

Two-Tier AWS Web Application with Private Database

1. Project Overview

This project demonstrates a secure two-tier architecture on AWS where:

- A public web server hosts a website and backend service.
- A private database server hosts MariaDB with no public access.
- The database can still access the internet only for updates and patching using a NAT Gateway.

The project focuses on real-world AWS networking, security, troubleshooting, and cost awareness.

2. Architecture Summary

High-Level Design

- VPC with a custom IPv4 CIDR
- Public Subnet
 - Web EC2 instance
 - Internet Gateway attached to VPC
- Private Subnet
 - DB EC2 instance (MariaDB)
 - No public IP
- NAT Gateway (Public, Regional)
 - Provides outbound internet access to private subnet
- Security Groups
 - Web SG: allows HTTP (80) and SSH (22 from admin IP)
 - DB SG: allows MySQL (3306) and SSH only from Web SG

Traffic Flow

- User → Web EC2 (HTTP)
- Web EC2 → DB EC2 (MySQL via private IP)
- DB EC2 → Internet (updates via NAT Gateway)

3. AWS Resources Used

Resource	Purpose
VPC	Network isolation
Public Subnet	Hosts web server
Private Subnet	Hosts database server
Internet Gateway	Internet access for public subnet
NAT Gateway (Regional, Public)	Outbound internet for private subnet
EC2 (Web)	Apache + Node.js backend
EC2 (DB)	MariaDB server
Security Groups	Traffic control
Route Tables	Traffic routing

4. Step-by-Step Implementation

4.1 VPC and Networking Setup

- Created a VPC with CIDR block (example: **10.0.0.0/16**).
- Created:
 - **public-subnet**
 - **private-subnet**
- Attached Internet Gateway to the VPC.

Route Tables

- Public Route Table:
 - **0.0.0.0/0** → **Internet Gateway**
 - Private Route Table:
 - **10.0.0.0/16** → **local**
 - **0.0.0.0/0** → **NAT Gateway**
-

4.2 Web Server EC2 (Public)

Configuration:

- Amazon Linux 2023
- Public IP enabled
- Security Group allows:
 - HTTP (80) from **0.0.0.0/0**
 - SSH (22) from admin IP

Installed Services:

```
sudo dnf install httpd nodejs -y
```

```
sudo systemctl start httpd
```

```
sudo systemctl enable httpd
```

Website Deployment:

- Copied frontend files to:

```
/var/www/html/
```

- Verified website access via:

http://<Web-EC2-Public-IP>

4.3 Private Database EC2

Configuration:

- Amazon Linux 2023
- No public IP
- Placed in private subnet
- Security Group allows:
 - MySQL (3306) only from Web SG
 - SSH (22) only from Web SG

Access Method:

- SSH hop:

Laptop → Web EC2 → DB EC2

4.4 NAT Gateway Setup

Reason:

Private subnet cannot access the internet directly. NAT Gateway enables outbound-only access.

Configuration:

- NAT Gateway type: Public
- Availability mode: Regional
- Elastic IP: Automatic allocation

Troubleshooting:

- Encountered **Blackhole** route status
- Resolved by re-adding the **0.0.0.0/0 → NAT Gateway** route after NAT became **Available**

4.5 MariaDB Installation and Configuration

After NAT was active:

```
sudo dnf install mariadb105-server -y
```

```
sudo systemctl start mariadb
```

```
sudo systemctl enable mariadb
```

Database Security:

```
sudo mysql_secure_installation
```

Database and User Creation:

```
CREATE DATABASE lokha_db;
```

```
CREATE USER 'lokha_user'@'%' IDENTIFIED BY 'StrongPassword';
```

```
GRANT ALL PRIVILEGES ON lokha_db.* TO 'lokha_user'@'%';
```

```
FLUSH PRIVILEGES;
```

4.6 Web → DB Connectivity Test

From Web EC2:

```
mysql -h <DB-PRIVATE-IP> -u lokha_user -p
```

Result:

- Successful connection
- Confirms:
 - DB has no public access

- Only web server can connect
-

4.7 Node.js Backend Integration

- Installed dependencies using:

`npm install`

- Backend started with:

`node server.js`

Issue Faced:

- Frontend showed **connection lost**

Root Cause:

- Frontend JavaScript was calling:

`http://localhost:3000`

- **localhost** in browser refers to user's PC, not EC2

Fix:

- Updated frontend API URL to:

`http://<Web-EC2-Public-IP>:3000`

5. Common Issues & Troubleshooting

Issue

Cause

Resolution

`dnf install`
timeout

No internet in private subnet

Added NAT Gateway

SSH permission
denied

Missing key on web EC2

Converted `.ppk` to
`.pem`

MariaDB access
denied

User/host mismatch or
password

Recreated DB user

`Cannot GET /`

No root route in Node.js

Expected behavior

`connection lost`

Frontend using localhost

Used EC2 public IP

6. Security Best Practices Followed

- Database has no public IP
- Security group references instead of CIDR for DB access
- NAT Gateway used instead of public DB exposure
- Root DB login disabled remotely
- Separate DB user for application

7. Screenshots

Screenshot of the AWS Management Console showing the EC2 Instances page. The console displays a list of instances, including 'server1' (i-05e0eb9c6382e55be) in the 'Running' state. The instance details for 'server1' are shown, including its VPC ID, Subnet ID, Availability Zone, and IP addresses. The instance is running on a t2.micro instance type in the ap-south-1 region.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
dbserver1	i-001eb6ad759d9838b	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1a	-	-	-	-
server1	i-05e0eb9c6382e55be	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1a	-	65.1.131.25	-	-

i-05e0eb9c6382e55be (server1)

Details | Status and alarms | Monitoring | Security | **Networking** | Storage | Tags

VPC ID: vpc-05e79e19cf17eb848 (project-vpc-last25) | Subnet ID: subnet-0466c756f12fed704 (public-subnet) | Availability zone: ap-south-1a

Availability zone ID: ap-s1-az1 | Outpost ID: -

Public IPv4 address: 65.1.131.25 | Private IPv4 addresses: 10.0.1.211 | IPv6 addresses: -

Secondary private IPv4 addresses: - | Carrier IP addresses (ephemeral): -

Hostname and DNS: Public DNS: - | Private IP DNS name (IPv4 only): ip-10-0-1-211.ap-south-1.compute.internal | IPv4-only IP based name: A record only | Public hostname type: Activate Windows

1.server1

Screenshot of the AWS Management Console showing the EC2 Instances page. The console displays a list of instances, including 'dbserver1' (i-001eb6ad759d9838b) in the 'Running' state. The instance details for 'dbserver1' are shown, including its VPC ID, Subnet ID, Availability Zone, and IP addresses. The instance is running on a t2.micro instance type in the ap-south-1 region.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
dbserver1	i-001eb6ad759d9838b	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1a	-	-	-	-
server1	i-05e0eb9c6382e55be	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1a	-	65.1.131.25	-	-

i-001eb6ad759d9838b (dbserver1)

Details | Status and alarms | Monitoring | Security | **Networking** | Storage | Tags

VPC ID: vpc-05e79e19cf17eb848 (project-vpc-last25) | Subnet ID: subnet-0c4ff6c991221909 (private-subnet) | Availability zone: ap-south-1a

Availability zone ID: ap-s1-az1 | Outpost ID: -

Public IPv4 address: - | Private IPv4 addresses: 10.0.2.232 | IPv6 addresses: -

Secondary private IPv4 addresses: - | Carrier IP addresses (ephemeral): -

Hostname and DNS: Public DNS: - | Private IP DNS name (IPv4 only): ip-10-0-2-232.ap-south-1.compute.internal | IPv4-only IP based name: A record only | Public hostname type: Activate Windows

2.database server

RouteTables | VPC Console | Instances | EC2 | ap-south-1 | Billing and Cost Management | ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTables:

