



Lab Certificate Manager

Date	@September 1, 2025
Multi-select	<div>Certificate Manager</div> <div>EC2</div> <div>Load Balancer</div> <div>NAT Gateways</div> <div>Route 53</div> <div>Route Table</div> <div>Security Group</div> <div>Subnet</div> <div>Target Group</div> <div>VPC</div>
Status	Done

Networking

- Create a VPC with CIDR (`10.0.0.0/16`)
- Create 4 Subnets
 - Public Subnet 1 (`10.0.0.0/24`) availability zone `1a`
 - Public Subnet 2 (`10.0.1.0/24`) availability zone `1b`
 - Private Subnet 1 (`10.0.2.0/24`) availability zone `1a`
 - Private Subnet 2 (`10.0.3.0/24`) availability zone `1b`
- Create Internet Gateway (`dev-ig`)
- Create NAT Gateway (`dev-nat`)
- Create a Security Group (`dev-sg`) with rules to allow `SSH` , `HTTP` , and `HTTPS` .

- Create Route Table
 - **Public RT** (associated with `dev-ig` , `Public Subnet 1` , and `Public Subnet 2`)
 - **Private RT** (associated with `dev-nat` , `Private Subnet 1` , and `Private Subnet 2`)
-

Instance Creation

- Launch Instance `Bastion Host` in `Public Subnet 1` and enable a `Auto-assign public IP`
 - Connect to this `Bastion Host` and insert the private key inside the instance:

```
vi key.pem  
chmod 400 key.pem
```

- Launch another instance `Private-EC2` in `Private Subnet 1` and disable `Auto-assign public IP` .
 - Connect to the `Private-EC2` using the private key and `private-ip` :

```
ssh -i private-key ec2-user private-ip
```

- Install `nginx` server on this private server:

```
sudo su -  
yum install nginx -y  
systemctl start nginx  
systemctl status nginx
```

Load Balancer

- Create Target Group `TG-1`

TG-1 Actions

Details
 am:aws:elasticloadbalancing:ap-south-1:226012781271:targetgroup/TG-1/7483141185c33ee0

Target type Instance	Protocol : Port HTTP: 80	Protocol version HTTP1	VPC vpc-017aba6a74e73db5a
IP address type IPv4	Load balancer APP-LB		

1 Total targets 1 Healthy 0 Unhealthy 0 Unused 0 Initial 0 Draining

0 Anomalous

► **Distribution of targets by Availability Zone (AZ)**
 Select values in this table to see corresponding filters applied to the Registered targets table below.

Targets | Monitoring | Health checks | Attributes | Tags

Registered targets (1) Info Anomaly mitigation: Not applicable Deregister Register targets

Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.

Filter targets

Instance ID	Name	Port	Zone	Health status	Health status details	Admini...	Overrid...	Launch...	Anomaly detection...
i-010c1d414b541072e	Private-EC2	80	ap-south-1a (a...	Healthy	-	No override	No overid...	Septembe...	Normal

- Create Load Balancer

APP-LB Actions

Details

Load balancer type Application	Status Active	VPC vpc-017aba6a74e73db5a	Load balancer IP address type IPv4
Scheme Internet-facing	Hosted zone ZP979RAFLXTN2K	Availability Zones subnet-020d7c95a8d6acd4f ap-south-1a (aps1-az1) subnet-03aa9f907c81feb86 ap-south-1b (aps1-az3)	Date created September 1, 2025, 16:51 (UTC+05:30)

Load balancer ARN
am:aws:elasticloadbalancing:ap-south-1:226012781271:loadbalancer/app/APP-LB/cf9e45b55ed49a98

DNS name Info
APP-LB-864568035.ap-south-1.elb.amazonaws.com (A Record)

Listeners and rules (1) Info Manage rules Manage listener Add listener

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.

Filter listeners

Protocol:Port	Default action	Rules	ARN	Security policy	Default SSL/TLS certificate	mTLS	Trust store
HTTP:80	Forward to target group TG-1 1 (100%) Target group stickiness: Off	1 rule	ARN	Not applicable	Not applicable	Not applicable	Not applic

- Access the Load Balancer DNS using `http`.

