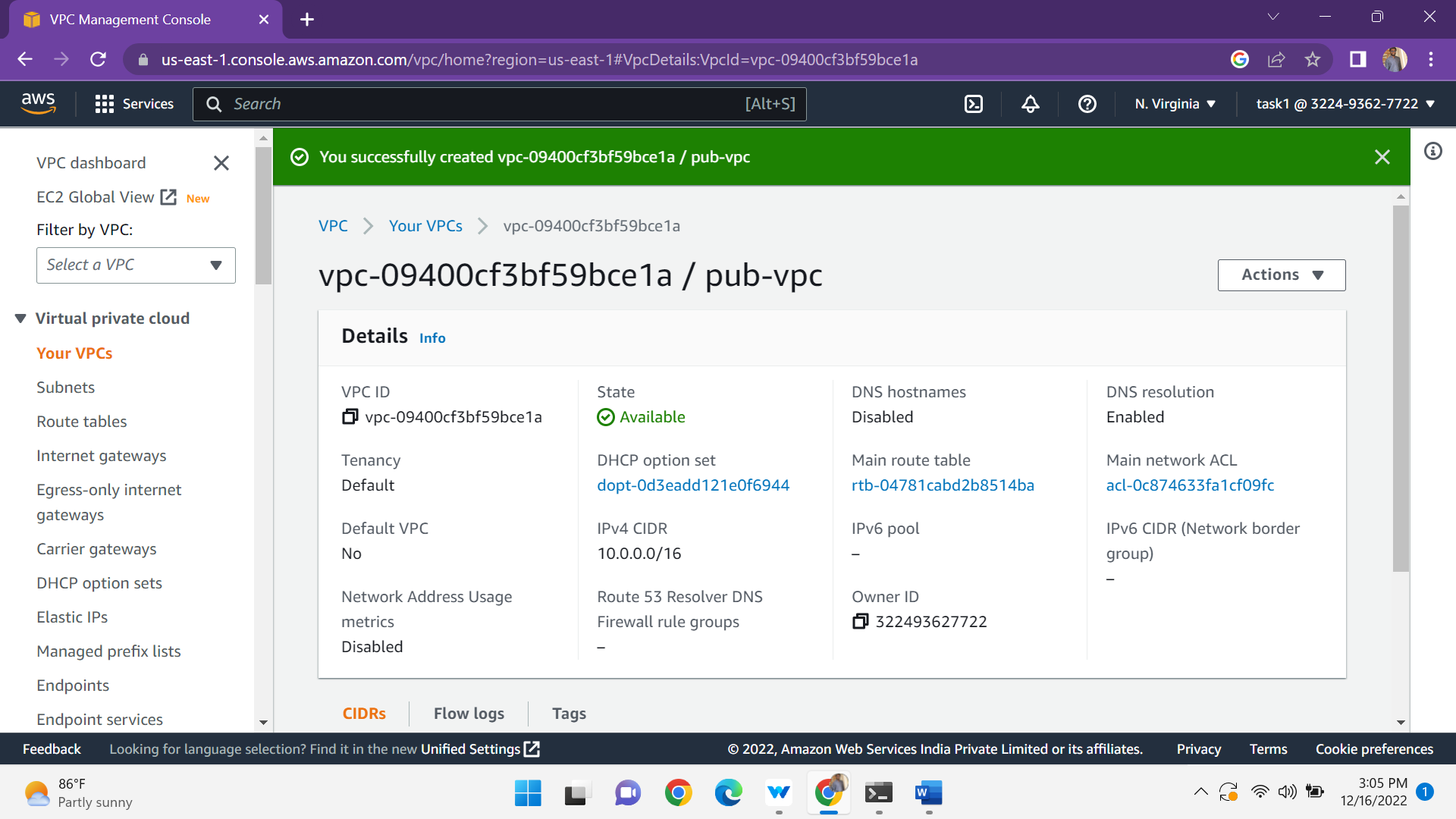
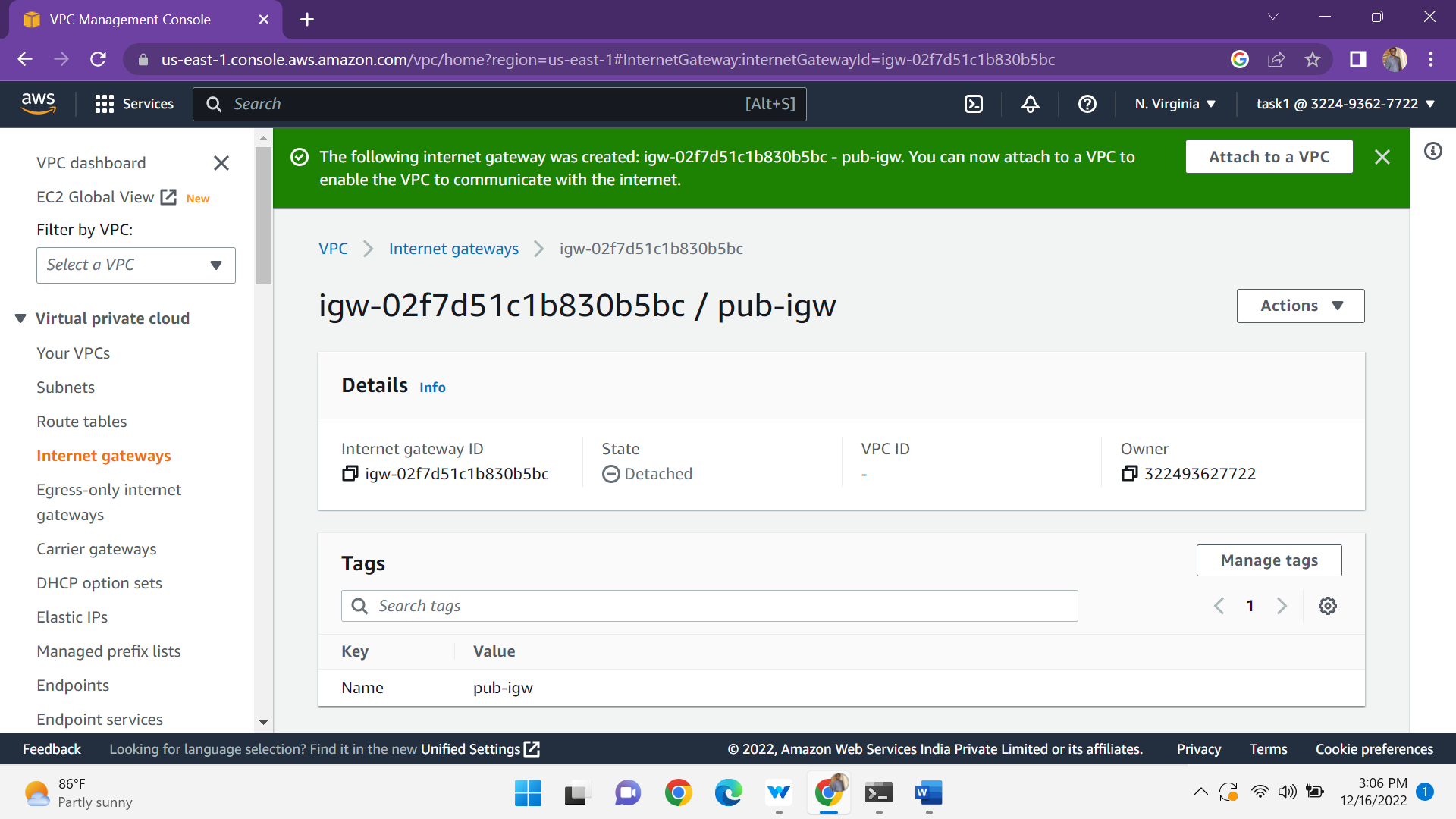
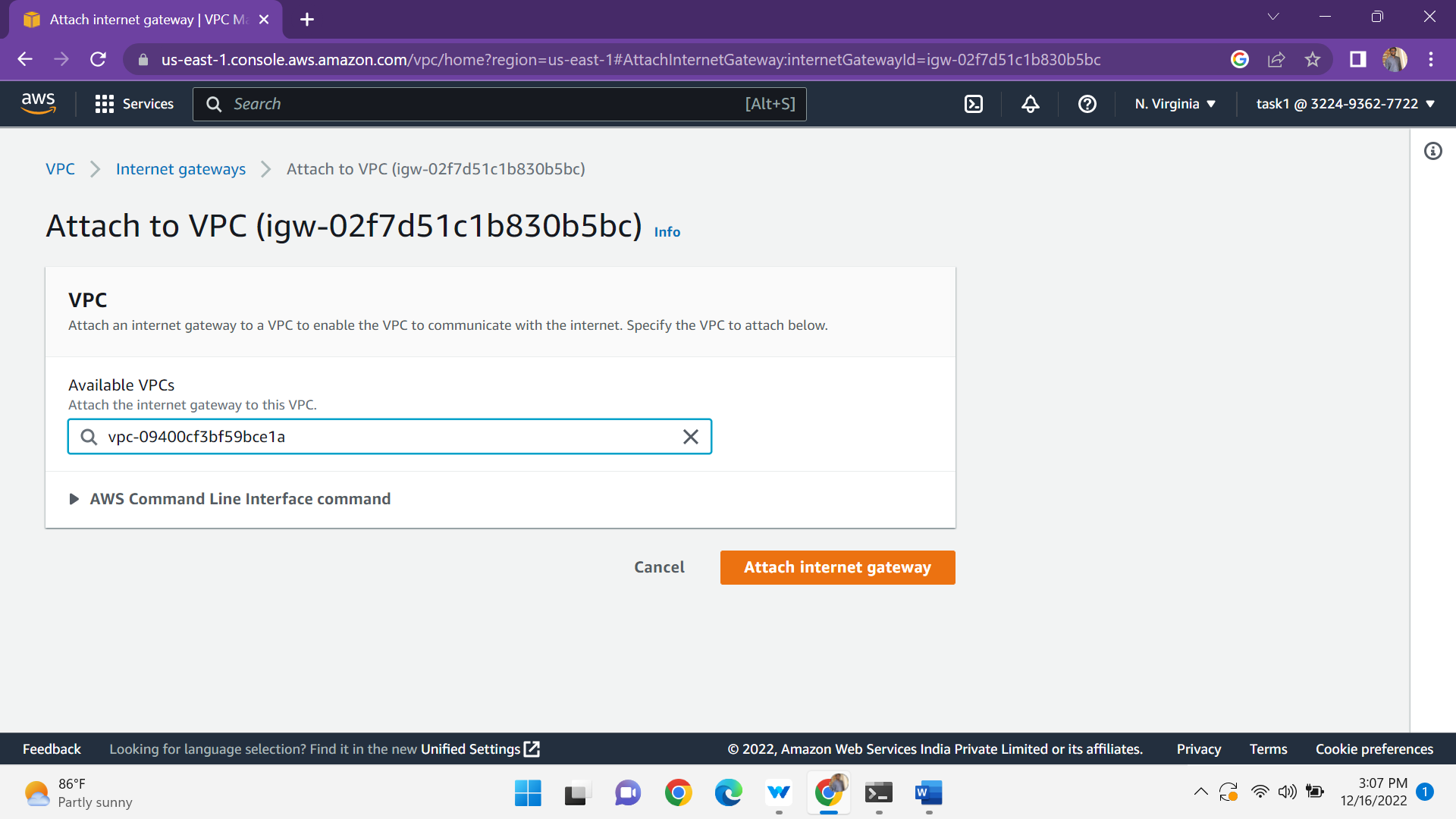
Create a vpc with cidr range: 10.0.0.0/16



And create the internet gateway the internet gateway attach the vpc to the internet gateway

