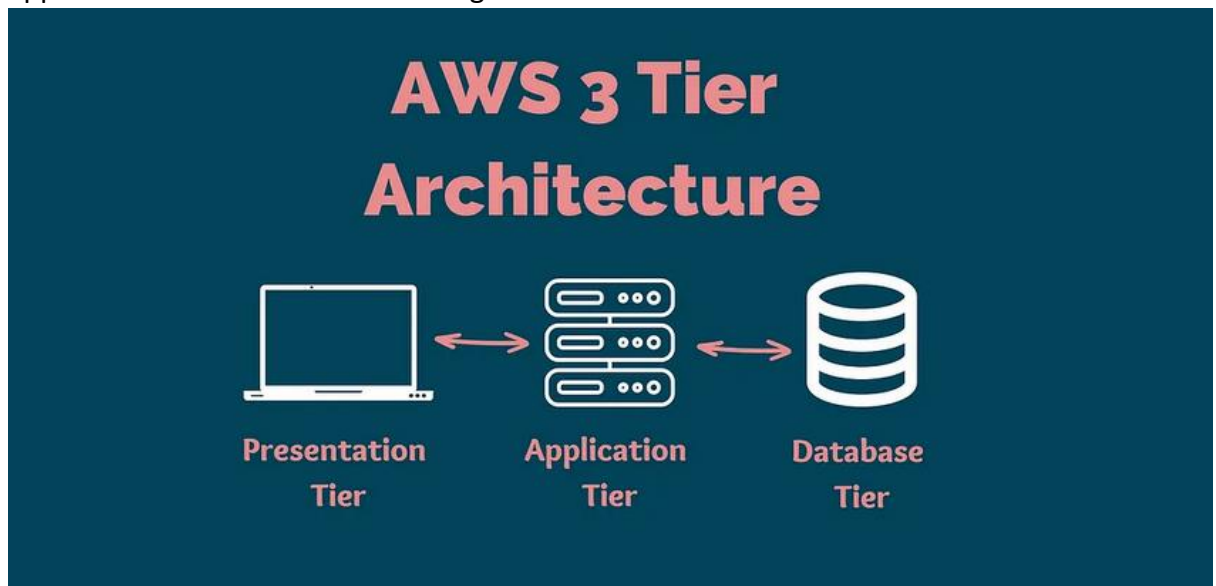


# PROJECT-01

## 3 TIER ARCHITECTURE

### What is three tier architecture?

- Three tier architecture is a well established software application architecture that organizes applications into three logical and physical computing tiers. The presentation tier or web tier, the application tier, and the database tier, where application data is stored and managed.



**Presentation tier :** The presentation tier is the user interface and communication layer of the application, where the end user interacts with the application. Its main purpose is to display information and collect information from the user. Thus top level tier can run on web,desktop application, or a graphical user interface. Web tiers are developed by using HTML,CSS and javascript.

**Application tier :** The application tier is also known as the logic tier or middle tier, is the heart of the application. In application tier the data that is collected in the presentation tier is processed sometimes against other information in the data tier. The application tier can also add, delete, or modify data in the data tier.

**Database tier :** The database tier is also known as data access tier or back-end, is where the information that is processed by the application is stored and managed. This can be a RDS management system such as PostgreSQL, MySQL, MariaDB, Oracle, DB2, Informix or

Microsoft SQL Server, or in a NoSQL Database server such as Cassandra, CouchDB, or MongoDB.

