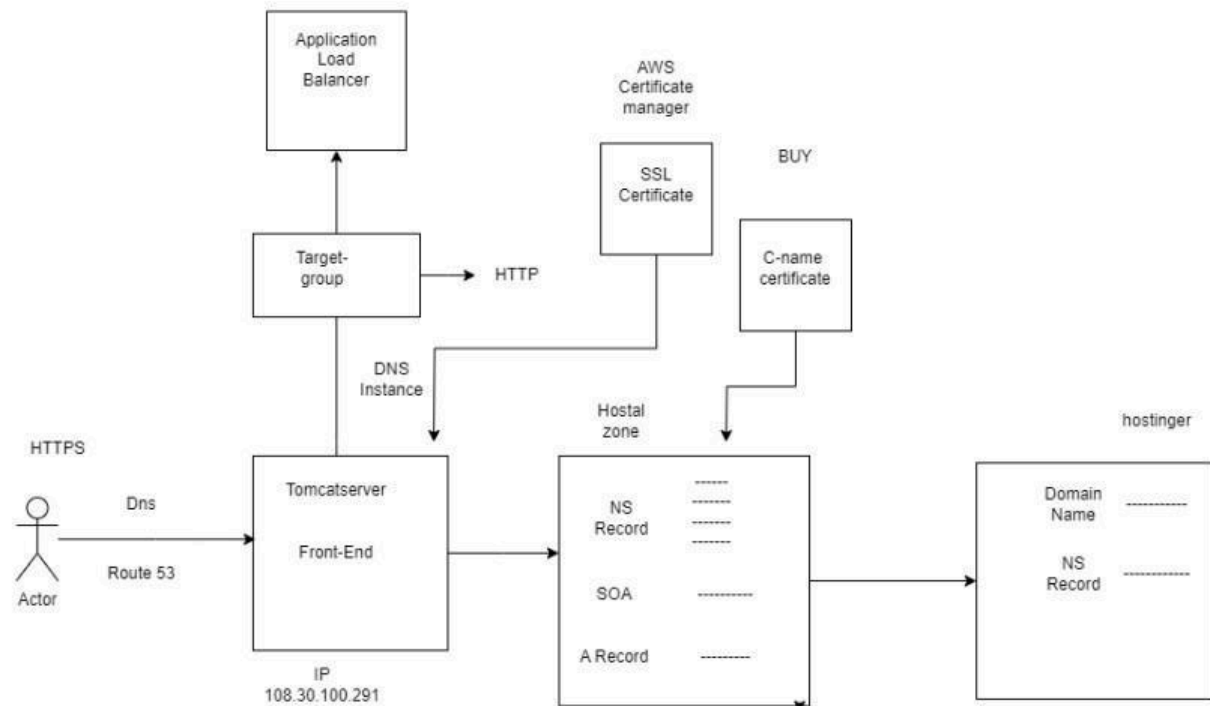


Route 53

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.

- Amazon Route 53 is a highly available and scalable Domain Name System(DNS) web service. Route 53 connect user requests to internet applications running on AWS or on- premises.
- It is essential for conversion of user friendly domain names into IP addresses so that internet communication can proceed without difficulties.

Diagrammatic Representation:



step 1: Create an instance & connect using it : -
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 displays the AWS Management Console interface for EC2 instances. At the top, there's a header with 'Instances (1/1)' and a search bar. Below this, a table lists the instance 'RDS-Test' with ID 'i-0d3160a951f2f9b2f', state 'Running', type 't2.micro', and status 'Initializing'. The instance details panel for 'i-0d3160a951f2f9b2f (RDS-Test)' is open, showing tabs for Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags. The Details tab is active, displaying the Instance summary with fields for Instance ID, Public IPv4 address (43.205.115.198), Private IPv4 addresses (172.31.39.207), Instance state (Running), and Public IPv4 DNS (ec2-43-205-115-198.ap-south-1.compute.amazonaws.com).

