AWS 3-Tier Architecture Project Documentation

Name: Kishan Deep Lamichhane

Project Title: Design and Implementation of AWS 3-Tier Architecture

Platform: Amazon Web Services (AWS)

---

1. Project Overview

This project demonstrates the design and implementation of a **secure, scalable, and highly available AWS 3-Tier Architecture**.

The architecture is divided into three layers:

- **Web Tier** – Handles HTTP/HTTPS requests from users.
- **Application Tier** – Processes business logic and communicates with the database.
- **Database Tier** – Stores application data securely.

Each tier is isolated using **VPCs, subnets, security groups, and load balancers**, and deployed across **two Availability Zones (AZs)** to ensure **fault tolerance** and **high availability**.

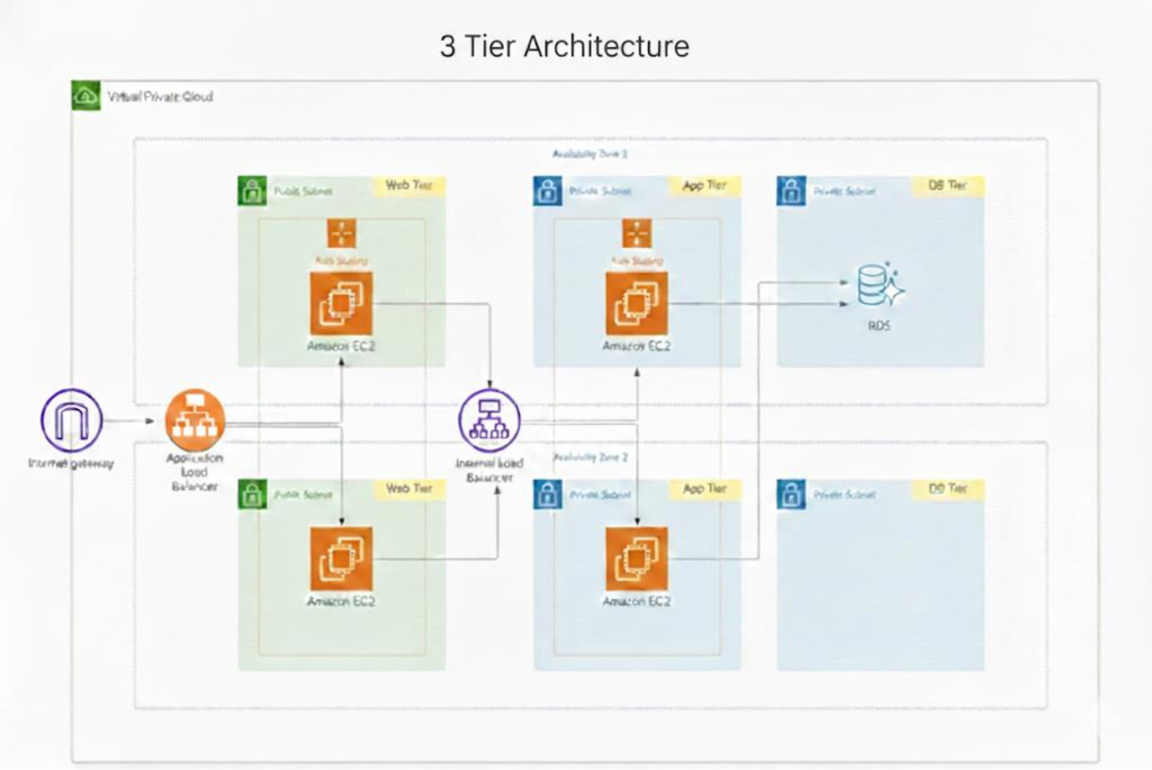


Figure: 3-Tier Architecture Diagram

2. VPC and Networking Architecture

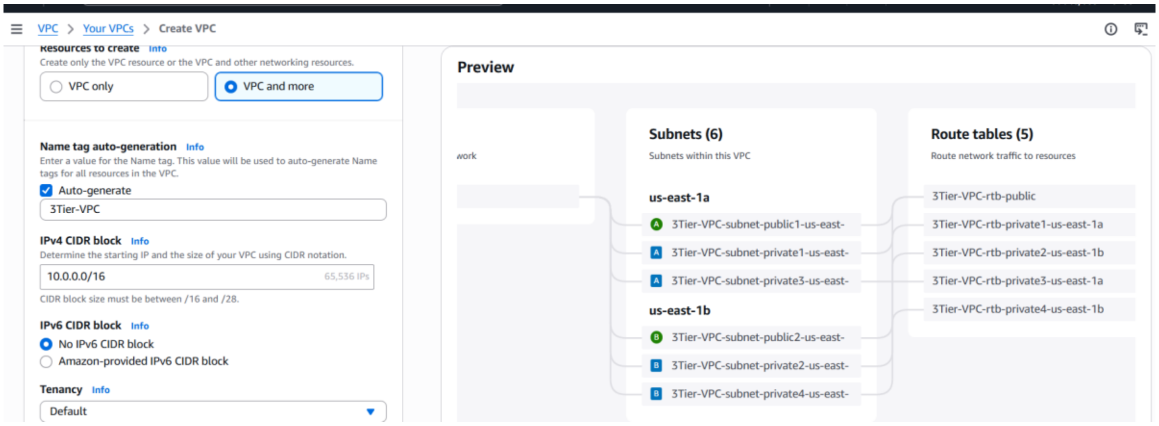
Custom VPC Configuration

- VPC Name: 3Tier-VPC
- CIDR: 10.0.0.0/16
- Spans two AZs for redundancy

Subnet Design

- **Public Subnets:** Web Tier
- **Private Subnets:** Application Tier, Database Tier

- Separates public-facing and private components for security



VPC > Your VPCs > Create VPC

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

○ VPC only ● VPC and more

Name tag auto-generation Info

Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☑ Auto-generate

3Tier-VPC

IPv4 CIDR block Info

Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16 65,536 IPs

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

● No IPv6 CIDR block

○ Amazon-provided IPv6 CIDR block

Tenancy Info

Default

Preview

Subnets (6)

Subnets within this VPC

us-east-1a

3Tier-VPC-subnet-public1-us-east-

3Tier-VPC-subnet-private1-us-east-

3Tier-VPC-subnet-private3-us-east-

us-east-1b

3Tier-VPC-subnet-public2-us-east-

3Tier-VPC-subnet-private2-us-east-

3Tier-VPC-subnet-private4-us-east-

Route tables (5)

Route network traffic to resources

3Tier-VPC-rtb-public

3Tier-VPC-rtb-private1-us-east-1a

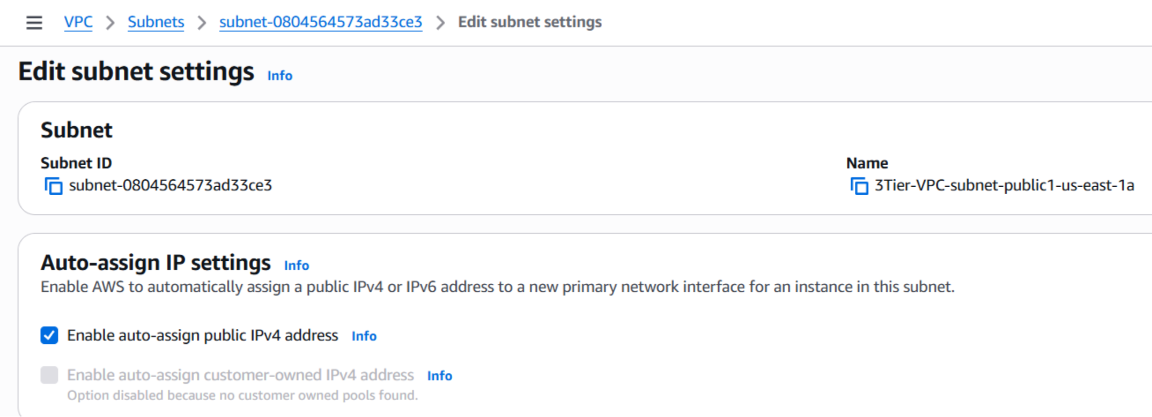
3Tier-VPC-rtb-private2-us-east-1b

3Tier-VPC-rtb-private3-us-east-1a

3Tier-VPC-rtb-private4-us-east-1b

Public IP Assignment

- Public subnets: **Auto-assign public IPv4 enabled**
- Private subnets: Public IP disabled



VPC > Subnets > subnet-0804564573ad33ce3 > Edit subnet settings

Edit subnet settings Info

Subnet

Subnet ID: subnet-0804564573ad33ce3

Name: 3Tier-VPC-subnet-public1-us-east-1a

Auto-assign IP settings Info

Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.

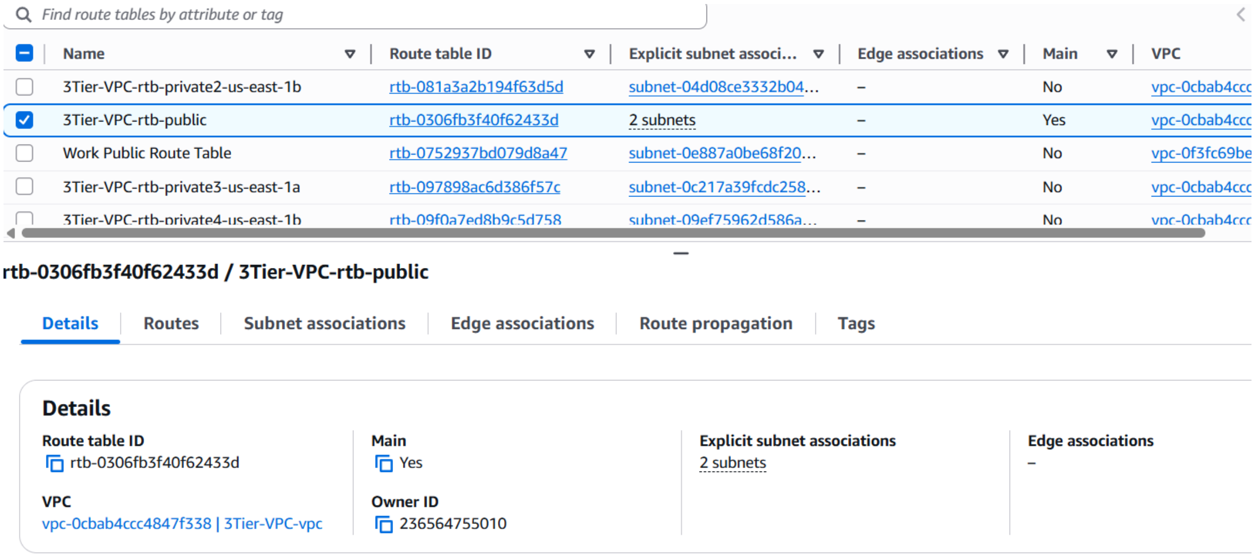
☑ Enable auto-assign public IPv4 address Info

□ Enable auto-assign customer-owned IPv4 address Info

Option disabled because no customer owned pools found.

Route Tables and Internet Gateway

- Public subnets associated with default route table
- Route **0.0.0.0/0** → **Internet Gateway** added for outbound traffic



☐	Name	Route table ID	Explicit subnet associ…	Edge associations	Main	VPC
☐	3Tier-VPC-rtb-private2-us-east-1b	rtb-081a3a2b194f63d5d	subnet-04d08ce3332b04…	–	No	vpc-0cbab4ccc
☑	3Tier-VPC-rtb-public	rtb-0306fb3f40f62433d	2 subnets	–	Yes	vpc-0cbab4ccc
☐	Work Public Route Table	rtb-0752937bd079d8a47	subnet-0e887a0be68f20…	–	No	vpc-0f3fc69be
☐	3Tier-VPC-rtb-private3-us-east-1a	rtb-097898ac6d386f57c	subnet-0c217a39fcdc258…	–	No	vpc-0cbab4ccc
☐	3Tier-VPC-rtb-private4-us-east-1b	rtb-09f0a7ed8b9c5d758	subnet-09ef75962d586a…	–	No	vpc-0cbab4ccc

rtb-0306fb3f40f62433d / 3Tier-VPC-rtb-public

Details

Route table ID: rtb-0306fb3f40f62433d

VPC: vpc-0cbab4ccc4847f338 | 3Tier-VPC-vpc

Main: Yes

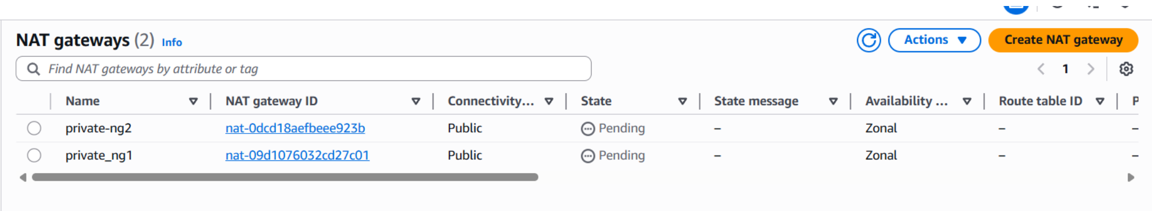
Owner ID: 236564755010

Explicit subnet associations: 2 subnets

Edge associations: –

NAT Gateway Configuration

- Two NAT Gateways (**private-ng1** and **private-ng2**) in separate AZs
- Allows private instances secure internet access

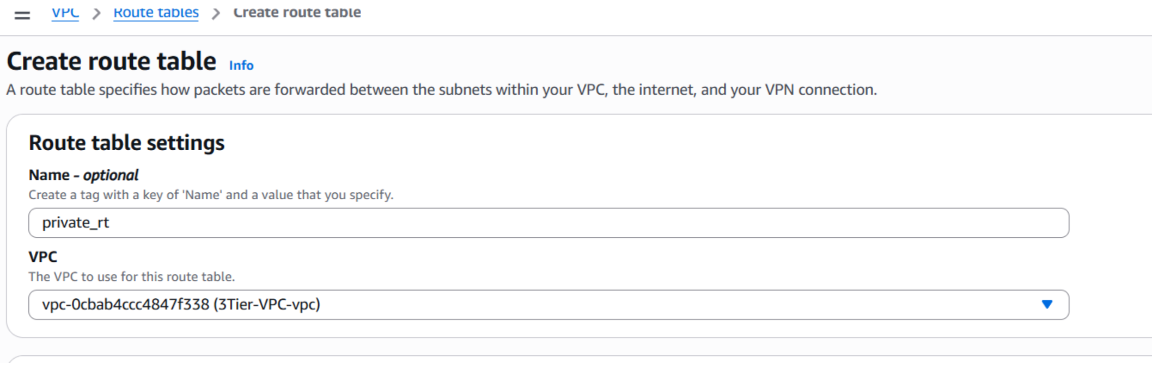


NAT gateways (2) Info

	Name	NAT gateway ID	Connectivity…	State	State message	Availability …	Route table ID	P
○	private-ng2	nat-0dcd18aefbeee923b	Public	Pending	–	Zonal	–	–
○	private_ng1	nat-09d1076032cd27c01	Public	Pending	–	Zonal	–	–