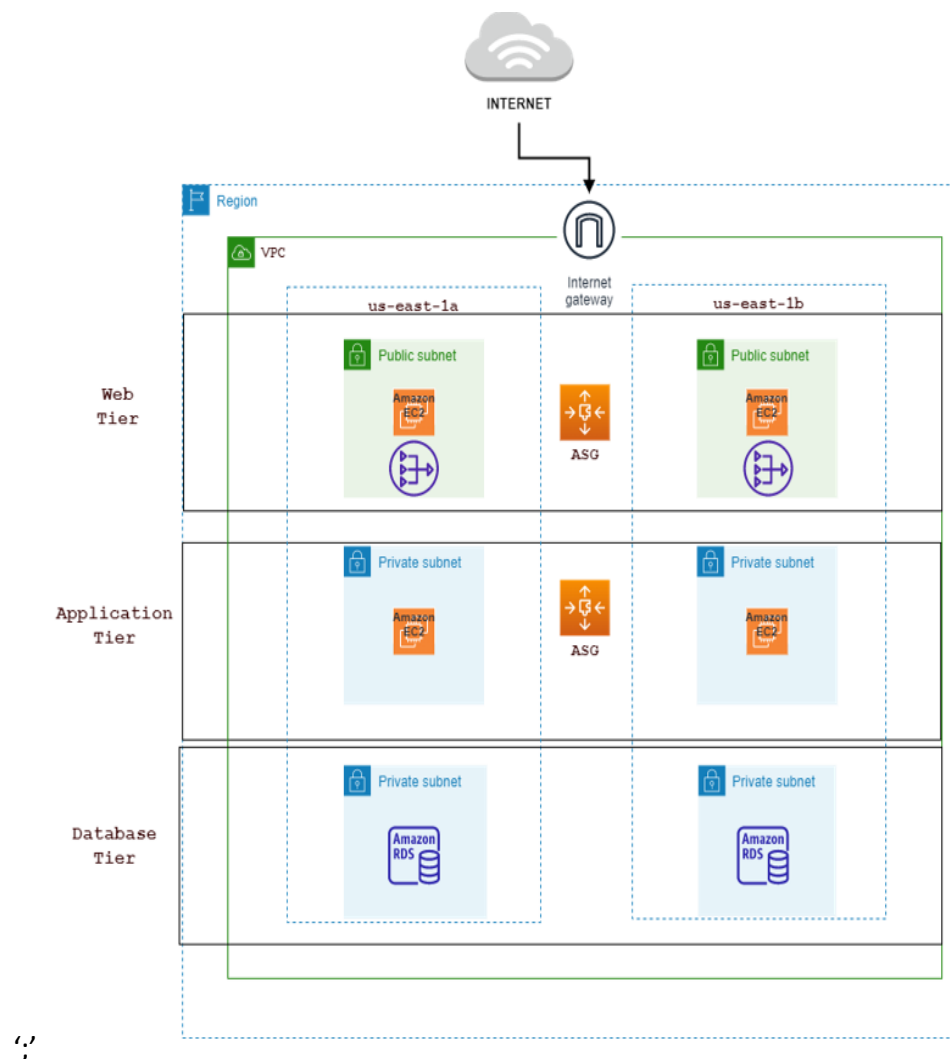
In a three tier application, all communication goes through the application tier. The web tier and the database tier cannot communicate directly with one another.

### Benefits of three tier architecture :

It's a logical and physical separation of functionality. Each tier can run on a separate OS and server platform-for example, web server, application server, database server. And each tier runs on atleast one dedicated server hardware or virtual server, so each services of each tier can be customized and optimized without impacting the other tiers.

And also faster development, improved scalability, improved reliability, and improved security.

### Project:



## VPC :

- Create a VPC with specific name [my-vpc] in a region Mumbai.

