

How to connect to private EC2 instance

Step 1. We have 2 instances, one public instance and another private instance, if not create them

The screenshot shows the AWS EC2 Instances page. There are two instances listed:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
rootlinuxbastion	i-038fe620fb367048f	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-23-23-13-38
linuxprivate	i-0af3fa665157fb10	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	-

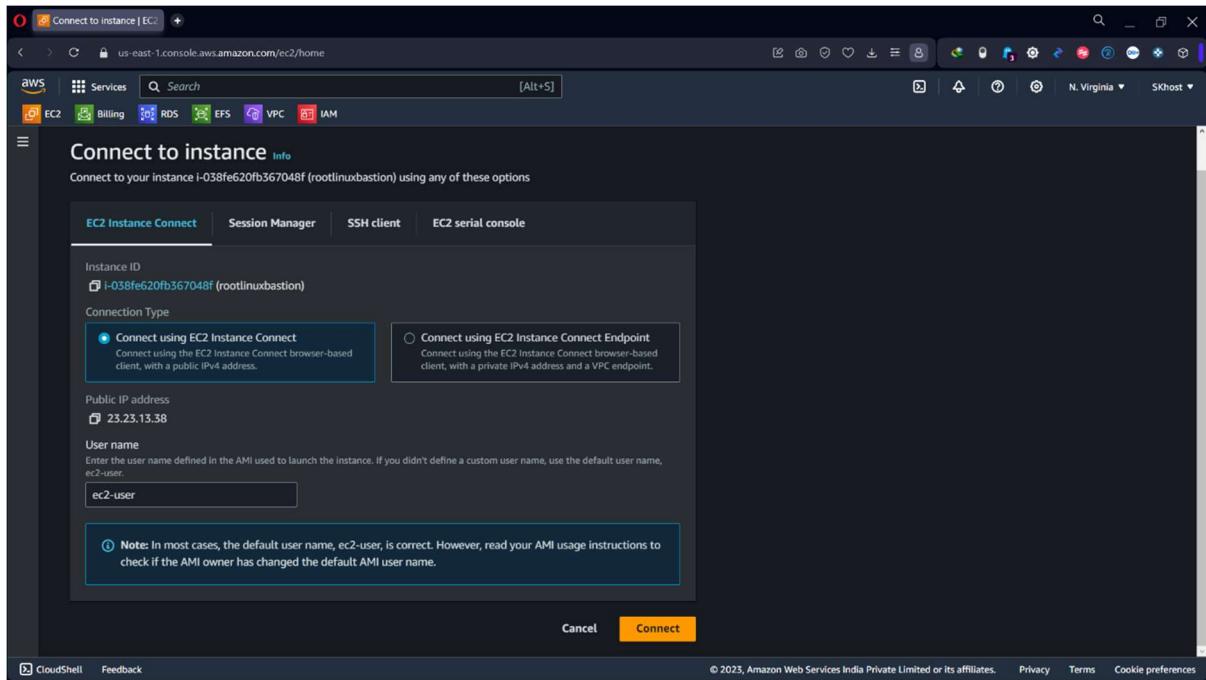
A modal window titled "Select an instance" is displayed, containing the same two instance entries.

Step 2. first, we will connect public instance using public ip

The screenshot shows the AWS EC2 Instance details page for the instance i-038fe620fb367048f (rootlinuxbastion). The "Connect" button is highlighted in red.

Instance summary for i-038fe620fb367048f (rootlinuxbastion)

Attribute	Value
Public IPv4 address	23.23.13.38 [open address]
Instance state	Running
Private IP DNS name (IPv4 only)	ip-10-0-1-17.ec2.internal
Instance type	t2.micro
VPC ID	vpc-08043d342756457e2 (My-Custom-vpc)
Subnet ID	subnet-0ad7c3b35cd8a9a0 (My-Custom-subnet-public1-us-east-1a)



