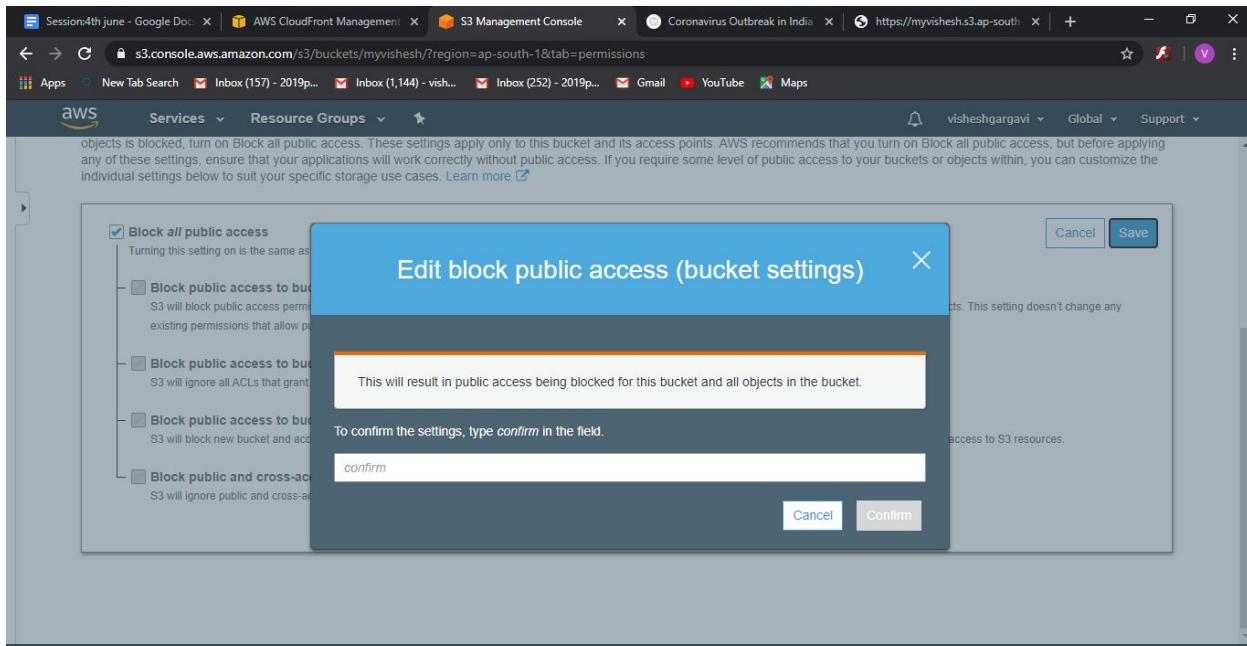
**Block public access to buckets and objects granted through new access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing 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.

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



Only give access to cdn knows as OAI (origin access identity)

Step 1: Select delivery method

Step 2: Create distribution

## Create Distribution

### Origin Settings

Origin Domain Name: myvishesh.s3.amazonaws.com

Origin Path:

Origin ID: S3-myvishesh-id

Restrict Bucket Access:  Yes  No

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

Comment: access-identity-

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

Origin Custom Headers: Header Name: Value:

### Default Cache Behavior Settings

Feedback English (US) Privacy Policy Terms of Use

Search here ENG 7:46 PM IN 6/4/2020

Session:4th june - Google Doc AWS CloudFront Management S3 Management Console Coronavirus Outbreak in India https://myvishesh.s3.ap-south-1.amazonaws.com

Feedback English (US) Privacy Policy Terms of Use

Search here ENG 7:46 PM IN 6/4/2020

Amazon S3 > myvishesh

### myvishesh

Overview Properties Bucket Policy CORS configuration

Bucket policy editor ARN: arn:aws:s3:::myvishesh  
Type to add a new policy or edit an existing policy in the text area below.

The block public access settings turned on for this bucket prevent granting public access.

1

Delete Cancel Save

Feedback English (US) Privacy Policy Terms of Use

Search here ENG 7:50 PM IN 6/4/2020

Screenshot of the AWS CloudFront Management console showing the "Create Distribution" step 2: Create distribution.

