Project Documentation

Project Title: AWS Static Website Architecture with Security & Performance Optimization

---

Objective

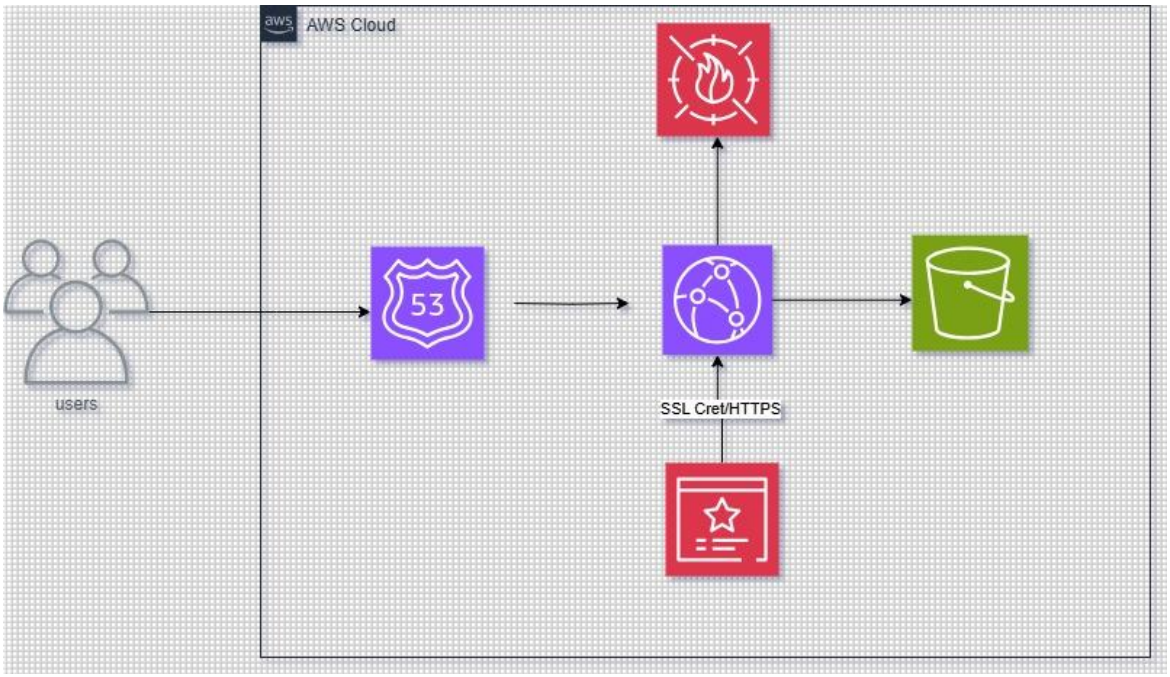
To design and deploy a secure, scalable, and high-performing static website hosted on Amazon S3, integrated with CloudFront for content delivery, AWS WAF for threat protection, and Route 53 for domain-level DNS routing. The architecture also ensures HTTPS encryption via AWS Certificate Manager (ACM), delivering a professional-grade solution for static content hosting.

Architecture Overview

Services Used:

- **Amazon S3** (Static Website Hosting)
- **Amazon CloudFront** (Global Content Delivery Network)
- **AWS WAF** (Web Application Firewall)
- **Amazon Route 53** (DNS Service)
- **AWS Certificate Manager (ACM)** (SSL/TLS Management)

Architecture Flow



Security Measures

- **AWS WAF** is attached to CloudFront to block common web exploits (e.g., SQL injection, XSS).
- **S3 Bucket** is configured with public access blocked. Only CloudFront is allowed using Origin Access Control (OAC).
- **HTTPS enabled** using a validated SSL certificate from **ACM** to ensure encrypted data transmission.

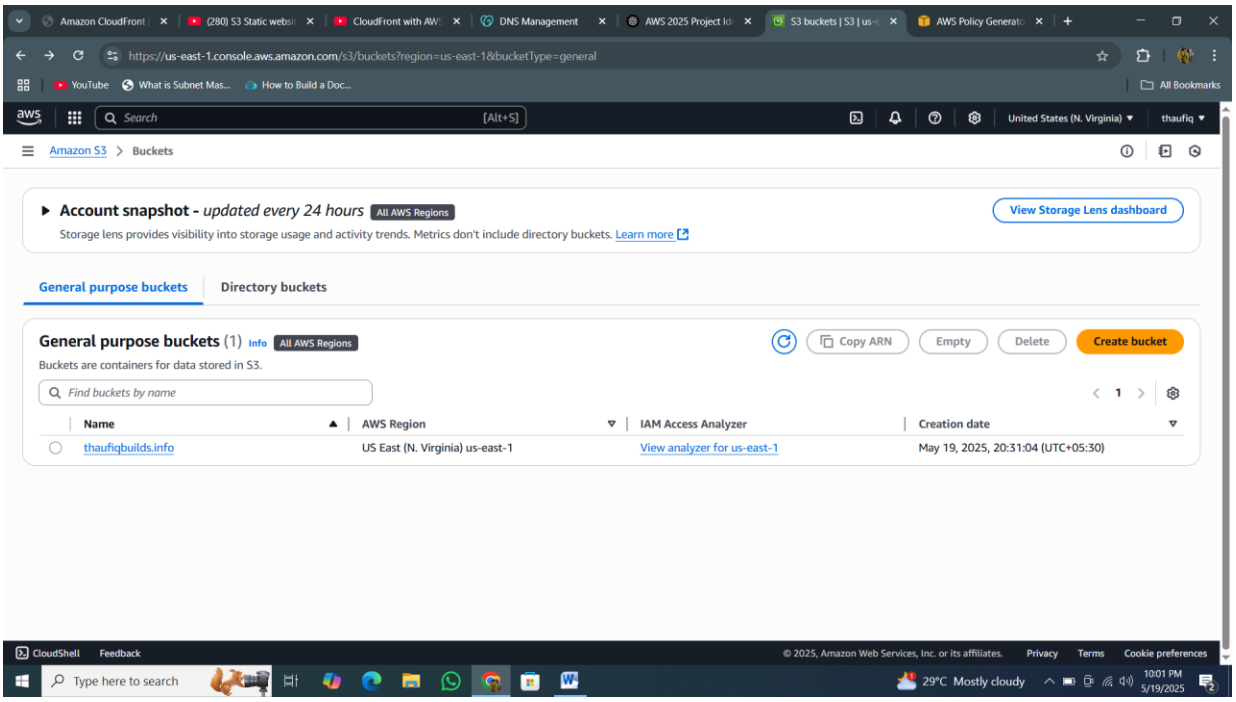
Performance Optimizations

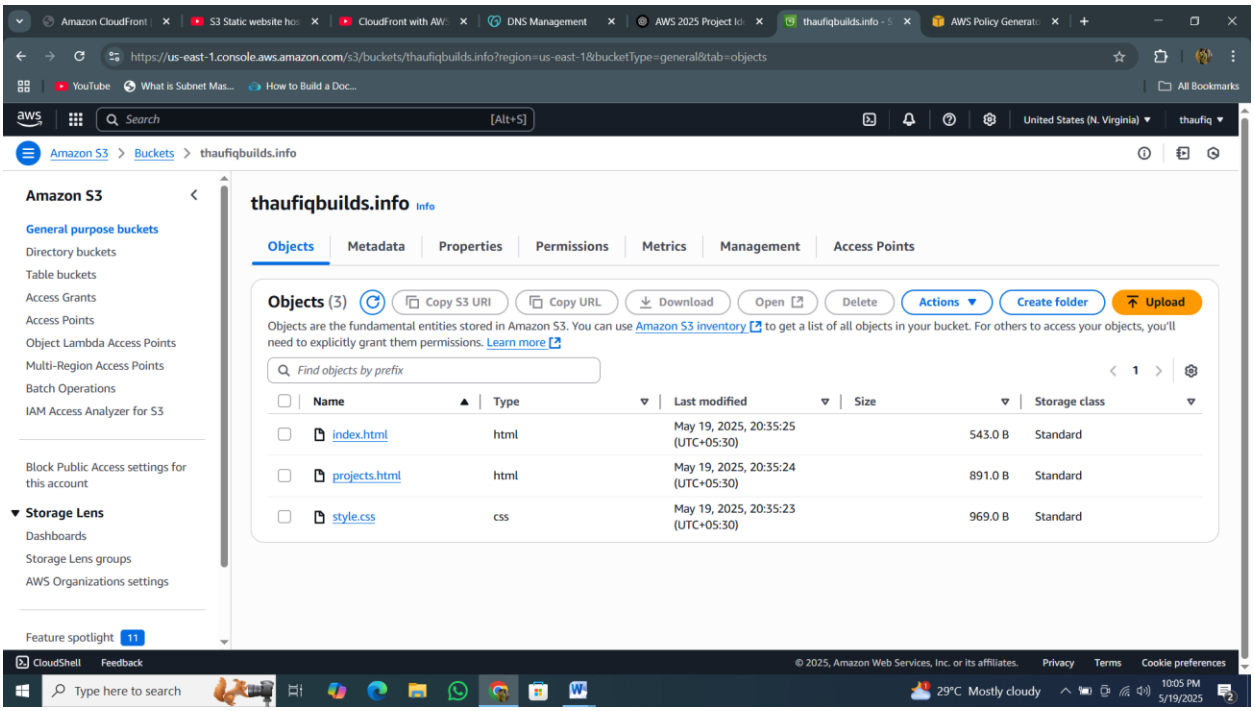
- **CloudFront caching** reduces latency by serving cached content from global edge locations.
- **Route 53 latency-based routing** (if enabled) ensures users are routed to the lowest-latency CloudFront edge.

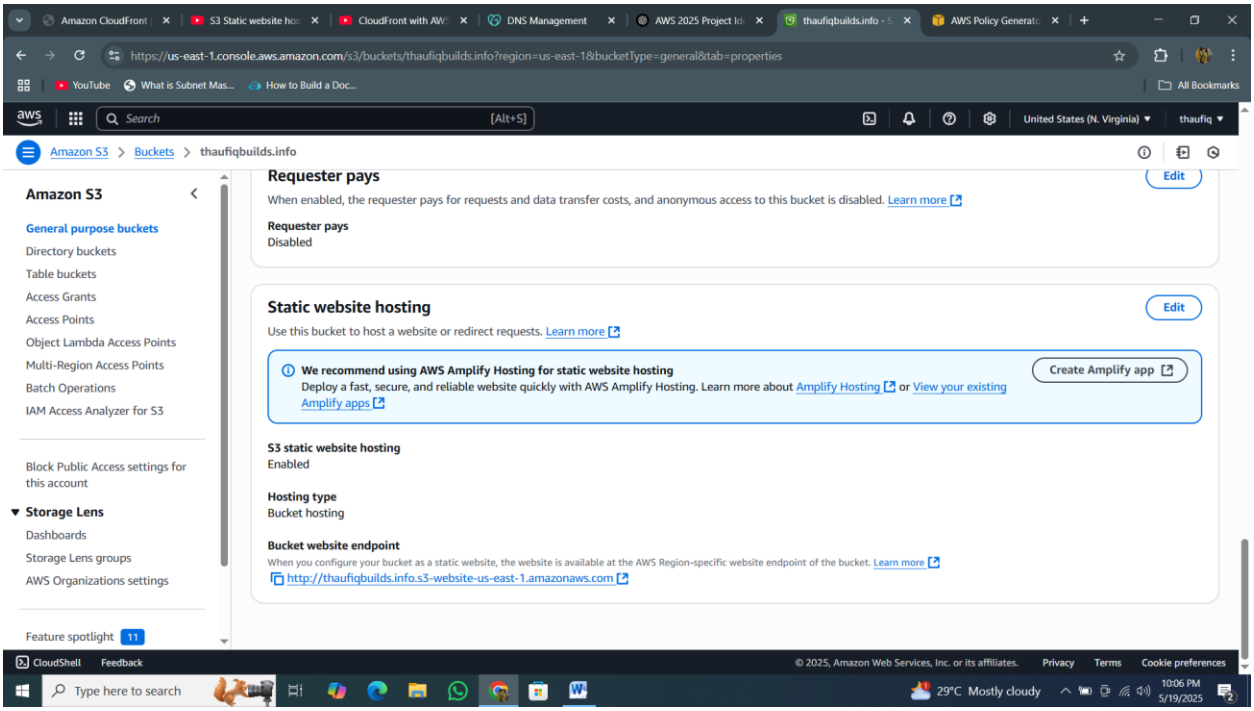
Step 1: S3 Static Website Hosting

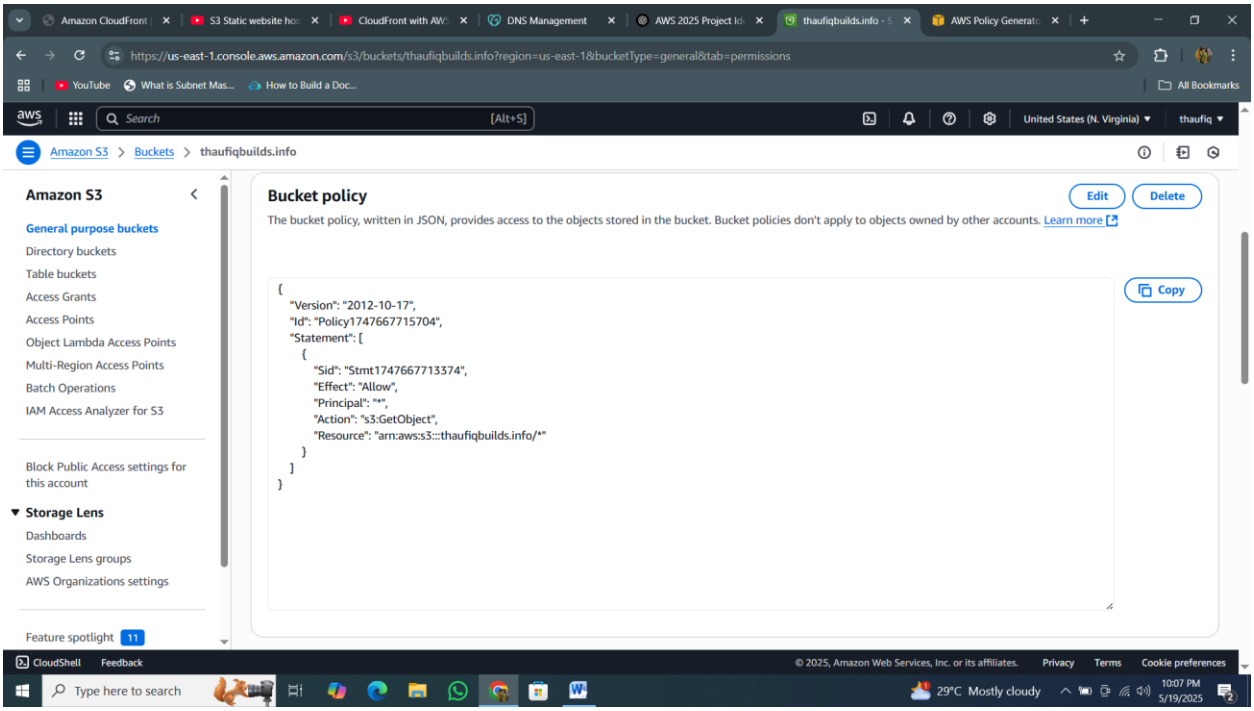
Service: Amazon S3

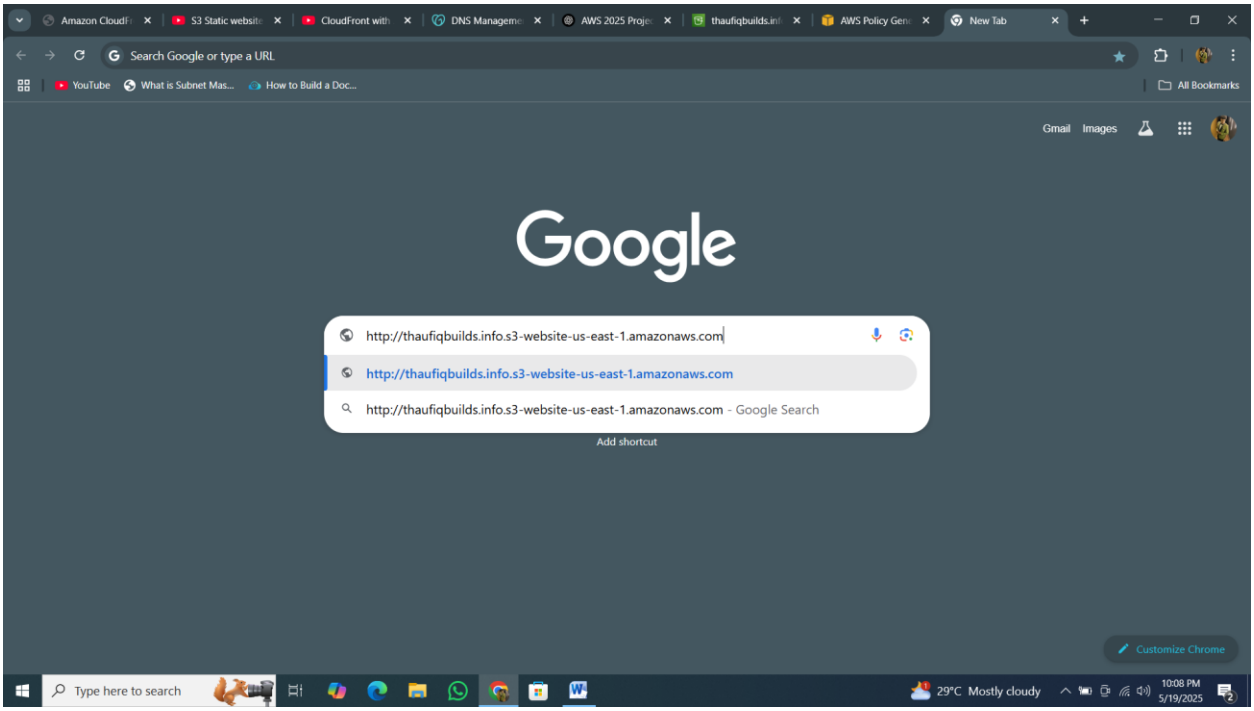
- Created a bucket named `thaufiqbuilds.info`
- Enabled static website hosting
- Uploaded your HTML, CSS, JS files
- Unblocked public access
- Added a bucket policy to allow public read
- Confirmed site accessible via S3 static website endpoint

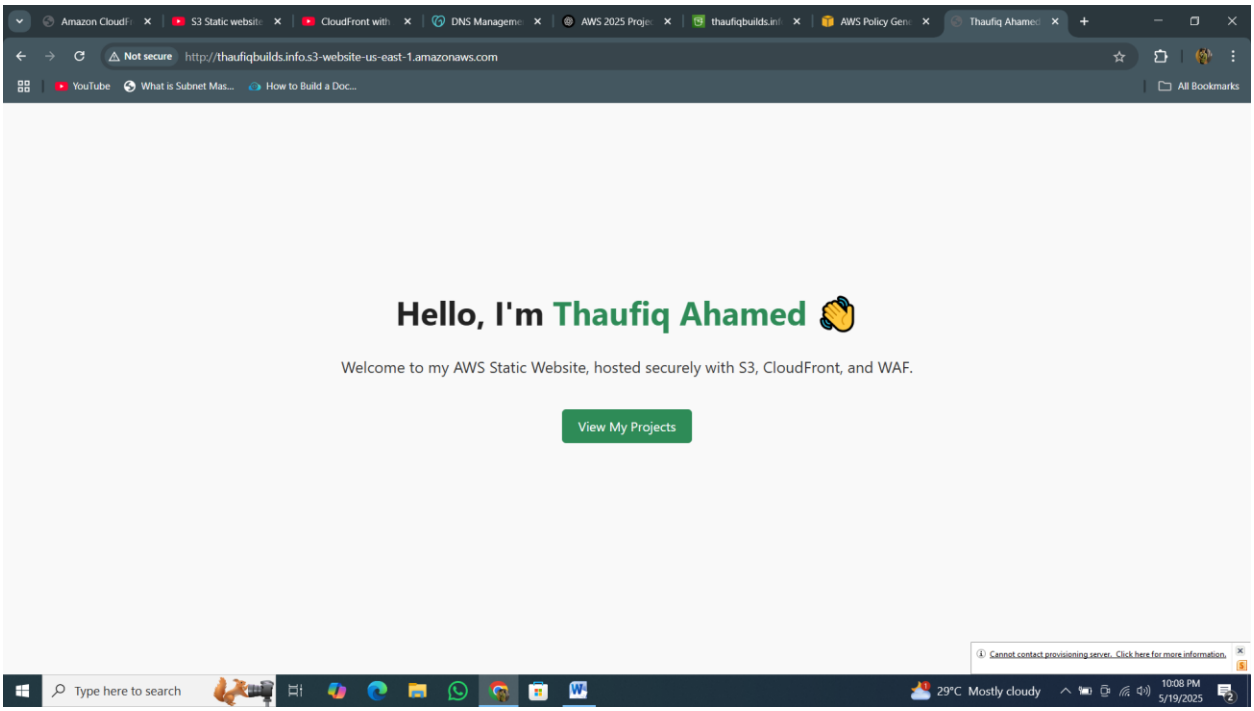


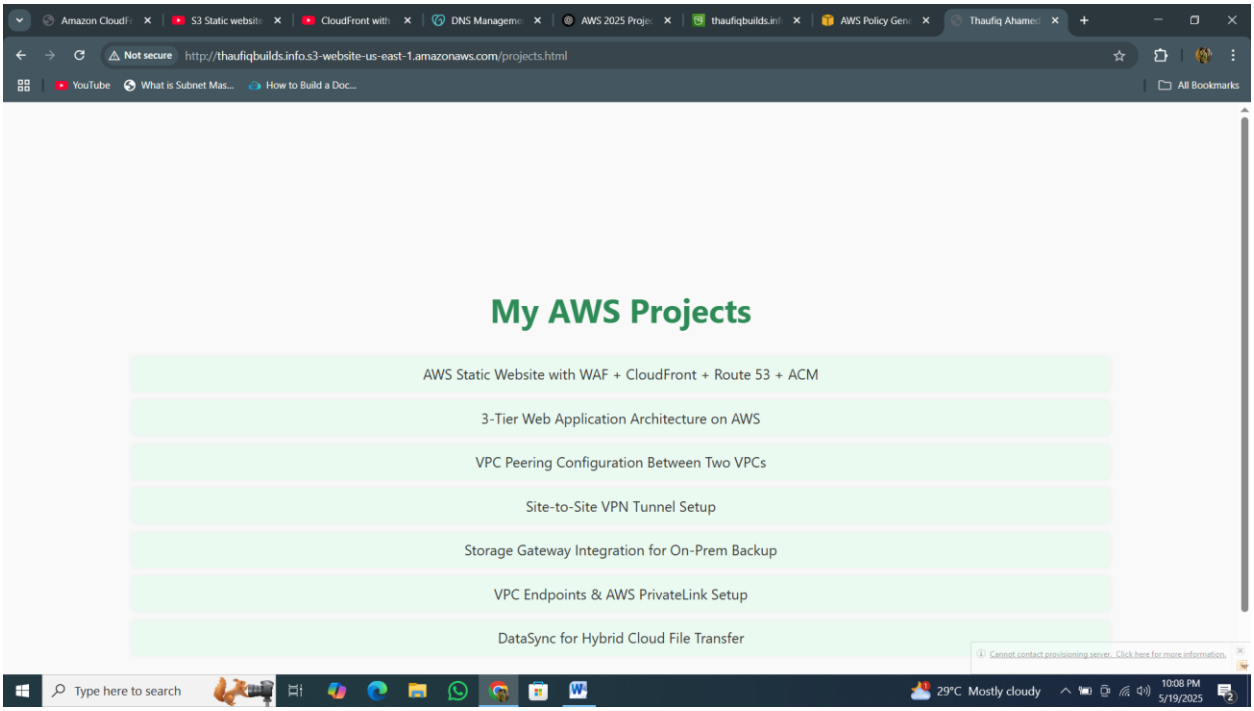

https://us-east-1.console.aws.amazon.com/s3/buckets/thaufiqbuilds.info?region=us-east-1&bucketType=general&tab=objects
Amazon S3 > Buckets > thaufiqbuilds.info
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight 11
thaufiqbuilds.info Info
Objects
Metadata
Properties
Permissions
Metrics
Management
Access Points
Objects (3)
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
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
Find objects by prefix
Name
Type
Last modified
Size
Storage class
index.html
html
May 19, 2025, 20:35:25 (UTC+05:30)
543.0 B
Standard
projects.html
html
May 19, 2025, 20:35:24 (UTC+05:30)
891.0 B
Standard
style.css
css
May 19, 2025, 20:35:23 (UTC+05:30)
969.0 B
Standard
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
29°C Mostly cloudy
10:05 PM
5/19/2025


