AMAZON WEB SERVIES(AWS)

Certificate Manager

AWS Certificate Manager (ACM) is designed to simplify and automate many of the tasks traditionally associated with provisioning and managing SSL/TLS certificates.

Before deploying a web application we should understand the basic concept of Secure Socket Layer (SSL).

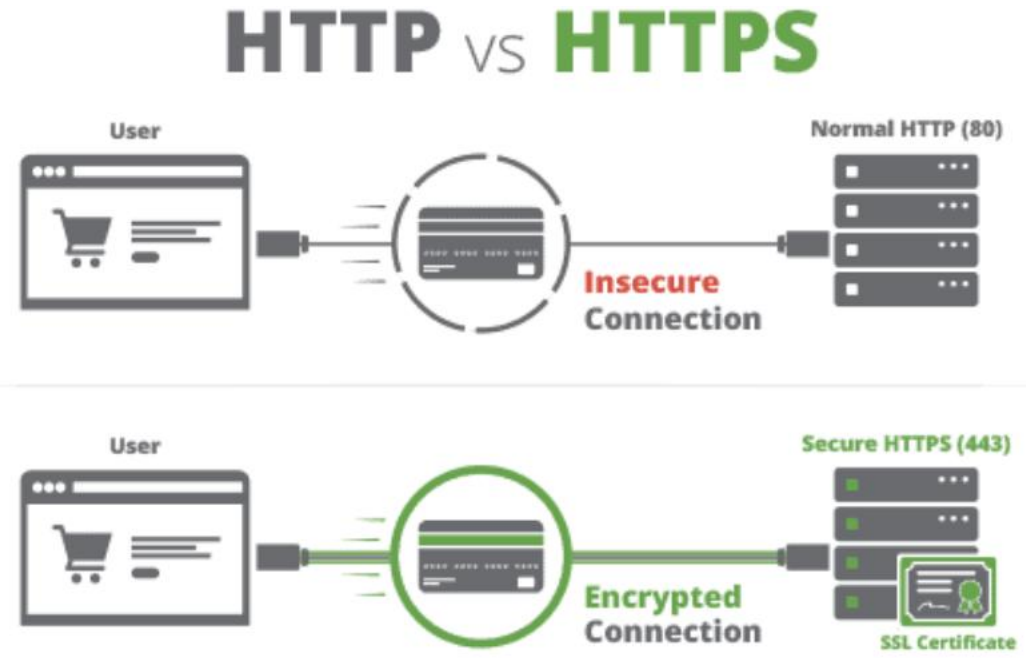
Overview of SSL/TLS Certificates

An SSL certificate is like an ID card or a badge that proves someone is who they say they are. SSL certificates are stored and displayed on the Web by a website's or application's server.

SSL (Secure Socket Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

Secure Sockets Layer/Transport Layer Security (SSL/TLS) is a must-have whenever sensitive data is moved to and from a website.

For instance, sites that require to fulfil compliance requirements such as PCI-DSS, FedRAMP, and HIPAA make extensive use of SSL/TLS. Unfortunately, provisioning and managing SSL/TLS certificates can entail a lot of work that is usually manual and not easily automated.

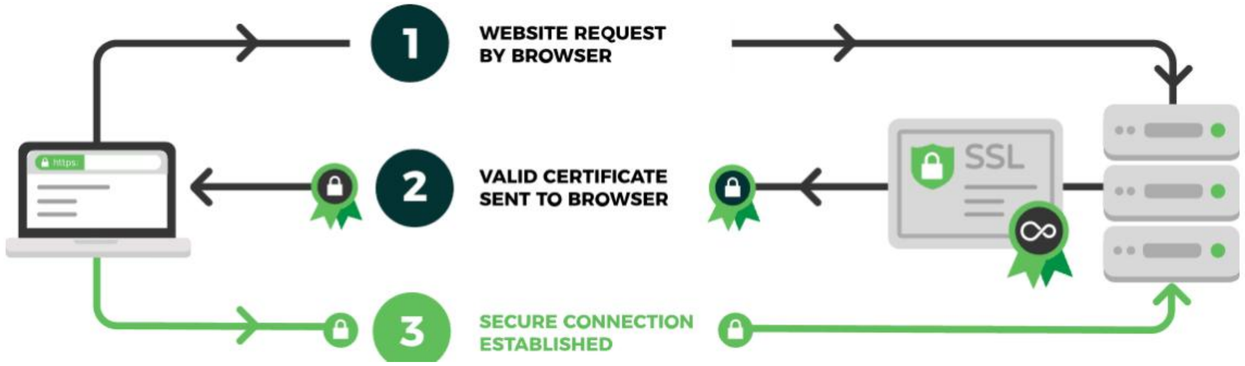


Transport Layer Security (TLS) is the successor protocol to SSL. TLS is an improved version of SSL. It works in much the same way as the SSL, using encryption to protect the transfer of data and information. The two terms are often used interchangeably in the industry although SSL is still widely used.

AMAZON WEB SERVIES(AWS)

How SSL/TLS works

1. A server attempts to connect to a website (i.e. a web-server) secured with SSL. The server requests the web-server to identify itself.
2. The web-server sends the server a copy of its SSL certificate.
3. The server checks to see whether or not it trusts the SSL certificate. If so, it sends a message to the web-server.
4. The web-server sends back a digitally signed acknowledgement to start an SSL encrypted session.
5. Encrypted data is shared between the server and the web-server.


1
WEBSITE REQUEST BY BROWSER
https:
2
VALID CERTIFICATE SENT TO BROWSER
SSL
3
SECURE CONNECTION ESTABLISHED

What is AWS Certificate Manager (ACM)?

AWS Certificate Manager is a service that lets us easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and our internal connected resources.

