

Deploy a secure, highly available, and scalable website.

High-availability

High-availability infrastructure is configured to deliver quality performance and handle different loads and failures with minimal or zero downtime.

Scalable

The ability to increase or decrease IT resources as needed to meet changing demand.

Step 1: Create a Security Group.

- Login into the AWS Console using the login credentials.
- Create a security group.
- Give an appropriate name, and description to that security group. Also, select the VPC.

The screenshot shows the 'Create security group' interface in the AWS EC2 console. At the top, there's a navigation bar with tabs for IAM, EC2, VPC, S3, and RDS. Below the navigation is a breadcrumb trail: EC2 > Security Groups > Create security group. The main area has a title 'Create security group' with an 'Info' link. A sub-instruction says: '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.' There are two main sections: 'Basic details' and 'Inbound rules'. Under 'Basic details', there are fields for 'Security group name' (containing 'my-created-sg') and 'Description' (containing 'Allow SSH,HTTP,HTTPS'). Under 'VPC info', a dropdown menu shows 'vpc-03154aac2524417ec'. Under 'Inbound rules', it says 'This security group has no inbound rules.' At the bottom, there are buttons for 'Add rule', 'CloudShell', and 'Feedback', along with copyright and legal links.

- Add SSH, HTTP, and HTTPS in the inbound rules.

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
SSH	TCP	22	Anywhere ▼	<input type="text"/> 0.0.0.0/0 X
HTTP	TCP	80	Anywhere ▼	<input type="text"/> 0.0.0.0/0 X
HTTPS	TCP	443	Anywhere ▼	<input type="text"/> 0.0.0.0/0 X

[Add rule](#)

Outbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info
All traffic	All	All	Custom ▼	<input type="text"/> 0.0.0.0/0 X

- The security group is created successfully.

Details

Security group name	Security group ID	Description
my-created-sg	sg-0c0847377c533b7b2	Allow SSH,HTTP,HTTPS
Owner	Inbound rules count	VPC ID
471112584668	3 Permission entries	vpc-03154aac2524417ec Edit
Outbound rules count	1 Permission entry	

Inbound rules | Outbound rules | Tags

Inbound rules (3)

<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range
<input type="checkbox"/>	-	sgr-0e21907edd9ac6...	IPv4	HTTPS	TCP	443
<input type="checkbox"/>	-	sgr-06bbdb943cebd00e	IPv4	HTTP	TCP	80
<input type="checkbox"/>	-	sgr-020dc74ea590d4d1f	IPv4	SSH	TCP	22

Step 2: Launch Templates

- Launch three EC2 Templates.

EC2 launch templates
Streamline, simplify and standardize instance launches

Use launch templates to automate instance launches, simplify permission policies, and enforce best practices across your organization. Save launch parameters in a template that can be used for on-demand launches and with managed services, including EC2 Auto Scaling and EC2 Fleet. Easily update your launch parameters by creating a new launch template version.

New launch template

Create launch template

Benefits and features

Streamline provisioning
Minimize steps to provision instances. With EC2 Auto Scaling, updates to a launch template can be automatically applied.

Simplify permissions
Create shorter, easier to manage IAM policies. [Learn more](#)

Documentation

[Documentation](#) [API reference](#)

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- Create a launch template, and give a name to that 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

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

Template version description

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

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 2023.5.2...[read more](#)
ami-06c68f701db090592

Virtual server type (instance type)
t2.micro

Firewall (security group)
my-created-sg

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

Create launch template

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- Likewise, Create three templates

- Mobile, Laptop, and Home these are the three different templates for different web pages.

The screenshot shows the AWS EC2 Launch Templates page. On the left, there's a navigation sidebar with links like EC2 Dashboard, EC2 Global View, Events, and Launch Templates. The main area displays a table titled "Launch Templates (3) Info" with columns for Launch Template ID, Launch Template Name, Default Version, Latest Version, Create Time, and Created By. The three entries are:

Launch Template ID	Launch Template Name	Default Version	Latest Version	Create Time	Created By
lt-0102c2575bc28b1b4	Mobile	1	1	2024-07-04T04:49:53.000Z	arn:aws:iam:....
lt-03fb0e5392ee6c28d	Laptop	1	1	2024-07-04T04:44:11.000Z	arn:aws:iam:....
lt-06fbaae080939ca6	Home	1	1	2024-07-04T04:47:04.000Z	arn:aws:iam:....

