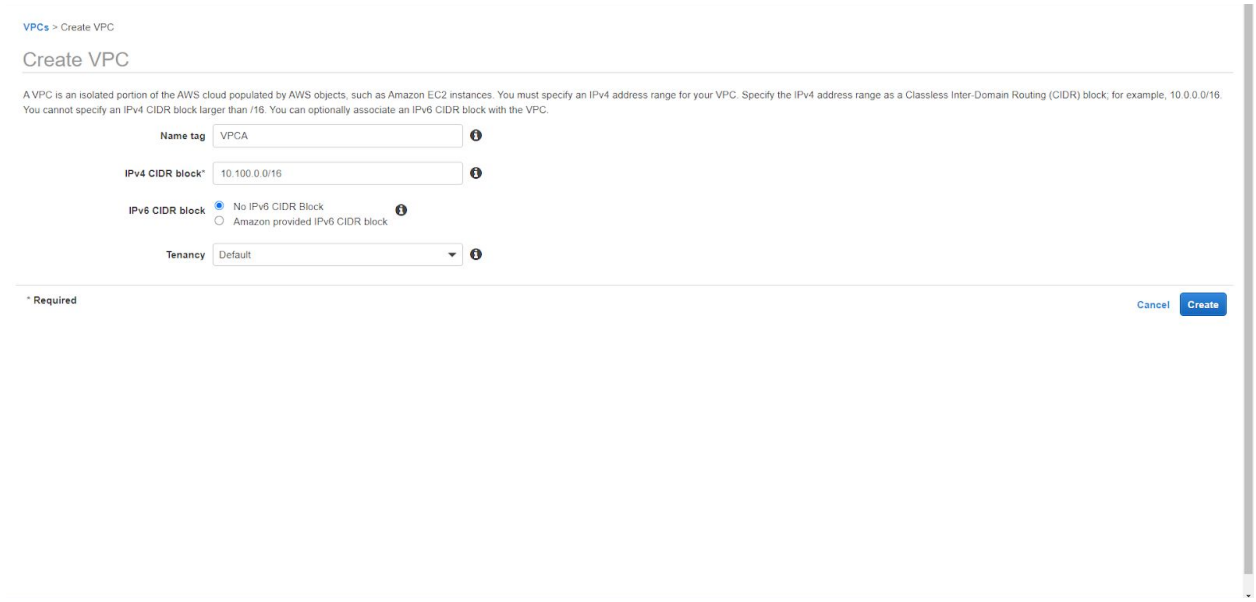
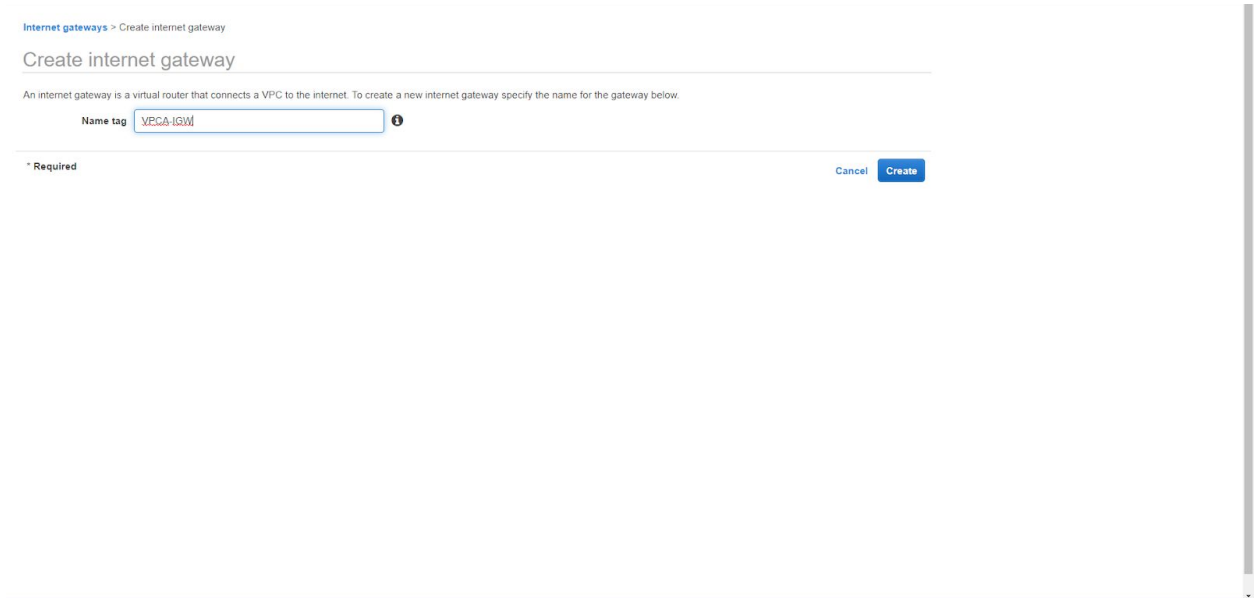
# Module 7 Lab 3: VPC Peering

## VPCs - Create VPC



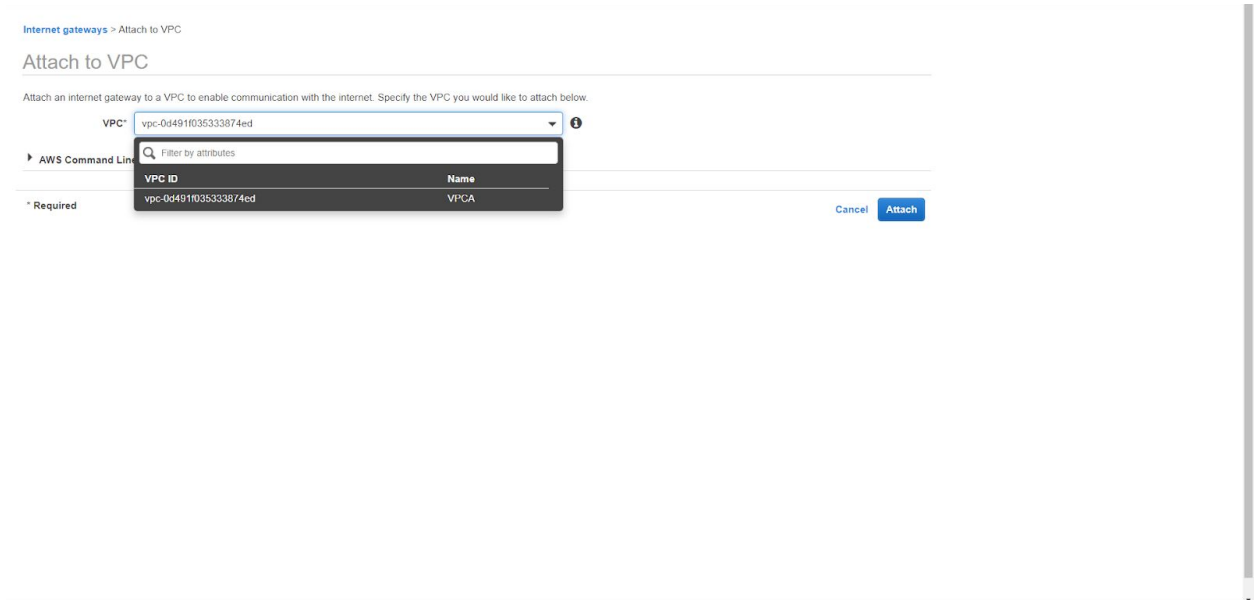

Two VPC's will be created, this is the first one.

## Internet gateways - Create internet gateway



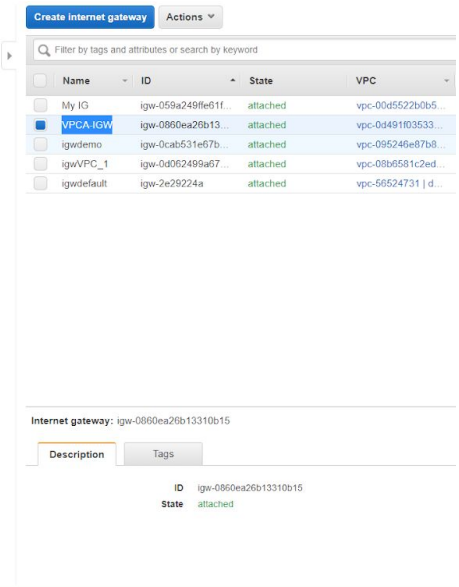

An IG will allow VPCA to access the Internet and public subnets.

Internet gateways - Attach to VPC



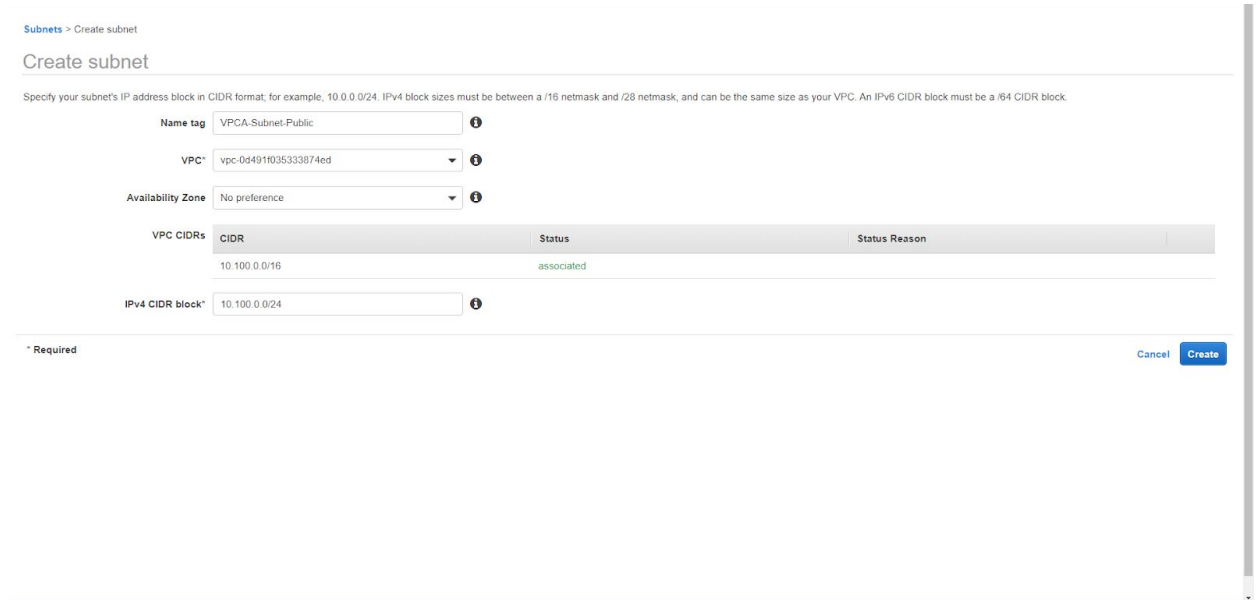

Only one IG at a time can be attached to a VPC, thus only the new VPCA is shown.

Internet Gateways Dashboard



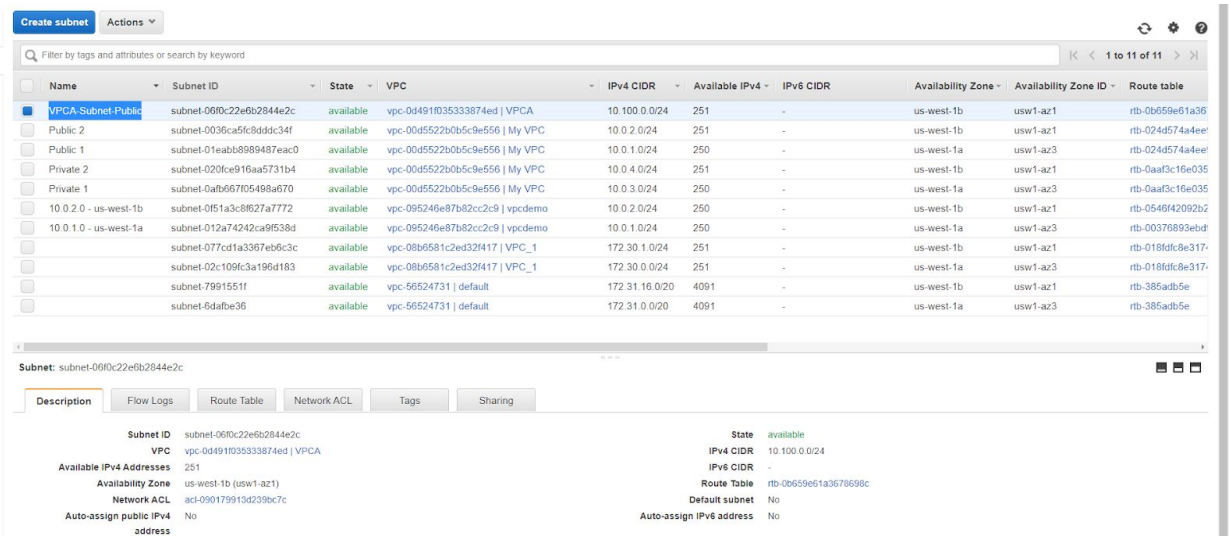

VPCA-IGW has been attached to VPCA.

## Subnets - Create subnet



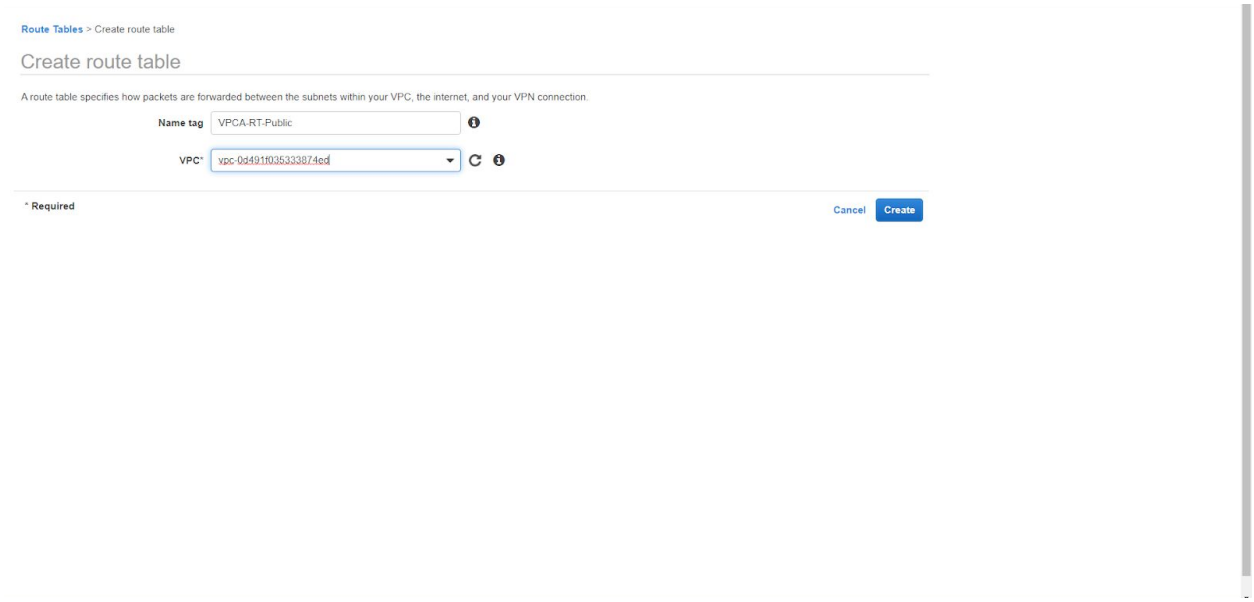

A public subnet for VPCA is created.

