

Project 3

Scenario

Your company wants to distribute their content in the form of a website to their global offices. However, due to some legal restrictions, you cannot distribute the content in France and Australia. You need to find a way to prevent these offices from accessing the data.

The content does not change very often; however, some of the files are very large, and you have to find a solution to minimize end user latency.

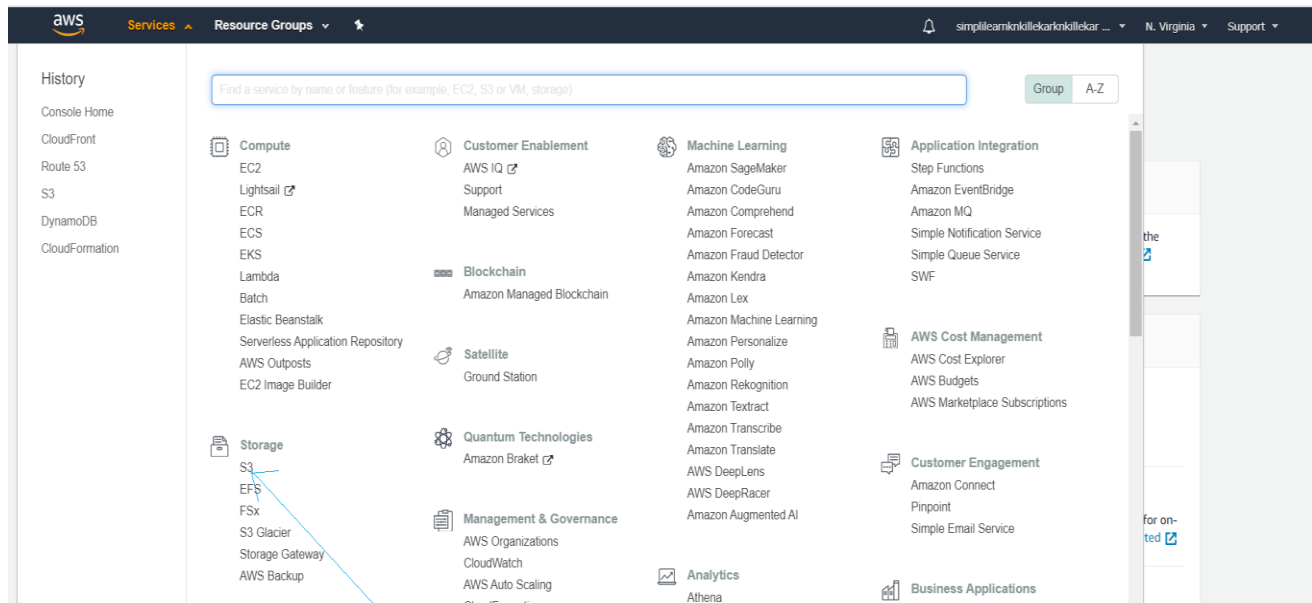
The last requirement is that the audit department wants to track whoever is accessing the website.

Goals of the project

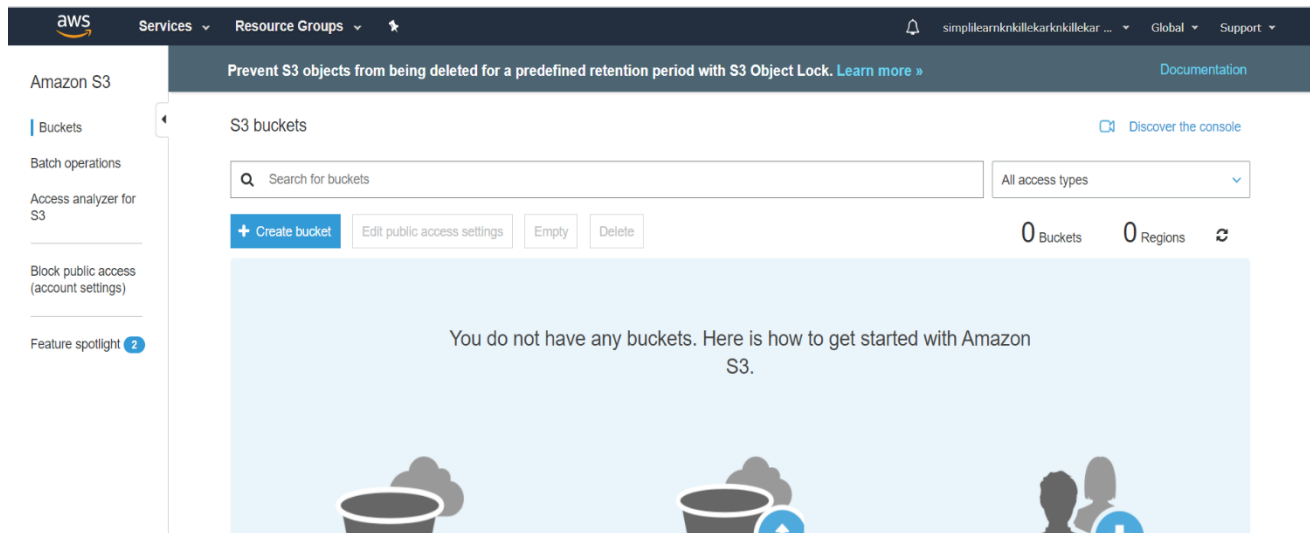
- Set up a static website using Amazon S3.
 1. Create a bucket and enable static website hosting.
 2. Enable logging.
- Set up a CloudFront distribution for the static website with Access Logs enabled.
- Set up Geo Restrictions to prevent users in France and Australia from accessing the data.
- Verify that logging is working.

Solution:

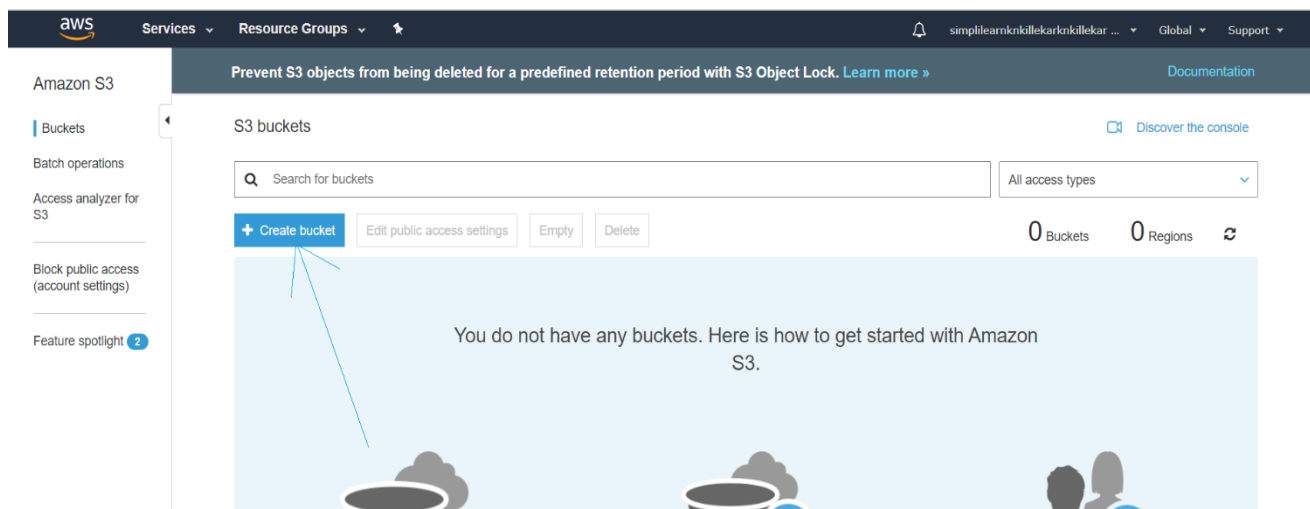
Step 1: Open AWS management console, click on Services. Go to storage section and click on S3 as shown in window below.



