**Assisted Practice: 6.2 Configure and Launch a NAT Instance**

This section will guide you to:

* Configure and launch a NAT instance that will allow another private instance to access the internet

This lab has three subsections, namely:

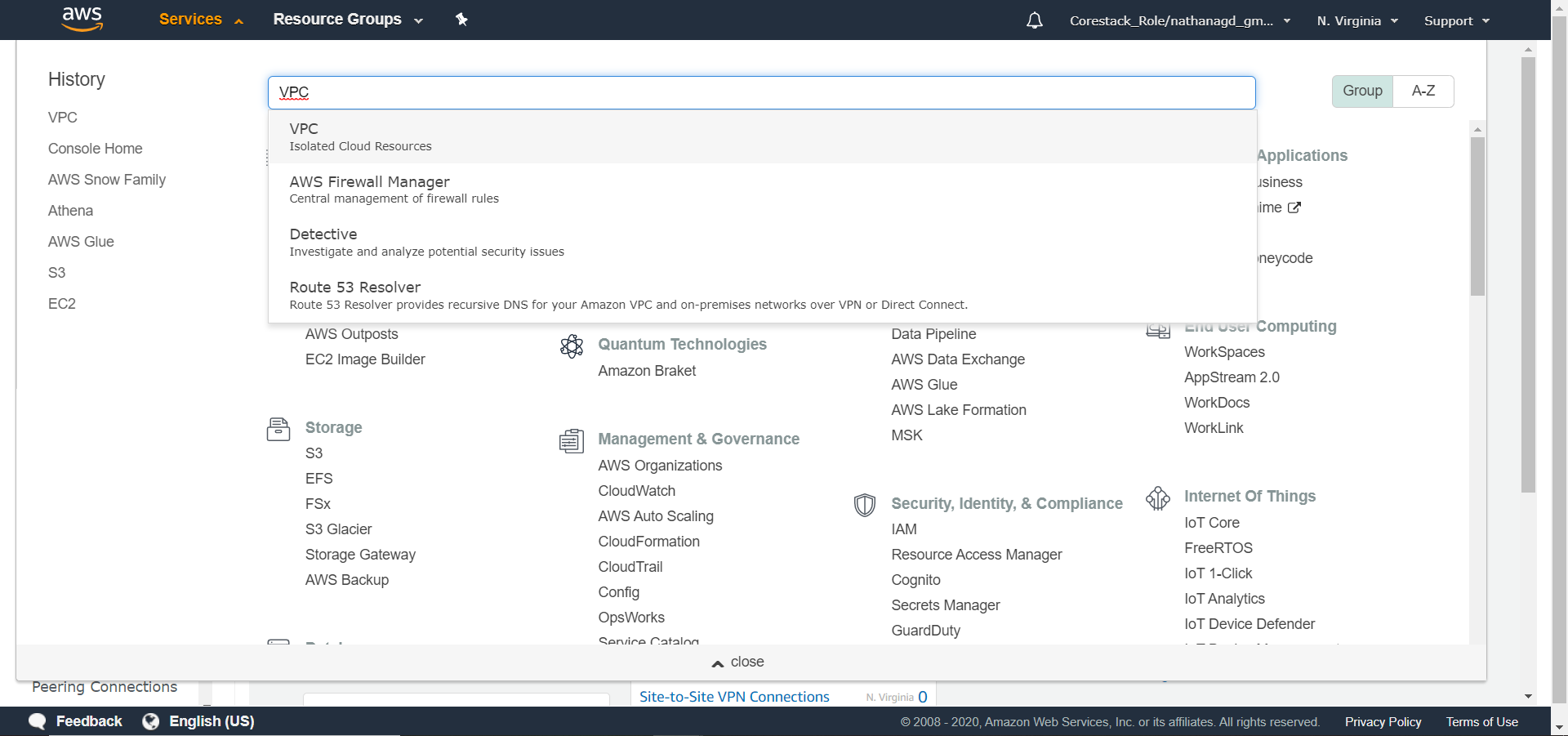
6.2.1 Creating a custom VPC

6.2.2 Creating a public and private subnet

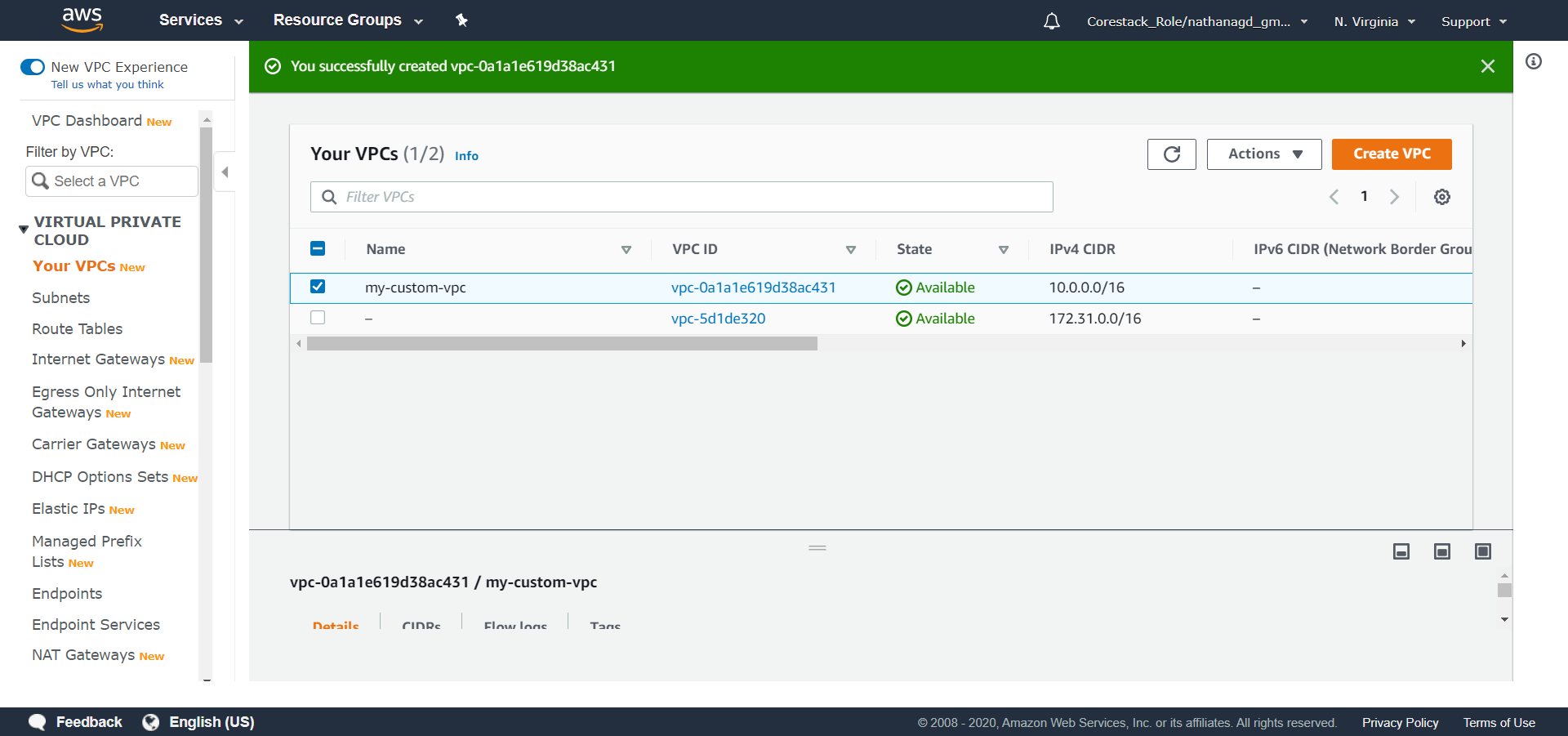
6.2.3 Creating a public NAT Instance and giving access to the internet

**Step 6.2.1:** Creating a custom VPC

* AWS VPC service is enabled in your practice lab.
* Refer **MEAN: Lab Guide - Phase 4** to learn how to use the lab.\
* Go to the Amazon dashboard
* Select **VPC**.