https://us-east-1.console.aws.amazon.com/s3/buckets/thaufiqbuilds.info?region=us-east-1&bucketType=general&tab=properties
Amazon S3 > Buckets > thaufiqbuilds.info
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight 11
Requester pays
When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. Learn more
Edit
Requester pays
Disabled
Static website hosting
Use this bucket to host a website or redirect requests. Learn more
Edit
We recommend using AWS Amplify Hosting for static website hosting
Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about Amplify Hosting or View your existing Amplify apps
Create Amplify app
S3 static website hosting
Enabled
Hosting type
Bucket hosting
Bucket website endpoint
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. Learn more
http://thaufiqbuilds.info.s3-website-us-east-1.amazonaws.com
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
29°C Mostly cloudy
10:06 PM
5/19/2025


https://us-east-1.console.aws.amazon.com/s3/buckets/thaufiqbuilds.info?region=us-east-1&bucketType=general&tab=permissions
Amazon S3 > Buckets > thaufiqbuilds.info
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight 11
Bucket policy
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more
Edit
Delete
Copy
{
"Version": "2012-10-17",
"Id": "Policy1747667715704",
"Statement": [
{
"Sid": "Stmt1747667713374",
"Effect": "Allow",
"Principal": "*",
"Action": "s3:GetObject",
"Resource": "arn:aws:s3:::thaufiqbuilds.info/*"
}
]
}
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
29°C Mostly cloudy
10:07 PM
5/19/2025


Search Google or type a URL
Gmail
Images
Google
http://thaufiqbuilds.info.s3-website-us-east-1.amazonaws.com
http://thaufiqbuilds.info.s3-website-us-east-1.amazonaws.com
http://thaufiqbuilds.info.s3-website-us-east-1.amazonaws.com - Google Search
Add shortcut
Customize Chrome
Type here to search
29°C Mostly cloudy
10:08 PM
5/19/2025

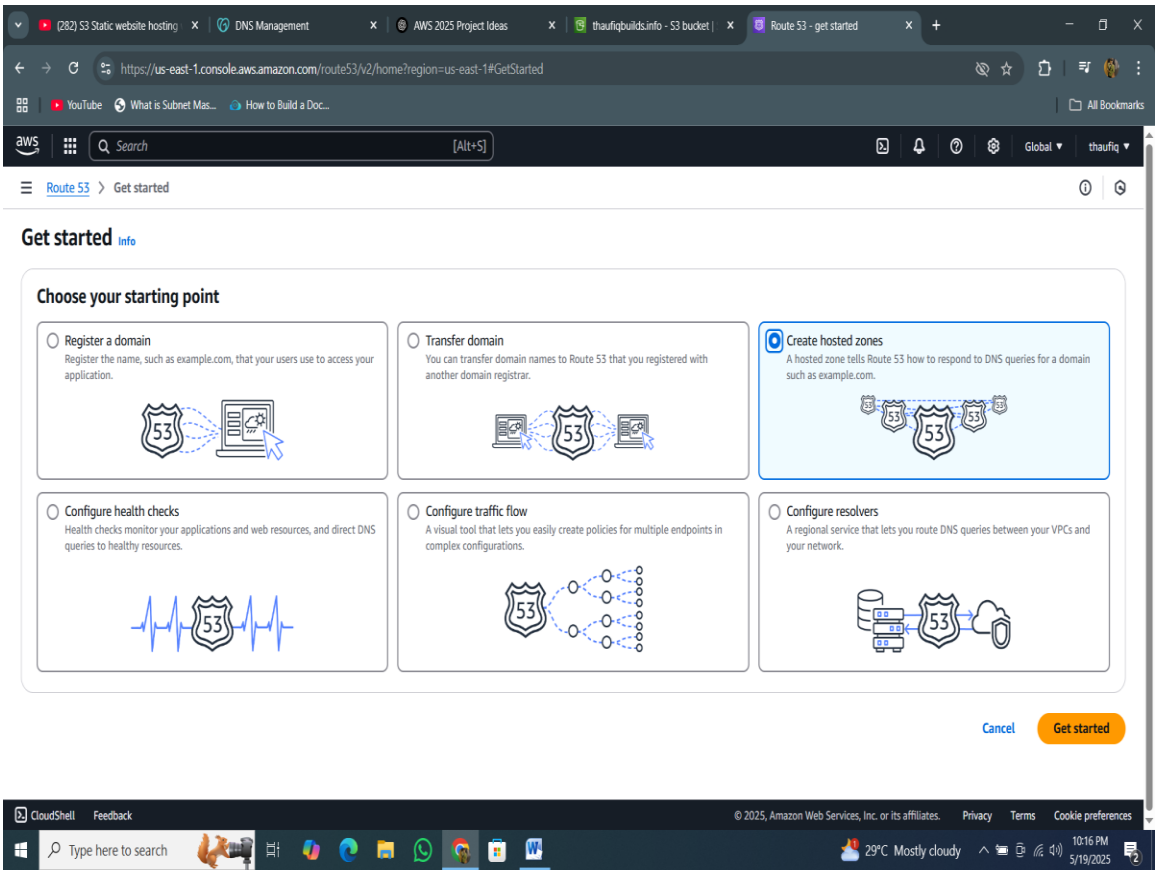

Not secure
http://thaufiqbuilds.info.s3-website-us-east-1.amazonaws.com
YouTube
What is Subnet Mas...
How to Build a Doc...
All Bookmarks
Hello, I'm Thaufiq Ahamed
Welcome to my AWS Static Website, hosted securely with S3, CloudFront, and WAF.
View My Projects
Type here to search
29°C Mostly cloudy
10:08 PM
5/19/2025

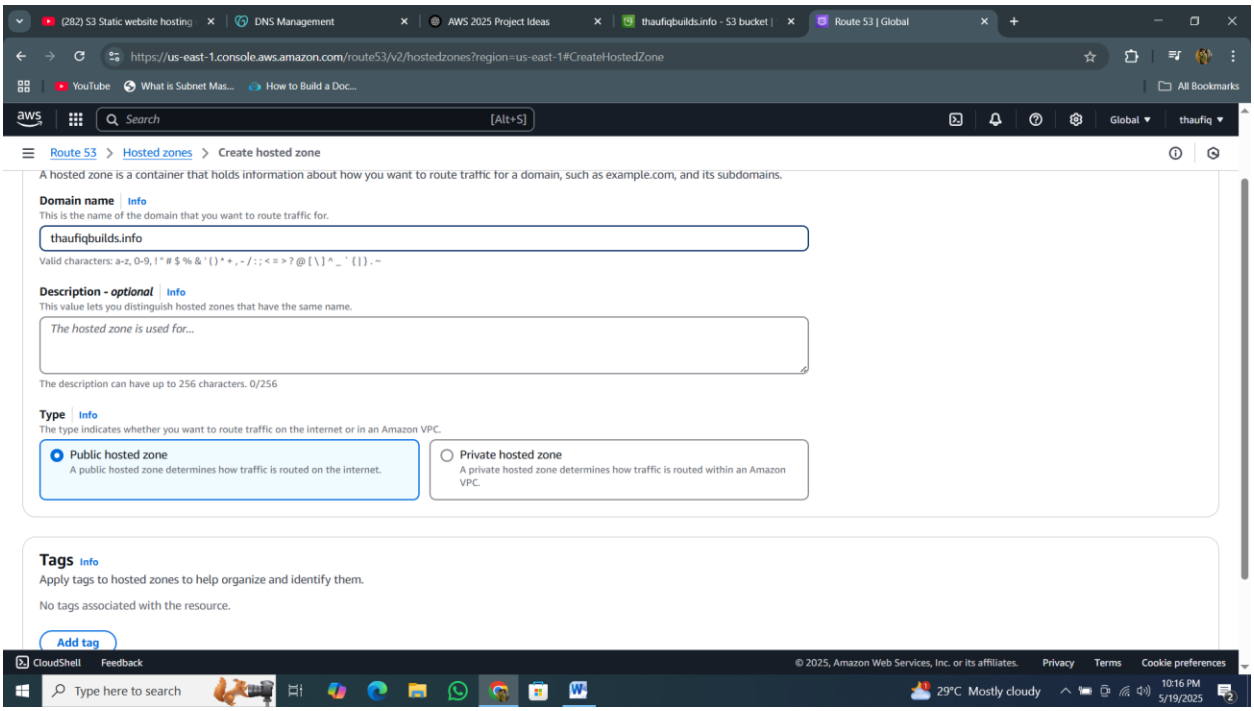

Not secure
http://thaufiqbuilds.info.s3-website-us-east-1.amazonaws.com/projects.html
YouTube
What is Subnet Mas...
How to Build a Doc...
All Bookmarks
My AWS Projects
AWS Static Website with WAF + CloudFront + Route 53 + ACM
3-Tier Web Application Architecture on AWS
VPC Peering Configuration Between Two VPCs
Site-to-Site VPN Tunnel Setup
Storage Gateway Integration for On-Prem Backup
VPC Endpoints & AWS PrivateLink Setup
DataSync for Hybrid Cloud File Transfer
Type here to search
29°C Mostly cloudy
10:08 PM
5/19/2025

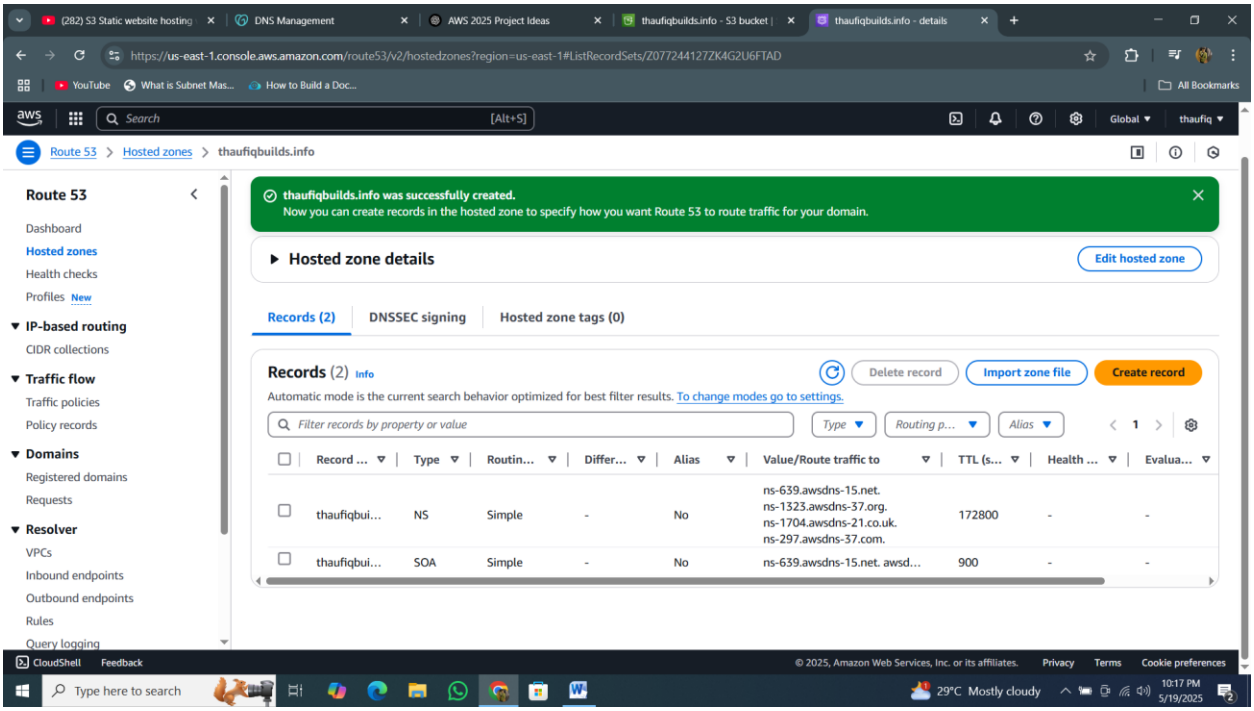
Step 2: Create a Public Hosted Zone in Route 53

Service: Route 53

1. Go to Route 53 → Hosted Zones → **Create Hosted Zone**
2. Enter your domain: `thaufiqbuilds.info`
3. Copy the 4 **NameServer (NS) records**



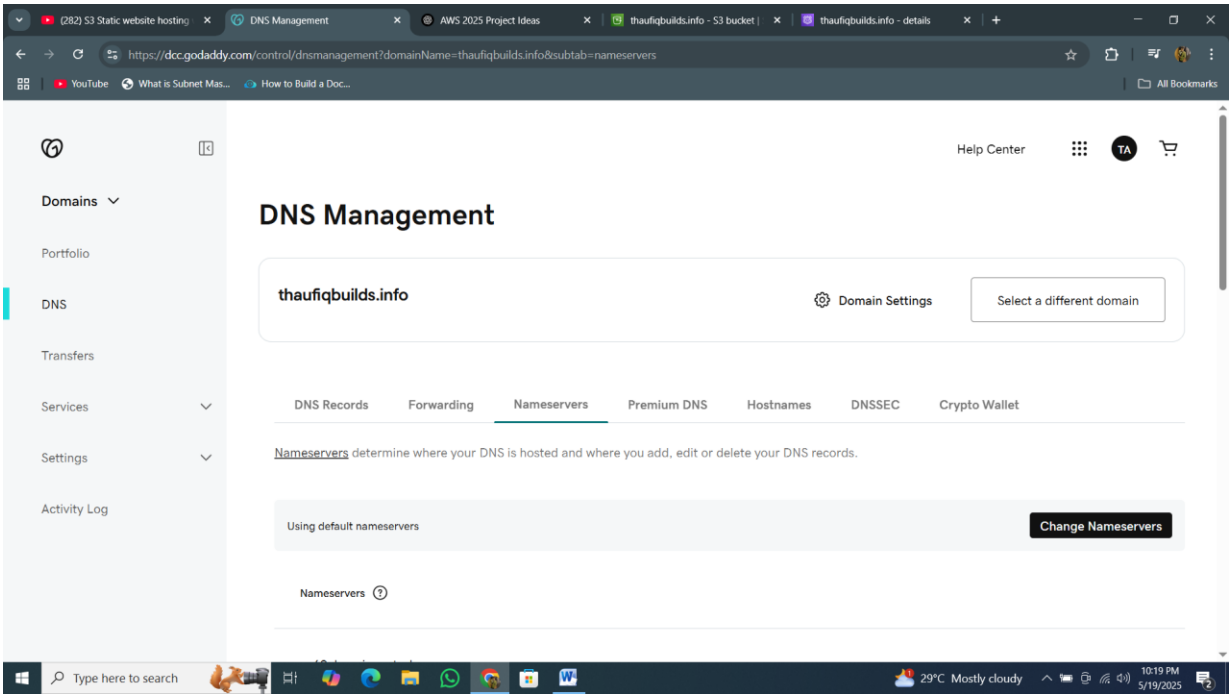

(282) S3 Static website hosting
DNS Management
AWS 2025 Project Ideas
thaufiqbuilds.info - S3 bucket |
Route 53 | Global
https://us-east-1.console.aws.amazon.com/route53/v2/hostedzones?region=us-east-1#CreateHostedZone
YouTube
What is Subnet Mas...
How to Build a Doc...
All Bookmarks
Search
[Alt+S]
Global
thaufiq
Route 53 > Hosted zones > Create hosted zone
A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.
Domain name | Info
This is the name of the domain that you want to route traffic for.
thaufiqbuilds.info
Valid characters: a-z, 0-9, ! " # $ % & ' ( ) * + , - / : ; < = > ? @ [\ ] ^ _ ` { | } . ~
Description - optional | Info
This value lets you distinguish hosted zones that have the same name.
The hosted zone is used for...
The description can have up to 256 characters. 0/256
Type | Info
The type indicates whether you want to route traffic on the internet or in an Amazon VPC.
Public hosted zone
A public hosted zone determines how traffic is routed on the internet.
Private hosted zone
A private hosted zone determines how traffic is routed within an Amazon VPC.
Tags Info
Apply tags to hosted zones to help organize and identify them.
No tags associated with the resource.
Add tag
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
29°C Mostly cloudy
10:16 PM
5/19/2025

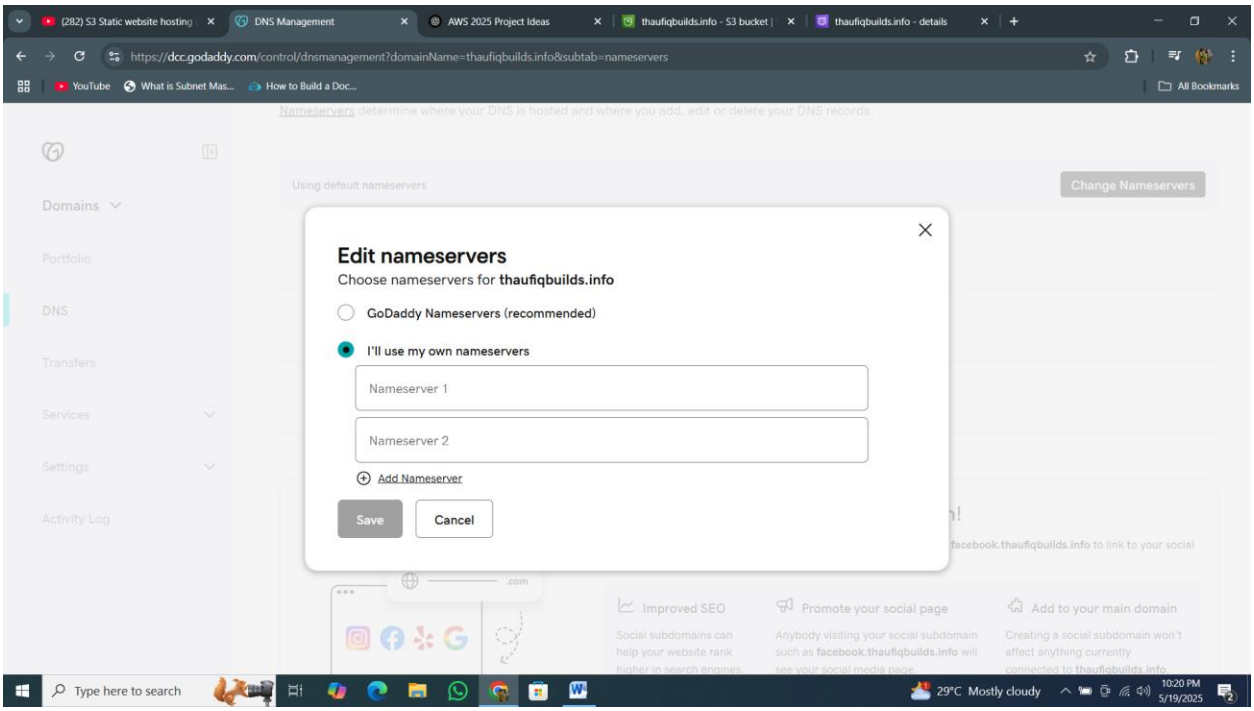

(282) S3 Static website hosting
DNS Management
AWS 2025 Project Ideas
thaufiqbuilds.info - S3 bucket |
thaufiqbuilds.info - details
https://us-east-1.console.aws.amazon.com/route53/v2/hostedzones?region=us-east-1#ListRecordSets/Z077244127ZK4G2U6FTAD
YouTube
What is Subnet Mas...
How to Build a Doc...
All Bookmarks
Search
[Alt+S]
Global
thaufiq
Route 53 > Hosted zones > thaufiqbuilds.info
Route 53
Dashboard
Hosted zones
Health checks
Profiles New
IP-based routing
CIDR collections
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Requests
Resolver
VPCs
Inbound endpoints
Outbound endpoints
Rules
Query logging
thaufiqbuilds.info was successfully created.
Now you can create records in the hosted zone to specify how you want Route 53 to route traffic for your domain.
Hosted zone details
Edit hosted zone
Records (2)
DNSSEC signing
Hosted zone tags (0)
Records (2) Info
Delete record
Import zone file
Create record
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.
Filter records by property or value
Type
Routing p...
Alias
1
Record ...
Type
Routin...
Differ...
Alias
Value/Route traffic to
TTL (s...
Health ...
Evalua...
thaufiqbui...
NS
Simple
-
No
ns-639.awsdns-15.net.
ns-1323.awsdns-37.org.
ns-1704.awsdns-21.co.uk.
ns-297.awsdns-37.com.
172800
-
-
thaufiqbui...
SOA
Simple
-
No
ns-639.awsdns-15.net. awsd...
900
-
-
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
29°C Mostly cloudy
10:17 PM
5/19/2025

