PROJECT - 1
3 - TIER ARCHITECTURE

Name: Ponduru venu gopal rao

Architecture Overview

The 3-tier architecture is a way of structuring software so that different parts of the system handle different jobs. This separation makes the system easier to manage, more secure, and better at handling growth.

- **Web Tier (Presentation Layer):** This is the part users interact with—like a website or app interface. It’s responsible for displaying information and taking user input.
- **Application Tier (Logic Layer):** This is the "brain" of the system. It processes requests, makes decisions, and moves data between the user interface and the database.
- **Database Tier (Data Layer):** This is where all the important data is stored securely. Only the application tier talks to it directly, keeping things organized and safe

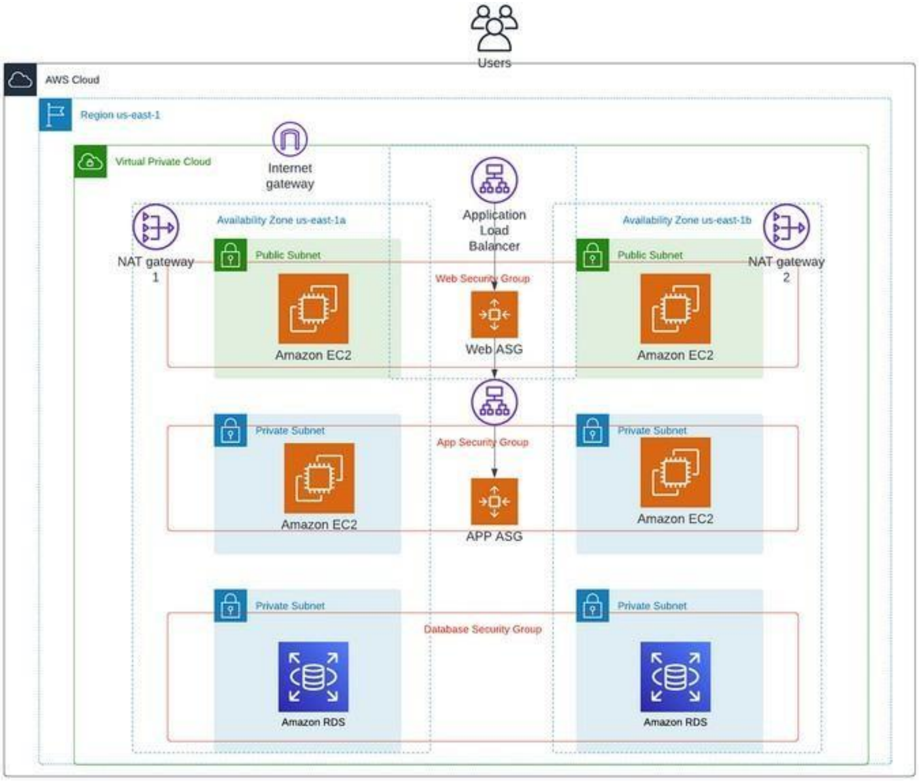


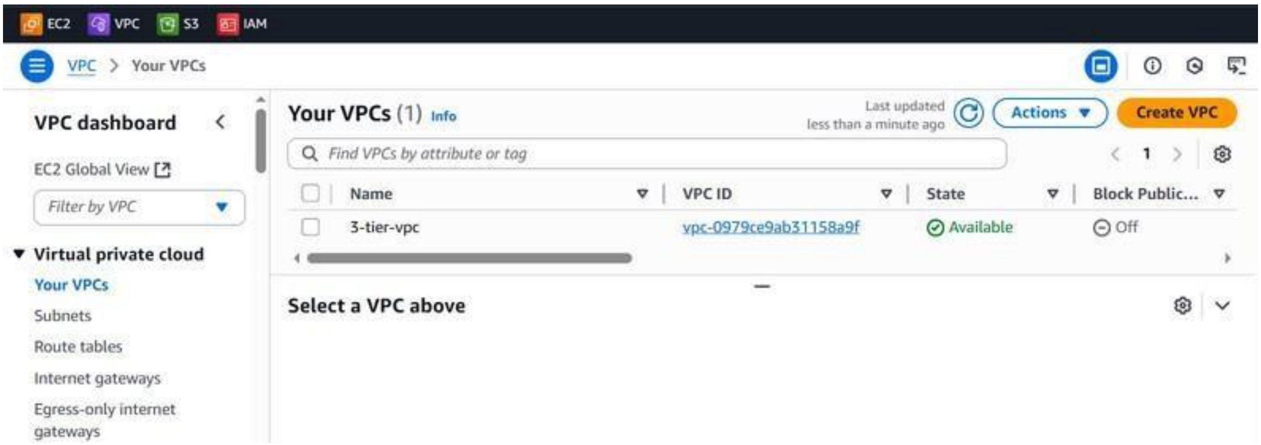
Figure: 3 - Tier Architecture

Steps to Create the 3-Tier Architecture:

1. Create VPC, Subnets – 6, Internet gate way – 1, Route tables – 2, Nat gate way – 1.
2. Launch an EC2 instance.
3. Create Load Balancer
4. Create an AMI (image).
5. Create Autoscaling group, Create launch template.
6. Create Subnet group.
7. Create Database (RDS).
8. Establish connection.

Step: 1 Create VPC and its components.

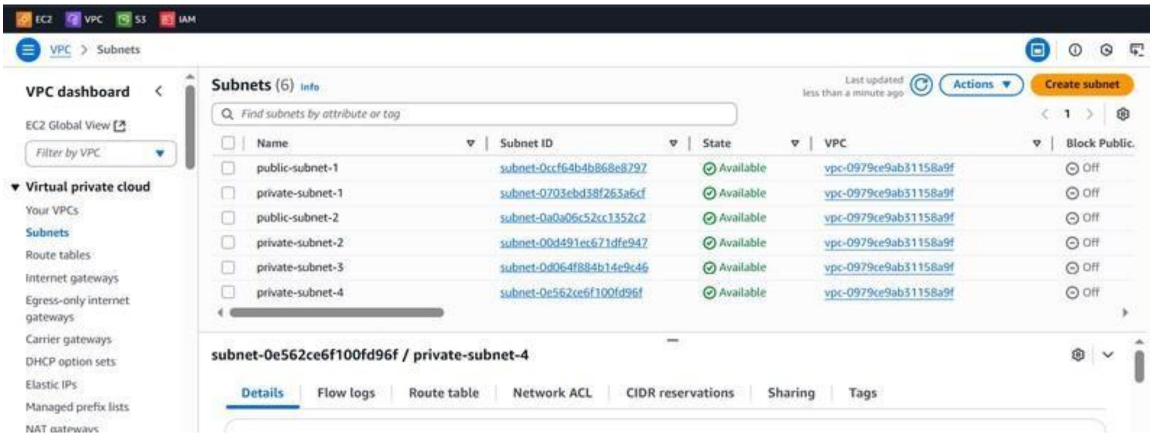
1. Create VPC:



Your VPCs (1) Info

Name	VPC ID	State	Block Public...
3-tier-vpc	vpc-0979ce9ab31158a9f	Available	Off

2. Subnet Setup: 2 Public, 4 Private

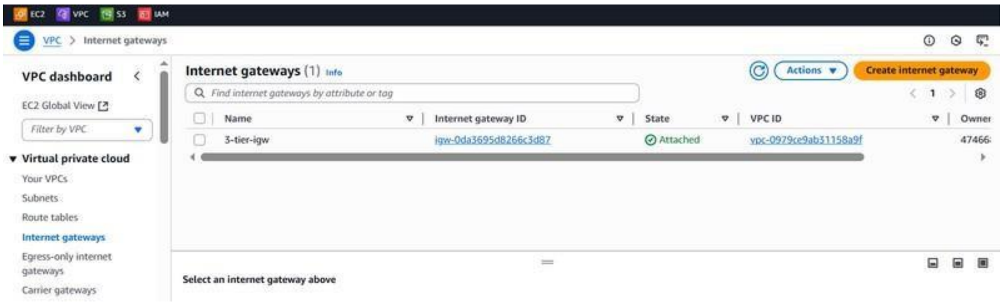


Subnets (6) Info

Name	Subnet ID	State	VPC	Block Public.
public-subnet-1	subnet-0ccf64b4b868e8797	Available	vpc-0979ce9ab31158a9f	Off
private-subnet-1	subnet-0703ebd38f263a6cf	Available	vpc-0979ce9ab31158a9f	Off
public-subnet-2	subnet-0a0a06c52cc1352c2	Available	vpc-0979ce9ab31158a9f	Off
private-subnet-2	subnet-00d491ec671dfe947	Available	vpc-0979ce9ab31158a9f	Off
private-subnet-3	subnet-0d064f884b14e9c46	Available	vpc-0979ce9ab31158a9f	Off
private-subnet-4	subnet-0e562ce6f100fd96f	Available	vpc-0979ce9ab31158a9f	Off

subnet-0e562ce6f100fd96f / private-subnet-4

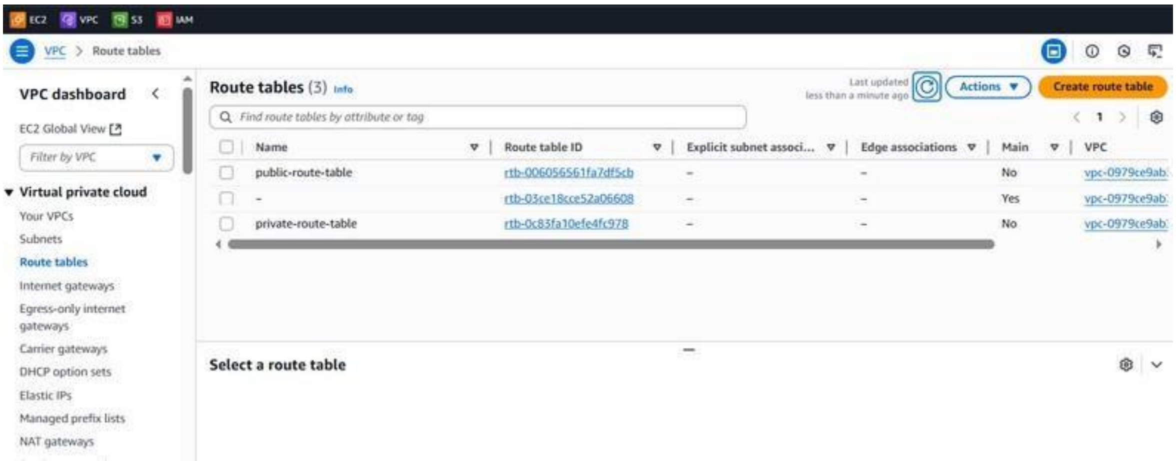
3. Internet Gateway Setup and attach to new VPC.