**Origin Settings**

- Origin Domain Name: myvishesh.s3.amazonaws.com
- Origin Path: (empty)
- Origin ID: S3-myvishesh-id
- Restrict Bucket Access: Yes (selected)
- Origin Access Identity: Create a New Identity (selected)
- Comment: access-identity-myvishesh.s3.amazonaws
- Grant Read Permissions on Bucket: Yes, Update Bucket Policy (selected)
- Origin Custom Headers: Header Name (empty), Value (empty)

**Default Cache Behavior Settings**

- Comment: access-identity-myvishesh.s3.amazonaws
- Grant Read Permissions on Bucket: Yes, Update Bucket Policy (selected)
- Origin Custom Headers: Header Name (empty), Value (empty)

**Default Cache Behavior Settings**

- Path Pattern: Default (\*)
- Viewer Protocol Policy: Redirect HTTP to HTTPS (selected)
- Allowed HTTP Methods: GET, HEAD (selected)
- Field-level Encryption Config: (dropdown menu)
- Cached HTTP Methods: GET, HEAD (Cached by default)
- Cache Based on Selected: None (Invalidate Cache)

default data 1 day 86400

Session/4th june - Google Doc | AWS CloudFront Management | S3 Management Console | Coronavirus Outbreak in India | https://myvishesh.s3.ap-south-1.amazonaws.com/ | +

console.aws.amazon.com/cloudfront/home?region=ap-south-1#create-distribution:

**Step 1: Select delivery method**

**Step 2: Create distribution**

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:

Comment:

Distribution State:  Enabled  Disabled

**Create Distribution**

Feedback English (US) © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Search here

s3.console.aws.amazon.com/s3/buckets/myvishesh/?region=ap-south-1&tab=permissions

Session/4th june - Google Doc | AWS CloudFront Management | S3 Management Console | Coronavirus Outbreak in India | https://myvishesh.s3.ap-south-1.amazonaws.com/ | +

Block public access Access Control List Bucket Policy CORS configuration

Bucket policy editor ARN: arn:aws:s3:::myvishesh

Type to add a new policy or edit an existing policy in the text area below.

**Bucket policy editor ARN: arn:aws:s3:::myvishesh**

The block public access settings turned on for this bucket prevent granting public access.

```

1 {
2     "Version": "2008-10-17",
3     "Id": "PolicyForCloudFrontPrivateContent",
4     "Statement": [
5         {
6             "Sid": "1",
7             "Effect": "Allow",
8             "Principal": {
9                 "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity E196W2XGG8A4F7"
10            },
11            "Action": "s3:GetObject",
12            "Resource": "arn:aws:s3:::myvishesh/*"
13        }
14    ]
15 }
```

**Delete** **Cancel** **Save**

Documentation Policy generator

Feedback English (US) © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Search here

Screenshot of the AWS CloudFront Management Console showing the CloudFront Distributions page.

**CloudFront Distributions**

Table of CloudFront Distributions:

Delivery Method	ID	Domain Name	Comment	Origin	CNAMEs	Status	State	Last Modified
Web	E1MKRGTLFNAK6	dakq84nnj9pa.cloudfront.net	-	myvishesh...	-	In Progress	Enabled	2020-06-04 19:59

**CloudFront Distribution Details (E1MKRGTLFNAK6)**

**General Tab**

ARN	arn:aws:cloudfront:410914255776:distribution/E1MKRGTLFNAK6
Log Prefix	-
Delivery Method	Web
Cookie Logging	Off
Distribution Status	Deployed
Comment	-
Price Class	Use All Edge Locations (Best Performance)
AWS WAF Web ACL	-
State	Enabled

**Origins and Origin Groups Tab**

Alternate Domain Names (CNAMEs)	Default CloudFront Certificate (*.cloudfront.net)
SSL Certificate	Default CloudFront Certificate (*.cloudfront.net)
Domain Name	dakq84nnj9pa.cloudfront.net

**Behaviors Tab**

Custom SSL Client Support	TLSv1
Security Policy	HTTP/2, HTTP/1.1, HTTP/1.0
Supported HTTP Versions	HTTP/2, HTTP/1.1, HTTP/1.0
IPv6	Enabled

**Restrictions Tab**

Default Root Object	-
Last Modified	2020-06-04 19:59 UTC+5:30
Log Bucket	-

The screenshot shows the AWS CloudFront Management Console. On the left, a sidebar menu includes 'Distributions', 'Reports & analytics' (with 'Cache statistics', 'Monitoring', 'Alarms', 'Popular objects', 'Top referrers', 'Usage', 'Viewers'), and 'Security' (with 'Origin access identity' selected). The main content area is titled 'Origin Access Identity' and displays a table with one item:

Comment	ID	Amazon S3 Canonical User ID
<input checked="" type="checkbox"/> access-identity-myvishesh.s3.amazonaws.com	E196W2XGG	7badb16a83638a3a2937e038e0391e

Below the table, two status messages are shown: 'Viewing 1 to 1 of 1 Items' and 'Viewing 1 to 1 of 1 Items'.