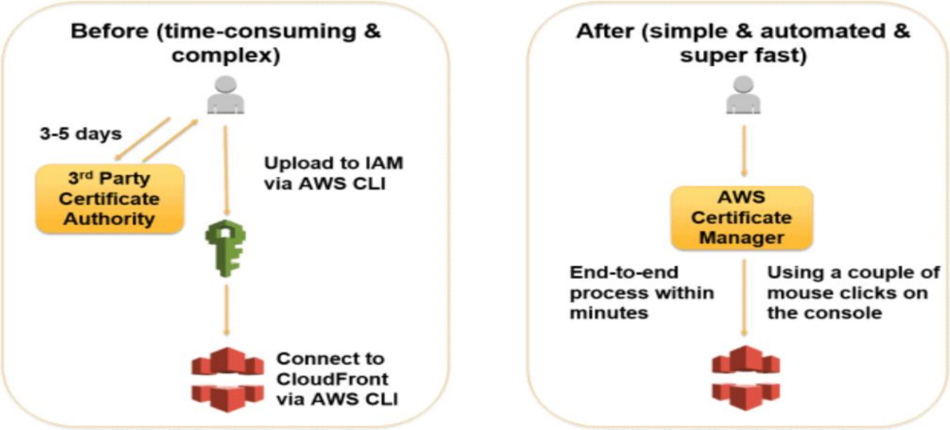
SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet as well as resources on private networks. AWS Certificate Manager removes the time-consuming manual process of purchasing, uploading, and renewing SSL/TLS certificates.

Why AWS Certificate Manager (ACM)?

ACM makes it easier to enable SSL/TLS for a website or application on the AWS platform. ACM eliminates many of the manual processes previously associated with using and managing SSL/TLS certificates.

ACM can also help us to avoid downtime due to misconfigured, revoked, or expired certificates by managing renewals. We get SSL/TLS protection and easy AWS certificate management. When we use ACM to manage certificates, certificate private keys are securely protected and stored using strong encryption and key management best practices.

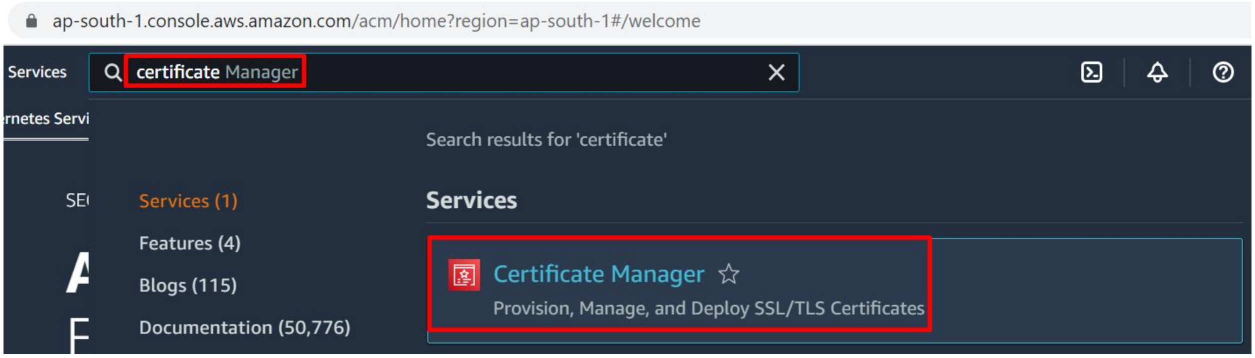
ACM let us use the AWS Management Console, AWS CLI, or AWS Certificate Manager APIs to centrally manage all of the SSL/TLS ACM certificates in an AWS Region.


Before (time-consuming & complex)
3-5 days
3rd Party Certificate Authority
Upload to IAM via AWS CLI
Connect to CloudFront via AWS CLI
After (simple & automated & super fast)
AWS Certificate Manager
End-to-end process within minutes
Using a couple of mouse clicks on the console

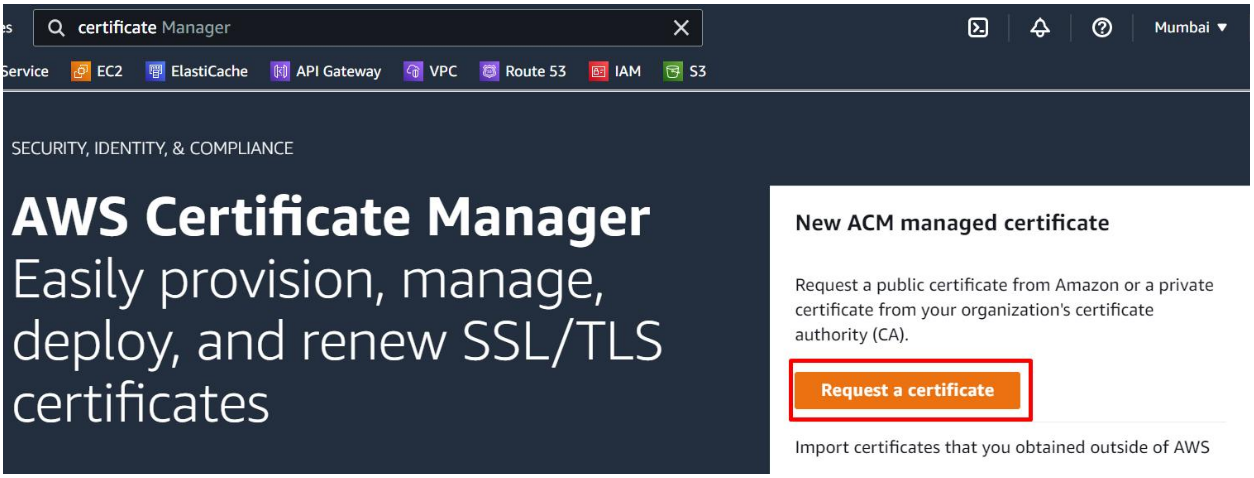
With AWS Certificate Manager, you will be able to quickly request a certificate, deploy it on ACM-integrated AWS resources, like Elastic Load Balancers, Amazon CloudFront distributions, and APIs on API Gateway, and let AWS Certificate Manager handle certificate renewals.

