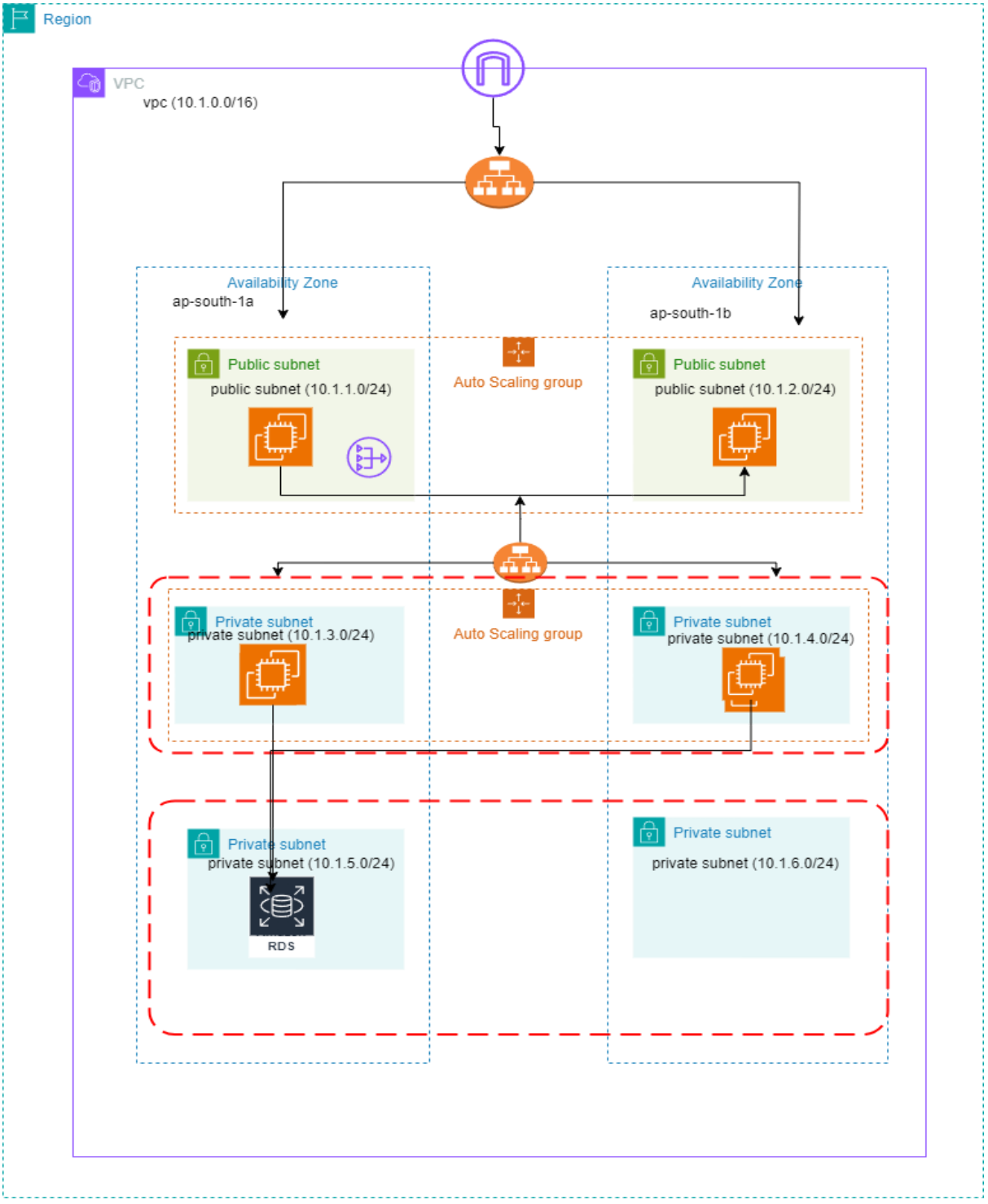
Fault-Tolerant Web Application: Building a Highly Available 3-Tier Architecture



Web Tier (Presentation Layer)

1. 2 **public** subnets
2. Minimum of 2 EC2 instances in an Auto Scaling Group.
3. EC2 Web Server Security Group allows inbound permission from the internet.
4. Bootstrap a static web page that already includes the static web page.
5. Create a public route table and associate the 2 **public** subnets.