Not secure <http://app-lb-864568035.ap-south-1.elb.amazonaws.com>

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
 Commercial support is available at nginx.com.

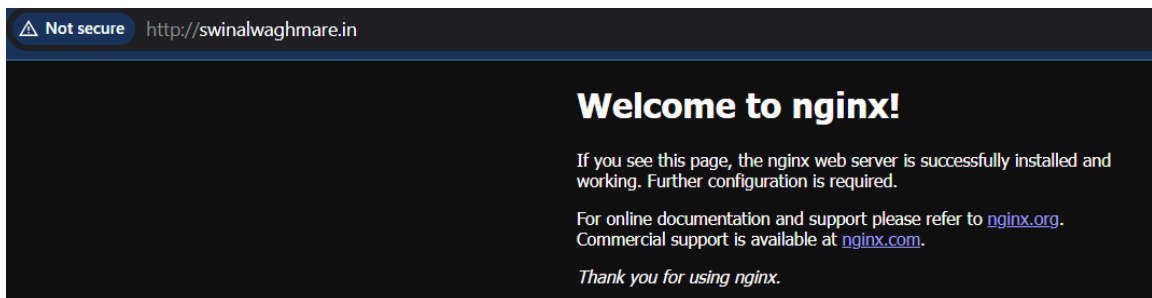
Thank you for using nginx.

Accessing the Load Balancer Using Domain

- Create an **A** Record (alias):

- Route traffic to **Application and Classic Load Balancer**
- Region: **Asia Pacific (Mumbai)**
- Endpoint: Select the Load Balancer
- Routing Policy: **Simple routing**

- Access the Load Balancer using the domain name `http://swinalwaghmare.in` .



Creation of Certificate

- Request a certificate:
 - Type: `Request a public certificate`
 - Domain name (e.g., `swinalwaghmare.in`)
 - Validation Method: `DNS Validation`
 - Key Algorithm: `RSA 2048`

Request public certificate

Domain names
Provide one or more domain names for your certificate.

Fully qualified domain name [Info](#)

swinalwaghmare.in

[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.

Allow export [Info](#)

☒ **Disable export**
Use this certificate only with integrated AWS services. The private key for this certificate will be disallowed for exporting from AWS.

☐ **Enable export**
Export this certificate and private key for use with any TLS workflow. ACM will charge your account based on the requested domains when the certificate is issued for the first time and for each renewal.

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**
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](#)

- Create the required **CNAME record** in Route 53 for Certificate Manager.

Domains (1) [Create records in Route 53](#) [Export to CSV](#)

Domain	Status	Renewal status	Type	CNAME name	CNAME value
swinalwaghmare.in	Success	-	CNAME	_04c15c180d02fd4141bd48fd49b597d0.swinalwaghmare.in.	_b9baf4c9b2da154ccb4f1772bb69dbf.xlfgmrnv4.validations.aws.

- Once validated, the certificate will be issued.

Certificates (1) [Refresh](#) [More actions](#) [Manage expiry events](#) [Import](#) [Request](#)

<input type="checkbox"/>	Certificate ID	Domain name	Type	Status	In use
<input type="checkbox"/>	c8f5708b-1f49-45f2-b7b7-4c177bb9fc03	swinalwaghmare.in	Amazon Issued	Issued	No

Adding an HTTPS Listener to the Load Balancer

- Add a listener for **HTTPS** and attach the certificate.

Add listener [Info](#)

Add a listener to your Application Load Balancer (ALB) to define how client requests and network traffic are routed within your application. Every listener is made up of a default action that's required and can only be edited. Additional rules can be added, edited and deleted from the listener.

► **Load balancer details:** APP-LB

Listener: HTTPS:443

A listener checks for connection requests using the protocol and port that you configure. The default action and any additional rules that you create determine how the Application Load Balancer routes requests to its registered targets.

Protocol
Used for connections from clients to the load balancer.

Port
The port on which the load balancer is listening for connections.

HTTPS 443
1-65535

Default action [Info](#)
The default action is used if no other rules apply. Choose the default action for traffic on this listener.

