AWS Training Hands-on

Day 5 6th July 2023

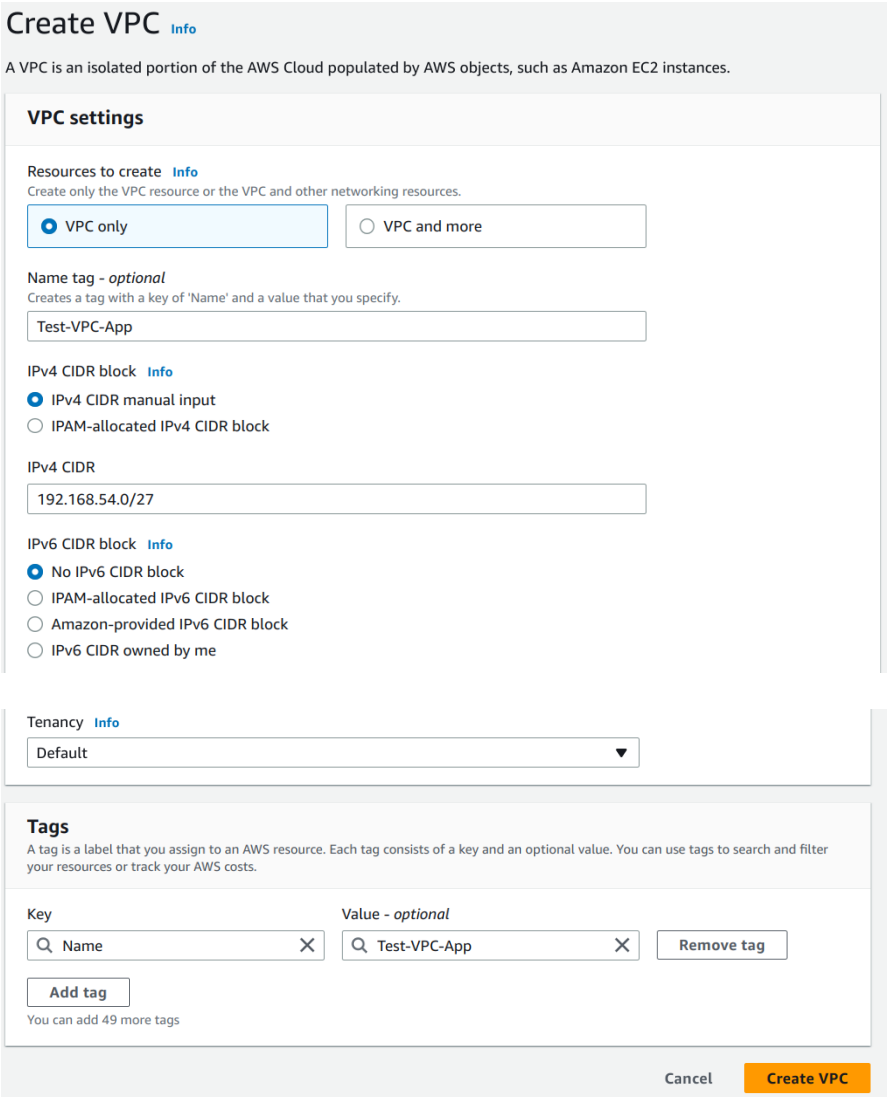
Task 1 - Create VPC peering connection and connect an EC2 instance with a RDS instance.

Step 1 - Login to the AWS management console and browse to the VPC console.

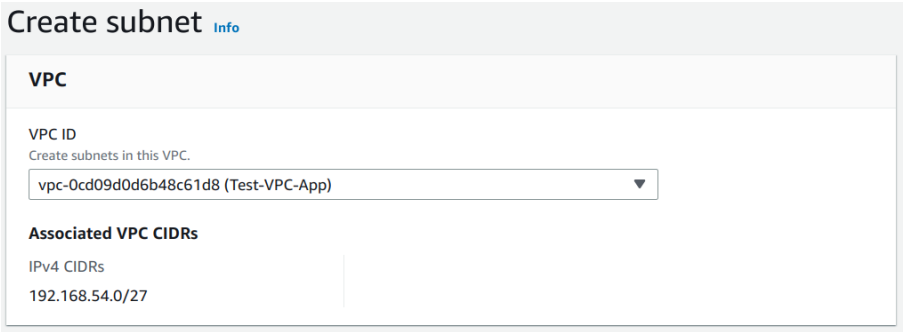
Create a VPC for the application environment with the following configurations -

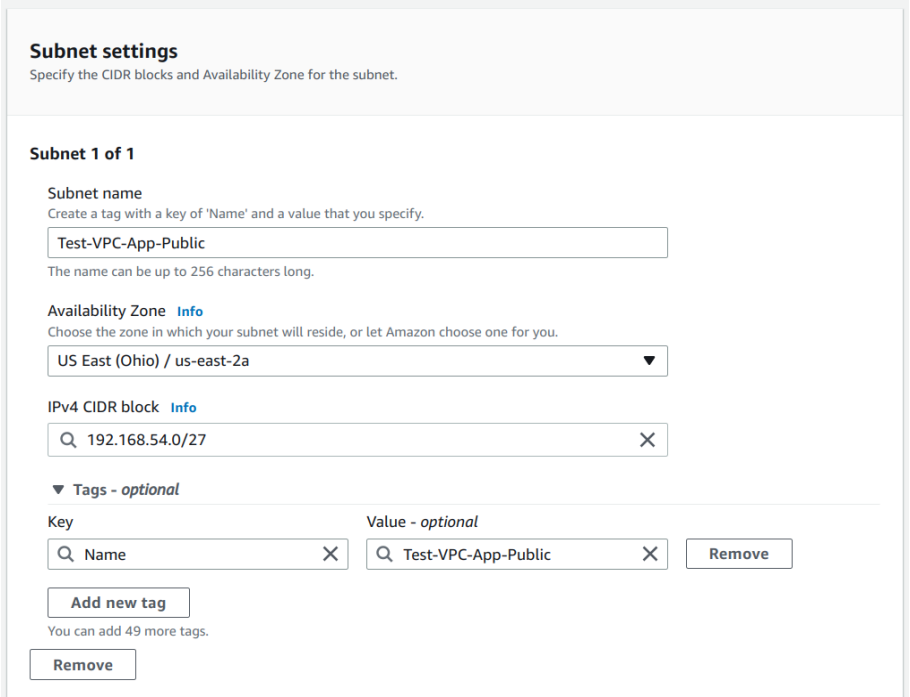
- **Name:** Test-VPC-App
- **IPv4 CIDR block:** Select "IPv4 CIDR manual input"
- **IPv4 CIDR:** 192.168.54.0/27
- **Tenancy:** Default

Click on "Click VPC"

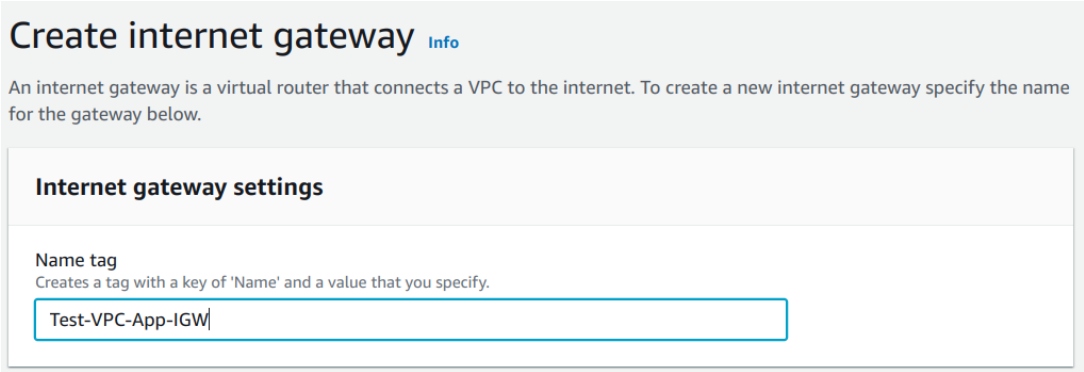


Step 2 - Create a public subnet inside the above VPC.