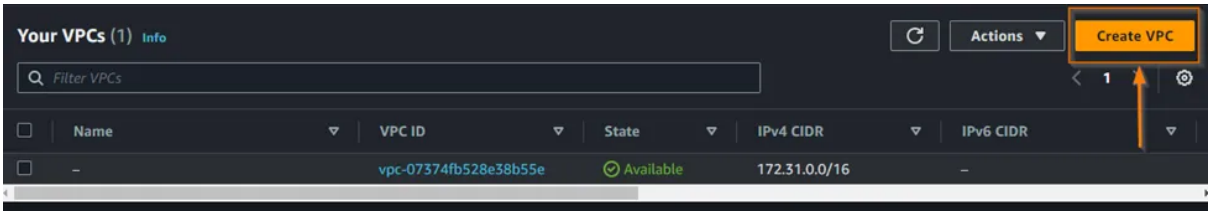
Application Tier

1. 2 **private** subnets
2. Minimum of 2 EC2 instances in an Auto Scaling Group.
3. EC2 Application Server Security Group allows inbound permission from the Web Server Security Group.
4. Associate with a private route table

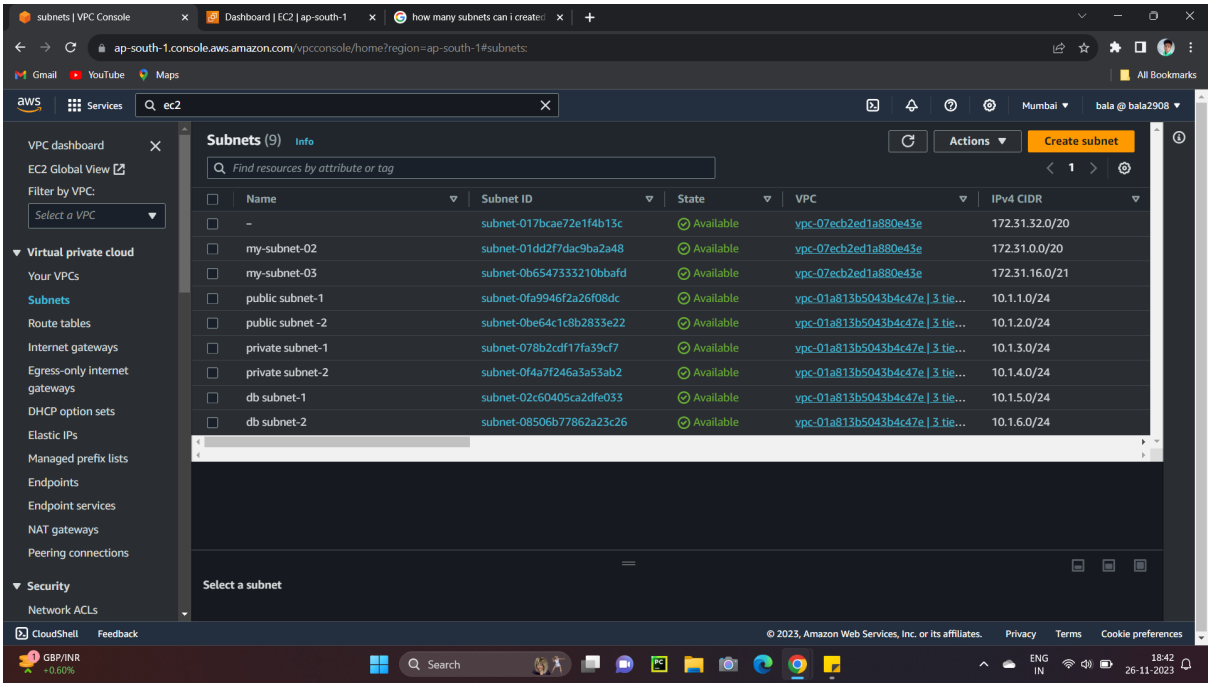
Database Tier

1. Use a free Tier **MySql** RDS Database.
2. The Database Security Group should allow inbound traffic for MySQL from the Application Server Security Group.
3. 2 private subnets.
4. Associate with a private route table.

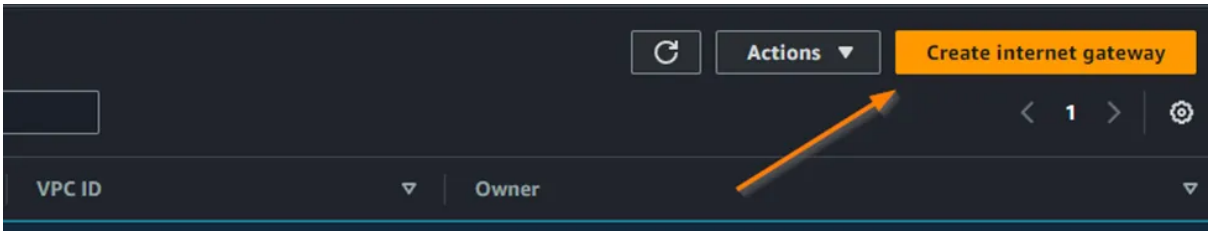
Step 1:

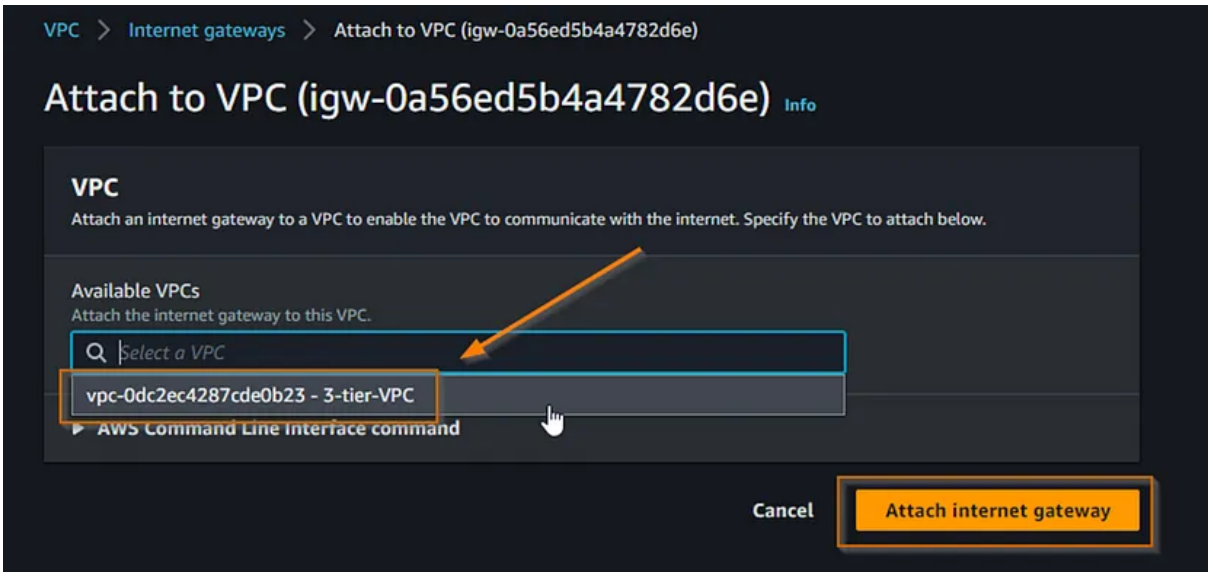


Create a vpc with subnets having two public subnets for web tier and two private subnets for each application tier and database tier.



Step2:

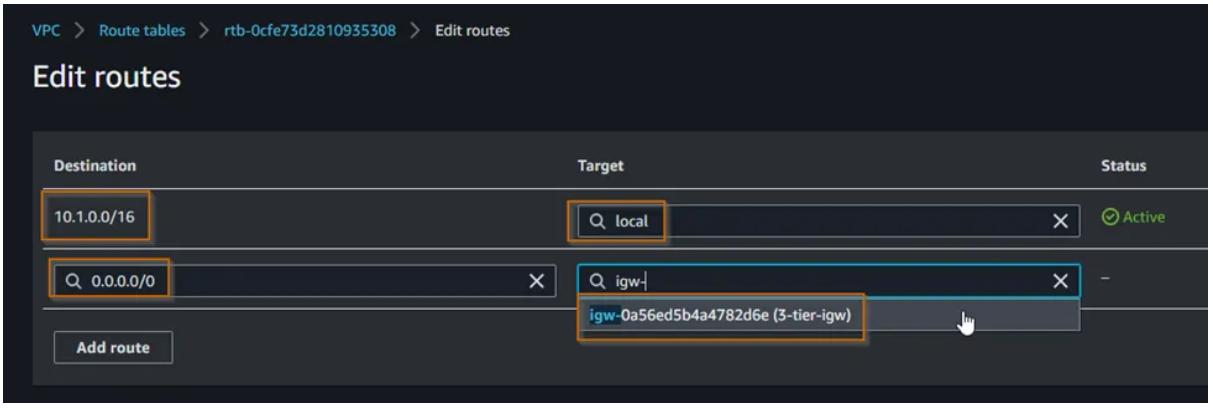




Create the internet gateway and attached to the created vpc.

Step 3:

Now we will create our Route Tables. We can find route tables in the VPC dashboard. We are adding 0.0.0.0/0 to the destination and selecting our IGW as the target.