Lab guide

Step-1: search for the certificate manager as shown below:


ap-south-1.console.aws.amazon.com/acm/home?region=ap-south-1#/welcome
Services
certificate Manager
rnetes Servi
Search results for 'certificate'
SE
Services (1)
Features (4)
Blogs (115)
Documentation (50,776)
Services
Certificate Manager
Provision, Manage, and Deploy SSL/TLS Certificates

Step-2: once we click on certificate manager, the following screen will be opened



SECURITY, IDENTITY, & COMPLIANCE

AWS Certificate Manager

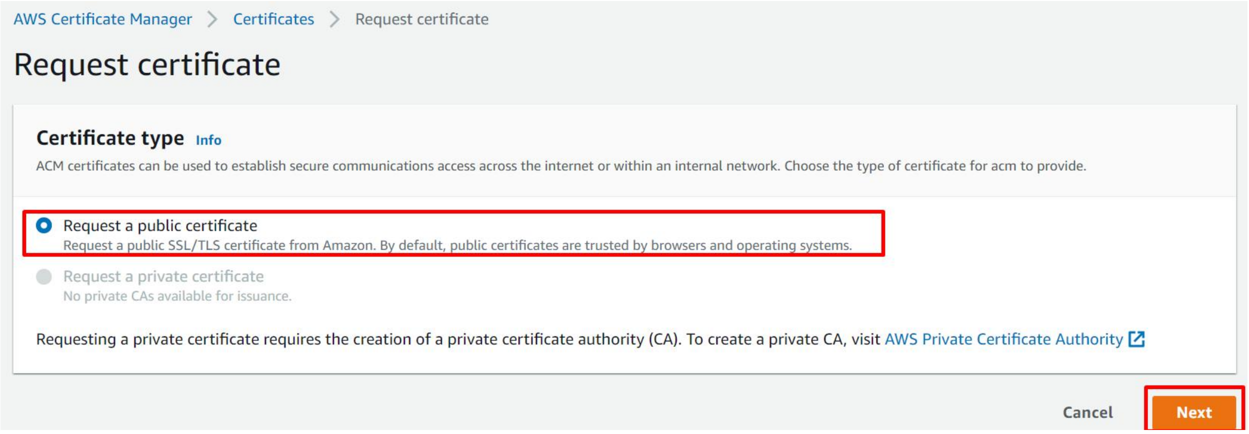
Easily provision, manage, deploy, and renew SSL/TLS certificates

New ACM managed certificate

Request a public certificate from Amazon or a private certificate from your organization's certificate authority (CA).

Import certificates that you obtained outside of AWS

Step-3: once we click on Request Certificate , we can see the below screen


AWS Certificate Manager > Certificates > Request certificate
Info
Cancel
Next

Request certificate

Certificate type

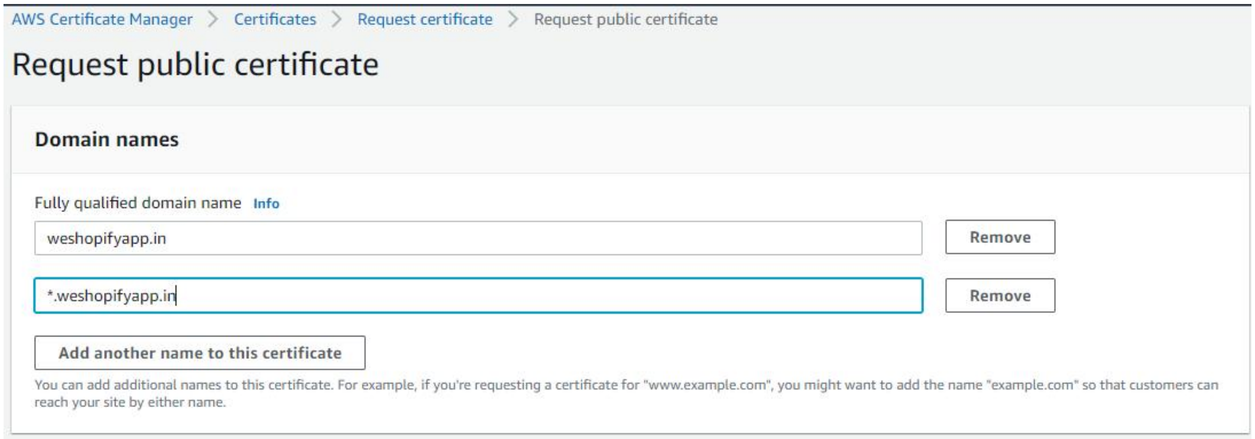
ACM certificates can be used to establish secure communications access across the internet or within an internal network. Choose the type of certificate for acm to provide.

● 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

Step-4: when we click on Request public certificate, the following will be opened


AWS Certificate Manager > Certificates > Request certificate > Request public certificate
Info
Remove
Remove
Add another name to this certificate