Private Route Table

- Private route table **private_rt** associated with Application Tier subnets
- All outbound traffic routed via NAT Gateway



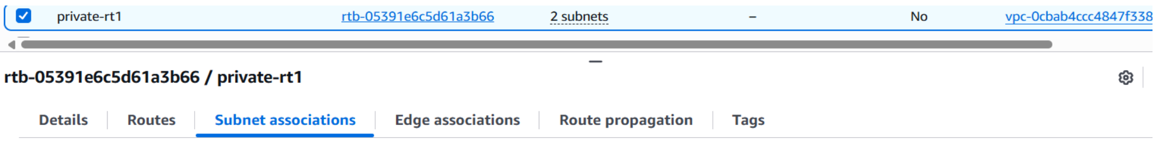
Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

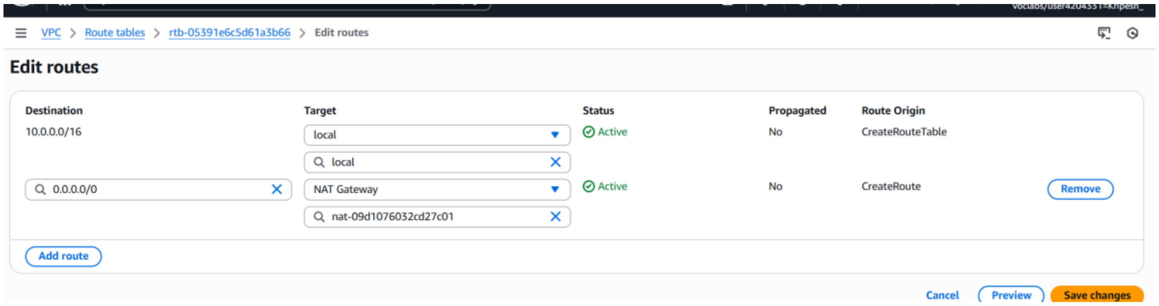
Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
private_rt

VPC
The VPC to use for this route table.
vpc-0cbab4ccc4847f338 (3Tier-VPC-vpc)



☑	private-rt1	rtb-05391e6c5d61a3b66	2 subnets	–	No	vpc-0cbab4ccc4847f338

rtb-05391e6c5d61a3b66 / private-rt1



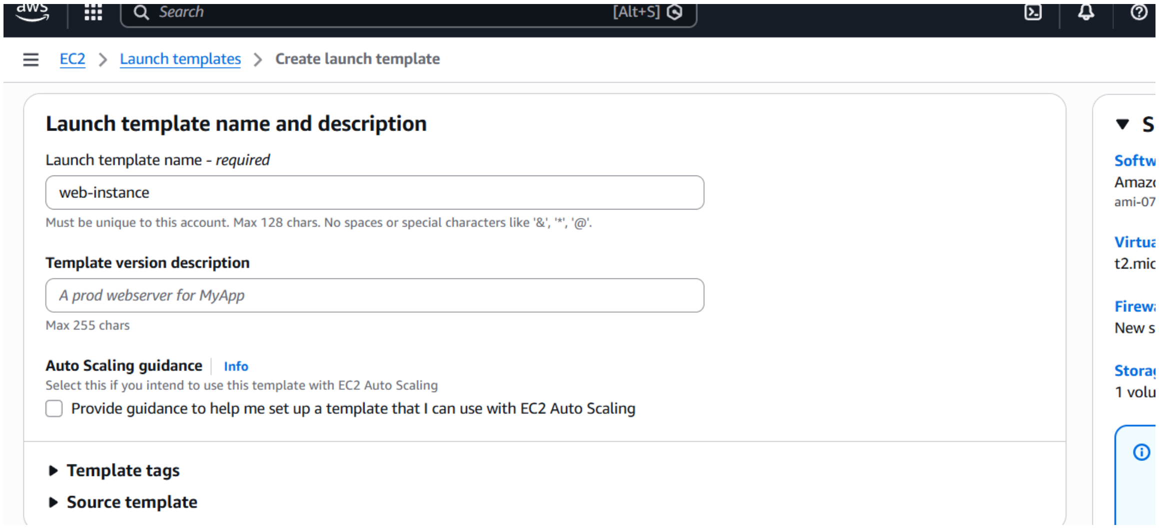
Edit routes

Destination	Target	Status	Propagated	Route Origin	
10.0.0.0/16	local local	Active	No	CreateRouteTable	
0.0.0.0/0	NAT Gateway nat-09d1076032cd27c01	Active	No	CreateRoute	Remove

3. Web Tier Architecture

Launch Template

- Name: **web-instance** for consistent EC2 deployment



Launch template name and description

Launch template name - *required*

web-instance

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

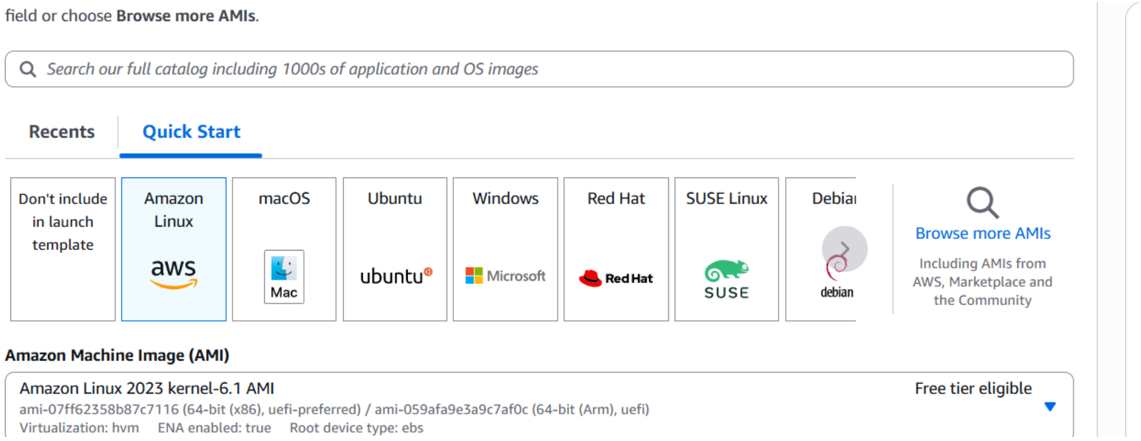
☐ Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

▸ Template tags

▸ Source template

EC2 Configuration

- **AMI:** Amazon Linux 2023
- **Instance Type:** t2.micro (cost-effective)
- **Key Pair:** mykeypair (for secure SSH access)


field or choose **Browse more AMIs**.

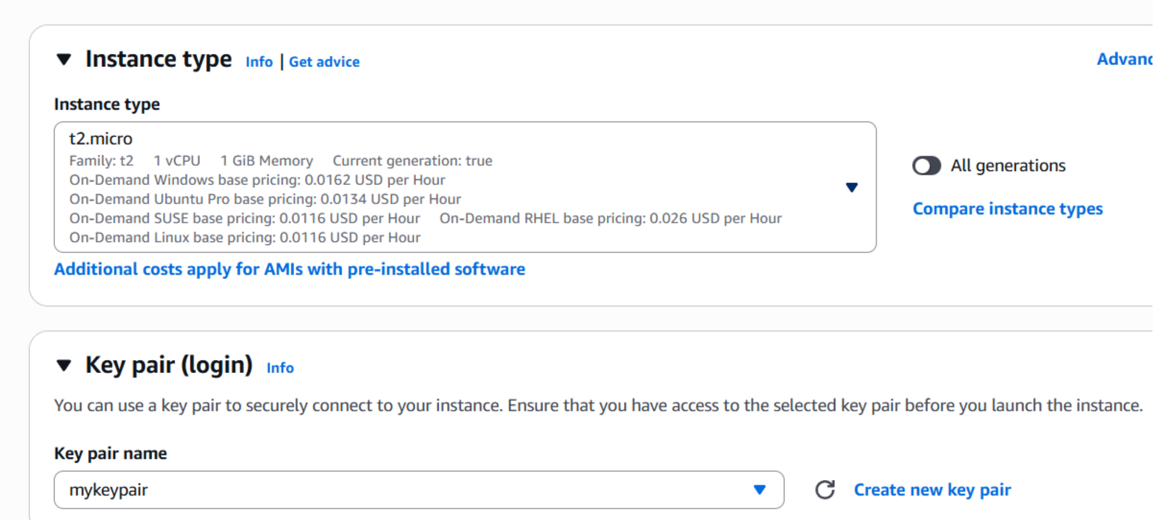
Search our full catalog including 1000s of application and OS images

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI — Free tier eligible

ami-07ff62358b87c7116 (64-bit (x86), uefi-preferred) / ami-059afa9e3a9c7af0c (64-bit (Arm), uefi)

Virtualization: hvm ENA enabled: true Root device type: ebs



▼ **Instance type** Info | Get advice

Advanc

Instance type

t2.micro
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

▼ **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

mykeypair

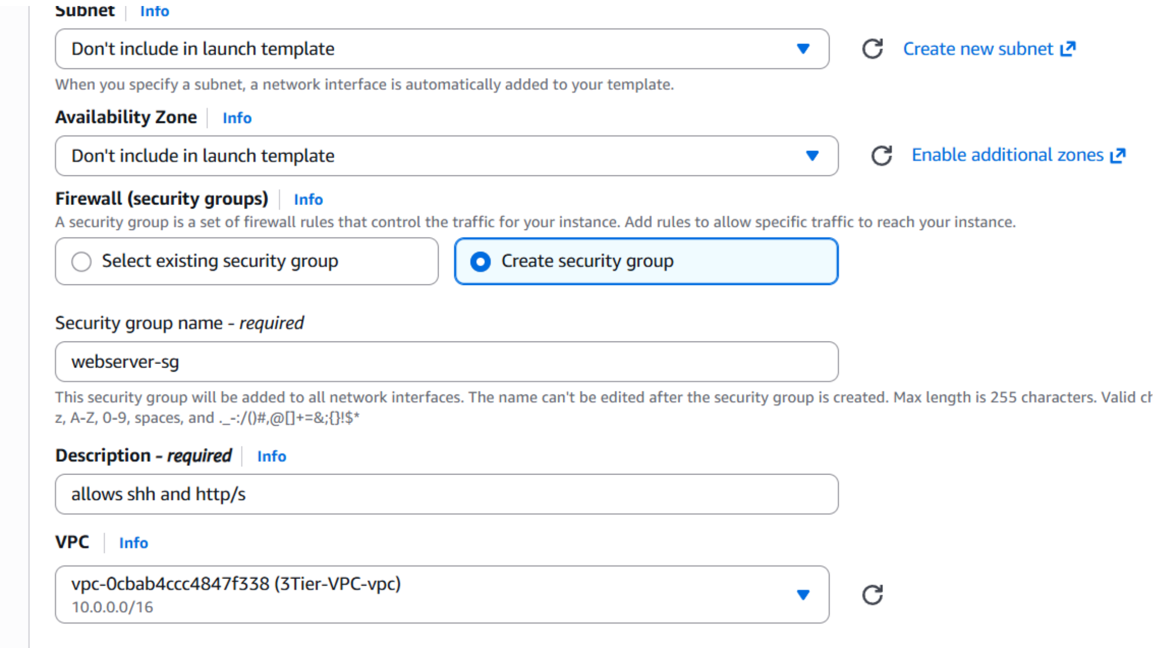
Create new key pair

Web Tier Security Group

The security group **webserver-sg** was configured with:

- SSH (22): Allowed only from my local IP
- HTTP (80) & HTTPS (443): Open to the internet

The subnet was left unselected so the Auto Scaling Group can choose AZs automatically.



Subnet Info

Don't include in launch template

Create new subnet

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

Availability Zone Info

Don't include in launch template

Enable additional zones

Firewall (security groups) Info

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

○ Select existing security group ● Create security group

Security group name - *required*

webserver-sg

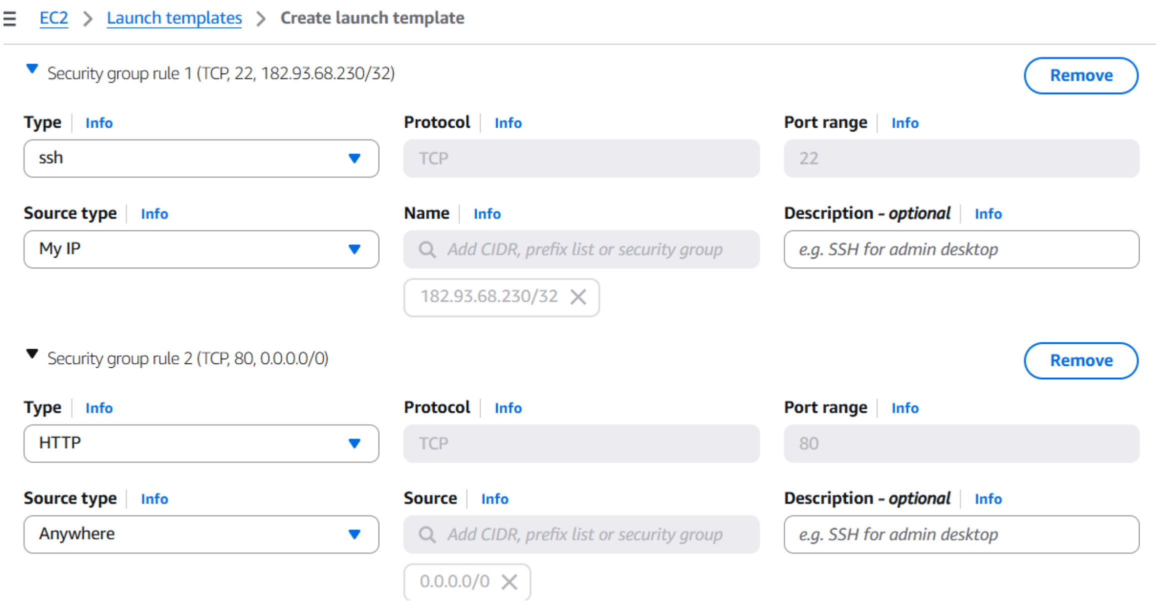
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid ch
z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* Info

allows shh and http/s

VPC Info

vpc-0cbab4ccc4847f338 (3Tier-VPC-vpc)
10.0.0.0/16



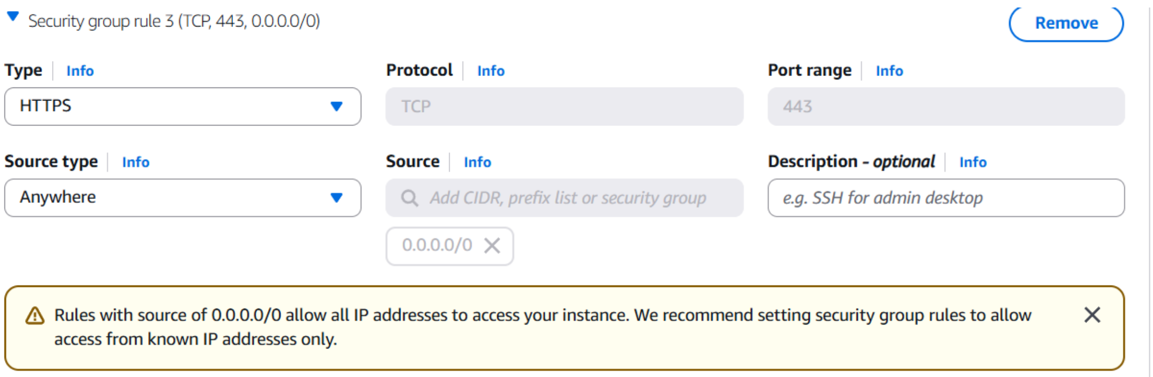
EC2 > Launch templates > Create launch template