Route tables (1/9)

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Owner ID
project-vpc-rtb-public	rtb-0fa88051290276b85	-	-	No	vpc-00a78809467770ea6 proj...	581483106531
-	rtb-0deaac8fbcc4c46c84	-	-	Yes	vpc-00a78809467770ea6 proj...	581483106531
project-vpc-rtb-private1-ap-south-1a	rtb-04310d858d7782b32	-	-	No	vpc-00a78809467770ea6 proj...	581483106531
-	rtb-059a7d9b4c4a0f09a	-	-	Yes	vpc-0e6feb31f67cea745 proj...	581483106531
project-vpc-rtb-private2-ap-south-1b	rtb-00a7d03d294f47b25	-	-	No	vpc-00a78809467770ea6 proj...	581483106531
-	rtb-0d7a8011cb259bf3	-	-	Yes	vpc-05a79e19cf17eb848 proj...	581483106531
public-rt	rtb-0b41dd0e03784a1ba	subnet-0466c756f12fed7...	-	No	vpc-05a79e19cf17eb848 proj...	581483106531
private-rt	rtb-08f785146a2152cc5	subnet-0c4ffebc9912219...	-	No	vpc-05a79e19cf17eb848 proj...	581483106531
-	rtb-0e507d0987f863bb	nat-1fc1cd59a81ec...	No	No	vpc-05a79e19cf17eb848 proj...	581483106531

rtb-08f785146a2152cc5 / private-rt

Details

Route table ID: rtb-08f785146a2152cc5

Main: No

Explicit subnet associations: subnet-0c4ffebc991221909 / private-subnet

Edge associations: -

VPC: vpc-05a79e19cf17eb848 | project-vpc-last25

Owner ID: 581483106531

Activate Windows
Go to Settings to activate Windows.

3.Routetable-private

RouteTables | VPC Console | Instances | EC2 | ap-south-1 | Billing and Cost Management | ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTables:

Route tables (1/9)

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Owner ID
project-vpc-rtb-public	rtb-0fa88051290276b85	-	-	No	vpc-00a78809467770ea6 proj...	581483106531
-	rtb-0deaac8fbcc4c46c84	-	-	Yes	vpc-00a78809467770ea6 proj...	581483106531
project-vpc-rtb-private1-ap-south-1a	rtb-04310d858d7782b32	-	-	No	vpc-00a78809467770ea6 proj...	581483106531
-	rtb-059a7d9b4c4a0f09a	-	-	Yes	vpc-0e6feb31f67cea745 proj...	581483106531
project-vpc-rtb-private2-ap-south-1b	rtb-00a7d03d294f47b25	-	-	No	vpc-00a78809467770ea6 proj...	581483106531
-	rtb-0d7a8011cb259bf3	-	-	Yes	vpc-05a79e19cf17eb848 proj...	581483106531
public-rt	rtb-0b41dd0e03784a1ba	subnet-0466c756f12fed7...	-	No	vpc-05a79e19cf17eb848 proj...	581483106531
private-rt	rtb-08f785146a2152cc5	subnet-0c4ffebc9912219...	-	No	vpc-05a79e19cf17eb848 proj...	581483106531
-	rtb-0e507d0987f863bb	nat-1fc1cd59a81ec...	No	No	vpc-05a79e19cf17eb848 proj...	581483106531

rtb-0b41dd0e03784a1ba / public-rt

Details

Route table ID: rtb-0b41dd0e03784a1ba

Main: No

Explicit subnet associations: subnet-0466c756f12fed704 / public-subnet

Edge associations: -

VPC: vpc-05a79e19cf17eb848 | project-vpc-last25

Owner ID: 581483106531

Activate Windows
Go to Settings to activate Windows.

