

**How to Connect to Private subnet MySQL RDS over SSH with Bastian Host**

**Let’s the Bastion & RDS Journey begins**



# **Steps**

1. **Create a custom VPC**
2. **Create a MySQL RDS instance on the free tier**

* It must be in the same VPC and subnet as the private ec2 instance

1. **Using the private ec2 instance**

- install the MySQL Client

- test that you can connect to the RDS instance using the MySQL client

4. **Create a tunnel**

- configure a tunnel connection from your macbook via the bastion to the private EC2 instance

1. **From your Local system**

* use the tunnel to connect to the RDS instance
* create a new database on the RDS instance
* create a table in the new database on the RDS instance

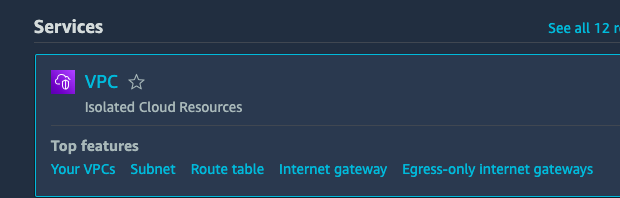
**Create a custom VPC**

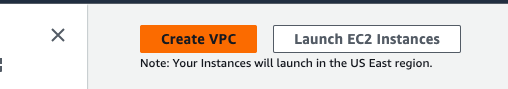
As we know, VPC stands for Virtual Private Cloud, the first step of every project is to create a VPC so that on top of that VPC only we can create EC2 instances, databases or any other resources.

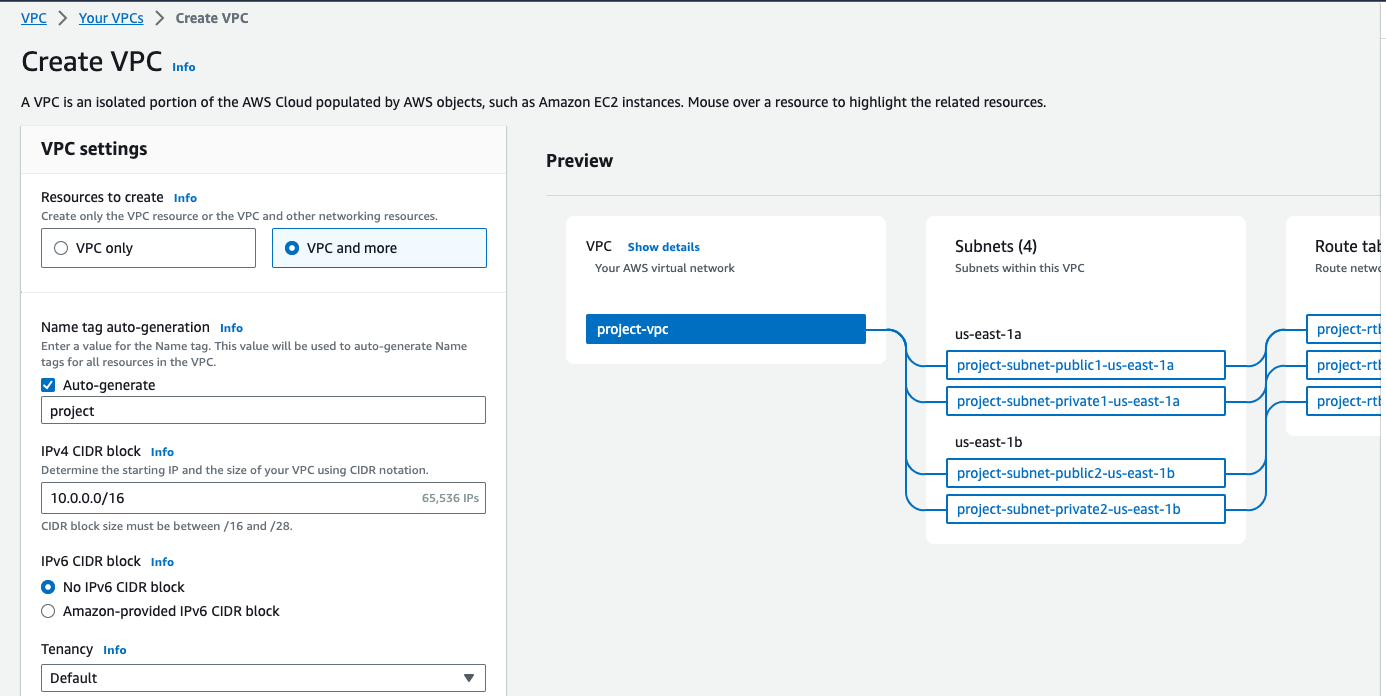
We can find a default VPC for every single region. That default VPC comes with multiple subnets, but the problem is all the subnets are public (Internet facing) only.

That is why it is always recommended to create our own default VPC and run all the resources there. Besides, in this project we need to create a VPC with multiple public & private subnets.

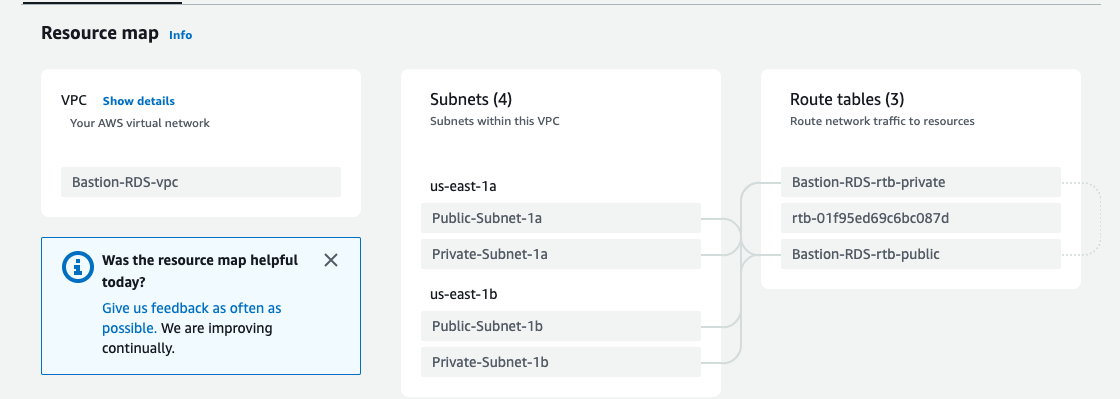
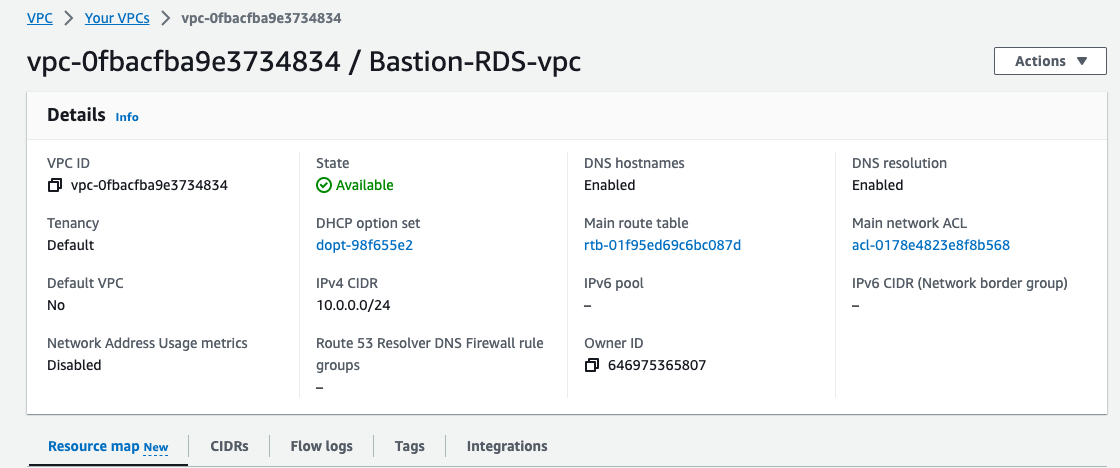
Public subnet resources are going to be Internet facing, however private subnet ones would be internal resources like if we need to provide Internet to the private subnet then we depend on additional services like NAT Gateway or NAT instances.



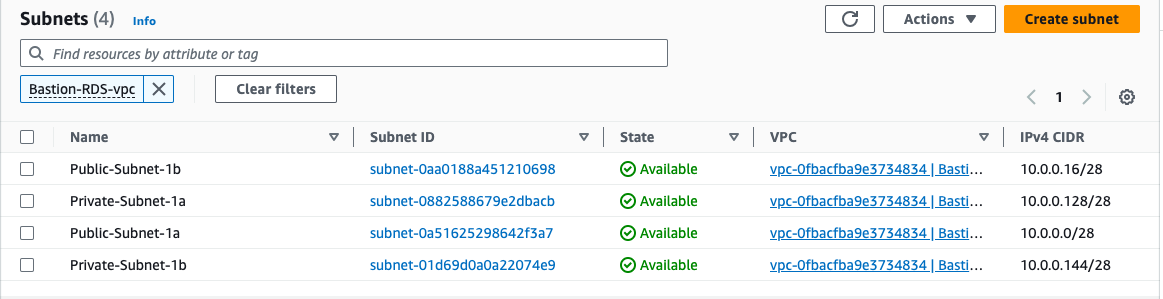




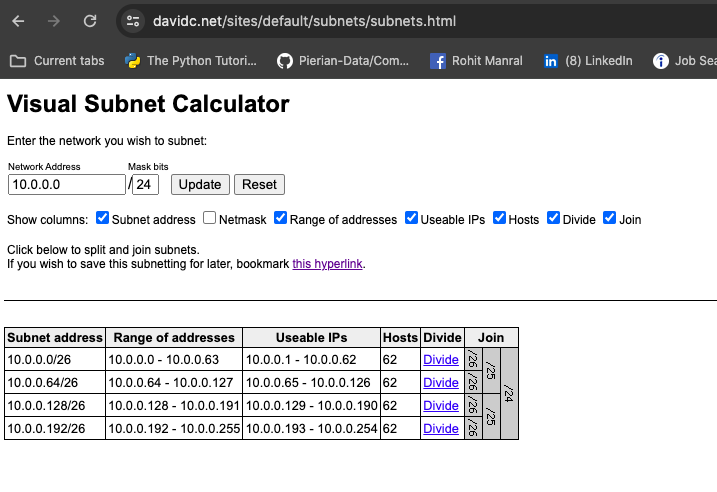
AWS supports from /28 to /16 CIDR block subnets which decides the range or size of the VPC.



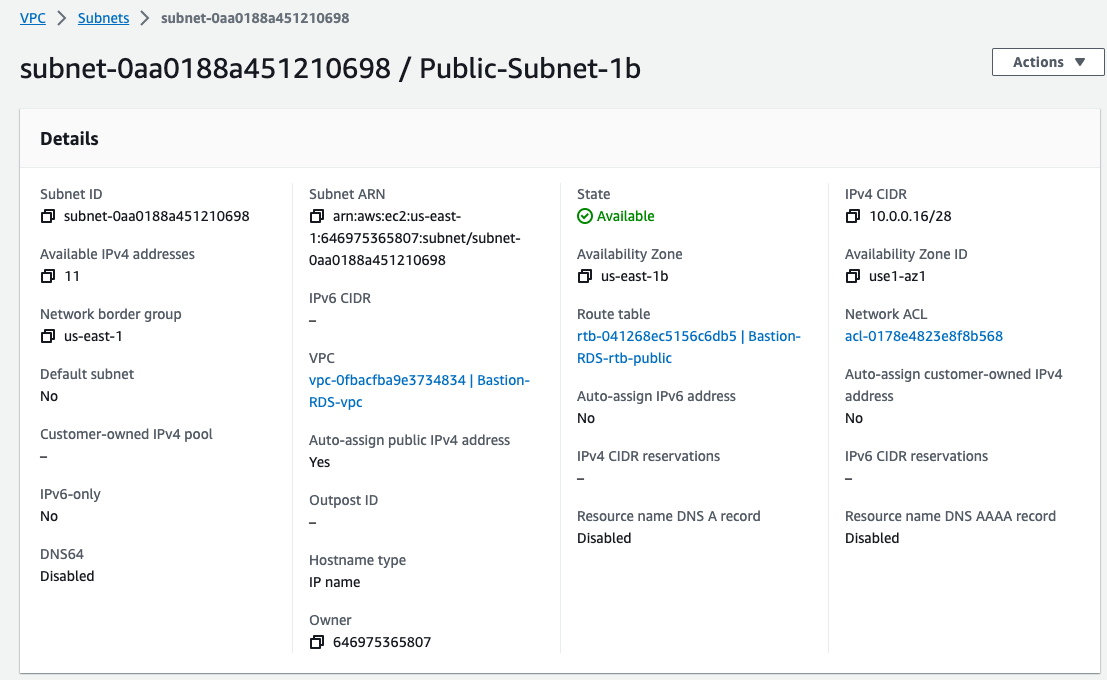
Now, coming to the subnets

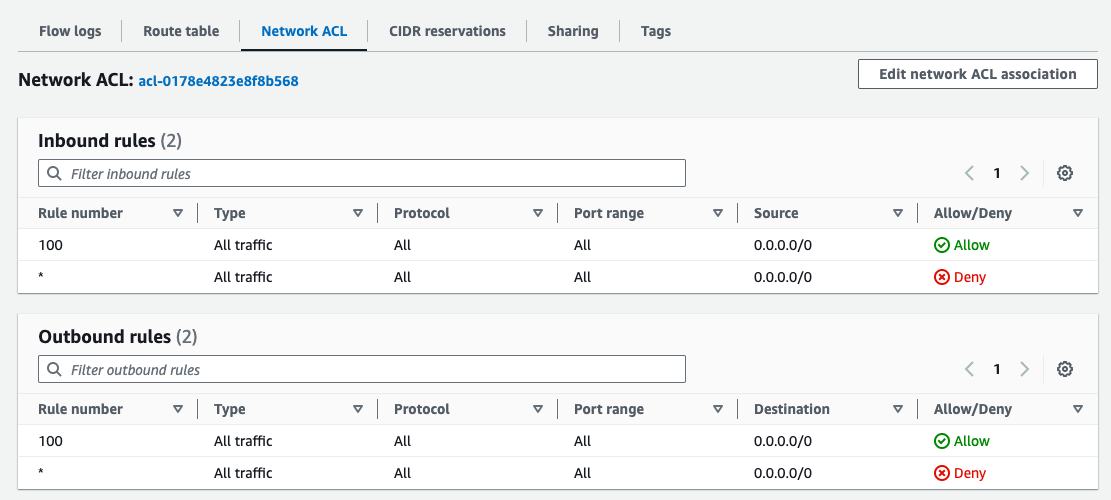
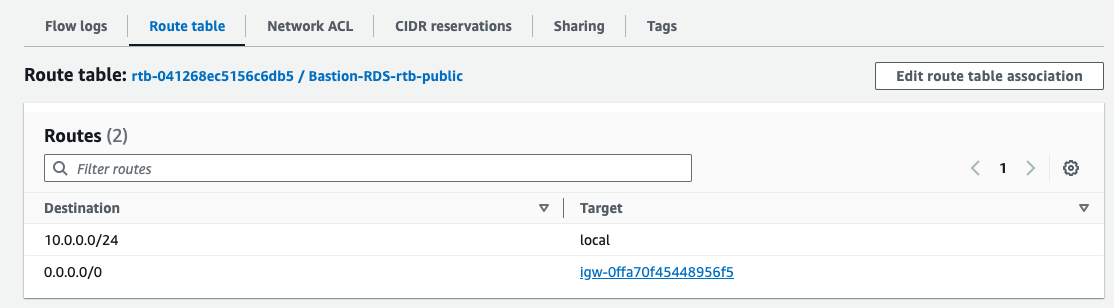


Creating 4 subnets:

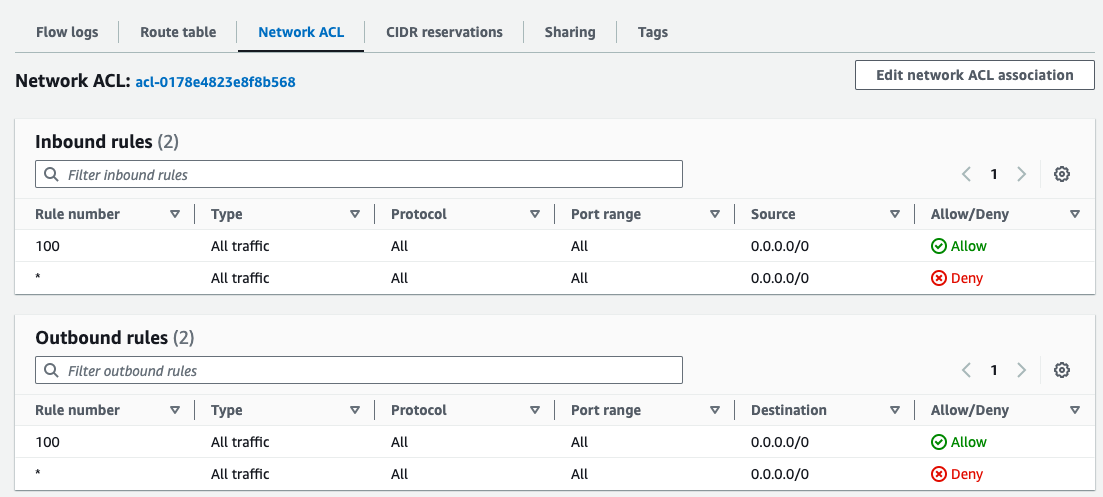
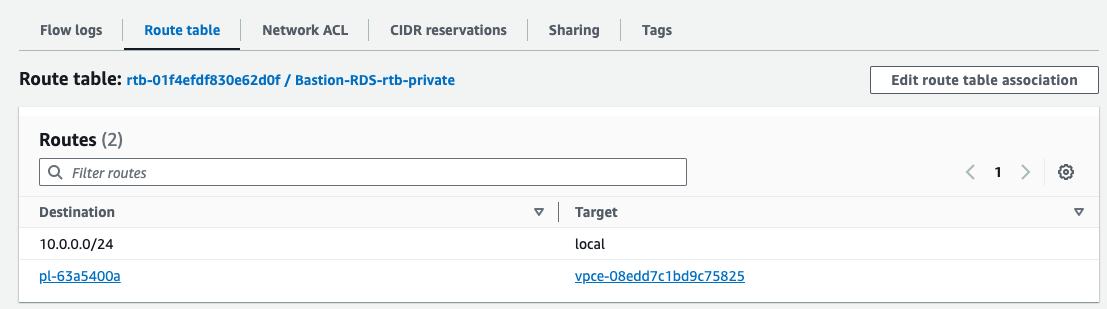
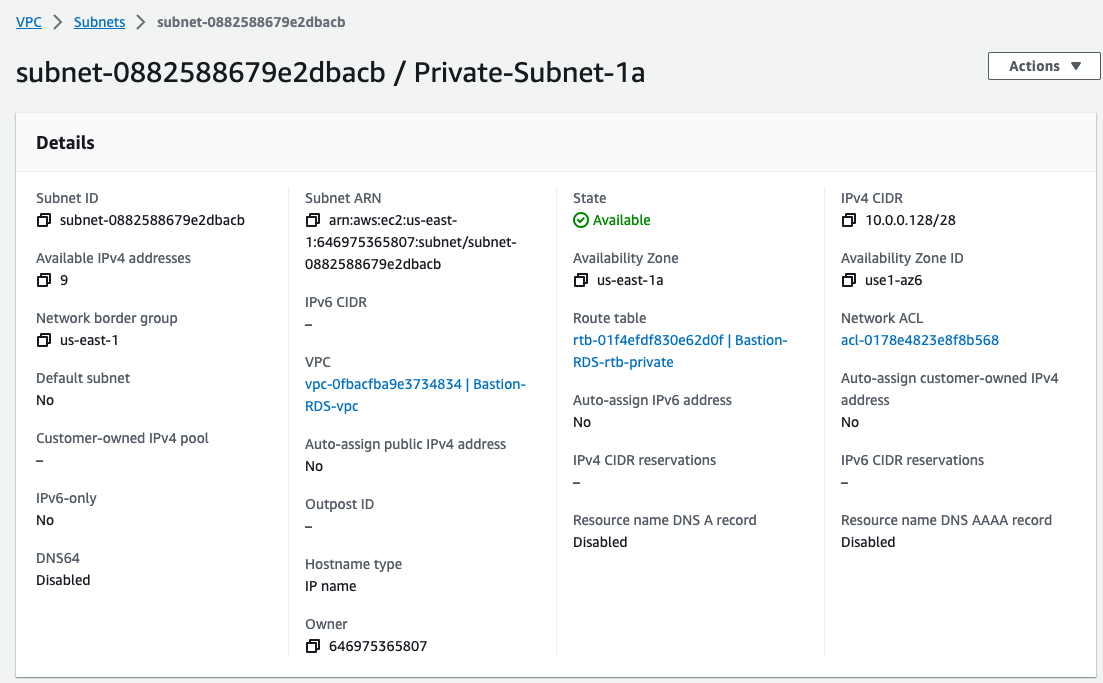


1. Public-Subnet-1b

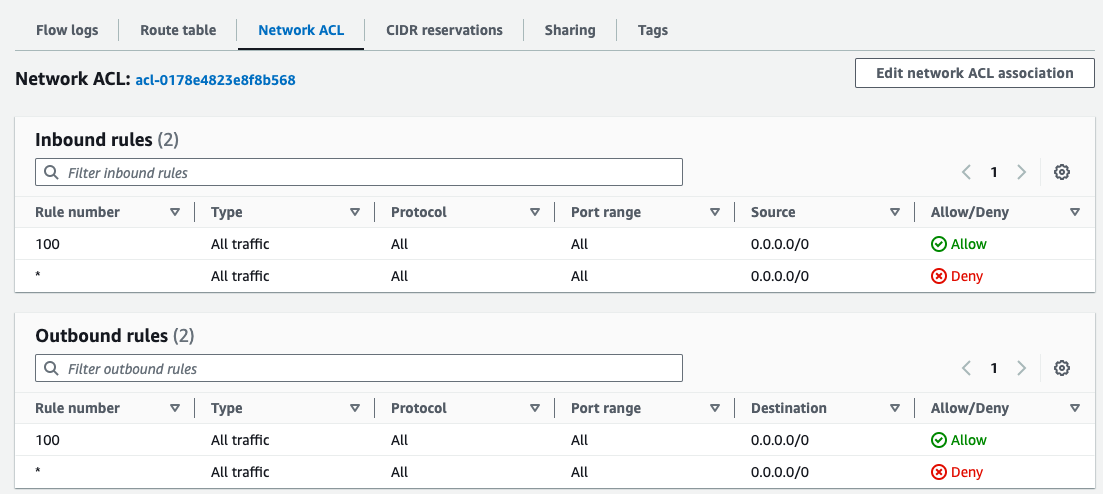
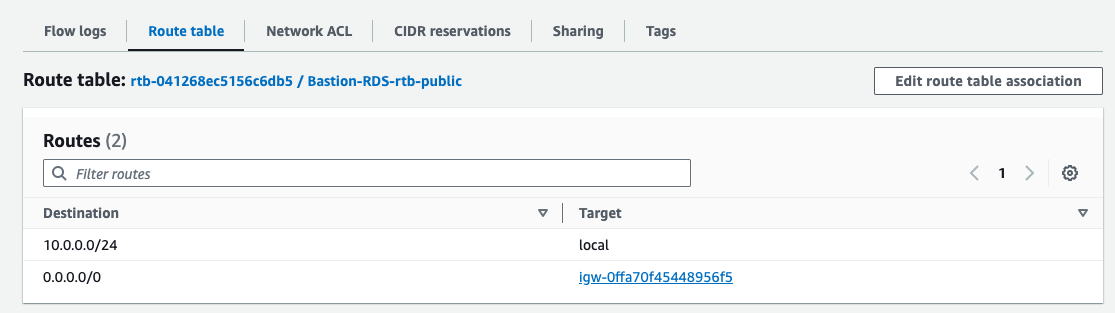
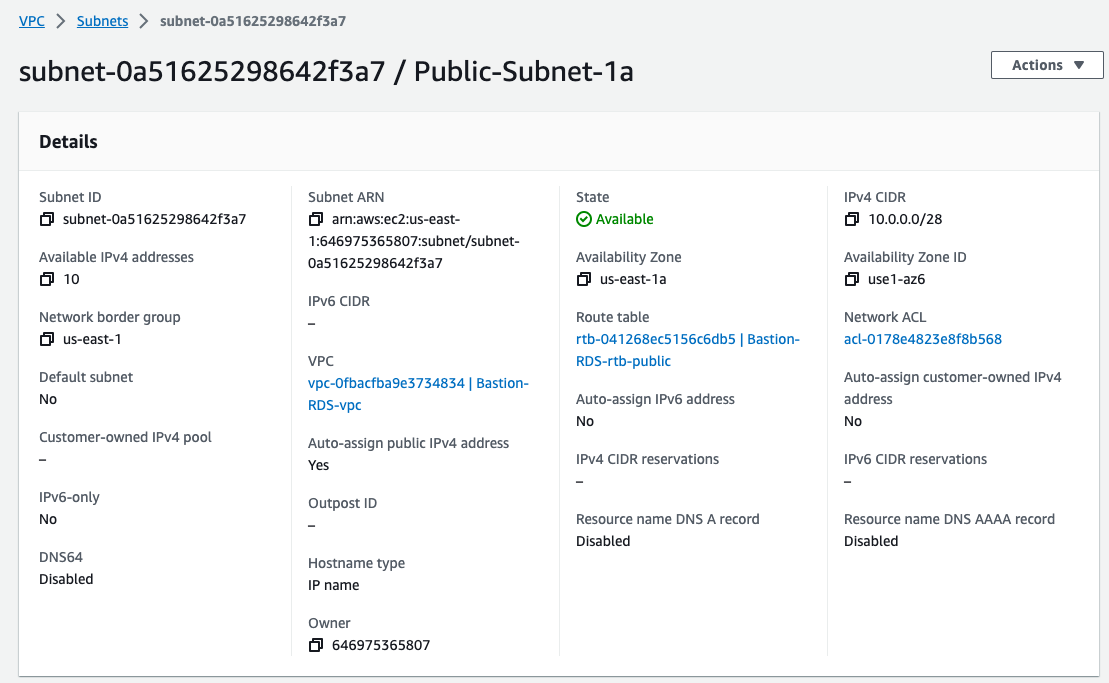




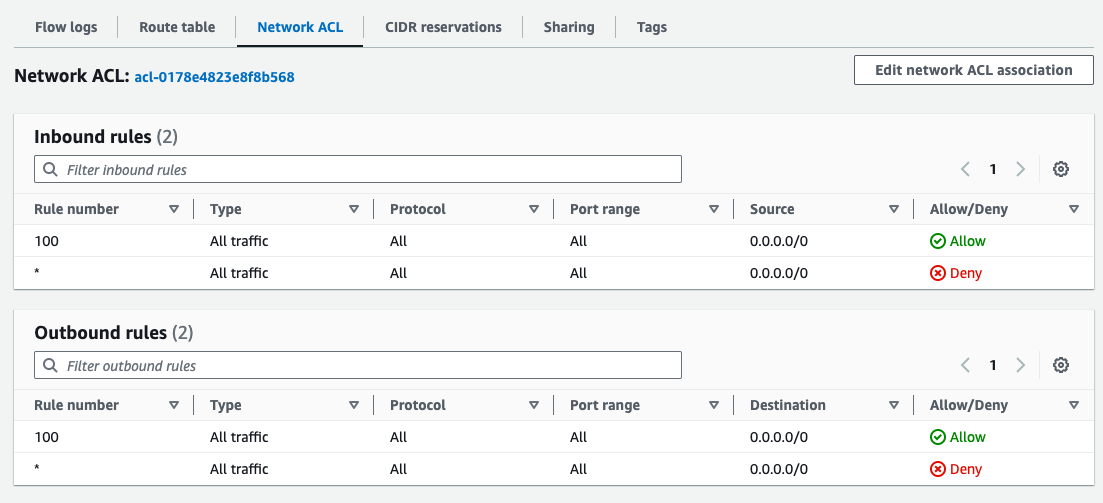
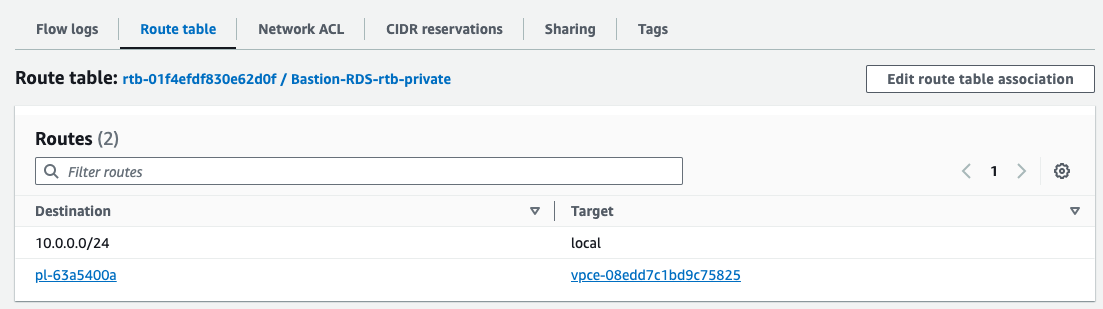
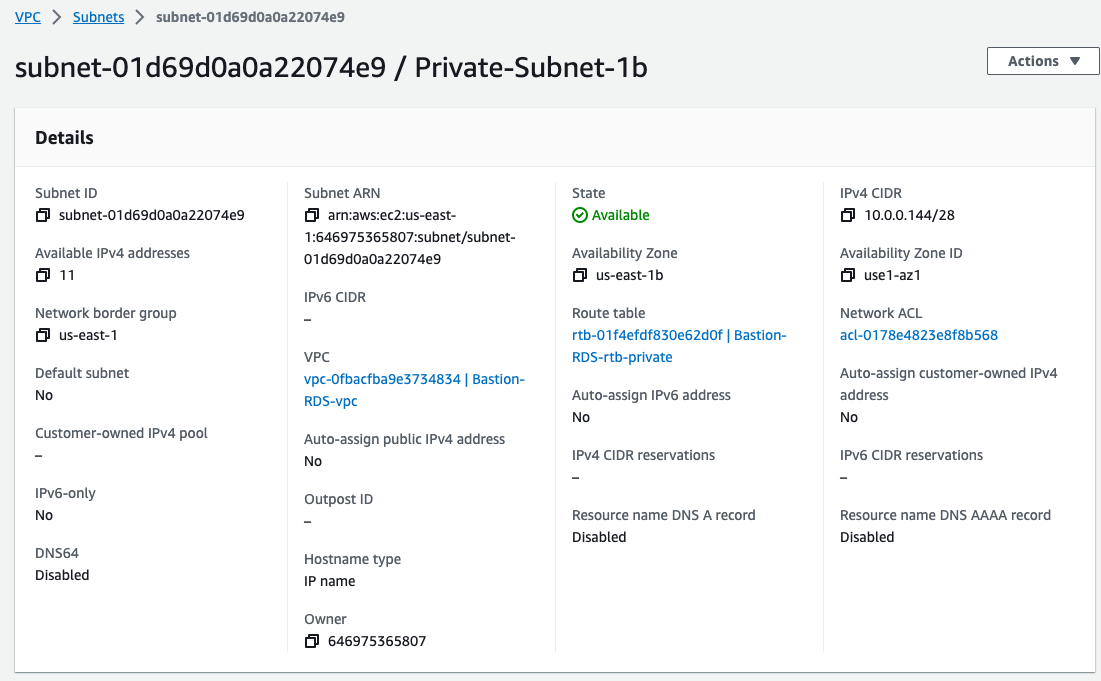
1. Private-Subnet-1a



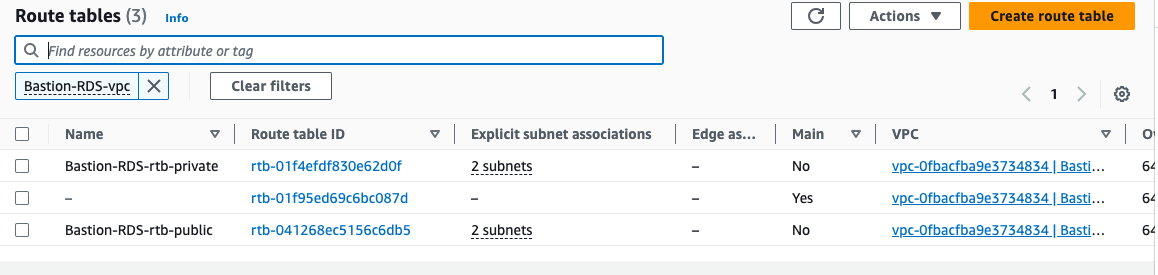
1. Public-Subnet-1a



1. Private-Subnet-1b



Route Tables

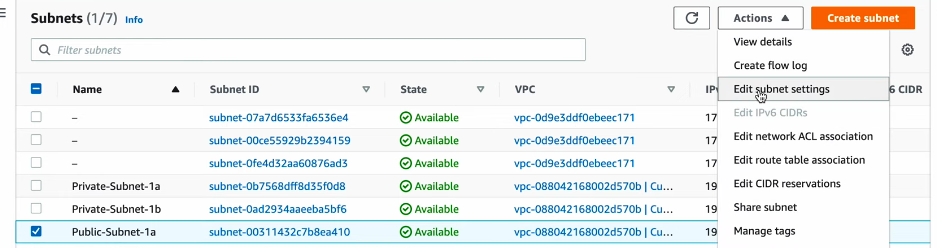


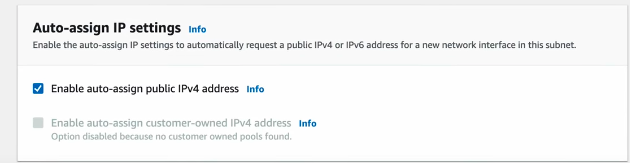
Both Private subnets are part of private route table that have only local route that enable internal communication.