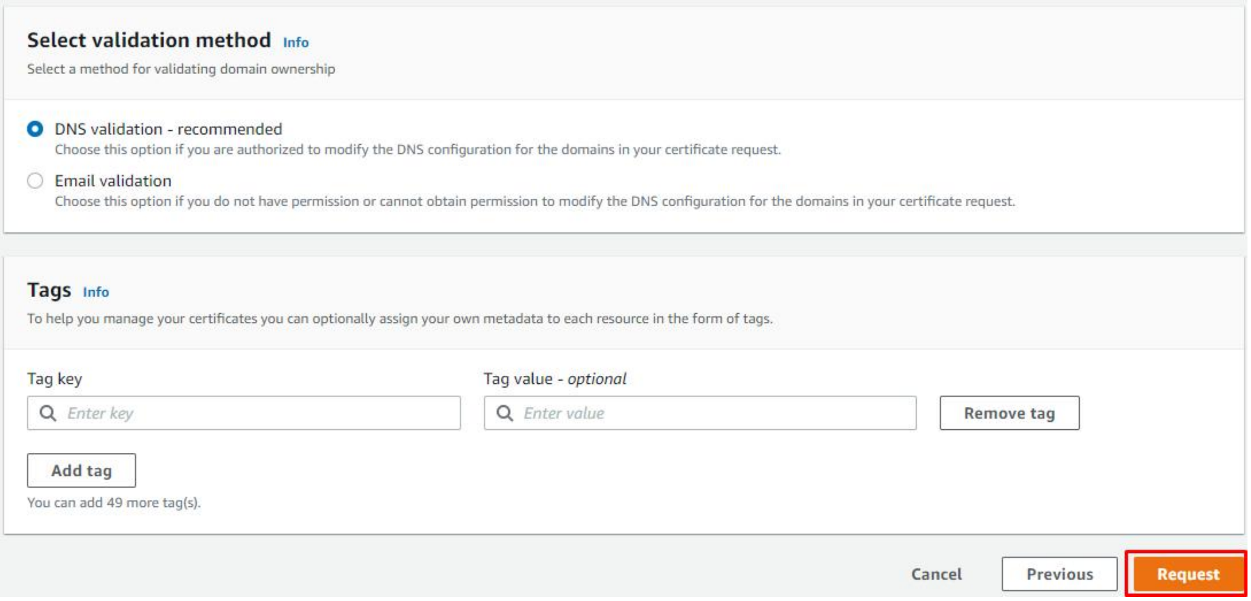
Request public certificate

Domain names

Fully qualified domain name: weshopifyapp.in

*.weshopifyapp.in

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.



Select 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.

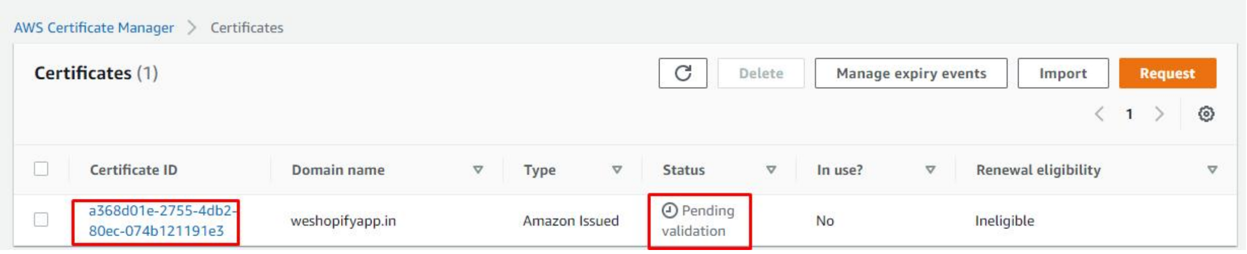
Tags Info

To help you manage your certificates you can optionally assign your own metadata to each resource in the form of tags.

Tag key: *Enter key*
Tag value - *optional*: *Enter value*

You can add 49 more tag(s).

Step-5: when we click on Request button, the certificate will be issued with the pending validation status as shown below:

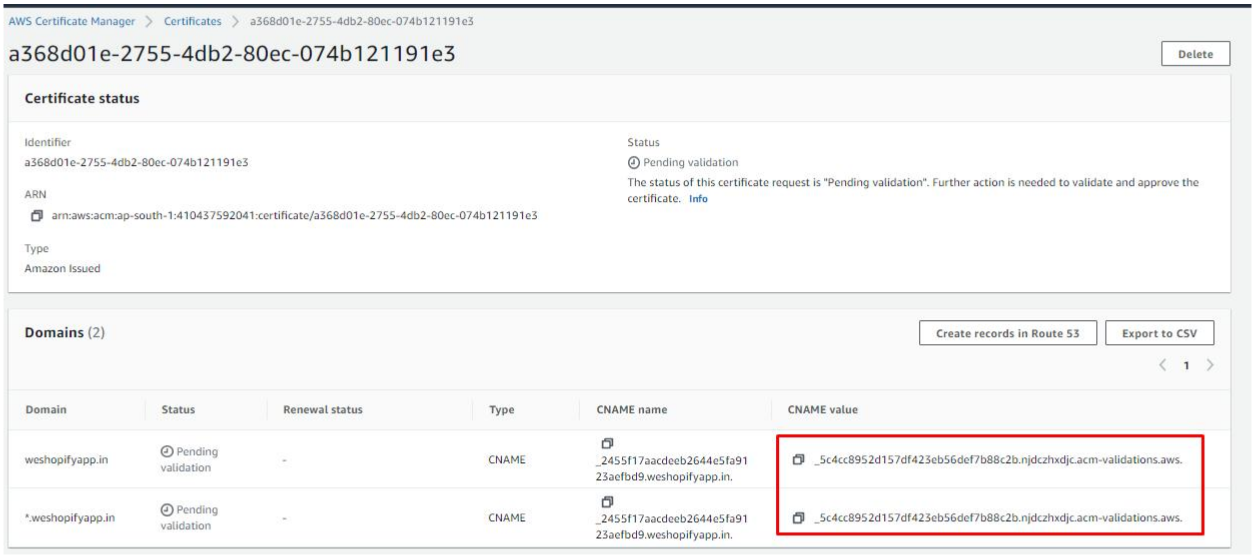


AWS Certificate Manager > Certificates

Certificates (1)

□	Certificate ID	Domain name	Type	Status	In use?	Renewal eligibility
□	a368d01e-2755-4db2-80ec-074b121191e3	weshopifyapp.in	Amazon Issued	Pending validation	No	Ineligible

Step-6: click on Certificate ID as shown below, and copy the CNAME name and value and create the Route Record in Route53.