4.Routetable-public

Screenshot of the AWS Management Console showing the NAT gateways page. The console displays a table of NAT gateways, with one gateway named 'project-nat' (ID: nat-1fc1cd59a81ecf504) listed. The gateway is in the 'Available' state, connected to a public route table (rtb-0e507d098...), and has a primary public IP address of 13.205.99.145. The console also shows the details of the gateway, including its NAT gateway ID, ARN, VPC, and connectivity type (Public).

NAT gateways (1/1)

Name	NAT gateway ID	Connectivity...	State	State message	Availability ...	Route table ID	Primary public IP ...	Primary private L...	Primary network...
project-nat	nat-1fc1cd59a81ecf504	Public	Available	-	Regional	rtb-0e507d098...	13.205.99.145	-	-

Details

NAT gateway ID: nat-1fc1cd59a81ecf504

NAT gateway ARN: arn:aws:ec2:ap-south-1:581483106531:natgateway/nat-1fc1cd59a81ecf504

VPC: vpc-05a79e19cf17eb848 / project-vpc-las25

Availability mode: Regional

Connectivity type: Public

Method of EIP allocation: Automatic

State: Available

Created: Wednesday, December 31, 2025 at 17:45:14 GMT+5:30

State message: Deleted

5.Nat gateways

Screenshot of the AWS Management Console showing the Elastic IP addresses page. The console displays a table of Elastic IP addresses, with one address (13.205.99.145) listed. The address is a public IP, allocated to the instance eipalloc-02b80afac31145921, and is associated with the NAT gateway nat-1fc1cd59a81ecf504. The console also shows the details of the address, including its allocation ID, reverse DNS record, and associated instance ID.

Elastic IP addresses (1/1)

Name	Allocated IPv4 addr...	Type	Allocation ID	Reverse DNS record	Associated instance ID	Private IP address	Association ID
-	13.205.99.145	Public IP	eipalloc-02b80afac31145921	-	-	13.205.99.145	eipassoc-0015b52a9a1631a08

Summary

Allocated IPv4 address: 13.205.99.145

Association ID: eipassoc-0015b52a9a1631a08

Network interface ID: -

Address pool: Amazon

Type: Public IP

Scope: VPC

Network interface owner account ID: -

Network border group: ap-south-1

Allocation ID: eipalloc-02b80afac31145921

Associated instance ID: -

Public DNS: -

Service managed: rnat

Reverse DNS record: -

Private IP address: 13.205.99.145

NAT Gateway ID: nat-1fc1cd59a81ecf504 (project-nat)

6.Elastic IP

Subnets (1/5) info

Find subnets by attribute or tag

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 CIDR association ID
-	subnet-08eb071b861d76e72	Available	vpc-0e6feb31f67cea745	Off	172.31.0.0/20	-	-
-	subnet-08f9cd372dc22cb54	Available	vpc-0e6feb31f67cea745	Off	172.31.16.0/20	-	-
-	subnet-0dd8c04de5f7db21a	Available	vpc-0e6feb31f67cea745	Off	172.31.32.0/20	-	-
public-subnet	subnet-0466c756f12fed7d4	Available	vpc-05e79e19cf17eb848 proje...	Off	10.0.1.0/24	-	-
private-subnet	subnet-0c4ffe6c991221909	Available	vpc-05e79e19cf17eb848 proje...	Off	10.0.2.0/24	-	-

subnet-0c4ffe6c991221909 / private-subnet

Details | Flow logs | Route table | Network ACL | CIDR reservations | Sharing | Tags

Details

Subnet ID: subnet-0c4ffe6c991221909

Subnet ARN: arn:aws:ec2:ap-south-1:581483106531:subnet/subnet-0c4ffe6c991221909

State: Available

IPv4 CIDR: 10.0.2.0/24

Available IPv4 addresses: 250

Availability Zone: ap-south-1a (ap-south-1a)

Network ACL: -

Auto-assign customer-owned IPv4 address: No

Subnet border group: ap-south-1

Default subnet: No

Customer-owned IPv4 pool: -

Block Public Access: Off

IPv6 CIDR association ID: -

VPC: vpc-05e79e19cf17eb848 | project-vpc-las25

Auto-assign public IPv4 address: No

Outpost ID: -

Route table: rtb-08f785146a2152c65 | private-rt

Auto-assign IPv6 address: No

IPv4 CIDR reservations: -

Activate Windows. Go to Settings to activate Windows.

