VIT®

Vellore Institute of Technology

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

**SCOPE**

FALL SEMESTER 2025-2026

## LAB ASSESSMENT -4

**Slot:** L13+L14

**Class**: VL2025260105679

**Programme Name & Branch:** B. Tech CSBS

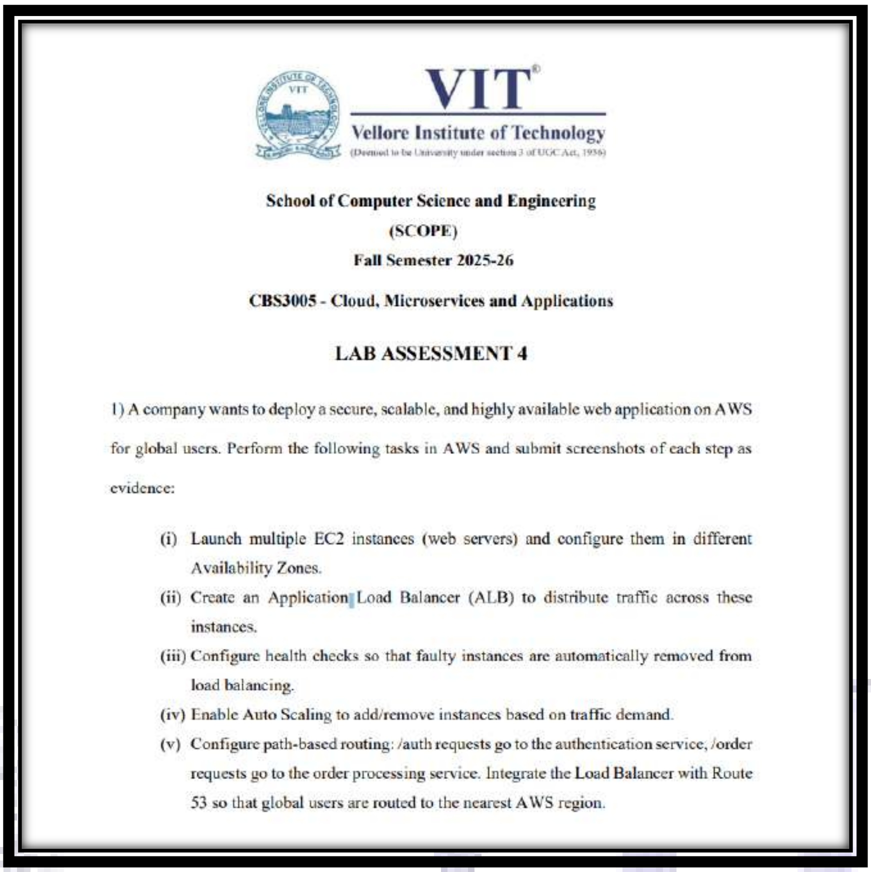
**Course code & Title**: CBS3005- CLOUD, MICROSERVICES AND APPLICATIONS LAB BASED COMPONENTS

**Faculty Name:** NITHYA K

**SUBMITTED BY: -**DIPANGSHU KUNDU

**REGISTRATION NUMBER**: - 22BBS0148

## QUESTION:



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

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.

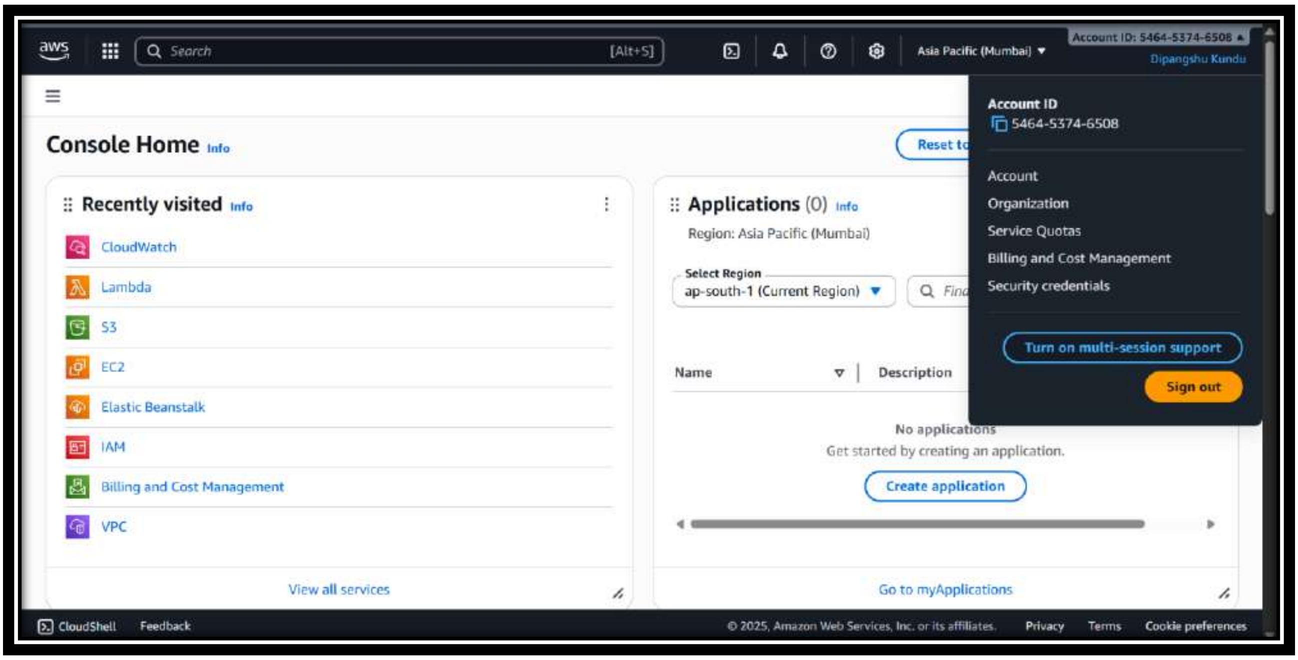
(iv) Enable Auto Scaling to add/remove instances based on traffic demand.

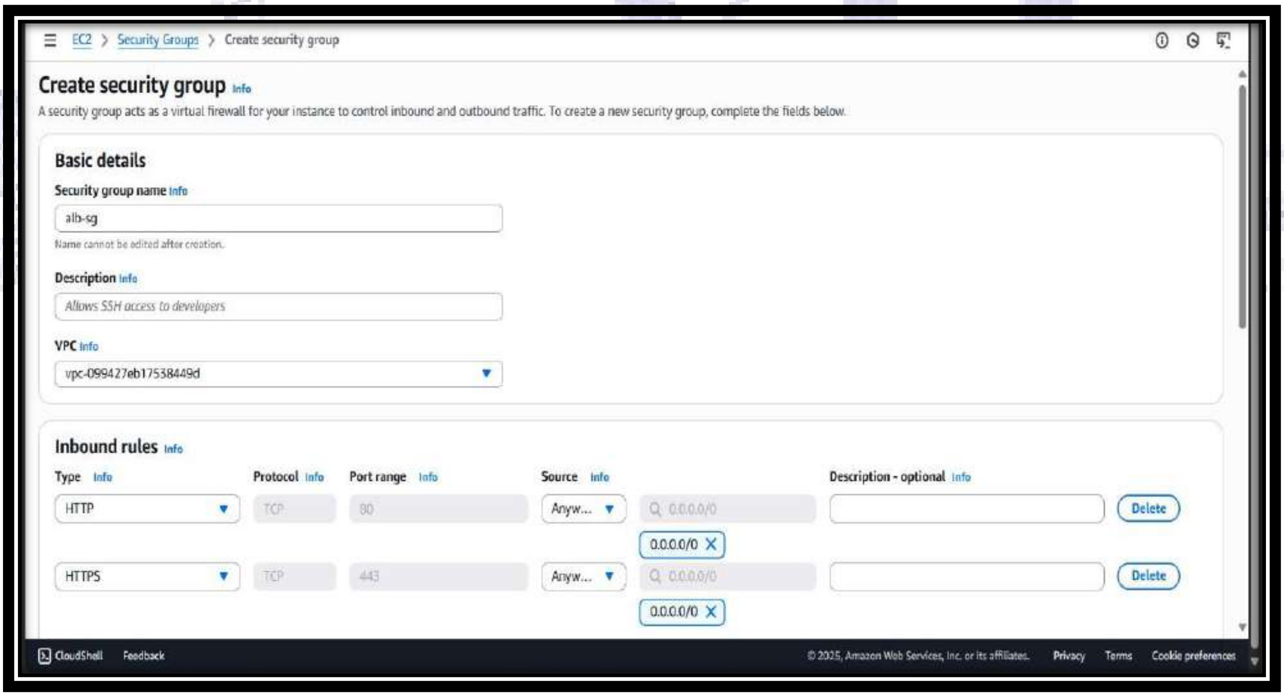
(v) Configure path-based routing: /auth requests go to the authentication service, /order requests go to the order processing service. Integrate the Load Balancer with Route 53 so that global users are routed to the nearest AWS region.

## SOLUTION: -

### Step 1: Create ALB Security Group (in ap-south-1, then repeat in us-east-1)

1. Go to **AWS Console → Services → EC2 → Network & Security → Security Groups → Create security group**.
2. Enter:
   - **Name tag**: alb-sg
   - **Description**: Allow HTTP/HTTPS from Internet
   - **VPC**: Select **Default VPC** (or your custom VPC).
3. Add **Inbound rules**:
   - HTTP, Port 80, Source 0.0.0.0/0
   - HTTPS, Port 443, Source 0.0.0.0/0 *(optional)*
4. Leave **Outbound rules** as default (allow all).
5. Click **Create security group**.




EC2 > Security Groups > Create security group
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

## Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

### Basic details

Security group name Info: alb-sg

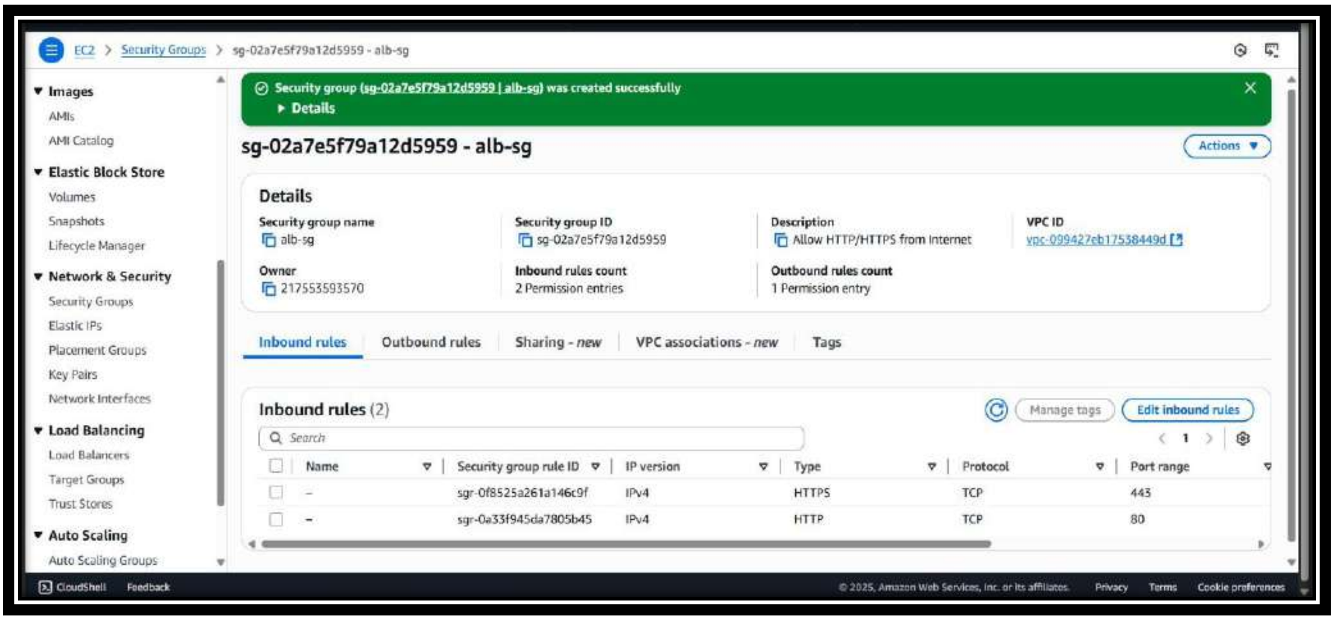
Name cannot be edited after creation.