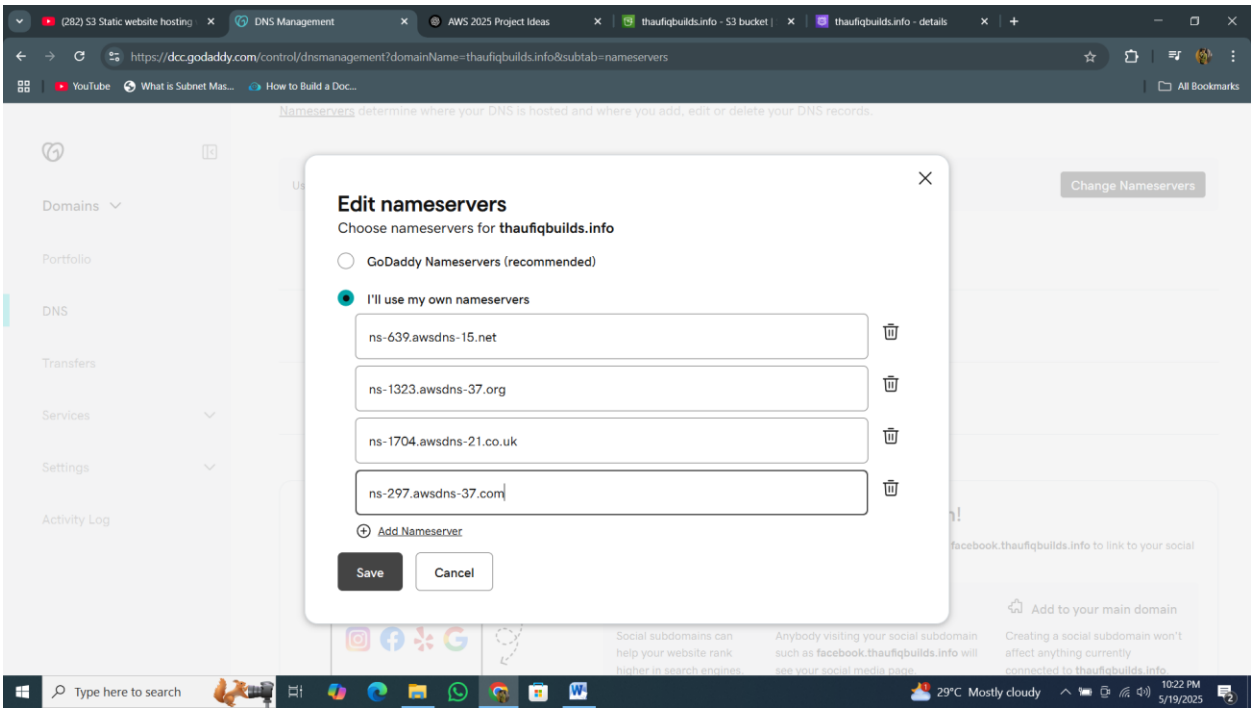
Step 3: Update GoDaddy Nameservers to Point to Route 53

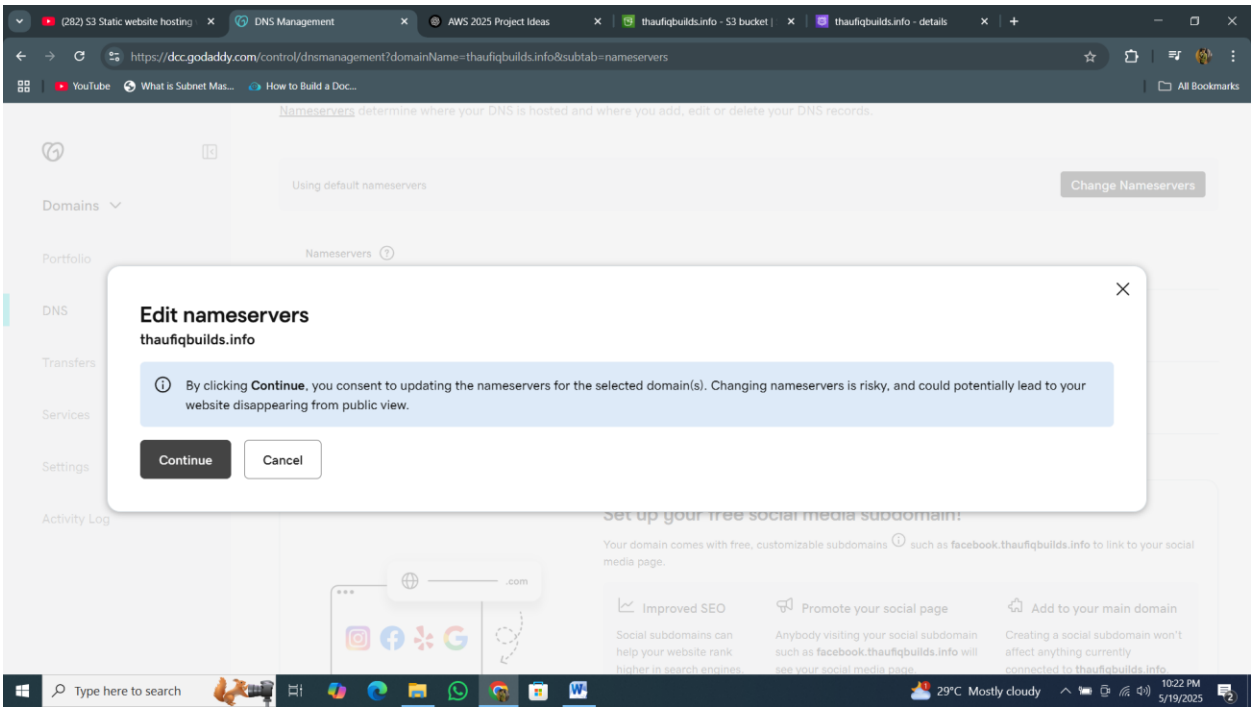
Outside AWS (GoDaddy)

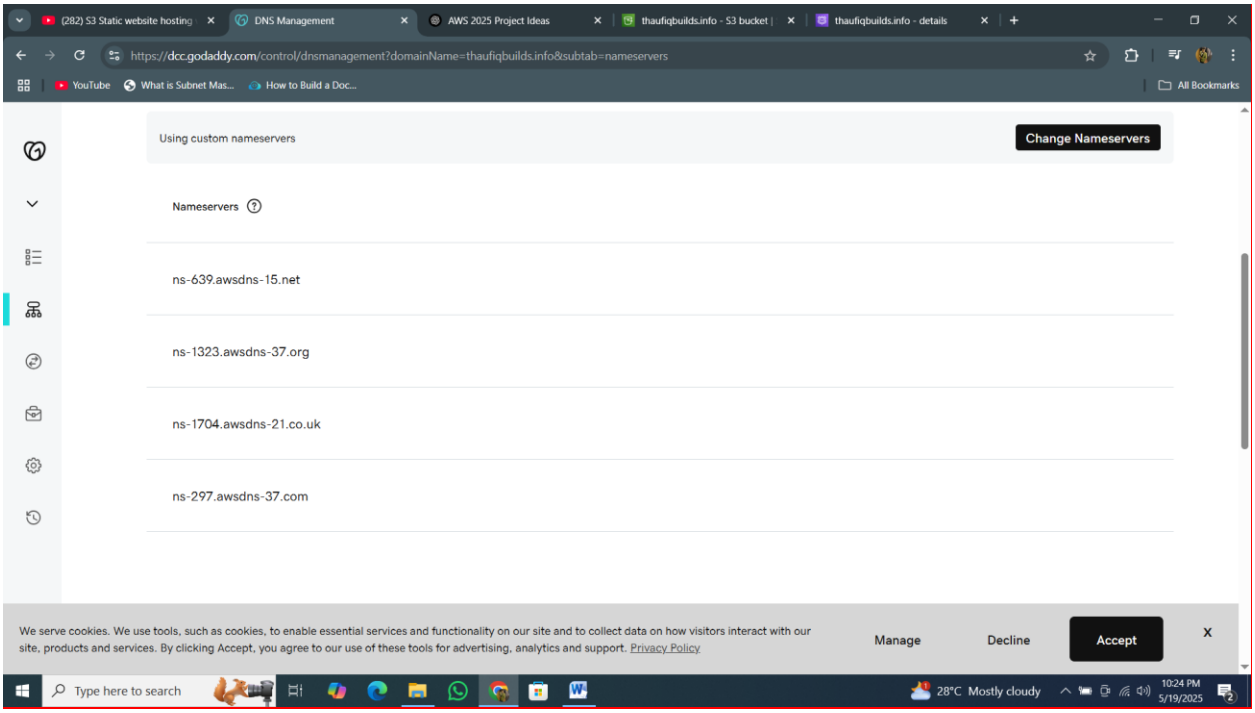
1. Go to GoDaddy → My Products → DNS
2. Find your domain (`thaufiqbuilds.info`)
3. Change nameservers to **Custom**
4. Paste the 4 NS records from Route 53




(282) S3 Static website hosting
DNS Management
AWS 2025 Project Ideas
thaufiqbuilds.info - S3 bucket
thaufiqbuilds.info - details
https://dcc.godaddy.com/control/dnsmanagement?domainName=thaufiqbuilds.info&subtab=nameservers
YouTube
What is Subnet Mas...
How to Build a Doc...
All Bookmarks
Nameservers determine where your DNS is hosted and where you add, edit or delete your DNS records.
Domains
Portfolio
DNS
Transfers
Services
Settings
Activity Log
Using default nameservers
Change Nameservers
Edit nameservers
Choose nameservers for thaufiqbuilds.info
GoDaddy Nameservers (recommended)
I'll use my own nameservers
Nameserver 1
Nameserver 2
Add Nameserver
Save
Cancel
Improved SEO
Promote your social page
Add to your main domain
Social subdomains can help your website rank higher in search engines
Anybody visiting your social subdomain such as facebook.thaufiqbuilds.info will see your social media page
Creating a social subdomain won't affect anything currently connected to thaufiqbuilds.info
facebook.thaufiqbuilds.info to link to your social
Type here to search
29°C Mostly cloudy
10:20 PM
5/19/2025


(282) S3 Static website hosting
DNS Management
AWS 2025 Project Ideas
thaufiqbuilds.info - S3 bucket
thaufiqbuilds.info - details
https://dcc.godaddy.com/control/dnsmanagement?domainName=thaufiqbuilds.info&subtab=nameservers
YouTube
What is Subnet Mas...
How to Build a Doc...
All Bookmarks
Nameservers determine where your DNS is hosted and where you add, edit or delete your DNS records.
Domains
Portfolio
DNS
Transfers
Services
Settings
Activity Log
Change Nameservers
Edit nameservers
Choose nameservers for thaufiqbuilds.info
GoDaddy Nameservers (recommended)
I'll use my own nameservers
ns-639.awsdns-15.net
ns-1323.awsdns-37.org
ns-1704.awsdns-21.co.uk
ns-297.awsdns-37.com
Add Nameserver
Save
Cancel
Add to your main domain
Social subdomains can help your website rank higher in search engines
Anybody visiting your social subdomain such as facebook.thaufiqbuilds.info will see your social media page
Creating a social subdomain won't affect anything currently connected to thaufiqbuilds.info
facebook.thaufiqbuilds.info to link to your social
Type here to search
29°C Mostly cloudy
10:22 PM
5/19/2025

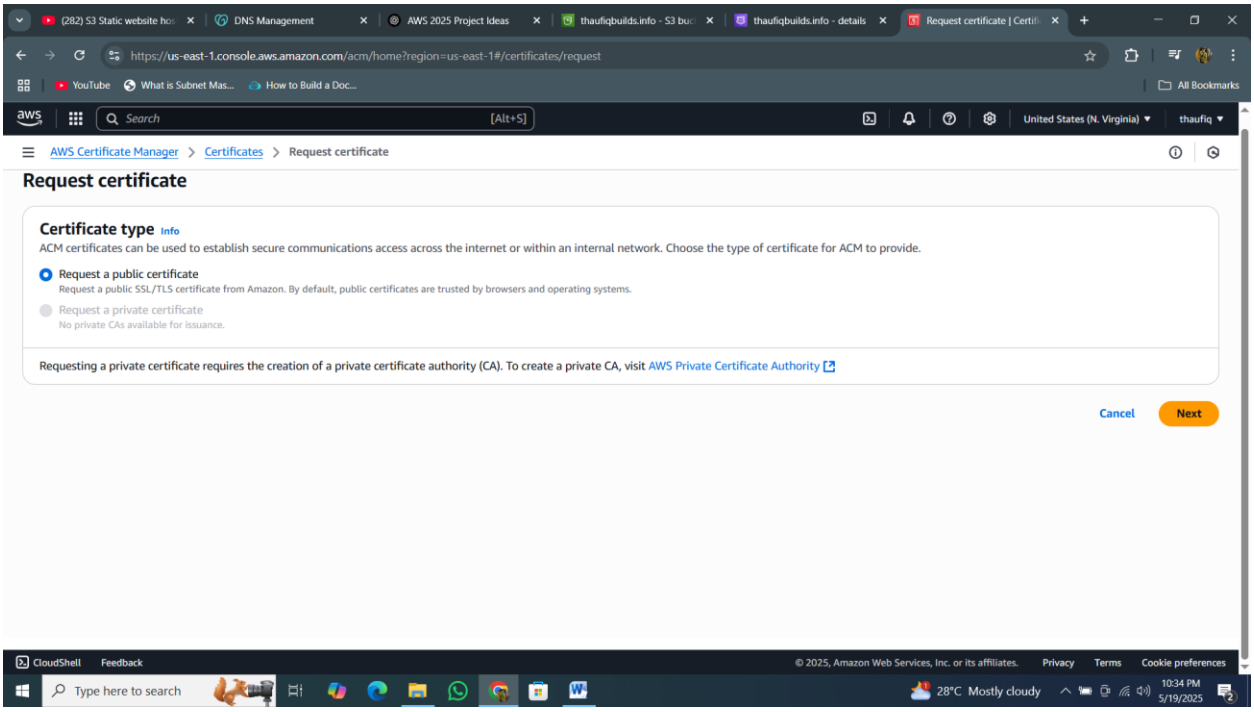

(282) S3 Static website hosting
DNS Management
AWS 2025 Project Ideas
thaufiqbuilds.info - S3 bucket |
thaufiqbuilds.info - details
https://dcc.godaddy.com/control/dnsmanagement?domainName=thaufiqbuilds.info&subtab=nameservers
YouTube
What is Subnet Mas...
How to Build a Doc...
All Bookmarks
Nameservers determine where your DNS is hosted and where you add, edit or delete your DNS records.
Domains
Portfolio
DNS
Transfers
Services
Settings
Activity Log
Using default nameservers
Change Nameservers
Nameservers
Edit nameservers
thaufiqbuilds.info
By clicking Continue, you consent to updating the nameservers for the selected domain(s). Changing nameservers is risky, and could potentially lead to your website disappearing from public view.
Continue
Cancel
Set up your free social media subdomain!
Your domain comes with free, customizable subdomains such as facebook.thaufiqbuilds.info to link to your social media page.
Improved SEO
Promote your social page
Add to your main domain
Type here to search
29°C Mostly cloudy
10:22 PM
5/19/2025

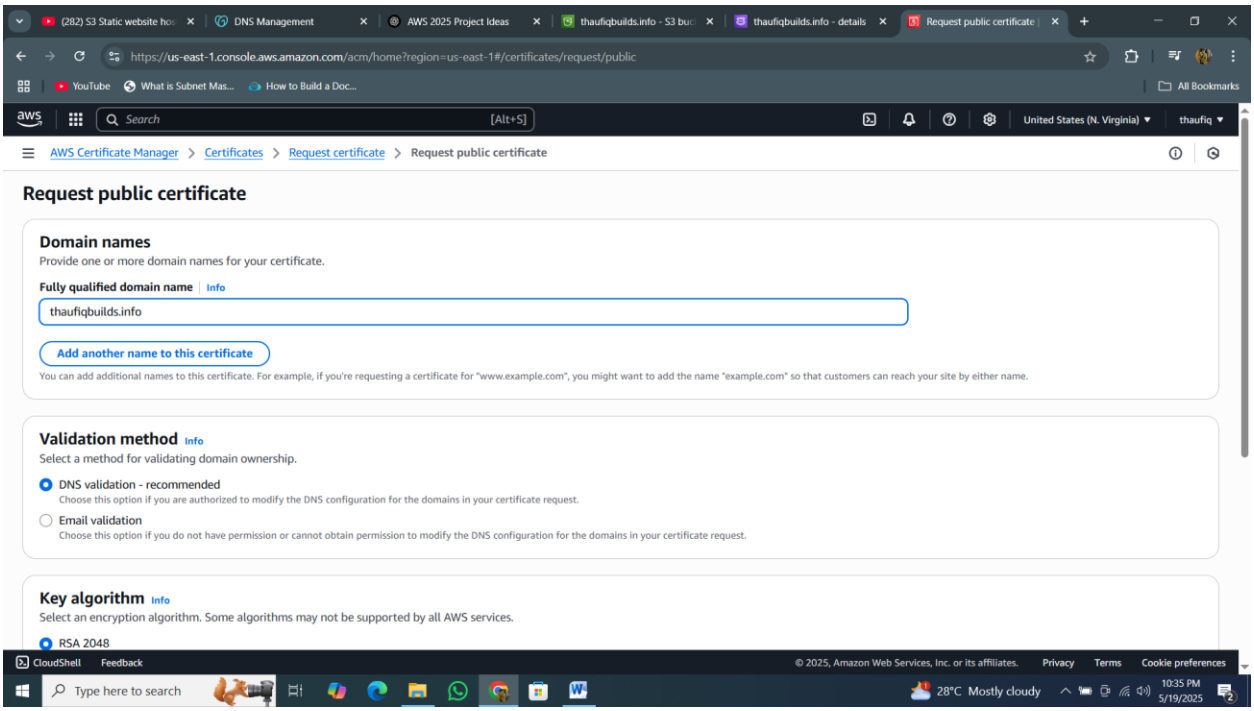

(282) S3 Static website hosting
DNS Management
AWS 2025 Project Ideas
thaufiqbuilds.info - S3 bucket |
thaufiqbuilds.info - details
https://dcc.godaddy.com/control/dnsmanagement?domainName=thaufiqbuilds.info&subtab=nameservers
YouTube
What is Subnet Mas...
How to Build a Doc...
All Bookmarks
Using custom nameservers
Change Nameservers
Nameservers
ns-639.awsdns-15.net
ns-1323.awsdns-37.org
ns-1704.awsdns-21.co.uk
ns-297.awsdns-37.com
We serve cookies. We use tools, such as cookies, to enable essential services and functionality on our site and to collect data on how visitors interact with our site, products and services. By clicking Accept, you agree to our use of these tools for advertising, analytics and support. Privacy Policy
Manage
Decline
Accept
Type here to search
28°C Mostly cloudy
10:24 PM
5/19/2025

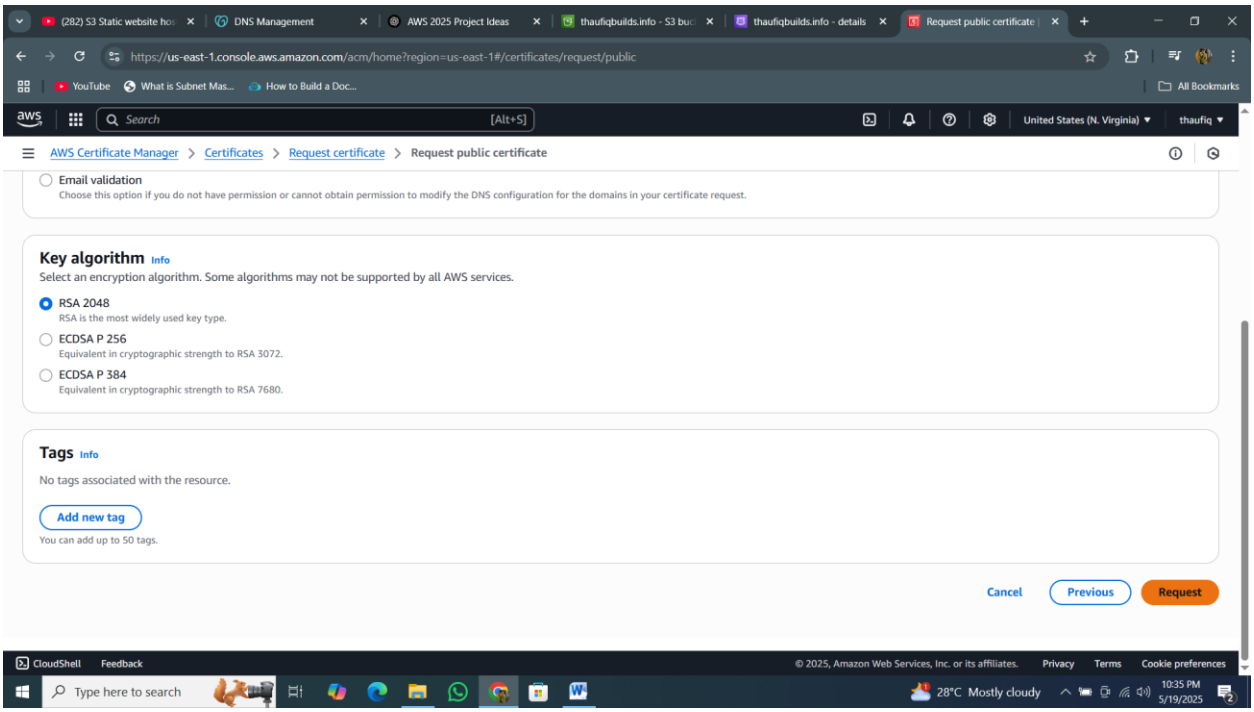
Step 4: Request SSL Certificate in AWS ACM