Both Public subnets have a route via internet gateway which means these 2 subnets can communicate with resources via internet or it can access internet.

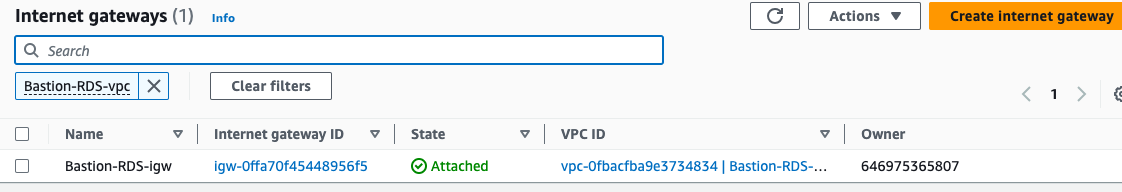
If you want to get connected to Private route/subnet resources, then we need to depend on jump server or bastion host.

Whatever the resources we are going to launch in public subnet needs a public IP address, so we can enable that setting as follows:

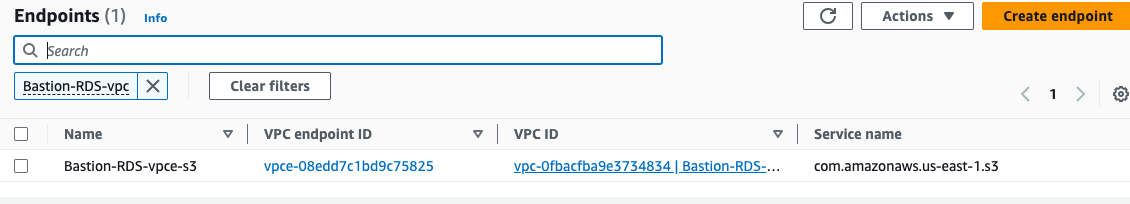




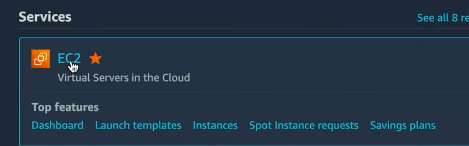
Internet Gateway



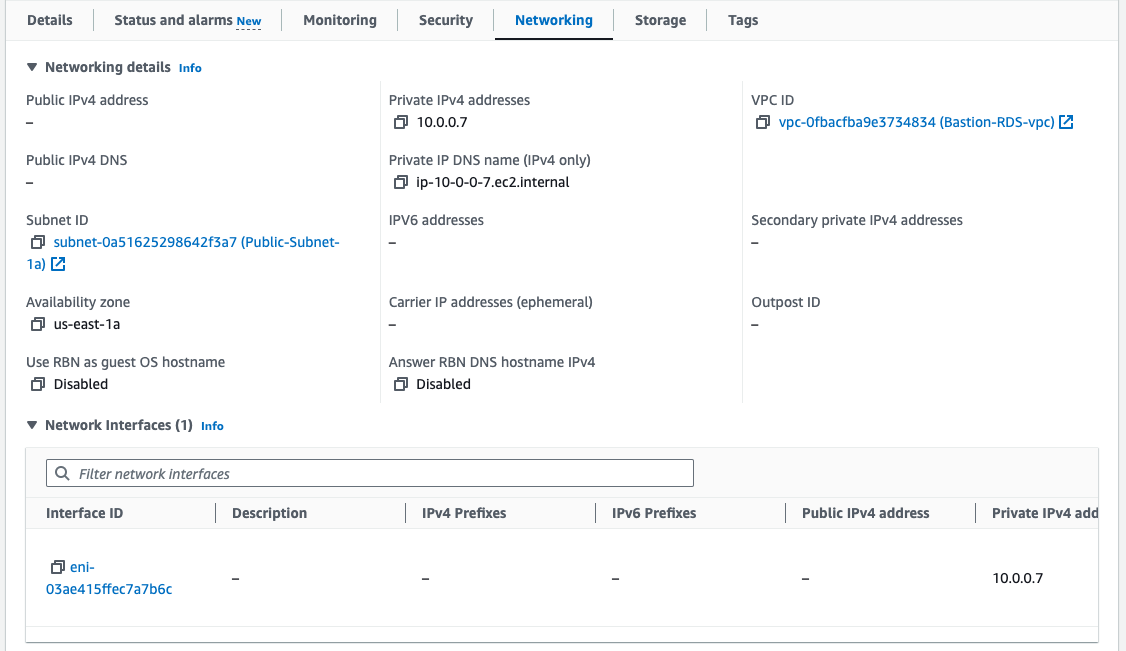
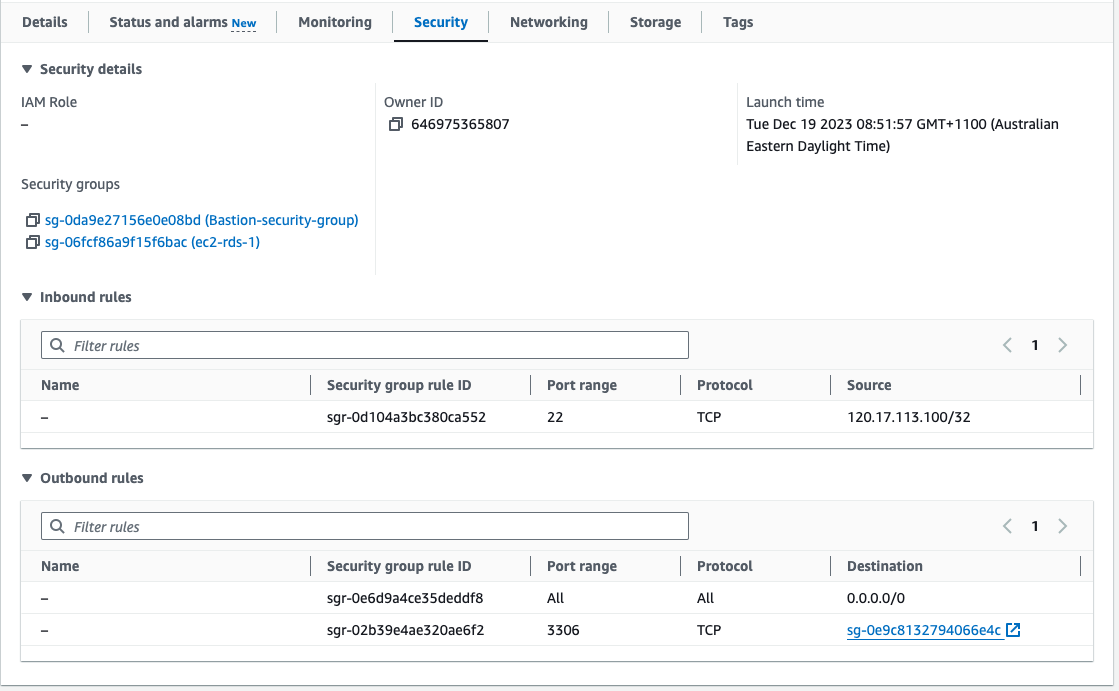
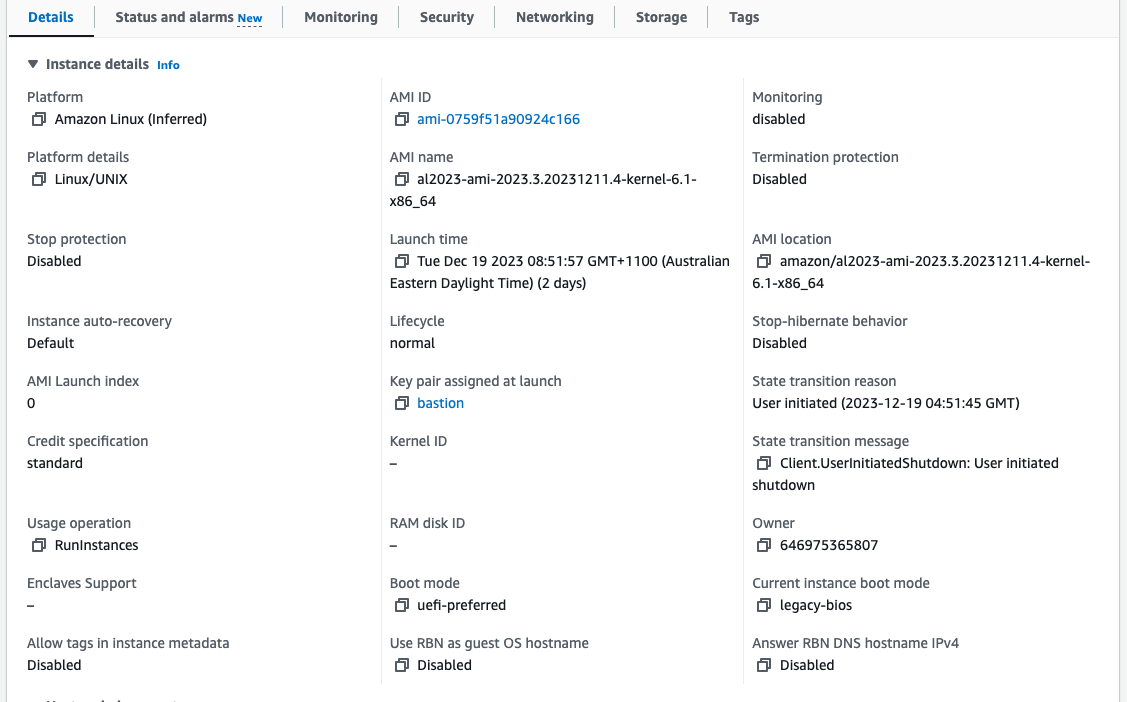
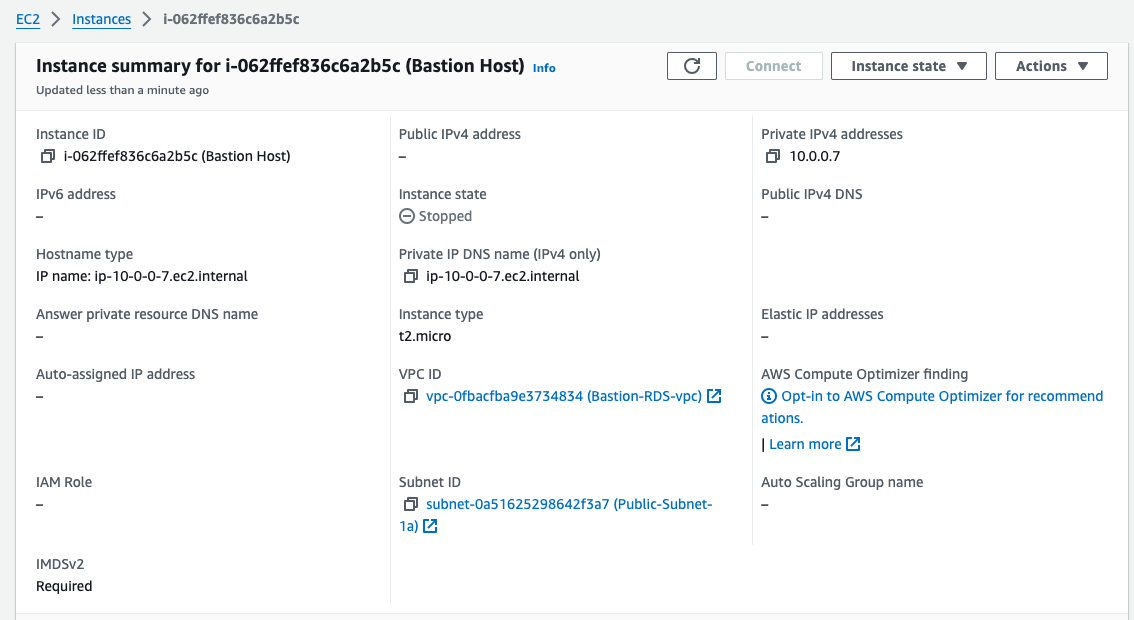
Endpoints



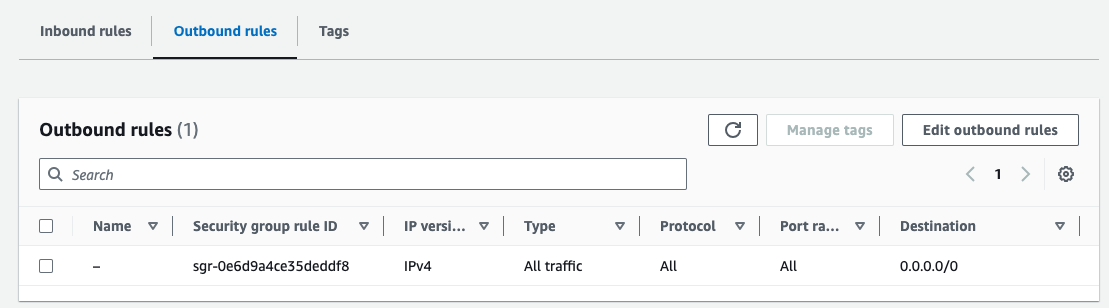
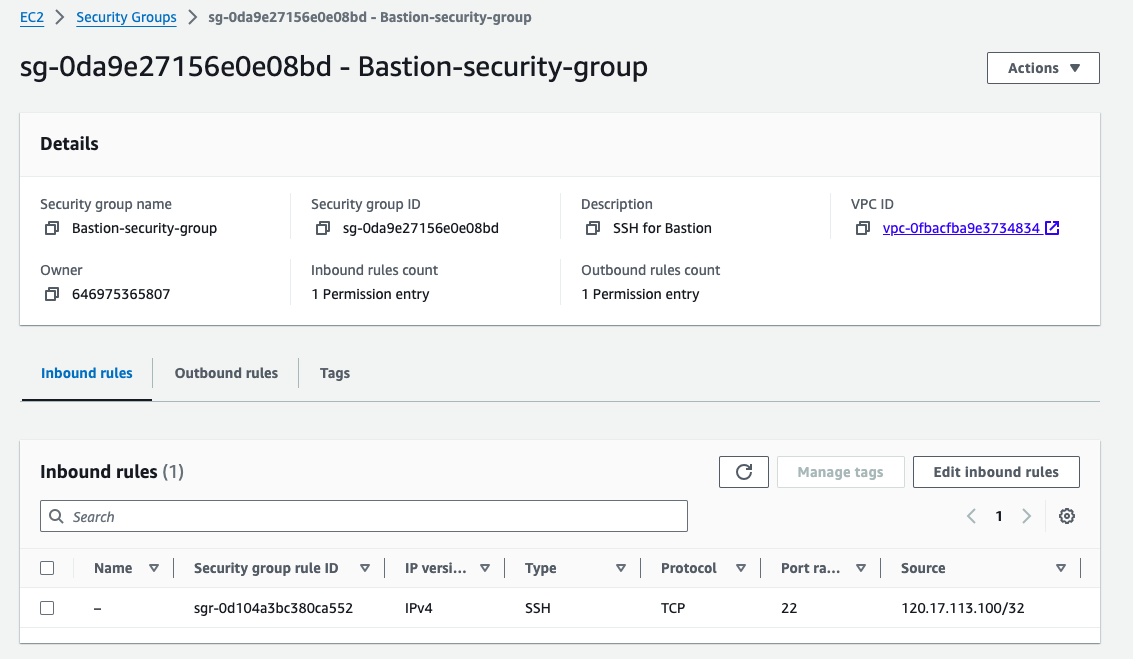
Finally, to test this VPC Architecture we will launch instances:



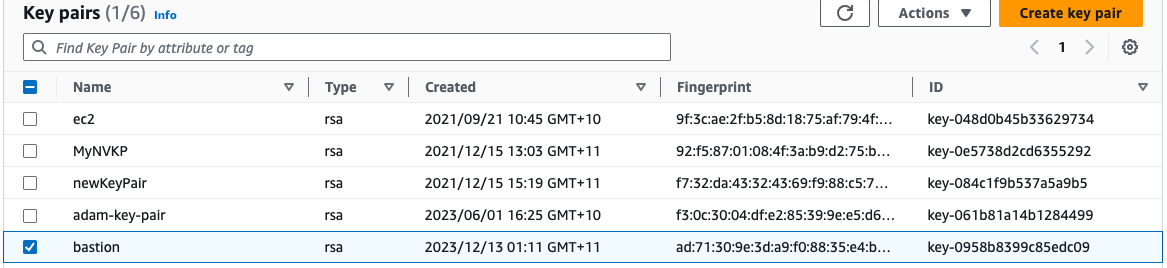
Creating **Bastion Host** instance



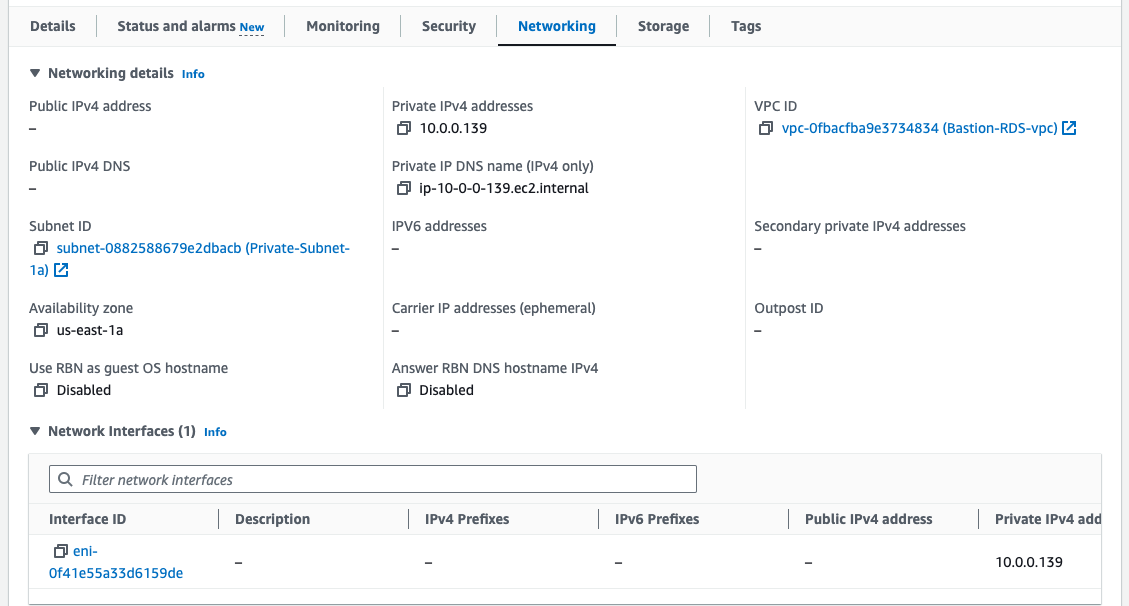
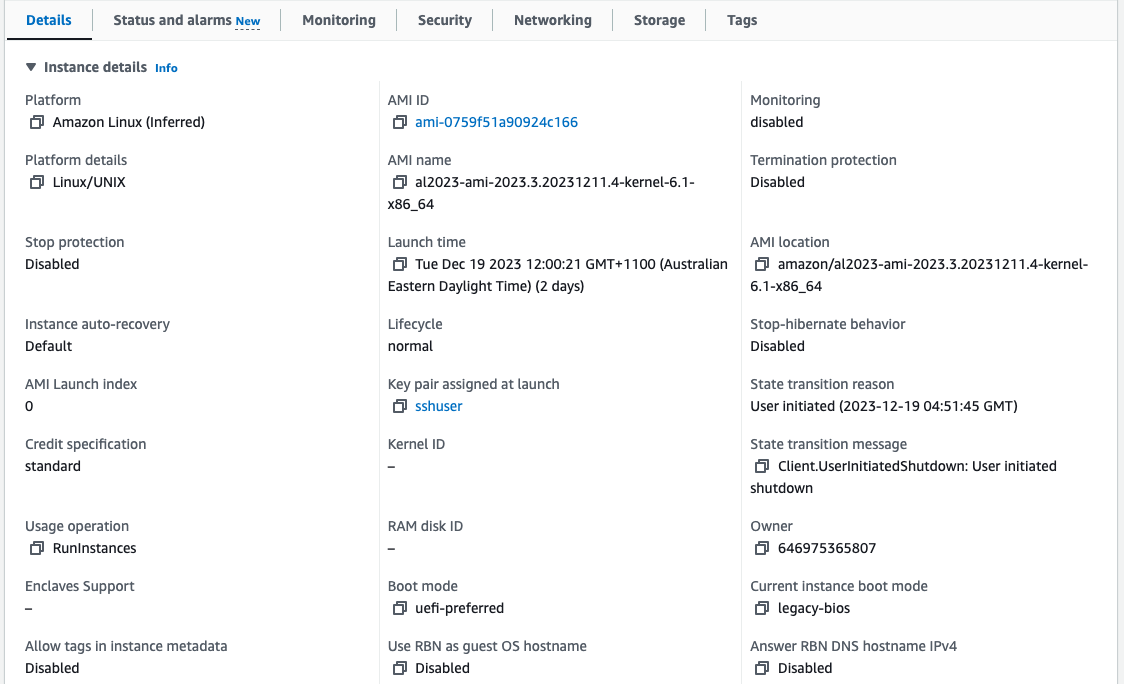
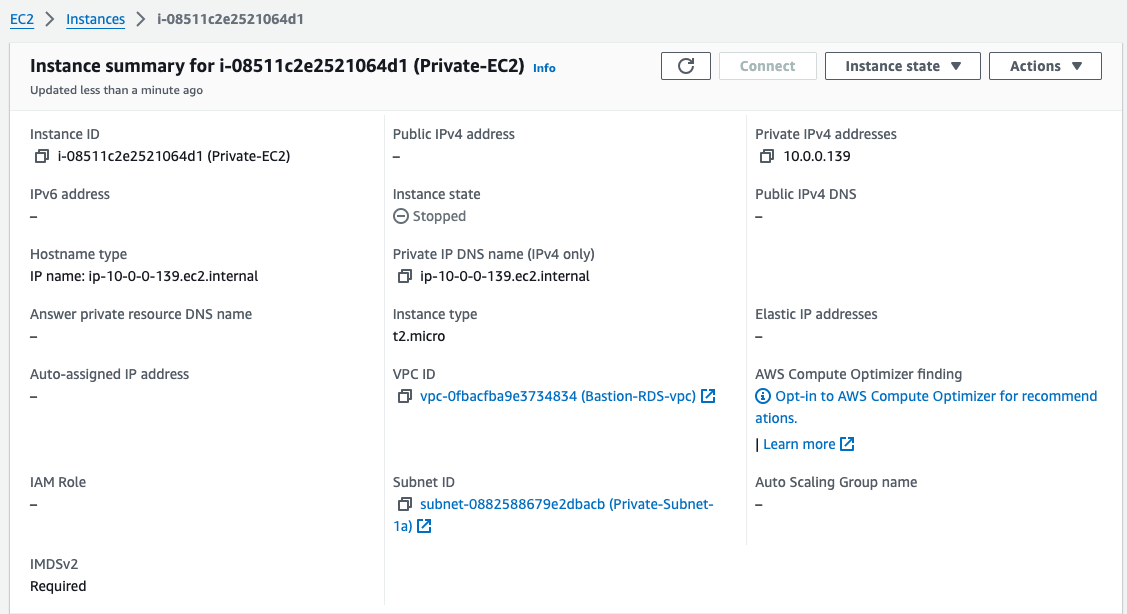
**Security Group** for **Bastion Host** instance



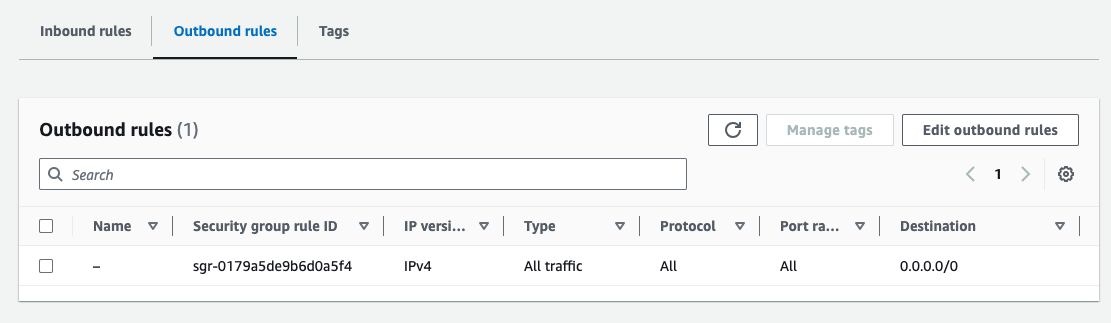
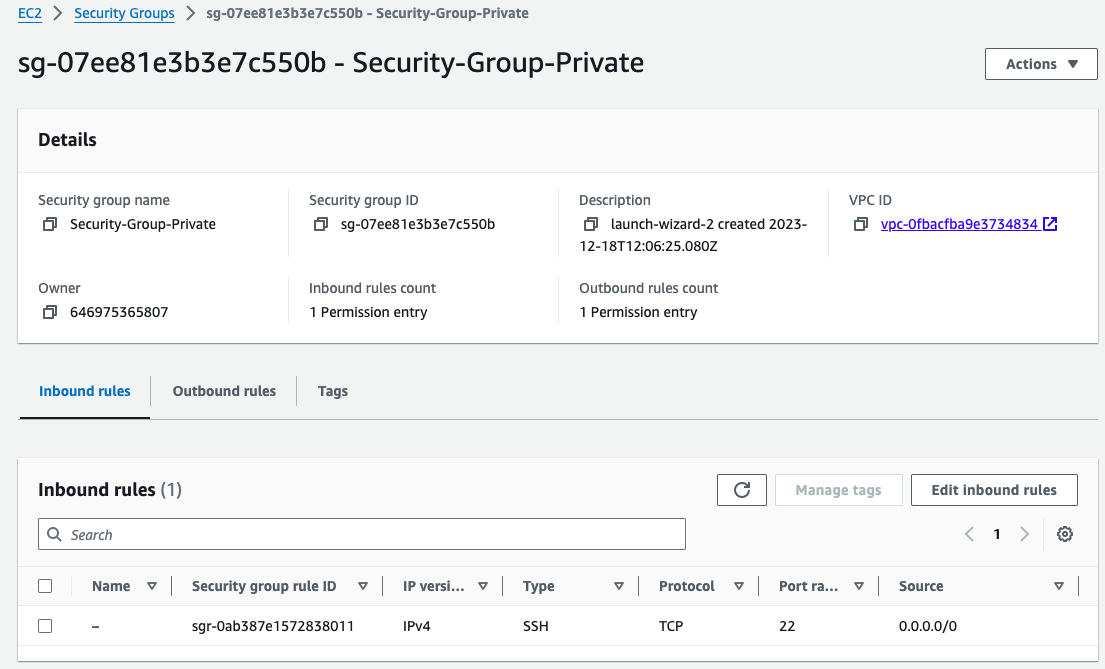
**Key Pair** for **Bastion Host** instance



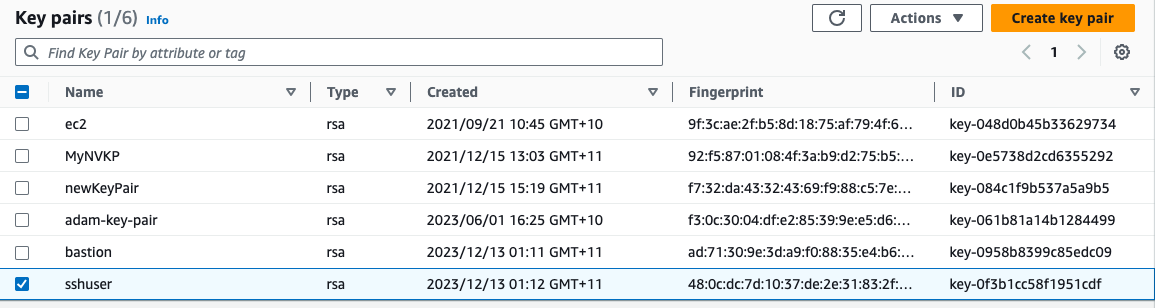
Creating **Private Linux** instance



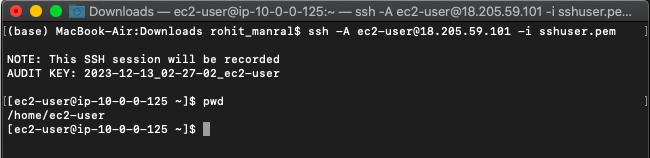
**Security Group** for **Bastion Host** instance



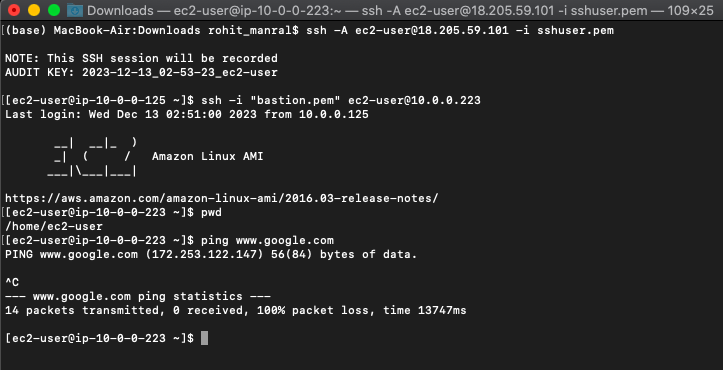
**Key Pair** for **Bastion Host** instance



Connection to **Bastion Host** instance



Connection to **Private Linux** instance

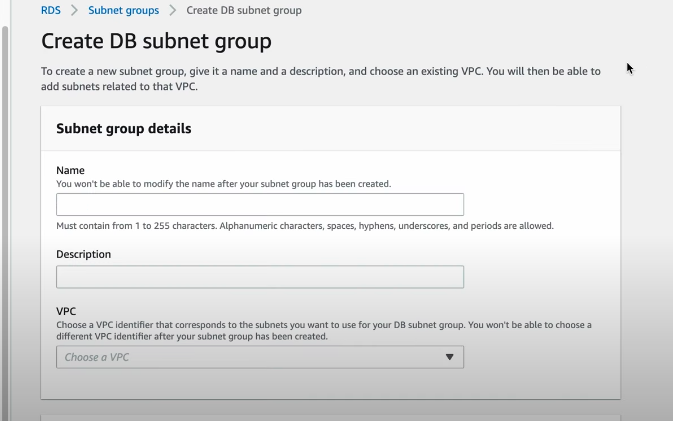


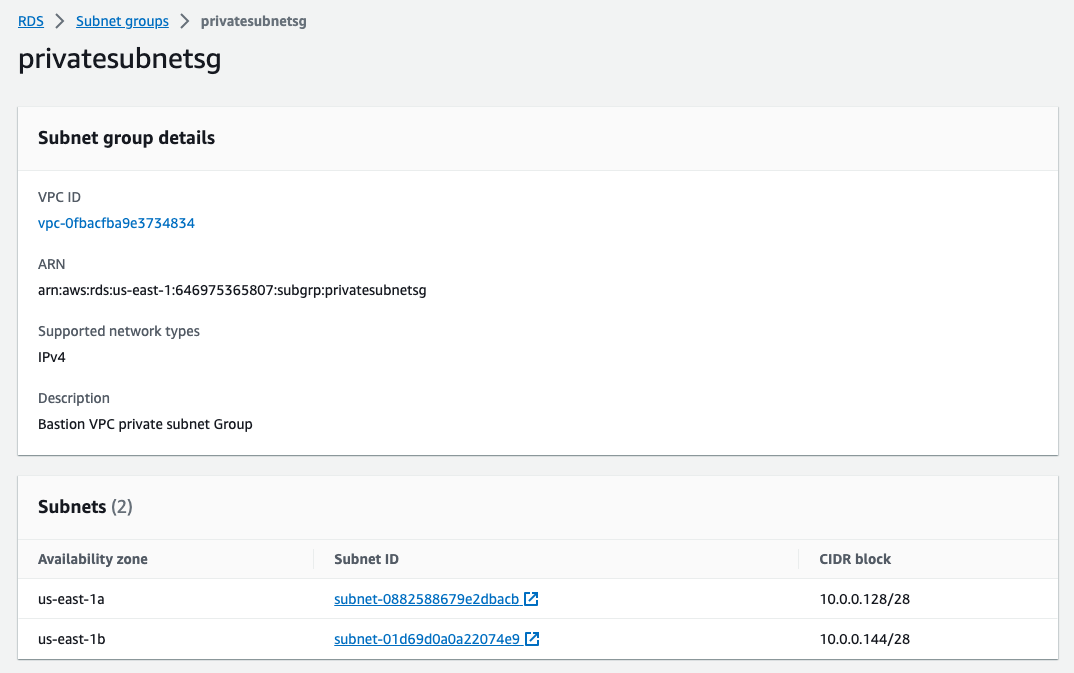
**How to Launch MySQL RDS DB instance in our Custom VPC’s Private subnet**

Here, we will use the two private subnets created above & create a subnet group, within that subnet group we will launch the MySQL RDS DB instance.