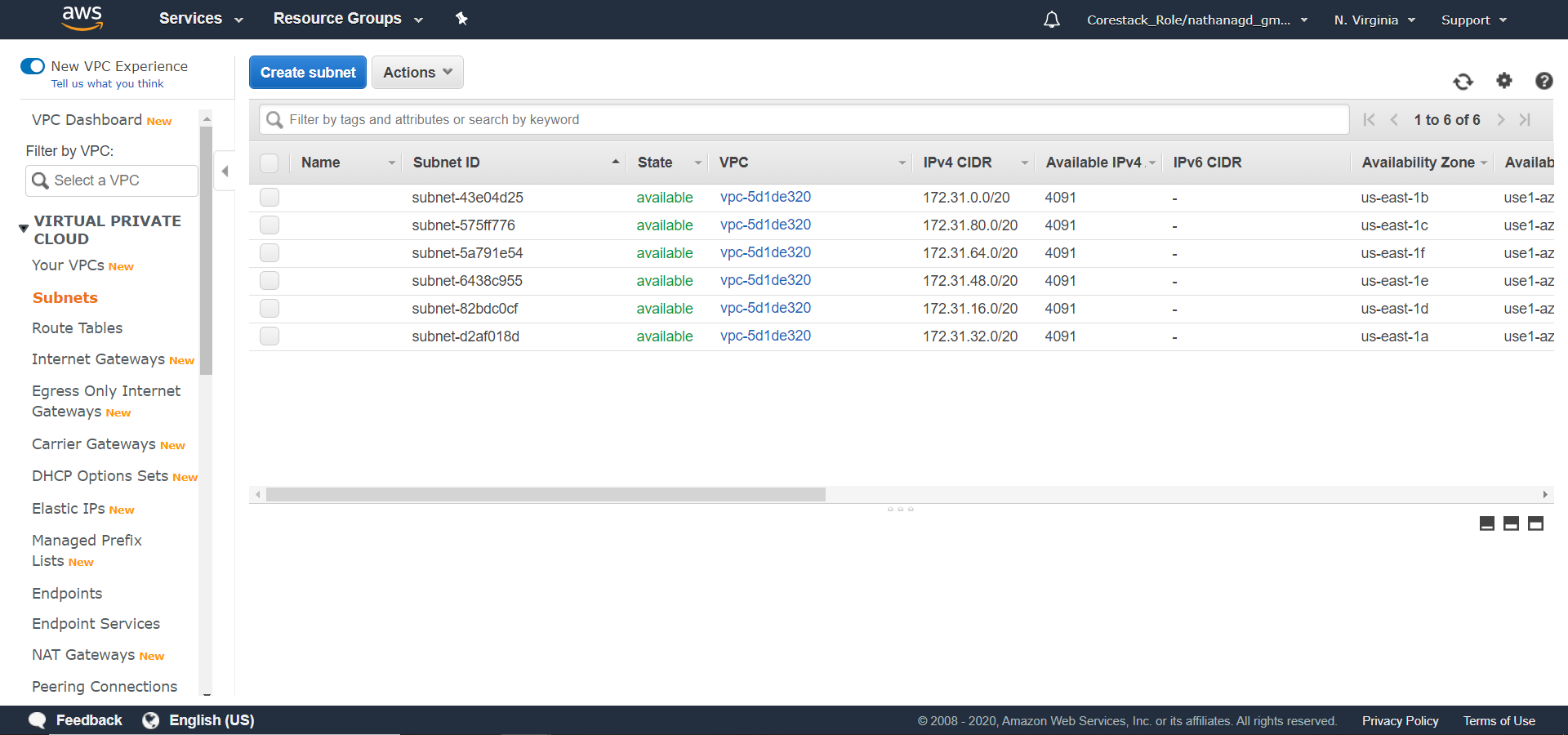


* Create a custom VPC as shown in the previous demo

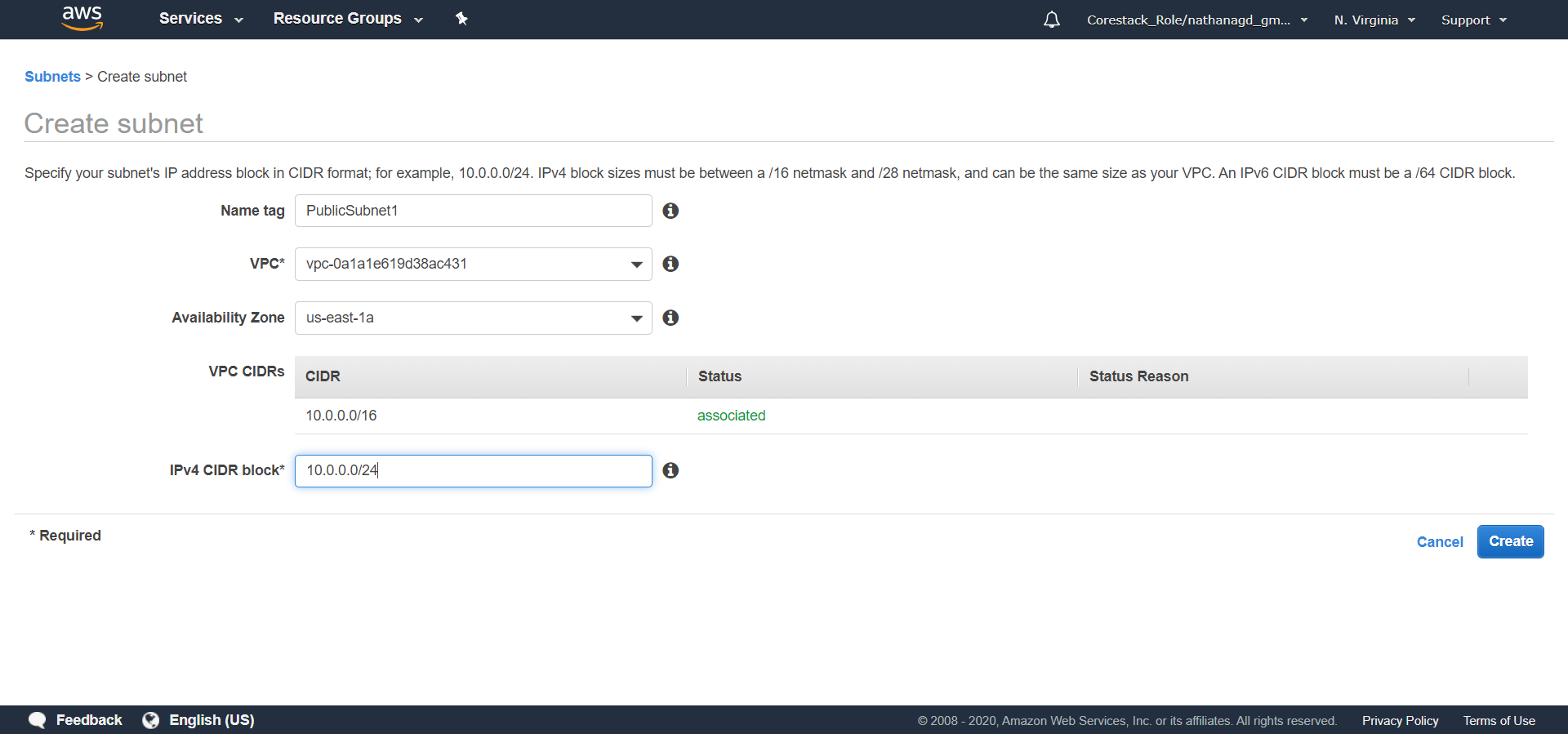


**Step 6.2.2:** Creating a public and private subnet

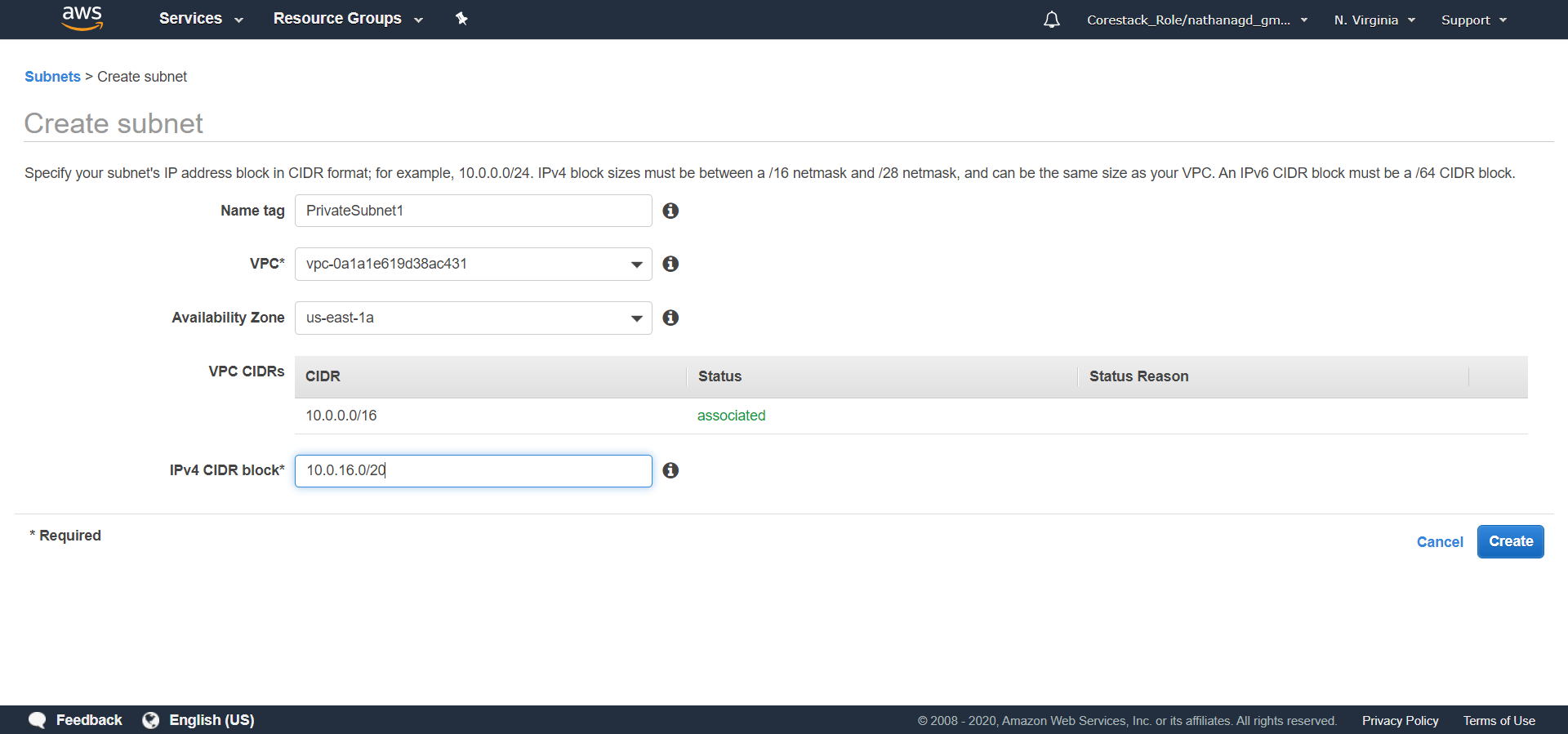
* Click on **Subnets**



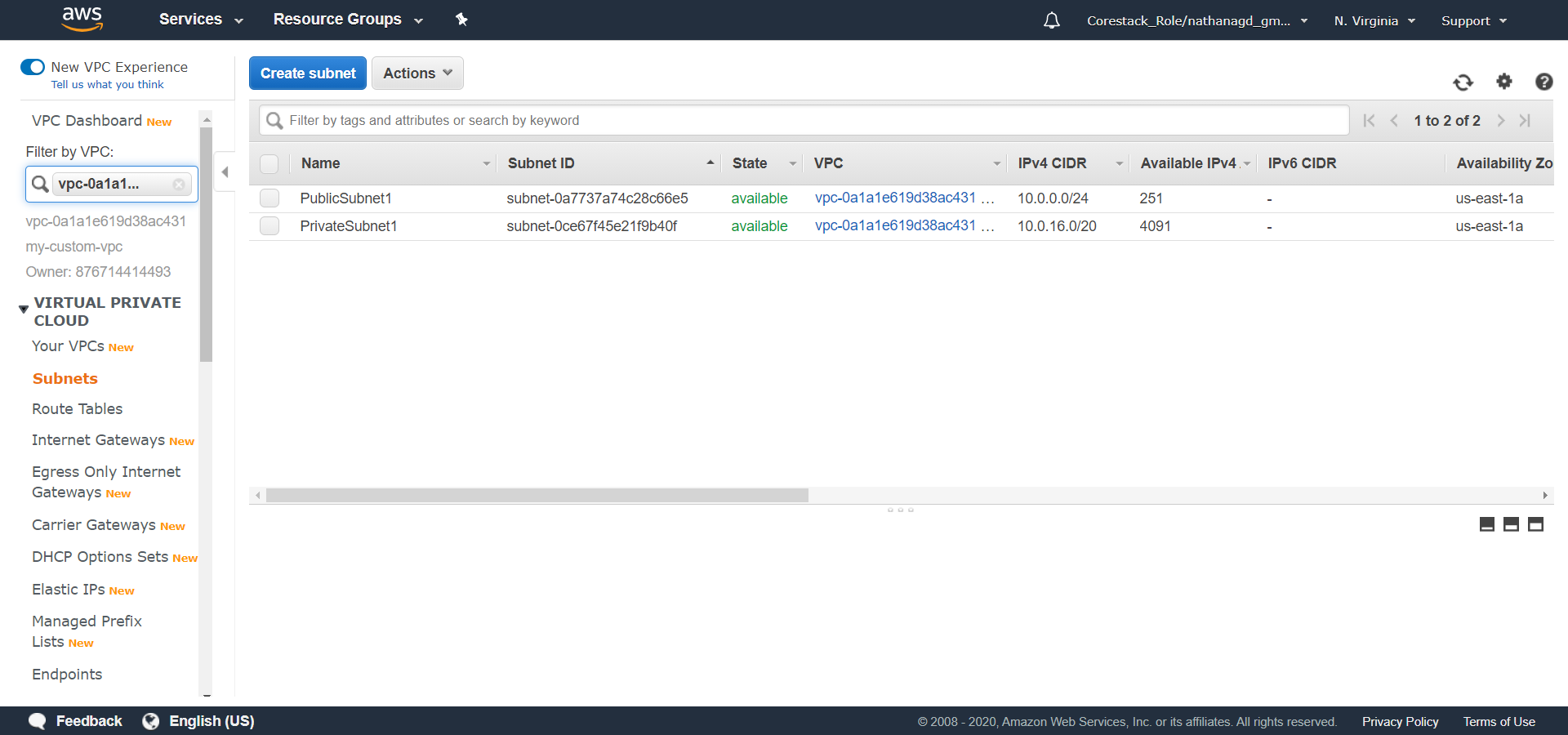
* Click on **Create Subnet**, and create a public subnet



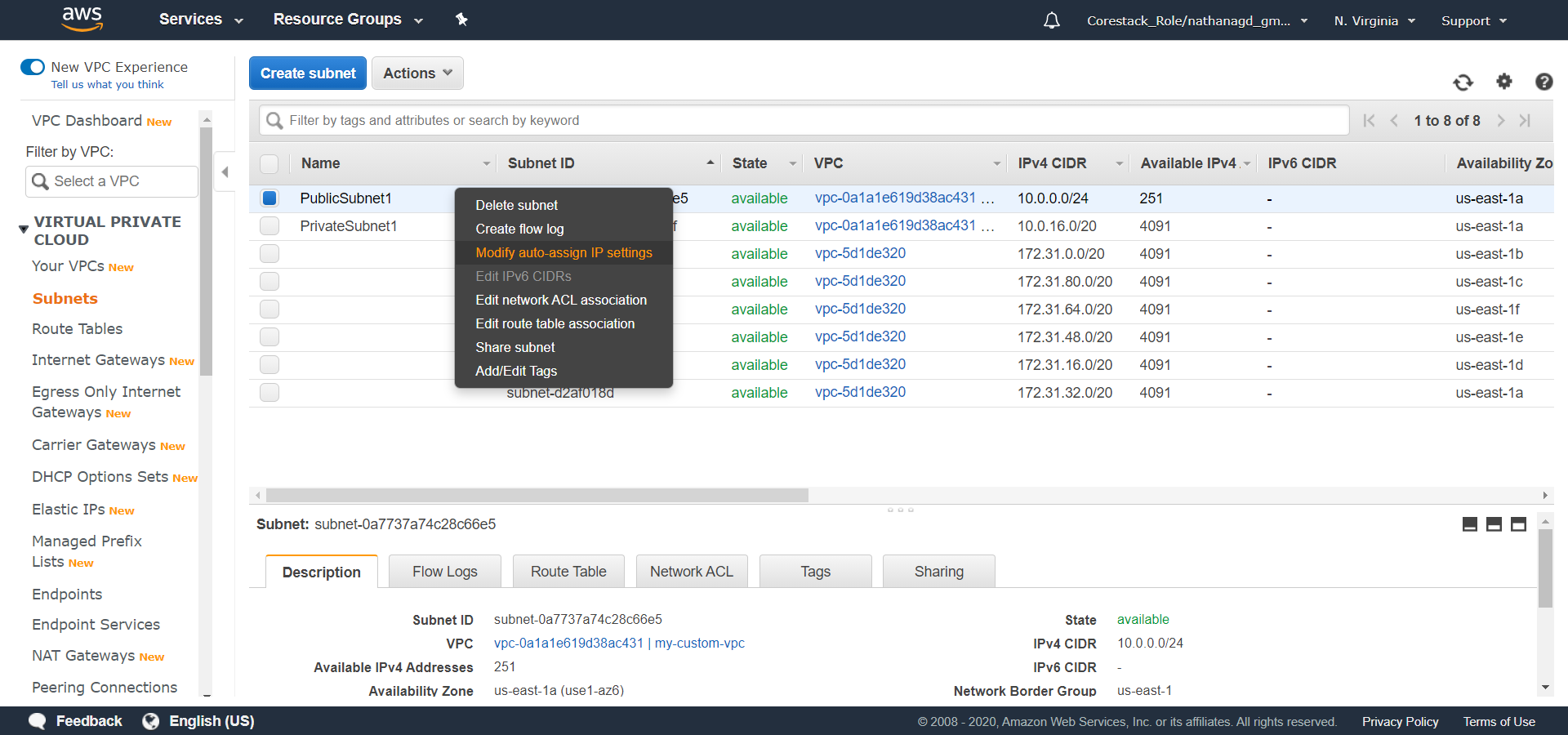
* Click on **Create Subnet,** and create a private subnet



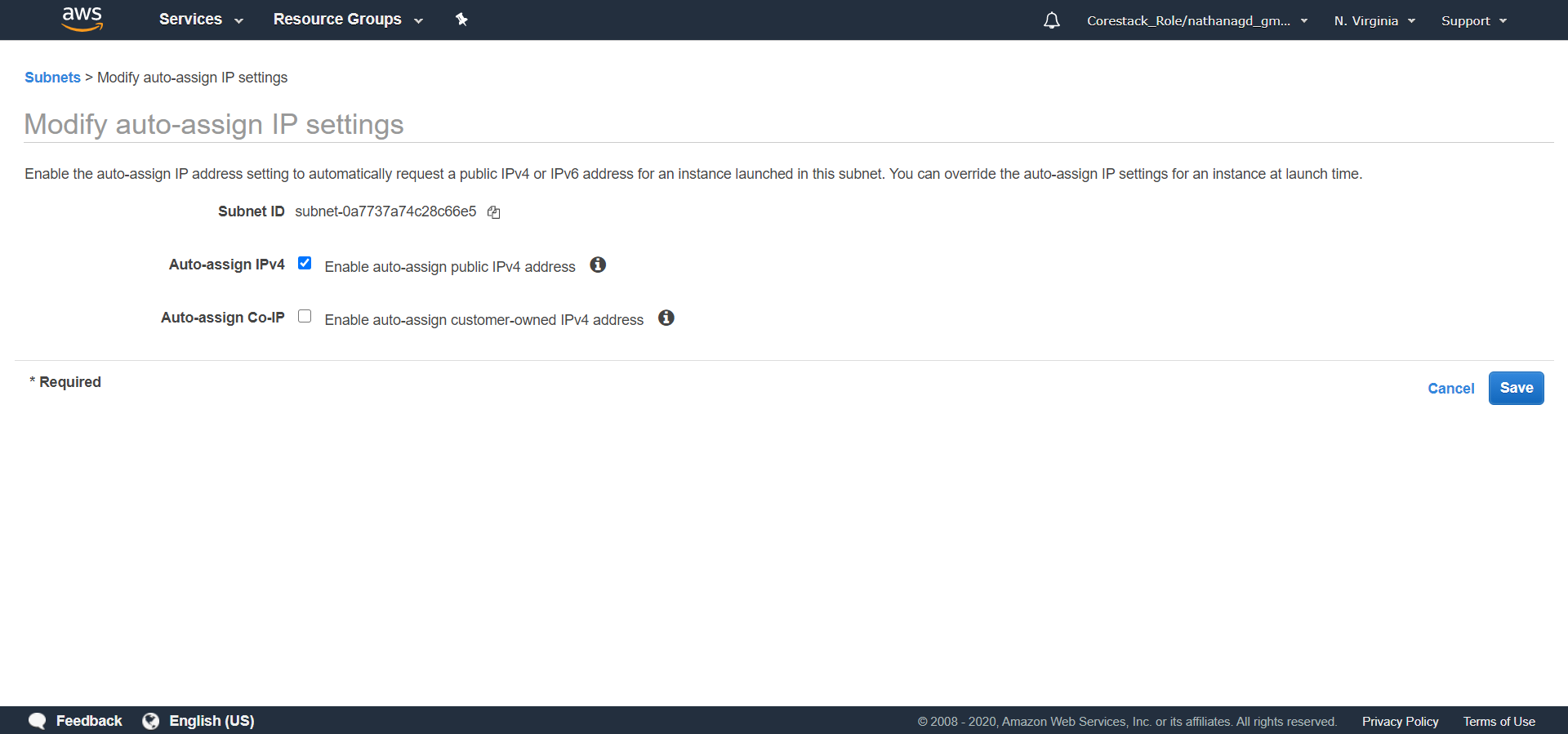
* Now, you can filter by VPC, and check the subnets associated with your custom VPC