whitelist port 443,80,22 in security group

The screenshot shows the 'Inbound rules' section of the AWS Management Console. It features a search bar and a table of rules. The table has columns for Name, Security group rule..., IP version, Type, Protocol, Port range, and Source. The rules listed are:

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
-	sg-0c2d25009c9c77e1a	IPv4	Custom TCP	TCP	3000	0.0.0.0/0
-	sg-0560d11b1acb1d4...	IPv4	HTTP	TCP	80	0.0.0.0/0
-	sg-0d0f55b33d27cac33	IPv4	Custom TCP	TCP	9100	0.0.0.0/0
-	sg-07f69a23725e4a5c6	IPv4	Custom TCP	TCP	9090	0.0.0.0/0
-	sg-01359984cf20e2dc3	IPv4	SSH	TCP	22	0.0.0.0/0
-	sg-0ff2cdd788af0811	IPv4	MySQL/Aurora	TCP	3306	0.0.0.0/0
-	sg-0f0cc7685363cbe9c	IPv4	NFS	TCP	2049	0.0.0.0/0
-	sg-08670a6cd9080d3c7	-	All traffic	All	All	sg-0d7e17di
-	sg-0b8eedf2afe62519e	IPv4	HTTPS	TCP	443	0.0.0.0/0

Step 2: Now Install the apache2 server in our ec2 instance

What is apache2?

→apache2 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.

sudo apt install apache2

then move to home directory of

apache2 `cd /var/www/html/`

Remove index.html file that already exist

```
No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-11-100:~$ cd /var/www/html/
ubuntu@ip-172-31-11-100:/var/www/html$ ls
index.html
ubuntu@ip-172-31-11-100:/var/www/html$ rm -rvf index.html
```

step 3: Now download the free css template

Sudo wget

<https://www.free-css.com/assets/files/free-css-templates/download/page295/guarder.zip>

Unzip the file

Sudo apt install unzip

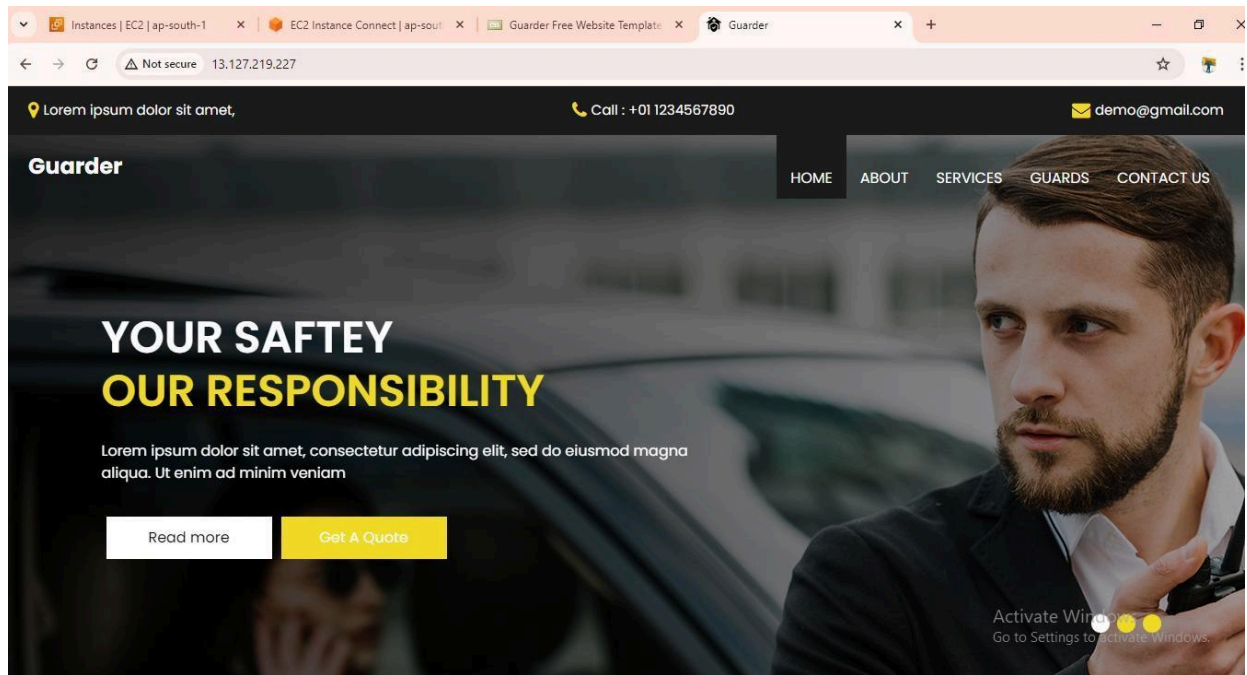
Now move only file from unzip directory to HTML