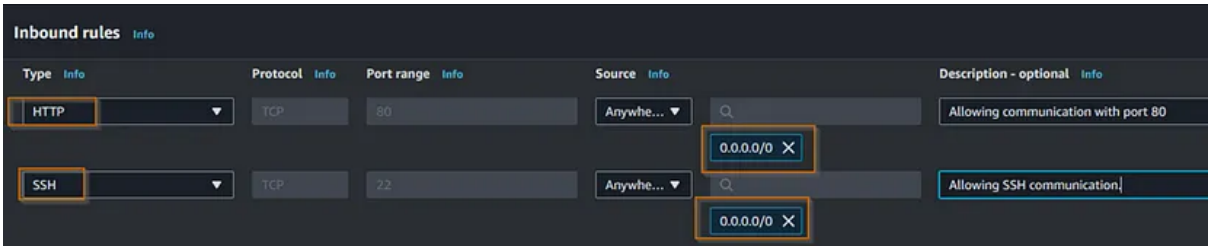


By associating your subnets with the custom route table, you can control the internet traffic routing behavior for the subnets.

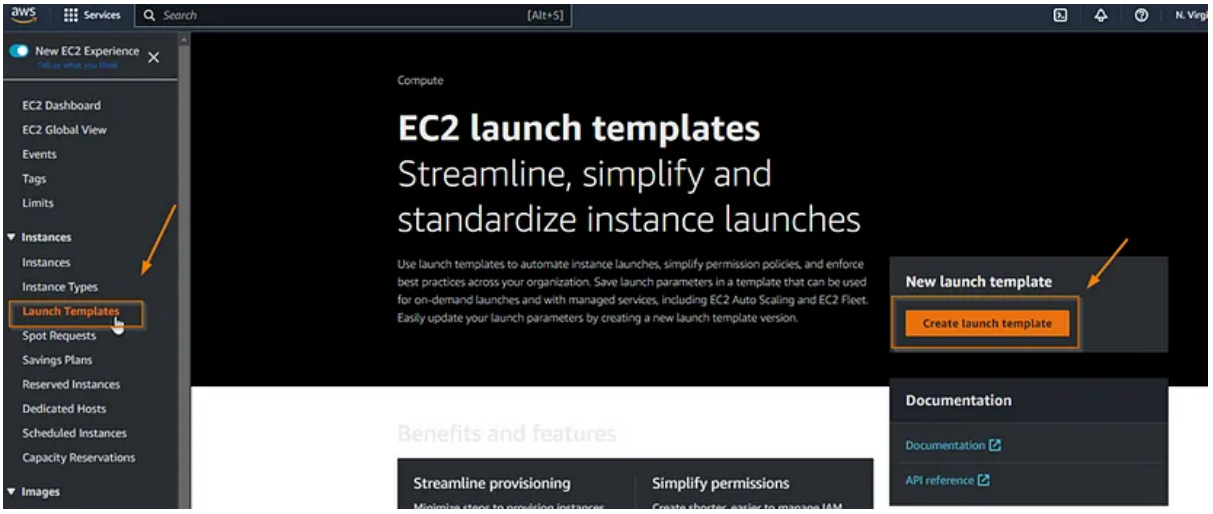
And create the route tables for the application and database tier and make sure not connect to the internet gateway to make private subnet.

Step 4:

Before creating instances ,create a security group for web tier which has to allow port 80(http) and ssh(22) from the source(0.0.0.0/0)anywhere.

