

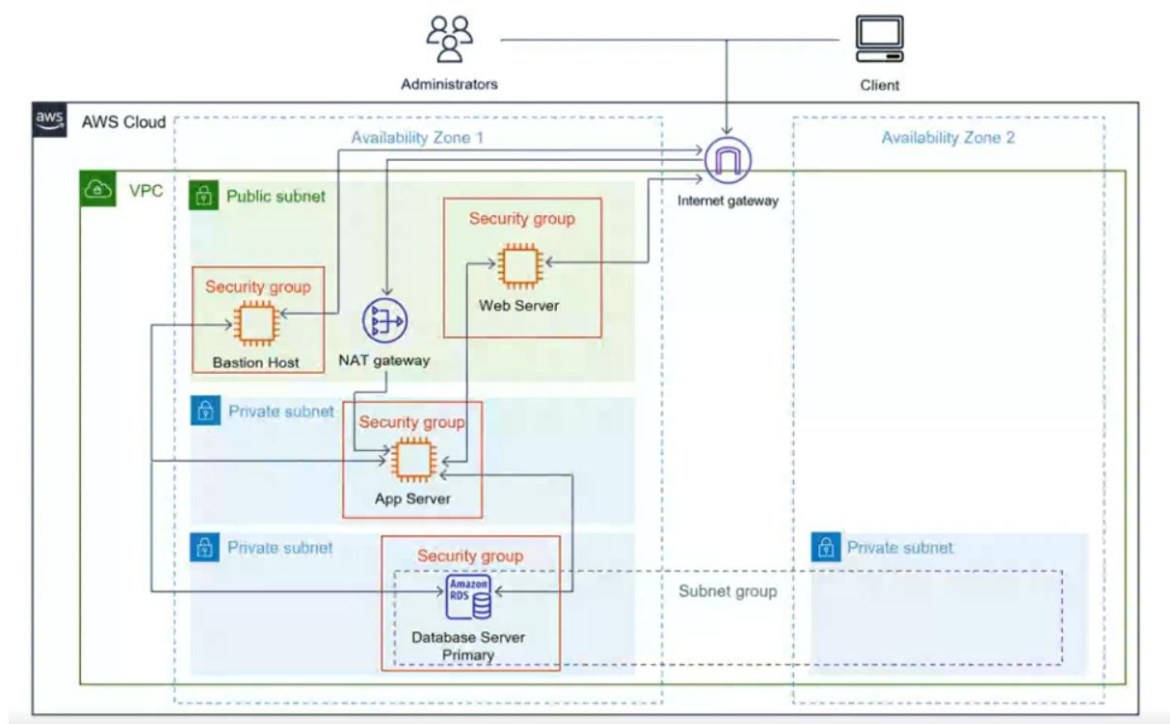
The following lab was created in a sandbox environment provided by AWS.

## Design and configure a high available 3-tier Architecture on AWS

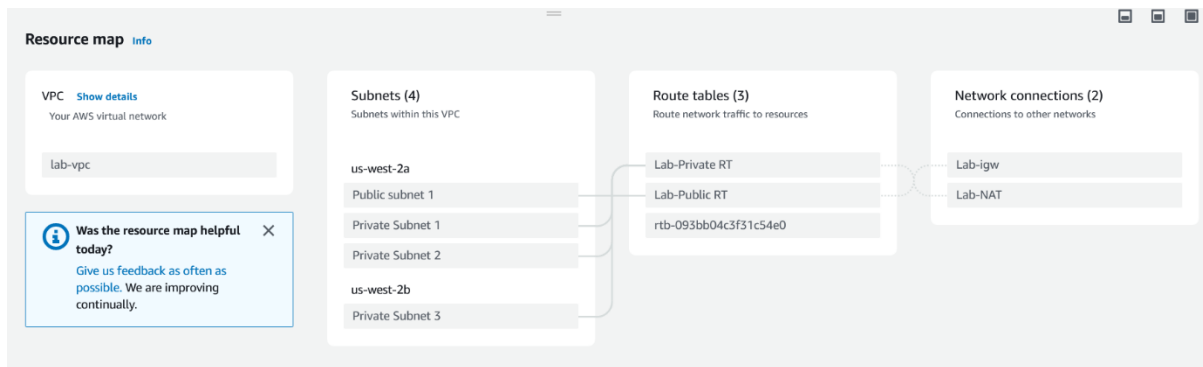
- Tier 1 - User/Presentation Tier
- Tier 2 - Application Tier
- Tier 3 - Data Tier

