

NAME: GARIKI PRATHIBHA
MAIL.ID: prathibhagariki437@gmail.com

3-Tier Architecture for Web Applications in AWS

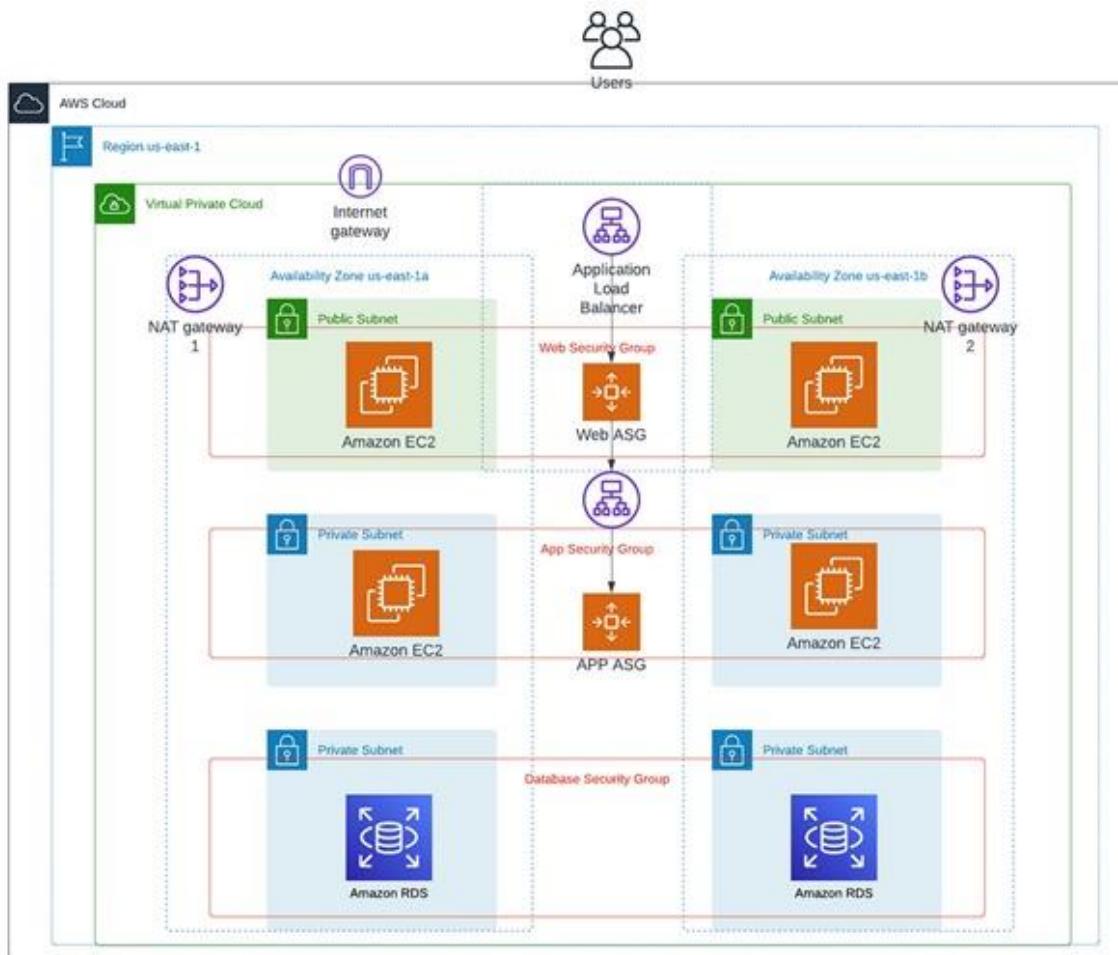


Fig: Creating a Highly Available 3-Tier Architecture for Web Applications in AWS

ABOUT:

In a three-tier application architecture, each tier serves a specific role and communicates with the other tiers to deliver a complete application experience. Implementing this architecture on AWS involves using various services to handle the presentation (web), application (logic), and data (database) layers.

VPC:

A Virtual Private Cloud (VPC) is a fundamental component in Amazon Web Services (AWS) that enables you to create a logically isolated network environment within the AWS cloud. It provides control over a virtualized network that mimics a traditional on-premises network, including IP address ranges, subnets, route tables, and network gateways. With VPC, you can securely deploy and manage your AWS resources, such as EC2 instances, RDS databases, and other services, in a private and controlled network space.

Go to AWS console, in that I was used **us-east-1a** and **us-east-1b** availability zones in **US East N.virginia** region

The screenshot shows the AWS EC2 Dashboard for the US East (N. Virginia) Region. The left sidebar includes links for EC2 Global View, Events, Console-to-Code, Instances, Images, and Elastic Block Store. The main area displays resource counts: Instances (running) 0, Auto Scaling Groups 0, Dedicated Hosts 0, Elastic IPs 1, Instances 0, Key pairs 2, Load balancers 0, Placement groups 0, Security groups 1, Snapshots 0, and Volumes 0. A 'Launch instance' button is present. To the right, the 'EC2 Free Tier Info' section shows 3 EC2 free tier offers in use, with one forecasted to exceed the limit. It also tracks offer usage monthly for Linux EC2 Instances, EBS Snapshot Usage, and Storage space on EBS.

Click on VPC in AWS console and then click on create VPC.

The screenshot shows the AWS VPC dashboard with 1 VPC listed. The table includes columns for Name, VPC ID, State, IPv4 CIDR, and IPv6 CIDR. The first VPC entry is named '-' with VPC ID 'vpc-076a95947448bcd1f', State 'Available', IPv4 CIDR '172.31.0.0/16', and IPv6 CIDR '-'. A 'Create VPC' button is located at the top right.

- Go to VPC dashboard click on create VPC.
- Click on VPC only and name tag as project-3tier.
- Give IPV4 CIDR (classless inter domain routing) as 10.0.0.0/16.
- Click on VPC, it is created.

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

VPC only VPC and more

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
project-3tier

IPv4 CIDR block [Info](#)
 IPv4 CIDR manual input IPAM-allocated IPv4 CIDR block

IPv4 CIDR
10.0.0.0/16
CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)
 No IPv6 CIDR block IPAM-allocated IPv6 CIDR block Amazon-provided IPv6 CIDR block IPv6 CIDR owned by me

Tenancy [Info](#)
Default

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - <i>optional</i>
<input type="text"/> Name X	<input type="text"/> project-3tier X Remove tag

Add tag

CloudShell Feedback

Subnets:

- **Public Subnets:** Subnets that have access to the internet via an Internet Gateway. Typically used for resources that need to be reachable from the outside, such as web servers.
- **Private Subnets:** Subnets that do not have direct internet access. Used for resources that should not be exposed to the internet, such as databases and application servers.