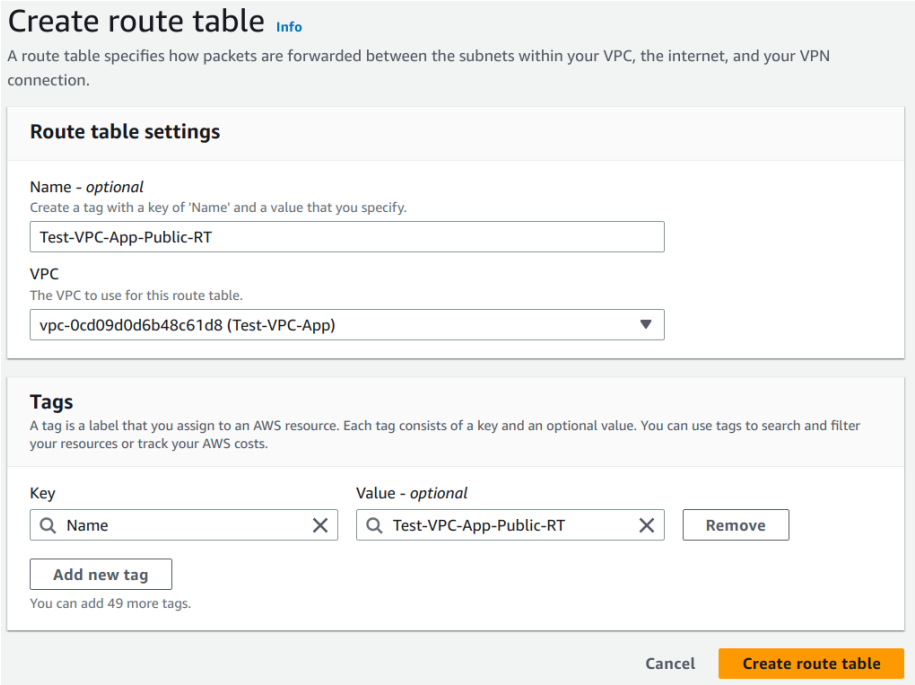


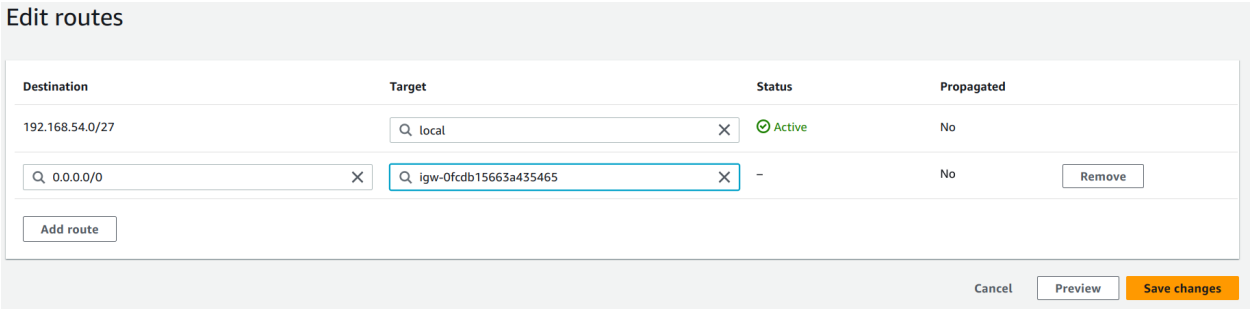


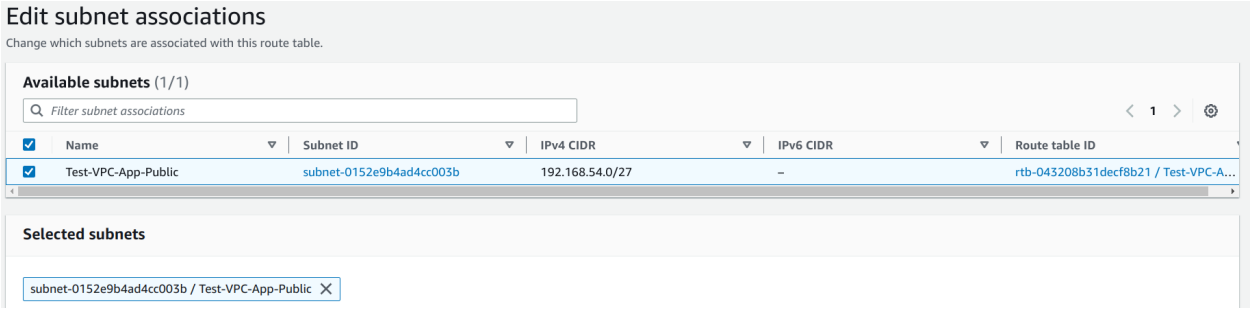
Step 3 - Create an Internet gateway and attach it to the VPC.



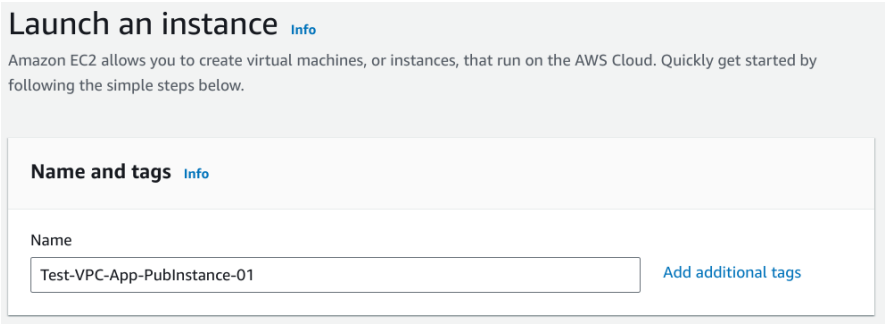
Step 4 - Create a route table for the public subnet and edit its subnet association and routes to route the internet facing traffic to the internet gateway.

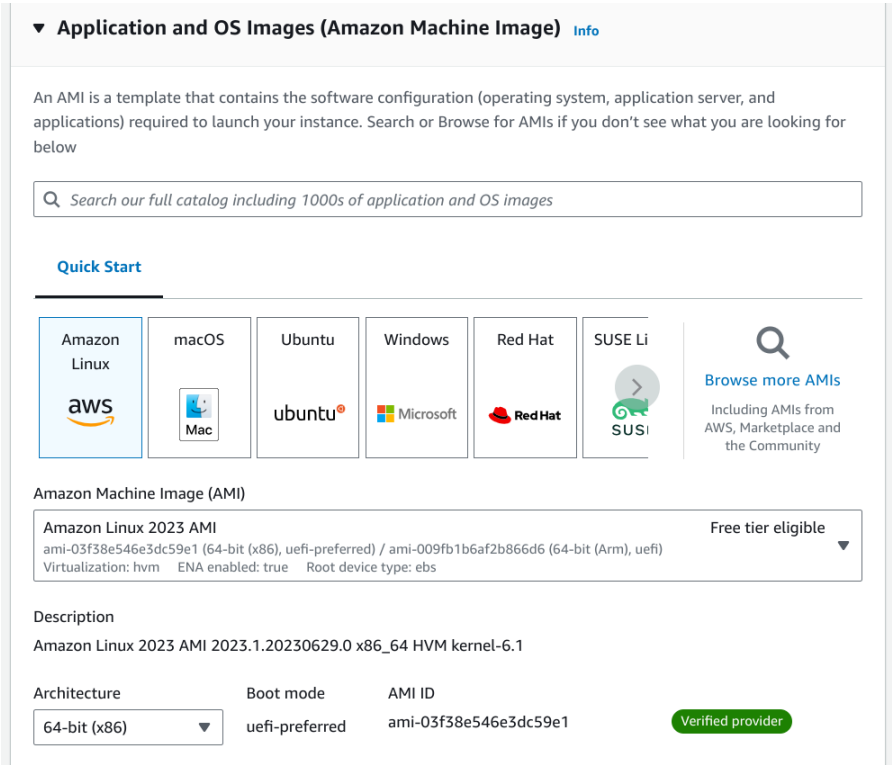


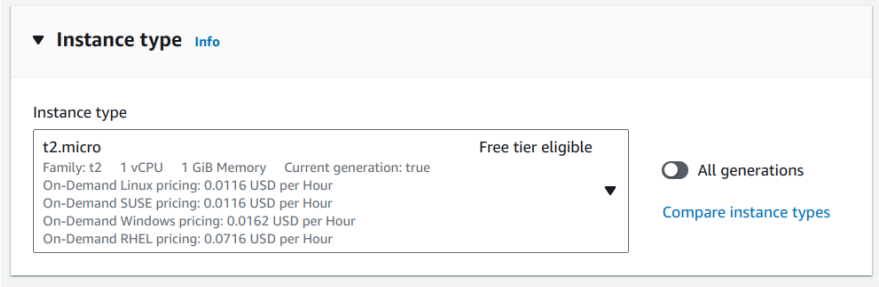




Step 5 - Launch an EC2 instance in the public subnet.







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 - *required*

PubInstancePem

Create new key pair

Network settings Info

VPC - *required* Info

vpc-0cd09d0d6b48c61d8 (Test-VPC-App)
192.168.54.0/27

Subnet Info

subnet-0152e9b4ad4cc003b Test-VPC-App-Public
VPC: vpc-0cd09d0d6b48c61d8 Owner: 237042273450
Availability Zone: us-east-2a IP addresses available: 27 CIDR: 192.168.54.0/27)

Create new subnet

Auto-assign public IP Info

Enable

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*

Public-SG

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

Allows traffic from internet

Inbound Security Group Rules

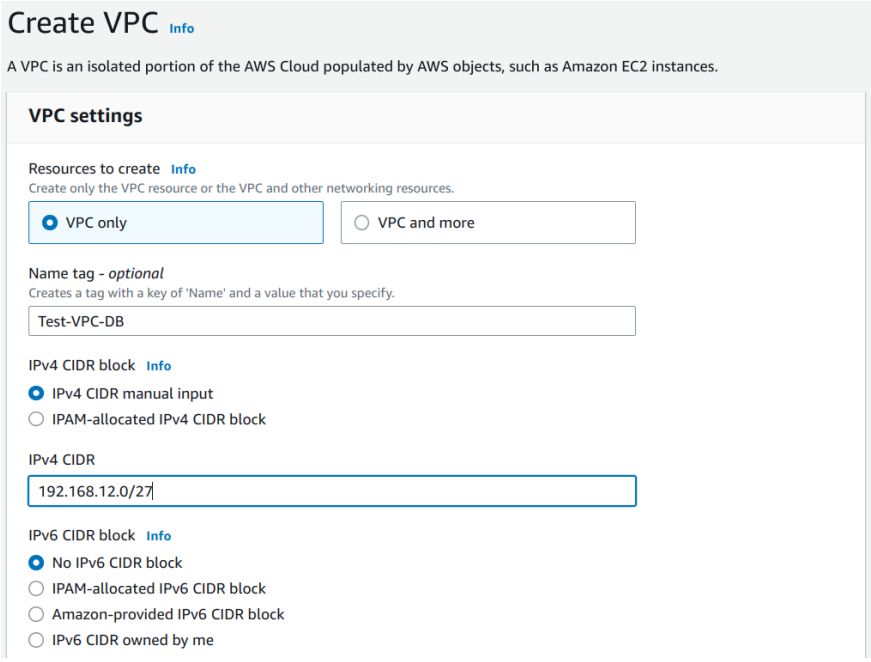
Security group rule 1 (TCP, 22, 0.0.0.0/0) Remove

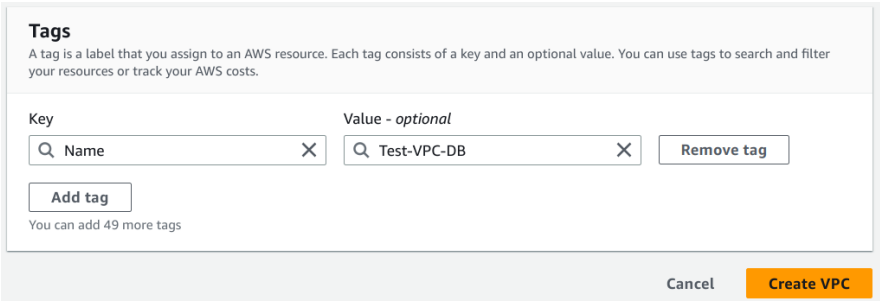
Type Info	Protocol Info	Port range Info
ssh	TCP	22

Source type Info	Source Info	Description - *optional* Info
Anywhere	*Add CIDR, prefix list or security* 0.0.0.0/0 ::/0	*e.g. SSH for admin desktop*

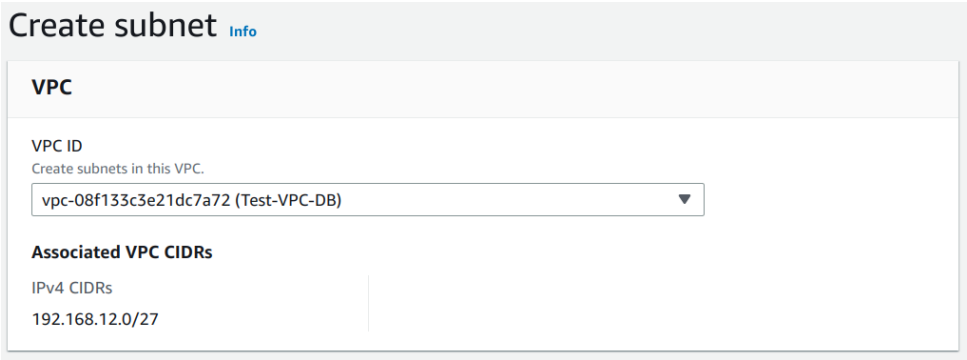
Step 6 - Create a Second VPC for a private database.