* To enable *auto-assign public IP address* for the public subnet, right-click on the public subnet and click on **Modify auto-assign IP settings**

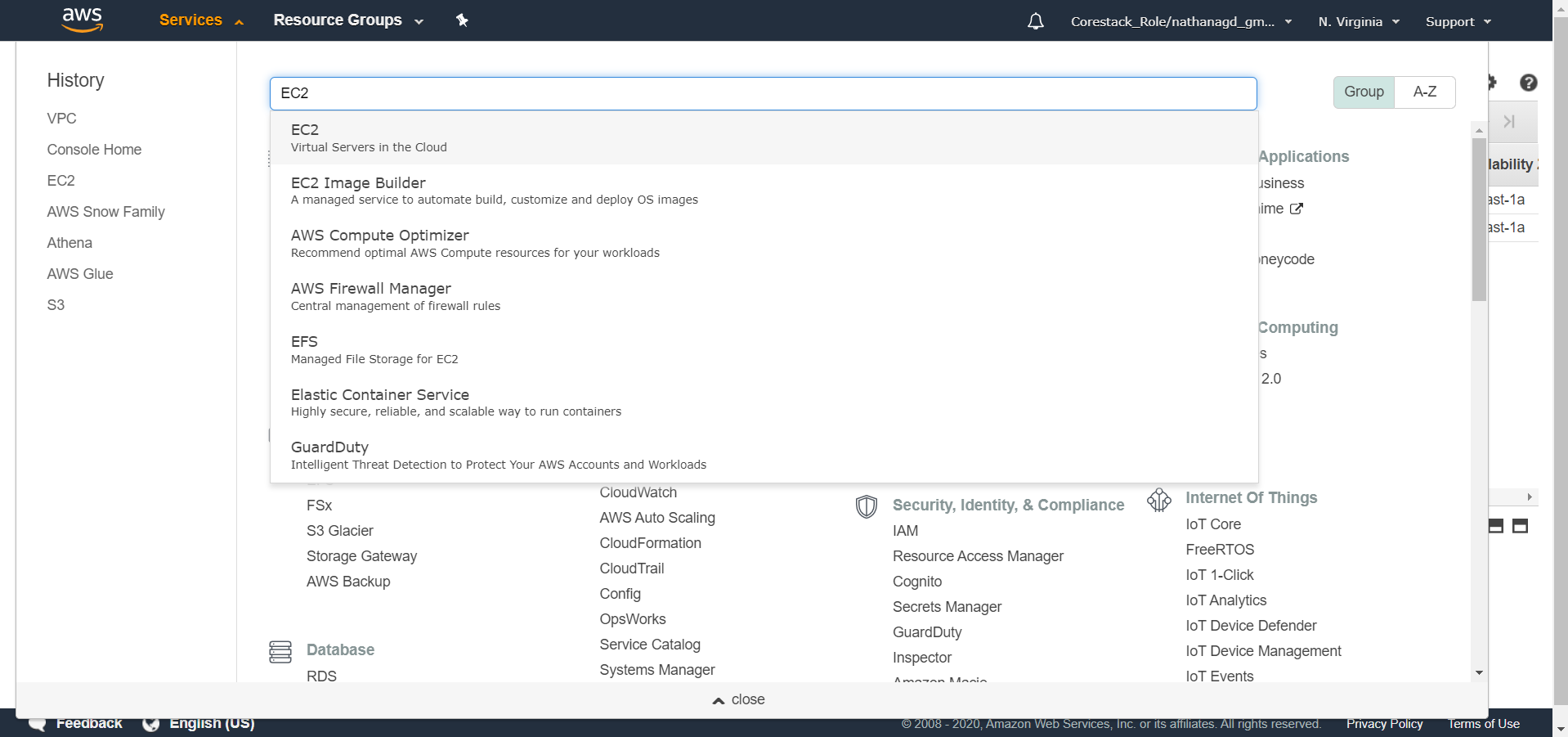


* Check the **Enable auto-assign IPv4 address** box

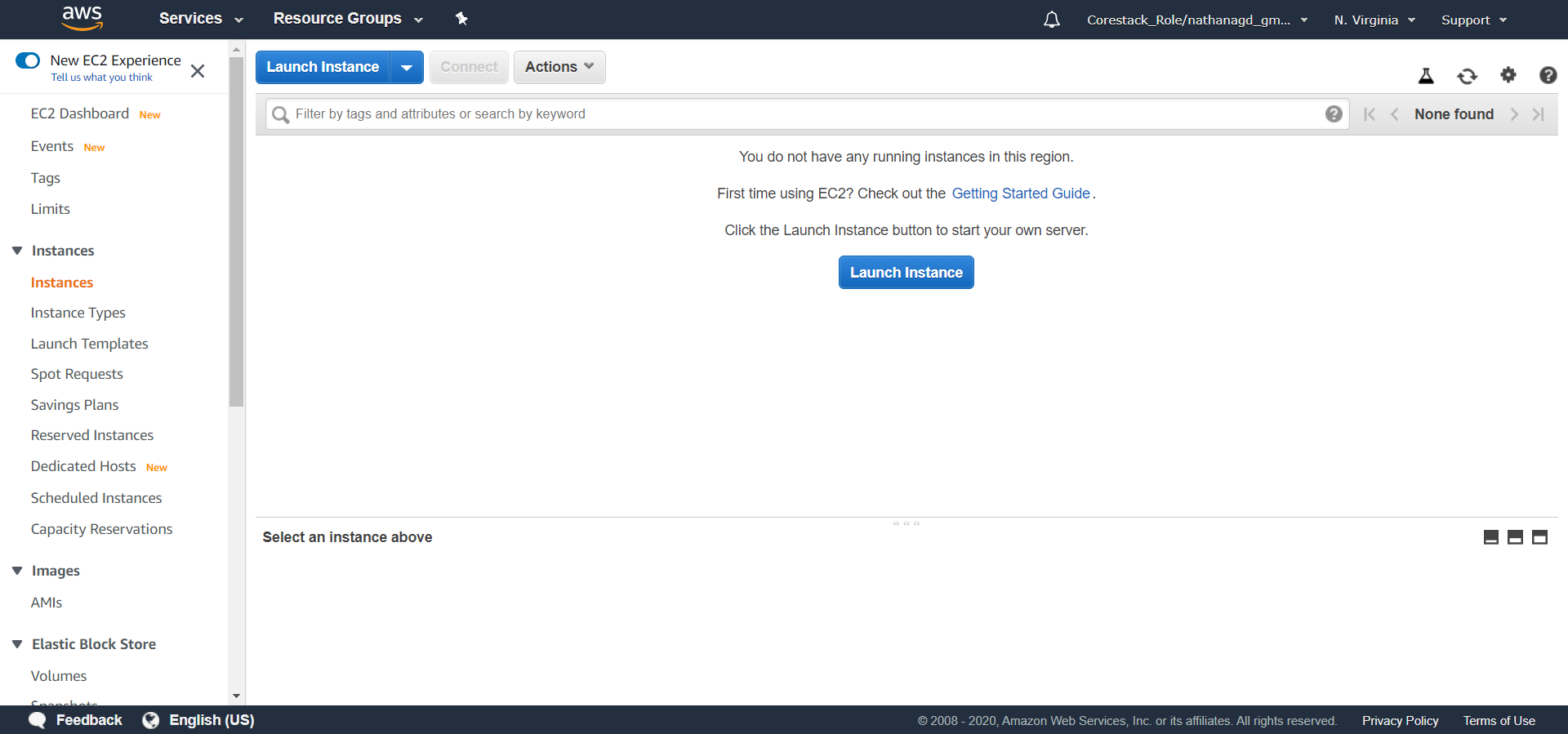


**Step 6.2.3:** Creating a public NAT Instance and giving access to the internet

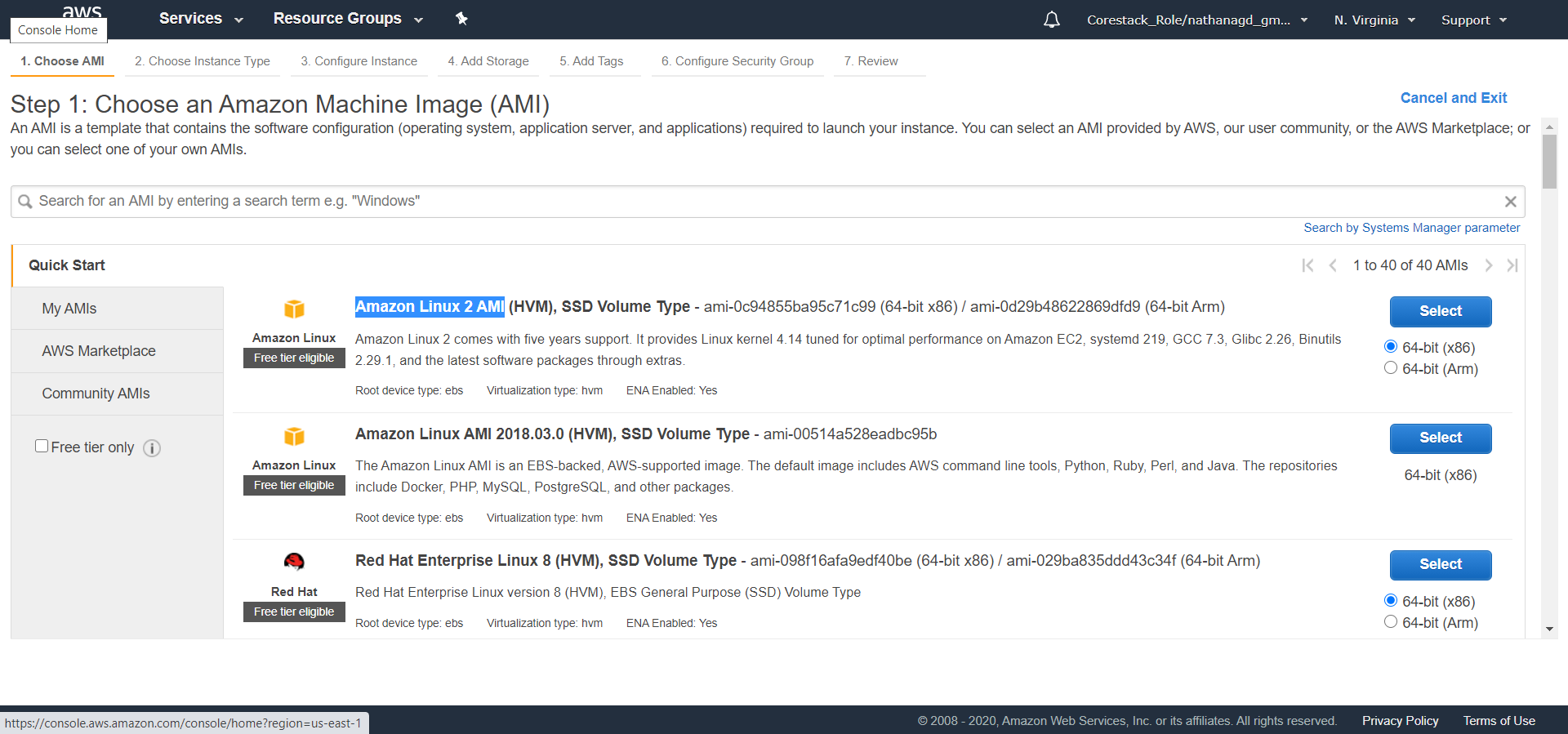
* Let us create a NAT public instance.
* Click on the search bar in **Services**, and search for EC2 and click on it