For this 3-tier architecture 6 subnets need to create, In that 2 subnets are public and remaining 4 subnets are private.

Subnets (6) <small>Info</small>								
		Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR		
<input type="checkbox"/>	Name	subnet-05c7ea83567eecd2f	Available	vpc-076a95947448bdc1f	172.31.16.0/20	-		
<input type="checkbox"/>	-	subnet-0b9cfb16fad95c2f	Available	vpc-076a95947448bdc1f	172.31.64.0/20	-		
<input type="checkbox"/>	-	subnet-0277bb2121683528a	Available	vpc-076a95947448bdc1f	172.31.48.0/20	-		
<input type="checkbox"/>	-	subnet-05b70f692039d0c37	Available	vpc-076a95947448bdc1f	172.31.80.0/20	-		
<input type="checkbox"/>	-	subnet-0c3fe36e6e264f75b	Available	vpc-076a95947448bdc1f	172.31.32.0/20	-		
<input type="checkbox"/>	-	subnet-0ed2965149f71bacb	Available	vpc-076a95947448bdc1f	172.31.0.0/20	-		

Subnet 1:

- Click on create subnet
- Select the VPC (project-3tier)
- Give the name tag as public1->select availability zone as US East(N.virginia)/us-east-1a
- Give CIDR as 10.0.7.0/24 and then click on create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-094fb96a7e0bf87 (project-3tier)

Associated VPC CIDs

IPv4 CIDs
10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
public1
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1a

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.7.0/24 256 IPs

Tags - optional

Key	Value - optional
<input type="text"/> Name	<input type="text"/> public1

Add new tag
You can add 49 more tags.
Remove

Add new subnet

Cancel **Create subnet**

Subnet 2:

- Click on create subnet
- Select the VPC (project-3tier)
- Give the name tag as public2->select availability zone as US East(N.virginia)/us-east-1b
- Give CIDR as 10.0.8.0/24 and then click on create subnet.

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
 256 IPs
< > ^ v

Tags - optional

Key	Value - optional
<input type="text" value="Name"/> X	<input type="text" value="public2"/> X
<input type="button" value="Remove"/>	

Subnet 3:

- Click on create subnet
- Select the VPC (project-3tier)
- Give the name tag as private1a->select availability zone as US East(N.virginia)/us-east-1a
- Give CIDR as 10.0.9.0/24 and then click on create subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

▼

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

▼

IPv4 subnet CIDR block

256 IPs
 < > ^ v

Tags - optional

Key	Value - optional
<input style="width: 100%; border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;" type="text" value="Name"/> X	<input style="width: 100%; border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;" type="text" value="private1a"/> X Remove
Add new tag	
You can add 49 more tags.	
Remove	
Add new subnet	

[Cancel](#) **Create subnet**

Subnet 4:

- Click on create subnet
- Select the VPC (project-3tier)
- Give the name tag as private1b->select availability zone as US East(N.virginia)/us-east-1a
- Give CIDR as 10.0.10.0/24 and then click on create subnet.

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone

[Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

▼

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

private1b

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (N. Virginia) / us-east-1a



Subnet 5:

- Click on create subnet
- Select the VPC (project-3tier)
- Give the name tag as private2a->select availability zone as US East(N.virginia)/us-east-1b
- Give CIDR as 10.0.11.0/24 and then click on create subnet.

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.



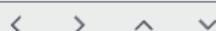
IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.



IPv4 subnet CIDR block

256 IPs



▼ Tags - optional

Key

Value - optional



You can add 49 more tags.

Subnet 6:

- Click on create subnet
- Select the VPC (project-3tier)
- Give the name tag as private2b->select availability zone as US East(N.virginia)/us-east-1b
- Give CIDR as 10.0.12.0/24 and then click on create subnet.

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone Info

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block Info

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block

256 IPs

▼ Tags - optional

Key

Value - optional

You can add 49 more tags.

Total 6 subnets we just created as shown in below.

Subnets (12) <small>Info</small>						
<small>Last updated 1 minute ago</small> <input type="button" value="C"/> <input type="button" value="Actions"/> <input type="button" value="Create subnet"/>						
	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
<input type="checkbox"/>	-	subnet-0c3fe36e6e264f25b	<input checked="" type="radio"/> Available	vpc-076a95947448bdc1f	172.31.32.0/20	-
<input type="checkbox"/>	-	subnet-0ed2965149f71bacb	<input checked="" type="radio"/> Available	vpc-076a95947448bdc1f	172.31.0.0/20	-
<input type="checkbox"/>	private1a	subnet-00fb6bf8dca4350df	<input checked="" type="radio"/> Available	vpc-094f0bf96a7e0bf87 proj...	10.0.9.0/24	-
<input type="checkbox"/>	private1b	subnet-01ea943739a261f04	<input checked="" type="radio"/> Available	vpc-094f0bf96a7e0bf87 proj...	10.0.10.0/24	-
<input type="checkbox"/>	private2a	subnet-049cc6335b1810327b	<input checked="" type="radio"/> Available	vpc-094f0bf96a7e0bf87 proj...	10.0.11.0/24	-
<input type="checkbox"/>	private2b	subnet-08a965bc9226fb87c	<input checked="" type="radio"/> Available	vpc-094f0bf96a7e0bf87 proj...	10.0.12.0/24	-
<input type="checkbox"/>	public1	subnet-0d95e3399af07f43a	<input checked="" type="radio"/> Available	vpc-094f0bf96a7e0bf87 proj...	10.0.7.0/24	-
<input type="checkbox"/>	public2	subnet-0b053e3261ccb4135	<input checked="" type="radio"/> Available	vpc-094f0bf96a7e0bf87 proj...	10.0.8.0/24	-

Internet gateway(IGW):

A gateway that provides internet access to resources in your VPC. It is attached to your VPC to enable communication between instances in your VPC and the internet.

- Click on create internet gateway->Give name tag as project-igw-> click on create.
- Once IGW created click on attach to a VPC
- Select the VPC and then click on attach internet gateway.

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag

Creates a tag with a key of 'Name' and a value that you specify.

project-igw

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Name

Value - optional

project-igw

X

Remove

Add new tag

You can add 49 more tags.

Cancel

Create internet gateway

The following internet gateway was created: igw-00b9cf5932d27e93 - project-igw. You can now attach to a VPC to enable the VPC to communicate with the internet.

Attach to a VPC

VPC > Internet gateways > igw-00b9cf5932d27e93

igw-00b9cf5932d27e93 / project-igw

Actions ▾

Details Info

Internet gateway ID
igw-00b9cf5932d27e93

State
Detached

VPC ID

-

Owner
891377141179

Tags

Search tags

Manage tags

Key | Value
Name | project-igw

< 1 > @

The following internet gateway was created: igw-00b9cf5932d27e93 - project-igw. You can now attach to a VPC to enable the VPC to communicate with the internet.