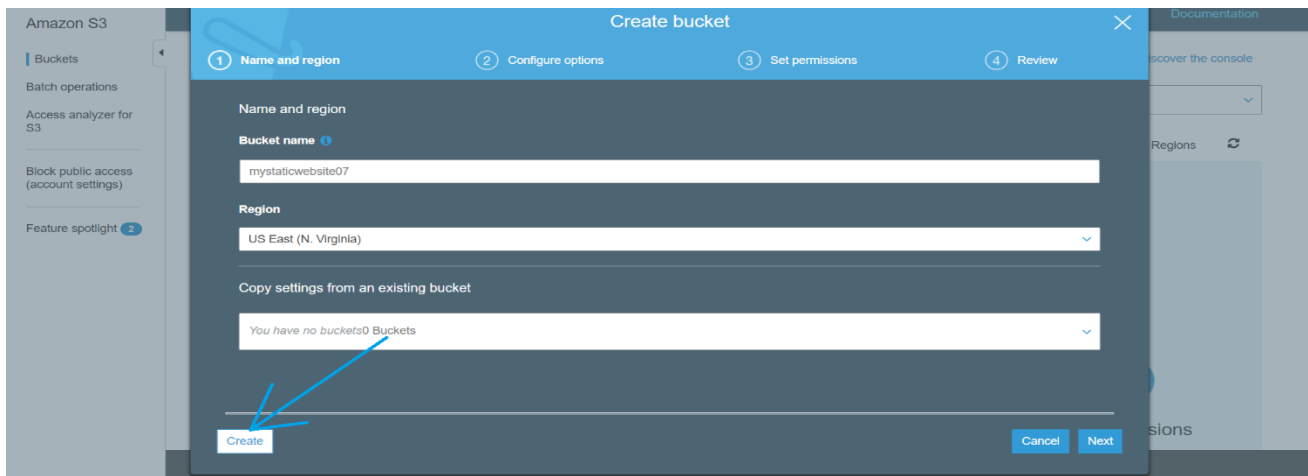
The following window will appear after clicking on S3.



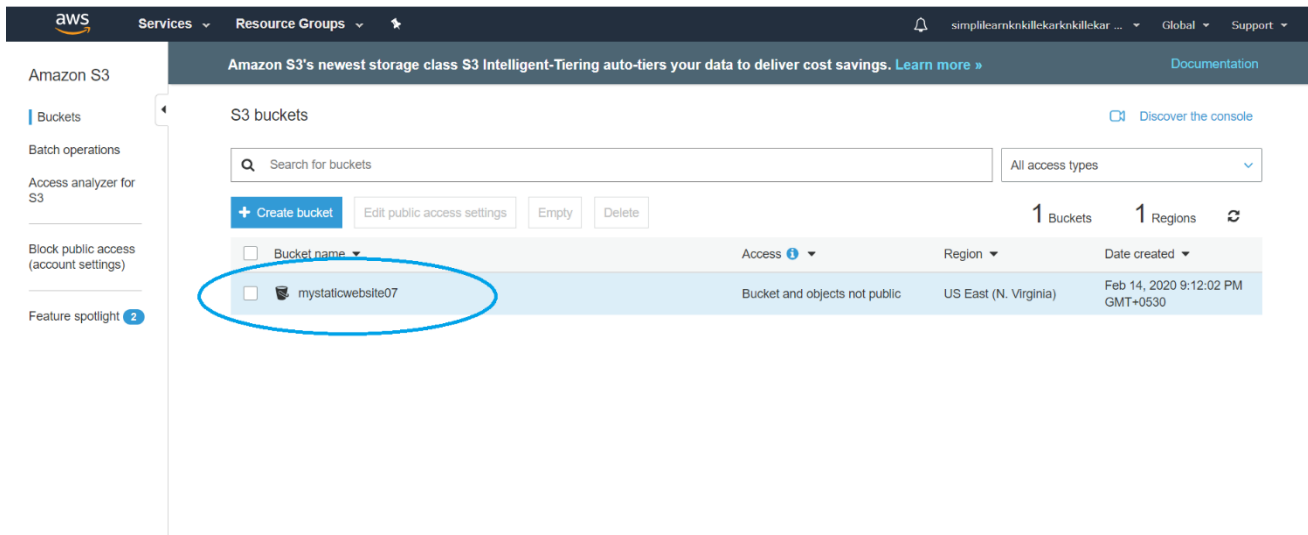
Step 2: Now click on **Create bucket** to create the bucket as shown below.



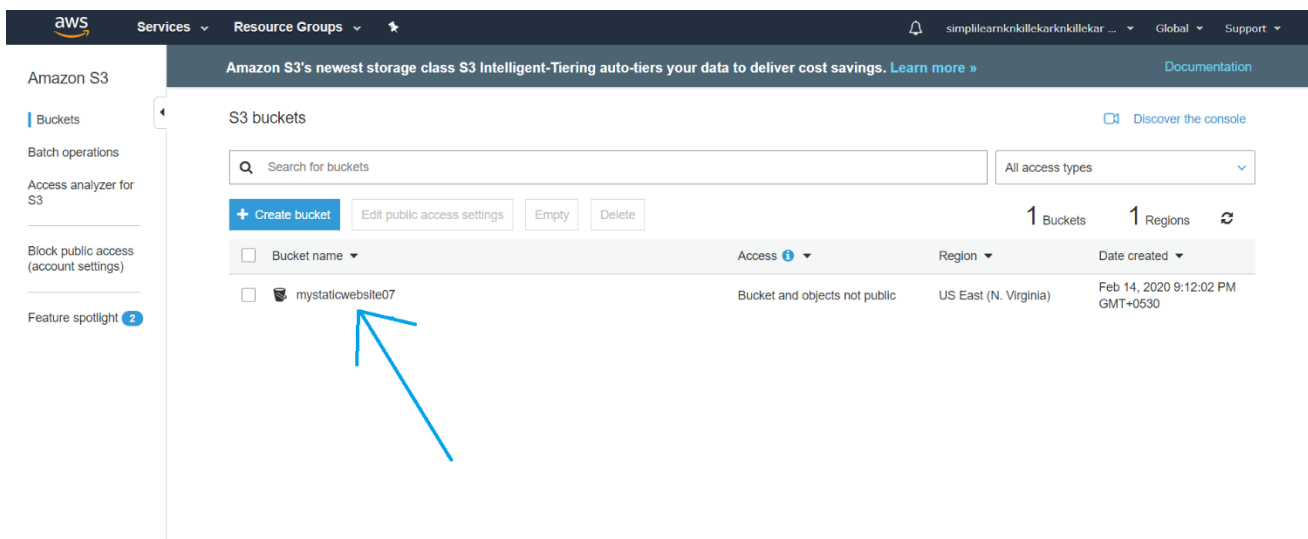
Click on Create bucket the following window will appear and enter the details as shown in the window below. The bucket name is **“mystaticwebsite07”** and region as **“US East(North Virginia)”**. After entering the details click on **Create** option as shown below.



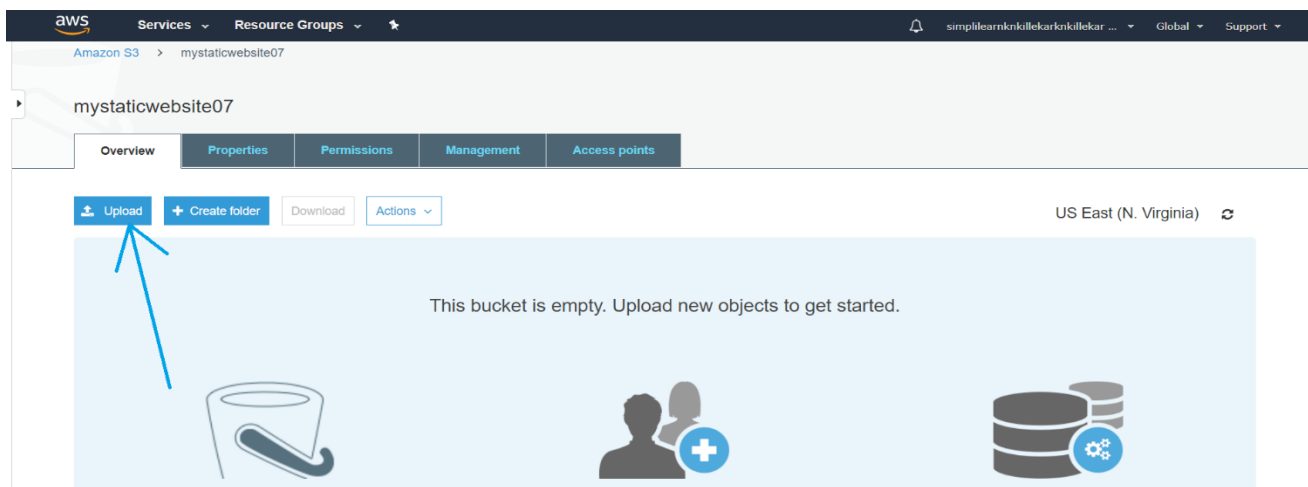
The bucket “mystaticwebsite07” is created successfully as shown in the window below.