Below the table, a modal window titled "Select a launch template" is open, showing the same three options.

Step 3: Create three Auto Scaling Group

- Search auto-scaling in the search box.

The screenshot shows the AWS EC2 Auto Scaling Groups page. On the left, there's a navigation sidebar with links like AMIs, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. The main area features a large banner with the text "Amazon EC2 Auto Scaling helps maintain the availability of your applications". Below the banner, there's a section titled "How it works" with a diagram showing four squares representing EC2 instances within an "Auto Scaling group". To the right, there are sections for "Pricing" and "Getting started". A prominent orange button labeled "Create Auto Scaling group" is located in the center-right area.

- Give a name to the auto-scaling group and choose the launch template.

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.
Laptop-ASG

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.

Laptop [▼](#) [Create a launch template](#) [C](#)

Version

- Check the Instance type requirements.

Choose instance launch options

Instance type requirements [Info](#) [Override launch template](#)

You can keep the same instance attributes or instance type from your launch template, or you can choose to override the launch template by specifying different instance attributes or manually adding instance types.

Launch template	Version	Description
Laptop ▼	Default	Template for Laptop

Instance type
t2.micro

Network [Info](#)

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC
Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-03154aac2524417cc [▼](#) [C](#)

Create a VPC [C](#)

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 [▼](#) [C](#)

- Select the Availability zones

Step 6 - optional
Add tags

Step 7
Review

Network Info

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC

Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-0315aac2524417ec
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

us-east-1a | subnet-0e91013ba56de1700 X
172.31.16.0/20 Default

us-east-1b | subnet-084b34959e98f67fa X
172.31.32.0/20 Default

us-east-1c | subnet-0c4ace3be3b1266bf X
172.31.0.0/20 Default

us-east-1d | subnet-05c7cb924207d162a X
172.31.80.0/20 Default

us-east-1e | subnet-087d94938c5d06932 X
172.31.48.0/20 Default

us-east-1f | subnet-0a30c0ae0fbccda18 X

- Select No load balancer, as we haven't yet created a load balancer

Step 3 - optional
Configure advanced options

Step 4 - optional
Configure group size and scaling

Step 5 - optional
Add notifications

Step 6 - optional
Add tags

Step 7
Review

Load balancing Info

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

No load balancer
Traffic to your Auto Scaling group will not be fronted by a load balancer.

Attach to an existing load balancer
Choose from your existing load balancers.

Attach to a new load balancer
Quickly create a basic load balancer to attach to your Auto Scaling group.

VPC Lattice integration options Info

To improve networking capabilities and scalability, integrate your Auto Scaling group with VPC Lattice. VPC Lattice facilitates communications between AWS services and helps you connect and manage your applications across compute services in AWS.

Select VPC Lattice service to attach

No VPC Lattice service
VPC Lattice will not manage your Auto Scaling group's network access and connectivity with other services.

Attach to VPC Lattice service
Incoming requests associated with specified VPC Lattice target groups will be routed to your Auto Scaling group.

Create new VPC Lattice service

Health checks

Health checks increase availability by replacing unhealthy instances. When you use multiple health checks, all are evaluated, and if at least one fails, instance replacement occurs.

- Configure group size and scaling

- Give the desired capacity(min.desired and max.desired)

Configure group size and scaling - *optional* [Info](#)

Define your group's desired capacity and scaling limits. You can optionally add automatic scaling to adjust the size of your group.

Group size [Info](#)

Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.

Desired capacity type

Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.

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	2

- Choose instance maintenance policy.

Instance maintenance policy [Info](#)

Control your Auto Scaling group's availability during instance replacement events. This includes health checks, instance refreshes, maximum instance lifetime features and events that happen automatically to keep your group balanced, called rebalancing events.