VPC > Internet gateways > Attach to VPC (igw-00b9cf5932d27e93)

Attach to VPC (igw-00b9cf5932d27e93) Info

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

vpc-094f0bf96a7e0bf87

X

▶ AWS Command Line Interface command

Cancel

Attach internet gateway

NAT gateway:

A managed service that allows instances in a private subnet to initiate outbound traffic to the internet while preventing unsolicited inbound traffic.

- Click on create NAT gateway
- Give name tag as project-nat-gw->select the public subnet(public2)->connectivity type should be public-
- Click on allocate Elastic IP and then click on create Nat gateway

The screenshot shows the 'Create NAT gateway' page in the AWS VPC console. The top navigation bar includes 'VPC', 'NAT gateways', and 'Create NAT gateway'. The main section is titled 'Create NAT gateway' with an 'Info' link. A descriptive text states: '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.' Below this is a 'NAT gateway settings' section. It includes fields for 'Name - optional' (containing 'project-nat-gw'), 'Subnet' (set to 'subnet-0b053e3261cbb4135 (public2)'), 'Connectivity type' (set to 'Public'), and 'Elastic IP allocation ID' (containing 'eipalloc-05094ef26c9a50c6e'). An 'Allocate Elastic IP' button is present. At the bottom of the settings section is a 'Additional settings' link.

Tags

Route tables:

Route tables control the routing of traffic within your VPC. You can define routes for directing traffic between subnets and to/from the internet or other networks.

For 3 tier architecture we need to create 2 route tables. One is for public subnets and another is for private subnets.

The screenshot shows the 'Route tables' list page in the AWS VPC console. The top navigation bar includes 'Route tables (2) Info', a search bar, and various filter and sort options. The main table lists two route tables with the following details:

Name	Route table ID	Explicit subnet assoc...	Edge associations	Main	VPC	Own...
-	rtb-025454e06cb8bb911	-	-	Yes	vpc-076a95947448bdc1f	89137
-	rtb-082efe5b0edcb40f6	-	-	Yes	vpc-094f0bf96a7e0bf87 proje...	89137

Route table1:

- Go to route tables under VPC field and click on create route table
- Give name tag as public-route->select VPC->click on create
- Once created click on action->Edit route->add IGW in add routes field->save changes.
- Click Edit subnet associations->select 2 public subnets [public1 & public2]->click on save associations.

VPC > Route tables > Create route table

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.

public-route

VPC
The VPC to use for this route table.

vpc-094f0bf96a7e0bf87 (project-3tier)

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - <i>optional</i>
Q Name X	Q public-route X Remove

Add new tag

You can add 49 more tags.

Cancel **Create route table**

VPC > Route tables > rtb-04ae8b03f17712cd > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
Q 0.0.0.0/0 X	Internet Gateway	-	No
	Q igw-00b9cf5932d27e93 X		Remove

Add route

Cancel Preview **Save changes**

VPC > Route tables > rtb-04ae8b03f17712cd2 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/6)				Route table ID
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	
<input checked="" type="checkbox"/> public1	subnet-0d95e3399af07f43a	10.0.7.0/24	-	Main (rtb-082efe5b0edcb40f6)
<input type="checkbox"/> private1a	subnet-00fb6bf8dc4350df	10.0.9.0/24	-	Main (rtb-082efe5b0edcb40f6)
<input checked="" type="checkbox"/> public2	subnet-0b053e3261ccb4135	10.0.8.0/24	-	Main (rtb-082efe5b0edcb40f6)
<input type="checkbox"/> private1b	subnet-01ea943739a261f04	10.0.10.0/24	-	Main (rtb-082efe5b0edcb40f6)
<input type="checkbox"/> private2b	subnet-08a965bc9226fb87c	10.0.12.0/24	-	Main (rtb-082efe5b0edcb40f6)
<input type="checkbox"/> private2a	subnet-049cc633b1810327b	10.0.11.0/24	-	Main (rtb-082efe5b0edcb40f6)

Selected subnets

- subnet-0d95e3399af07f43a / public1
- subnet-0b053e3261ccb4135 / public2

Cancel Save associations

Route table2:

- Click on create route table
- Give name tag as private-route->select VPC->click on create
- Once created click on action->Edit route->add NAT gateway in add routes field->save changes.
- Click Edit subnet associations->select 4 private subnets [private1a,private1b,private2a & private2b]->click on save associations.

VPC > Route tables > Create route table

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.

VPC
The VPC to use for this route table.

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="private-route"/>
Add new tag You can add 49 more tags.	

Cancel Create route table

VPC > Route tables > rtb-09603bd825fab759 > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
Q_ 0.0.0.0/0	NAT Gateway	-	No
	Q_ nat-0dd4d40991caf8487	X	

[Add route](#) [Remove](#)

[Cancel](#) [Preview](#) [Save changes](#)

VPC > Route tables > rtb-09603bd825fab759 > Edit 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
public1	subnet-0d95e3399af07f45a	10.0.7.0/24	-	rtb-04ae8b03f17712cd2 / public-route
private1a	subnet-00fb6bf8dca4350df	10.0.9.0/24	-	Main (rtb-082efe5b0edcb40f6)
public2	subnet-0b053e3261ccb4135	10.0.8.0/24	-	rtb-04ae8b03f17712cd2 / public-route
private1b	subnet-01ea943739a261f04	10.0.10.0/24	-	Main (rtb-082efe5b0edcb40f6)
private2b	subnet-08a965bc9226fb87c	10.0.12.0/24	-	Main (rtb-082efe5b0edcb40f6)
private2a	subnet-049cc633b1810327b	10.0.11.0/24	-	Main (rtb-082efe5b0edcb40f6)

Selected subnets

- subnet-00fb6bf8dca4350df / private1a X
- subnet-01ea943739a261f04 / private1b X
- subnet-08a965bc9226fb87c / private2b X
- subnet-049cc633b1810327b / private2a X

[Cancel](#) [Save associations](#)

EC2 instance:

Amazon EC2 (Elastic Compute Cloud) is a core component of Amazon Web Services (AWS) that provides scalable computing capacity in the cloud. It allows you to launch and manage virtual servers, known as instances, which can run various applications and workloads.

Instance1:

- Go to EC2 dashboard and click on launch instance
- Give name tag as project-3tier-public1->select ubuntu -> create key pair and named as project-3tier
- Click on network settings->select VPC as project-3tier->select subnet public1->Enable the Auto assign public IP->create security group name as sg3tier->add http port number 80 for security group-> click on launch instance.
- The overall configuration as shown following slides.

