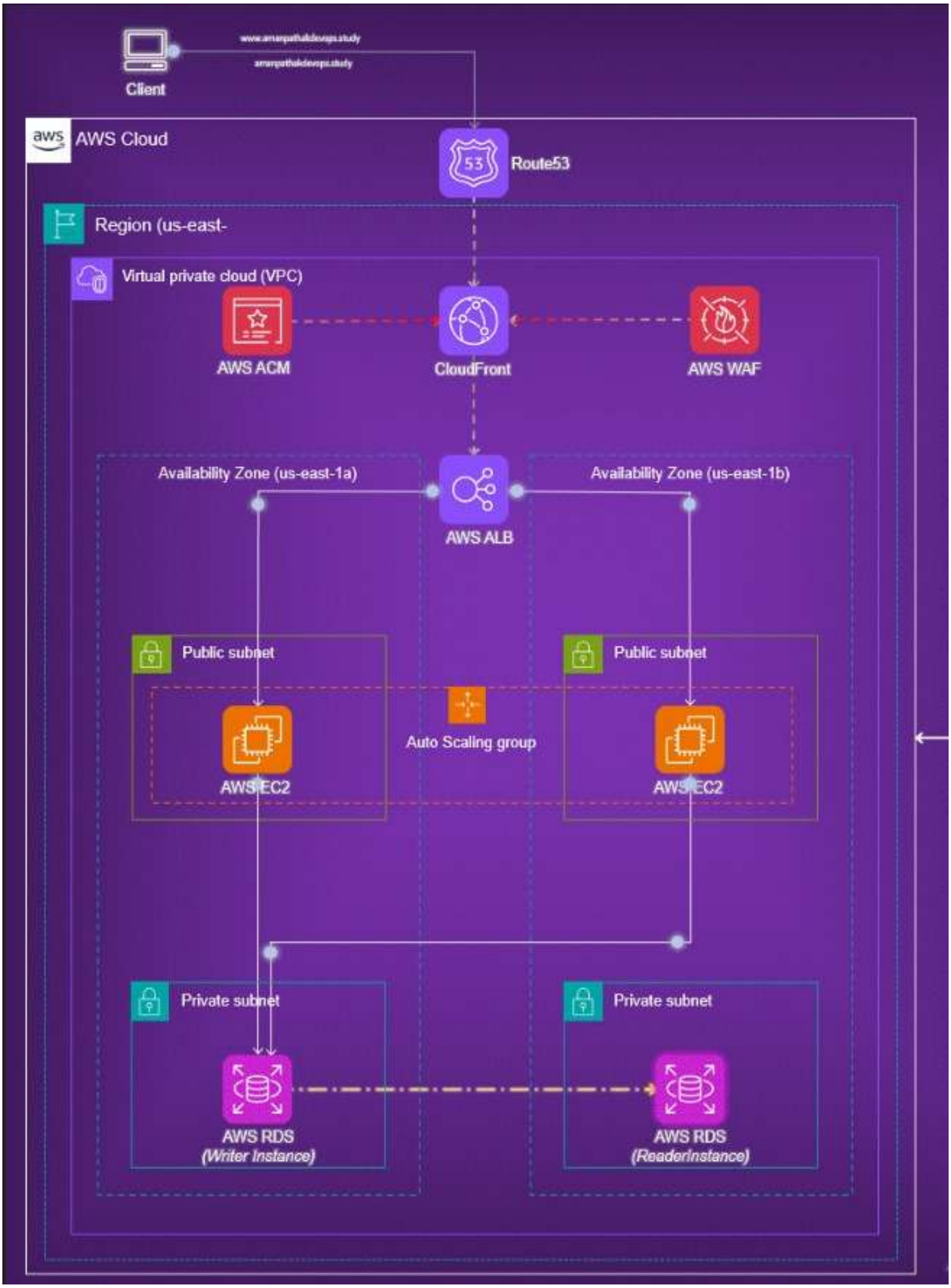
Project-2: Route53



This AWS architecture ensures a secure, scalable, and highly available web application setup. Route 53 routes traffic to CloudFront, which uses WAF for protection and ACM for SSL. Traffic is then sent to an Application Load Balancer (ALB) that distributes it to EC2 instances in an Auto Scaling Group across two Availability Zones. The EC2 instances handle application logic and connect to RDS databases (Writer and Reader) hosted in private subnets. This setup improves performance, ensures redundancy, and enhances security.

Step-1 : VPC Set Up

i) Create vpc (cidr- 10.0.0.0/16, tag- route-53)

ii) Edit vpc (enable DNS hostnames)

iii) Create subnets (public-1a 10.0.1.0/24, public-1b 10.0.2.0/24, private-1a 10.0.3.0/24, private-1b 10.0.4.0/24)

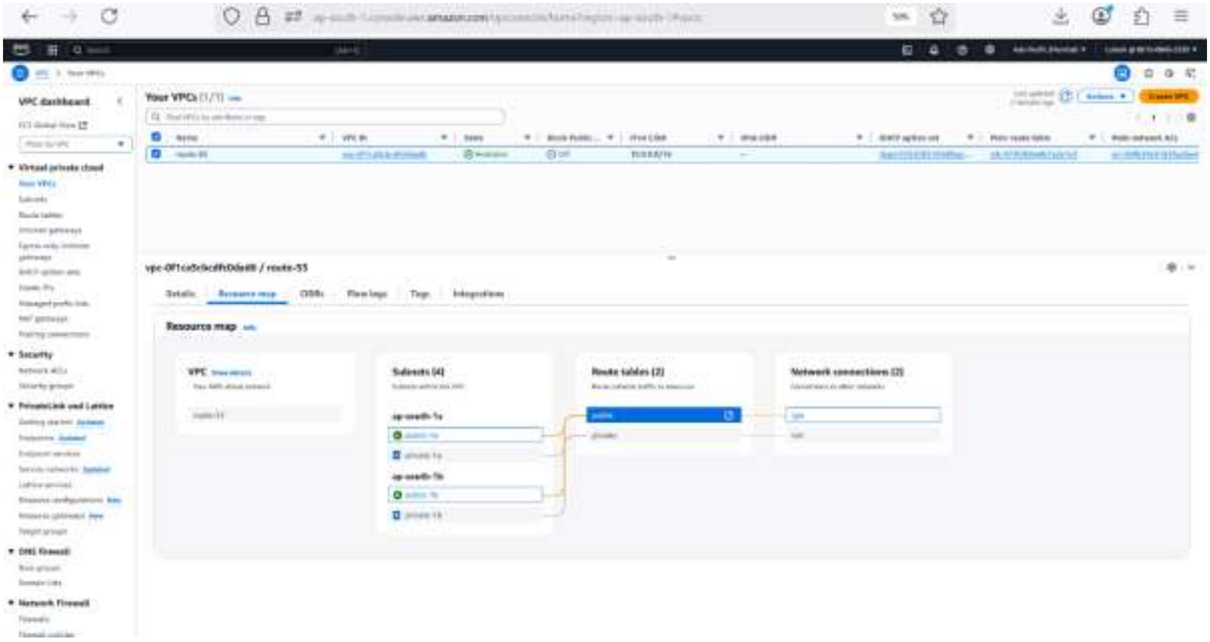
iv) Create internet gateway and attach it to vpc

v) Create route table (public, private)

vi) Edit route tables (add igw to public route and associate it with public subnets, add private subnet to private route table)

vii) Create Nat gateway for security associate it with elastic ip

viii) Edit private route table and add Nat gateway



VPC dashboard

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Security

PrivateLink and Lattice

DNS Firewall

Network Firewall

Your VPCs (1/1)

Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table	Main network ACL
route-55	[illegible]	Available	Off	10.0.0.0/16	–	[illegible]	[illegible]	[illegible]

vpc-0f1ca5cbcdfc0dad8 / route-55

Details | Resource map | CIDRs | Flow logs | Tags | Integrations

Resource map

VPC

route-55

Subnets (4)

ap-south-1a

public-1a

private-1a

ap-south-1b

public-1b

private-1b

Route tables (2)

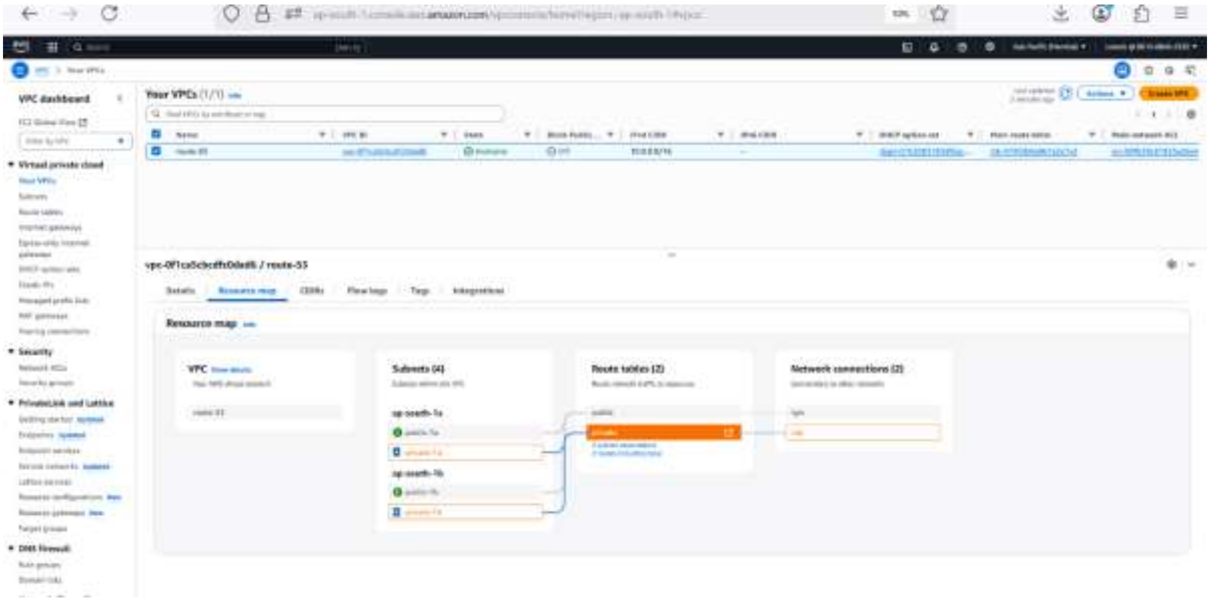
public

private

Network connections (2)

igw

nat



VPC dashboard

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Security

PrivateLink and Lattice

DNS Firewall

Your VPCs (1/1)

Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table	Main network ACL
route-55	[illegible]	Available	Off	10.0.0.0/16	–	[illegible]	[illegible]	[illegible]

vpc-0f1ca5cbcdfc0dad8 / route-55

Details | Resource map | CIDRs | Flow logs | Tags | Integrations

Resource map

VPC

route-55

Subnets (4)

ap-south-1a

public-1a

private-1a

ap-south-1b

public-1b

private-1b

Route tables (2)

public

private

Network connections (2)

igw

nat

Step-2 : EC2 Set Up

i) Create ec2 instance Name as public-1a and public-1b

ii) Select subnet public-1a for public -1a ec2, instance type is t2.micro, ami is amazon linux

iii) Create a key pair

iv) Create security group add ssh, http and https – 22,80,443

v) After creating two instance then come to next stage

vi) Create launch Templates, use recently used ami only and add instance type and security group to it

vii) Now, create a target group name it as route, add two instance init and include as pending only, create it

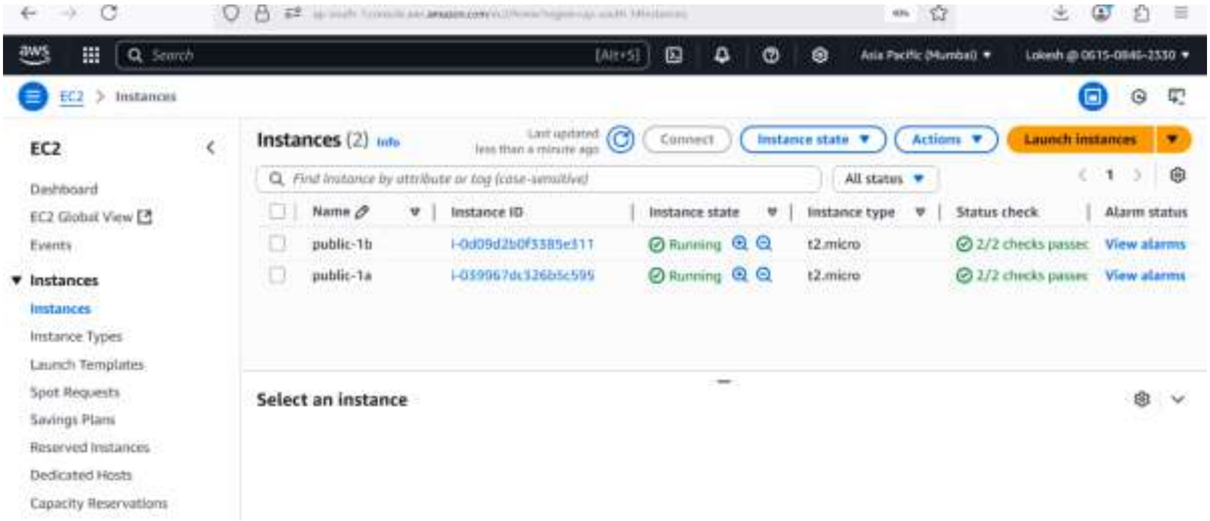
viii) Check target group health

ix) Create a load balancer name it as route-lb

x) Edit load balance, click on add listener add path base condition and add two ec2 instance, give http and https to secure browser

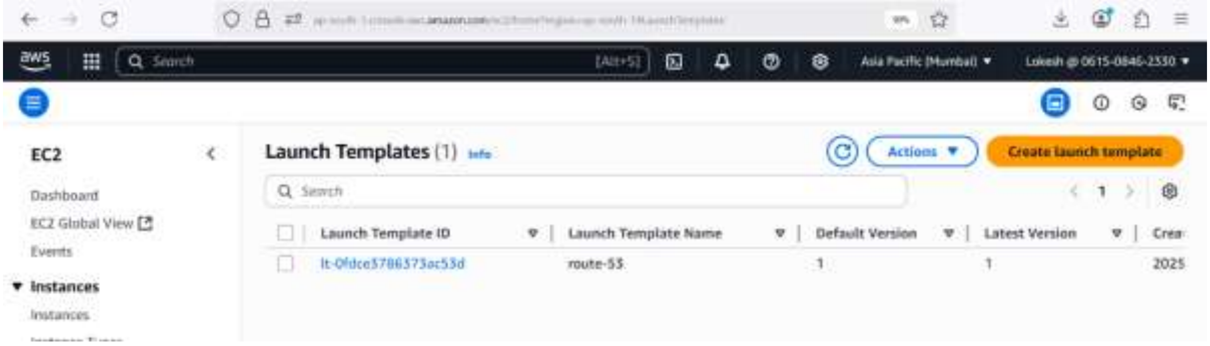
xi) Create auto scaling group and add min-max instance to launch