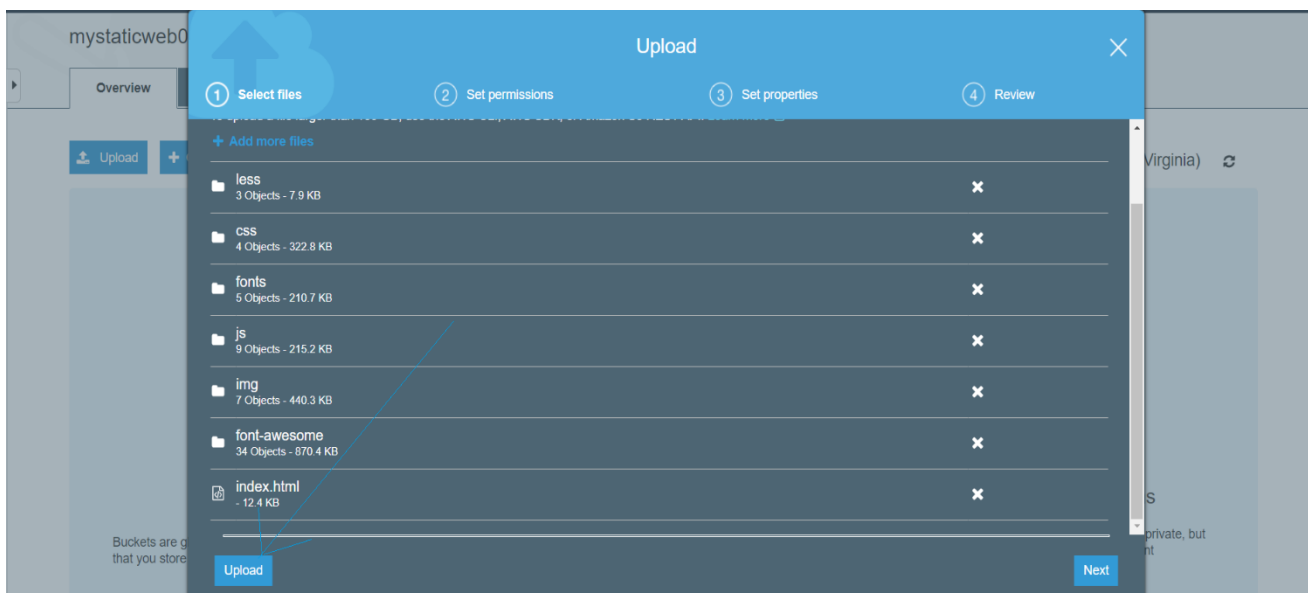
Step 3: To upload the static website files, click on the bucket name “mystaticwebsite07” as shown in the window below.



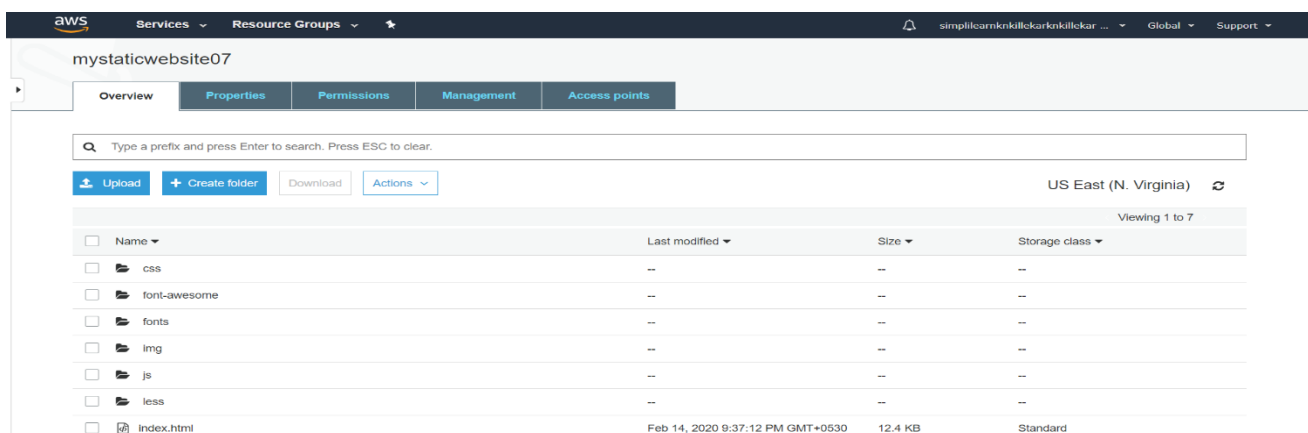
The following window will appear and select the upload option as shown below.



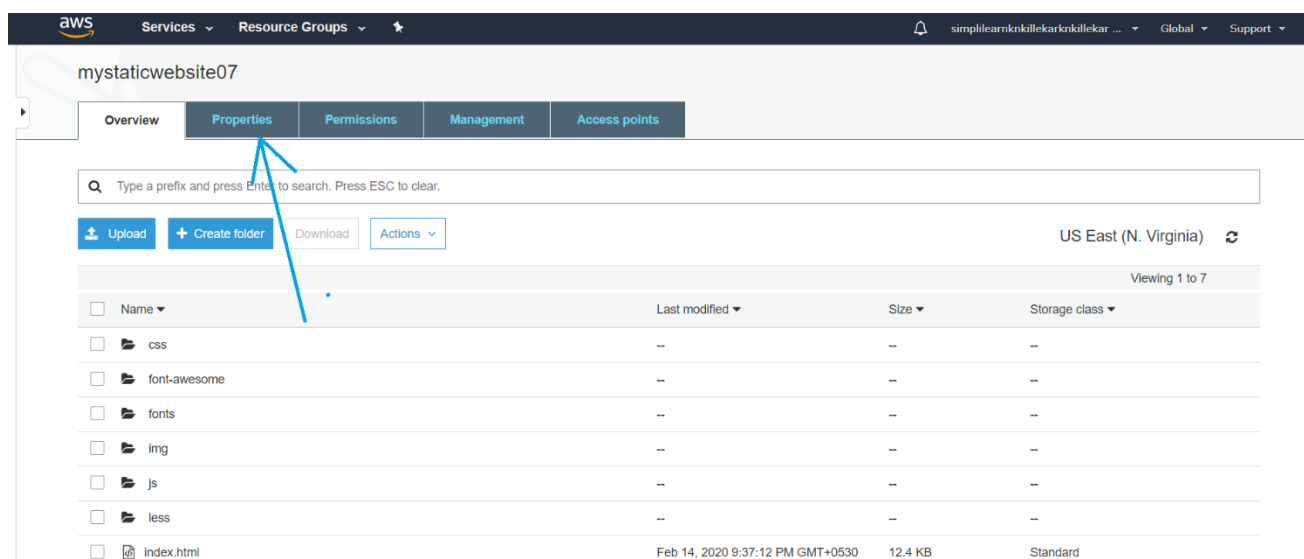
A window will appear as shown below and click on “Add files” or “Drag & Drop” the static website files from the local drive to the bucket created in last step. The following window will appear after adding files as shown below and click on “Upload” option.



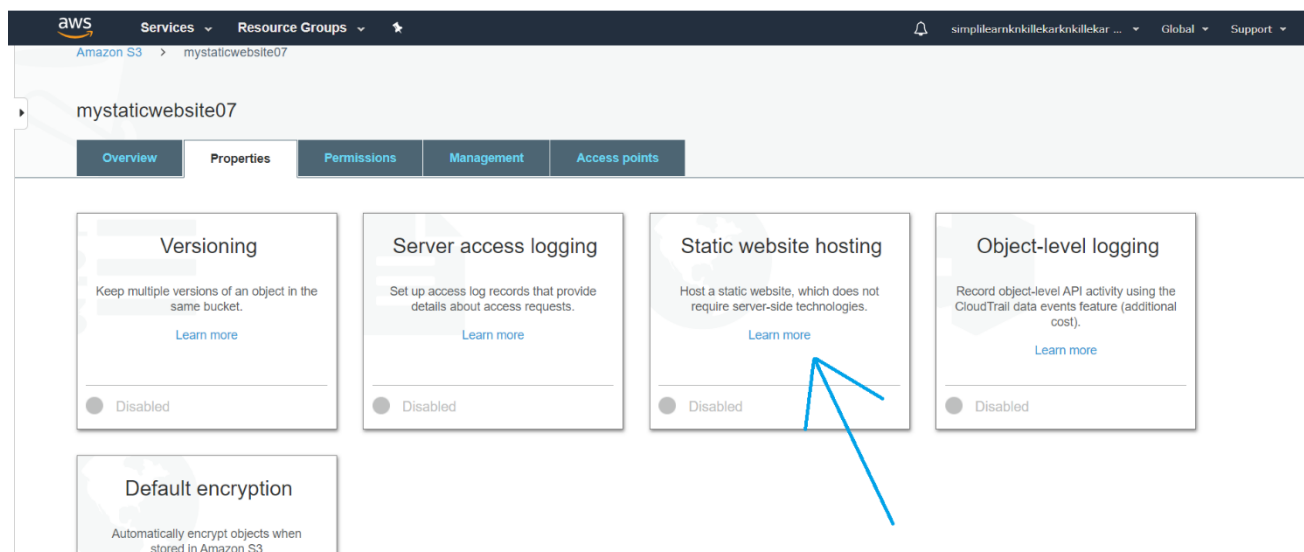
It will take couple of minutes to upload the files in the bucket. After the successful upload, the following window will display.