Name: Ofir Bar on

- Requested architecture in the lab:



- Created VPC, 1 Public subnet, 3 Private subnets, 2 Route tables, Internet Gateway and NAT. (Private Subnet 3 is on different availability zone)



- Associate Subnets with their respective route table.

<input checked="" type="checkbox"/>	Lab-Private RT	rtb-0129695c0c5dfab0d	3 subnets	-	No	vpc-09e7e306712b16d5f   lab-vpc	7541894...
<input type="checkbox"/>	Lab-Public RT	rtb-0dc61c5f4de45f116	subnet-0e9966a235cdcd4...	-	No	vpc-09e7e306712b16d5f   lab-vpc	7541894...

rtb-0129695c0c5dfab0d / Lab-Private RT							
Details Routes Subnet associations Edge associations Route propagation Tags							
Explicit subnet associations (3)							
Find subnet association							
Name	Subnet ID	IPV4 CIDR	IPV6 CIDR				
Private Subnet 1	subnet-022fd72d73cb7c761	192.168.2.0/24	-				
Private Subnet 2	subnet-0e81cf7321663a3b8	192.168.3.0/24	-				
Private Subnet 3	subnet-0de0f8bd44997b392	192.168.4.0/24	-				
Subnets without explicit associations (0)							

- Attach Internet Gateway to my VPC.

<input checked="" type="checkbox"/>	Lab-igw	igw-02112dae094cfb01b	Attached	vpc-09e7e306712b16d5f   lab-vpc	754189472461
<input type="checkbox"/>	-	igw-03a0775f3896e0a5b	Attached	vpc-0779453598ce7b48f	754189472461

igw-02112dae094cfb01b / Lab-igw			
Details Tags			
Details			
Internet gateway ID	State	VPC ID	Owner
igw-02112dae094cfb01b	Attached	vpc-09e7e306712b16d5f   lab-vpc	754189472461

- NAT with associated Elastic ip address.

Lab-NATnat-0379ba545611b2d3cPublic

Details

Secondary IPv4 addresses

Monitoring

Tags

Details

NAT gateway ID

nat-0379ba545611b2d3c

NAT gateway ARN

arn:aws:ec2:us-west-2:754189472461:natgateway/nat-0379ba545611b2d3c

VPC

vpc-09e7e306712b16d5f / lab-vpc

Connectivity type

Public

Primary public IPv4 address

44.240.162.102

Subnet

subnet-0c9966a235dcd4244 / Public subnet 1

- Create Security groups for each server.

<input type="checkbox"/>	Web Server	<a href="#">sg-09d3932e339f0d5ac</a>	Web Server	<a href="#">vpc-09e7e306712b16d5f</a>	Web Server
<input type="checkbox"/>	Database Server	<a href="#">sg-0e47fd6caa0c1d1a5</a>	Database Server	<a href="#">vpc-09e7e306712b16d5f</a>	Database Serv
<input type="checkbox"/>	Bastion host	<a href="#">sg-01a3c6c56dd37627b</a>	Bastion host	<a href="#">vpc-09e7e306712b16d5f</a>	Bastion host
<input checked="" type="checkbox"/>	App Server	<a href="#">sg-0c5f3f0172fd51bc2</a>	App Server	<a href="#">vpc-09e7e306712b16d5f</a>	App Server

- Assing to each SG the inbound rules they need.