Description Info: Allows SSH access to developers

VPC Info: vpc-099427eb17538449d

### Inbound rules Info

| Type Info | Protocol Info | Port range Info | Source Info | | Description - optional Info | |
|---|---|---|---|---|---|---|
| HTTP | TCP | 80 | Anyw... | 0.0.0.0/0<br>0.0.0.0/0 ✕ | | Delete |
| HTTPS | TCP | 443 | Anyw... | 0.0.0.0/0<br>0.0.0.0/0 ✕ | | Delete |



Security group (sg-02a7e5f79a12d5959 | alb-sg) was created successfully

sg-02a7e5f79a12d5959 - alb-sg

Details

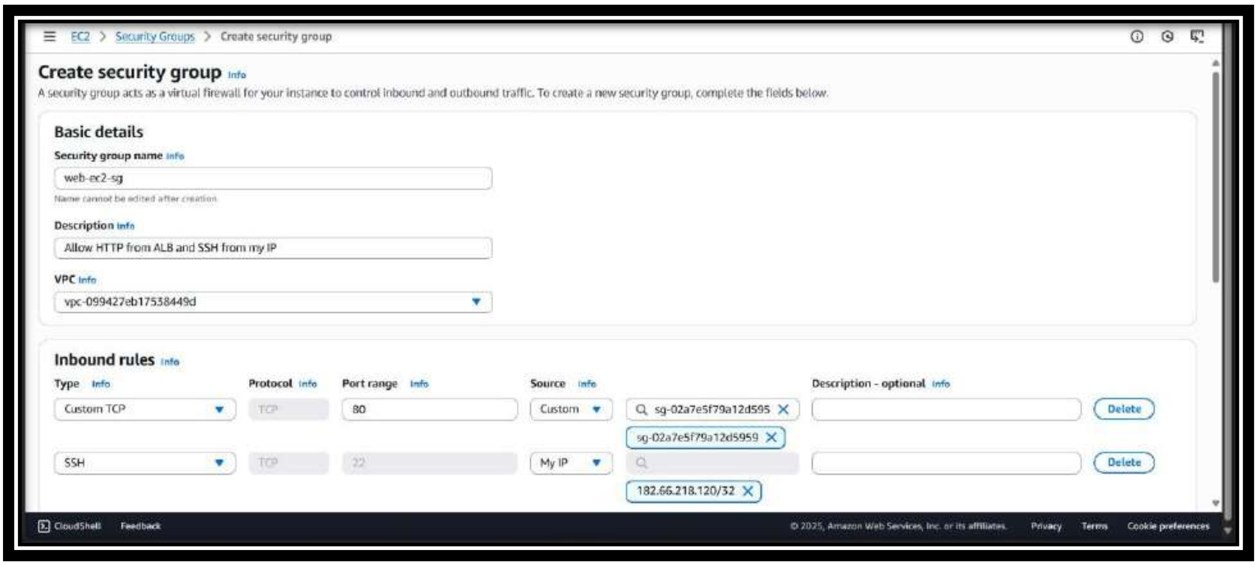
Security group name: alb-sg
Security group ID: sg-02a7e5f79a12d5959
Description: Allow HTTP/HTTPS from Internet
VPC ID: vpc-099427eb17538449d
Owner: 217553593570
Inbound rules count: 2 Permission entries
Outbound rules count: 1 Permission entry

Inbound rules (2)

| Name | Security group rule ID | IP version | Type | Protocol | Port range |
|---|---|---|---|---|---|
| – | sgr-0f8525a261a146c9f | IPv4 | HTTPS | TCP | 443 |
| – | sgr-0a33f945da7805b45 | IPv4 | HTTP | TCP | 80 |

## Step 2: Create EC2 / Web Security Group (in ap-south-1, then repeat in us-east-1)

1. Click **Create security group** again.
2. Enter:
   - **Name tag**: web-ec2-sg
   - **Description**: Allow HTTP from ALB and SSH from my IP
   - **VPC**: Select the **same VPC** used for the ALB security group.
3. Add **Inbound rules**:
   - **Custom TCP Rule**: Port 80 → Source: **Custom** → **Security Group** → **select alb-sg** (this ensures only the ALB can access EC2 on port 80).
   - **SSH**: Port 22 → Source: **My IP** (your public IP, in /32 format).
4. Leave **Outbound rules** as default (allow all).
5. Click **Create security group**.



## Create security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

### Basic details

Security group name: web-ec2-sg

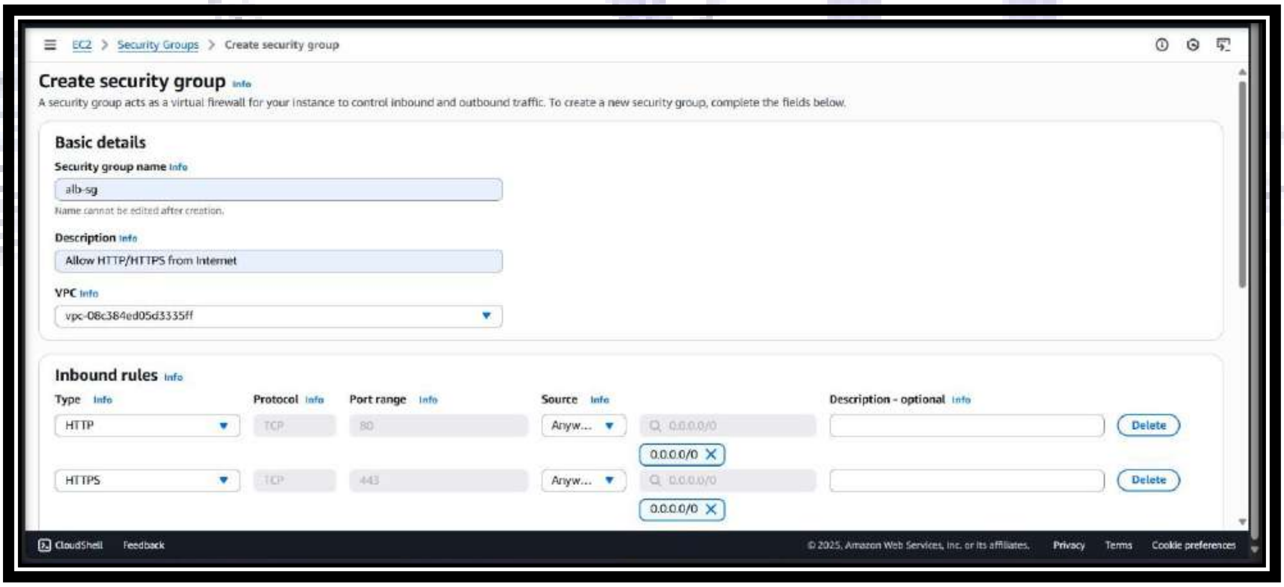
Name cannot be edited after creation.

Description: Allow HTTP from ALB and SSH from my IP

VPC: vpc-099427eb17538449d

### Inbound rules

| Type | Protocol | Port range | Source | | Description - optional | |
|---|---|---|---|---|---|---|
| Custom TCP | TCP | 80 | Custom | sg-02a7e5f79a12d595<br>sg-02a7e5f79a12d5959 | | Delete |
| SSH | TCP | 22 | My IP | 182.66.218.120/32 | | Delete |



## Create security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

### Basic details

Security group name: alb-sg

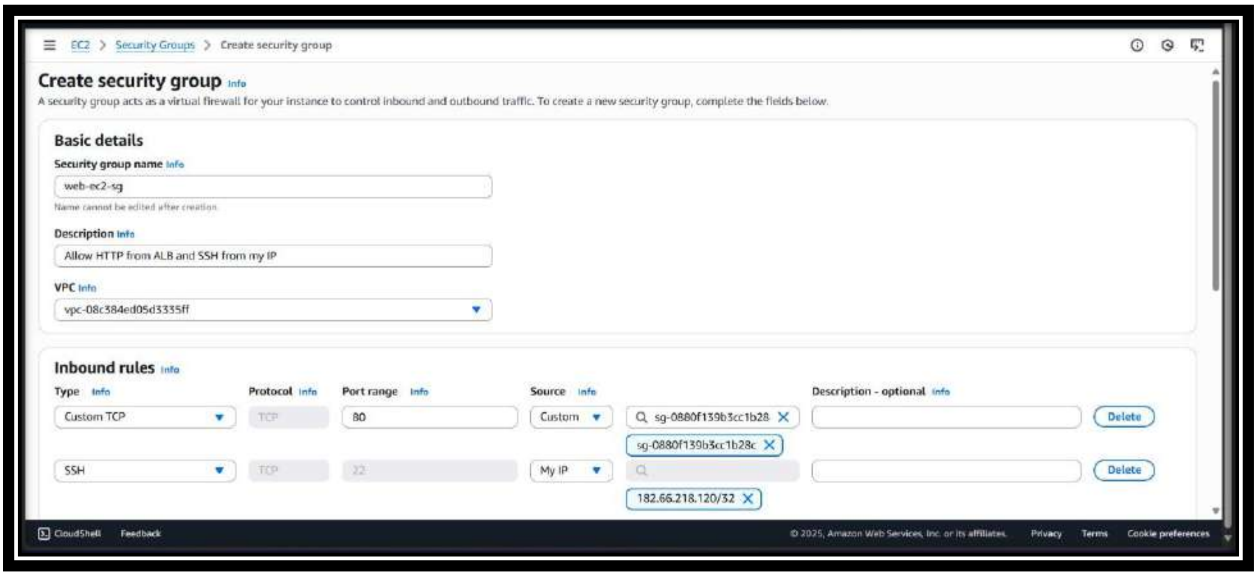
Name cannot be edited after creation.

Description: Allow HTTP/HTTPS from Internet

VPC: vpc-08c384ed05d3335ff

### Inbound rules

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



EC2 > Security Groups > Create security group

**Create security group** Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

**Basic details**

Security group name: web-ec2-sg

Name cannot be edited after creation.

Description: Allow HTTP from ALB and SSH from my IP

VPC: vpc-08c384ed05d3335ff

**Inbound rules**

| Type | Protocol | Port range | Source | | Description - optional | |
|---|---|---|---|---|---|---|
| Custom TCP | TCP | 80 | Custom | sg-0880f139b3cc1b28<br>sg-0880f139b3cc1b28c | | Delete |
| SSH | TCP | 22 | My IP | 182.66.218.120/32 | | Delete |

## Step 3: Launch EC2 Instances (Web Servers)

In **ap-south-1**, create 4 instances (auth-1, auth-2, order-1, order-2) — each service spread across two Availability Zones (AZ1 & AZ2). Later, repeat in **us-east-1**.

1. Go to **EC2 → Instances → Launch instances**.
2. Configure the first instance:
   - **Name**: auth-1
   - **AMI**: Amazon Linux 2 (HVM)
   - **Instance type**: t3.micro
   - **Key pair**: Select or create (download .pem)
   - **Network settings**:
     - VPC: Default (or your VPC)
     - Subnet: AZ1 (e.g., ap-south-1a)
     - Auto-assign Public IP: Enable
     - Security group: web-ec2-sg

- **User data**:

```
#!/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
```

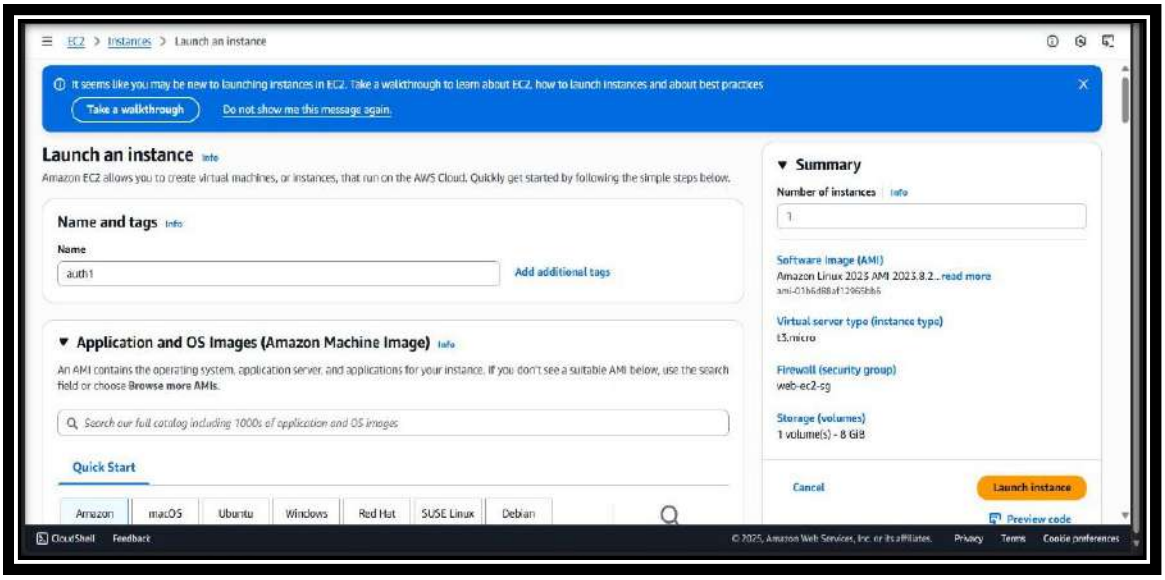
- Click **Launch instance**.