Service: AWS Certificate Manager (ACM)

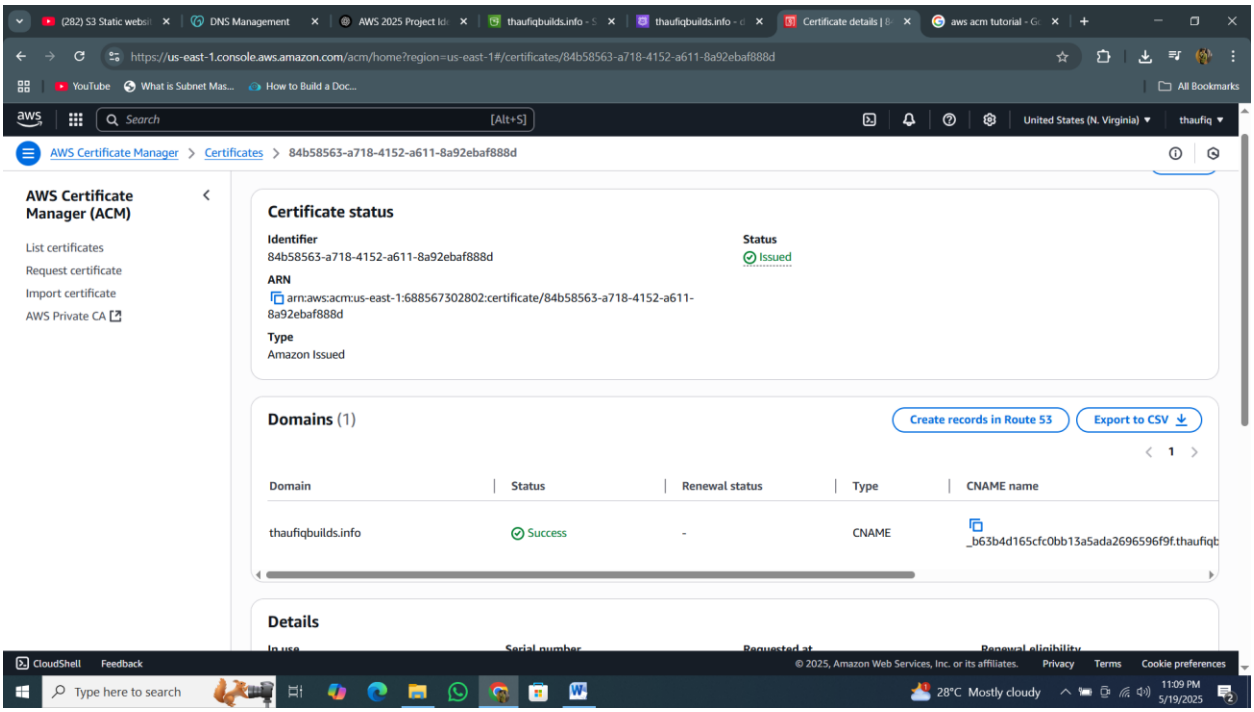
1. Go to ACM → Request certificate → **Public certificate**
2. Enter domain name: `thaufiqbuilds.info` (also add `www.thaufiqbuilds.info` if needed)
3. Choose **DNS validation**
4. ACM will show a CNAME record → Go to Route 53 → Add that as a **new record**
5. Wait until ACM shows **"Issued"**




(282) S3 Static website hos
DNS Management
AWS 2025 Project Ideas
thaufiqbuilds.info - S3 buc
thaufiqbuilds.info - details
Request public certificate
https://us-east-1.console.aws.amazon.com/acm/home?region=us-east-1#/certificates/request/public
YouTube
What is Subnet Mas...
How to Build a Doc...
All Bookmarks
aws
Search
[Alt+S]
United States (N. Virginia)
thaufiq
AWS Certificate Manager > Certificates > Request certificate > Request public certificate
Request public certificate
Domain names
Provide one or more domain names for your certificate.
Fully qualified domain name Info
thaufiqbuilds.info
Add another name to this certificate
You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name.
Validation method Info
Select a method for validating domain ownership.
DNS validation - recommended
Choose this option if you are authorized to modify the DNS configuration for the domains in your certificate request.
Email validation
Choose this option if you do not have permission or cannot obtain permission to modify the DNS configuration for the domains in your certificate request.
Key algorithm Info
Select an encryption algorithm. Some algorithms may not be supported by all AWS services.
RSA 2048
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
28°C Mostly cloudy
10:35 PM
5/19/2025


(282) S3 Static website hos
DNS Management
AWS 2025 Project Ideas
thaufiqbuilds.info - S3 buc
thaufiqbuilds.info - details
Request public certificate
https://us-east-1.console.aws.amazon.com/acm/home?region=us-east-1#/certificates/request/public
YouTube
What is Subnet Mas...
How to Build a Doc...
All Bookmarks
aws
Search
[Alt+S]
United States (N. Virginia)
thaufiq
AWS Certificate Manager > Certificates > Request certificate > Request public certificate
Email validation
Choose this option if you do not have permission or cannot obtain permission to modify the DNS configuration for the domains in your certificate request.
Key algorithm Info
Select an encryption algorithm. Some algorithms may not be supported by all AWS services.
RSA 2048
RSA is the most widely used key type.
ECDSA P 256
Equivalent in cryptographic strength to RSA 3072.
ECDSA P 384
Equivalent in cryptographic strength to RSA 7680.
Tags Info
No tags associated with the resource.
Add new tag
You can add up to 50 tags.
Cancel
Previous
Request
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
28°C Mostly cloudy
10:35 PM
5/19/2025

CLICK on create record in route 53 and automatically a record is create route53 then only ssl cretificate is issued



Step 5: Create CloudFront Distribution

Service: Amazon CloudFront

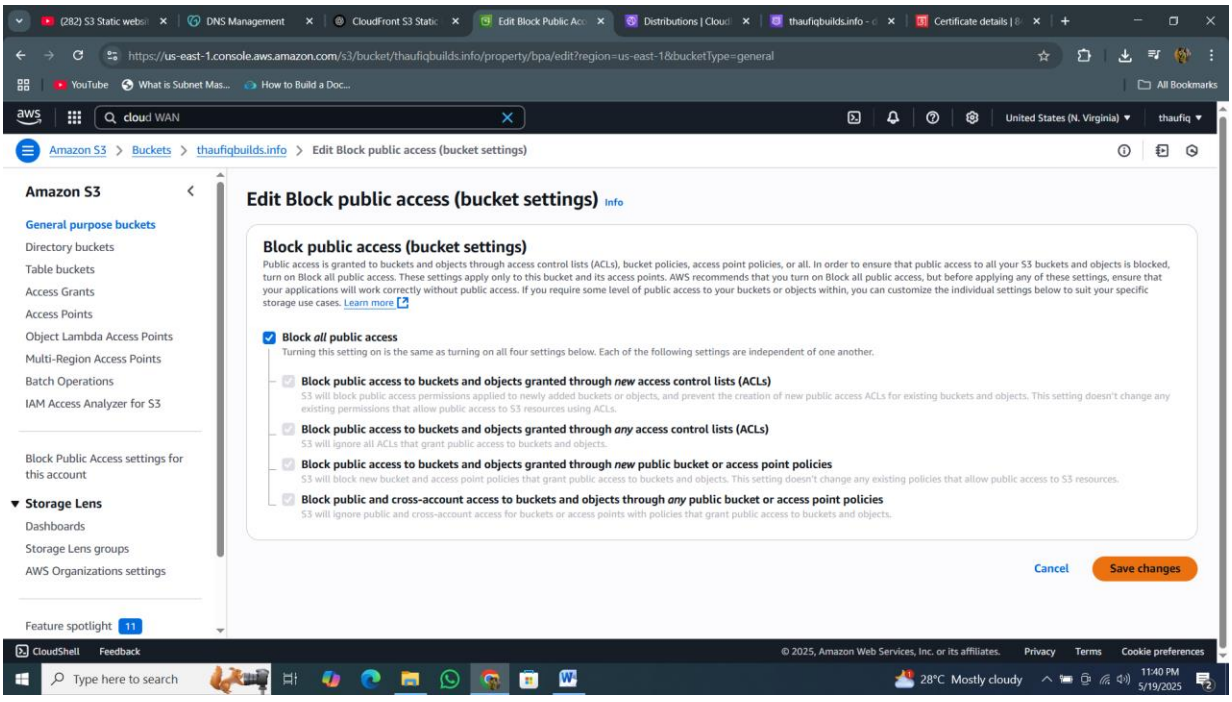
1. Go to the CloudFront console and click **Create Distribution**.
2. For **Origin domain**, enter your **S3 bucket REST endpoint** (not the static website endpoint).
   Example: `thaufiqbuilds.info.s3.<region>.amazonaws.com`
3. Under **Origin Access**, enable **Origin Access Identity (OAI)**:
   - Create a new OAI or choose an existing one.
   - This allows CloudFront to securely access your private S3 bucket.
4. Update your **S3 bucket policy** to allow access only from the OAI and block all public access.
5. For **Viewer protocol policy**, select **Redirect HTTP to HTTPS** to enforce secure access.

6. In **Alternate domain names (CNAMEs)**, add your custom domain: `thaufiqbuilds.info`.
7. For **SSL Certificate**, choose **Custom SSL Certificate** (for example, from ACM) and select your certificate.
8. Leave other settings as default and click **Create Distribution**.

NOTE : The S3 static website endpoint is a public endpoint designed for hosting static content and does not support private access mechanisms like OAI. If the bucket is public, anyone can access the website URL directly, bypassing CloudFront.

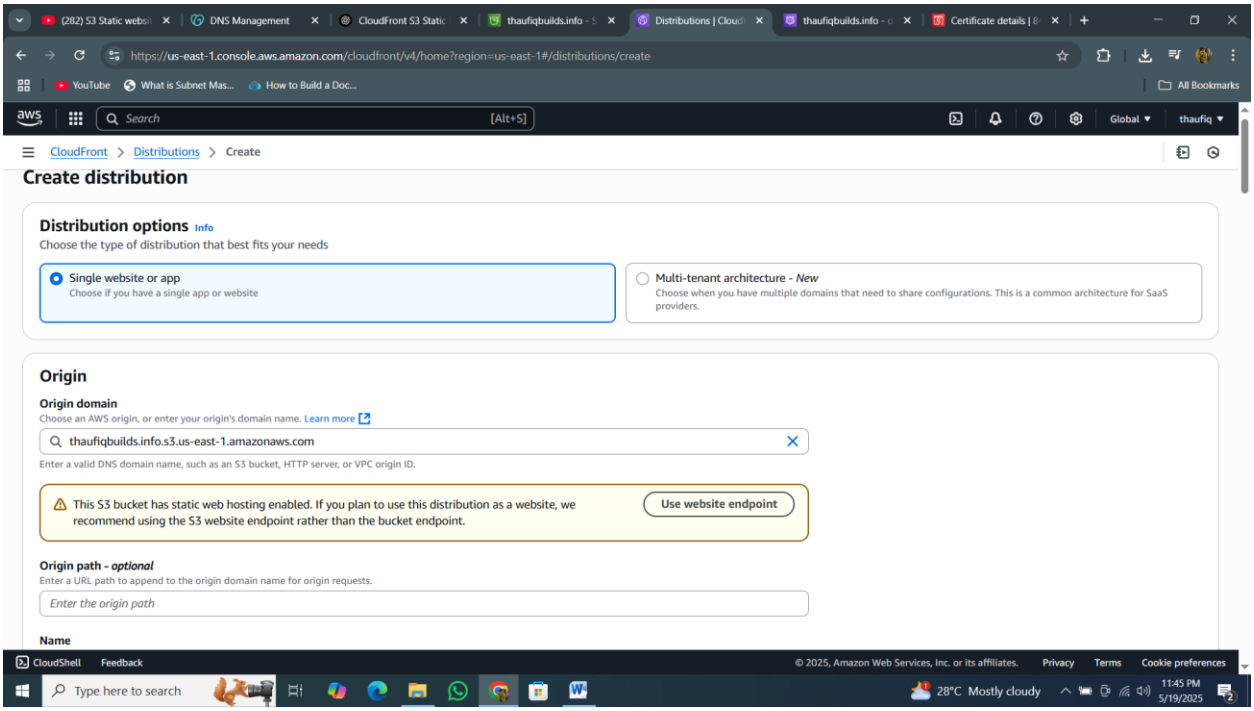
. Solution / Best Practice:

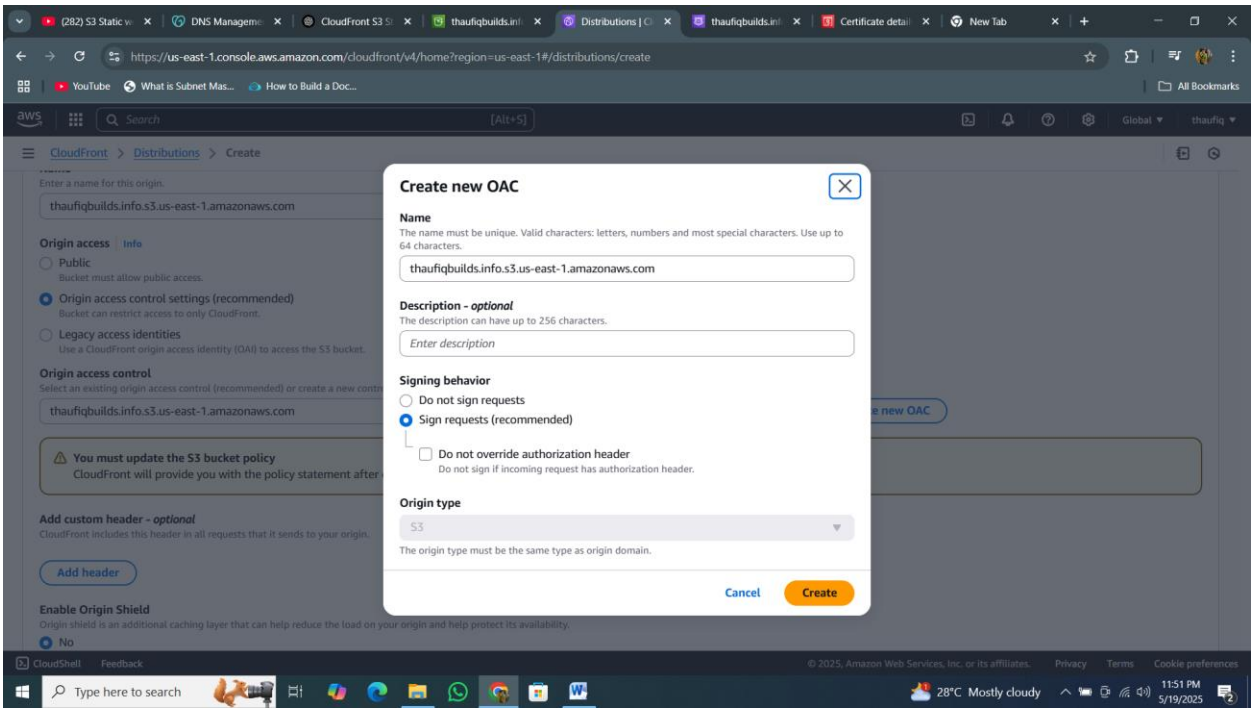
To restrict access **only via CloudFront**, use the **S3 bucket REST endpoint** (e.g., `thaufiqbuilds.info.s3.<region>.amazonaws.com`) as the CloudFront origin and enable **Origin Access Identity (OAI)**. Then, make the bucket private by blocking public access. This ensures only CloudFront can fetch the content and users must access via CloudFron

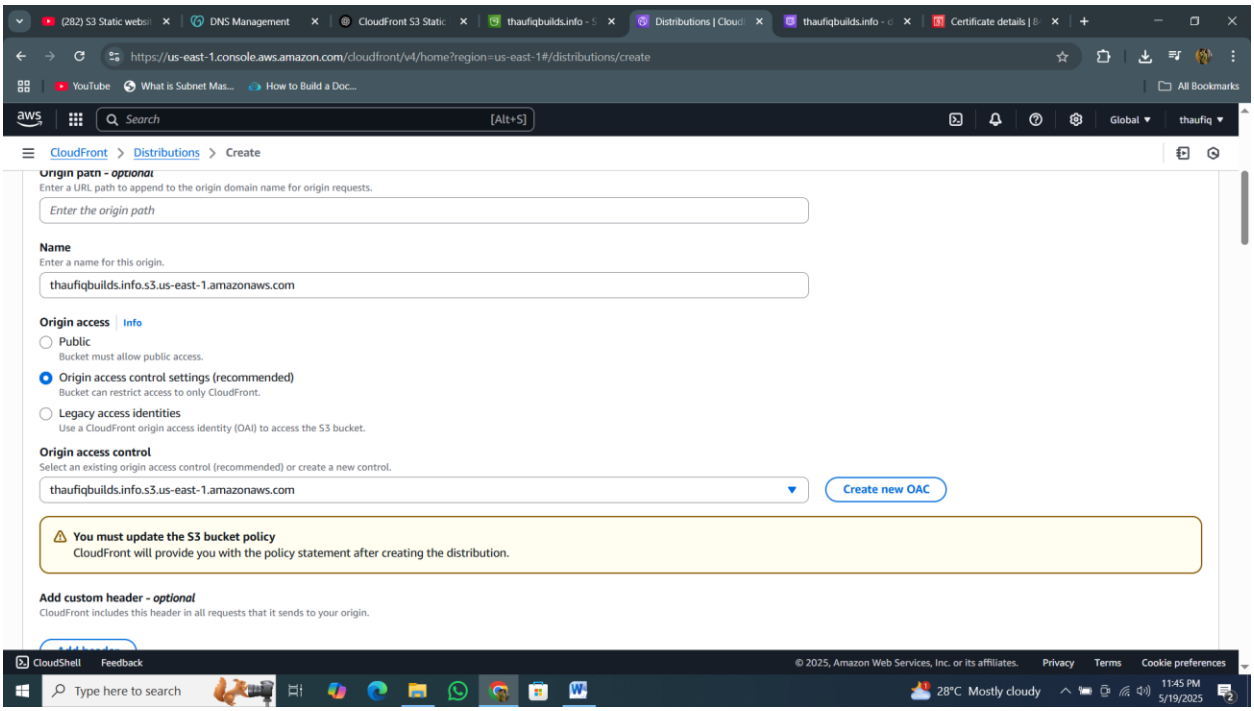


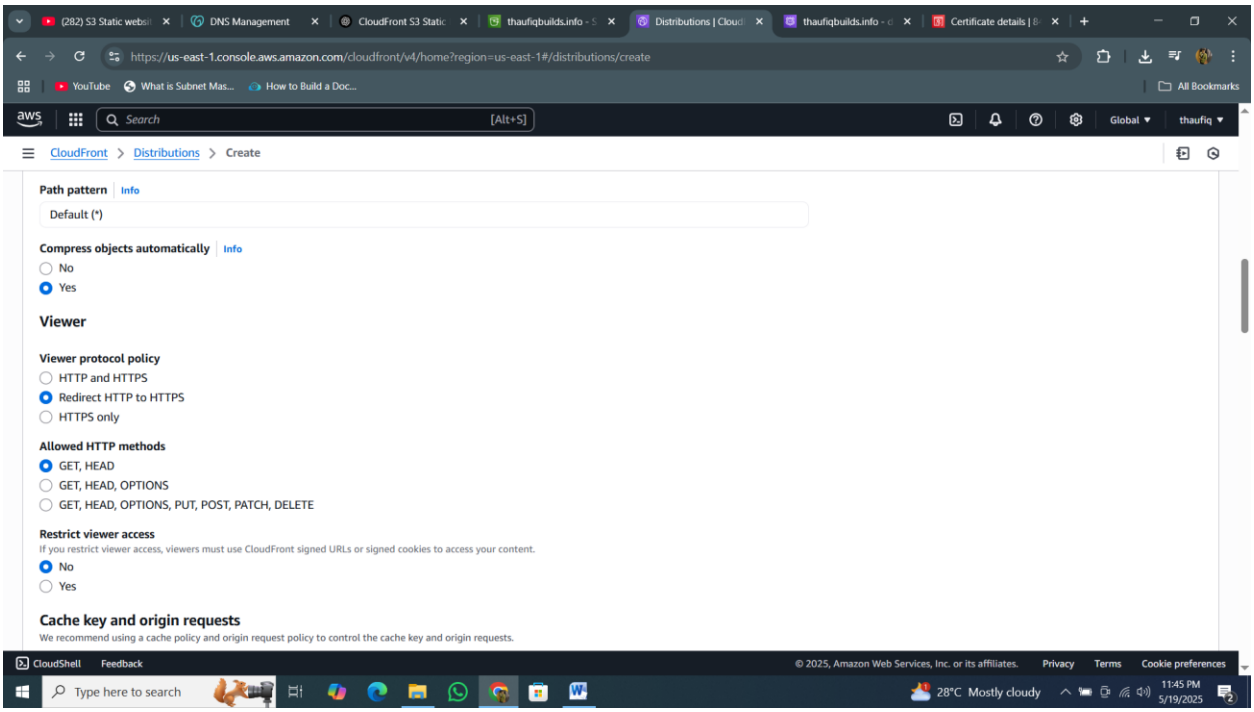
Even though we made the buck private the user can acess the the bucket via cloudfront right (through the bucket policy)