AWS Certificate Manager > Certificates > a368d01e-2755-4db2-80ec-074b121191e3

a368d01e-2755-4db2-80ec-074b121191e3

Certificate status

Identifier
a368d01e-2755-4db2-80ec-074b121191e3

ARN
arn:aws:acm:ap-south-1:410437592041:certificate/a368d01e-2755-4db2-80ec-074b121191e3

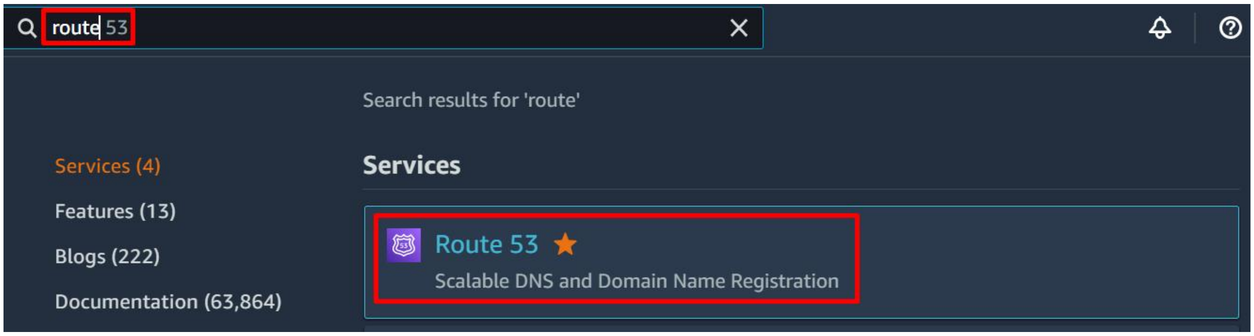
Type
Amazon Issued

Status
Pending validation
The status of this certificate request is "Pending validation". Further action is needed to validate and approve the certificate. Info

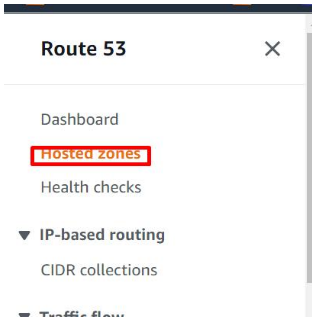
Domains (2)

Domain	Status	Renewal status	Type	CNAME name	CNAME value
weshopifyapp.in	Pending validation	-	CNAME	_2455f17aacdeeb2644e5fa9123aefbd9.weshopifyapp.in.	_5c4cc8952d157df423eb56def7b88c2b.njdczhxdjc.acm-validations.aws.
*.weshopifyapp.in	Pending validation	-	CNAME	_2455f17aacdeeb2644e5fa9123aefbd9.weshopifyapp.in.	_5c4cc8952d157df423eb56def7b88c2b.njdczhxdjc.acm-validations.aws.

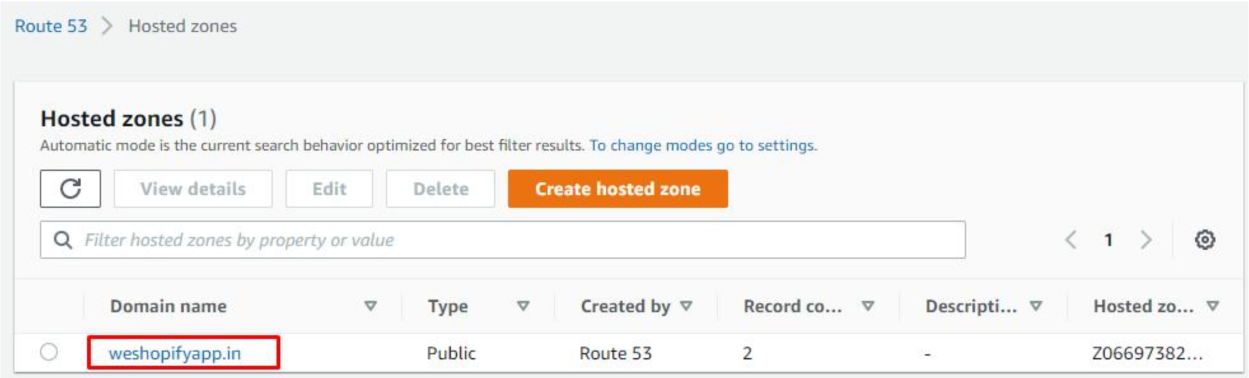
Step-7: update the certificate manager records in Route 53 with the ACM CNAME and CNAME Value as shown below. Search for route 53 in search bar as shown below:



B. Click on hosted zone as shown below:



C. Once we click on Hosted Zones the following screen will be opened



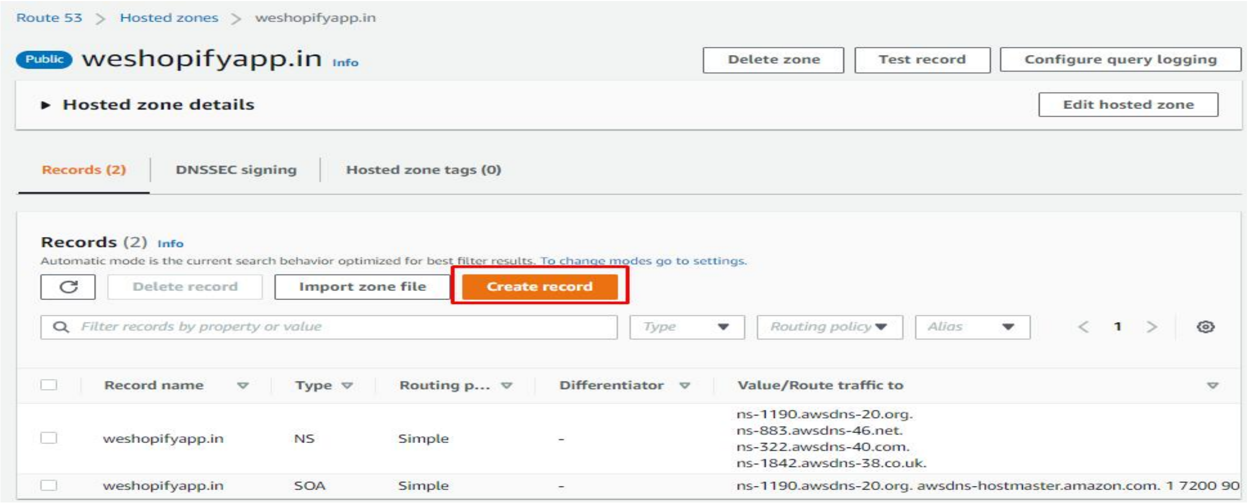
Route 53 > Hosted zones

Hosted zones (1)

Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

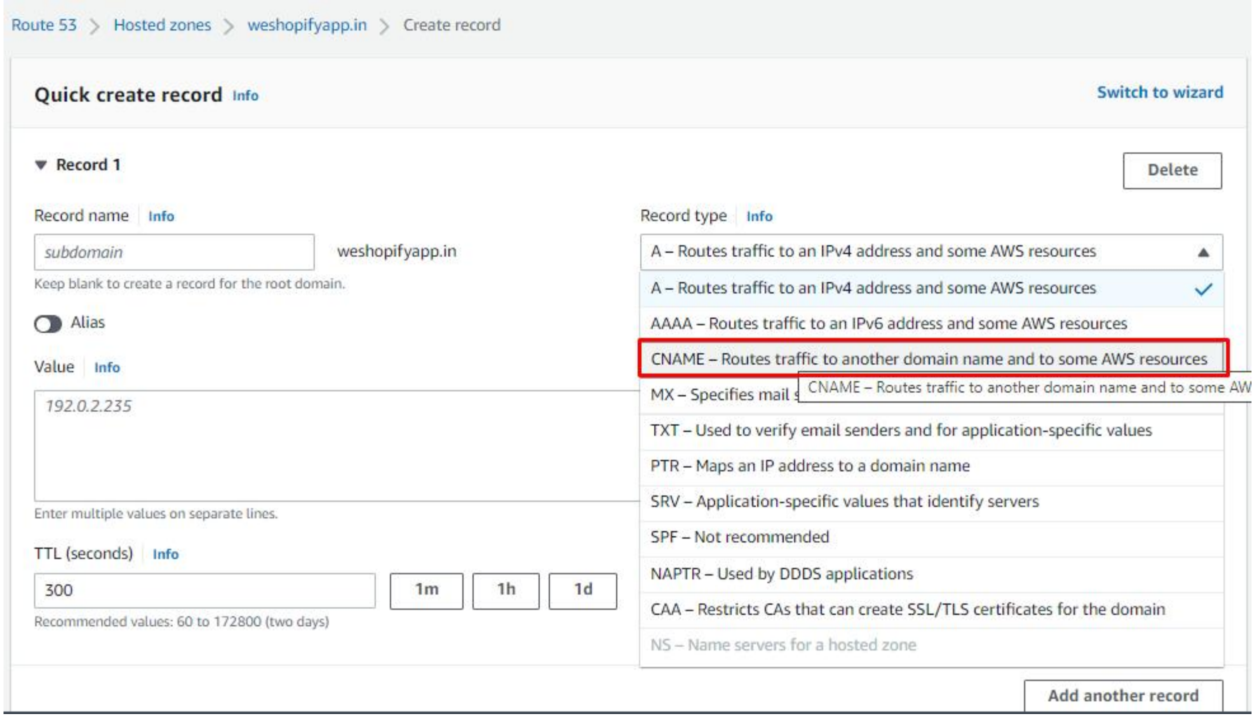
	Domain name	Type	Created by	Record co...	Descripti...	Hosted zo...
○	weshopifyapp.in	Public	Route 53	2	-	Z06697382...

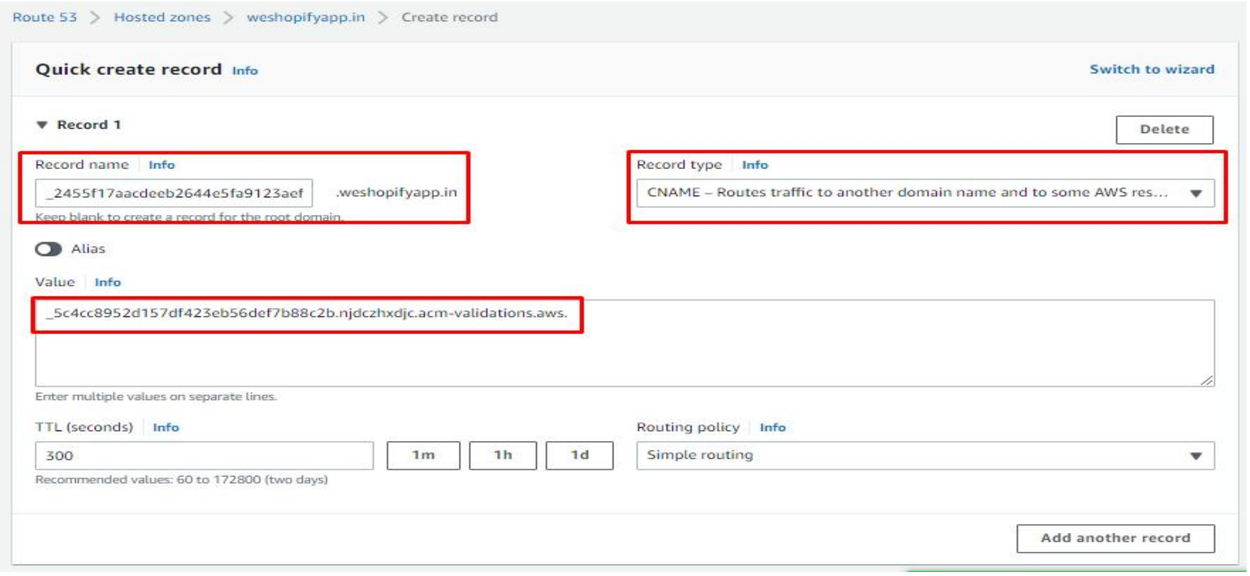
D. When we click on already create hosted zone the following page will be displayed.