xii) After creating asg you can see two instance were created in the instance



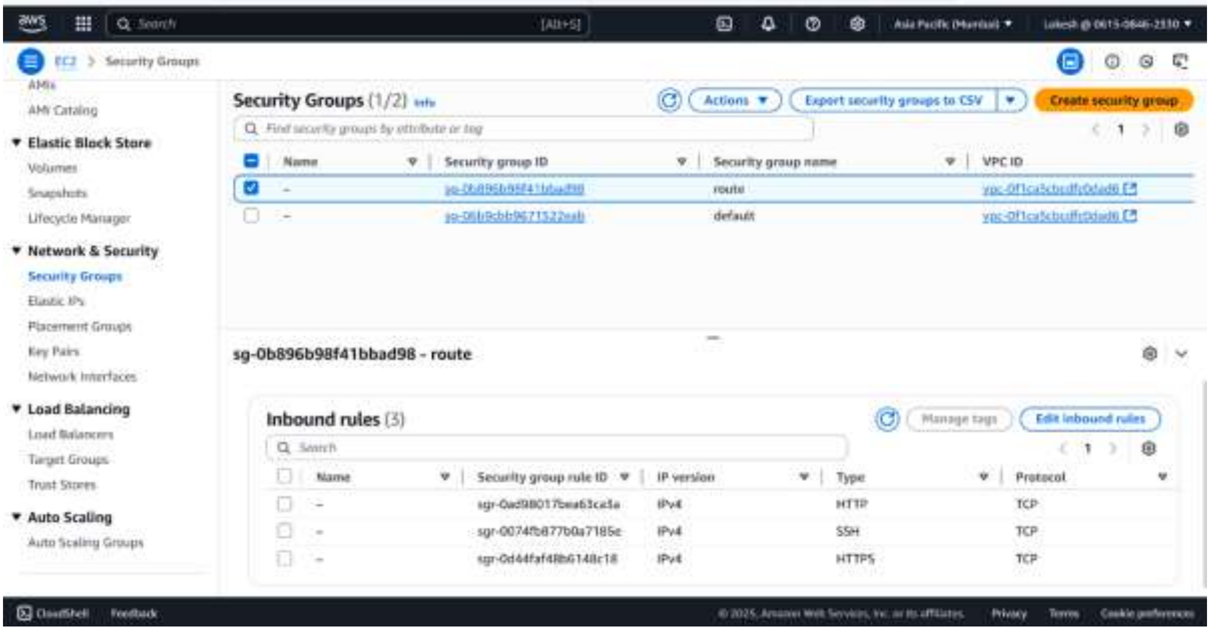
Instances (2) Info

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
□	public-1b	i-0d09d2b0f3385e311	Running	t2.micro	2/2 checks passec	View alarms
□	public-1a	i-039967dc326b5c595	Running	t2.micro	2/2 checks passec	View alarms



Launch Templates (1) Info

	Launch Template ID	Launch Template Name	Default Version	Latest Version	Crea
□	lt-0fdce3786373ac53d	route-53	1	1	2025



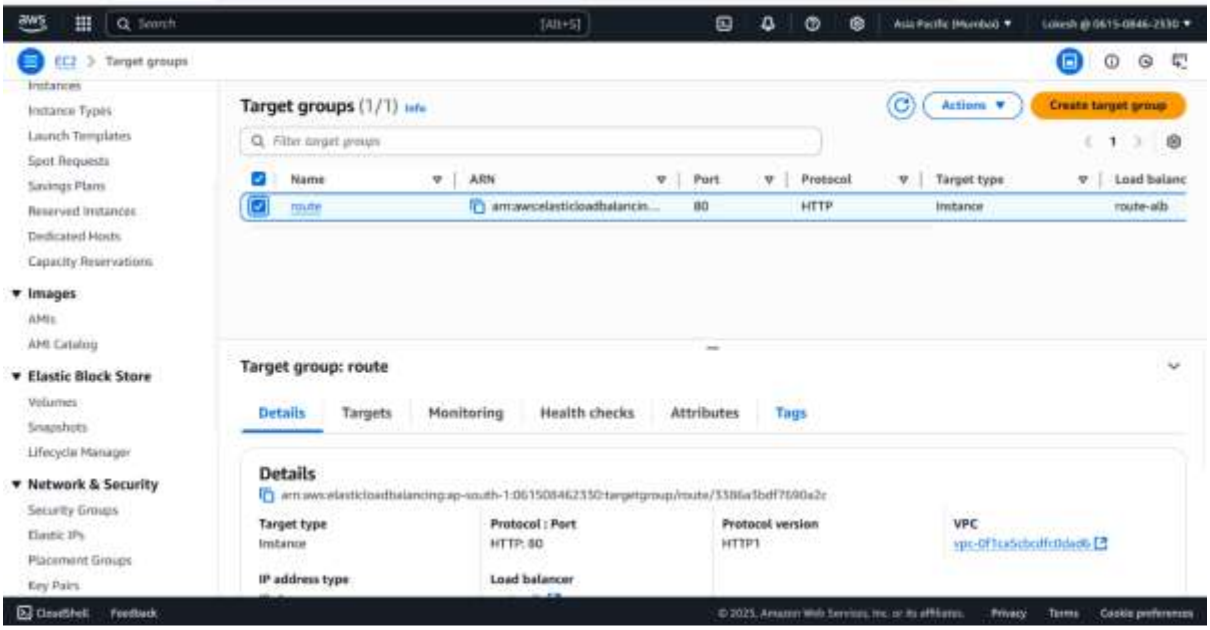
Security Groups (1/2) Info

☐	Name	Security group ID	Security group name	VPC ID
☑	–	sg-0b896b98f41bbad98	route	vpc-0f1ca5cbcdfc0dad6
☐	–	sg-06b9cbb9671522eab	default	vpc-0f1ca5cbcdfc0dad6

sg-0b896b98f41bbad98 - route

Inbound rules (3)

☐	Name	Security group rule ID	IP version	Type	Protocol
☐	–	sgr-0ad98017bea63ca5a	IPv4	HTTP	TCP
☐	–	sgr-0074fb877b0a7185e	IPv4	SSH	TCP
☐	–	sgr-0d44faf48b6148c18	IPv4	HTTPS	TCP



Target groups (1/1) Info

☑	Name	ARN	Port	Protocol	Target type	Load balanc
☑	route	arn:aws:elasticloadbalancin...	80	HTTP	Instance	route-alb