Choose a replacement behavior depending on your availability requirements

Mixed behavior	Prioritize availability	Control costs	Flexible
<input checked="" type="radio"/> No policy For rebalancing events, new instances will launch before terminating others. For all other events, instances terminate and launch at the same time.	<input type="radio"/> Launch before terminating Launch new instances and wait for them to be ready before terminating others. This allows you to go above your desired capacity by a given percentage and may temporarily increase costs.	<input type="radio"/> Terminate and launch Terminate and launch instances at the same time. This allows you to go below your desired capacity by a given percentage and may temporarily reduce availability.	<input type="radio"/> Custom behavior Set custom values for the minimum and maximum amount of available capacity. This gives you greater flexibility in setting how below and over your desired capacity EC2 Auto Scaling goes when replacing instances.

Instance scale-in protection

Scale-in protection prevents newly launched instances from being terminated by scaling activities. Make sure to remove scale-in protection for the group or individual instances when instances are ready to be terminated.

Enable instance scale-in protection

Cancel [Skip to review](#) [Previous](#) [Next](#)

- Create the same configuration of the auto-scaling group for home and mobile templates

The screenshot shows the AWS EC2 Auto Scaling groups page. At the top, there are navigation links for IAM, EC2, VPC, S3, and RDS. The main heading is "Auto Scaling groups (3) Info". Below this is a search bar and a table with columns: Name, Launch template/configuration, Instances, Status, Desired capacity, Min, Max, and Availability zone. The table lists three groups: "Mobile-ASG" (Mobile | Version Default, 0 instances, Updating capacity..., 2 desired, 2 min, 2 max, us-east-1a, ...), "Home-ASG" (Home | Version Default, 2 instances, -, 2 desired, 2 min, 2 max, us-east-1a, ...), and "Laptop-ASG" (Laptop | Version Default, 2 instances, -, 2 desired, 2 min, 2 max, us-east-1a, ...). A message at the bottom left says "0 Auto Scaling groups selected". The footer includes links for CloudShell, Feedback, and copyright information: "© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".

Step 4: Create target group

- Create three different target group.

The screenshot shows the AWS EC2 Target groups page. On the left, a sidebar menu includes "Elastic Block Store" (Volumes, Snapshots, Lifecycle Manager), "Network & Security" (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), "Load Balancing" (Load Balancers, Target Groups, Trust Stores New), and "Auto Scaling" (Auto Scaling Groups, Settings). The main heading is "Target groups Info". Below it is a search bar and a table with columns: Name, ARN, Port, Protocol, Target type, and Load balancer. A message in the center says "No target groups" and "You don't have any target groups in us-east-1". A "Create target group" button is at the bottom. A message at the bottom left says "0 target groups selected". The footer includes links for CloudShell, Feedback, and copyright information: "© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".

- Specific group details, Choose the target type.

The screenshot shows the 'Specify group details' step of a wizard. The left sidebar has two steps: 'Step 1: Specify group details' (selected) and 'Step 2: Register targets'. The main area is titled 'Basic configuration' with a note: 'Settings in this section can't be changed after the target group is created.' It asks to 'Choose a target type' with four options: 'Instances' (selected), 'IP addresses', 'Lambda function', and 'Application Load Balancer'. The 'Instances' section includes a bulleted list: 'Supports load balancing to instances within a specific VPC.', 'Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.'

- Give a name for the target group.

The screenshot shows the 'Create target group' page. The 'Target group name' field is filled with 'Home-TG'. Below it, a note says: 'A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.' The 'Protocol : Port' section shows 'HTTP' selected as the protocol and '80' as the port. The 'IP address type' section shows 'IPv4' selected. The 'VPC' section lists a single VPC entry: 'vpc-03154aac2524417ec IPv4 VPC CIDR: 172.31.0.0/16'. The 'Protocol version' section shows 'HTTP1' selected. The bottom of the page includes standard AWS footer links: CloudShell, Feedback, © 2024, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

- Give the health check path

Health checks

The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol: HTTP

Health check path: /home

Up to 1024 characters allowed.