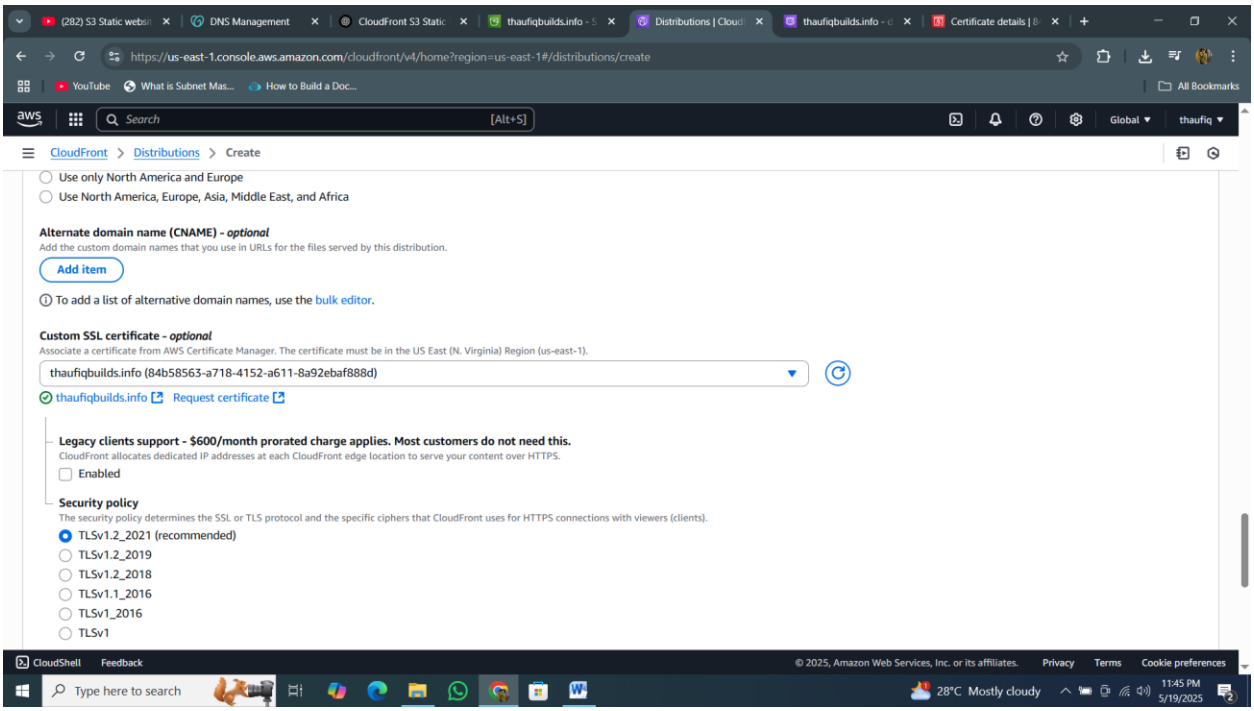
Let we create cloud front distribution

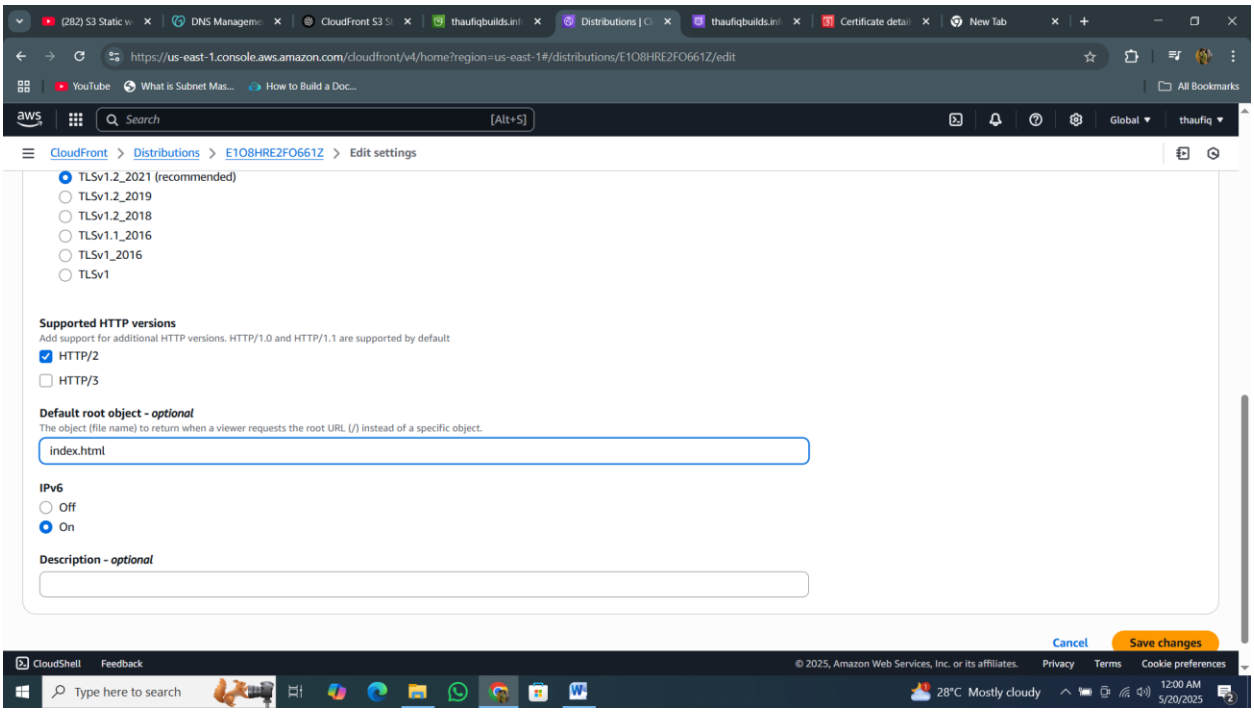


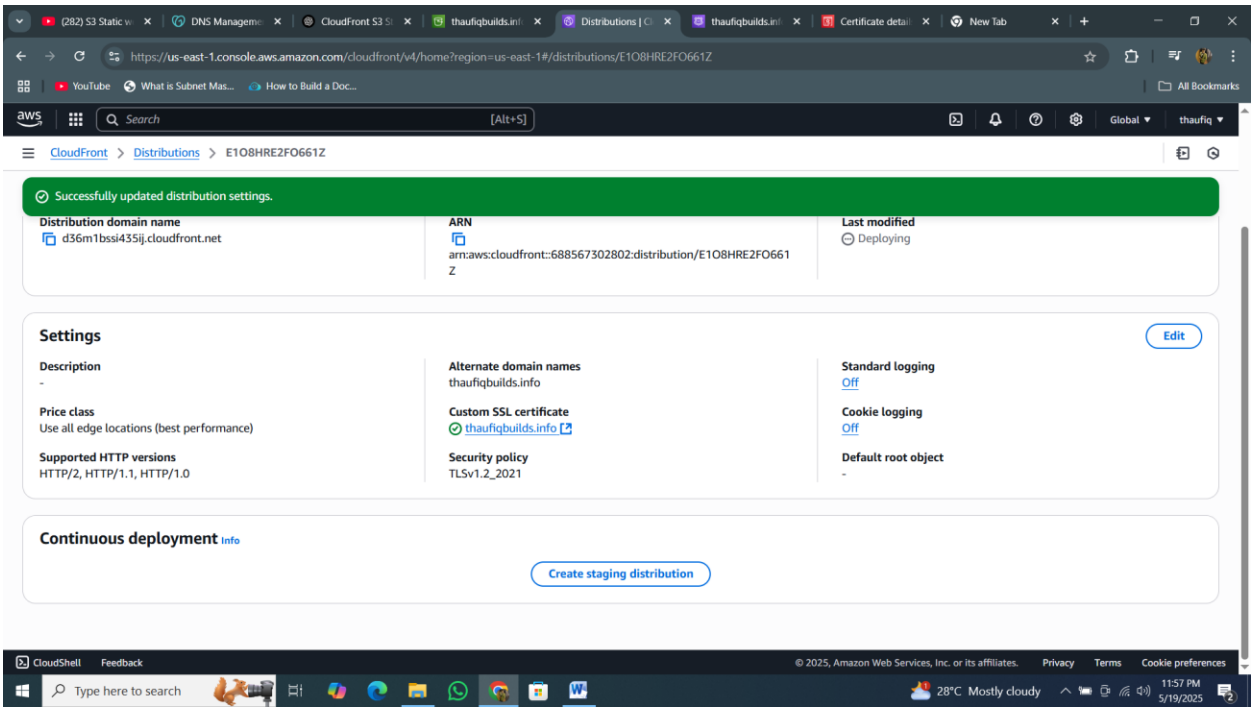


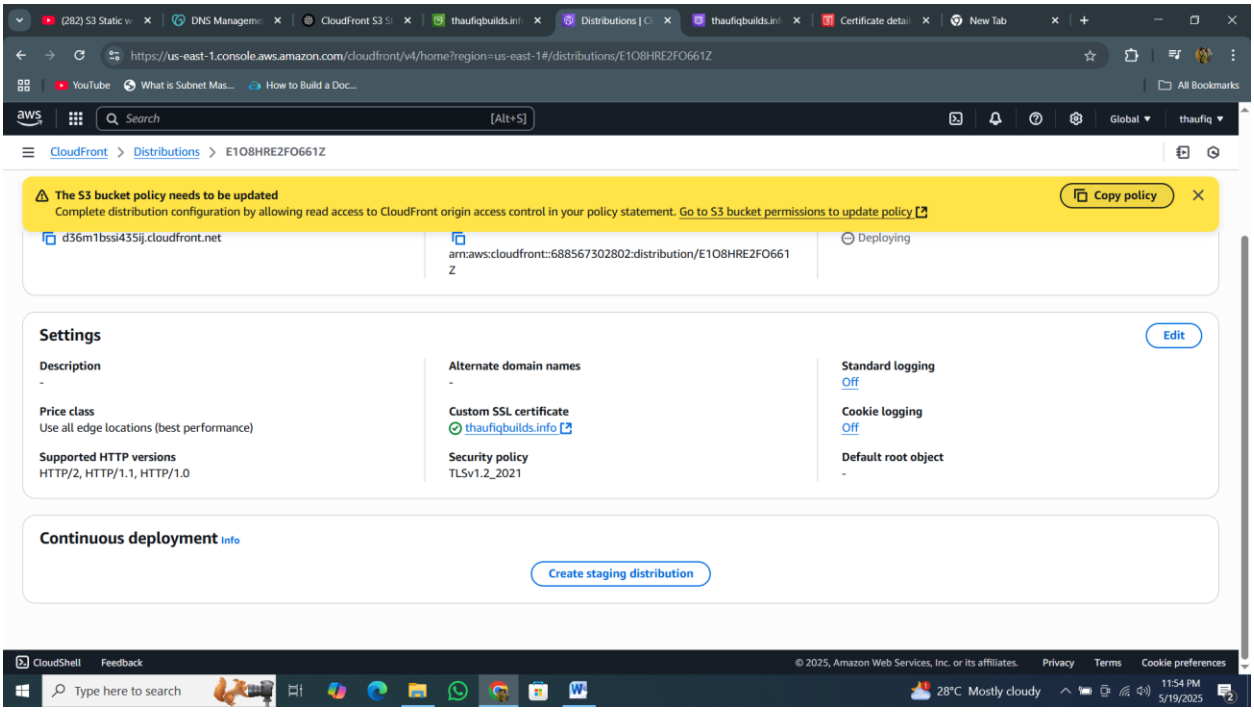

https://us-east-1.console.aws.amazon.com/cloudfront/v4/home?region=us-east-1#/distributions/create
CloudFront > Distributions > Create
Origin path - optional
Enter a URL path to append to the origin domain name for origin requests.
Enter the origin path
Name
Enter a name for this origin.
thaufiqbuilds.info.s3.us-east-1.amazonaws.com
Origin access | Info
Public
Bucket must allow public access.
Origin access control settings (recommended)
Bucket can restrict access to only CloudFront.
Legacy access identities
Use a CloudFront origin access identity (OAI) to access the S3 bucket.
Origin access control
Select an existing origin access control (recommended) or create a new control.
thaufiqbuilds.info.s3.us-east-1.amazonaws.com
Create new OAC
You must update the S3 bucket policy
CloudFront will provide you with the policy statement after creating the distribution.
Add custom header - optional
CloudFront includes this header in all requests that it sends to your origin.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
28°C Mostly cloudy
11:45 PM
5/19/2025


https://us-east-1.console.aws.amazon.com/cloudfront/v4/home?region=us-east-1#/distributions/create
CloudFront > Distributions > Create
Path pattern | Info
Default (*)
Compress objects automatically | Info
No
Yes
Viewer
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
Restrict viewer access
If you restrict viewer access, viewers must use CloudFront signed URLs or signed cookies to access your content.
No
Yes
Cache key and origin requests
We recommend using a cache policy and origin request policy to control the cache key and origin requests.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
28°C Mostly cloudy
11:45 PM
5/19/2025

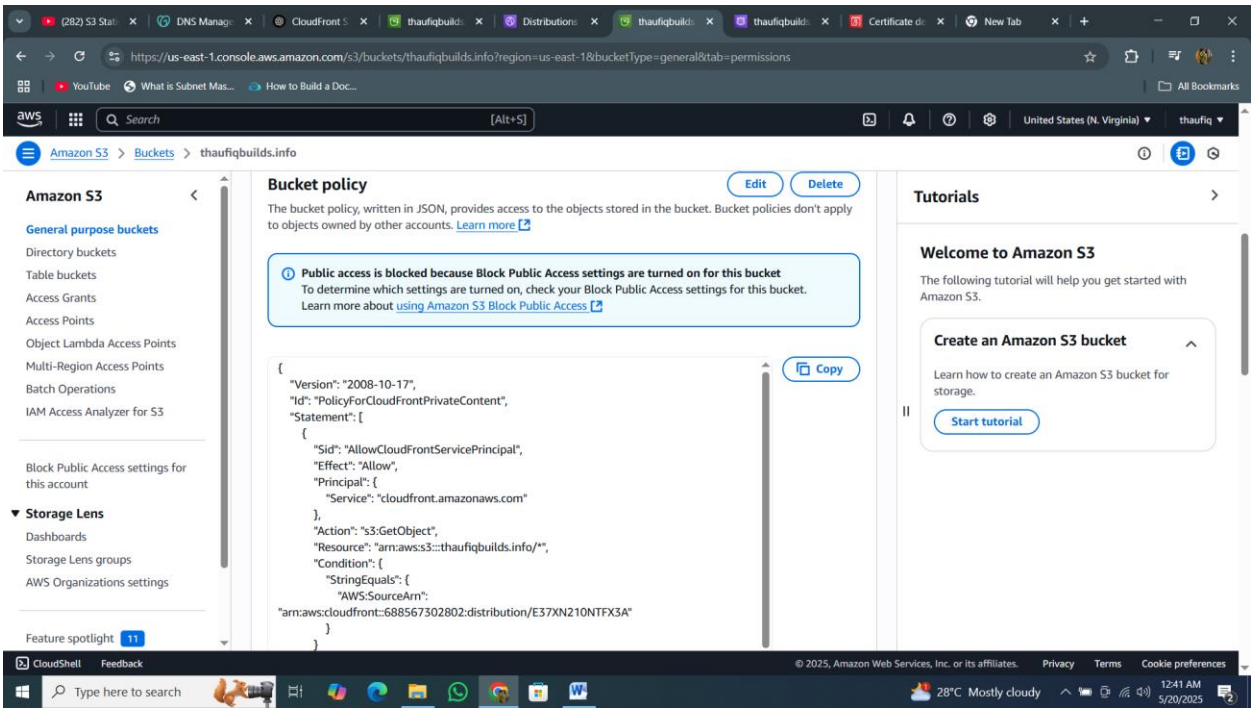

https://us-east-1.console.aws.amazon.com/cloudfront/v4/home?region=us-east-1#/distributions/create
CloudFront > Distributions > Create
Use only North America and Europe
Use North America, Europe, Asia, Middle East, and Africa
Alternate domain name (CNAME) - optional
Add the custom domain names that you use in URLs for the files served by this distribution.
Add item
To add a list of alternative domain names, use the bulk editor.
Custom SSL certificate - optional
Associate a certificate from AWS Certificate Manager. The certificate must be in the US East (N. Virginia) Region (us-east-1).
thaufiqbuilds.info (84b58563-a718-4152-a611-8a92ebaf888d)
thaufiqbuilds.info
Request certificate
Legacy clients support - $600/month prorated charge applies. Most customers do not need this.
CloudFront allocates dedicated IP addresses at each CloudFront edge location to serve your content over HTTPS.
Enabled
Security policy
The security policy determines the SSL or TLS protocol and the specific ciphers that CloudFront uses for HTTPS connections with viewers (clients).
TLSv1.2_2021 (recommended)
TLSv1.2_2019
TLSv1.2_2018
TLSv1.1_2016
TLSv1_2016
TLSv1
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
28°C Mostly cloudy
11:45 PM
5/19/2025


https://us-east-1.console.aws.amazon.com/cloudfront/v4/home?region=us-east-1#/distributions/E1O8HRE2FO661Z/edit
CloudFront > Distributions > E1O8HRE2FO661Z > Edit settings
TLSv1.2_2021 (recommended)
TLSv1.2_2019
TLSv1.2_2018
TLSv1.1_2016
TLSv1_2016
TLSv1
Supported HTTP versions
Add support for additional HTTP versions. HTTP/1.0 and HTTP/1.1 are supported by default
HTTP/2
HTTP/3
Default root object - optional
The object (file name) to return when a viewer requests the root URL (/) instead of a specific object.
index.html
IPv6
Off
On
Description - optional
Cancel
Save changes
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
28°C Mostly cloudy
12:00 AM
5/20/2025





Copy the bucket policy and edit the bucket policy

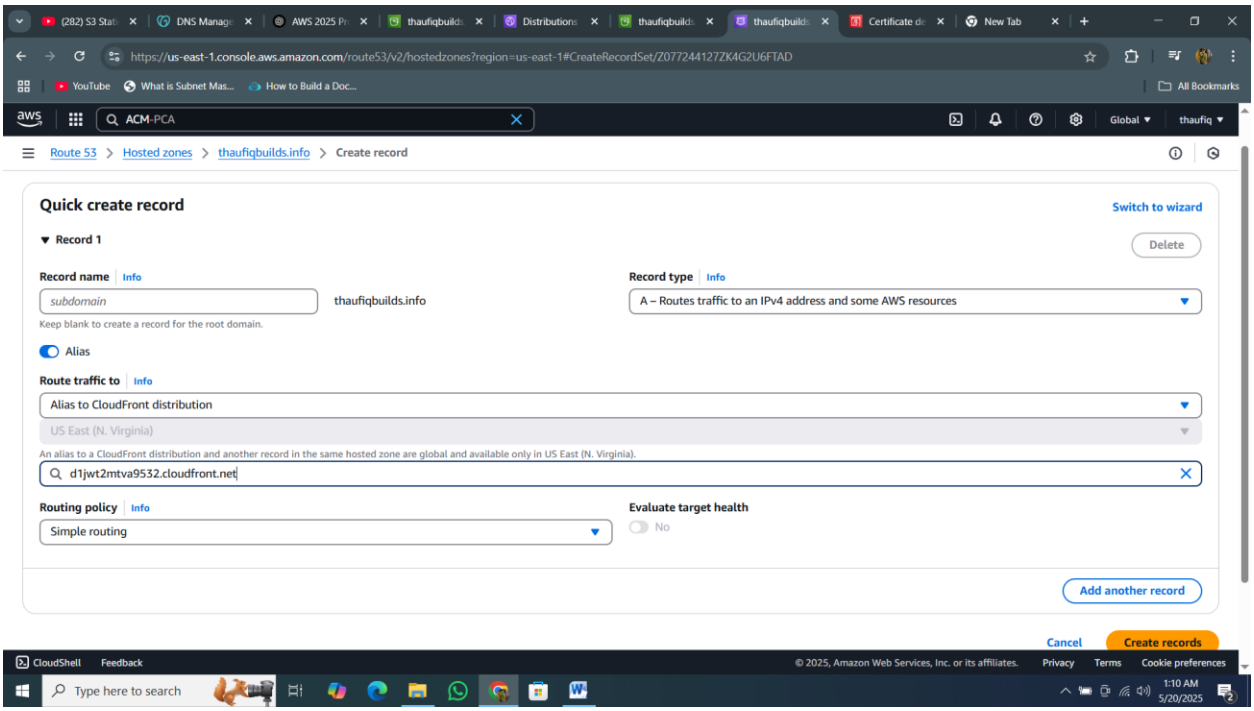


-

Step 6: Point Domain to CloudFront in Route 53

Service: Route 53

1. Go to Hosted Zone → `thaufiqbuilds.info`
2. Click **Create Record**
   - Record type: A (IPv4)
   - Alias: Yes
   - Alias target: Select your **CloudFront distribution**
3. Save



Step 7: Add AWS WAF (Web Application Firewall)

1. Go to WAF

- Open AWS Console → Search **"WAF & Shield"** → Open it.

2. Create Web ACL

- Click **"Web ACLs"** on the left → Click **"Create web ACL"**.

3. Web ACL Settings

- **Name:** `S3Website-WAF`
- **Region:** □ Select **CloudFront (Global)** (important — WAF for CloudFront is global).
- **Resource type:** Leave as default.
- Click **Next**.

