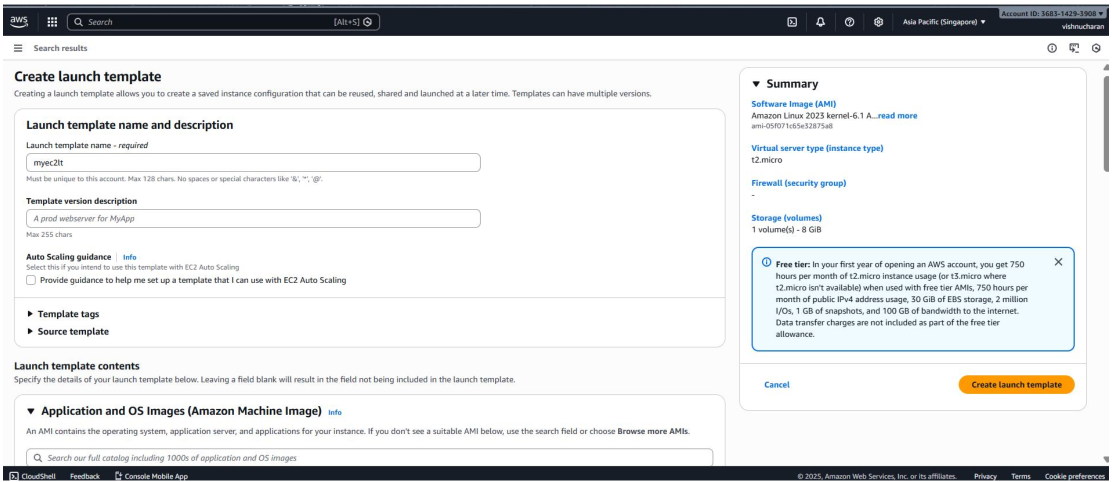
Scalable Web Application using **NLB + EC2 Auto Scaling**

1. Create Launch Template (EC2)



Search [Alt+S]

Asia Pacific (Singapore) ▼

Account ID: 3683-1429-3908 ▼

vishnucharan

Search results

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*

myec2lt

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.

▼ **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

▼ **Summary**

Software Image (AMI)
Amazon Linux 2023 kernel-6.1 A...read more
ami-05f071c65e32875a8

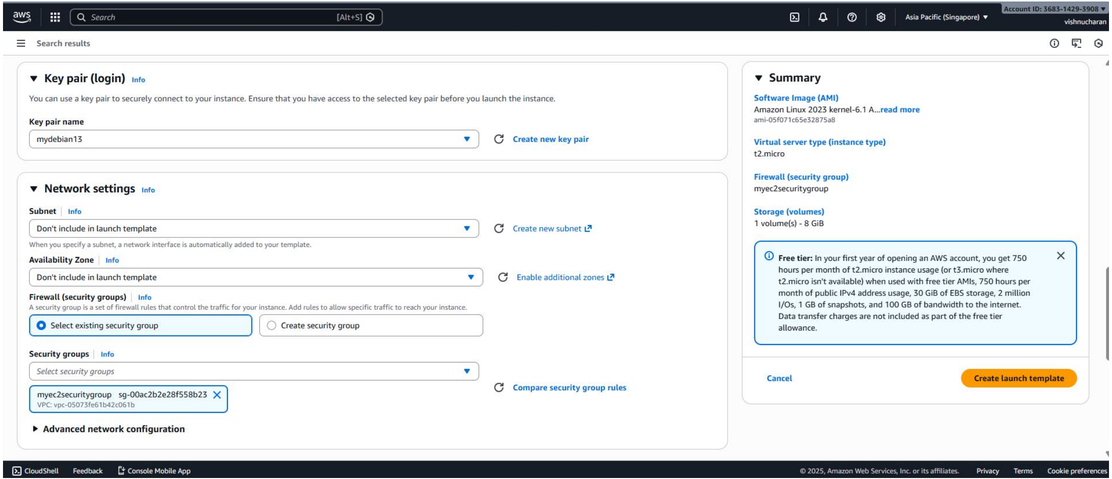
Virtual server type (instance type)
t2.micro

Firewall (security group)
-

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

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. Data transfer charges are not included as part of the free tier allowance.

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



Search [Alt+S]

Asia Pacific (Singapore) ▼

Account ID: 3683-1429-3908 ▼

vishnucharan

Search results

▼ **Key pair (login)** Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name

mydebian13 ▼

▼ **Network settings** Info

Subnet | Info

Don't include in launch template ▼

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

Availability Zone | Info

Don't include in launch template ▼

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 ▼

myec2securitygroup sg-00ac2b2e28f558b23
VPC: vpc-05073fe61b42c061b

▶ Advanced network configuration

▼ **Summary**

Software Image (AMI)
Amazon Linux 2023 kernel-6.1 A...read more
ami-05f071c65e32875a8

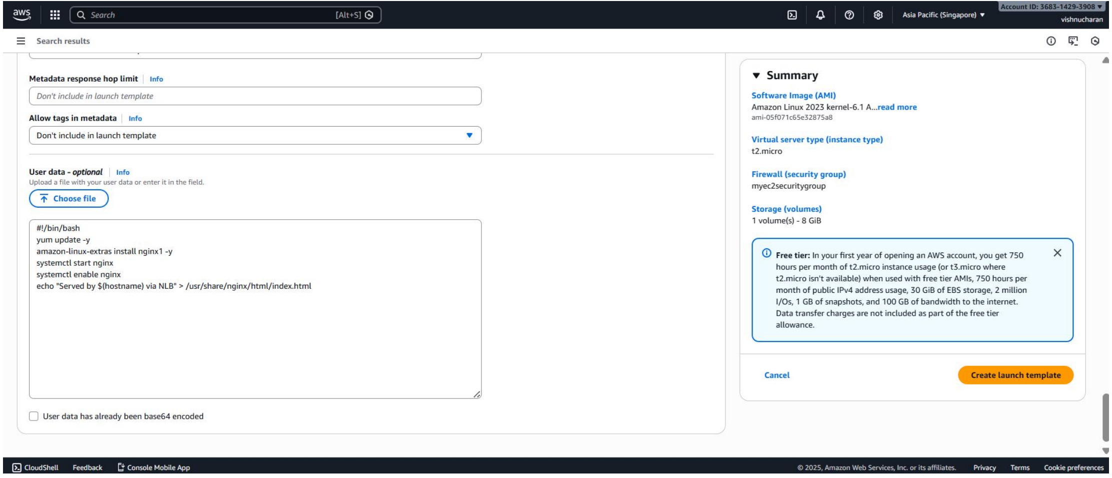
Virtual server type (instance type)
t2.micro

Firewall (security group)
myec2securitygroup

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

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. Data transfer charges are not included as part of the free tier allowance.