## VPC - Subnets



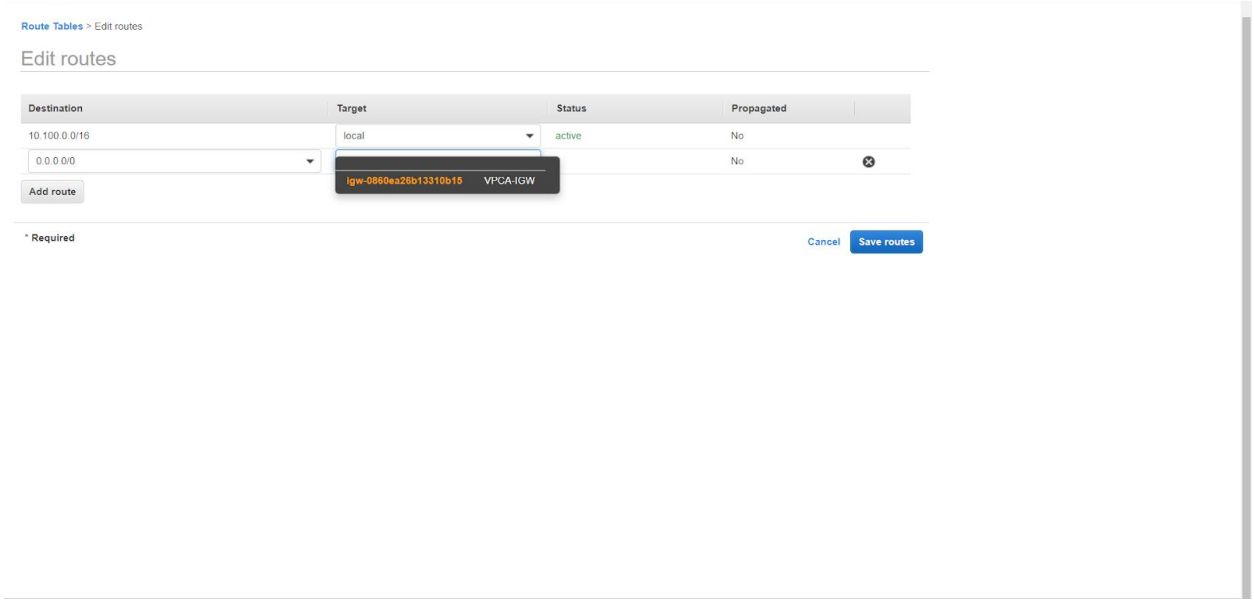

VPCA public subnet is created.

Route Tables - Create route table



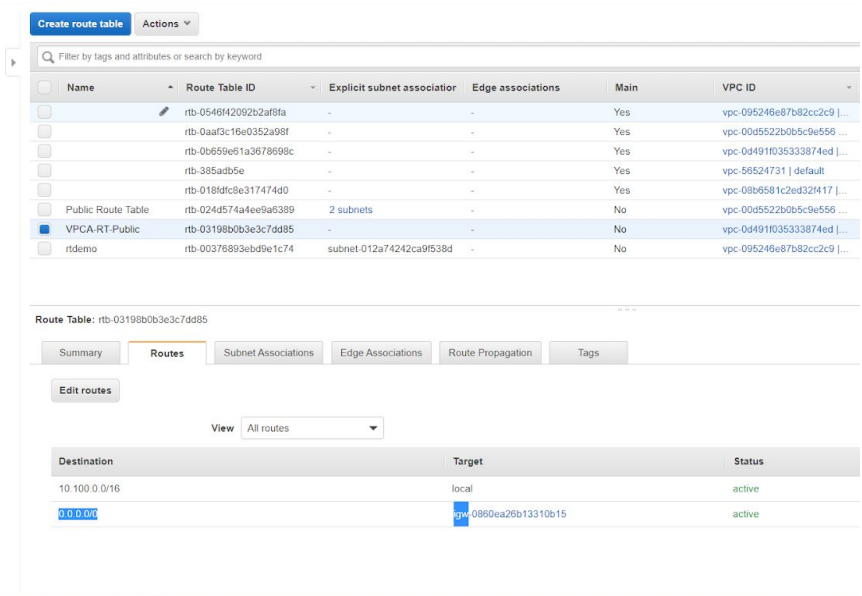

A route table is created for VPCA.

Route Tables - Edit routes



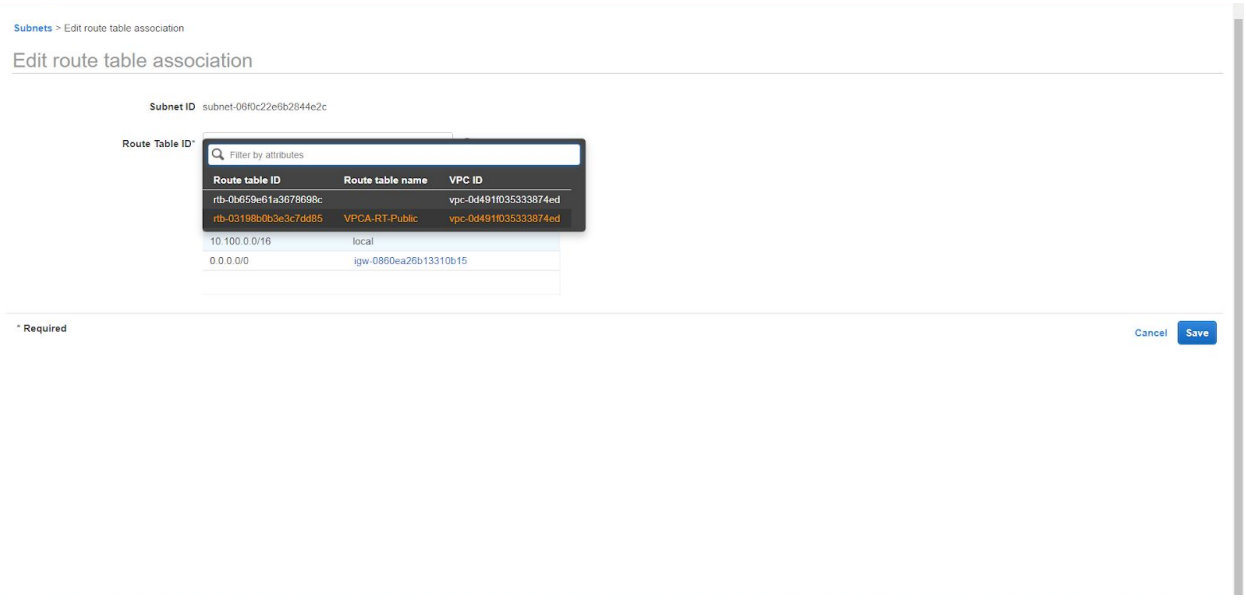

At this point, only internal traffic can be routed. Editing routes can allow external traffic.In essence, all traffic not on 10.100.0.0/16 will be allowed through the IG. Non-local traffic can be sent out into the Internet.

VPC - Route table



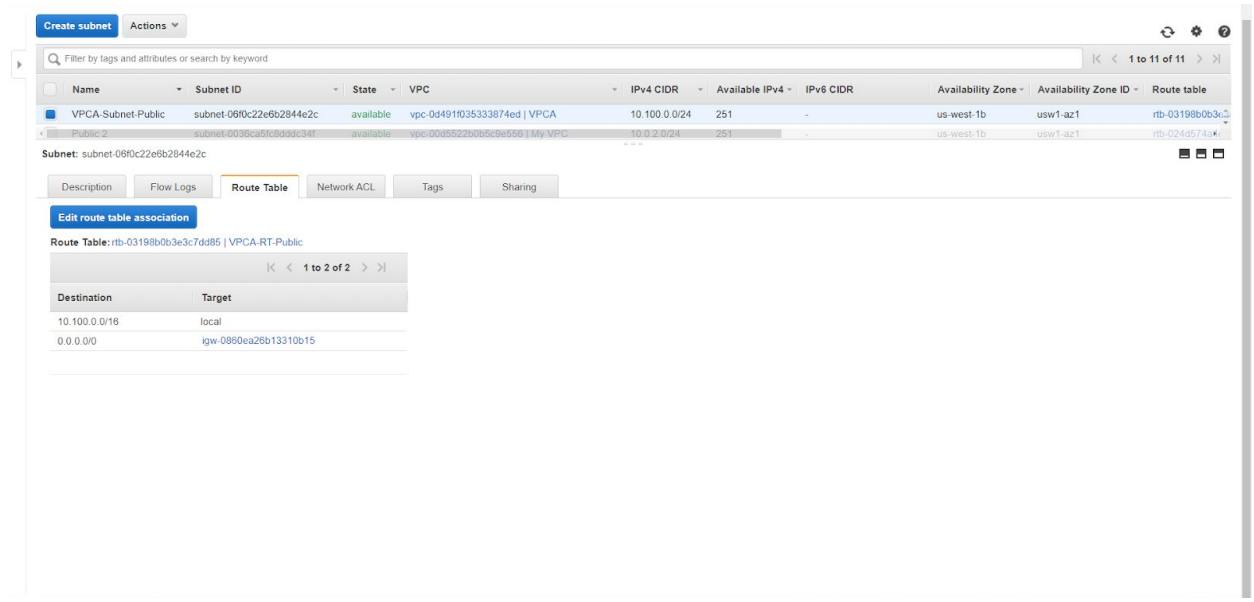

The public route table has been updated.

Subnets - Edit route table association



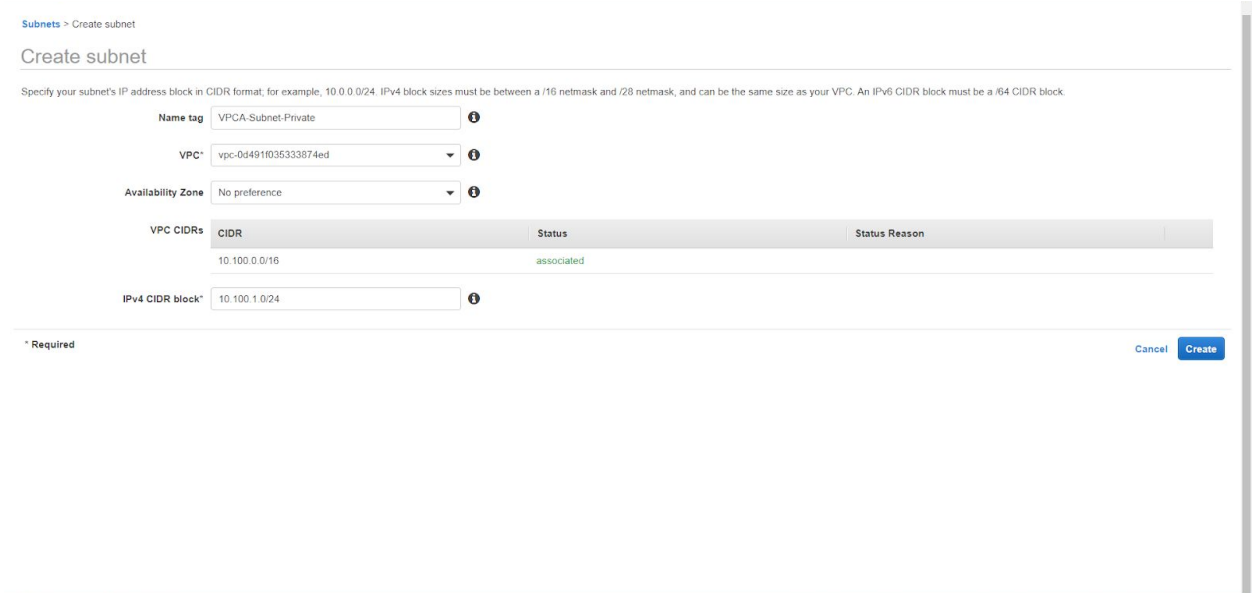

The subnet VPCA needs to be associated with the route table just created.

## VPC - Subnets



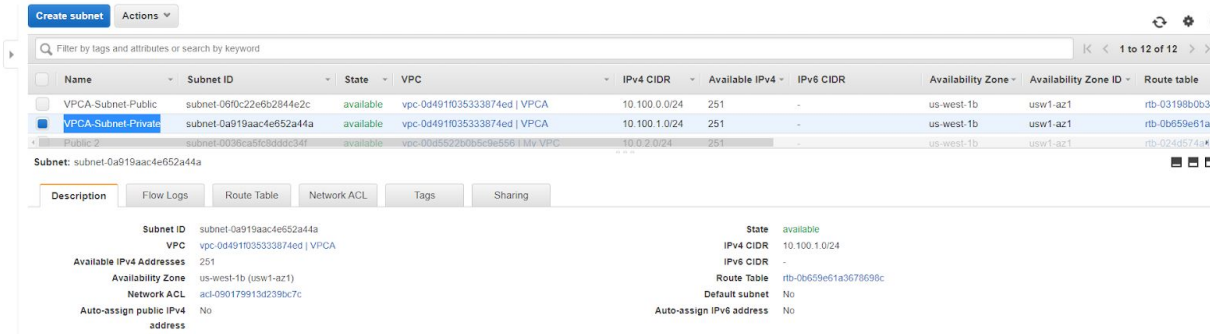

Correct routing table information.

## Subnets - Create subnet



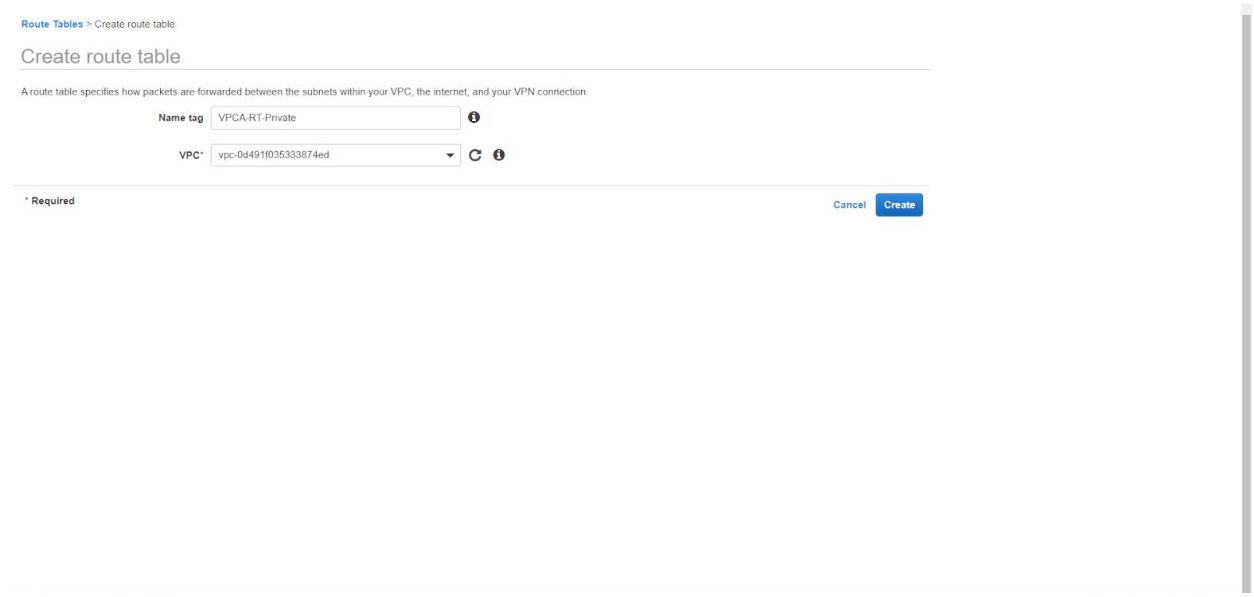

A private subnet will be created.