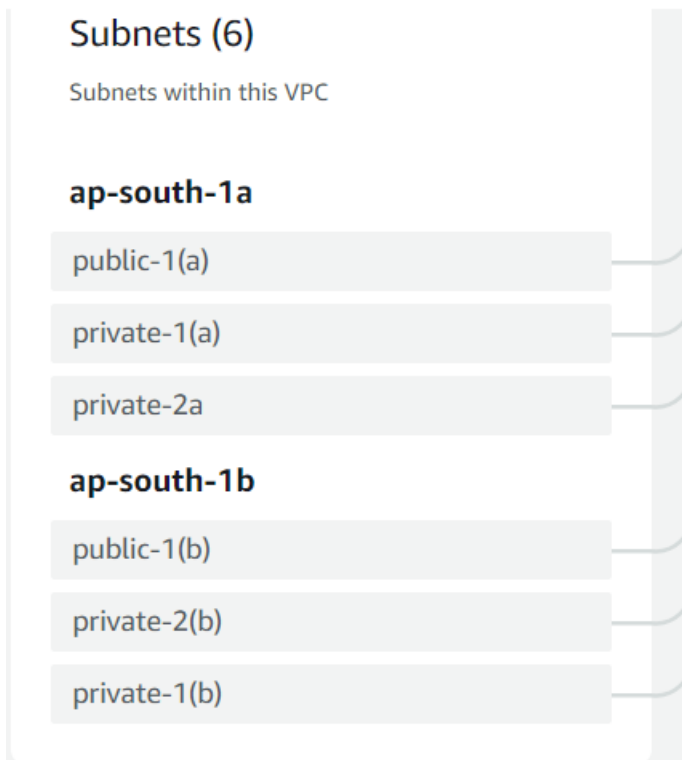
VPC > Your VPCs > vpc-0833c36a909f1fa7a

vpc-0833c36a909f1fa7a / my-vpc Actions ▼

**Details** [Info](#)

VPC ID vpc-0833c36a909f1fa7a	State <span>Available</span>	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set <a href="#">dopt-0f2dc3342626fb6af</a>	Main route table <a href="#">rtb-087217d20e4bed5aa / public-rt</a>	Main network ACL <a href="#">acl-04521a5ae1f42a9e1</a>
Default VPC No	IPv4 CIDR 172.0.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID <a href="#">905418408977</a>	

- Now create 6 subnets [1 public, 2 private subnets in one availability zone and same for the other subnets but in different availability zone] with in the same VPC.



- Create a internet gateway and click on actions and attach it to the respective VPC.

VPC > Internet gateways > igw-05922053b0ec57103

igw-05922053b0ec57103 / igw Actions ▼

**Details** [Info](#)

Internet gateway ID <a href="#">igw-05922053b0ec57103</a>	State <span>Attached</span>	VPC ID <a href="#">vpc-0833c36a909f1fa7a / my-vpc</a>	Owner <a href="#">905418408977</a>
--	--------------------------------	--	---------------------------------------

- And create route tables and associate them with subnets along with the internet connection attaches to the [1a & 2a] public subnets.

VPC > Route tables > rtb-087217d20e4bed5aa

## rtb-087217d20e4bed5aa / public-rt Actions ▾

**Details** [Info](#)

Route table ID rtb-087217d20e4bed5aa	Main Yes	Explicit subnet associations <a href="#">2 subnets</a>	Edge associations –
VPC vpc-0833c36a909f1fa7a   my-vpc	Owner ID 905418408977		

Routes **Subnet associations** Edge associations Route propagation Tags

**Explicit subnet associations (2)** Edit subnet associations

Find subnet association

Name ▾	Subnet ID ▾	IPv4 CIDR ▾	IPv6 CIDR ▾
public-1(a)	<a href="#">subnet-09960df767675b8af</a>	172.0.0.0/22	–
public-1(b)	<a href="#">subnet-03dadda928ca4bfa2</a>	172.0.12.0/24	–

Routes **Subnet associations** Edge associations Route propagation Tags

**Routes (2)** Both ▾ Edit routes

Filter routes

Destination ▾	Target ▾	Status ▾	Propagated ▾
0.0.0.0/0	<a href="#">igw-05922053b0ec57103</a>	Active	No
172.0.0.0/16	local	Active	No

- And also set the public route tables as main route tables.

Route tables (1/4) [Info](#) Refresh Actions ▴ Create route table

Find resources by attribute or tag

<input type="checkbox"/>	Name ▾	Route table ID ▾	Explicit subnet associ... ▾	Edge associations ▾
<input checked="" type="checkbox"/>	public-rt	<a href="#">rtb-087217d20e4bed5aa</a>	<a href="#">2 subnets</a>	–
<input type="checkbox"/>	private-rt	<a href="#">rtb-00395ca1fcaf5508d</a>	<a href="#">4 subnets</a>	–
<input type="checkbox"/>	–	<a href="#">rtb-0e250c6fa86b2a690</a>	–	–
<input type="checkbox"/>	–	<a href="#">rtb-0f4039efbdee14643</a>	–	–

View details > Settings  
Set main route table  
Edit subnet associations [6a909f1fa7a |](#)  
Edit edge associations [6a909f1fa7a |](#)  
Edit route propagation [3c51584d76a](#)  
Edit routes [6a909f1fa7a |](#)  
Manage tags  
Delete route table

- Goto all subnet and click on edit subnets settings to auto assign IPV4.