3. Launch auth-2 the same way, but choose a **different subnet** (AZ2, e.g., ap-south-1b) and change the **Name** to auth-2.
4. Launch order-1 and order-2 in the same way, but change the **Name** and **User data**:

```
#!/bin/bash
yum update -y
yum install -y httpd
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
systemctl enable httpd
systemctl start httpd
```

- order-1: AZ1 (e.g., ap-south-1a)
- order-2: AZ2 (e.g., ap-south-1b)

5. Confirm all four instances (auth-1, auth-2, order-1, order-2) are running in **different AZs** and note their private/public IPs.
6. Repeat the same process in **us-east-1** with consistent naming (e.g., us-auth-1, us-auth-2, us-order-1, us-order-2).



EC2 > Instances > Launch an instance

It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices

Take a walkthrough | Do not show me this message again.

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: auth1

Add additional tags

▼ Application and OS Images (Amazon Machine Image) Info

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose **Browse more AMIs**.

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon | macOS | Ubuntu | Windows | Red Hat | SUSE Linux | Debian

▼ Summary

Number of instances Info: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.8.2...read more
ami-01b6d88af12965bb6

Virtual server type (instance type): t3.micro

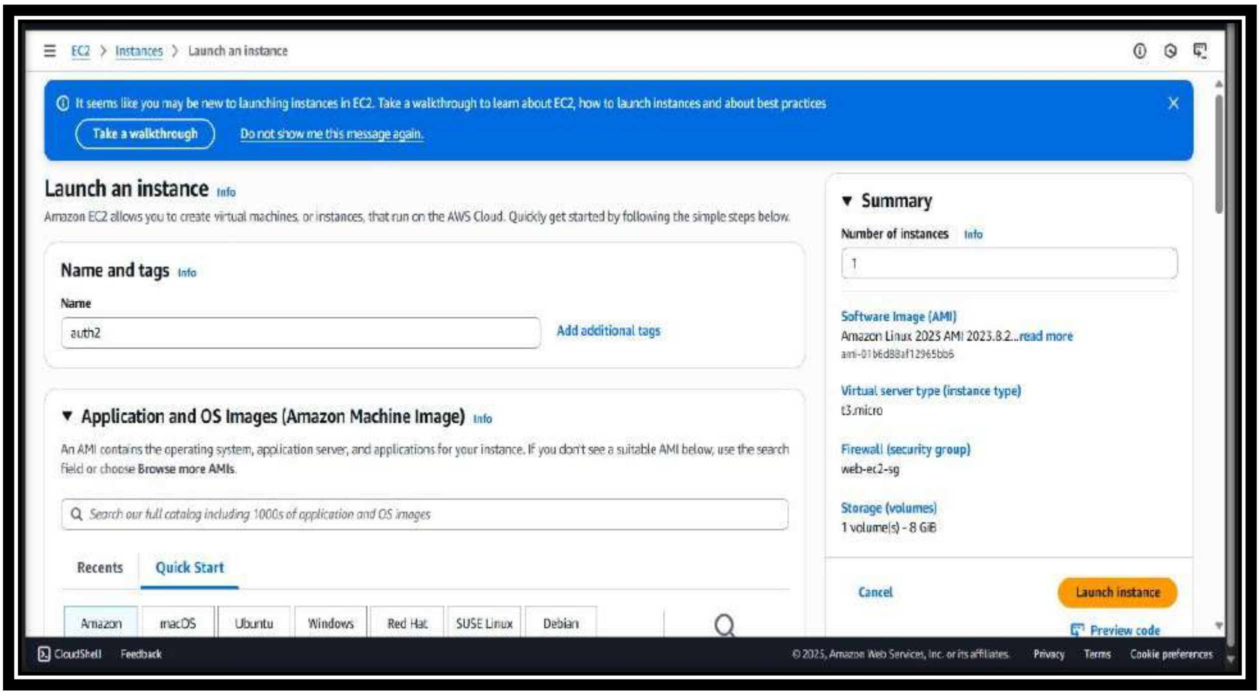
Firewall (security group): web-ec2-sg

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

Cancel | Launch instance

Preview code

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



EC2 > Instances > Launch an instance

It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: auth2

Application and OS Images (Amazon Machine Image) Info

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.

Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Debian

Summary

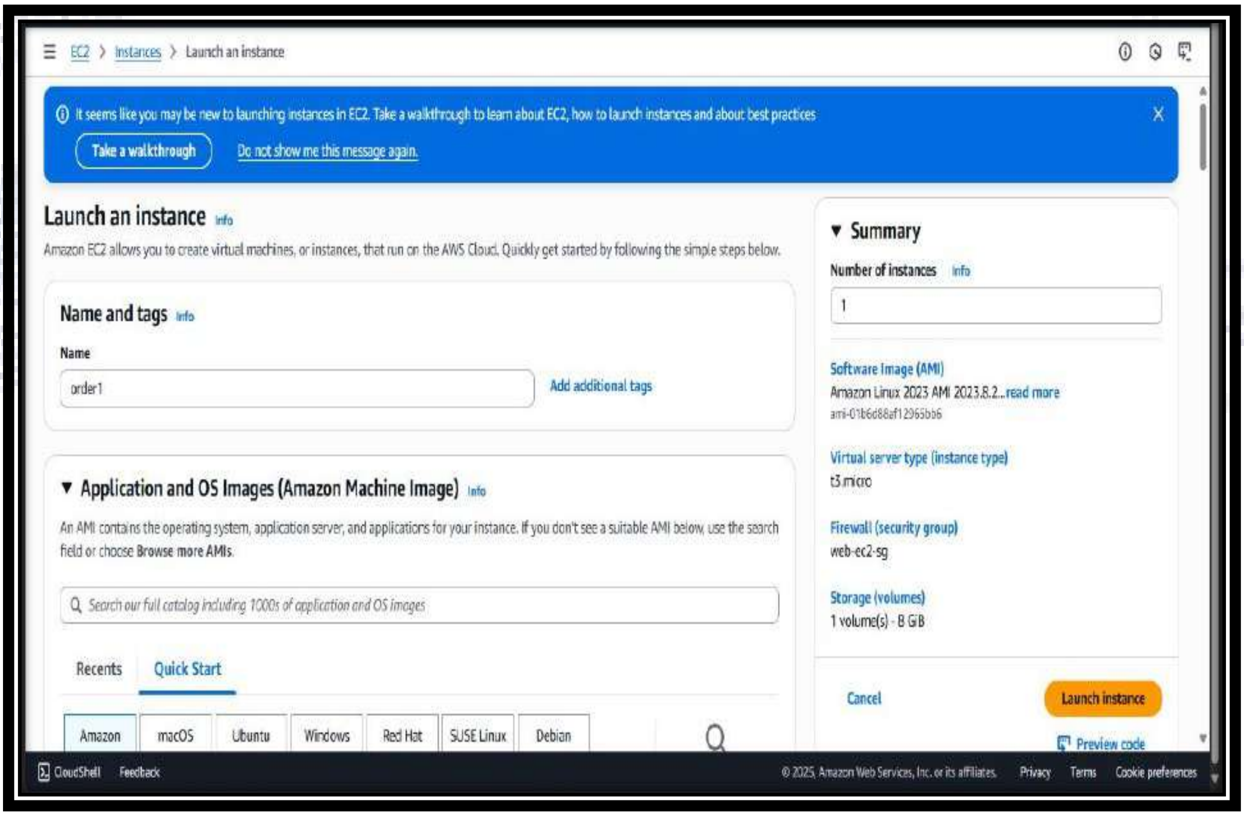
Number of instances Info: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.8.2...read more ami-01b6d88af12965bb6

Virtual server type (instance type): t3.micro

Firewall (security group): web-ec2-sg

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



EC2 > Instances > Launch an instance

It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: order1

Application and OS Images (Amazon Machine Image) Info

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.

Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Debian

Summary

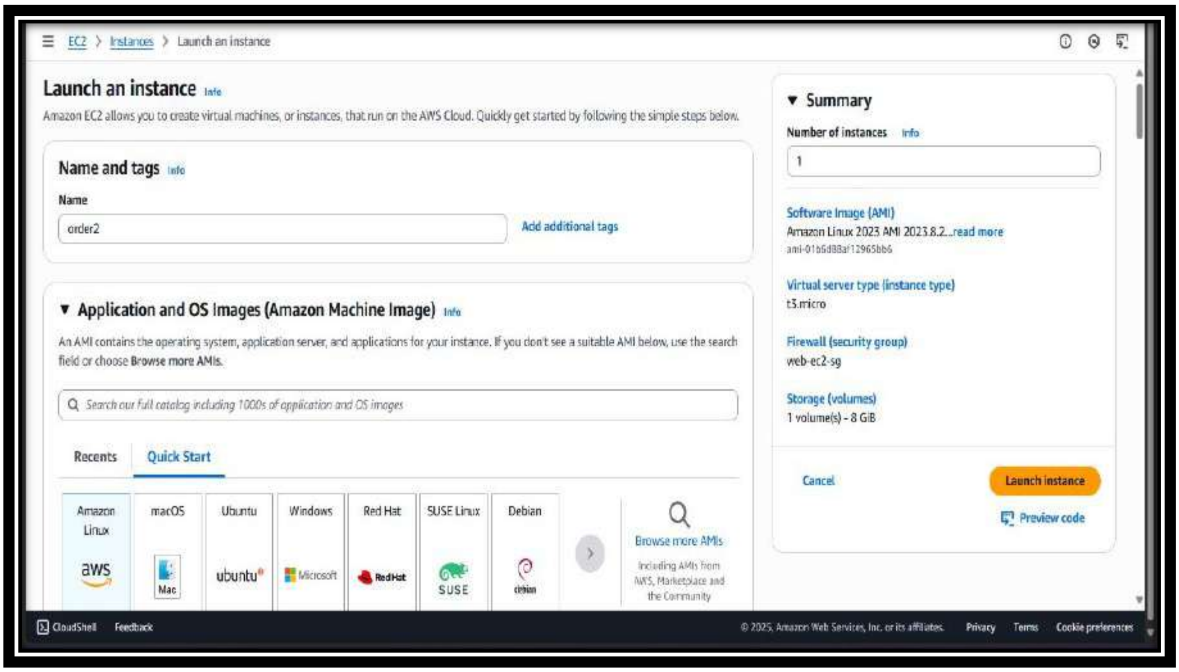
Number of instances Info: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.8.2...read more ami-01b6d88af12965bb6

Virtual server type (instance type): t3.micro

Firewall (security group): web-ec2-sg

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



Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name: order2

Add additional tags

Application and OS Images (Amazon Machine Image)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.