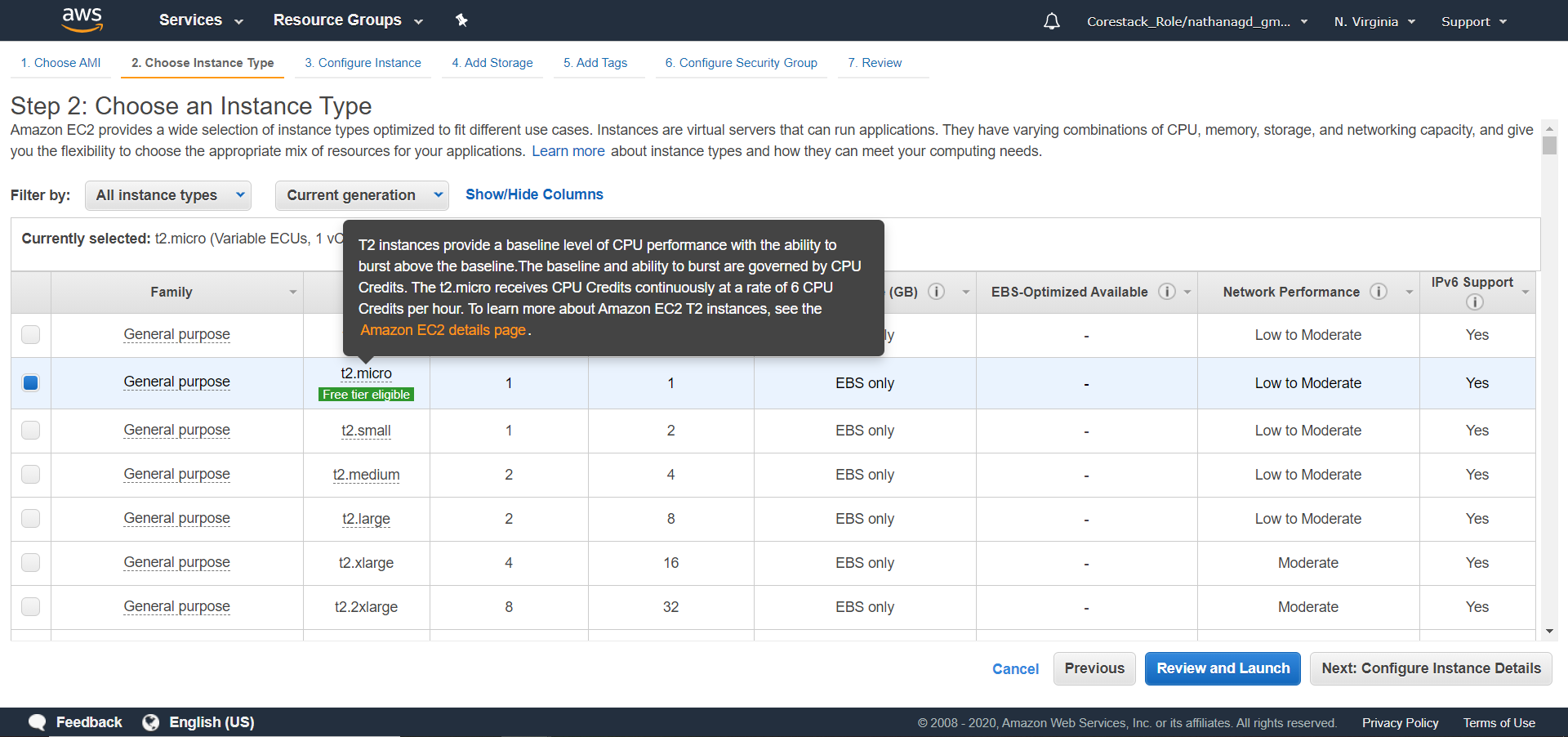
* Click on the **Launch Instance** button



* Select **Amazon Linux 2 AMI**



* Select **t2.micro**

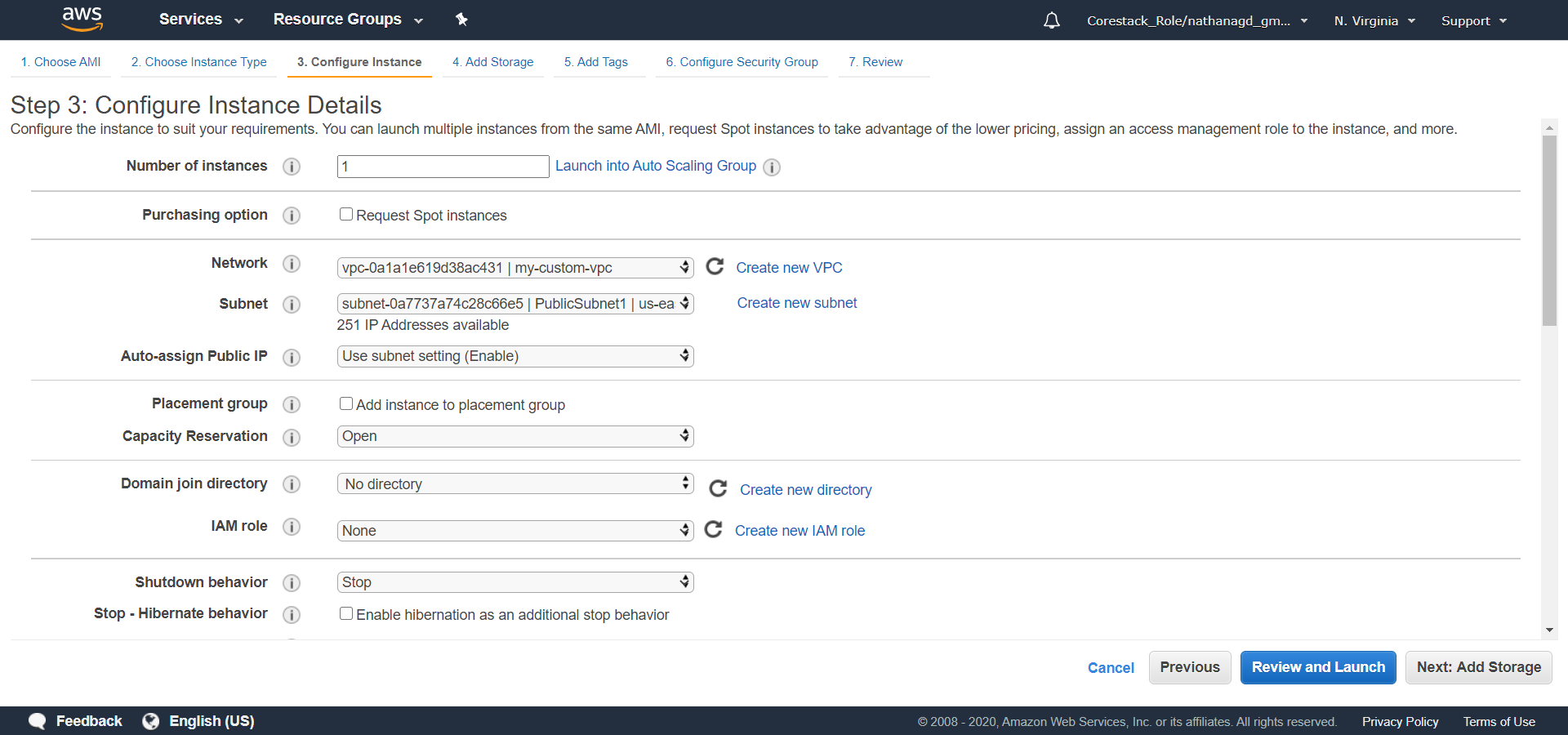


* Under **Configure Instance Details**:

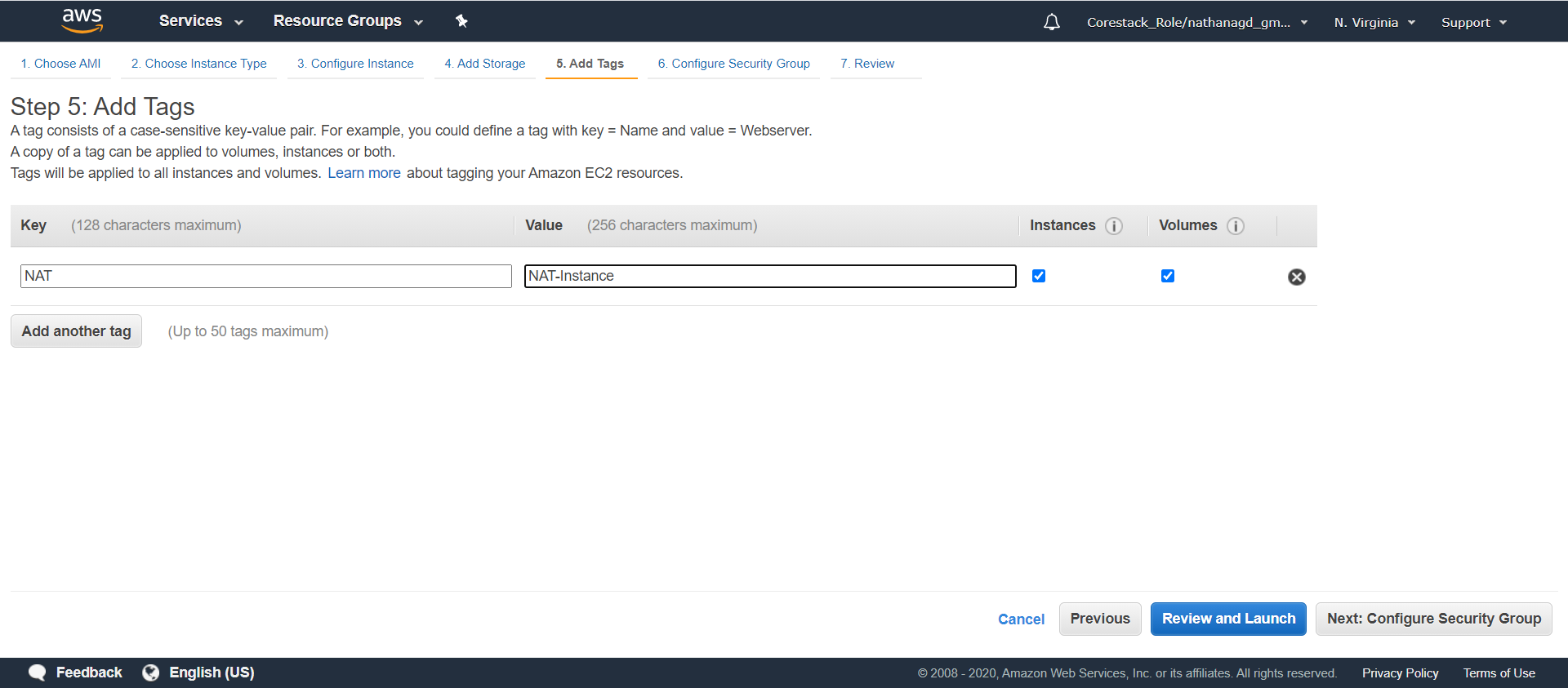
Select **my-custom-vpc in Network**

Select **public subnet in Subnet**

Enable the **Auto-assign Public IP** (This can be changed under the subnet section, like it was done while creating a public subnet)



* Keep the storage as it is
* Add a tag to recognize your NAT instance later



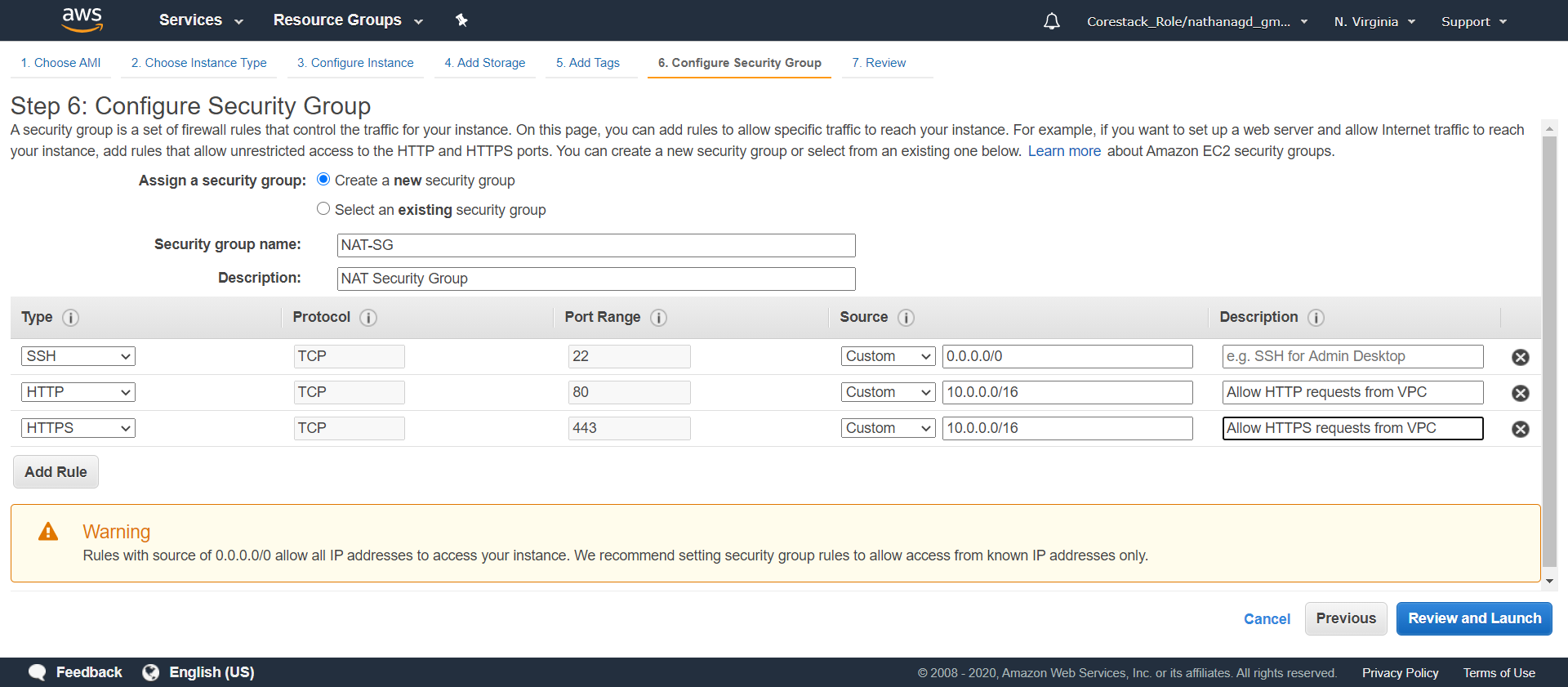
* To configure the security group, you need to:

Name the security group and provide a description

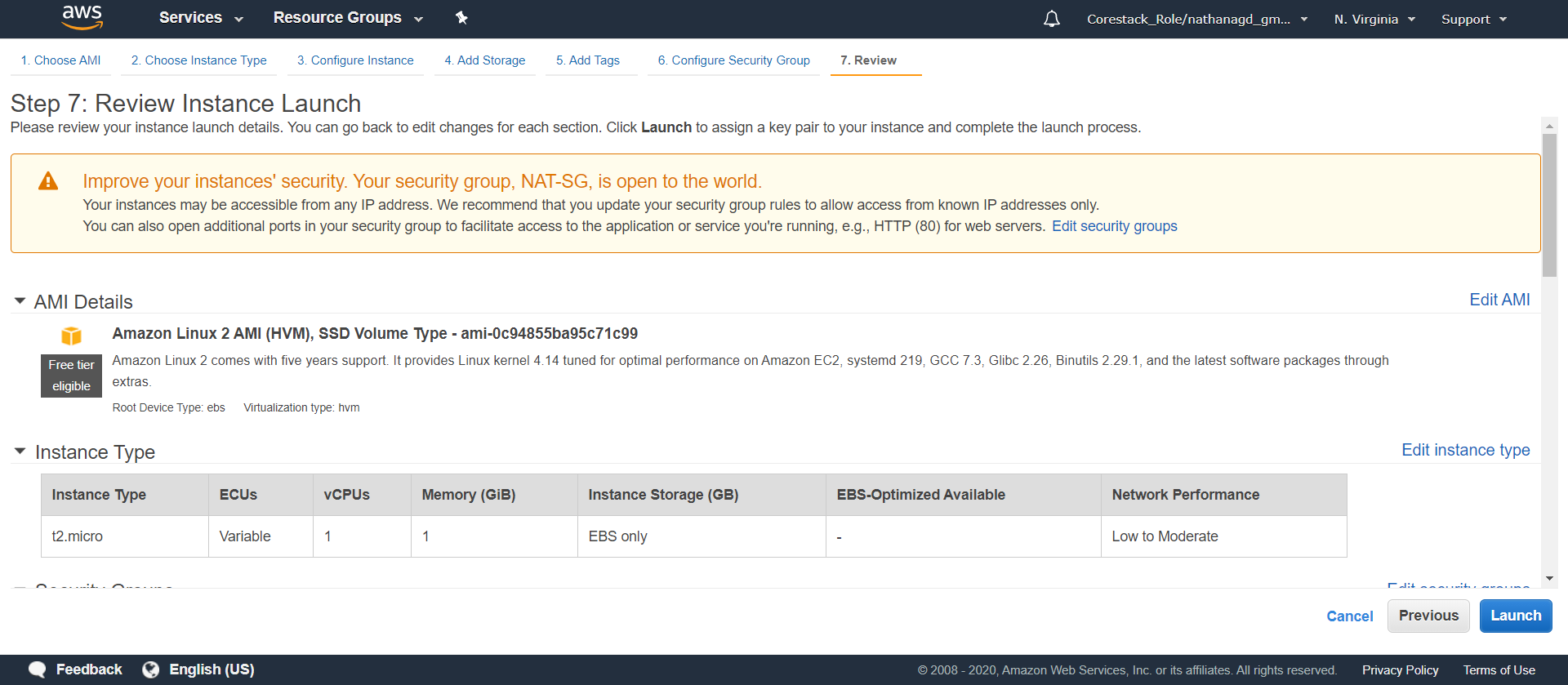
Click on **Add Rule,** and add some rules for the security group

Select **HTTP** under **Type,** give source as 10.0.0.0/16, and add a description

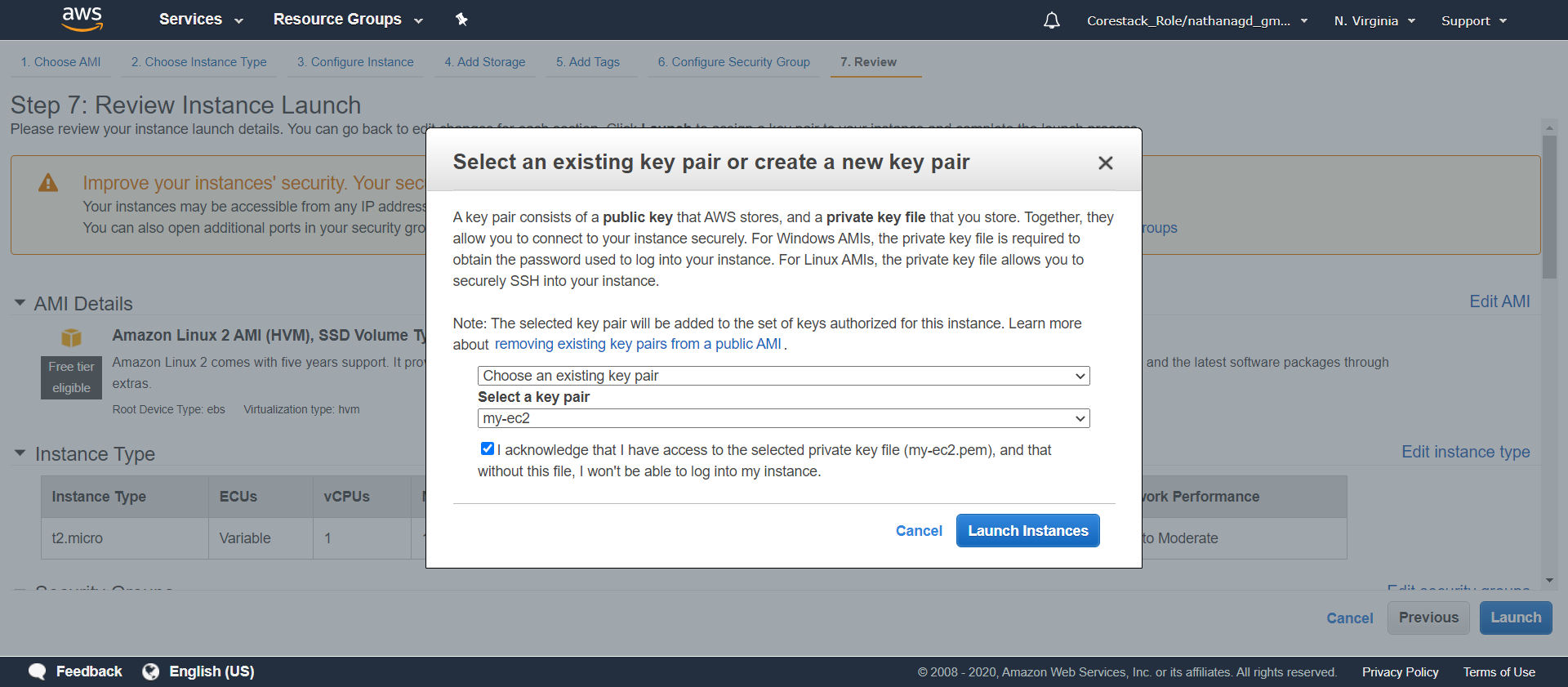
Select **HTTPS** under **Type**, give source as 10.0.0.0/16, and add a description



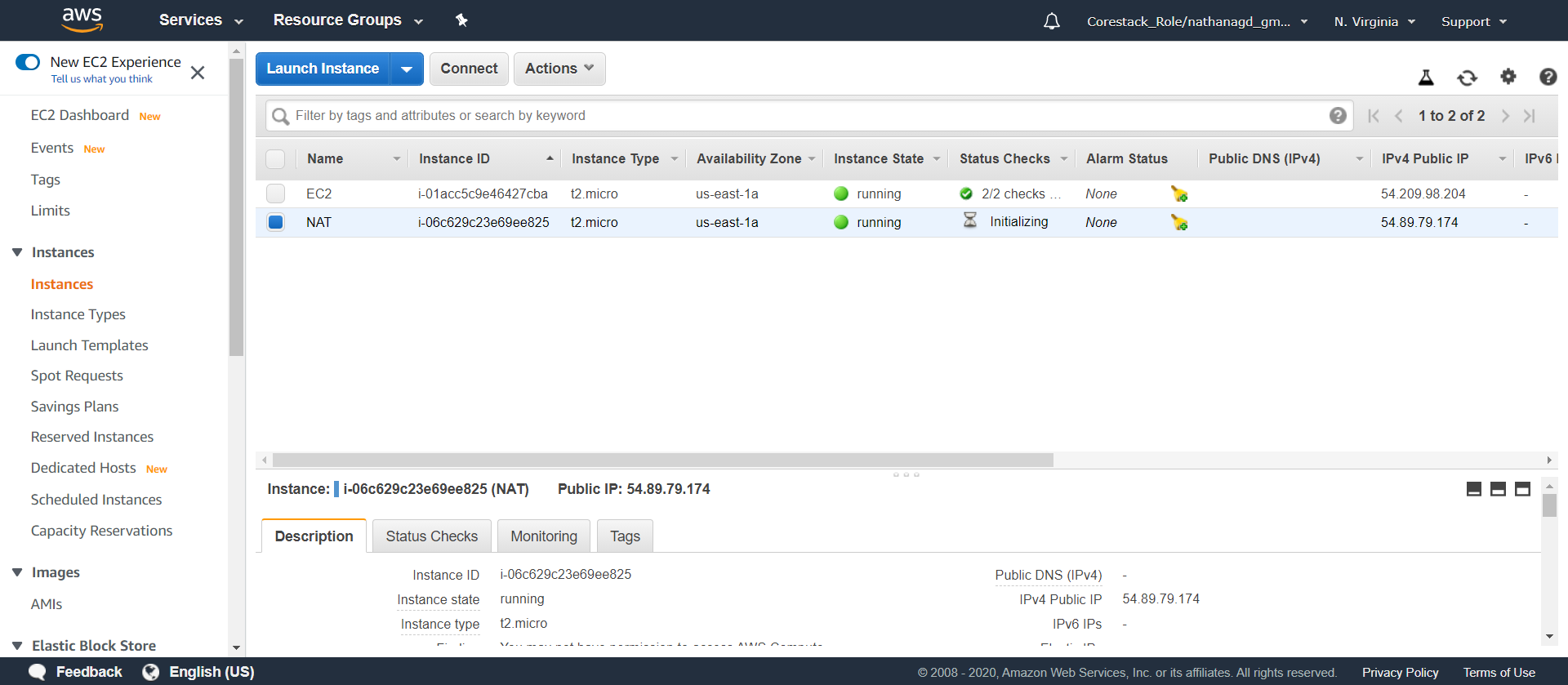
* Click on **Review and Launch**



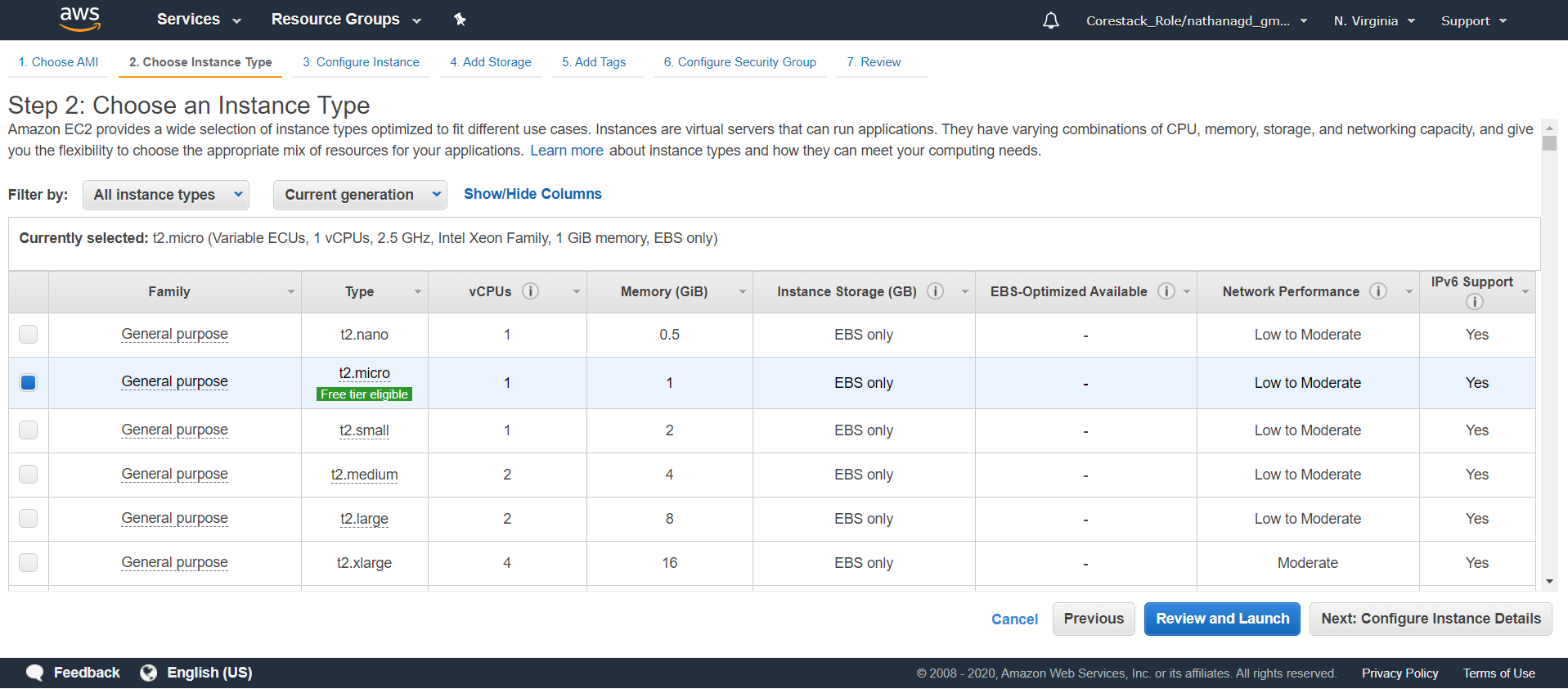
* Click on **Launch**. If this is your first instance, then download and keep the key pair. If not, use the previous instance of which you already have a downloaded key pair



* Click on **Launch Instance**, and your instance will be launched



* Now, let us create a private instance
* Click on **Launch Instance**, select **Amazon Linux 2 AMI (HVM)**, and choose machine type as **t2.micro**