Security group rule ID	Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>	
sgr-0c0459982b37cc2b6	HTTPS ▼	TCP	443	Custom ▼	<input type="text" value="Q"/> <input type="text" value="0.0.0.0/0"/> X	<input type="button" value="Delete"/>
sgr-0a0ad59bc76c7ef03	HTTP ▼	TCP	80	Custom ▼	<input type="text" value="Q"/> <input type="text" value="0.0.0.0/0"/> X	<input type="button" value="Delete"/>
sgr-059719af5ca452d14	MYSQL/Aurora ▼	TCP	3306	Custom ▼	<input type="text" value="Q"/> <input type="text" value="sg-0e47fd6caa0c1d1a5"/> X	<input type="button" value="Delete"/>
sgr-03047f5ff78f0ce3b	SSH ▼	TCP	22	Custom ▼	<input type="text" value="Q"/> <input type="text" value="sg-01a3c6c56dd37627b"/> X	<input type="button" value="Delete"/>
sgr-01e56c50acec2564c	All ICMP - IPv4 ▼	ICMP	All	Custom ▼	<input type="text" value="Q"/> <input type="text" value="sg-09d3932e339fd5ac"/> X	<input type="button" value="Delete"/>
<input type="button" value="Add rule"/>						

- Create 3 instances: Web Server and Bastion host in Public Subnet 1 and App Server in Private Subnet 1.

<input type="checkbox"/>	Web Server	<a href="#">i-0b621efa27a5dfa00</a>	<span>Running</span>	t2.micro	<span>2/2 checks passed</span> <a href="#">View alarms</a> +	us-west-2a
<input type="checkbox"/>	App Server	<a href="#">i-090f33523c21be0fd</a>	<span>Running</span>	t2.micro	<span>2/2 checks passed</span> <a href="#">View alarms</a> +	us-west-2a
<input checked="" type="checkbox"/>	Bastion Host	<a href="#">i-0b44b826e455ff716</a>	<span>Running</span>	t2.micro	<span>2/2 checks passed</span> <a href="#">View alarms</a> +	us-west-2a

#### Instance: [i-0b44b826e455ff716](#) (Bastion Host)

[Details](#) | 
 [Status and alarms](#) New | 
 [Monitoring](#) | 
 [Security](#) | 
 [Networking](#) | 
 [Storage](#) | 
 [Tags](#)

##### ▼ Instance summary [Info](#)

Instance ID <a href="#">i-0b44b826e455ff716</a> (Bastion Host)	Public IPv4 address 52.32.177.16 <a href="#">open address</a>	Private IPv4 addresses 192.168.1.23
IPv6 address -	Instance state <span>Running</span>	Public IPv4 DNS -
Hostname type IP name: ip-192-168-1-23.us-west-2.compute.internal	Private IP DNS name (IPv4 only) ip-192-168-1-23.us-west-2.compute.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t2.micro	

- Create a Subnet group which include Private Subnet 2 and Private Subnet 3.

private subnet group

Subnet group details

VPC ID

vpc-09e7e306712b16d5f

ARN

arn:aws:rds:us-west-2:754189472461:subgrp:private subnet group

Supported network types

IPv4

Description

Private Subnet Group 2,3

Subnets (2)

Availability zone	Subnet ID	CIDR block
us-west-2a	<a href="#">subnet-0e81cf7321663a3b8</a>	192.168.3.0/24
us-west-2b	<a href="#">subnet-0de0f8bd44997b392</a>	192.168.4.0/24

- Create DB in RDS (using “Database Server” SG which I created earlier, assign my VPC and Subnet group)

lab-db

Summary

DB identifier	Status	Role	Engine
lab-db	✔ Available	Instance	MariaDB
CPU	Class	Current activity	Region & AZ
<div>2.57%</div>	db.t3.micro	<div>0 Connections</div>	us-west-2a

Connectivity & securityMonitoringLogs & eventsConfigurationMaintenance & backupsTags

Connectivity & security

Endpoint & port	Networking	Security
Endpoint	Availability Zone	VPC security groups
lab-db.c3eo28su4dqt.us-west-2.rds.amazonaws.com	us-west-2a	<a href="#">Database Server (sg-0e47fd6caa0c1d1a5)</a>
Port	VPC	✔ Active
3306	<a href="#">lab-vpc (vpc-09e7e306712b16d5f)</a>	Publicly accessible
	Subnet group	No