4. Add Rules (you can customize later)

You can:

- Add **Managed Rules** (recommended):
  - Click **Add managed rule groups** → Choose:
    - `AWS-AWSManagedRulesCommonRuleSet` (blocks known bad requests)
    - `AWS-AWSManagedRulesAmazonIpReputationList`
  - Click **Add rule groups**.
- You can also add your own custom rules later (for IP blocking, geo restrictions, etc.).

Click **Next**.

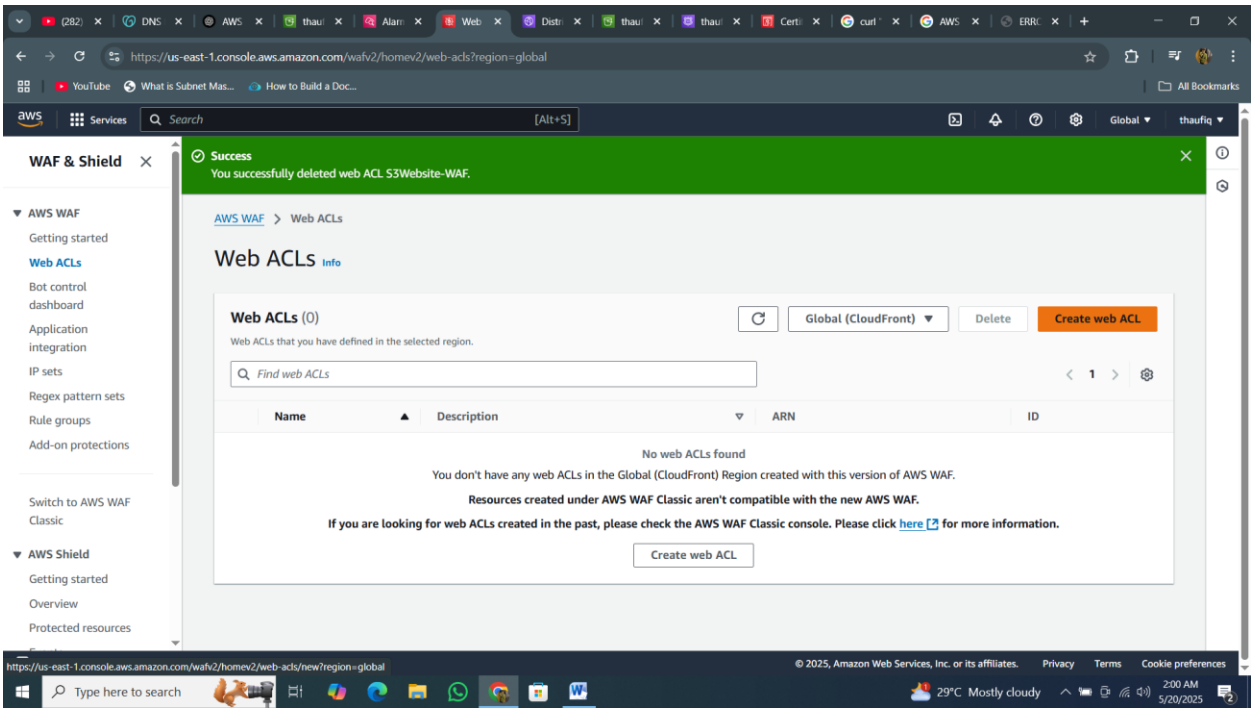
5. Default Action

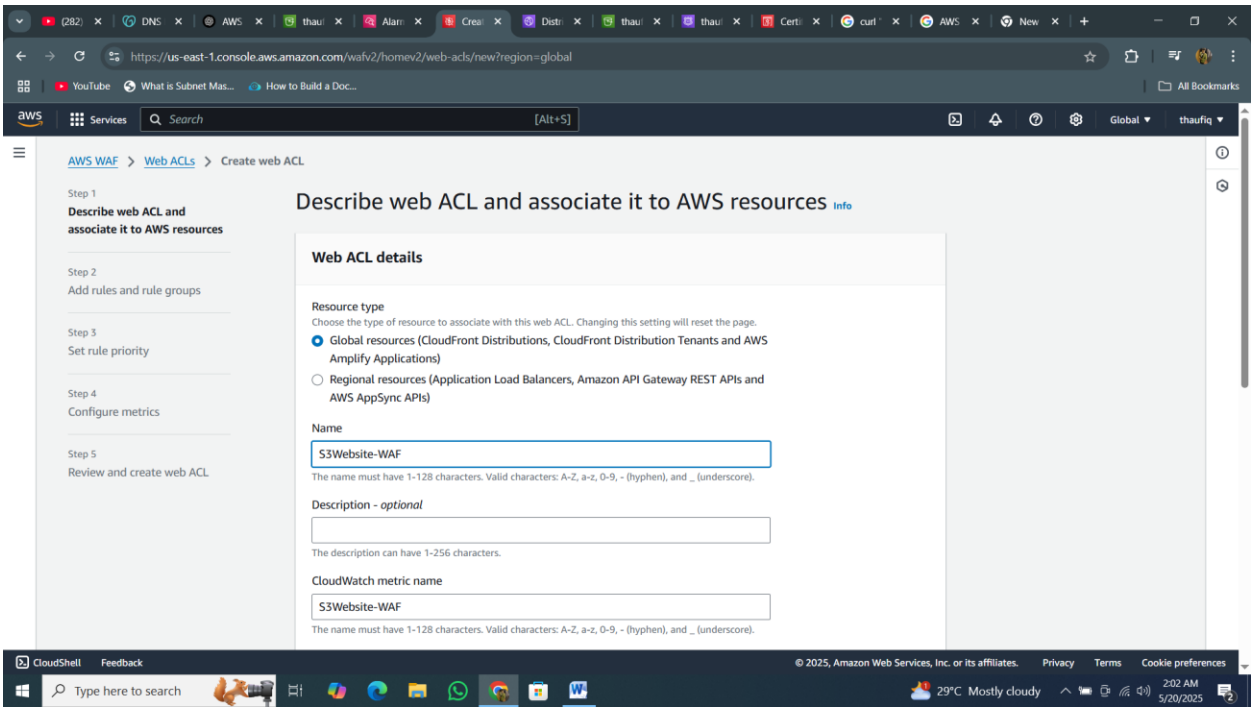
- Choose: `Allow` (block only if rules match).

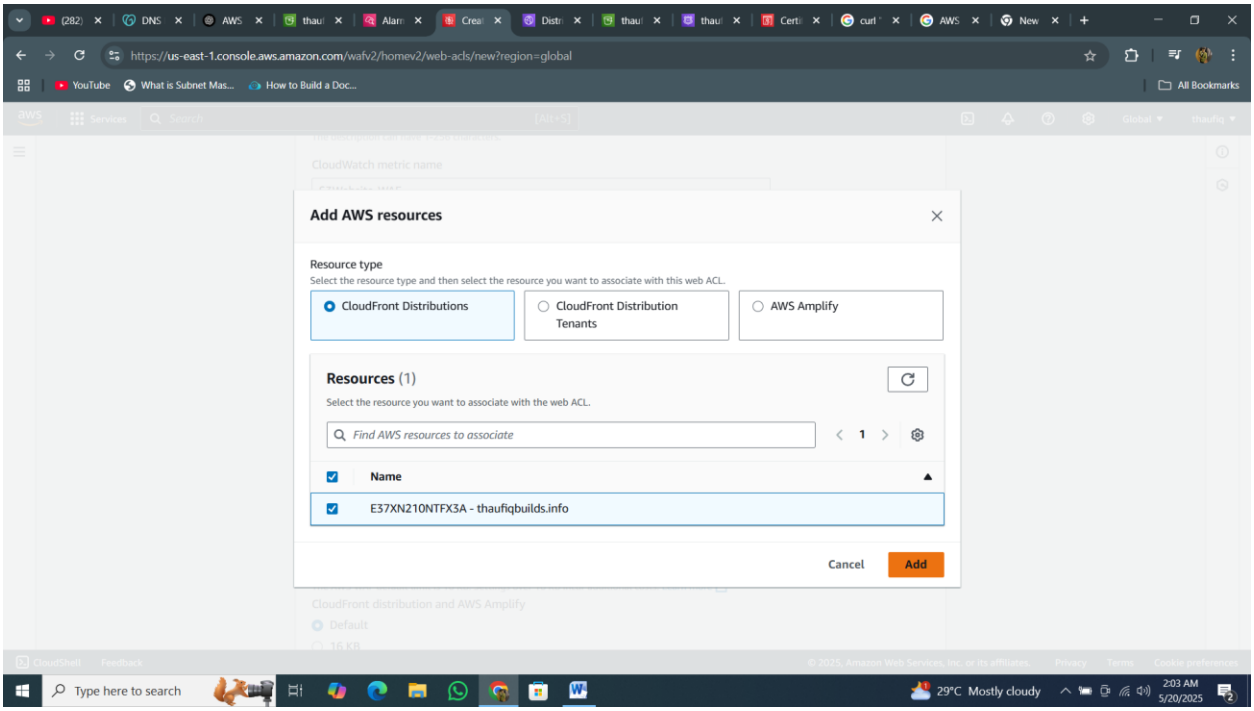
6. Logging & Metrics (Optional)

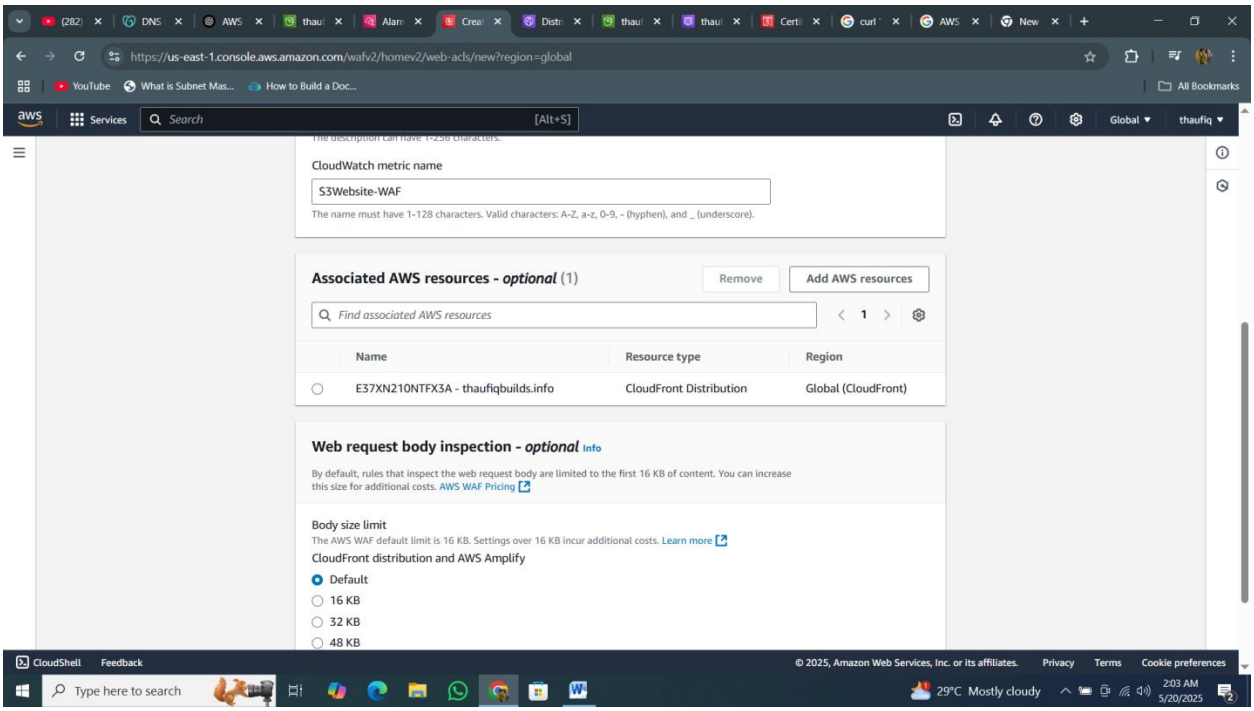
- You can enable logging to an S3 bucket or CloudWatch logs (recommended for production).

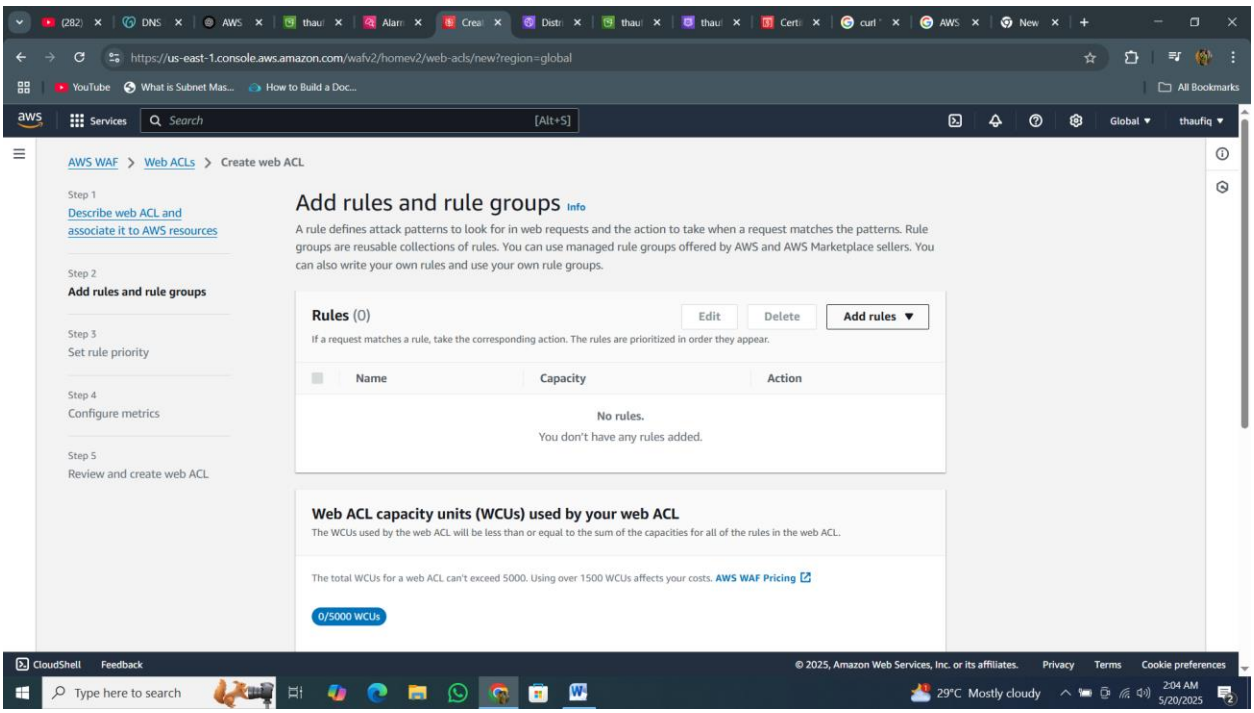
Click **Next**.

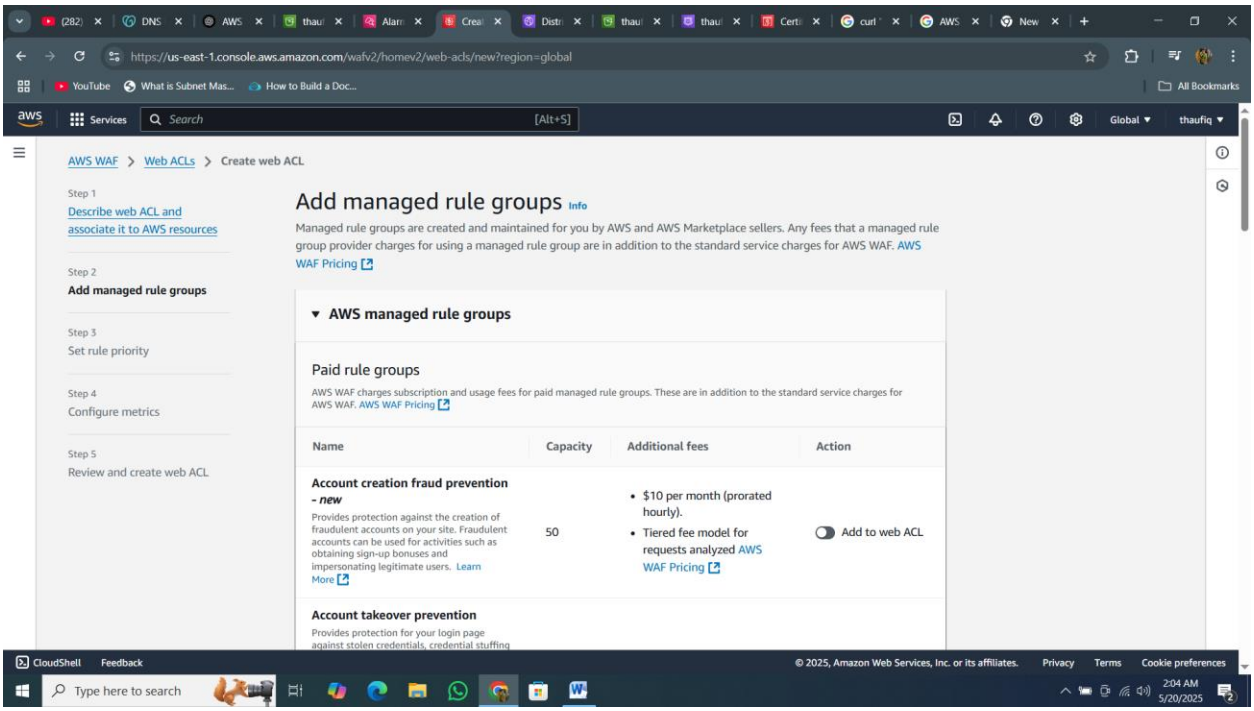


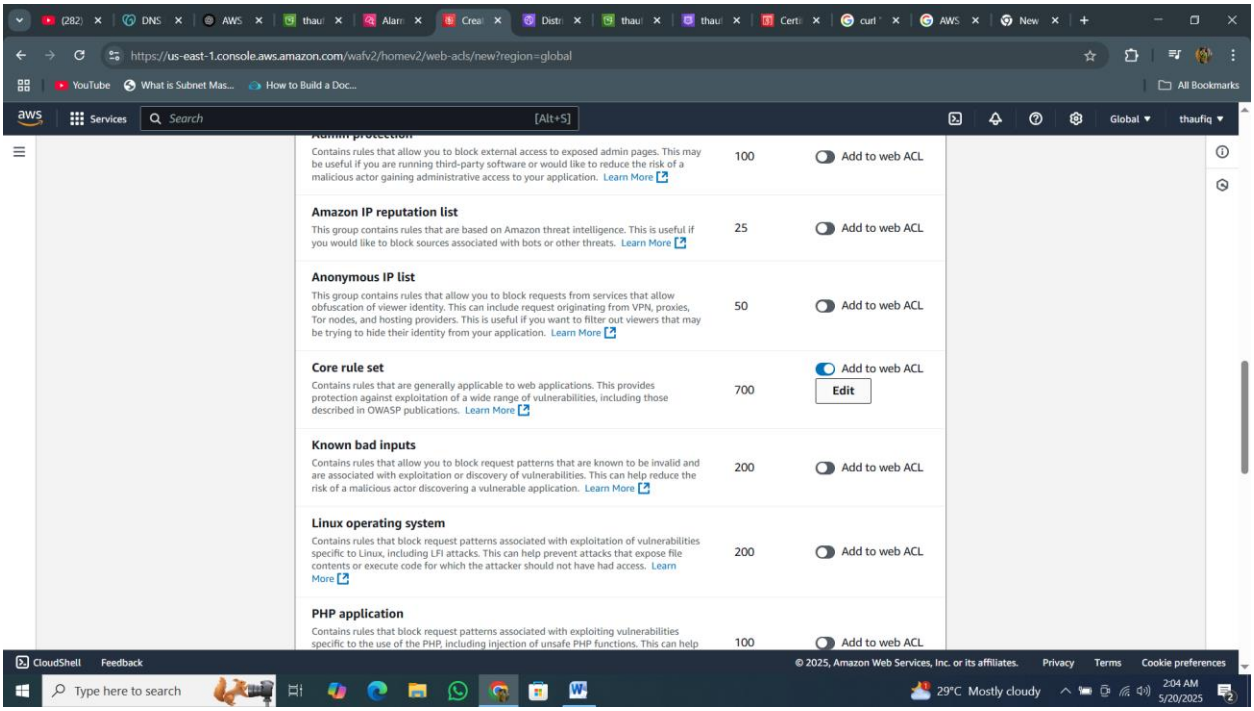

https://us-east-1.console.aws.amazon.com/wafv2/homev2/web-acls/new?region=global
AWS WAF > Web ACLs > Create web ACL
Step 1
Describe web ACL and associate it to AWS resources
Step 2
Add rules and rule groups
Step 3
Set rule priority
Step 4
Configure metrics
Step 5
Review and create web ACL
Describe web ACL and associate it to AWS resources Info
Web ACL details
Resource type
Choose the type of resource to associate with this web ACL. Changing this setting will reset the page.
Global resources (CloudFront Distributions, CloudFront Distribution Tenants and AWS Amplify Applications)
Regional resources (Application Load Balancers, Amazon API Gateway REST APIs and AWS AppSync APIs)
Name
S3Website-WAF
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).
Description - optional
The description can have 1-256 characters.
CloudWatch metric name
S3Website-WAF
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
29°C Mostly cloudy
2:02 AM
5/20/2025