Go to **RDS --> Subnet Groups**

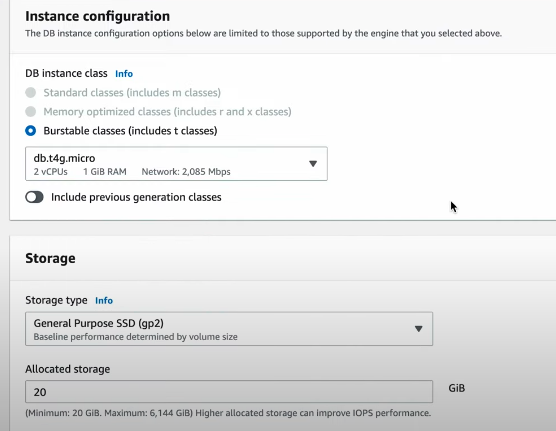
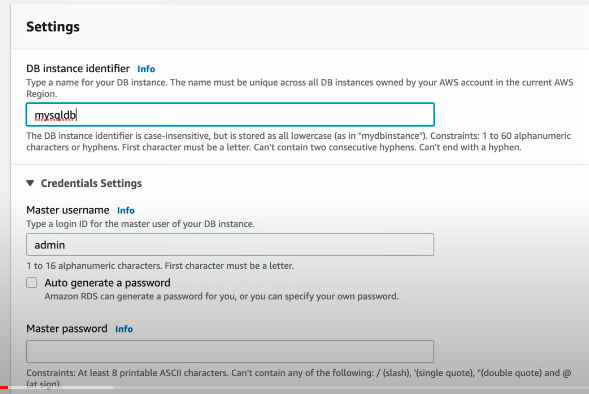
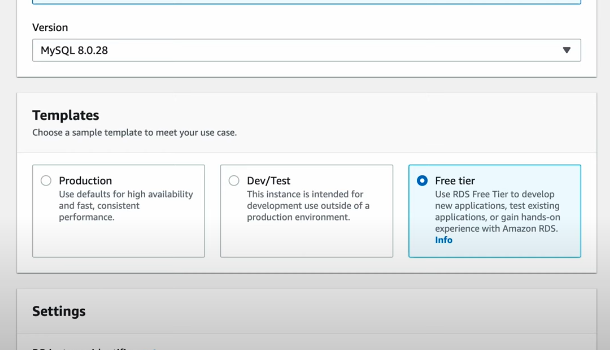
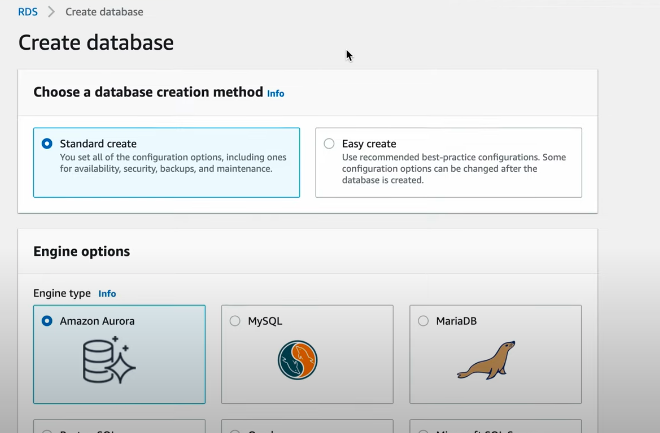




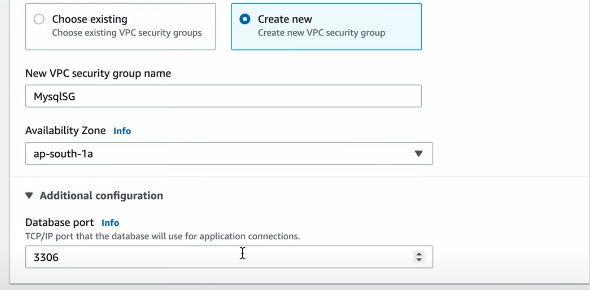


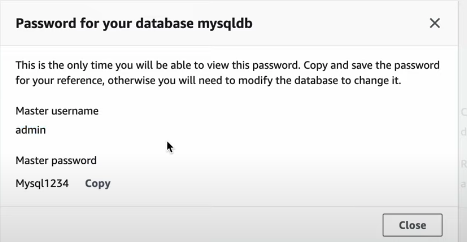
Above, we selected both the private subnets.

Now, install one MySQL DB instance



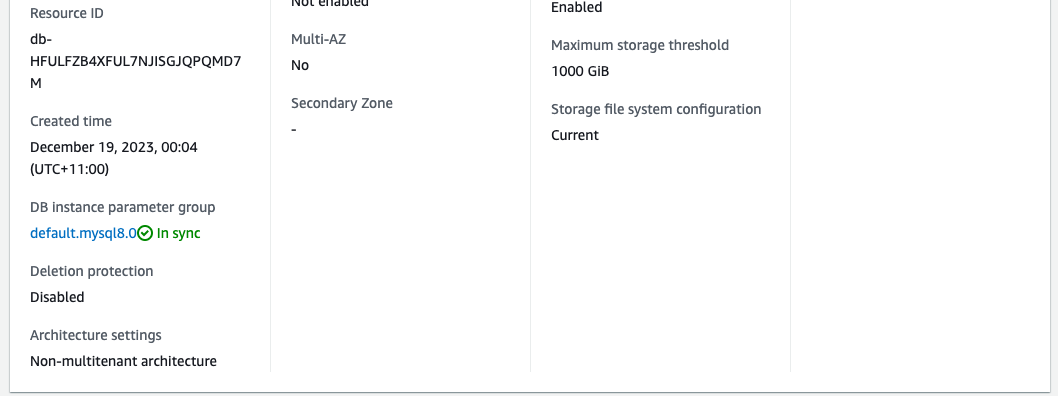
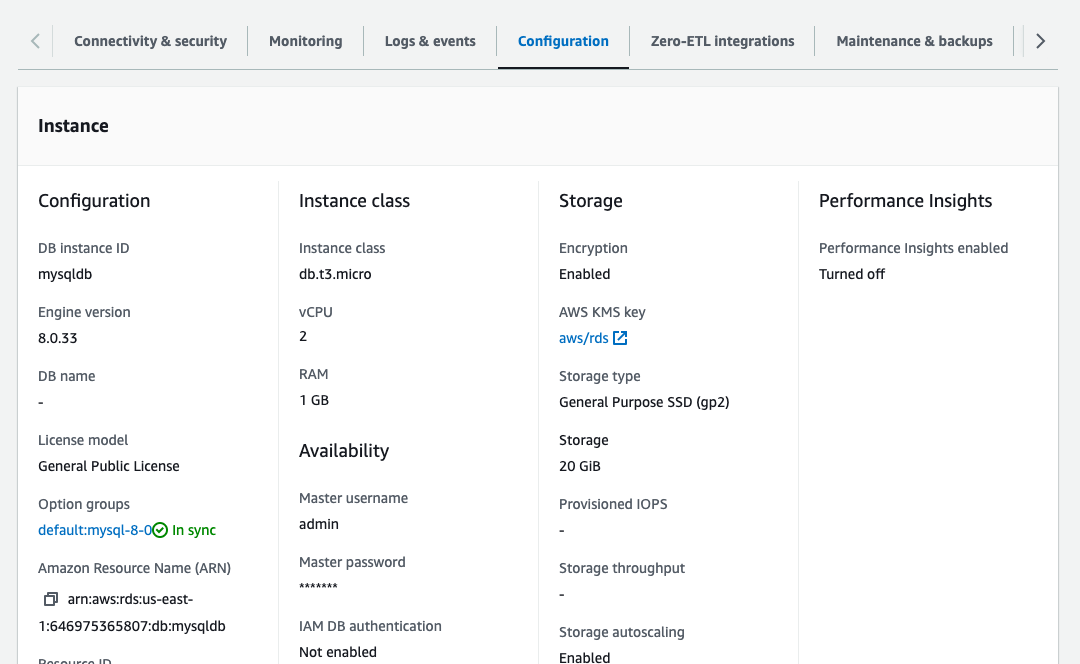
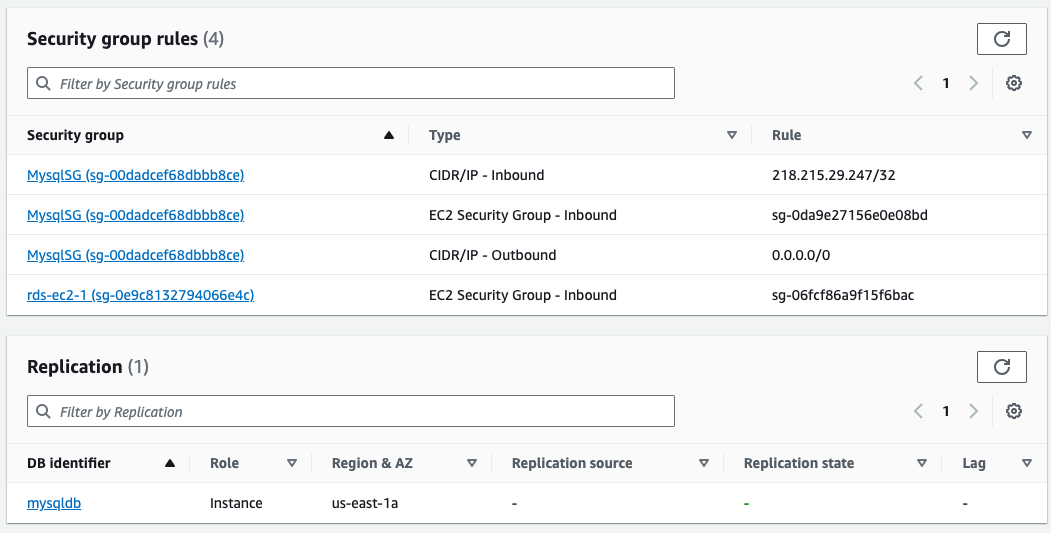
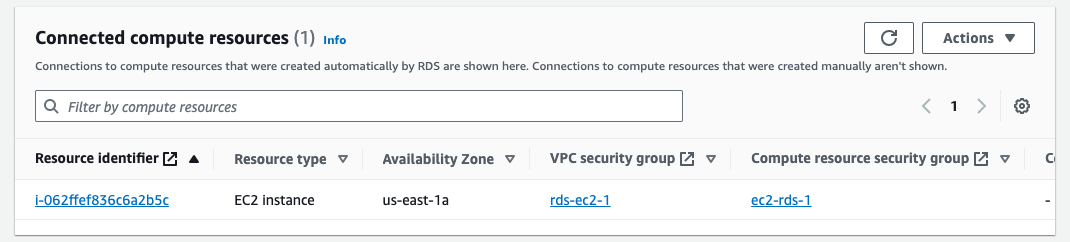
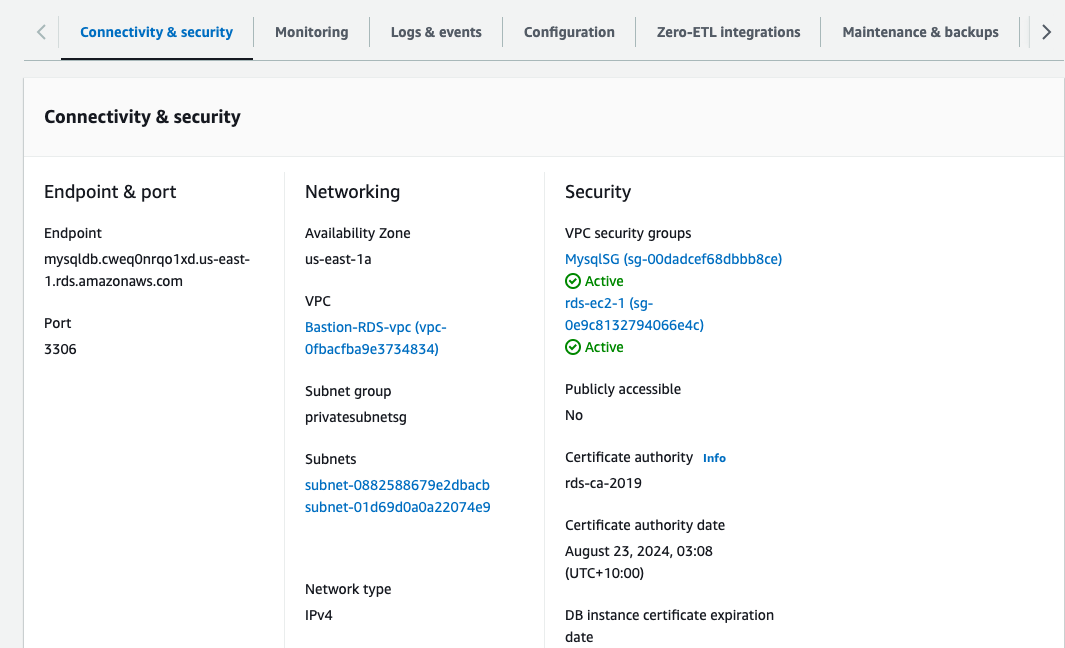
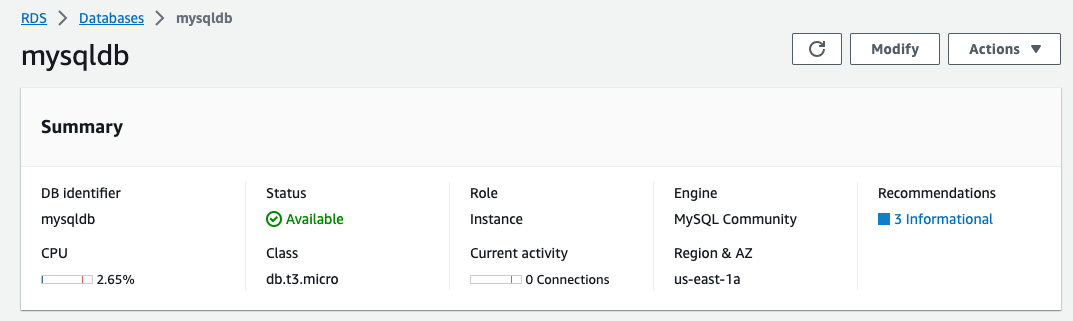
We need to create a new Security Group for RDS DB instance “MysqlSG”:





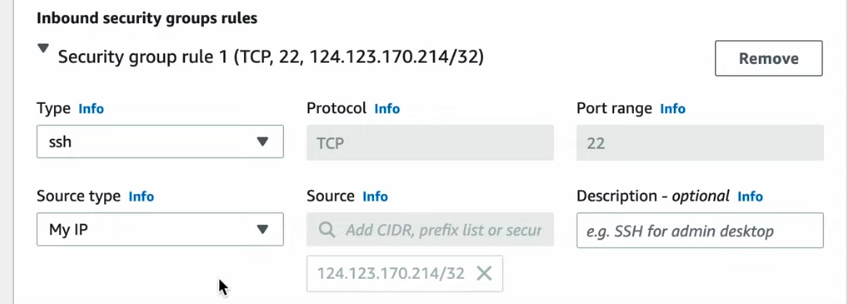
**Followed by the resultant RDS instance: -**



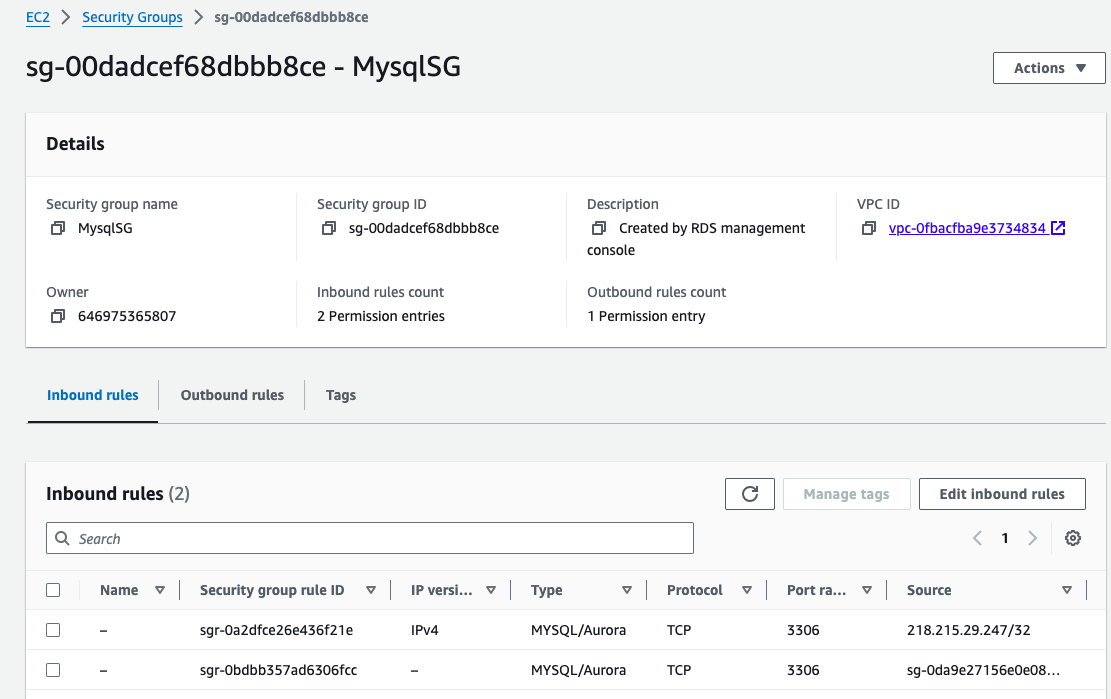


So, we cannot get connected to this DB from our local network, however we have to use the SSH connection to connect to this RDS database via our Bastion EC2 instance that we created before.