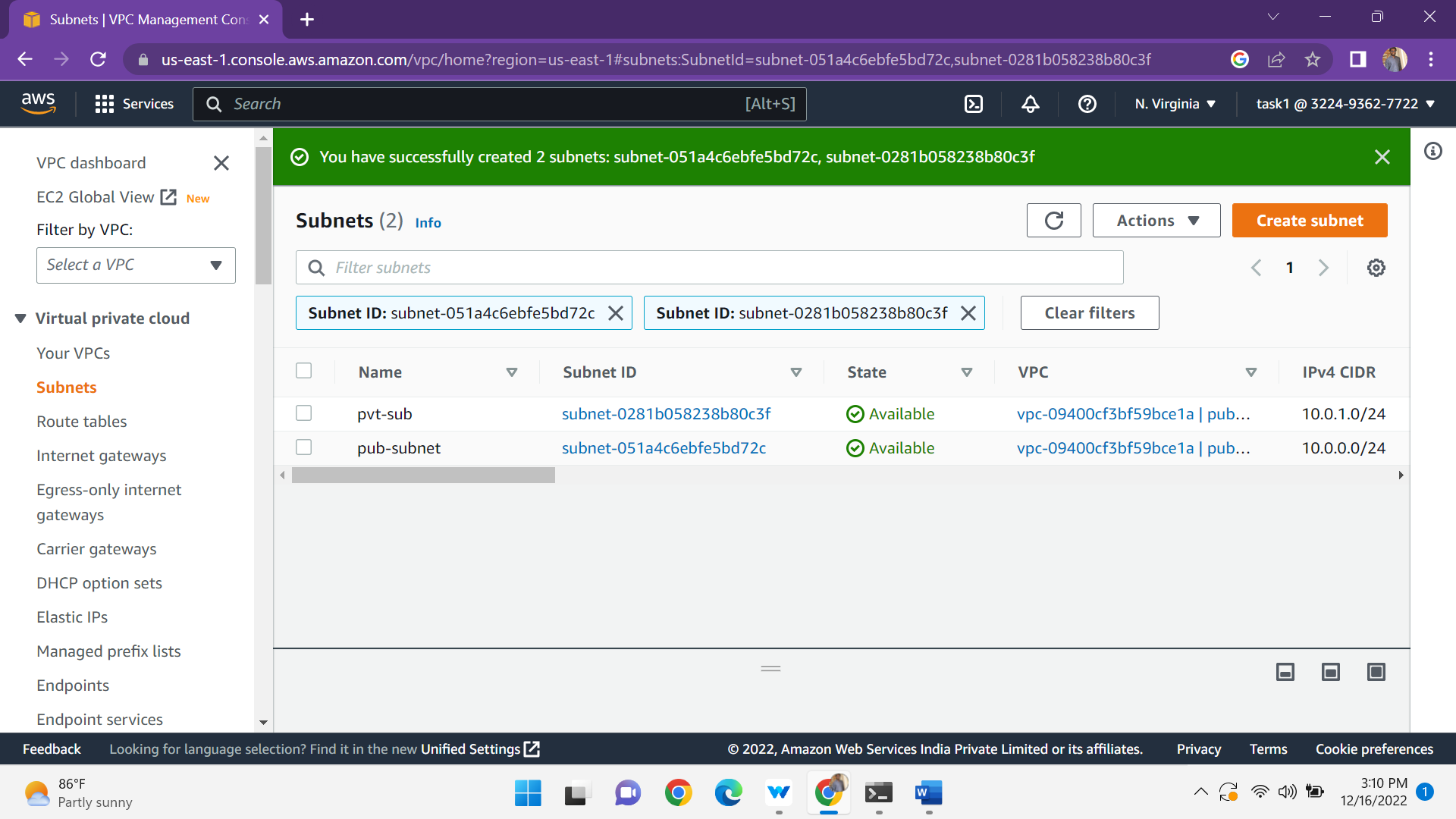




And then create a two subnets one is private and another one is public subnet with the cidr ranges is

Pub cidr: 10.0.0.0/24

Pvt cidr : 10.0.1.0/24



Create a route table:

A route table contains set of rules, called routes that determine where network traffic from your subnet or gateway is directed.

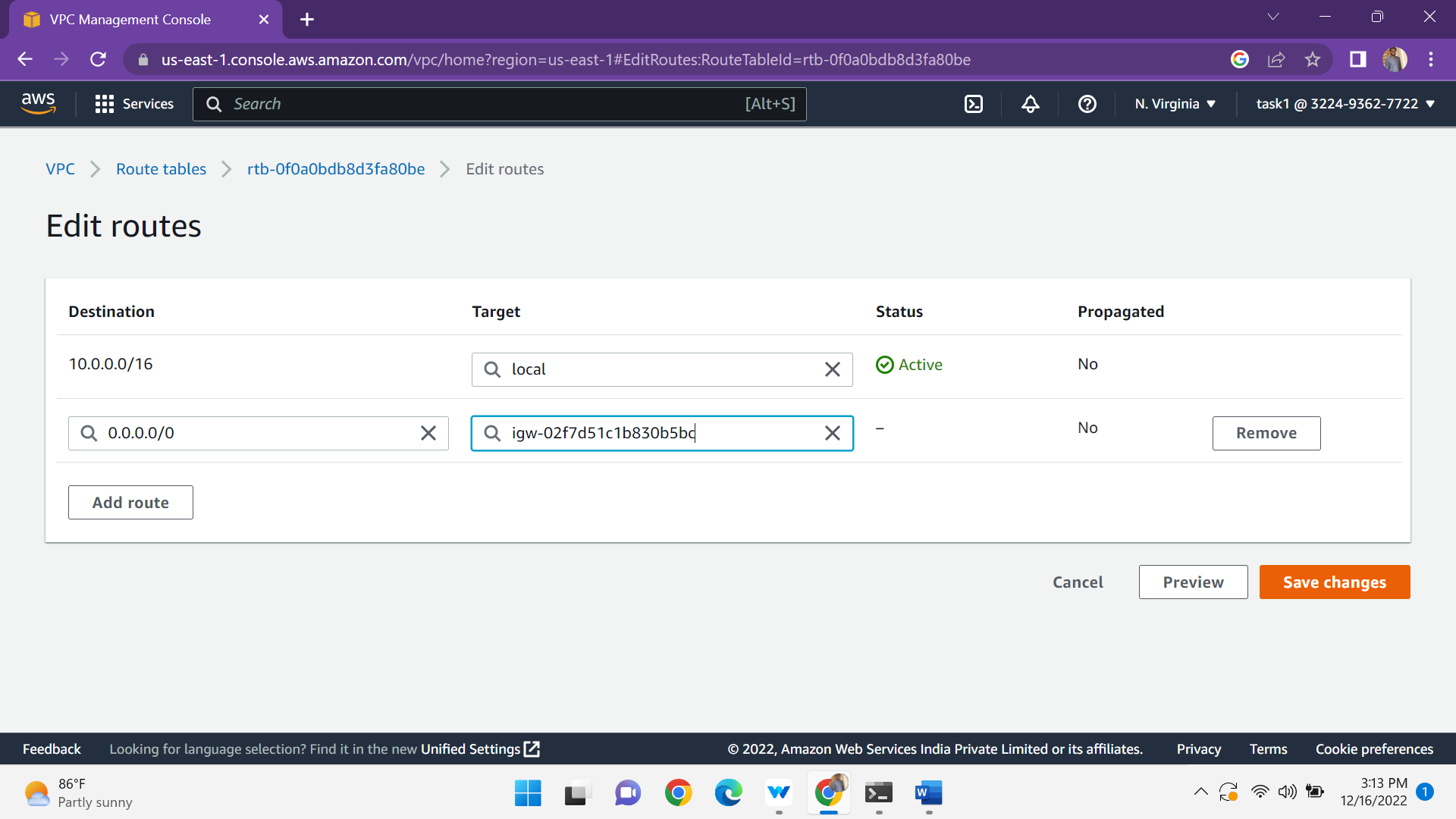
Create a two route tables one is private and another one is public the public route table is attached to the internet gateway.