VPC - Subnets



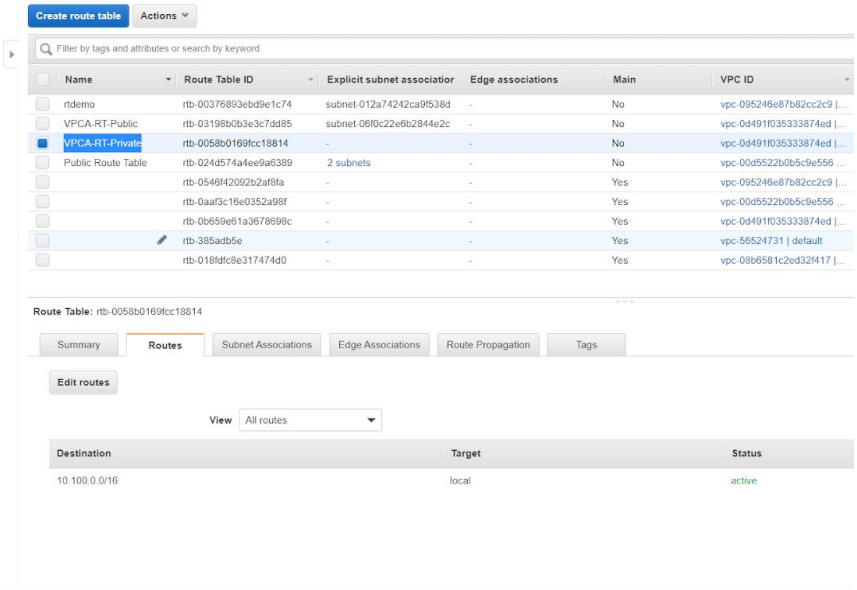

A private subnet is created.

Route Tables - Create route table



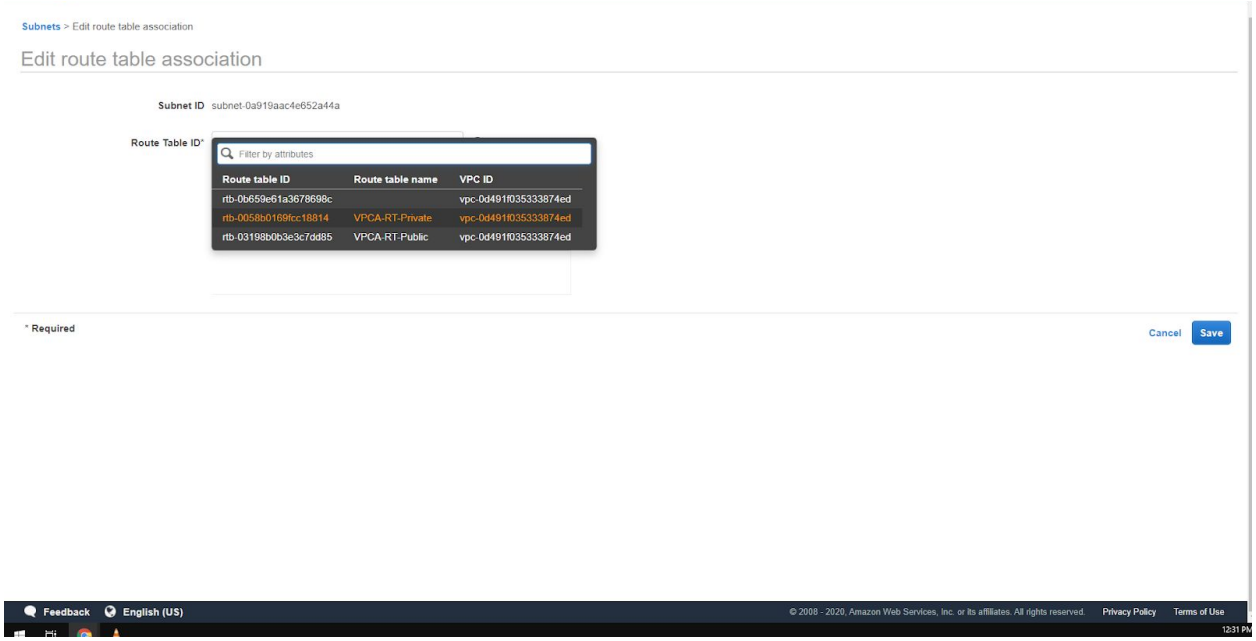

Any traffic that cannot be routed into the internal subnet will be lost.

VPC - Create route table



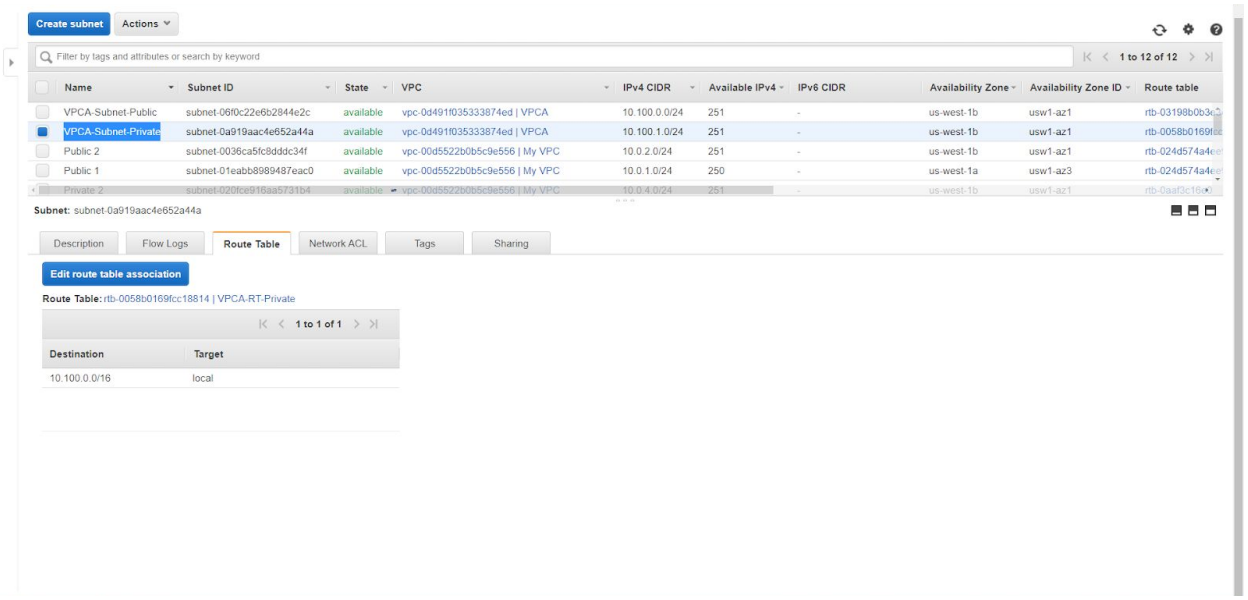

There is no need to allow traffic from 0.0.0.0/0 because this is a private subnet.

Subnets - Edit route table association



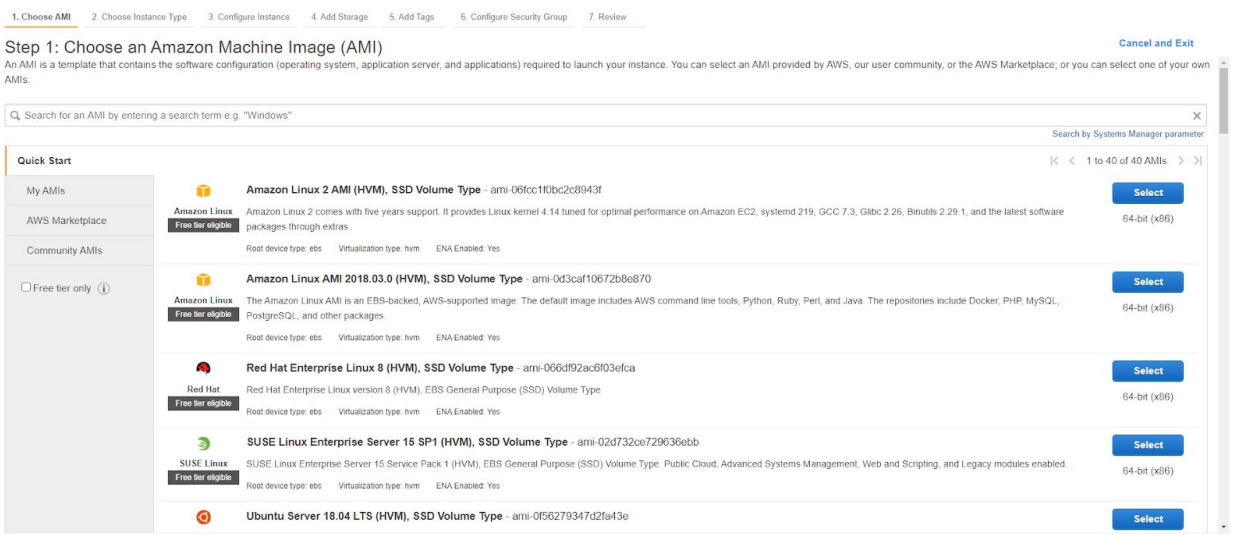

However, the routing tables still require to be associated with the correct private subnet.

## VPC - Subnets



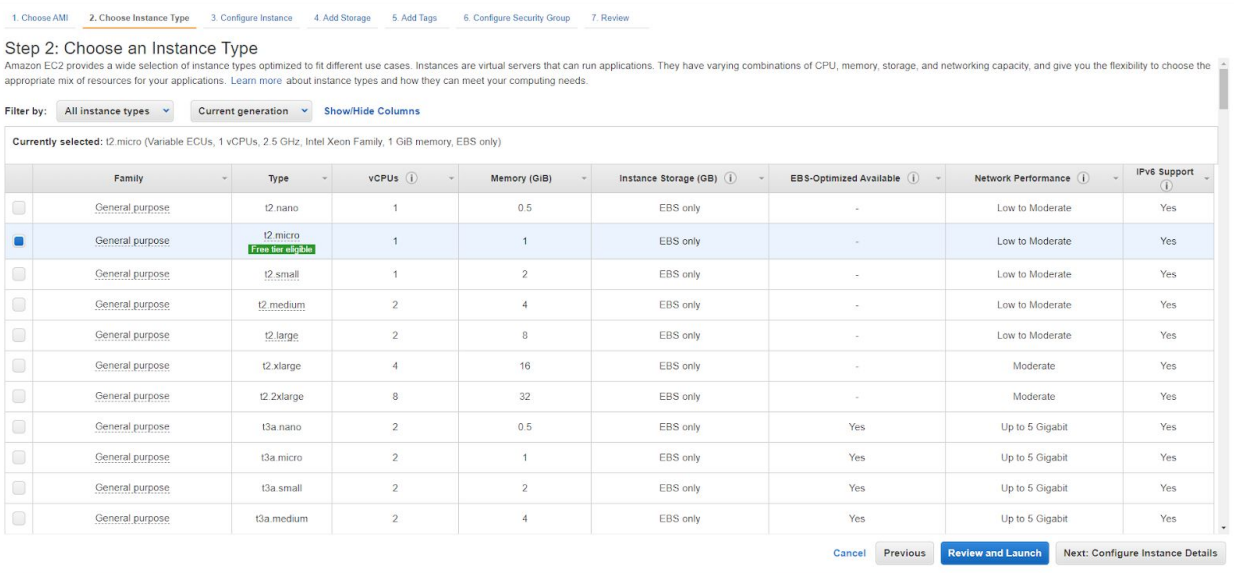

The VPCA private subnet is now associated with a route table that only allows internal traffic.

## EC2 - Choose AMI



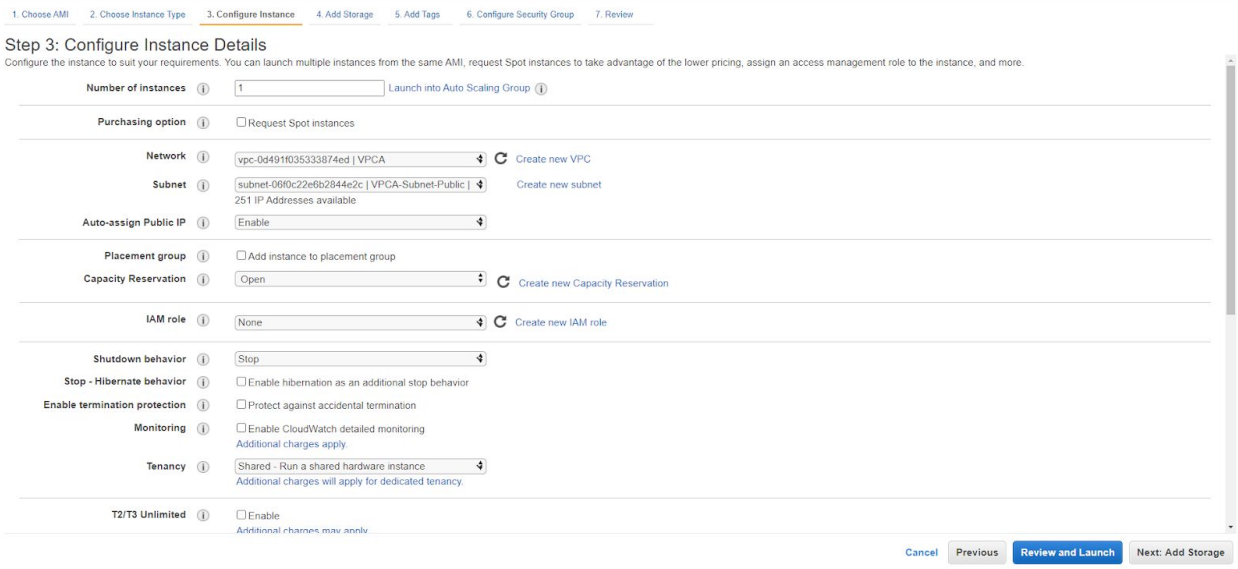

The first of two new EC2 instances will be set up. Amazon Linux 2 AMI selected.