Security group rule 1 (TCP, 22, 182.93.68.230/32)

Type: ssh	Protocol: TCP	Port range: 22
Source type: My IP	Name: Add CIDR, prefix list or security group 182.93.68.230/32	Description - *optional*: *e.g. SSH for admin desktop*

Security group rule 2 (TCP, 80, 0.0.0.0/0)

Type: HTTP	Protocol: TCP	Port range: 80
Source type: Anywhere	Source: Add CIDR, prefix list or security group 0.0.0.0/0	Description - *optional*: *e.g. SSH for admin desktop*



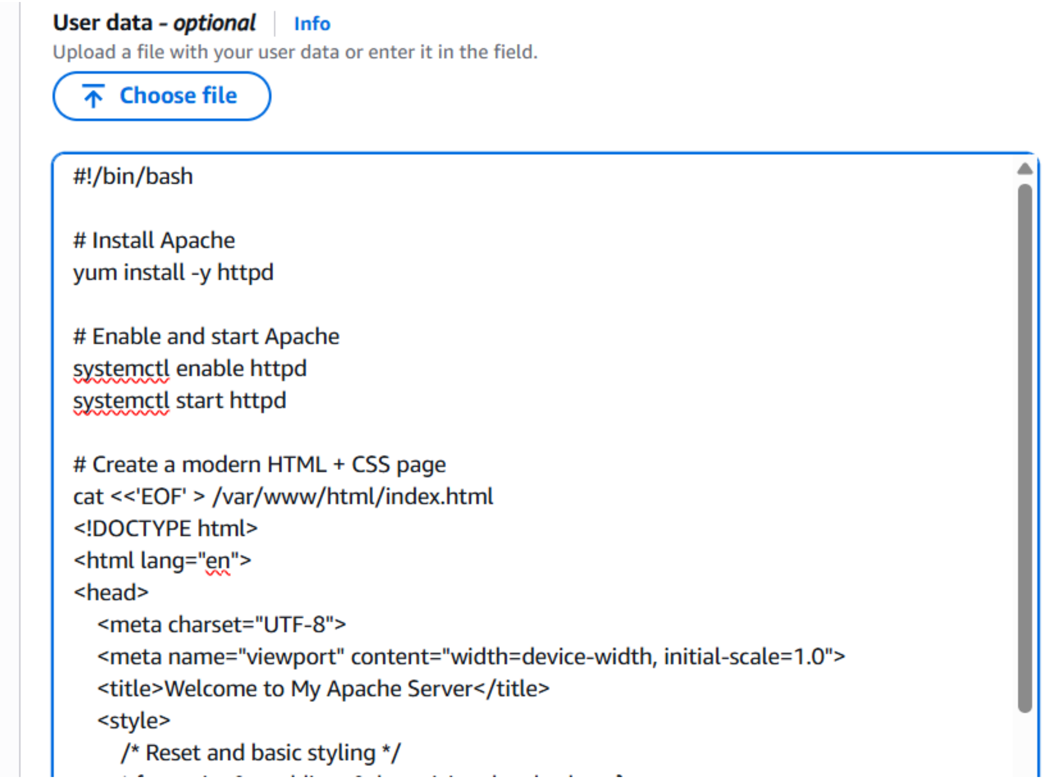
Security group rule 3 (TCP, 443, 0.0.0.0/0)

Type: HTTPS	Protocol: TCP	Port range: 443
Source type: Anywhere	Source: Add CIDR, prefix list or security group 0.0.0.0/0	Description - *optional*: *e.g. SSH for admin desktop*

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

User Data Automation

- Installs Apache webserver and deploys HTML page automatically

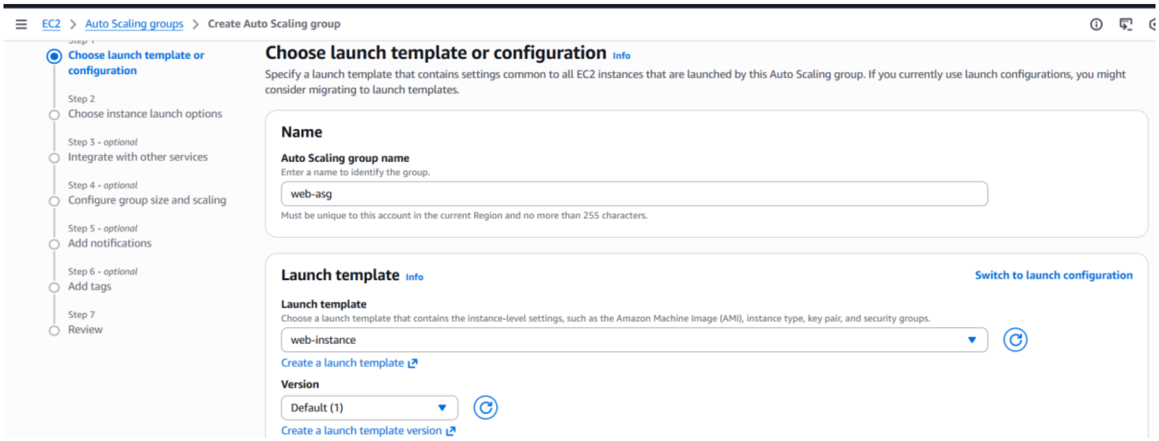


User data - *optional* | Info
Upload a file with your user data or enter it in the field.
Choose file

```
#!/bin/bash

# Install Apache
yum install -y httpd

# Enable and start Apache
systemctl enable httpd
systemctl start httpd

# Create a modern HTML + CSS page
cat <<'EOF' > /var/www/html/index.html
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Welcome to My Apache Server</title>
  <style>
    /* Reset and basic styling */
```

Auto Scaling Group

- Name: **web-asg**
- Deployed across two public subnets in separate AZs



EC2 > Auto Scaling groups > Create Auto Scaling group
● 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

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.

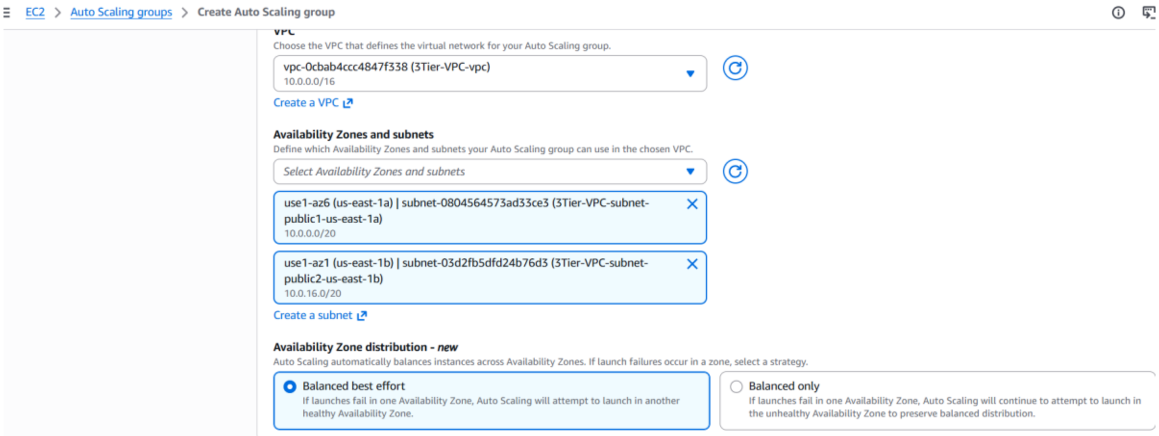
Name

Auto Scaling group name
Enter a name to identify the group.
web-asg
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.
web-instance
Create a launch template

Version
Default (1)
Create a launch template version



EC2 > Auto Scaling groups > Create Auto Scaling group

VPC

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

vpc-0cbab4ccc4847f338 (3Tier-VPC-vpc)
10.0.0.0/16

Create a VPC

Availability Zones and subnets

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

Select Availability Zones and subnets

use1-az6 (us-east-1a) | subnet-0804564573ad33ce3 (3Tier-VPC-subnet-public1-us-east-1a)
10.0.0.0/20

use1-az1 (us-east-1b) | subnet-03d2fb5dfd24b76d3 (3Tier-VPC-subnet-public2-us-east-1b)
10.0.16.0/20

Create a subnet

Availability Zone distribution - *new*

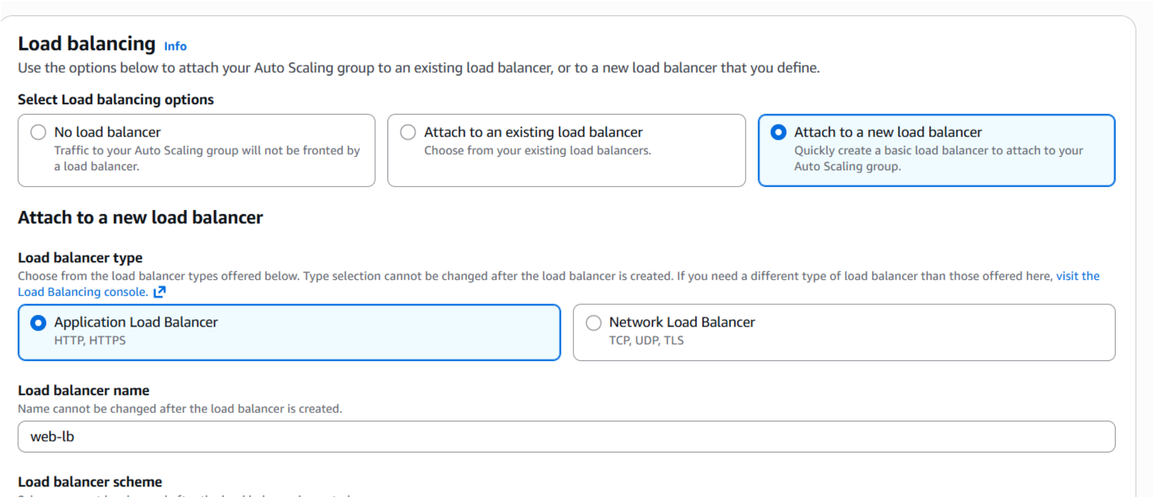
Auto Scaling automatically balances instances across Availability Zones. If launch failures occur in a zone, select a strategy.

● 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.

Elastic Load Balancer

Internet-facing ALB: **web-lb** → target group **web-tg**



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 a new load balancer

Load balancer type

Choose from the load balancer types offered below. Type selection cannot be changed after the load balancer is created. If you need a different type of load balancer than those offered here, visit the Load Balancing console.

● Application Load Balancer
HTTP, HTTPS

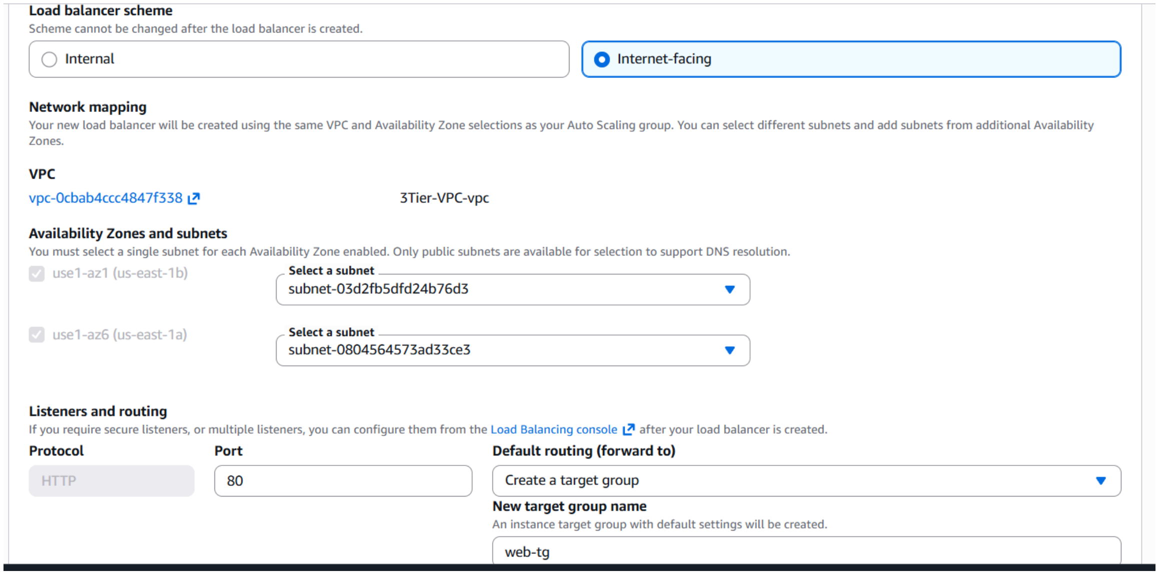
○ Network Load Balancer
TCP, UDP, TLS

Load balancer name

Name cannot be changed after the load balancer is created.

web-lb

Load balancer scheme



Load balancer scheme

Scheme cannot be changed after the load balancer is created.

○ Internal ● Internet-facing

Network mapping

Your new load balancer will be created using the same VPC and Availability Zone selections as your Auto Scaling group. You can select different subnets and add subnets from additional Availability Zones.

VPC

vpc-0cbab4ccc4847f338 3Tier-VPC-vpc

Availability Zones and subnets

You must select a single subnet for each Availability Zone enabled. Only public subnets are available for selection to support DNS resolution.

☑ use1-az1 (us-east-1b)	Select a subnet: subnet-03d2fb5dfd24b76d3
☑ use1-az6 (us-east-1a)	Select a subnet: subnet-0804564573ad33ce3

Listeners and routing

If you require secure listeners, or multiple listeners, you can configure them from the Load Balancing console after your load balancer is created.