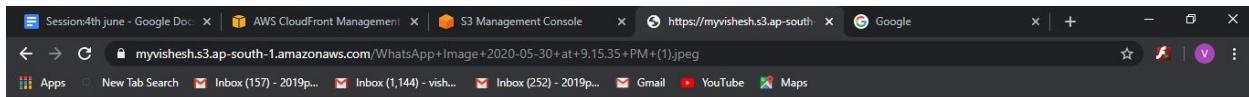
origin access identity is like a user name

The screenshot shows the AWS S3 Management Console. On the left, a sidebar menu includes 'Buckets', 'Batch operations', 'Access analyzer for S3', 'Block public access (account settings)', and 'Feature spotlight'. The main content area is titled 'Archive all of your long-term data into Amazon S3 Glacier Deep Archive to save costs. Learn more »' and shows a message: 'We've temporarily re-enabled the previous version of the S3 console while we continue to work on the new one.' Below this is a section for 'S3 buckets' with a search bar and buttons for '+ Create bucket', 'Edit public access settings', 'Empty', and 'Delete'. A list of buckets is shown, with 'myvishesh' selected. A modal window for 'myvishesh' is open, displaying the following details:

Permissions	
Owner	vishesh8199
Block public access	Enabled
Bucket policy	Yes
Access control list	1 Grantees
CORS configuration	No

Management	
Lifecycle	Disabled
Replication	Disabled
Analytics	Disabled
Inventory	Disabled
Metrics	Disabled

At the bottom of the modal, there is a 'Copy Bucket ARN' button.



CloudFront

Distributions

What's new \*

Reports & analytics

- Cache statistics
- Monitoring
- Alarms
- Popular objects
- Top referrers
- Usage
- Viewers

Security

- Origin access identity
- Public key
- Field-level encryption

How to accelerate your dynamic content with Amazon EC2 as an origin. [Learn more](#)

CloudFront Distributions

Create Distribution Distribution Settings Delete Enable Disable

Delivery Method	ID	Domain Name	Comment	Origin	CNAMEs	Status	State	Last Update
Web	E1MKRGTEFNAK6	dakq84nnj9pa.cloudfront.net	-	myvishesh	-	Deployed	Enabled	2020-

Feedback English (US) © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Screenshot of the AWS CloudFront Management console showing the popular objects report. The URL is [https://console.aws.amazon.com/cloudfront/home?region=ap-south-1#popular\\_urls](https://console.aws.amazon.com/cloudfront/home?region=ap-south-1#popular_urls).

**CloudFront Popular Objects Report**

Start Date: 2020-05-22 | End Date: 2020-06-04 | Web Distribution: E1MKRGTEFLNAK6 (myvishesl) | Update | CSV

The following report shows selected values from CloudFront access logs for the 50 most popular objects by number of requests. The Popular Objects report is available only for web distributions that had activity during the specified period and that have not been deleted. For information about how columns in the table map to columns in the access logs and about how the popularity of objects is calculated, see [CloudFront Popular Objects Report](#).

**Show Details**

Object	Req	Hit	Miss	Hits	Bytes From Miss:	Total Bytes	Incomplete I	2x:	3x:	4x:	5x:
1 /WhatsApp+Image+2020-05-30+aI+9.15.35+PM+(1).ji	4	0	2	0.00	1.54 KB	2.79 KB	0	0	4	0	0

Viewing 1 to 1 of 1 Items

Feedback English (US)

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Search here

Screenshot of the AWS CloudFront Management console showing the viewers reports. The URL is [https://console.aws.amazon.com/cloudfront/home?region=ap-south-1#viewers\\_reports](https://console.aws.amazon.com/cloudfront/home?region=ap-south-1#viewers_reports).