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



Search [Alt+S]

Asia Pacific (Singapore) ▼

Account ID: 3683-1429-3908 ▼

vishnucharan

Search results

Metadata response hop limit | Info

Don't include in launch template

Allow tags in metadata | Info

Don't include in launch template ▼

User data - *optional* | Info

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

```
#!/bin/bash
yum update -y
amazon-linux-extras install nginx1 -y
systemctl start nginx
systemctl enable nginx
echo "Served by $(hostname) via NLB" > /usr/share/nginx/html/index.html
```

□ User data has already been base64 encoded

▼ **Summary**

Software Image (AMI)
Amazon Linux 2023 kernel-6.1 A...read more
ami-05f071c65e32875a8

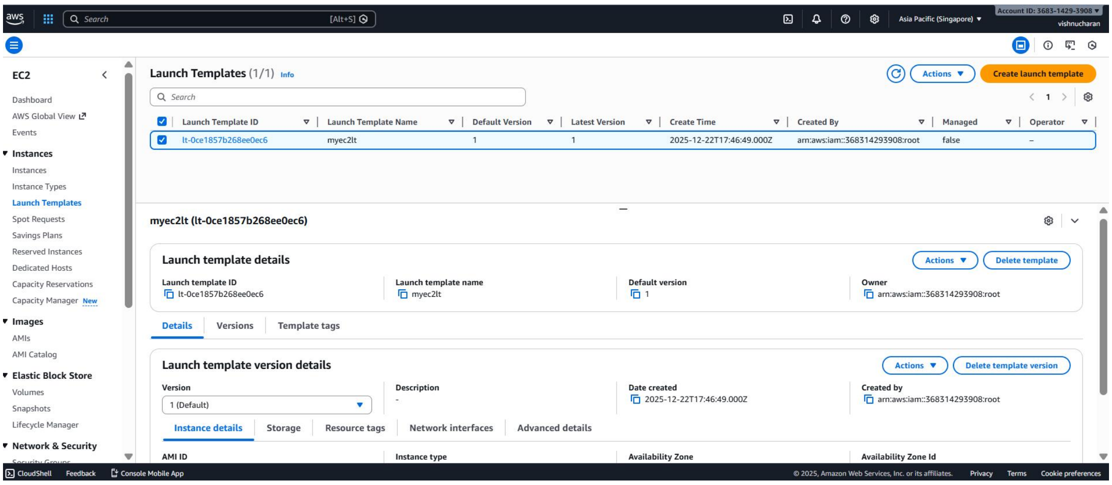
Virtual server type (instance type)
t2.micro

Firewall (security group)
myec2securitygroup

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

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. Data transfer charges are not included as part of the free tier allowance.

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



Launch Templates (1/1)

☑	Launch Template ID	Launch Template Name	Default Version	Latest Version	Create Time	Created By	Managed	Operator
☑	lt-0ce1857b268ee0ec6	myec2lt	1	1	2025-12-22T17:46:49.000Z	arn:aws:iam::368314293908:root	false	–

myec2lt (lt-0ce1857b268ee0ec6)

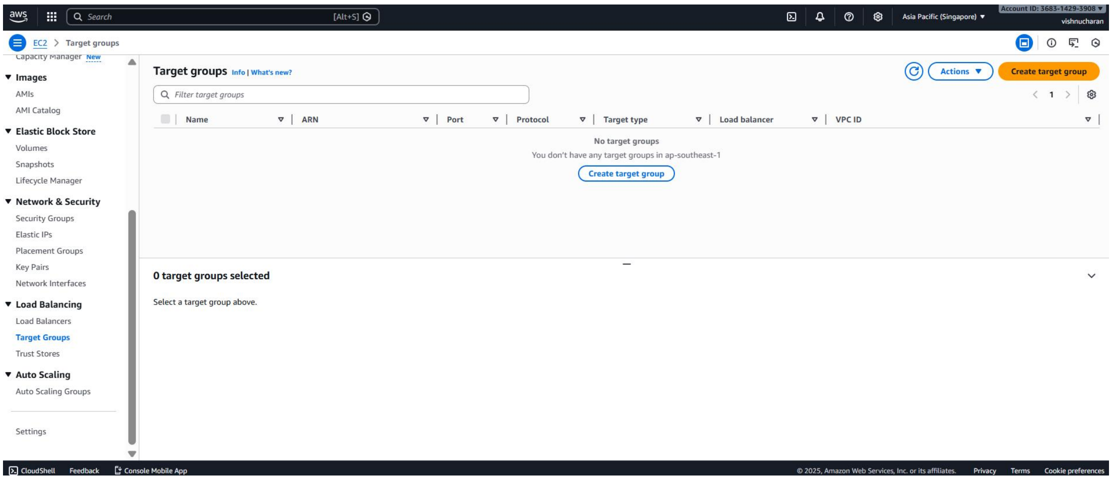
Launch template details

Launch template ID: lt-0ce1857b268ee0ec6
Launch template name: myec2lt
Default version: 1
Owner: arn:aws:iam::368314293908:root

Launch template version details

Version: 1 (Default)
Description: -
Date created: 2025-12-22T17:46:49.000Z
Created by: arn:aws:iam::368314293908:root

2. Create Target Group (Critical for NLB)



Target groups

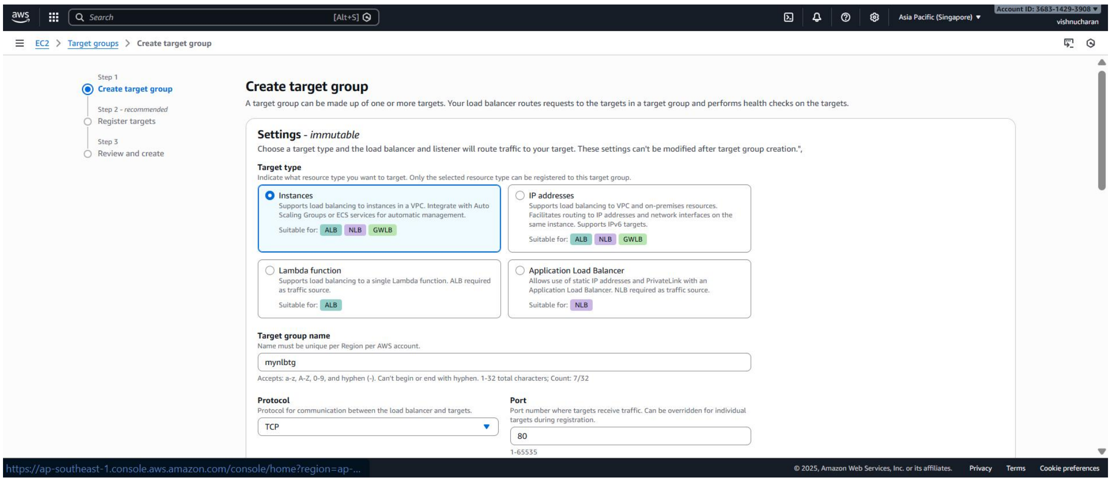
□	Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID

No target groups

You don't have any target groups in ap-southeast-1

0 target groups selected

Select a target group above.



