VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering

(SCOPE)

Fall Semester 2025-26

CBS3005 - Cloud, Microservices and Applications

LAB ASSESSMENT 4

Submitted by-

YASH GARG

22BBS0183

1) A company wants to deploy a secure, scalable, and highly available web application on AWS for global users. Perform the following tasks in AWS and submit screenshots of each step as evidence:

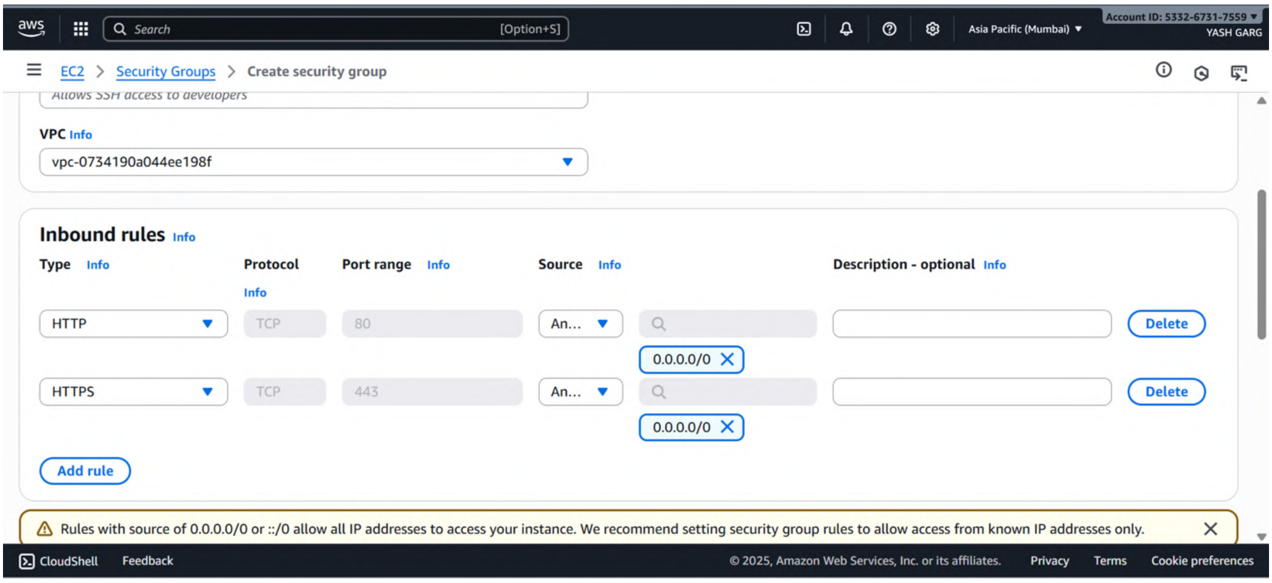
(i) Launch multiple EC2 instances (web servers) and configure them in different Availability Zones.
(ii) Create an Application Load Balancer (ALB) to distribute traffic across these instances.
(iii) Configure health checks so that faulty instances are automatically removed from load balancing.
(iv) Enable Auto Scaling to add/remove instances based on traffic demand.
(v) Configure path-based routing: /auth requests go to the authentication service, /order requests go to the order processing service. Integrate the Load Balancer with Route 53 so that global users are routed to the nearest AWS region.

1) Create security groups (do in each region)

Do these steps in **ap-south-1** first, then repeat in **us-east-1**.

A. Create ALB security group

1. Services → **EC2** → left sidebar → **Network & Security** → **Security Groups** → **Create security group**.
2. Fields:
   - Name tag: blt-kf
   - Description: Allow HTTP/HTTPS from Internet
   - VPC: choose Default or your VPC
3. Inbound rules:
   - Type: HTTP / Port: 80 / Source: 0.0.0.0/0
   - Type: HTTPS / Port: 443 / Source: 0.0.0.0/0 (optional)
4. Outbound: keep default (allow all)
5. Create security group.



EC2 > Security Groups > Create security group

Allows SSH access to developers

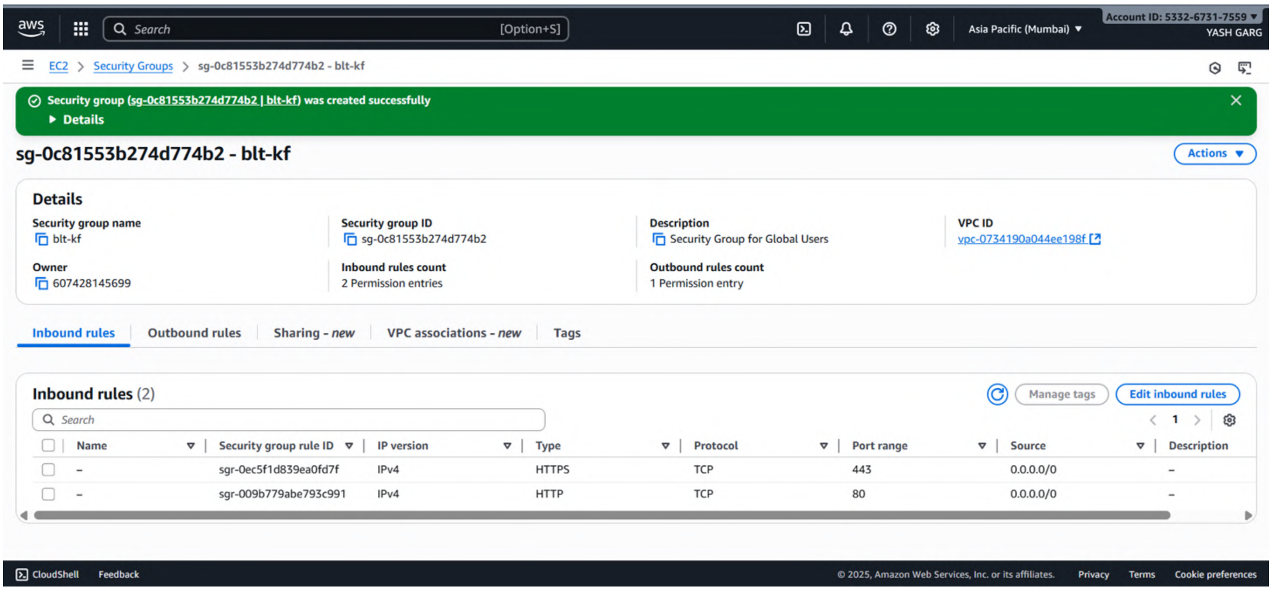
VPC Info

vpc-0734190a044ee198f

Inbound rules Info

Type	Protocol	Port range	Source		Description - optional
HTTP	TCP	80	An...	0.0.0.0/0	
HTTPS	TCP	443	An...	0.0.0.0/0	

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.



EC2 > Security Groups > sg-0c81553b274d774b2 - blt-kf

Security group (sg-0c81553b274d774b2 | blt-kf) was created successfully

sg-0c81553b274d774b2 - blt-kf

Details

Security group name: blt-kf

Security group ID: sg-0c81553b274d774b2

Description: Security Group for Global Users

VPC ID: vpc-0734190a044ee198f

Owner: 607428145699

Inbound rules count: 2 Permission entries

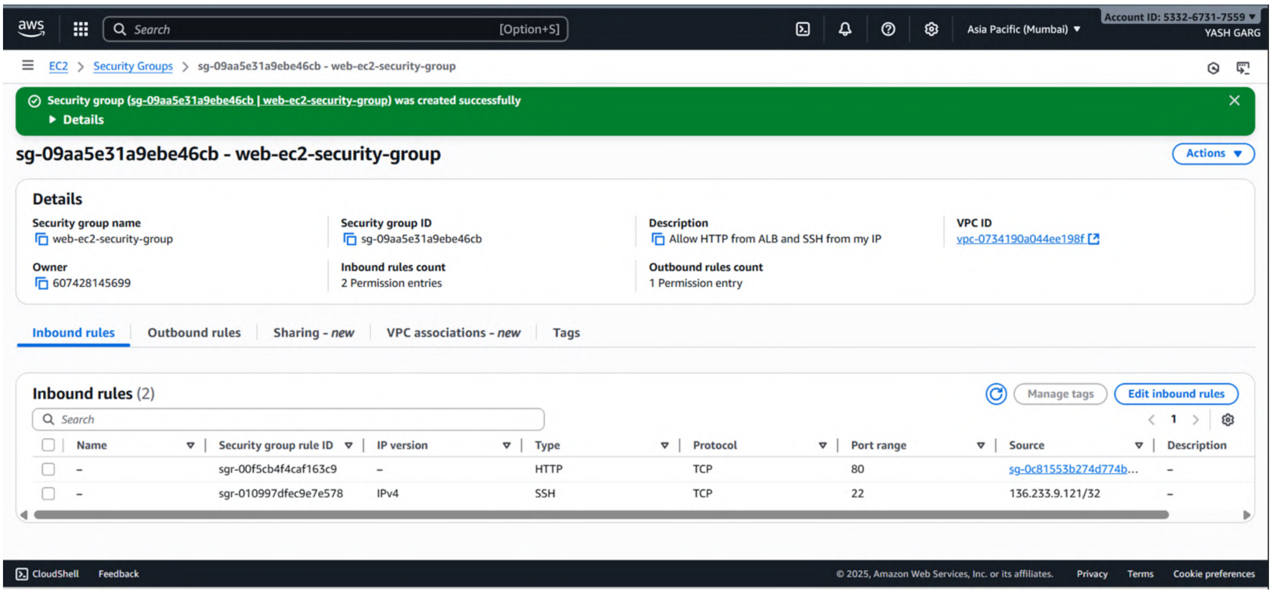
Outbound rules count: 1 Permission entry

Inbound rules (2)

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
–	sgr-0ec5f1d839ea0fd7f	IPv4	HTTPS	TCP	443	0.0.0.0/0	–
–	sgr-009b779abe793c991	IPv4	HTTP	TCP	80	0.0.0.0/0	–

B. Create EC2/web security group

1. Click **Create security group** again.
2. Fields:
   - Name: web-ec2-sg
   - Description: Allow HTTP from ALB and SSH from my IP
   - VPC: same VPC
3. Inbound rules:
   - Custom TCP Rule: Port 80 — Source: choose **Custom** then **Security group** and select alb-sg (this allows only ALB to reach EC2 on 80)
   - SSH: Port 22 — Source: YourIP/32 (enter your public IP)
4. Create.



aws
Search [Option+S]
Asia Pacific (Mumbai) ▼
Account ID: 5332-6731-7559 ▼
YASH GARG
EC2 > Security Groups > sg-09aa5e31a9ebe46cb - web-ec2-security-group

Security group (sg-09aa5e31a9ebe46cb | web-ec2-security-group) was created successfully

▸ Details

sg-09aa5e31a9ebe46cb - web-ec2-security-group

Details

Security group name: web-ec2-security-group

Security group ID: sg-09aa5e31a9ebe46cb

Description: Allow HTTP from ALB and SSH from my IP

VPC ID: vpc-0734190a044ee198f

Owner: 607428145699

Inbound rules count: 2 Permission entries

Outbound rules count: 1 Permission entry

Inbound rules (2)

	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
□	–	sgr-00f5cb4f4caf163c9	–	HTTP	TCP	80	sg-0c81553b274d774b...	–
□	–	sgr-010997dfec9e7e578	IPv4	SSH	TCP	22	136.233.9.121/32	–

2) Launch EC2 instances (web servers)

Goal: create 2 Auth instances (AZ1 & AZ2) and 2 Order instances (AZ1 & AZ2) in each region. Do these in **ap-south-1** first. Later repeat in **us-east-1**.

A. Launch auth-1 (AZ1)

1. Services → **EC2** → **Instances** → **Launch instances**.
2. **Name and tags**: auth-1
3. **Application and OS image (AMI)**: Amazon Linux 2 AMI (HVM)
4. **Instance type**: t3.micro (free tier friendly)
5. **Key pair (login)**: choose existing key pair or create a new key pair (download .pem) — keep safe.

6. Network settings:
   - VPC: Default (or your VPC)
   - Subnet: choose Subnet in AZ **ap-south-1a** (or any AZ for AZ1)
   - Auto-assign Public IP: Enable (so you can test from the internet)
   - Security group: select web-ec2-sg (the one that allows ALB Security Group)
7. **Advanced details → User data** (paste below so instance serves an easy health page /health and index):
8. #!/bin/bash
9. yum update -y
10. yum install -y httpd
11. echo "Auth Service - $(curl -s http://169.254.169.254/latest/meta-data/instance-id)" > /var/www/html/index.html
12. echo "OK" > /var/www/html/health
13. systemctl enable httpd
14. systemctl start httpd
15. Click **Launch instance**.

B. Launch auth-2 (AZ2)

- Repeat above but choose a different **Subnet** (ap-south-1b). Name auth-2.

