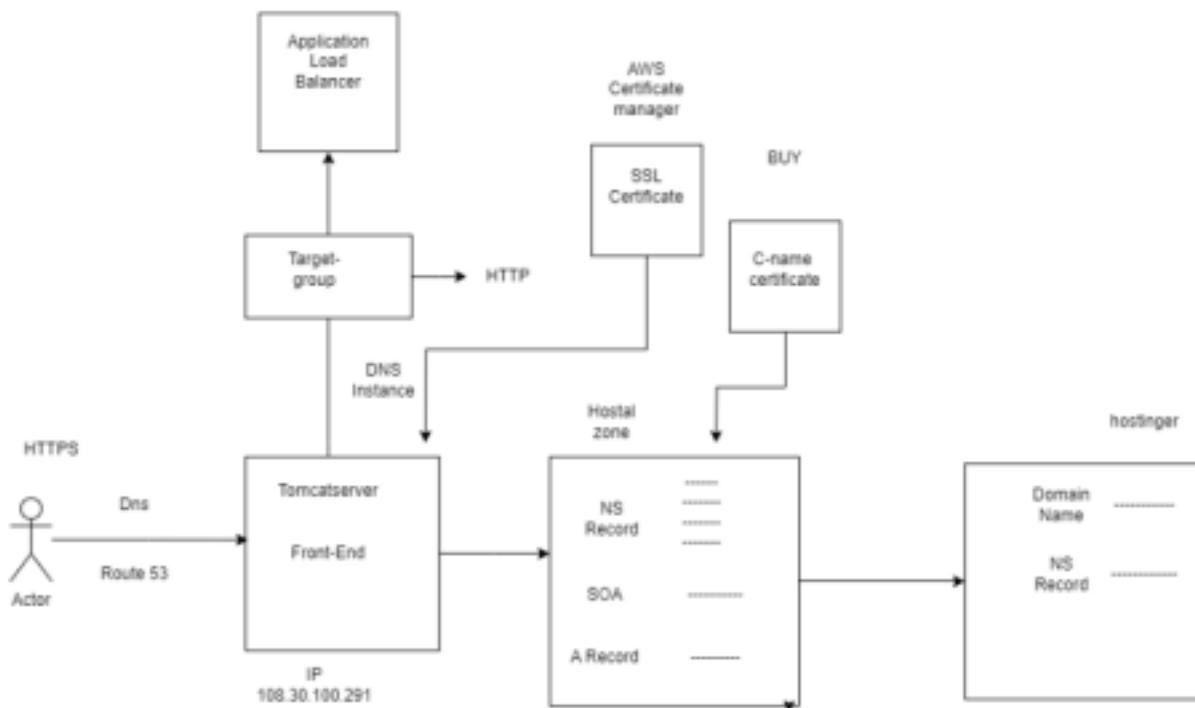


Task: Create Hosted Zone in Route53 ,bind ip with 3rd party Domain provider and make website ssl certified using ACM and Application Load Balancer in AWS.

Diagrammatic Representation:



Step 1: Create an EC2 instance and connect to it using ->

Ssh -i private_rsa_key ec2-user@public_ip

What is an ec2 instance ? → An EC2 instance is a virtual server provided by Amazon Web Services (AWS) that allows users to run applications on the cloud with scalable computing resources. It can be configured with various operating systems, storage options, and network settings to meet specific needs.

The screenshot shows the AWS EC2 Instances page. A green banner at the top indicates "Successfully initiated termination (deletion) of i-0b0fff27d63b52988". Below this, a table lists one instance: "route_task" (Instance ID: i-00007bc333c9db675, Instance state: Running, Instance type: t2.micro, Status check: 2/2 checks passed, Availability Zone: ap-south-1b, Public IPv4 DNS: ec2-65-2-71-251.ap-so..., Public IPv4 address: 65.2.71.251). The sidebar on the left includes sections for EC2 Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), Network & Security (Security Groups, Elastic IPs, Placement Groups), CloudShell, and Feedback.

The screenshot shows a terminal window with the command: "ssh -i seytan.cloud.pem ec2-user@65.2.71.251". The response indicates that the host's fingerprint is being checked: "The authenticity of host '65.2.71.251 (65.2.71.251)' can't be established. ED25519 key fingerprint is SHA256:8XpjYmJ401zd8XTElsAkCBFVL+Dq8ILyyiG72xDIZK. This key is not known by any other names." The user is prompted to continue connecting: "Are you sure you want to continue connecting (yes/no/[fingerprint])? yes_".