Create target group

A target group can be made up of one or more targets. Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Settings - *immutable*

Choose a target type and the load balancer and listener will route traffic to your target. These settings can't be modified after target group creation.",

Target type

Indicate what resource type you want to target. Only the selected resource type can be registered to this target group.

● Instances
Supports load balancing to instances in a VPC. Integrate with Auto Scaling Groups or ECS services for automatic management.
Suitable for: ALB NLB GWLB

○ IP addresses
Supports load balancing to VPC and on-premises resources. Facilitates routing to IP addresses and network interfaces on the same instance. Supports IPv6 targets.
Suitable for: ALB NLB GWLB

○ Lambda function
Supports load balancing to a single Lambda function. ALB required as traffic source.
Suitable for: ALB

○ Application Load Balancer
Allows use of static IP addresses and PrivateLink with an Application Load Balancer. NLB required as traffic source.
Suitable for: NLB

Target group name

Name must be unique per Region per AWS account.

mynlbtg

Accepts: a-z, A-Z, 0-9, and hyphen (-). Can't begin or end with hyphen. 1-32 total characters; Count: 7/32

Protocol

Protocol for communication between the load balancer and targets.

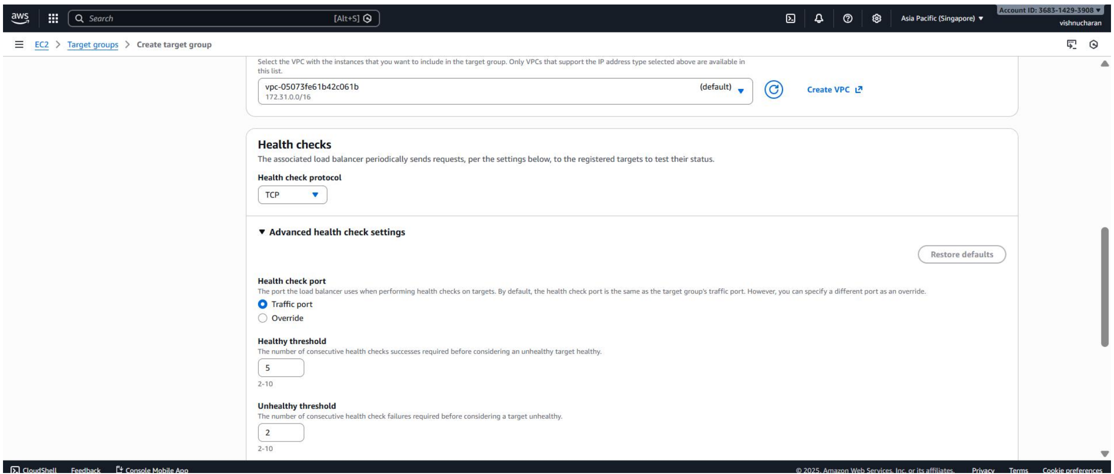
TCP

Port

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

80

1-65535



aws
Search [Alt+S]
Asia Pacific (Singapore) ▼
Account ID: 3683-1429-3908 ▼
vishnucharan
EC2 > Target groups > Create target group

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-05073fe61b42c061b (default)
172.31.0.0/16

Health checks

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

Health check protocol: TCP

▼ Advanced health check settings

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.

5

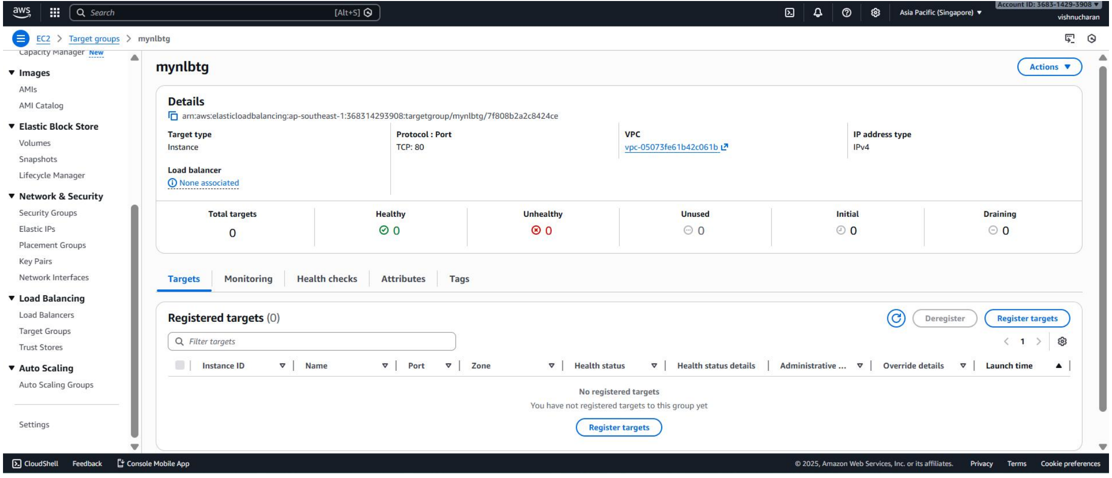
2-10

Unhealthy threshold

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

2

2-10



mynlbtg

Details

arn:aws:elasticloadbalancing:ap-southeast-1:368314293908:targetgroup/mynlbtg/7f808b2a2c8424ce

Target type	Protocol : Port	VPC	IP address type
Instance	TCP: 80	vpc-05073fe61b42c061b	IPv4

Load balancer

None associated

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

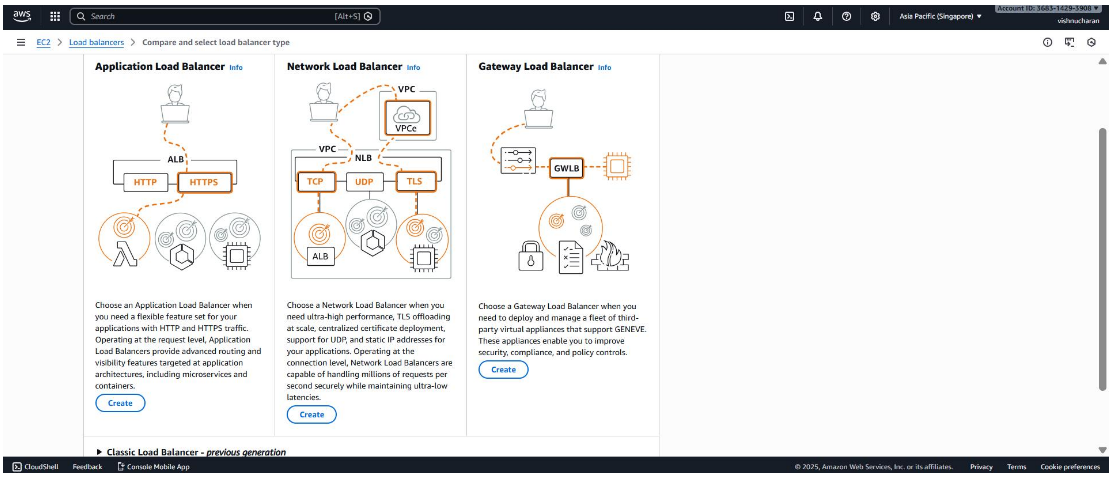
Registered targets (0)