**CloudFront**

End Date: 2020-06-04 | Update | CSV

The following charts show information about the devices from which CloudFront received requests for the selected distribution. The Devices charts are available only for web distributions that had activity during the specified period and that have not been deleted.

**Devices** Show Details Pie Chart

Device Type	Percentage
Desktop	~75%
Unknown	~20%
Mobile	~5%

Feedback English (US)

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Search here

Screenshot of the AWS CloudFront Management Console showing usage reports for a specific distribution.

**CloudFront Usage Report (End Date: 2020-06-04)**

The following charts show selected values from the AWS Usage Report for CloudFront. If you choose All Web Distributions in the Distribution list, the charts include totals for all of your web distributions that had activity during the specified period and that have not been deleted. If you choose All Deleted Web Distributions, the charts include totals for all of your deleted web distributions that had activity during the specified period. If you choose a region that is not in the price class for your distribution, the charts may not show any usage. Charts are not available for RTMP distributions. For more information, see [CloudFront Usage Charts](#).

**Number of Requests (Millions | Thousands | Not Scaled) Show Details**

Number of HTTP Requests (checked) Number of HTTPS Requests (checked)

Time UTC

**Metrics Summary**

Category	Total	Average	Minimum	Maximum
Number of HTTP Requests	0	0	0	0
Number of HTTPS Requests	0	0	0	0
All Requests	0	0	0	0

Feedback English (US) © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

**CloudFront Distribution Settings (E1MKRGTLFNAK)**

**Restrictions**

If you need to prevent users in selected countries from accessing your content, you can specify either a whitelist (countries where they can access your content) or a blacklist (countries where they cannot). For more information, see [Restricting the Geographic Distribution of Your Content](#) in the [Amazon CloudFront Developer Guide](#).

**Geo Restriction**

Restriction	Status	Type
Geo Restriction	Disabled	-

Viewing 1 to 1 of 1 Items

Feedback English (US) © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Screenshot of the AWS CloudFront Management console showing the CloudFront Distributions page.

The left sidebar shows the navigation menu:

- Distributions
- Reports & analytics
  - Cache statistics
  - Monitoring
  - Alarms
  - Popular objects
  - Top referrers
  - Usage
  - Viewers
- Security
  - Origin access identity
  - Public key
  - Field-level encryption

The main content area displays the following information:

CloudFront Distributions > E1MKRGTLEFNAK6

Loading...

At the bottom of the main content area, there is a note about geographic distribution restrictions:

If you need to prevent users in selected countries from accessing your content, you can specify either a whitelist (countries where they can access your content) or a blacklist (countries where they cannot). For more information, see [Restricting the Geographic Distribution of Your Content](#) in the [Amazon CloudFront Developer Guide](#).

Below this note is a table titled "Edit" showing one item:

	Restriction	Status	Type
<input type="checkbox"/>	Geo Restriction	Enabled	Whitelist

Feedback English (US)

Screenshot of the AWS CloudFront Management console showing the "Edit Geo-Restrictions" page.