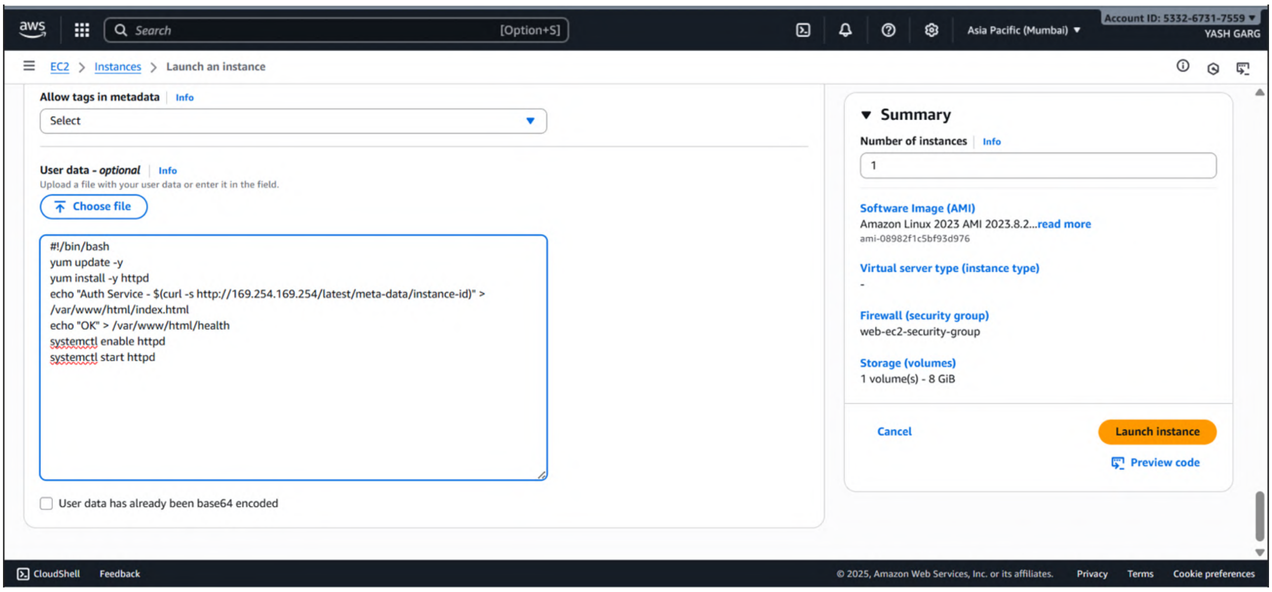
C. Launch order-1 and order-2

- Follow same steps but change names and the user-data index.html message:
- echo "Order Service - $(curl -s http://169.254.169.254/latest/meta-data/instance-id)" > /var/www/html/index.html
- echo "OK" > /var/www/html/health
- Create in AZ1 and AZ2 respectively.

D. Confirm instances

1. EC2 → Instances → you should see auth-1, auth-2, order-1, order-2. Ensure their **Availability Zone** column shows different AZs (for HA).
2. Note private IPs / public IPs.

Repeat these steps in the other region (create auth-1/us-east-1, etc.). Keep naming consistent (e.g., ap-auth-1, us-auth-1) to avoid confusion.



aws
Search [Option+S]
Asia Pacific (Mumbai)
Account ID: 5332-6731-7559
YASH GARG
EC2 > Instances > Launch an instance

Allow tags in metadata | Info

Select

User data - *optional* | Info

Upload a file with your user data or enter it in the field.

Choose file

```
#!/bin/bash
yum update -y
yum install -y httpd
echo "Auth Service - $(curl -s http://169.254.169.254/latest/meta-data/instance-id)" >
/var/www/html/index.html
echo "OK" > /var/www/html/health
systemctl enable httpd
systemctl start httpd
```

□ User data has already been base64 encoded

Summary

Number of instances | Info

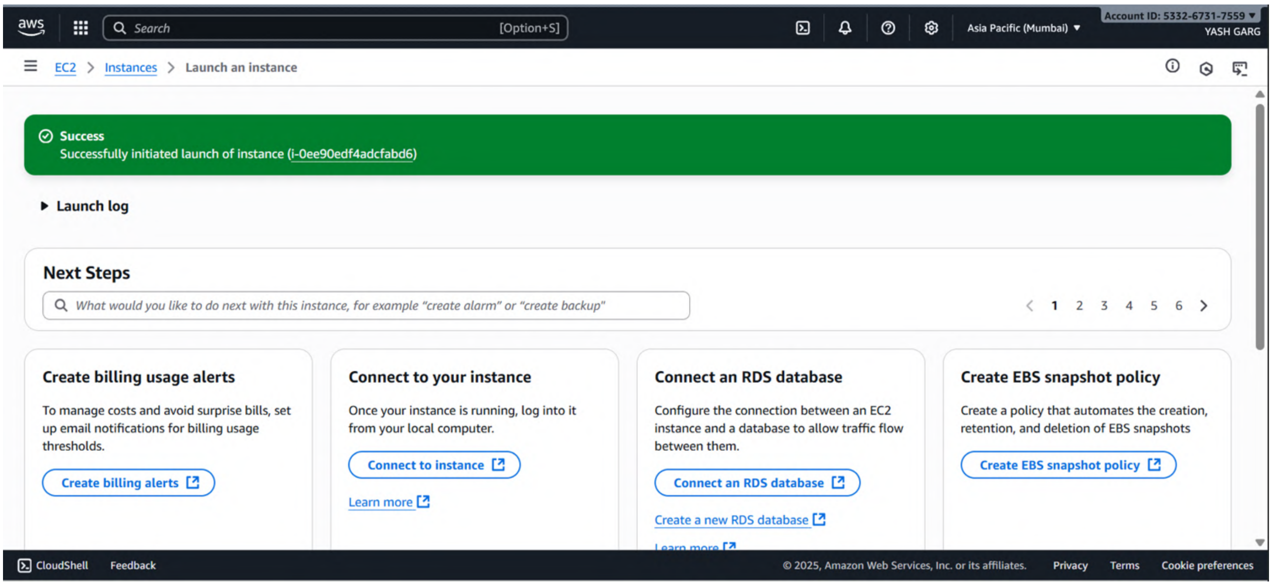
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-08982f1c5bf93d976

Virtual server type (instance type)
-

Firewall (security group)
web-ec2-security-group

Storage (volumes)
1 volume(s) - 8 GiB



aws
Search [Option+S]
Asia Pacific (Mumbai)
Account ID: 5332-6731-7559
YASH GARG
EC2 > Instances > Launch an instance

Success
Successfully initiated launch of instance (i-0ee90edf4adcfabd6)

▸ Launch log

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"

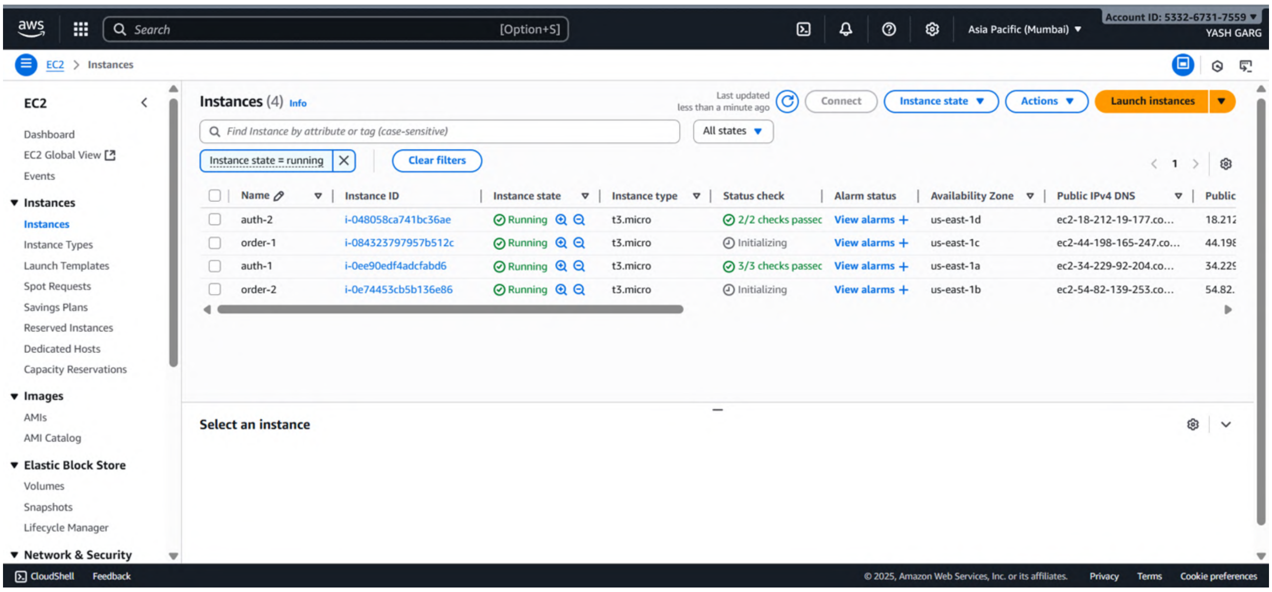
< 1 2 3 4 5 6 >

Create billing usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing usage thresholds.
Create billing alerts

Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more

Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database
Learn more

Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create EBS snapshot policy



Instances (4) Info

Find Instance by attribute or tag (case-sensitive)

Instance state = running

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public
□	auth-2	i-048058ca741bc36ae	Running	t3.micro	2/2 checks passec	View alarms +	us-east-1d	ec2-18-212-19-177.co...	18.212
□	order-1	i-084323797957b512c	Running	t3.micro	Initializing	View alarms +	us-east-1c	ec2-44-198-165-247.co...	44.198
□	auth-1	i-0ee90edf4adcfabd6	Running	t3.micro	3/3 checks passec	View alarms +	us-east-1a	ec2-34-229-92-204.co...	34.229
□	order-2	i-0e74453cb5b136e86	Running	t3.micro	Initializing	View alarms +	us-east-1b	ec2-54-82-139-253.co...	54.82.

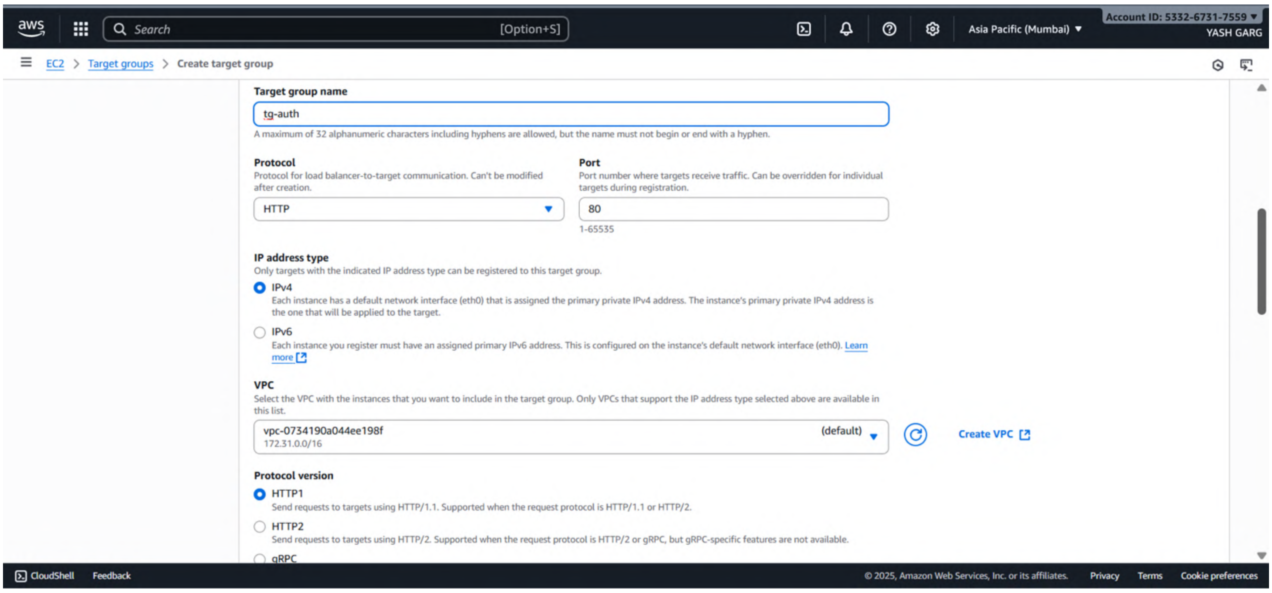
Select an instance

3) Create Target Groups (per region, per service)

In each region create two target groups: tg-auth and tg-order.