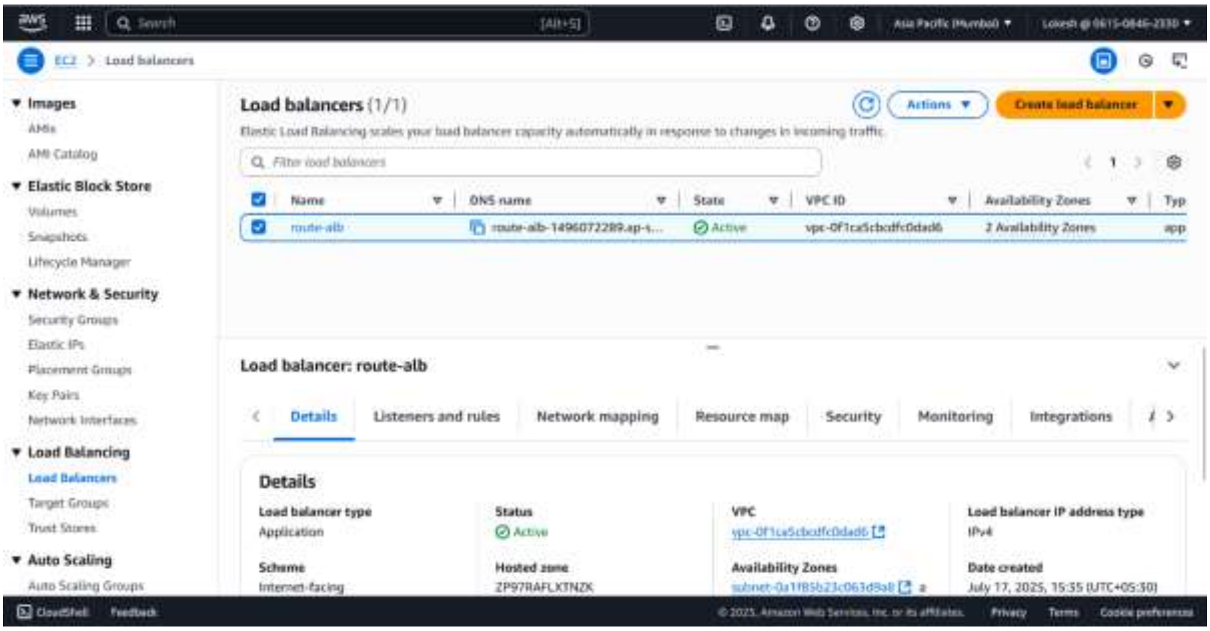
Target group: route

Details | Targets | Monitoring | Health checks | Attributes | Tags

Details

arn:aws:elasticloadbalancing:ap-south-1:061508462330:targetgroup/route/3386a3bdf7690a2c

Target type	Protocol : Port	Protocol version	VPC
Instance	HTTP: 80	HTTP1	vpc-0f1ca5cbcdfc0dad6
IP address type	Load balancer		



Load balancers (1/1)

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

☑	Name	DNS name	State	VPC ID	Availability Zones	Typ
☑	route-alb	route-alb-1496072289.ap-s...	✓ Active	vpc-0f1ca5cbcdfc0dad6	2 Availability Zones	app

Load balancer: route-alb

Details | Listeners and rules | Network mapping | Resource map | Security | Monitoring | Integrations

Details

Load balancer type
Application

Status
✓ Active

VPC
vpc-0f1ca5cbcdfc0dad6

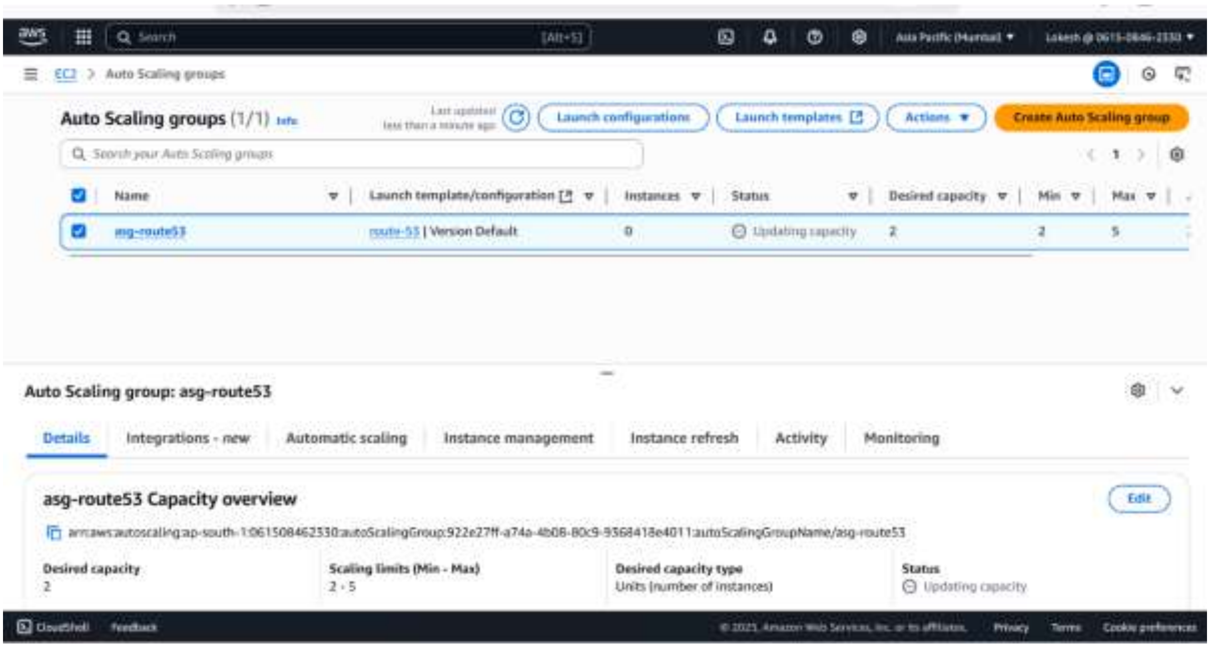
Load balancer IP address type
IPv4

Scheme
Internet-facing

Hosted zone
ZP97RAFLXTNZK

Availability Zones
subnet-0a1f85b23c063d9a8 a

Date created
July 17, 2025, 15:35 (UTC+05:30)



Auto Scaling groups (1/1)

☑	Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max
☑	asg-route53	route-53 | Version Default	0	Updating capacity	2	2	5

Auto Scaling group: asg-route53

Details | Integrations - new | Automatic scaling | Instance management | Instance refresh | Activity | Monitoring

asg-route53 Capacity overview

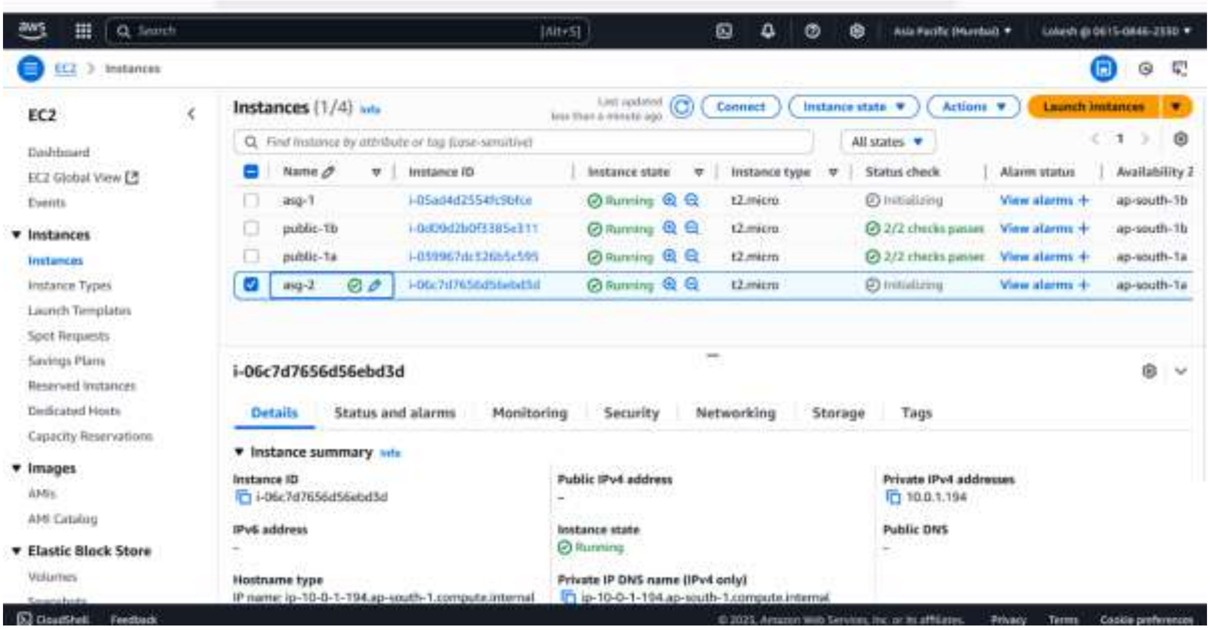
arn:aws:autoscaling:ap-south-1:061508462330:autoScalingGroup:922e27ff-a74a-4b08-80c9-9368418e4011:autoScalingGroupName/asg-route53