Step 2: Now Install the httpd server in our ec2 instance

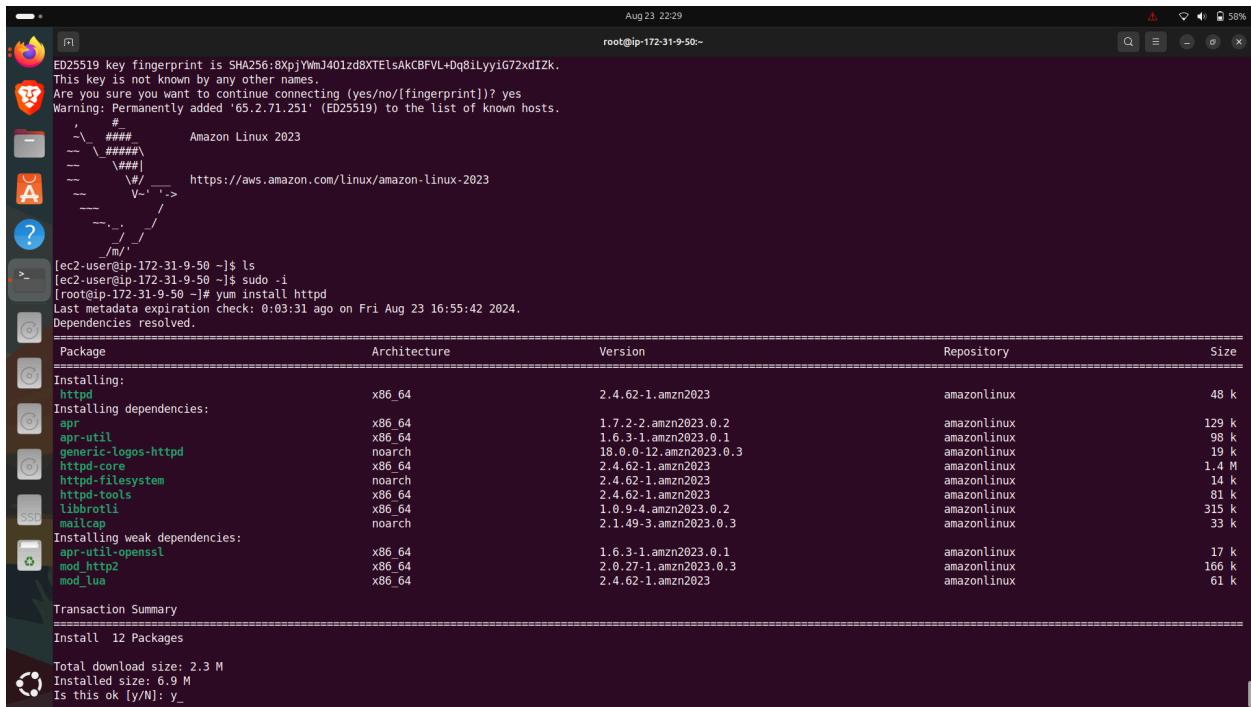
Sudo -i

Yum install httpd -y

What is httpd ?

→httpd is the Apache HTTP Server, an open-source web server software used to serve web pages and applications over the internet. It handles requests from clients (like browsers) and delivers the requested content, often running on Linux-based systems.

Home directory of httpd is -> /var/www/html/

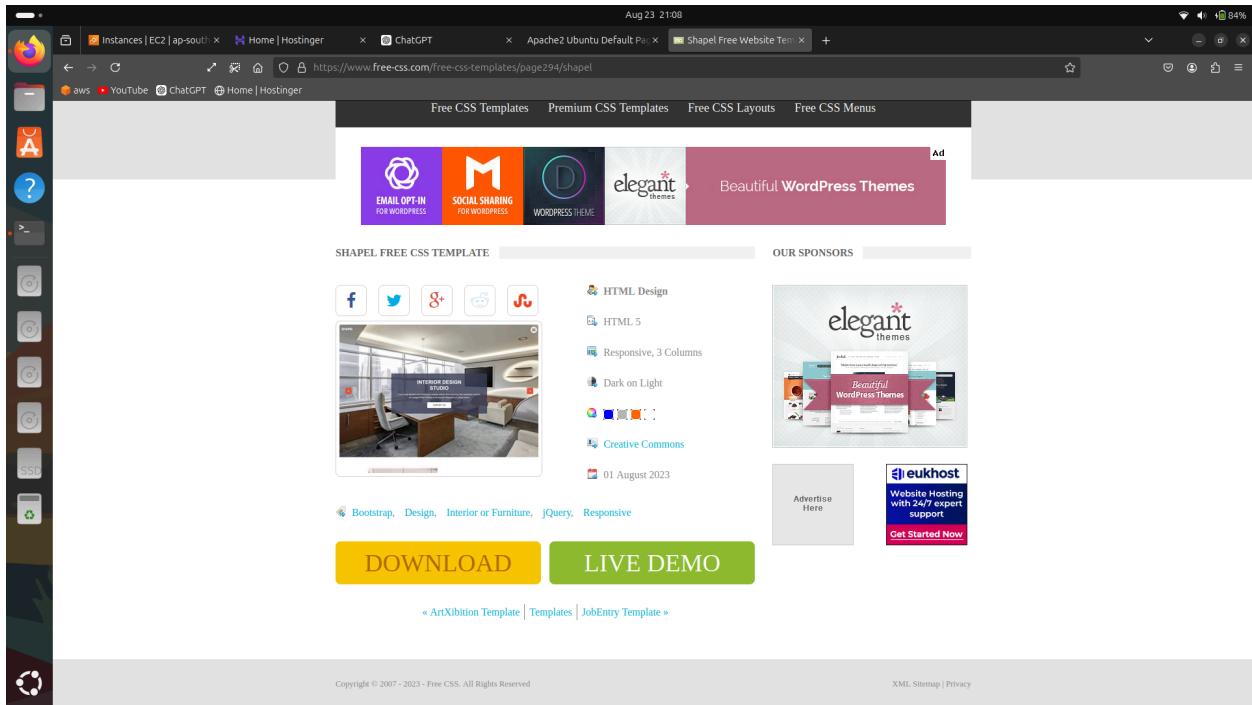


```
Aug 23 22:29
root@ip-172-31-9-50:~#
ED25519 key fingerprint is SHA256:8XpjYWmJ401zd8XTElsAkCBFVL+Dq8iLyyiG72xdIZk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '65.2.71.251' (ED25519) to the list of known hosts.
# 
~~\ #####
~~ \#####
-- \
-- \
\#/
-- \
\#/
https://aws.amazon.com/linux/amazon-linux-2023
-- \
-- \
-- \
\#/
[ec2-user@ip-172-31-9-50 ~]$ ls
[ec2-user@ip-172-31-9-50 ~]$ sudo -i
[root@ip-172-31-9-50 ~]# yum install httpd
Last metadata expiration check: 0:03:31 ago on Fri Aug 23 16:55:42 2024.
Dependencies resolved.
=====
Package           Architecture Version      Repository  Size
=====
Installing:
httpd            x86_64       2.4.62-1.amzn2023 amazonlinux 48 k
Installing dependencies:
apr              x86_64       1.7.2-2.amzn2023.0.2 amazonlinux 129 k
apr-util         x86_64       1.6.3-1.amzn2023.0.1 amazonlinux 98 k
generic-logos-httpd   noarch    18.0.0-12.amzn2023.0.3 amazonlinux 19 k
httpd-core       x86_64       2.4.62-1.amzn2023 amazonlinux 1.4 M
httpd-filesystem noarch    2.4.62-1.amzn2023 amazonlinux 14 k
httpd-tools      x86_64       2.4.62-1.amzn2023 amazonlinux 81 k
libbrotli        x86_64       1.0.9-4.amzn2023.0.2 amazonlinux 315 k
mailcap          noarch    2.1.49-3.amzn2023.0.3 amazonlinux 33 k
Installing weak dependencies:
apr-util-openssl x86_64       1.6.3-1.amzn2023.0.1 amazonlinux 17 k
mod_http2        x86_64       2.0.27-1.amzn2023.0.3 amazonlinux 166 k
mod_lua          x86_64       2.4.62-1.amzn2023 amazonlinux 61 k
Transaction Summary
=====
Install 12 Packages

Total download size: 2.3 M
Installed size: 6.9 M
Is this ok [y/N]: y_
```