directory **sudo mv guarder-html/***

/var/www/html

```
ubuntu@ip-172-31-11-100:~$ ls
guarder-html  guarder.zip
ubuntu@ip-172-31-11-100:~$ sudo mv guarder-html/* /var/www/html
ubuntu@ip-172-31-11-100:~$ cd /var/www/html/
ubuntu@ip-172-31-11-100:/var/www/html$ ls
about.html  contact.html  css  fonts  guard.html  images  index.html  js  service.html
ubuntu@ip-172-31-11-100:/var/www/html$
```

Public ip to host website



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

Here we will use hostinger as a 3rd party domain provider and we will use prathameshenterprises.shop 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 .

Here we can purchase Domain from

various vendors Example:- Hostinger,

GoDaddy, Bigrock, etc...

- **We use domain to identify websites and make them easier for people to access.**

Then create hosted zones from Route53 service

- A hosted zone is a container for records, and records contain information about how you want to route traffic for a specific domain.

Domain name [Info](#)

This is the name of the domain that you want to route traffic for.

Valid characters: a-z, 0-9, ! " # \$ % & ' () * + , - / : ; < = > ? @ [\] ^ _ ` { | } . ~

Description - optional [Info](#)

This value lets you distinguish hosted zones that have the same name.

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**

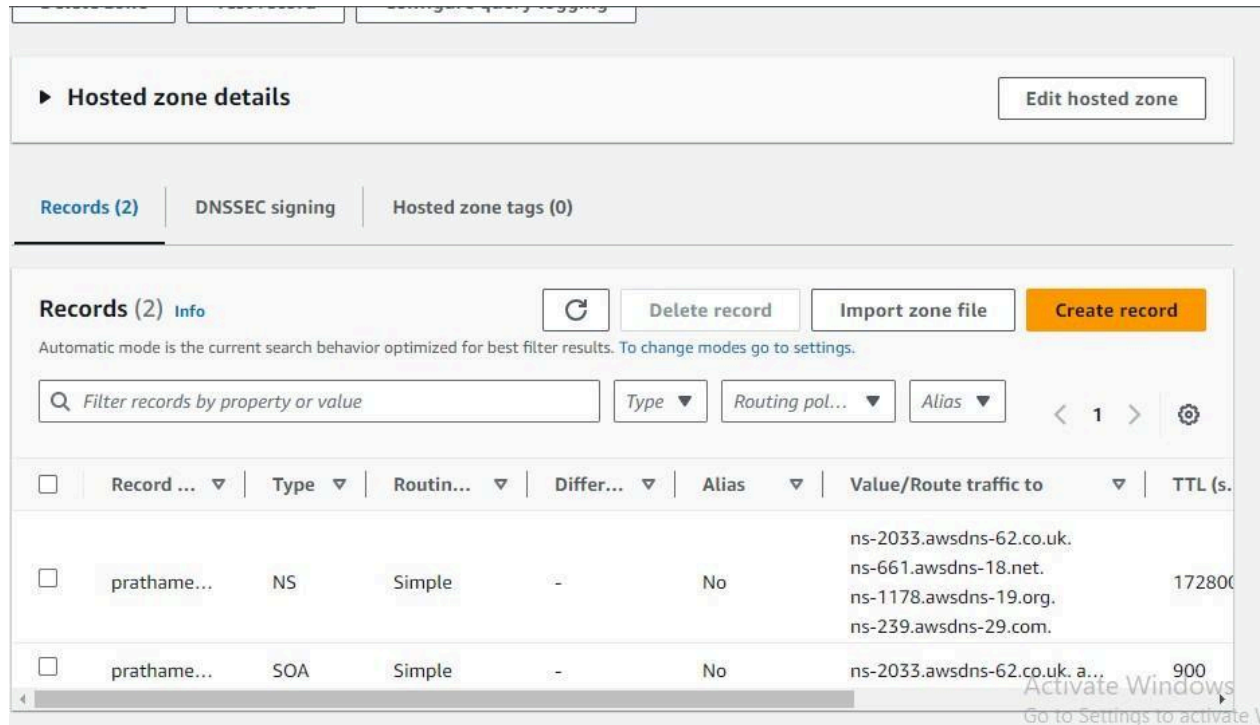
A public hosted zone determines how traffic is routed on the internet.