Internet gateways (1) Info

Name	Internet gateway ID	State	VPC ID	Owner
3-tier-igw	igw-0da3695d8266c3d87	Attached	vpc-0979ce9ab31158a9f	47466

4. Create Route tables

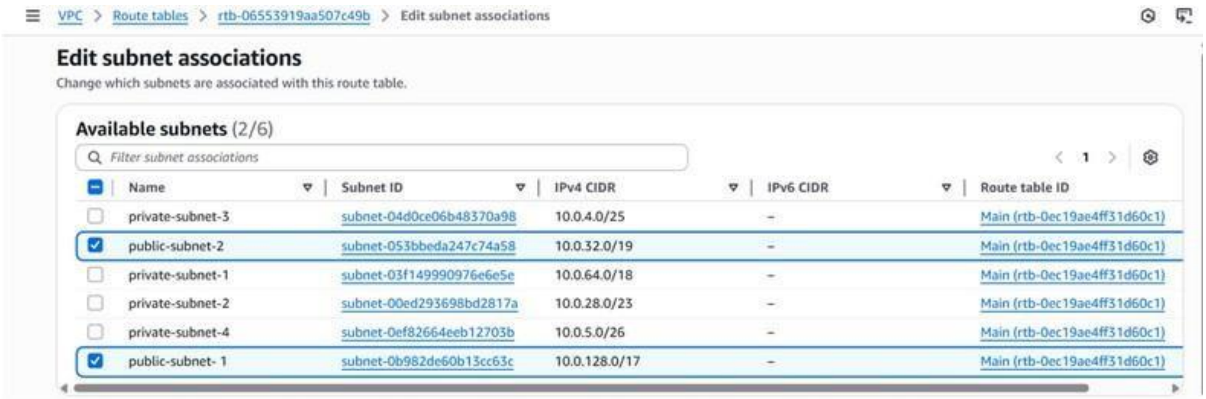


Route tables (3) Info

	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
□	public-route-table	rtb-006056561fa7df5cb	–	–	No	vpc-0979ce9ab
□	-	rtb-03ce18cce52a06608	–	–	Yes	vpc-0979ce9ab
□	private-route-table	rtb-0c83fa10efe4fc978	–	–	No	vpc-0979ce9ab

Select a route table

5. Associate Subnets with Route Tables

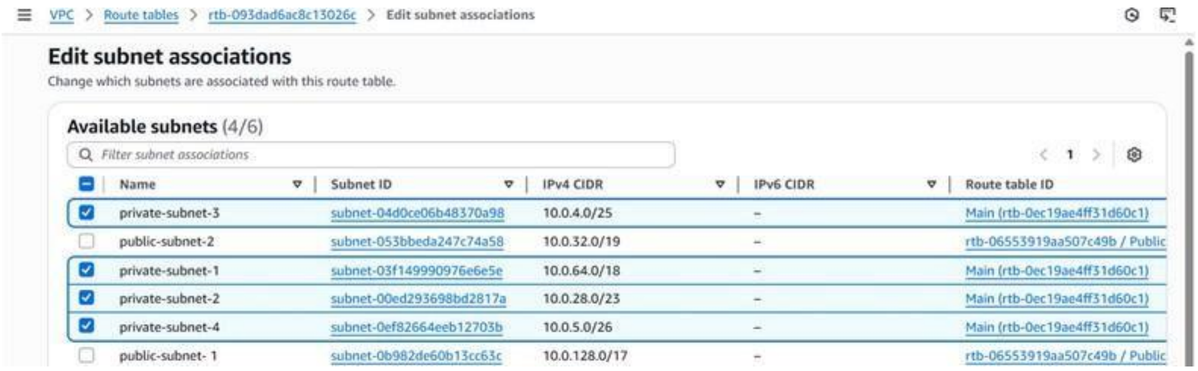

VPC > Route tables > rtb-06553919aa507c49b > Edit subnet associations
Filter subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/6)

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
□	private-subnet-3	subnet-04d0ce06b48370a98	10.0.4.0/25	–	Main (rtb-0ec19ae4ff31d60c1)
☑	public-subnet-2	subnet-053bbeda247c74a58	10.0.32.0/19	–	Main (rtb-0ec19ae4ff31d60c1)
□	private-subnet-1	subnet-03f149990976e6e5e	10.0.64.0/18	–	Main (rtb-0ec19ae4ff31d60c1)
□	private-subnet-2	subnet-00ed293698bd2817a	10.0.28.0/23	–	Main (rtb-0ec19ae4ff31d60c1)
□	private-subnet-4	subnet-0ef82664eeb12703b	10.0.5.0/26	–	Main (rtb-0ec19ae4ff31d60c1)
☑	public-subnet- 1	subnet-0b982de60b13cc63c	10.0.128.0/17	–	Main (rtb-0ec19ae4ff31d60c1)


VPC > Route tables > rtb-093dad6ac8c13026c > Edit subnet associations
Filter subnet associations

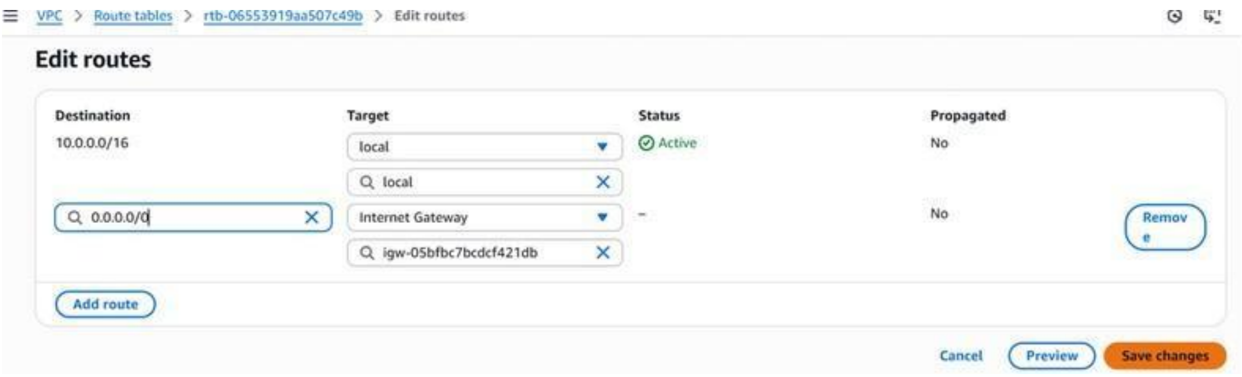
Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (4/6)

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☑	private-subnet-3	subnet-04d0ce06b48370a98	10.0.4.0/25	–	Main (rtb-0ec19ae4ff31d60c1)
□	public-subnet-2	subnet-053bbeda247c74a58	10.0.32.0/19	–	rtb-06553919aa507c49b / Public
☑	private-subnet-1	subnet-03f149990976e6e5e	10.0.64.0/18	–	Main (rtb-0ec19ae4ff31d60c1)
☑	private-subnet-2	subnet-00ed293698bd2817a	10.0.28.0/23	–	Main (rtb-0ec19ae4ff31d60c1)
☑	private-subnet-4	subnet-0ef82664eeb12703b	10.0.5.0/26	–	Main (rtb-0ec19ae4ff31d60c1)
□	public-subnet- 1	subnet-0b982de60b13cc63c	10.0.128.0/17	–	rtb-06553919aa507c49b / Public

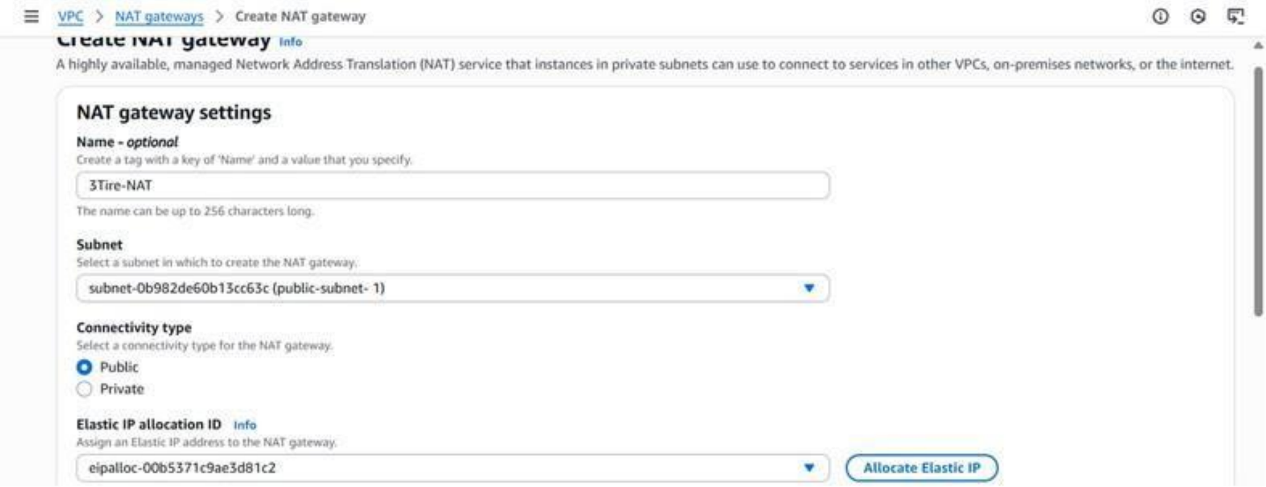
6. Attach Public Route Table to Internet Gateway (via Edit Routes)



Edit routes

Destination	Target	Status	Propagated	
10.0.0.0/16	local local	Active	No	
0.0.0.0/0	Internet Gateway igw-05bfbc7bcdcf421db	-	No	Remove

7. Create NAT gateway



VPC > NAT gateways > Create NAT gateway

Create NAT gateway Info

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

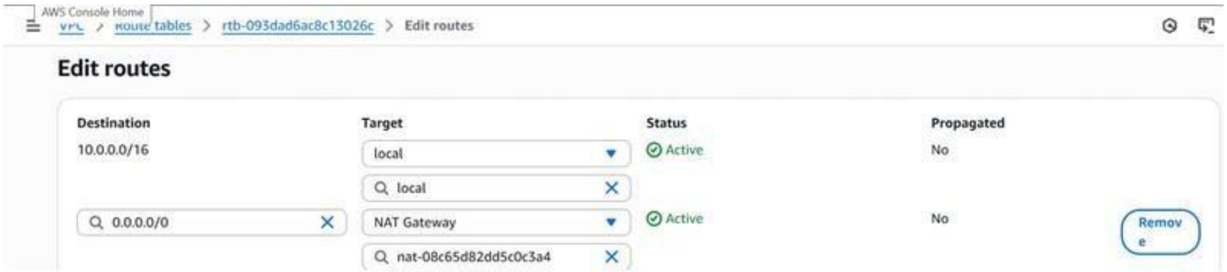
Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
3Tire-NAT
The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.
subnet-0b982de60b13cc63c (public-subnet- 1)

Connectivity type
Select a connectivity type for the NAT gateway.
● Public
○ Private

Elastic IP allocation ID Info
Assign an Elastic IP address to the NAT gateway.
eipalloc-00b5371c9ae3d81c2

8. Attach Private Route Table to NAT Gateway



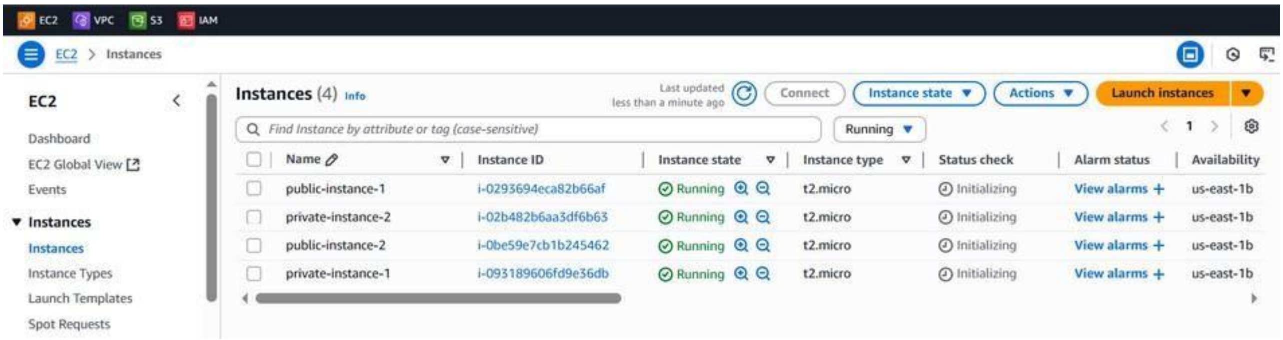
AWS Console Home
VPC > Route tables > rtb-093dad6ac8c13026c > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local local	Active	No
0.0.0.0/0	NAT Gateway nat-08c65d82dd5c0c3a4	Active	No

Step: 2 Launch an EC2 instance.