Step 3:Now install any free css template to host webpage

Sudo wget url_of_webpage_codes



Extract this file and then copy the sub-files and sub-folder to the home directory of httpd

```
ubuntu@ip-172-31-33-39:~/var/www/html$ sudo wget https://www.free-css.com/assets/files/free-css-templates/download/page294/shapel.zip
--2024-08-23 15:39:40-- https://www.free-css.com/assets/files/free-css-templates/download/page294/shapel.zip
Resolving www.free-css.com (www.free-css.com)... 217.160.0.242, 2001:9db:10ff:ff00::28f
Connecting to www.free-css.com (www.free-css.com)|217.160.0.242|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1390016 (1.3M) [application/zip]
Saving to: 'shapel.zip'

shapel.zip          100%[=====] 1.33M 1.53MB/s   in 0.9s

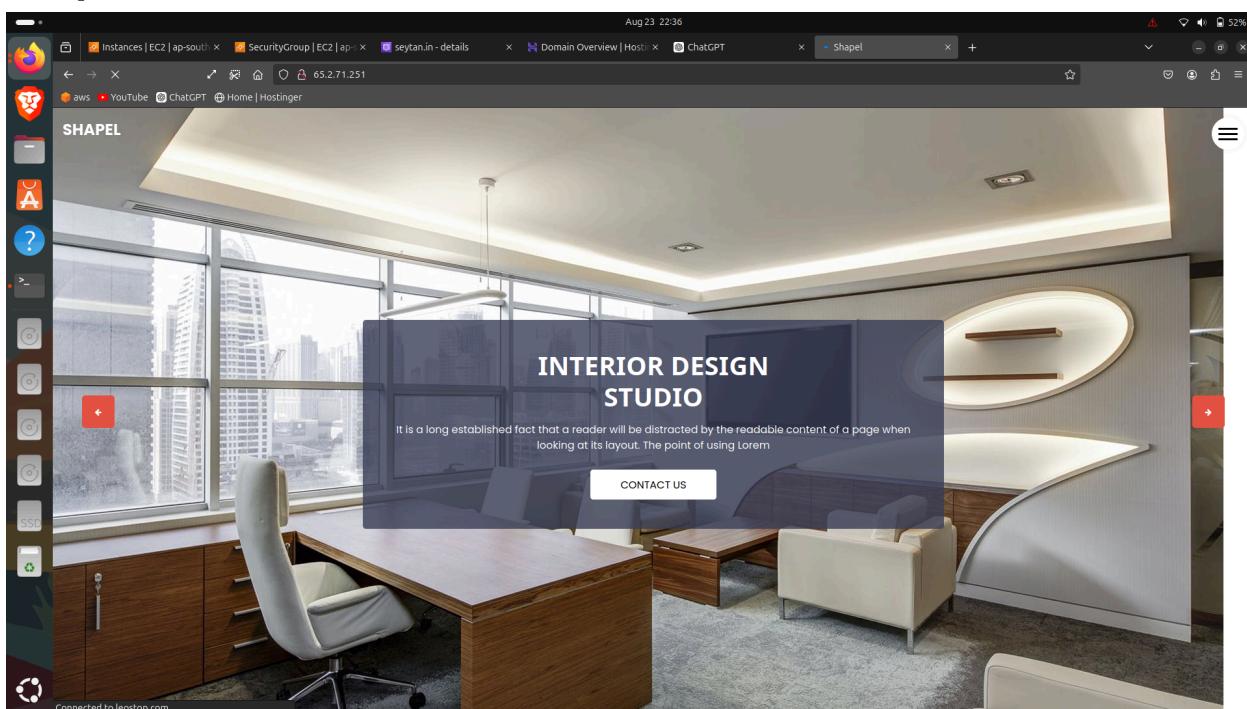
2024-08-23 15:39:42 (1.53 MB/s) - 'shapel.zip' saved [1390016/1390016]
```

Step 4: Whitelist the port number 80 and 443 in security group of ec2 instance .

Inbound rules (9)								
	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	
□	-	sgr-0c2d25009c9c77e1a	IPv4	Custom TCP	TCP	3000	0.0.0.0/0	
□	-	sgr-0560d11b1acb1d4...	IPv4	HTTP	TCP	80	0.0.0.0/0	
□	-	sgr-0d0f55b33d27cac33	IPv4	Custom TCP	TCP	9100	0.0.0.0/0	
□	-	sgr-07f69a23725e5a5c6	IPv4	Custom TCP	TCP	9090	0.0.0.0/0	
□	-	sgr-01359984cf20e2dc3	IPv4	SSH	TCP	22	0.0.0.0/0	
□	-	sgr-0ff2cddd788af0811	IPv4	MySQL/Aurora	TCP	3306	0.0.0.0/0	
□	-	sgr-0f0cc7685363cbe9c	IPv4	NFS	TCP	2049	0.0.0.0/0	
□	-	sgr-08670a6cd9080d3c7	-	All traffic	All	All	sg-0d7e17da	
□	-	sgr-0b8eedf2afe62519e	IPv4	HTTPS	TCP	443	0.0.0.0/0	

Now paste Public ip in the web browser to see your website working or not.

Output:

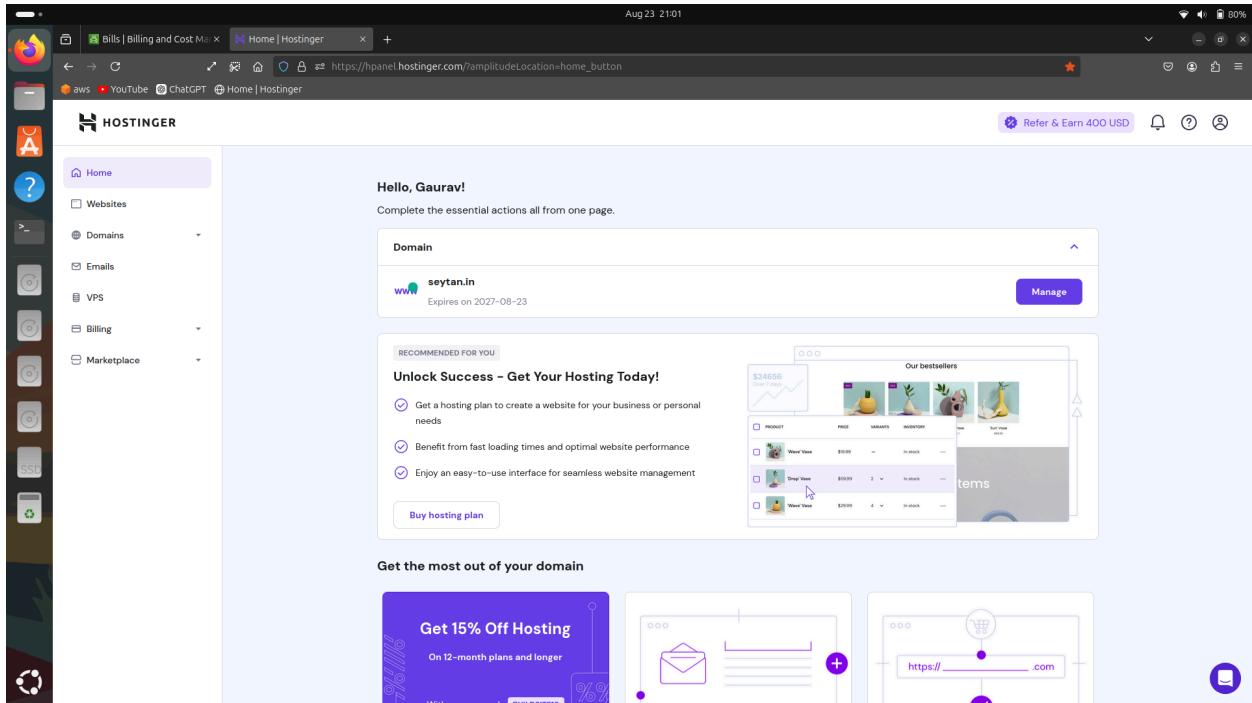


Step 5: Purchase a domain from 3rd party vendor.

Here we will use hostinger as a 3rd party domain provider and we will use seytan.in domain.

What is Domain ?

→ A domain is a human-readable address used to access websites on the internet, such as "example.com." It serves as a user-friendly way to identify and reach specific IP addresses, which are the underlying numerical addresses of servers hosting the website.



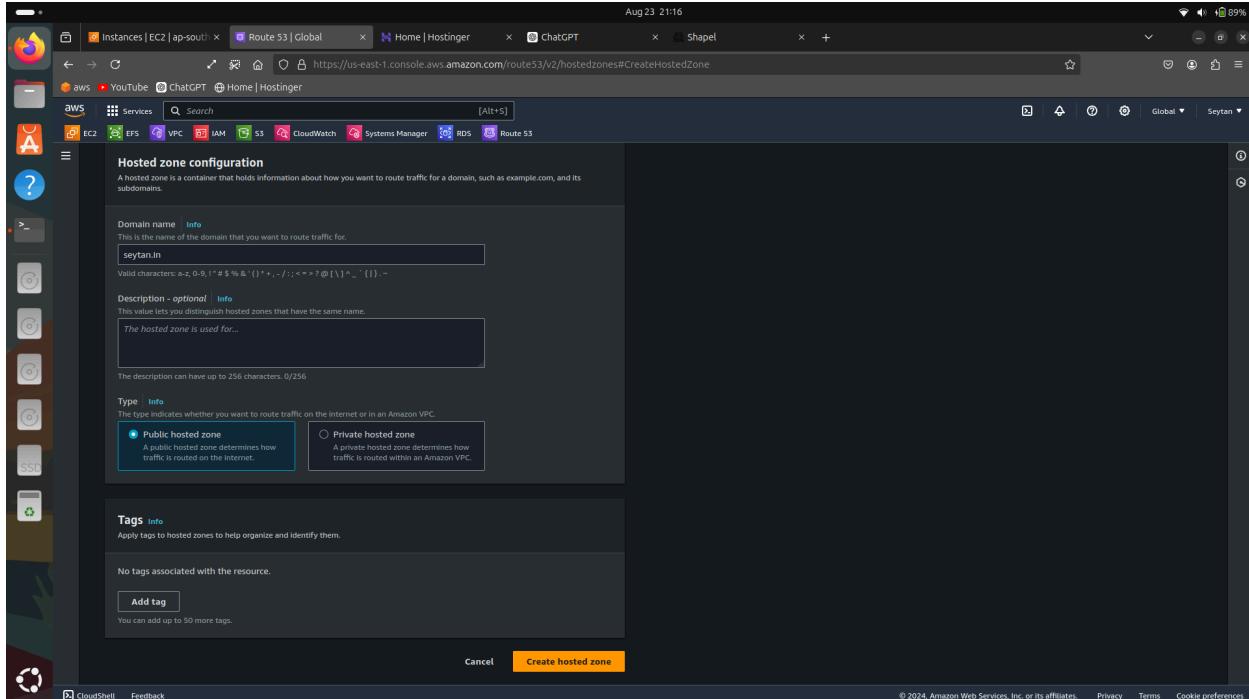
Step 6: Now Create Hosted Zone in Route53 to bind our domain with our_public ip .

What is Route53 ?

→ Amazon Route 53 is a scalable DNS (Domain Name System) web service by AWS that routes end-user requests to internet applications.

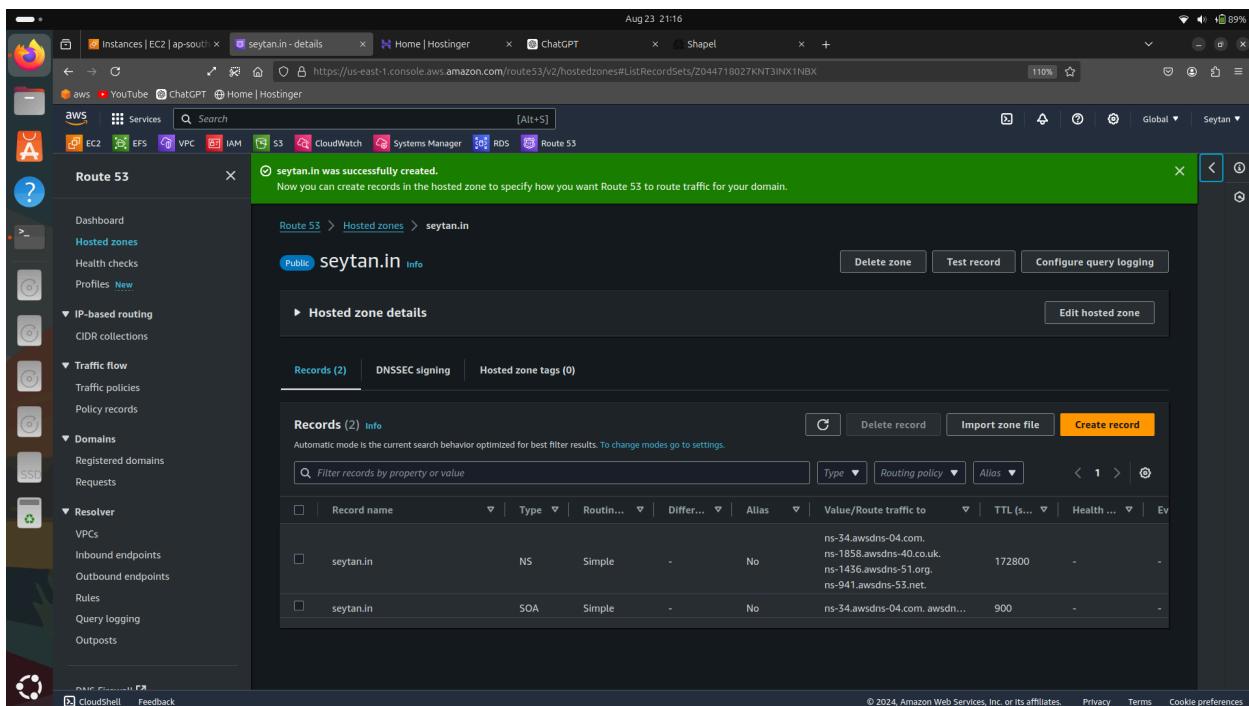
What is Hosted Zones in Route53 ?