Protocol	Port	Default routing (forward to)
HTTP	80	Create a target group

New target group name

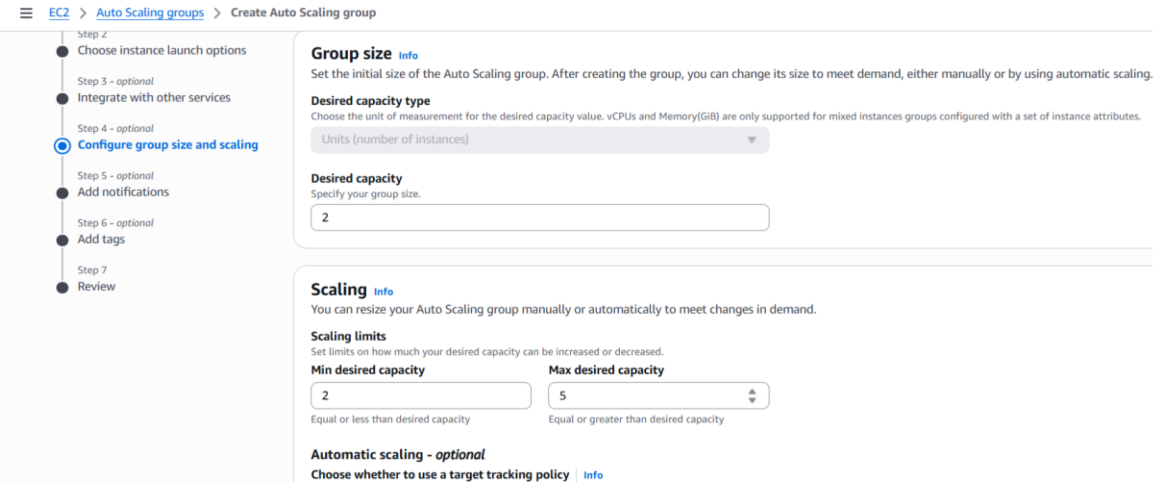
An instance target group with default settings will be created.

web-tg

Auto Scaling Policy

- **Minimum:** 2
- **Desired:** 2
- **Maximum:** 5

A target tracking policy scales instances when average CPU utilization exceeds **50%**.



☰ EC2 > Auto Scaling groups > Create Auto Scaling group

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

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.

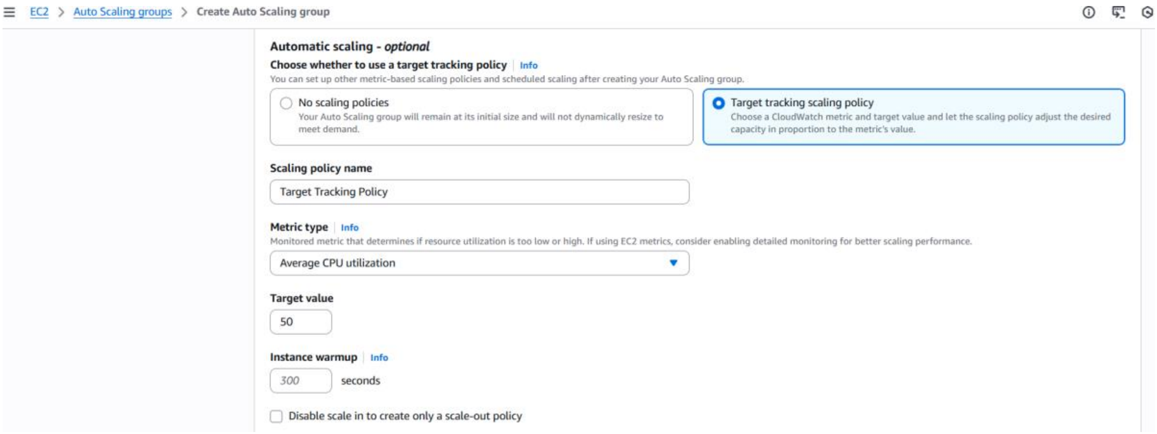
Scaling limits

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

Min desired capacity	Max desired capacity
2	5
Equal or less than desired capacity	Equal or greater than desired capacity

Automatic scaling - *optional*

Choose whether to use a target tracking policy Info



EC2 > Auto Scaling groups > Create Auto Scaling group

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
Target Tracking Policy

Metric type | Info
Monitored metric that determines if resource utilization is too low or high. If using EC2 metrics, consider enabling detailed monitoring for better scaling performance.
Average CPU utilization ▼

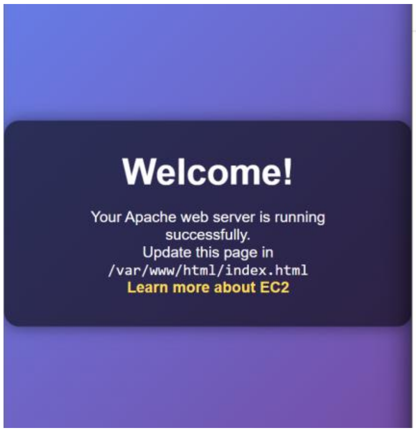
Target value
50

Instance warmup | Info
300 seconds

□ Disable scale in to create only a scale-out policy

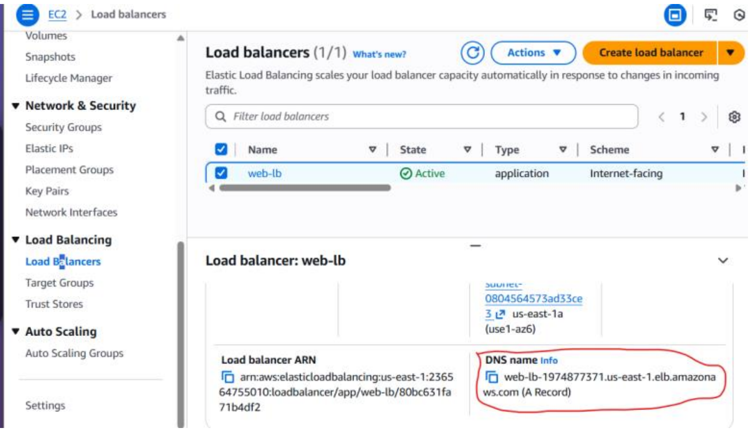
Verification

- Open ALB public DNS → website loads successfully
- SSH access restricted to local IP



Welcome!

Your Apache web server is running successfully.
Update this page in
/var/www/html/index.html
Learn more about EC2



Load balancers (1/1)

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

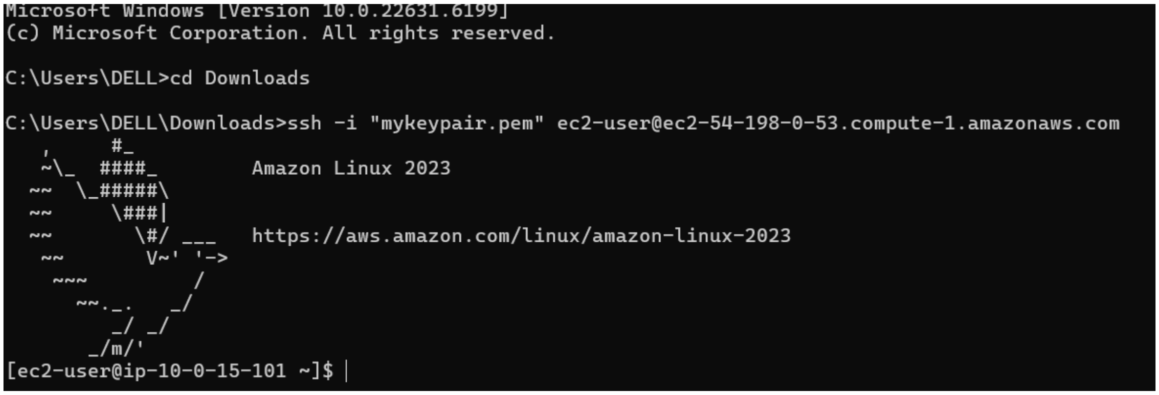
☑	Name	State	Type	Scheme
☑	web-lb	Active	application	Internet-facing

Load balancer: web-lb

subnet-0804564573ad33ce3 us-east-1a (use1-az6)

Load balancer ARN
arn:aws:elasticloadbalancing:us-east-1:236564755010:loadbalancer/app/web-lb/80bc631fa71b4df2

DNS name Info
web-lb-1974877371.us-east-1.elb.amazonaws.com (A Record)

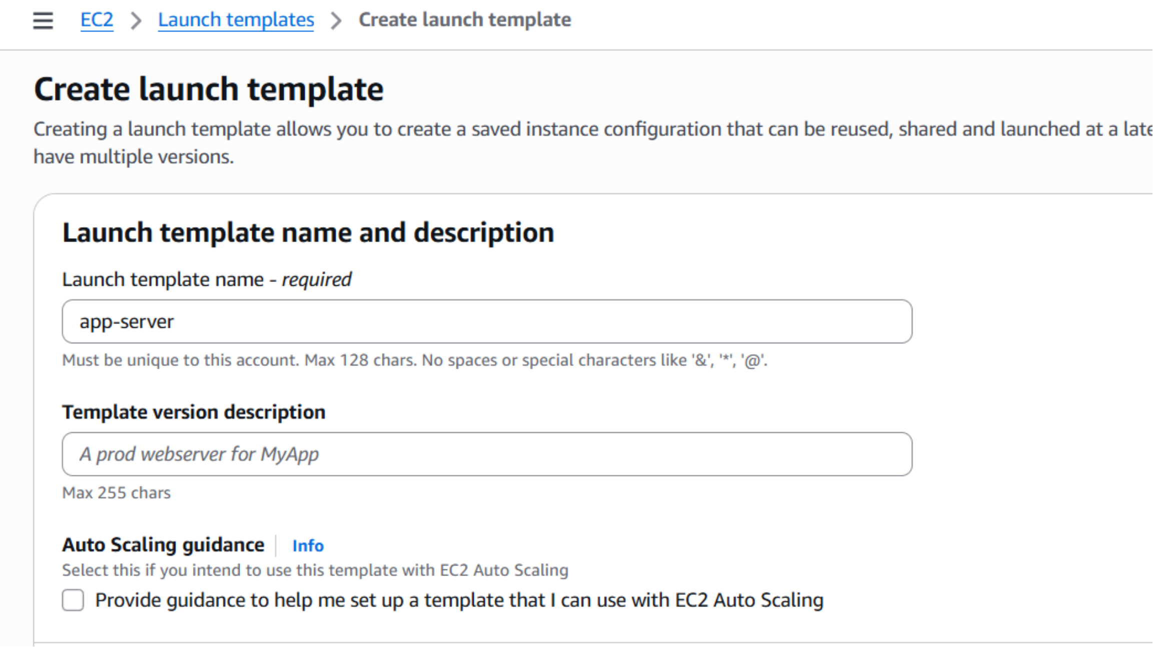


```
Microsoft Windows [Version 10.0.22631.6199]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL>cd Downloads

C:\Users\DELL\Downloads>ssh -i "mykeypair.pem" ec2-user@ec2-54-198-0-53.compute-1.amazonaws.com
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-15-101 ~]$ 
```

4. Application Tier Architecture

Launch Template

Name: **app-server** for consistent deployment



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 late have multiple versions.

Launch template name and description

Launch template name - *required*

app-server

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

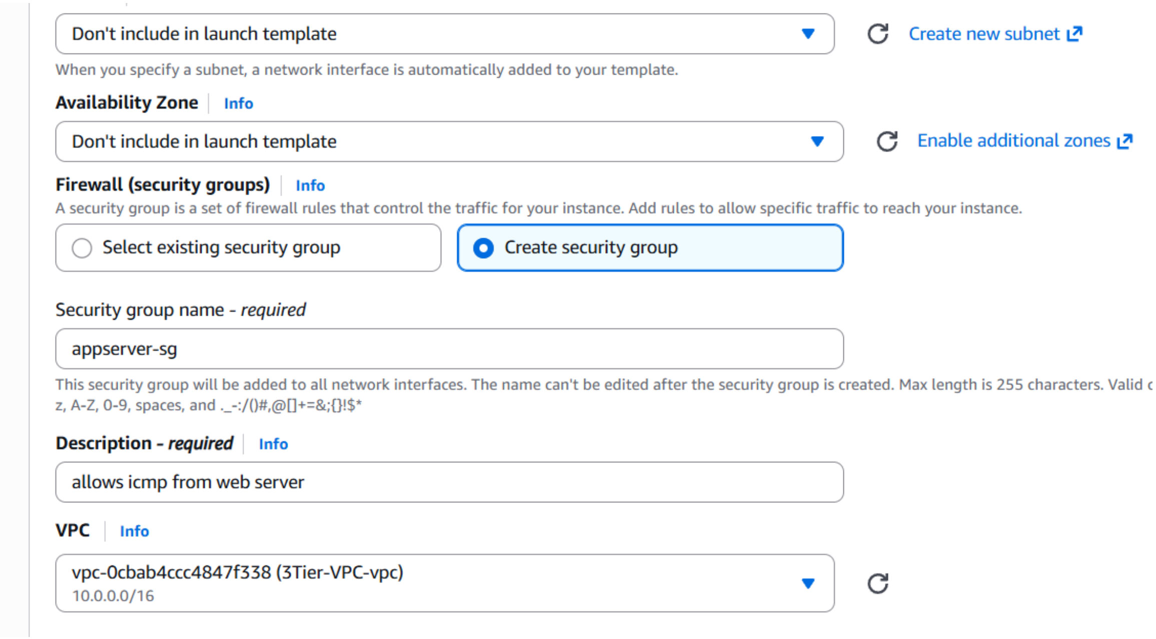
Select this if you intend to use this template with EC2 Auto Scaling

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

Application Security Group

The security group **appserver-sg** was configured with:

- ICMP (Ping) → From **webserver-sg** for connectivity test



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 group name - *required*

appserver-sg

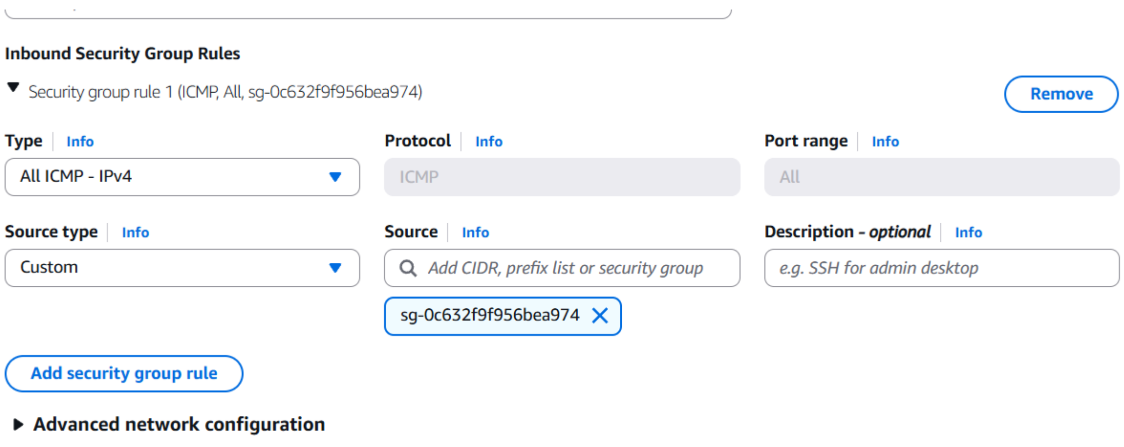
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid c
z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* | Info

allows icmp from web server

VPC | Info

vpc-0cbab4ccc4847f338 (3Tier-VPC-vpc)
10.0.0.0/16 ▼



Inbound Security Group Rules

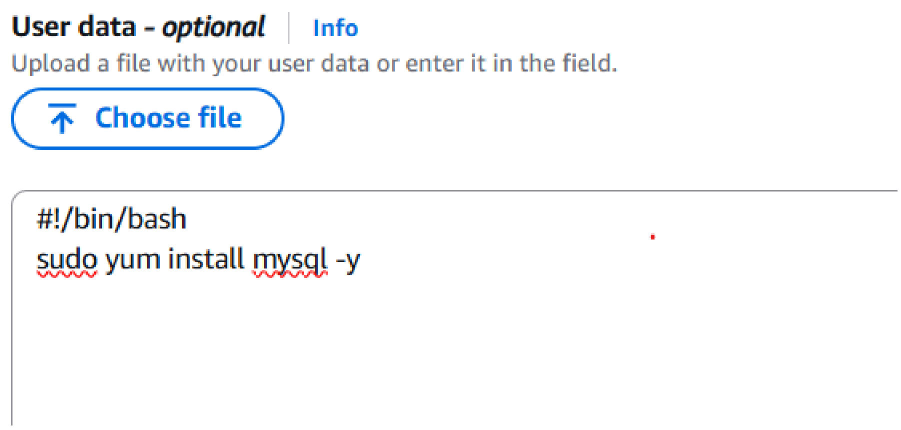
▼ Security group rule 1 (ICMP, All, sg-0c632f9f956bea974)

Type | Info	**Protocol** | Info	**Port range** | Info
All ICMP - IPv4 ▼	ICMP	All
Source type | Info	**Source** | Info	**Description - *optional*** | Info
Custom ▼	Add CIDR, prefix list or security group sg-0c632f9f956bea974 ✕	e.g. SSH for admin desktop

▶ **Advanced network configuration**

User Data Script

Installs MySQL client for communication with Database Tier



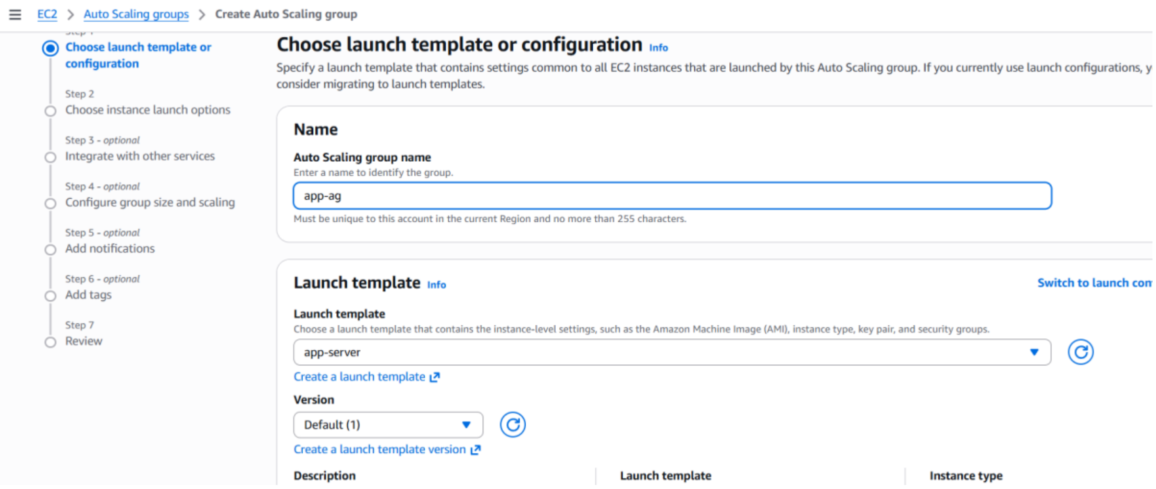
User data - *optional* Info

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

```
#!/bin/bash
sudo yum install mysql -y
```

Auto Scaling Group

- Name: **app-asg**
- Deployed across private subnets in two AZs



EC2 > Auto Scaling groups > Create Auto Scaling group
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

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, y consider migrating to launch templates.

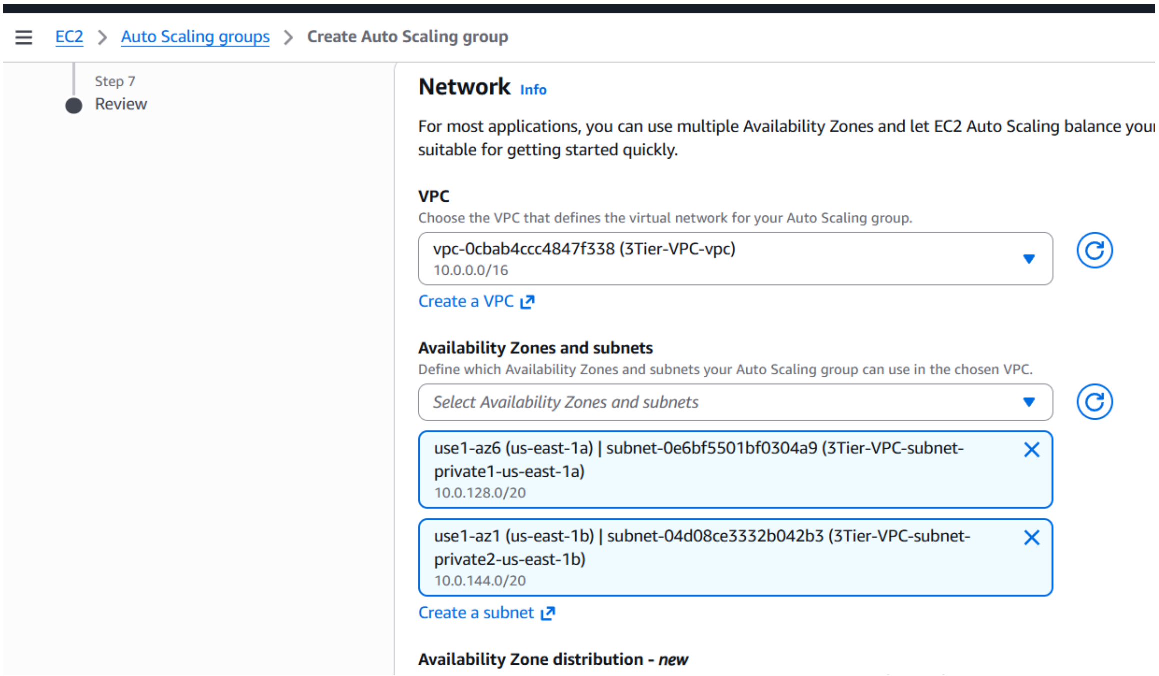
Name

Auto Scaling group name
Enter a name to identify the group.
app-ag
Must be unique to this account in the current Region and no more than 255 characters.

Launch template Info

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.
app-server

Version
Default (1)



EC2 > Auto Scaling groups > Create Auto Scaling group

Step 7
Review

Network Info

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance you
suitable for getting started quickly.

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

vpc-0cbab4ccc4847f338 (3Tier-VPC-vpc)
10.0.0.0/16

Create a VPC

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

Select Availability Zones and subnets

use1-az6 (us-east-1a) | subnet-0e6bf5501bf0304a9 (3Tier-VPC-subnet-private1-us-east-1a)
10.0.128.0/20

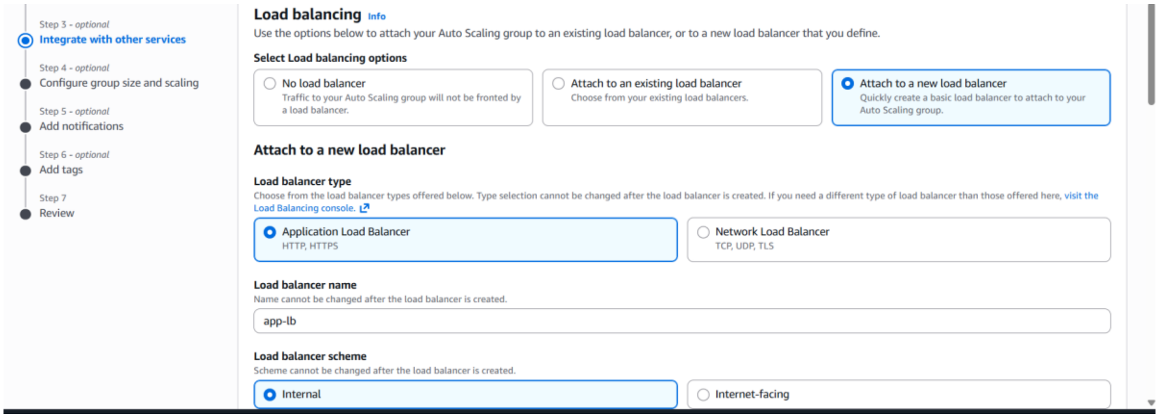
use1-az1 (us-east-1b) | subnet-04d08ce3332b042b3 (3Tier-VPC-subnet-private2-us-east-1b)
10.0.144.0/20

Create a subnet

Availability Zone distribution - *new*

Elastic Load Balancer

Internal-load balancer**: app-lb** → target group **app-tg**



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

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 a new load balancer

Load balancer type
Choose from the load balancer types offered below. Type selection cannot be changed after the load balancer is created. If you need a different type of load balancer than those offered here, visit the Load Balancing console.

● Application Load Balancer
HTTP, HTTPS

○ Network Load Balancer
TCP, UDP, TLS

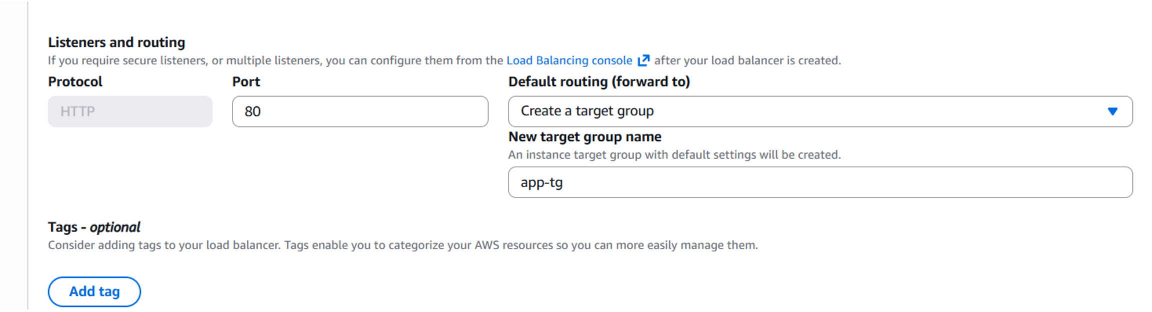
Load balancer name
Name cannot be changed after the load balancer is created.

app-lb

Load balancer scheme
Scheme cannot be changed after the load balancer is created.

● Internal

○ Internet-facing



Listeners and routing
If you require secure listeners, or multiple listeners, you can configure them from the Load Balancing console after your load balancer is created.

Protocol	Port	Default routing (forward to)
HTTP	80	Create a target group

New target group name
An instance target group with default settings will be created.

app-tg

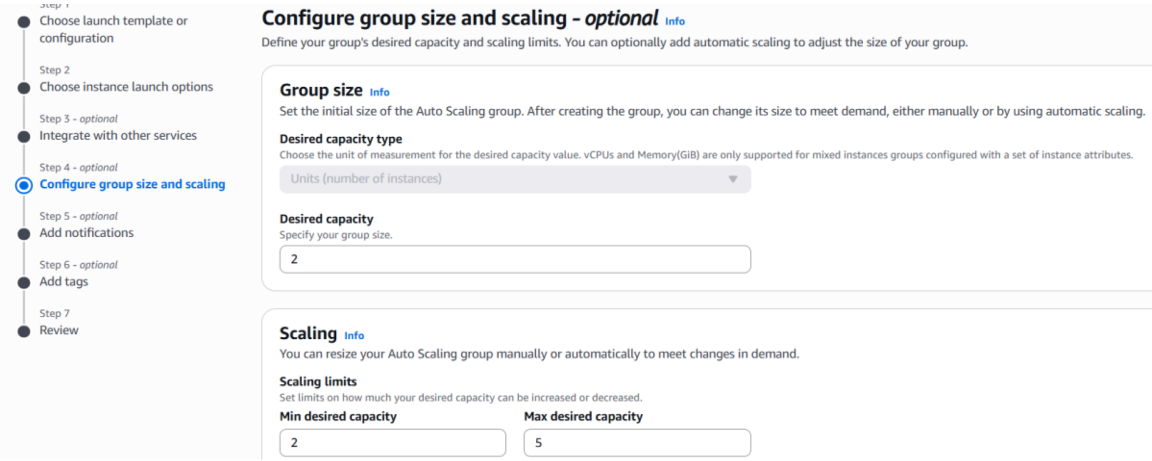
Tags - *optional*
Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them.

Add tag

Scaling Policy

- **Minimum:** 2
- **Desired:** 2
- **Maximum:** 5

A target tracking policy scales instances when average CPU utilization exceeds **50%**.