□	Instance ID	Name	Port	Zone	Health status	Health status details	Administrative ...	Override details	Launch time

No registered targets

You have not registered targets to this group yet

3. Create Network Load Balancer



aws
Search [Alt+S]
Asia Pacific (Singapore) ▼
Account ID: 3683-1429-3908 ▼
vishnucharan
EC2 > Load balancers > Compare and select load balancer type
ALB
HTTP
HTTPS
VPC
VPCe
VPC
NLB
TCP
UDP
TLS
ALB
GWLB

Application Load Balancer Info

Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

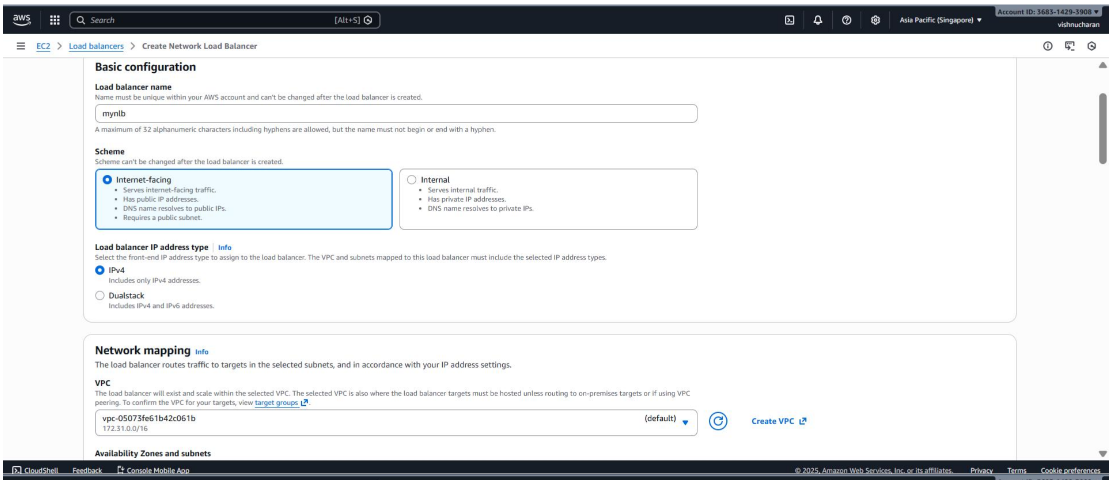
Network Load Balancer Info

Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

Gateway Load Balancer Info

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 you to improve security, compliance, and policy controls.

▶ Classic Load Balancer - *previous generation*


aws
Search [Alt+S]
Asia Pacific (Singapore) ▾
Account ID: 3683-1429-3908 ▾
vishnucharan
EC2 > Load balancers > Create Network 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.

mynlb

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

Scheme
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.

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.

● IPv4
Includes only IPv4 addresses.

○ Dualstack
Includes IPv4 and IPv6 addresses.

Network mapping Info

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

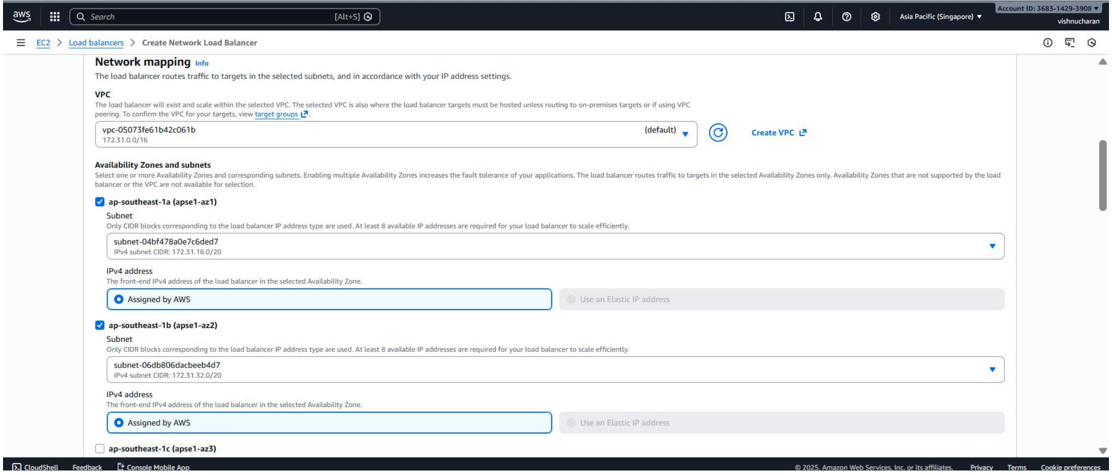
VPC
The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to on-premises targets or if using VPC peering. To confirm the VPC for your targets, view target groups.

vpc-05073fe61b42c061b (default)
172.31.0.0/16

Create VPC

Availability Zones and subnets

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


aws
Search [Alt+S]
Asia Pacific (Singapore) ▾
Account ID: 3683-1429-3908 ▾
vishnucharan
EC2 > Load balancers > Create Network Load Balancer

Network mapping Info

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

VPC
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 on-premises targets or if using VPC peering. To confirm the VPC for your targets, view target groups.

vpc-05073fe61b42c061b (default)
172.31.0.0/16

Create VPC

Availability Zones and subnets
Select one or more Availability Zones and corresponding subnets. Enabling multiple Availability Zones increases the fault tolerance of your applications. The load balancer routes traffic to targets in the selected Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

☑ **ap-southeast-1a (apse1-az1)**

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-04bf478a0e7c6ded7
IPv4 subnet CIDR: 172.31.16.0/20

IPv4 address
The front-end IPv4 address of the load balancer in the selected Availability Zone.

● Assigned by AWS ○ Use an Elastic IP address

☑ **ap-southeast-1b (apse1-az2)**

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.