**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.



After creating hosted zone create Record

- Record is created to define how traffic is routed for a domain and its subdomains. There are two types of hosted zones: public and private
- Public hosted zones : contain records that specify how traffic is routed on the internet.
- Private hosted zones: Contain records that specify how traffic is routed within one or more Amazon Virtual Private Clouds(Amazon VPCs)

Create record [Info](#)

Quick create record

[Switch to wizard](#)

▼ Record 1

[Delete](#)Record name [Info](#)

prathameshenterprises.shop

Record type [Info](#)

Keep blank to create a record for the root domain.

☐ AliasValue [Info](#)

Enter multiple values on separate lines.

[Activate Windows](#)
Go to Settings to activate Windows.Record name [Info](#)

prathameshenterprises.shop

Record type [Info](#)

Keep blank to create a record for the root domain.

☐ AliasValue [Info](#)

Enter multiple values on separate lines.

TTL (seconds) [Info](#)Routing policy [Info](#)

Recommended values: 60 to 172800 (two days)

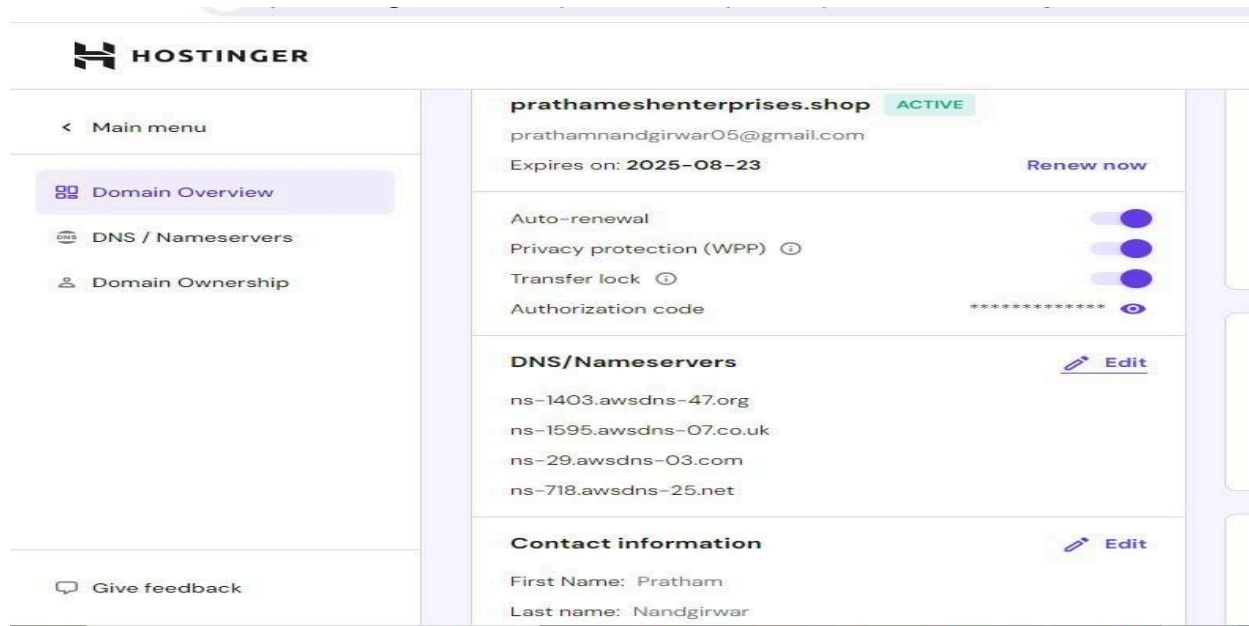
[Add another record](#)[Activate Windows](#)[Go to Settings to activate Windows.](#)