## EC2 - Instance type



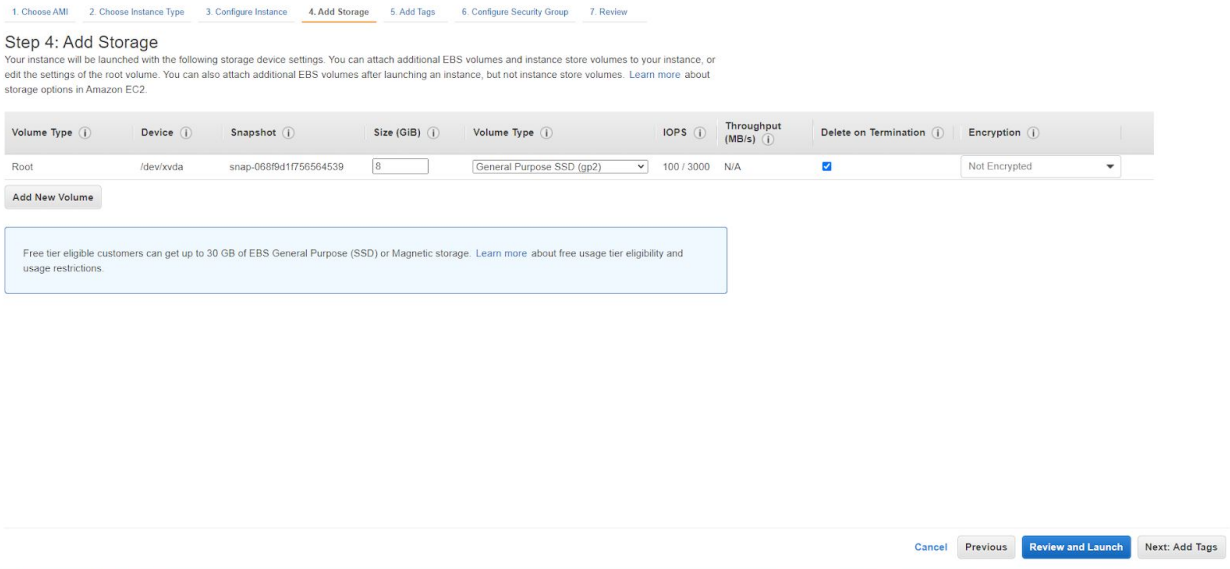

The free tier is selected.

## EC2 - Configure Instance



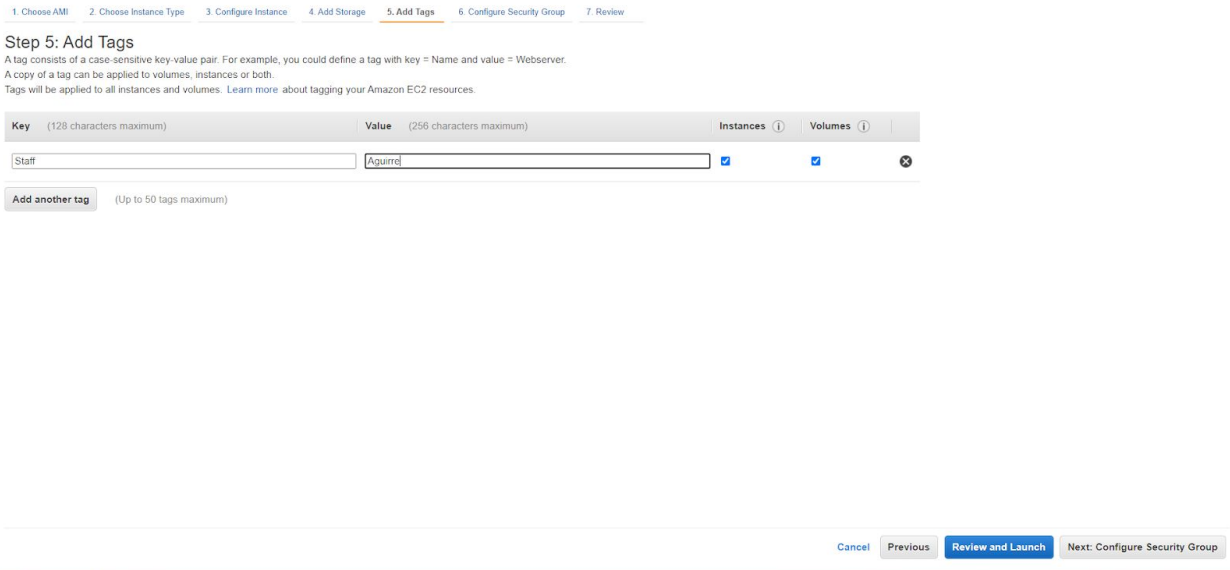

Note that an auto-assigned Public IP is enabled.

## EC2- Add Storage



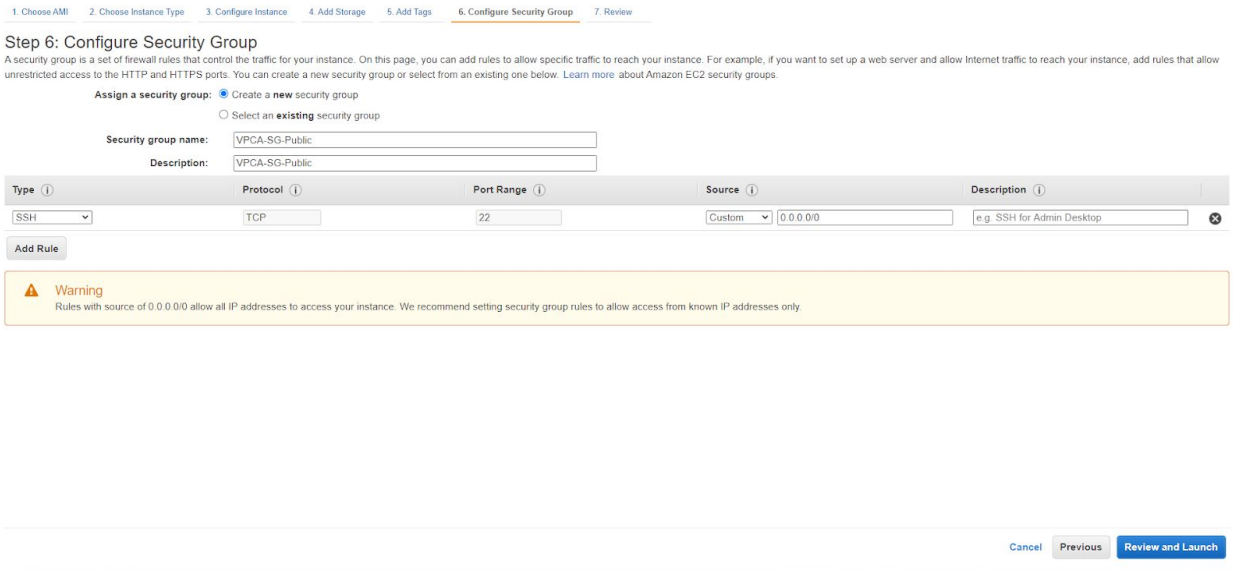

Default storage is selected.

## EC2 - Add Tags



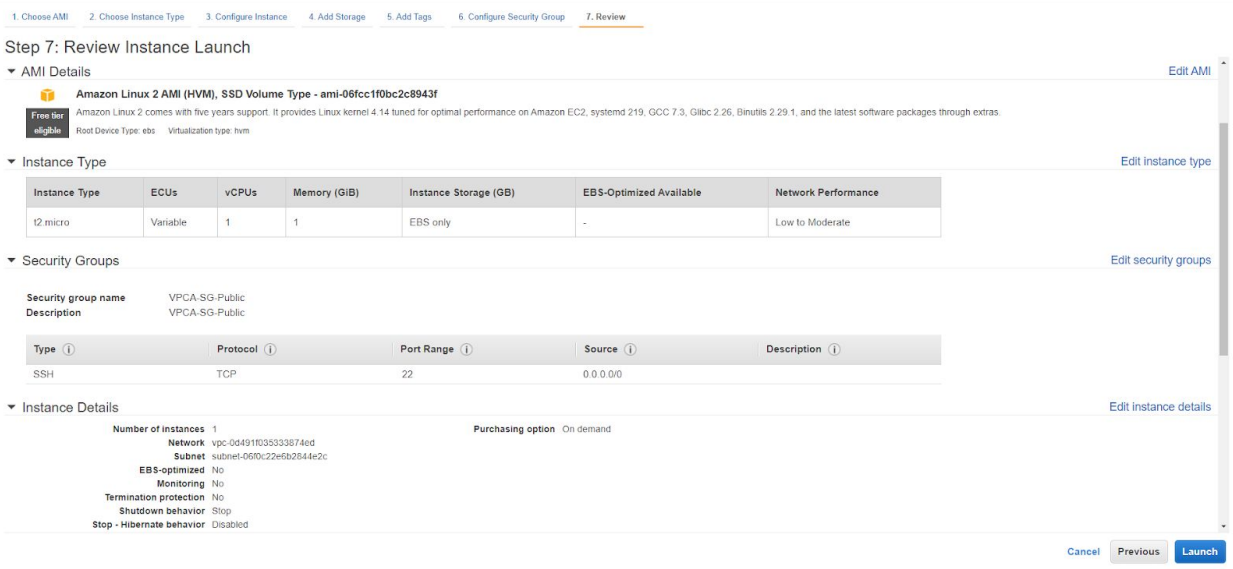

Tags were established.

## EC2 - Configure Security Group



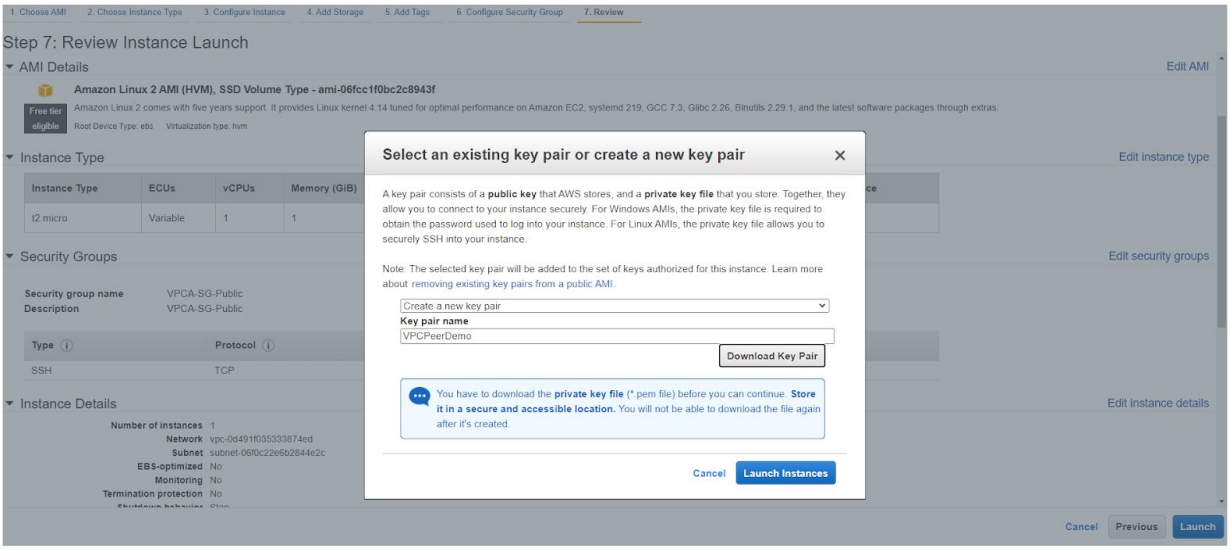

Only SSH will be allowed into this EC2 instance.

## EC2 - Review



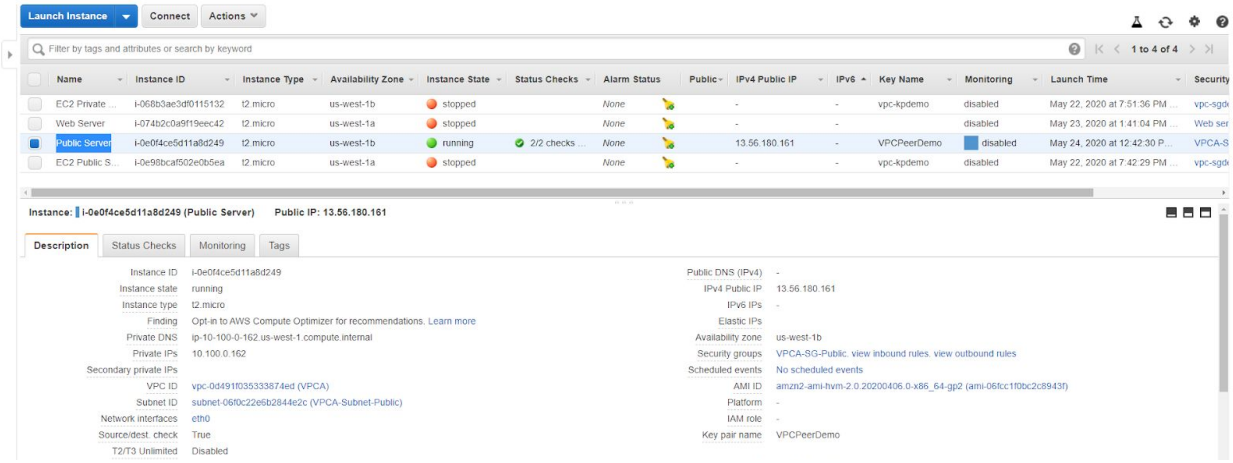

The review page for the EC2 instance.

New key pair



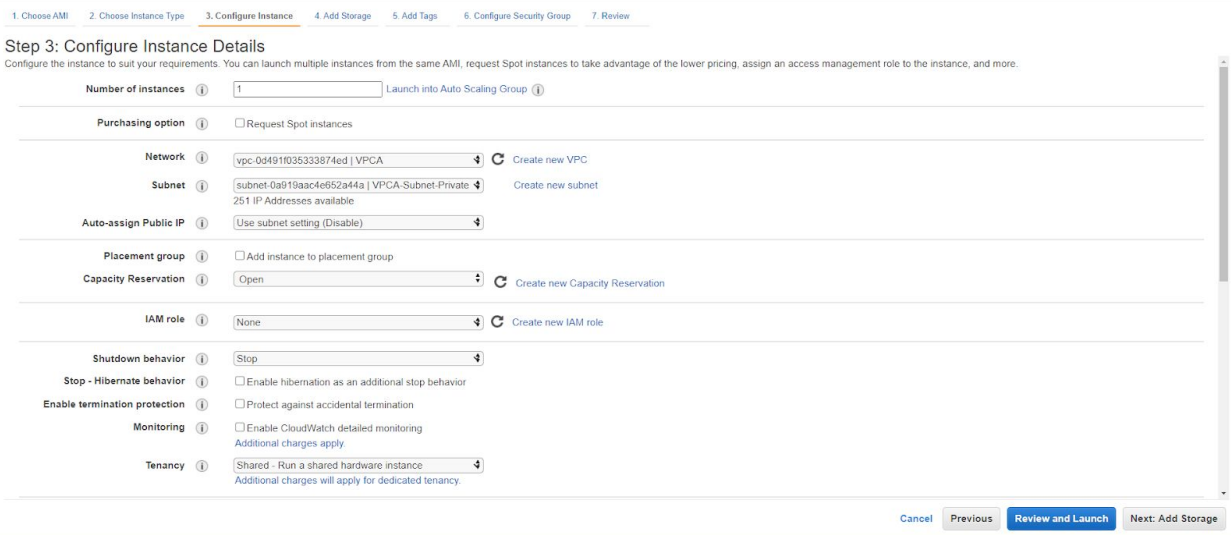

Note that a Key pair has been saved locally.