Search our full catalog including 1000s of application and OS images

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.8.2...read more ami-01b5d88af12965bb6

Virtual server type (instance type): t3.micro

Firewall (security group): web-ec2-sg

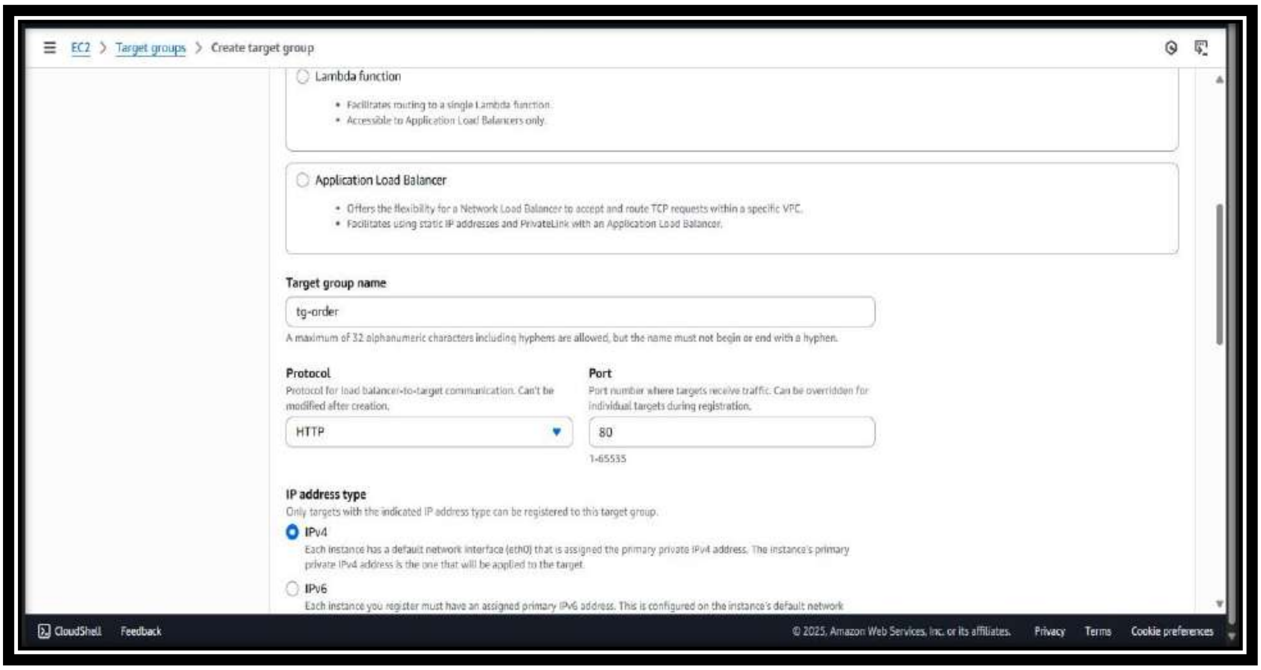
Storage (volumes): 1 volume(s) - 8 GiB

© 2025, Amazon Web Services, Inc. or its affiliates.

## Step 4: Create Target Groups (per region, per service)

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

1. Go to **EC2 → Load Balancing → Target Groups → Create target group**.
2. Configure the first target group:
   - **Target type**: Instance
   - **Protocol**: HTTP
   - **Port**: 80
   - **VPC**: Select your VPC
   - **Name**: tg-auth
3. Configure **Health checks**:
   - Protocol: HTTP
   - Path: /health
   - Success codes: 200
   - Interval: 30s
   - Healthy threshold: 3
   - Unhealthy threshold: 3
4. Click **Create target group**.
5. After creation, go to the **Targets** tab → **Register targets** → select **auth-1** and **auth-2** → Port 80 → **Register**.
6. Repeat the same process to create **tg-order**, then register **order-1** and **order-2**.



EC2 > Target groups > Create target group

○ Lambda function

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

○ Application Load Balancer

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

tg-order

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.

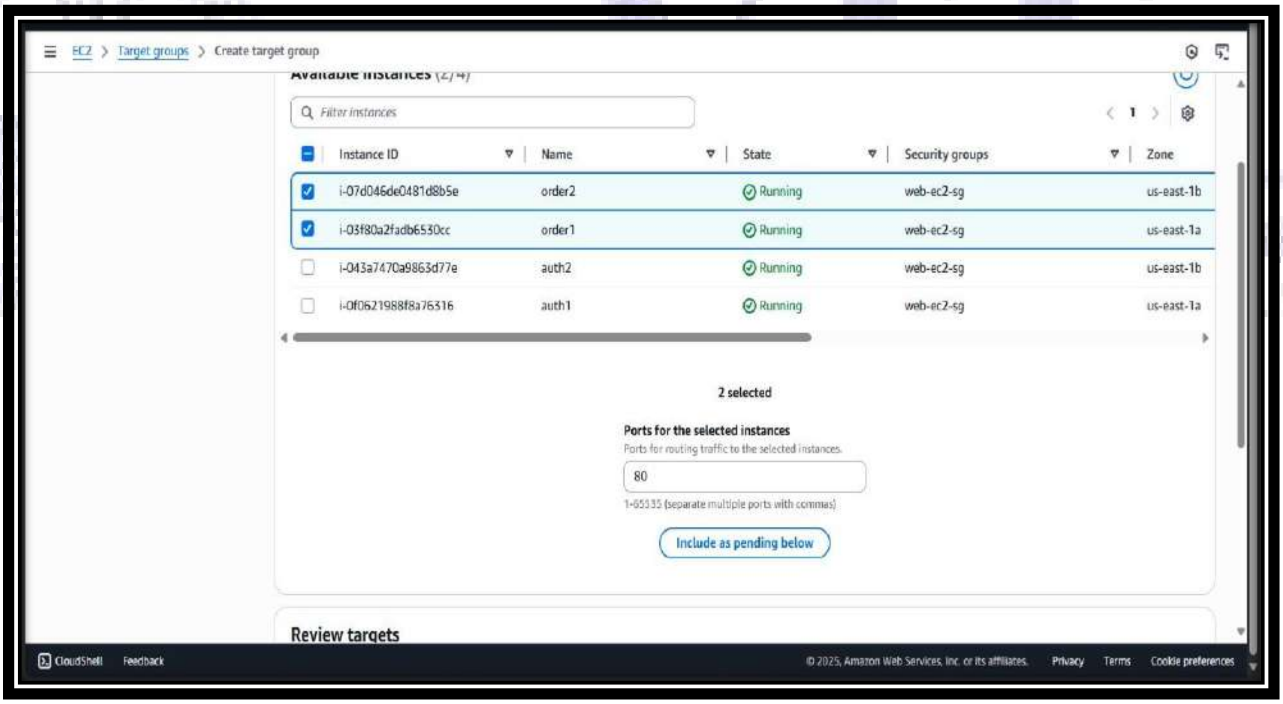
● IPv4

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

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



EC2 > Target groups > Create target group

Available instances (2/4)

Filter instances

|  | Instance ID | Name | State | Security groups | Zone |
|---|---|---|---|---|---|
| ☑ | i-07d046de0481d8b5e | order2 | Running | web-ec2-sg | us-east-1b |
| ☑ | i-03f80a2fadb6530cc | order1 | Running | web-ec2-sg | us-east-1a |
| □ | i-043a7470a9863d77e | auth2 | Running | web-ec2-sg | us-east-1b |
| □ | i-0f0621988f8a76316 | auth1 | Running | web-ec2-sg | us-east-1a |

2 selected

Ports for the selected instances

Ports for routing traffic to the selected instances.

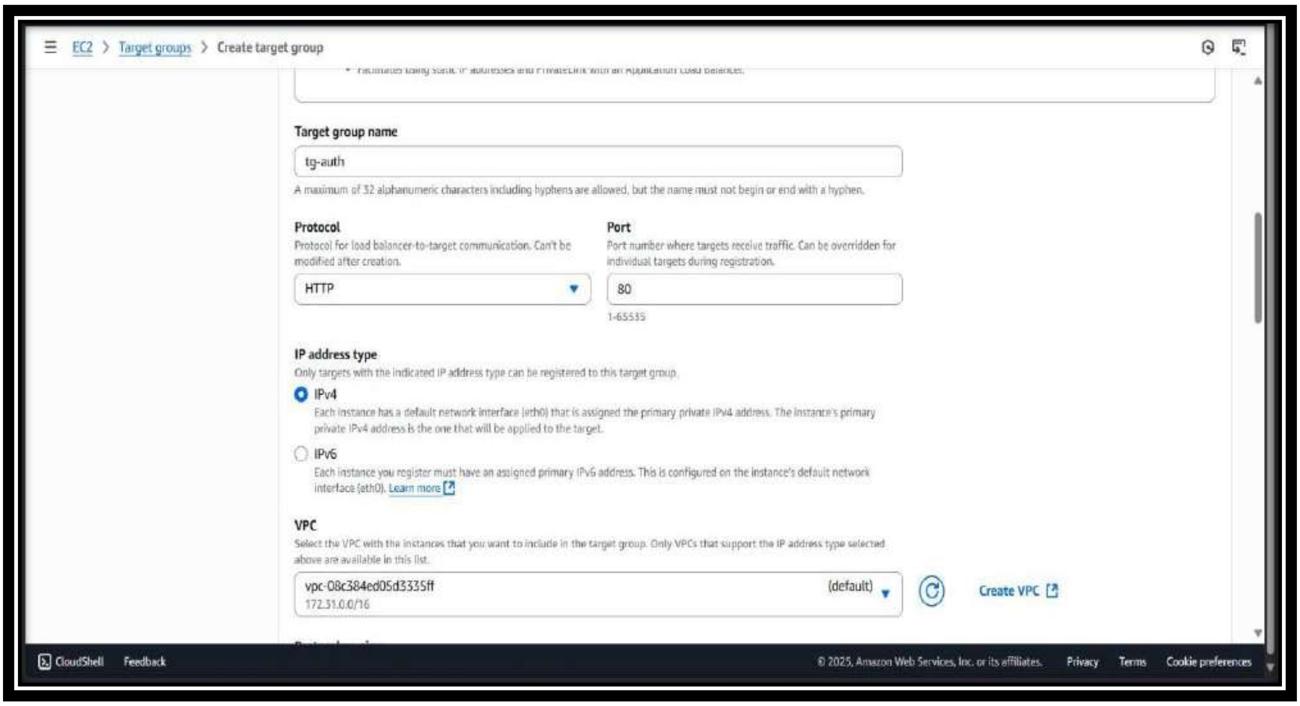
80

1-65535 (separate multiple ports with commas)

Include as pending below

Review targets

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



EC2 > Target groups > Create target group

• Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

**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.

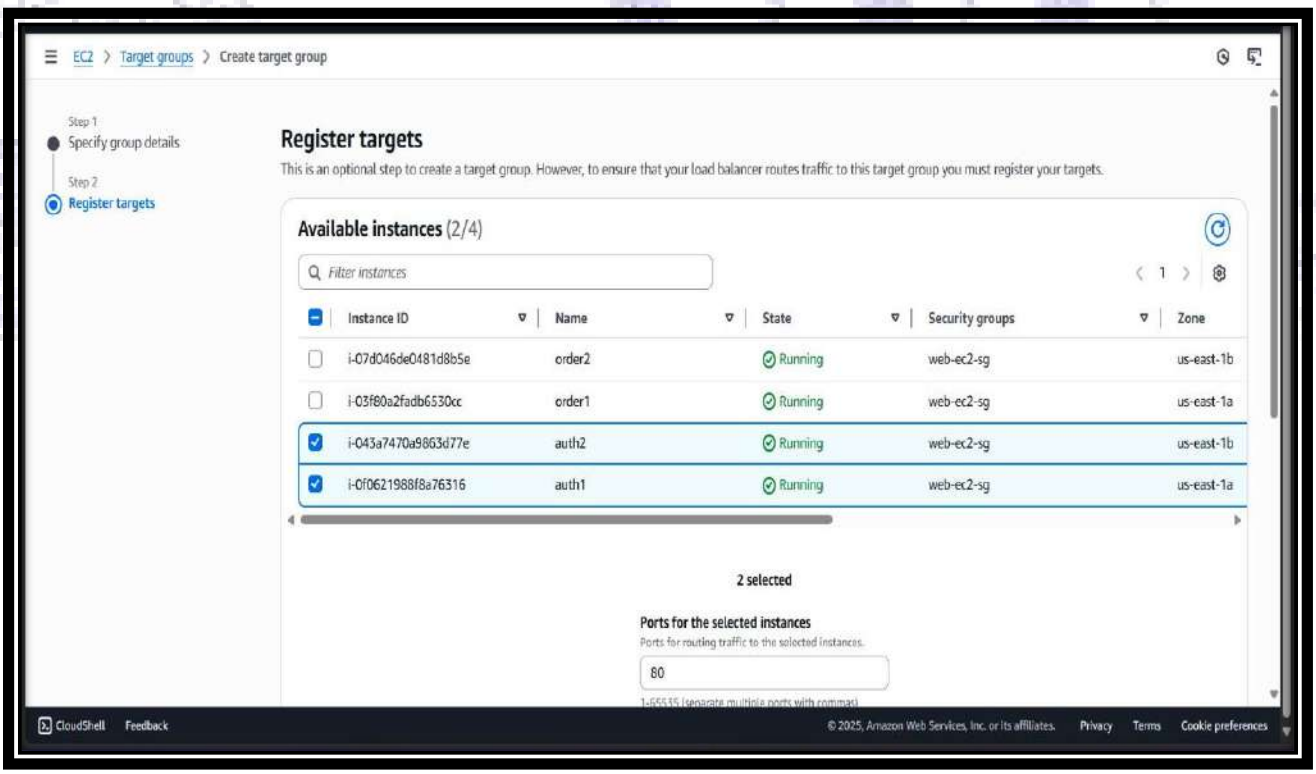
○ IPv6

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-08c384ed05d3335ff (default)
172.31.0.0/16



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 |
|---|---|---|---|---|---|
| ☐ | i-07d046de0481d8b5e | order2 | Running | web-ec2-sg | us-east-1b |
| ☐ | i-03f80a2fadb6530cc | order1 | Running | web-ec2-sg | us-east-1a |
| ☑ | i-043a7470a9863d77e | auth2 | Running | web-ec2-sg | us-east-1b |
| ☑ | i-0f0621988f8a76316 | auth1 | Running | web-ec2-sg | us-east-1a |

2 selected

**Ports for the selected instances**

Ports for routing traffic to the selected instances.