1. Services → **EC2** → left menu → **Load Balancing** → **Target Groups** → **Create target group**.
2. Fields:
   - Target type: **Instance**
   - Protocol: **HTTP**
   - Port: 80
   - VPC: choose your VPC
   - Name: tg-auth
3. Health checks:
   - Protocol: HTTP
   - Path: /health
   - Success codes: 200
   - Interval: 30 s, Healthy threshold: 3, Unhealthy threshold: 3
4. Click **Create**.
5. After creation → **Targets** tab → **Register targets** → select auth-1 and auth-2 → Port 80 → Register.

Repeat to create tg-order and register order-1 and order-2.


aws
Search
[Option+S]
Asia Pacific (Mumbai)
Account ID: 5332-6731-7559
YASH GARG
EC2 > Target groups > Create target group

Target group name

tg-auth

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

Protocol

Protocol for load balancer-to-target communication. Can't be modified after creation.

HTTP

Port

Port number where targets receive traffic. Can be overridden for individual targets during registration.

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.

○ IPv6
Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). Learn more

VPC

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

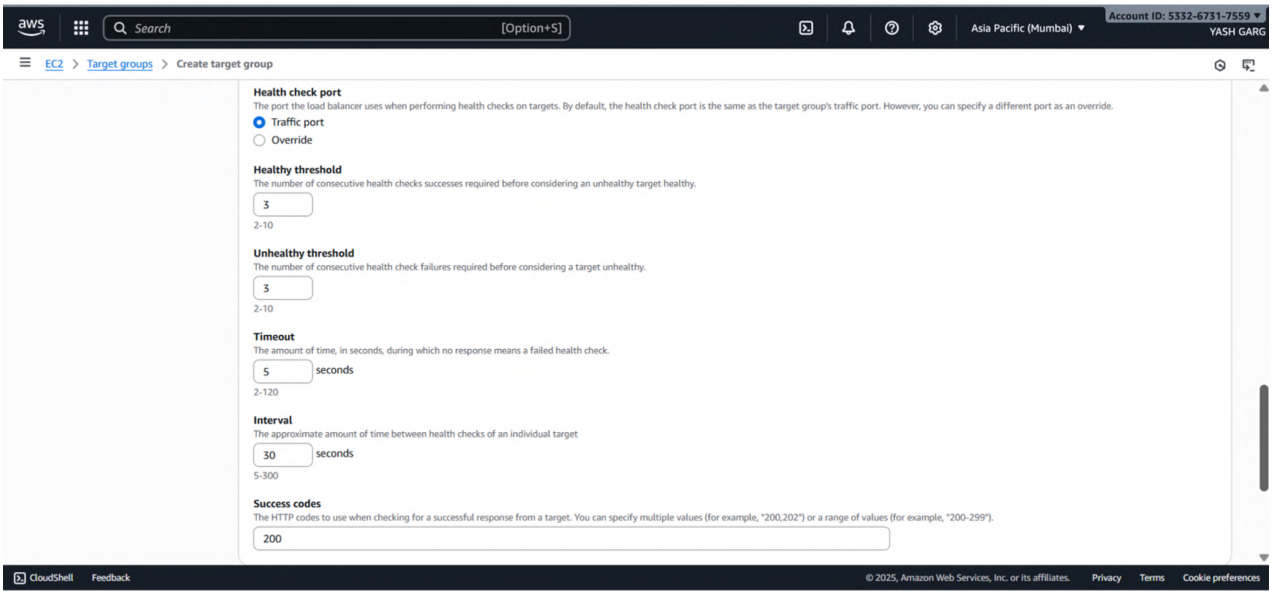
vpc-0734190a044ee198f (default)
172.31.0.0/16

Protocol version

● HTTP1
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

○ HTTP2
Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.

○ gRPC



aws
Search [Option+S]
Asia Pacific (Mumbai) ▼
Account ID: 5332-6731-7559 ▼
YASH GARG
EC2 > Target groups > Create target group

Health check port

The port the load balancer uses when performing health checks on targets. By default, the health check port is the same as the target group's traffic port. However, you can specify a different port as an override.

● Traffic port

○ Override

Healthy threshold

The number of consecutive health checks successes required before considering an unhealthy target healthy.

3

2-10

Unhealthy threshold

The number of consecutive health check failures required before considering a target unhealthy.

3

2-10

Timeout

The amount of time, in seconds, during which no response means a failed health check.

5 seconds

2-120

Interval

The approximate amount of time between health checks of an individual target

30 seconds

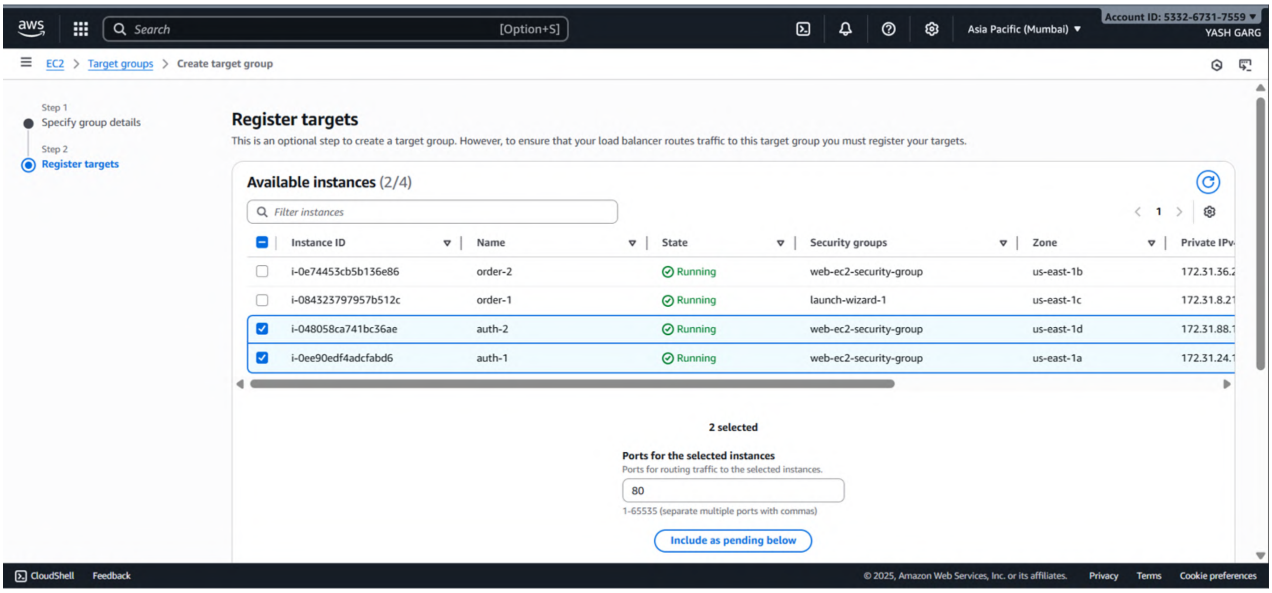
5-300

Success codes

The HTTP codes to use when checking for a successful response from a target. You can specify multiple values (for example, "200,202") or a range of values (for example, "200-299").

200

CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



aws
Search [Option+S]
Asia Pacific (Mumbai) ▼
Account ID: 5332-6731-7559 ▼
YASH GARG
EC2 > Target groups > Create target group
Step 1
Specify group details
Step 2
Register targets

Register targets

This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

Available instances (2/4)

Filter instances

	Instance ID	Name	State	Security groups	Zone	Private IPv
□	i-0e74453cb5b136e86	order-2	✓ Running	web-ec2-security-group	us-east-1b	172.31.36.2
□	i-084323797957b512c	order-1	✓ Running	launch-wizard-1	us-east-1c	172.31.8.21
☑	i-048058ca741bc36ae	auth-2	✓ Running	web-ec2-security-group	us-east-1d	172.31.88.1
☑	i-0ee90edf4adcfabd6	auth-1	✓ Running	web-ec2-security-group	us-east-1a	172.31.24.1

2 selected

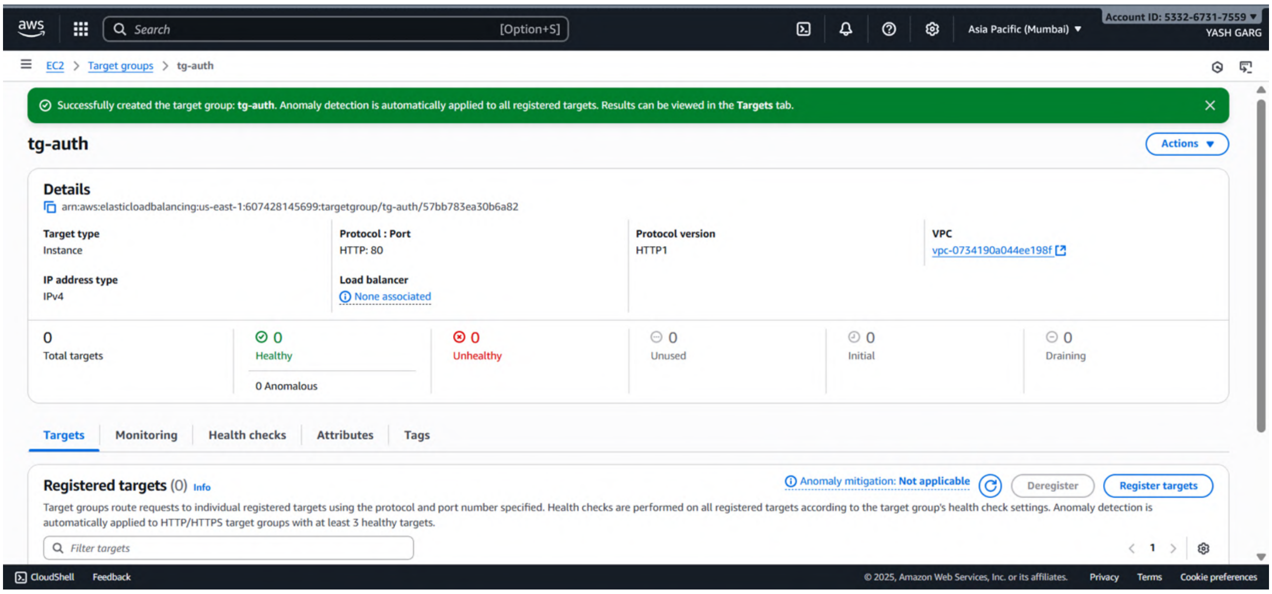
Ports for the selected instances

Ports for routing traffic to the selected instances.

80

1-65535 (separate multiple ports with commas)

Include as pending below
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



aws
Search [Option+S]
Asia Pacific (Mumbai) ▼
Account ID: 5332-6731-7559 ▼
YASH GARG
EC2 > Target groups > tg-auth

Successfully created the target group: **tg-auth**. Anomaly detection is automatically applied to all registered targets. Results can be viewed in the **Targets** tab.

tg-auth

Details

arn:aws:elasticloadbalancing:us-east-1:607428145699:targetgroup/tg-auth/57bb783ea30b6a82

Target type
Instance

Protocol : Port
HTTP: 80

Protocol version
HTTP1

VPC
vpc-0734190a044ee198f

IP address type
IPv4

Load balancer
None associated

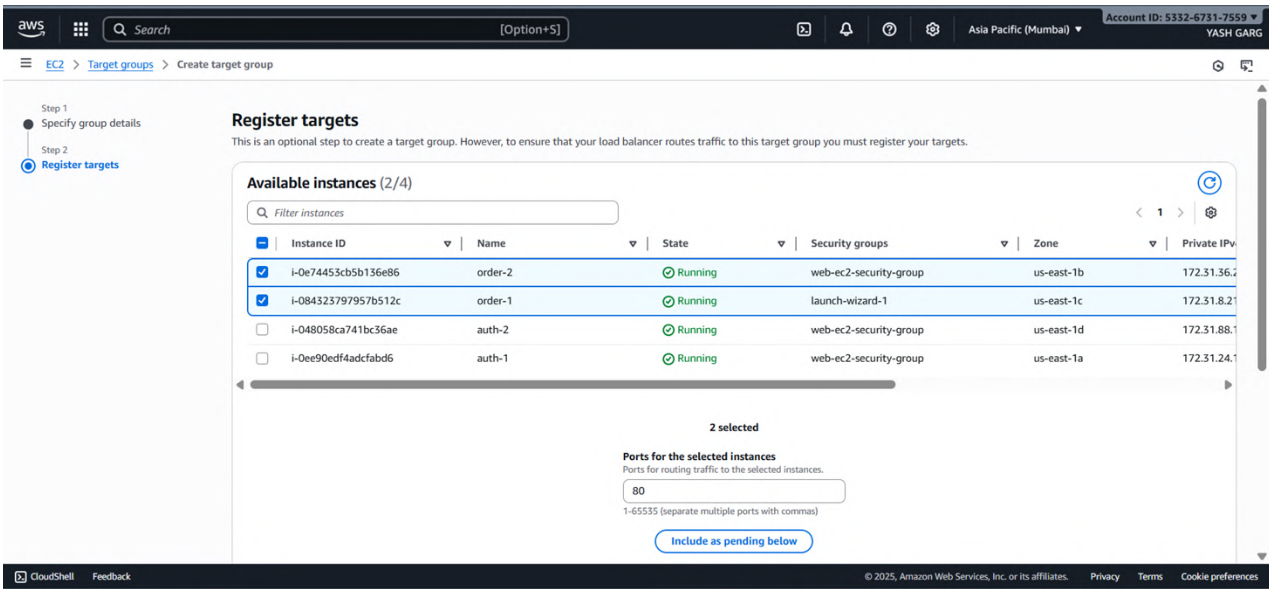
0	✓ 0	☒ 0	0	0	0
Total targets	Healthy 0 Anomalous	Unhealthy	Unused	Initial	Draining