Name and tags [Info](#)

Name

[Add additional tags](#)

▼ 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](#)

[Recent](#) | [My AMIs](#) | [Quick Start](#)



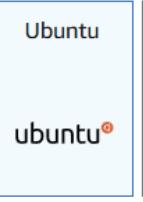
Amazon
Linux





macOS





Ubuntu





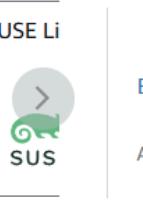
Windows





Red Hat





SUSE Li



🔍 [Browse more AMIs](#)
 Including AMIs from AWS, Marketplace and the Community

Key pair name - *required*

[Create new key pair](#)

▼ Network settings [Info](#)

VPC - *required* [Info](#)

vpc-094f0bf96a7e0bf87 (project-3tier)
 10.0.0.0/16

[Create new VPC](#)

Subnet [Info](#)

subnet-0d95e3399af07f43a public
 VPC: vpc-094f0bf96a7e0bf87 Owner: 891377141179 Availability Zone: us-east-1a
 IP addresses available: 251 CIDR: 10.0.7.0/24

[Create new subnet](#)

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*

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 characters: a-z, A-Z, 0-9, spaces, and _-:/()#@[]+=&;!\$*

Description - *required* [Info](#)

Inbound Security Group Rules

- Security group rule 1 (TCP, 22, 0.0.0.0/0)

Type	Info	Protocol	Info	Port range	Info
ssh		TCP		22	

 Source type: Anywhere

Source	Info
Add CIDR, prefix list or security	e.g. SSH for admin desktop

 Description - optional: 0.0.0.0/0
- Security group rule 2 (TCP, 80, 0.0.0.0/0)

Type	Info	Protocol	Info	Port range	Info
HTTP		TCP		80	

 Source type: Custom

Source	Info
Add CIDR, prefix list or security	e.g. SSH for admin desktop

 Description - optional: 0.0.0.0/0

⚠️ 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.

Add security group rule

Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS ...read more
ami-04a81a99f5ec58529

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel Launch instance Review commands

Instance2:

- click on launch instance.
- Give name tag as project-3tier-public2->select ubuntu -> select key pair as project-3tier
- Click on network settings->select VPC as project-3tier->select subnet public2->Enable the Auto assign public IP->select the existing security group-sg3tier-> click on launch instance.
- The overall configuration as shown following slides

Name and tags [Info](#)

Name: project-3tier-public2 [Add additional tags](#)

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

Recents My AMIs Quick Start

Amazon Linux	macOS	Ubuntu	Windows	Red Hat	SUSE Li

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM) SSD Volume Type Free tier eligible

Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Key pair name - required
project-3tier

Network settings [Info](#)

VPC - required [Info](#)
vpc-094f0bf96a7e0bf87 (project-3tier)
10.0.0.16

Subnet [Info](#)
subnet-0b053e3261cbb4135 public2
VPC: vpc-094f0bf96a7e0bf87 Owner: 891377141179 Availability Zone: us-east-1b IP addresses available: 250 CIDR: 10.0.8.0/24

Create new subnet

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

Common security groups [Info](#)
Select security groups
sg3tier sg-05c7c41fc082a090a X
VPC: vpc-094f0bf96a7e0bf87

Compare security group rules

Security warning that you add or remove here will be applied to or removed from all your network interfaces

Currently creating AMI ami-0880189ef7da344d4 from instance i-09bdb991de60cc1b1. Check that the AMI status is 'Available' before deleting the instance or carrying out other actions related to this AMI.

Instances (1/2) Info		Connect	Instance state	Actions	Launch instances			
<input type="text"/> Find Instance by attribute or tag (case-sensitive)		All states						
<input checked="" type="checkbox"/>	Name ↗	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
<input checked="" type="checkbox"/>	project-3tier-public1	i-09bdb991de60cc1b1	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-
<input type="checkbox"/>	project-3tier-public2	i-00ebc0136c20c6e9c	Running	t2.micro	-	View alarms +	us-east-1b	-

EC2 > Instances > [i-09bdb991de60cc1b1](#) > Connect to instance

Connect to instance [Info](#)

Connect to your instance i-09bdb991de60cc1b1 (project-3tier-public1) using any of these options

- EC2 Instance Connect
- Session Manager
- SSH client**
- EC2 serial console

Instance ID
 [i-09bdb991de60cc1b1 \(project-3tier-public1\)](#)

- Open an SSH client.
- Locate your private key file. The key used to launch this instance is project-3tier.pem
- Run this command, if necessary, to ensure your key is not publicly viewable.
 chmod 400 "project-3tier.pem"
- Connect to your instance using its Public IP:
 98.80.8.145

Command copied

ssh -i "project-3tier.pem" ubuntu@98.80.8.145

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.

- Once created the instance click on connect and copy the ssh command in SSH client field and then go to git bash and connect to the server.
- Once connected change to root user->sudo -i
- Then update the server->apt update -y
- Install apache2->apt install apache2 -y
- Change directory path->cd /var/www/html
- Remove the default index.html and create new file.
- Restart->systemctl restart apache2
- Output shown in below slide.

```
root@ip-10-0-7-30:/var/www/html#
root@ip-10-0-7-30:/var/www/html# curl 10.0.7.30:80
#!/bin/bash
#####
Author-prathibha gariki
version-1
#####

hi this is from public1 instance
root@ip-10-0-7-30:/var/www/html#
```

- Once created the instance2 click on connect and copy the ssh command in SSH client field and then go to git bash and connect to the server.
- Once connected change to root user->sudo -i
- Then update the server->apt update -y
- Install apache2->apt install apache2 -y
- Change directory path->cd /var/www/html
- Remove the default index.html and create new file.
- Restart->systemctl restart apache2
- Output shown in below slide.

```
root@ip-10-0-8-32:/var/www/html#
#####
hi this is from public2 instance
root@ip-10-0-8-32:/var/www/html#
```

Load balancer:

A load balancer distributes incoming network or application traffic across multiple servers to ensure no single server becomes overwhelmed. This improves the availability, reliability, and scalability of applications

Step1:

Target group:

- For load balancer first we need to create Target group

- Click on create Target group->select instances under choose target type->select VPC project-3tier->select instances under register targets->click on include as pending below->click on create target group
- Once target group created go to load balancer.

The screenshot shows the AWS Management Console with the EC2 service selected. On the left, the navigation pane includes sections for Images, AMIs, AMI Catalog, Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), Load Balancing (Load Balancers, Target Groups), and more. The main content area displays the 'Target groups' page, which is currently empty. A prominent orange 'Create target group' button is at the top right. Below it, a message states 'No target groups' and 'You don't have any target groups in us-east-1'. A 'Create target group' button is also located here. At the bottom, a message says '0 target groups selected' and 'Select a target group above.'.

EC2 > Target groups > Create target group

Step 1
Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration
Settings in this section can't be changed after the target group is created.

Choose a target type

Instances

- Supports load balancing to instances within a specific VPC.
- Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.