VPC > Subnets > [subnet-09960df767675b8af](#) > Edit subnet settings

## Edit subnet settings [Info](#)

**Subnet**

Subnet ID subnet-09960df767675b8af	Name public-1(a)
---------------------------------------	---------------------

**Auto-assign IP settings** [Info](#)

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

☒ Enable auto-assign public IPv4 address [Info](#)  
☐ Enable auto-assign customer-owned IPv4 address [Info](#)  
Option disabled because no customer owned pools found.

- Create a Nat gateway for one way traffic attach to the private route table.

VPC > NAT gateways > nat-09d020a78b23c0807

nat-09d020a78b23c0807 / nat-gw

Actions

Details

NAT gateway ID  
nat-09d020a78b23c0807

NAT gateway ARN  
arn:aws:ec2:ap-south-1:905418408977:natgateway/nat-09d020a78b23c0807

VPC  
vpc-0833c36a909f1fa7a / my-vpc

Connectivity type  
Public

Primary public IPv4 address  
13.200.42.29

Subnet  
subnet-09960df767675b8af / public-1(a)

State  
Available

Primary private IPv4 address  
172.0.3.149

Created  
Thursday, March 21, 2024 at 09:36:51 GMT+5:30

State message  
Info

Primary network interface ID  
eni-07167b95a82d0a81a

Deleted

VPC > Route tables > rtb-00395ca1fc5508d

rtb-00395ca1fc5508d / private-rt

Actions

Details Info

Route table ID  
rtb-00395ca1fc5508d

VPC  
vpc-0833c36a909f1fa7a | my-vpc

Main  
No

Owner ID  
905418408977

Explicit subnet associations  
4 subnets

Edge associations

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Both Edit routes

Filter routes

< 1 > ⚙

Destination	Target	Status	Propagated
0.0.0.0/0	nat-09d020a78b23c0807	Active	No
172.0.0.0/16	local	Active	No

- After all connections established in VPC.



### Web tier:

- create a web tier launch template

## 1. Give a specific name my-template1

### 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*

launch

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

Template version description

A prod webserver for MyApp

Max 255 chars

Auto Scaling guidance [Info](#)

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

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

## 2. Click on AMI: ubuntu

### ▼ 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

Q

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

Recents

Quick Start

Don't include in launch template

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu®

Windows

Microsoft

Red H

Red

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

#### Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type

Free tier eligible ▼

ami-007020fd9c84e18c7 (64-bit (x86)) / ami-09c443d9277298026 (64-bit (Arm))

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

#### Description

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2024-03-01

### 3. Instance type: t2 micro (1GB – free tier)

**▼ Instance type** [Info](#) | [Get advice](#) Advanced

Instance type

t2.micro Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true

On-Demand Linux base pricing: 0.0124 USD per Hour

On-Demand Windows base pricing: 0.017 USD per Hour

On-Demand RHEL base pricing: 0.0724 USD per Hour

On-Demand SUSE base pricing: 0.0124 USD per Hour

☐ All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

### 4. A new or existing key pair

**▼ Key pair (login)** [Info](#)

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

Key pair name

dell

[Create new key pair](#)

### 5. Create a new security group and add inbound rules for SSH & HTTP

[EC2](#) > [Security Groups](#) > sg-05975b4c8d233ec13 - my-secure-1

sg-05975b4c8d233ec13 - my-secure-1 Actions ▼

**Details**

Security group name	Security group ID	Description	VPC ID
my-secure-1	sg-05975b4c8d233ec13	allow	vpc-0833c36a909f1fa7a <a href="#">link</a>
Owner	Inbound rules count	Outbound rules count	
905418408977	3 Permission entries	2 Permission entries	

### 6. Now let's launch the template

[EC2](#) > [Launch templates](#) > lanuch

lanuch (lt-059f38721aac21b2a) Actions ▼ Delete template

**Launch template details**

Launch template ID	Launch template name	Default version	Owner
lt-059f38721aac21b2a	lanuch	1	arn:aws:iam:905418408977:root

[Details](#) | [Versions](#) | [Template tags](#)

- Create auto-scaling with following settings
  1. Click on the auto scaling group and give a name
  2. Attach the created templet
  3. Select the created VPC [i.e. my-vpc] along with two public subnets
  4. Create a new application load balancer with target groups