Registered targets (0) Info

Anomaly mitigation: **Not applicable**

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
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences


aws
Search [Option+S]
Asia Pacific (Mumbai)
Account ID: 5332-6731-7559
YASH GARG
EC2 > Target groups > Create target group
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Step 1
Specify group details

Step 2
Register targets

Register targets

This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

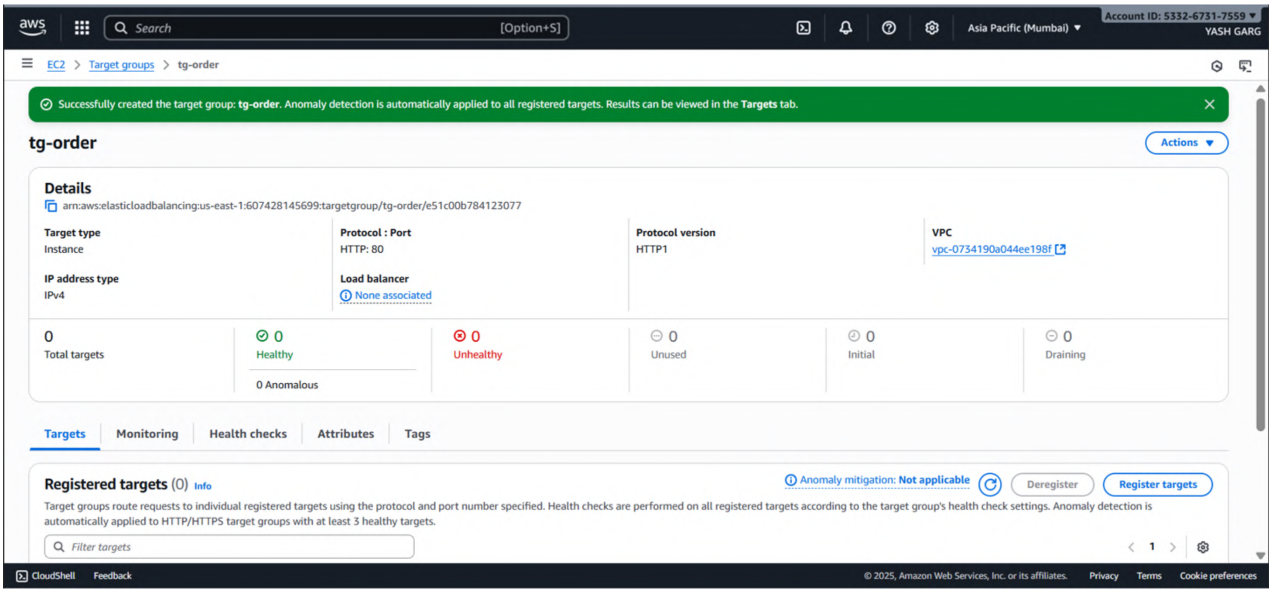
Available instances (2/4)

Filter instances

	Instance ID	Name	State	Security groups	Zone	Private IPv
☑	i-0e74453cb5b136e86	order-2	✓ Running	web-ec2-security-group	us-east-1b	172.31.36.2
☑	i-084323797957b512c	order-1	✓ Running	launch-wizard-1	us-east-1c	172.31.8.21
□	i-048058ca741bc36ae	auth-2	✓ Running	web-ec2-security-group	us-east-1d	172.31.88.1
□	i-0ee90edf4adcfabd6	auth-1	✓ Running	web-ec2-security-group	us-east-1a	172.31.24.1

2 selected

Ports for the selected instances
Ports for routing traffic to the selected instances.
80
1-65535 (separate multiple ports with commas)



Successfully created the target group: **tg-order**. Anomaly detection is automatically applied to all registered targets. Results can be viewed in the **Targets** tab.

tg-order

Details
arn:aws:elasticloadbalancing:us-east-1:607428145699:targetgroup/tg-order/e51c00b784123077

Target type
Instance

Protocol : Port
HTTP: 80

Protocol version
HTTP1

VPC
vpc-0734190a044ee198f

IP address type
IPv4

Load balancer
None associated

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

Registered targets (0) Info

Anomaly mitigation: **Not applicable**

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

4) Create an Application Load Balancer (ALB) and configure path-based routing

You'll create 1 ALB per region and use listener rules for path-based routing.

1. Services → **EC2** → **Load Balancers** → **Create Load Balancer** → **Application Load Balancer**.
2. Basic configuration:
   - Name: alb-web-ap-south-1 (for Mumbai region)
   - Scheme: internet-facing
   - IP address type: ipv4
3. Listeners:
   - Add HTTP : 80 (you may add HTTPS 443 later if you have certs)
4. Availability Zones:
   - VPC: default or your VPC
   - Select at least **2 subnets** (one per AZ) — ensures ALB spans multiple AZs

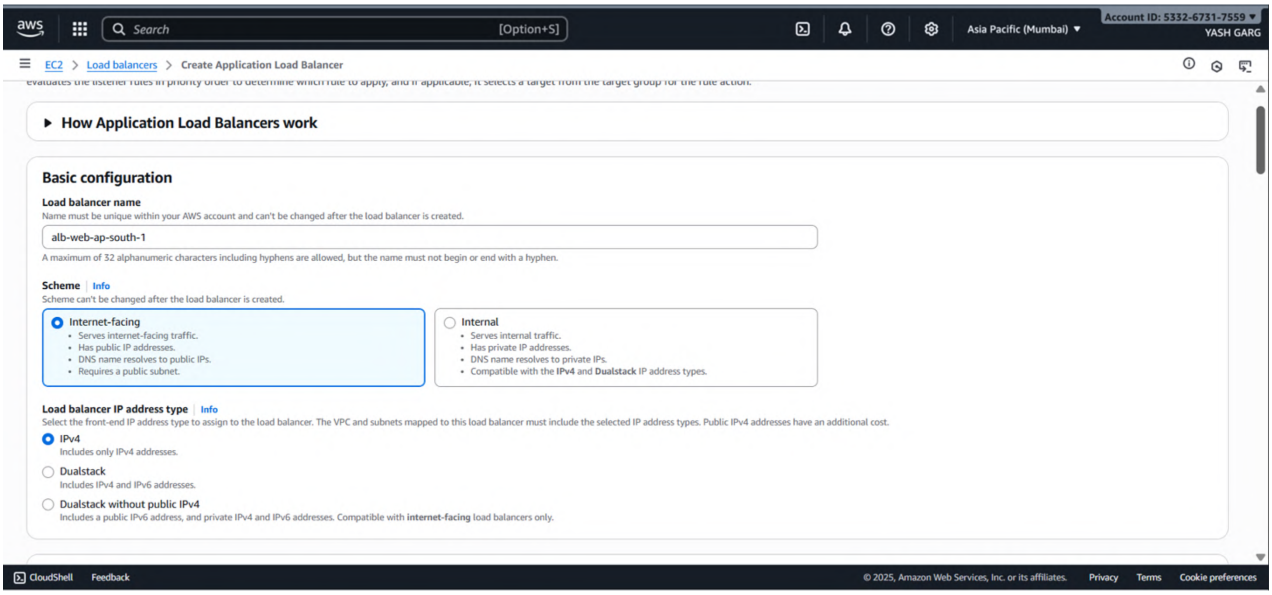
5. Security group: select alb-sg
6. Configure routing:
   - Default target group: you can set default to tg-auth or create a dummy page — we will create rules to route based on path. Choose tg-auth as default or create a small tg-default.
7. Create load balancer (wait for provisioning).

A. Configure Listener rules (path-based)

1. In **Load Balancers** list click alb-web-ap-south-1 → **Listeners** tab → click the **HTTP:80** listener → View/edit rules.
2. You'll see default rule. Click + to add a rule before default:
   - Condition: **If path is** — enter /auth* or /auth/* and /auth (you can use path pattern /auth*)
   - Action: **Forward** to target group tg-auth
   - Add another rule:
     - Condition: Path is /order*
     - Action: Forward to tg-order
3. Save rules. Ensure default rule goes to some target (or returns 404).

B. Verify ALB health checks / target health

1. Load Balancers → select ALB → **Target groups** tab → click tg-auth → **Targets** → confirm healthy.
2. If unhealthy, check instance user-data and /health path.


aws
Search [Option+S]
Asia Pacific (Mumbai) ▾
Account ID: 5332-6731-7559 ▾
YASH GARG
EC2 > Load balancers > Create Application Load Balancer
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the target group for the rule action.

▸ How Application Load Balancers work

Basic configuration

Load balancer name
Name must be unique within your AWS account and can't be changed after the load balancer is created.
alb-web-ap-south-1
A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme | Info
Scheme can't be changed after the load balancer is created.

● Internet-facing
- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name resolves to public IPs.
- Requires a public subnet.

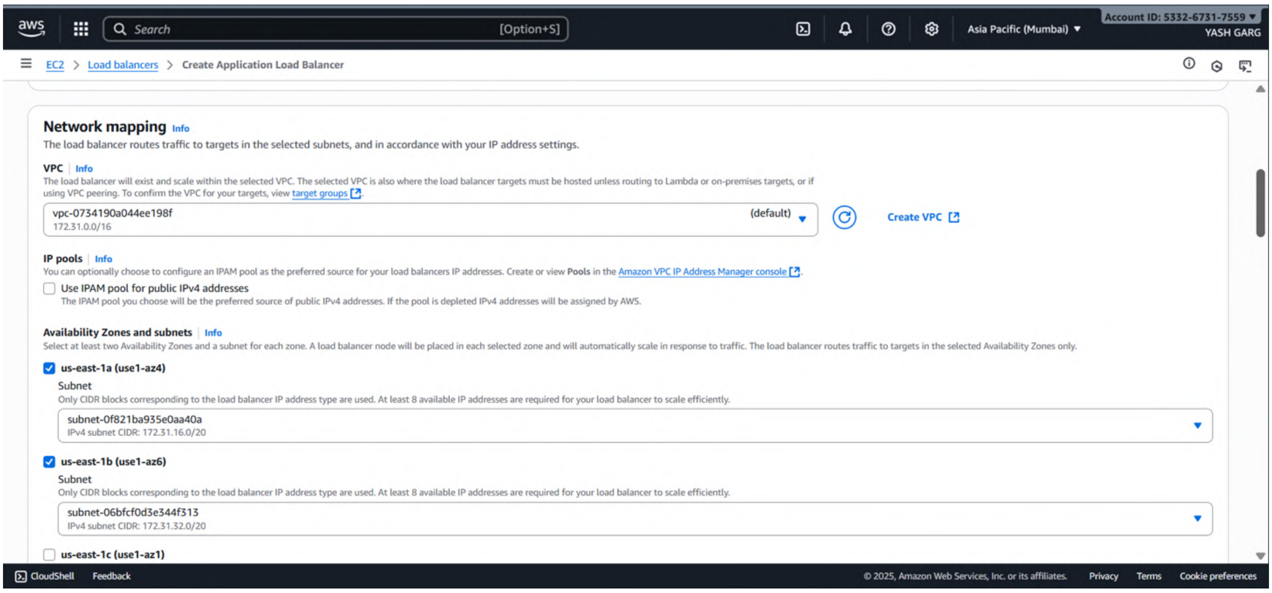
○ Internal
- Serves internal traffic.
- Has private IP addresses.
- DNS name resolves to private IPs.
- Compatible with the **IPv4** and **Dualstack** IP address types.

Load balancer IP address type | Info
Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.

● IPv4
Includes only IPv4 addresses.

○ Dualstack
Includes IPv4 and IPv6 addresses.

○ Dualstack without public IPv4
Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with **internet-facing** load balancers only.


aws
Search [Option+S]
Asia Pacific (Mumbai)
Account ID: 5332-6731-7559
YASH GARG
EC2 > Load balancers > Create Application Load Balancer
Create VPC
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Network mapping Info

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC | Info

The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view target groups.

vpc-0734190a044ee198f (default)
172.31.0.0/16

IP pools | Info

You can optionally choose to configure an IPAM pool as the preferred source for your load balancers IP addresses. Create or view **Pools** in the Amazon VPC IP Address Manager console.

□ Use IPAM pool for public IPv4 addresses
The IPAM pool you choose will be the preferred source of public IPv4 addresses. If the pool is depleted IPv4 addresses will be assigned by AWS.