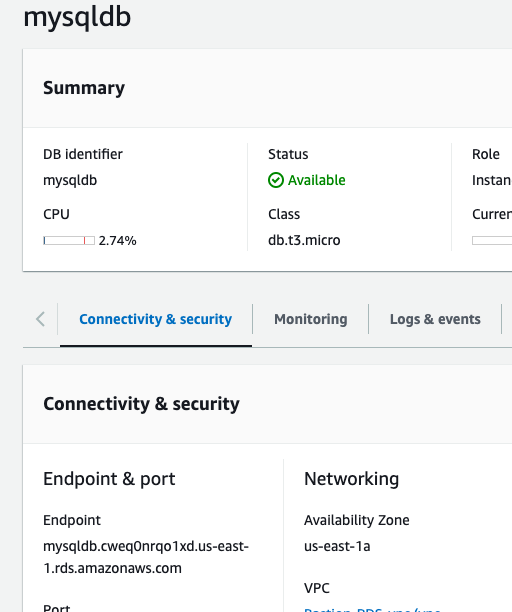
This Bastion EC2 instance is to use as an intermediate SSH connectivity. Check below the inbound security group rules for Bastion-RDS instance.



Below is the RDS database instance’s security group inbound rules:

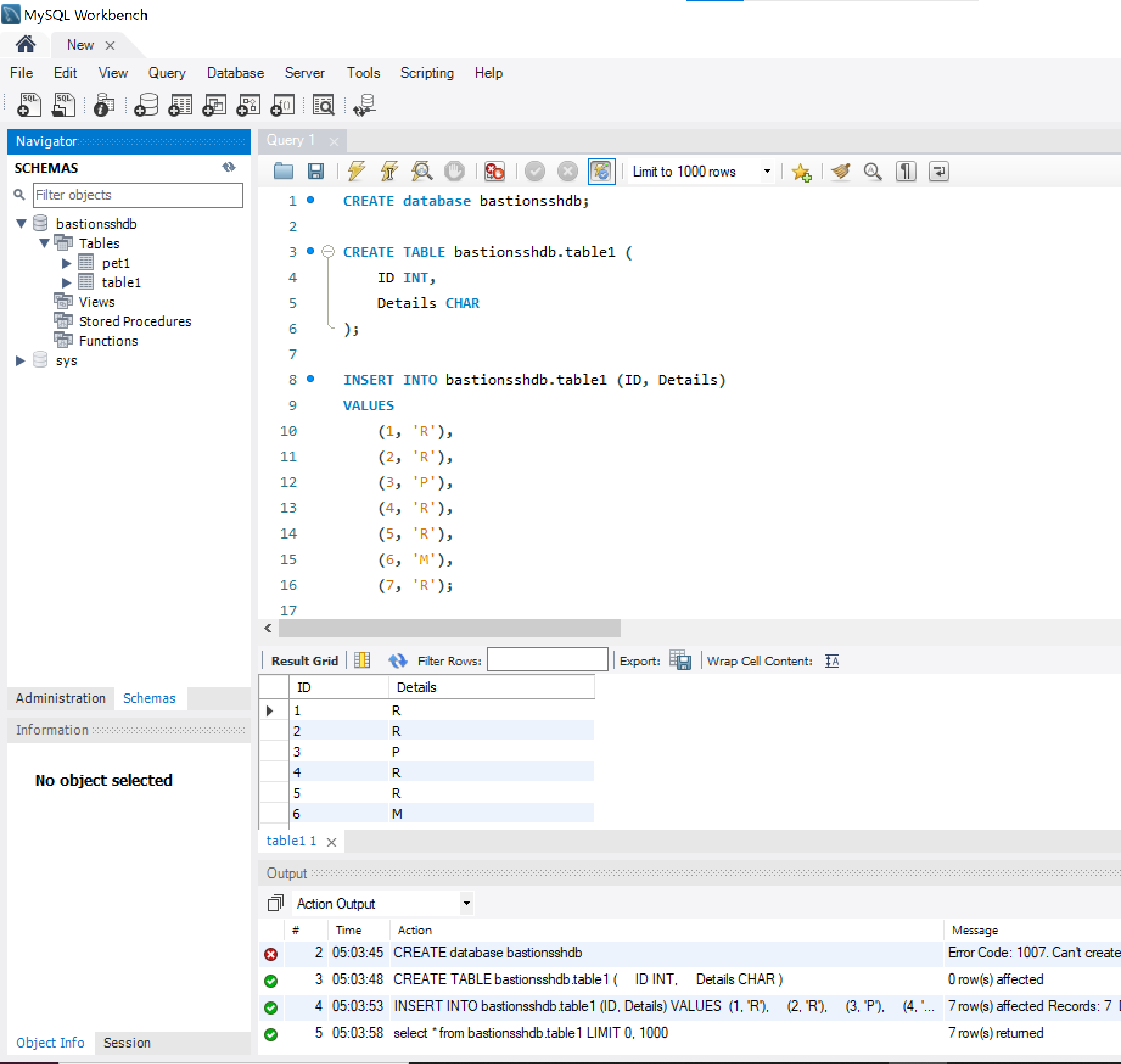
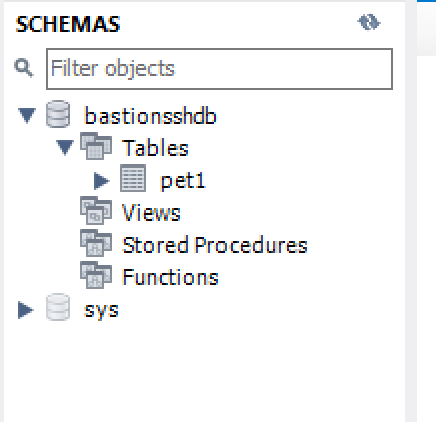
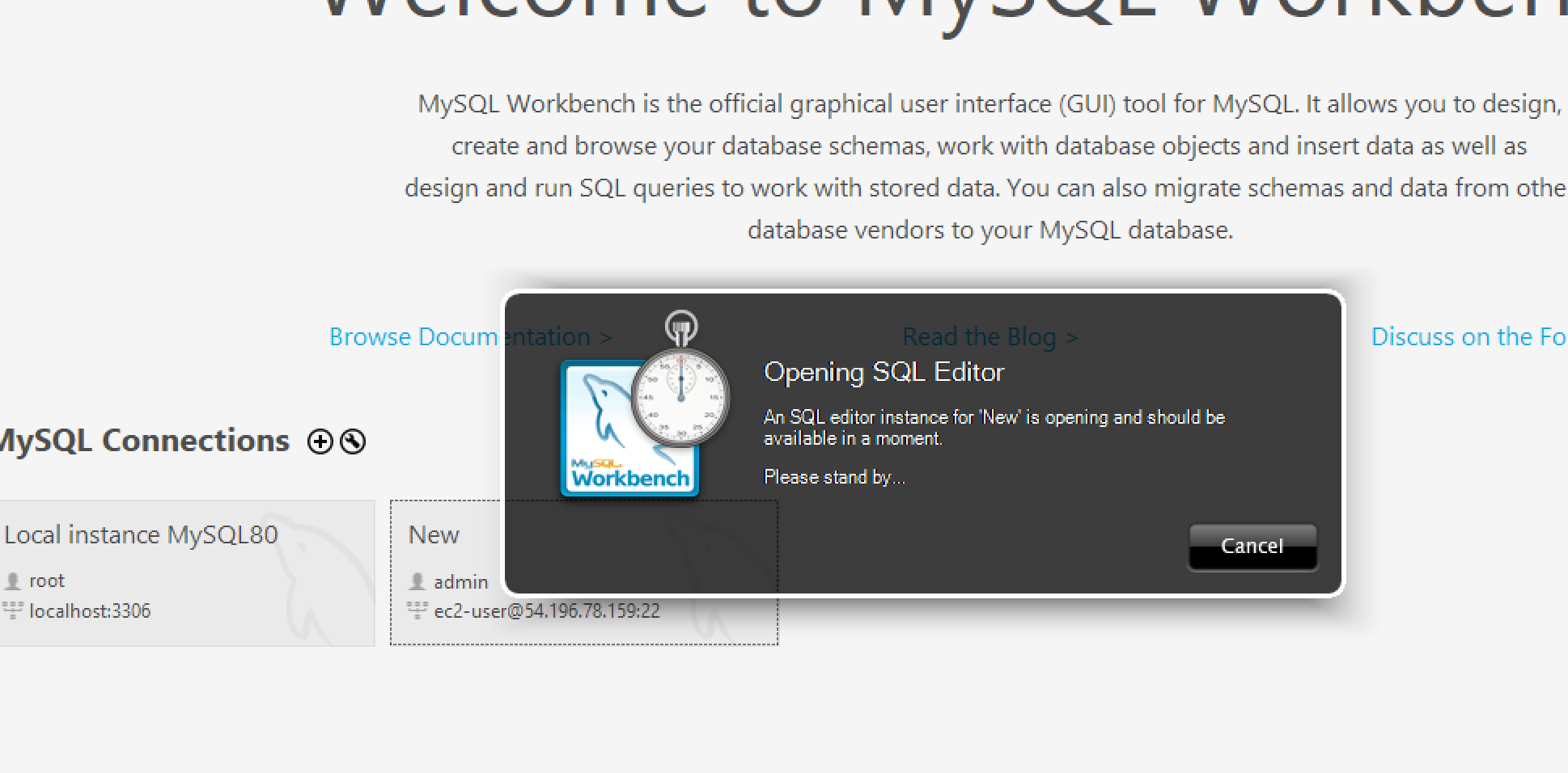
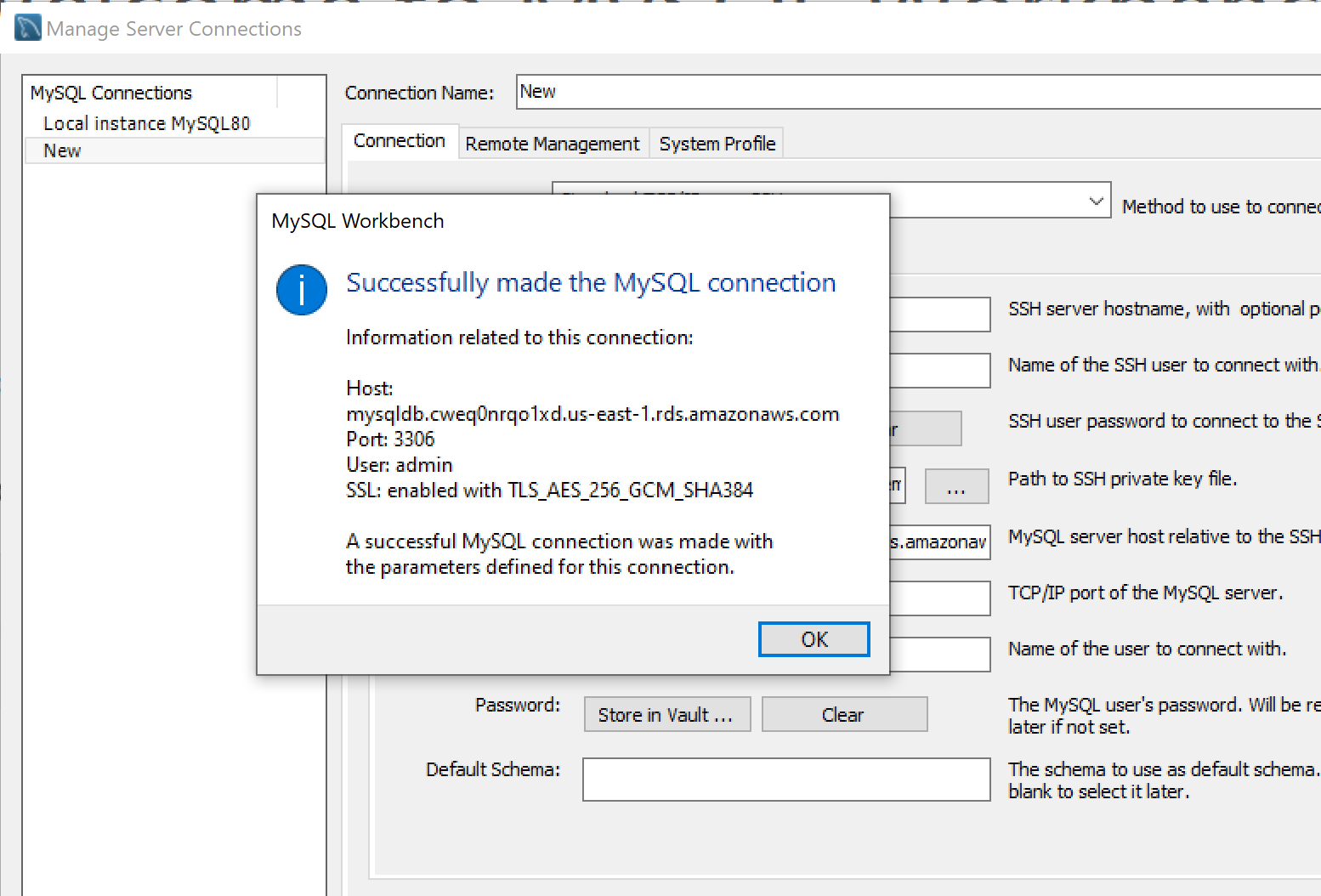
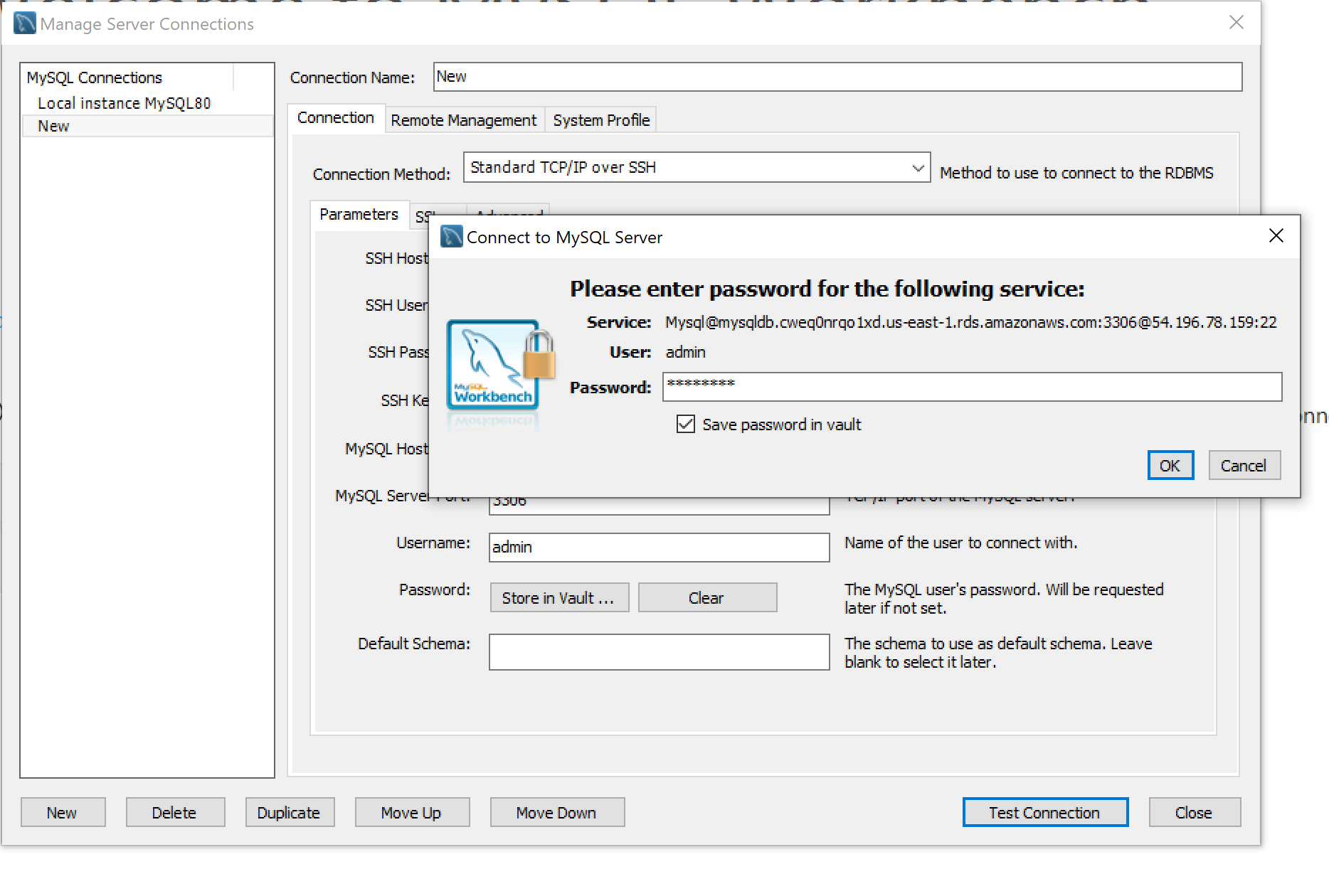
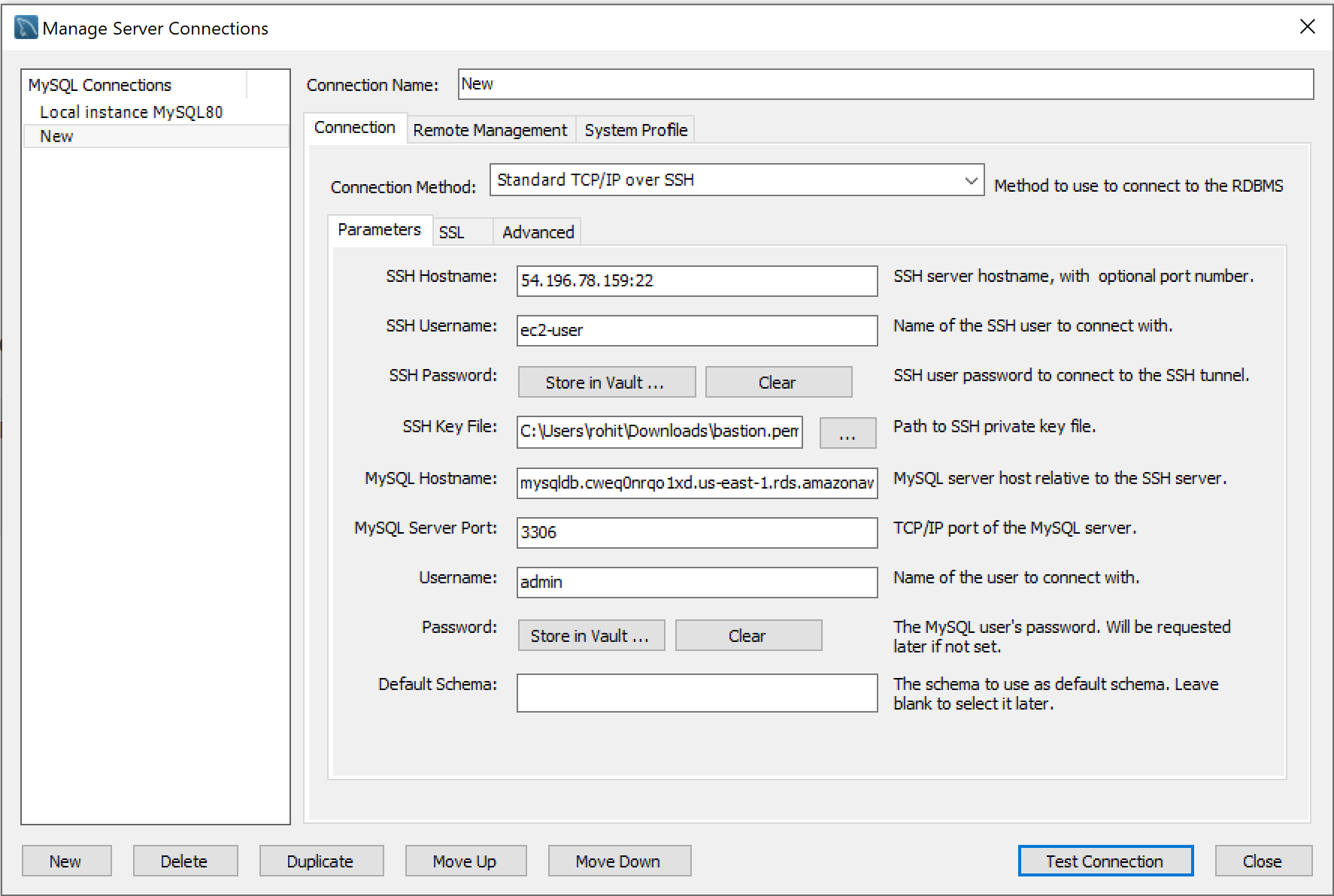
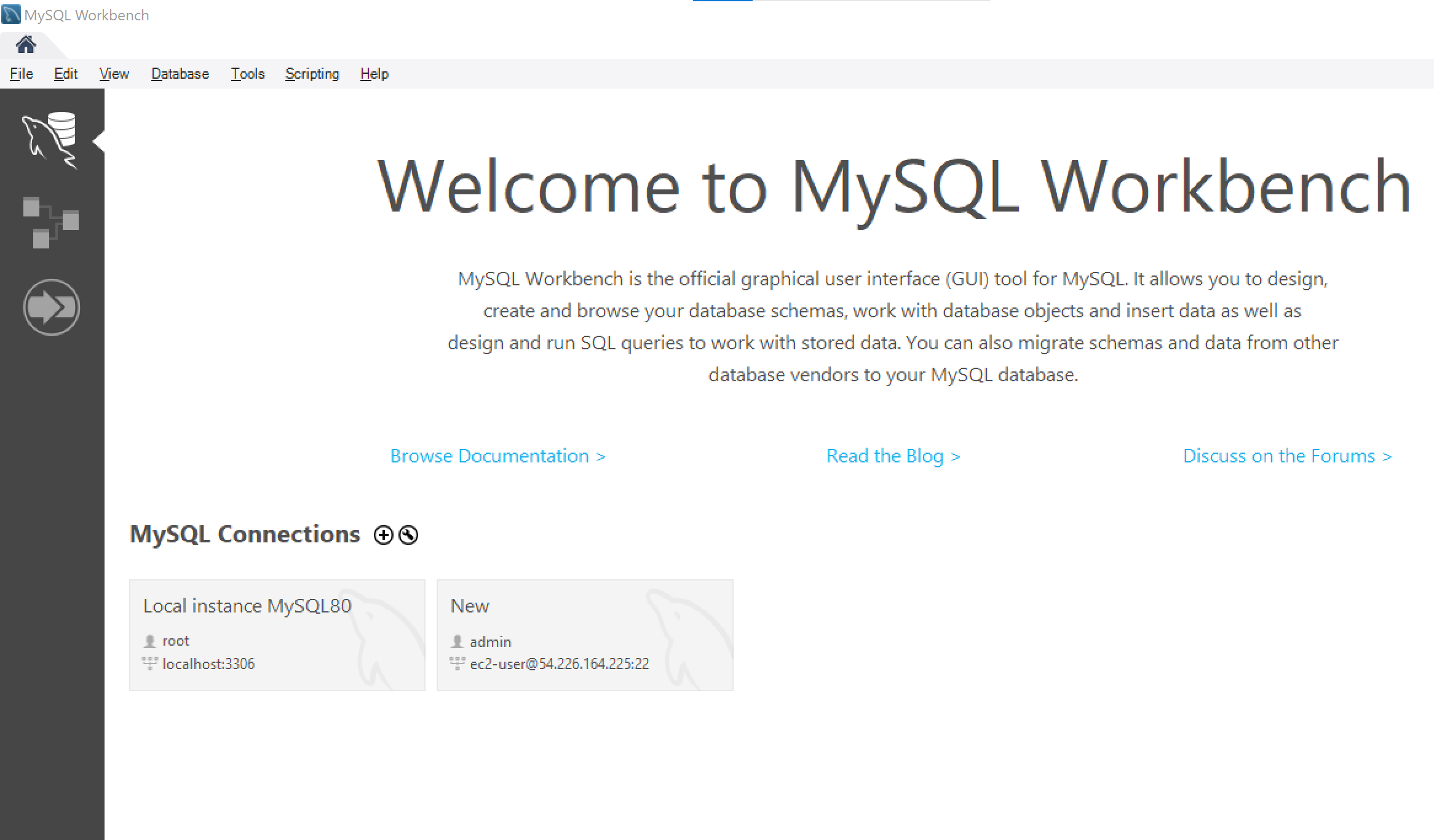