Authentication action - optional [Info](#)
Authentication requires IPv4 connectivity to authentication endpoints. [Learn more](#)

☐ **Authenticate users**
Configure user authentication through either OpenID Connect (OIDC) or Amazon Cognito.

Routing action

☒ Forward to target groups ☐ Redirect to URL ☐ Return fixed response

Forward to target group [Info](#)
Choose a target group and specify routing weight or [create target group](#)

Target group
TG-1
Target type: Instance, IPv4 | Target stickiness: Off HTTP 1 100%
0-999

+ Add target group
You can add up to 4 more target groups.

Target group stickiness [Info](#)
Enables the load balancer to bind a user's session to a specific target group. To use stickiness the client must support cookies. If you want to bind a user's session to a specific target, turn on the Target Group attribute Stickiness.

☐ Turn on target group stickiness

Secure listener settings [Info](#)

Security policy [Info](#)
Your load balancer uses a Secure Socket Layer (SSL) negotiation configuration called a security policy to manage SSL connections with clients. [Compare security policies](#)

Security category
All security policies

Policy name
ELBSecurityPolicy-TLS13-1-2-Res-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.

swinalwaghmare.in
c815708b-1149-45f2-b767-4c1776b9fc03

[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.

- Now the Load Balancer has two listeners: HTTP and HTTPS .

APP-LB [Info](#) [Actions](#)

Details

Load balancer type Application	Status Active	VPC vpc-017ab6a74e73db5a	Load balancer IP address type IPv4
Scheme Internet-facing	Hosted zone ZP97RAFLXNZK	Availability Zones subnet-020d7c95a8d6acd4f ap-south-1a (aps1-az1) subnet-03aa9f907c81feb86 ap-south-1b (aps1-az3)	Date created September 1, 2025, 16:51 (UTC+05:30)
Load balancer ARN arn:aws:elasticloadbalancing:ap-south-1:226012781271:loadbalancer/app/APP-LB/cf9e45b55ed48a98		DNS name Info APP-LB-864568035.ap-south-1.elb.amazonaws.com (A Record)	

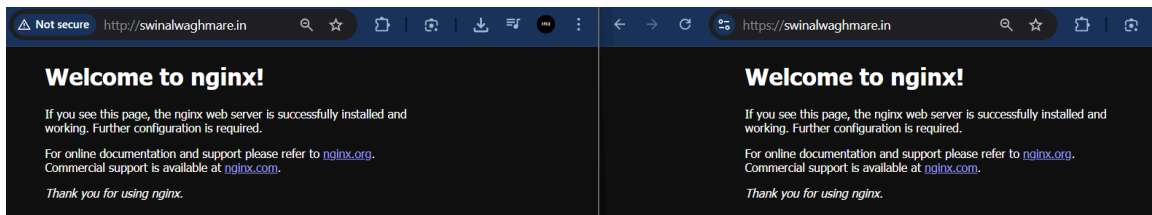
Listeners and rules [Info](#) [Manage rules](#) [Manage listener](#) [Add listener](#)

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.