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

The NS Records are to copied to our hostinger nameservers.

DNS//:Nameservers

- Here we change nameservers for our domain name and telling the internet to look elsewhere to find details about where our website can be found.



< Main menu

Domain Overview

DNS / Nameservers

Domain Ownership

Select Nameservers

☐ Use Hostinger nameservers (recommended)

☒ Change nameservers

ns-2033.awsdns-62.co.uk

ns-661.awsdns-18.net

ns-1178.awsdns-19.org

ns-239.awsdns-29.com

Save Cancel

Step 8: 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.

Load balancer types

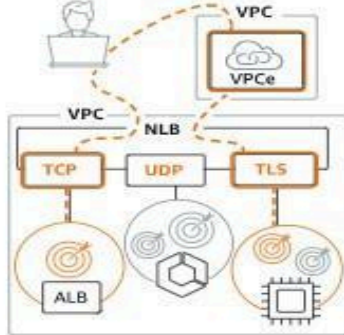
Application Load Balancer [Info](#)



Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

Create


Network Load Balancer [Info](#)



Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

Create

Gateway Load Balancer [Info](#)



Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

Create

to its registered targets.

▼ Listener HTTPS:443

Remove

Protocol

Port

Default action

Info

HTTPS

:

443

Forward to

Select a target group

↺

↻

1-65535

Create target group

Listener tags - optional

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

Add listener tag

You can add up to 50 more tags.

Add listener

Secure listener settings

Info

These settings will apply to all of your secure listeners. Once created, you can manage these settings per listener.

Here change the protocol to HTTPS

- Here we change port to https to provide encryption to the data & secure our website.

Then create target group

- Target groups are used to route traffic to specific application endpoints.

• 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

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

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

HTTP

80

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.

Here change the protocol to HTTP

1-65535 (separate multiple ports with commas)

Include as pending below

1 selection is now pending below. Include more or register targets when ready.

Review targets

Targets (1)

Remove all pending

Show only pending < 1 > ⚙

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address
i-064a26419cd187688	RDS-Test	80	Running	default	ap-south-1b	172.31.11.100

1 pending

CancelPreviousActivateCreate target group

Go to Settings to activate Windows Firewall

Now attach the target group to load balancer

Security categoryAll security policies

Policy nameELBSecurityPolicy-TLS13-1-2-2021-06 (recommended)

Default SSL/TLS server certificate

The certificate used if a client connects without SNI protocol, or if there are no matching certificates. You can source this certificate from AWS Certificate Manager (ACM), Amazon Identity and Access Management (IAM), or import a certificate. This certificate will automatically be added to your listener certificate list.

From ACM

From IAM

Import certificate

Certificate (from ACM)

The selected certificate will be applied as the default SSL/TLS server certificate for this load balancer's secure listeners.