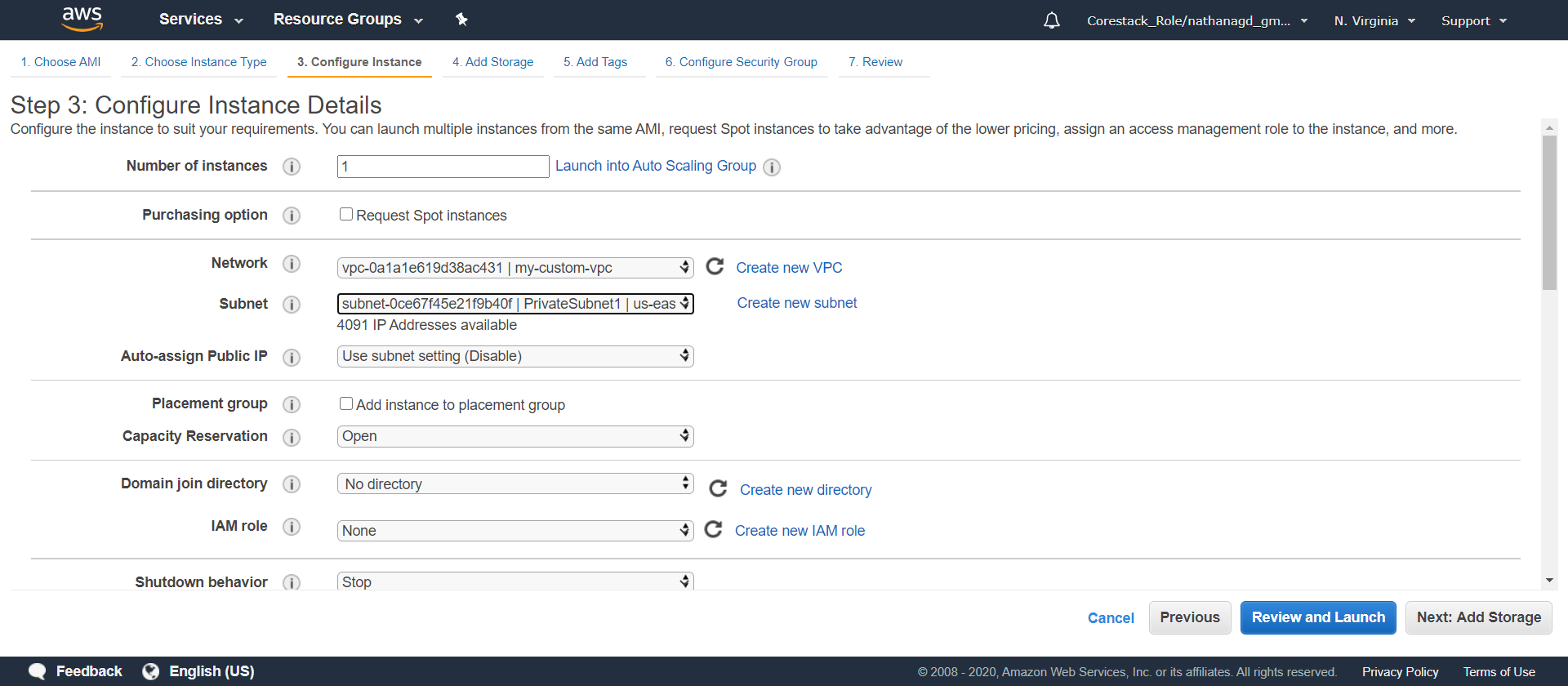


* Under **Configure Instance Details**:

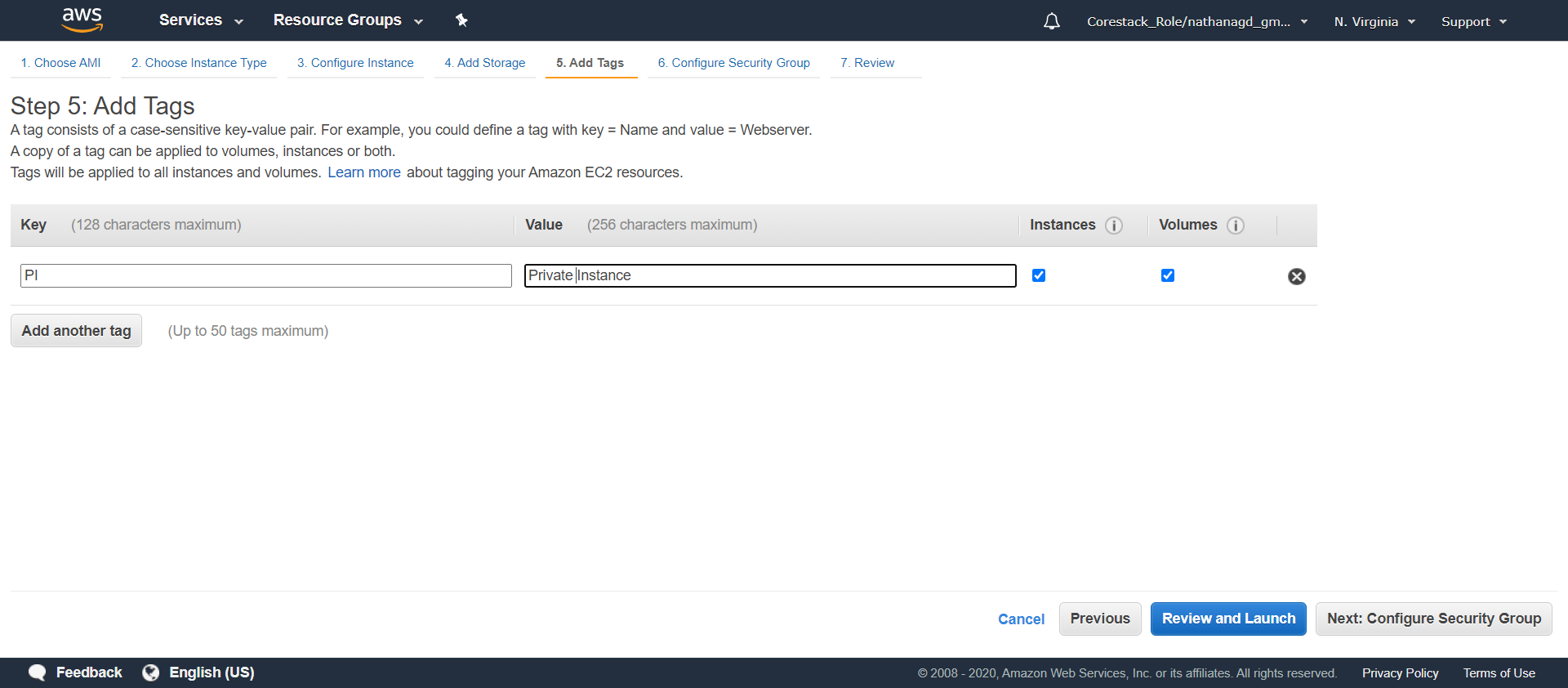
Select **my-custom-vpc** in **Network**

Select **private subnet in Subnet**

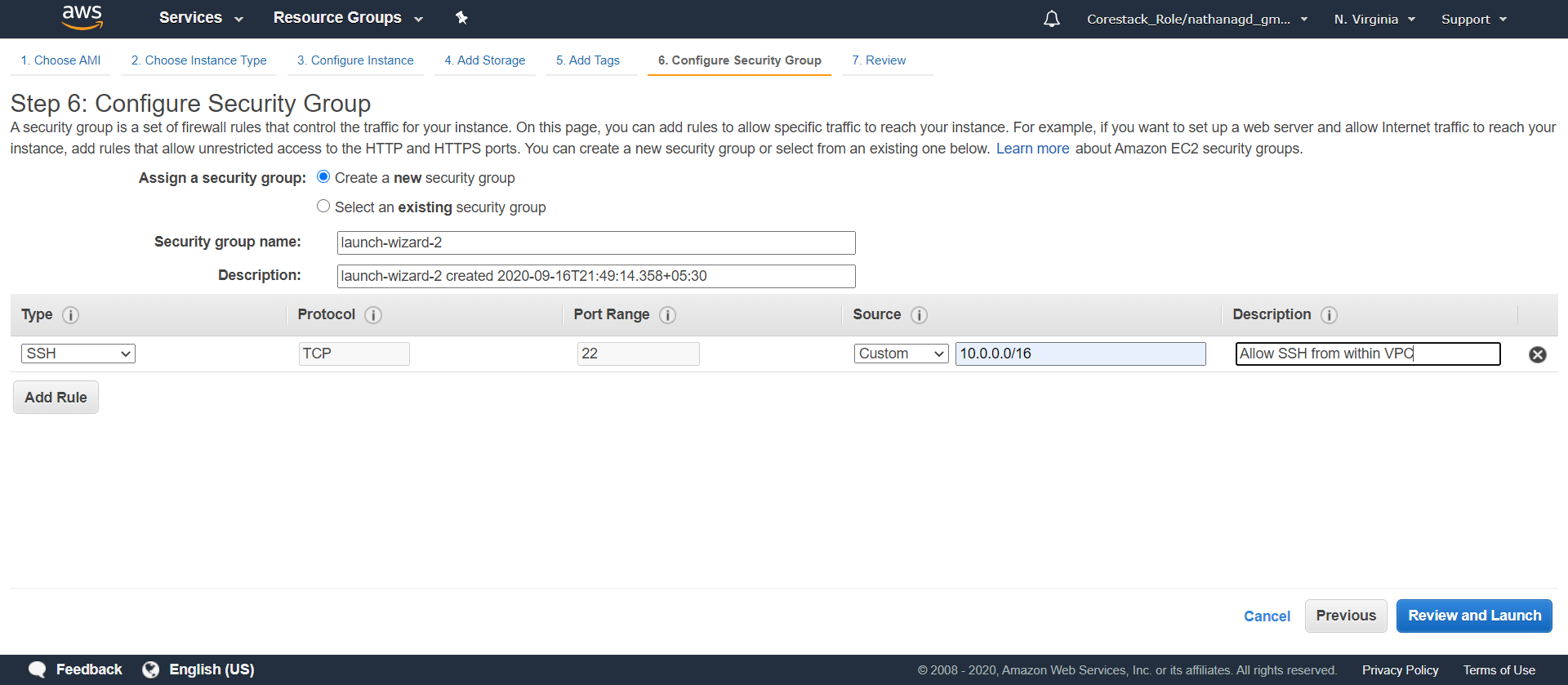
Keep **Auto-assign Public IP** as disabled, as this is a private subnet



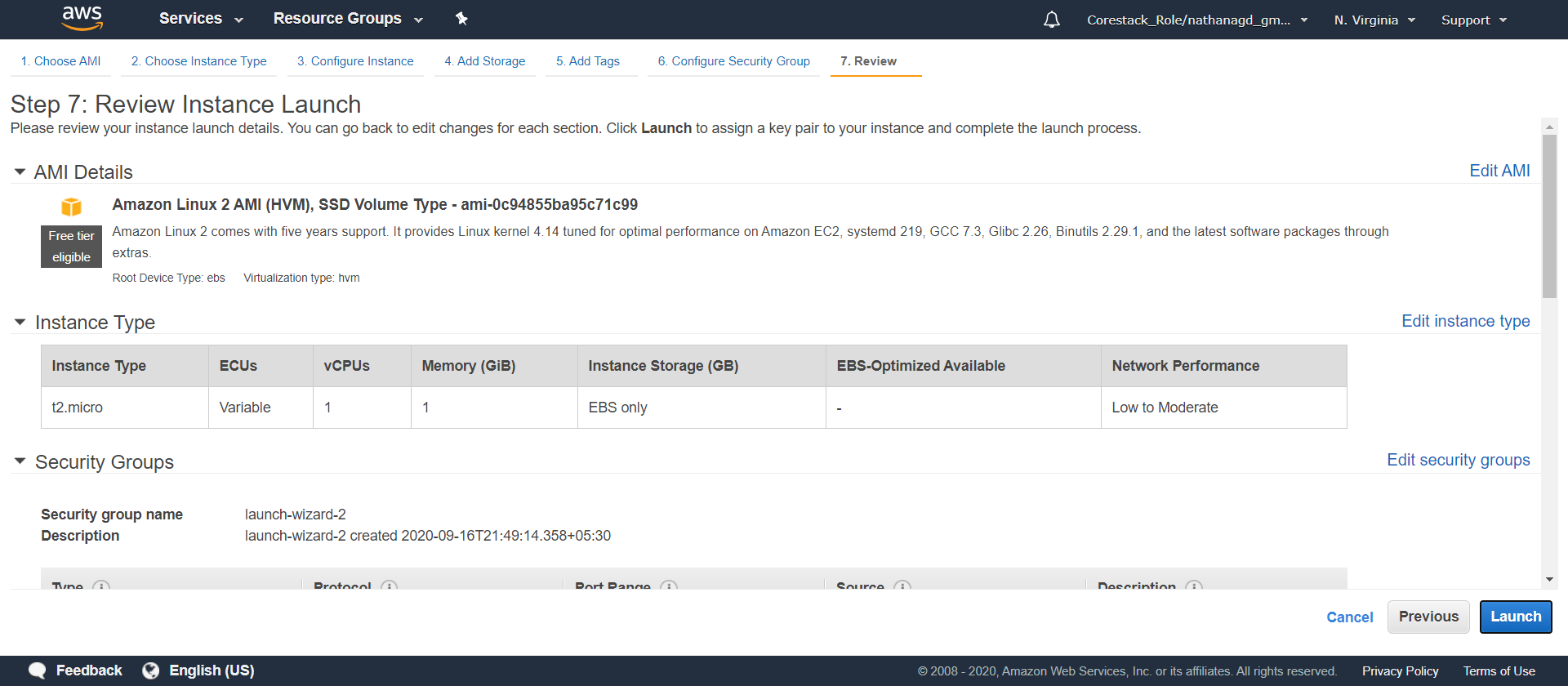
* Keep the storage as it is
* Add a tag to recognize your NAT instance later



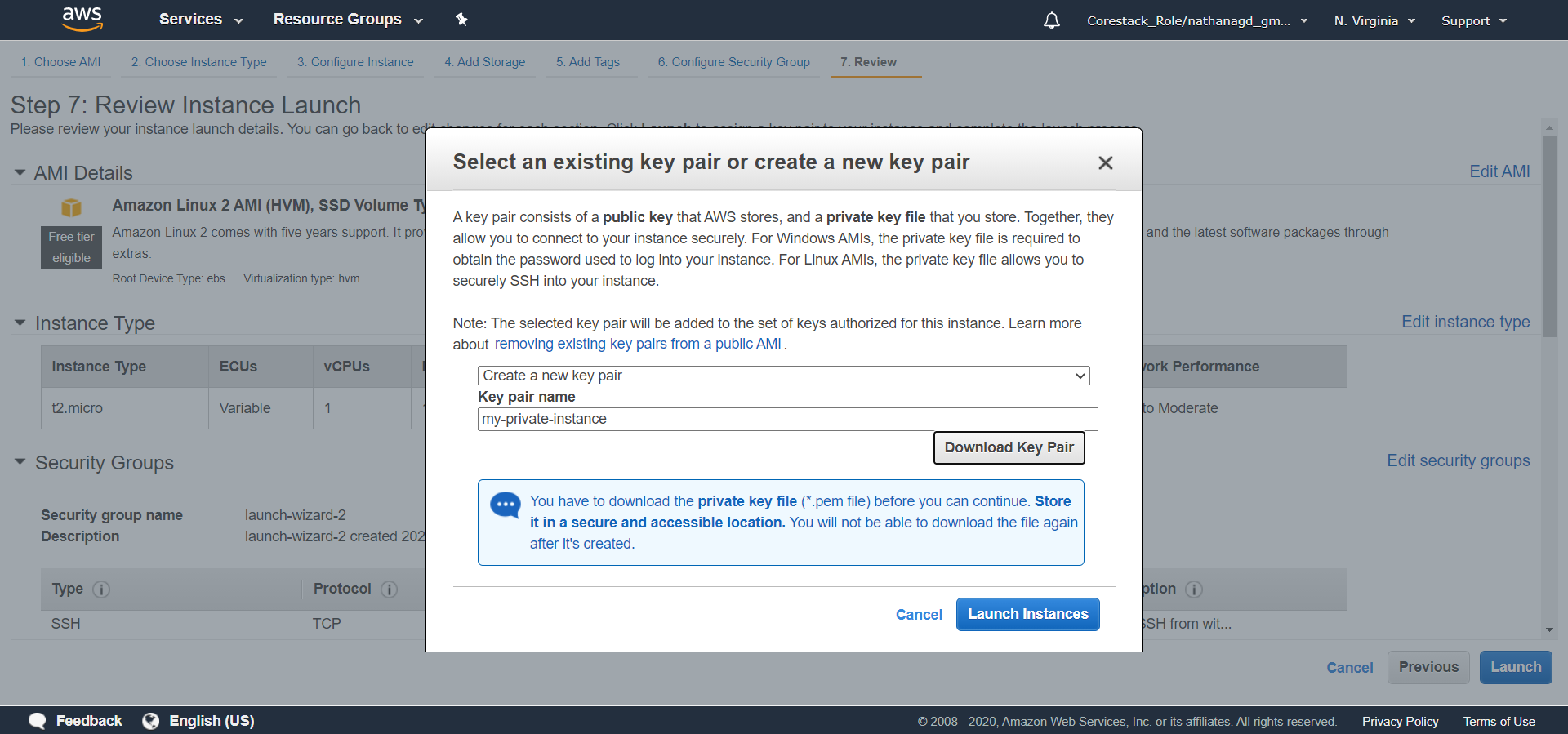
* Now, configure the security group
* Change the SSH Rule. Keep **Source** as 10.0.0.0/16, and add a **Description**