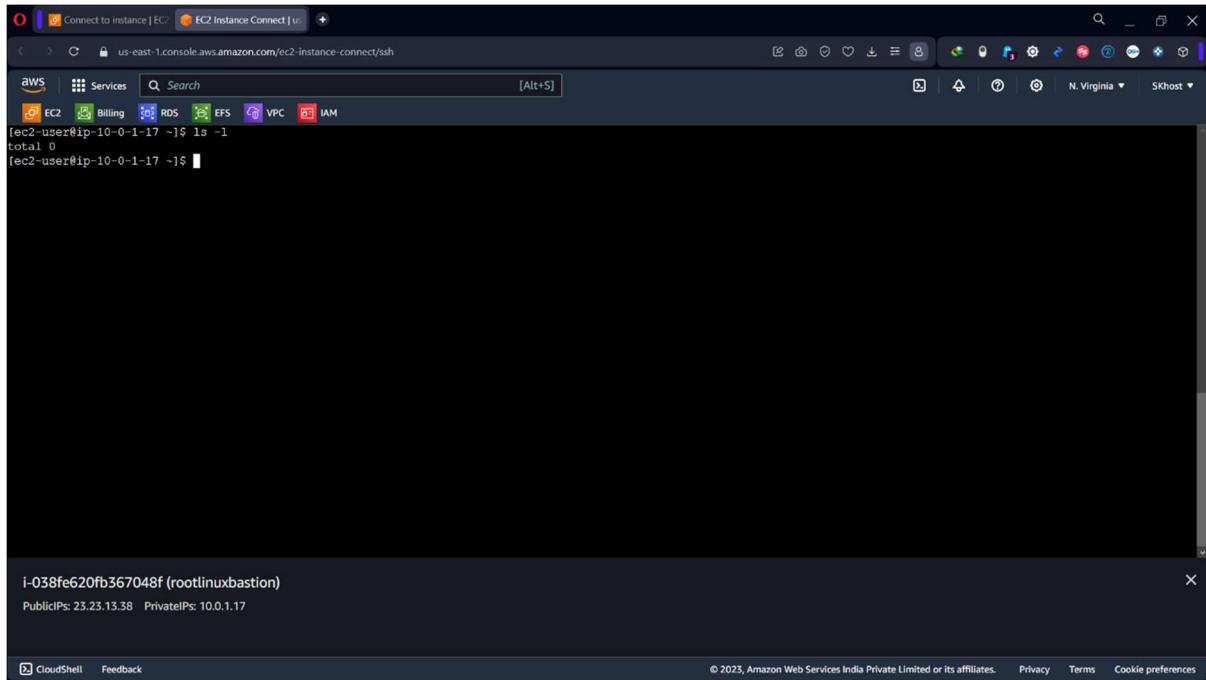
Step 3. we will check if it have access to internet or not by pinging google.com

```
[ec2-user@ip-10-0-1-17 ~]$ ping google.com
PING google.com (172.253.63.101) 56(84) bytes of data.
64 bytes from bi-in-f101.le100.net (172.253.63.101): icmp_seq=1 ttl=102 time=1.66 ms
64 bytes from bi-in-f101.le100.net (172.253.63.101): icmp_seq=2 ttl=102 time=1.71 ms
64 bytes from bi-in-f101.le100.net (172.253.63.101): icmp_seq=3 ttl=102 time=1.77 ms
64 bytes from bi-in-f101.le100.net (172.253.63.101): icmp_seq=4 ttl=102 time=1.72 ms

64 bytes from bi-in-f101.le100.net (172.253.63.101): icmp_seq=5 ttl=102 time=1.71 ms
64 bytes from bi-in-f101.le100.net (172.253.63.101): icmp_seq=6 ttl=102 time=1.73 ms
^C
--- google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 500ms
rtt min/avg/max/mdev = 1.655/1.717/1.772/0.034 ms
[ec2-user@ip-10-0-1-17 ~]$
```

i-038fe620fb367048f (rootlinuxbastion)
PublicIPs: 23.23.13.38 PrivateIPs: 10.0.1.17