Select a certificate

↻

[Request new ACM certificate](#)

Client certificate handling

Info

Client certificates are used to make authenticated requests to remote servers. [Learn more](#)

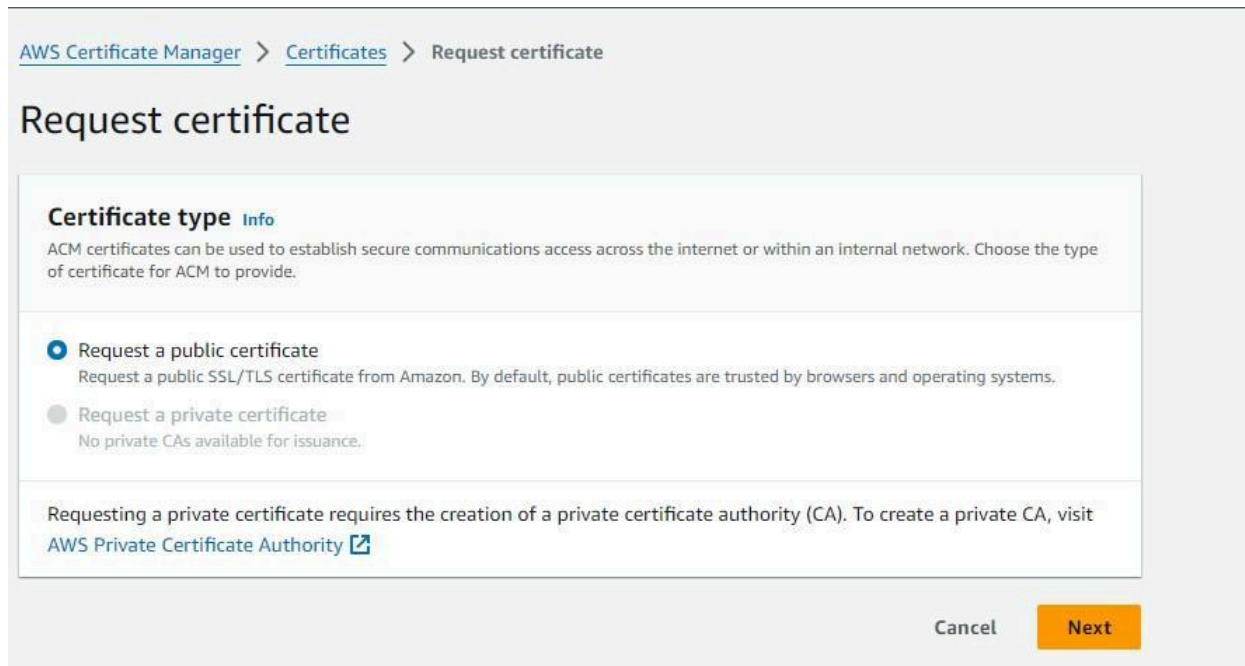
Mutual authentication (mTLS)

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.

Step 9: Now our domain is working properly 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.ACM is designed to protect and manage the private keys used with SSL/TLS certificates..



The screenshot shows the 'Request certificate' page in the AWS Certificate Manager console. The breadcrumb navigation at the top reads 'AWS Certificate Manager > Certificates > Request certificate'. The main heading is 'Request certificate'. Below this, there is a section titled 'Certificate type' with an 'Info' link. The text explains that ACM certificates can be used for internet or internal network access and asks the user to choose the type. There are two radio button options: 'Request a public certificate' (selected) and 'Request a private certificate'. The 'Request a private certificate' option is disabled with a note: 'No private CAs available for issuance.' Below the options, a note states: 'Requesting a private certificate requires the creation of a private certificate authority (CA). To create a private CA, visit [AWS Private Certificate Authority](#).' At the bottom right, there are 'Cancel' and 'Next' buttons.

AWS Certificate Manager > Certificates > Request certificate

Request certificate

Certificate type [Info](#)

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.

Requesting a private certificate requires the creation of a private certificate authority (CA). To create a private CA, visit [AWS Private Certificate Authority](#)

Cancel Next

Here we have to give domain name

Certificate status

Identifier

7627c0f8-8c22-40ad-b72f-7de0aa4cb836

Status

⌚ Pending validation [Info](#)

ARN

arn:aws:acm:ap-south-1:211125410545:certificate/7627c0f8-8c22-40ad-b72f-7de0aa4cb836

Type

Amazon Issued

Domains (1)

Create records in Route 53

Export to CSV

< 1 >

Domain	Status	Renewal status	Type	CNAME name
prathameshenterprises.shop	⌚ Pending validation	-	CNAME	_33859a37b3rises.shop

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.