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

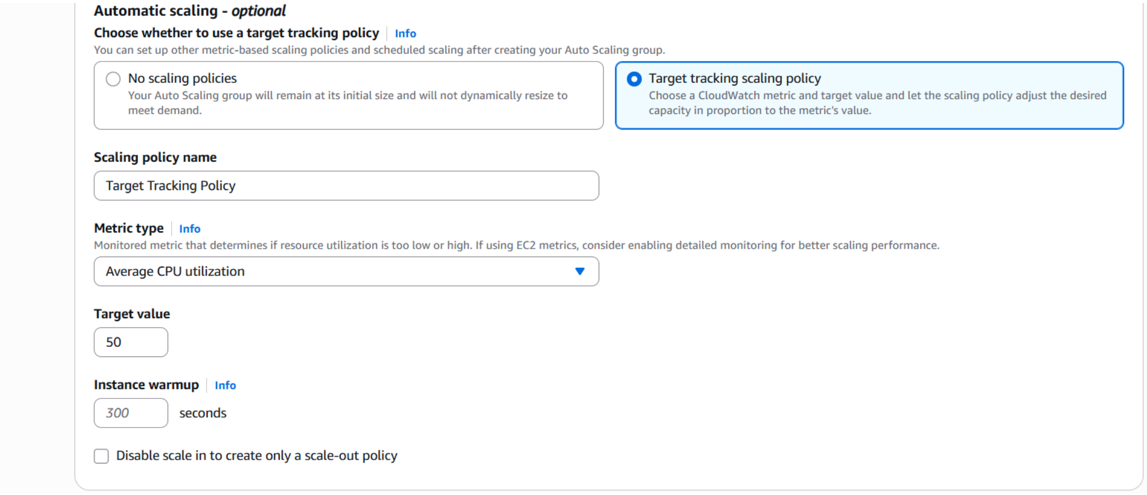
Scaling Info

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
2

Max desired capacity
5



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
Target Tracking Policy

Metric type Info
Monitored metric that determines if resource utilization is too low or high. If using EC2 metrics, consider enabling detailed monitoring for better scaling performance.
Average CPU utilization

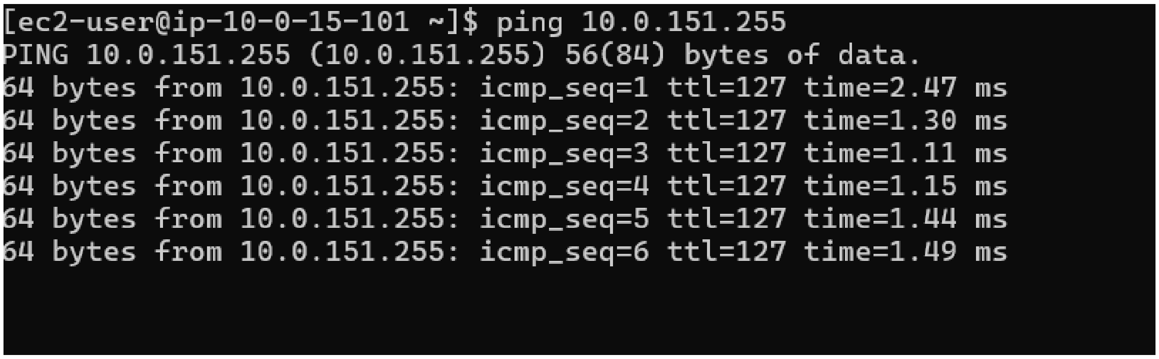
Target value
50

Instance warmup Info
300 seconds

□ Disable scale in to create only a scale-out policy

Connectivity Test

Ping from Web Tier → Application Tier successful

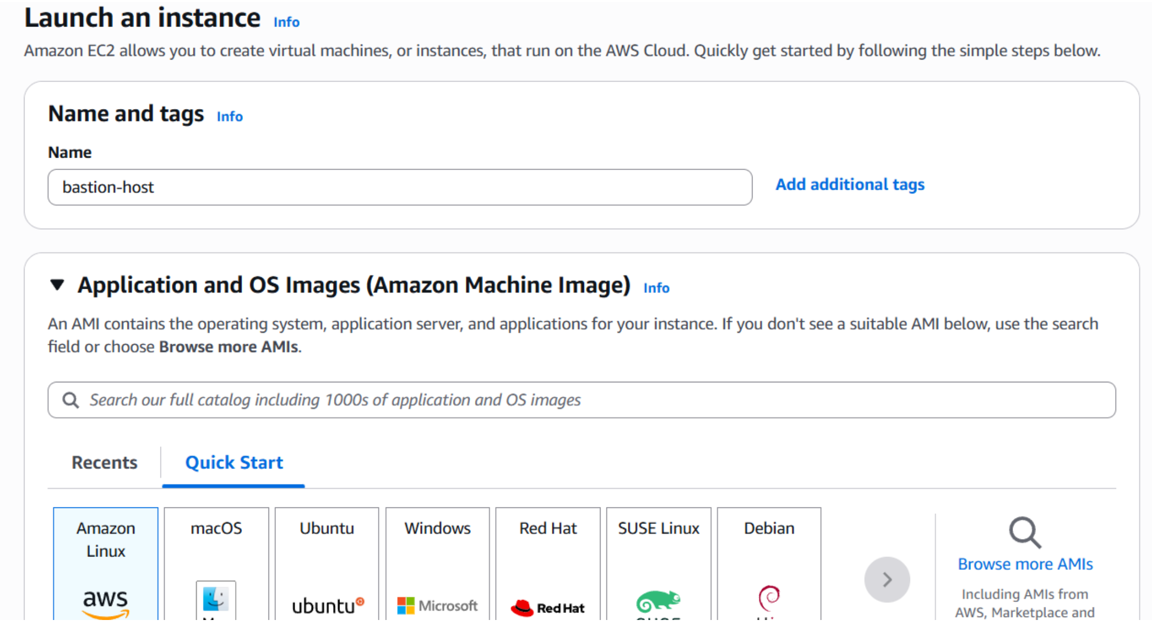


```
[ec2-user@ip-10-0-15-101 ~]$ ping 10.0.151.255
PING 10.0.151.255 (10.0.151.255) 56(84) bytes of data.
64 bytes from 10.0.151.255: icmp_seq=1 ttl=127 time=2.47 ms
64 bytes from 10.0.151.255: icmp_seq=2 ttl=127 time=1.30 ms
64 bytes from 10.0.151.255: icmp_seq=3 ttl=127 time=1.11 ms
64 bytes from 10.0.151.255: icmp_seq=4 ttl=127 time=1.15 ms
64 bytes from 10.0.151.255: icmp_seq=5 ttl=127 time=1.44 ms
64 bytes from 10.0.151.255: icmp_seq=6 ttl=127 time=1.49 ms
```

---

5. Bastion Host

- **Bastion Host Name:** bastion-host
- **AMI:** Amazon Linux 2023
- **Instance Type:** t2.micro
- **Key Pair:** Same keypair used for other EC2 instances
- **Purpose:** Acts as a secure jump server for accessing private instances



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: bastion-host

Add additional tags

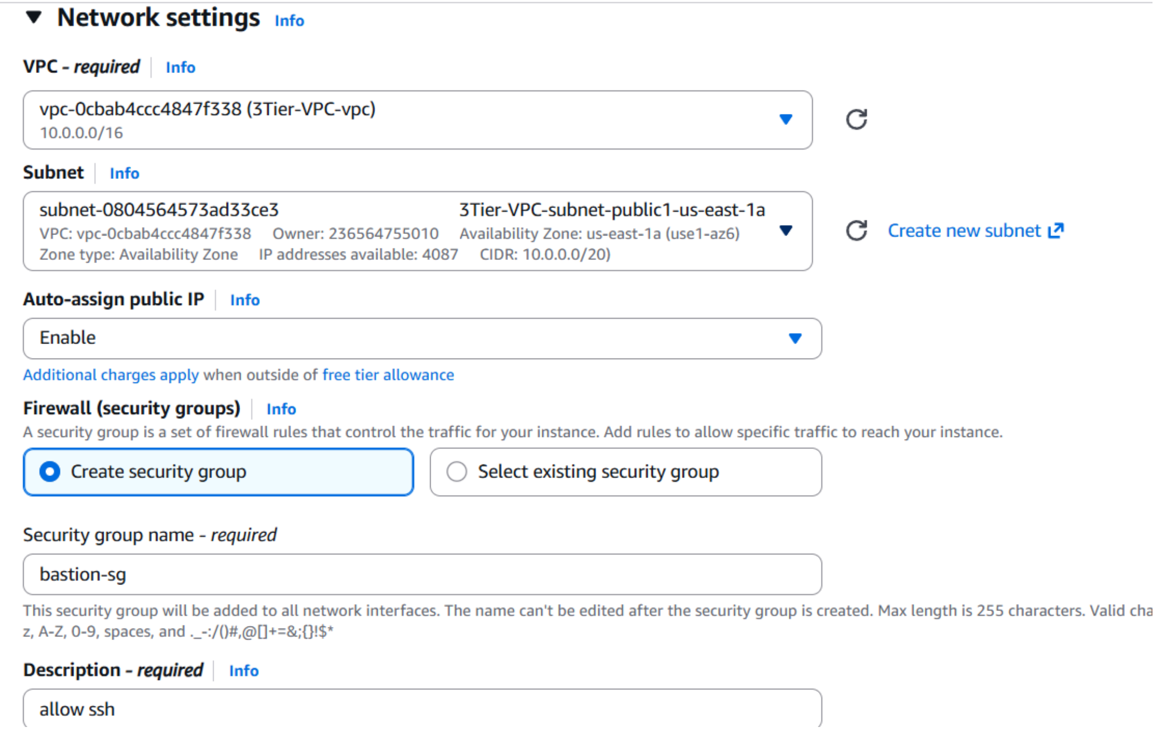
▼ Application and OS Images (Amazon Machine Image) Info

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

Security Configuration

- Placed in **public subnet (Web Tier)**
- Auto-assign public IP enabled
- Security group bastion-sg allows **SSH (22)** only from my local IP
- Inbound rules of **appserver-sg** edited to allow SSH access only from the Bastion Host **(bastion-sg)**



▼ **Network settings** Info

VPC - *required* | Info

vpc-0cbab4ccc4847f338 (3Tier-VPC-vpc)
10.0.0.0/16

Subnet | Info

subnet-0804564573ad33ce3 3Tier-VPC-subnet-public1-us-east-1a
VPC: vpc-0cbab4ccc4847f338 Owner: 236564755010 Availability Zone: us-east-1a (use1-az6)
Zone type: Availability Zone IP addresses available: 4087 CIDR: 10.0.0.0/20)

Auto-assign public IP | Info

Enable

Additional charges apply when outside of free tier allowance

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.

● Create security group ○ Select existing security group

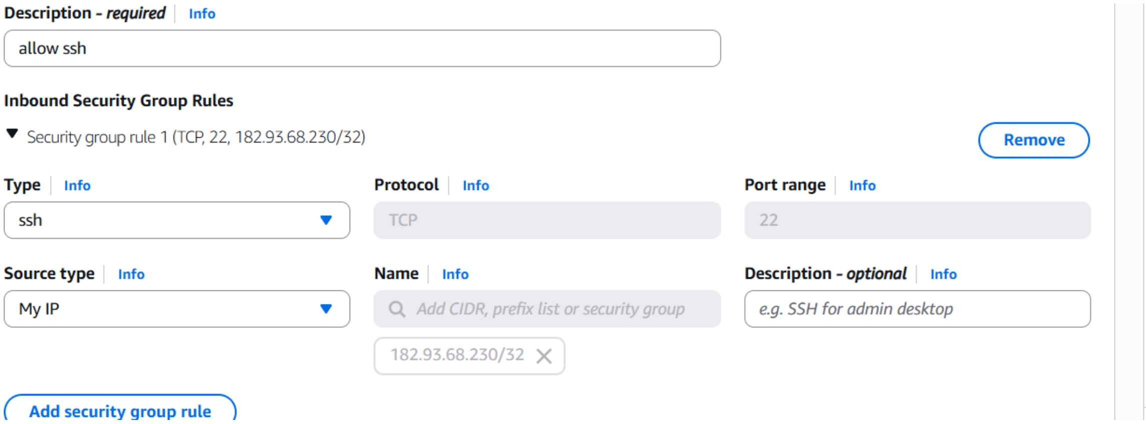
Security group name - *required*

bastion-sg

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid cha
z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* | Info

allow ssh



Description - *required* | Info

allow ssh

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 182.93.68.230/32)

Type | Info: ssh

Protocol | Info: TCP

Port range | Info: 22

Source type | Info: My IP

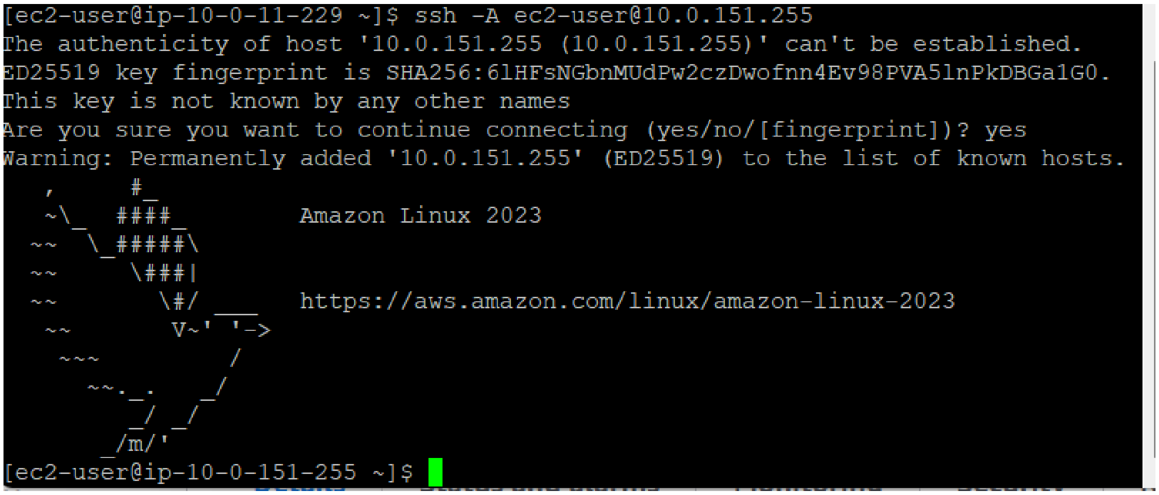
Name | Info: Add CIDR, prefix list or security group
182.93.68.230/32 ✕

Description - *optional* | Info: e.g. SSH for admin desktop

Secure SSH Access

- **SSH Agent Forwarding** implemented using **PuTTY + Pageant**
- .ppk private key securely loaded into Pageant
- PuTTY connects to Bastion Host via **public IP**
- From Bastion Host, private EC2 instances are accessed without storing private keys on the server

- Command to access private instances: **ssh -A ec2-user@[Private_IP]**



```
[ec2-user@ip-10-0-11-229 ~]$ ssh -A ec2-user@10.0.151.255
The authenticity of host '10.0.151.255 (10.0.151.255)' can't be established.
ED25519 key fingerprint is SHA256:6lHFsNGbnMUdPw2czDwofnn4Ev98PVA5lnPkDBGa1G0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.151.255' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-151-255 ~]$
```

6. Database Tier

Security Group

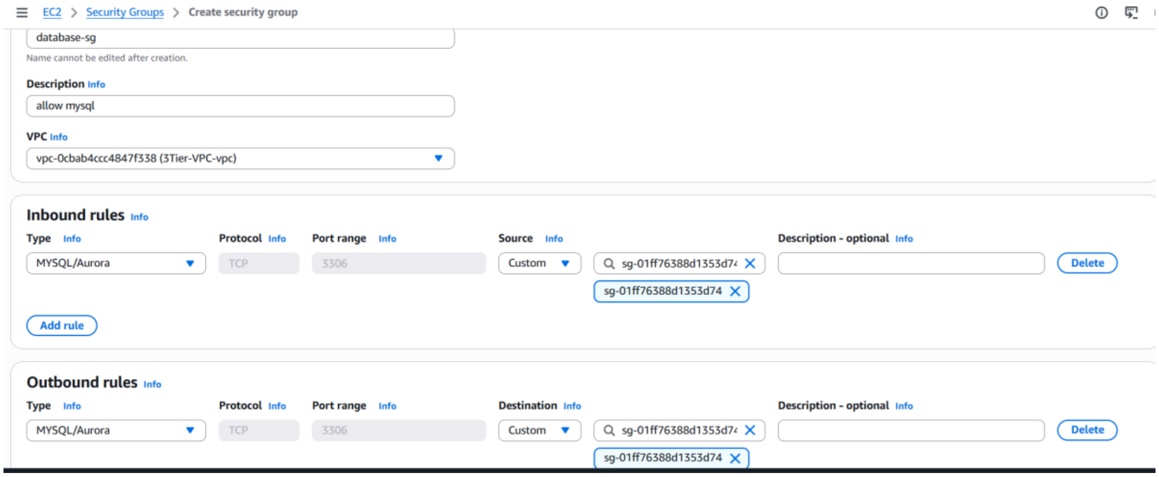
The security group **database-sg** was configured with:

- Inbound MySQL/Aurora (3306) → From **appserver-sg** only
- Outbound MySQL/Aurora (3306) → To **appserver-sg** only

And Also in **app-server-sg** define,

- Outbound MySQL/Aurora (3306) → To **database-sg** only
- Inbound MySQL/Aurora (3306) → From **database-sg** only

Purpose: Ensures secure bidirectional communication only between Application Tier and Database Tier



EC2 > Security Groups > Create security group

database-sg

Name cannot be edited after creation.