1. Launch EC2 Instances: 2 Public & 2 Private



Instances (4) Info

Last updated less than a minute ago

Find Instance by attribute or tag (case-sensitive)

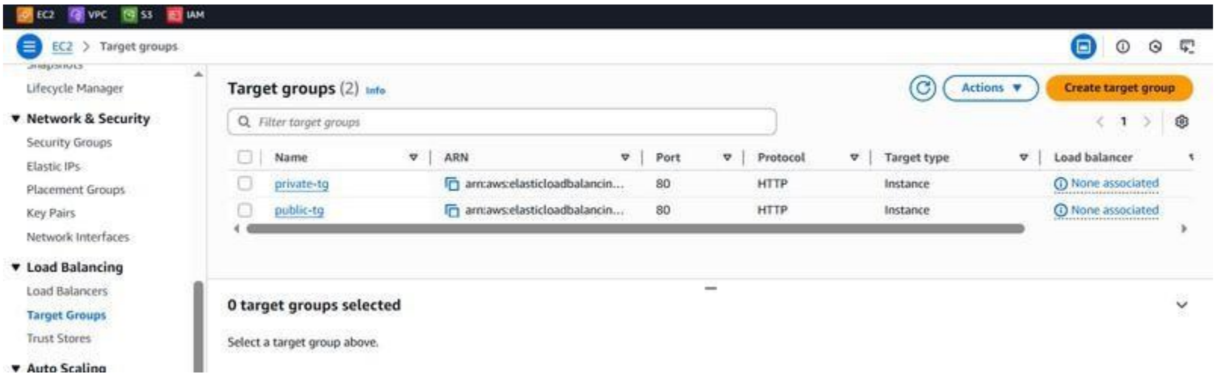
Running

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
public-instance-1	i-0293694eca82b66af	Running	t2.micro	Initializing	View alarms +	us-east-1b
private-instance-2	i-02b482b6aa3df6b63	Running	t2.micro	Initializing	View alarms +	us-east-1b
public-instance-2	i-0be59e7cb1b245462	Running	t2.micro	Initializing	View alarms +	us-east-1b
private-instance-1	i-093189606fd9e36db	Running	t2.micro	Initializing	View alarms +	us-east-1b

Step 3: Create Load Balancer

1. Create Two Target Groups

- Public Target Group
- Private Target Group



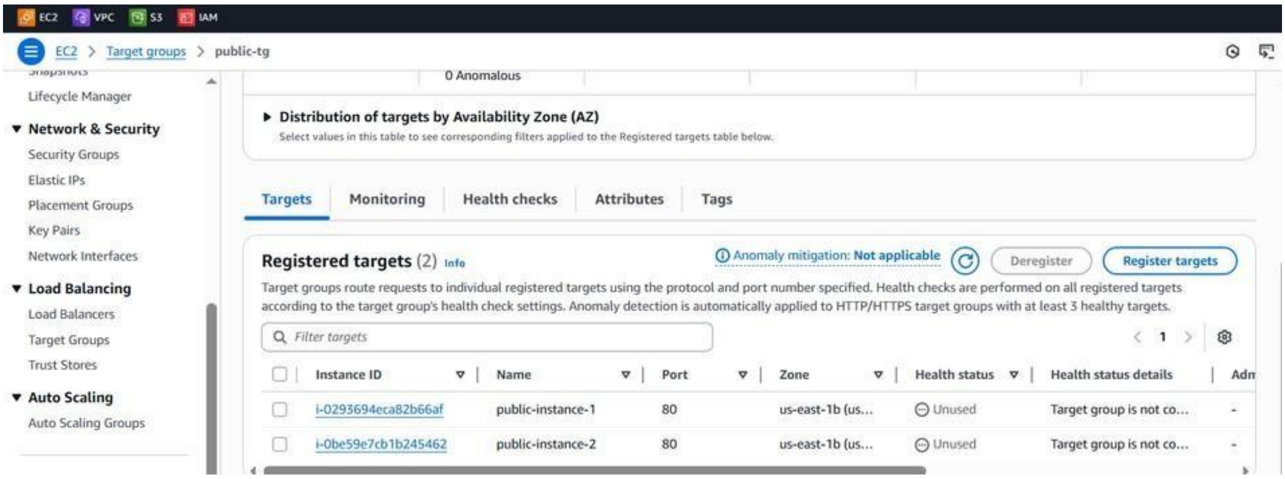
Target groups (2) Info

Name	ARN	Port	Protocol	Target type	Load balancer
private-tg	arn:aws:elasticloadbalancin...	80	HTTP	Instance	None associated
public-tg	arn:aws:elasticloadbalancin...	80	HTTP	Instance	None associated

0 target groups selected

Select a target group above.

2. Associate EC2 Instances with Their Respective Target Groups



0 Anomalous

Distribution of targets by Availability Zone (AZ)

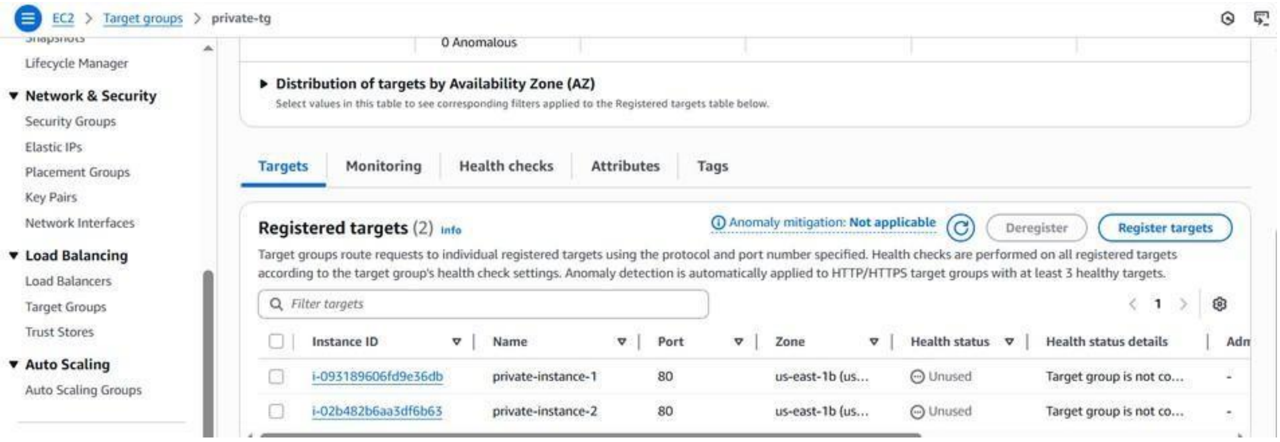
Select values in this table to see corresponding filters applied to the Registered targets table below.

Registered targets (2) Info

Anomaly mitigation: Not applicable

Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.

Instance ID	Name	Port	Zone	Health status	Health status details	Adn
i-0293694eca82b66af	public-instance-1	80	us-east-1b (us...	Unused	Target group is not co...	-
i-0be59e7cb1b245462	public-instance-2	80	us-east-1b (us...	Unused	Target group is not co...	-



0 Anomalous

Distribution of targets by Availability Zone (AZ)

Select values in this table to see corresponding filters applied to the Registered targets table below.

Registered targets (2) Info

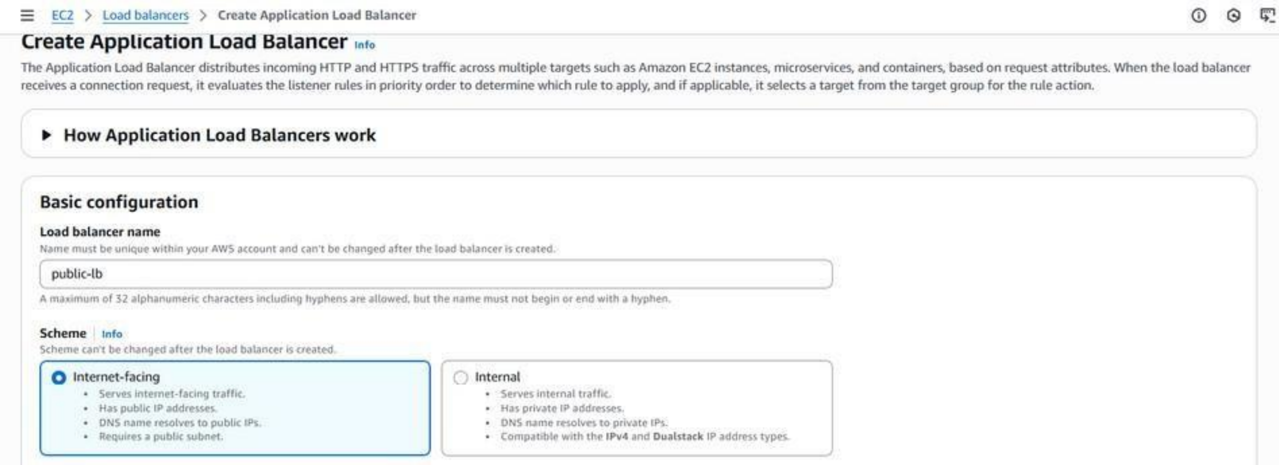
Anomaly mitigation: Not applicable

Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.

Instance ID	Name	Port	Zone	Health status	Health status details	Adn
i-093189606fd9e36db	private-instance-1	80	us-east-1b (us...	Unused	Target group is not co...	-
i-02b482b6aa3df6b63	private-instance-2	80	us-east-1b (us...	Unused	Target group is not co...	-

3. Create Application Load Balancers: Public & Private

- Public Load Balancer – Internet-Facing
- Private Load Balancer – Internal-Facing



Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the target group for the rule action.