EC2 Dashboard



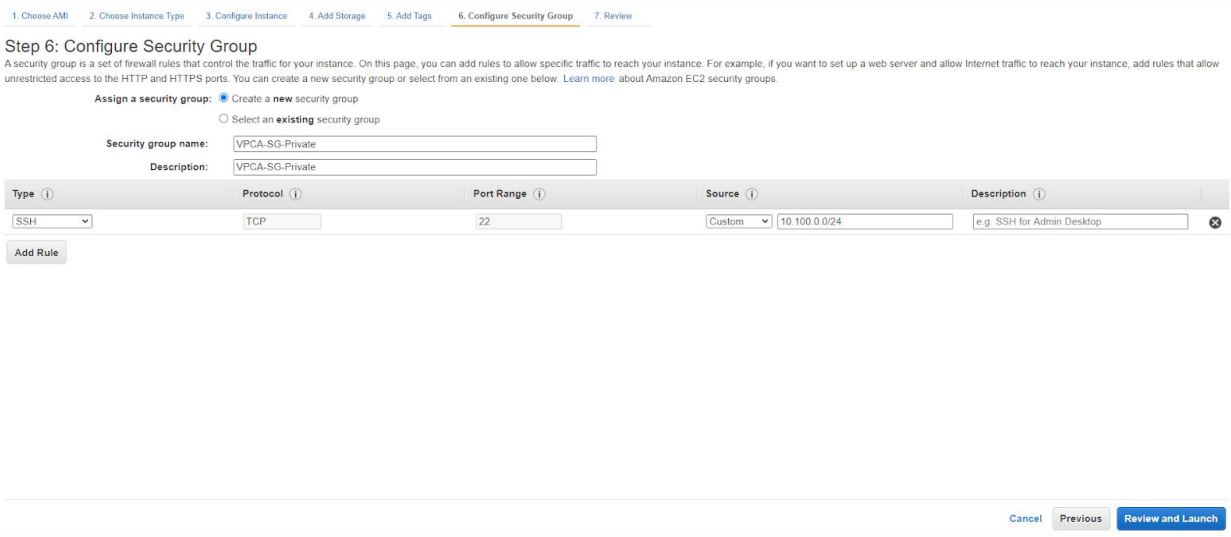

The EC2 Public Server is now running.

## EC2 - Configure Instance



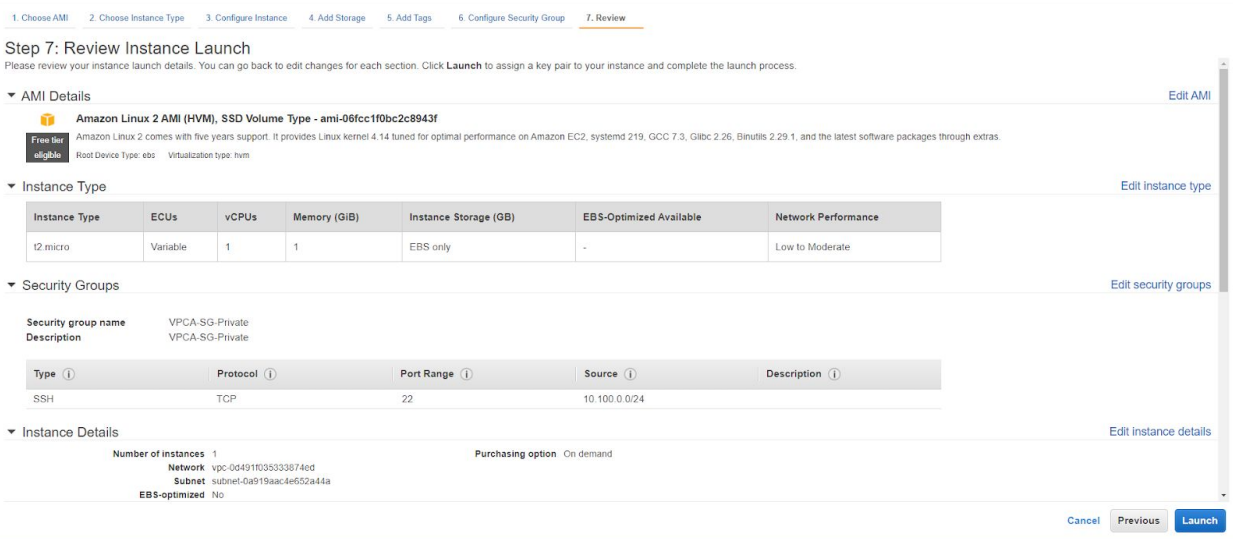

The second private EC2 instance is created. Note that VPCA and VPCA private are selected. Because this is an internal non-public facing instance, auto-assign public IP is disabled.

## EC2 - Configure Security Group



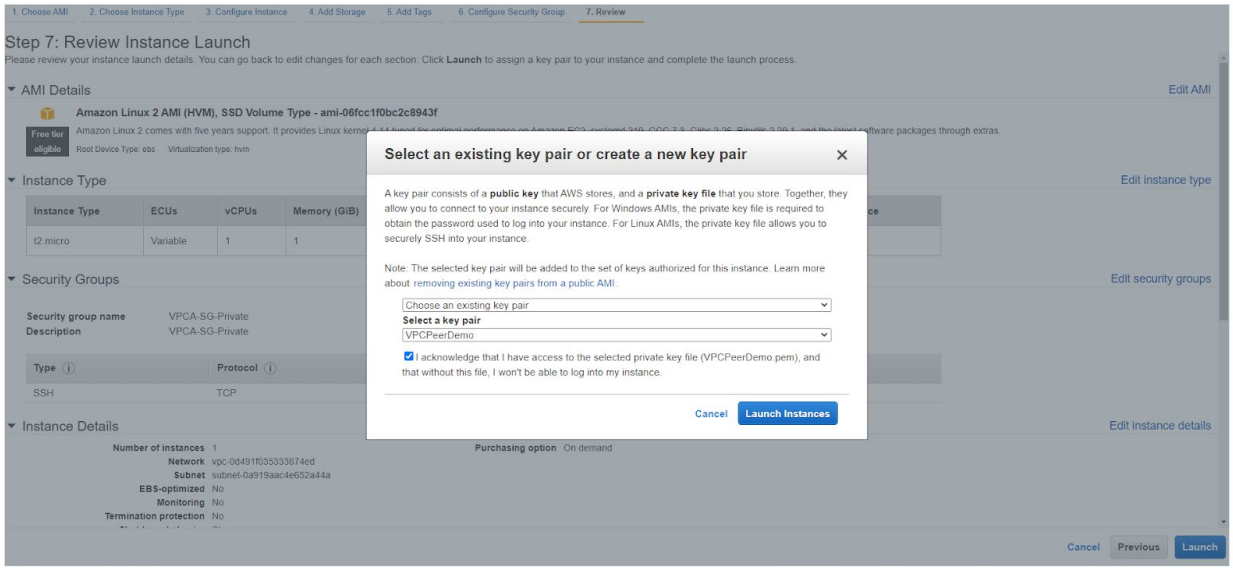

SSH traffic from the 10.100.0.0/24 net will be allowed.

## EC2 - Review



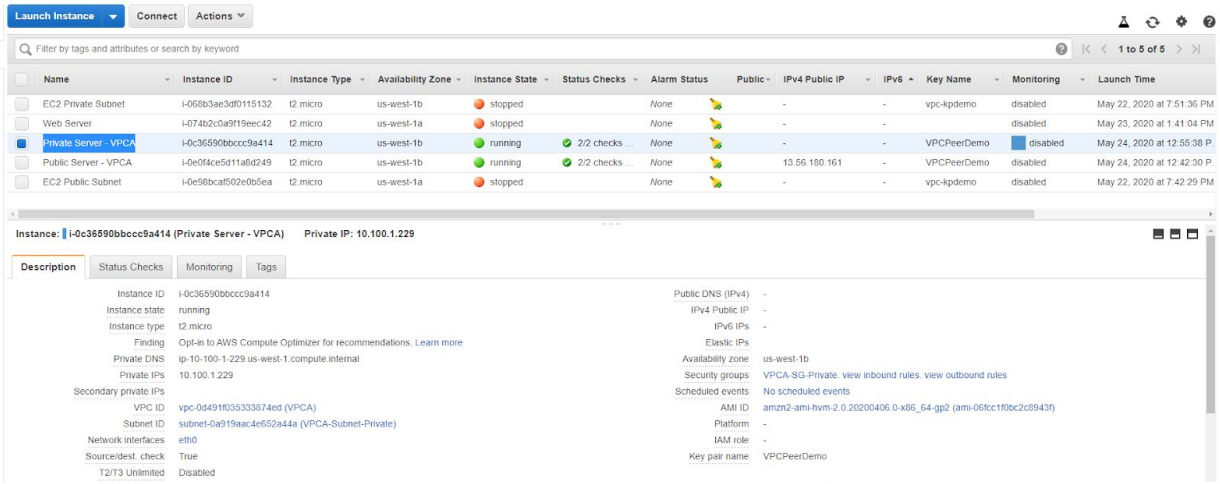

The EC2 instance review page before launch.

## EC2 - key pair



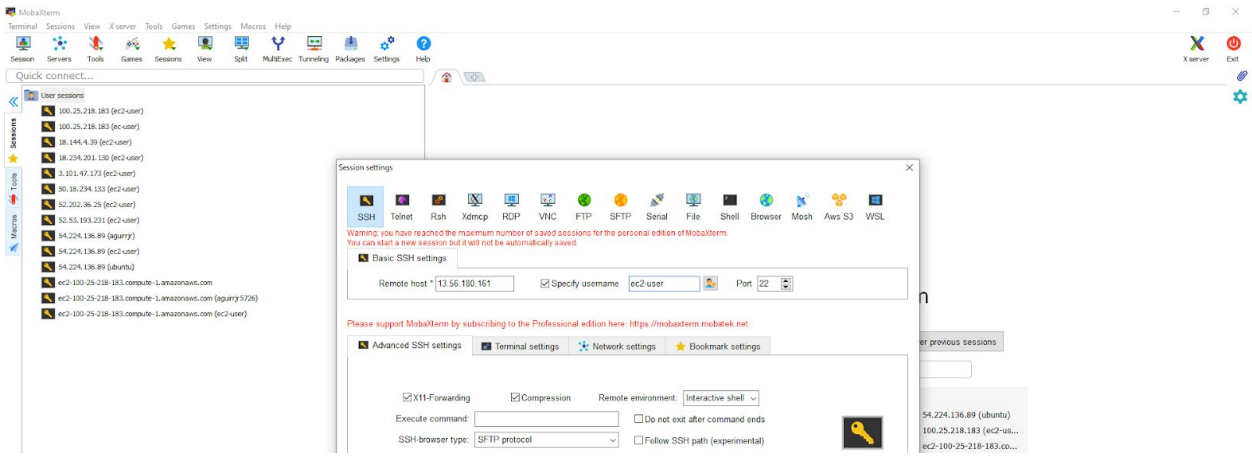

The same previously downloaded key pair is provisioned.

## EC2 Dashboard



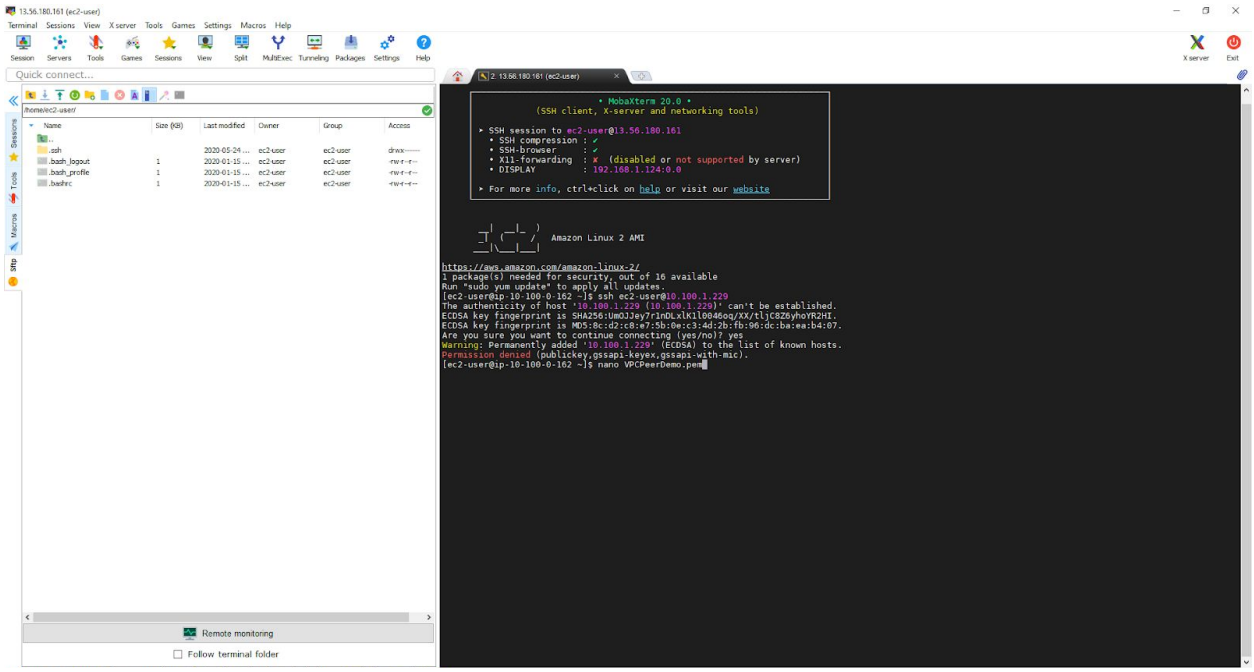

Private Server is now running. Note the lack of an IPv4 Public IP.

## MobaXterm




MobaXterm will be used to SSH into the Public subnet.

MobaXterm




While attempting to SSH into the private instance from the public instance, a permission denial error occurs. Since the pem file is not located on the EC2 instance, a new file must be created.

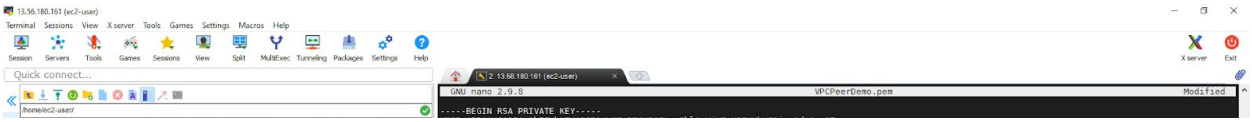
Locally saved PEM file


This is the pem file saved locally when the first EC2 instance was created.

Windows 10 - Notepad

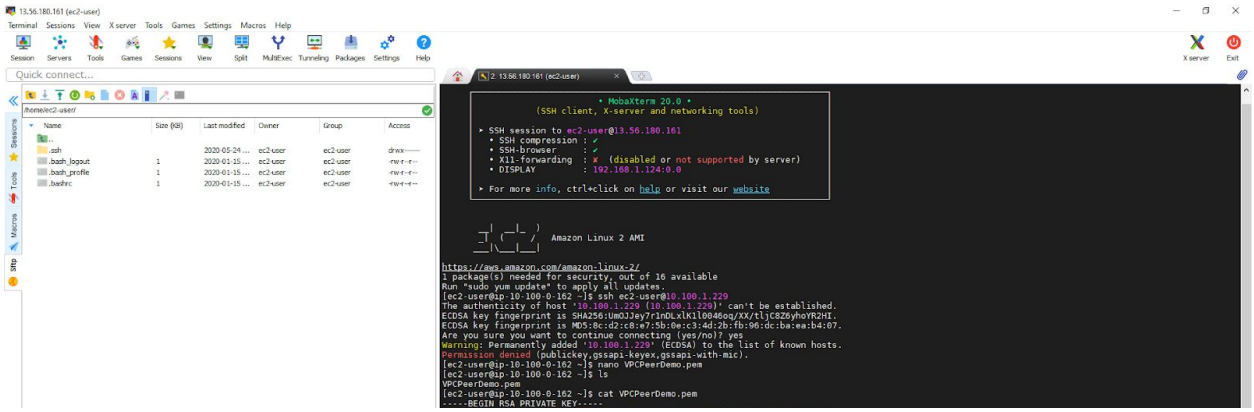

Using notepad, the contents of the pem file are displayed. The complete text must be copied.