A screenshot of a computer

Description automatically generated

Graphical user interface, text

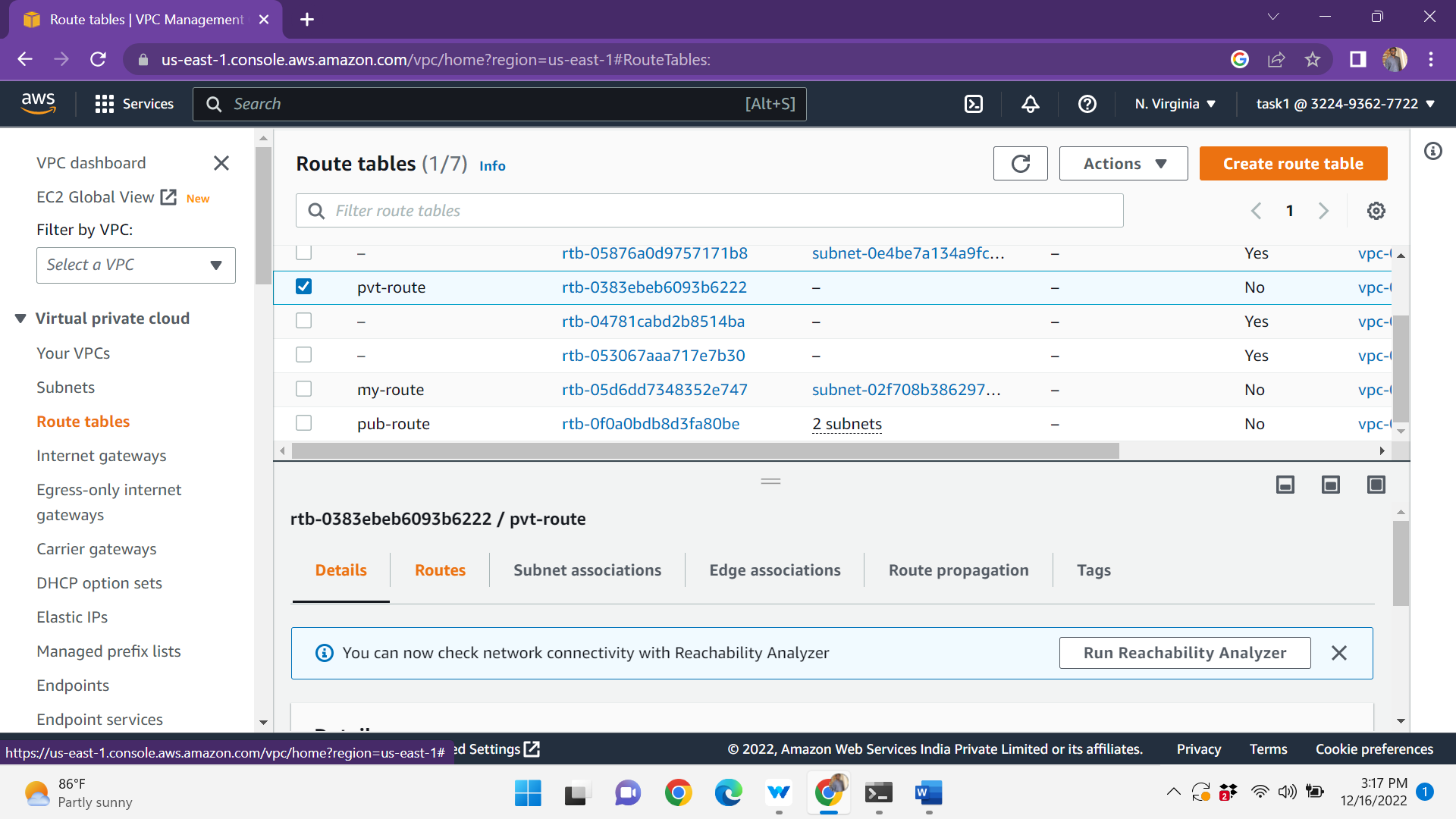
Description automatically generated

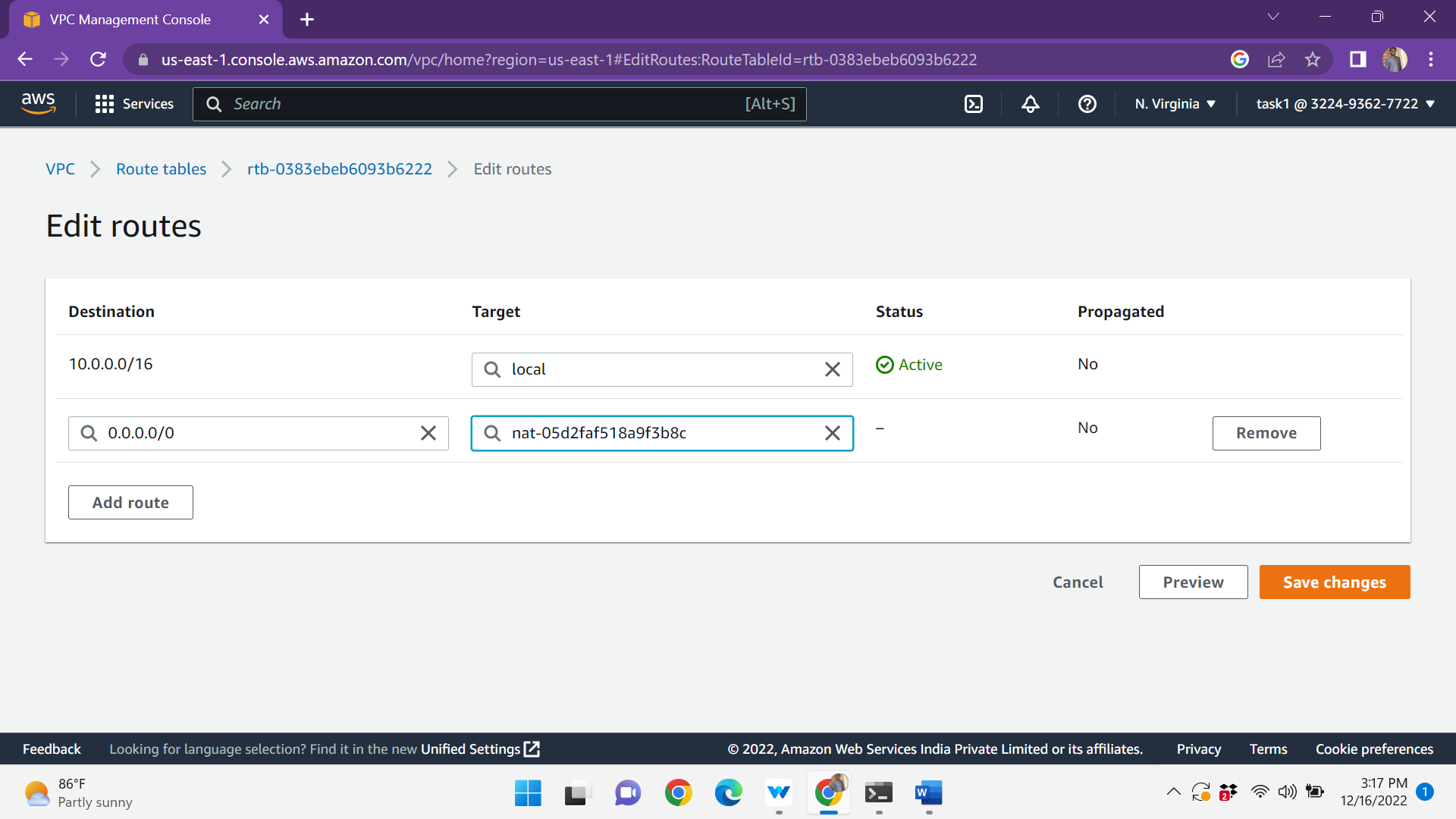


Both the routes are edit to subnet association

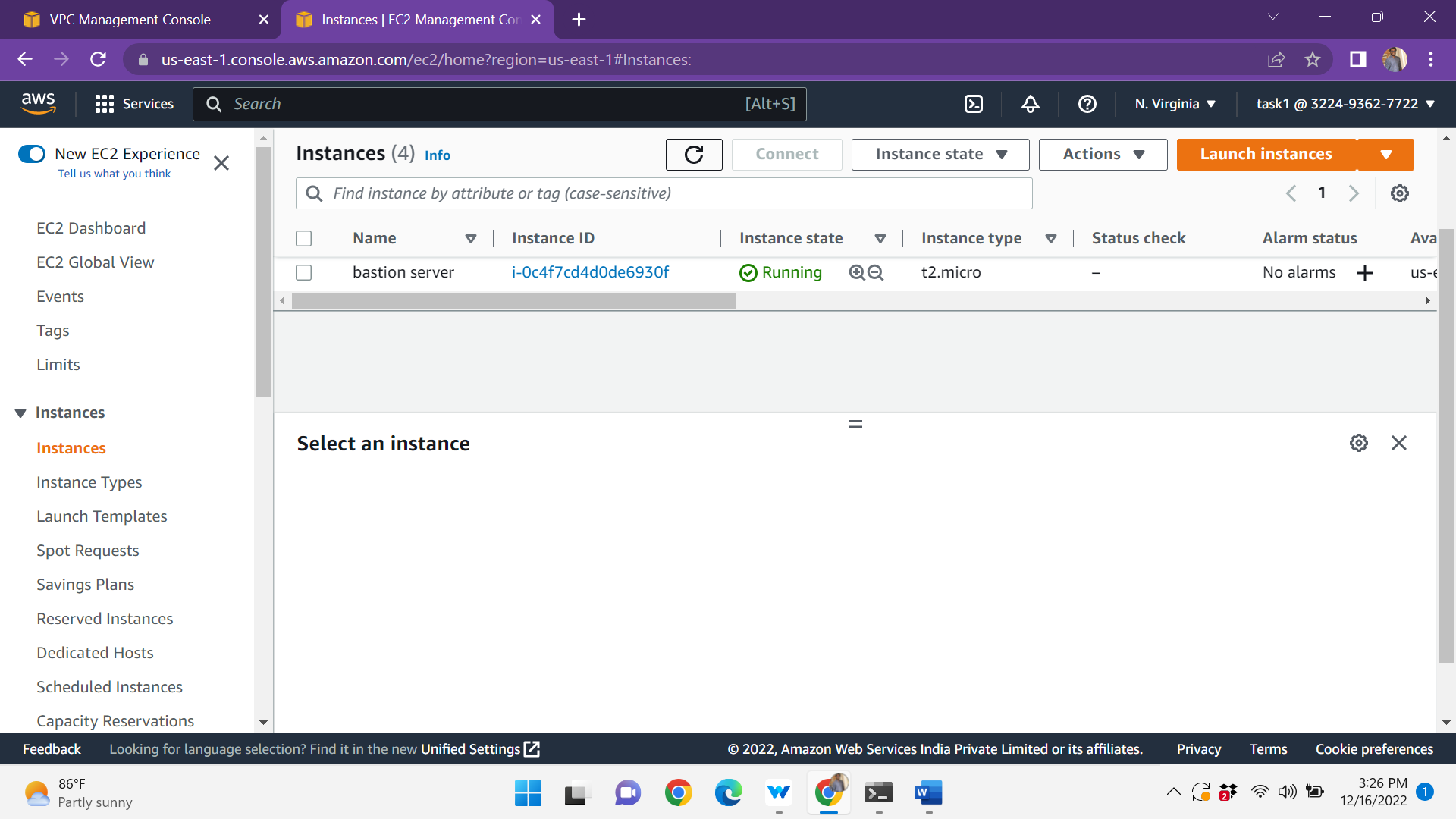


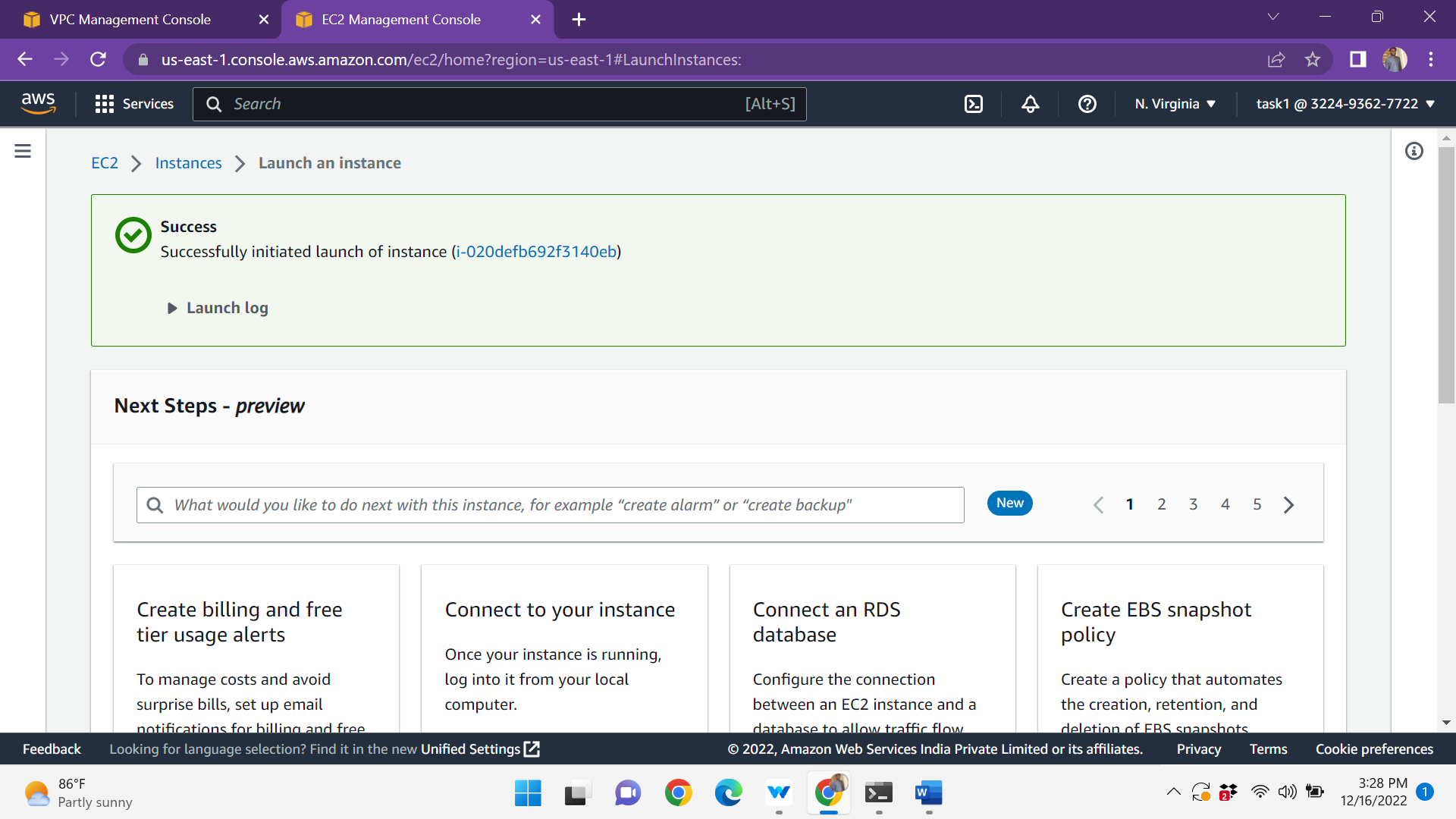
Create a nat gateway the nat gateway is connected to the private instance.