Create DNS records in Amazon Route 53 (1/1)

1 match

Validation status = Pending validation X

Validation status = Failed X

Is domain in Route 53? = Yes X

Clear filters

< 1 >

<input checked="" type="checkbox"/>	Domain	Validation status	Is domain in Route 53?
<input checked="" type="checkbox"/>	prathameshenterprises.shop	Pending validation	Yes

Cancel

Create records

7627c0f8-8c22-40ad-b72f-7de0aa4cb836

Delete

Certificate status

Identifier

7627c0f8-8c22-40ad-b72f-7de0aa4cb836

Status

Issued

ARN

arn:aws:acm:ap-south-1:211125410545:certificate/7627c0f8-8c22-40ad-b72f-7de0aa4cb836

Type

Amazon Issued

Domains (1)

Create records in Route 53

Export to CSV

Activate Windows 1

Go to Settings to activate Windows

After receiving certificate add it to load balancer

All security policies ▾ ELBSecurityPolicy-TLS13-1-2-2021-06 (recommended) ▾

Default SSL/TLS server certificate

The certificate used if a client connects without SNI protocol, or if there are no matching certificates. You can source this certificate from AWS Certificate Manager (ACM), Amazon Identity and Access Management (IAM), or import a certificate. This certificate will automatically be added to your listener certificate list.

Certificate source

☒ From ACM ☐ From IAM ☐ Import certificate

Certificate (from ACM)

The selected certificate will be applied as the default SSL/TLS server certificate for this load balancer's secure listeners.

prathameshenterprises.shop ▾ 7627c0f8-8c22-40ad-b72f-7de0aa4cb836 ↻

[Request new ACM certificate](#) ↗

Client certificate handling [Info](#)

Client certificates are used to make authenticated requests to remote servers. [Learn more](#) ↗

☐ Mutual authentication (mTLS)

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.

► Load balancer tags - optional

Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For

Activate Win
Go to Settings to

Step 11: Now We have to Edit the A Record to point the domain to the load balancer dns instead of public ip.