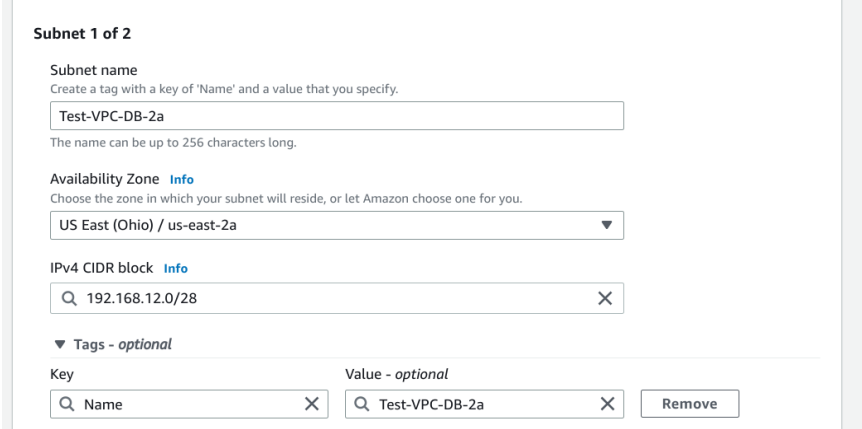
- **Name:** Test-VPC-DB
- **IPv4 CIDR block:** Select “IPv4 CIDR manual input”
- **IPv4 CIDR:** 192.168.12.0/27
- **Tenancy:** Default

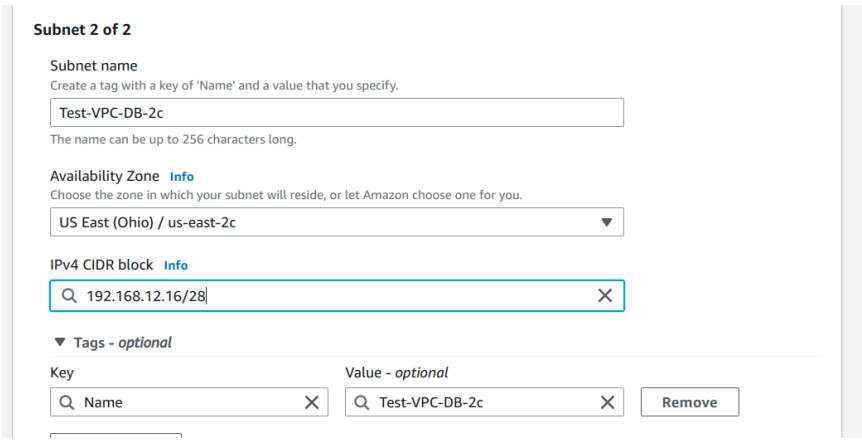




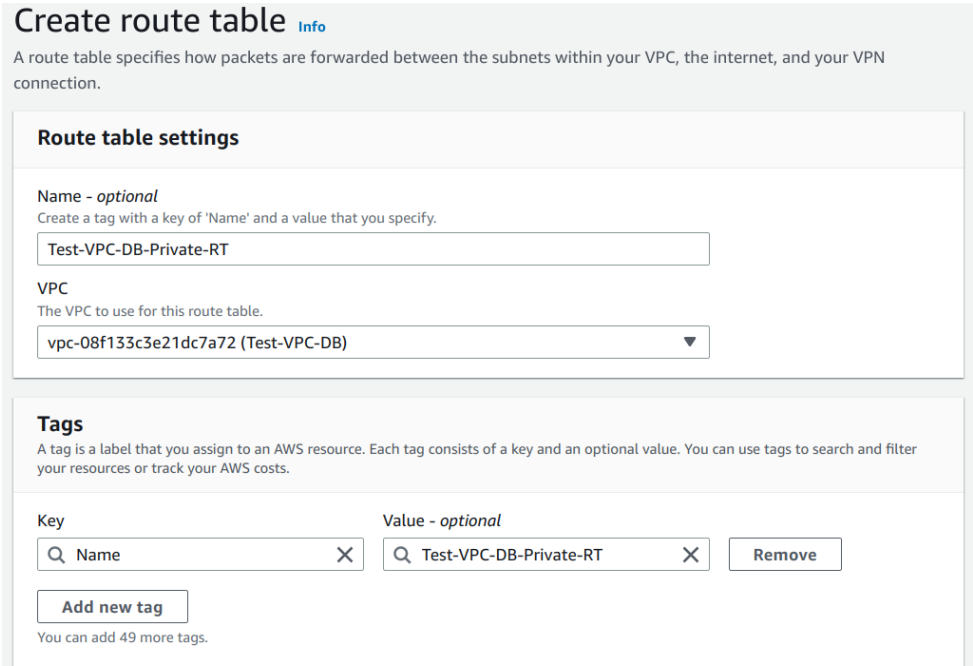
Step 7 - Create two private subnets in the above VPC.

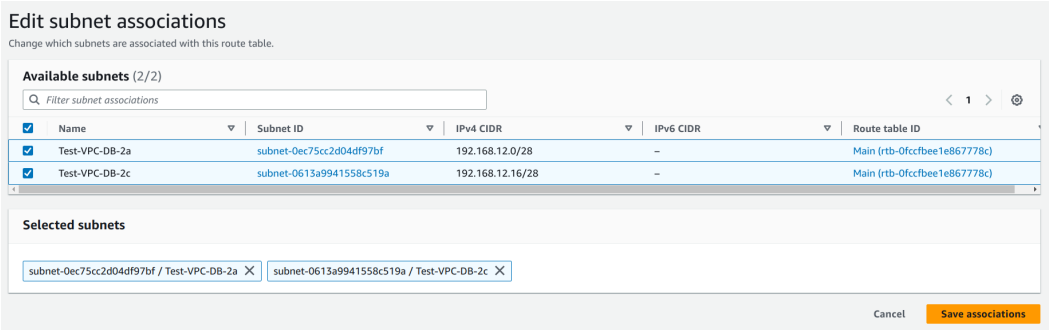






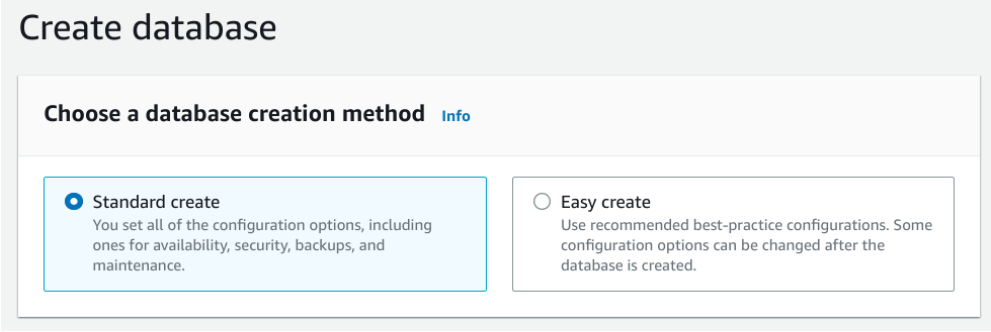
Step 8 - Create a route table for the above subnet.

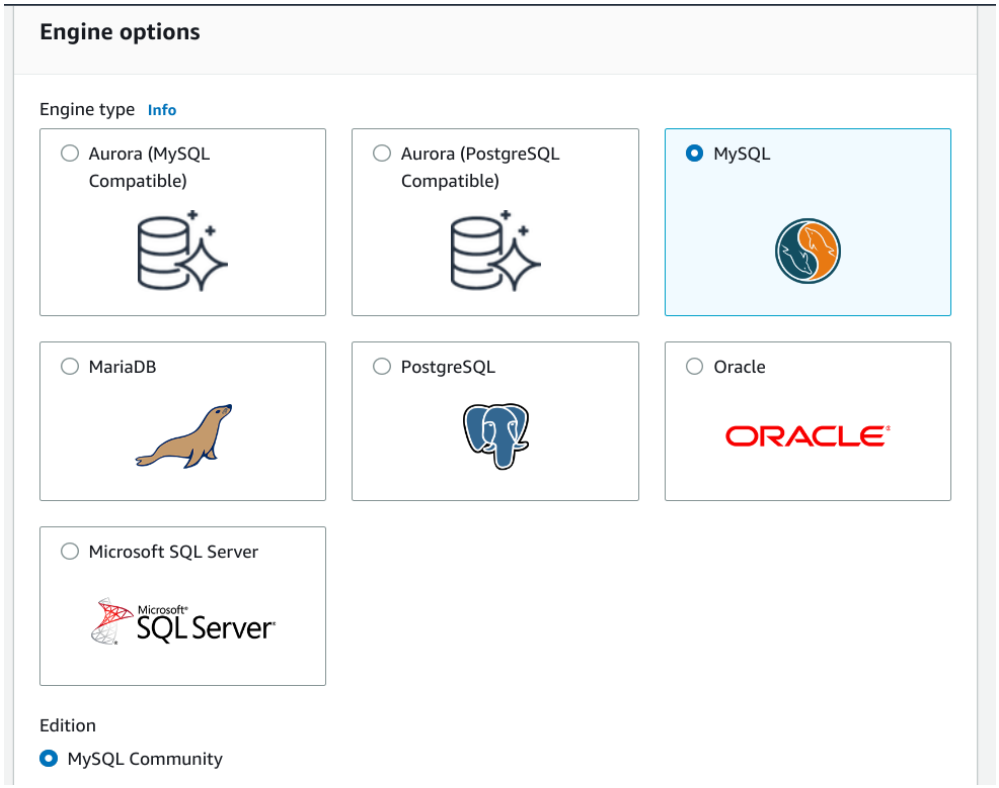




Step 9 - Create a RDS instance in the above VPC.