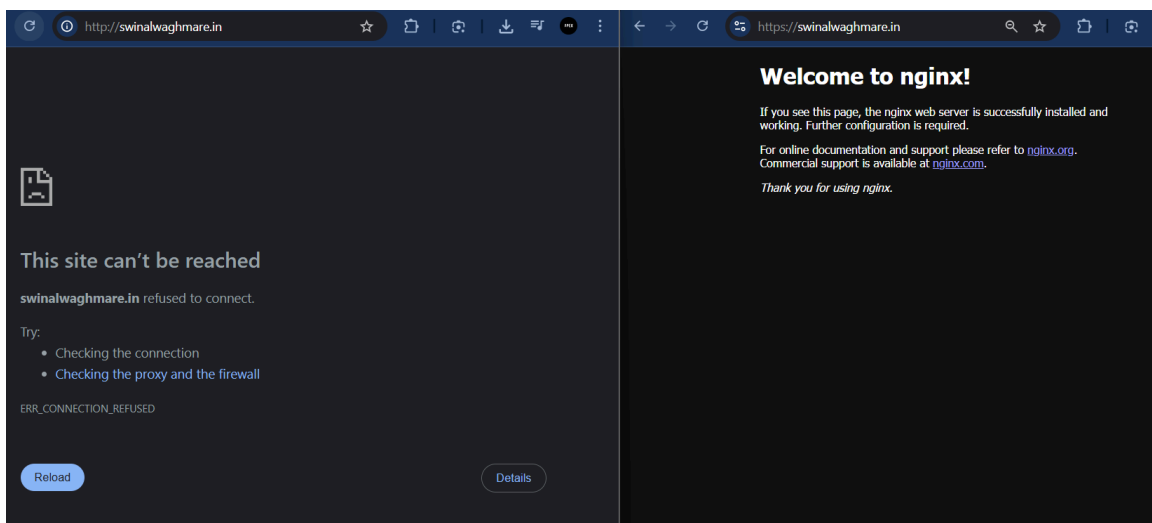
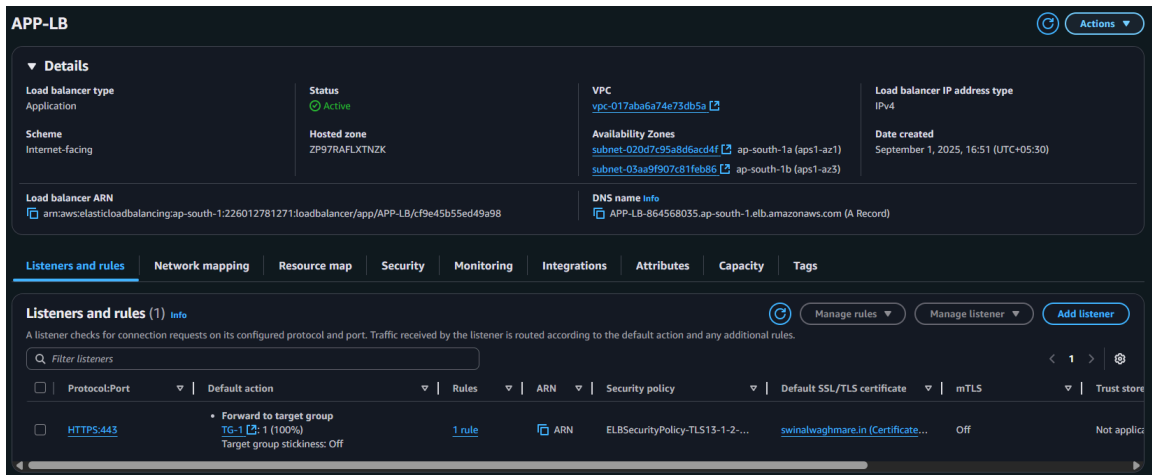
Filter listeners

Protocol:Port	Default action	Rules	ARN	Security policy	Default SSL/TLS certificate	mTLS	Trust store
<input type="checkbox"/> HTTPS:443	Forward to target group TG-1 (100%) Target group stickiness: Off	1 rule	ARN	ELBSecurityPolicy-TLS13-1-2-...	swinalwaghmare.in (Certificate...	Off	Not applic
<input type="checkbox"/> HTTP:80	Forward to target group TG-1 (100%) Target group stickiness: Off	1 rule	ARN	Not applicable	Not applicable	Not applicable	Not applic

- Since we already have a record in Route 53 for the domain, we can access the domain using both http and https .



- If we delete one of the listeners (e.g., **HTTP**), the domain will only be accessible via the remaining protocol (**HTTPS**).



Accessing Through Sub Domain

- Create a subdomain record: **api.swinalwaghmare.in**.

Create record info

Quick create record Switch to wizard

▼ Record 1 Delete

Record name info .swinalwaghmare.in Record type info A - Routes traffic to an IPv4 address and some AWS resources ▼

Keep blank to create a record for the root domain.