IP addresses

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

Lambda function

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

Application Load Balancer

IPv4
Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.

IPv6
Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#)

VPC
Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

project-3tier
 vpn-094f0bf96a7e0bf87
 IPv4 VPC CIDR: 10.0.0.0/16

Protocol version

HTTP1
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

HTTP2
Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.

gRPC
Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Health checks

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

Health check protocol

HTTP

EC2 > Target groups > Create target group

Step 1
[Specify group details](#)

Step 2
Register targets

Register targets
This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

Available instances (2/2)

Instance ID	Name	State	Security groups	Zone
i-00ebc0136c20c6e9c	project-3tier-public2	Running	sg3teir	us-east-1b
i-09bdb991de60cc1b1	project-3tier-public1	Running	sg3teir	us-east-1a

2 selected

Ports for the selected instances
Ports for routing traffic to the selected instances.
80

1-65535 (separate multiple ports with commas)

EC2 > Load balancers

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

Name	DNS name	State	VPC ID	Availability Zones	Type	Date created
No load balancers You don't have any load balancers in us-east-1						

Create load balancer

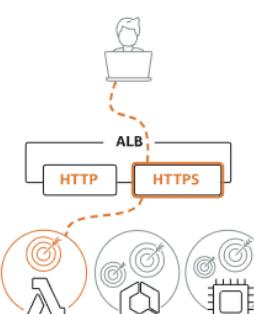
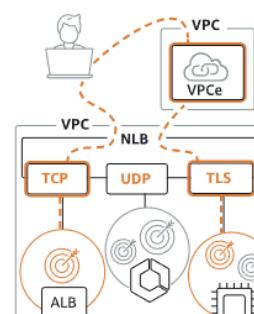
0 load balancers selected

Select a load balancer above.

- Go to load balancer and click on create load balancer.
- Select application load balancer

Compare and select load balancer type

A complete feature-by-feature comparison along with detailed highlights is also available. [Learn more](#)

Load balancer types		
Application Load Balancer Info  <p>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.</p> <p>Create</p>	Network Load Balancer Info  <p>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-</p>	Gateway Load Balancer Info  <p>Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.</p> <p>Create</p>

- Give name tag as tier1-lb->click on internet facing under scheme field->select VPC project-3tier->select availability zone us-east-1a & us-east-1b->select subnets public1 & public2->select security group->select target group (lb-tg)->remaining fields leave as default and click on next->click on create load balancer.

► 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.

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

Scheme Info

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

Internet-facing

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

Internal

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

Load balancer IP address type Info

Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.

IPv4

Includes only IPv4 addresses.

Dualstack

Includes IPv4 and IPv6 addresses.

Dualstack without public IPv4

Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with **internet-facing** load balancers only.

VPC Info

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 Lambda or on-premises traffic using VPC peering. To confirm the VPC for your targets, view [target groups](#). For a new VPC, [create a VPC](#).

vpc-094f0bf96a7e0bf87

IPv4 VPC CIDR: 10.0.0.0/16



Mappings Info

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

Availability Zones

us-east-1a (use1-az4)

Subnet

subnet-0d95e3399af07f43a
IPv4 subnet CIDR: 10.0.7.0/24

public1 ▾

IPv4 address

Assigned by AWS

us-east-1b (use1-az6)

Subnet

subnet-0b053e3261cbb4135
IPv4 subnet CIDR: 10.0.8.0/24

public2 ▾

IPv4 address

Assigned by AWS

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

Select up to 5 security groups

sg3teir sg-05c7c41fc082a090a VPC: vpc-094f0bf96a7e0bf87

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 HTTP:80

Protocol: HTTP Port: 80 Default action: [Info](#)

Forward to: lb-tq Target type: Instance, IPv4

HTTP Remove

Create target group

Listener tags - optional

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

Add listener tag

You can add up to 50 more tags.

[All (*)]

EC2 > Load balancers > tier1-lb

tier1-lb

Actions

▼ Details

Load balancer type Application	Status Provisioning	VPC vpc-094f0bf96a7e0bf87	Load balancer IP address type IPv4
Scheme Internet-facing	Hosted zone Z355XDOTRQ7X7K	Availability Zones subnet-0d95e3399af07f43a us-east-1a (use1-az4) subnet-0b053e3261cbb4135 us-east-1b (use1-az6)	Date created August 4, 2024, 18:05 (UTC+05:30)
Load balancer ARN arn:aws:elasticloadbalancing:us-east-1:891377141179:loadbalancer/app/tier1-lb/edb0a02281d95520	DNS name Info tier1-lb-823066743.us-east-1.elb.amazonaws.com (A Record)		

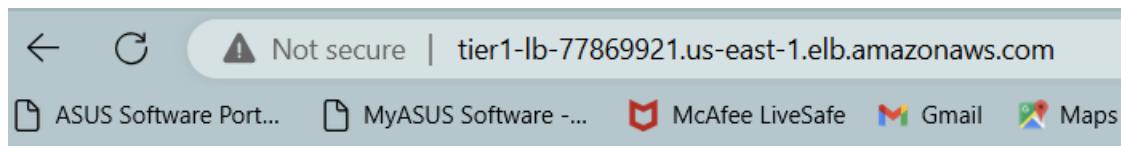
Listeners and rules Network mapping Resource map - new Security Monitoring Integrations Attributes Tags

- Once load balancer created copy the DNS name and paste it in chrome.
- Output shown in below slides.

Not secure | tier1-lb-77869921.us-east-1.elb.amazonaws.com

ASUS Software Port... MyASUS Software ... McAfee LiveSafe Gmail Maps YouTube DXC udemy N

/bin/bash ##### Author-prathibha gariki version-1 ##### hi this is from public1 instance



Auto scaling:

AWS Auto Scaling is a service that automatically adjusts the number of compute resources (such as EC2 instances) based on current demand. This helps maintain performance and optimize costs by scaling your resources up or down according to defined policies

- Create image using instance->select instance and click actions->image and templates->create image.
- Give name tag as my-img under create image field as shown in below slides.

A screenshot of the AWS EC2 Instances page. The left sidebar shows navigation options like EC2 Dashboard, EC2 Global View, Events, and Instances. The Instances section is expanded, showing sub-options like Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, and Capacity Reservations. The main content area shows a table titled "Instances (1/1) Info" with one row. The row details are: Name: project-3tier-p..., Instance ID: i-09bdb991de60cc1b1, Instance state: Running, Instance type: t2.micro, Status check: Initializing, Alarm status: View alarms +, Availability Zone: us-east-1a, Public IPv4: - (IP address is not visible). To the right of the table, there is a context menu with options: Actions ▾, Connect, Instance state ▾, Find Instance by attribute or tag (case-sensitive), All states ▾, Connect, View details, Manage instance state, Instance settings, Networking, Security, Image and templates, Monitor and troubleshoot. A tooltip for the "Actions" menu shows "Launch instances" as the selected option. Below the table, there is a detailed view for the instance i-09bdb991de60cc1b1, titled "project-3tier-public". It shows tabs for Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags. Under the Details tab, there is a "Instance summary" section with fields for Instance ID (i-09bdb991de60cc1b1), Public IPv4 address (not visible), and Private IPv4 addresses (not visible).