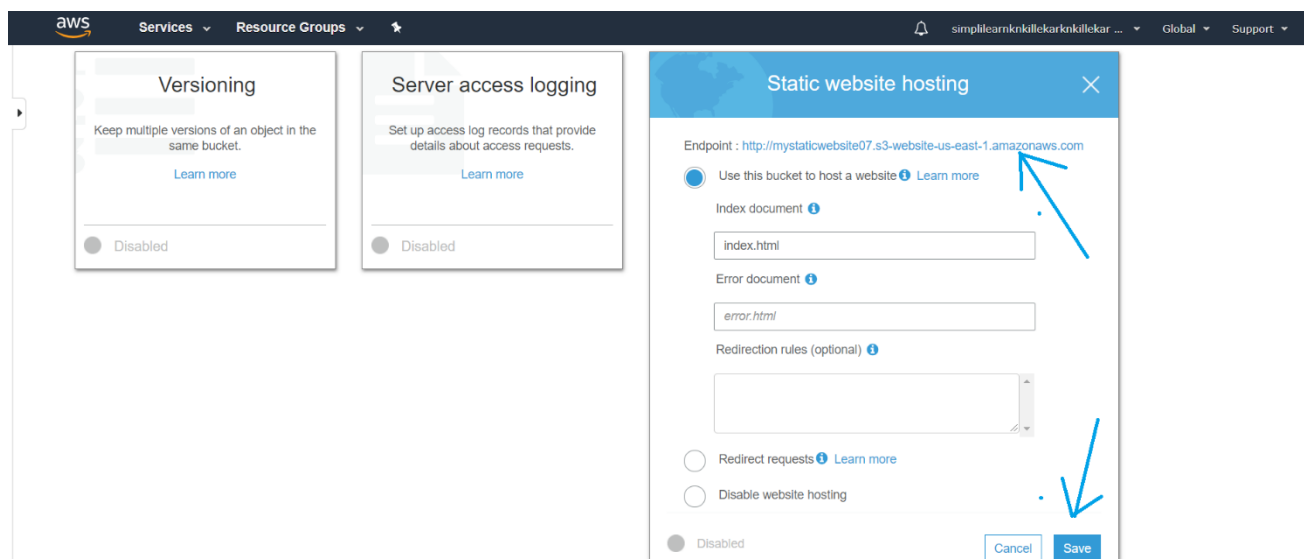
Step 4: To enable the static website hosting, click on the **“Properties”** tab as shown in the window below.



Click on **“Properties”** tab, a window will appear as shown below and select **“Static website hosting”** option as shown below.



Now click on “Static website hosting” select “Use this bucket to host a website” option and enter the following details and copy the Endpoint as shown in the window below and click on “Save” option.

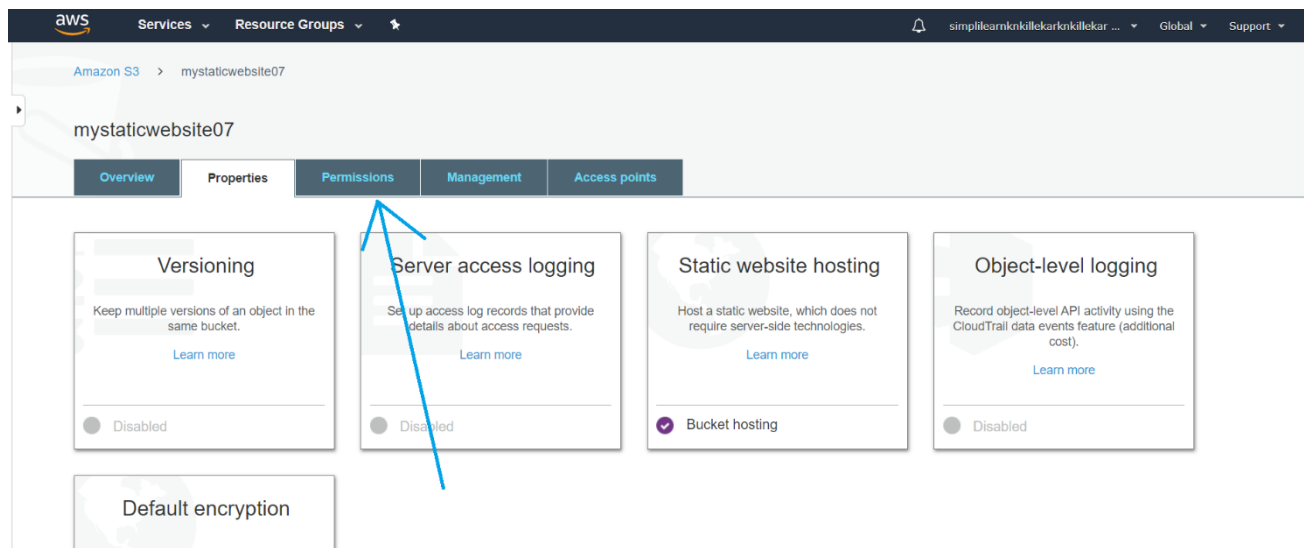


The screenshot shows the AWS Management Console interface for configuring static website hosting. The main window is titled "Static website hosting" and contains the following fields and options:

- Endpoint:** `http://mystaticwebsite07.s3-website-us-east-1.amazonaws.com` (indicated by a blue arrow).
- Use this bucket to host a website:** Selected (indicated by a blue arrow).
- Index document:** `index.html`
- Error document:** `error.html`
- Redirection rules (optional):** (Empty text area)
- Redirect requests:** Unselected
- Disable website hosting:** Unselected
- Buttons:** "Cancel" and "Save" (indicated by a blue arrow).

On the left side of the console, there are two other configuration cards: "Versioning" and "Server access logging", both currently set to "Disabled".

Step 5: Now go to “Permissions” tab to set the permission to access the website as shown below.



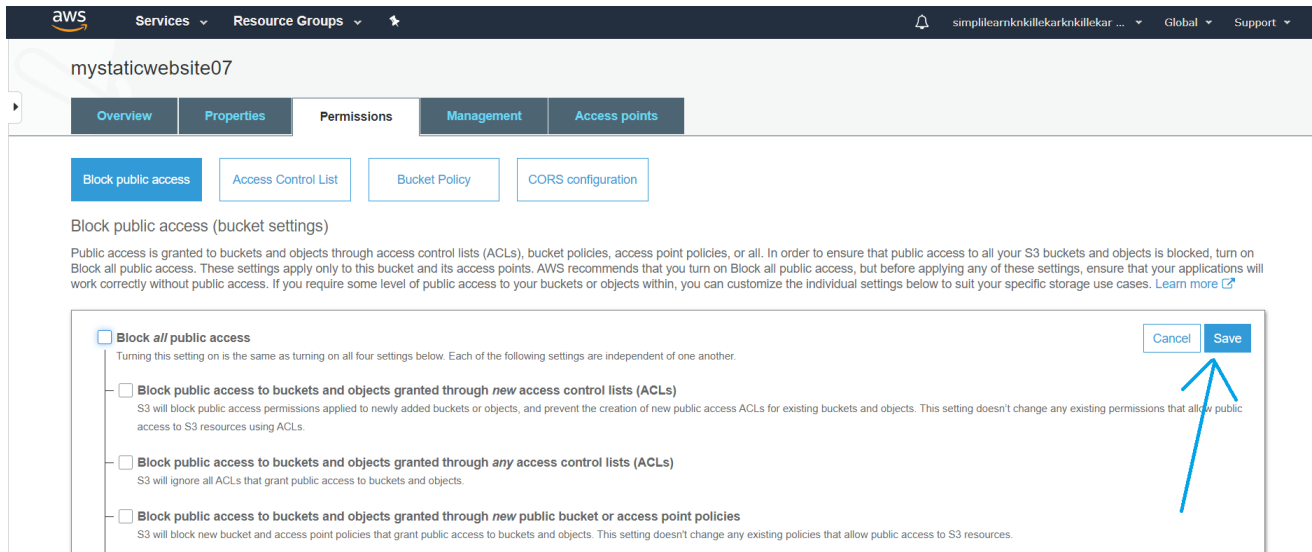
The screenshot shows the AWS Management Console interface for the S3 bucket "mystaticwebsite07". The "Permissions" tab is selected, and the "Static website hosting" card is highlighted with a blue arrow. The "Static website hosting" card shows the "Bucket hosting" option selected with a checkmark. Other tabs visible include "Overview", "Properties", "Management", and "Access points".