The RDS instance stores the backup data and logs for redundancy in other availability zones. And the data of the RDS instance is also stored in the other availability zone. Therefore the specified VPC requires at least two subnets each in different AZs.





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**

Settings

DB instance identifier **Info**

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

Test-VPC-UserDB

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ **Credentials Settings**

Master username **Info**

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

admin

1 to 16 alphanumeric characters. First character must be a letter.

☐ Manage master credentials in AWS Secrets Manager

Manage master user credentials in Secrets Manager. RDS can generate a password for you and manage it throughout its lifecycle.

If you manage the master user credentials in Secrets Manager, some RDS features aren't supported.
Learn more

☐ Auto generate a password

Amazon RDS can generate a password for you, or you can specify your own password.

Master password **Info**

••••••••

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote), "(double quote) and @ (at sign).

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.

Network type Info

To use dual-stack mode, make sure that you associate an IPv6 CIDR block with a subnet in the VPC you specify.

- (●) **IPv4**
  Your resources can communicate only over the IPv4 addressing protocol.
- ( ) **Dual-stack mode**
  Your resources can communicate over IPv4, IPv6, or both.

Virtual private cloud (VPC) Info

Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

Test-VPC-DB (vpc-08f133c3e21dc7a72)
2 Subnets, 2 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

DB subnet group Info

Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

default-vpc-08f133c3e21dc7a72
2 Subnets, 2 Availability Zones

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

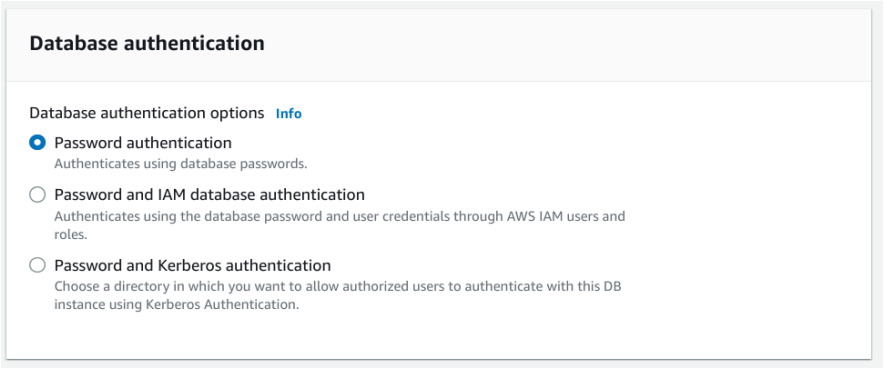
New VPC security group name

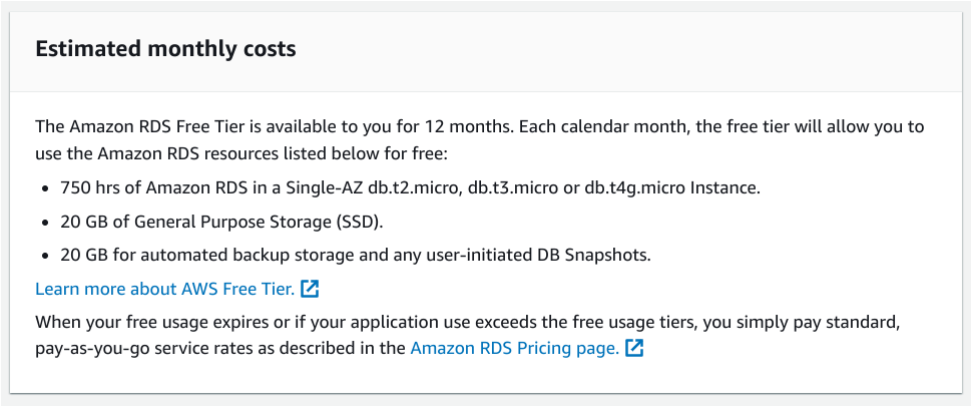
Test-VPC-DB-SG

Availability Zone Info

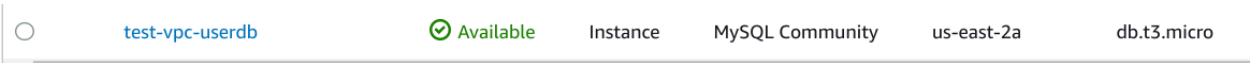
us-east-2a

Manage your database user credentials through your DB engine's native password authentication features.





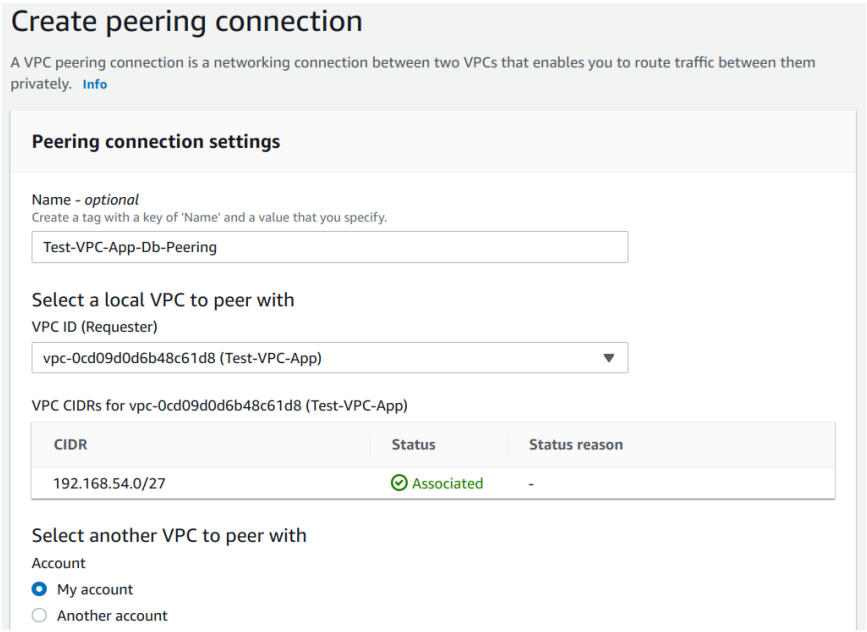
The RDS instance is created successfully.

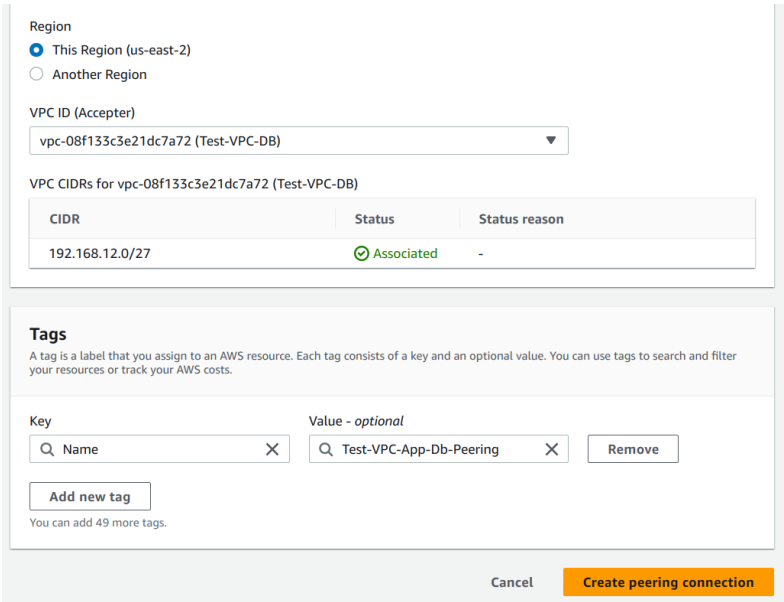


Step 10 - Connect the RDS instance to the EC2 instance created in another VPC by making a Peering connection between the two VPCs.

A VPC peering connection is made by assigning a requester VPC and an acceptor VPC. The requester VPC requests the other VPC to establish a peering connection by accepting the request for the same.

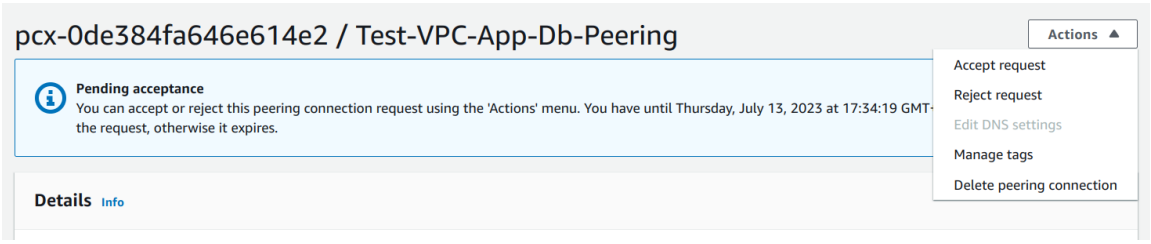
Here the requester VPC is - “Test-VPC-App”, and acceptor VPC is - “Test-VPC-DB”



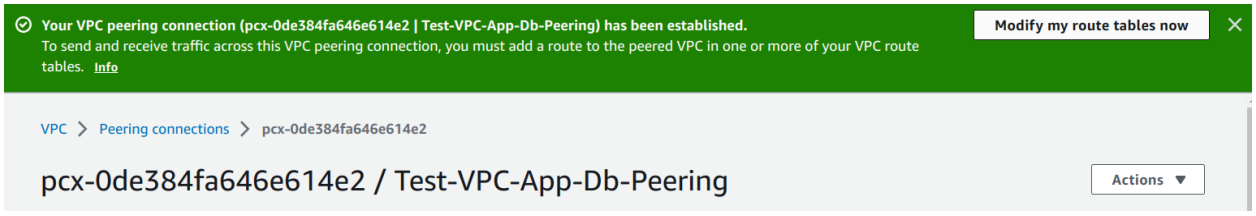


Step 11 - Accept the peering connection request.