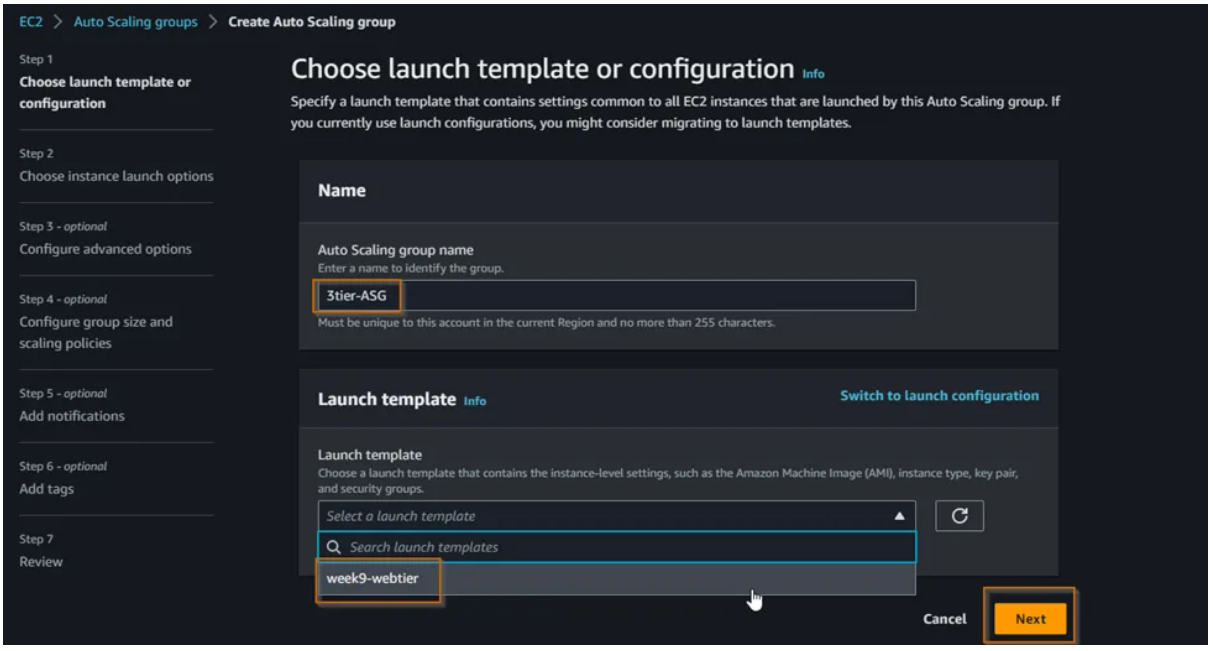


Step 5:

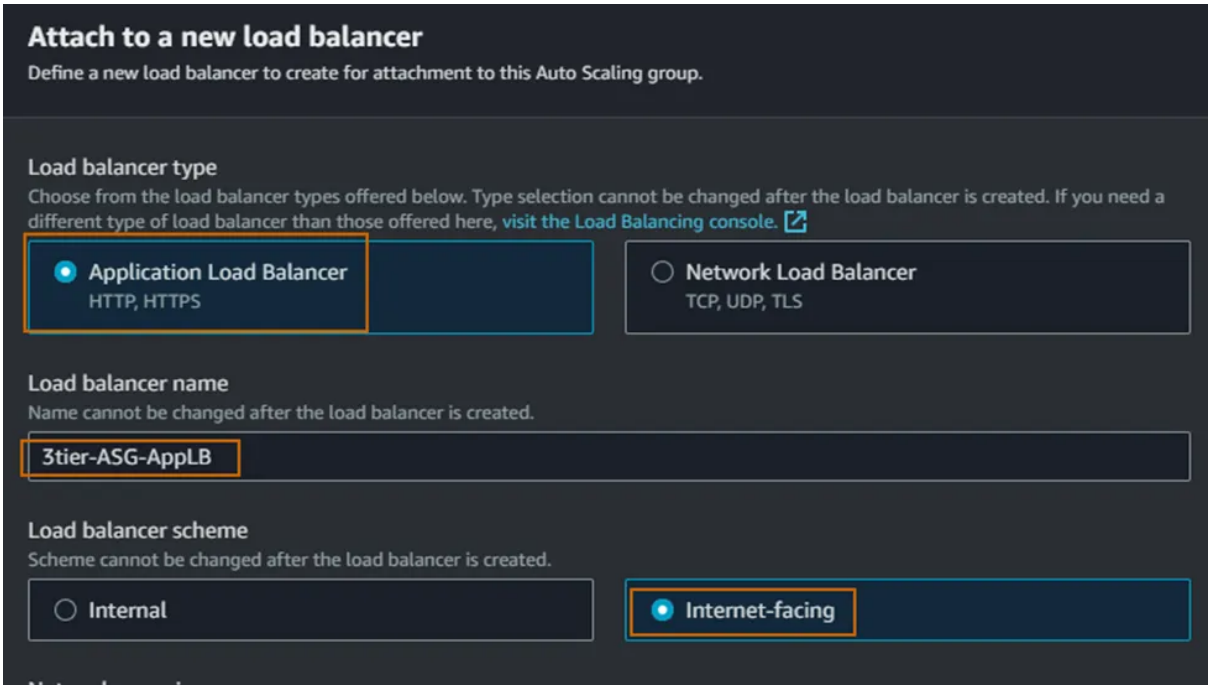


And create a launch templates for auto scaling group as per our free tier.(make sure you add the key pair ,security group and bootstrap script to enable web server for our instance).