80

1-65535 (separate multiple ports with commas)

## Step 5: Create Application Load Balancer (ALB) and Configure Path-Based Routing

Create **1 ALB per region** and set up path-based listener rules.

1. Go to **EC2 → Load Balancers → Create Load Balancer → Application Load Balancer**.
2. **Basic configuration**:
   - Name: alb-web-ap-south-1 (for Mumbai region; adjust name per region).
   - Scheme: Internet-facing.
   - IP address type: IPv4.
3. **Listeners**:
   - Add HTTP : 80 (optionally add HTTPS : 443 later if certificates are available).
4. **Availability Zones**:
   - VPC: Default (or your VPC).
   - Select at least **2 subnets** (one per AZ) so ALB spans multiple AZs.
5. **Security group**: Select **alb-sg**.
6. **Configure routing**:
   - Default target group: Select tg-auth (or create a tg-default if you prefer a dummy).
7. Click **Create load balancer** and wait until it is provisioned.

---

### A. Configure Listener Rules (Path-Based Routing)

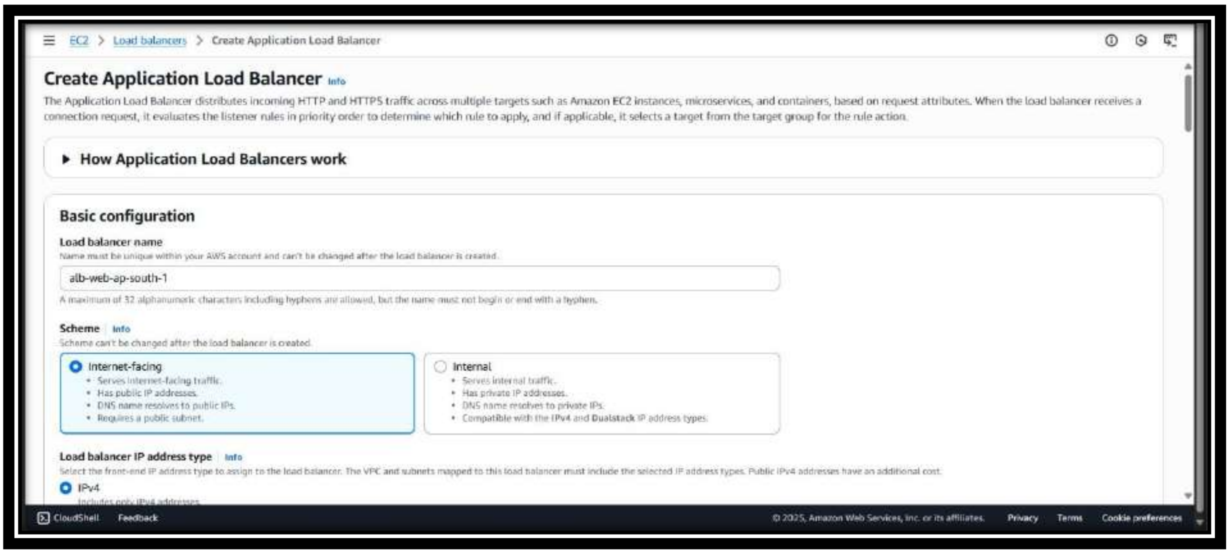
1. In the **Load Balancers list**, select **alb-web-ap-south-1** → go to **Listeners** tab → choose **HTTP:80** listener → click **View/edit rules**.
2. Add rules before the default:
   - Rule 1:
     - Condition: Path is /auth*
     - Action: Forward to **tg-auth**
   - Rule 2:
     - Condition: Path is /order*
     - Action: Forward to **tg-order**
3. Save rules. Ensure the **default rule** points to some target group (e.g., tg-auth or tg-default) or returns 404.

---

### B. Verify ALB and Target Health

1. Go to **Load Balancers → select ALB → Target groups tab**.
2. Select tg-auth → **Targets** → confirm targets (auth-1, auth-2) show as **healthy**.
3. Repeat for tg-order.

4. If unhealthy, check the EC2 instance **user-data** and confirm the /health endpoint works.



EC2 > Load balancers > Create Application Load Balancer

## Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request attributes. When the load balancer receives a connection request, it 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.

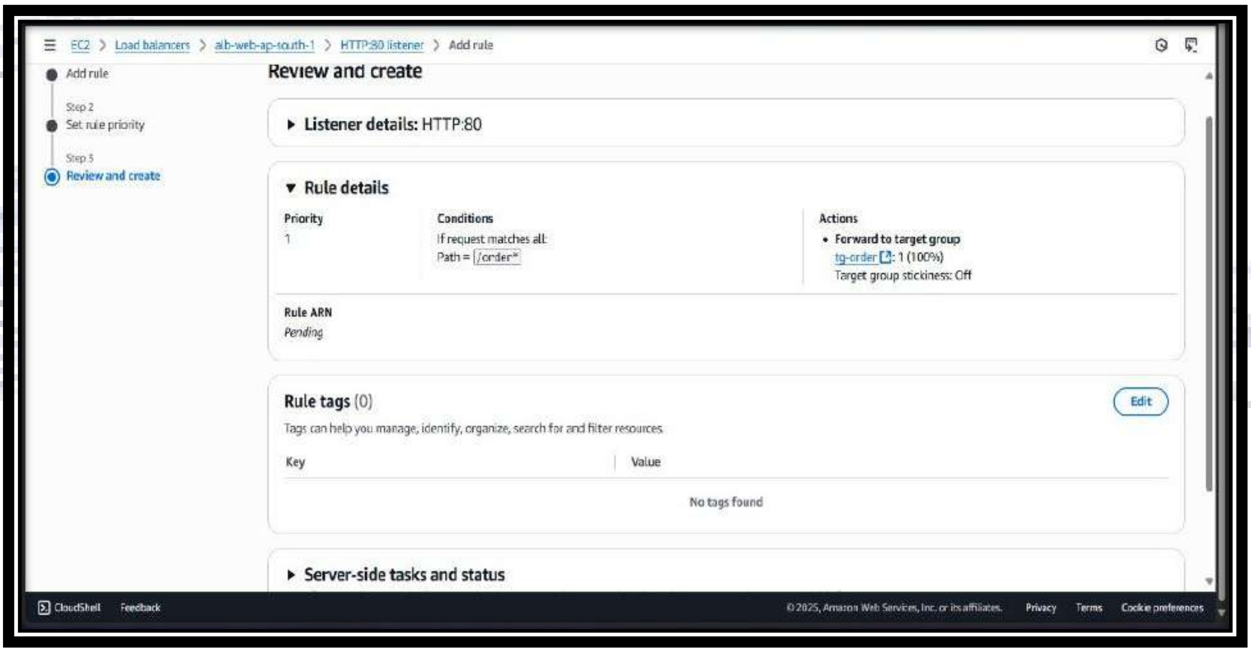
○ Internal
- Serves internal traffic.
- Has private IP addresses.
- DNS name resolves to private IPs.
- Compatible with the **IPv4** and **Dualstack** IP address types.

**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.



EC2 > Load balancers > alb-web-ap-south-1 > HTTP:80 listener > Add rule

## Review and create

▸ Listener details: HTTP:80

▾ Rule details

| Priority | Conditions | Actions |
|---|---|---|
| 1 | If request matches all:<br>Path = /order* | • Forward to target group<br>tg-order: 1 (100%)<br>Target group stickiness: Off |

Rule ARN

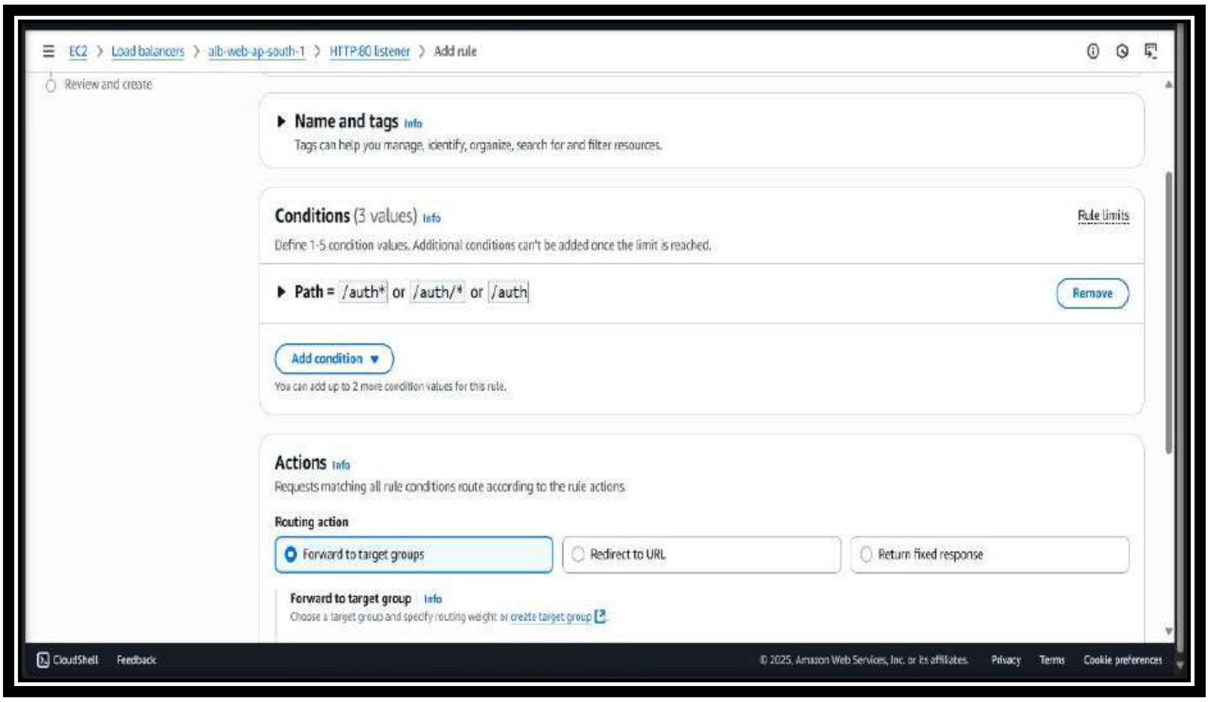
*Pending*

Rule tags (0)

Tags can help you manage, identify, organize, search for and filter resources.

| Key | Value |
|---|---|
| No tags found | |

▸ Server-side tasks and status



☰ EC2 > Load balancers > alb-web-ap-south-1 > HTTP:80 listener > Add rule

▸ Name and tags Info

Tags can help you manage, identify, organize, search for and filter resources.

Conditions (3 values) Info

Define 1-5 condition values. Additional conditions can't be added once the limit is reached.

▸ Path = /auth* or /auth/* or /auth

You can add up to 2 more condition values for this rule.

Actions Info

Requests matching all rule conditions route according to the rule actions.