MobaXterm



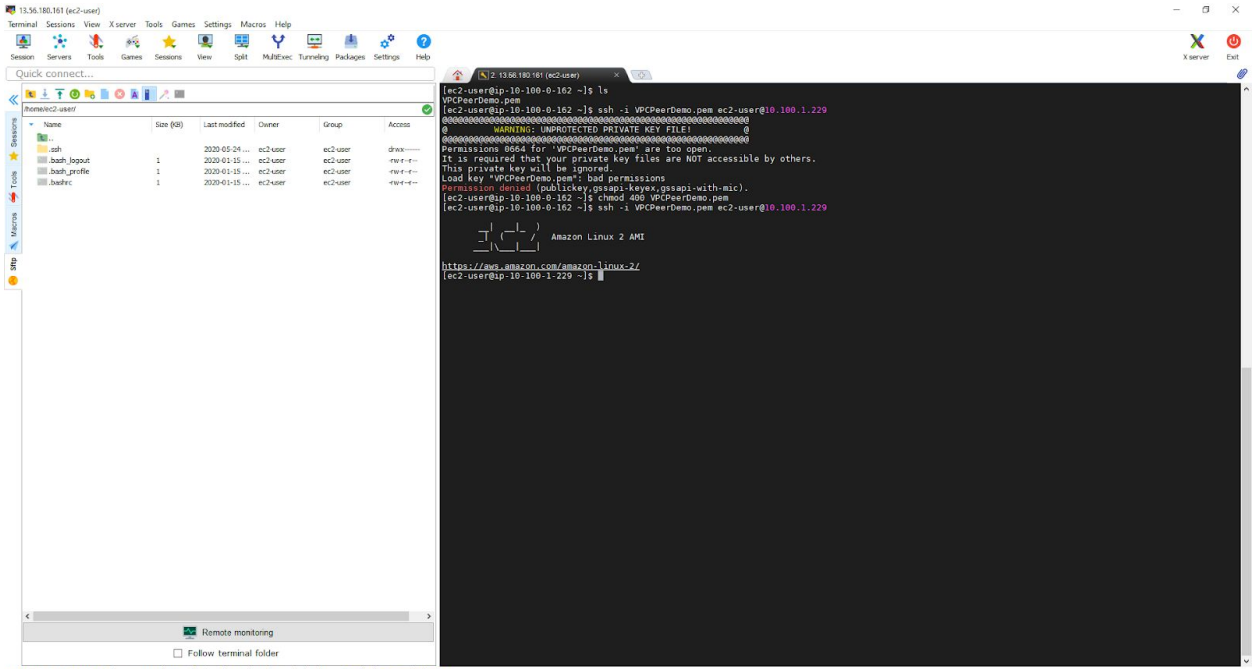

The text is pasted into the file. Note that MobaXterm confirms the correct text before pasting.

MobaXterm



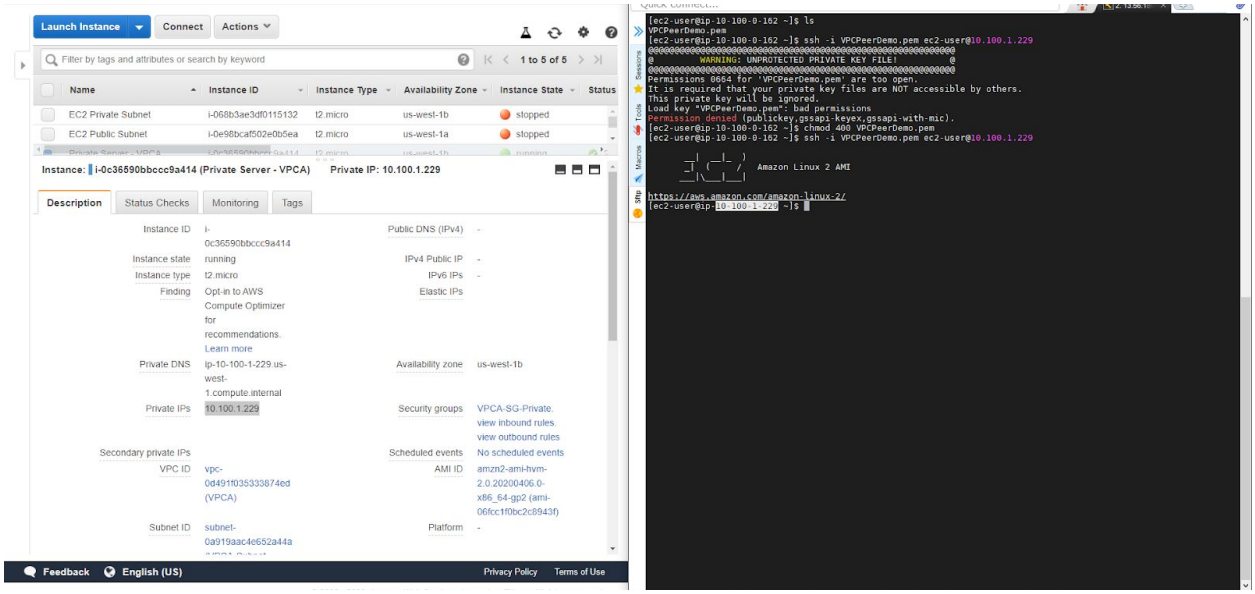

Using the ls command to list files in the current working directory. The contents of the pem file are correct.

MobaXterm



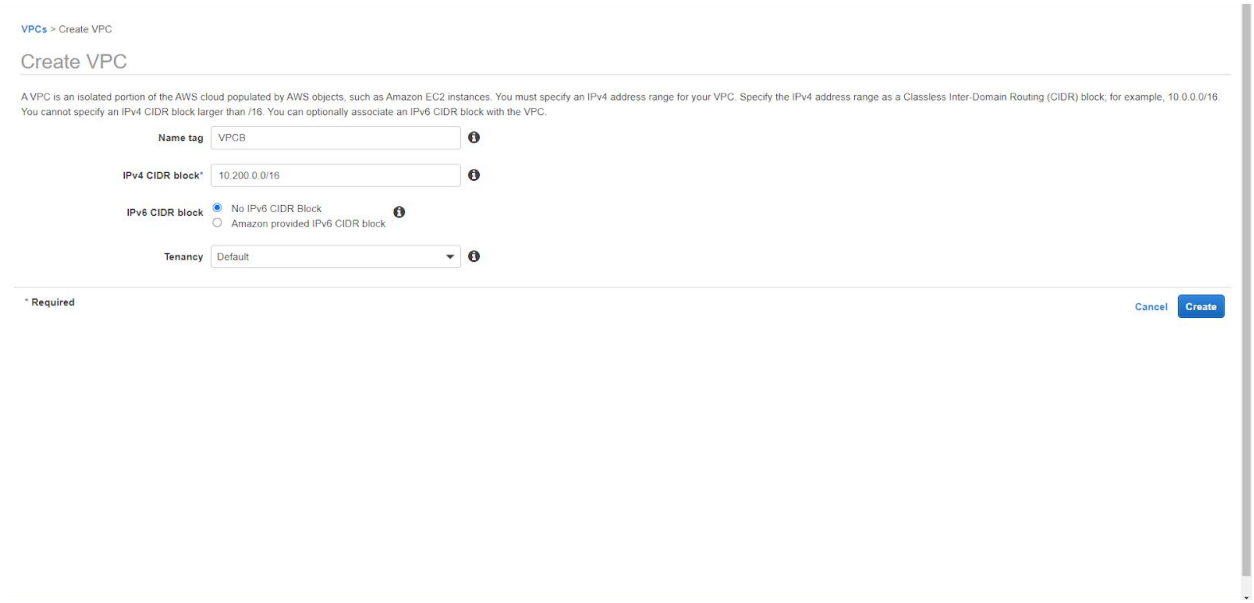

A permission warning occurs. To fix this a chmod 400 command is issued. The local computer has connected to the private EC2 instance through the public EC2 instance.

AWS Console/MobaXterm



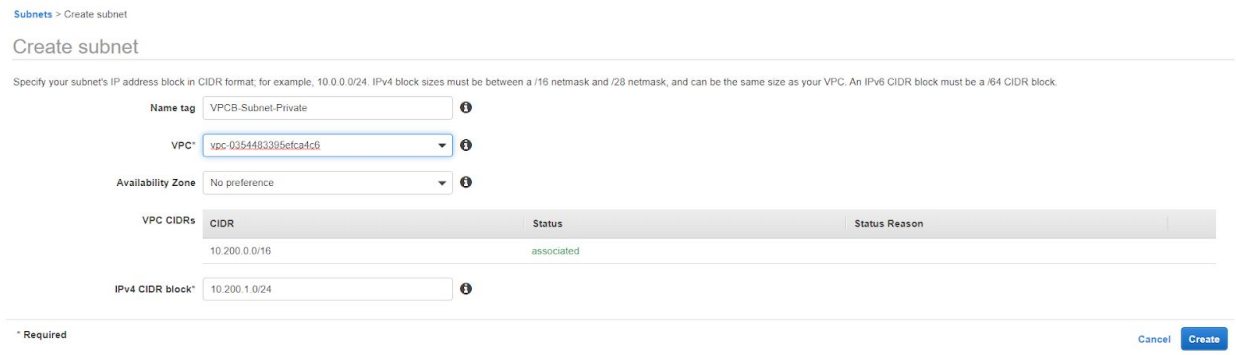

A SSH session has been established to the private EC2 instance.

VPCs - Create VPC



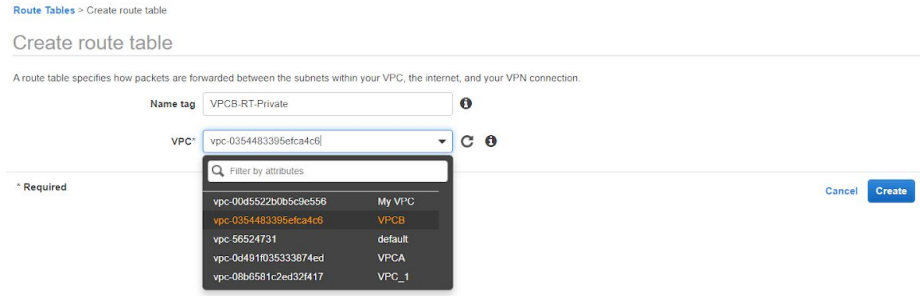

Now the VPC to peer connect to will be created. An IG is not required because there will be no internet access.

## Subnets - Create subnet



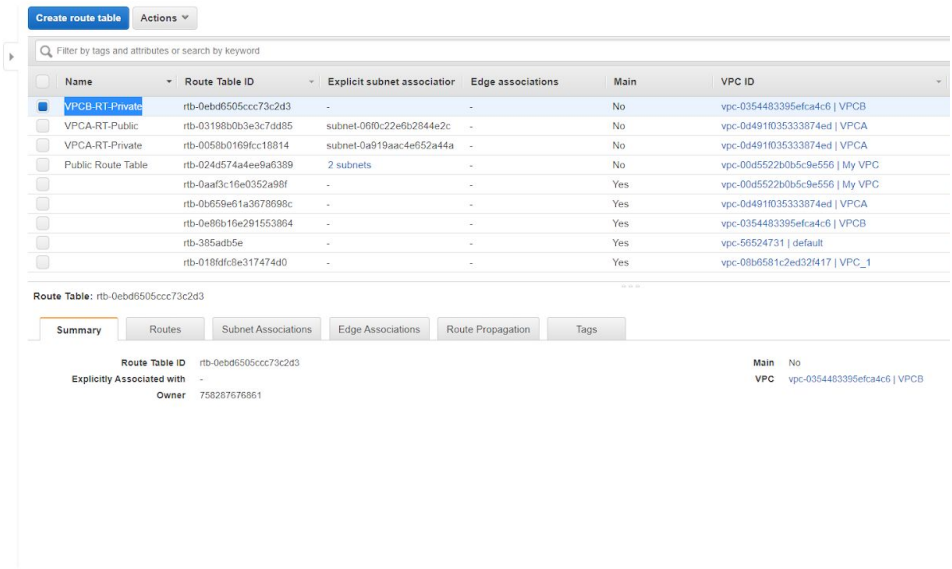

This subnet will belong to the VPCB just created.

## Route Tables - Create route table



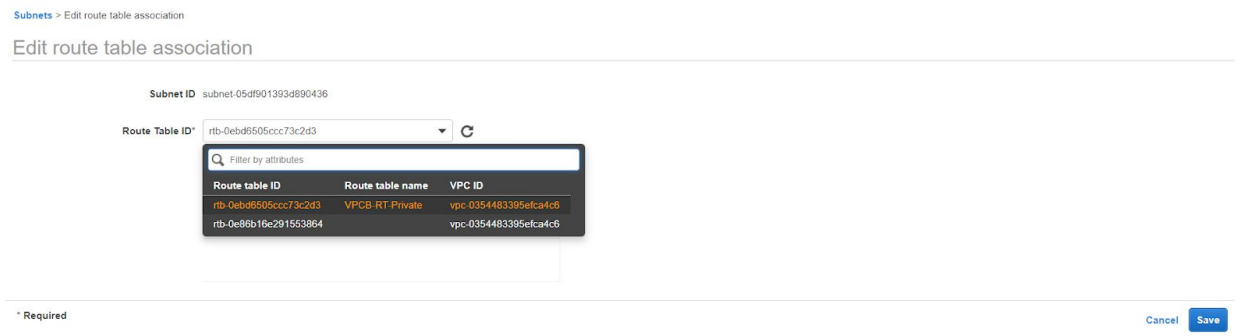

This routing table will apply to the VPCB subnet.

VPC - Route tables



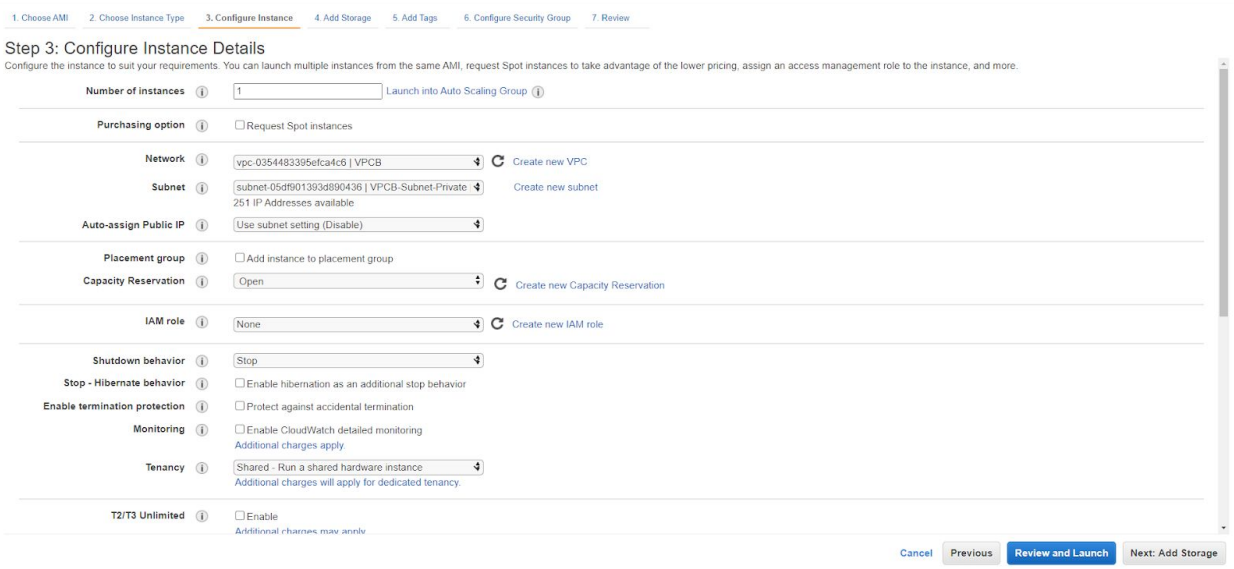

The route table is created for VPCB.