Below the tabs, there are four configuration cards:

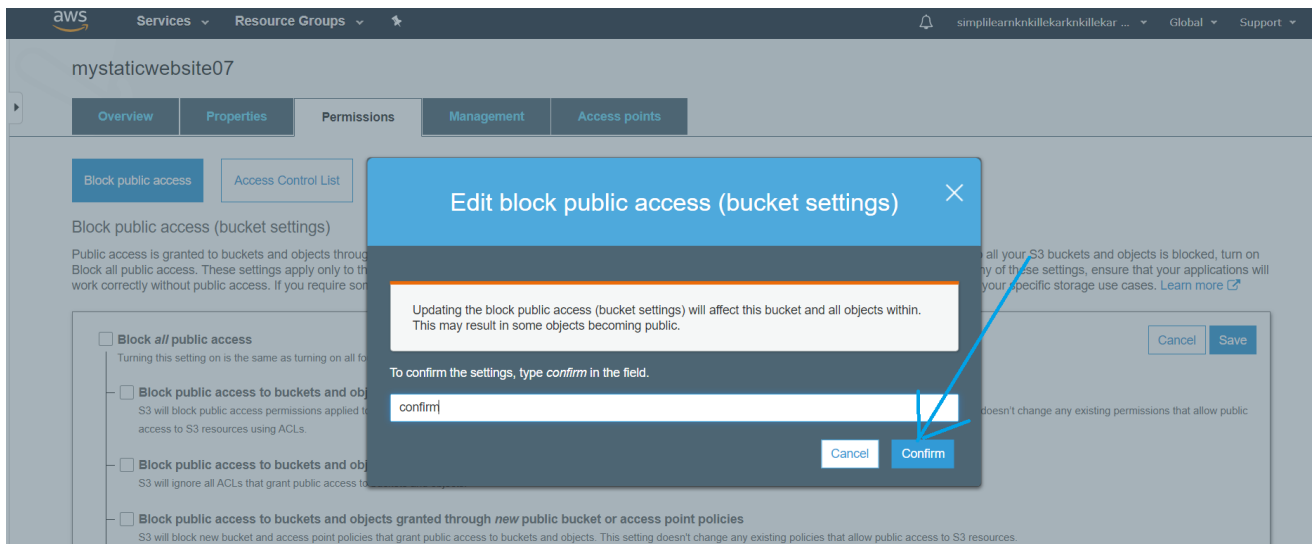
- Versioning:** Disabled
- Server access logging:** Disabled (indicated by a blue arrow)
- Static website hosting:** Bucket hosting (Selected)
- Object-level logging:** Disabled

At the bottom, there is a "Default encryption" card.

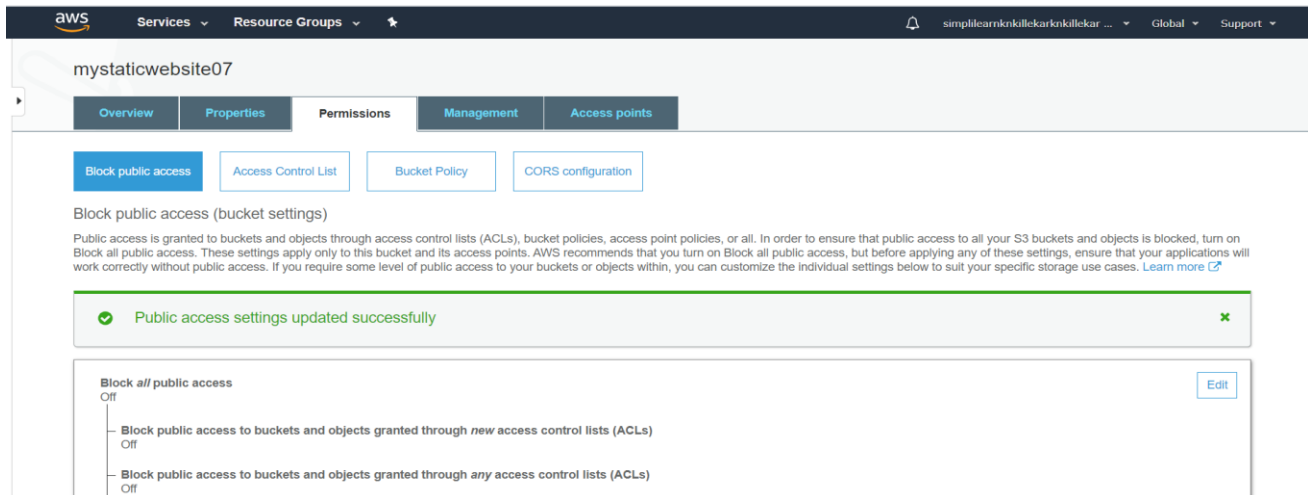
After selecting Permission tab go to “**Block public access**” option and click on “**Edit**” option as shown below. Uncheck the “Block all public access” option and click on “**Save**” option.



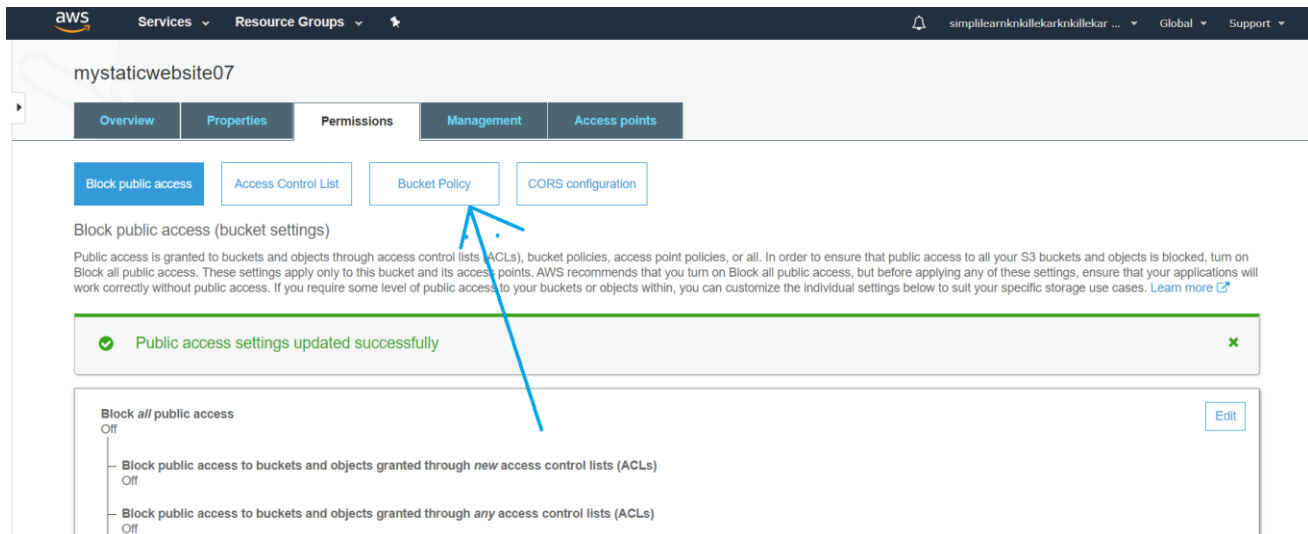
After saving, a window will appear and type “confirm” in the field and click on confirm as shown in the window below.



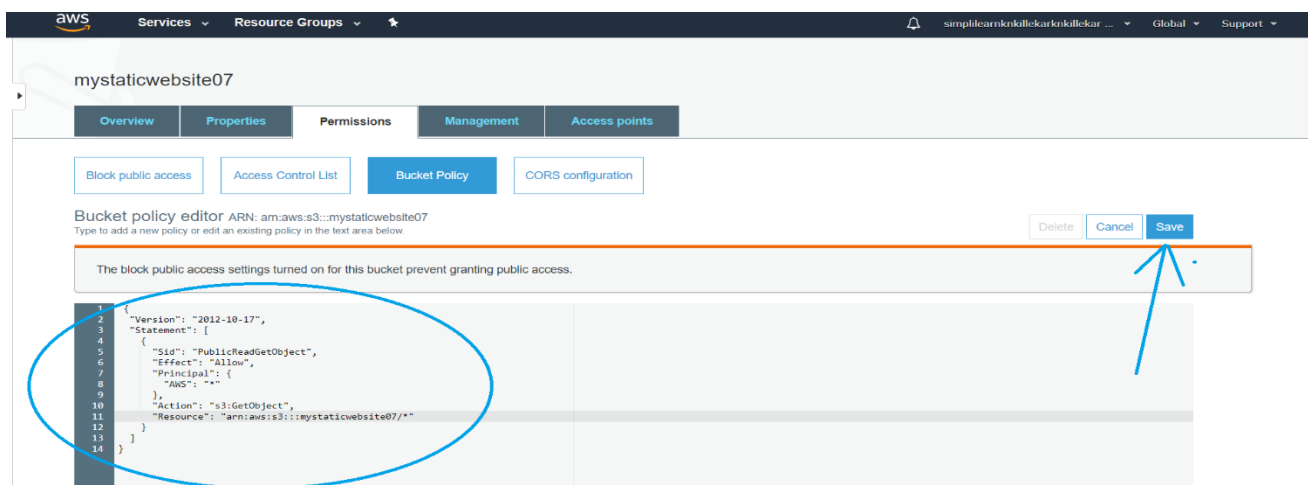
A window will appear with the message **“Public access settings updated successfully”** as shown below.