7.Private subnet

Subnets (1/5) info

Find subnets by attribute or tag

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 CIDR association ID
-	subnet-08eb071b861d76e72	Available	vpc-0e6feb31f67cea745	Off	172.31.0.0/20	-	-
-	subnet-08f9cd372dc22cb54	Available	vpc-0e6feb31f67cea745	Off	172.31.16.0/20	-	-
-	subnet-0dd8c04de5f7db21a	Available	vpc-0e6feb31f67cea745	Off	172.31.32.0/20	-	-
public-subnet	subnet-0466c756f12fed7d4	Available	vpc-05e79e19cf17eb848 proje...	Off	10.0.1.0/24	-	-
private-subnet	subnet-0c4ffe6c991221909	Available	vpc-05e79e19cf17eb848 proje...	Off	10.0.2.0/24	-	-

subnet-0466c756f12fed7d4 / public-subnet

Details | Flow logs | Route table | Network ACL | CIDR reservations | Sharing | Tags

Details

Subnet ID: subnet-0466c756f12fed7d4

Subnet ARN: arn:aws:ec2:ap-south-1:581483106531:subnet/subnet-0466c756f12fed7d4

State: Available

IPv4 CIDR: 10.0.1.0/24

Available IPv4 addresses: 250

Availability Zone: ap-south-1a (ap-south-1a)

Network ACL: -

Auto-assign customer-owned IPv4 address: No

Subnet border group: ap-south-1

Default subnet: No

Customer-owned IPv4 pool: -

Block Public Access: Off

IPv6 CIDR association ID: -

VPC: vpc-05e79e19cf17eb848 | project-vpc-las25

Auto-assign public IPv4 address: No

Outpost ID: -

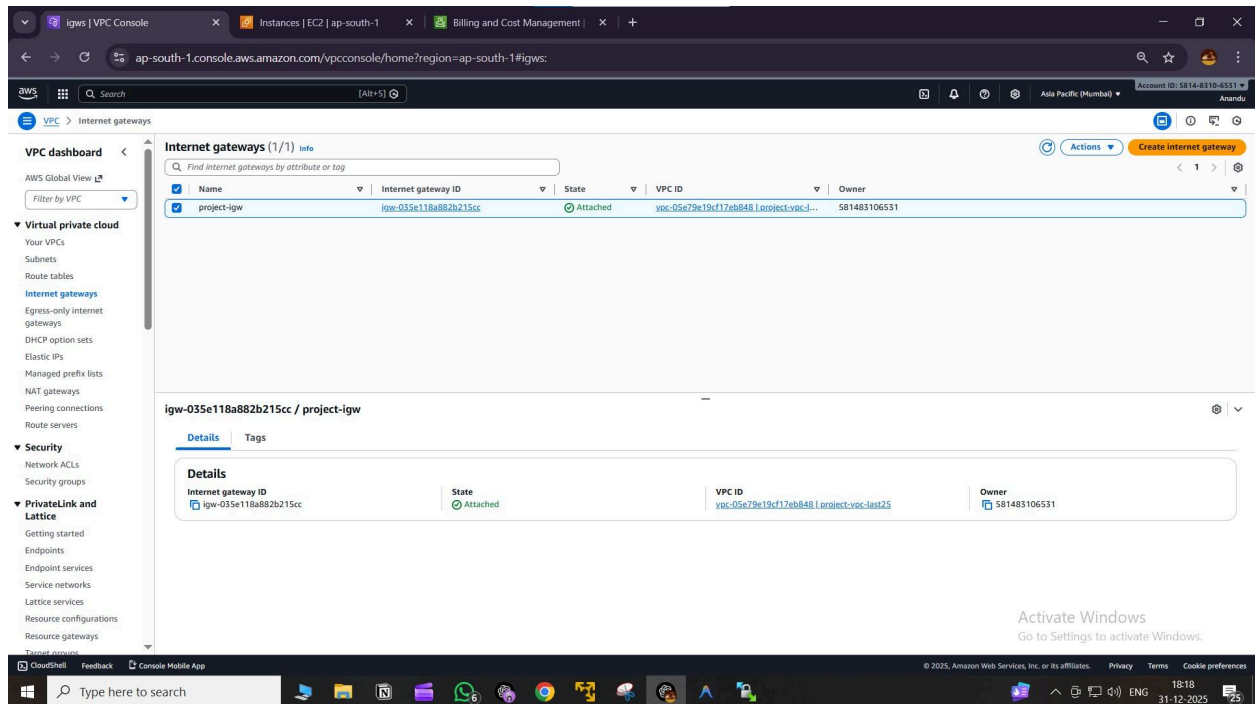
Route table: rtb-0b41dd0e03784a1ba | public-rt