Step 4. checking the files inside the public subnet

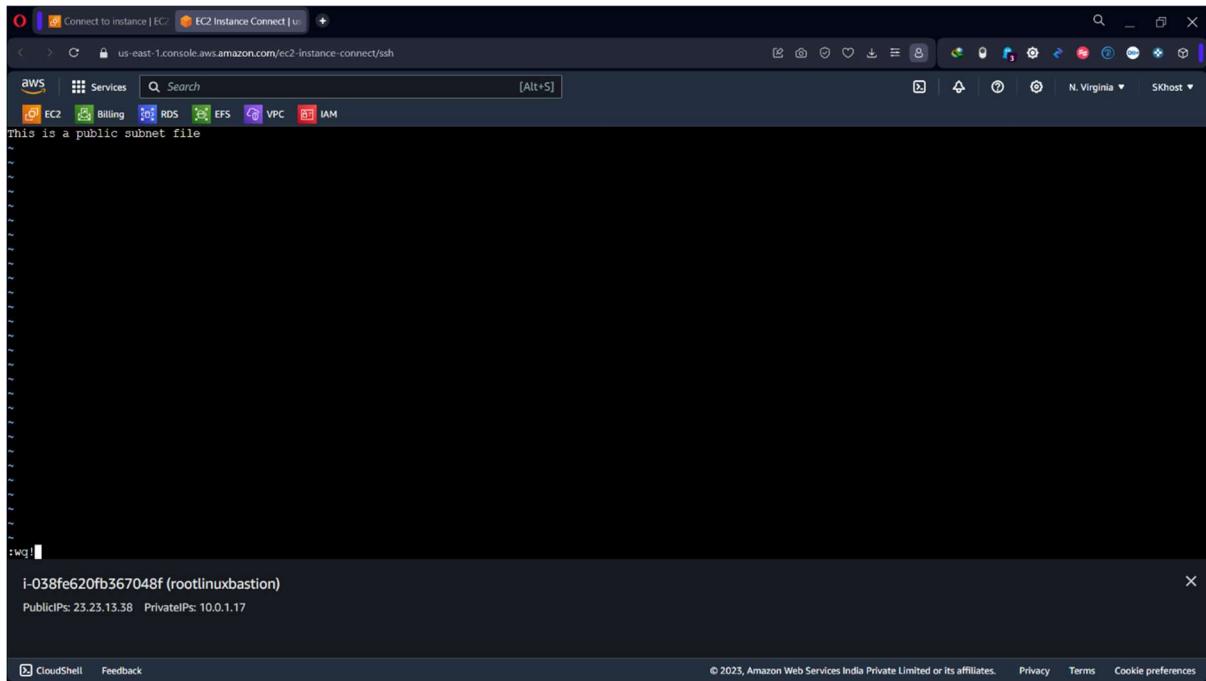


```
[ec2-user@ip-10-0-1-17 ~]$ ls -l
total 0
[ec2-user@ip-10-0-1-17 ~]$
```

i-038fe620fb367048f (rootlinuxbastion)
Public IPs: 23.23.13.38 Private IPs: 10.0.1.17

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Step 5. we will create a sample.txt file with content : “This is a public subnet file”



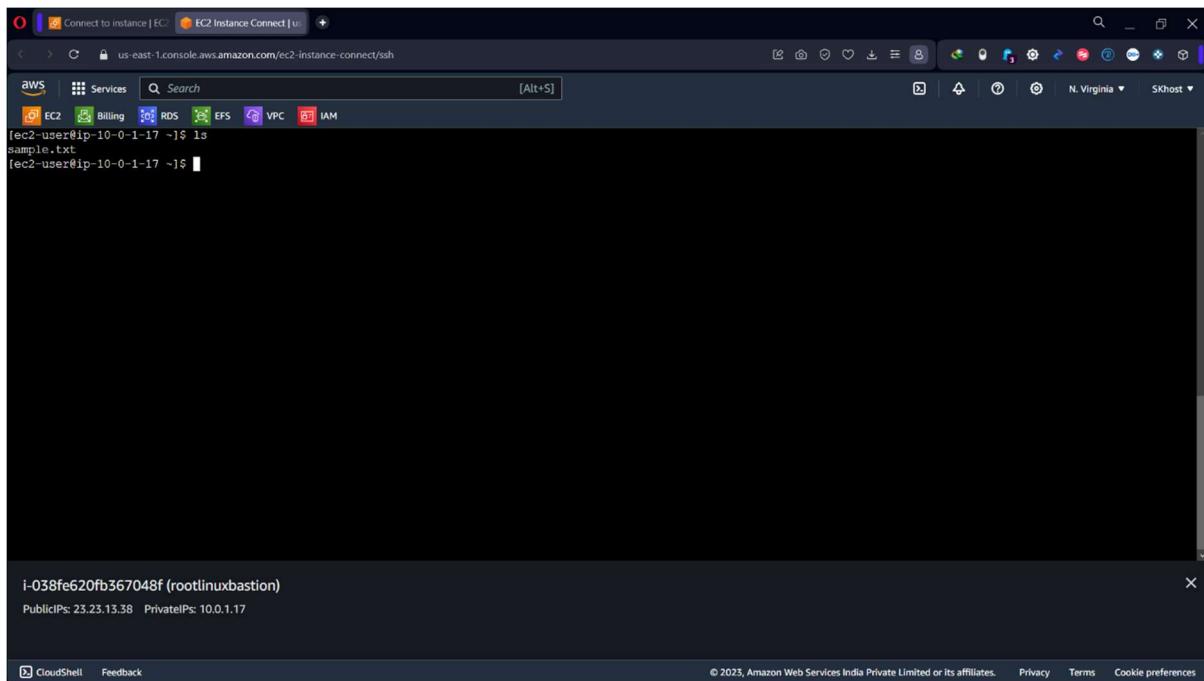
```
This is a public subnet file
```

```
:wq!
```

```
i-038fe620fb367048f (rootlinuxbastion)  
Public IPs: 23.23.13.38 Private IPs: 10.0.1.17
```