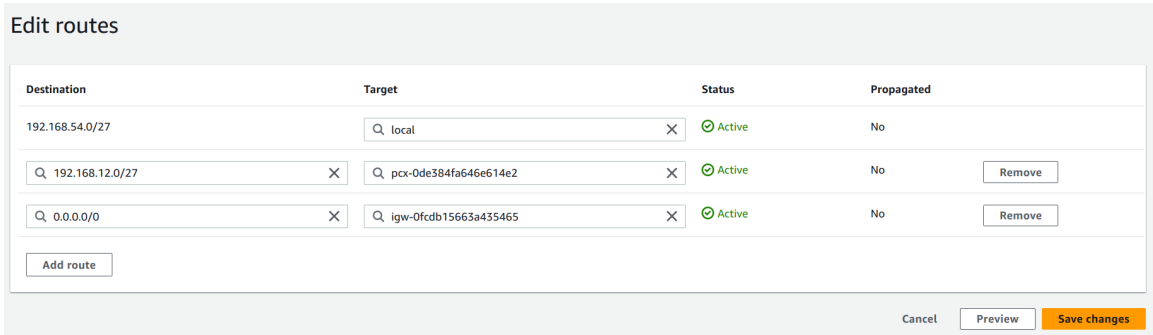
As both the VPCs are in the same account therefore we can see the pending request dialog.



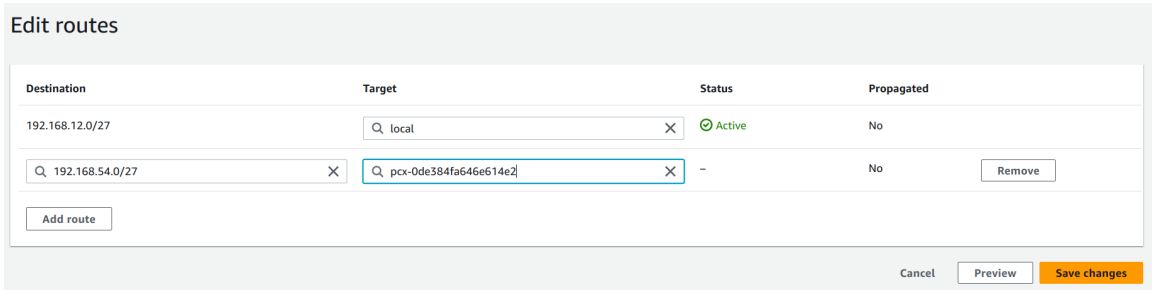
Step 12 - Modify the route tables of both the VPCs.



1. Route table of the **"Test-VPC-App"** VPC should contain a route to forward the traffic for the **"Test-VPC-DB"** VPC i.e., for the CIDR block of **"192.168.12.0/27"** to the peering connection as a target.



2. Route table of the **"Test-VPC-DB"** VPC should contain a route to forward the traffic for the **"Test-VPC-App"** VPC i.e., for the CIDR block of **"192.168.54.0/27"** to the peering connection as a target.



Step 13 - Checking if the RDS instance is accessible from the EC2 instance in the "Test-VPC-App" VPC.

Using **"nc"** command to listen to the port of the RDS instance and verify that the EC2 instance can connect to the RDS instance.

```
[ec2-user@ip-192-168-54-8 ~]$ nc -zv test-vpc-userdb.cso7be6o9p5s.us-east-2.rds.amazonaws.com 3306
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Connected to 192.168.12.9:3306.
Ncat: 0 bytes sent, 0 bytes received in 0.04 seconds.
```

Step 14 - Connect to the RDS instance.

Use the **"mysql"** command to connect to the instance, enter the endpoint, port and username of the database.

Enter the password for the user.

```
[ec2-user@ip-192-168-54-8 ~]$ mysql --version
mysql  Ver 15.1 Distrib 10.5.18-MariaDB, for Linux (x86_64) using  EditLine wrapper
[ec2-user@ip-192-168-54-8 ~]$ mysql -h test-vpc-userdb.cso7be6o9p5s.us-east-2.rds.amazonaws.com -P 3306 -u admin -p
Enter password:
```

Step 15 - Display databases, create a new database.

```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
4 rows in set (0.001 sec)

MySQL [(none)]> create database users;
Query OK, 1 row affected (0.006 sec)

MySQL [(none)]> use users;
Database changed
MySQL [users]> show tables;
Empty set (0.002 sec)
```

Step 16 - Create table "userDetails" with fields - "UserId, userName, and UserAddress"

Use the **"CREATE TABLE"** command to create a new table.

```
MySQL [users]> CREATE TABLE userDetails (UserId int, UserName varchar(255), UserAddress varchar(255));
Query OK, 0 rows affected (0.023 sec)

MySQL [users]> show tables;
+-----------------+
| Tables_in_users |
+-----------------+
| userDetails     |
+-----------------+
1 row in set (0.001 sec)
```

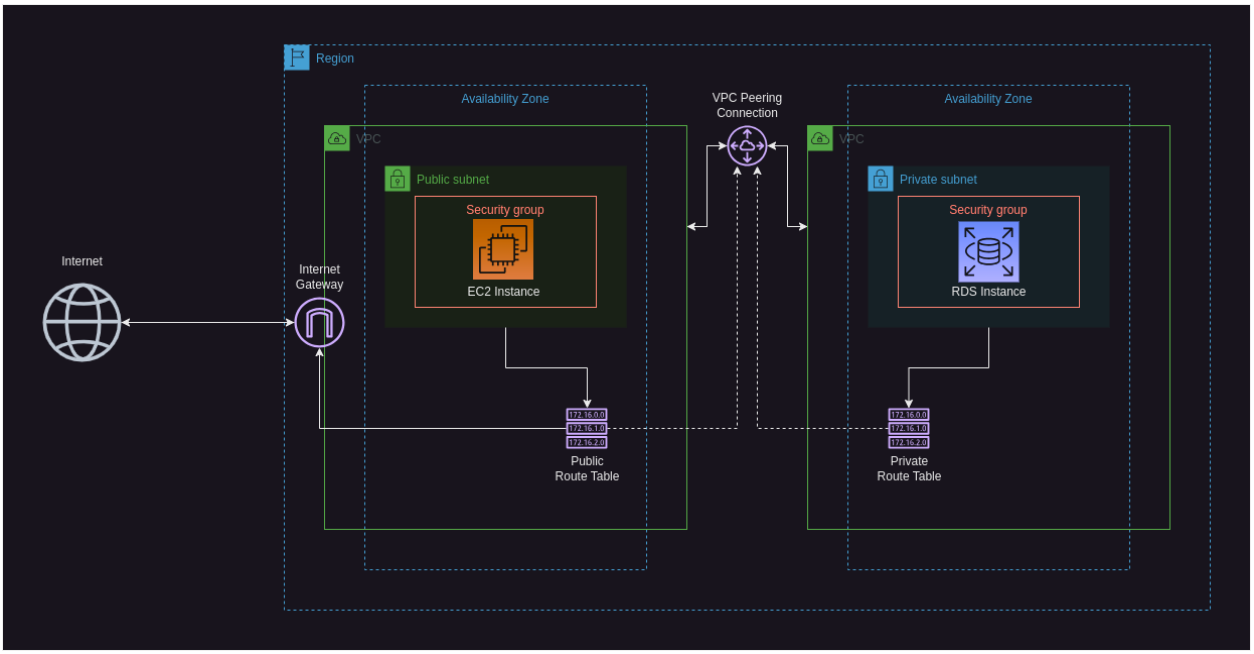
Step 17 - Insert data into the table.

Use the **"INSERT INTO <tablename> VALUES"** command.

Use the **"SELECT"** command to display the content of the table.

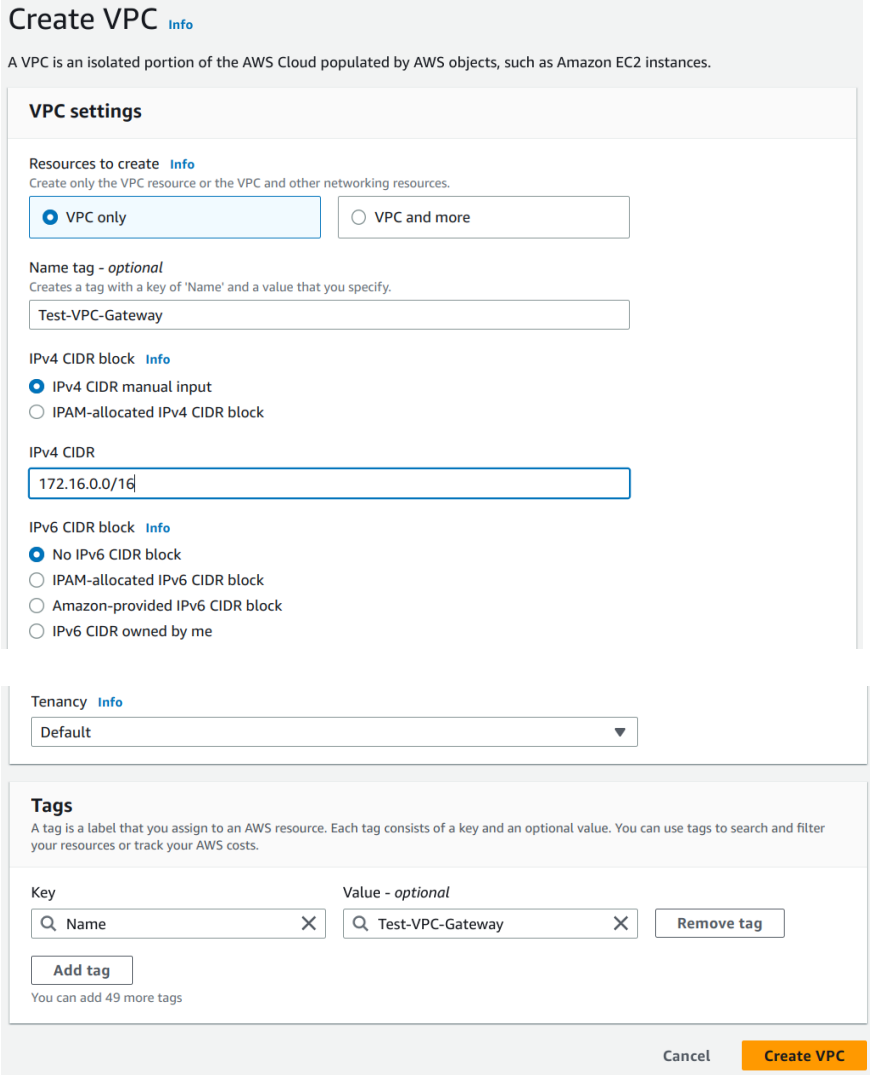
```
MySQL [users]> INSERT INTO userDetails (UserId, UserName, UserAddress) VALUES (01, "User1SK", "Indore");
Query OK, 1 row affected (0.005 sec)

MySQL [users]> SELECT * FROM userDetails;
+--------+----------+-------------+
| UserId | UserName | UserAddress |
+--------+----------+-------------+
|      1 | User1SK  | Indore      |
+--------+----------+-------------+
1 row in set (0.001 sec)
```