Route 53 > Hosted zones > weshopifyapp.in
Public weshopifyapp.in Info
Delete zone
Test record
Configure query logging
▸ Hosted zone details
Edit hosted zone
Records (2)
DNSSEC signing
Hosted zone tags (0)
Records (2) Info
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.
Delete record
Import zone file
Create record
Filter records by property or value
Type
Routing policy
Alias
1

□	Record name	Type	Routing p...	Differentiator	Value/Route traffic to
□	weshopifyapp.in	NS	Simple	-	ns-1190.awsdns-20.org. ns-883.awsdns-46.net. ns-322.awsdns-40.com. ns-1842.awsdns-38.co.uk.
□	weshopifyapp.in	SOA	Simple	-	ns-1190.awsdns-20.org. awsdns-hostmaster.amazon.com. 1 7200 90

C. Click on Create record button as we will get the following screen as shown below , change the record type to CNAME from A as shown below:


Route 53 > Hosted zones > weshopifyapp.in > Create record
Quick create record Info
Switch to wizard
▾ Record 1
Delete
Record name Info
subdomain
weshopifyapp.in
Keep blank to create a record for the root domain.
Alias
Value Info
192.0.2.235
Enter multiple values on separate lines.
TTL (seconds) Info
300
1m
1h
1d
Recommended values: 60 to 172800 (two days)
Record type Info
A – Routes traffic to an IPv4 address and some AWS resources
A – Routes traffic to an IPv4 address and some AWS resources ✓
AAAA – Routes traffic to an IPv6 address and some AWS resources
CNAME – Routes traffic to another domain name and to some AWS resources
MX – Specifies mail s
CNAME – Routes traffic to another domain name and to some AW
TXT – Used to verify email senders and for application-specific values
PTR – Maps an IP address to a domain name
SRV – Application-specific values that identify servers
SPF – Not recommended
NAPTR – Used by DDDS applications
CAA – Restricts CAs that can create SSL/TLS certificates for the domain
NS – Name servers for a hosted zone
Add another record



Route 53 > Hosted zones > weshopifyapp.in > Create record

Quick create record Info

Switch to wizard

▼ Record 1

Delete

Record name | Info

_2455f17aacdeeb2644e5fa9123aef .weshopifyapp.in

Keep blank to create a record for the root domain.

Record type | Info

CNAME – Routes traffic to another domain name and to some AWS res... ▼

○ Alias

Value | Info

_5c4cc8952d157df423eb56def7b88c2b.njdczhxdjc.acm-validations.aws.

Enter multiple values on separate lines.

TTL (seconds) | Info

300

1m 1h 1d

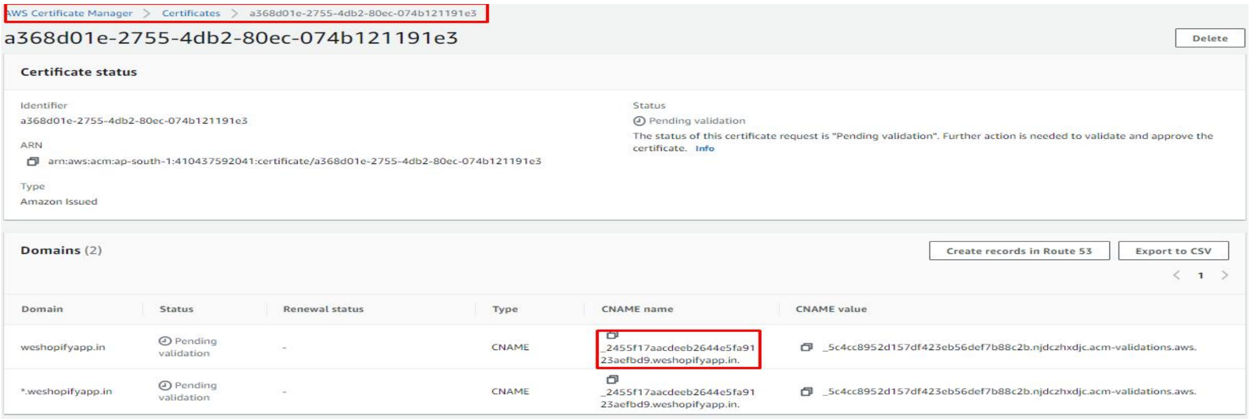
Recommended values: 60 to 172800 (two days)

Routing policy | Info

Simple routing ▼

Add another record

Here give the record name as certificate manager created records CNAME as shown below:



AWS Certificate Manager > Certificates > a368d01e-2755-4db2-80ec-074b121191e3

a368d01e-2755-4db2-80ec-074b121191e3

Delete

Certificate status

Identifier
a368d01e-2755-4db2-80ec-074b121191e3

ARN
arn:aws:acm:ap-south-1:410437592041:certificate/a368d01e-2755-4db2-80ec-074b121191e3

Type
Amazon Issued

Status
Pending validation
The status of this certificate request is "Pending validation". Further action is needed to validate and approve the certificate. Info

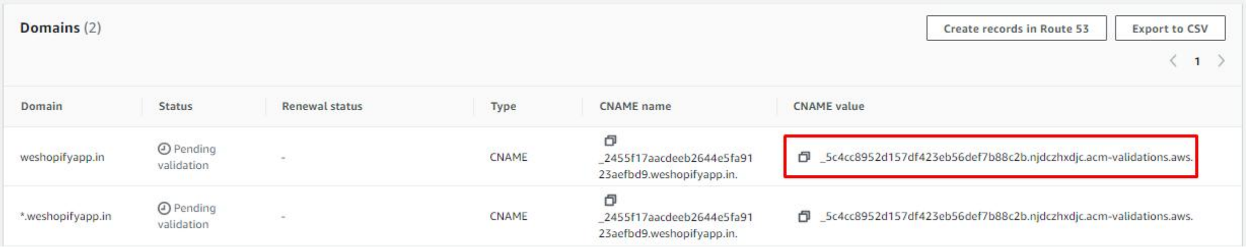
Domains (2)

Create records in Route 53 | Export to CSV

< 1 >

Domain	Status	Renewal status	Type	CNAME name	CNAME value
weshopifyapp.in	Pending validation	-	CNAME	_2455f17aacdeeb2644e5fa9123aefbd9.weshopifyapp.in.	_5c4cc8952d157df423eb56def7b88c2b.njdczhxdjc.acm-validations.aws.
*.weshopifyapp.in	Pending validation	-	CNAME	_2455f17aacdeeb2644e5fa9123aefbd9.weshopifyapp.in.	_5c4cc8952d157df423eb56def7b88c2b.njdczhxdjc.acm-validations.aws.