► Advanced health check settings

Attributes

Certain default attributes will be applied to your target group. You can view and edit them after creating the target group.

► Tags - optional

Consider adding tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.

- And create all three target groups.

Target groups (3) info

Name	ARN	Port	Protocol	Target type	Load balancer
Mobile-TG	arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/Mobile-TG/5555555555555555	80	HTTP	Instance	None associated
Laptop-TG	arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/Laptop-TG/5555555555555555	80	HTTP	Instance	None associated
Home-TG	arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/Home-TG/5555555555555555	80	HTTP	Instance	None associated

0 target groups selected

Select a target group above.

Step 5: Attach target group to the Auto-scaling group

- Go to the auto-scaling group and on a particular group.
- Scroll down and in the load balancer click on edit.
- Select the Application Load balancer
- Now, select the target group that you want to attach the auto-scaling group.
- Likewise, attach all three target groups to the auto-scaling group.

The screenshot shows the AWS Management Console with the EC2 service selected. On the left, the navigation sidebar includes options like Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. The main content area is titled 'Edit Mobile-ASG' and shows the 'Load balancing - optional' configuration. Under 'Load balancers', there is a dropdown menu labeled 'Select target groups' which has 'Mobile-TG | HTTP' selected. A note below the dropdown states: 'One of your target groups is not yet associated with any load balancer. In order for routing and scaling to occur, you will need to attach the target group to a load balancer. This can be done later in the [Load Balancing console](#).
Mobile-TG | HTTP
Load balancer: Not associated with any load balancer'.

Step 6 :Create a Load Balancer

- Select the load balancer from sidebar.

The screenshot shows the AWS Management Console with the EC2 service selected. Under the 'Load Balancing' section, the 'Load Balancers' tab is active. The main area displays a table with the heading 'Load balancers'. A message at the top right says 'No load balancers' and 'You don't have any load balancers in us-east-1'. Below this, a message says '0 load balancers selected' and 'Select a load balancer above.' At the bottom right of the table area is a large orange button labeled 'Create load balancer'.

- Choose a load Balancer type(Application Load Balancer)

The screenshot shows the 'Compare and select load balancer type' page. It features three cards: 'Application Load Balancer Info' (ALB), 'Network Load Balancer Info' (NLB), and 'Gateway Load Balancer Info' (GWLB). Each card includes a diagram and a brief description of its use case.

Load balancer types		
Application Load Balancer Info	Network Load Balancer Info	Gateway Load Balancer Info
<p>Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operation at the request level.</p>	<p>Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and GENEVE.</p>	<p>Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable</p>

- In, Basic Configuration, give a name to the load balancer.

Basic configuration

Load balancer name
Name must be unique within your AWS account and can't be changed after the load balancer is created.
ASG-ELB-Webpage

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
An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. [Learn more](#)

Internal
An internal load balancer routes requests from clients to targets using private IP addresses. Compatible with the IPv4 and Dualstack IP address types.

Load balancer IP address type [Info](#)
Select the type of IP addresses that your subnets use. 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.

Network mapping [Info](#)
The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- Select the availability zones in the Network.

Network mapping [Info](#)
The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC [Info](#)
Select the virtual private cloud (VPC) for your targets or you can [create a new VPC](#). Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

vpc-03154aac2524417ec
IPv4 VPC CIDR: 172.31.0.0/16

Mappings [Info](#)
Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

us-east-1a (use1-az4)
Subnet
subnet-0e91013ba56de1700

IPv4 address
Assigned by AWS

us-east-1b (use1-az6)
Subnet
subnet-084b34959e98f67fa

IPv4 address
Assigned by AWS

us-east-1c (use1-az1)
Subnet

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- Attach the Security group.
- Add the Listeners port as 443 for HTTPS.

The screenshot shows the AWS VPC service page. In the 'Security groups' section, a single security group named 'my-created-sg' is listed. In the 'Listeners and routing' section, there are two listeners: one for 'HTTP:80' and one for 'HTTPS:443'. The 'HTTPS:443' listener has its port set to 443, and its default action is 'Forward to Home-TG'.