Architecture Diagram for the above solution

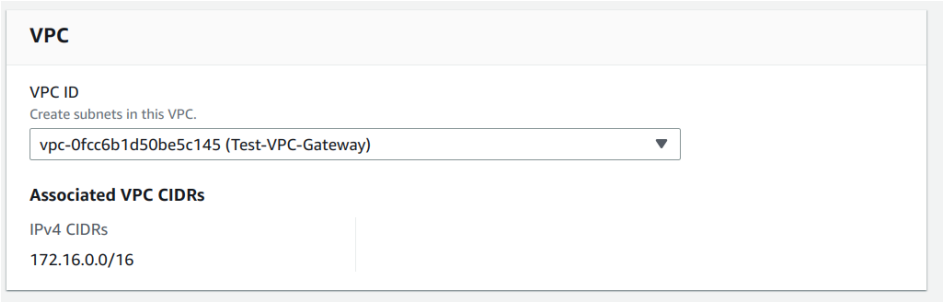


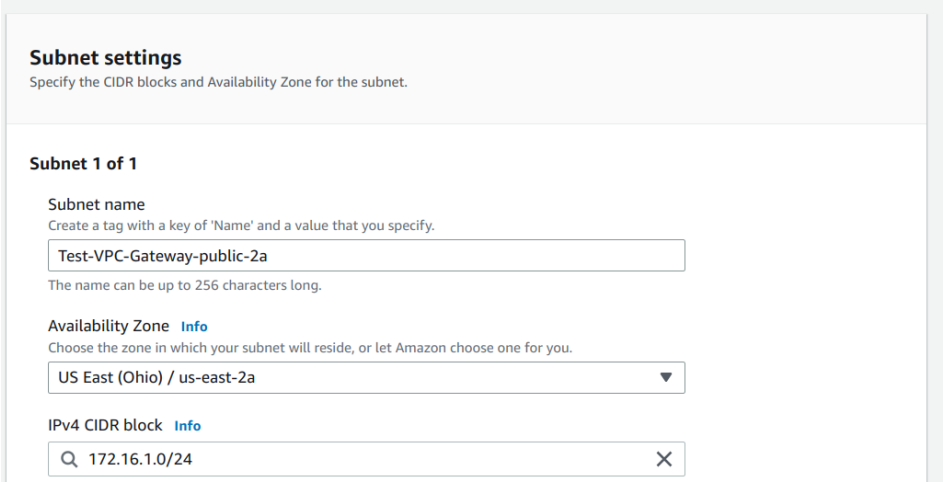
Task 2 - Create a gateway endpoint to connect EC2 inside a VPC to a S3 bucket.

Step 1 - Create a VPC with a CIDR block - “172.16.0.0/16”

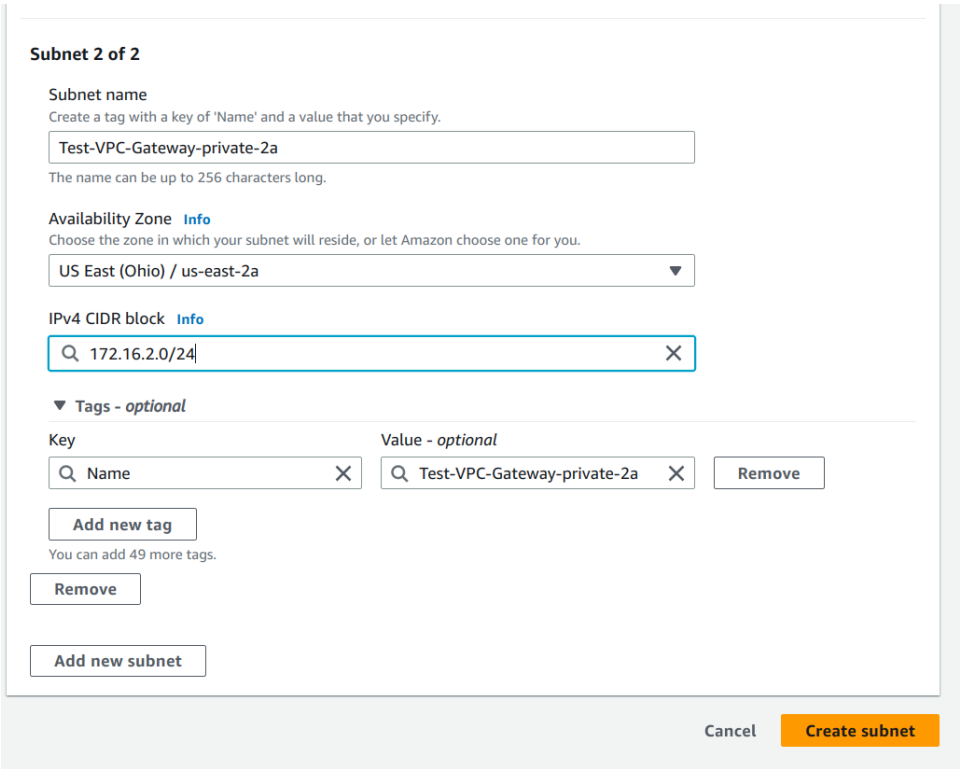


Step 2 - Create a public subnet.

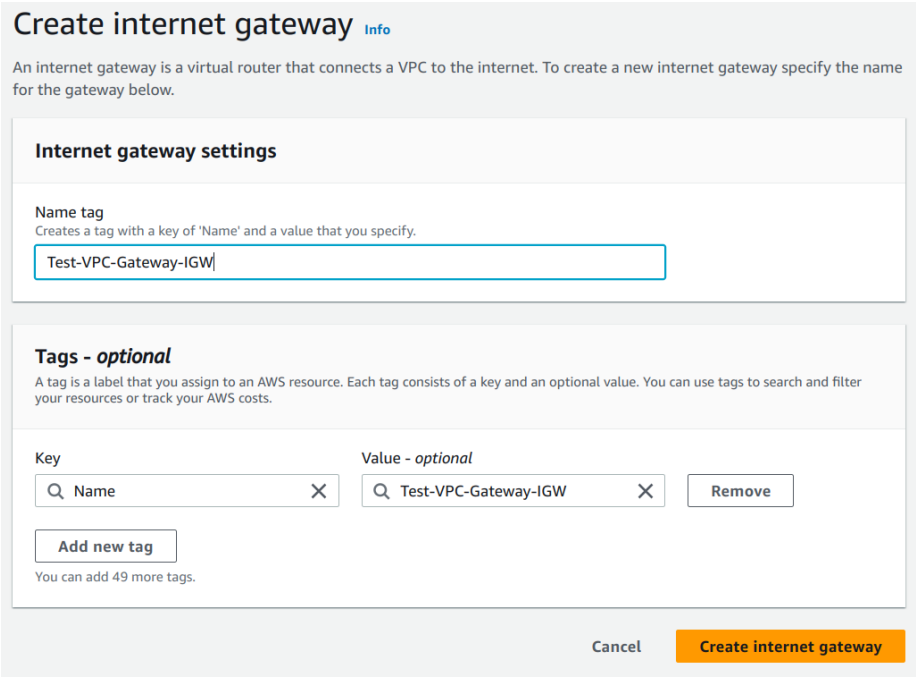




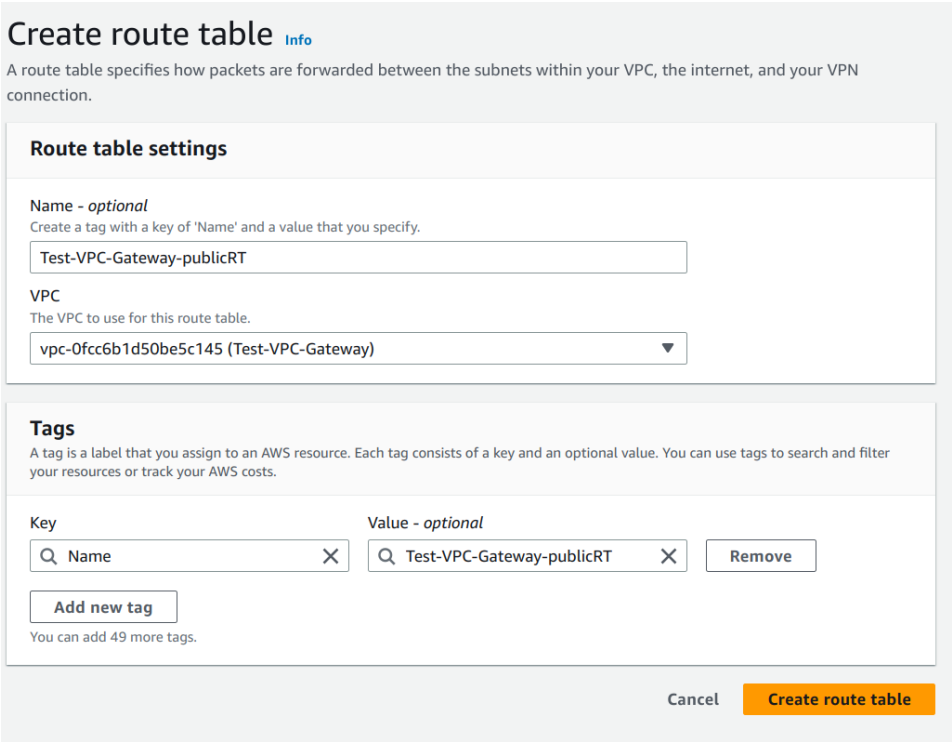
Step 2 - Create a private subnet in the VPC.