Step 6 :

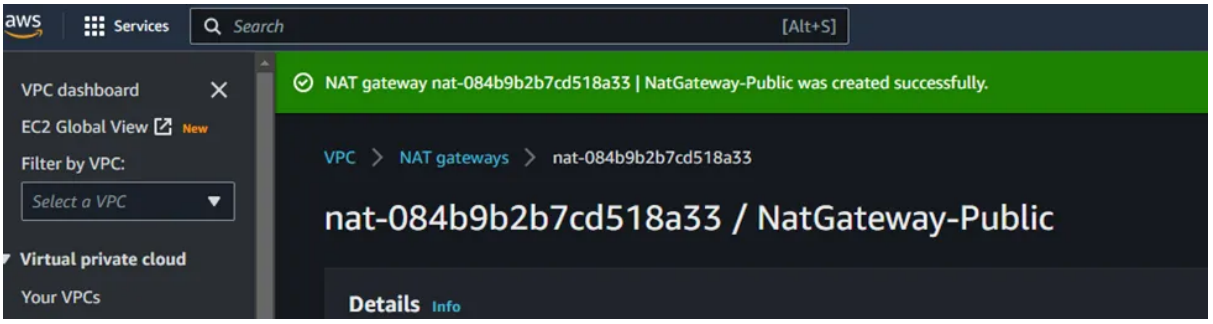


Create a auto scaling group with two availability zones for high availability .

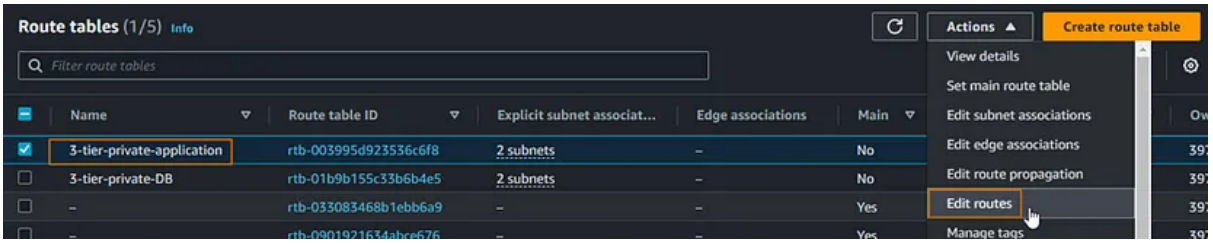


and attach a new application load balancer(for distributing incoming application across multiple targets such as ec2 instances in multiples availability zones for high availability for application)

Step 7:



Create a nat gateway (choose the public subnet and allocate the static ip) ,we will need to attach it to our private route table.



And connect a nat gateway to the private subnet route table for internet connectivity.

VPC - *required* Info

vpc-0dc2ec4287cde0b23 (3-tier-VPC)
10.1.0.0/16

Inbound security groups rules

Security group rule 1 (ICMP, All, sg-05de260cffa4c95dd) Remove

Type Info	Protocol Info	Port range Info
All ICMP - IPv4	ICMP	All

Source type Info	Source Info	Description - *optional* Info
Custom	Add CIDR, prefix list or security sg-05de260cffa4c95dd	e.g. SSH for admin desktop

Security group rule 2 (TCP, 80, sg-05de260cffa4c95dd) Remove

Type Info	Protocol Info	Port range Info
HTTP	TCP	80

Source type Info	Source Info	Description - *optional* Info
Custom	Add CIDR, prefix list or security sg-05de260cffa4c95dd	e.g. SSH for admin desktop

Security group rule 3 (TCP, 22, sg-05de260cffa4c95dd) Remove

Type Info	Protocol Info	Port range Info
ssh	TCP	22

Source type Info	Source Info	Description - *optional* Info
Custom	Add CIDR, prefix list or security sg-05de260cffa4c95dd	e.g. SSH for admin desktop

To ensure that the two private subnets can be accessed through the Web server security group, it is necessary to create a new security group. The Web server security group should be set as the source for

each protocol in the new security group. Note: ICMP is what is going to allow us to ping our internal instances.

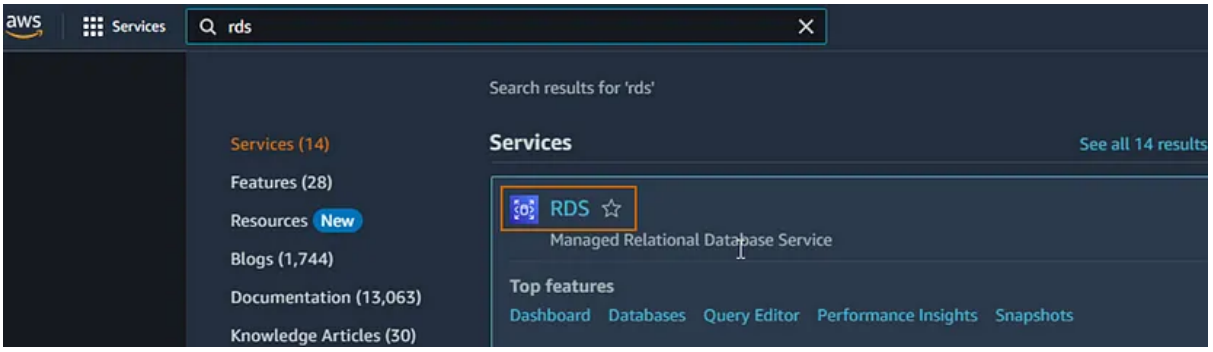
Step 8:

I decided to bootstrap a tomcat server since it is a popular applications server, however, this is not an actual application tier as we don’t have any provided code to run on the EC2 instances.