▸ How Application Load Balancers work

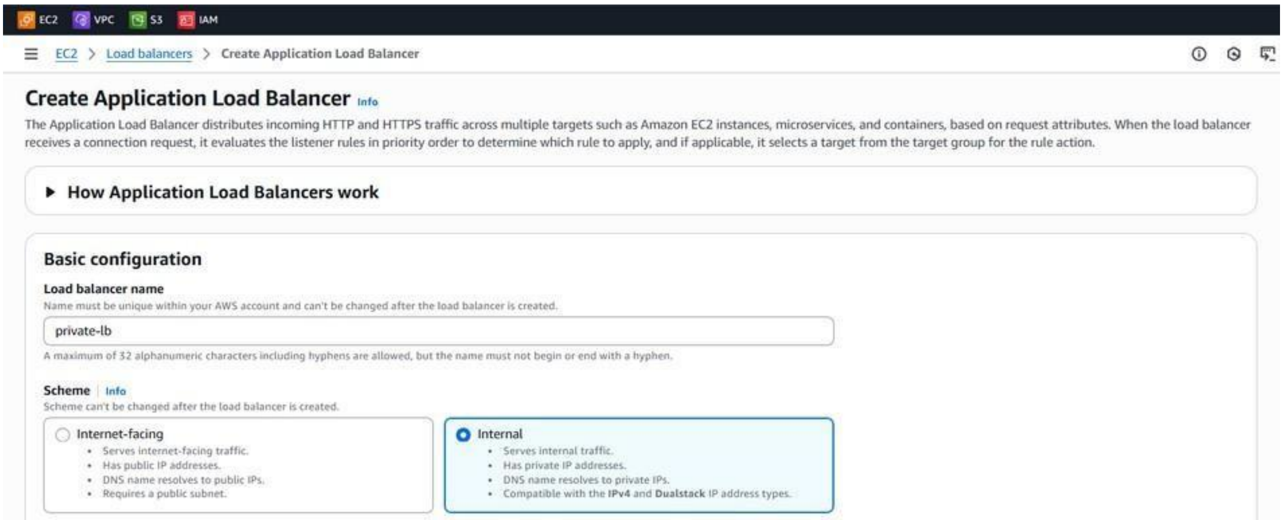
Basic configuration

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

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

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

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



Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the target group for the rule action.

▸ How Application Load Balancers work

Basic configuration

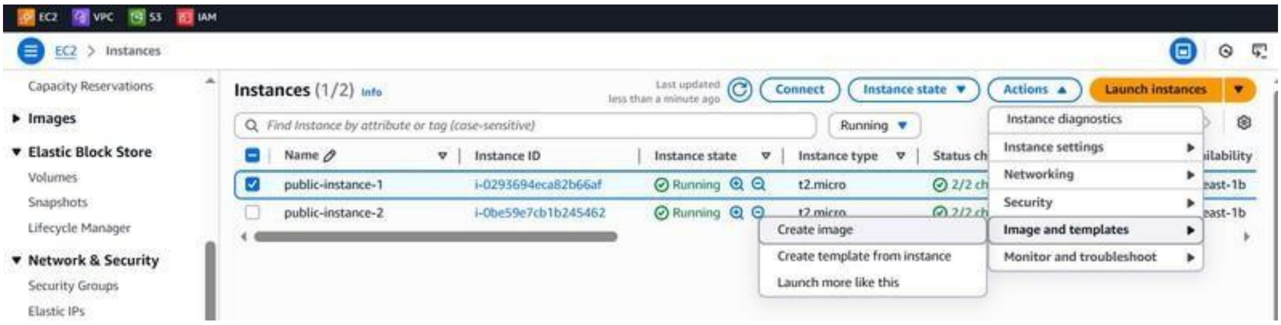
Load balancer name
Name must be unique within your AWS account and can't be changed after the load balancer is created.
private-lb
A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

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

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

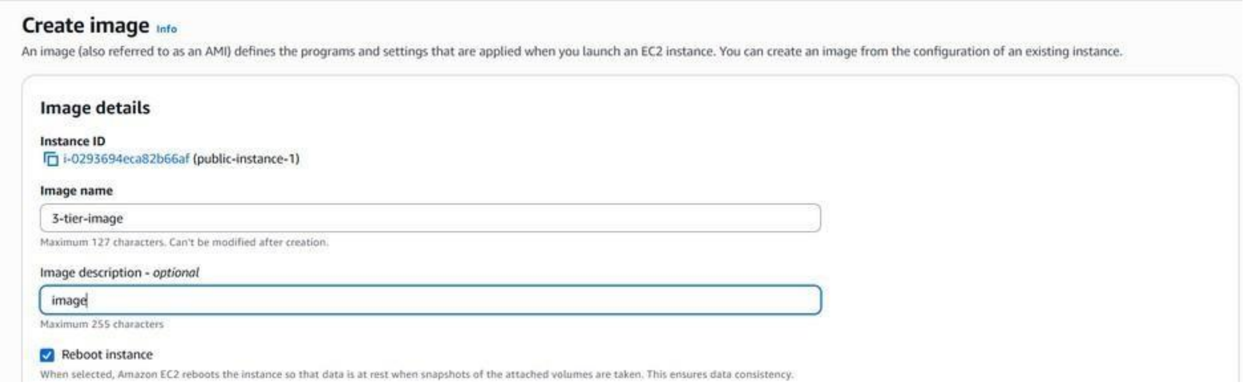
● Internal
- Serves internal traffic.
- Has private IP addresses.
- DNS name resolves to private IPs.
- Compatible with the **IPv4** and **Dualstack** IP address types.

Step 4: Create an Amazon Machine Image (AMI)



Instances (1/2) Info

☑	Name	Instance ID	Instance state	Instance type	Status ch	…ilability
☑	public-instance-1	i-0293694eca82b66af	Running	t2.micro	2/2 ch	…east-1b
□	public-instance-2	i-0be59e7cb1b245462	Running	t2.micro	2/2 ch	…east-1b



Create image Info

An image (also referred to as an AMI) defines the programs and settings that are applied when you launch an EC2 instance. You can create an image from the configuration of an existing instance.

Image details

Instance ID
i-0293694eca82b66af (public-instance-1)

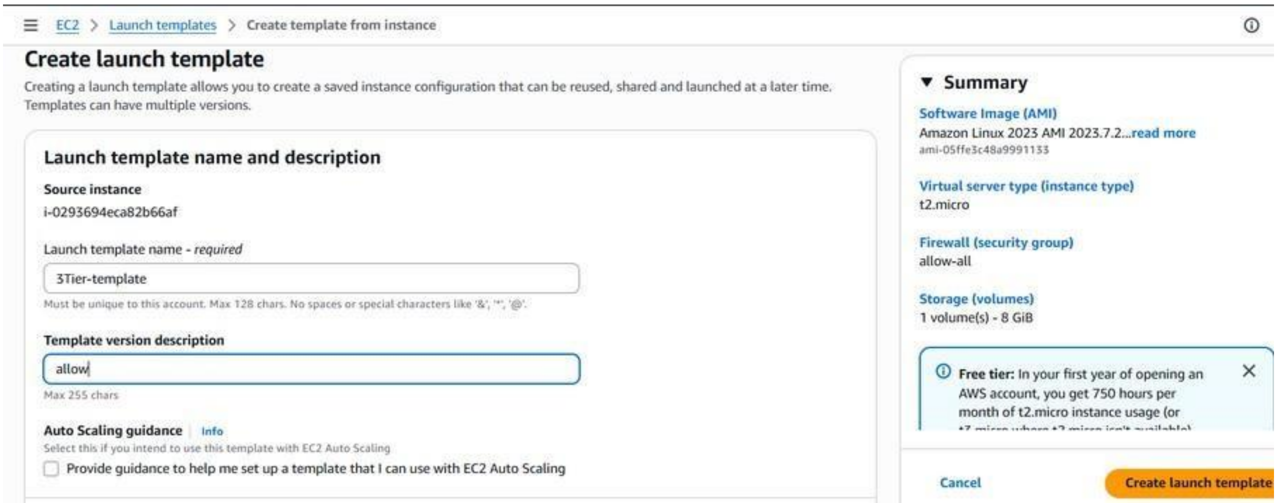
Image name
3-tier-image
Maximum 127 characters. Can't be modified after creation.

Image description - *optional*
image
Maximum 255 characters

☑ Reboot instance
When selected, Amazon EC2 reboots the instance so that data is at rest when snapshots of the attached volumes are taken. This ensures data consistency.

Step 5: Create an Auto Scaling Group

1. Create launch template - Public



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

Source instance
i-0293694eca82b66af

Launch template name - *required*
3Tier-template
Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.

Template version description
allow
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

Summary

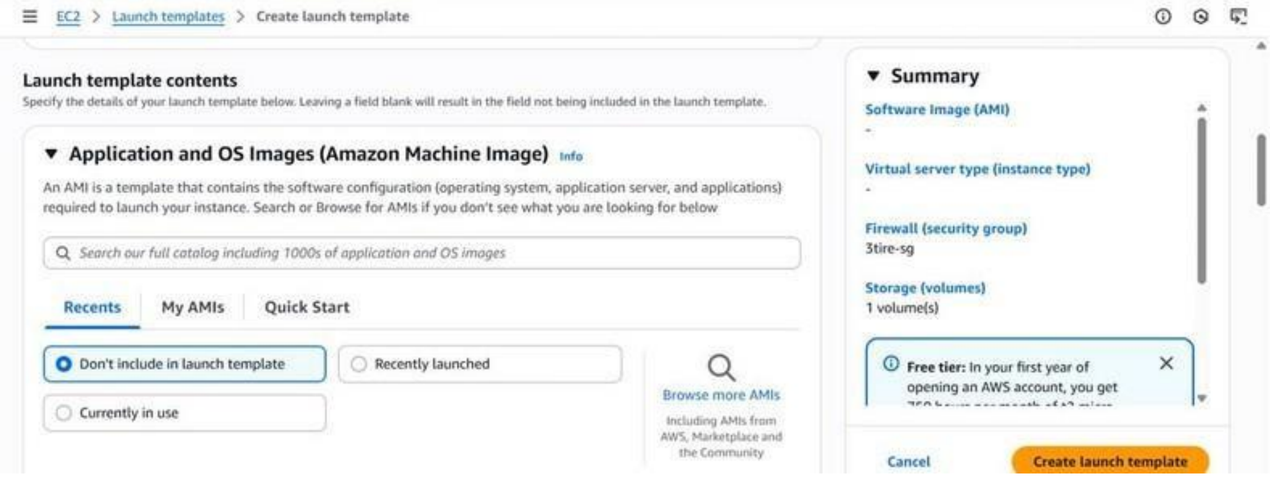
Software Image (AMI)
Amazon Linux 2023 AMI 2023.7.2...read more
ami-05ffe3c48a9991133

Virtual server type (instance type)
t2.micro

Firewall (security group)
allow-all

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



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 is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