→ A hosted zone in Route 53 is a container for records that define how traffic is routed for a specific domain or subdomain.



Step 7: After Creating Hosted Zone it will give us 2 records NS and SOA.

The NS Records are to be copied to our hostinger nameservers.



The screenshot shows the 'DNS / Nameservers' section of the Hostinger control panel. The left sidebar has 'Main menu' with 'Domain Overview' and 'DNS / Nameservers' selected. The right main area has tabs for 'DNS records', 'Child nameservers', 'DNSSEC', 'Forwarding', and 'DNS history'. Under 'Nameservers', it says 'Nameservers handle internet requests for your domain. You can use Hostinger nameservers or use custom nameservers to point to other hosting provider.' It lists 'ns1.dns-parking.com' and 'ns2.dns-parking.com'. Below this, under 'Select Nameservers', the 'Change nameservers' radio button is selected. A list of four nameservers is shown: ns-34.awsdns-04.com, ns-1858.awsdns-40.co.uk, ns-1436.awsdns-51.org, and ns-941.awsdns-53.net. At the bottom are 'Save' and 'Cancel' buttons.

A modal dialog box is displayed over the main interface. The title is 'Nameservers changed!'. The message says 'Your nameservers has been changed to:' followed by a list of four nameservers: ns-34.awsdns-04.com, ns-1858.awsdns-40.co.uk, ns-1436.awsdns-51.org, and ns-941.awsdns-53.net. Below this, a note says 'It might take up to 24 hours for the domain to propagate to the new nameservers.' At the bottom right of the dialog is a 'Close' button.

What is ns record and soa record ?

- 1) An NS (Name Server) record specifies the authoritative name servers for a domain, directing queries to the correct servers for DNS resolution.
- 2) An SOA (Start of Authority) record provides essential information about a DNS zone, including the primary name server, the email of the domain administrator, and the domain's serial number and refresh times.

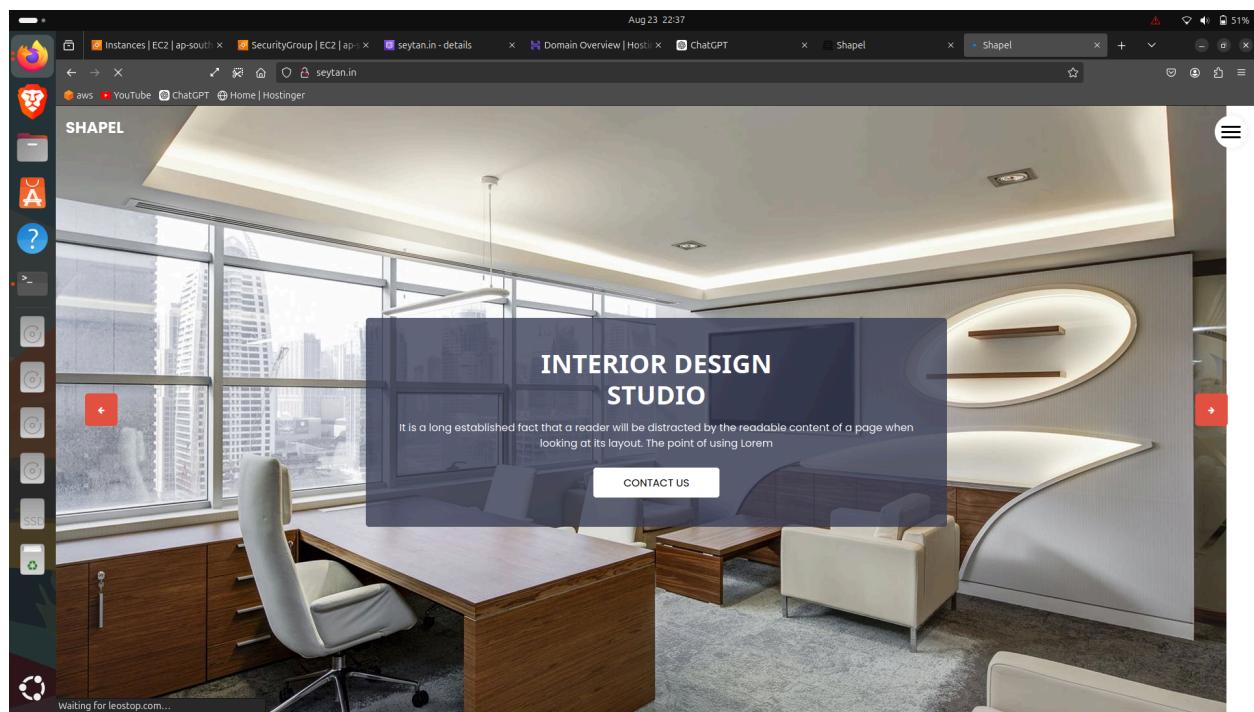
Step 8: Now Create A-record and enter our public ip to bind with the domain.

After this you can enter the domain name seytan.in to see your domain is working or not .