Desired capacity
2

Scaling limits (Min - Max)
2 - 5

Desired capacity type
Units (number of instances)

Status
Updating capacity



Instances (1/4) Info

Last updated less than a minute ago

Find Instance by attribute or tag (case-sensitive)

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Z
☐	asg-1	i-05ad4d2554fc9bfce	Running	t2.micro	Initializing	View alarms +	ap-south-1b
☐	public-1b	i-0d09d2b0f3385e311	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1b
☐	public-1a	i-039967dc126b5c595	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1a
☑	asg-2	i-06c7d7656d56ebd3d	Running	t2.micro	Initializing	View alarms +	ap-south-1a

i-06c7d7656d56ebd3d

Details | Status and alarms | Monitoring | Security | Networking | Storage | Tags

▼ Instance summary Info

Instance ID: i-06c7d7656d56ebd3d

Public IPv4 address: –

Private IPv4 addresses: 10.0.1.194

IPv6 address: –

Instance state: Running

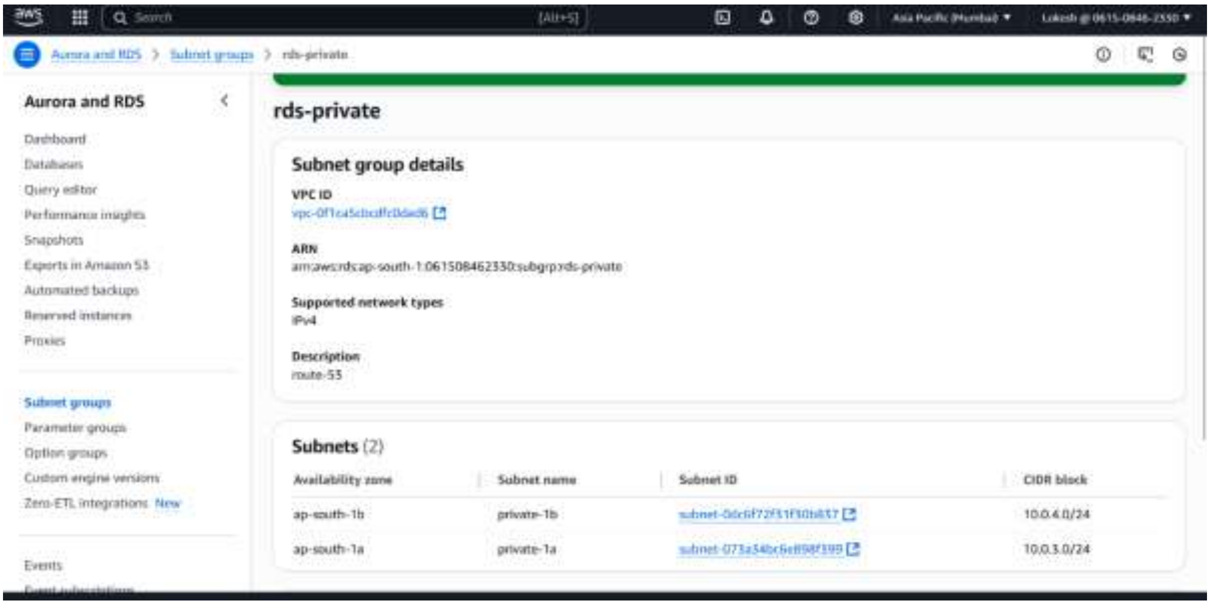
Public DNS: –

Hostname type: IP name: ip-10-0-1-194.ap-south-1.compute.internal

Private IP DNS name (IPv4 only): ip-10-0-1-194.ap-south-1.compute.internal

Step-3:RDS

i) Create rds
ii) Create subnets groups where we can launch databases
iii) Select private-1a, private-1b
iv) Now come to database
v) Create database and select mysql engine type
vi) Select 2 instance type of rds
vii) Edit name in user and self managed password
viii) Select public access as yes
ix) Create rds



rds-private

Subnet group details

VPC ID
vpc-0f1ca5cbcdfc0da06

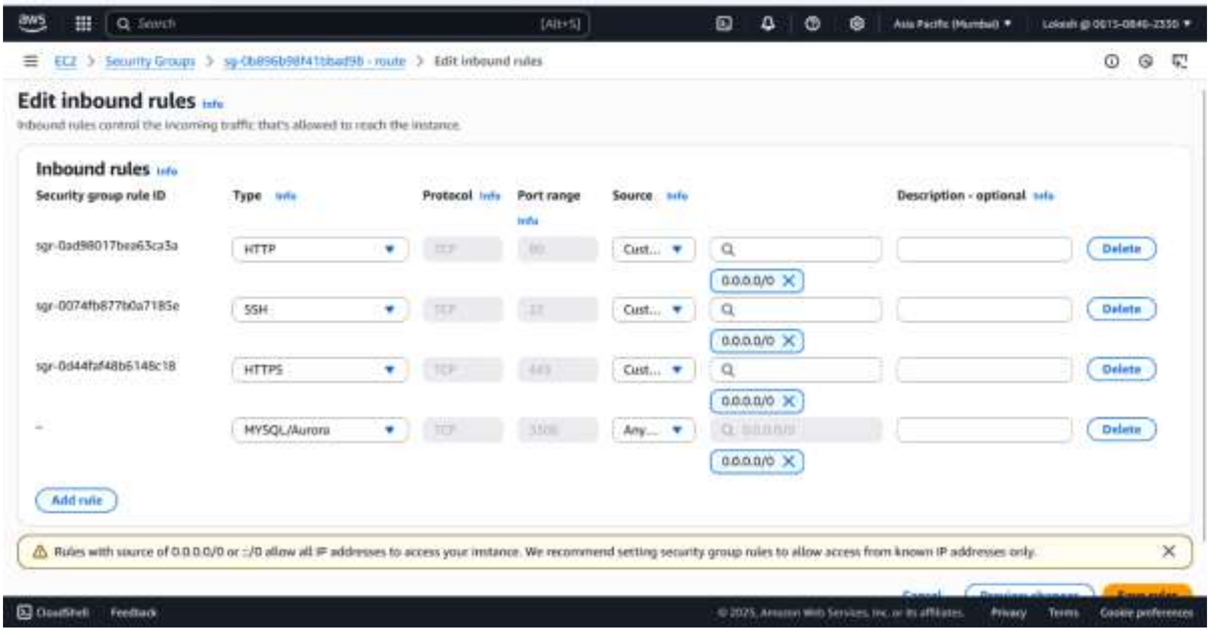
ARN
arn:aws:rds:ap-south-1:061508462330:subgrp:rds-private

Supported network types
IPv4

Description
route-53

Subnets (2)

Availability zone	Subnet name	Subnet ID	CIDR block
ap-south-1b	private-1b	subnet-0dc6f72f31f30b837	10.0.4.0/24
ap-south-1a	private-1a	subnet-073a34bc6e898f399	10.0.3.0/24


aws
Search
[Alt+S]
Asia Pacific (Mumbai) ▼
Lokesh @ 0615-0846-2330 ▼
EC2 > Security Groups > sg-0b896b98f41bbad98 - route > Edit inbound rules
Add rule
Cancel
Preview changes
Save rules
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