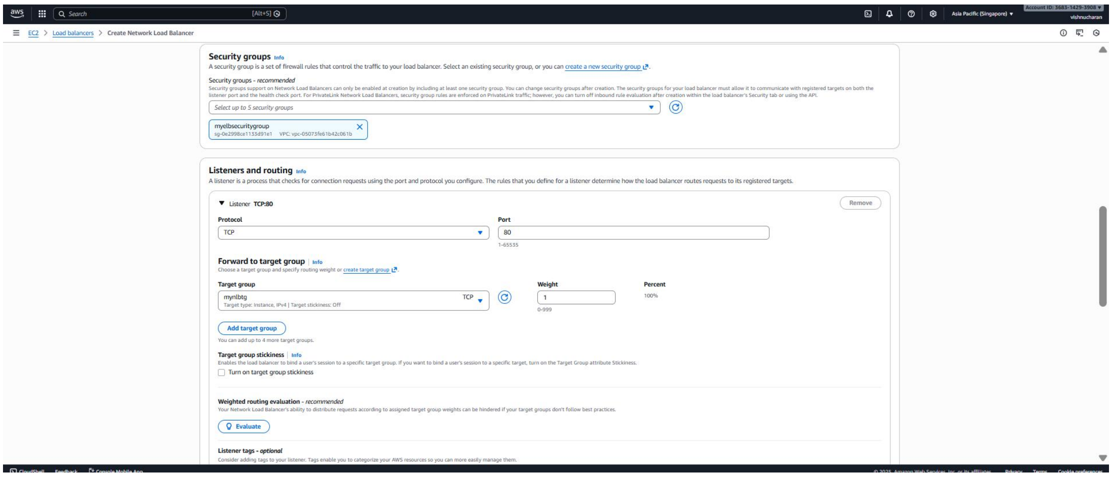
subnet-06db806dacbeeb4d7
IPv4 subnet CIDR: 172.31.32.0/20

IPv4 address
The front-end IPv4 address of the load balancer in the selected Availability Zone.

● Assigned by AWS ○ Use an Elastic IP address

☐ **ap-southeast-1c (apse1-az3)**

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


aws
Search [Alt+S]
Asia Pacific (Singapore) ▾
Account ID: 3683-1429-3908 ▾
vishnucharan
EC2 > Load balancers > Create Network Load Balancer

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 - *recommended*
Security groups support on Network Load Balancers can only be enabled at creation by including at least one security group. You can change security groups after creation. The security groups for your load balancer must allow it to communicate with registered targets on both the listener port and the health check port. For PrivateLink Network Load Balancers, security group rules are enforced on PrivateLink traffic; however, you can turn off inbound rule evaluation after creation within the load balancer's Security tab or using the API.

Select up to 5 security groups

myelbsecuritygroup
sg-0e2998ce1133d91e1 VPC: vpc-05073fe61b42c061b

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 **TCP:80**

Remove

Protocol
TCP

Port
80
1-65535

Forward to target group Info
Choose a target group and specify routing weight or create target group.

Target group
mynlbtg TCP
Target type: Instance, IPv4 | Target stickiness: Off

Weight
1
0-999

Percent
100%

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

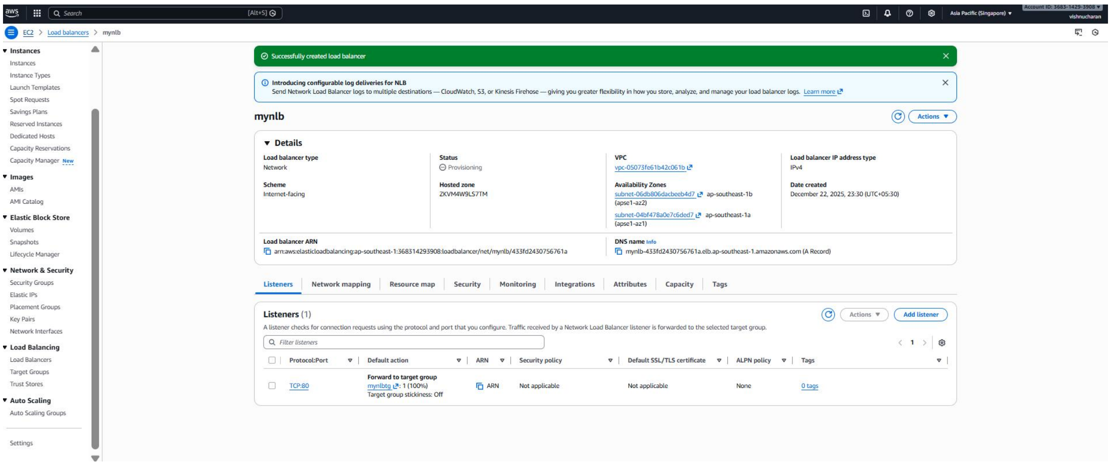
Target group stickiness Info
Enables the load balancer to bind a user's session to a specific target group. If you want to bind a user's session to a specific target, turn on the Target Group attribute Stickiness.

☐ Turn on target group stickiness

Weighted routing evaluation - *recommended*
Your Network Load Balancer's ability to distribute requests according to assigned target group weights can be hindered if your target groups don't follow best practices.

Evaluate

Listener tags - *optional*
Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.



Successfully created load balancer

Introducing configurable log deliveries for NLB
Send Network Load Balancer logs to multiple destinations — CloudWatch, S3, or Kinesis Firehose — giving you greater flexibility in how you store, analyze, and manage your load balancer logs. Learn more

mynlb

▾ Details

Load balancer type Network	**Status** Provisioning	**VPC** vpc-05073fe61b42c061b	**Load balancer IP address type** IPv4
Scheme Internet-facing	**Hosted zone** ZKVM4W9LS7TM	**Availability Zones** subnet-06db806dacbeeb4d7 ap-southeast-1b (apse1-az2) subnet-04bf478a0e7c6ded7 ap-southeast-1a (apse1-az1)	**Date created** December 22, 2025, 23:30 (UTC+05:30)

Load balancer ARN
arn:aws:elasticloadbalancing:ap-southeast-1:368314293908:loadbalancer/net/mynlb/433fd2430756761a

DNS name Info
mynlb-433fd2430756761a.elb.ap-southeast-1.amazonaws.com (A Record)

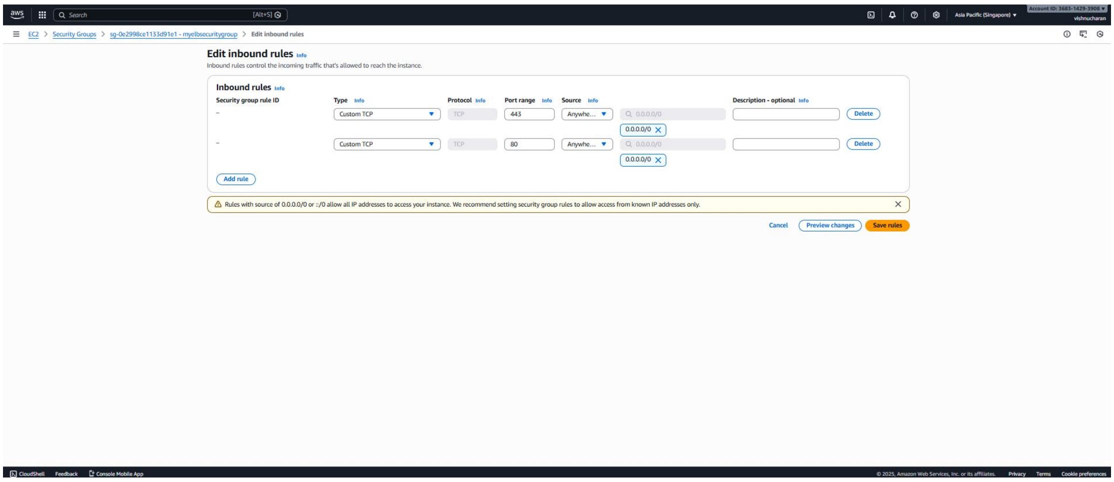
Listeners (1)

A listener checks for connection requests using the protocol and port that you configure. Traffic received by a Network Load Balancer listener is forwarded to the selected target group.