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

● Don't include in launch template
○ Recently launched
○ Currently in use

Summary

Software Image (AMI)
-

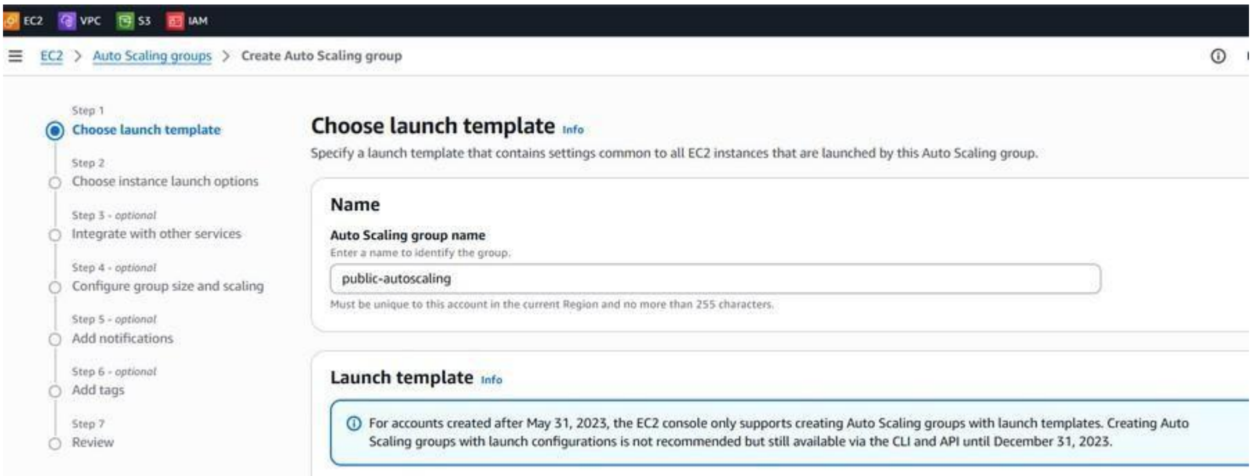
Virtual server type (instance type)
-

Firewall (security group)
3tire-sg

Storage (volumes)
1 volume(s)

Free tier: In your first year of opening an AWS account, you get

2. Create Auto Scaling Group - Public



Choose launch template Info

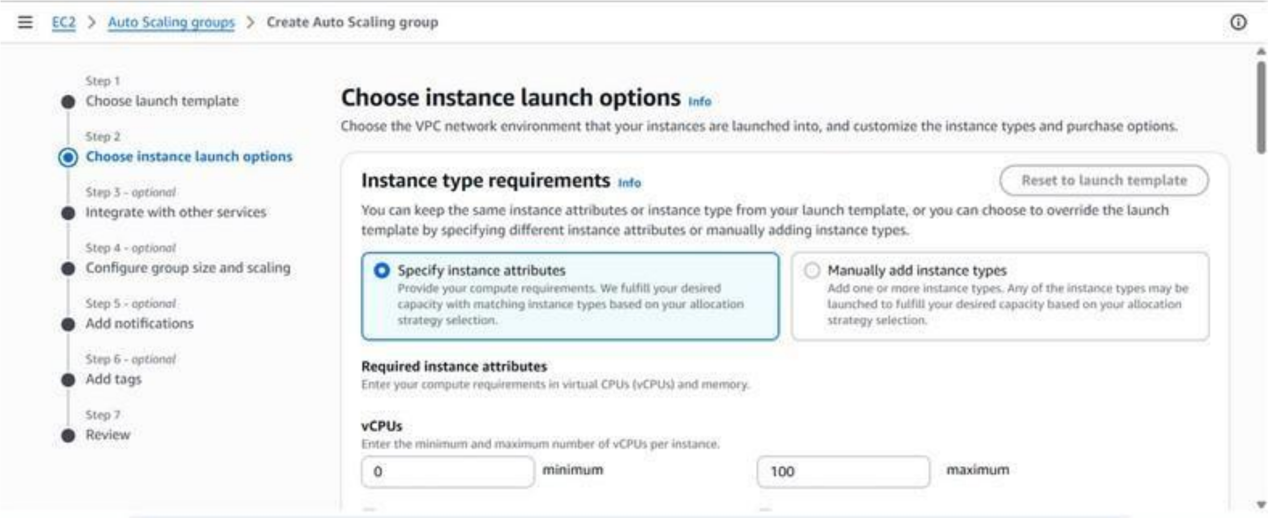
Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group.

Name

Auto Scaling group name
Enter a name to identify the group.
public-autoscaling
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.



EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1
Choose launch template

Step 2
Choose instance launch options

Step 3 - *optional*
Integrate with other services

Step 4 - *optional*
Configure group size and scaling

Step 5 - *optional*
Add notifications

Step 6 - *optional*
Add tags

Step 7
Review

Choose 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

Reset to 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.

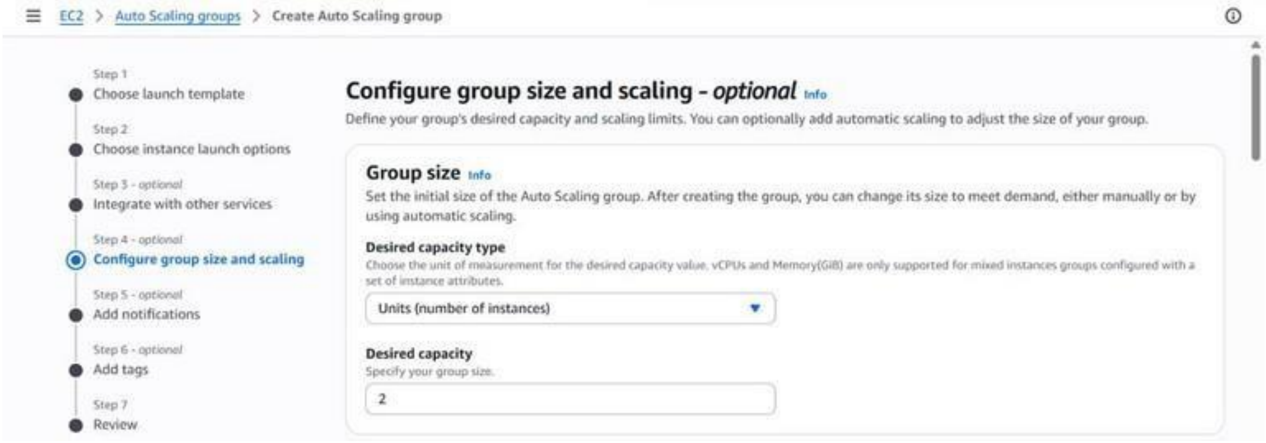
● Specify instance attributes
Provide your compute requirements. We fulfill your desired capacity with matching instance types based on your allocation strategy selection.

○ Manually add instance types
Add one or more instance types. Any of the instance types may be launched to fulfill your desired capacity based on your allocation strategy selection.

Required instance attributes
Enter your compute requirements in virtual CPUs (vCPUs) and memory.

vCPUs
Enter the minimum and maximum number of vCPUs per instance.

0 minimum 100 maximum



EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1
Choose launch template

Step 2
Choose instance launch options

Step 3 - *optional*
Integrate with other services

Step 4 - *optional*
Configure group size and scaling

Step 5 - *optional*
Add notifications

Step 6 - *optional*
Add tags

Step 7
Review

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

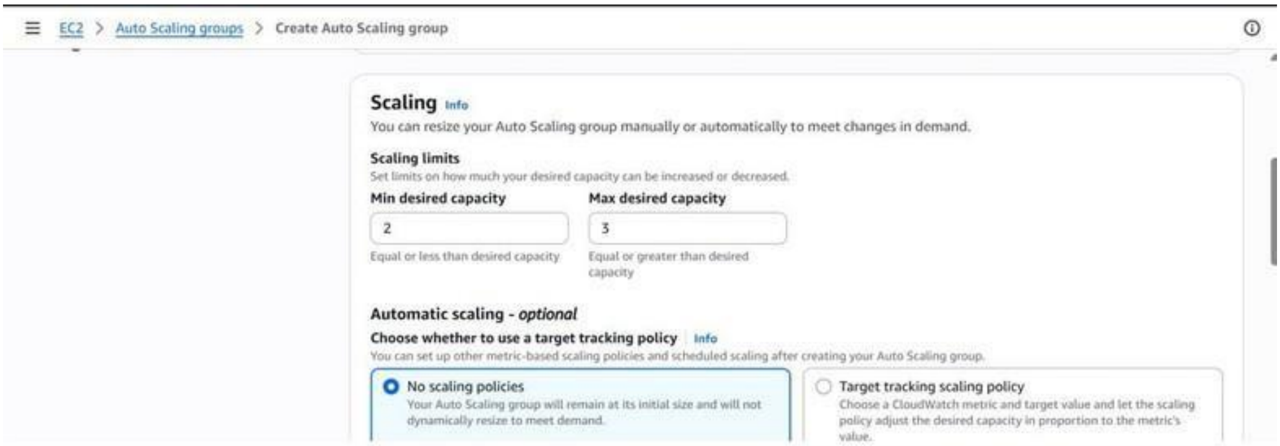
Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.

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



EC2 > Auto Scaling groups > Create Auto Scaling group

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
Equal or less than desired capacity

Max desired capacity
3
Equal or greater than desired capacity

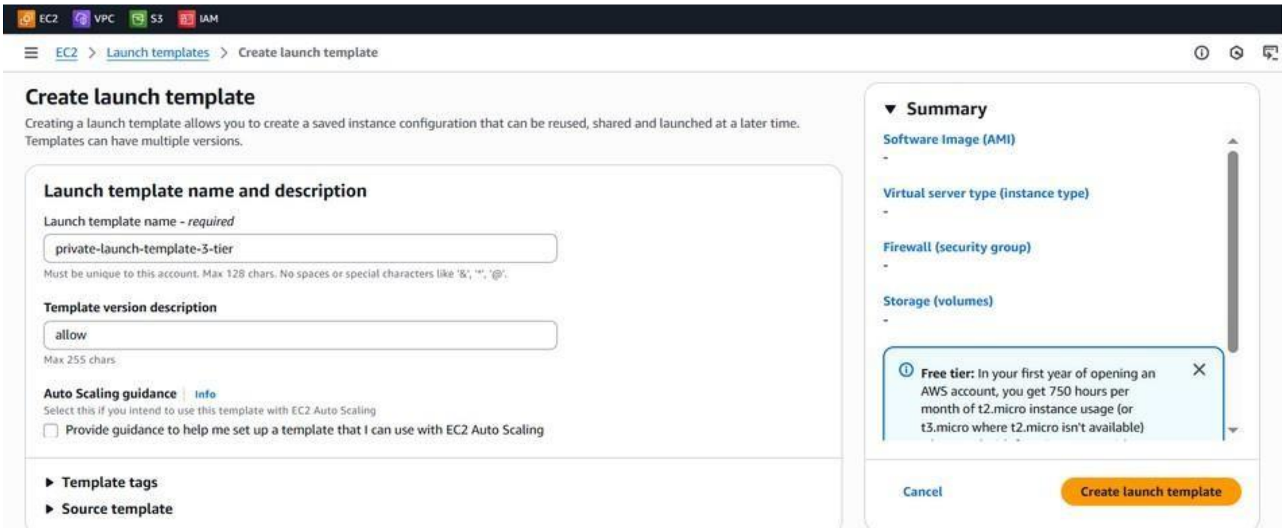
Automatic scaling - *optional*

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.