## 5. Configure the group size and scaling for desired capacity servers needed.

Details
Activity
Automatic scaling
Instance management
Monitoring
Instance refresh

Group details
Edit

Auto Scaling group name auto-1	Desired capacity 2	Desired capacity type Units (number of instances)	Amazon Resource Name (ARN) arn:aws:autoscaling:ap-south-1:905418408977:autoScalingGroup:dc7cf54d-2813-424c-8c0b-8b7c4453303c:autoScalingGroupName/auto-1
Date created Thu Mar 21 2024 09:49:36 GMT+0530 (India Standard Time)	Minimum capacity 2	Status -	
	Maximum capacity 5		

Launch template
Edit

Launch template lt-059f38721aac21b2a lanuch	AMI ID ami-007020fd9c84e18c7	Instance type t2.micro	Owner arn:aws:iam::905418408977:root
Version Default	Security groups -	Security group IDs sg-05975b4c8d233ec13	Create time Thu Mar 21 2024 09:44:13 GMT+0530 (India Standard Time)

- Now we can go to EC2 to check whether the 2 instances are running successfully by using auto scaling.

Instances (2) Info
Connect
Instance state
Actions
Launch instances

Find Instance by attribute or tag (case-sensitive)
All states

pub
Clear filters

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DN!
<input type="checkbox"/>	pub-1	i-074155ed3c349680d	Running	t2.micro	2/2 checks passed	View alarms	ap-south-1b	-
<input type="checkbox"/>	pub-2	i-07765a7f7b1561bfb	Running	t2.micro	2/2 checks passed	View alarms	ap-south-1a	-

- Let's try to connect one of the instances in web.

```
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/pro

System information as of Thu Mar 21 05:04:13 UTC 2024

System load:  0.0           Processes:            96
Usage of /:   20.7% of 7.57GB Users logged in:        0
Memory usage: 20%           IPv4 address for eth0: 172.0.12.247
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Thu Mar 21 04:24:26 2024 from 13.233.177.3
ubuntu@ip-172-0-12-247:~$ sudo -i
root@ip-172-0-12-247:~#
```



## Application tier:

- Create a web tier launch template
  1. Give a specific name my-template2
  2. AMI: Ubuntu
  3. Instance type: t2.micro [1GB-free tier]
  4. New or existing key pair
  5. Create a new security group and add inbound rules for SSH & HTTP
  6. Now let's launch template

EC2 > Launch templates > lanuch

lanuch (lt-059f38721aac21b2a) Actions ▾ Delete template

**Launch template details**

Launch template ID	Launch template name	Default version	Owner
lt-059f38721aac21b2a	lanuch	1	arn:aws:iam::905418408977:root

[Details](#) | [Versions](#) | [Template tags](#)

- Create auto-scaling group and give a name
  1. Click on auto-scaling group and give a name
  2. Attach the created template
  3. Select 3-tier-vpc along with two private subnets
  4. Create a new application load balancer with target groups
  5. Configure the group size and scaling for desired capacity servers needed

[Details](#) | [Activity](#) | [Automatic scaling](#) | [Instance management](#) | [Monitoring](#) | [Instance refresh](#)

**Group details** Edit

Auto Scaling group name auto-2	Desired capacity 2	Desired capacity type Units (number of instances)	Amazon Resource Name (ARN) arn:aws:autoscaling:ap-south-1:905418408977:autoScalingGroup:fb9d248d-b3ef-4daf-bb92-767d891527b0:autoScalingGroupName/auto-2
Date created Thu Mar 21 2024 09:53:06 GMT+0530 (India Standard Time)	Minimum capacity 2	Status -	
	Maximum capacity 5		

**Launch template** Edit

Launch template lt-059f38721aac21b2a lanuch	AMI ID ami-007020fd9c84e18c7	Instance type t2.micro	Owner arn:aws:iam::905418408977:root
Version Default	Security groups -	Security group IDs sg-05975b4c8d233ec13	Create time Thu Mar 21 2024 09:44:13 GMT+0530 (India Standard Time)

- Now we can see that two more instances using auto scaling are created within two private subnets that I have assigned a specific name to identify the private subnets as

private1 & private.