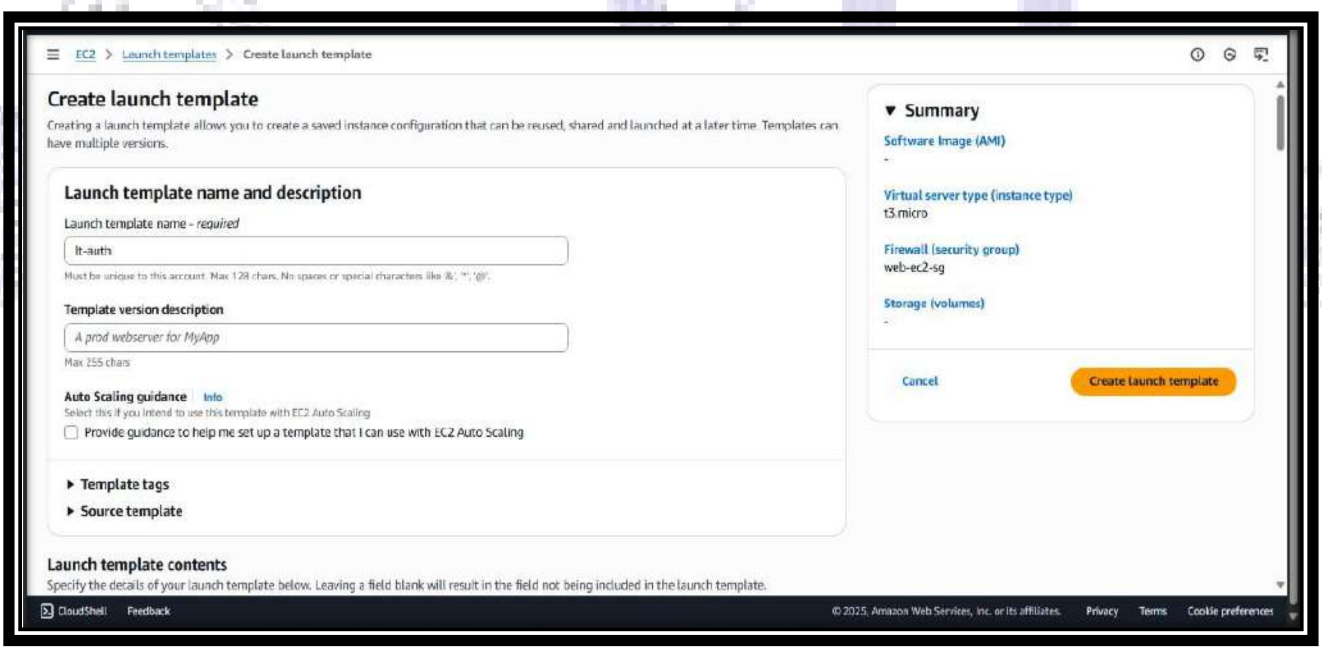
Routing action

● 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

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



☰ EC2 > Launch templates > Create launch template

Create launch template

Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched at a later time. Templates can have multiple versions.

Launch template name and description

Launch template name - *required*

lt-auth

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)

-

Virtual server type (instance type)

t3.micro

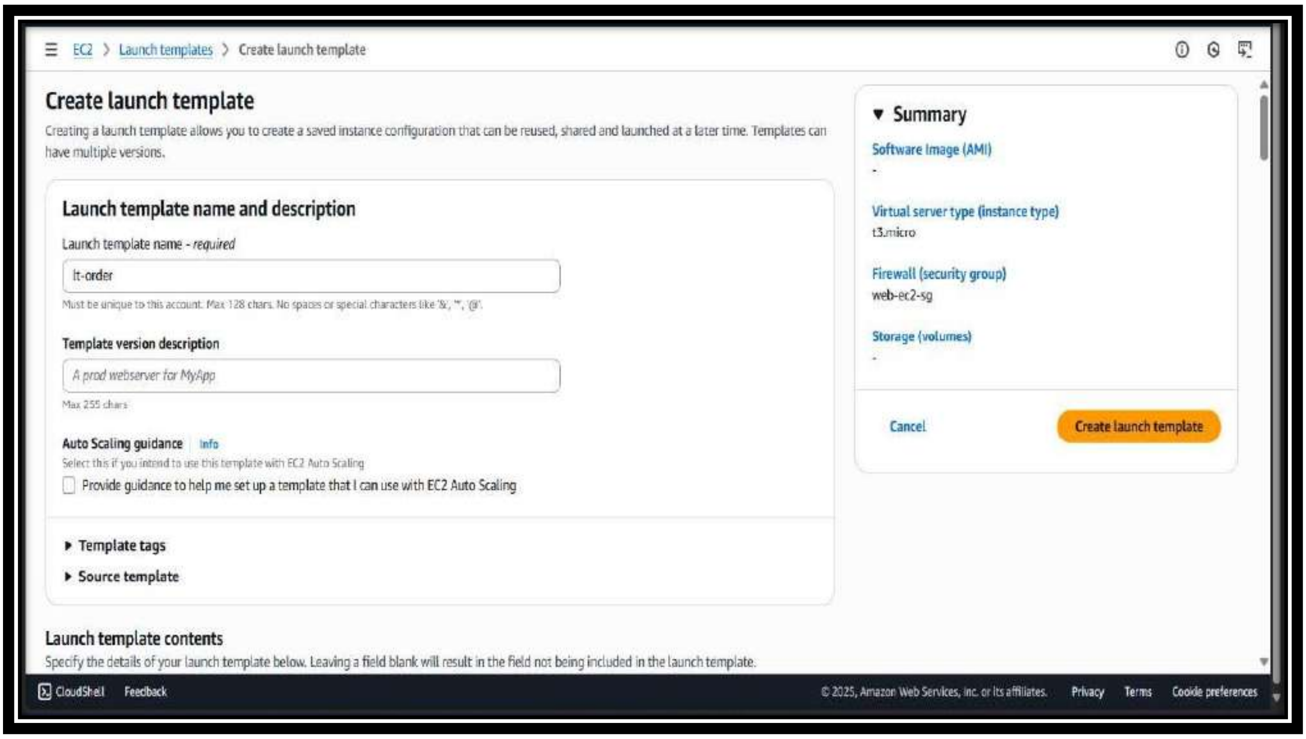
Firewall (security group)

web-ec2-sg

Storage (volumes)

-

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



EC2 > Launch templates > Create launch template

Create launch template

Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched at a later time. 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)
-

Virtual server type (instance type)
t3.micro

Firewall (security group)
web-ec2-sg

Storage (volumes)
-

## Step 6: Configure Auto Scaling (per region, per service) — GUI Only

We'll create **Launch Templates** and **Auto Scaling Groups (ASGs)** for each service. The ASGs will attach to the ALB target groups and automatically register/deregister instances.

---

### A. Create Launch Templates

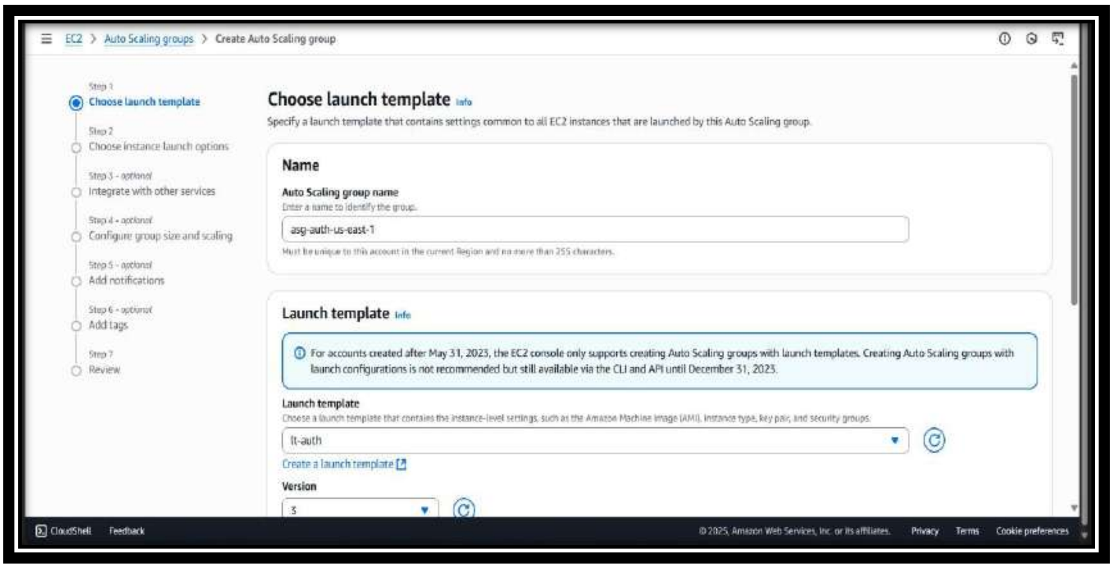
1. Go to **EC2 → Launch Templates → Create launch template**.
2. Configure:
   - **Name**: lt-auth (for the auth service).
   - **AMI**: Amazon Linux 2.
   - **Instance type**: t3.micro.
   - **Key pair**: Same as used earlier.
   - **Network settings**: Leave blank (ASG will assign subnets).
   - **Security group**: web-ec2-sg.
   - **Advanced user data**: Use the same startup script from the manual auth instances (so they serve /health).
3. Click **Create launch template**.
4. Repeat to create **lt-order** (with the order service user-data).

---

### B. Create Auto Scaling Groups

1. Go to **EC2 → Auto Scaling Groups → Create Auto Scaling group**.

2. Select the **launch template** (lt-auth).
3. **ASG name**: asg-auth-ap-south-1.



Choose launch template

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-us-east-1

Must be unique to this account in the current Region and no more than 255 characters.

Launch template

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

Version

3

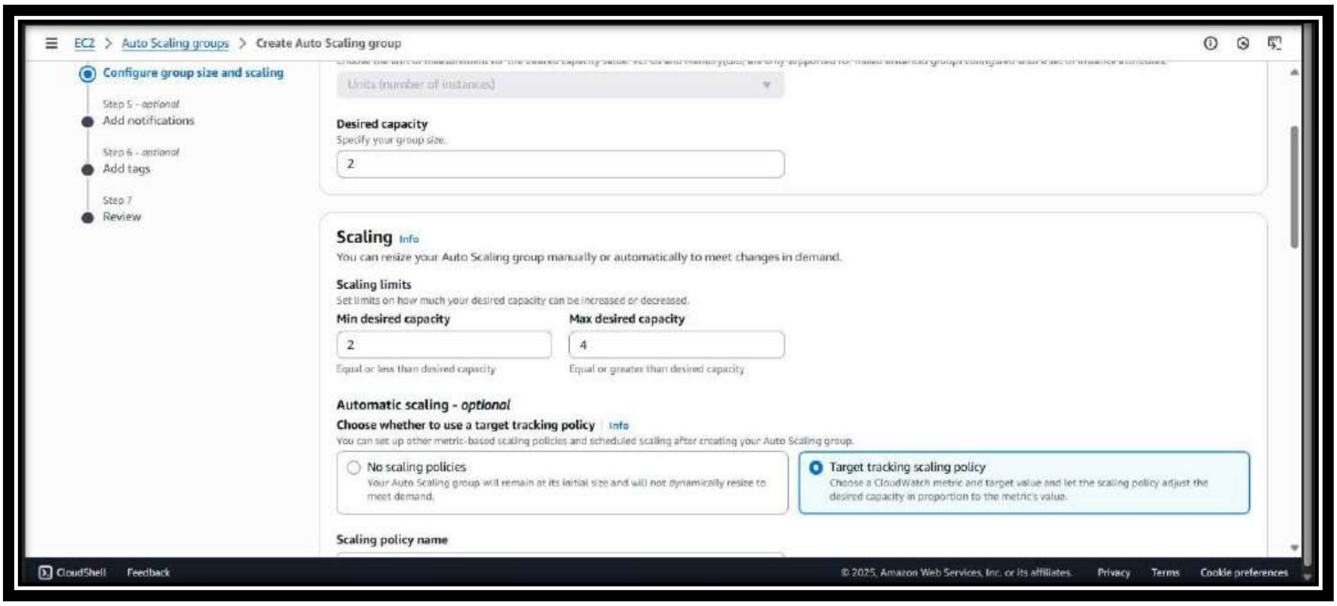
© 2025, Amazon Web Services, Inc. or its affiliates.

4. Select **VPC** and choose **two subnets** (AZ1 + AZ2).
5. **Attach to load balancer**:
   - Choose **Attach to an existing load balancer** → select **alb-web-ap-south-1**.
   - Target group: **tg-auth**.
6. **Set group size**:
   - Minimum: 2
   - Desired: 2
   - Maximum: 4
7. **Scaling policies**:
   - Choose **Target tracking** (e.g., Average CPU utilization target = 50%).
   - Or use **ALB request count per target** (e.g., 50 requests per instance).
8. Review and click **Create Auto Scaling group**.
9. Repeat the same process to create **asg-order-ap-south-1** using **lt-order** and attach to **tg-order**.