Availability Zones and subnets | Info

Select at least two Availability Zones and a subnet for each zone. A load balancer node will be placed in each selected zone and will automatically scale in response to traffic. The load balancer routes traffic to targets in the selected Availability Zones only.

☑ **us-east-1a (use1-az4)**

Subnet
Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

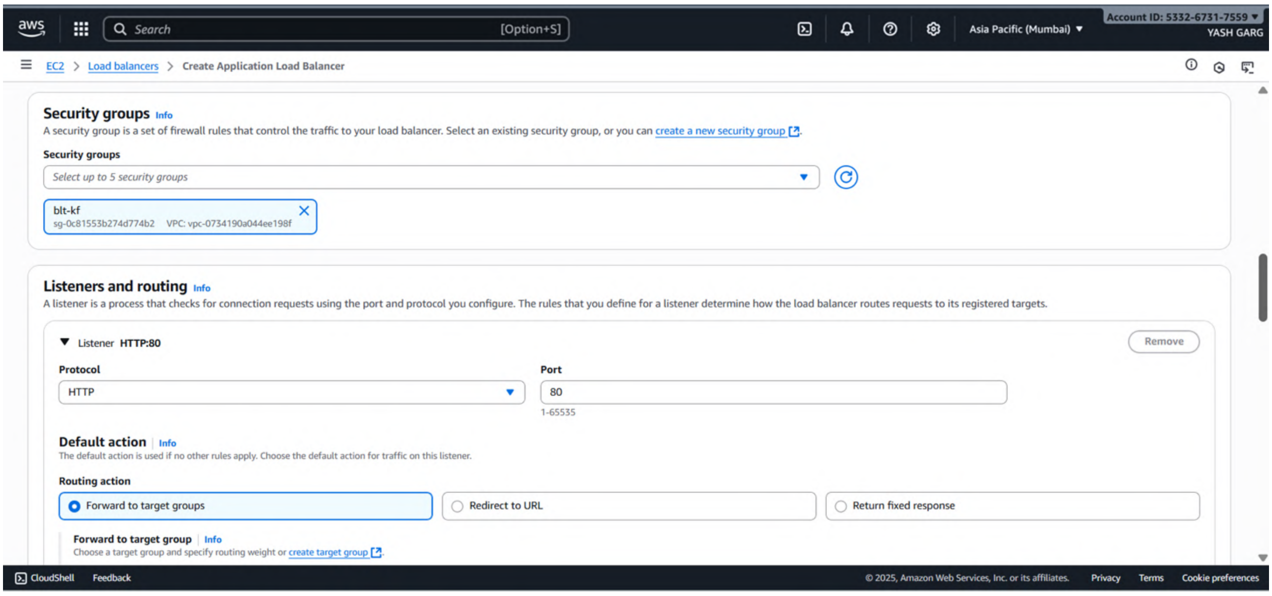
subnet-0f821ba935e0aa40a
IPv4 subnet CIDR: 172.31.16.0/20

☑ **us-east-1b (use1-az6)**

Subnet
Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-06bfcf0d3e344f313
IPv4 subnet CIDR: 172.31.32.0/20

□ **us-east-1c (use1-az1)**


aws
Search [Option+S]
Asia Pacific (Mumbai)
Account ID: 5332-6731-7559
YASH GARG
EC2 > Load balancers > Create Application Load Balancer
Remove
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Security groups Info

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group.

Security groups

Select up to 5 security groups

blt-kf
sg-0c81553b274d774b2 VPC: vpc-0734190a044ee198f

Listeners and routing Info

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener **HTTP:80**

Protocol: HTTP

Port: 80
1-65535

Default action | Info

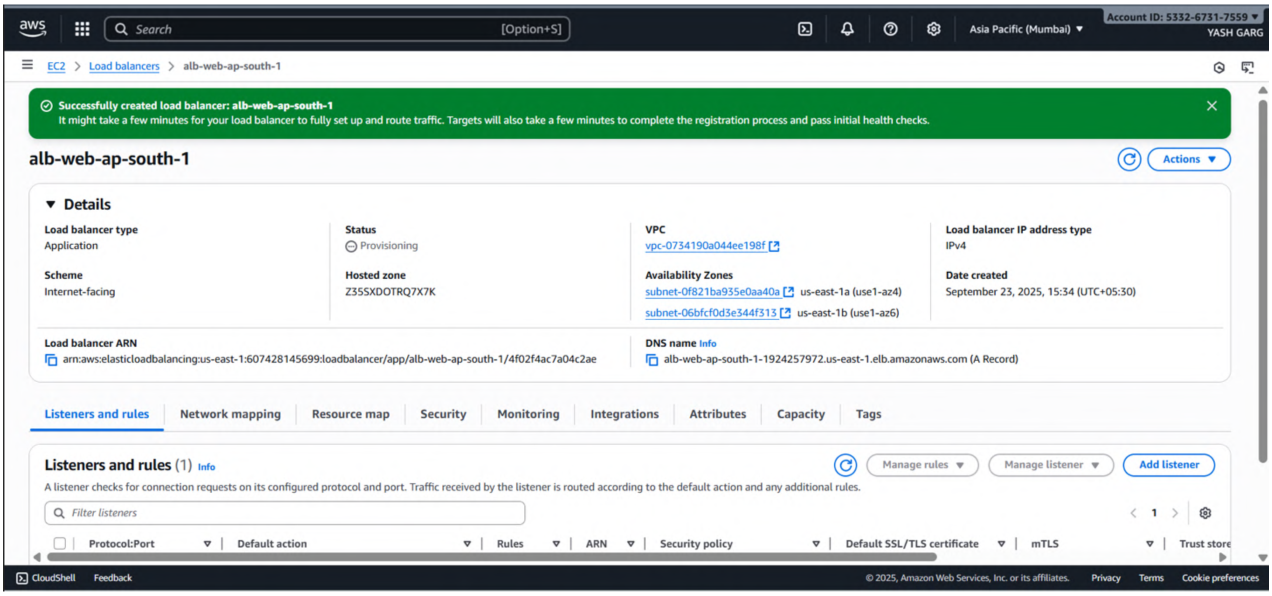
The default action is used if no other rules apply. Choose the default action for traffic on this listener.

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.



Successfully created load balancer: alb-web-ap-south-1
It might take a few minutes for your load balancer to fully set up and route traffic. Targets will also take a few minutes to complete the registration process and pass initial health checks.

alb-web-ap-south-1

▼ **Details**

Load balancer type Application	**Status** Provisioning	**VPC** vpc-0734190a044ee198f	**Load balancer IP address type** IPv4
Scheme Internet-facing	**Hosted zone** Z35SXDOTRQ7X7K	**Availability Zones** subnet-0f821ba935e0aa40a us-east-1a (use1-az4) subnet-06bfcf0d3e344f313 us-east-1b (use1-az6)	**Date created** September 23, 2025, 15:34 (UTC+05:30)

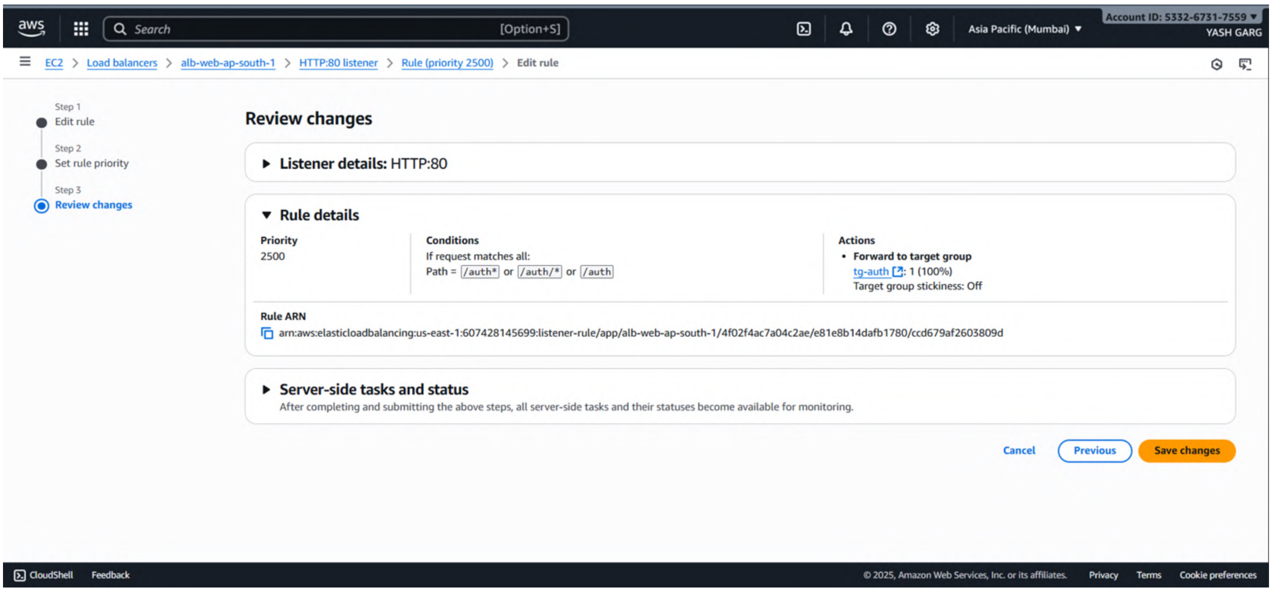
Load balancer ARN
arn:aws:elasticloadbalancing:us-east-1:607428145699:loadbalancer/app/alb-web-ap-south-1/4f02f4ac7a04c2ae

DNS name Info
alb-web-ap-south-1-1924257972.us-east-1.elb.amazonaws.com (A Record)

Listeners and rules (1) 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	Default SSL/TLS certificate	mTLS	Trust store



Search [Option+S]
Asia Pacific (Mumbai)
Account ID: 5332-6731-7559
YASH GARG
EC2 > Load balancers > alb-web-ap-south-1 > HTTP:80 listener > Rule (priority 2500) > Edit rule
Step 1 Edit rule
Step 2 Set rule priority
Step 3 Review changes

Review changes

Listener details: HTTP:80

Rule details

Priority	Conditions	Actions
2500	If request matches all: Path = /auth* or /auth/* or /auth	• Forward to target group tg-auth: 1 (100%) Target group stickiness: Off

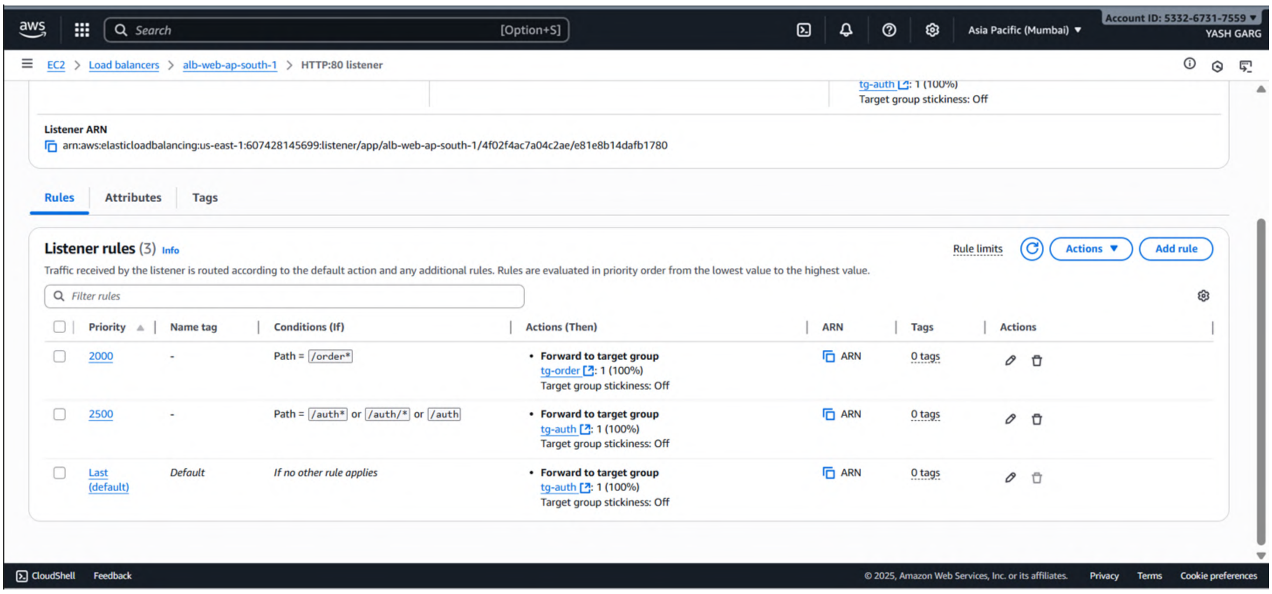
Rule ARN

arn:aws:elasticloadbalancing:us-east-1:607428145699:listener-rule/app/alb-web-ap-south-1/4f02f4ac7a04c2ae/e81e8b14dafb1780/ccd679af2603809d

Server-side tasks and status

After completing and submitting the above steps, all server-side tasks and their statuses become available for monitoring.