Step 9:

Now back to the auto-scaling group, as we did previously, we will repeat the same steps for the application tier.while creating a launch template for application tier and add the private subnets as we created for the application tier.

Step 10:



And now create the rds and add the two private subnets as we created for the rds tier to the subnets groups in rds.(and make sure no to the public access)

Public access Info

- Yes
  RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.
- No
  RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

VPC security group (firewall) Info

Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

- Choose existing
  Choose existing VPC security groups
- Create new
  Create new VPC security group

Existing VPC security groups

Choose one or more options

application-tier-SG ×

Auto Scaling groups | EC2 | ap-s | Databases | RDS | ap-south-1 | Designing a Fault-Tolerant Web | Google Lens

ap-south-1.console.aws.amazon.com/rds/home?region=ap-south-1#databases:

Gmail YouTube Maps All Bookmarks

aws Services Search [Alt+S] Mumbai bala @ bala2908

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
- Events
- Event subscriptions

Creating database database-1
Your database might take a few minutes to launch.
You can use settings from database-1 to simplify configuration of suggested database add-ons while we finish creating your DB for you.

View credential details

RDS > Databases

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 (1)

Group resources | Modify | Actions | Restore from S3 | Create database

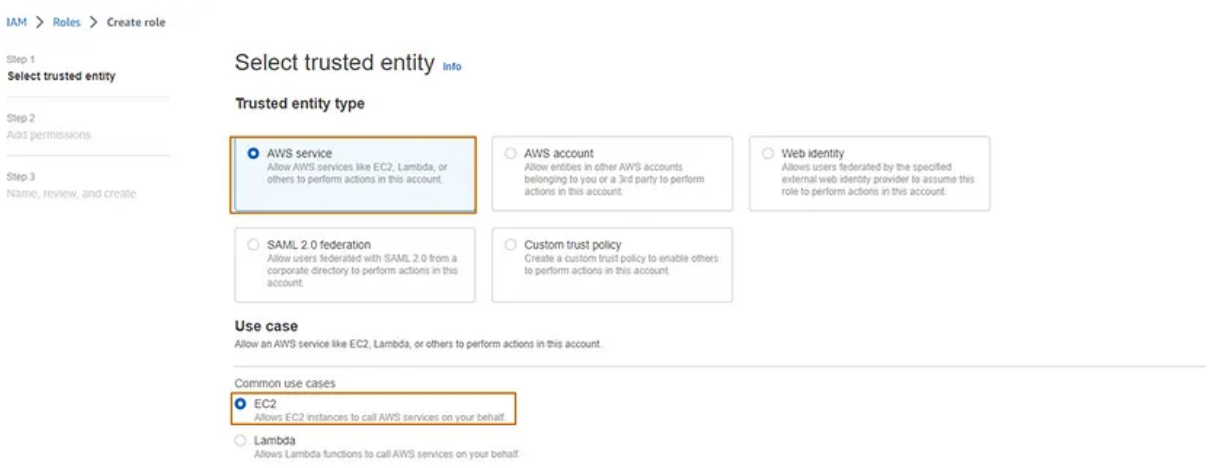
Filter by databases

DB identifier	Status	Role	Engine	Region & AZ	Size	Actions	CPU	Current activity
database-1	Creating	Instance	MySQL Community	ap-south-1b	db.t2.micro	-	-	