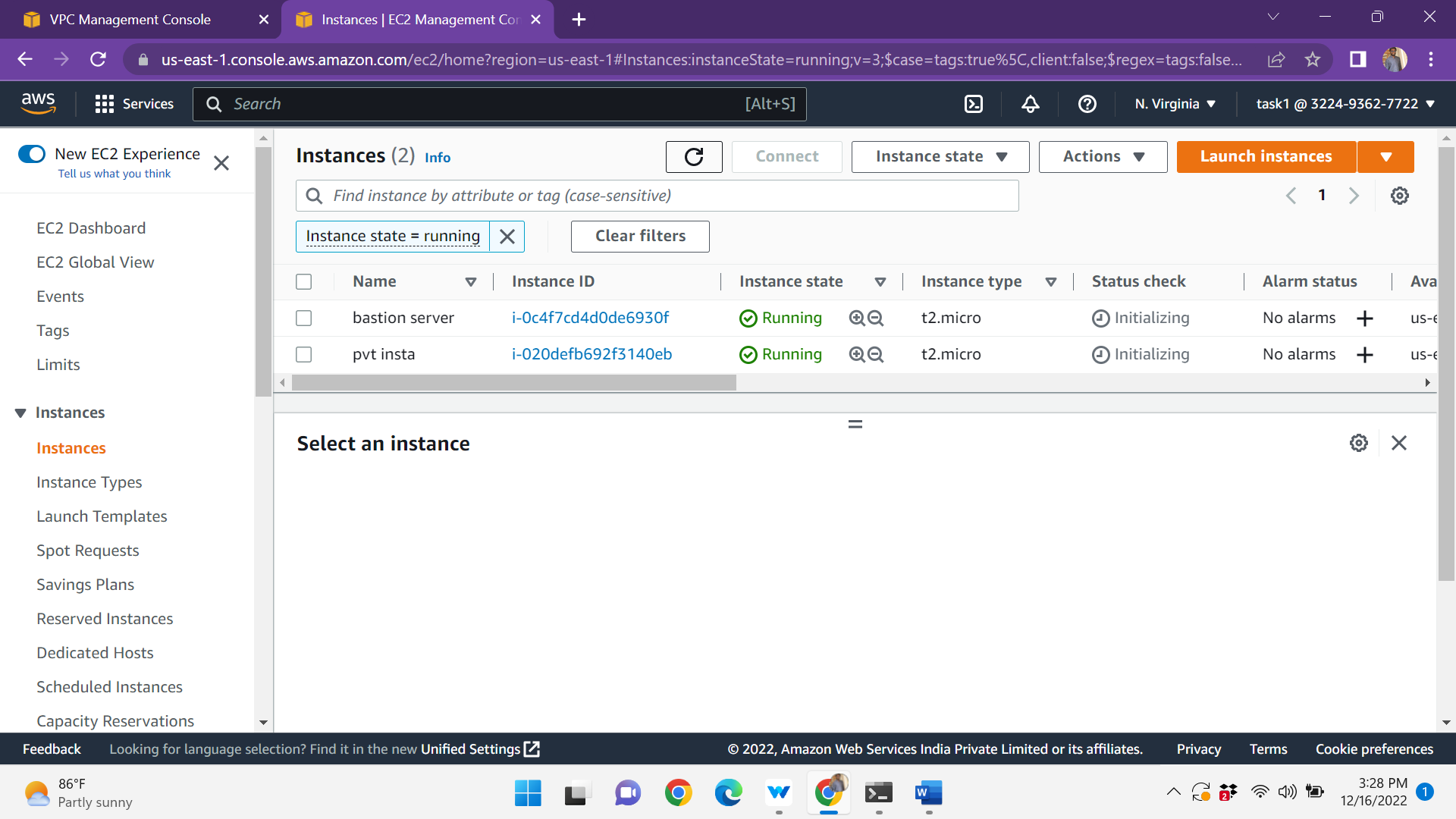




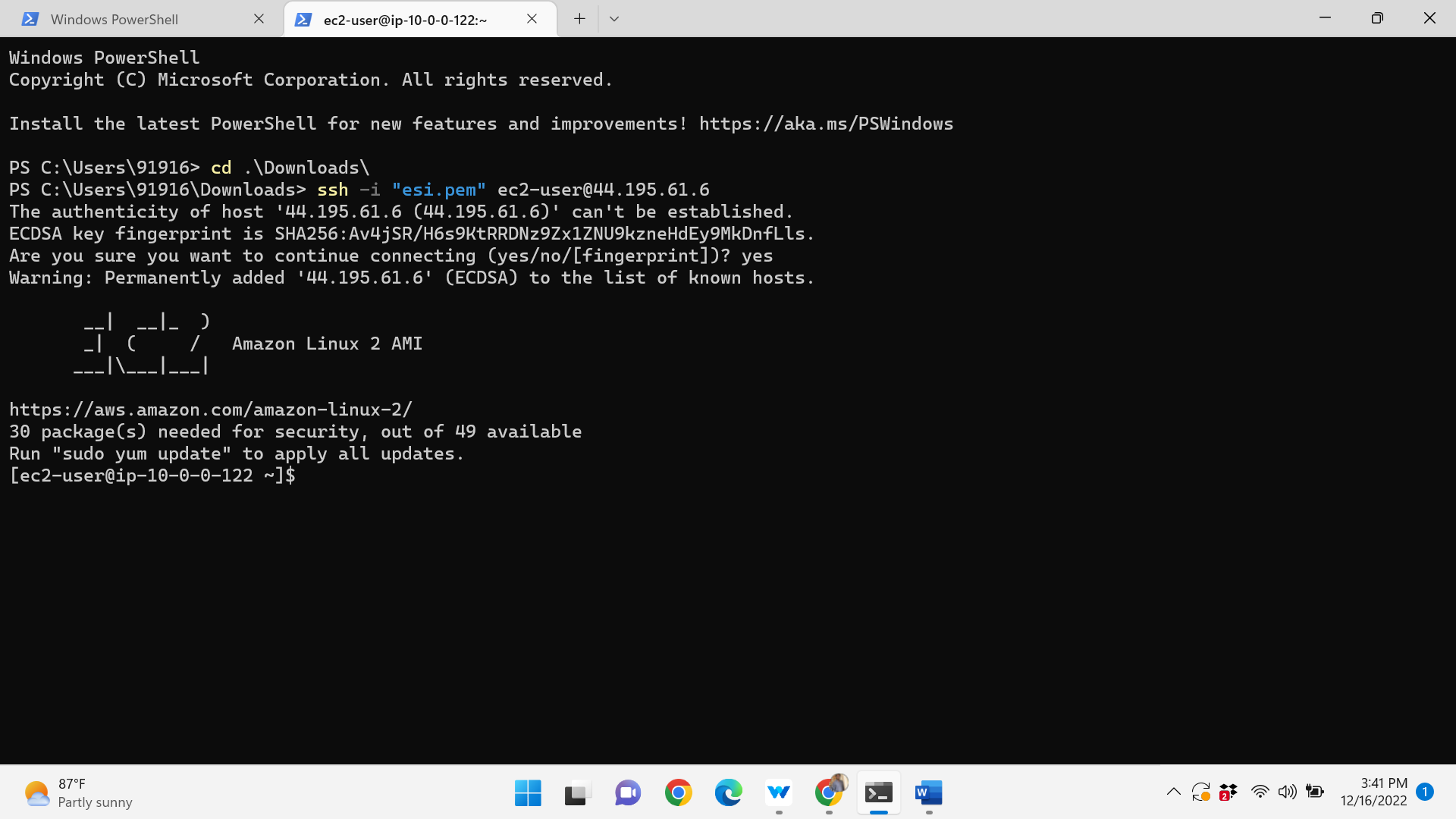
Create a ec2 instance public and the private instances