Cancel
Previous
Save changes
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



Search [Option+S]
Asia Pacific (Mumbai)
Account ID: 5332-6731-7559
YASH GARG
EC2 > Load balancers > alb-web-ap-south-1 > HTTP:80 listener

tg-auth: 1 (100%)
Target group stickiness: Off

Listener ARN

arn:aws:elasticloadbalancing:us-east-1:607428145699:listener/app/alb-web-ap-south-1/4f02f4ac7a04c2ae/e81e8b14dafb1780

Listener rules (3) Info

Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.

Priority	Name tag	Conditions (If)	Actions (Then)	ARN	Tags	Actions
2000	-	Path = /order*	• Forward to target group tg-order: 1 (100%) Target group stickiness: Off	ARN	0 tags	
2500	-	Path = /auth* or /auth/* or /auth	• Forward to target group tg-auth: 1 (100%) Target group stickiness: Off	ARN	0 tags	
Last (default)	Default	If no other rule applies	• Forward to target group tg-auth: 1 (100%) Target group stickiness: Off	ARN	0 tags	

CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

5) Configure Auto Scaling (per region, per service) — GUI only

We'll create Launch Templates and Auto Scaling Groups (ASGs) that attach to the appropriate target group; the ASG will auto register instances with ALB.

A. Create a Launch Template

1. Services → **EC2** → left menu → **Instances** → **Launch Templates** → **Create launch template**.
2. Name: lt-auth (for the auth service)
3. Template content:
   - AMI: Amazon Linux 2
   - Instance type: t3.micro
   - Key pair: same as earlier
   - Network settings: leave (ASG will choose subnets)
   - Security group: web-ec2-sg

- Advanced user data: same user-data used for auth instances (so the ASG instances serve /health)

4.Create launch template

Repeat and create lt-order.

B.Create Auto Scaling Group

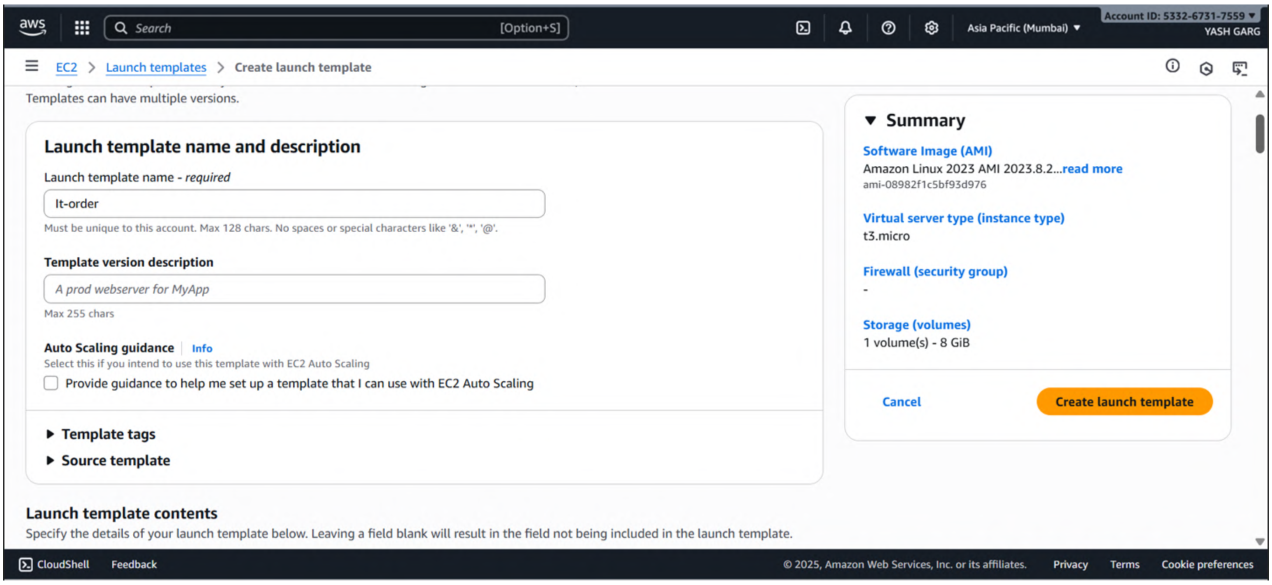
2. Services → EC2 → Auto Scaling → Auto Scaling Groups → Create Auto Scaling group.
3. Choose launch template: select lt-auth.
4. ASG name: asg-auth-ap-south-1.
5. Choose VPC and select **two subnets** (AZ1 and AZ2).
6. Attach to load balancer:
    - Select **Attach to an existing load balancer** → choose the ALB alb-web-ap-south-1.
    - Select target group: tg-auth (so ASG will register instances to that target group)
7. Set group size:
    - Minimum capacity: 2
    - Desired capacity: 2
    - Maximum capacity: 4
8. Configure scaling policies:
    - Choose **Target tracking scaling policy** → Average CPU utilization target value e.g. 50% **OR** choose **ALB request count per target** (if available) with a target request value (e.g., 50).
9. Review and create.

Repeat steps to create asg-order-ap-south-1 using lt-order and attach to tg-order.

B. Verify Auto Scaling

1. After creation go to Auto Scaling Groups → select the ASG → **Instances** tab → verify EC2 instances launched by ASG (they will have names generated by ASG).
2. Confirm these instances appear as healthy in the associated target group.

Repeat Launch Template + ASG creation in the **other region** (us-east-1) — create identical resources there and attach to that region's ALB and target groups.



aws
Search [Option+S]
Asia Pacific (Mumbai) ▼
Account ID: 5332-6731-7559 ▼
YASH GARG
EC2 > Launch templates > Create launch template

Templates can have multiple versions.

Launch template name and description

Launch template name - *required*

lt-order

Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.

Template version description

A prod webserver for MyApp

Max 255 chars

Auto Scaling guidance Info

Select this if you intend to use this template with EC2 Auto Scaling

□ Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

▶ Template tags

▶ Source template

Launch template contents

Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

▼ Summary

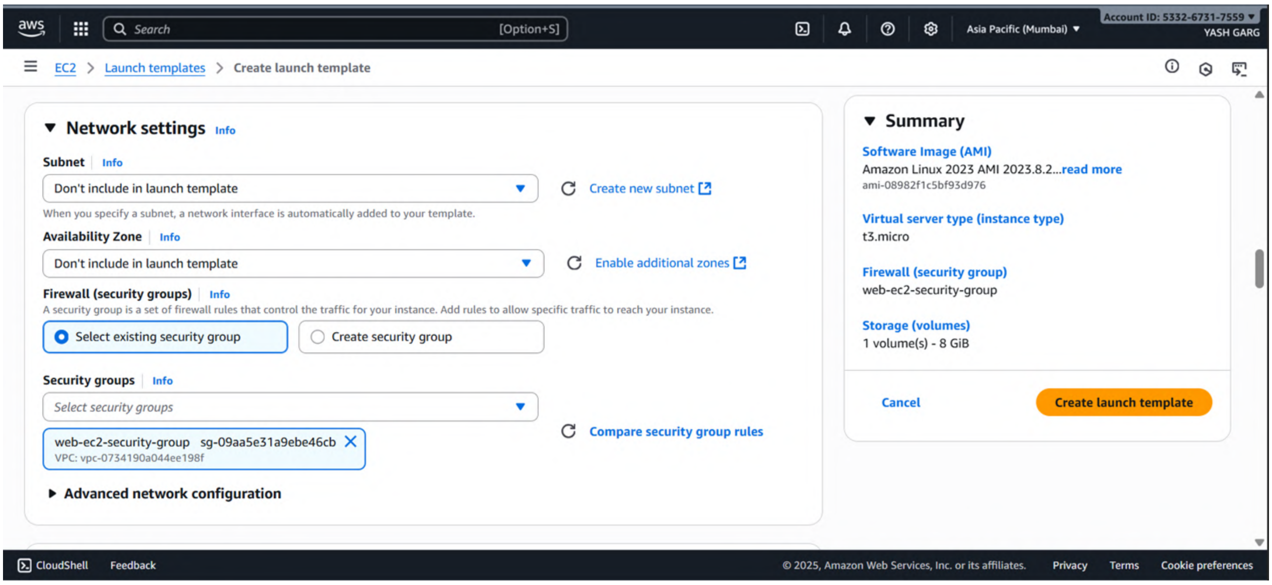
Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-08982f1c5bf93d976

Virtual server type (instance type)
t3.micro

Firewall (security group)
-

Storage (volumes)
1 volume(s) - 8 GiB

Cancel
Create launch template
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



aws
Search [Option+S]
Asia Pacific (Mumbai) ▼
Account ID: 5332-6731-7559 ▼
YASH GARG
EC2 > Launch templates > Create launch template

▼ Network settings Info

Subnet Info

Don't include in launch template ▼

Create new subnet

When you specify a subnet, a network interface is automatically added to your template.

Availability Zone Info

Don't include in launch template ▼

Enable additional zones

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Select existing security group ○ Create security group

Security groups Info

Select security groups ▼

web-ec2-security-group sg-09aa5e31a9ebe46cb ✕
VPC: vpc-0734190a044ee198f

Compare security group rules

▶ Advanced network configuration

▼ Summary

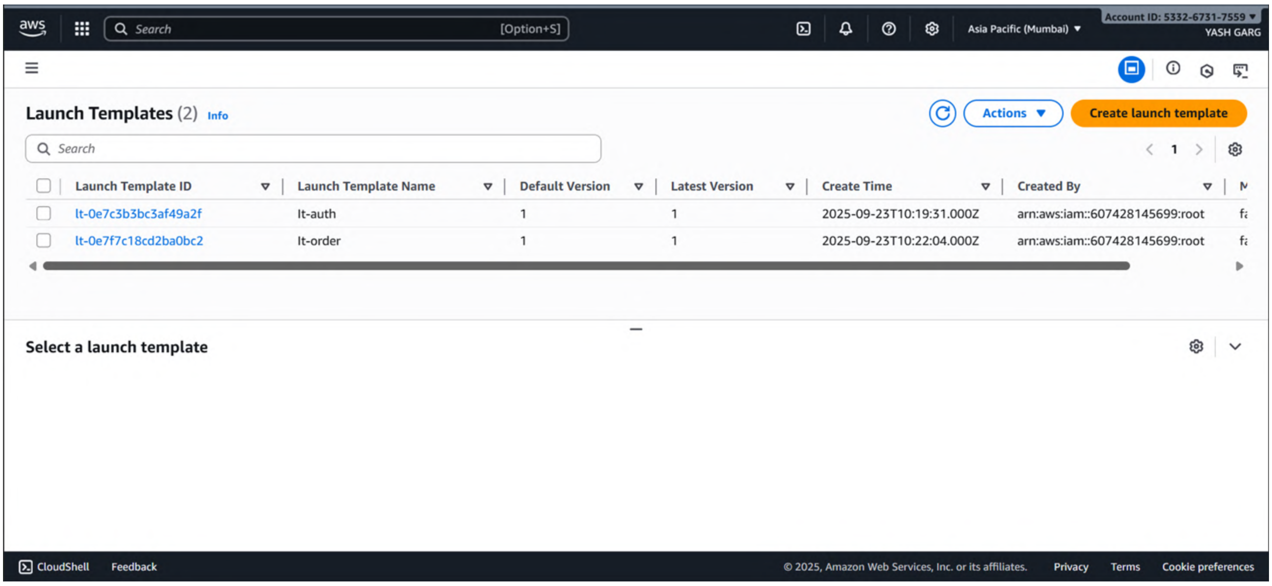
Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-08982f1c5bf93d976

Virtual server type (instance type)
t3.micro

Firewall (security group)
web-ec2-security-group

Storage (volumes)
1 volume(s) - 8 GiB

Cancel
Create launch template
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



aws
Search [Option+S]
Asia Pacific (Mumbai) ▼
Account ID: 5332-6731-7559 ▼
YASH GARG
Actions ▼
Create launch template
Search