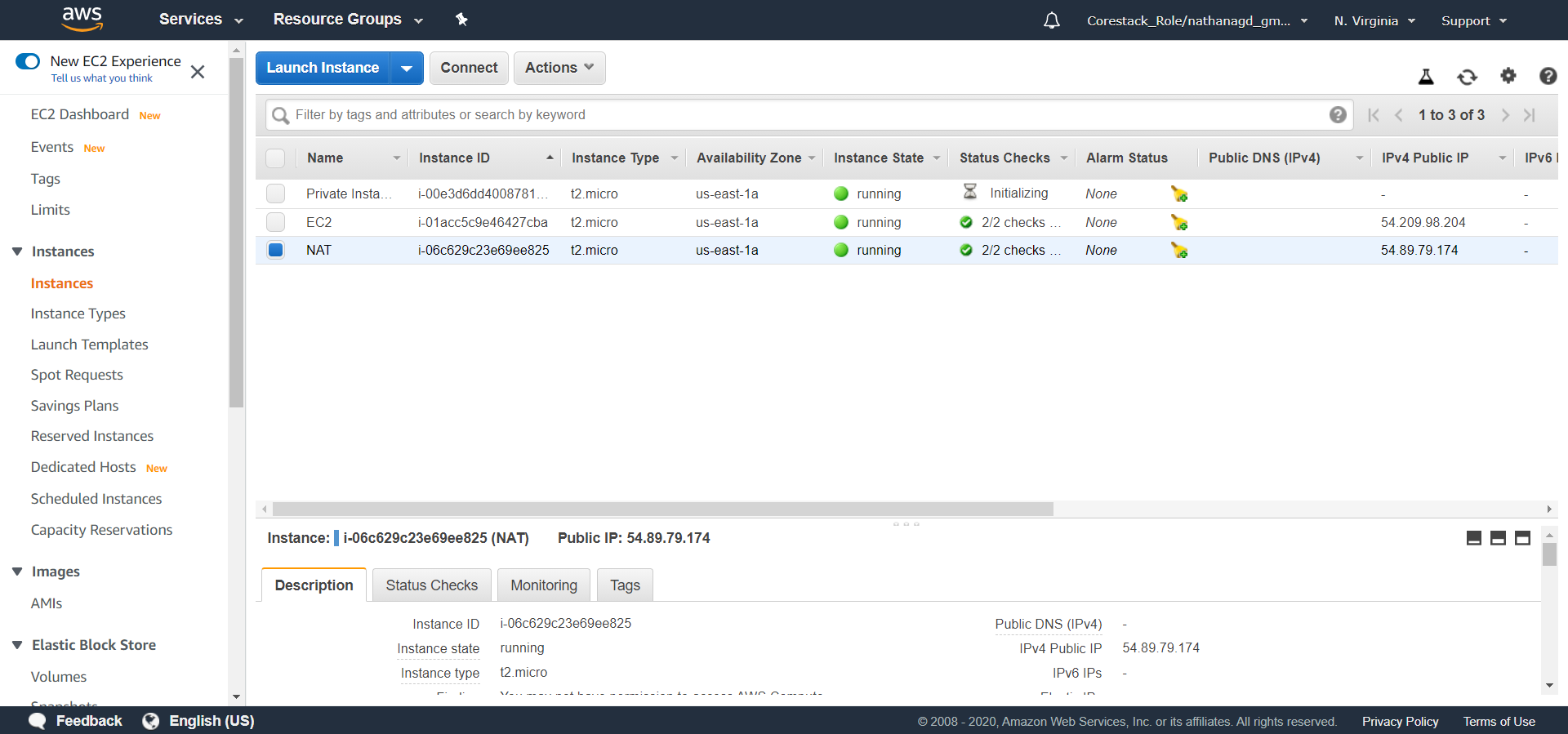
* Click on **Review and Launch**



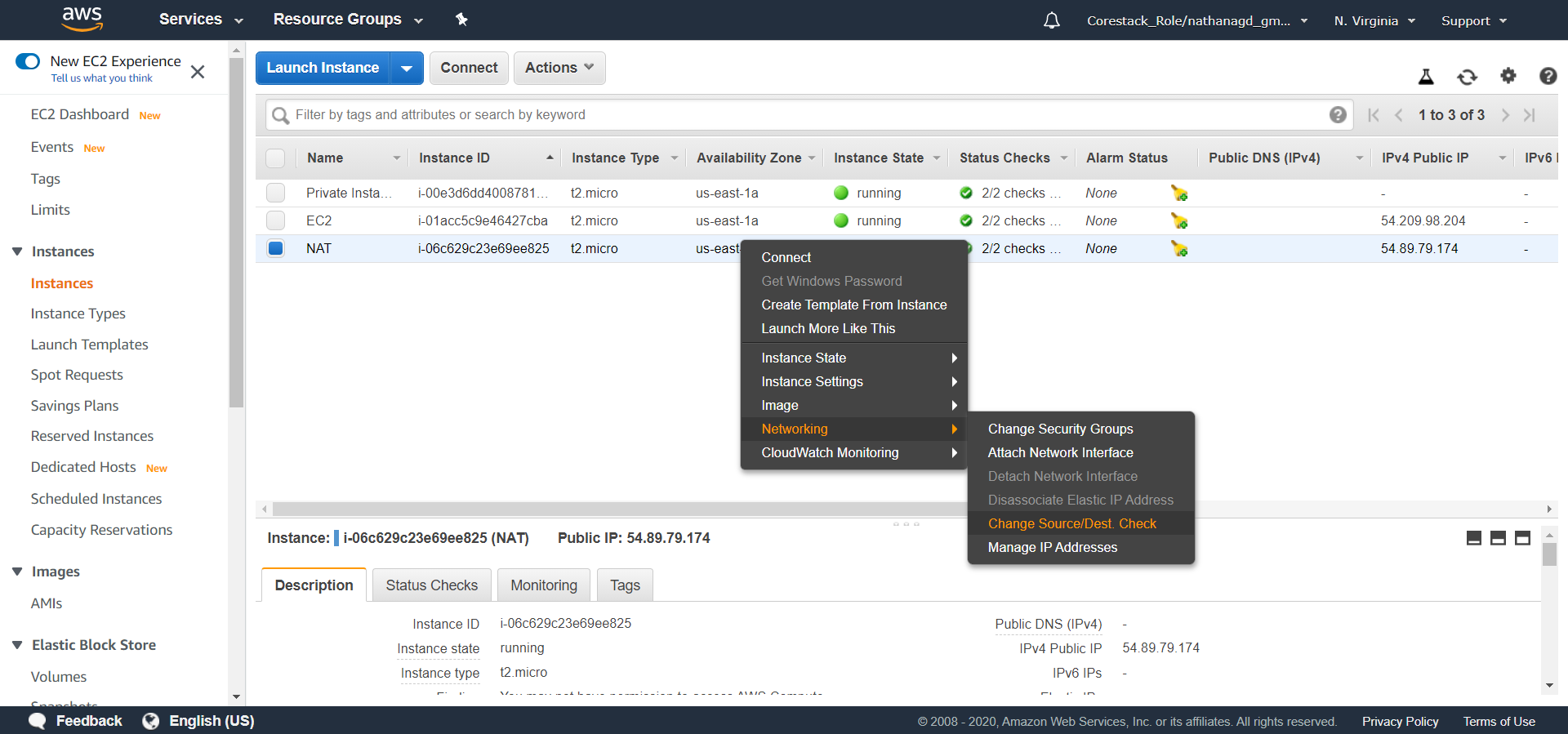
* Click on **Launch**. This time, create a new key pair, as it is going to be specific to the private instance. Also, download and keep it



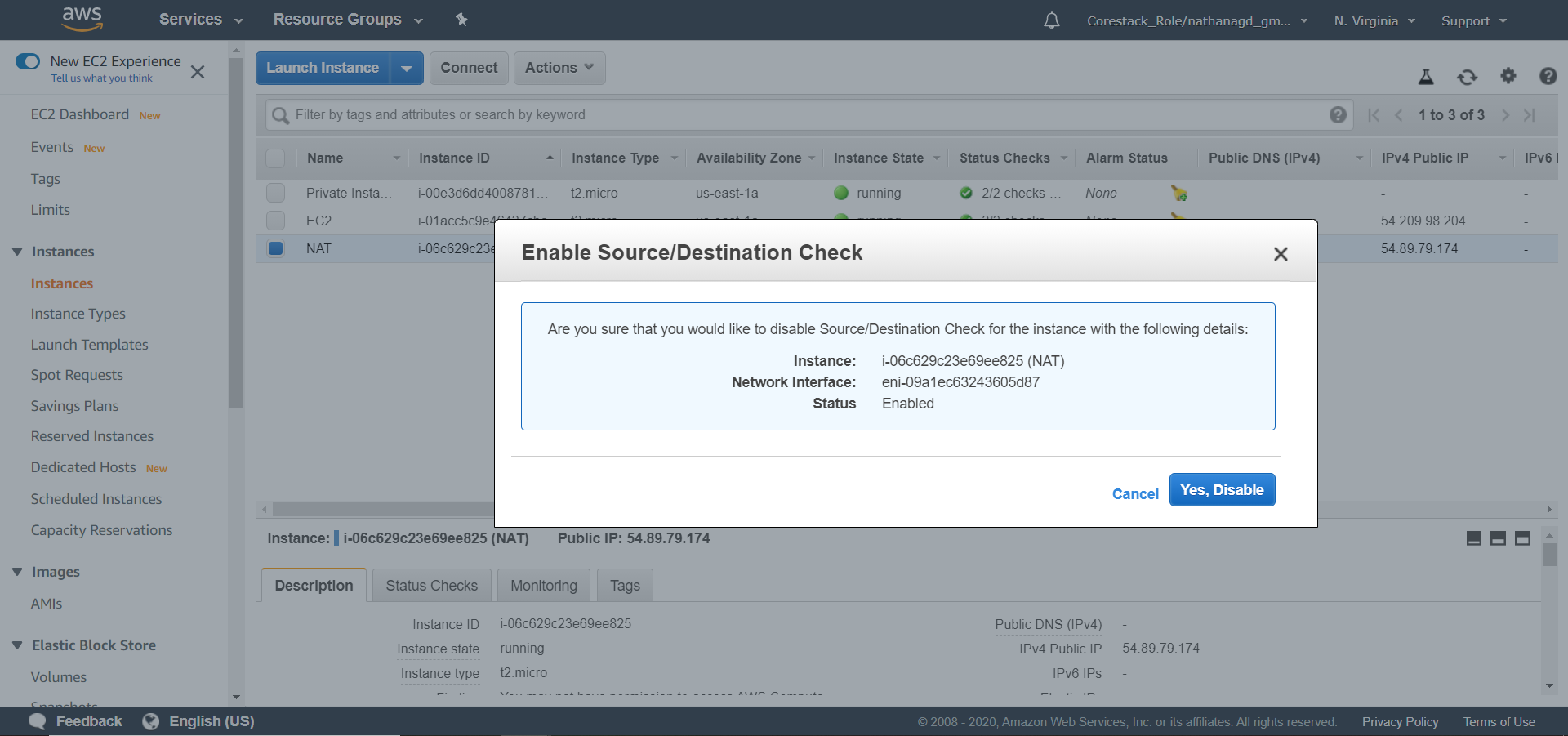
* Click on **Launch Instances**, and your instance will be launched



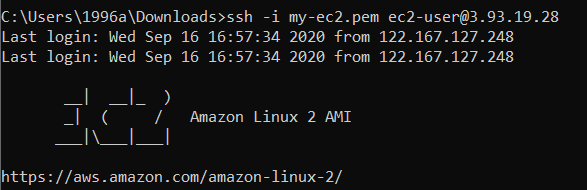
* Disable the source/destination check for this instance
* Right-click on the NAT instance -> Networking -> Change Source/Dest Check