**Geo-Restriction Settings**

Enable Geo-Restriction:  Yes  No

Restriction Type:  Whitelist  Blacklist

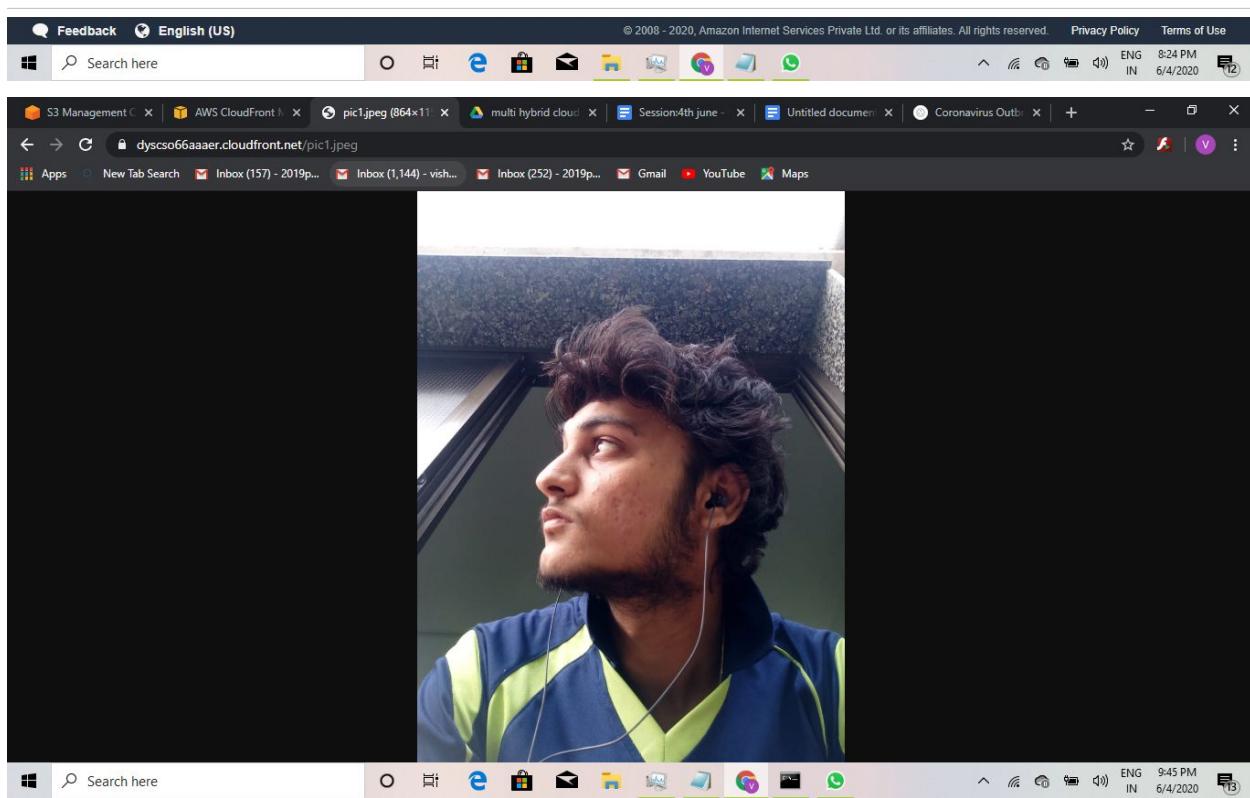
Countries:

Country Code -- Country Name
AF -- AFGHANISTAN
AX -- ALAND ISLANDS
AL -- ALBANIA
DZ -- ALGERIA
AS -- AMERICAN SAMOA
AD -- ANDORRA

IN -- INDIA

Add >> << Remove

Cancel Yes, Edit



CloudFront Popular Objects Report

Start Date: 2020-05-22 | End Date: 2020-06-04 | Web Distribution: EB5C5W2WUAVP3 (myvishesh) | Update | CSV

Object	Req	Hit	Miss	Hits	Bytes From Miss	Total Bytes	Incomplete	2x:	3x:	4x:	5x:
/pic1.jpeg	1	0	1	0.00	109.93 KB	109.93 KB	0	1	0	0	0
/favicon.ico	1	0	0	0.00	0 B	483 B	0	0	0	1	0

Distributions  
What's new \*

Reports & analytics  
Cache statistics  
Monitoring  
Alarms  
**Popular objects**  
Top referrers  
Usage  
Viewers

Security  
Origin access identity  
Public key  
Field-level encryption

Show Details

Viewing 1 to 2 of 2 Items

Object	Req	Hit	Miss	Hits	Bytes From Miss	Total Bytes	Incomplete	2x:	3x:	4x:	5x:
/pic1.jpeg	1	0	1	0.00	109.93 KB	109.93 KB	0	1	0	0	0
/favicon.ico	1	0	0	0.00	0 B	483 B	0	0	0	1	0

Viewing 1 to 2 of 2 Items

Feedback English (US)

Search here

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

ENG 9:50 PM IN 6/4/2020

Step 1: Select delivery method  
Step 2: **Create distribution**

### Create Distribution

#### Origin Settings

Origin Domain Name: 13.233.208.63

Origin Path: /my.html

Origin ID: Custom-13.233.208.63/my.html

Minimum Origin SSL Protocol:  TLSv1.2  
 TLSv1.1  
 TLSv1  
 SSLv3

Origin Protocol Policy:  HTTP Only  
 HTTPS Only  
 Match Viewer

Origin Response Timeout: 30

Origin Keep-alive Timeout: 5

HTTP Port: 80

Feedback English (US)