What is A record ? → An A record, or Address record, maps a domain name to its corresponding IPv4 address, allowing browsers to locate the server hosting the website

Requests	Record ...	Type	Routin...	Differ...	Alias	Value/Route traffic to	TTL
Resolver	seytan.in	A	Simple	-	No	65.27.71.251	60
/PCs	seytan.in	NS	Simple	-	No	ns-34.awsdns-04.com. ns-1858.awsdns-40.co.uk. ns-1436.awsdns-51.org. ns-541.awsdns-53.net.	172800
Inbound endpoints	seytan.in	SOA	Simple	-	No	ns-34.awsdns-04.com. awsdn...	900
Outbound endpoints	_deab7b6...	CNAME	Simple	-	No	_f9885588e80726d88f6468...	300
Rules							
Query logging							
Outposts							

Output:



Step 9: Now our domain is working property but the connection is not secured as we have not attached any ssl certificate with our domain.

So now we will Request a ssl Certificate from ACM Service in aws .

What is ACM →ACM (AWS Certificate Manager) is a service by AWS that allows you to easily provision, manage, and deploy SSL/TLS certificates for use with AWS services and your websites to secure network communications.

The screenshot shows two parts of the AWS Management Console:

Top Window (Request certificate):

- Header: Aug 23 22:38, https://ap-south-1.console.aws.amazon.com/acm/home?region=ap-south-1#certificates/request
- Left sidebar: Services (EC2, EFS, VPC, IAM, S3, CloudWatch, Systems Manager, RDS, Route 53, Certificate Manager)
- Current View: AWS Certificate Manager > Certificates > Request certificate
- Form:
 - Certificate type:** Request a public certificate (selected)
 - Description: ACM certificates can be used to establish secure communications access across the Internet or within an internal network. Choose the type of certificate for ACM to provide.
 - Request a public certificate: Request a public SSL/TLS certificate from Amazon. By default, public certificates are trusted by browsers and operating systems.
 - Request a private certificate: No private CAs available for issuance.
 - Note: Requesting a private certificate requires the creation of a private certificate authority (CA). To create a private CA, visit [AWS Private Certificate Authority](#).
- Buttons: Cancel, Next

Bottom Window (Domain Overview):

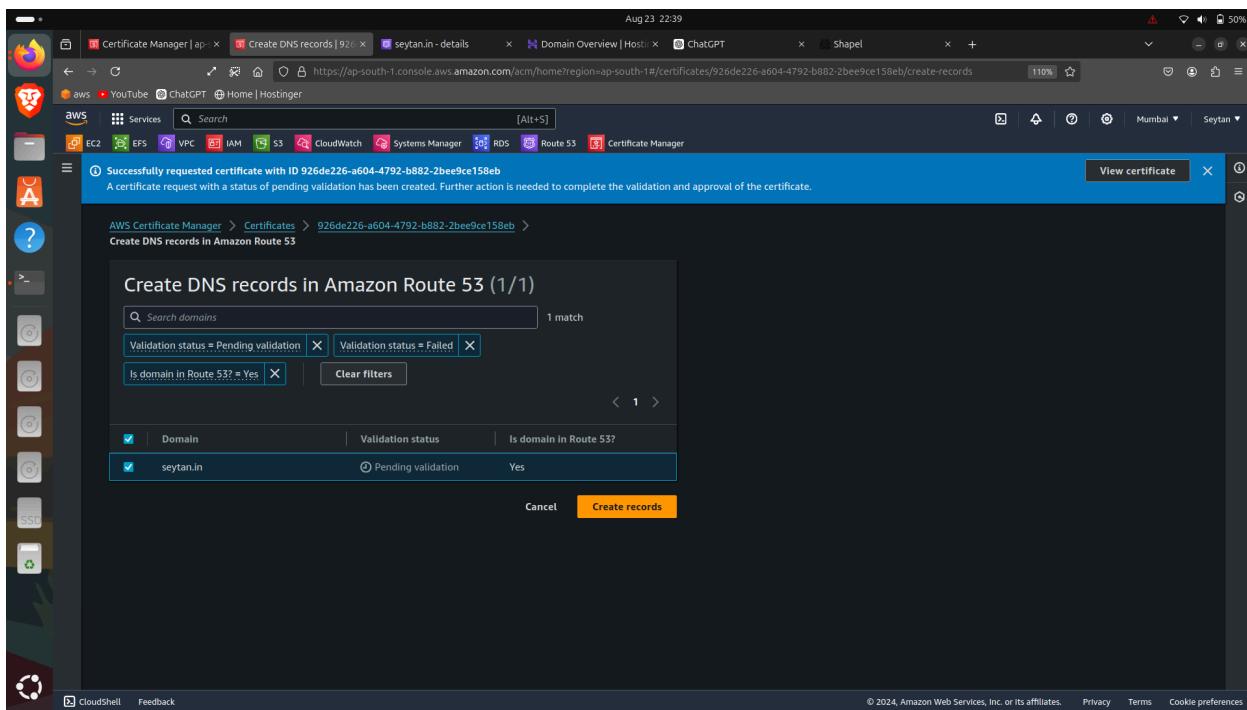
- Header: Domains (1)
- Table:

Domain	Status	Renewal status	Type	CNAME name
seytan.in	Pending validation	-	CNAME	_deab7b60bca7c45169b4d0f7447fb56e.seytan.in.
- Buttons: Create records In Route 53, Export to CSV

Step 10 : After Creating Certificate create CName record in Our hosted zone .

What is CName record ? →

When using ACM (AWS Certificate Manager), a CNAME record is often required to verify domain ownership. AWS provides a unique CNAME that you must add to your DNS records, which allows ACM to confirm that you control the domain before issuing an SSL/TLS certificate.