☒ Alias

Route traffic to info

Alias to Application and Classic Load Balancer ▼

Asia Pacific (Mumbai) ▼

✕

Alias hosted zone ID: ZP97RAFLXTN2K

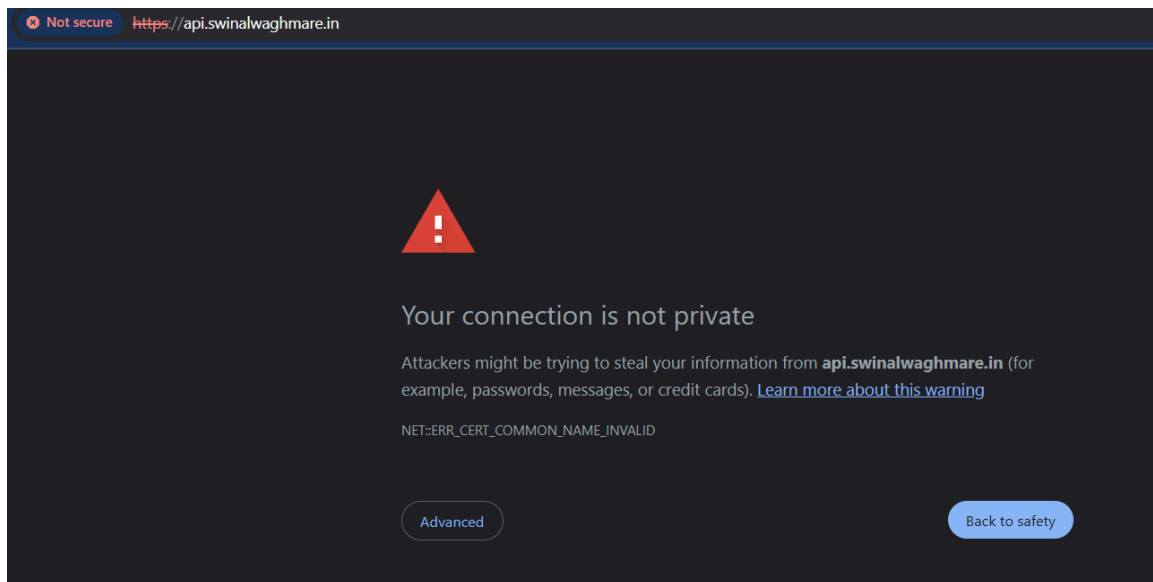
Routing policy info Simple routing ▼

Evaluate target health ☒ Yes

Add another record

Cancel Create records

- Since we only have an **HTTPS** listener, this subdomain cannot be accessed via **https** because the certificate is mapped only to **swinalwaghmare.in**.



- To allow access via **http**, add an **HTTP listener** to the Load Balancer.

APP-LB Actions

Details
Load balancer type
Application
Scheme
Internet-facing
Load balancer ARN
arn:aws:elasticloadbalancing:ap-south-1:226012781271:loadbalancer/app/APP-LB/cf9e45b55ed49a98

Status
Active
Hosted zone
ZP97RAFLXTNZK
VPC
vpc-017aba6a74e73db5a
Availability Zones
subnet-020d7c95a8d6acd4f ap-south-1a (aps1-az1)
subnet-03aa9f907c81feb86 ap-south-1b (aps1-az3)
Load balancer IP address type
IPv4
Date created
September 1, 2025, 16:51 (UTC+05:30)

DNS name info
APP-LB-864568035.ap-south-1.elb.amazonaws.com (A Record)

Listeners and rules (2) info Manage rules Manage listener Add listener

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.

Filter listeners

Protocol:Port	Default action	Rules	ARN	Security policy	Default SSL/TLS certificate	mTLS	Trust store
<input type="checkbox"/> HTTP:80	<ul style="list-style-type: none"> Forward to target group TG-1 [100%] Target group stickiness: Off 	1 rule	ARN	Not applicable	Not applicable	Not applicable	Not applicable
<input type="checkbox"/> HTTPS:443	<ul style="list-style-type: none"> Forward to target group TG-1 [100%] Target group stickiness: Off 	1 rule	ARN	ELBSecurityPolicy-TLS13-1-2-...	swinalwaghmare.in (Certificate...	Off	Not applicable

- After adding the listener, the subdomain can be accessed using `http`.