Search here

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

ENG 9:51 PM IN 6/4/2020

Instances | EC2 Metrics | AWS CloudFront | pic1.jpeg (864x11) | multi hybrid cloud | Session:4th june - | Untitled document | Coronavirus Outbreak | +

console.aws.amazon.com/cloudfront/home?region=ap-south-1#create-distribution:

Step 1: Select delivery method  
Step 2: Create distribution

### Default Cache Behavior Settings

Path Pattern Default (\*)

Viewer Protocol Policy  Redirect HTTP to HTTPS  HTTP and 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)

Object Caching  Use Origin Cache Headers  Customize

Feedback English (US) © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Search here

Instances | EC2 Metrics | AWS CloudFront | pic1.jpeg (864x11) | multi hybrid cloud | Session:4th june - | Untitled document | Coronavirus Outbreak | +

console.aws.amazon.com/cloudfront/home?region=ap-south-1#create-distribution:

Step 1: Select delivery method  
Step 2: Create distribution

Logging  Off  On

Bucket for Logs

Log Prefix

Cookie Logging  Off  On

Enable IPv6

Comment

Distribution State  Enabled  Disabled

 com.amazonaws.services.cloudfront.model.InvalidArgumentException: The parameter origin name cannot be an IP address. (Service: AmazonCloudFront; Status Code: 400; Error Code: InvalidArgument; Request ID: 6af58222-6f4f-4826-9de5-b544fc8c35d0; Proxy: null)

Cancel Back Create Distribution

Feedback English (US) © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Search here

ENG 9:51 PM IN 6/4/2020 [13]

Screenshot of the AWS CloudFront 'Create Distribution' wizard, Step 2: Create distribution.

**Step 1: Select delivery method**

**Step 2: Create distribution**

### Origin Settings

Origin Domain Name: ec2-13-233-208-63.ap-south-1.compute.amazonaws.com

Origin Path: /my.html

Origin ID: Custom-13.233.208.63/my.html

Minimum Origin SSL Protocol: TLSv1.2 (radio button)

Origin Protocol Policy: HTTP Only (radio button)