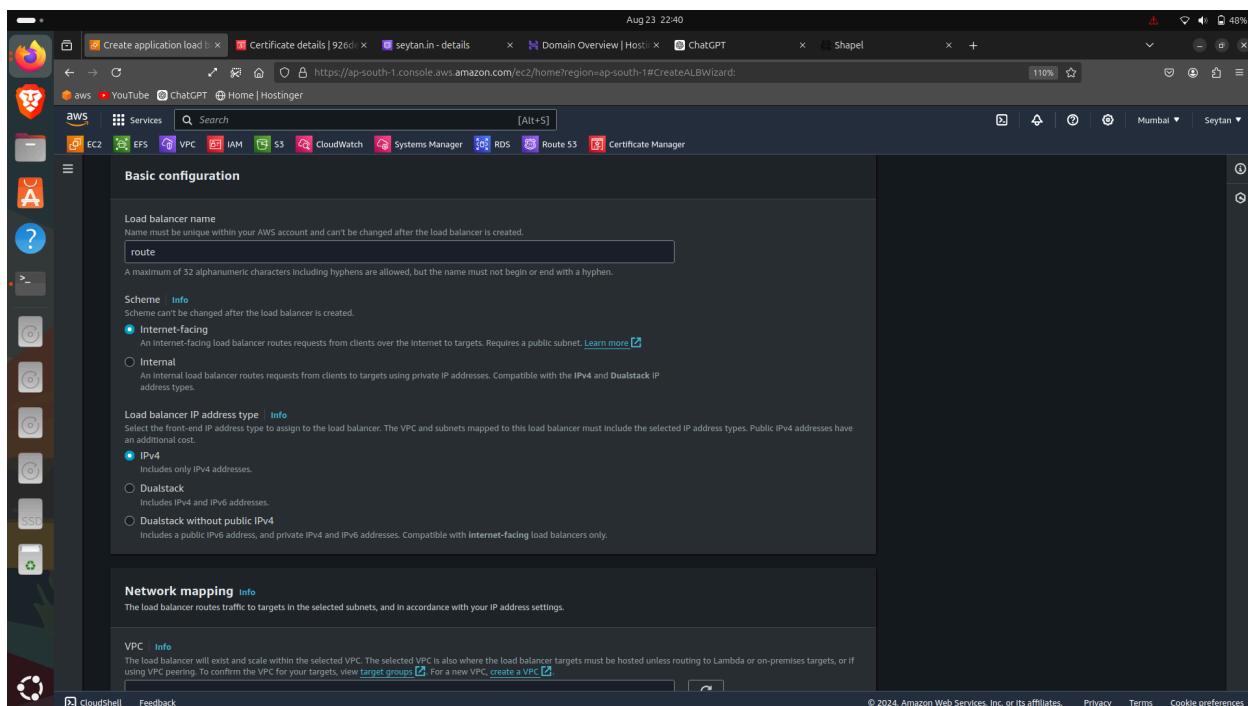
Step 11: Now We need to create a Application Load balancer and Target Group for using the ACM Certificate so we can redirect from http to https.

What is Application Load balancer ?

→ An Application Load Balancer (ALB) is an AWS service that distributes incoming application traffic across multiple targets, such as EC2 instances, based on request content, improving availability and scalability. It operates at the application layer (Layer 7) of the OSI model and supports advanced routing features like path-based and host-based routing.

What is Target Group ?

→ A target group in AWS is a set of resources, such as EC2 instances or IP addresses, that the Application Load Balancer routes traffic to based on the configured rules. It allows you to manage and monitor the health of these resources and balance the load among them.



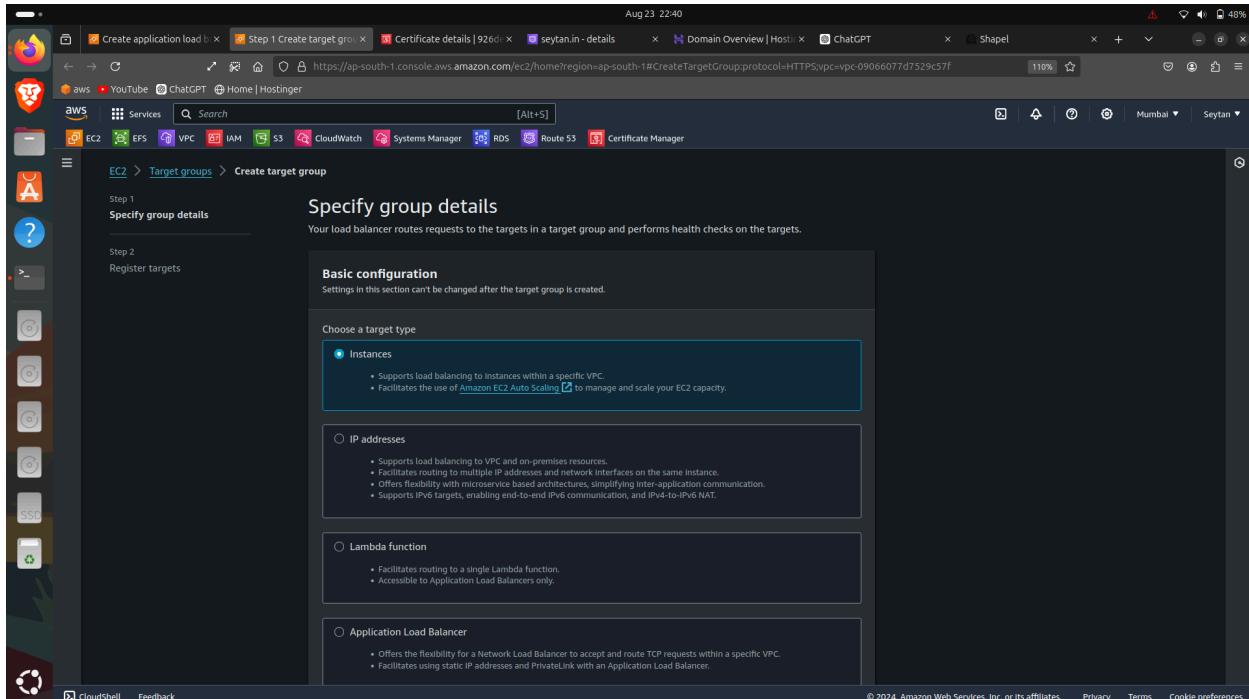
Assign ACM Certificate to our Load balancer

The screenshot shows the AWS CloudFront Create Distribution wizard at step 4, titled 'SSL Configuration'. It displays the 'Default SSL/TLS server certificate' section. Under 'Certificate source', the 'From ACM' option is selected, and a dropdown menu shows 'seytan.in 926de226-604-4792-b882-2bee9ce158eb'. There is also a 'Request new ACM certificate' button. Below this, the 'Client certificate handling' section includes a checkbox for 'Mutual authentication (mTLS)'. A note states: 'Mutual TLS (Transport Layer Security) authentication offers two-way peer authentication. It adds a layer of security over TLS and allows your services to verify the client that's making the connection.' At the bottom, there is a note about 'Load balancer tags - optional' and a link to 'Optimize with service integrations - optional'.

Make Load Balancer To Listen on Https

The screenshot shows the AWS CloudFront Create Distribution wizard at step 5, titled 'Listener Configuration'. It displays the 'Listener HTTPS:443' configuration. The 'Protocol' is set to 'HTTPS' and the 'Port' is '443'. The 'Default action' is set to 'Forward to tg' with 'Target type: Instance, IPv4' and 'HTTP' selected. There is a 'Create target group' button. Below this, the 'Listener tags - optional' section has a note: 'Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.' A 'Create listener tag' button is present. At the bottom, the 'Secure listener settings' section notes: 'These settings will apply to all of your secure listeners. Once created, you can manage these settings per listener.' The 'Security policy' section is identical to the previous screenshot, showing 'All security policies' and 'ELBSecurityPolicy-TLS13-1-2-2021-06 (recommended)'.