And in the value of the route 53 domain, create record, cname value give the cname value from the cetificate manager



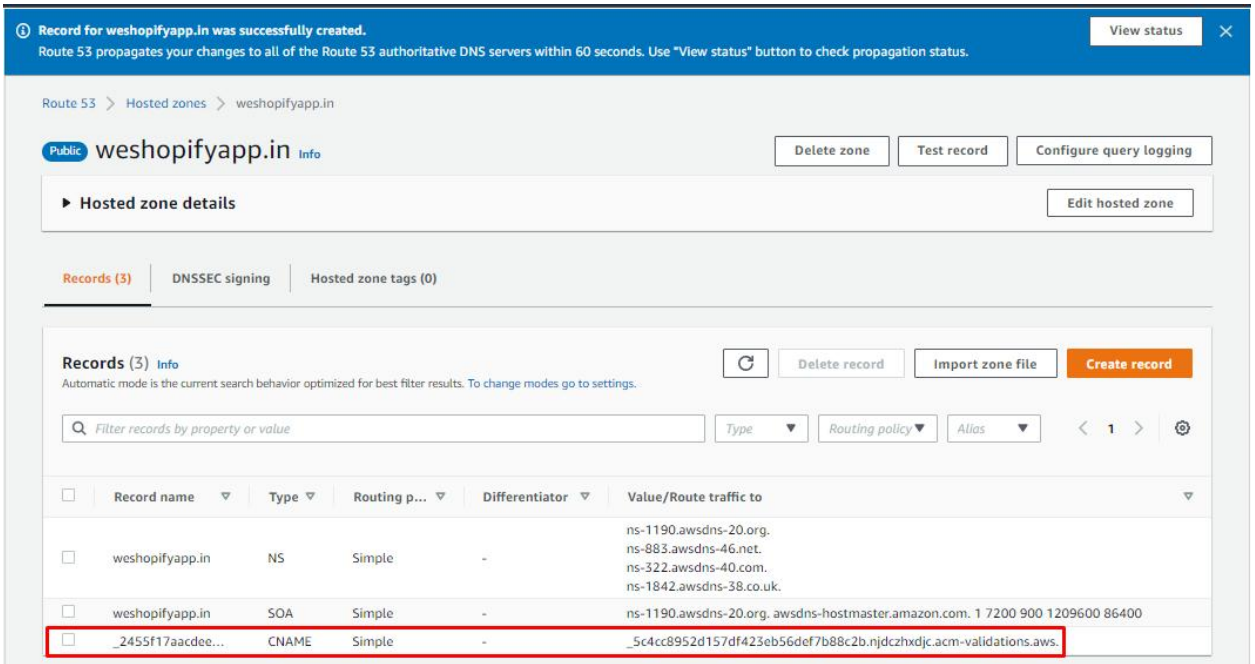
Domains (2)

Create records in Route 53 | Export to CSV

< 1 >

Domain	Status	Renewal status	Type	CNAME name	CNAME value
weshopifyapp.in	Pending validation	-	CNAME	_2455f17aacdeeb2644e5fa9123aefbd9.weshopifyapp.in.	_5c4cc8952d157df423eb56def7b88c2b.njdczhxdjc.acm-validations.aws.
*.weshopifyapp.in	Pending validation	-	CNAME	_2455f17aacdeeb2644e5fa9123aefbd9.weshopifyapp.in.	_5c4cc8952d157df423eb56def7b88c2b.njdczhxdjc.acm-validations.aws.

Clcik on Create records, the added record can be seen as shown below:



Record for weshopifyapp.in was successfully created.
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.

Route 53 > Hosted zones > weshopifyapp.in

Public weshopifyapp.in Info

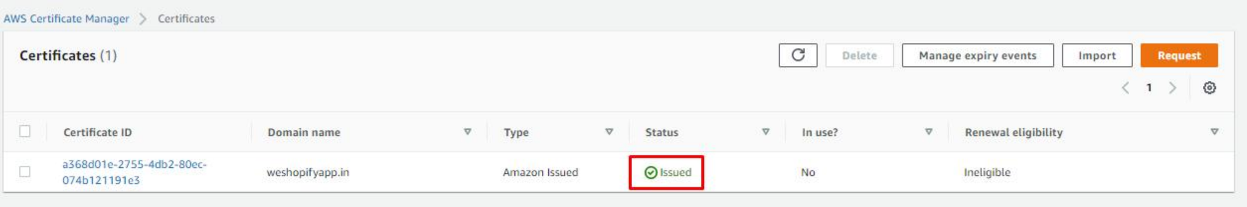
▸ Hosted zone details

Records (3) | DNSSEC signing | Hosted zone tags (0)

Records (3) Info
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

□	Record name	Type	Routing p...	Differentiator	Value/Route traffic to
□	weshopifyapp.in	NS	Simple	-	ns-1190.awsdns-20.org. ns-883.awsdns-46.net. ns-322.awsdns-40.com. ns-1842.awsdns-38.co.uk.
□	weshopifyapp.in	SOA	Simple	-	ns-1190.awsdns-20.org. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
□	_2455f17aacdee...	CNAME	Simple	-	_5c4cc8952d157df423eb56def7b88c2b.njdczhxdjc.acm-validations.aws.

Now go to certificate manager and refresh the status we can see the status as certificate issued by the certificate manager



AWS Certificate Manager > Certificates

Certificates (1)

□	Certificate ID	Domain name	Type	Status	In use?	Renewal eligibility
□	a368d01e-2755-4db2-80ec-074b121191e3	weshopifyapp.in	Amazon Issued	✓ Issued	No	Ineligible