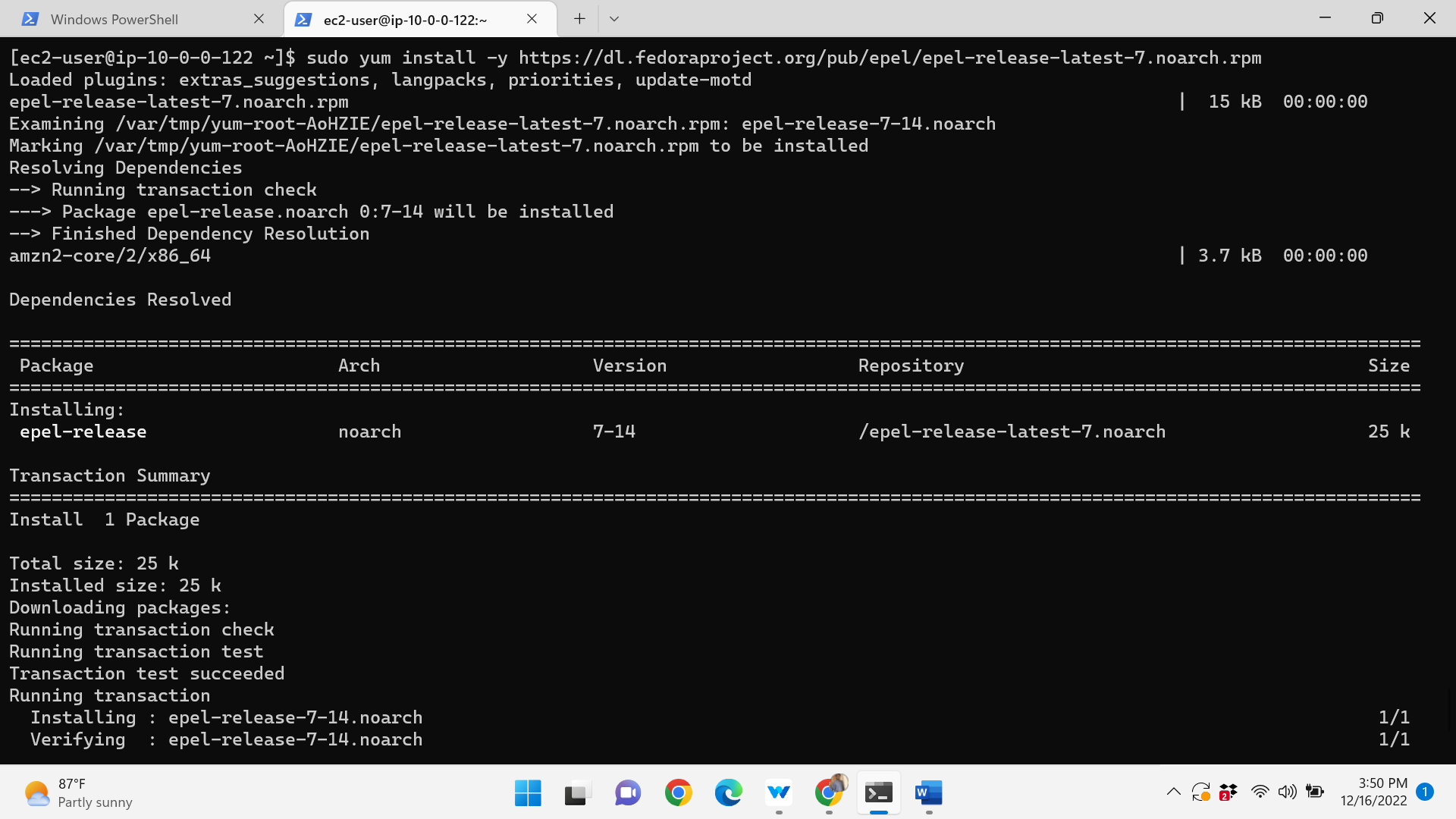




The instance is connected to the terminal

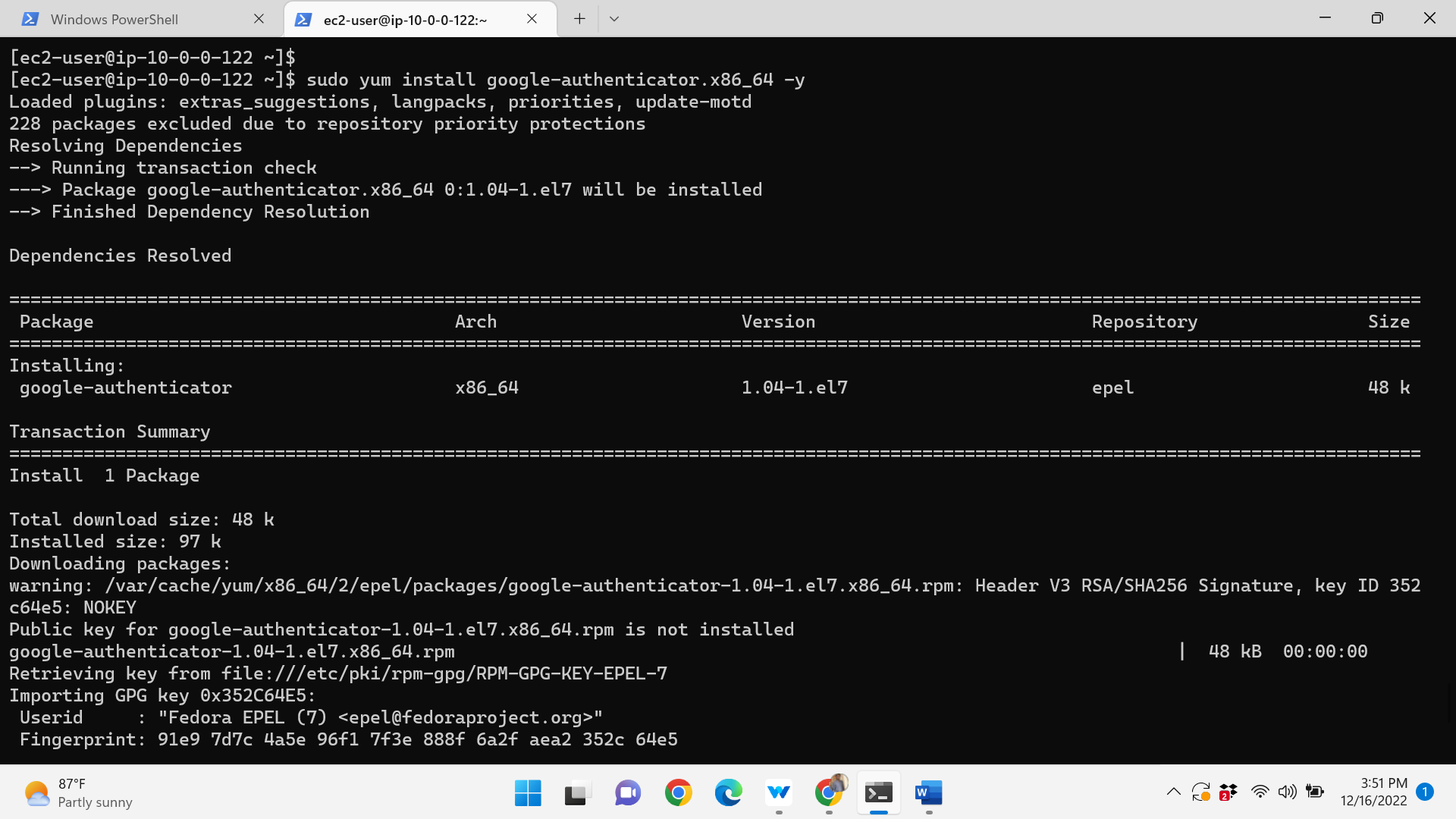


Sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm



And after install the google-authenticator by using the following command

Sudo yum install google-authenticator.x80\_64 -y

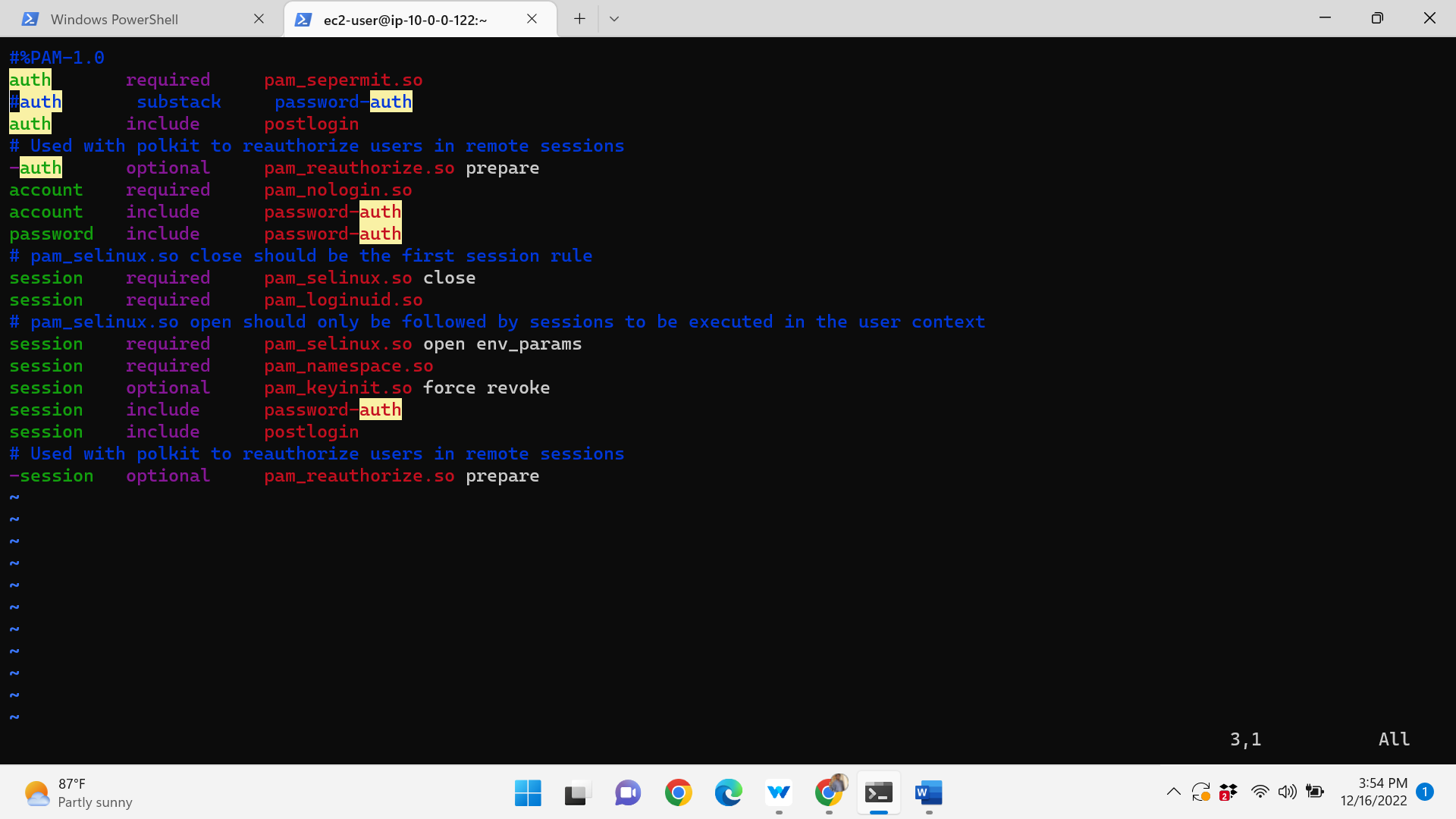


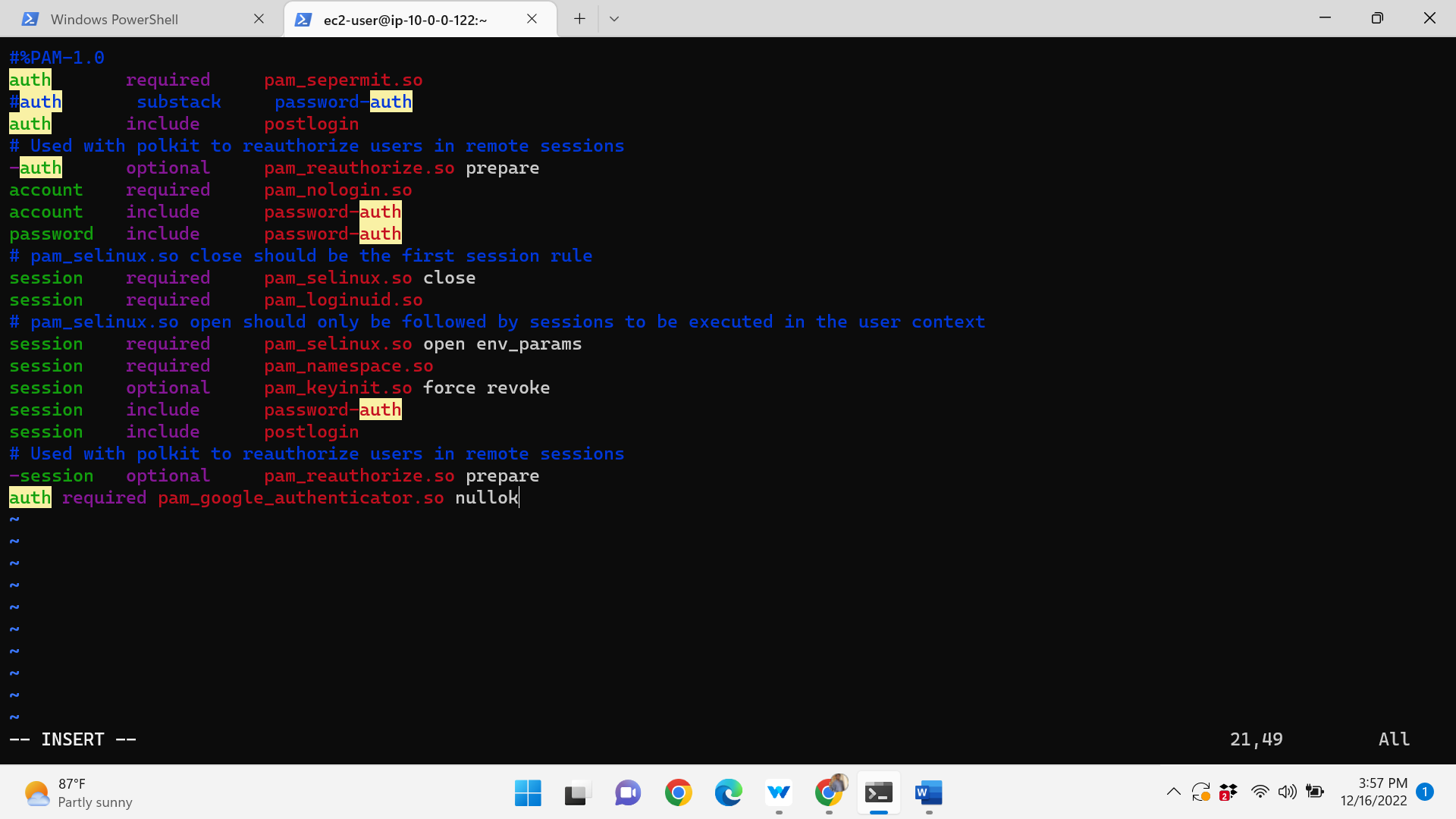
In this step we are modifying some files and editing to install google authentication and to setup MFA in ec2-instance.

Sudo vi /etc/pam.d/sshd

In the bottom we can add these lines on the file.