Step 12 : Create target group for load balancer with port 80 and protocol http .



The screenshot shows the 'Basic configuration' section of the AWS Lambda function creation wizard. It lists three target types:

- Instances**:
 - Supports load balancing to instances within a specific VPC.
 - Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.
- IP addresses**:
 - Supports load balancing to VPC and on-premises resources.
 - Facilitates routing to multiple IP addresses and network interfaces on the same instance.
 - Offers flexibility with microservice-based architectures, simplifying inter-application communication.
 - Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.
- Lambda function**:
 - Facilitates routing to a single Lambda function.
 - Accessible to Application Load Balancers only.
- Application Load Balancer**:
 - Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
 - Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name: tg

Protocol : Port:
Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation.
HTTPS 443
1-65535

IP address type: Only targets with the indicated IP address type can be registered to this target group.
 IPv4: Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.
 IPv6: Each instance you register must have an assigned primary IPv6 address. This is configured on the

Step 13: Now We have to Edit the A Record to point the domain to the load balancer dns instead of public ip.

Here we use Routing Policies→

Routing policies in Route 53 define how DNS queries are handled. They determine which IP address or resource is returned based on factors like health, latency, or geography.

There are 8 types of routing policy

1. **Simple routing policy** Use for a single resource that performs a given function for your domain.
2. **Failover routing policy** Use when you want to configure active-passive failover. .
3. **Geolocation routing policy** Use when you want to route traffic based on the location of your users.
4. **Geoproximity routing policy** Use when you want to route traffic based on the location of your resources and, optionally, shift traffic from resources in one location to resources in another location.
5. **Latency routing policy** Use when you have resources in multiple AWS Regions and you want to route traffic to the Region that provides the best latency .
6. **IP-based routing policy** Use when you want to route traffic based on the location of your users, and have the IP addresses that the traffic originates from.
7. **Multivalue answer routing policy** Use when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random.
8. **Weighted routing policy** Use to route traffic to multiple resources in proportions that you specify .

The screenshot shows the AWS Route 53 console with the domain `seytan.in`. A modal window titled "Edit record" is open, displaying a success message: "seytan.in was successfully updated. Route 53 propagates your changes to all of the Route 53 authoritative DNS servers within 60 seconds. Use "View status" button to check propagation status." The modal also shows the configuration for an Alias record:

- Record name:** Info
- subdomain:** seytan.in
- Route traffic to:** Alias to Application and Classic Load Balancer (Asia Pacific (Mumbai))
- Routing policy:** Simple routing

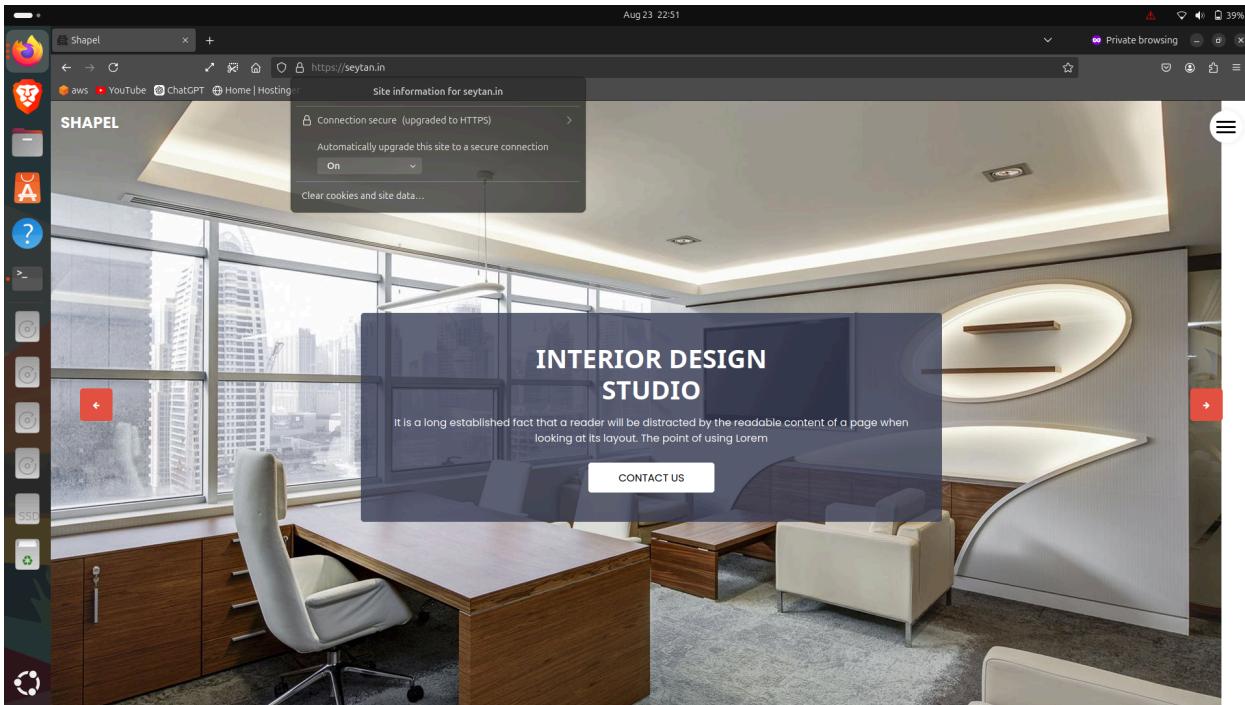
The main table lists four records:

Type	Value/Route traffic to	TTL
A	65.2.71.251	60
NS	ns-34.awsdns-04.com, ns-1858.awsdns-40.co.uk, ns-1436.awsdns-51.org, ns-941.awsdns-53.net	1728
SOA	ns-34.awsdns-04.com. awsdns-04.com. 900	900
CNAME	_f9885588e80726d88f6468...	300

Step 14: Now hit the seytan.in domain in any browser .

Here , we can see Our domain is now showing connection secure as we have attached the SSL Certificate to it .

Output :



Conclusion: By following these steps, you will have configured your domain to be managed by Route 53, secured your website with an SSL/TLS certificate, and set up an ALB to handle and route HTTPS traffic efficiently, ensuring secure and reliable access to your web application.