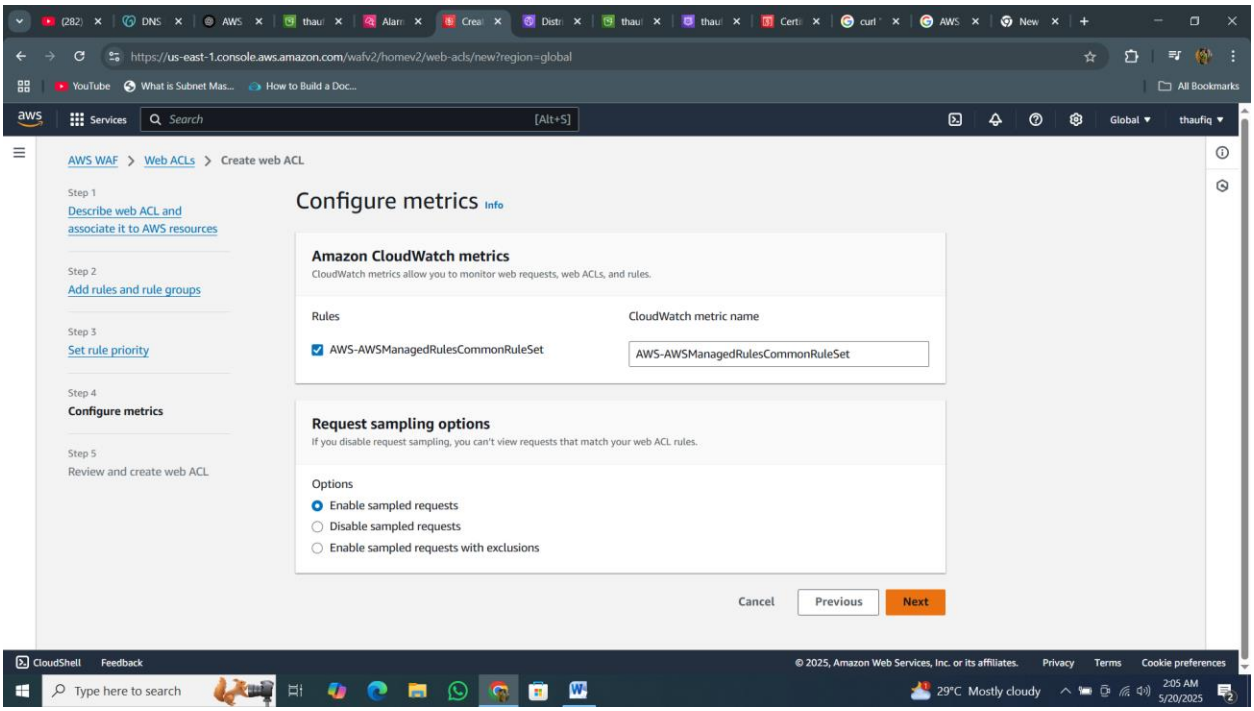

https://us-east-1.console.aws.amazon.com/wafv2/homev2/web-acls/new?region=global
Add AWS resources
Resource type
Select the resource type and then select the resource you want to associate with this web ACL.
CloudFront Distributions
CloudFront Distribution Tenants
AWS Amplify
Resources (1)
Select the resource you want to associate with the web ACL.
Find AWS resources to associate
Name
E37XN210NTFX3A - thaufiqbuilds.info
Cancel
Add
Type here to search
29°C Mostly cloudy
2:03 AM
5/20/2025

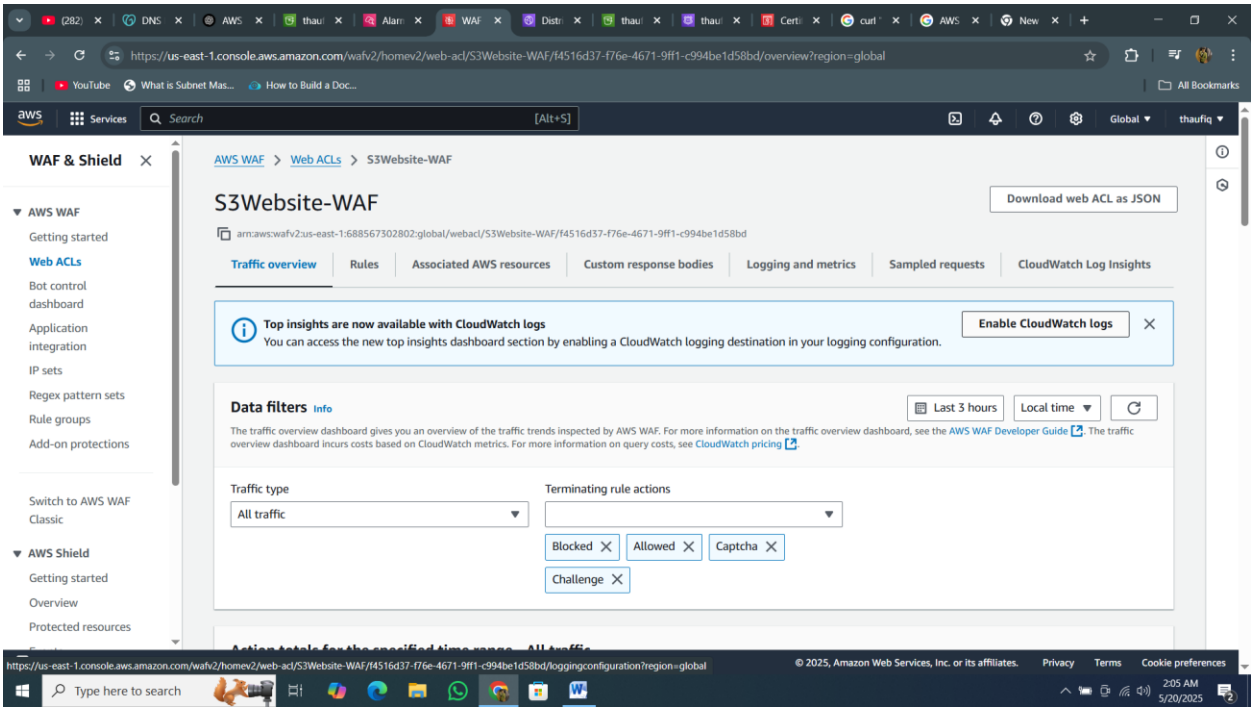

https://us-east-1.console.aws.amazon.com/wafv2/homev2/web-acls/new?region=global
CloudWatch metric name
S3Website-WAF
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).
Associated AWS resources - optional (1)
Remove
Add AWS resources
Find associated AWS resources
Name
Resource type
Region
E37XN210NTFX3A - thaufiqbuilds.info
CloudFront Distribution
Global (CloudFront)
Web request body inspection - optional Info
By default, rules that inspect the web request body are limited to the first 16 KB of content. You can increase this size for additional costs. AWS WAF Pricing
Body size limit
The AWS WAF default limit is 16 KB. Settings over 16 KB incur additional costs. Learn more
CloudFront distribution and AWS Amplify
Default
16 KB
32 KB
48 KB
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
29°C Mostly cloudy
2:03 AM
5/20/2025

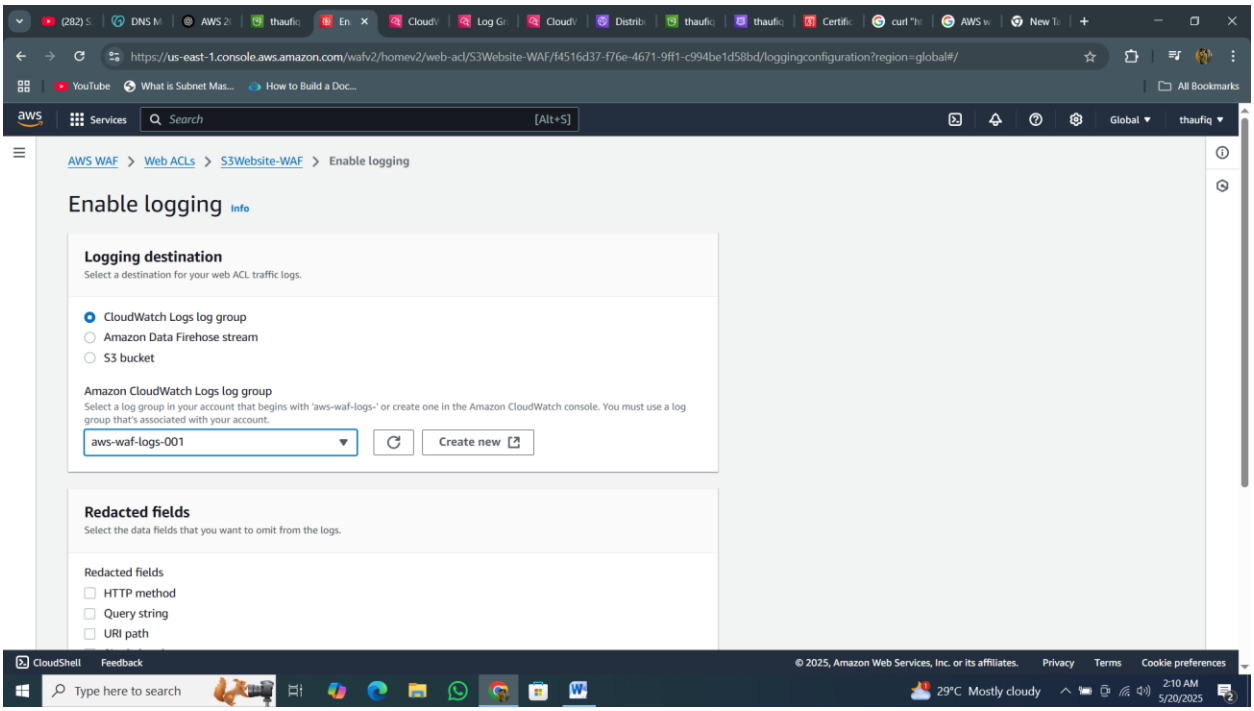

https://us-east-1.console.aws.amazon.com/wafv2/homev2/web-acls/new?region=global
AWS WAF > Web ACLs > Create web ACL
Step 1
Describe web ACL and associate it to AWS resources
Step 2
Add rules and rule groups
Step 3
Set rule priority
Step 4
Configure metrics
Step 5
Review and create web ACL
Add rules and rule groups Info
A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.
Rules (0)
Edit
Delete
Add rules
If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.
Name
Capacity
Action
No rules.
You don't have any rules added.
Web ACL capacity units (WCUs) used by your web ACL
The WCUs used by the web ACL will be less than or equal to the sum of the capacities for all of the rules in the web ACL.
The total WCUs for a web ACL can't exceed 5000. Using over 1500 WCUs affects your costs. AWS WAF Pricing
0/5000 WCUs
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
29°C Mostly cloudy
2:04 AM
5/20/2025

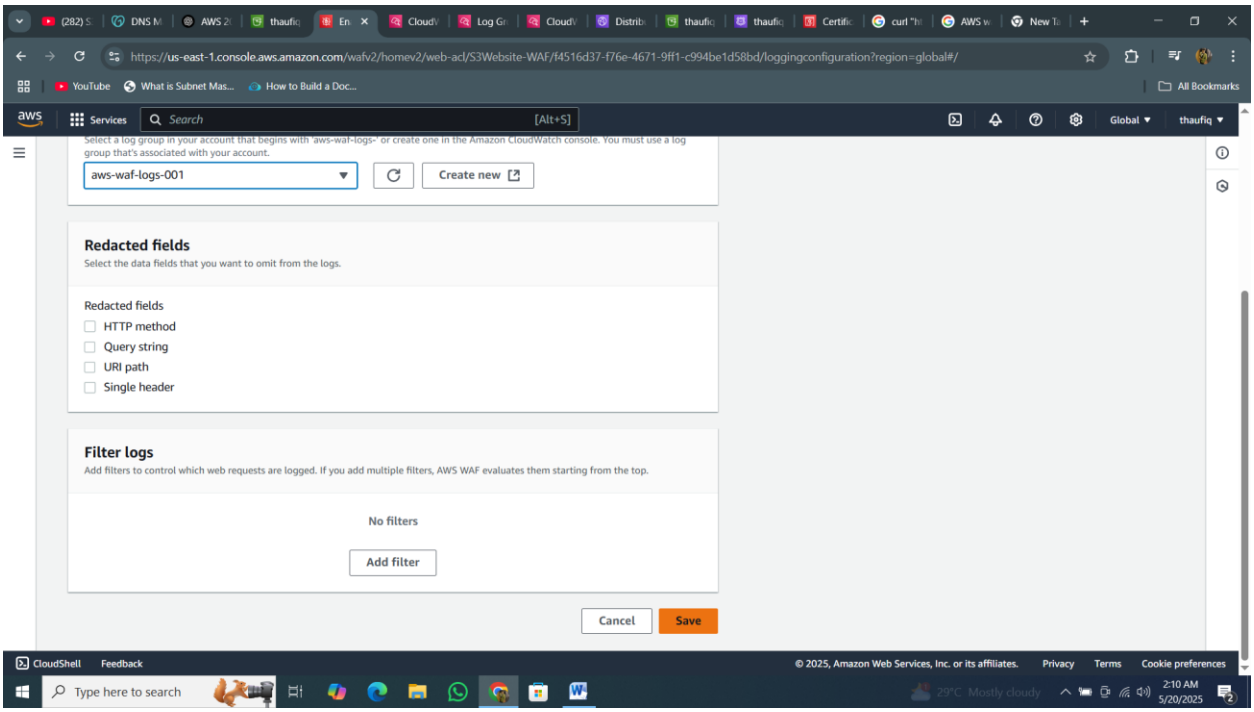

https://us-east-1.console.aws.amazon.com/wafv2/homev2/web-acls/new?region=global
AWS WAF > Web ACLs > Create web ACL
Step 1
Describe web ACL and associate it to AWS resources
Step 2
Add managed rule groups
Step 3
Set rule priority
Step 4
Configure metrics
Step 5
Review and create web ACL
Add managed rule groups Info
Managed rule groups are created and maintained for you by AWS and AWS Marketplace sellers. Any fees that a managed rule group provider charges for using a managed rule group are in addition to the standard service charges for AWS WAF. AWS WAF Pricing
AWS managed rule groups
Paid rule groups
AWS WAF charges subscription and usage fees for paid managed rule groups. These are in addition to the standard service charges for AWS WAF. AWS WAF Pricing
Name
Capacity
Additional fees
Action
Account creation fraud prevention - new
Provides protection against the creation of fraudulent accounts on your site. Fraudulent accounts can be used for activities such as obtaining sign-up bonuses and impersonating legitimate users. Learn More
50
$10 per month (prorated hourly).
Tiered fee model for requests analyzed AWS WAF Pricing
Add to web ACL
Account takeover prevention
Provides protection for your login page against stolen credentials, credential stuffing
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
2:04 AM
5/20/2025


https://us-east-1.console.aws.amazon.com/wafv2/homev2/web-acls/new?region=global
Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application. Learn More
100
Add to web ACL
Amazon IP reputation list
This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats. Learn More
25
Add to web ACL
Anonymous IP list
This group contains rules that allow you to block requests from services that allow obfuscation of viewer identity. This can include request originating from VPN, proxies, Tor nodes, and hosting providers. This is useful if you want to filter out viewers that may be trying to hide their identity from your application. Learn More
50
Add to web ACL
Core rule set
Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications. Learn More
700
Add to web ACL
Edit
Known bad inputs
Contains rules that allow you to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application. Learn More
200
Add to web ACL
Linux operating system
Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access. Learn More
200
Add to web ACL
PHP application
Contains rules that block request patterns associated with exploiting vulnerabilities specific to the use of the PHP, including injection of unsafe PHP functions. This can help
100
Add to web ACL
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
29°C Mostly cloudy
2:04 AM
5/20/2025


https://us-east-1.console.aws.amazon.com/wafv2/homev2/web-acls/new?region=global
Search
[Alt+S]
Global
thaufiq
AWS WAF > Web ACLs > Create web ACL
Step 1
Describe web ACL and associate it to AWS resources
Step 2
Add rules and rule groups
Step 3
Set rule priority
Step 4
Configure metrics
Step 5
Review and create web ACL
Configure metrics Info
Amazon CloudWatch metrics
CloudWatch metrics allow you to monitor web requests, web ACLs, and rules.
Rules
CloudWatch metric name
AWS-AWSManagedRulesCommonRuleSet
AWS-AWSManagedRulesCommonRuleSet
Request sampling options
If you disable request sampling, you can't view requests that match your web ACL rules.
Options
Enable sampled requests
Disable sampled requests
Enable sampled requests with exclusions
Cancel
Previous
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
29°C Mostly cloudy
2:05 AM
5/20/2025


https://us-east-1.console.aws.amazon.com/wafv2/homev2/web-acl/S3Website-WAF/f4516d37-f76e-4671-9ff1-c994be1d58bd/overview?region=global
WAF & Shield
AWS WAF
Getting started
Web ACLs
Bot control dashboard
Application integration
IP sets
Regex pattern sets
Rule groups
Add-on protections
Switch to AWS WAF Classic
AWS Shield
Getting started
Overview
Protected resources
AWS WAF > Web ACLs > S3Website-WAF
S3Website-WAF
Download web ACL as JSON
arn:aws:wafv2:us-east-1:688567302802:global/webacl/S3Website-WAF/f4516d37-f76e-4671-9ff1-c994be1d58bd
Traffic overview
Rules
Associated AWS resources
Custom response bodies
Logging and metrics
Sampled requests
CloudWatch Log Insights
Top insights are now available with CloudWatch logs
You can access the new top insights dashboard section by enabling a CloudWatch logging destination in your logging configuration.
Enable CloudWatch logs
Data filters Info
Last 3 hours
Local time
The traffic overview dashboard gives you an overview of the traffic trends inspected by AWS WAF. For more information on the traffic overview dashboard, see the AWS WAF Developer Guide. The traffic overview dashboard incurs costs based on CloudWatch metrics. For more information on query costs, see CloudWatch pricing.
Traffic type
All traffic
Terminating rule actions
Blocked
Allowed
Captcha
Challenge
https://us-east-1.console.aws.amazon.com/wafv2/homev2/web-acl/S3Website-WAF/f4516d37-f76e-4671-9ff1-c994be1d58bd/loggingconfiguration?region=global
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
2:05 AM
5/20/2025


https://us-east-1.console.aws.amazon.com/wafv2/homev2/web-acl/S3Website-WAF/f4516d37-f76e-4671-9ff1-c994be1d58bd/loggingconfiguration?region=global#/
Services
Search
[Alt+S]
Global
thaufiq
AWS WAF > Web ACLs > S3Website-WAF > Enable logging
Enable logging Info
Logging destination
Select a destination for your web ACL traffic logs.
CloudWatch Logs log group
Amazon Data Firehose stream
S3 bucket
Amazon CloudWatch Logs log group
Select a log group in your account that begins with 'aws-waf-logs-' or create one in the Amazon CloudWatch console. You must use a log group that's associated with your account.
aws-waf-logs-001
Create new
Redacted fields
Select the data fields that you want to omit from the logs.
Redacted fields
HTTP method
Query string
URI path
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
29°C Mostly cloudy
2:10 AM
5/20/2025


https://us-east-1.console.aws.amazon.com/wafv2/homev2/web-acl/S3Website-WAF/f4516d37-f76e-4671-9ff1-c994be1d58bd/loggingconfiguration?region=global#/
Services
Search
[Alt+S]
Global
thaufiq
aws-waf-logs-001
Create new
Redacted fields
Select the data fields that you want to omit from the logs.
Redacted fields
HTTP method
Query string
URI path
Single header
Filter logs
Add filters to control which web requests are logged. If you add multiple filters, AWS WAF evaluates them starting from the top.
No filters
Add filter
Cancel
Save
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
2:10 AM
5/20/2025

Click save

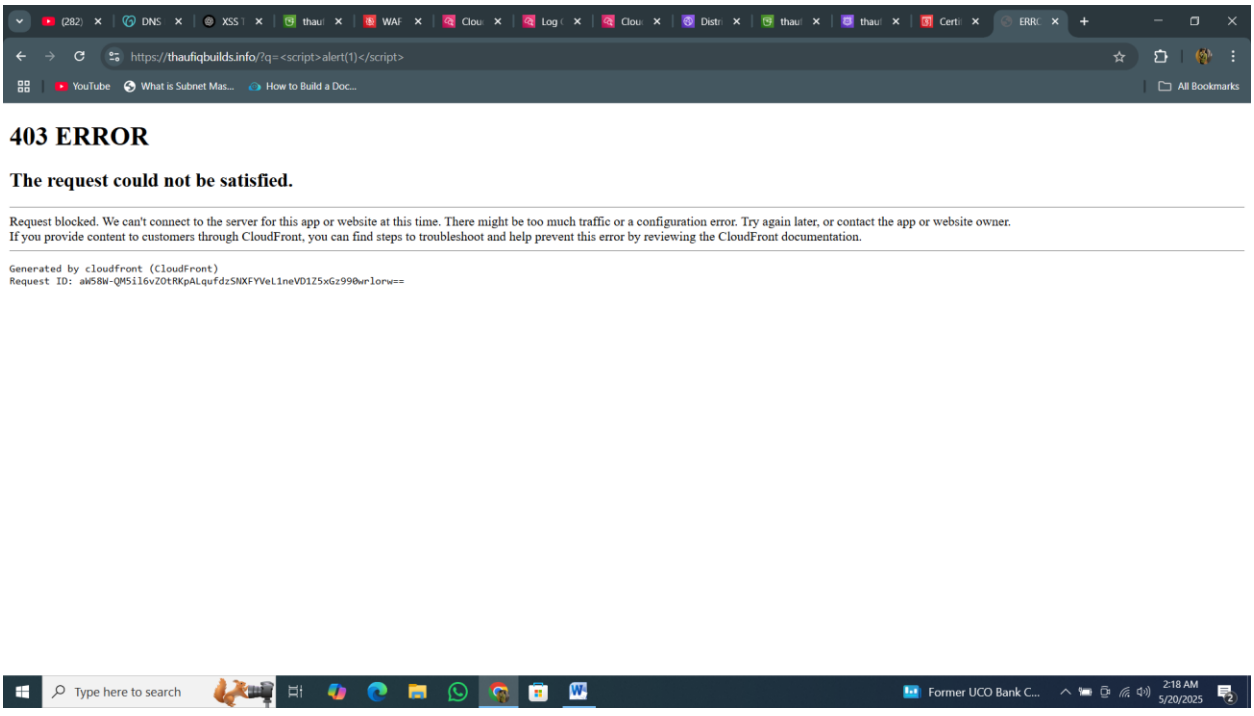
Core Rule Set (CRS) — ⭐ SELECT THIS

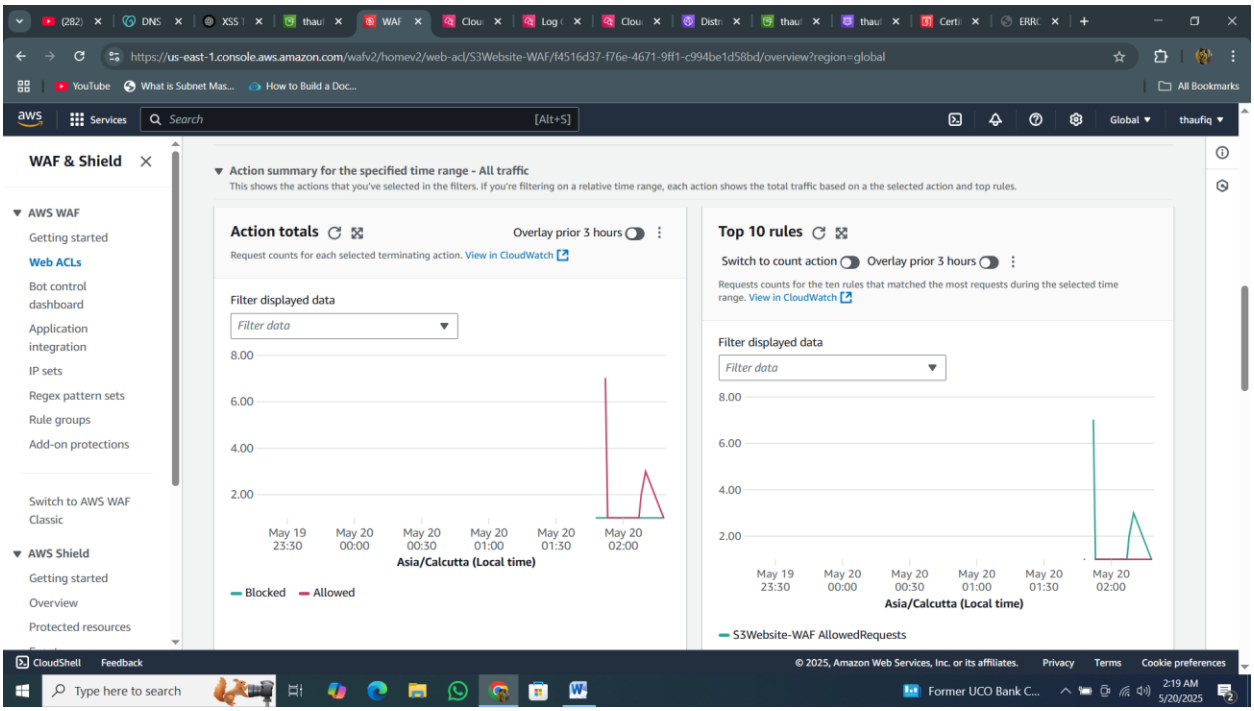
- ✅ Protects against OWASP Top 10 (SQLi, XSS, LFI, etc.).
- ✅ Covers general app-layer threats.
- ✅ **Must-have for all websites**.