Auto-assign IPv6 address: No

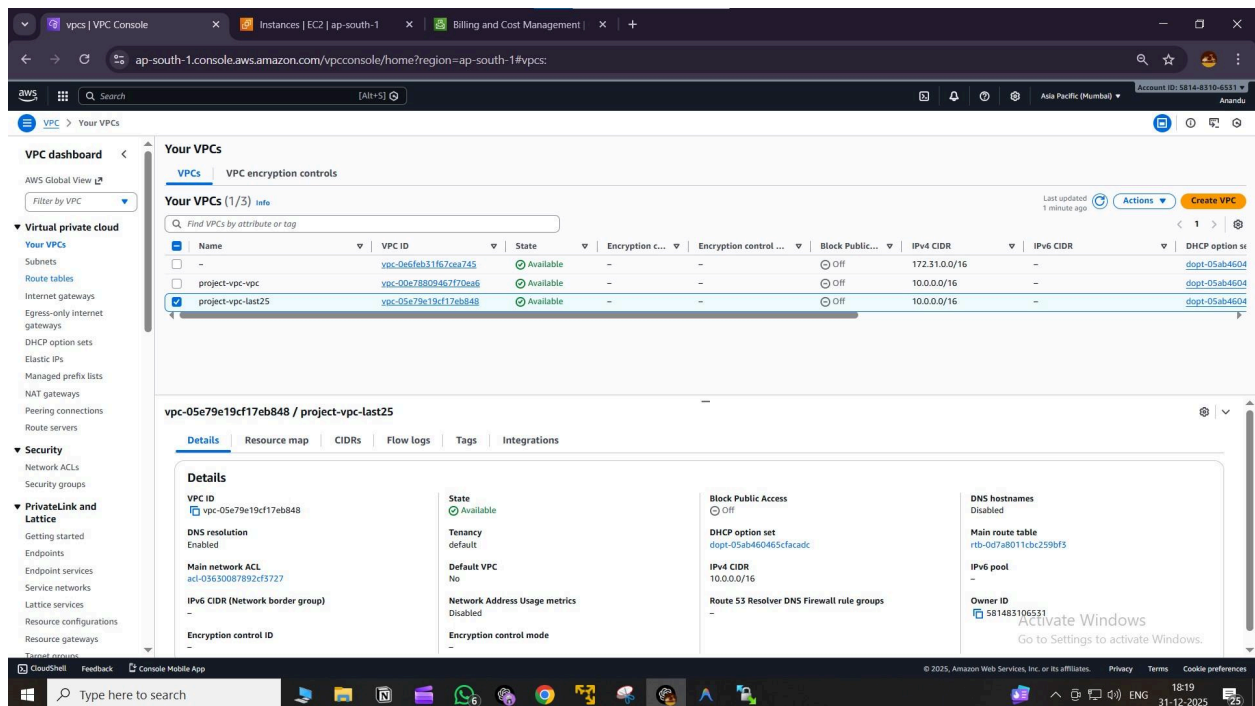
IPv4 CIDR reservations: -

Activate Windows. Go to Settings to activate Windows.

