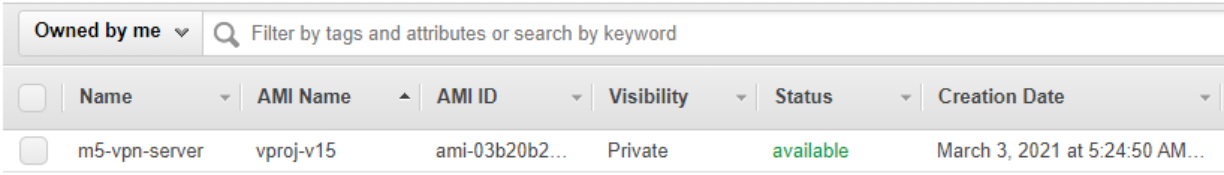
Milestone 5 Goal

Create an AMI that can be launched on EC2 as a VPN share images of you testing it.

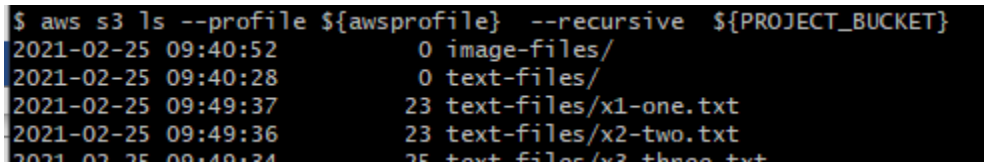
Solution

- Using Milestone 4 automated scripts, create Security Group and EC2 Instance (referred here as the VPN Server EC2 instance).
- Create Elastic IP address and associate it with the VPN Server EC2 Instance.
- SSH into the VPN Server EC2 Instance and configure the [Interface] section of the /etc/wireguard/wg0.conf.
- Create an AMI Image:
  - 

- Terminate the VPN Server EC2 Instance

Test

The following steps can be repeat a few times, to demonstrate the reusable AMI as the VPN Server:

- Use the above AMI to create the VPN Server EC2 Instance and associate the same Elastic IP address.
- SSH into the VPN server EC2 instance:
  - Update the /etc/wireguard/wg0.conf with [Peer]'s PublicKey and AllowedIPs.
  - systemctl restart wg-quick@wg0
- No changes in the laptop VPN WireGuard.
- With no changes to AWS S3 Bucket (containing policy to let securely go through VPN Server, see Milestone 3), access the S3 bucket.
  - 

- Terminate the VPN Server EC2 Instance.

Summary

Created an AMI containing the VPN Server. With this AMI, new VPN Server can be instantiated with minimal configuration.