Instances (2) [Info](#) Refresh Connect Instance state ▾ Actions ▾ Launch instances ▾

All states ▾

Instance state = running × pri × Clear filters < 1 > ⚙

<input type="checkbox"/>	Name ↗	Instance ID	Instance state ▾	Instance type ▾	Status check	Alarm status	Availability Zone ▾	Public IPv4 DNS
<input type="checkbox"/>	pri-2	i-0565856acca5a29ee	Running 🔍	t2.micro	2/2 checks passed	<a href="#">View alarms +</a>	ap-south-1b	-
<input type="checkbox"/>	pri-1	i-0bf78cabacca67090	Running 🔍	t2.micro	2/2 checks passed	<a href="#">View alarms +</a>	ap-south-1a	-

- Lets connect to the private EC2 instance from the public by using the key.pem

```
root@ip-172-0-12-247:~# ssh -i "key.pem" ubuntu@172.0.20.44
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-1014-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Thu Mar 21 05:09:52 UTC 2024

System load:  0.0                       Processes:            96
Usage of /:   20.7% of 7.57GB           Users logged in:     0
Memory usage: 21%                       IPv4 address for eth0: 172.0.20.44
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Thu Mar 21 04:27:26 2024 from 172.0.12.247
ubuntu@ip-172-0-20-44:~$ sudo -i
root@ip-172-0-20-44:~#
```

## Data tier :

- Create a security group add inbound and outbound rules for MySQL/Aurora.

Inbound rules (3)

🔄

Manage tags

Edit inbound rules

🔍 Search

< 1 > ⚙️

<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range
<input type="checkbox"/>	-	sgr-0f24eee93bc63a24c	IPv4	SSH	TCP	22
<input type="checkbox"/>	-	sgr-03ed6b915b56e25f3	IPv4	Custom TCP	TCP	0
<input type="checkbox"/>	-	sgr-0fdc6da2d9cd8beba	IPv4	MySQL/Aurora	TCP	3306

Inbound rules

Outbound rules

Tags

Outbound rules (2)

🔄

Manage tags

Edit outbound rules

🔍 Search

< 1 > ⚙️

<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range
<input type="checkbox"/>	-	sgr-08e4fb10a3dfb7425	IPv4	All traffic	All	All
<input type="checkbox"/>	-	sgr-09802ab3f6e7d4a93	IPv4	MySQL/Aurora	TCP	3306

- Create a database subnet groups by attaching 2 private subnets which are in different availability zones in RDS and attach my-vpc.

Subnet group details

VPC ID

vpc-0833c36a909f1fa7a [🔗](#)

ARN

arn:aws:rds:ap-south-1:905418408977:subgrp:sb-1

Supported network types

IPv4

Description

allow

Subnets (2)

Availability zone	Subnet ID	CIDR block
ap-south-1b	<a href="#">subnet-0e6c243f4a1e920e2</a> <a href="#">🔗</a>	172.0.52.0/24
ap-south-1a	<a href="#">subnet-024fd226e06ab2496</a> <a href="#">🔗</a>	172.0.32.0/22

- Now create [relational database] database.

RDS > Databases > database-1

## database-1

### Summary

DB identifier database-1	Status Available	Role Instance	Engine MySQL Community	Recommendations
CPU 3.05%	Class db.t3.micro	Current activity 0 Connections	Region & AZ ap-south-1a	

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

### Connectivity & security

Endpoint & port	Networking	Security
Endpoint database-1.clqsiq2k4wi3.ap-south-1.rds.amazonaws.com	Availability Zone ap-south-1a VPC	VPC security groups <a href="#">my-secure-1 (sg-05975b4c8d233ec13)</a>

- Connect to the database.
  1. Connect to the server
  2. Install MySQL
  3. And enter command `MySQL -h YOUR_DB_ENDPOINT -P 3306 -u`

`YOUR_DB_USERNAME -p` in this command instead of `your_db_endpoint` we should enter our database endpoint and also edit username as well after that enter password that you have given while creating a relational database.

```
[ec2-user@ip-10-0-156-224 ~]$ mysql -h brainiac-webapp-db.cgwzuzkgdaxy.us-east-1
.rds.amazonaws.com -P 3306 -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 115
Server version: 8.0.28 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)]> |
```