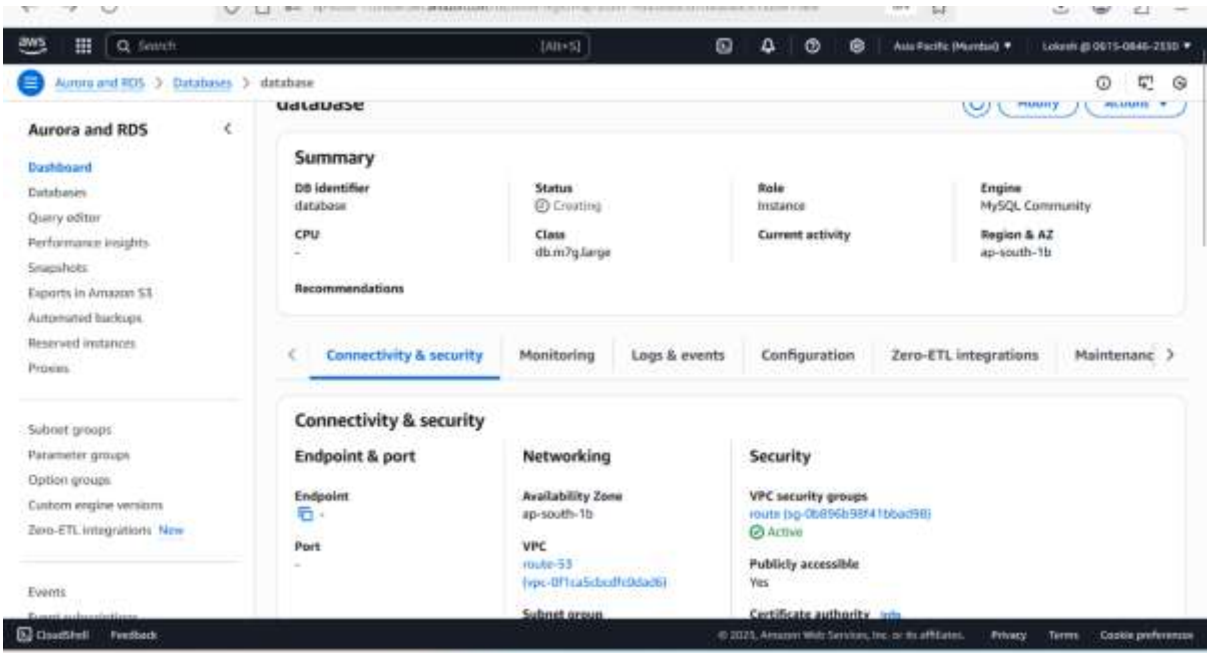
Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-0ad98017bea63ca3a	HTTP ▼	TCP	80	Cust... ▼	0.0.0.0/0 ✕		Delete
sgr-0074fb877b0a7185e	SSH ▼	TCP	22	Cust... ▼	0.0.0.0/0 ✕		Delete
sgr-0d44faf48b6148c18	HTTPS ▼	TCP	443	Cust... ▼	0.0.0.0/0 ✕		Delete
–	MYSQL/Aurora ▼	TCP	3306	Any... ▼	0.0.0.0/0 ✕		Delete

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.



database

Summary

DB identifier	Status	Role	Engine
database	Creating	Instance	MySQL Community
CPU	**Class**	**Current activity**	**Region & AZ**
-	db.m7g.large		ap-south-1b

Recommendations

Connectivity & security

Endpoint & port	Networking	Security
Endpoint -	**Availability Zone** ap-south-1b	**VPC security groups** route (sg-0b896b98f41bbad98) Active
Port -	**VPC** route-53 (vpc-0f1ca5cbcdfc0dad6)	**Publicly accessible** Yes
	Subnet group	**Certificate authority** Info

Step-4: Configure Route 53 and Domain Name

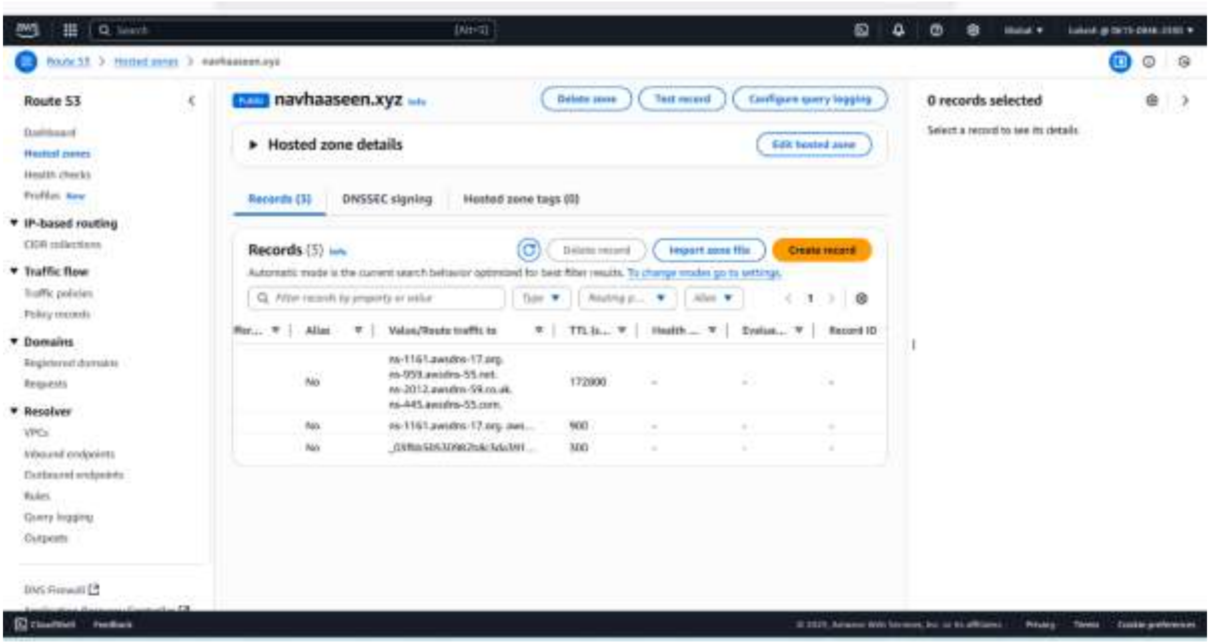
i. Created a Hosted Zone in Route 53 using a custom domain name.

ii. Created an Alias Record pointing to the Load Balancer.

iii. Added an additional Alias Record if required.

iv. Mapped the Name Servers (NS) provided by Route 53 to the domain name in a domain registrar (e.g., GoDaddy).