Lets test it WAF will block these and return a `403 Forbidden` if it's working correctly ⭐

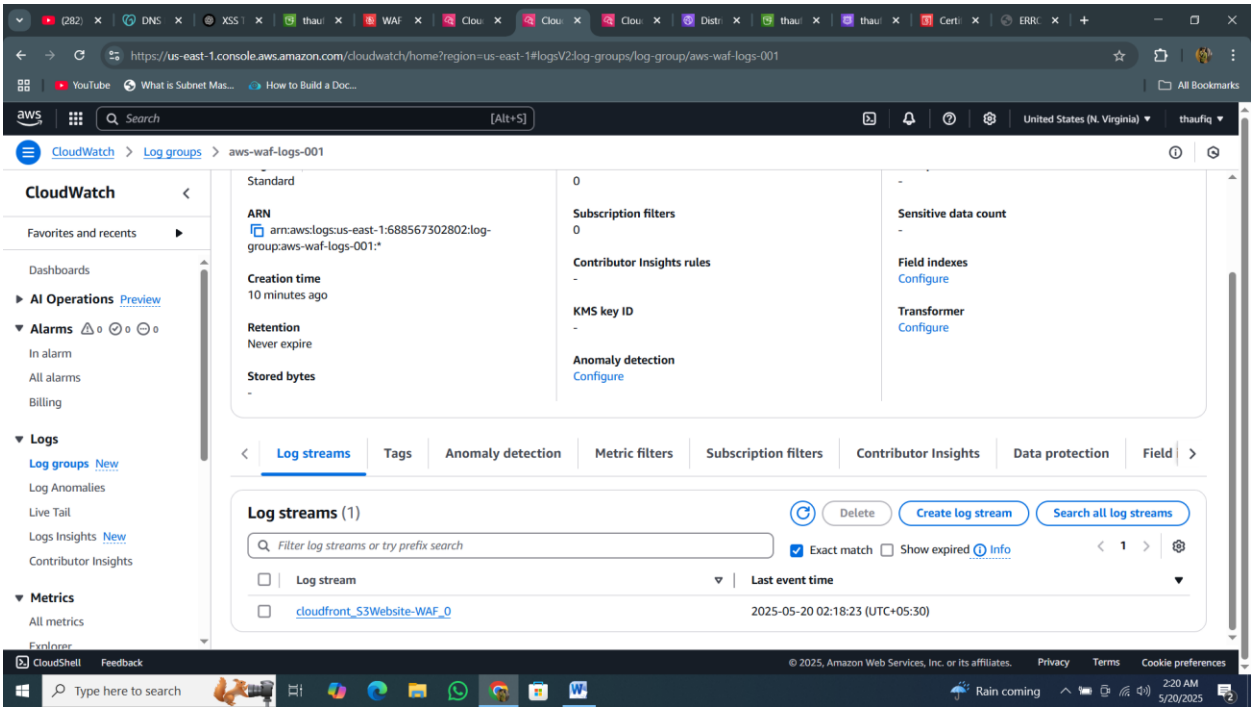
Test pattern

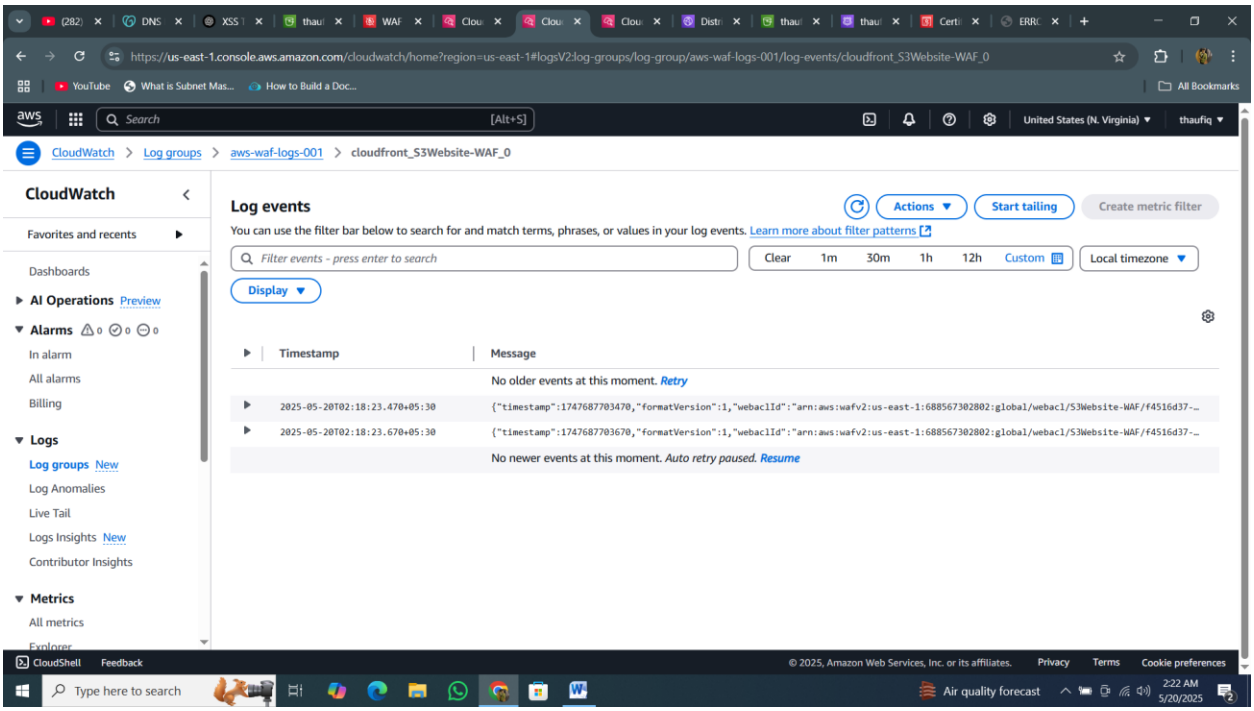
XSS test – Append to URL: https://thaufiqbuilds.info/?q=<script>alert(1)</script>

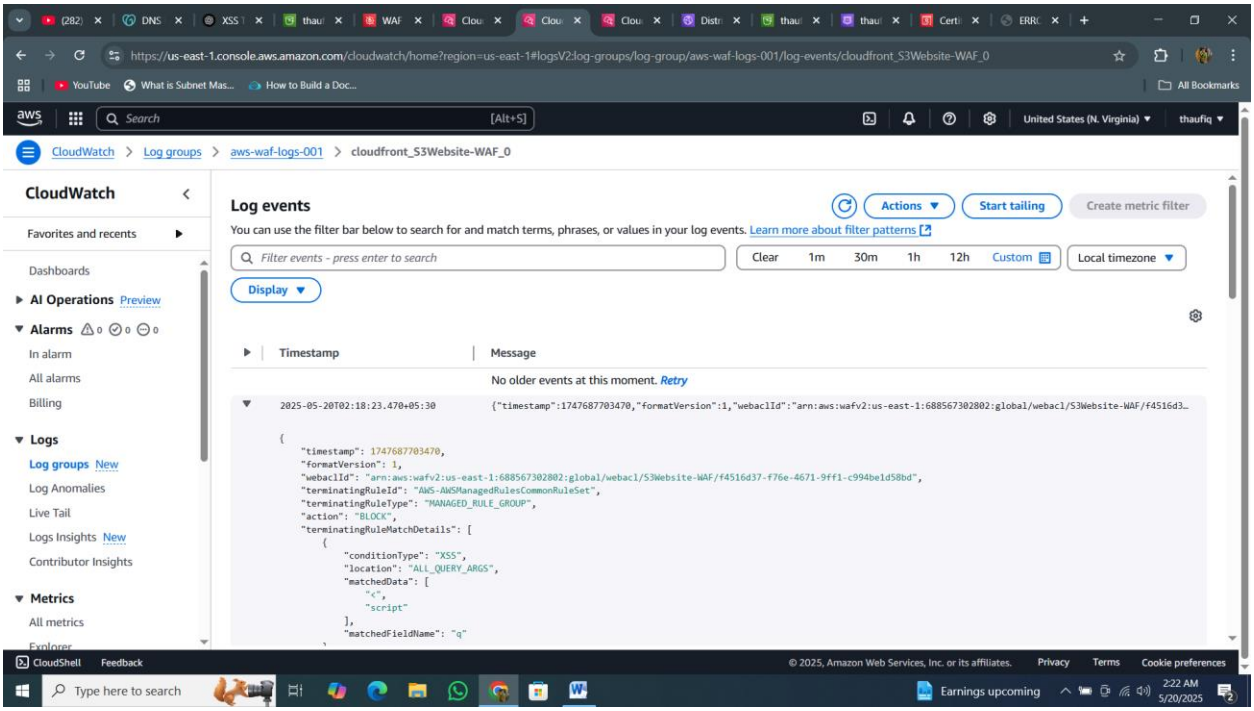




Cloud watch log

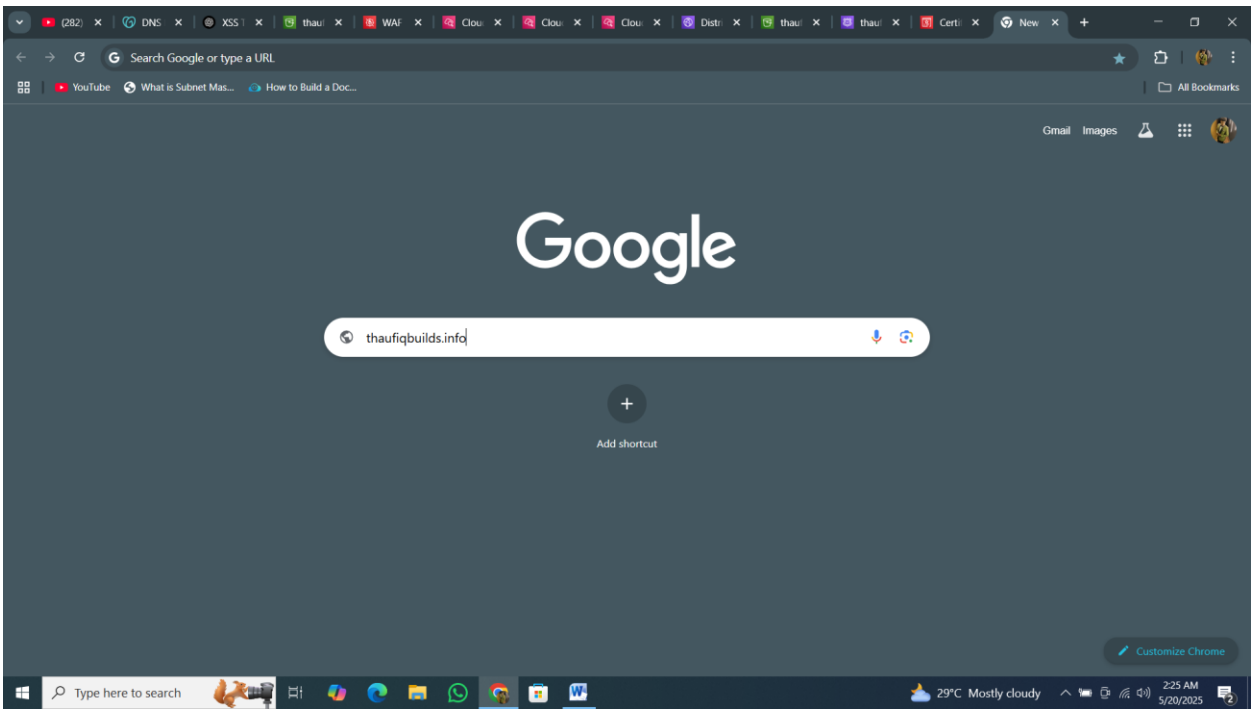


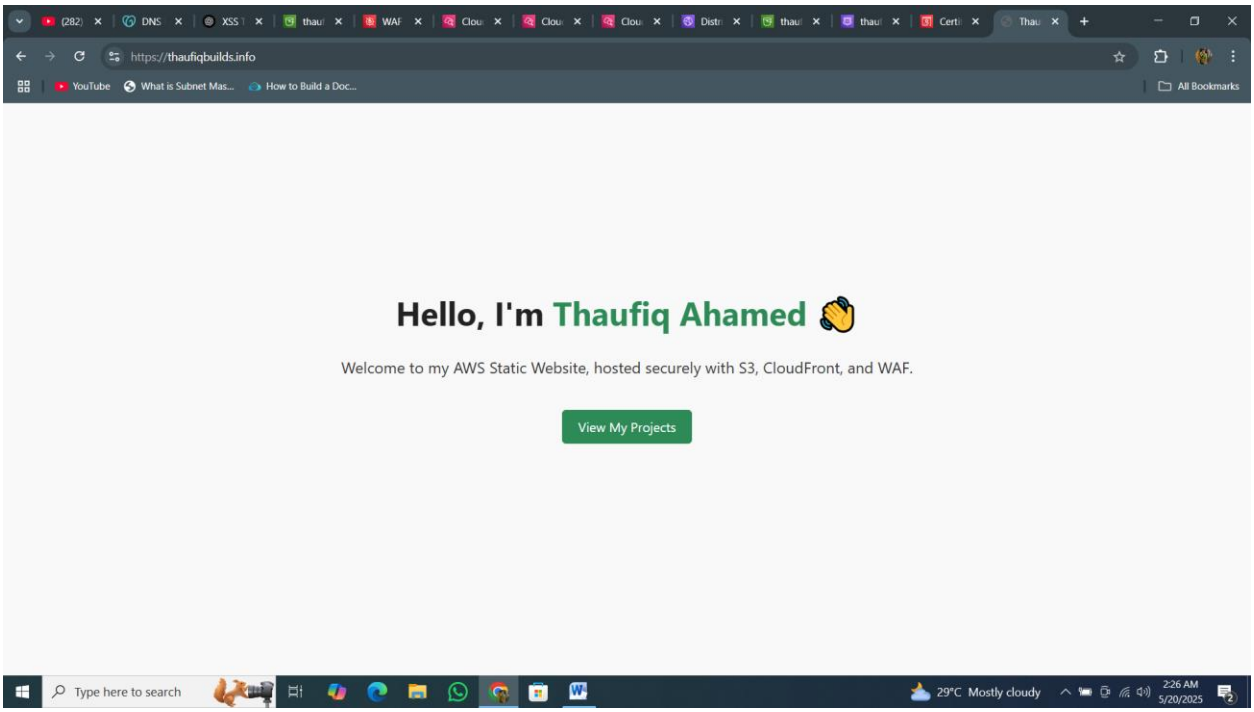


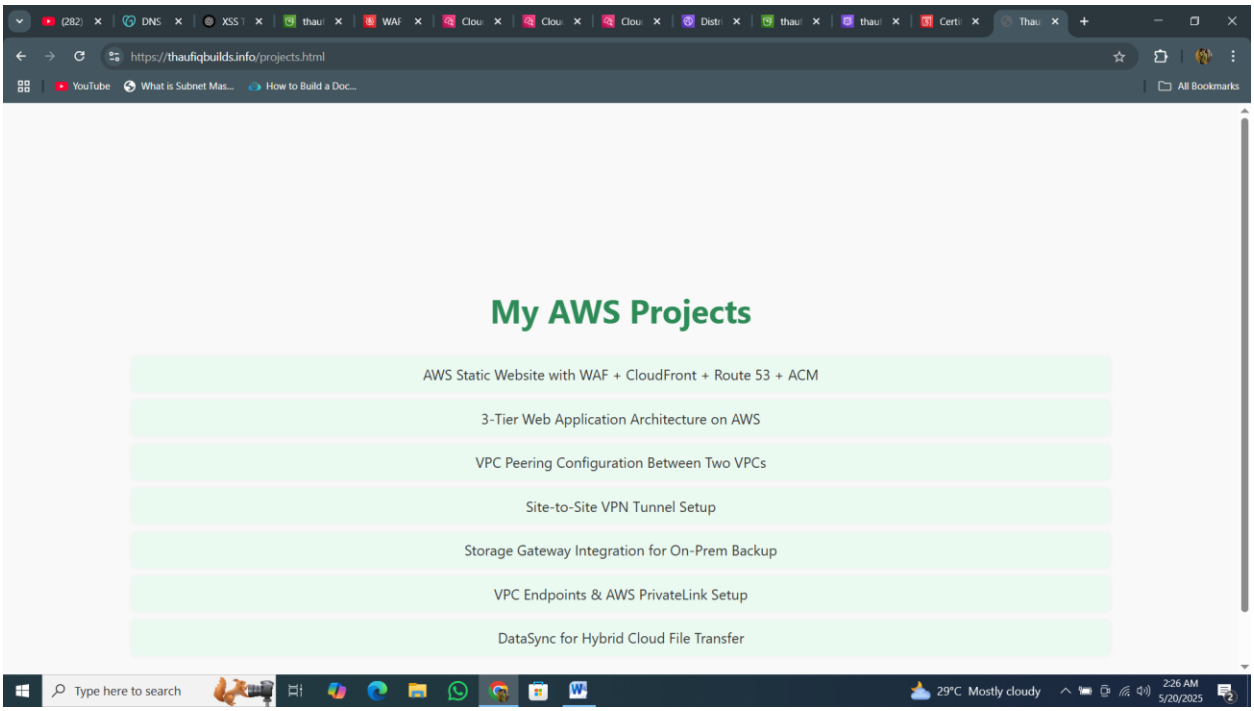


OK done waf it perfectly working

Know we try the normal with your domine we see the https also the brower







Final Result:

You now have:

 A secure, fast, global static site at:
`https://thaufiqbuilds.info`

 Protected with:

- **HTTPS**
- **CDN performance**
- **Custom domain**
- **Web firewall**

Conclusion

This project successfully demonstrates the deployment of a **secure, performant, and highly available static website** using core AWS services. By integrating **Amazon S3**, **Route 53**, **Amazon CloudFront**, **AWS Certificate Manager (ACM)**, and **AWS Web Application Firewall (WAF)**, we have created a modern web hosting architecture that not only delivers content at low latency but also ensures **robust security and domain-level branding**.

Key highlights of this project include:

- **HTTPS-secured access** using ACM-integrated SSL certificates for encrypted communication.

- **Custom domain name** resolution via Route 53 for professional web presence.
- **Global content delivery** powered by CloudFront for reduced latency and caching.
- **WAF protection** using managed rules (like Core Rule Set, IP Reputation, and Anonymous IP List) to block common threats including XSS, injection attempts, and traffic from suspicious IPs.
- **Tested WAF rules** with real-world malicious patterns to confirm rule effectiveness and response.

This architecture follows **AWS Well-Architected Framework** principles, specifically around **security, performance efficiency, and reliability**, making it an ideal choice for hosting modern static websites that require enterprise-grade protection without server-side complexity.