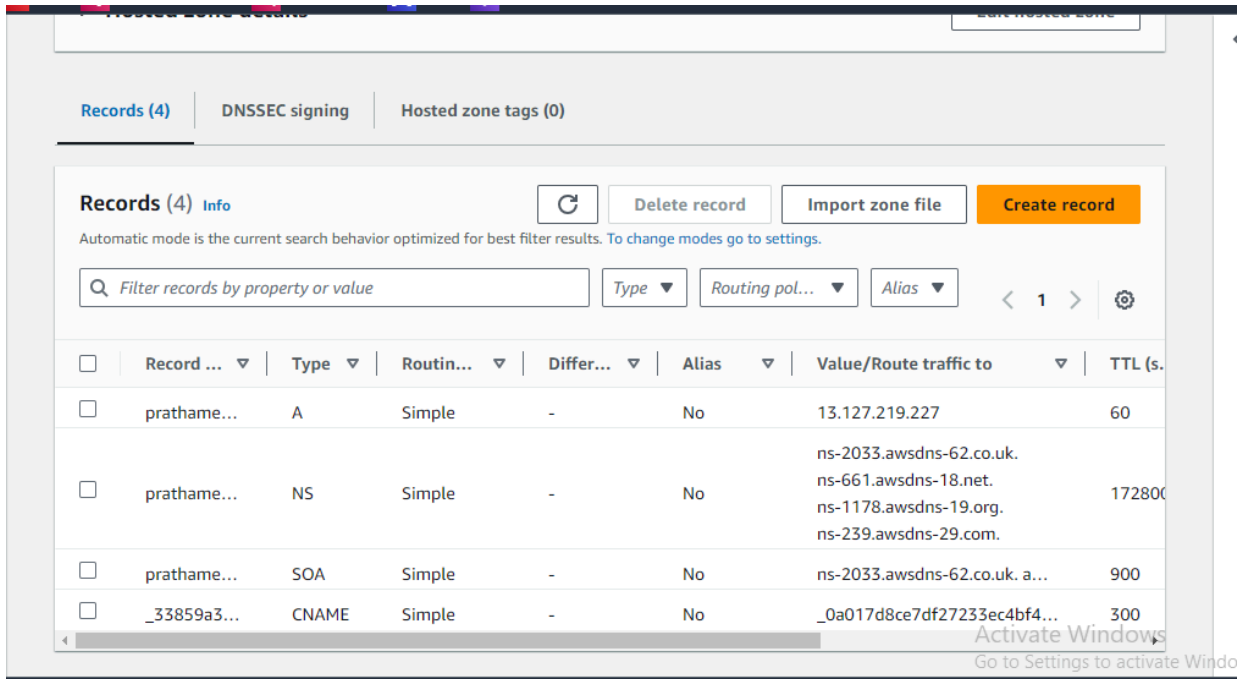
Here we use Routing Policies→

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

- **Simple routing policy** □ Use for a single resource that performs a given function for your domain.
- **Failover routing policy** □ Use when you want to configure active-passive failover.
- **Geolocation routing policy** □ Use when you want to route traffic based on the location of your users.
- **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.
- **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 .
- **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.
- **Multivalue answer routing policy** □ Use when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random.

- **Weighted routing policy** □ Use to route traffic to multiple resources in proportions that you specify .



The screenshot displays the AWS Route 53 console interface for a specific hosted zone. At the top, there are tabs for 'Records (4)', 'DNSSEC signing', and 'Hosted zone tags (0)'. Below the tabs, there's a section for 'Records (4)' with an 'Info' link, a refresh button, and buttons for 'Delete record', 'Import zone file', and 'Create record'. A search bar is present with the placeholder text 'Filter records by property or value'. Below the search bar, there are dropdown menus for 'Type', 'Routing pol...', and 'Alias'. A table of records is shown with columns: Record, Type, Routin..., Differ..., Alias, Value/Route traffic to, and TTL (s.). The table contains five records: 1. Record 'prathame...' of Type 'A' with Value '13.127.219.227' and TTL '60'. 2. Record 'prathame...' of Type 'NS' with Value 'ns-2033.awsdns-62.co.uk, ns-661.awsdns-18.net, ns-1178.awsdns-19.org, ns-239.awsdns-29.com.' and TTL '172800'. 3. Record 'prathame...' of Type 'SOA' with Value 'ns-2033.awsdns-62.co.uk. a...' and TTL '900'. 4. Record '_33859a3...' of Type 'CNAME' with Value '_0a017d8ce7df27233ec4bf4...' and TTL '300'. 5. Record 'prathame...' of Type 'A' with Value '13.127.219.227' and TTL '60'. At the bottom right, there is a watermark that says 'Activate Windows Go to Settings to activate Windows'.

Record ...	Type	Routin...	Differ...	Alias	Value/Route traffic to	TTL (s.)
<input type="checkbox"/> prathame...	A	Simple	-	No	13.127.219.227	60
<input type="checkbox"/> prathame...	NS	Simple	-	No	ns-2033.awsdns-62.co.uk. ns-661.awsdns-18.net. ns-1178.awsdns-19.org. ns-239.awsdns-29.com.	172800
<input type="checkbox"/> prathame...	SOA	Simple	-	No	ns-2033.awsdns-62.co.uk. a...	900
<input type="checkbox"/> _33859a3...	CNAME	Simple	-	No	_0a017d8ce7df27233ec4bf4...	300
<input type="checkbox"/> prathame...	A	Simple	-	No	13.127.219.227	60

Record name [Info](#)

prathameshenterprises
.shop

Keep blank to create a record for the root domain.

Record type [Info](#)

☒ Alias

Route traffic to [Info](#)

Alias hosted zone ID: ZP97RAFLXTNZK

Routing policy [Info](#)

Evaluate target health

☒ No

Step 12: Now hit the prathameshenterprises.shop domain in any browser .

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

<https://prathameshenterprises.shop/>