Step 6: Next, go to “Bucket Policy” tab as shown below.



Write the Bucket policy as shown in the window below and click on “Save” option.



Now the bucket has the public access as shown in the window below.

aws Services Resource Groups

mystaticwebsite07

Overview Properties Permissions Management Access points

Block public access Access Control List Bucket Policy Public CORS configuration

This bucket has public access
You have provided public access to this bucket. We highly recommend that you never grant any kind of public access to your S3 bucket.

Bucket policy editor ARN: am:aws:s3::mystaticwebsite07
Type to add a new policy or edit an existing policy in the text area below. [Delete] [Cancel] [Save]

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

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "PublicReadGetObject",
6       "Effect": "Allow",
7       "Principal": {
8         "AWS": "*"
9       },
10      "Action": "s3:GetObject",
11      "Resource": "arn:aws:s3::mystaticwebsite07/*"
12    }
13  ]
14 }
```

Next, enter the copied Endpoint in the browser as shown below and test whether website is working or no.

← → ↻ http://mystaticwebsite07.s3-website-us-east-1.amazonaws.com

Apps TF-Idf and Cosine si... Building a Simple C... Build a Simple Chat... 101: Pre-processing... 5 Minute ML: Chatb... Creating a ChatBot... How To Develop a... Ultimate Guide to L... pomegranate plant...

Google Learning on SI... Inbox prexam.vtu.ac...

The following window shows that static website is hosted successfully in S3.

← → ↻ Not secure | mystaticwebsite07.s3-website-us-east-1.amazonaws.com

Apps TF-Idf and Cosine si... Building a Simple C... Build a Simple Chat... 101: Pre-processing... 5 Minute ML: Chatb... Creating a ChatBot... How To Develop a... Ultimate Guide to L... pomegranate plant...

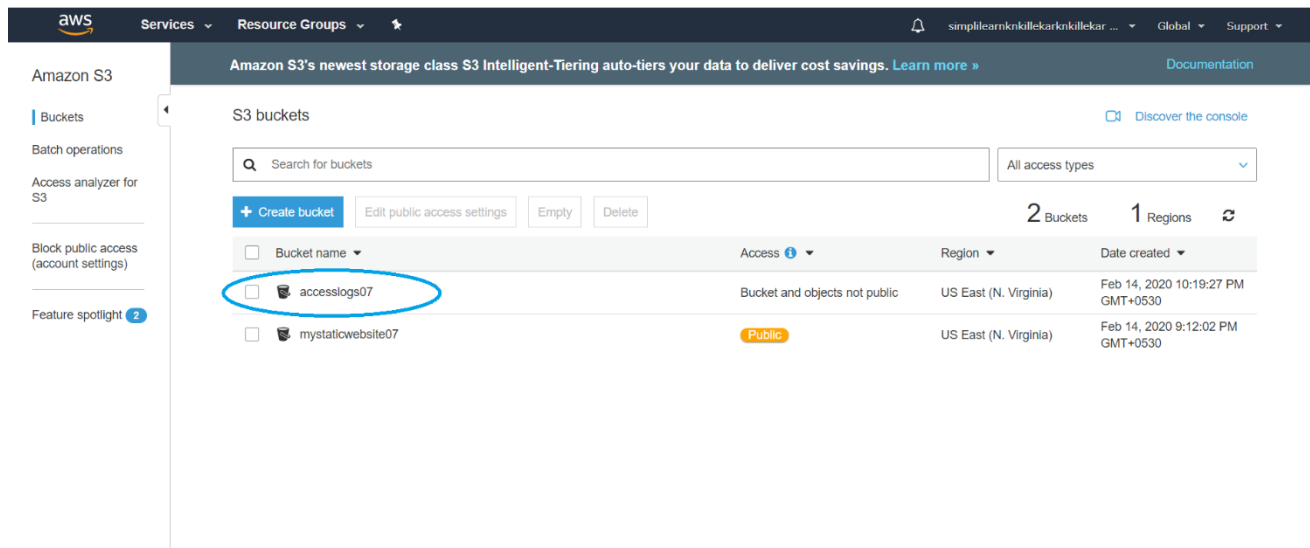
START BOOTSTRAP ABOUT SERVICES PORTFOLIO CONTACT

YOUR FAVORITE SOURCE OF FREE BOOTSTRAP THEMES

Start Bootstrap can help you build better websites using the Bootstrap CSS framework! Just download your template and start going, no strings attached!

FIND OUT MORE

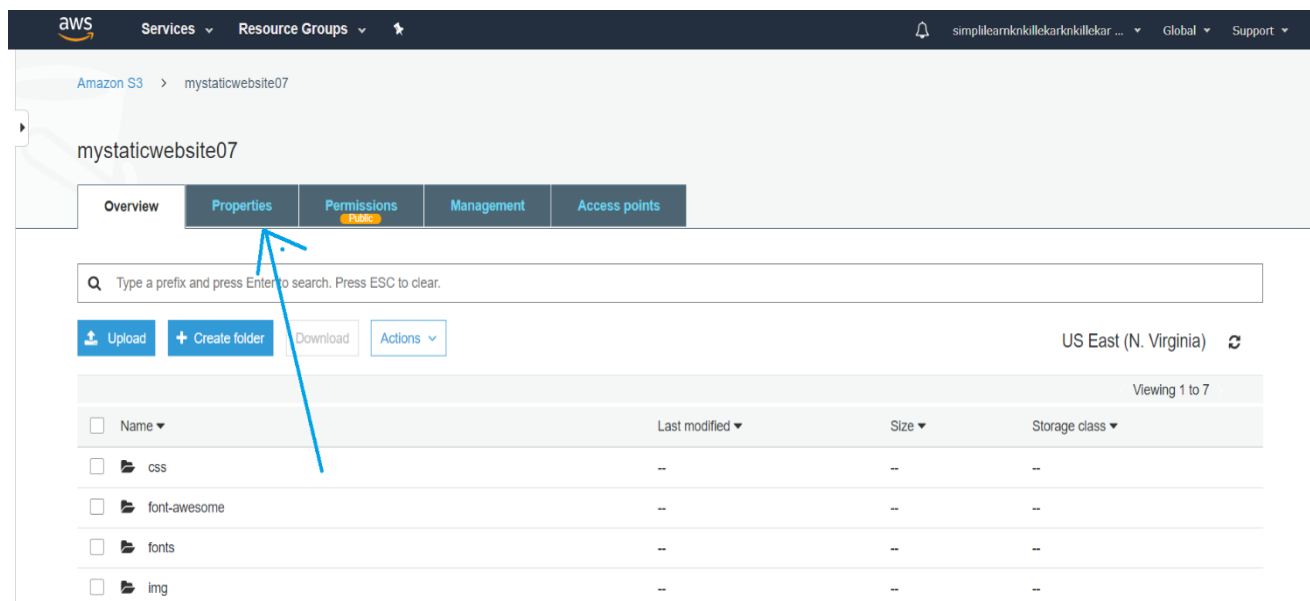
Step 7: Now create one more bucket by the name “**accesslogs07**” in the same **region** to store the server access log files. Repeat the same steps to create the bucket. The “**accesslogs07**” bucket is created as shown in window below.



The screenshot shows the AWS S3 console interface. On the left sidebar, the 'Buckets' section is selected. The main area displays a list of S3 buckets. The bucket 'accesslogs07' is highlighted with a blue circle. The table shows the following data:

Bucket name	Access	Region	Date created
accesslogs07	Bucket and objects not public	US East (N. Virginia)	Feb 14, 2020 10:19:27 PM GMT+0530
mystaticwebsite07	Public	US East (N. Virginia)	Feb 14, 2020 9:12:02 PM GMT+0530

Step 8: Now click on “**mystaticwebsite07**” bucket and select “**Properties**” option as shown in window below.



The screenshot shows the AWS S3 console interface for the 'mystaticwebsite07' bucket. The 'Properties' tab is selected, and a blue arrow points to it. The main area displays the bucket's contents, including a search bar and a list of objects.

Amazon S3 > mystaticwebsite07

mystaticwebsite07

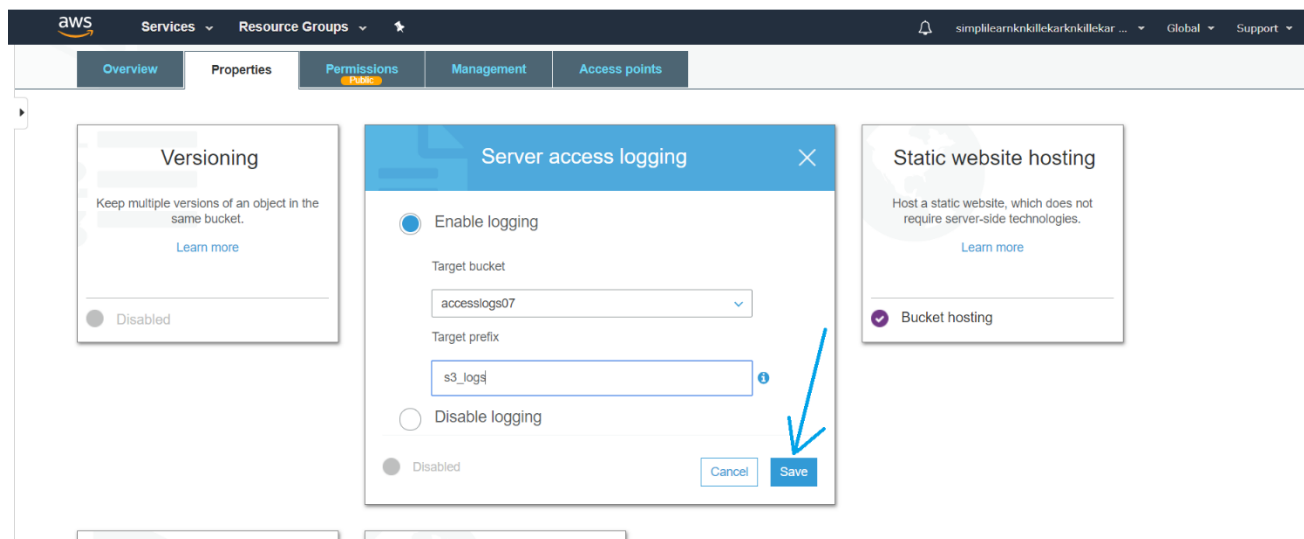
Overview Properties Permissions Management Access points

US East (N. Virginia)

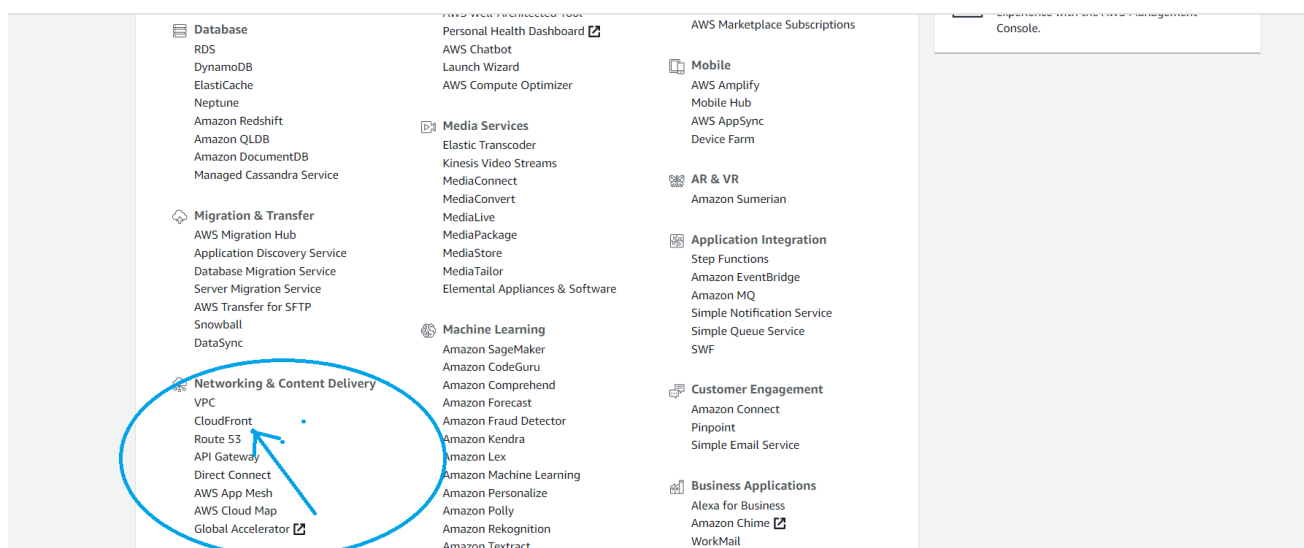
Viewing 1 to 7

Name	Last modified	Size	Storage class
css	--	--	--
font-awesome	--	--	--
fonts	--	--	--
img	--	--	--

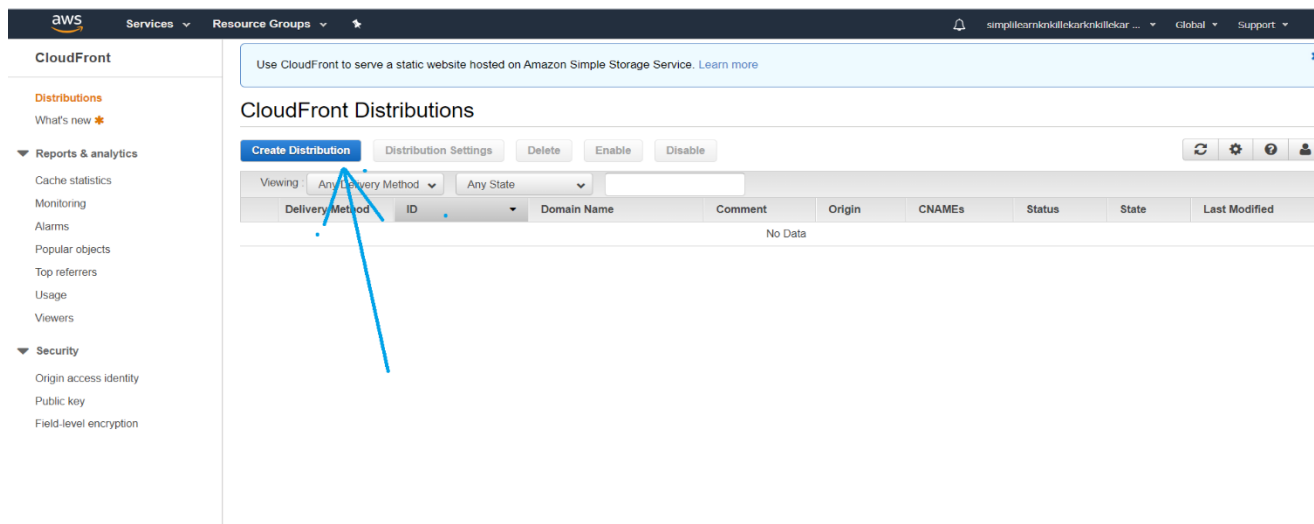
Click on “Properties” option and click on “Server access logging” option and select “Enable Logging” option. Select the target bucket as “accesslogs07” and enter target prefix as “s3_logs” shown in window below and click on “Save” option.



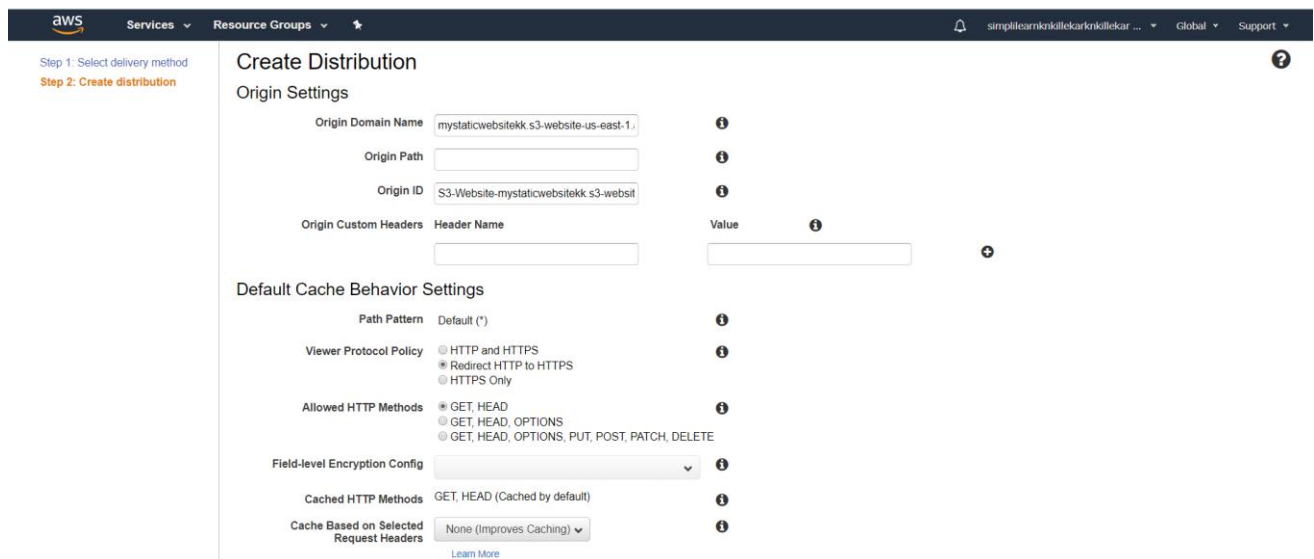
Step 9: Now to minimize the user end latency, I will host the static website using “Cloudfront” service with access logs enabled. To do this, go to AWS management console and select “CloudFront” from **Networking & Content Delivery** section as shown in window below.



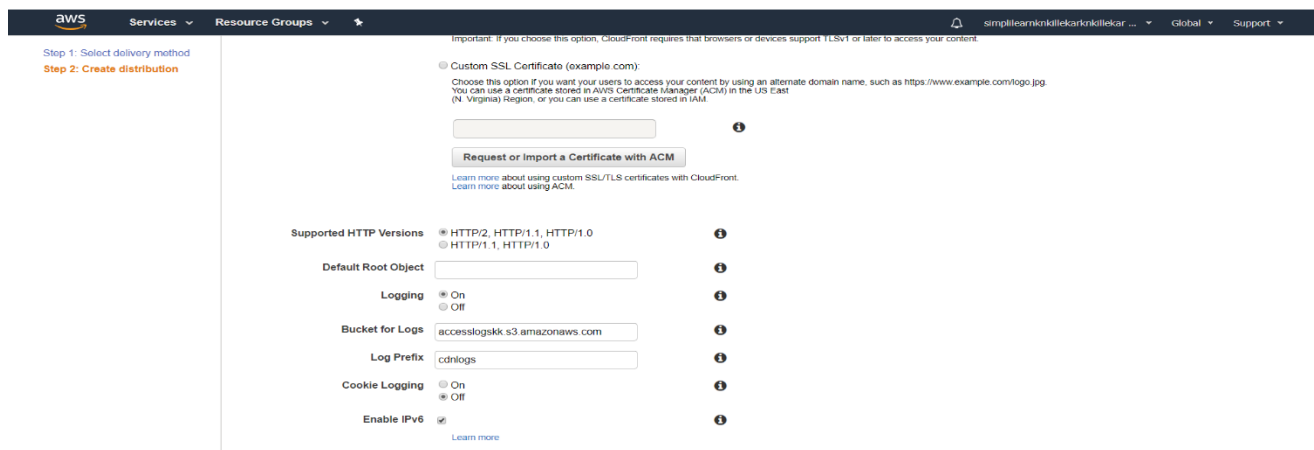
Following window will appear as shown below.



Now click on “Create Distribution” and click “Get started” option in web section. Fill the details as shown in window below.



Select “Logging” to **on** and choose bucket for logs as “accesslogsk.s3.amazonaws.com” and enter the log prefix as “cdnlogs as shown in window below.



Next click on “Create Distribution” as shown in window below.

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

Logging ☒ On
☐ Off

Bucket for Logs

Log Prefix

Cookie Logging ☐ On
☒ Off

Enable IPv6 ☒ [Learn more](#)

Comment

Distribution State ☒ Enabled
☐ Disabled

[Cancel](#) [Back](#) [Create Distribution](#)

Step 10: Now select the created distribution and click on distribution settings as shown in window below.

CloudFront

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

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 checked="" type="checkbox"/> Web	E2VZDM5OSH3E9	d1f8r4c3u28sf.cloudfront.net	-	mystaticwebsite	-	In Progress	Enabled	2020-02-14 23:10 UTC+5