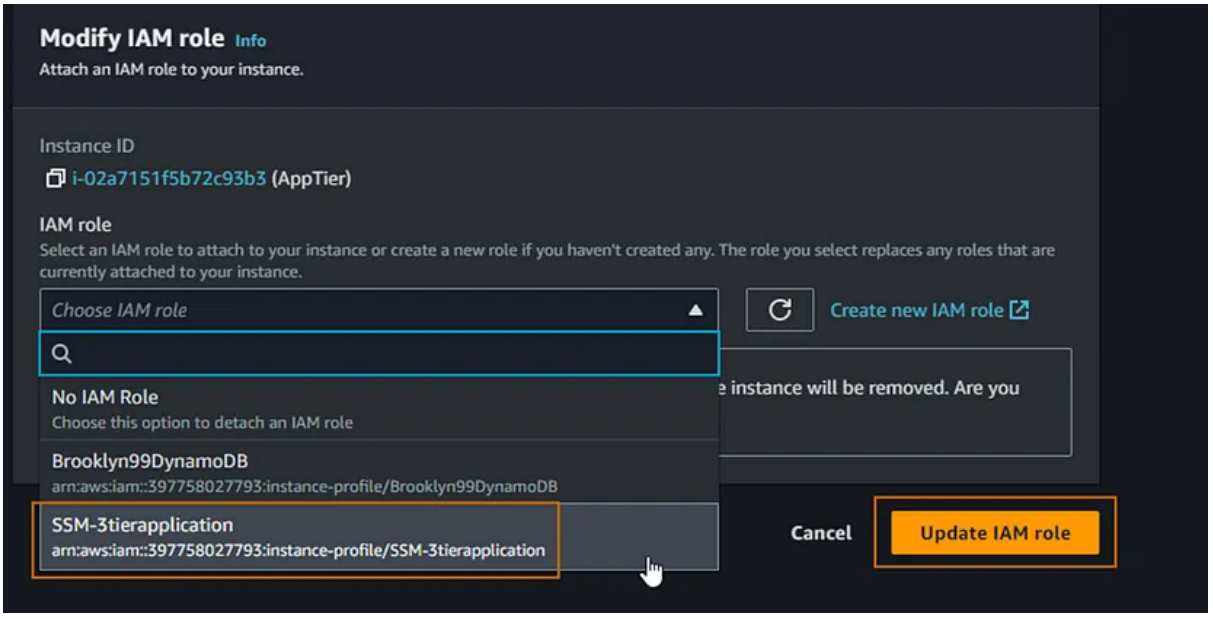
CloudShell Feedback

27°C Cloudy Search ENG IN 09:31 27-11-2023

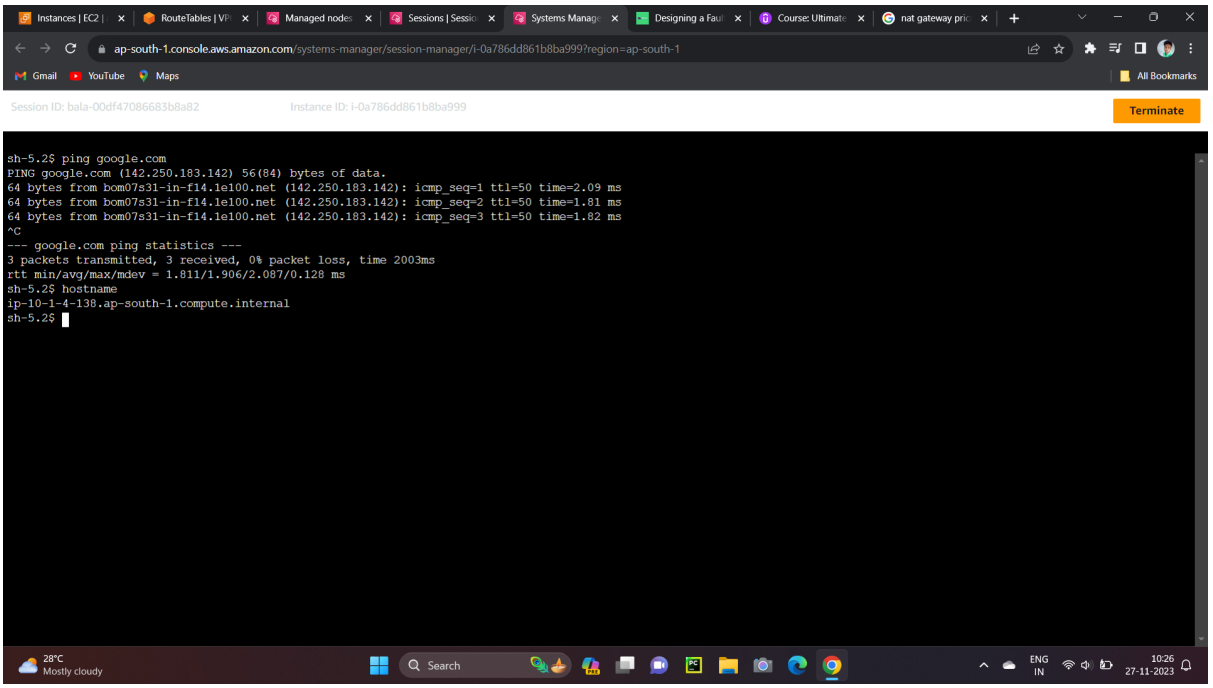
Step 11:



For secure connection you can use aws system manager to connect our instance in a secure way (for that create iam role to access instance and in the fleet manager you can see the instance .)



Step 12:



We should now be able to communicate with our instances in our private network through our session manager.