Finally, the DB instance creation is completed, besides for the RDS we are going to get an endpoint not IP address to get connected with the RDS DB instance directly from the local network.



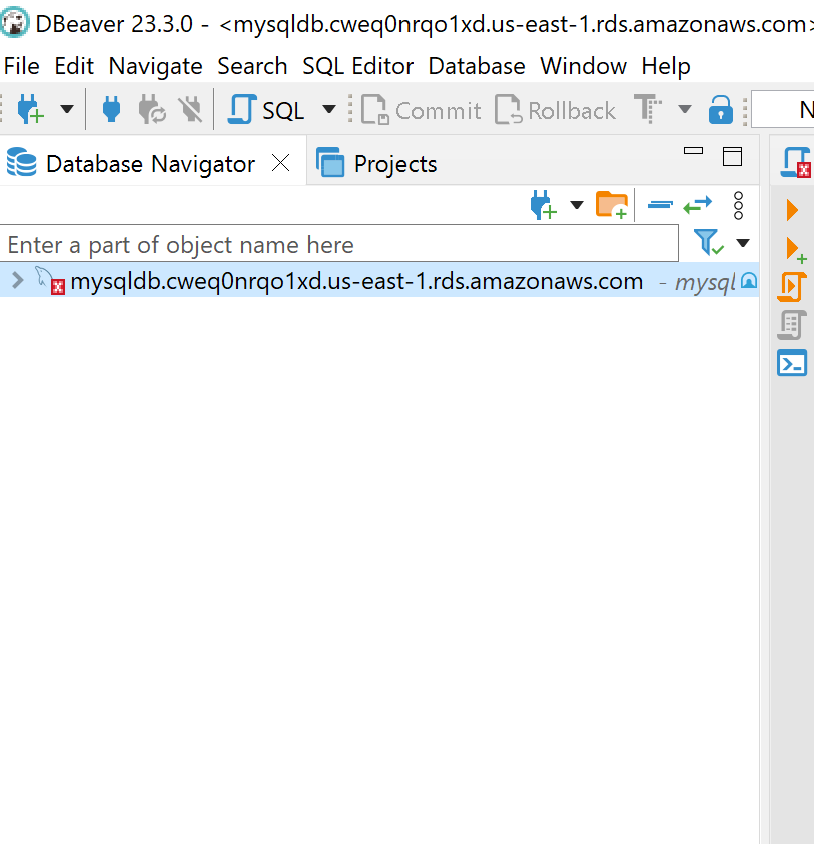
**How to connect to the Custom VPC’s Private subnet database from our local system with SSH connection via MySQL Workbench/ DBeaver**