Step 7: Create an AWS Certificate Manager

- Search AWS Certificate Manager in the search bar in the console.

The screenshot shows the AWS Certificate Manager (ACM) service page. On the left, a sidebar lists options: 'List certificates', 'Request certificate', 'Import certificate', and 'AWS Private CA'. The main area features the title 'AWS Certificate Manager' and the sub-headline 'Easily provision, manage, deploy, and renew SSL/TLS certificates'. To the right, a 'New ACM managed certificate' section includes a 'Request a certificate' button. Below it, another section for 'Import a certificate' and 'Create a private CA' is visible. At the bottom, a 'How it works' section provides a brief overview of the process.

- Give your DNS Name, and request the certificate.

AWS Certificate Manager (ACM)

Certificates (1)

Certificate ID	Domain name	Type	Status
45c4e62c-e330-4e6d-9caf-16e5cd4ce699	devopsprac.shop	Amazon Issued	Issued

- Once the certificate is issued then, click on the Certificate ID.
- Create a record in route53.

AWS Certificate Manager (ACM)

Identifier: 45c4e62c-e330-4e6d-9caf-16e5cd4ce699 Status: Issued

ARN: arn:aws:acm:us-east-1:471112584668:certificate/45c4e62c-e330-4e6d-9caf-16e5cd4ce699

Type: Amazon Issued

Domains (1)

Domain	Status	Renewal status	Type	CNAME name
devopsprac.shop	Success	-	CNAME	_802a59d2800e2d628872e2682dd9372.p.

- Select the Is domain in Route53, select the domain name, and Click on Create Record.

Create DNS records in Amazon Route 53 (0/1)

Domain	Validation status	Is domain in Route 53?
devopsprac.shop	Success	Yes

Cancel Create records

- In the Security policy, you need to give a certificate for HTTPS. Select your certificate.

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

Security category Policy name
All security policies ELBSecurityPolicy-TLS13-1-2-2021-06 (recommended)

Default SSL/TLS server certificate
The certificate used if a client connects without SNI protocol, or if there are no matching certificates. You can source this certificate from AWS Certificate Manager (ACM), Amazon Identity and Access Management (IAM), or import a certificate. This certificate will automatically be added to your listener certificate list.

Certificate source
 From ACM From IAM Import certificate

Certificate (from ACM)
The selected certificate will be applied as the default SSL/TLS server certificate for this load balancer's secure listeners.
devopsprac.shop [45c4e62c-e330-4e6d-9caf-16e5cd4ce699](#) [G](#)

[Request new ACM certificate](#)

Client certificate handling [Info](#)
Client certificates are used to make authenticated requests to remote servers. [Learn more](#)

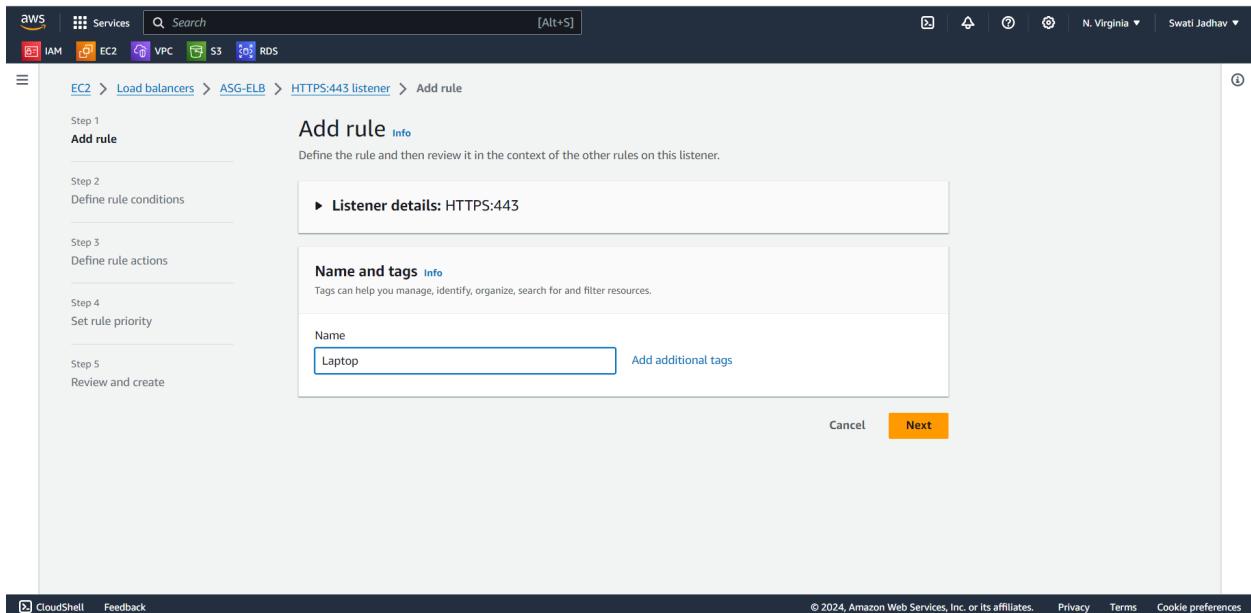
Mutual authentication (mTLS)
Mutual TLS (Transport Layer Security) authentication offers two-way peer authentication. It adds a layer of security over TLS and allows your services to verify the client that's making the connection.