v. Verified that the domain name was resolving to the Load Balancer successfully



Public navhaaseen.xyz Info

Hosted zone details

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

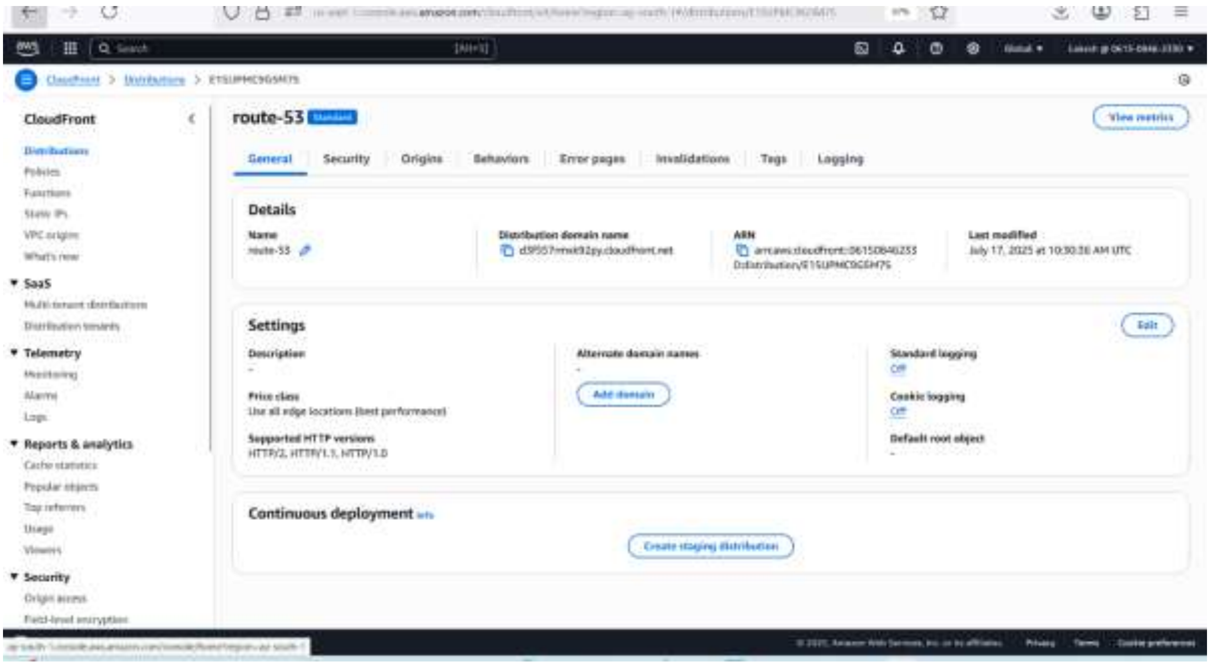
Records (3) Info

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

Rer...	Alias	Value/Route traffic to	TTL (s...	Health ...	Evalua...	Record ID
	No	ns-1161.awsdns-17.org. ns-959.awsdns-55.net. ns-2012.awsdns-59.co.uk. ns-445.awsdns-55.com.	172800	-	-	-
	No	ns-1161.awsdns-17.org. awı...	900	-	-	-
	No	_0Sf8b5D530982bdc3da3f41...	300	-	-	-

Step-5: Secure the Domain

i. Initially, the domain used HTTP and was not secure.
ii. To make it secure: o Created a WAF (Web Application Firewall).
iii. Requested an SSL/TLS certificate in AWS Certificate Manager (ACM).
iv. Set up a CloudFront Distribution using the certificate.
v. Added an HTTPS listener to the Load Balancer.
vi. Verified the domain was accessible securely (HTTPS) using the CloudFront domain.



route-53 Standard

Details

Name
route-53

Distribution domain name
d9557mwt92py.cloudfront.net

ARN
arn:aws:cloudfront::06150846233
D:distribution/E1SUPMC9G5M75

Last modified
July 17, 2025 at 10:30:38 AM UTC

Settings

Description
-

Price class
Use all edge locations (best performance)

Supported HTTP versions
HTTP/2, HTTP/1.1, HTTP/1.0

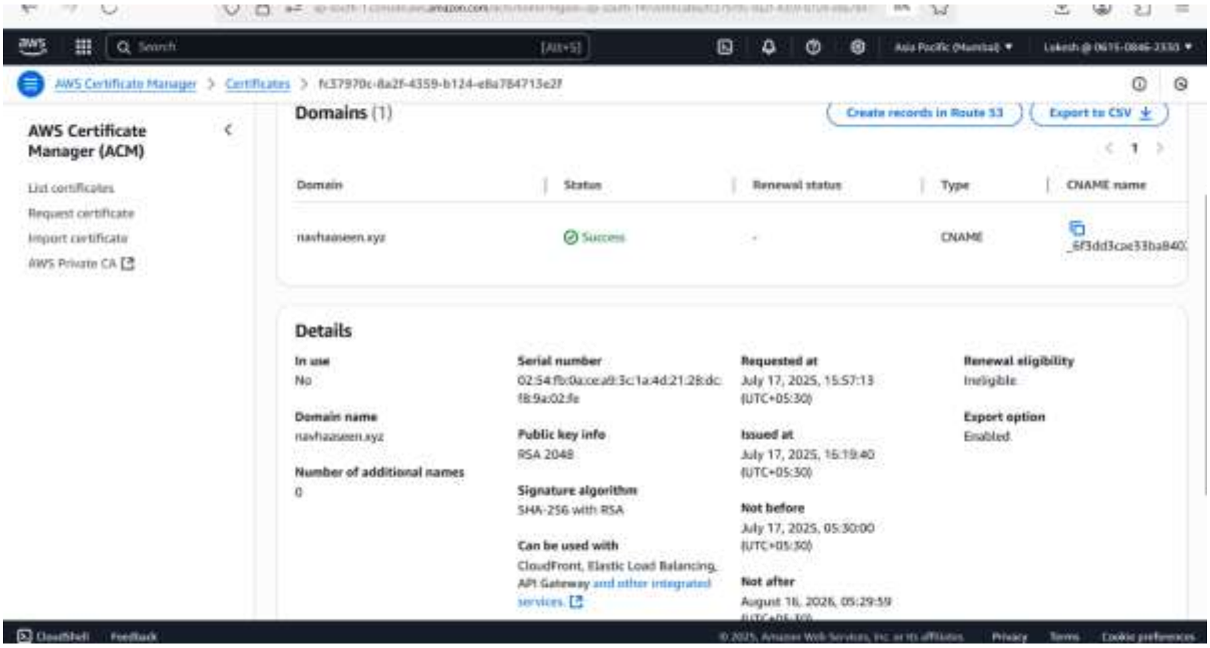
Alternate domain names
-

Standard logging
Off

Cookie logging
Off

Default root object
-

Continuous deployment Info


AWS Certificate Manager > Certificates > fc37970c-8a2f-4359-b124-e8a784713e2f
AWS Certificate Manager (ACM)
List certificates
Request certificate
Import certificate
AWS Private CA
Create records in Route 53
Export to CSV
1
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Domains (1)

Domain	Status	Renewal status	Type	CNAME name
navhaaseen.xyz	✓ Success	-	CNAME	_6f3dd3cae33ba840

Details

In use
No

Domain name
navhaaseen.xyz

Number of additional names
0

Serial number
02:54:fb:0a:ce:a9:3c:1a:4d:21:28:dc:f8:9a:02:fe

Public key info
RSA 2048

Signature algorithm
SHA-256 with RSA

Can be used with
CloudFront, Elastic Load Balancing, API Gateway and other integrated services.

Requested at
July 17, 2025, 15:57:13 (UTC+05:30)

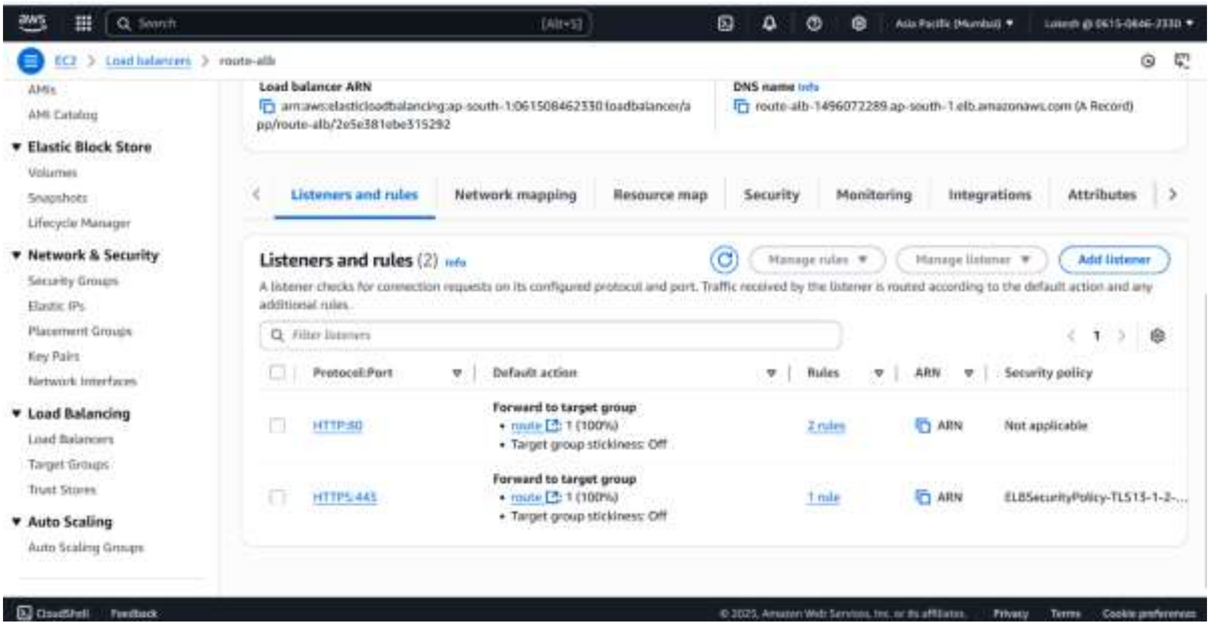
Issued at
July 17, 2025, 16:19:40 (UTC+05:30)