Filter listeners

□	Protocol:Port	Default action	ARN	Security policy	Default SSL/TLS certificate	ALPN policy	Tags
□	TCP:80	**Forward to target group** mynlbtg: 1 (100%) Target group stickiness: Off	ARN	Not applicable	Not applicable	None	0 tags

NLB Security group(Inbound rules):-


Search [Alt+S]
Asia Pacific (Singapore) ▾
vishnucharan
EC2 > Security Groups > sg-0e2998ce1133d91e1 - myelbsecuritygroup > Edit inbound rules
Add rule
Delete
Cancel
Preview changes
Save rules
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Edit inbound rules Info

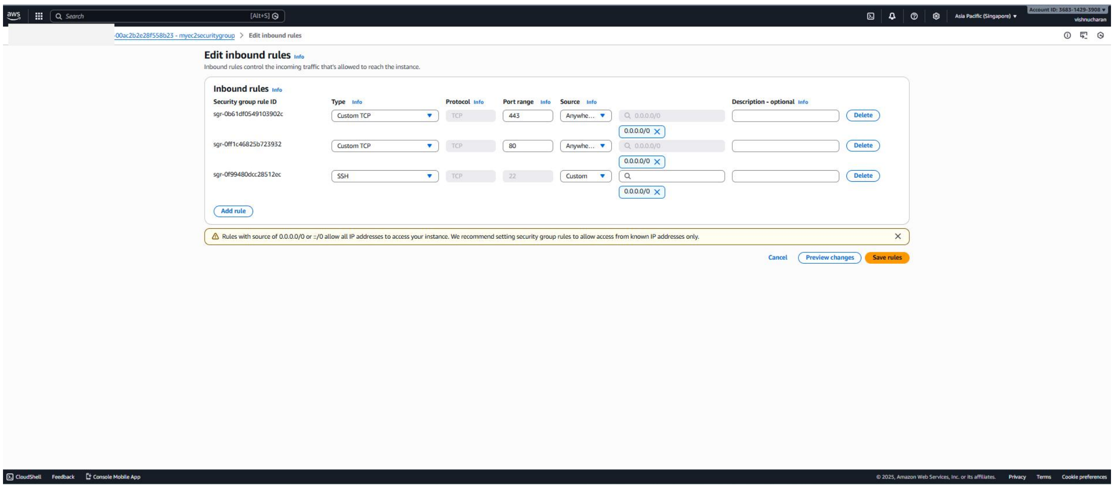
Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source		Description - optional
–	Custom TCP	TCP	443	Anywhe...	0.0.0.0/0	
–	Custom TCP	TCP	80	Anywhe...	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 group(Inbound rules):-


Search [Alt+S]
Asia Pacific (Singapore) ▾
vishnucharan
00ac2b2e28f558b23 - myec2securitygroup > Edit inbound rules
Add rule
Delete
Cancel
Preview changes
Save rules
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Edit inbound rules Info

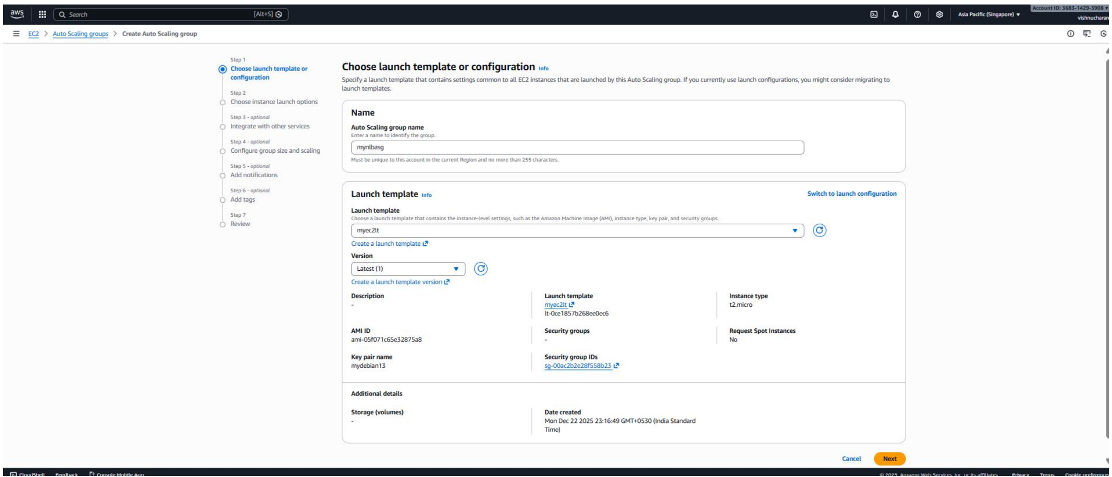
Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source		Description - optional
sgr-0b61df0549103902c	Custom TCP	TCP	443	Anywhe...	0.0.0.0/0	
sgr-0ff1c46825b723932	Custom TCP	TCP	80	Anywhe...	0.0.0.0/0	
sgr-0f99480dcc28512ec	SSH	TCP	22	Custom	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.

4. Create Auto Scaling Group


aws
Search
[Alt+S]
Asia Pacific (Singapore) ▾
Account ID: 3683-1429-3908 ▾
vishnucharan
EC2 > Auto Scaling groups > Create Auto Scaling group
Step 1
Choose launch template or configuration
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
Cancel
Next

Choose launch template or configuration Info

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group. If you currently use launch configurations, you might consider migrating to launch templates.