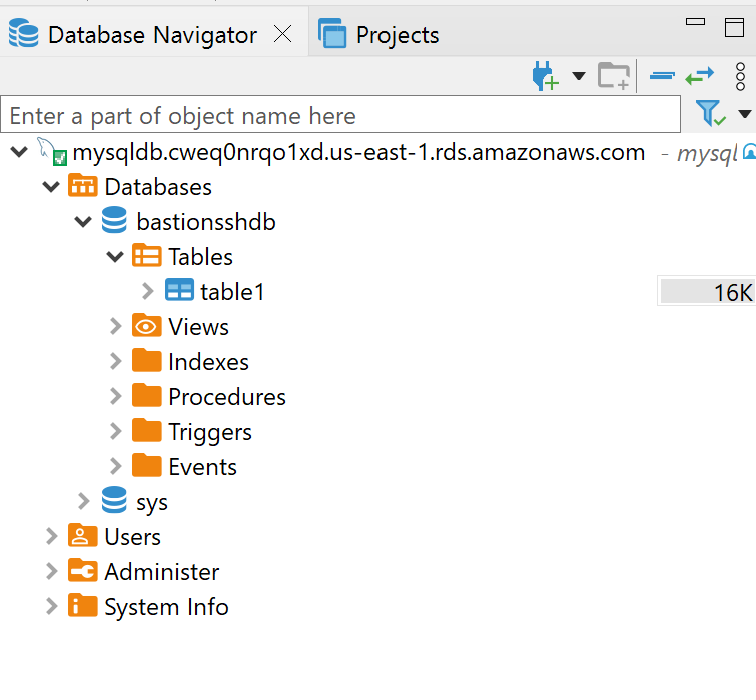
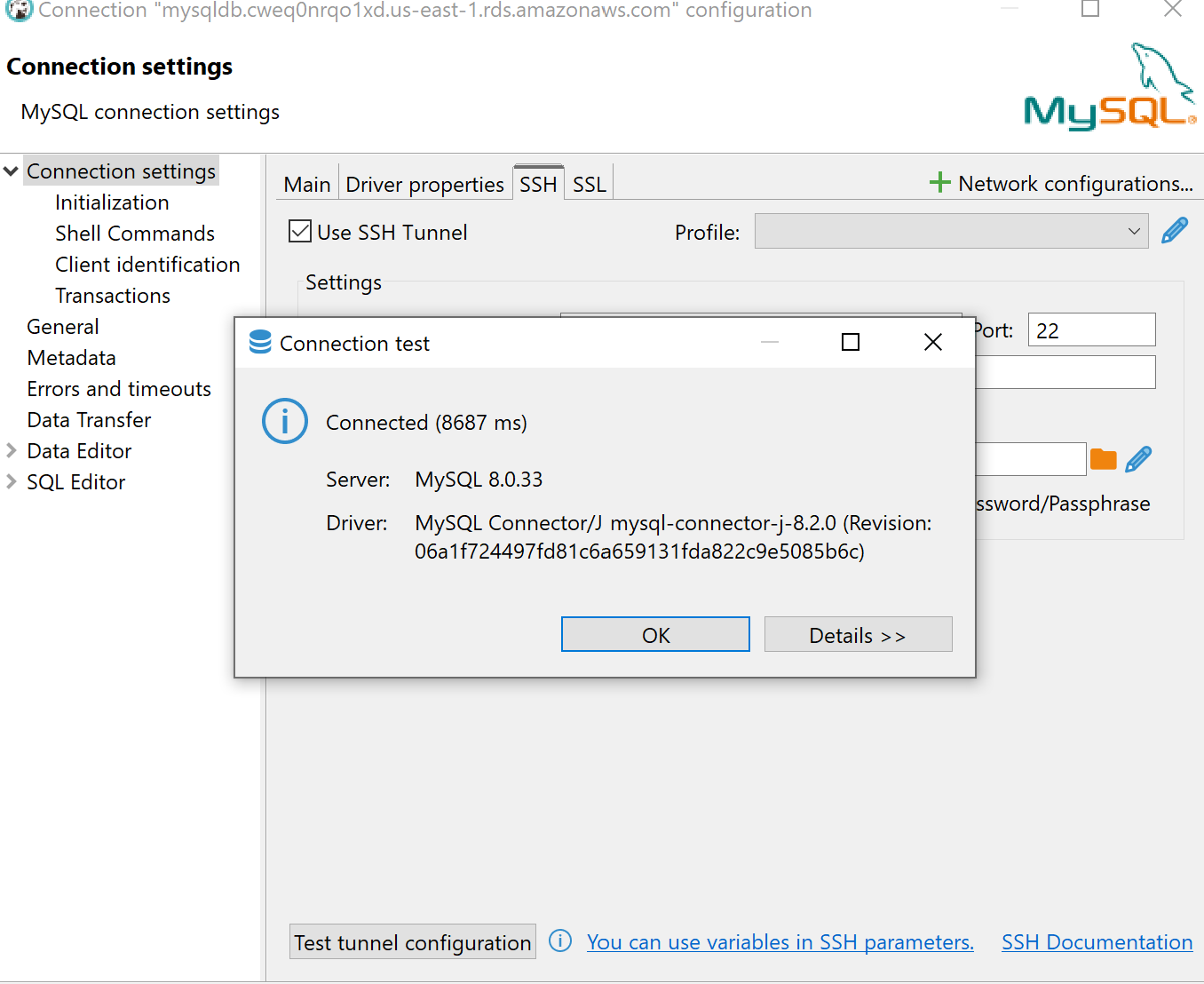
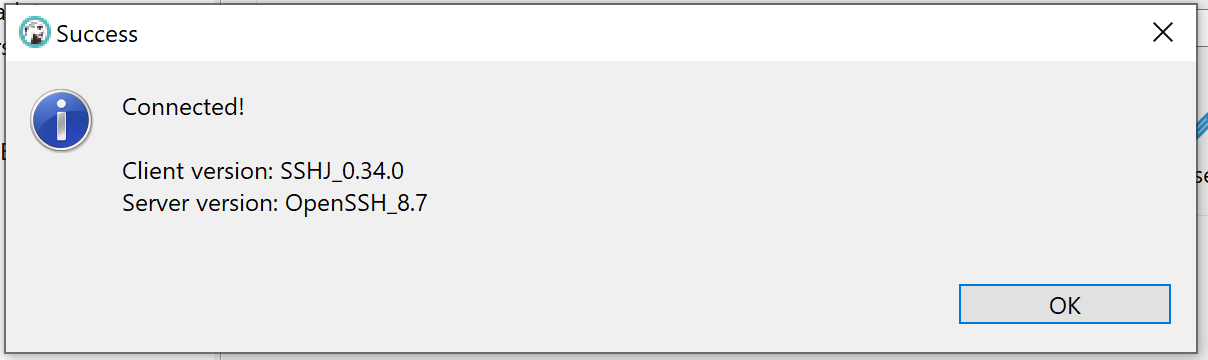
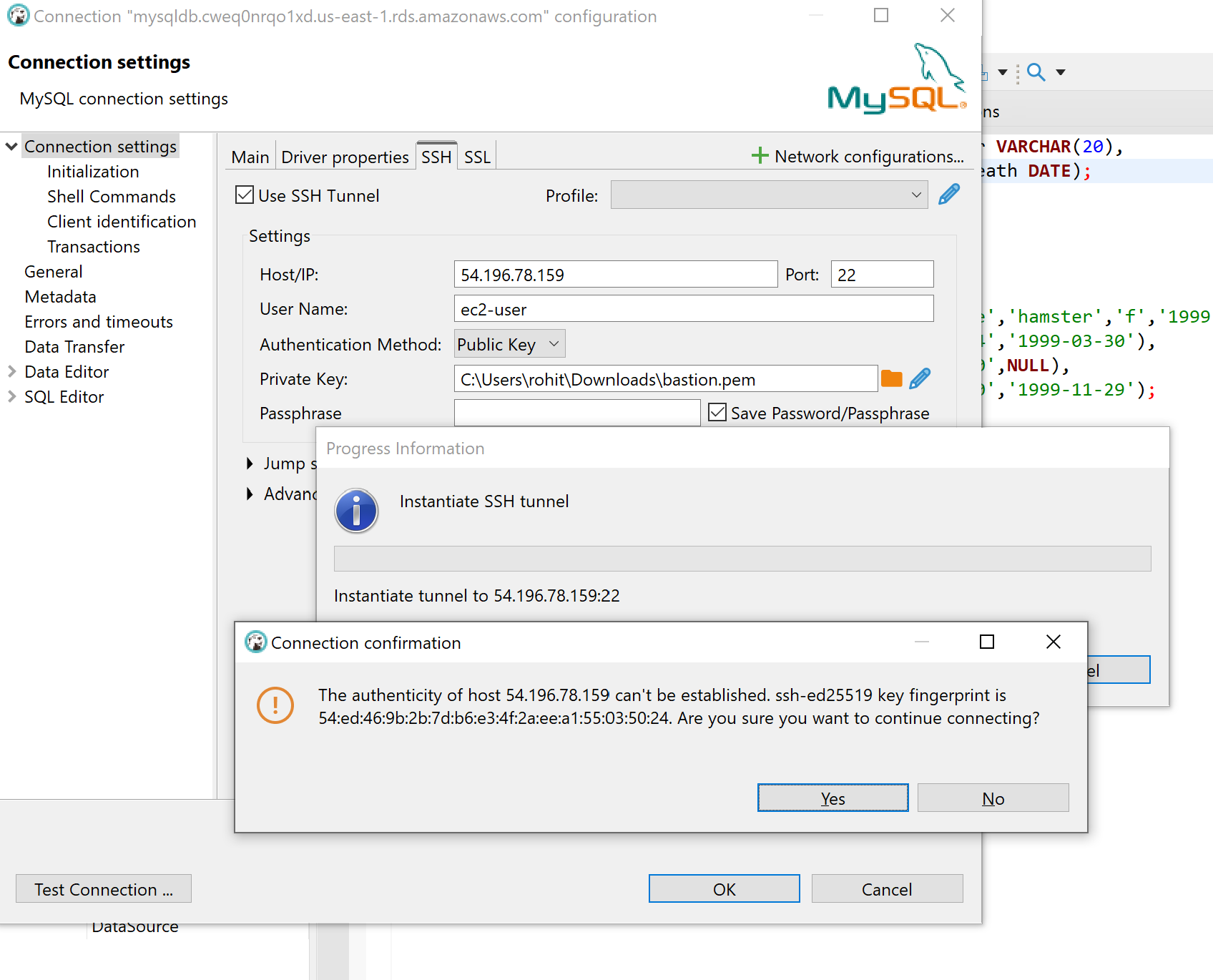
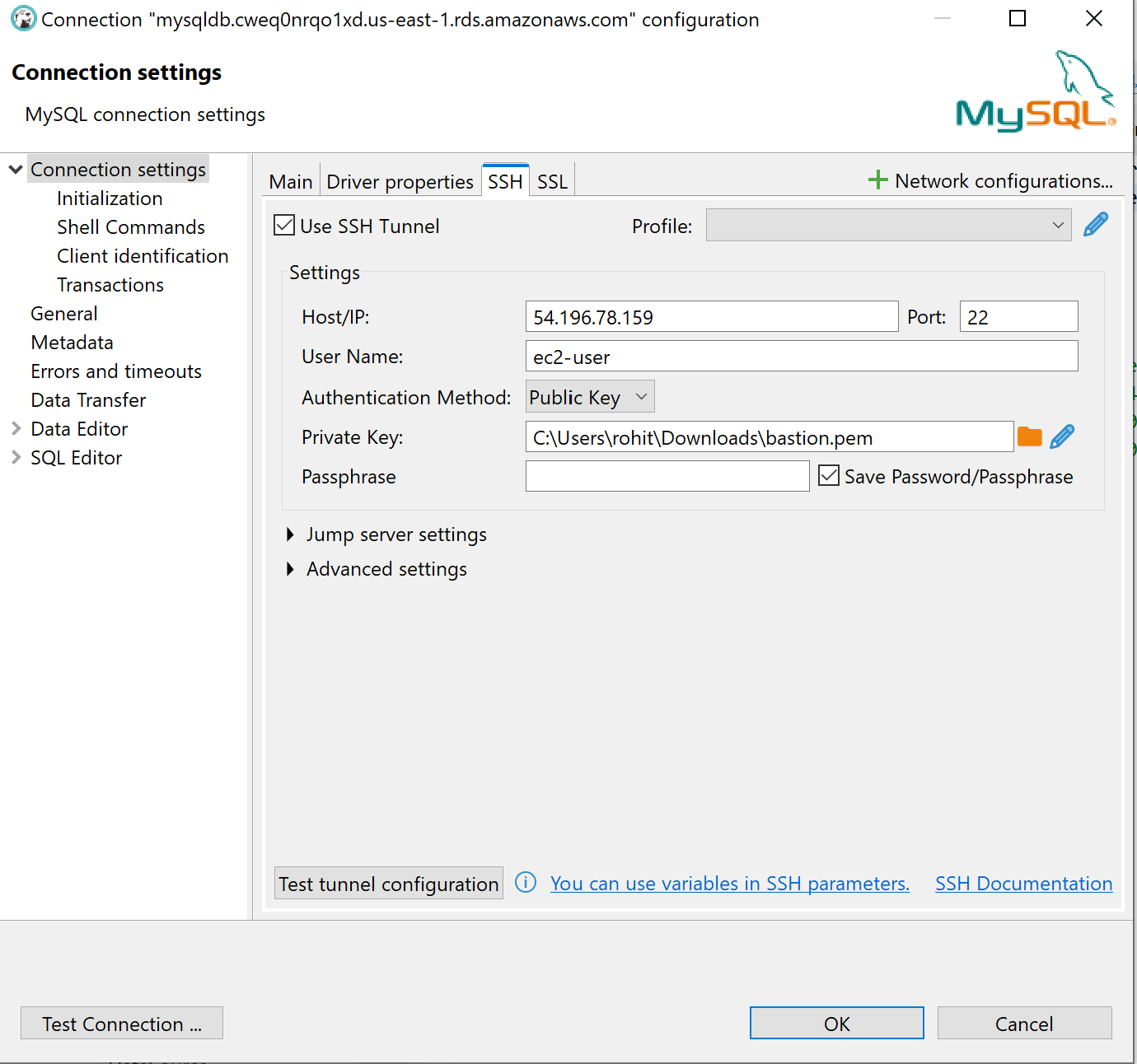
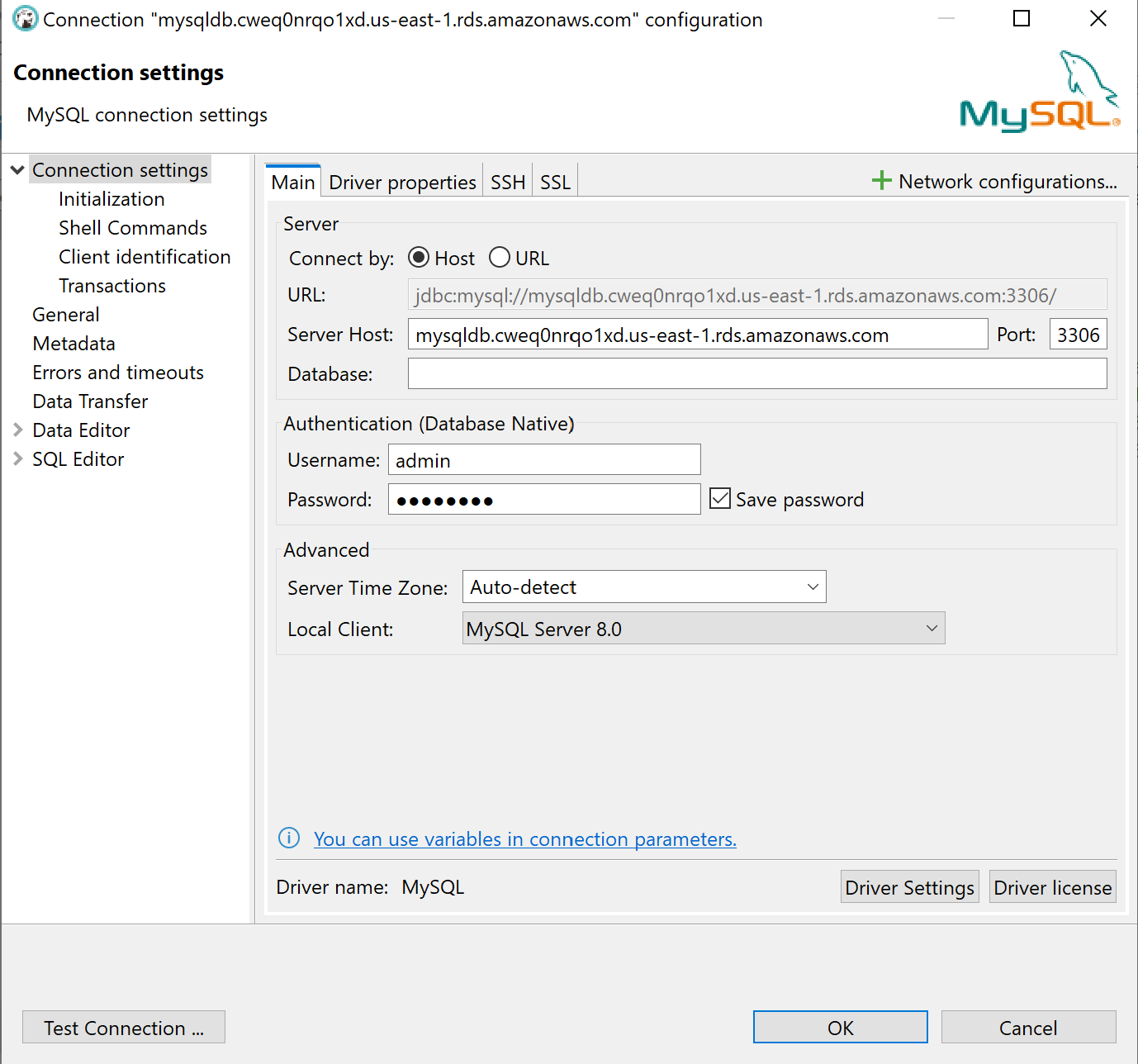
1. **SSH connection via MySQL Workbench**

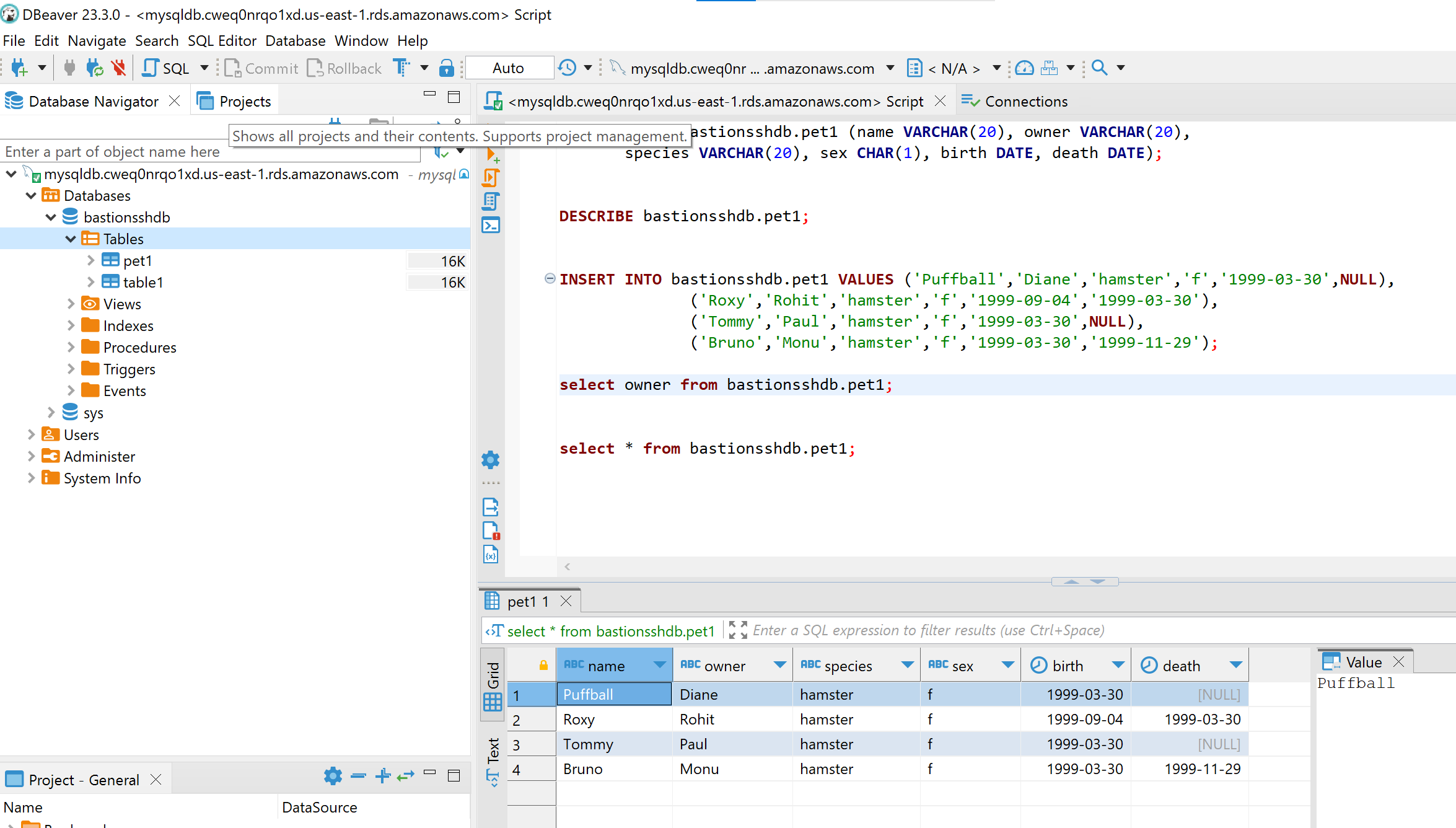
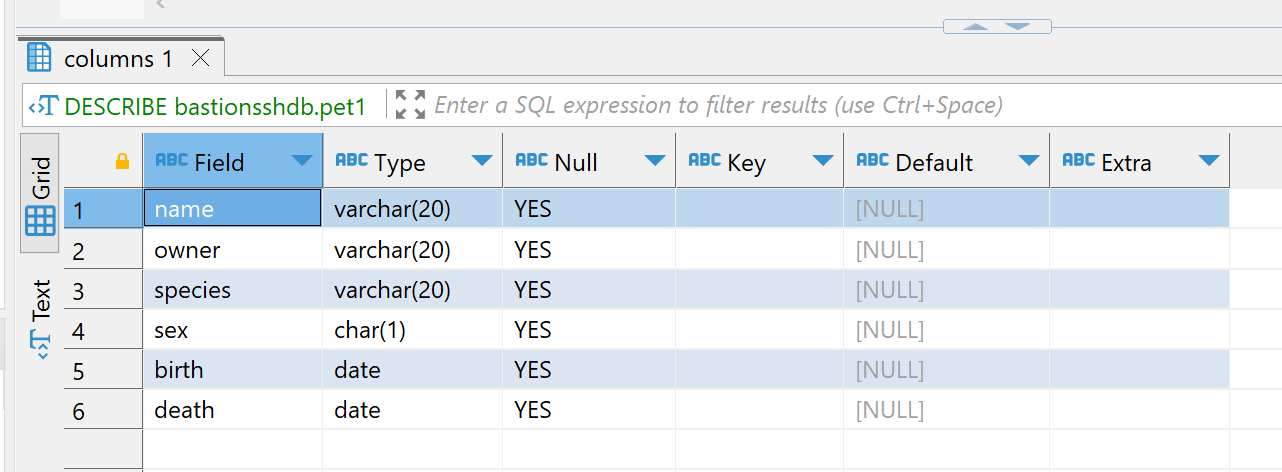


[**Troubleshoot**: In case you unable to establish the **SSH connection** from the **Bastion Host** to the **RDS MySQL DB** instance then go for following check:

1. Check the Inbound Security Group rules of both **Bastion Host** and **RDS DB** instance
2. Check the current **My IP** of **Bastion host** which can keep changing whenever you change the **Internet/WiFi source**.]
3. SSH connection via DBeaver







References

* <https://www.youtube.com/watch?v=CpW85hqLIRc>
* <https://www.youtube.com/watch?v=qulcnNu8g7o>