---

## C. Verify Auto Scaling

1. Go to **Auto Scaling Groups → select an ASG → Instances tab**.
2. Confirm new EC2 instances are launched automatically (names generated by ASG).
3. Verify these instances appear as **healthy** in their associated target groups.



EC2 > Auto Scaling groups > Create Auto Scaling group
Configure group size and scaling
Step 5 - optional
Add notifications
Step 6 - optional
Add tags
Step 7
Review
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Units (number of instances)

**Desired capacity**
Specify your group size.
2

**Scaling** Info
You can resize your Auto Scaling group manually or automatically to meet changes in demand.

**Scaling limits**
Set limits on how much your desired capacity can be increased or decreased.

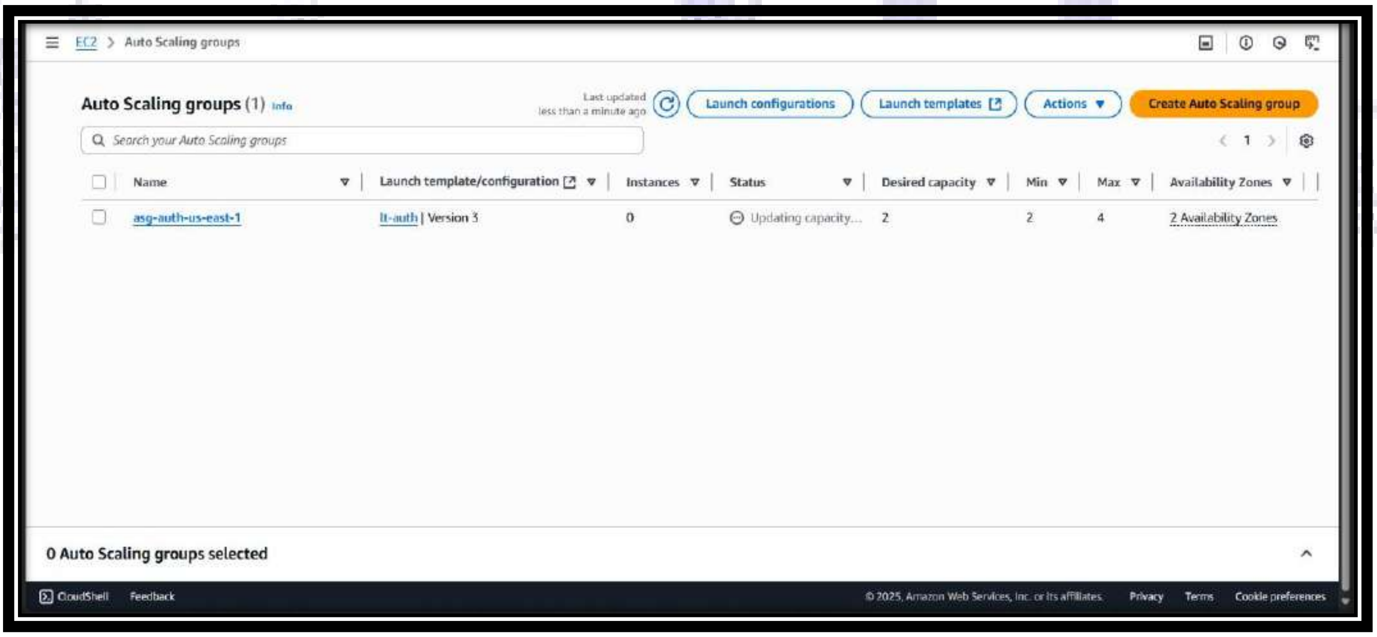
| Min desired capacity | Max desired capacity |
|---|---|
| 2 | 4 |
| Equal or less than desired capacity | Equal or greater than desired capacity |

**Automatic scaling - *optional***
**Choose whether to use a target tracking policy** Info
You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

○ No scaling policies
Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

● Target tracking scaling policy
Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.

**Scaling policy name**



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 |
|---|---|---|---|---|---|---|---|---|
| □ | asg-auth-us-east-1 | lt-auth \| Version 3 | 0 | Updating capacity... | 2 | 2 | 4 | 2 Availability Zones |

0 Auto Scaling groups selected

## Step 7: Configure Route 53 for Global DNS (Latency-Based Routing)

Integrate the regional ALBs with **Route 53** so users are routed to the nearest healthy ALB/region.

---

## A. Create or Use a Hosted Zone

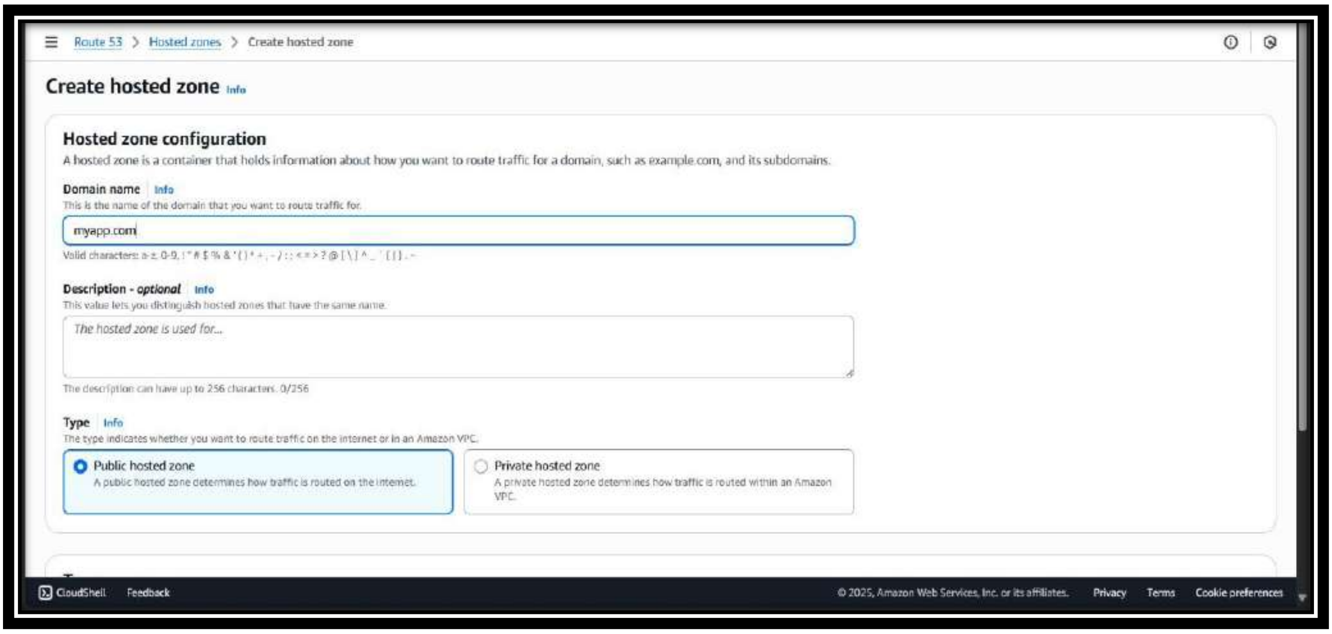
1. Go to **Route 53 → Hosted zones → Create hosted zone** (skip if you already have one).
2. Enter:
   - **Domain name**: yourdomain.com
   - **Type**: Public hosted zone
3. Click **Create hosted zone**.

   📷 Screenshot: Hosted zone created (e.g., 16-hosted-zone.png).

---

## B. Create Latency Records for ALBs

1. Inside the hosted zone, click **Create record**.
2. **Record name**: www (or @ for root domain).
3. **Routing policy**: **Latency**.
4. First record → **ap-south-1 ALB**:
   - Alias → **Application and Classic Load Balancer**
   - Region: **Asia Pacific (Mumbai)**
   - Select **alb-web-ap-south-1** from dropdown
   - **Evaluate target health**: Yes
   - Save record.
5. Second record → **us-east-1 ALB**:
   - Same record name: www
   - Routing policy: **Latency**
   - Alias → **ALB in US East (N. Virginia)**
   - Select **alb-web-us-east-1**
   - **Evaluate target health**: Yes
   - Save record.



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.

myapp.com

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

Description - *optional* Info

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

*The hosted zone is used for...*

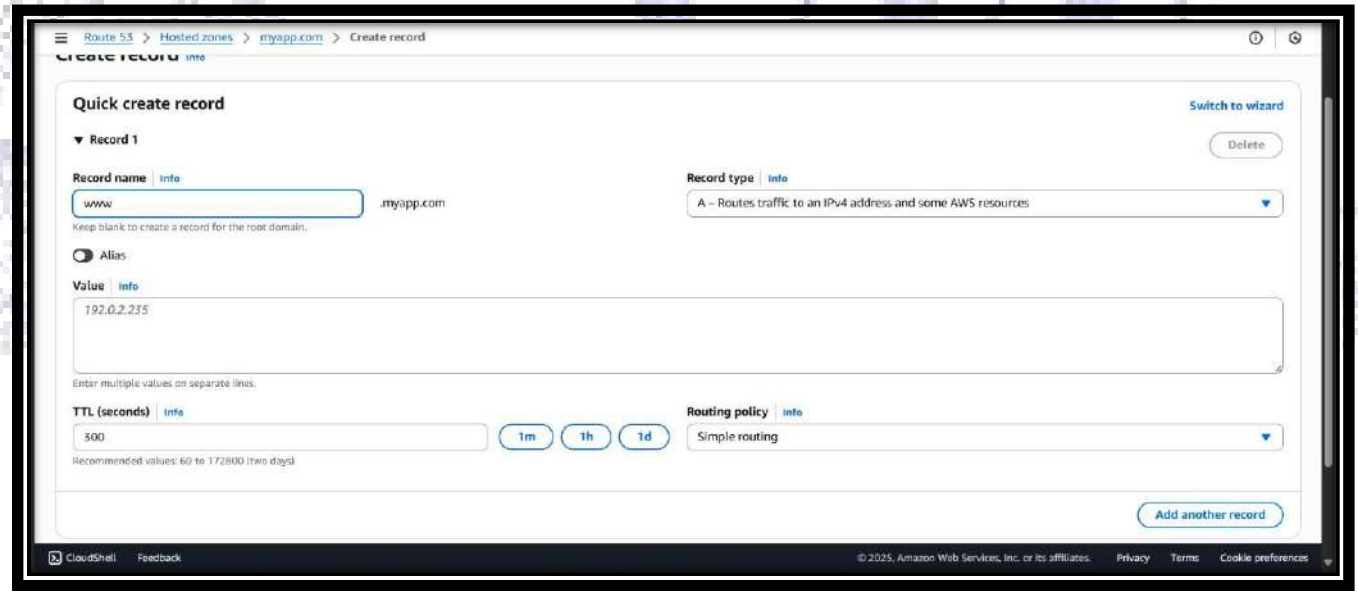
The description can have up to 256 characters. 0/256

Type Info

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

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

○ Private hosted zone
A private hosted zone determines how traffic is routed within an Amazon VPC.