3. Create launch template - Private



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*: private-launch-template-3-tier

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

Template version description: allow

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

▾ Summary

Software Image (AMI): -

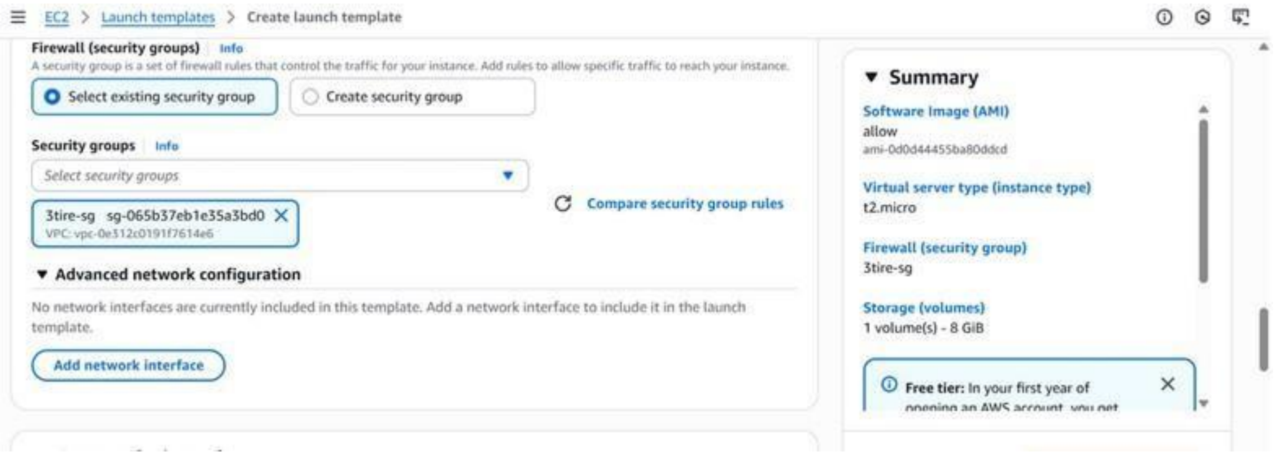
Virtual server type (instance type): -

Firewall (security group): -

Storage (volumes): -

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)

Cancel
Create launch template


EC2 > Launch templates > Create 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

3tire-sg sg-065b37eb1e35a3bd0
VPC: vpc-0e312c0191f7614e6

Compare security group rules

▾ Advanced network configuration

No network interfaces are currently included in this template. Add a network interface to include it in the launch template.

▾ Summary

Software Image (AMI): allow
ami-0d0d44455ba80ddcd

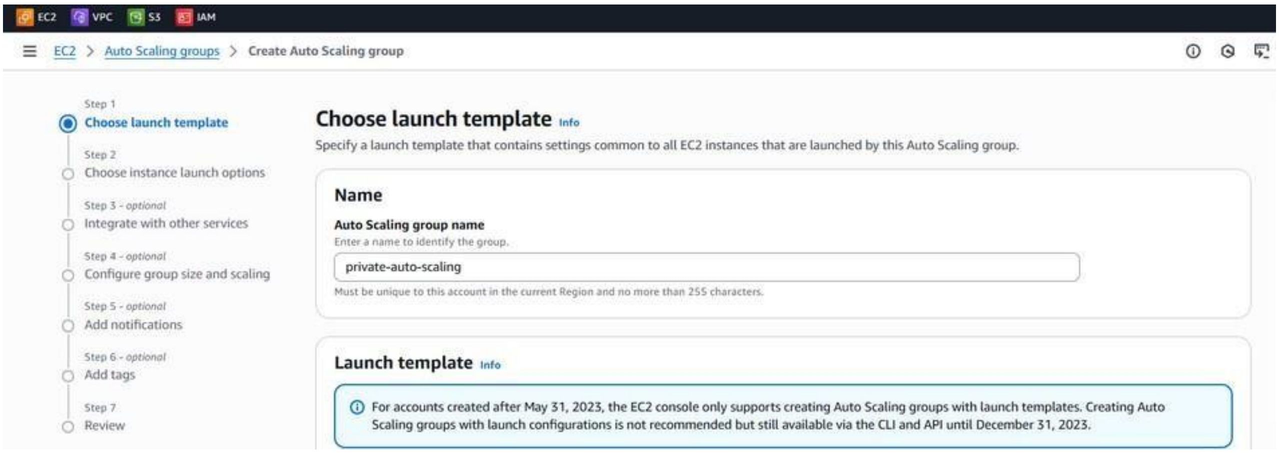
Virtual server type (instance type): t2.micro

Firewall (security group): 3tire-sg

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

Free tier: In your first year of opening an AWS account, you get

4. Create Autoscaling group - Private



Step 1
Choose launch template

Step 2
Choose instance launch options

Step 3 - *optional*
Integrate with other services

Step 4 - *optional*
Configure group size and scaling

Step 5 - *optional*
Add notifications

Step 6 - *optional*
Add tags

Step 7
Review

Choose launch template Info

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

Name

Auto Scaling group name

Enter a name to identify the group.

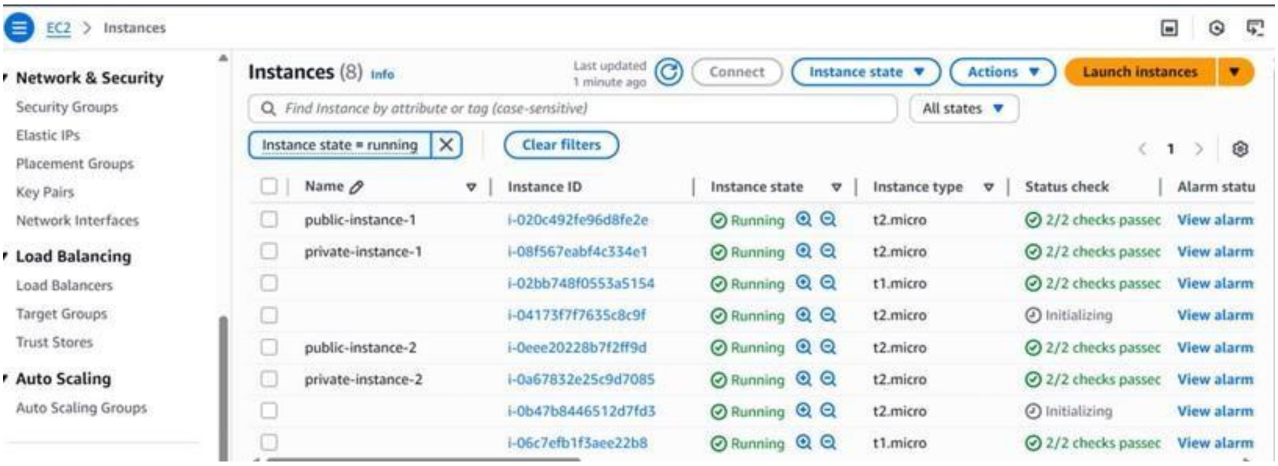
private-auto-scaling

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.

5. Auto Scaling Launches 4 Additional Instances (2 Public, 2 Private)

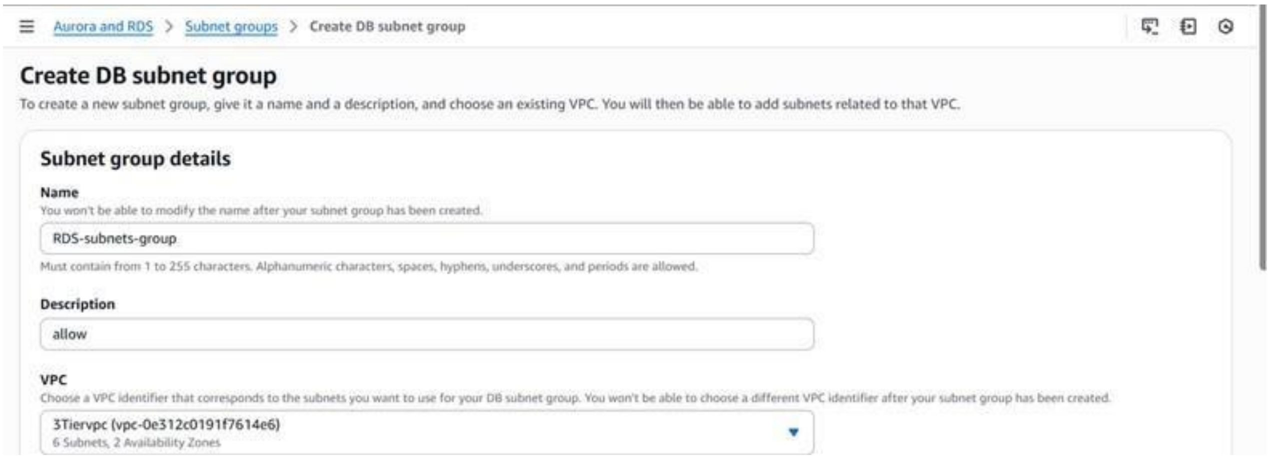


Instances (8) Info

Instance state = running ✕

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm statu
□	public-instance-1	i-020c492fe96d8fe2e	✓ Running	t2.micro	✓ 2/2 checks passec	View alarm
□	private-instance-1	i-08f567eabf4c334e1	✓ Running	t2.micro	✓ 2/2 checks passec	View alarm
□		i-02bb748f0553a5154	✓ Running	t1.micro	✓ 2/2 checks passec	View alarm
□		i-04173f7f7635c8c9f	✓ Running	t2.micro	Initializing	View alarm
□	public-instance-2	i-0eee20228b7f2ff9d	✓ Running	t2.micro	✓ 2/2 checks passec	View alarm
□	private-instance-2	i-0a67832e25c9d7085	✓ Running	t2.micro	✓ 2/2 checks passec	View alarm
□		i-0b47b8446512d7fd3	✓ Running	t2.micro	Initializing	View alarm
□		i-06c7efb1f3aee22b8	✓ Running	t1.micro	✓ 2/2 checks passec	View alarm

Step 6: Create Subnet Group



Create DB subnet group

To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

Subnet group details

Name

You won't be able to modify the name after your subnet group has been created.