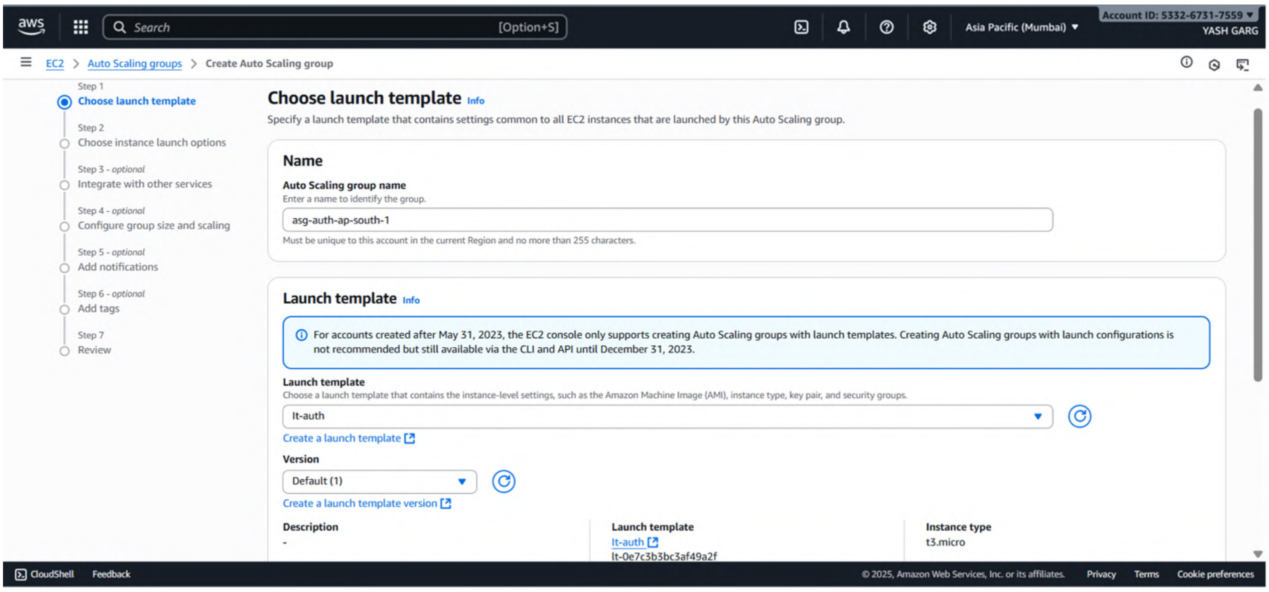
Launch Templates (2) Info

□	Launch Template ID	Launch Template Name	Default Version	Latest Version	Create Time	Created By	M
□	lt-0e7c3b3bc3af49a2f	lt-auth	1	1	2025-09-23T10:19:31.000Z	arn:aws:iam::607428145699:root	fa
□	lt-0e7f7c18cd2ba0bc2	lt-order	1	1	2025-09-23T10:22:04.000Z	arn:aws:iam::607428145699:root	fa

Select a launch template

CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Auto-Scaling Group:


aws
Search [Option+S]
Asia Pacific (Mumbai) ▼
Account ID: 5332-6731-7559 ▼
YASH GARG
EC2 > Auto Scaling groups > Create Auto Scaling group
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Step 1
● Choose launch template

Step 2
○ Choose instance launch options

Step 3 - *optional*
○ Integrate with other services

Step 4 - *optional*
○ Configure group size and scaling

Step 5 - *optional*
○ Add notifications

Step 6 - *optional*
○ Add tags

Step 7
○ Review

Choose launch template Info

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group.

Name

Auto Scaling group name
Enter a name to identify the group.
asg-auth-ap-south-1
Must be unique to this account in the current Region and no more than 255 characters.

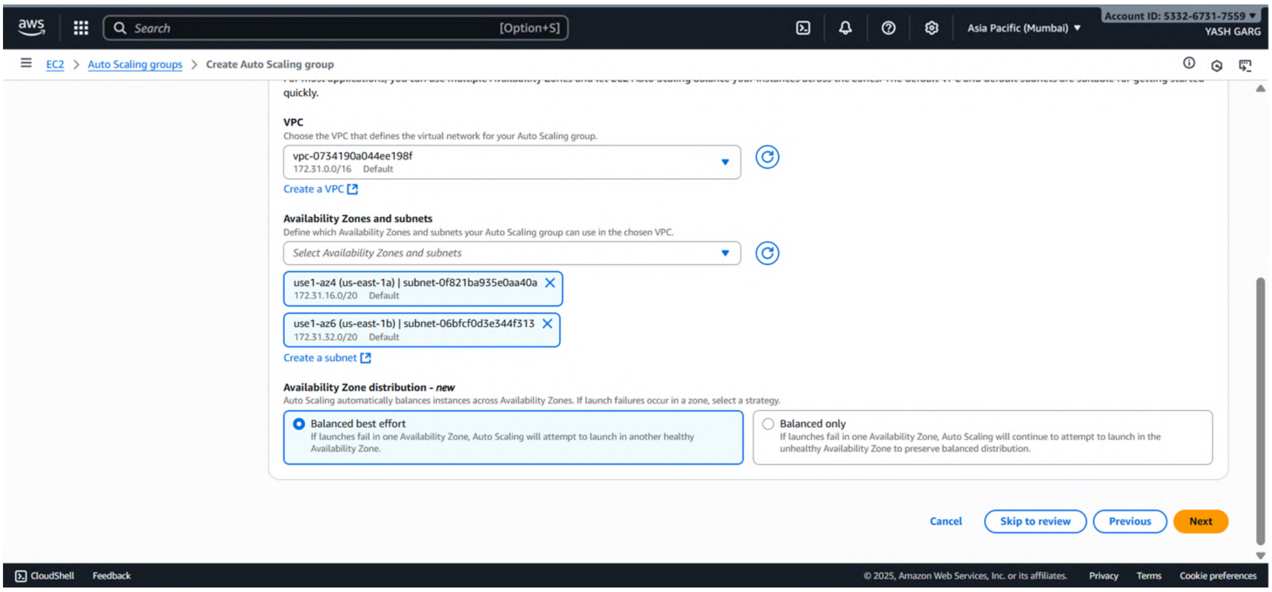
Launch template Info

ⓘ For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

Launch template
Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.
lt-auth ▼
Create a launch template

Version
Default (1) ▼
Create a launch template version

Description	Launch template	Instance type
-	lt-auth lt-0e7c3b3bc3af49a2f	t3.micro


aws
Search [Option+S]
Asia Pacific (Mumbai) ▼
Account ID: 5332-6731-7559 ▼
YASH GARG
EC2 > Auto Scaling groups > Create Auto Scaling group
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

quickly.

VPC
Choose the VPC that defines the virtual network for your Auto Scaling group.
vpc-0734190a044ee198f
172.31.0.0/16 Default
Create a VPC

Availability Zones and subnets
Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.
Select Availability Zones and subnets

use1-az4 (us-east-1a) | subnet-0f821ba935e0aa40a ✕
172.31.16.0/20 Default

use1-az6 (us-east-1b) | subnet-06bfcf0d3e344f313 ✕
172.31.32.0/20 Default

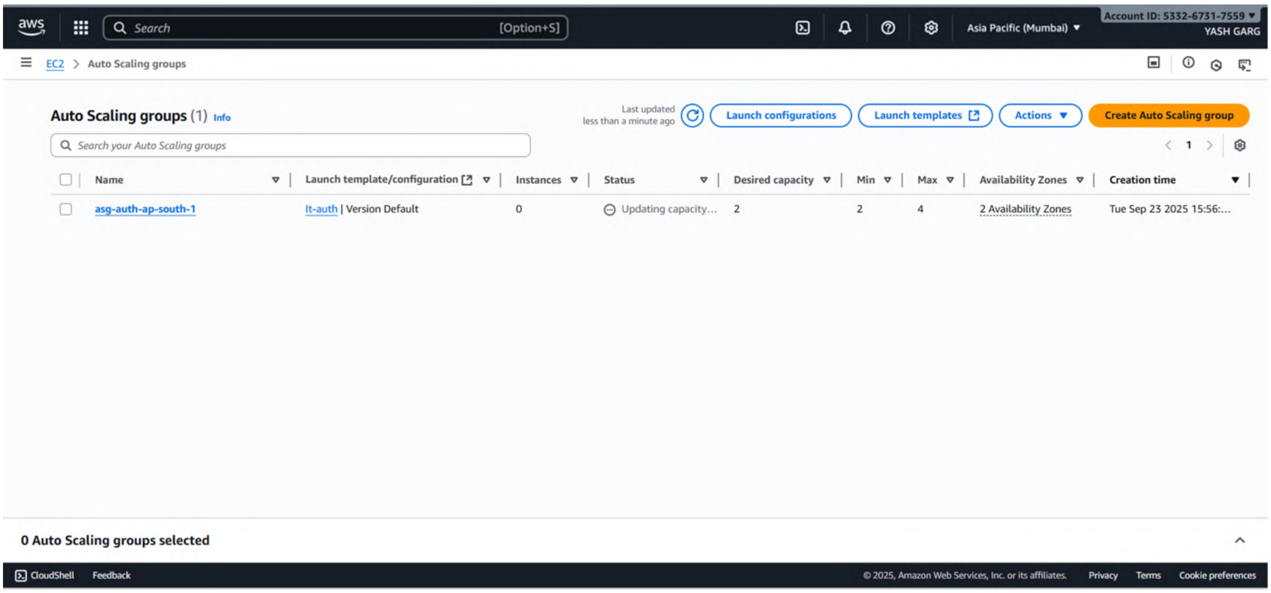
Create a subnet

Availability Zone distribution - *new*
Auto Scaling automatically balances instances across Availability Zones. If launch failures occur in a zone, select a strategy.

● Balanced best effort
If launches fail in one Availability Zone, Auto Scaling will attempt to launch in another healthy Availability Zone.

○ Balanced only
If launches fail in one Availability Zone, Auto Scaling will continue to attempt to launch in the unhealthy Availability Zone to preserve balanced distribution.

Cancel
Skip to review
Previous
Next


aws
Search [Option+S]
Asia Pacific (Mumbai) ▼
Account ID: 5332-6731-7559 ▼
YASH GARG
EC2 > Auto Scaling groups
Last updated less than a minute ago
Launch configurations
Launch templates
Actions ▼
Create Auto Scaling group
Search your Auto Scaling groups
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Auto Scaling groups (1) Info

□	Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability Zones	Creation time
□	asg-auth-ap-south-1	lt-auth | Version Default	0	Updating capacity...	2	2	4	2 Availability Zones	Tue Sep 23 2025 15:56:...

0 Auto Scaling groups selected

6) Route 53 — Global DNS to route users to nearest region (latency)

Now integrate ALBs with Route 53 so global users are routed to the nearest healthy ALB / region.

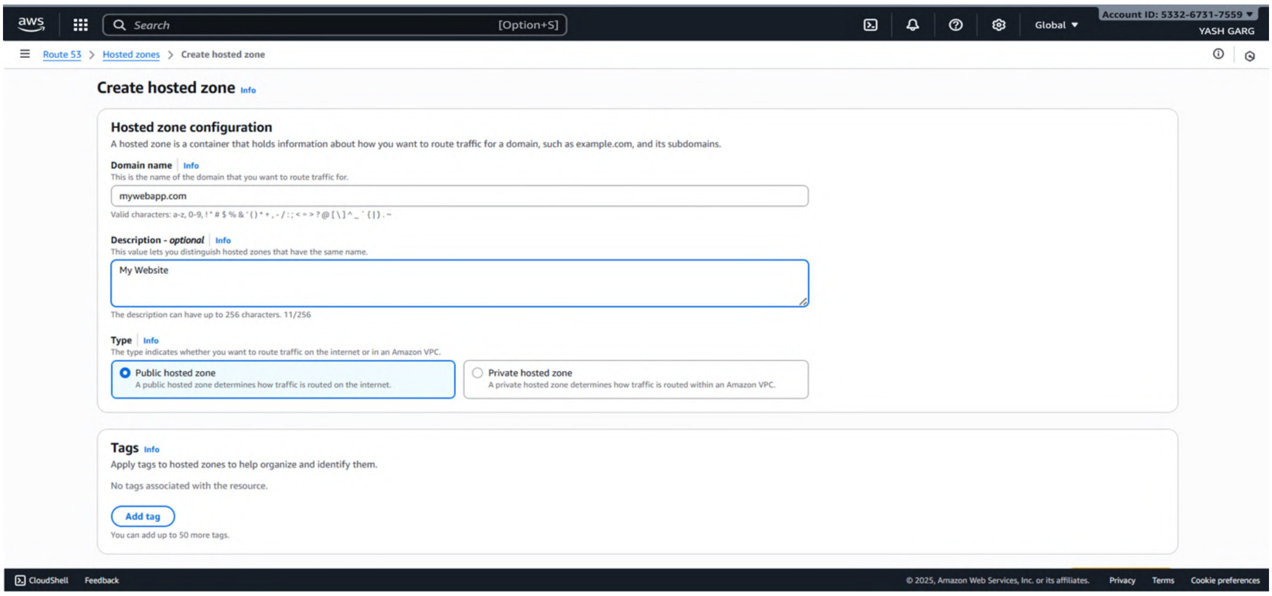
A. Create or use an existing hosted zone

1. Services → **Route 53** → **Hosted zones** → **Create hosted zone** (if you don't have a domain).
   - Domain name: yourdomain.com
   - Type: Public hosted zone
2. Click **Create hosted zone**.