Route 53 > Hosted zones > myapp.com > Create record

Create record Info

Quick create record

Switch to wizard

▼ Record 1

Delete

Record name Info

www .myapp.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

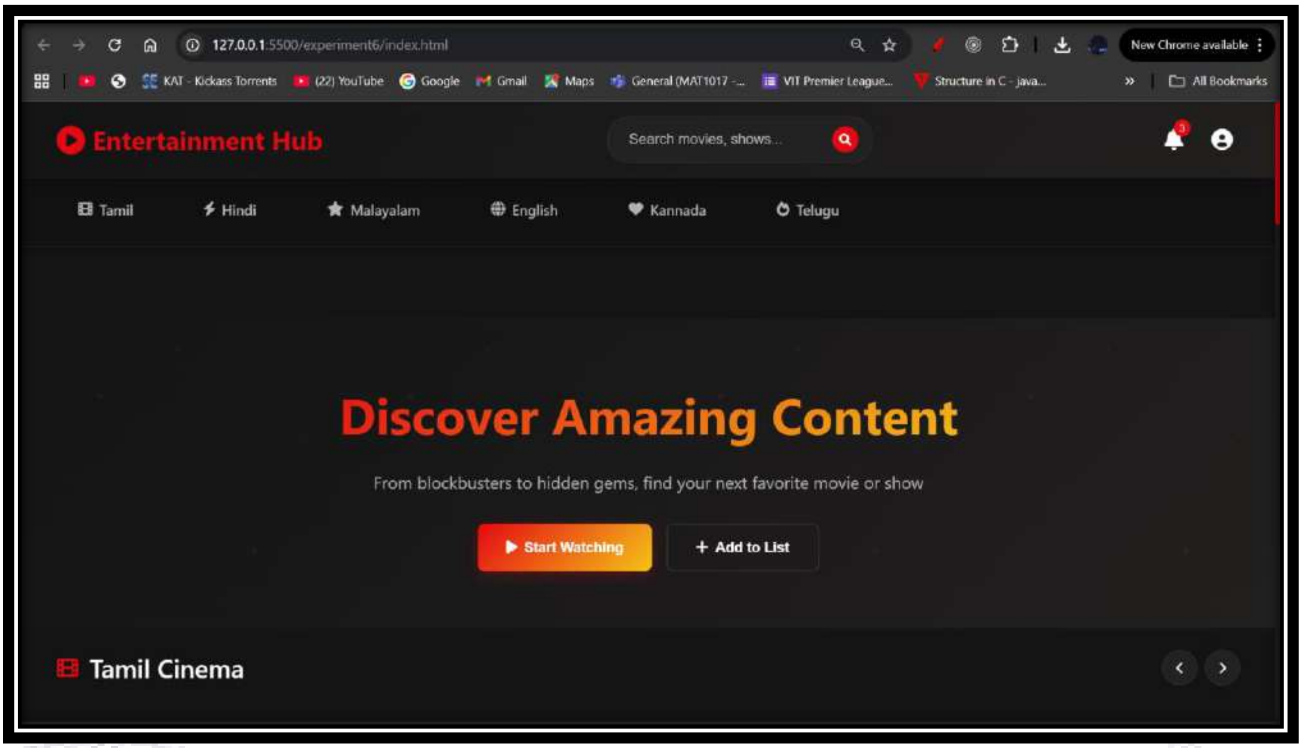
Recommended values: 60 to 172800 (two days)

Routing policy Info

Simple routing

Add another record

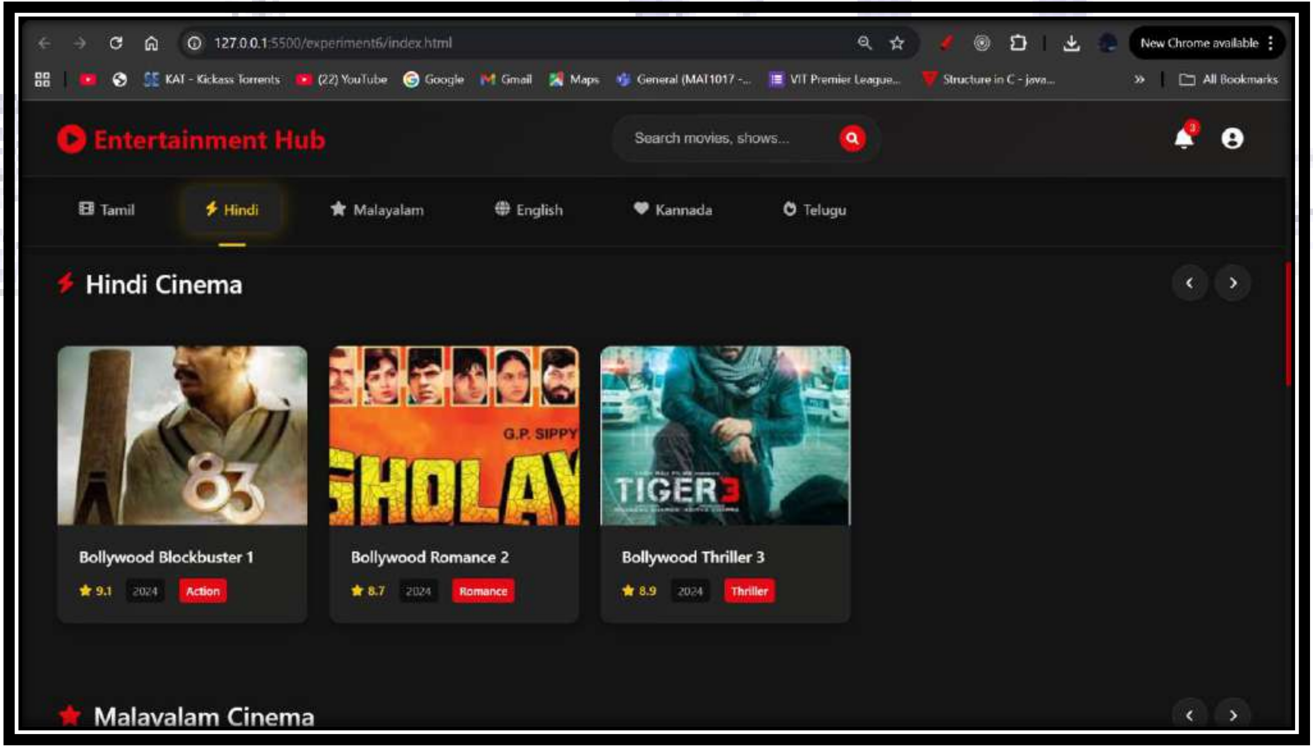
# LIVE WEBSITE



Discover Amazing Content

From blockbusters to hidden gems, find your next favorite movie or show

Tamil Cinema



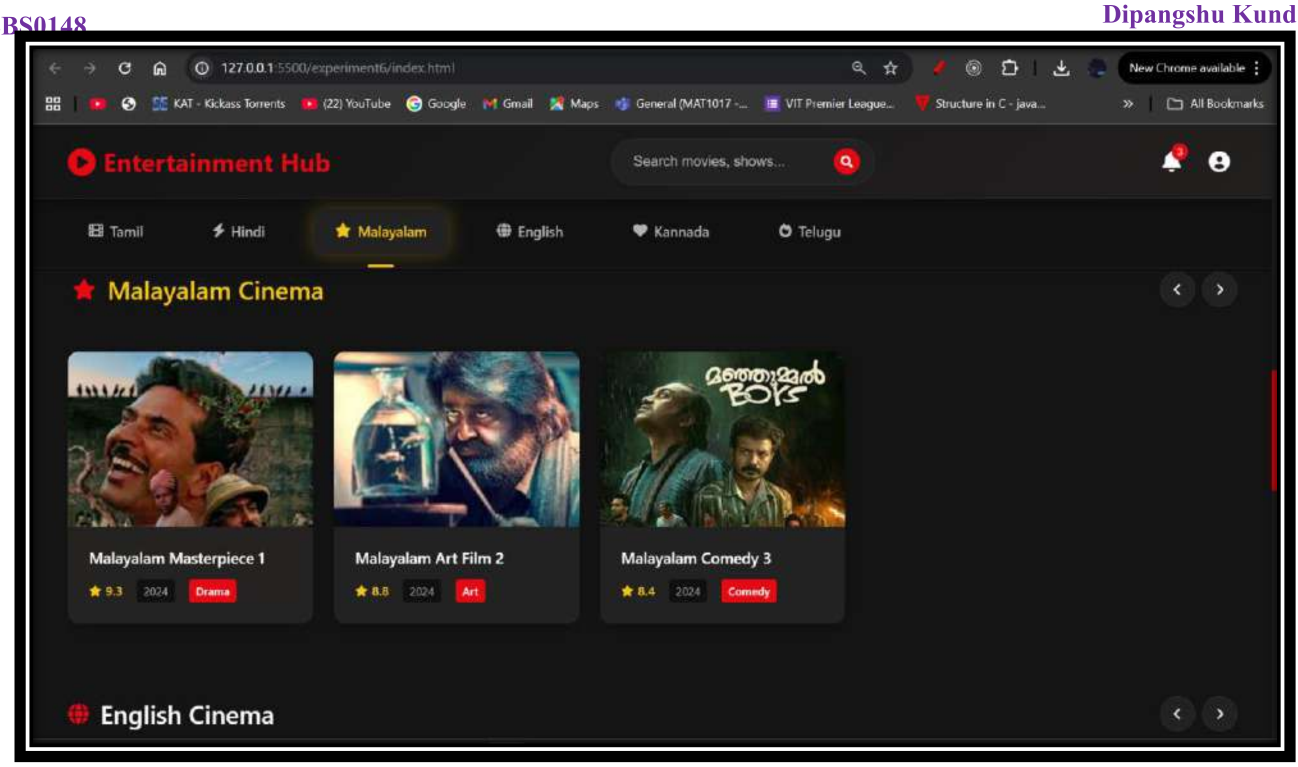
Hindi Cinema

Bollywood Blockbuster 1
★ 9.1 2024 Action

Bollywood Romance 2
★ 8.7 2024 Romance

Bollywood Thriller 3
★ 8.9 2024 Thriller

Malayalam Cinema



127.0.0.1:5500/experiment6/index.html

# Entertainment Hub

Search movies, shows...

Tamil | Hindi | Malayalam | English | Kannada | Telugu

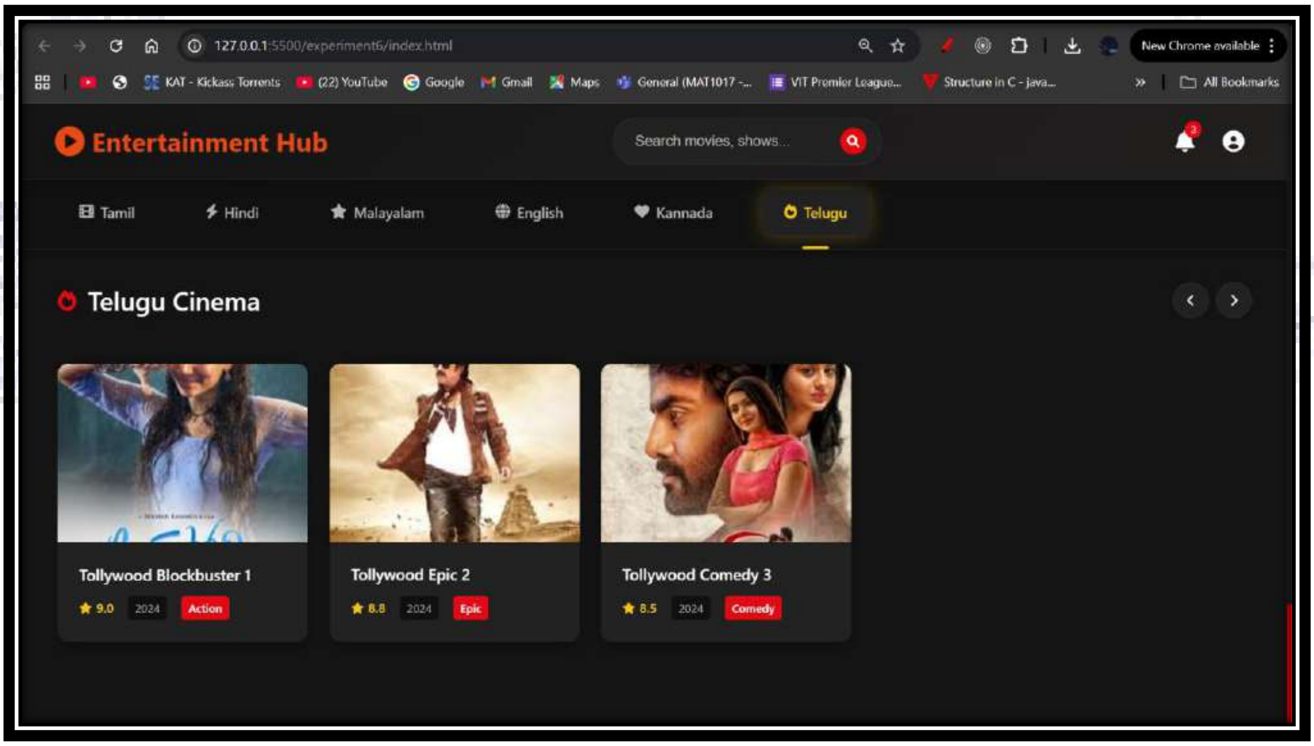
## Malayalam Cinema

Malayalam Masterpiece 1 — 9.3 · 2024 · Drama

Malayalam Art Film 2 — 8.8 · 2024 · Art

Malayalam Comedy 3 — 8.4 · 2024 · Comedy

## English Cinema



127.0.0.1:5500/experiment6/index.html

# Entertainment Hub

Search movies, shows...

Tamil | Hindi | Malayalam | English | Kannada | Telugu

## Telugu Cinema

Tollywood Blockbuster 1 — 9.0 · 2024 · Action

Tollywood Epic 2 — 8.8 · 2024 · Epic

Tollywood Comedy 3 — 8.5 · 2024 · Comedy