RDS-subnets-group

Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

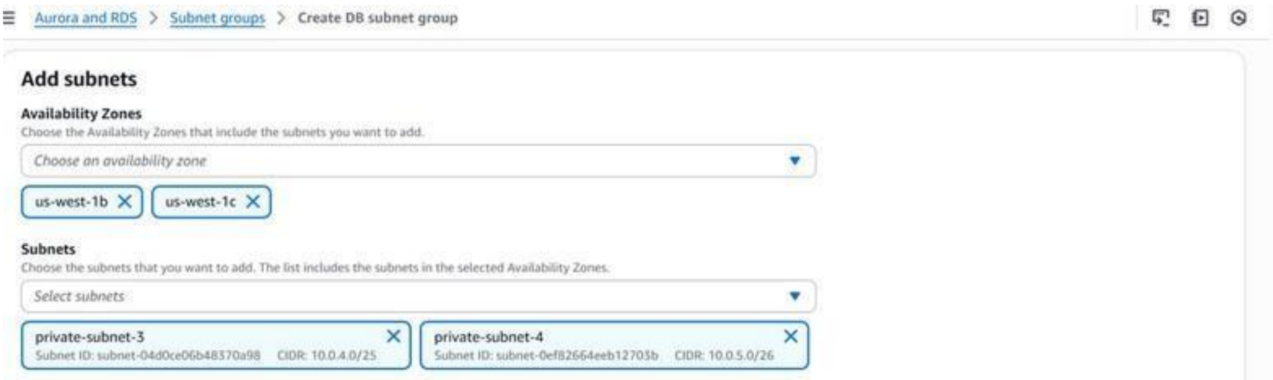
Description

allow

VPC

Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.

3Tiervpc (vpc-0e312c0191f7614e6)
6 Subnets, 2 Availability Zones



Add subnets

Availability Zones

Choose the Availability Zones that include the subnets you want to add.

Choose an availability zone

us-west-1b ✕ us-west-1c ✕

Subnets

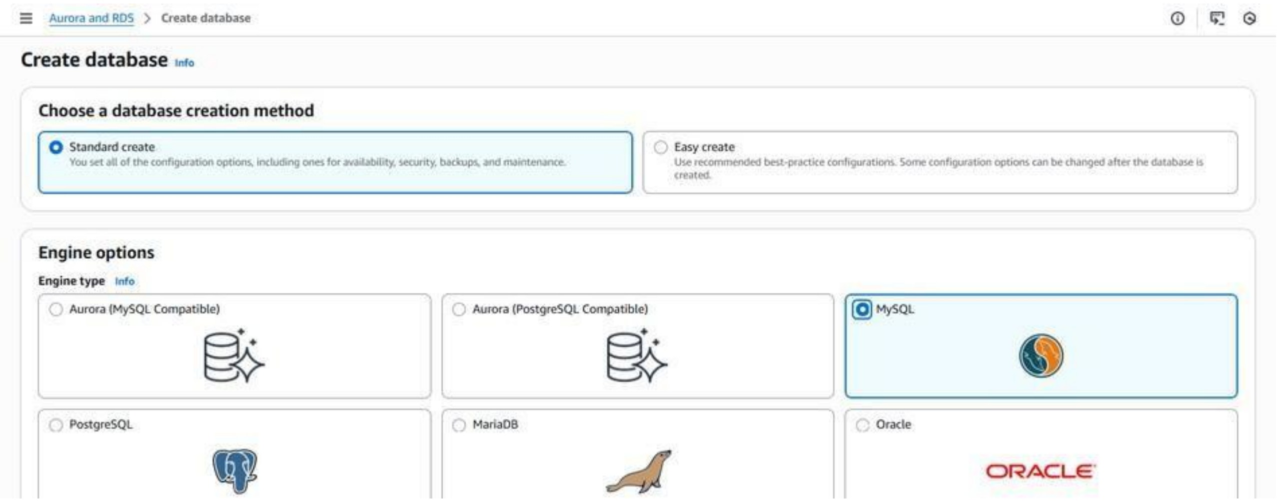
Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.

Select subnets

private-subnet-3 ✕
Subnet ID: subnet-04d0ce06b48370a98 CIDR: 10.0.4.0/25

private-subnet-4 ✕
Subnet ID: subnet-0ef82664eeb12703b CIDR: 10.0.5.0/26

Step 7: Create Database (RDS Instance)



Create database Info

Choose a database creation method

● Standard create
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)

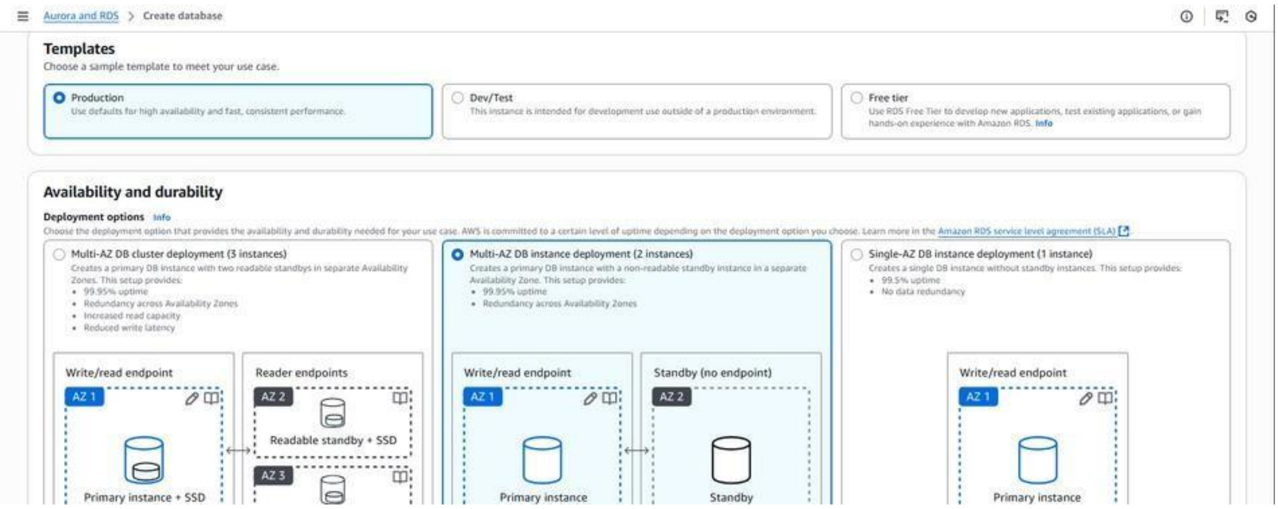
○ Aurora (PostgreSQL Compatible)

● MySQL

○ PostgreSQL

○ MariaDB

○ Oracle



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

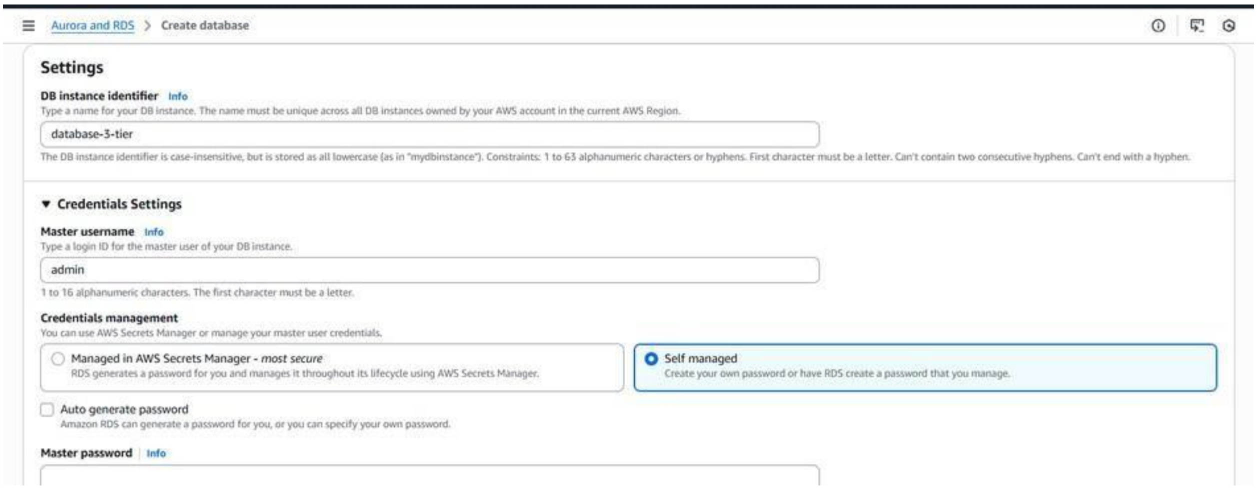
Deployment options Info

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



Settings

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-3-tier

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.

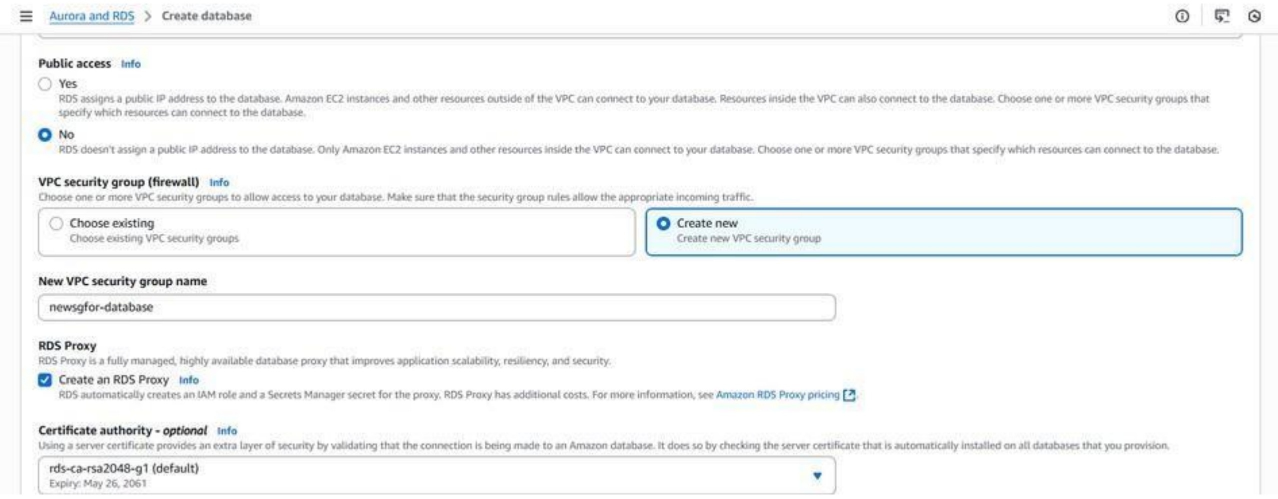
Credentials management
You can use AWS Secrets Manager or manage your master user credentials.