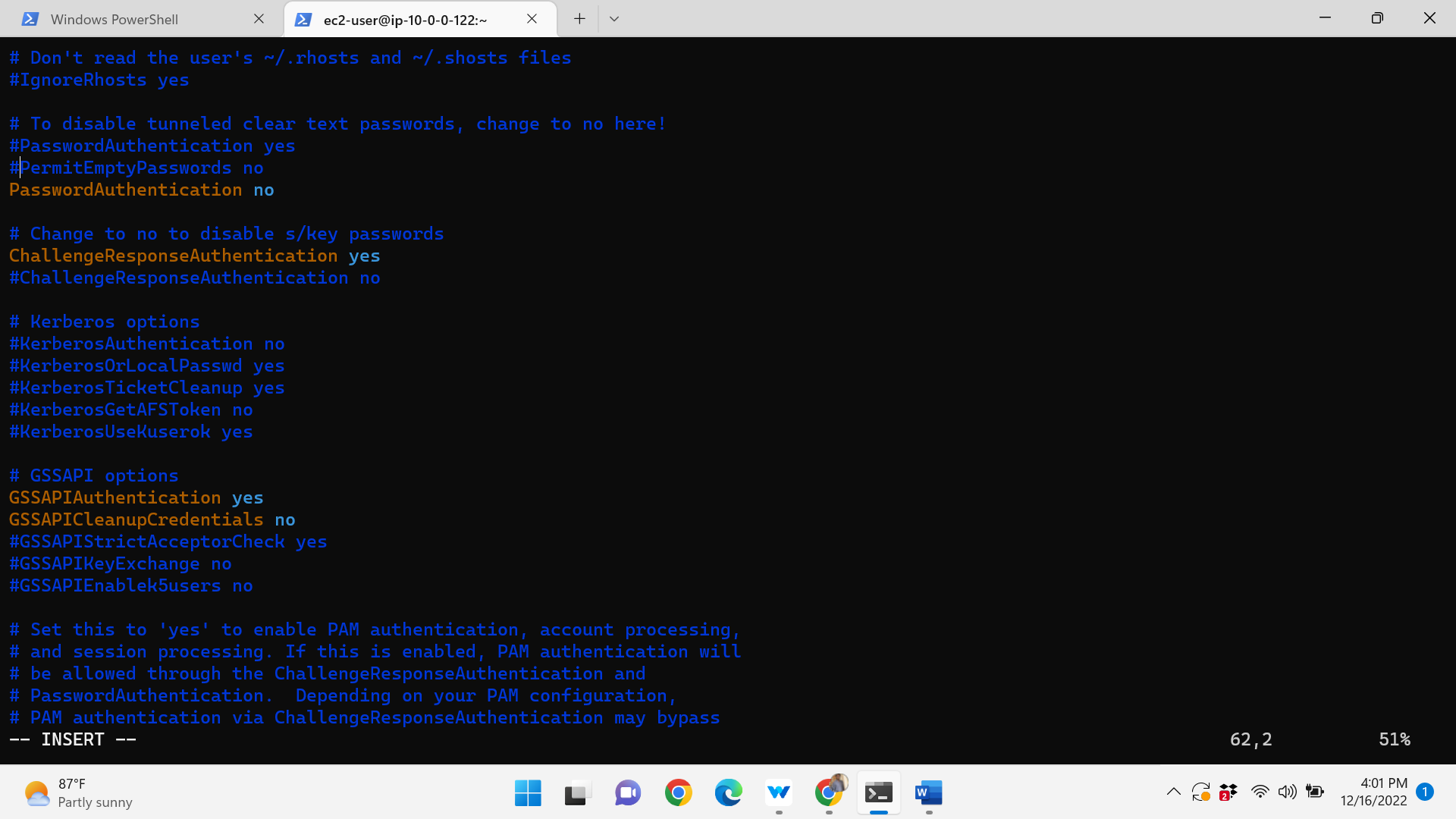
Auth required pam\_google\_authenticator.so nullok



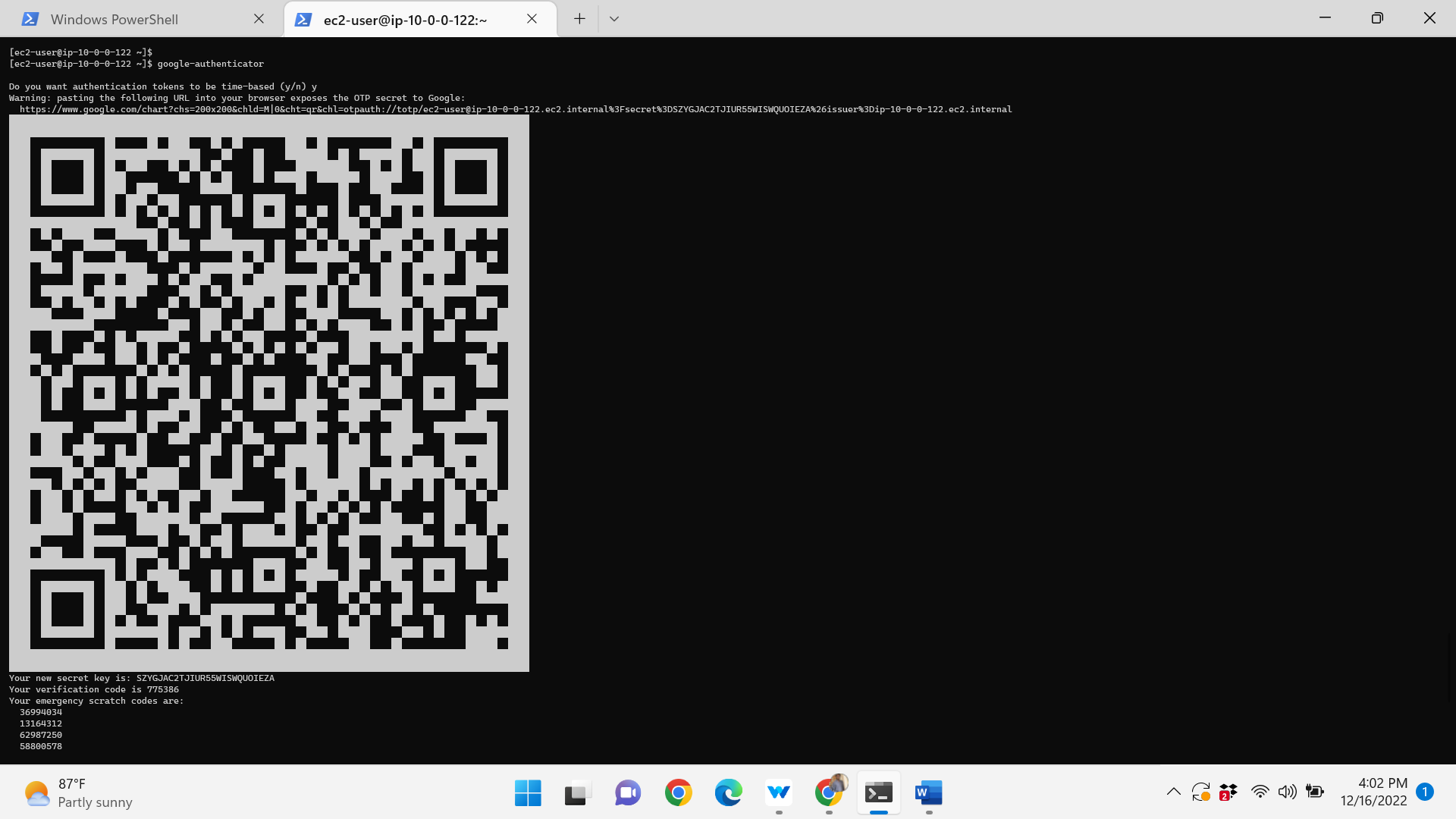


Update the sshd configuration

In this step we are going to tell sshd that we have one more level of multifactor authentication for the user to login along with the Keybased authentication

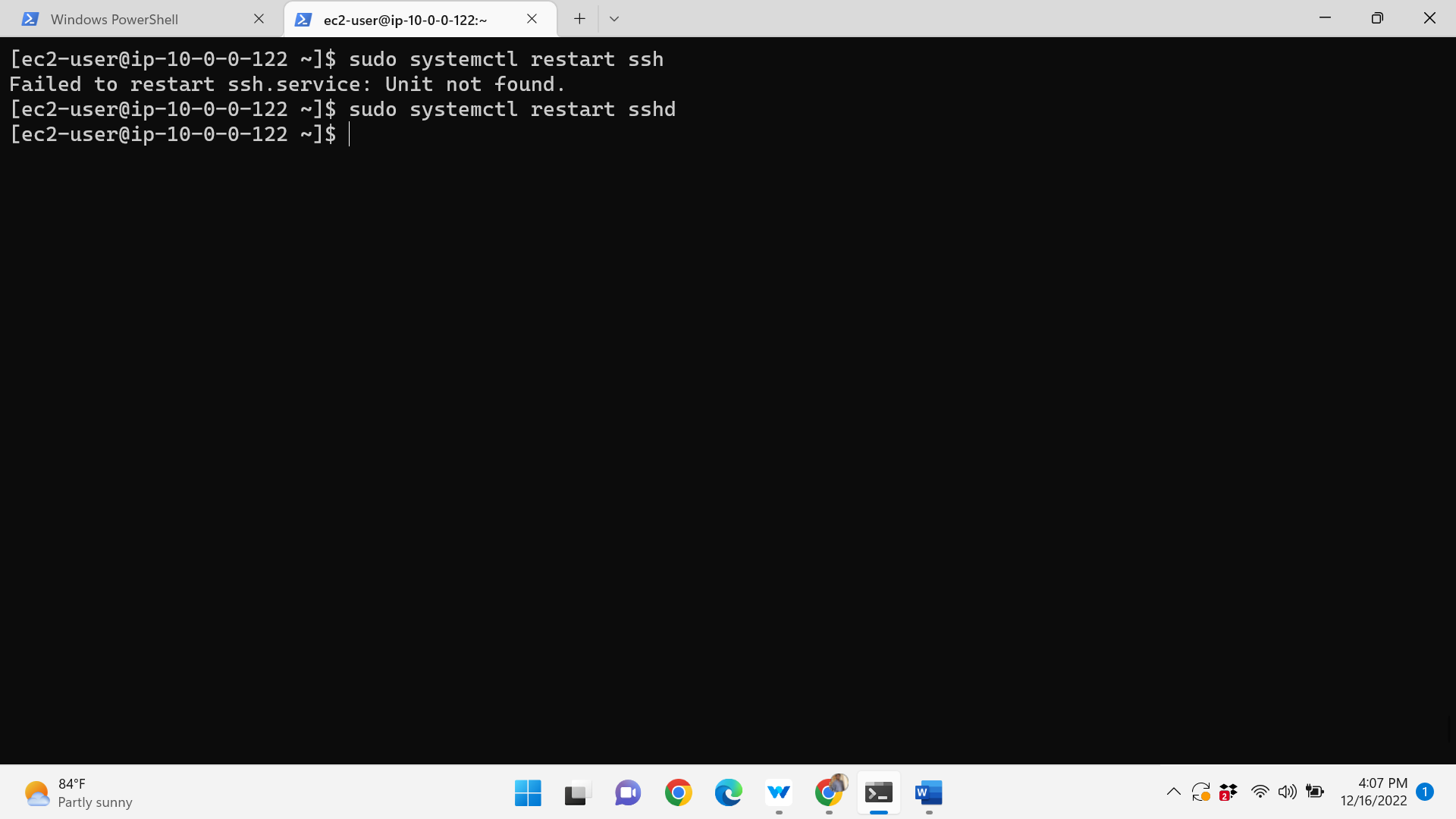


In the ec2-instance install the google authenticator it gives the bar code the bar code can scan through your mobile.in mobile install the google authentication after scanning it sends a verification code and enters the verification in ec2-instance.