Now go to restrictions tab select “Geo Restriction” and click on edit as shown in window below.

CloudFront Distributions > E2VZDM5OSH3E9

[General](#) [Origins and Origin Groups](#) [Behaviors](#) [Error Pages](#) [Restrictions](#) [Invalidations](#) [Tags](#)

[Edit](#)

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](#).

Restriction	Status	Type
<input checked="" type="checkbox"/> Geo Restriction	Disabled	-

Next enable geo restriction to **yes** and select **blacklist** option. Add Australia and France to blacklist as shown in window below and click on “Yes, edit” option.

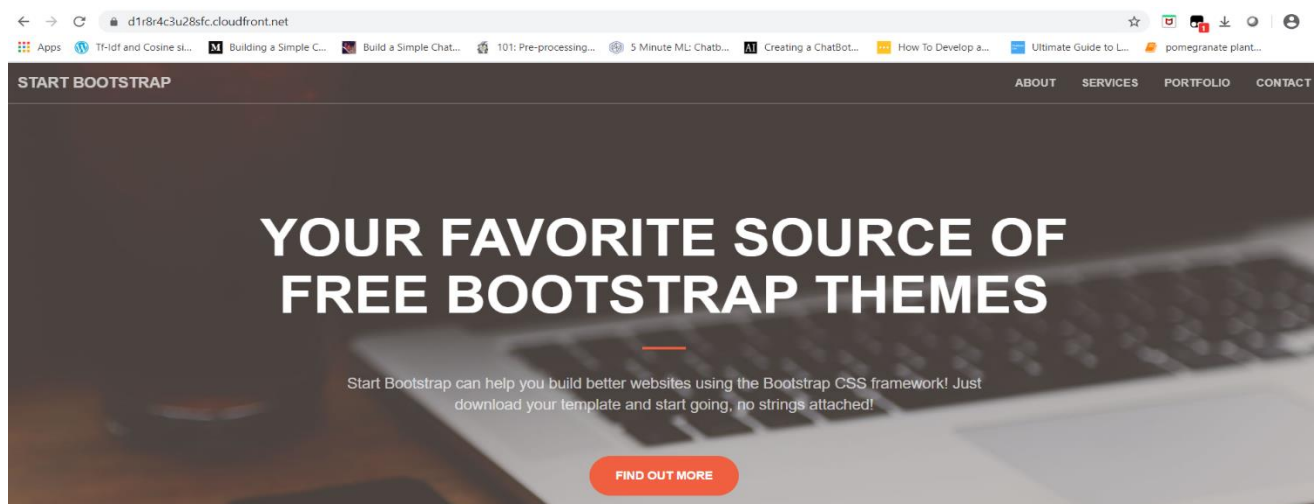
The screenshot shows the 'Edit Geo-Restrictions' page in the AWS IAM console. The 'Enable Geo-Restriction' is set to 'Yes', 'Restriction Type' is 'Blacklist', and 'Countries' includes 'FR -- FRANCE' and 'AU -- AUSTRALIA'. A blue arrow points to the 'Yes, Edit' button.

Step 11: Now copy the domain name as shown below and enter it in browser to test the website.

The screenshot shows the 'CloudFront Distributions' page in the AWS console. The table lists one distribution with the domain name 'd1r8r4c3u28sfc.cloudfront.net' circled in the 'Domain Name' column.

Delivery Method	ID	Domain Name	Comment	Origin	CNAMEs	Status	State	Last Modified
Web	EZVZDM5OSHK3E9	d1r8r4c3u28sfc.cloudfront.net	-	mysticwebsite	-	In Progress	Enabled	2020-02-14 23:21 UTC+5

The static website is successfully hosted using cloudfront as shown in window below.



Step 12: The access log files are stored in **accesslogskk** bucket in the folder cdnlogs as shown in window below.

The screenshot displays the AWS S3 console interface. At the top, the navigation bar shows 'aws', 'Services', and 'Resource Groups'. The breadcrumb trail indicates the path: 'Amazon S3 > accesslogskk > cdnlogs'. The bucket name 'accesslogskk' is prominently displayed, with an 'Overview' tab selected. Below the bucket name, there is a search bar and a toolbar with buttons for 'Upload', 'Create folder', 'Download', and 'Actions'. The region 'US East (N. Virginia)' is noted. A table lists the contents of the bucket, with columns for 'Name', 'Last modified', 'Size', and 'Storage class'. A single file is listed: 'E2VZDM5OSHK3E9.2020-02-14-17.41776db9.gz', which is circled in blue. The file's details are: Last modified 'Feb 14, 2020 11:25:25 PM GMT+0530', Size '2.2 KB', and Storage class 'Standard'. The interface also shows 'Viewing 1 to 1' at the bottom right of the table.

Name	Last modified	Size	Storage class
E2VZDM5OSHK3E9.2020-02-14-17.41776db9.gz	Feb 14, 2020 11:25:25 PM GMT+0530	2.2 KB	Standard