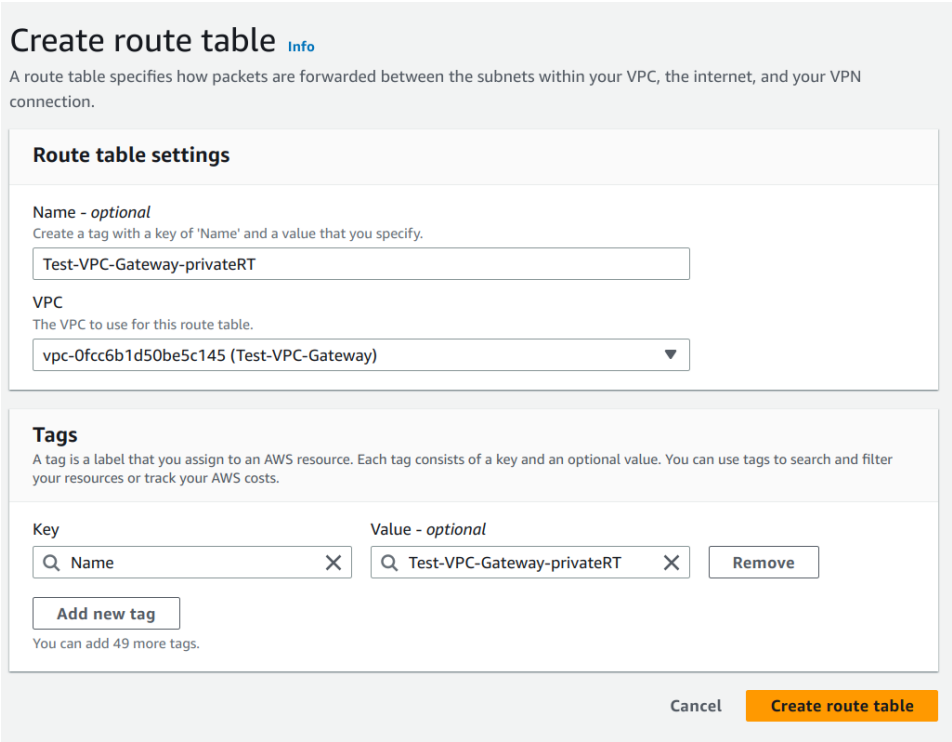
Step 3 - Create an internet gateway and attach it to the VPC.



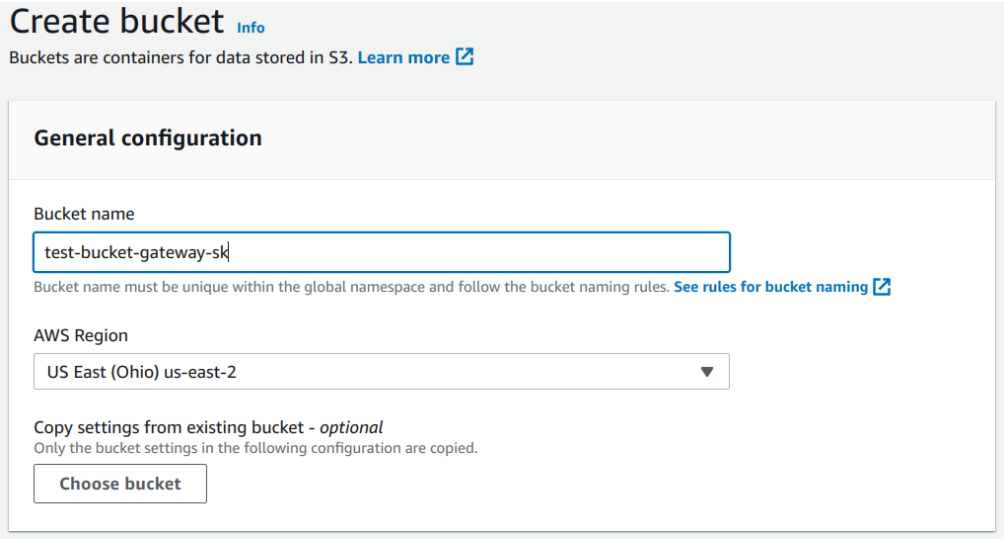
Step 4 - Create route table and edit routes and subnet association.

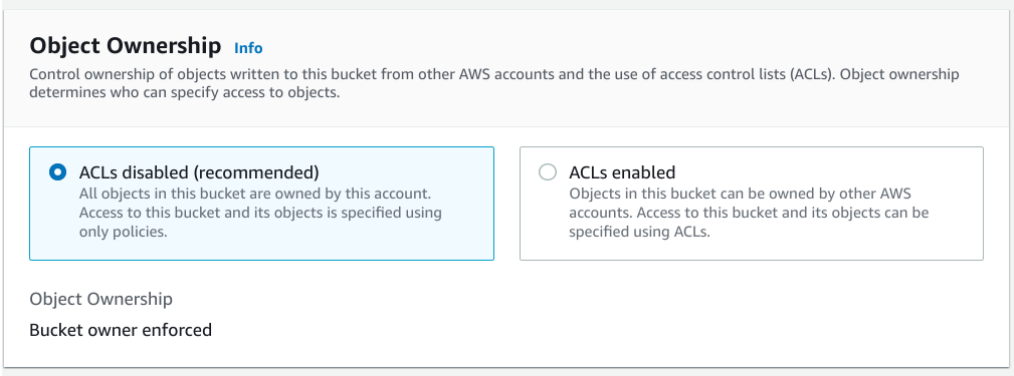


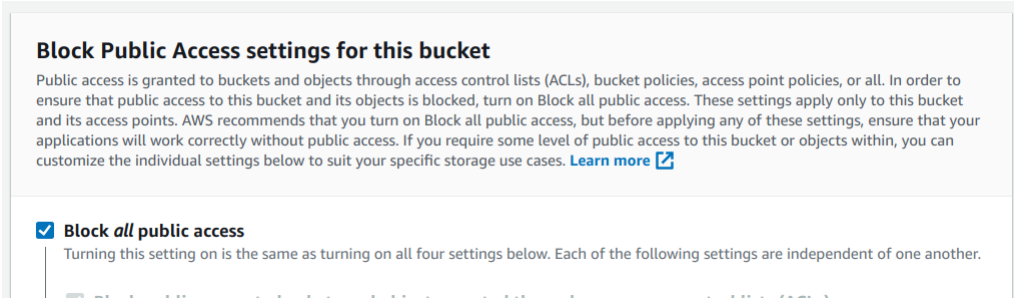
Step 5 - Create a private route table.

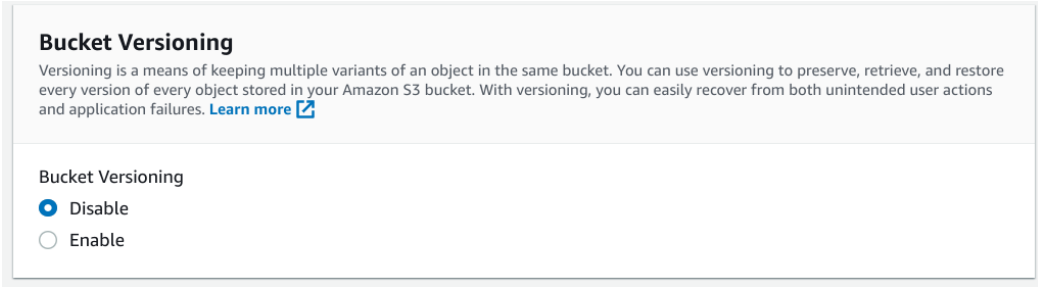


Step 6 - Create a S3 bucket.



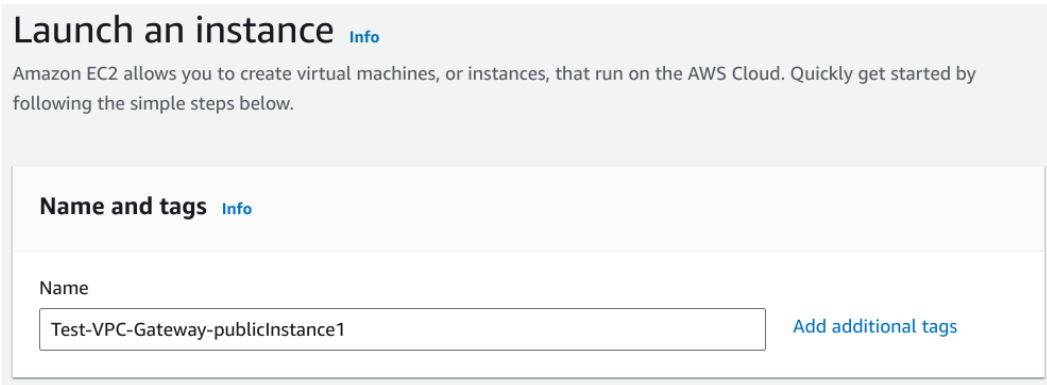






Step 6 - Launch EC2 instance in the public subnet.

It will be used to SSH into the private instance.



Instance type Info

Instance type

t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux pricing: 0.0116 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour

All generations

Compare instance types

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 - *required*

PubInstancePem

Create new key pair

Network settings Info

VPC - *required* Info

vpc-0fcc6b1d50be5c145 (Test-VPC-Gateway)
172.16.0.0/16

Subnet Info

subnet-07fa403bbaca163df Test-VPC-Gateway-public-2a
VPC: vpc-0fcc6b1d50be5c145 Owner: 237042273450 Availability Zone: us-east-2a
IP addresses available: 251 CIDR: 172.16.1.0/24)

Create new subnet

Auto-assign public IP Info

Enable

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*

public-SG

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

launch-wizard-1 created 2023-07-06T16:49:50.519Z

Inbound Security Group Rules

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

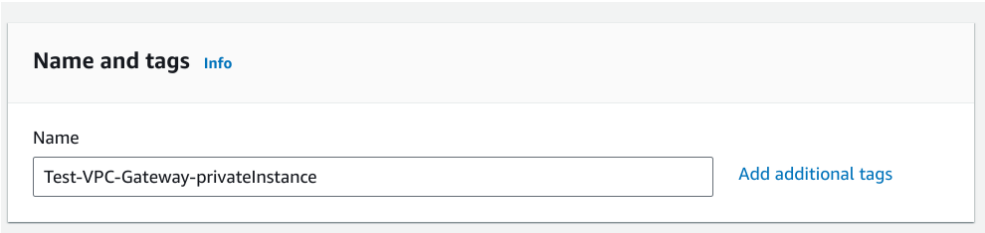
Remove

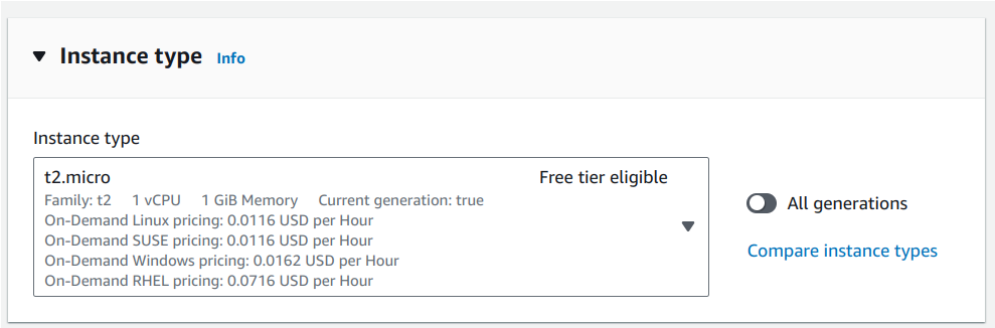
Type Info	Protocol Info	Port range Info
ssh	TCP	22