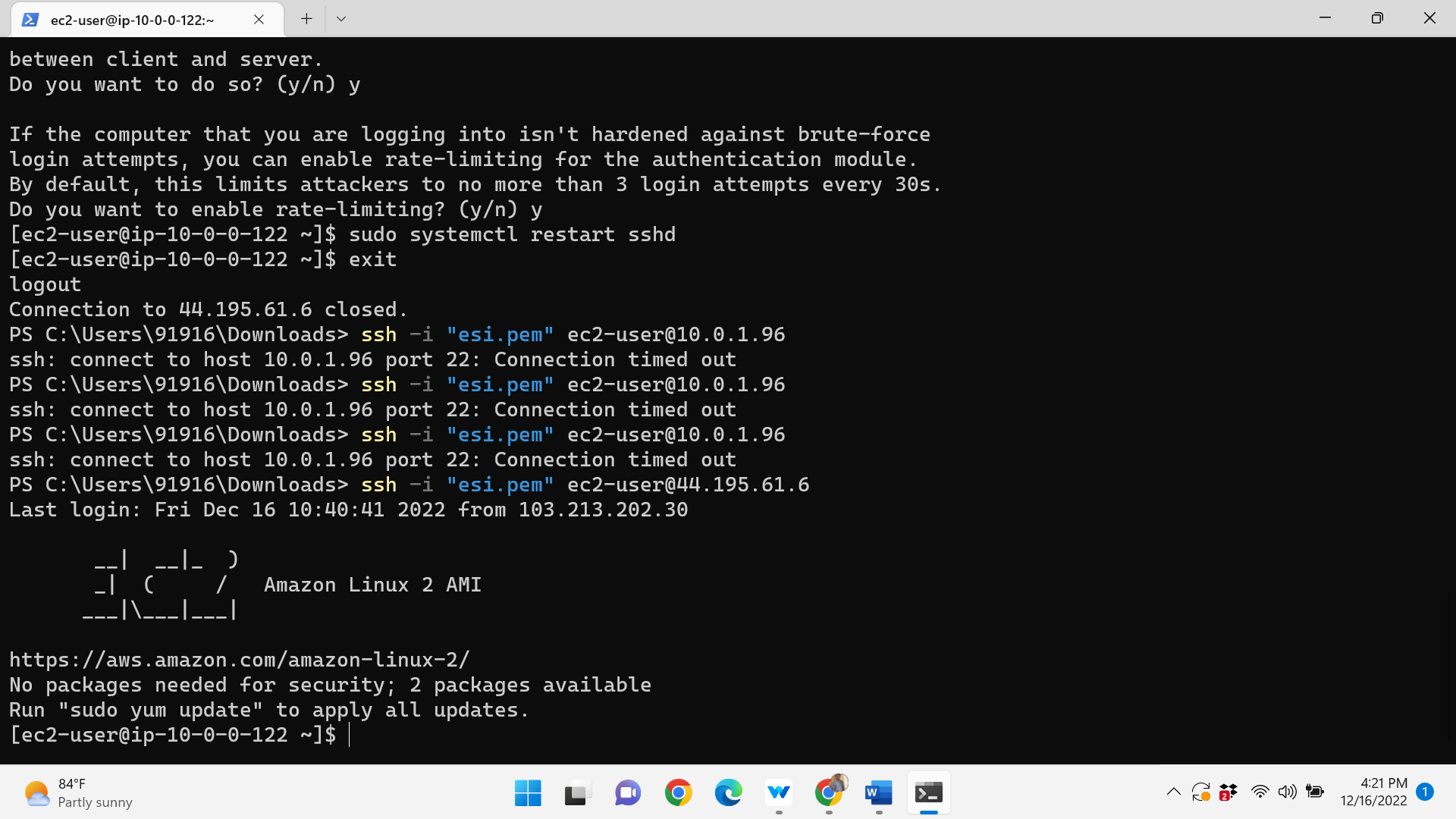
Restart the ssh by using the following command