Name

Auto Scaling group name

Enter a name to identify the group.

mynlbasg

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

Launch template Info

Switch to launch configuration

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.

myec2lt ▾

Create a launch template

Version

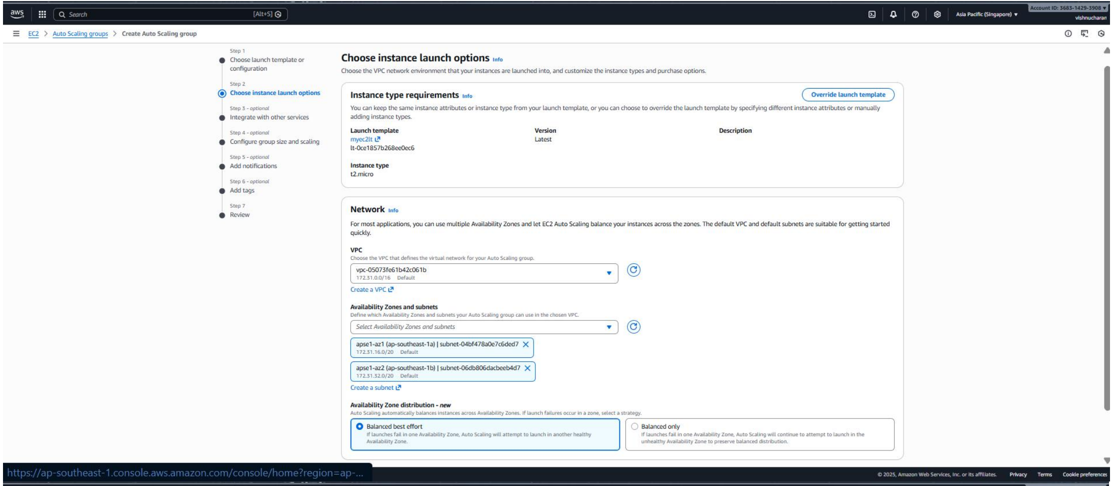
Latest (1) ▾

Create a launch template version

Description -	**Launch template** myec2lt lt-0ce1857b268ee0ec6	**Instance type** t2.micro
AMI ID ami-05f071c65e32875a8	**Security groups** -	**Request Spot Instances** No
Key pair name mydebian13	**Security group IDs** sg-00ac2b2e28f558b23	

Additional details

Storage (volumes) -	**Date created** Mon Dec 22 2025 23:16:49 GMT+0530 (India Standard Time)


aws
Search
[Alt+S]
Asia Pacific (Singapore) ▾
Account ID: 3683-1429-3908 ▾
vishnucharan
EC2 > Auto Scaling groups > Create Auto Scaling group
Step 1
Choose launch template or configuration
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
https://ap-southeast-1.console.aws.amazon.com/console/home?region=ap-...
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Choose instance launch options Info

Choose the VPC network environment that your instances are launched into, and customize the instance types and purchase 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 myec2lt lt-0ce1857b268ee0ec6	**Version** Latest	**Description**
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-05073fe61b42c061b
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

apse1-az1 (ap-southeast-1a) | subnet-04bf478a0e7c6ded7 ✕
172.31.16.0/20 Default

apse1-az2 (ap-southeast-1b) | subnet-06db806dacbeeb4d7 ✕
172.31.32.0/20 Default

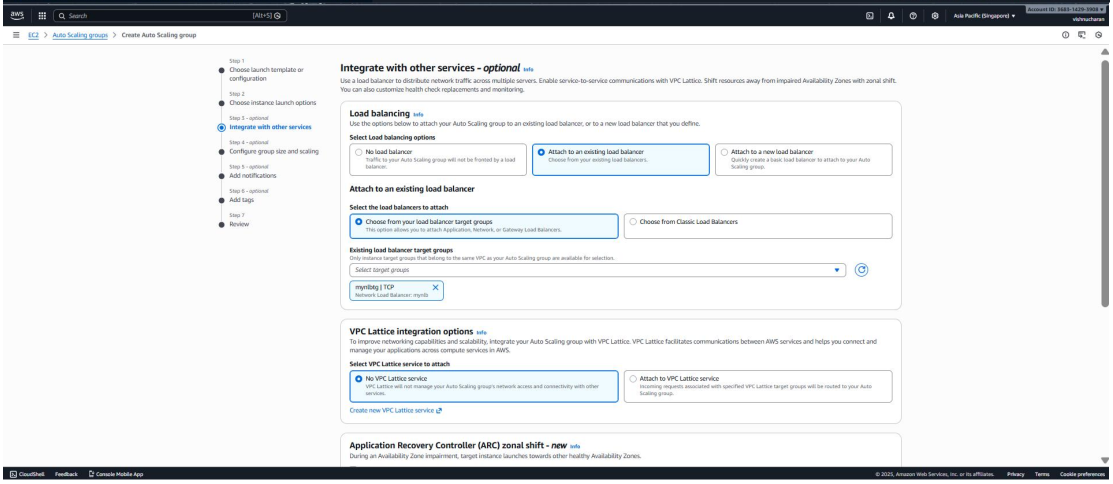
Create a subnet

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.


aws
Search
[Alt+S]
Asia Pacific (Singapore) ▾
Account ID: 3683-1429-3908 ▾
vishnucharan
EC2 > Auto Scaling groups > Create Auto Scaling group
Step 1
Choose launch template or configuration
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
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Integrate with other services - *optional* Info

Use a load balancer to distribute network traffic across multiple servers. Enable service-to-service communications with VPC Lattice. Shift resources away from impaired Availability Zones with zonal shift. You can also customize health check replacements and monitoring.

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.

Select Load balancing options

○ 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.

Attach to an existing load balancer

Select the load balancers to attach

● Choose from your load balancer target groups
This option allows you to attach Application, Network, or Gateway Load Balancers.

○ Choose from Classic Load Balancers

Existing load balancer target groups

Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

Select target groups

mynlbtg | TCP ✕
Network Load Balancer: mynlb

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

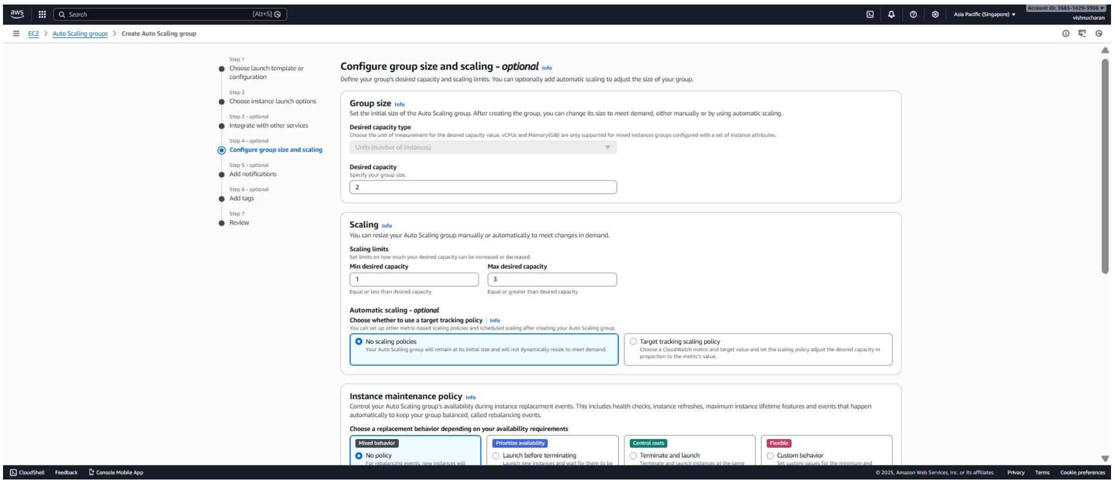
● No VPC Lattice service
VPC Lattice will not manage your Auto Scaling group's network access and connectivity with other services.