► Load balancer tags - optional
Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For example, you can have Key = production-webserver, or Key = webserver, and Value = production.

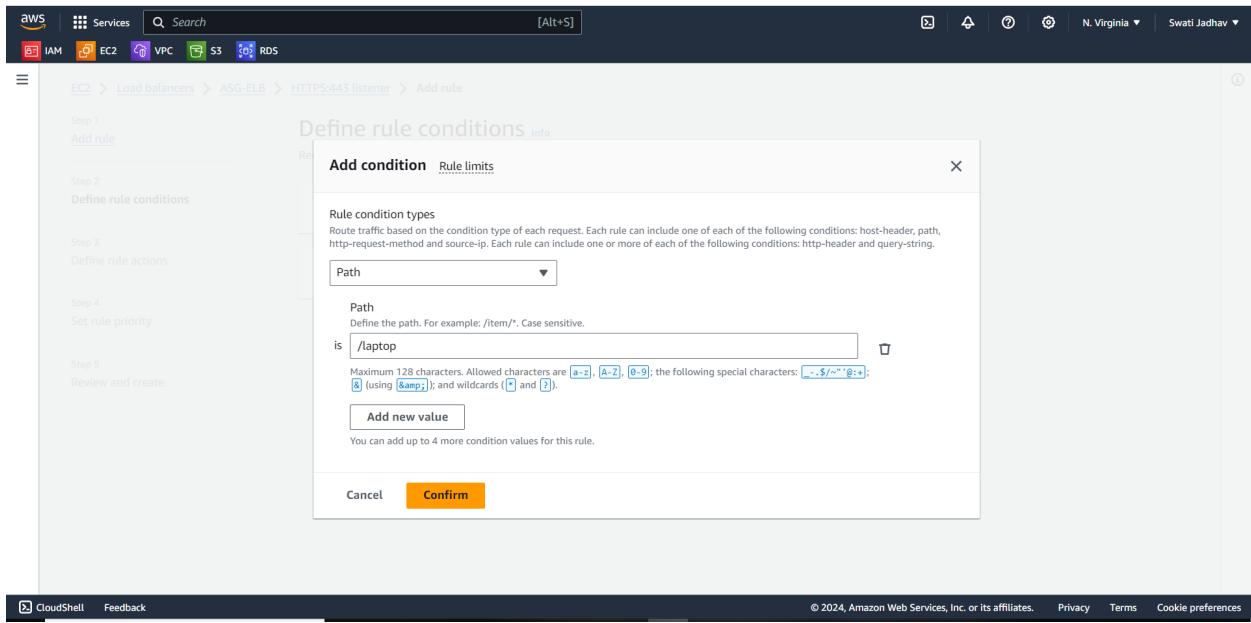
- The load balancer is successfully created.