○ 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



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
RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

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

New VPC security group name
newsgfor-database

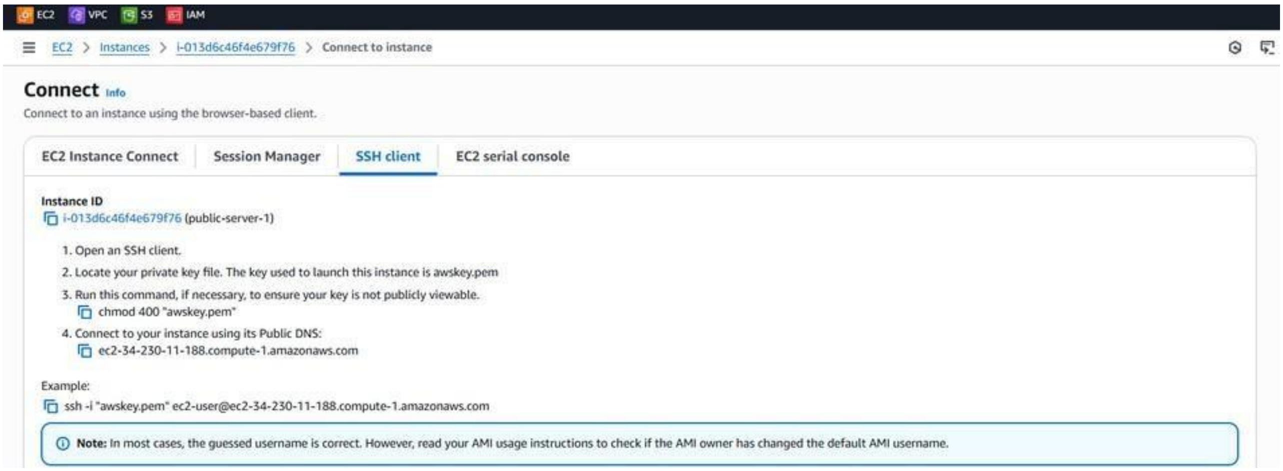
RDS Proxy
RDS Proxy is a fully managed, highly available database proxy that improves application scalability, resiliency, and security.

☑ 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 automatically installed on all databases that you provision.

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

Step 8: Establish Connection



Connect Info
Connect to an instance using the browser-based client.

Instance ID
i-013d6c46f4e679f76 (public-server-1)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is awskey.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
   chmod 400 "awskey.pem"
4. Connect to your instance using its Public DNS:
   ec2-34-230-11-188.compute-1.amazonaws.com

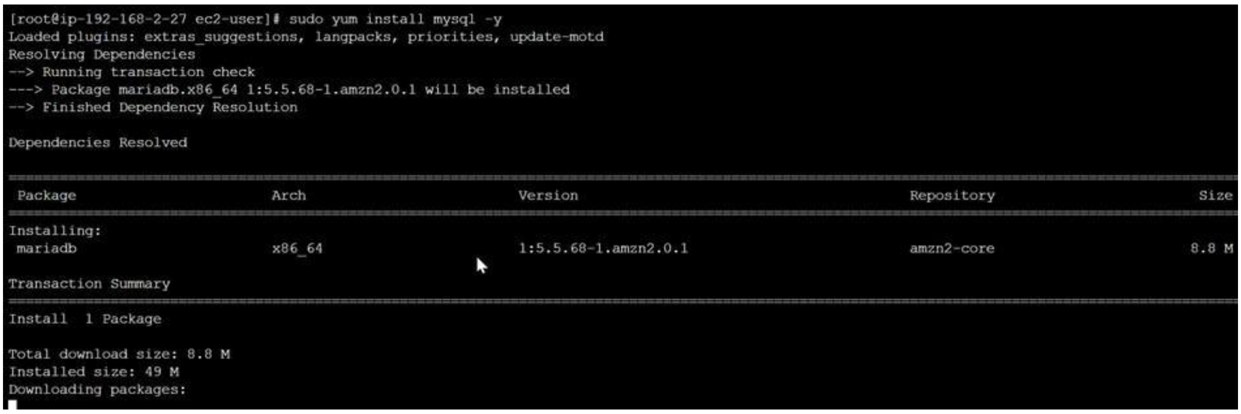
Example:

```
ssh -i "awskey.pem" ec2-user@ec2-34-230-11-188.compute-1.amazonaws.com
```

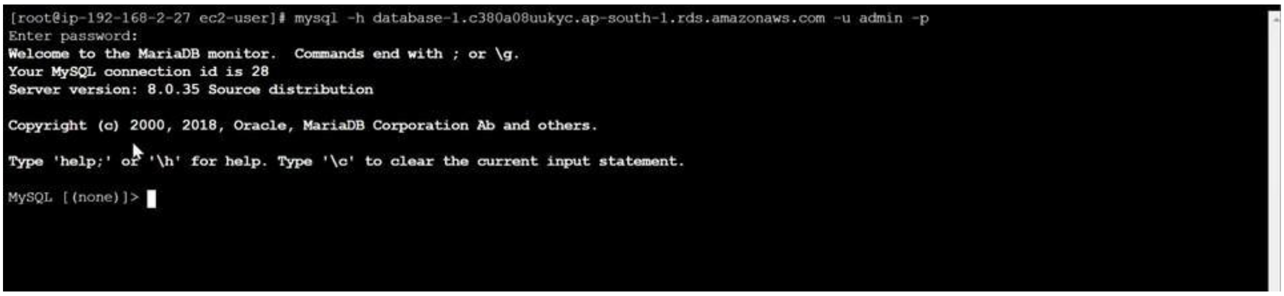
Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

After connecting to the server, run:

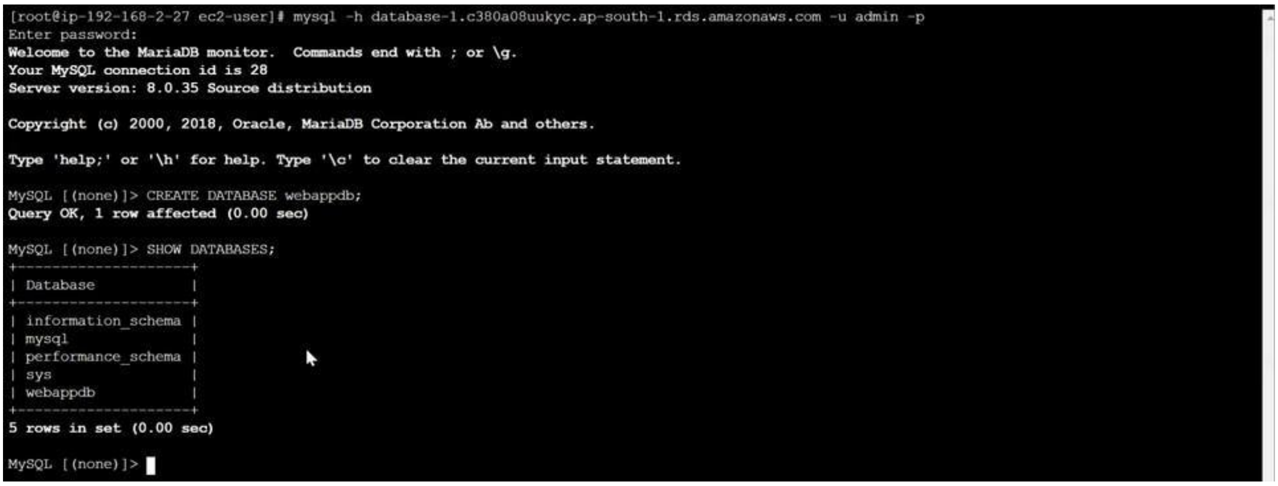
- sudo -i
- apt update -y
- sudo apt install mysql-server -y



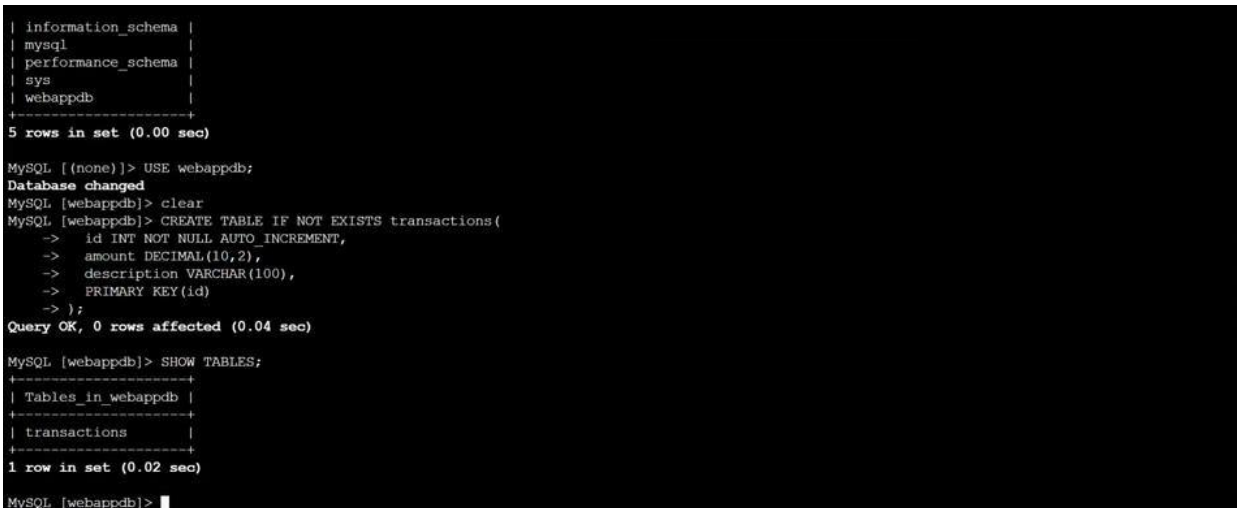
```
[root@ip-192-168-2-27 ec2-user]# sudo yum install mysql -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Resolving Dependencies
--> Running transaction check
---> Package mariadb.x86_64 1:5.5.68-1.amzn2.0.1 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
 Package                     Arch                    Version                              Repository        Size
================================================================================================================
Installing:
 mariadb                     x86_64                  1:5.5.68-1.amzn2.0.1                 amzn2-core       8.8 M

Transaction Summary
================================================================================================================
Install  1 Package

Total download size: 8.8 M
Installed size: 49 M
Downloading packages:
```



```
[root@ip-192-168-2-27 ec2-user]# mysql -h database-1.c380a08uukyc.ap-south-1.rds.amazonaws.com -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 28
Server version: 8.0.35 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)]> 
```



```
[root@ip-192-168-2-27 ec2-user]# mysql -h database-1.c380a08uukyc.ap-south-1.rds.amazonaws.com -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 28
Server version: 8.0.35 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)]> CREATE DATABASE webappdb;
Query OK, 1 row affected (0.00 sec)

MySQL [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| webappdb           |
+--------------------+
5 rows in set (0.00 sec)

MySQL [(none)]> 
```



```
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| webappdb           |
+--------------------+
5 rows in set (0.00 sec)

MySQL [(none)]> USE webappdb;
Database changed
MySQL [webappdb]> clear
MySQL [webappdb]> CREATE TABLE IF NOT EXISTS transactions(
    ->    id INT NOT NULL AUTO_INCREMENT,
    ->    amount DECIMAL(10,2),
    ->    description VARCHAR(100),
    ->    PRIMARY KEY(id)
    -> );
Query OK, 0 rows affected (0.04 sec)

MySQL [webappdb]> SHOW TABLES;
+--------------------+
| Tables_in_webappdb |
+--------------------+
| transactions       |
+--------------------+
1 row in set (0.02 sec)

MySQL [webappdb]> 
```