Sudo systemctl restart ssh



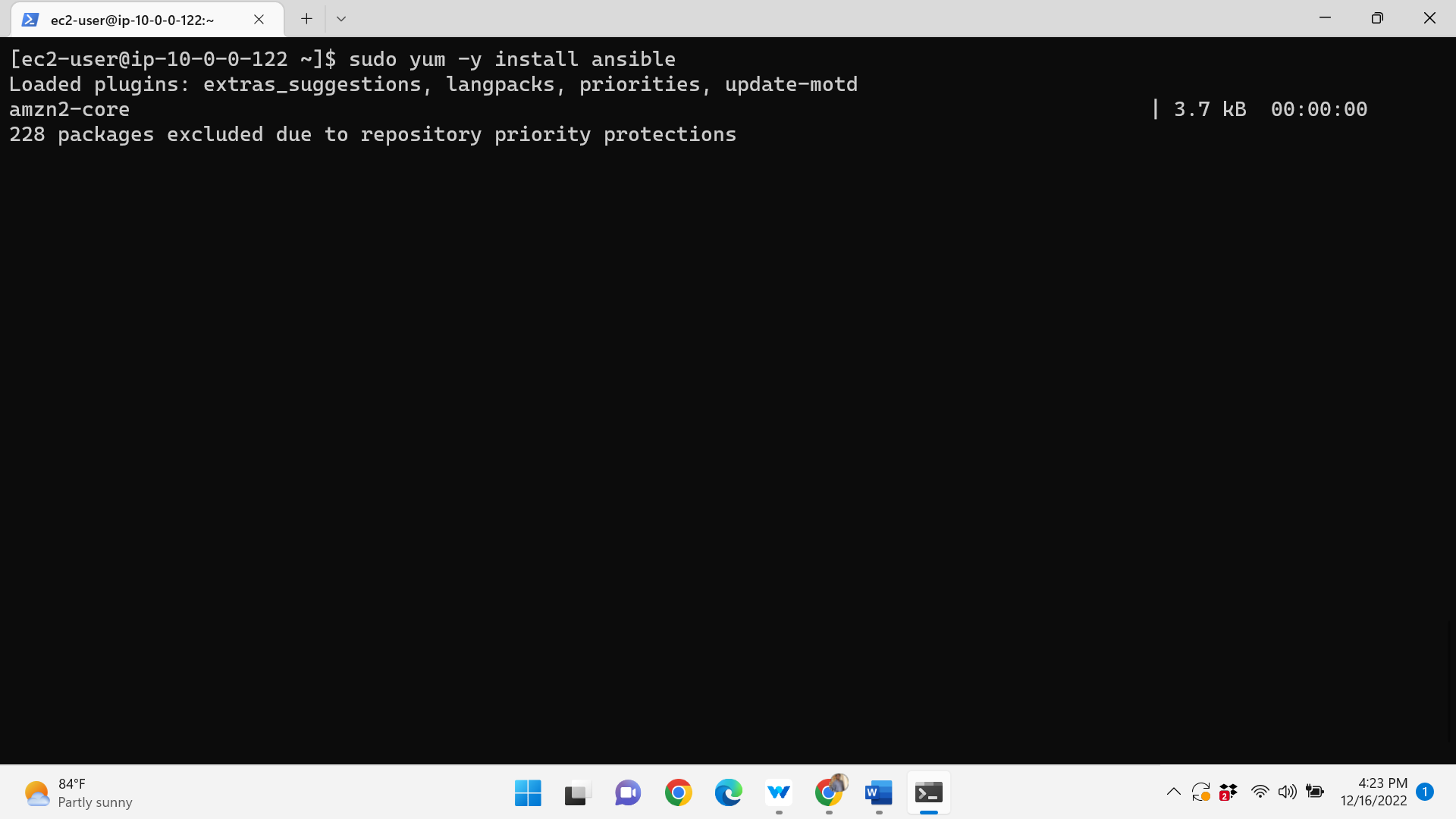
And exit from the instance



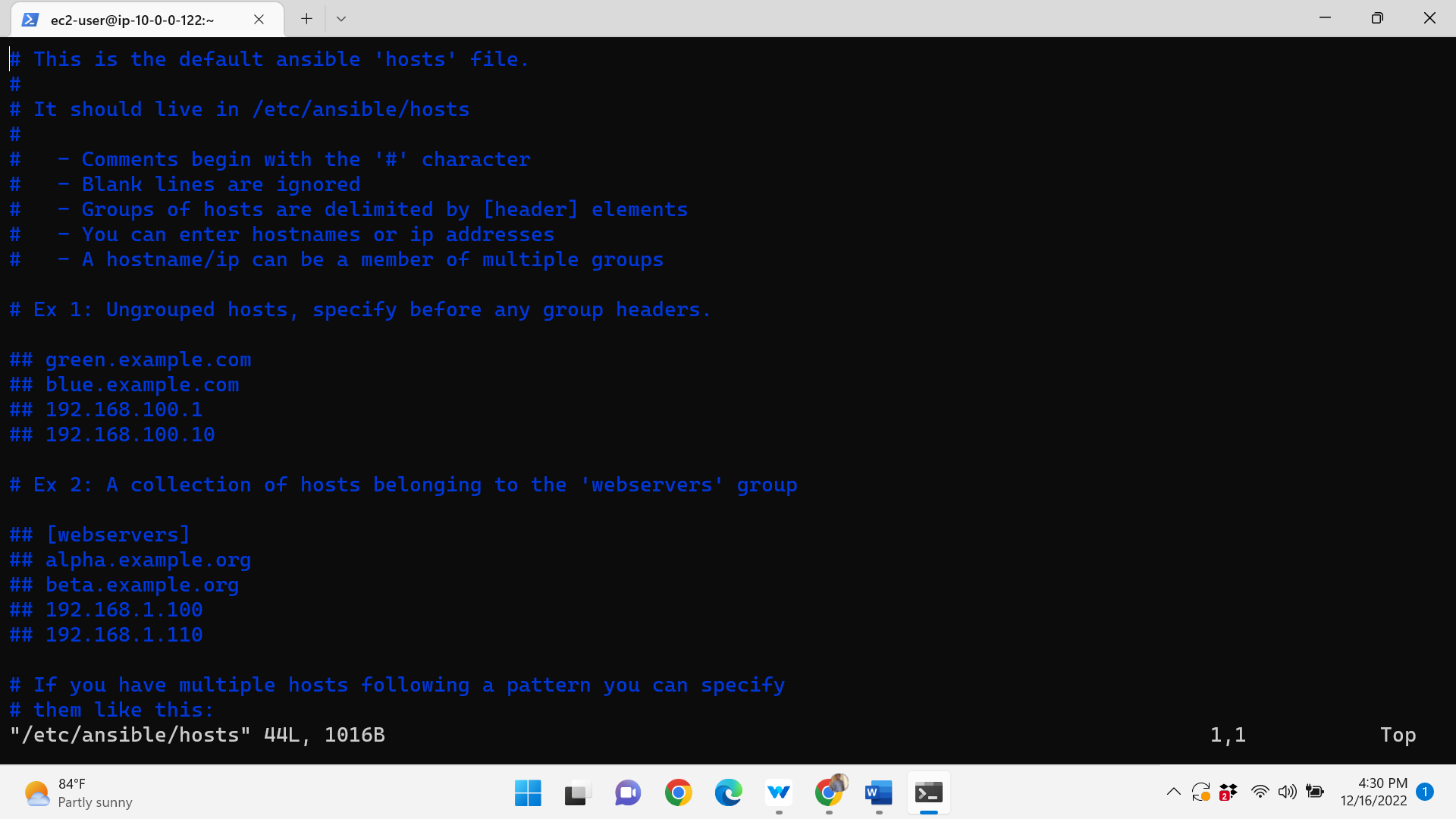


And connect the public instance to the terminal

Install ansible -sudo yum -y install ansible

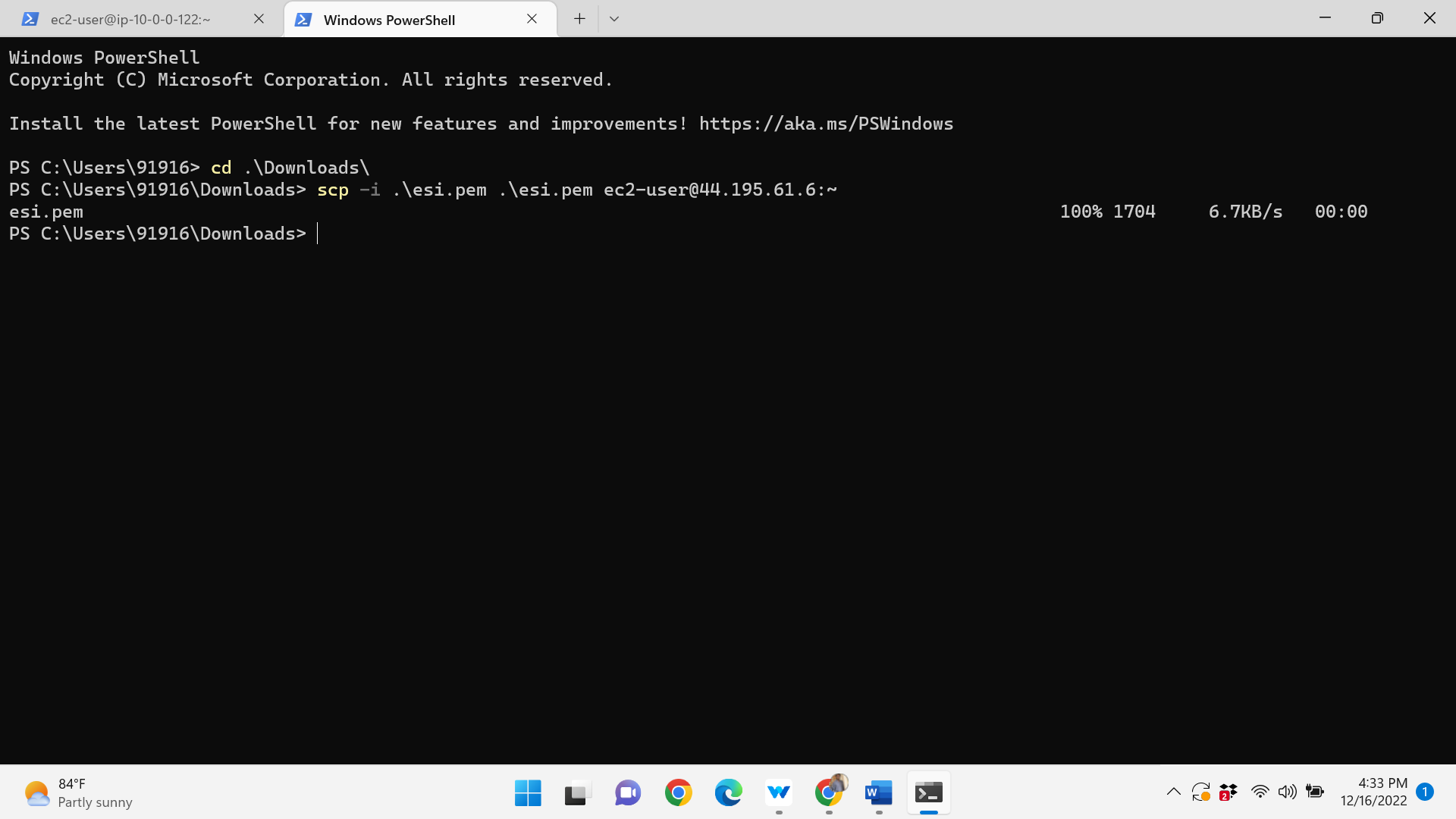


Sudo vi /etc/ansible/hosts edit the script



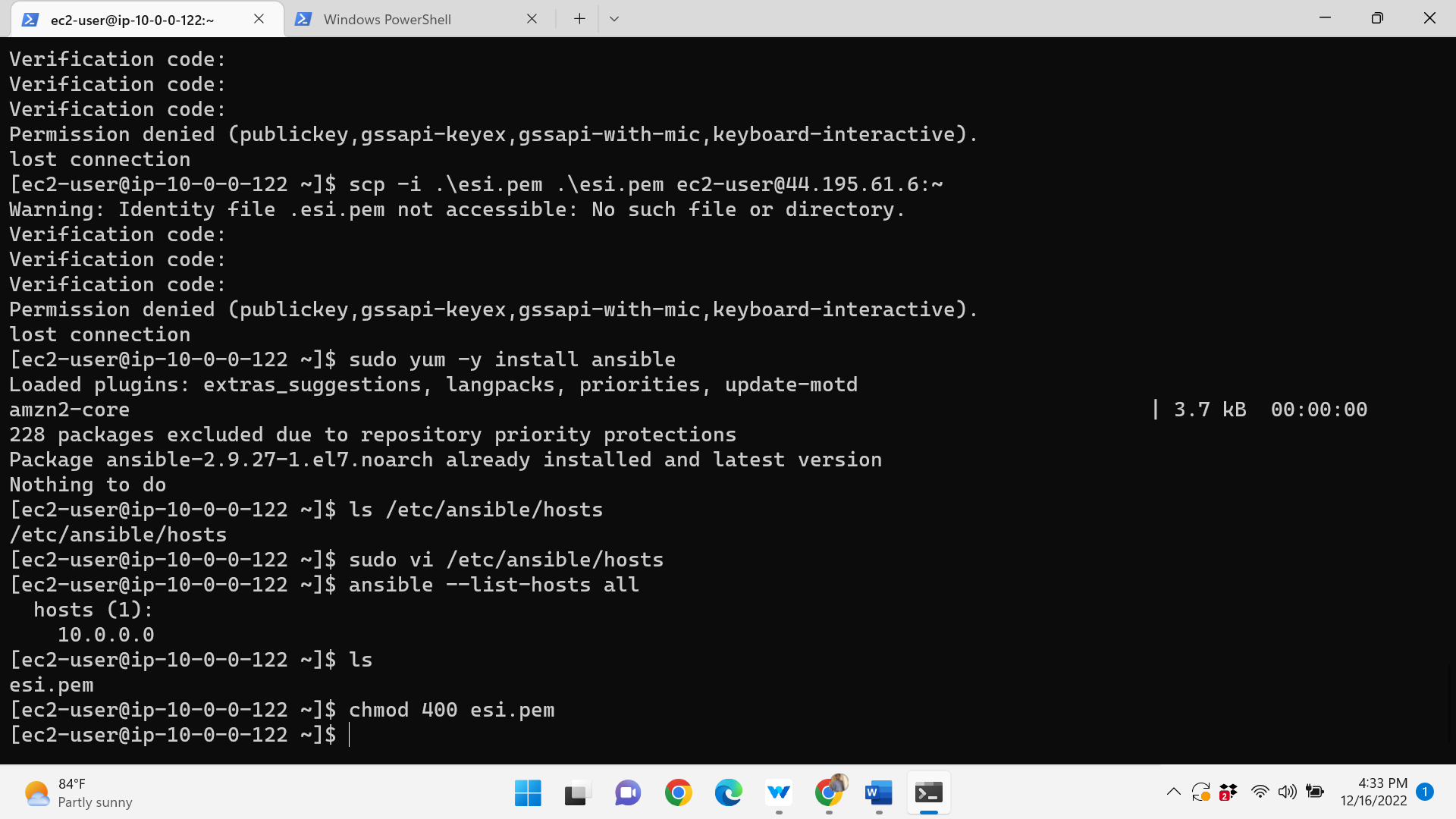
Give the command copy the keypair

Scp -I .\esi.pem .\esi.pem ec2-user@public ip :~



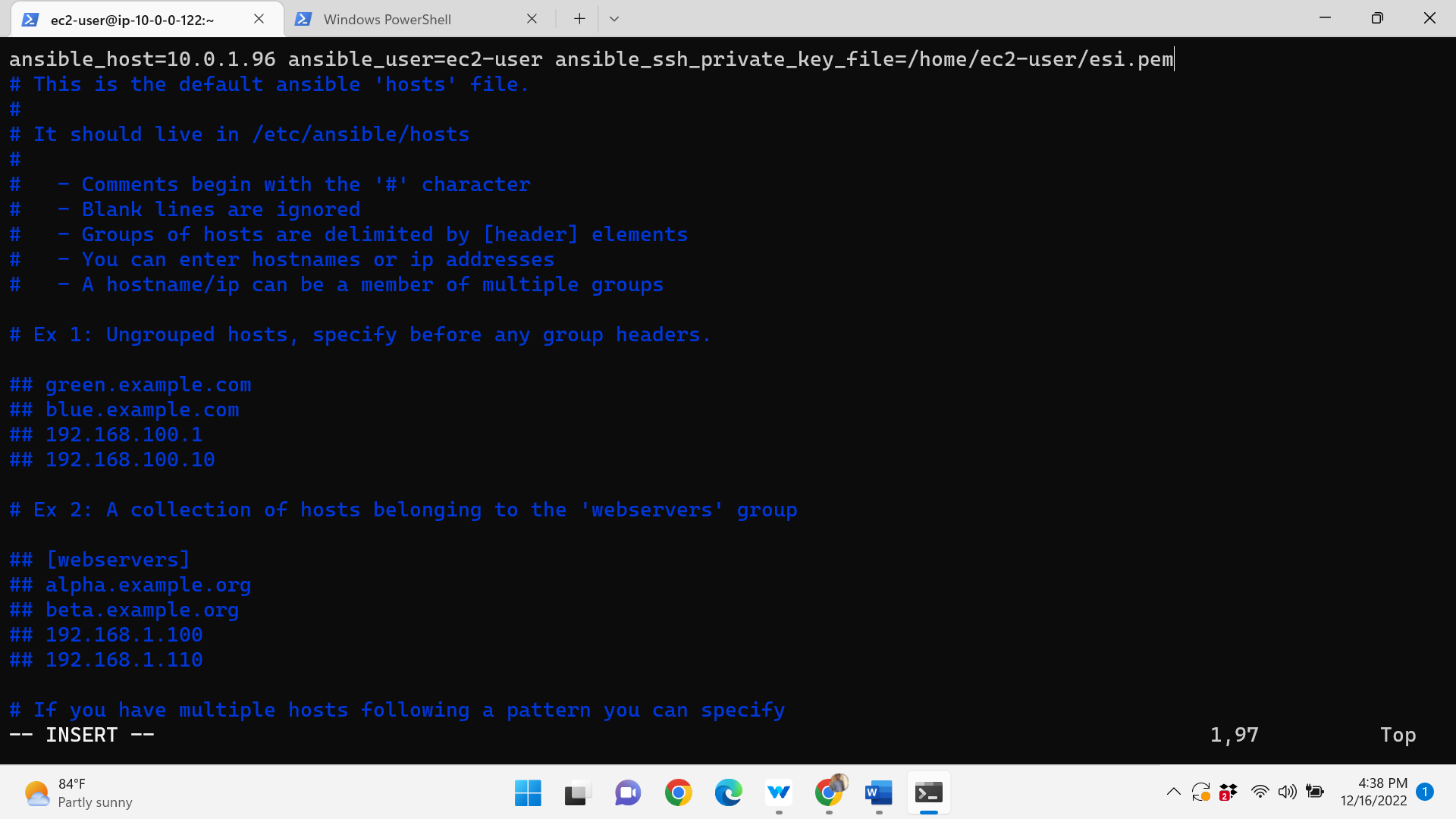
Give the read permissions to the keypair

Chmod 400 esi.pem



Edit the script

Ansible\_host=pvtip ansible\_user=ec2-user ansible\_ssh\_private\_key\_file=home/ec2-user/keypair



Finally ping the server by using the command

Sudo all -m ping