Subnets - Edit route table association



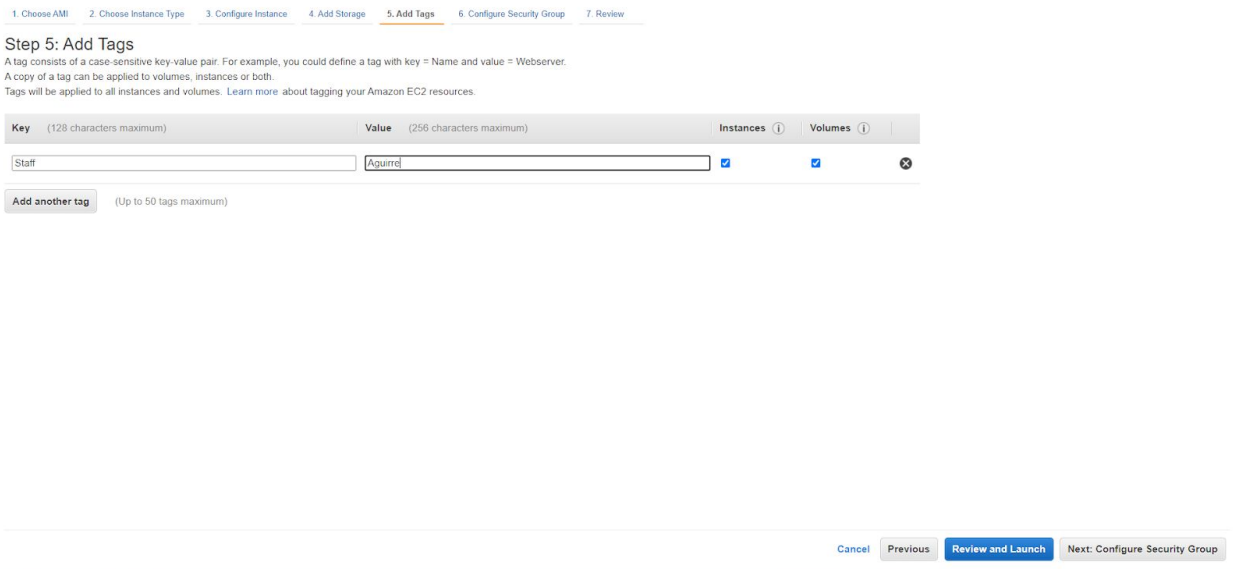

The route VPCB subnet is now associated with the VPCB route table. Traffic will route locally.

## EC2 - Configure instance



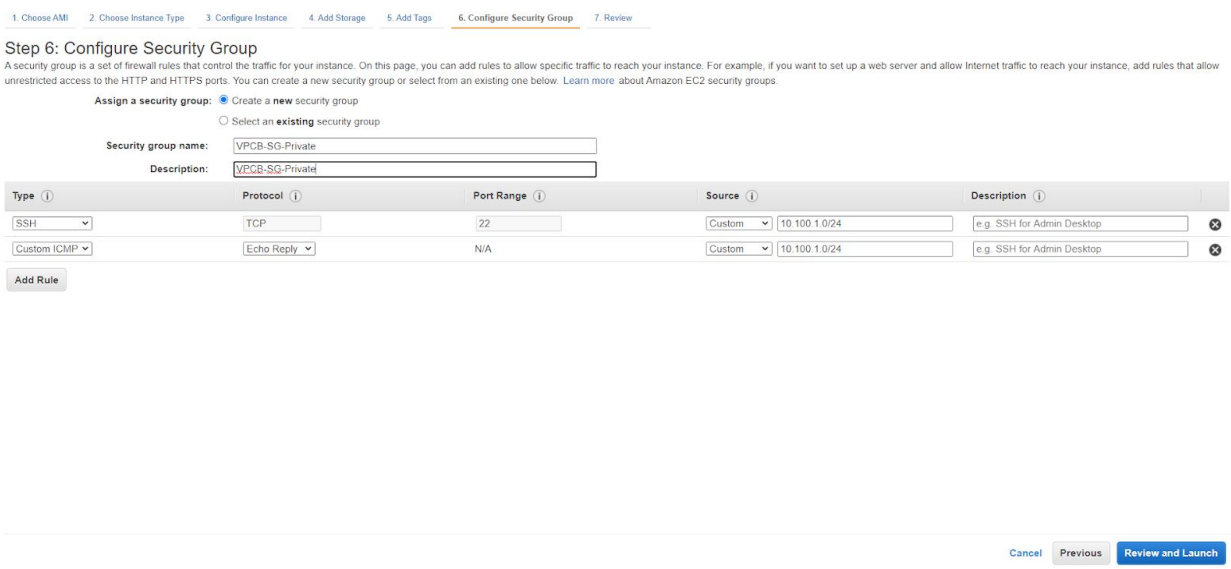

A new EC2 instance will now be created. Note VPCB and Private subnets are provisioned and auto-assign Public IP is disabled.

## EC2 - Add Tags



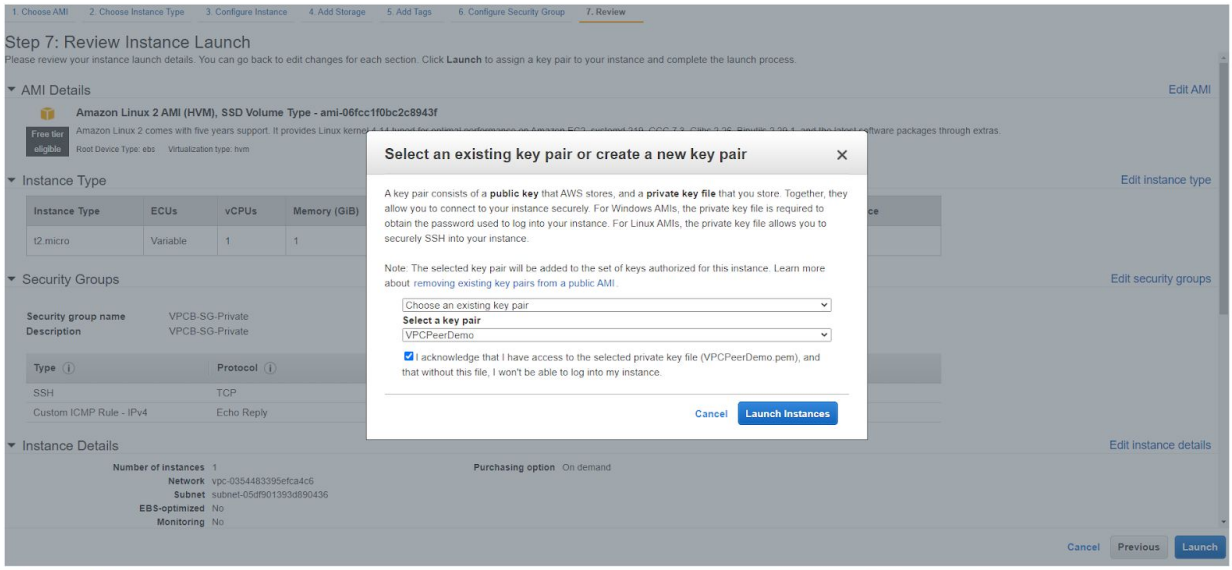

Staff tags established instance ownership.

## EC2 - Configure Security Group



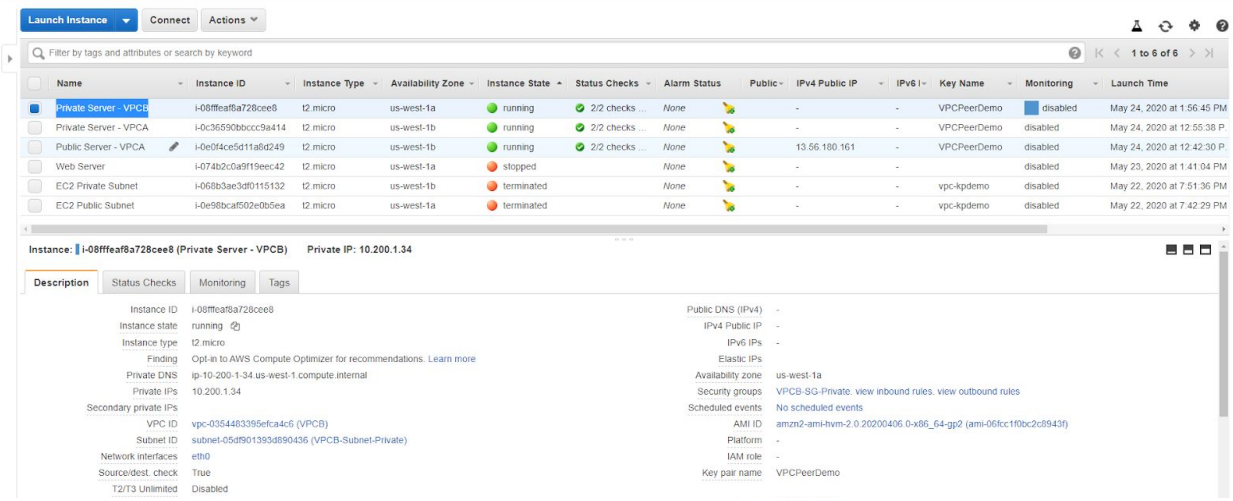

A security group for SSH and ICMP is created.

## EC2 - Review



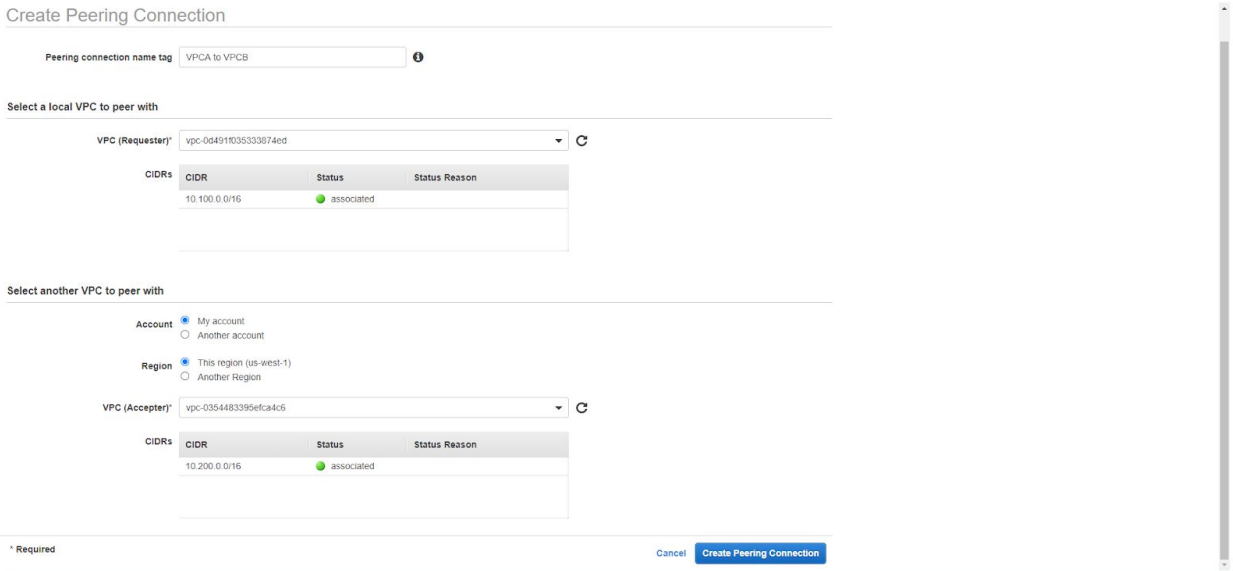

The key pair from the first EC2 instance is still in use.

## EC2 Dashboard



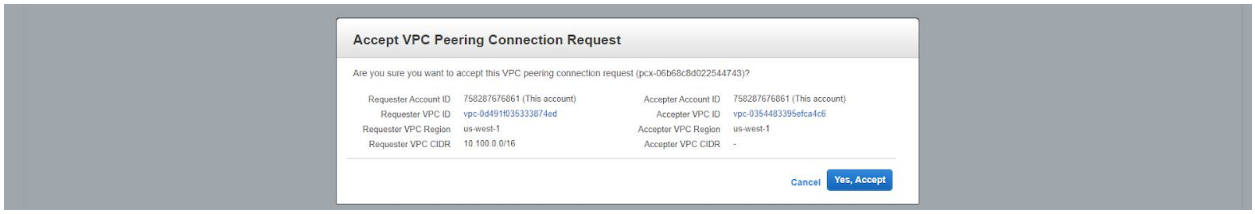

Private server now running.

## Peering Connection - Create Peering Connection

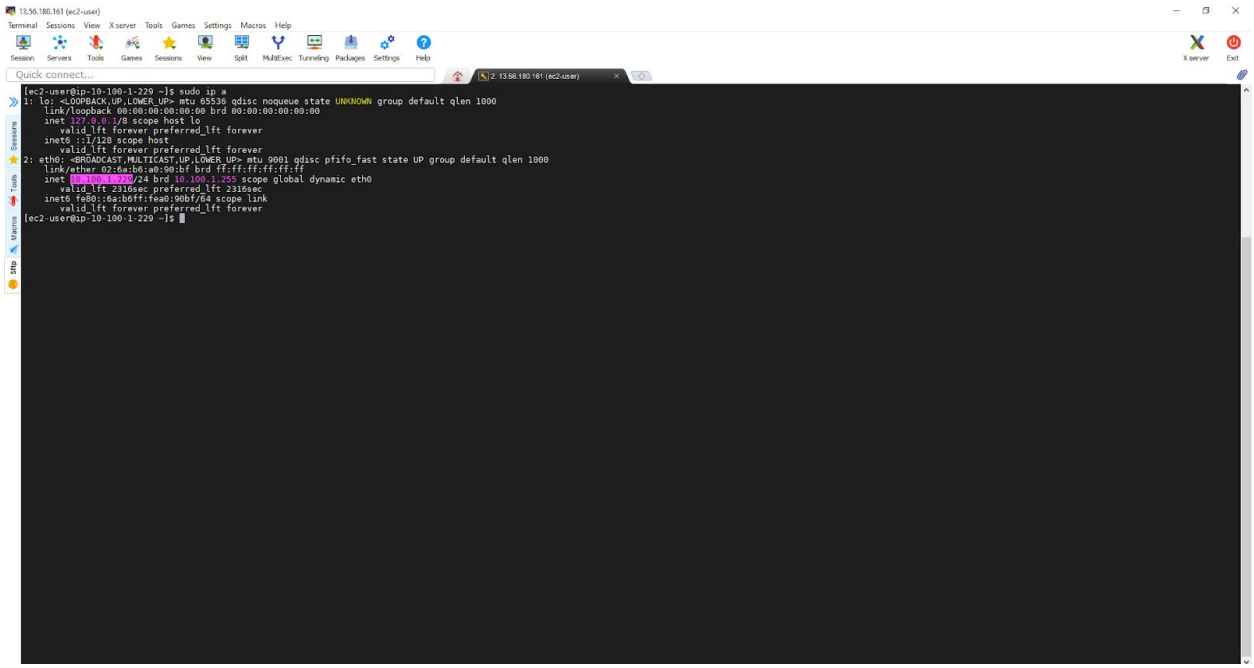



A Peer Connection will be established between VPCA and VPCB.