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.

Instance ID

i-09bdb991de60cc1b1 (project-3tier-public)

Image name

my-img

Maximum 127 characters. Can't be modified after creation.

Image description - optional

Image description

Maximum 255 characters

No reboot

Enable

Instance volumes

Storage type	Device	Snapshot	Size	Volume type	IOPS	Throughput	Delete on termination	Encrypted
EBS	/...	Create new snap...	8	EBS General Pur...	3000		<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

[Add volume](#)

ⓘ During the image creation process, Amazon EC2 creates a snapshot of each of the above volumes.

- Once image created go to EC2 dashboard and click on templates
- Give name tag as 1tier-template-as->template version as nothing
- Click the network settings and select existing security group as shown in below.

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*

1tier-template-as

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

Template version description

nothing

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)

sg3teir

Storage (volumes)

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel

Create launch template

Network settings [Info](#)

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.

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

[Compare security group rules](#)

Security groups [Info](#)

Select security groups

sg3teir sg-05c7c41fc082a090a X
VPC: vpc-09af0bf96a7e0bf87

► Advanced network configuration

Storage (volumes) [Info](#)

No volume details are currently included in this template. Add a new volume to include it in the launch template

[Add new volume](#)

- Go to auto scaling and click on create auto scaling groups
- Give name tag as 1tier-as
- Select created target group-1tier-template-as
- Select the VPC -> select availability zone us-east-1a (public1 subnet) & us-east-1b (public2 subnet)->click attached to an existing load balancer->select existing target group.

- Give desired capacity as 2, min capacity as 2 and max capacity as 3
 - Select target tracking scaling policy under auto scaling options.
 - Click on create auto scaling.

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1

Choose launch template

Step 2

Choose instance launch options

Step 3 - optional

Configure advanced options

Step 4 - optional

Configure group size and scaling

Step 5 - optional

Add notifications

Step 6 - optional

Add tags

Step 7

Review

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.

1tier-as

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

Launch template Info

i For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

Launch template

Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

1tier-template-as

[Create a launch template](#)

Version

t2.micro/t2.micro/t2.micro/t2.micro

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-094f0bf96a7e0bf87 (project-3tier)
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

us-east-1a | subnet-0d95e3399af07f43a (public1) X
10.0.7.0/24

us-east-1b | subnet-0b053e3261cbb4135 (public2) X
10.0.8.0/24

[Create a subnet](#)

[Cancel](#)

[Skip to review](#)

[Previous](#)

[Next](#)

CONTROL OVER 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.

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 that you want to attach to your Auto Scaling group.

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



lb-tg | HTTP



Application Load Balancer: tier1-lb

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	3
Equal or less than desired capacity	Equal or greater than desired capacity

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

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

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

Scaling policy name
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 ▾

Auto Scaling groups (1) Info									
Create Auto Scaling group < 1 >									
<input type="checkbox"/> Name Launch template/configuration ▾ Instances ▾ Status ▾ Desired capacity ▾ Min ▾ Max ▾ Availability Zones									
<input type="checkbox"/>	Name	1tier-as	1tier-template-as Version Default	2	-	2	2	3	us-east-1a, us-east-1b

Once auto scaling created another 2 extra instances added. Previously 2 instances created and after auto scaling another 2 instances added to total 4 instances.

Instances (4) Info									
<input type="checkbox"/> Connect Instance state ▾ Actions ▾ Launch instances ▾									
<input type="checkbox"/> Find instance by attribute or tag (case-sensitive)									
<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	
<input type="checkbox"/>	project-3tier-public1	i-09bdb991de60cc1b1	Running	t2.micro	2/2 checks passed		us-east-1a	-	
<input type="checkbox"/>		i-067cadfc15561780e	Running	t2.micro	2/2 checks passed		us-east-1a	-	
<input type="checkbox"/>		i-01b094db955c35892	Running	t2.micro	2/2 checks passed		us-east-1b	-	
<input type="checkbox"/>	project-3tier-public2	i-00ebc0136c20c6e9c	Running	t2.micro	2/2 checks passed		us-east-1b	-	

Auto scaling for private subnets:

- Give name tag as 2tier-template-private->template version as nothing
- Click the network settings and select existing security group and click on create launch template as shown in below.

[EC2](#) > [Launch templates](#) > Create launch template

Create launch template

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

Launch template name and description

Launch template name - *required*

2tier-template-private

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

Template version description

nothing

Max 255 chars

▼ Network settings [Info](#)

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.

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

sg3teir sg-05c7c41fc082a090a X
VPC: vpc-094f0bf96a7e0bf87

[Compare security group rules](#)

[Advanced network configuration](#)

▼ Storage (volumes) [Info](#)

EBS Volumes

[Hide details](#)

Volume 1 (AMI Root) / 8 GiB EBS General purpose SSD (gp2)

Software Image (AMI)

my-img
ami-0880189ef7da344d4

Virtual server type (instance type)

t2.micro

Firewall (security group)

sg3teir

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

[Cancel](#)

[Create launch template](#)

- Go to auto scaling and click on create auto scaling groups
- Give name tag as 2tier-as
- Select created target group-2tier-template-private
- Select the VPC -> select availability zone us-east-1a (private1a subnet) & us-east-1b (private2a subnet)->click attached to new load balancer->for load balancer give name tag as lb-private -> click on internet facing->select private1a & private2a subnets under availability zone->click on create target group->give name as lb-tg-private.
- Give desired capacity as 2, min capacity as 2 and max capacity as 3

- Select target tracking scaling policy under auto scaling options.
- Click on create auto scaling.

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1 Choose launch template

Step 2 Choose instance launch options

Step 3 - optional Configure advanced options

Step 4 - optional Configure group size and scaling

Step 5 - optional Add notifications

Step 6 - optional Add tags

Step 7 Review

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.

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

Launch template Info

i For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

Launch template
Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.
 C

[Create a launch template](#)

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.
 C

[Create a VPC](#)

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

X

X

[Create a subnet](#)

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

Load balancing Info

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

No load balancer

Traffic to your Auto Scaling group will not be fronted by a load balancer.

Attach to an existing load balancer

Choose from your existing load balancers.

Attach to a new load balancer

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

Attach to a new load balancer

Define a new load balancer to create for attachment to this Auto Scaling group.