Not secure http://api.swinalwaghmare.in

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

Accessing Subdomain via HTTPS

- Create a certificate for the subdomain.

a2bc02bc-638d-490a-bdab-bda3eee86658 Delete

Certificate status

Identifier
a2bc02bc-638d-490a-bdab-bda3eee86658
Status
Issued
ARN
arn:aws:acm:ap-south-1:226012781271:certificate/a2bc02bc-638d-490a-bdab-bda3eee86658
Type
Amazon Issued

Domains (1) Create records in Route 53 Export to CSV

Domain	Status	Renewal status	Type	CNAME name	CNAME value
api.swinalwaghmare.in	Success	-	CNAME	_a6afe618ds9d837fae1f3a8f0338122c.api.swinalwaghmare.in.	_12db5d284eeb0c552be37ae548b395f0.x-validations.aws.

- Add an `HTTPS` listener for the subdomain in the Load Balancer.

Listener: HTTPS:444
A listener checks for connection requests using the protocol and port that you configure. The default action and any additional rules that you create determine how the Application Load Balancer routes requests to its registered targets.

Protocol
Used for connections from clients to the load balancer.
HTTPS

Port
The port on which the load balancer is listening for connections.
444
1-65535

Default action [Info](#)
The default action is used if no other rules apply. Choose the default action for traffic on this listener.

Authentication action - optional [Info](#)
Authentication requires IPv4 connectivity to authentication endpoints. [Learn more](#) [🔗](#)
☐ **Authenticate users**
Configure user authentication through either OpenID Connect (OIDC) or Amazon Cognito.

Routing action
☒ **Forward to target groups** ☐ Redirect to URL ☐ Return fixed response

Forward to target group [Info](#)
Choose a target group and specify routing weight or [create target group](#) [🔗](#).

Target group	Weight	Percent
TG-1 Target type: Instance, IPv4 Target stickiness: Off	1 0-999	100%

[+ Add target group](#)
You can add up to 4 more target groups.

Target group stickiness [Info](#)
Enables the load balancer to bind a user's session to a specific target group. To use stickiness the client must support cookies. If you want to bind a user's session to a specific target, turn on the Target Group attribute Stickiness.
☐ **Turn on target group stickiness**

Secure listener settings [Info](#)

Security policy [Info](#)
Your load balancer uses a Secure Socket Layer (SSL) negotiation configuration called a security policy to manage SSL connections with clients. [Compare security policies](#) [🔗](#)

Security category
All security policies

Policy name
ELBSecurityPolicy-TLS13-1-2-Res-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.

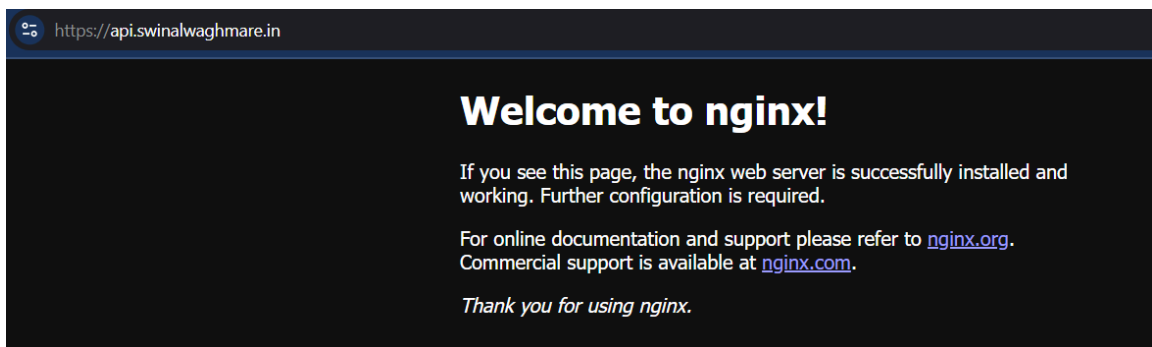
Certificate source
☒ From ACM ☐ From IAM ☐ Import certificate

Certificate (from ACM)
The selected certificate will be applied as the default SSL/TLS server certificate for this load balancer's secure listeners.
api.swinalwaghmare.in
a2bc02bc-658d-490a-bda8-bda5eed86658

[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.

- Now the subdomain `api.swinalwaghmare.in` can be accessed securely via `https`.



Creating a Wildcard Certificate for All Subdomains

- Create a wildcard certificate `.swinalwaghmare.in`.