8.Public subnet



9. Internet Gateway



10. VPC

RouteTables | VPC Console | Security groups | EC2 | ap-south-1 | Billing and Cost Management | ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#SecurityGroups

EC2 > Security Groups

Security Groups (8) info

Find security groups by attribute or tag

<input type="checkbox"/>	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules
<input type="checkbox"/>	-	sg-0122efdd757e9a19e	launch-wizard-2	yqc-0e6feb31167cea745_1	launch-wizard-2 created 2025-12-19T0...	581483106531	3 Perr
<input type="checkbox"/>	-	sg-09c75657e26cb75d	wordpress	yqc-0e6feb31167cea745_1	wordpress created 2025-11-25T12:48:0...	581483106531	3 Perr
<input type="checkbox"/>	-	sg-092acae708e340e39	default	yqc-0e6feb31167cea745_1	default VPC security group	581483106531	1 Perr
<input type="checkbox"/>	-	sg-0ba8e498fba7fb558	db-sg	yqc-05e79e19cf17eb848_1	db-sg 2025-12-31T09:02:29.667Z	581483106531	2 Perr
<input type="checkbox"/>	-	sg-0a84e25b4fdaab4c4d	web-sg	yqc-05e79e19cf17eb848_1	Web Server (Public)31/12/25	581483106531	2 Perr
<input type="checkbox"/>	-	sg-0b93b16f52e19b325	launch-wizard-1	yqc-0e6feb31167cea745_1	launch-wizard-1 created 2025-12-19T0...	581483106531	3 Perr
<input type="checkbox"/>	-	sg-002208b95c8bb0d3	default	yqc-05e79e19cf17eb848_1	default VPC security group	581483106531	1 Perr
<input type="checkbox"/>	-	sg-0a0a5e52dd79aa636	default	yqc-00e7880946770eaf_1	default VPC security group	581483106531	1 Perr

Select a security group

Activate Windows
Go to Settings to activate Windows.

CloudShell Feedback Console Mobile App

Type here to search

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

18:21
31-12-2025

11.security Group

10

10

100

```
ec2-user@ip-10-0-1-211:~  
Enter current password for root (enter for none):  
OK, successfully used password, moving on...  
  
Setting the root password or using the unix_socket ensures that nobody  
can log into the MariaDB root user without the proper authorisation.  
  
You already have your root account protected, so you can safely answer 'n'.  
  
Switch to unix_socket authentication [Y/n] ^C  
Aborting!  
  
Cleaning up...  
[ec2-user@ip-10-0-1-211 ~]$ mysql -h 10.0.2.232 -u lokha_user -p  
Enter password:  
Welcome to the MariaDB monitor.  Commands end with ; or \g.  
Your MariaDB connection id is 19  
Server version: 10.5.29-MariaDB MariaDB Server  
  
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
MariaDB [(none)]> █
```

14.connectig to db server via server1

7. Cost Management & Cleanup

Charged Resources

- EC2 instances
- NAT Gateway
- Elastic IP

Cleanup Actions

- Terminated EC2 instances
- Deleted NAT Gateway
- Released Elastic IP

Free Resources (no cost):

- VPC
- Subnets
- Route Tables
- Security Groups

8. Final Outcome

This project successfully demonstrates:

- Secure AWS networking
- Real-world two-tier architecture
- Controlled database access
- Outbound-only internet from private subnet
- Practical troubleshooting skills

9. Interview-Ready Summary

“I deployed a two-tier AWS architecture with a public web server and a private database server. The database has no public IP and is accessible only from the web server using security group references. A NAT Gateway provides outbound internet access for patching while maintaining isolation.”

10. Conclusion

This project provides a strong foundation in AWS networking, security, and application deployment, closely matching real production environments and interview expectations.