Peering Connections - Request

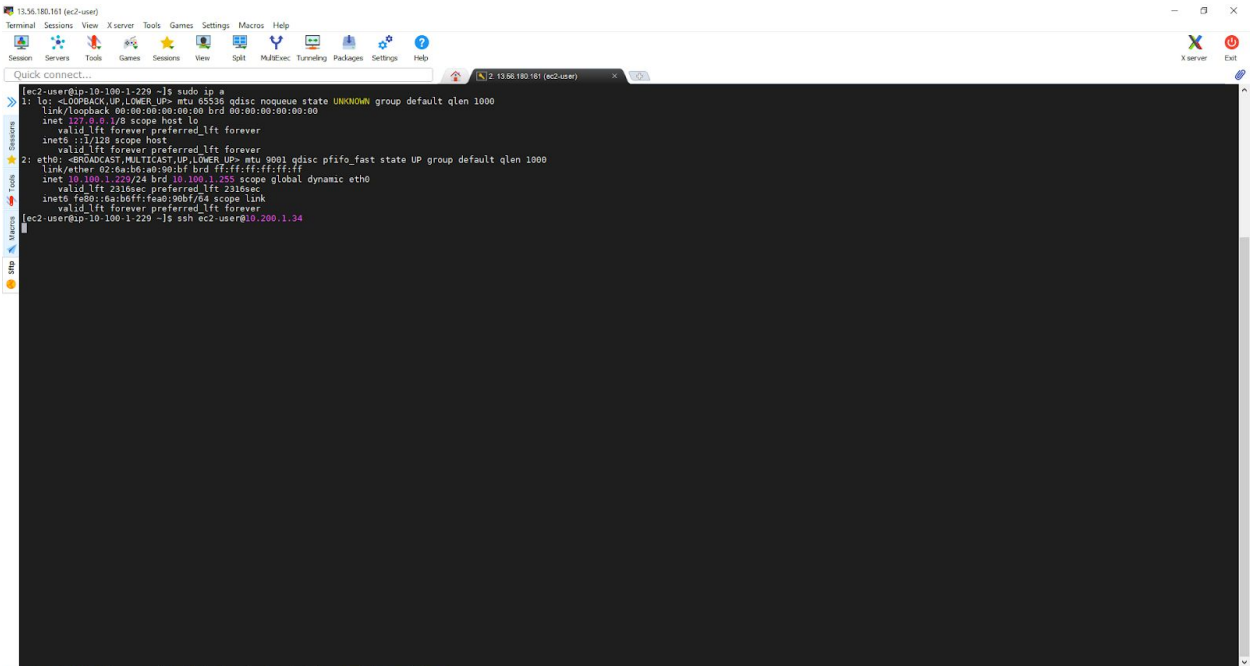



The connection must be accepted before a peer connection is made.



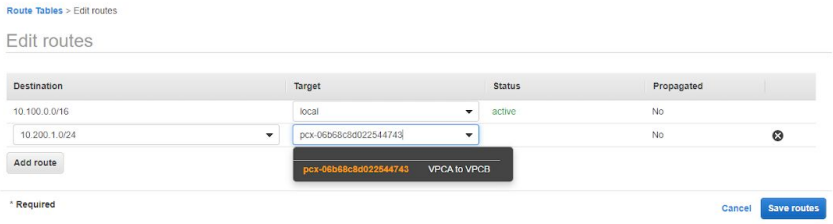

Next a peer connection from the private VPCA to private VPCB will be established. Using the command sudo ip a, to verify the IP corresponds to the private VPCA IP.

MobaXterm



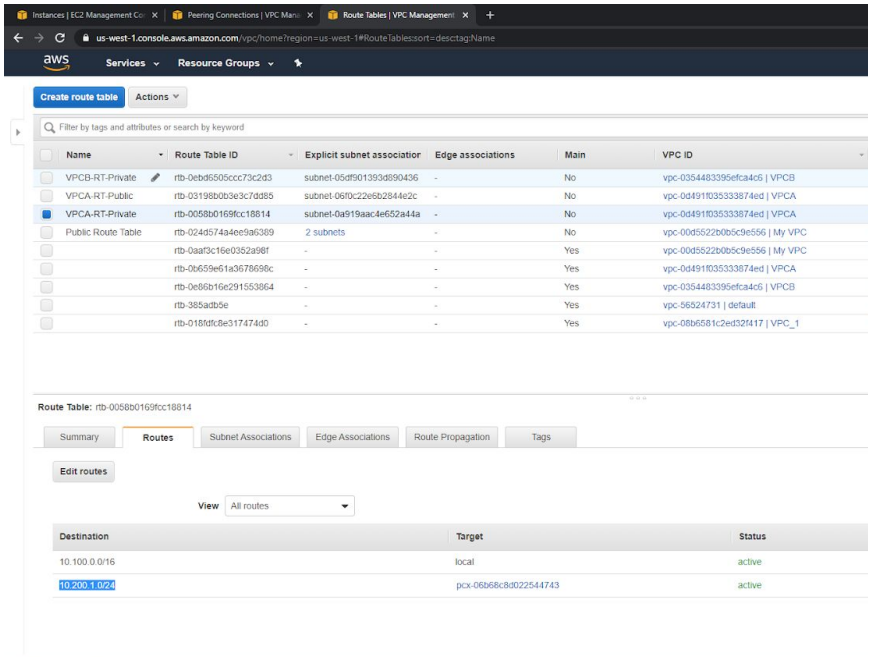

The connection hangs. This is because the routing tables are not properly set up between VPCA and VPCB.

Route Tables - Edit routes

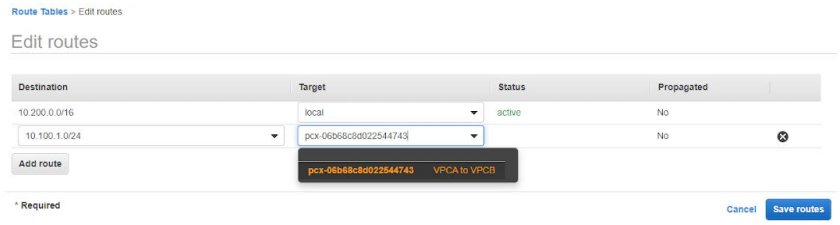



By establishing the VPCB destination and Peer Connection target, a connection can be made between VPCA and VPCB. Note the same change must be established for VPCB private.

VPC - Route tables

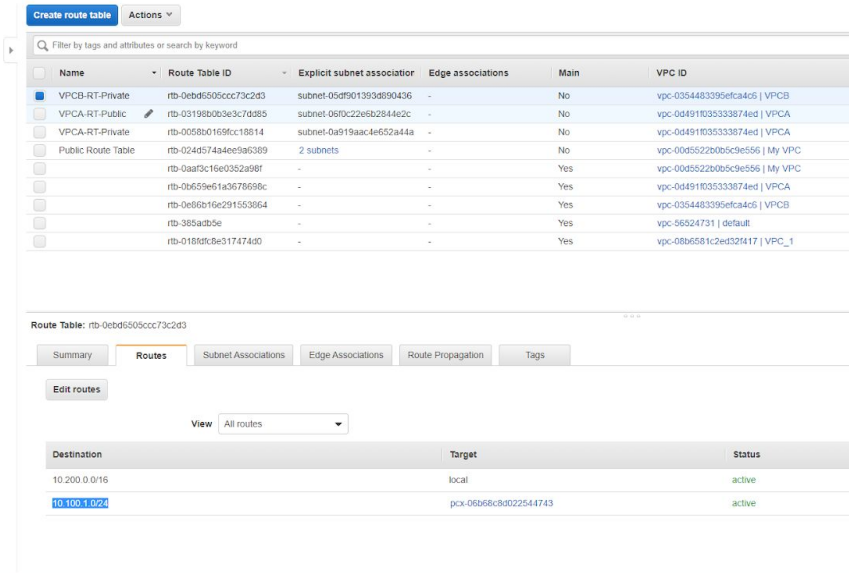



Note 10.200.1.0/24 is listed under Routes.

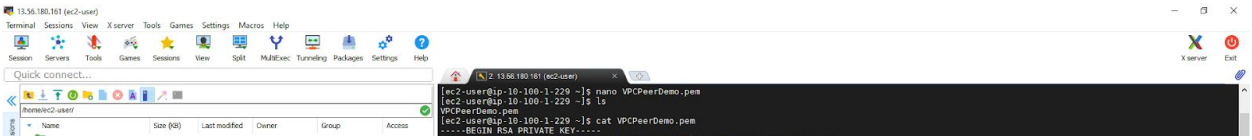



By establishing the VPCA destination and Peer Connection target, a connection can be made between VPCA and VPCB.

VPC - Route tables

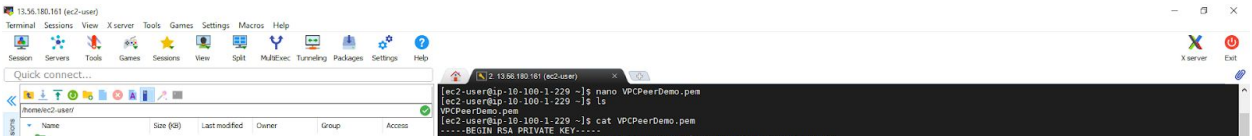



Note 10.100.1.0/24 is listed under Routes.



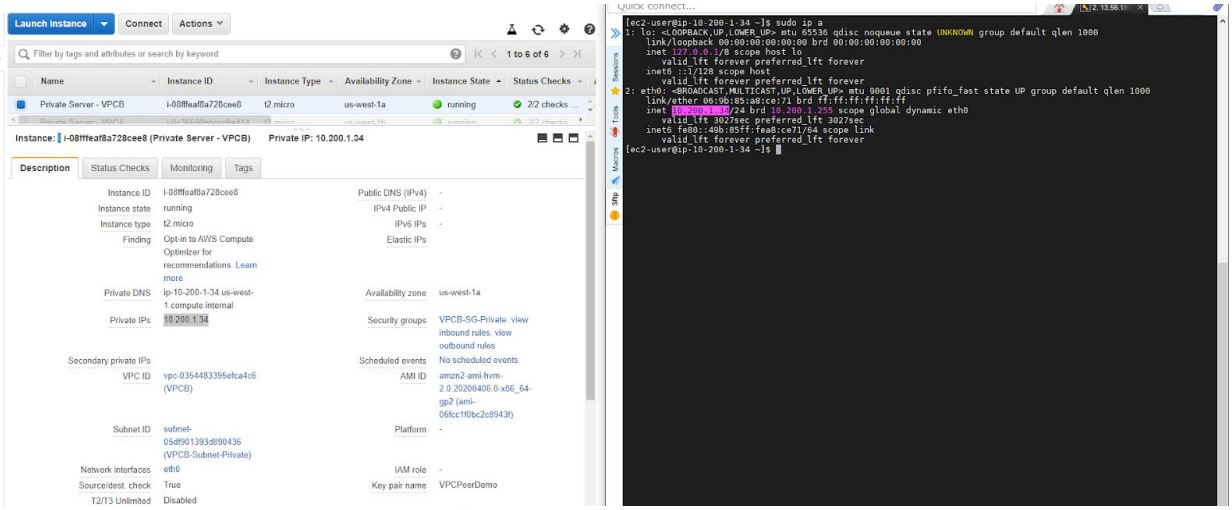

The pem key must be saved to the EC2 instance. Permissions are changed to 400 with the chmod command.

MobaXterm



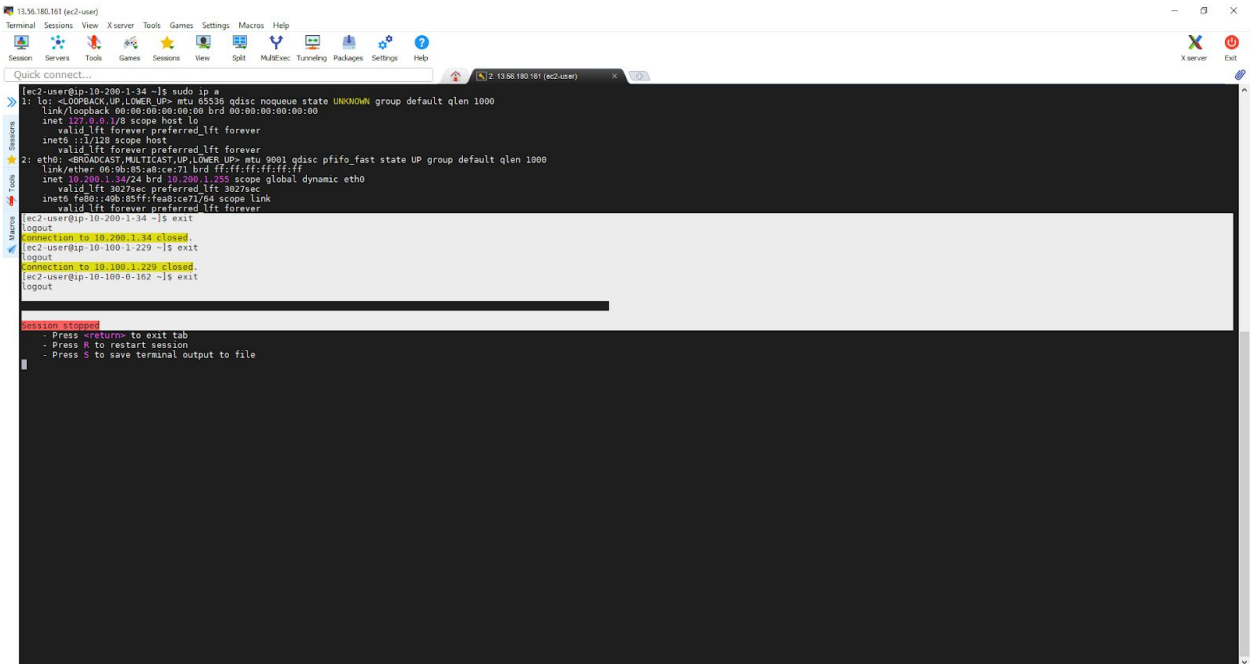

Success! A properly configured Peer Connection has been established between VPCA and VPCB.

AWS Console/MobaXterm




As these are private VPC's with an IP defined route table, there is no other way to have an active connection to the Private server of VPCB.

MobaXterm




Another verification method for subnet connections is when exiting MobaXterm. MobaXterm will display the IP's used in the SSH sessions. Each IP matches the EC2 instance IP.