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.

lb-private

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-094f0bf96a7e0bf87 [\[?\]](#)

project-3tier

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.

us-east-1a

subnet-00fb6bf8dca4350df



us-east-1b

subnet-049cc633b1810327b



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.

lb-tq-private

EC2 health checks

Always enabled

Additional health check types - *optional* | [Info](#)

Turn on Elastic Load Balancing health checks Recommended

Elastic Load Balancing monitors whether instances are available to handle requests. When it reports an unhealthy instance, EC2 Auto Scaling can replace it on its next periodic check.

EC2 Auto Scaling will start to detect and act on health checks performed by Elastic Load Balancing.

To avoid unexpected terminations, first verify the settings of these health checks in the [Load Balancer console](#) 



Turn on VPC Lattice health checks

VPC Lattice can monitor whether instances are available to handle requests. If it considers a target as failed a health check, EC2 Auto Scaling replaces it after its next periodic check.

Health check grace period | [Info](#)

This time period delays the first health check until your instances finish initializing. It doesn't prevent an instance from terminating when placed into a non-running state.

seconds

Additional settings

Monitoring | [Info](#)

Enable group metrics collection within CloudWatch

Default instance warmup | [Info](#)

The amount of time that CloudWatch metrics for new instances do not contribute to the group's aggregated instance metrics, as their usage data is not reliable yet.

Enable default instance warmup

[Cancel](#)

[Skin to review](#)

[Previous](#)

[Next](#)

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	3
Equal or less than desired capacity	Equal or greater than desired capacity

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

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

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

After autoscaling for private subnets (private1a & private 2a) another 2 instances added. Previously 4 instances are available after autoscaling another 2 instances added total 6 instances.

Instances (6) Info									
<input type="text"/> Find Instance by attribute or tag (case-sensitive) All states ▾ Connect Instance state ▾ Actions ▾ Launch instances ▼ 									
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	
project-3tier-public1	i-09bdb991de60cc1b1	Running Q Q	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-	98.80.8.145	
	i-0cbe1fe30e7d5c7d6	Running Q Q	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-	-	
	i-067adfc15561780e	Running Q Q	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-	-	
	i-01b094db95c35892	Running Q Q	t2.micro	2/2 checks passed	View alarms +	us-east-1b	-	-	
project-3tier-public2	i-00ebc0136c20c6e9c	Running Q Q	t2.micro	2/2 checks passed	View alarms +	us-east-1b	-	54.81.12.80	
	i-00a9e41d8f366d395	Running Q Q	t2.micro	2/2 checks passed	View alarms +	us-east-1b	-	-	

RDS:

1.DB subnet:

- Go to subnet group and click on create DB subnet group.
- Give name tag as my-3tier-project-db
- Select VPC project-3tier and then click on create DB subnet.

The screenshot shows the AWS RDS Subnet groups page. The left sidebar includes options like Dashboard, Databases, Query Editor, Performance insights, Snapshots, Exports in Amazon S3, Automated backups, Reserved instances, and Proxies. Under the Subnet groups section, there are links for Parameter groups, Option groups, Custom engine versions, Zero-ETL Integrations, Events, and Event subscriptions. A Recommendations section is also present. The main content area displays a table titled 'Subnet groups (0)' with columns for Name, Description, Status, and VPC. A message states 'No db subnet groups' and 'You don't have any db subnet groups.' A prominent orange button at the top right says 'Create DB 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.

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

Description

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 change the VPC identifier after your subnet group has been created.

2.Create database:

- Go to RDS and click on create database
- Click on standard create->click on my SQL engine option->click on multi AZ DB cluster->click production in templates->click on self-managed->create password->click on do not include an ec2 instance-> select VPC->select DB subnet group.
- Public access click yes->select existing security group
- Remaining fields leave as default and click on create database as shown below slides.

Amazon RDS

Dashboard
Databases
Query Editor
Performance insights
Snapshots
Exports in Amazon S3
Automated backups
Reserved instances
Proxies

Subnet groups
Parameter groups
Option groups
Custom engine versions
Zero-ETL integrations [New](#)

RDS > Databases

Introducing Aurora I/O-Optimized
Aurora's I/O-Optimized is a new cluster storage configuration that offers predictable pricing for all applications and improved price-performance, with up to 40% costs savings for I/O-intensive applications.

Consider creating a Blue/Green Deployment to minimize downtime during upgrades
You may want to consider using Amazon RDS Blue/Green Deployments and minimize your downtime during upgrades. A Blue/Green Deployment provides a staging environment for changes to production databases. [RDS User Guide](#) [Aurora User Guide](#)

Databases (0)

Group resources Modify Actions

DB identifier Status Role Engine Region & AZ Size Recommendations CPU Current activity Maintenance VPC Mul

No instances found

RDS > Create database

Create database

Choose a database creation method [Info](#)

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 

MariaDB 

Engine version [Info](#)

View the engine versions that support the following database features.

[▼ Hide filters](#)

Show versions that support the Multi-AZ DB cluster [Info](#)

Create a Multi-AZ DB cluster with one primary DB instance and two readable standby DB instances. Multi-AZ DB clusters provide up to 2x faster transaction commit latency and automatic failover in typically under 35 seconds.

Show versions that support the Amazon RDS Optimized Writes [Info](#)

Amazon RDS Optimized Writes improves write throughput by up to 2x at no additional cost.

Engine Version

MySQL 8.0.35



Enable RDS Extended Support [Info](#)

Amazon RDS Extended Support is a paid offering [↗](#). By selecting this option, you consent to being charged for this offering if you are running your database major version past the RDS end of standard support date for that version. Check the end of standard support date for your major version in the [RDS for MySQL documentation](#) [↗](#).

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

[▼ Credentials Settings](#)

Master username [Info](#)

Type a login ID for the master user of your DB cluster.

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](#)

Password strength Neutral

Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / " @

Confirm master password [Info](#)

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 cluster.

project-3tier (vpc-094f0bf96a7e0bf87)

6 Subnets, 2 Availability Zones



Only VPCs with a corresponding DB subnet group are listed.

⚠ The VPC subnets must be in 3 Availability Zones (AZs) for the Multi-AZ DB cluster. The current subnets are in **2 AZs (us-east-1a, us-east-1b)**. Add a subnet in a different AZ than the current subnets.

[Add new subnet](#)

ⓘ 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 cluster can use in the VPC that you selected.

my-3tier-project-db

2 Subnets, 2 Availability Zones



Public access [Info](#)

Yes

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

No

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

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

sg3teir 

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

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

► Additional configuration

Successfully created database [database-3tier](#)

You can use settings from database-3tier to simplify configuration of [suggested database add-ons](#) while we finish creating your DB for you.