Description Info

allow mysql

VPC Info

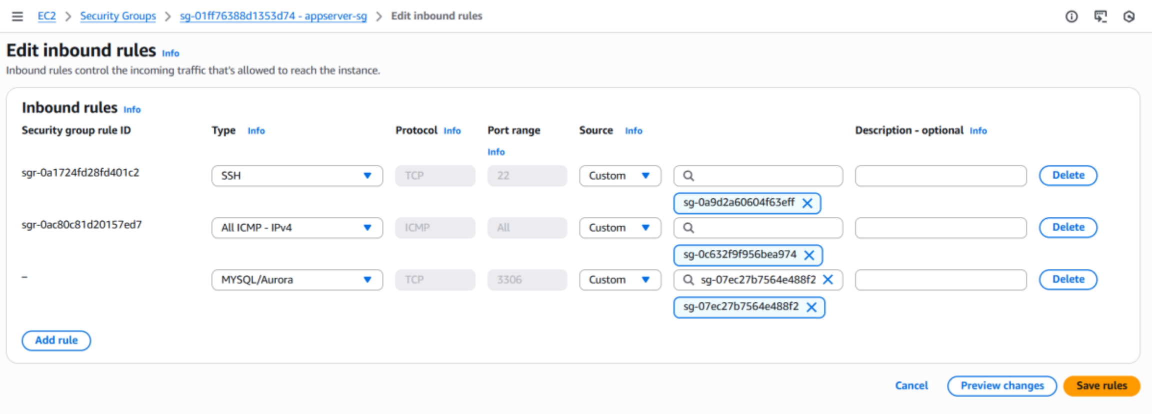
vpc-0cbab4ccc4847f338 (3Tier-VPC-vpc)

Inbound rules

Type	Protocol	Port range	Source		Description - optional
MYSQL/Aurora	TCP	3306	Custom	sg-01ff76388d1353d74 sg-01ff76388d1353d74	

Outbound rules

Type	Protocol	Port range	Destination		Description - optional
MYSQL/Aurora	TCP	3306	Custom	sg-01ff76388d1353d74 sg-01ff76388d1353d74	



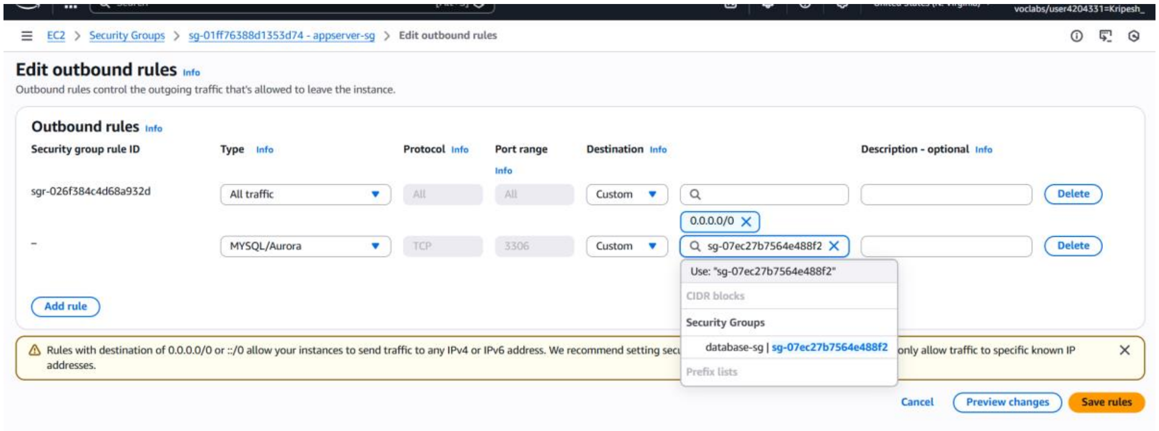
EC2 > Security Groups > sg-01ff76388d1353d74 - appserver-sg > Edit inbound rules

Edit inbound rules

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

Inbound rules

Security group rule ID	Type	Protocol	Port range	Source		Description - optional
sgr-0a1724fd28fd401c2	SSH	TCP	22	Custom	sg-0a9d2a60604f63eff	
sgr-0ac80c81d20157ed7	All ICMP - IPv4	ICMP	All	Custom	sg-0c632f9f956bea974	
–	MYSQL/Aurora	TCP	3306	Custom	sg-07ec27b7564e488f2 sg-07ec27b7564e488f2	



voclabs/user4204331=Kripesh_

EC2 > Security Groups > sg-01ff76388d1353d74 - appserver-sg > Edit outbound rules

Edit outbound rules

Outbound rules control the outgoing traffic that's allowed to leave the instance.

Outbound rules

Security group rule ID	Type	Protocol	Port range	Destination		Description - optional
sgr-026f384c4d68a932d	All traffic	All	All	Custom	0.0.0.0/0	
–	MYSQL/Aurora	TCP	3306	Custom	sg-07ec27b7564e488f2	

Use: "sg-07ec27b7564e488f2"

CIDR blocks

Security Groups

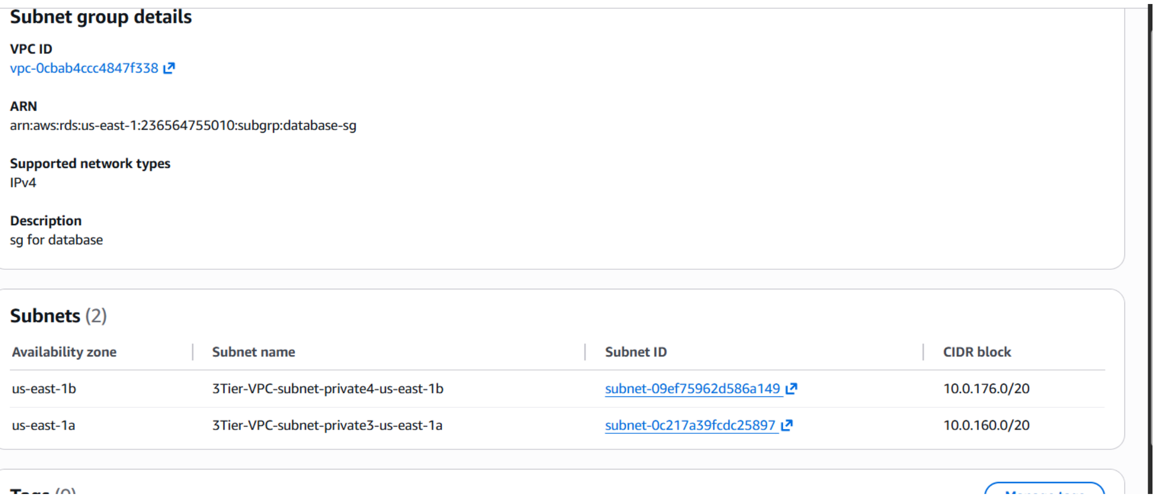
database-sg | sg-07ec27b7564e488f2

Prefix lists

⚠ Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting secu only allow traffic to specific known IP addresses.

DB Subnet Group

- Private subnets across two AZs



Subnet group details

VPC ID
vpc-0cbab4ccc4847f338

ARN
arn:aws:rds:us-east-1:236564755010:subgrp:database-sg

Supported network types
IPv4

Description
sg for database

Subnets (2)

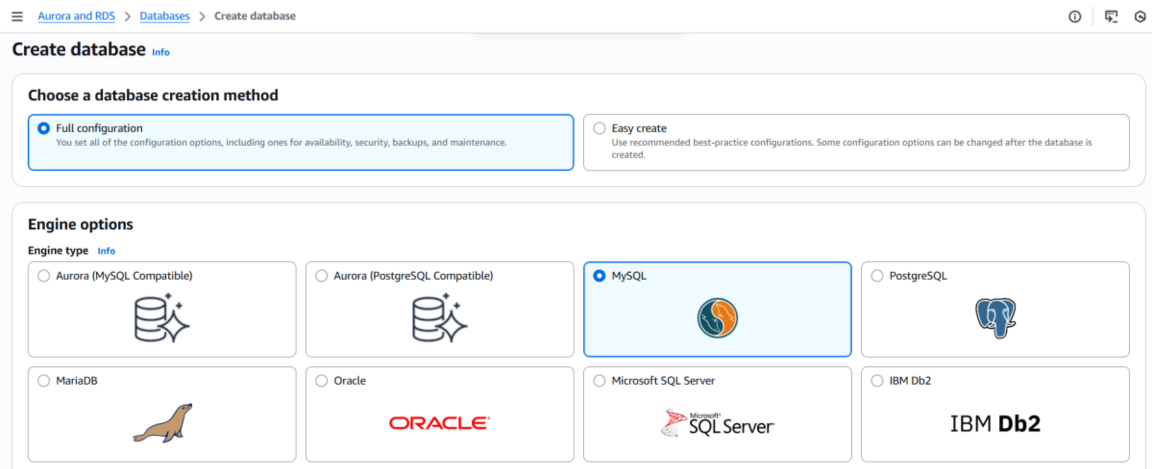
Availability zone	Subnet name	Subnet ID	CIDR block
us-east-1b	3Tier-VPC-subnet-private4-us-east-1b	subnet-09ef75962d586a149	10.0.176.0/20
us-east-1a	3Tier-VPC-subnet-private3-us-east-1a	subnet-0c217a39fcdc25897	10.0.160.0/20

Tags (0)

RDS Configuration

RDS Configuration

- **Engine:** MySQL
- **Deployment:** Single-AZ (Free tier)
- **Public Access:** No
- **DB Name:** database_1
- **Automated Backups:** Enabled
- **Associated SG:** database-sg
- **AZ:** us-east-1a



Aurora and RDS > Databases > Create database

Create database Info

Choose a database creation method

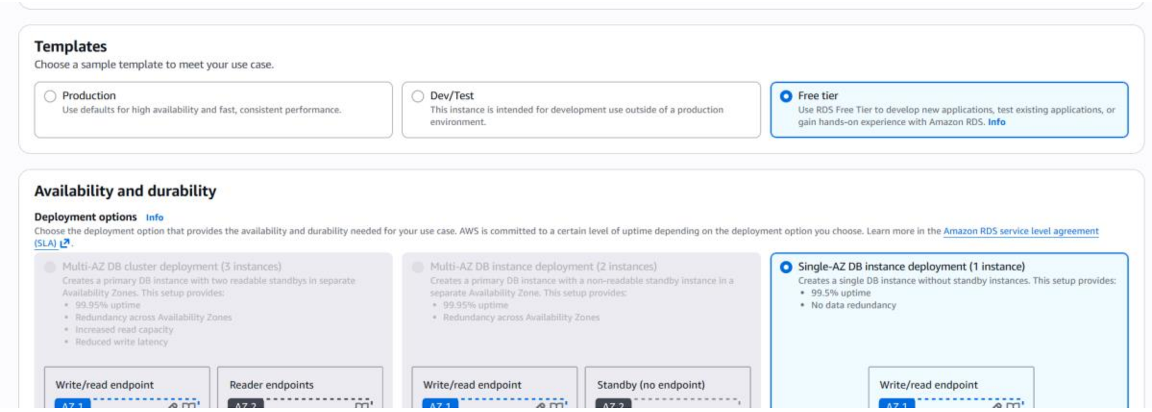
● Full configuration
You set all of the configuration options, including ones for availability, security, backups, and maintenance.

○ Easy create
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine options

Engine type Info

○ Aurora (MySQL Compatible)
○ Aurora (PostgreSQL Compatible)
● MySQL
○ PostgreSQL
○ MariaDB
○ Oracle
○ Microsoft SQL Server
○ IBM Db2



Templates

Choose a sample template to meet your use case.

○ Production
Use defaults for high availability and fast, consistent performance.

○ Dev/Test
This instance is intended for development use outside of a production environment.

● Free tier
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS. Info

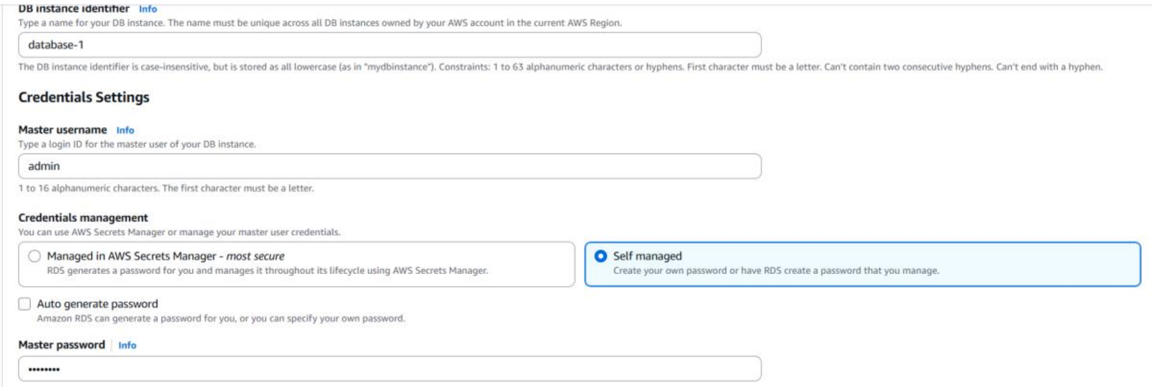
Availability and durability

Deployment options Info
Choose the deployment option that provides the availability and durability needed for your use case. AWS is committed to a certain level of uptime depending on the deployment option you choose. Learn more in the Amazon RDS service level agreement (SLA).