Origin Response Timeout: 30

Origin Keep-alive Timeout: 5

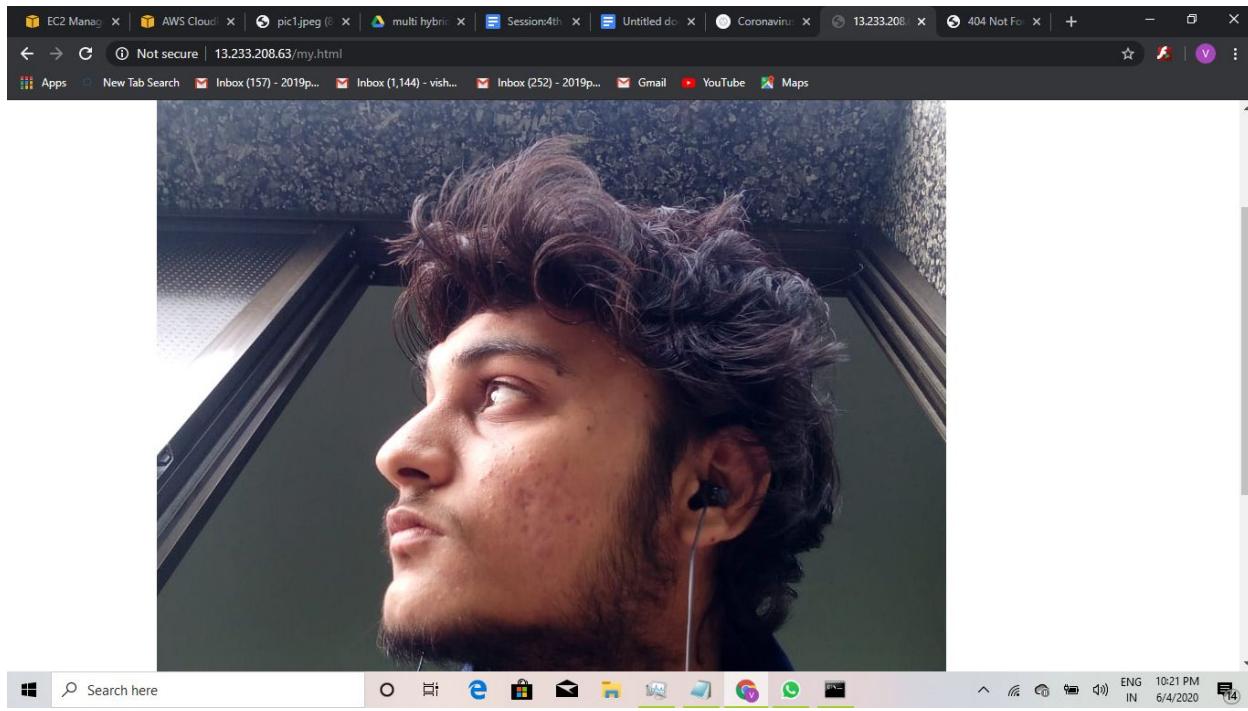
HTTP Port: 80

Feedback English (US) Privacy Policy Terms of Use

Not secure | 13.233.208.63/my.html

welcome to my website





```
C:\Users\user>cd Downloads
```

```
C:\Users\user\Downloads>ssh -l ec2-user 13.233.208.63 -i mykey1111.pem
Last login: Thu Jun 4 16:24:33 2020 from 157.37.235.116
```

```
_)_ _| )
_| ( / Amazon Linux 2 AMI
__\|_|_||
```

```
https://aws.amazon.com/amazon-linux-2/
4 package(s) needed for security, out of 8 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-43-66 ~]$ sudo su - root
Last login: Thu Jun 4 16:24:45 UTC 2020 on pts/2
[root@ip-172-31-43-66 ~]# cd var/www/htmkl
-bash: cd: var/www/htmkl: No such file or directory
[root@ip-172-31-43-66 ~]# cd var/www/html
-bash: cd: var/www/html: No such file or directory
[root@ip-172-31-43-66 ~]# systemctl start httpd
[root@ip-172-31-43-66 ~]# cd var/www/html
-bash: cd: var/www/html: No such file or directory
[root@ip-172-31-43-66 ~]# pwd
/root
[root@ip-172-31-43-66 ~]# cd /var/www/html
[root@ip-172-31-43-66 html]# ls
```

my.html

```
[root@ip-172-31-43-66 html]# cat my.html
welcome to my website
```



```
[root@ip-172-31-43-66 html]# systemctl status httpd
```

- httpd.service - The Apache HTTP Server

```
  Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
```

```
  Active: active (running) since Thu 2020-06-04 16:29:10 UTC; 16min ago
```

```
    Docs: man:httpd.service(8)
```

```
 Main PID: 29949 (httpd)
```

```
 Status: "Total requests: 12; Idle/Busy workers 83/16;Requests/sec: 0.0125; Bytes served/sec: 11 B/sec"
```

```
 CGroup: /system.slice/httpd.service
```

```
 └─29949 /usr/sbin/httpd -DFOREGROUND
   ├─29950 /usr/sbin/httpd -DFOREGROUND
   ├─29951 /usr/sbin/httpd -DFOREGROUND
   ├─29952 /usr/sbin/httpd -DFOREGROUND
   ├─29953 /usr/sbin/httpd -DFOREGROUND
   ├─29954 /usr/sbin/httpd -DFOREGROUND
   └─30018 /usr/sbin/httpd -DFOREGROUND
```

Jun 04 16:29:10 ip-172-31-43-66.ap-south-1.compute.internal systemd[1]: Starting The Apache HTTP Server...

Jun 04 16:29:10 ip-172-31-43-66.ap-south-1.compute.internal systemd[1]: Started The Apache HTTP Server.

```
[root@ip-172-31-43-66 html]# vi my.html
```

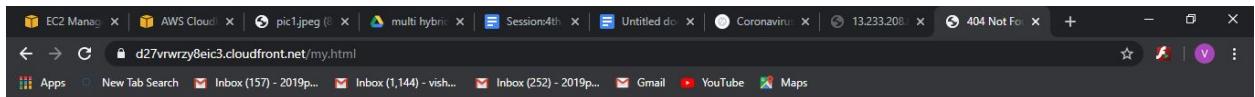
```
[root@ip-172-31-43-66 html]# vi my.html
```

```
[root@ip-172-31-43-66 html]# cat my.html
```

```
welcome to my website
```



```
[root@ip-172-31-43-66 html]#
```



## Not Found

The requested URL was not found on this server.