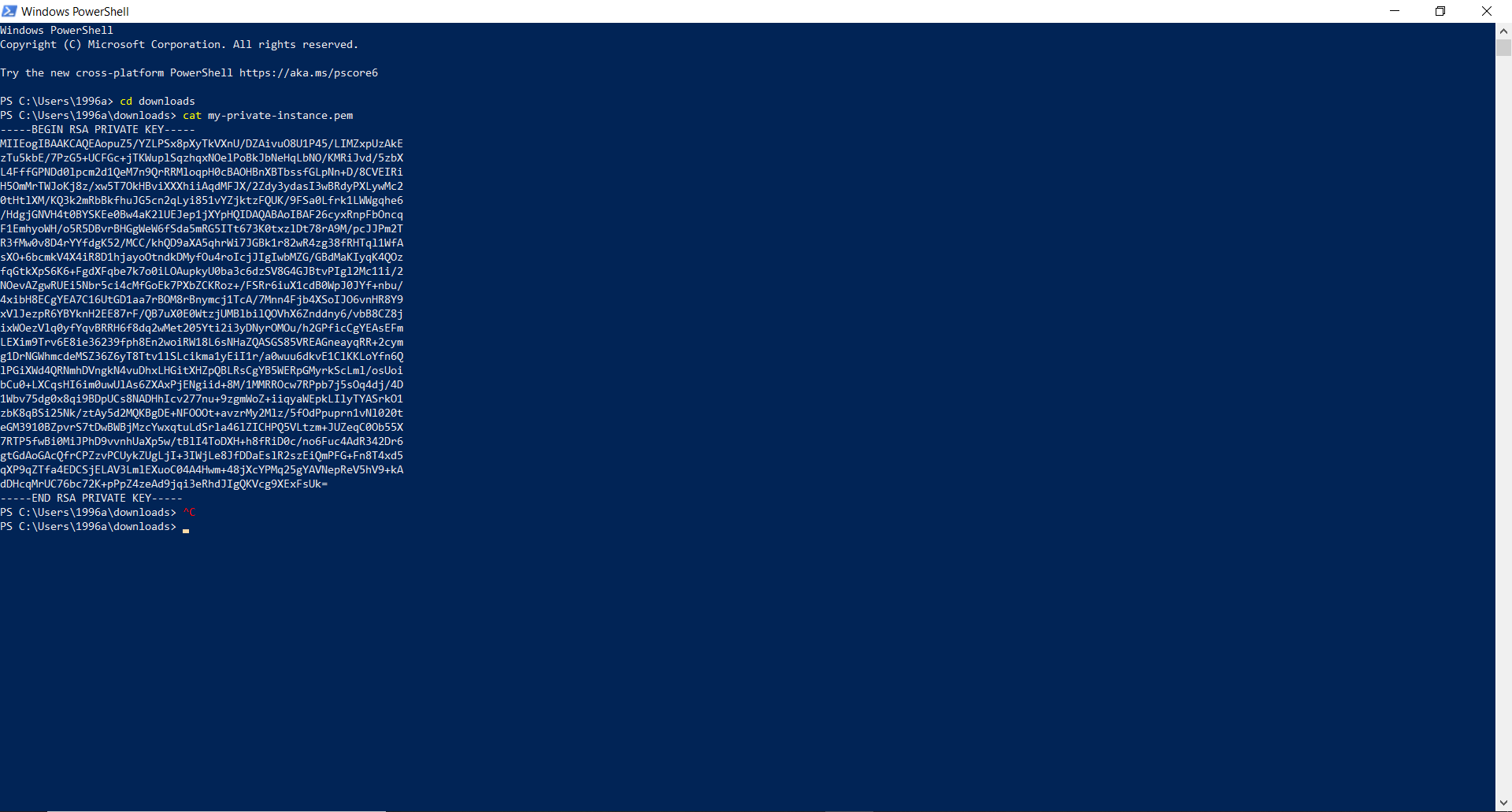
* Click on the **Yes, Disable** button



* You should be able to SSH into your private instance from your public instance.
* Let’s open the terminal, and do this right now.



* Find the private key value.



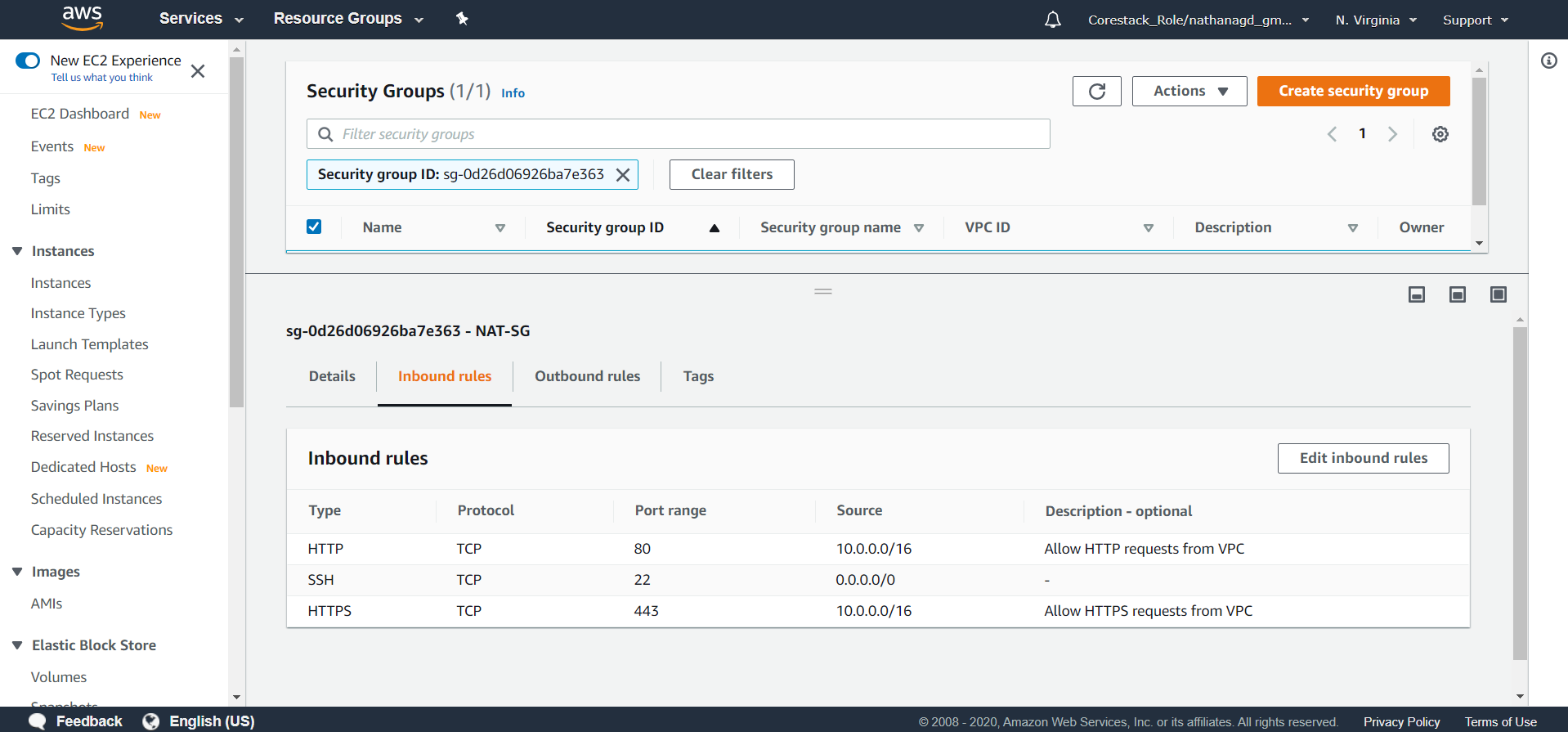
* Add the complete key in a private key using SSH



* You need to set the write permission of the private key file, so use *chmod* to set it.

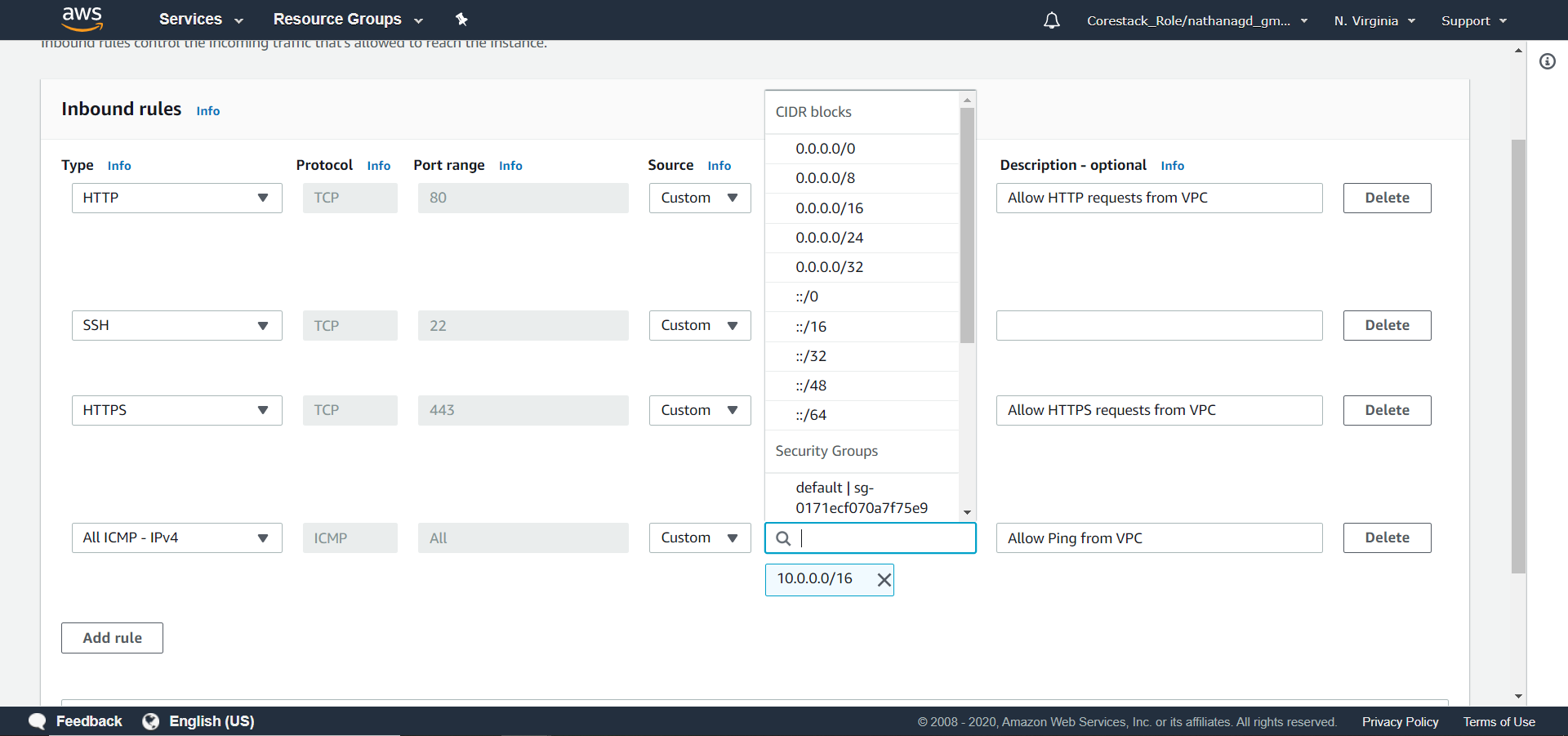


* Now, change the inbound rule for the NAT instance to provide access to the internet
* Go to the AWS NAT Instance, and right-click on the **NAT Instance**

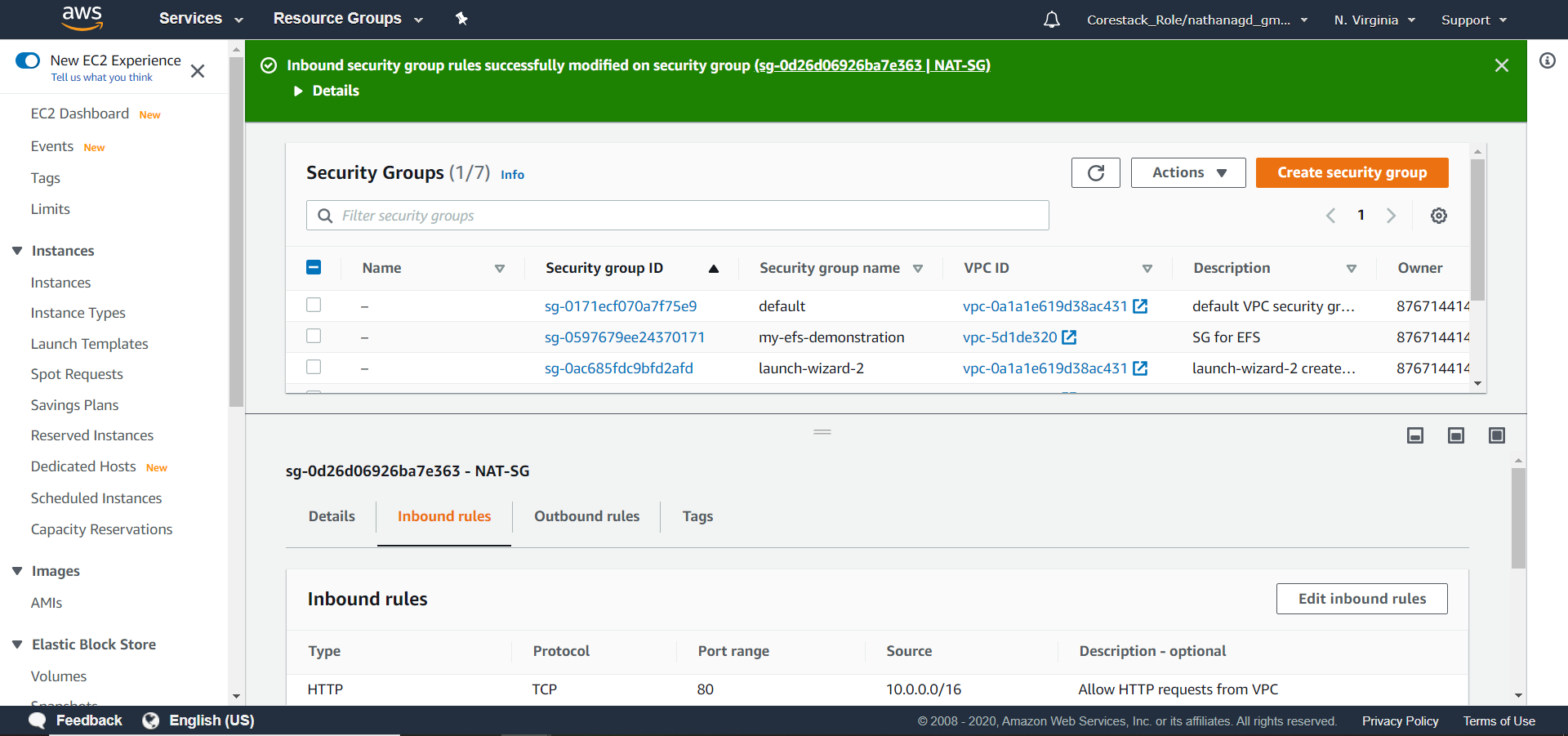


* Click on **Edit Inbound Rules**

Add **ALL ICMP – IPV4**, and add source as 10.0.0.0/16



* Scroll down, and click on **Save**



* You will be able to access the internet using the public instance.