Certificates (3)						
More actions Manage expiry events Import Request						
<input type="checkbox"/>	Certificate ID	Domain name	Type	Status	In use	Renewal eligibility
<input type="checkbox"/>	dff8971f-4b77-4289-866c-970abe1790c9	*swinalwagmare.in	Amazon Issued	Issued	No	Ineligible
<input type="checkbox"/>	a2bc02bc-638d-490a-bdab-bda3eee86658	api.swinalwagmare.in	Amazon Issued	Issued	Yes	Eligible
<input type="checkbox"/>	c8f5708b-1f49-45f2-b7b7-4c177bb9fc03	swinalwagmare.in	Amazon Issued	Issued	No	Ineligible

- Create a subdomain record: `aws.swinalwagmare.in`.

Create record

Quick create record

Record 1

Record name

aws

.swinalwagmare.in

Record type

A – Routes traffic to an IPv4 address and some AWS resources

Alias

Route traffic to

Alias to Application and Classic Load Balancer

Asia Pacific (Mumbai)

dualstack-APP-LB-864568035.ap-south-1.elb.amazonaws.com

Routing policy

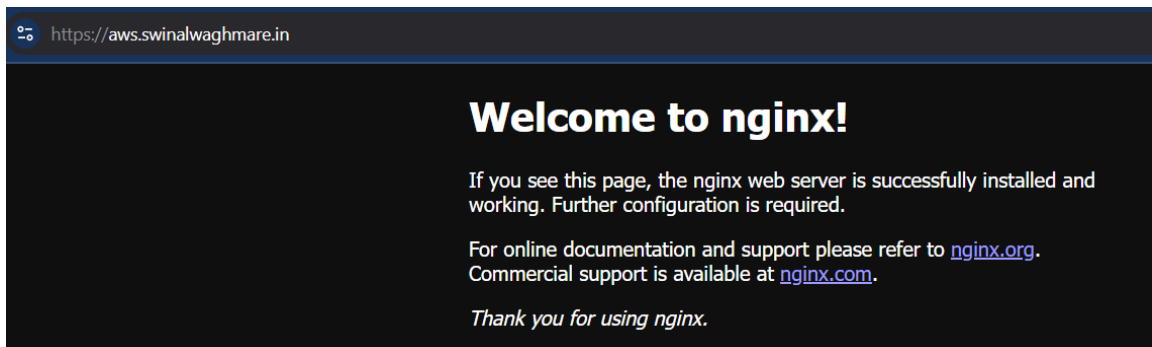
Simple routing

Evaluate target health

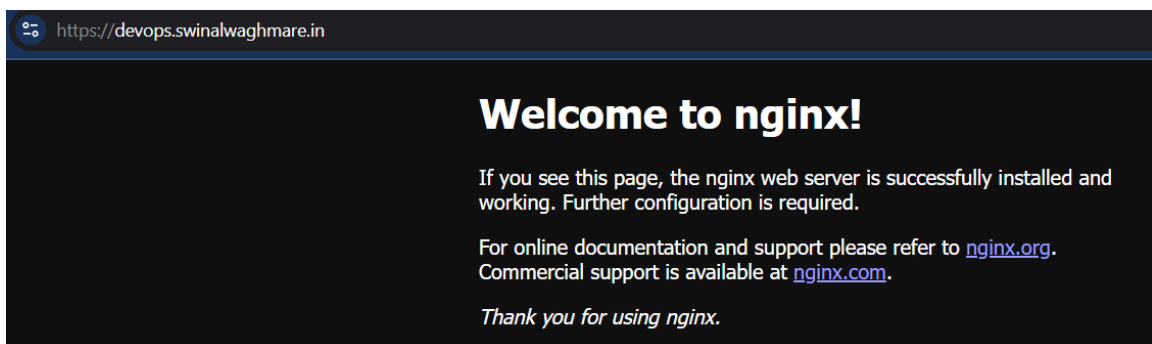
Yes

Add another record

- Add an `HTTPS` listener to the Load Balancer for this subdomain.



- Create another subdomain record for testing: `devops.swinalwagmare.in`.



- This subdomain can also be accessed via `https` using the same wildcard certificate.