○ 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

Application Recovery Controller (ARC) zonal shift - *new* Info

During an Availability Zone impairment, target instance launches towards other healthy Availability Zones.


aws
Search
[Alt+S]
Asia Pacific (Singapore) ▾
Account ID: 3683-1429-3908 ▾
vishnucharan
EC2 > Auto Scaling groups > Create Auto Scaling group
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Step 1
Choose launch template or configuration

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

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
1
Equal or less than desired capacity

Max desired capacity
3
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.

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.

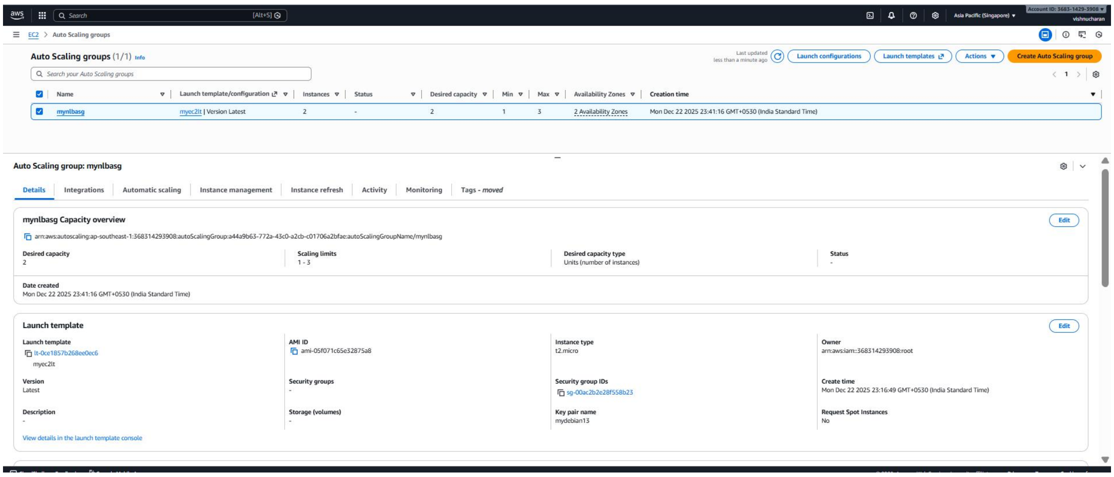
Choose a replacement behavior depending on your availability requirements

Mixed behavior
● No policy
For rebalancing events, new instances will

Prioritize availability
○ Launch before terminating
Launch new instances and wait for them to be

Control costs
○ Terminate and launch
Terminate and launch instances at the same

Flexible
○ Custom behavior
Set custom values for the minimum and


aws
Search
[Alt+S]
Asia Pacific (Singapore) ▾
Account ID: 3683-1429-3908 ▾
vishnucharan
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
1

Auto Scaling groups (1/1) Info

☑	Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability Zones	Creation time
☑	mynlbasg	myec2lt | Version Latest	2	-	2	1	3	2 Availability Zones	Mon Dec 22 2025 23:41:16 GMT+0530 (India Standard Time)

Auto Scaling group: mynlbasg

mynlbasg Capacity overview

arn:aws:autoscaling:ap-southeast-1:368314293908:autoScalingGroup:a44a9b63-772a-43c0-a2cb-c01706a2bfae:autoScalingGroupName/mynlbasg

Desired capacity
2

Scaling limits
1 - 3

Desired capacity type
Units (number of instances)

Status
-

Date created
Mon Dec 22 2025 23:41:16 GMT+0530 (India Standard Time)

Launch template

Launch template
lt-0ce1857b268ee0ec6
myec2lt

AMI ID
ami-05f071c65e32875a8

Instance type
t2.micro

Owner
arn:aws:iam::368314293908:root

Version
Latest

Security groups
-

Security group IDs
sg-00ac2b2e28f558b23

Create time
Mon Dec 22 2025 23:16:49 GMT+0530 (India Standard Time)

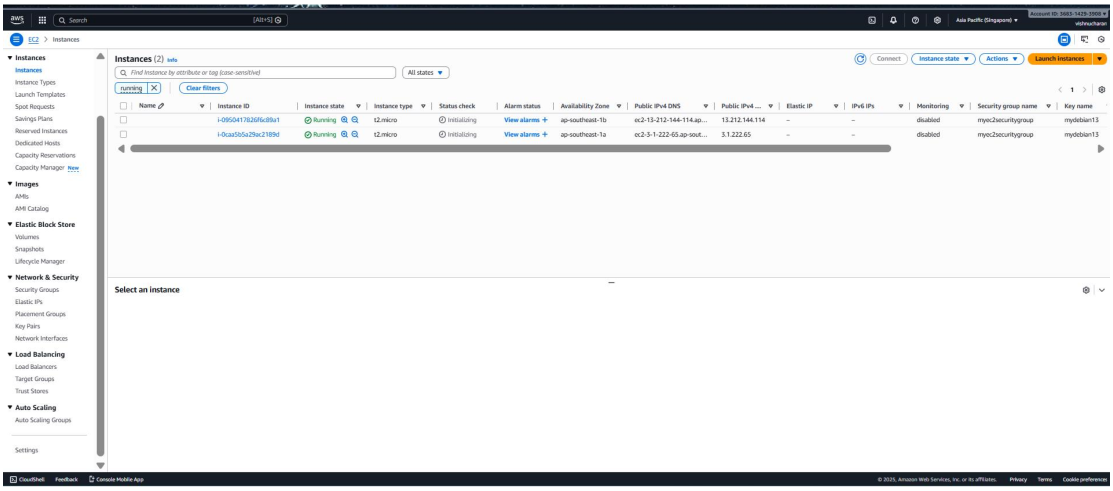
Description
-

Storage (volumes)
-

Key pair name
mydebian13

Request Spot Instances
No

View details in the launch template console



Instances (2) Info

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitoring	Security group name	Key name
□		i-0950417826f6c89a1	Running	t2.micro	Initializing	View alarms +	ap-southeast-1b	ec2-13-212-144-114.ap...	13.212.144.114	–	–	disabled	myec2securitygroup	mydebian13
□		i-0caa5b5a29ac2189d	Running	t2.micro	Initializing	View alarms +	ap-southeast-1a	ec2-3-1-222-65.ap-sout...	3.1.222.65	–	–	disabled	myec2securitygroup	mydebian13

Select an instance