- Click on the ALB name and scroll to manage the rules.
- Check the Check box next to the port.

- Add rule for Laptop then click next.



- In the add condition, Select the path in the dropdown, and give the path that you want, and click on Confirm.



- Now in action give the target group.

Actions

Action types

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

Use OpenID or Amazon Cognito
Include authentication using either OpenID Connect (OIDC) or Amazon Cognito.

Routing actions

Forward to target groups Redirect to URL Return fixed response

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

Target group

Target group	HTTP	Weight	Percent
Laptop-TG Target type: Instance, IPv4	HTTP	1	100%

[Add target group](#)

You can add up to 4 more target groups.

Target group stickiness Info
Stickiness enables the load balancer to bind a user's session to a specific target group. To use stickiness the client must support cookies.

Turn on target group stickiness

- Set the priority for the rule.

Rule: Laptop

Priority
Rule priority controls the evaluation order of a rule within the listener's set of rules. You can leave gaps in priority numbers.

2

1 - 50000

Listener rules (3) Info

Mobile Priority 2 Conditions (If): Path Pattern is /mobile Actions (Then): Forward to target group (Mobile-TG: 1 (100%)), Target group stickiness: Off

Laptop Priority 2 Conditions (If): Path Pattern is /laptop Actions (Then): Forward to target group (Laptop-TG: 1 (100%)), Target group stickiness: Off

- Review and create the rule.

Step 1
[Add rule](#)

Step 2
[Define rule conditions](#)

Step 3
[Define rule actions](#)

Step 4
[Set rule priority](#)

Step 5
Review and create

Rule details: Laptop

Priority	Conditions (If)	Actions (Then)
1	If request matches all: Path Pattern is /laptop	Forward to target group • Laptop-TG : 1 (100%) • Target group stickiness: Off

Rule ARN
Pending

Rule tags (1)

Key	Value
Name	Laptop

Cancel | Previous | **Create**

- Likewise, Create rule for mobile also.

Listener ARN
[arn:aws:elasticloadbalancing:us-east-1:471112584668:listener/app/ASG-ELB/7912d9b563a0797b/f2b022574c949b97](#)

Rules | Certificates | Security | Tags

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.

<input type="checkbox"/>	Name tag	Priority	Conditions (If)	Actions (Then)	ARN
<input type="checkbox"/>	Laptop	1	Path Pattern is /laptop	Forward to target group • Laptop-TG : 1 (100%) • Target group stickiness: Off	ARN
<input type="checkbox"/>	Mobile	2	Path Pattern is /mobile	Forward to target group • Mobile-TG : 1 (100%) • Target group stickiness: Off	ARN
<input type="checkbox"/>	Default	Last (default)	If no other rule applies	Forward to target group • Home-TG : 1 (100%) • Target group stickiness: Off	ARN

Rule limits | [C](#) | Actions ▾ | Add rule

- In Route 53, Create one hosted zone.
- Click on the hosted zone, you will get the value that you will have to add in the Hostinger(From where you have purchased the DNS)

- The record will be created

Route 53 > Hosted zones > devopsprac.shop

Hosted zone details

Records (3)

Record ...	Type	Routin...	Differ...	Alias	Value/Route traffic to	TTL (s...)	Health ...
devopspr...	NS	Simple	-	No	ns-411.awsdns-51.com. ns-670.awsdns-19.net. ns-1227.awsdns-25.org. ns-1753.awsdns-27.co.uk.	172800	-
devopspr...	SOA	Simple	-	No	ns-411.awsdns-51.com. awsd...	900	-
_802a59d...	CNAME	Simple	-	No	_8ce2bacc9b898e2d8de9ea8...	300	-

When you hit the DNS the website is successfully displayed.

Welcome to my Home Page ip-172-31-67-29.ec2.internal

- The connection for the Website is secure.

Connection is secure

Summary

You have successfully set up a scalable and load-balanced infrastructure that secures your connection with HTTPS and SSL. This will ensure that your application can handle increased traffic and provide a secure connection for users.