Screenshot #16: Hosted zone created.
Filename: 16-hosted-zone.png

B. Create latency records that point to regional ALBs

1. In the hosted zone → **Create record**.
2. Record name: www (or root @ if you want)
3. Routing policy: choose **Latency**.
4. Set one record for **ap-south-1 ALB**:
   - Select **Alias** → Alias to **Application and Classic Load Balancer** → Region: Asia Pacific (Mumbai) → select the ALB alb-web-ap-south-1 from dropdown.
   - Evaluate target health: **Yes**
   - Save record.
5. Create another **Latency** record for the other region:
   - Same record name: www
   - Routing policy: **Latency**
   - Alias to ALB in US East (N. Virginia) → select alb-web-us-east-1.
   - Evaluate target health: **Yes**
6. Now Route 53 will route users to the ALB (region) with lowest latency, and will avoid regions whose ALB is unhealthy (because Evaluate target health is on).


aws
Search [Option+S]
Global ▾
Account ID: 5332-6731-7559 ▾
YASH GARG
Route 53 > Hosted zones > Create hosted zone

Create hosted zone Info

Hosted zone configuration

A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.

Domain name | Info
This is the name of the domain that you want to route traffic for.
mywebapp.com
Valid characters: a-z, 0-9, ! " # $ % & ' ( ) * + , - / : ; < = > ? @ [\ ] ^ _ ` { | } . ~

Description - *optional* | Info
This value lets you distinguish hosted zones that have the same name.
My Website
The description can have up to 256 characters. 11/256

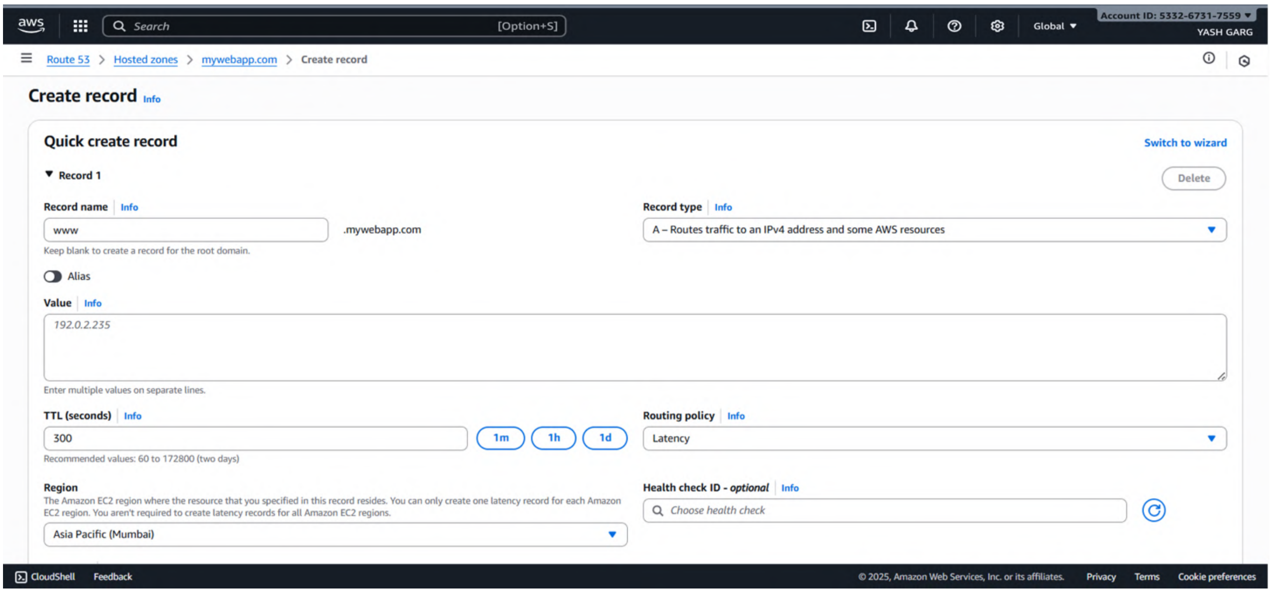
Type | Info
The type indicates whether you want to route traffic on the internet or in an Amazon VPC.

● 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.
No tags associated with the resource.
Add tag
You can add up to 50 more tags.

CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Search [Option+S]
Global ▾
Account ID: 5332-6731-7559 ▾
YASH GARG
Route 53 > Hosted zones > mywebapp.com > Create record

Create record Info

Quick create record

▼ Record 1

Record name | Info
www .mywebapp.com
Keep blank to create a record for the root domain.

Record type | Info
A – Routes traffic to an IPv4 address and some AWS resources

Alias

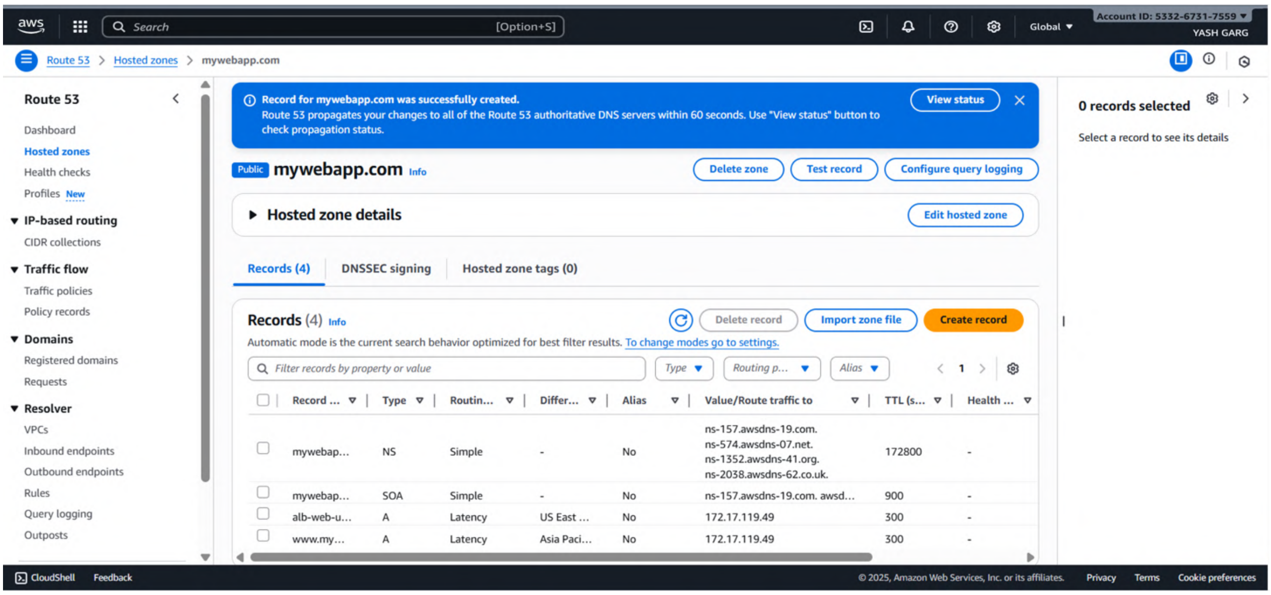
Value | Info
192.0.2.235
Enter multiple values on separate lines.

TTL (seconds) | Info
300 1m 1h 1d
Recommended values: 60 to 172800 (two days)

Routing policy | Info
Latency

Region
The Amazon EC2 region where the resource that you specified in this record resides. You can only create one latency record for each Amazon EC2 region. You aren't required to create latency records for all Amazon EC2 regions.
Asia Pacific (Mumbai)

Health check ID - *optional* | Info
Choose health check



Record for mywebapp.com 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.

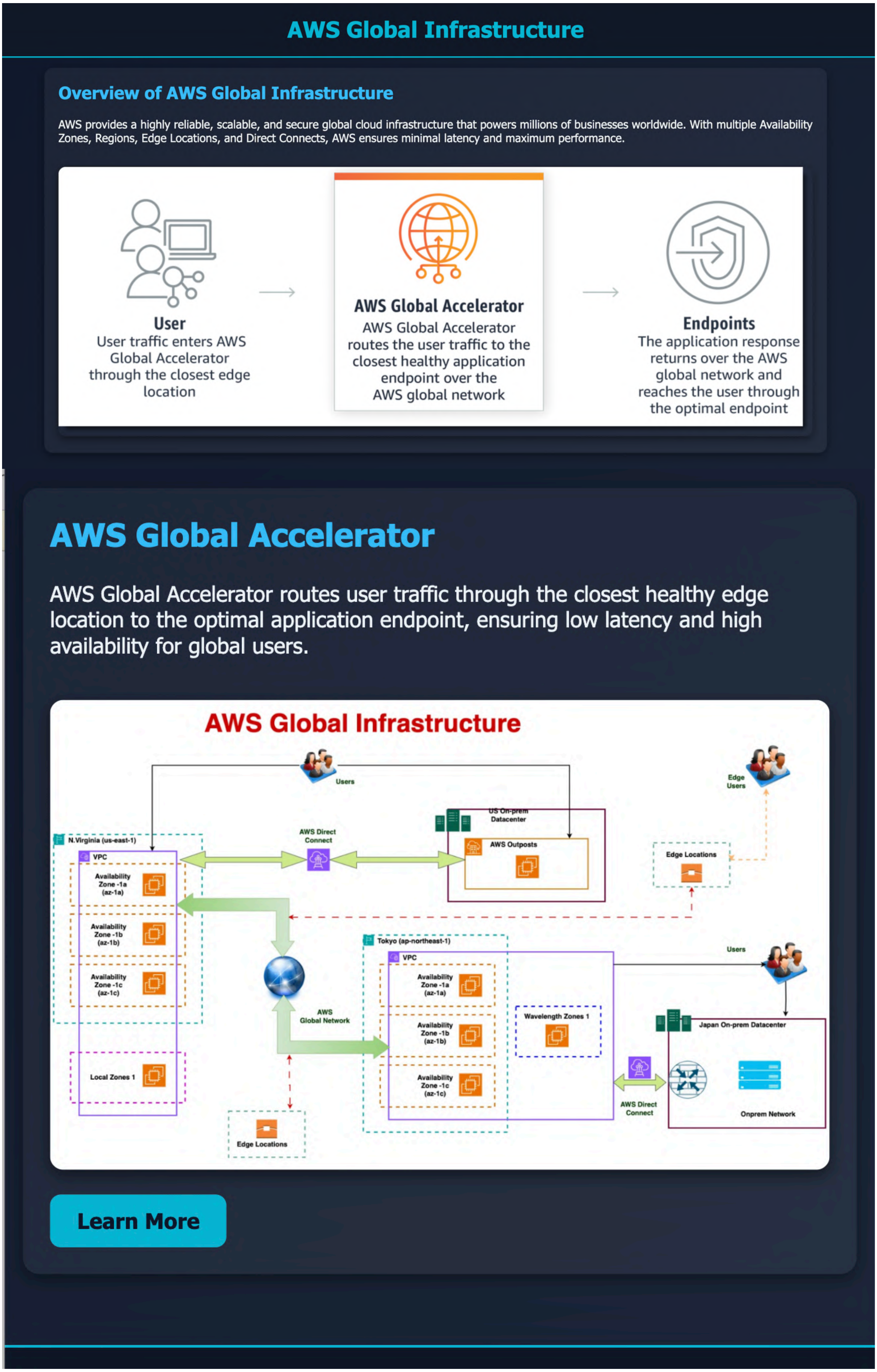
Public mywebapp.com Info

0 records selected
Select a record to see its details

Records (4) Info

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

□	Record ...	Type	Routin...	Differ...	Alias	Value/Route traffic to	TTL (s...	Health ...
□	mywebap...	NS	Simple	-	No	ns-157.awsdns-19.com. ns-574.awsdns-07.net. ns-1352.awsdns-41.org. ns-2038.awsdns-62.co.uk.	172800	-
□	mywebap...	SOA	Simple	-	No	ns-157.awsdns-19.com. awsd...	900	-
□	alb-web-u...	A	Latency	US East ...	No	172.17.119.49	300	-
□	www.my...	A	Latency	Asia Paci...	No	172.17.119.49	300	-



AWS Global Infrastructure

Overview of AWS Global Infrastructure

AWS provides a highly reliable, scalable, and secure global cloud infrastructure that powers millions of businesses worldwide. With multiple Availability Zones, Regions, Edge Locations, and Direct Connects, AWS ensures minimal latency and maximum performance.

User
User traffic enters AWS Global Accelerator through the closest edge location

→

AWS Global Accelerator
AWS Global Accelerator routes the user traffic to the closest healthy application endpoint over the AWS global network

→

Endpoints
The application response returns over the AWS global network and reaches the user through the optimal endpoint

AWS Global Accelerator

AWS Global Accelerator routes user traffic through the closest healthy edge location to the optimal application endpoint, ensuring low latency and high availability for global users.

Learn More