Not before
July 17, 2025, 05:30:00 (UTC+05:30)

Not after
August 16, 2026, 05:29:59 (UTC+05:30)

Renewal eligibility
Ineligible

Export option
Enabled



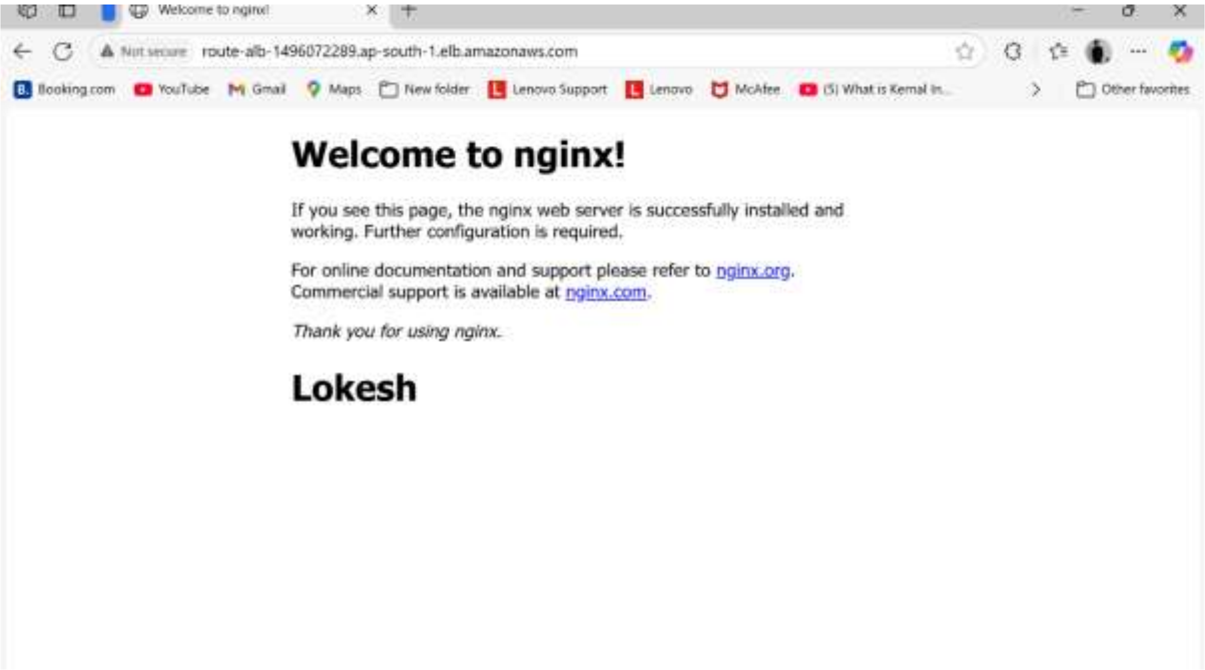
Load balancer ARN
arn:aws:elasticloadbalancing:ap-south-1:061508462330:loadbalancer/app/route-alb/2e5e381ebe315292

DNS name Info
route-alb-1496072289.ap-south-1.elb.amazonaws.com (A Record)

Listeners and rules (2) Info

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.

□	Protocol:Port	Default action	Rules	ARN	Security policy
□	HTTP:80	**Forward to target group** • route: 1 (100%) • Target group stickiness: Off	2 rules	ARN	Not applicable
□	HTTPS:443	**Forward to target group** • route: 1 (100%) • Target group stickiness: Off	1 rule	ARN	ELBSecurityPolicy-TLS13-1-2-...



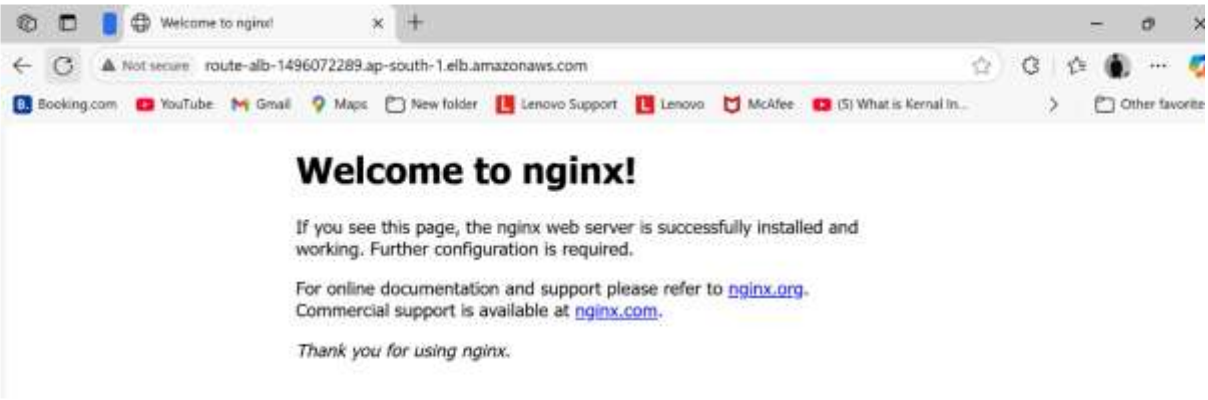
Welcome to nginx!

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.

Lokesh

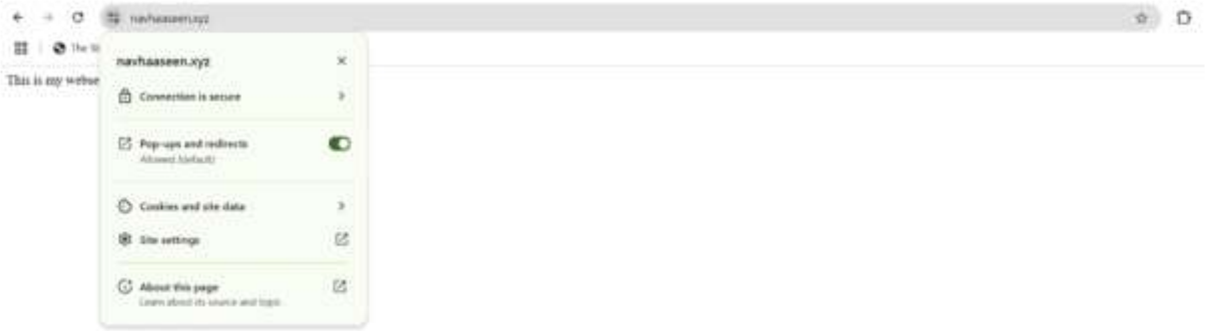


Welcome to nginx!

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.



This is my webse

navhaaseen.xyz

LOKESH BHEEMAGANI

lokeshbheemagani@gmail.com