[View connection details](#)

Notifications  0  0  2  0  0

RDS > Databases > database-3tier

database-3tier

[C](#) [Modify](#) [Actions ▾](#)

Related

Filter by databases

DB identifier	Status	Role	Engine	Region & AZ	Size	Recommendations
database-3tier	Available	Multi-AZ DB cluster	MySQL Community	us-east-1	3 instances	
database-3tier-instance-1	Available	Writer instance	MySQL Community	us-east-1a	db.m5d.large	
database-3tier-instance-2	Available	Reader instance	MySQL Community	us-east-1b	db.m5d.large	
database-3tier-instance-3	Available	Reader instance	MySQL Community	us-east-1c	db.m5d.large	

[Connectivity & security](#) | [Monitoring](#) | [Logs & events](#) | [Configuration](#) | [Maintenance & backups](#) | [Tags](#) | [Recommendations](#)

Find resources

Endpoint name	Status	Type	Port
database-3tier.cluster-c9emcoqj2lvz.us-east-1.rds.amazonaws.com	Available	Writer	3306
database-3tier.cluster-ro-c9emcoqj2lvz.us-east-1.rds.amazonaws.com	Available	Reader	3306

Connected compute resources (0) [Info](#)

Connections to compute resources that were created automatically by RDS are shown here. Connections to compute resources that were created manually aren't shown.

Filter by compute resources

Resource identifier	Resource type	Availability Zone	VPC security group	Compute resource security group	Connected proxy
No connected compute resources					

No connected compute resources that were created automatically to display.

Set up EC2 connection Set up Lambda connection

Proxies (0)

Create proxy

connection

Set up EC2 connection [Info](#)

Select EC2 instance

Database

database-3tier [Edit](#)

EC2 instance

Choose the EC2 instance to connect to this database. Only EC2 instances in the same VPC as the database are shown. If no EC2 instances in the same VPC are available, you can create a new EC2 instance.

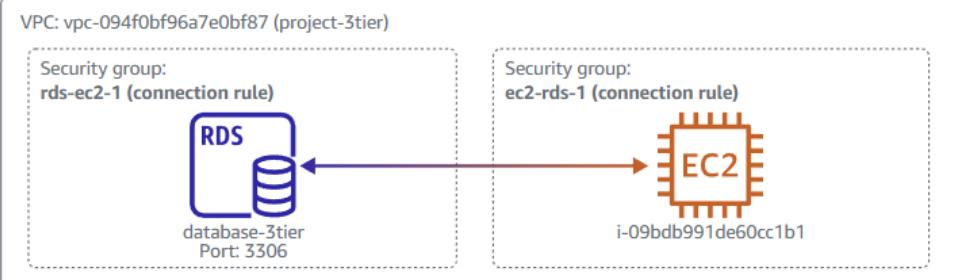
i-09bdb991de60cc1b1
project-3tier-public1 us-east-1a

Create EC2 instance [Edit](#)

Cancel Continue

You are setting up a connection between RDS database [database-3tier](#) and EC2 instance [i-09bdb991de60cc1b1](#).

To set up a connection between the database and the EC2 instance, VPC security group **rds-ec2-1** is added to the database, and VPC security group **ec2-rds-1** is added to the EC2 instance.



Bold indicates an addition being made to set up a connection.

Changes to RDS database: database-3tier

Attribute	Current value	New value
Security group	sg3teir	sg3teir, rds-ec2-1

Changes to EC2 instance: i-09bdb991de60cc1b1

Attribute	Current value	New value
Security group	sg3teir	sg3teir, ec2-rds-1

Cancel

Previous

Set up

Edit VPC settings Info

VPC details

VPC ID
vpc-094f0bf96a7e0bf87
Name
project-3tier

DHCP settings

DHCP option set Info

dopt-01d606309be84088f ▾

DNS settings

- Enable DNS resolution Info
- Enable DNS hostnames Info

Network Address Usage metrics settings

- Enable Network Address Usage metrics Info

[Cancel](#)

[Save](#)

EC2 > Instances > i-09bdb991de60cc1b1 > Connect to instance

Connect to instance Info

Connect to your instance i-09bdb991de60cc1b1 (project-3tier-public1) using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID

[i-09bdb991de60cc1b1 \(project-3tier-public1\)](#)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is project-3tier.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
 chmod 400 "project-3tier.pem"
4. Connect to your instance using its Public DNS:

ec2-98-80-8-145.compute-1.amazonaws.com

Command copied

ssh -i "project-3tier.pem" ubuntu@ec2-98-80-8-145.compute-1.amazonaws.com

i 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.

- Once created the RDS connect to the private instance through public instance.

```
root@ip-10-0-7-30:~$ sudo -i
root@ip-10-0-7-30:~# vi project-3tier.pem
root@ip-10-0-7-30:~# chmod 777 project-3tier.pem
root@ip-10-0-7-30:~# ssh -i "project-3tier.pem" root@10.0.9.36
The authenticity of host '10.0.9.36 (10.0.9.36)' can't be established.
ED25519 key fingerprint is SHA256:Z0AlhjCybm6+dCtfRuf8zeGdYITJow43lwLk/2sKLU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.9.36' (ED25519) to the list of known hosts.
@@@@@@@WARNING: UNPROTECTED PRIVATE KEY FILE! @@@@@
Permissions 0777 for 'project-3tier.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "project-3tier.pem": bad permissions
root@10.0.9.36: Permission denied (publickey).
root@ip-10-0-7-30:~#
```

- Install MY SQL->sudo apt install mysql-server
- Restart ->sudo systemctl start mysql service
- Mysql -h database-3tier.cluster-c9emcoqj2lvz.us-east-1.rds.amazonaws.com(rds end point) - u admin -p->Enter password-> u can connect to my SQL as shown in below

```
root@ip-10-0-7-30:~# mysql -h database-3tier.cluster-c9emcoqj2lvz.us-east-1.rds.amazonaws.com -u admin -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 62
Server version: 8.0.35 Source distribution

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> |
```

- For creating table->

```
CREATE TABLE Persons (
    ID int,
    LastName varchar(255),
    FirstName varchar(255),
    Age varchar(255)
);
```

- Create the table in in my sql
- The output of creating table as shown in below.

```
ERROR 1146 (42S02): Table 'serverproject.secureprojectpersons' doesn't exist
mysql> INSERT INTO Persons (ID, LastName, FirstName, Age) VALUES ('7', 'aws', 'devops', '10');
Query OK, 1 row affected (0.01 sec)

mysql> INSERT INTO Persons (ID, LastName, FirstName, Age) VALUES ('8', 'aws', 'k8s', '8');
Query OK, 1 row affected (0.00 sec)

mysql> select * from Persons;
+----+-----+-----+-----+
| ID | LastName | FirstName | Age |
+----+-----+-----+-----+
|  7 | aws     | devops   | 10  |
|  8 | aws     | k8s     |  8  |
+----+-----+-----+-----+
2 rows in set (0.00 sec)
```