○ Multi-AZ DB cluster deployment (3 instances)
Creates a primary DB instance with two readable standbys in separate Availability Zones. This setup provides:
- 99.95% uptime
- Redundancy across Availability Zones
- Increased read capacity
- Reduced write latency

○ Multi-AZ DB instance deployment (2 instances)
Creates a primary DB instance with a non-readable standby instance in a separate Availability Zone. This setup provides:
- 99.95% uptime
- Redundancy across Availability Zones

● Single-AZ DB instance deployment (1 instance)
Creates a single DB instance without standby instances. This setup provides:
- 99.5% uptime
- No data redundancy



DB instance identifier Info
Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

database-1

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 63 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

Credentials Settings

Master username Info
Type a login ID for the master user of your DB instance.

admin

1 to 16 alphanumeric characters. The first character must be a letter.

Credentials management
You can use AWS Secrets Manager or manage your master user credentials.

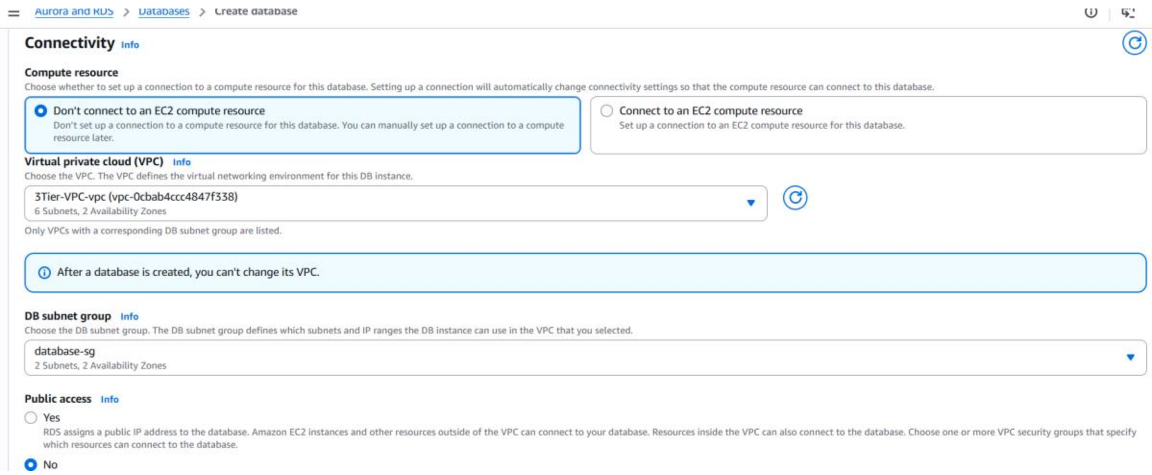
○ Managed in AWS Secrets Manager - *most secure*
RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.

● Self managed
Create your own password or have RDS create a password that you manage.

□ Auto generate password
Amazon RDS can generate a password for you, or you can specify your own password.

Master password Info

••••••••



Aurora and RDS > Databases > Create database

Connectivity Info

Compute resource

Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

● Don't connect to an EC2 compute resource
Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

○ Connect to an EC2 compute resource
Set up a connection to an EC2 compute resource for this database.

Virtual private cloud (VPC) Info

Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

3Tier-VPC-vpc (vpc-0cbab4ccc4847f338)
6 Subnets, 2 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change its VPC.

DB subnet group Info

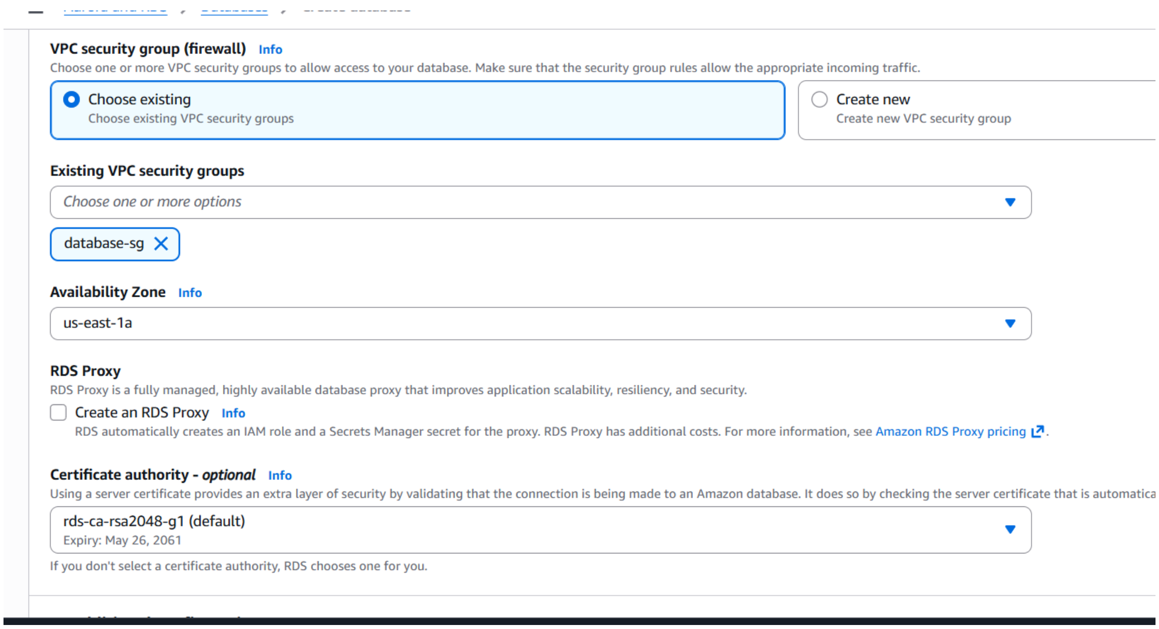
Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

database-sg
2 Subnets, 2 Availability Zones

Public access Info

○ Yes
RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.

● No



VPC security group (firewall) Info

Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

● Choose existing
Choose existing VPC security groups

○ Create new
Create new VPC security group

Existing VPC security groups

Choose one or more options

database-sg ✕

Availability Zone Info

us-east-1a

RDS Proxy

RDS Proxy is a fully managed, highly available database proxy that improves application scalability, resiliency, and security.

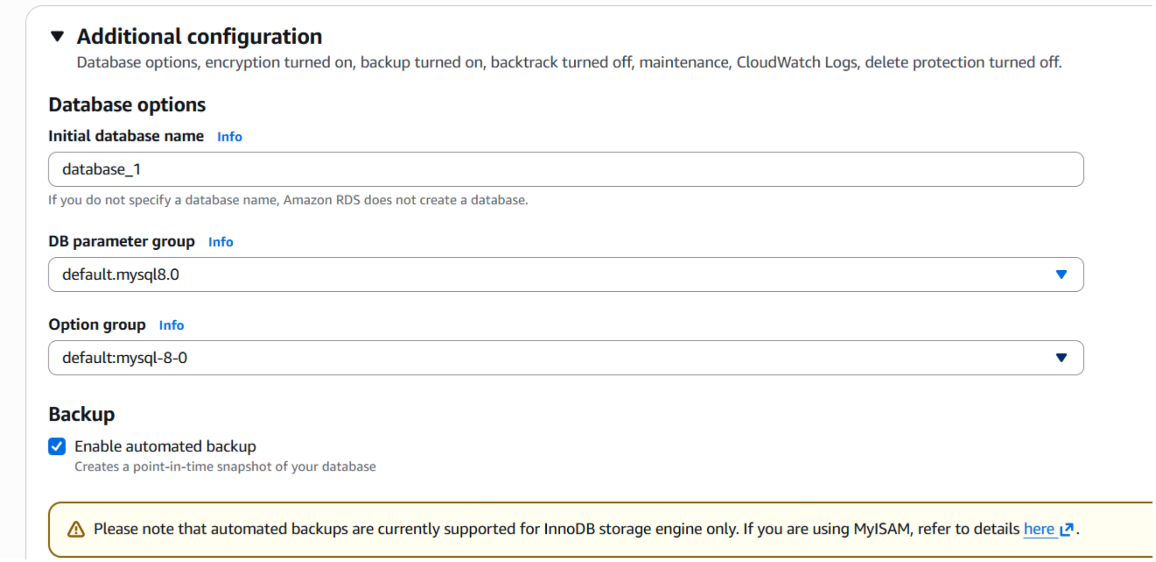
□ Create an RDS Proxy Info
RDS automatically creates an IAM role and a Secrets Manager secret for the proxy. RDS Proxy has additional costs. For more information, see Amazon RDS Proxy pricing.

Certificate authority - *optional* Info

Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatica

rds-ca-rsa2048-g1 (default)
Expiry: May 26, 2061

If you don't select a certificate authority, RDS chooses one for you.



▼ **Additional configuration**

Database options, encryption turned on, backup turned on, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned off.

Database options

Initial database name Info

database_1

If you do not specify a database name, Amazon RDS does not create a database.

DB parameter group Info

default.mysql8.0 ▼

Option group Info

default:mysql-8-0 ▼

Backup

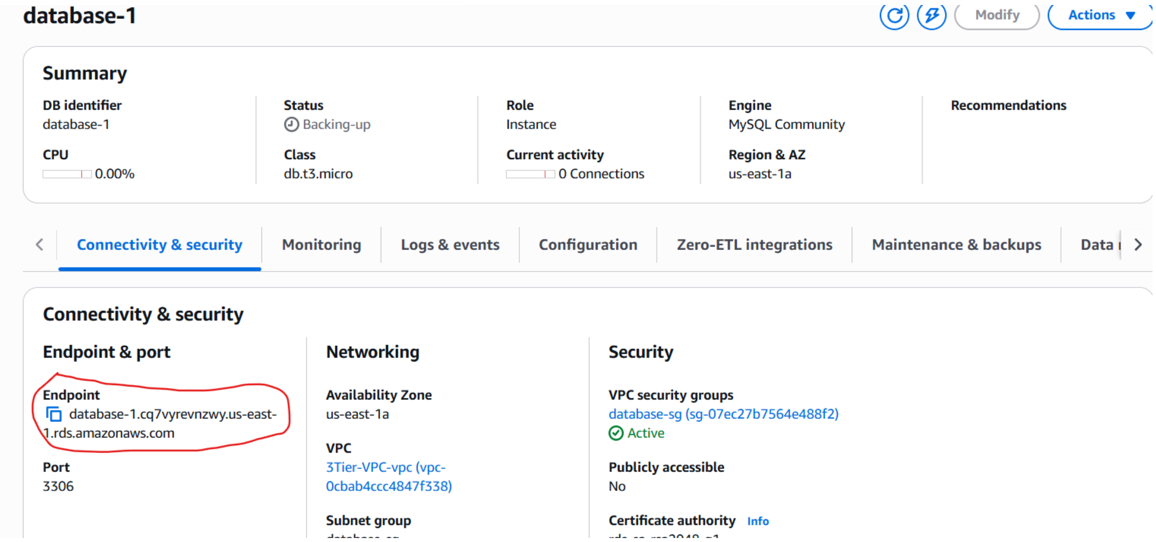
☑ Enable automated backup

Creates a point-in-time snapshot of your database

⚠ Please note that automated backups are currently supported for InnoDB storage engine only. If you are using MyISAM, refer to details here.

Database Connectivity Test

The endpoint (highlighted in red) is the unique address that the Application Tier servers use to connect to the database layer.



database-1

Summary

DB identifier	Status	Role	Engine	Recommendations
database-1	Backing-up	Instance	MySQL Community	
CPU	**Class**	**Current activity**	**Region & AZ**	
0.00%	db.t3.micro	0 Connections	us-east-1a	

Connectivity & security

Endpoint & port

Endpoint
database-1.cq7vyrevnzwy.us-east-1.rds.amazonaws.com

Port
3306

Networking

Availability Zone
us-east-1a

VPC
3Tier-VPC-vpc (vpc-0cbab4ccc4847f338)

Subnet group

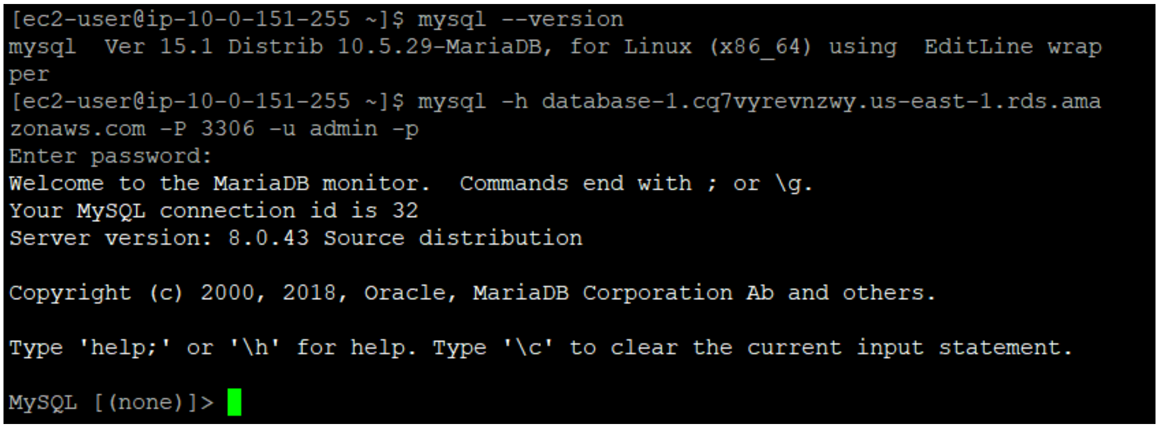
Security

VPC security groups
database-sg (sg-07ec27b7564e488f2)
✓ Active

Publicly accessible
No

Certificate authority Info

From Application Tier: **mysql -h [endpoint] -u admin –p**



```
[ec2-user@ip-10-0-151-255 ~]$ mysql --version
mysql  Ver 15.1 Distrib 10.5.29-MariaDB, for Linux (x86_64) using  EditLine wrap
per
[ec2-user@ip-10-0-151-255 ~]$ mysql -h database-1.cq7vyrevnzwy.us-east-1.rds.ama
zonaws.com -P 3306 -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 32
Server version: 8.0.43 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

- Successful login confirms Bastion → App Tier → Database Tier workflow

---

7. Key Learnings & Challenges

- Implemented **high availability** using **multi-AZ deployment**.
- Configured **secure private subnet communication** using **NAT Gateway**.
- Learned **Auto Scaling policies** and **ALB configuration**.
- Secured **private instance access** using **Bastion Host** and **SSH Agent Forwarding**.

---

8. Conclusion

This project demonstrates a **production-style AWS 3-Tier Architecture** with focus on:

- **High Availability:** Multi-AZ deployment
- **Security:** SG isolation, no public database access, Bastion host for secure private access
- **Scalability:** Auto Scaling Groups & Load Balancers
- **Automation:** Launch templates + user data scripts