- Upload .pem key to Bastion Host

```
PS C:\Users\kingo> Pscp -scp -P 22 -i '.\Downloads\labsuser.ppk' -l user ec2-user '.\Downloads\labsuser.pem' ec2-user@52.32.177.16:/home/ec2-user
The host key is not cached for this server:
 52.32.177.16 (port 22)
You have no guarantee that the server is the computer you
think it is.
The server's ssh-ed25519 key fingerprint is:
 ssh-ed25519 255 SHA256:N7p1UmXnw0ULoJXoTQa25LB70QI3w9pmy4gnth5uMVg
If you trust this host, enter "y" to add the key to PSCP's
cache and carry on connecting.
If you want to carry on connecting just once, without adding
the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n, Return cancels connection, i for more info) y
pscp: ec2-user: No such file or directory

labsuser.pem          | 1 kB |   1.6 kB/s | ETA: 00:00:00 | 100%
PS C:\Users\kingo> |
```

- SSH to Bastion Host, Check that the upload was successful and SSH to App Server.

```
ec2-user@ip-192-168-2-243:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"

#_
~\  #####      Amazon Linux 2
~~ \  #####\
~~  \###|      AL2 End of Life is 2025-06-30.
~~   \#/
~~    V~' '->
~~~
~~~ /
~~~ /
~~~ /
~~~ /m/ '-

A newer version of Amazon Linux is available!

Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-192-168-1-23 ~]$ ls
labsuser.pem
[ec2-user@ip-192-168-1-23 ~]$ chmod 400 labsuser.pem
[ec2-user@ip-192-168-1-23 ~]$ ssh -i labsuser.pem ec2-user@192.168.2.243
The authenticity of host '192.168.2.243 (192.168.2.243)' can't be established.
ECDSA key fingerprint is SHA256:sAp3Uyt1RMPQ1c5qsxjo7N6UFeA4jpiaHhCF7AVgANK.
ECDSA key fingerprint is MD5:63:1f:71:92:34:8f:31:bf:f6:e2:d2:51:bf:38:c1:b2.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.2.243' (ECDSA) to the list of known hosts.
```

- Ping Web Server to check connection.

```

ec2-user@ip-192-168-2-243:~
Warning: Permanently added '192.168.2.243' (ECDSA) to the list of known hosts.
#_
~\#### Amazon Linux 2
~~\#####
~~\#####\
~~\###| AL2 End of Life is 2025-06-30.
~~\#/
~~V~'-'>
~~~
~~~. /
~~~ /
~~~ /m/'
A newer version of Amazon Linux is available!
Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-192-168-2-243 ~]$ ls
[ec2-user@ip-192-168-2-243 ~]$ ping 192.168.1.5
PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data.
64 bytes from 192.168.1.5: icmp_seq=1 ttl=255 time=0.998 ms
64 bytes from 192.168.1.5: icmp_seq=2 ttl=255 time=0.455 ms
64 bytes from 192.168.1.5: icmp_seq=3 ttl=255 time=0.452 ms
64 bytes from 192.168.1.5: icmp_seq=4 ttl=255 time=0.451 ms
^C
--- 192.168.1.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3031ms
rtt min/avg/max/mdev = 0.451/0.589/0.998/0.236 ms
[ec2-user@ip-192-168-2-243 ~]$

```

- Connect to Database and show databases.

```

[ec2-user@ip-192-168-2-243 ~]$ mysql --user=root -p --host=lab-db.c3eo28su4dqt.us-west-2.rds.amazonaws.com
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 53
Server version: 10.6.14-MariaDB managed by https://aws.amazon.com/rds/

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)]> show databases;
+-----+
| Database |
+-----+
| LabDB |
| information_schema |
| innodb |
| mysql |
| performance_schema |
| sys |
+-----+
6 rows in set (0.00 sec)

```