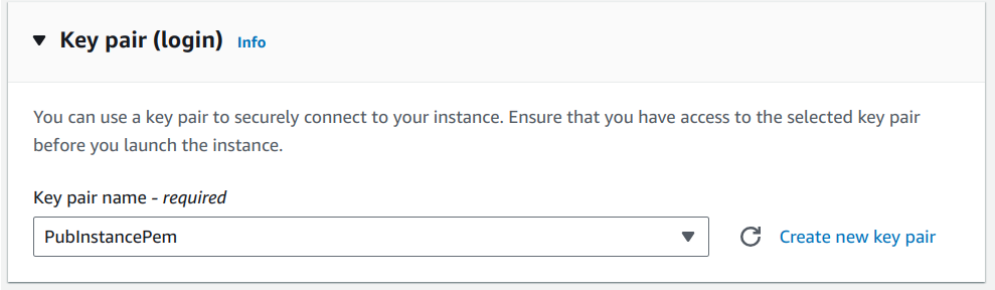
Source type Info	Source Info	Description - *optional* Info
Anywhere	*Add CIDR, prefix list or security*	*e.g. SSH for admin desktop*

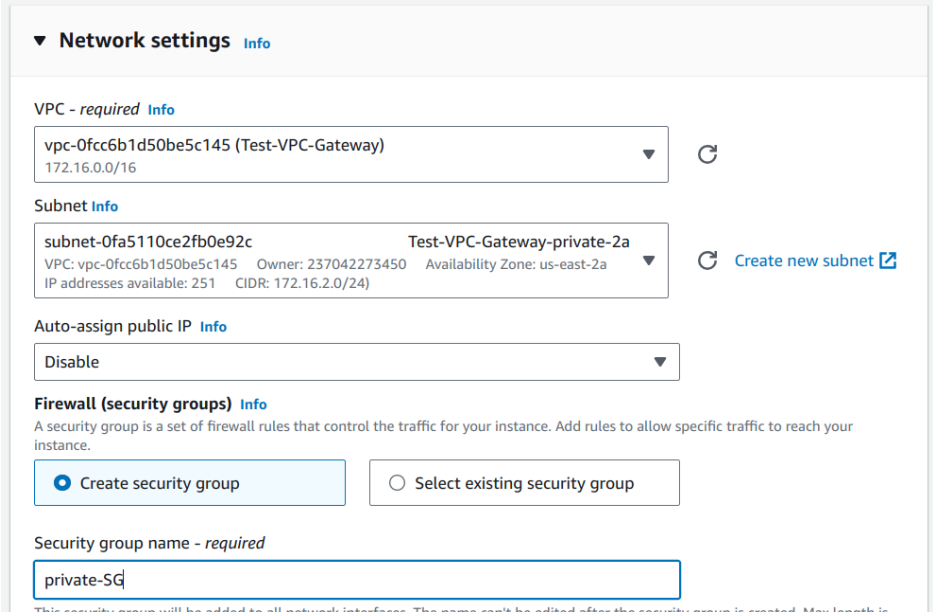
0.0.0.0/0 ::/0

Step 7 - Launch EC2 instance in the private subnet.









Description - *required* Info

launch-wizard-1 created 2023-07-06T16:54:39.182Z

Inbound Security Group Rules

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

Type Info	Protocol Info	Port range Info
ssh	TCP	22

Source type Info	Source Info	Description - *optional* Info
Anywhere	Add CIDR, prefix list or security 0.0.0.0/0 ::/0	e.g. SSH for admin desktop

Step 8 - Create an endpoint for the VPC.

Create endpoint Info

There are three types of VPC endpoints – Interface endpoints, Gateway Load Balancer endpoints, and Gateway endpoints. Interface endpoints and Gateway Load Balancer endpoints are powered by AWS PrivateLink, and use an Elastic Network Interface (ENI) as an entry point for traffic destined to the service. Interface endpoints are typically accessed using the public or private DNS name associated with the service, while Gateway endpoints and Gateway Load Balancer endpoints serve as a target for a route in your route table for traffic destined for the service.

Endpoint settings

Name tag - *optional*

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

my-endpoint-01

Service category

Select the service category

- (●) AWS services — Services provided by Amazon
- ( ) PrivateLink Ready partner services — Services with an AWS Service Ready designation
- ( ) AWS Marketplace services — Services that you've purchased through AWS Marketplace
- ( ) EC2 Instance Connect Endpoint — An elastic network interface that allow you to connect to resources in a private subnet
- ( ) Other endpoint services — Find services shared with you by service name

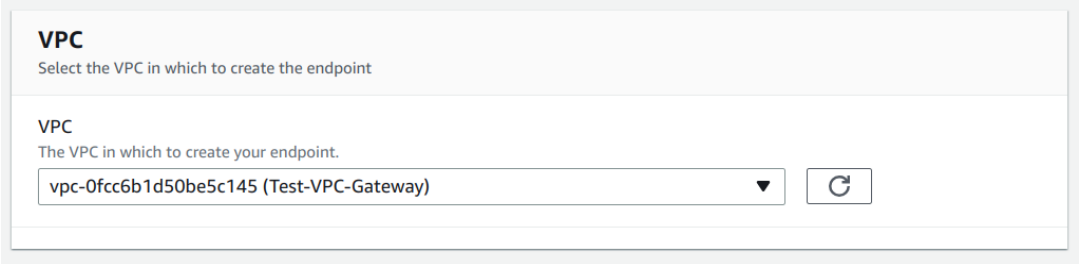
Services (1/2)

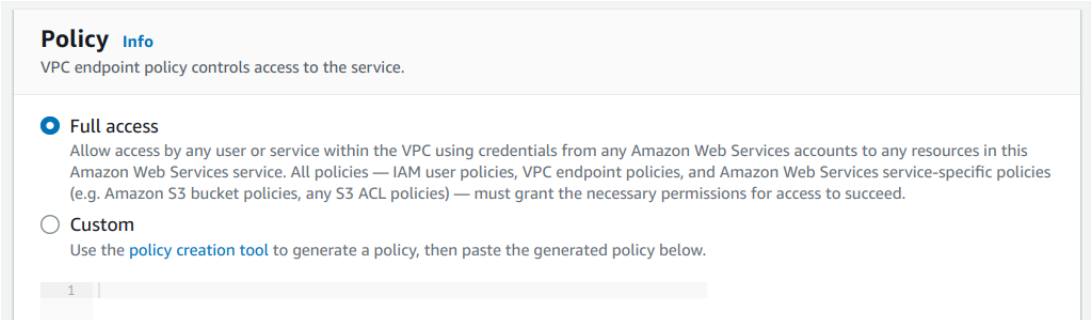
Find resources by attribute or tag

Service Name = com.amazonaws.us-east-2.s3 Clear filters

1

	Service Name	Owner	Type
(●)	com.amazonaws.us-east-2.s3	amazon	Gateway
( )	com.amazonaws.us-east-2.s3	amazon	Interface





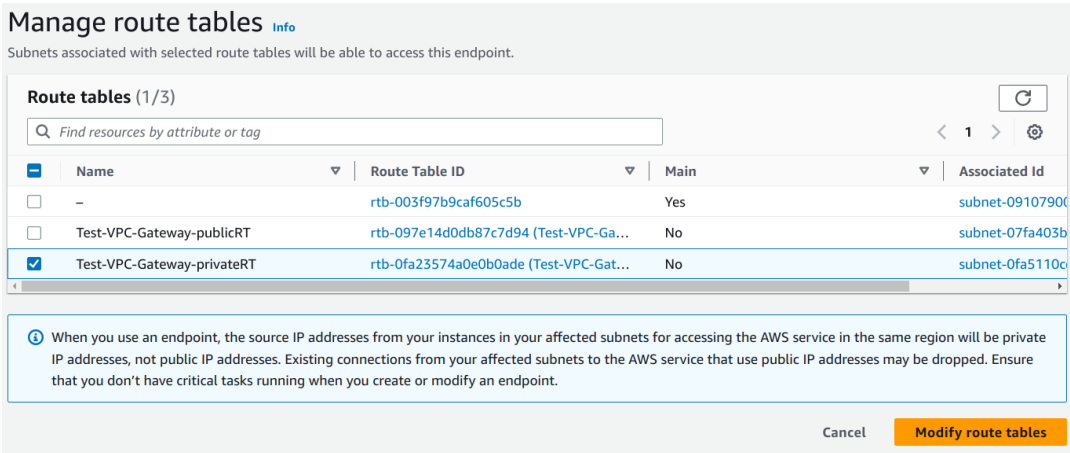
Step 9 - Connect to the private instance through the public instance.

Check if the S3 bucket can be listed in the private instance. When the endpoint is not associated with the route table of the private subnet, it is not possible to access the S3 bucket.

```
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-172-16-2-70 ~]$ aws configure
AWS Access Key ID [None]: AKIATOMGSBSVAWXCEIQR
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-2
Default output format [None]:
```

```
[ec2-user@ip-172-16-2-70 ~]$ aws s3 ls
```

Step 10 - Modify the route table for the VPC endpoint. Attach the private route table to the VPC endpoint.



Step 11 - Creating a sample file and uploading it to the bucket.

```
[ec2-user@ip-172-16-2-70 ~]$ aws s3 ls
2023-07-06 15:42:28 test-bucket-gateway-sk
[ec2-user@ip-172-16-2-70 ~]$ vi sampleFile
[ec2-user@ip-172-16-2-70 ~]$ cat sampleFile
This is a sample file to be uploaded in S3 bucket
[ec2-user@ip-172-16-2-70 ~]$ aws s3 cp sampleFile s3://test-bucket-gateway-sk/sampleFile
upload: ./sampleFile to s3://test-bucket-gateway-sk/sampleFile
[ec2-user@ip-172-16-2-70 ~]$ aws s3 ls s3://test-bucket-gateway-sk/
2023-07-06 17:22:51         50 sampleFile
```

Step 12 - Download the uploaded file into the instance and display its content.

```
[ec2-user@ip-172-16-2-70 ~]$ aws s3 cp s3://test-bucket-gateway-sk/sampleFile downloadedSampleFile
download: s3://test-bucket-gateway-sk/sampleFile to ./downloadedSampleFile
[ec2-user@ip-172-16-2-70 ~]$ cat downloadedSampleFile
This is a sample file to be uploaded in S3 bucket
[ec2-user@ip-172-16-2-70 ~]$
```

Architecture diagram for the above solution.