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

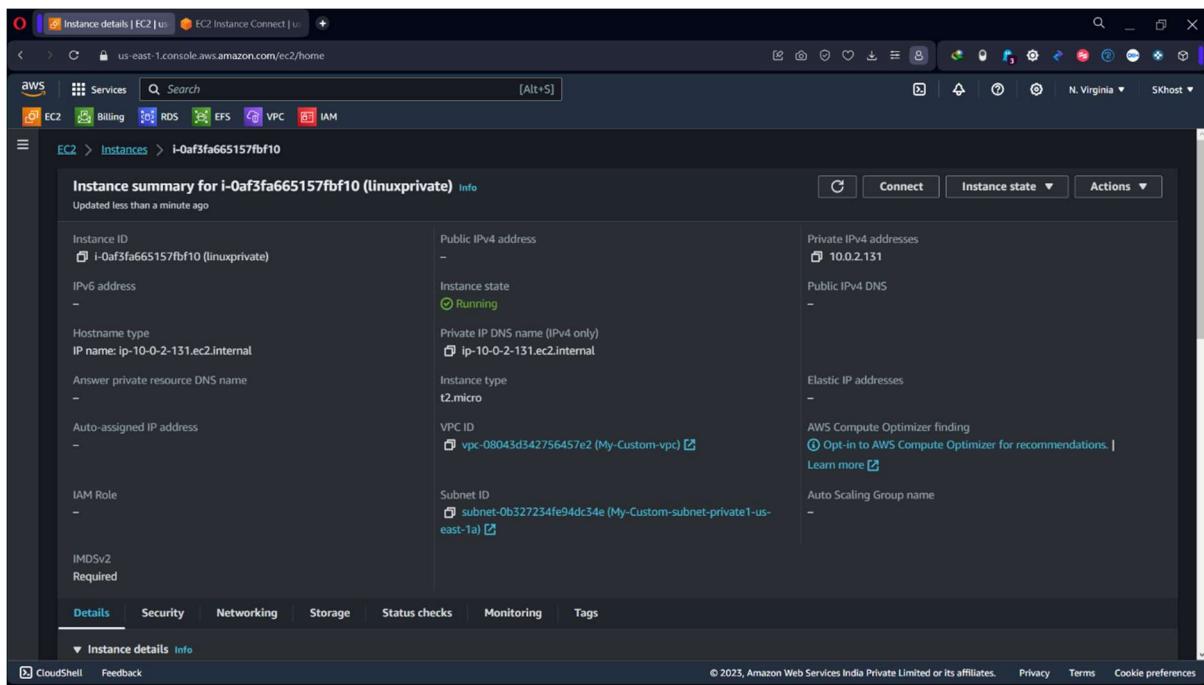
Step 6. Verify the file has been created and saved properly



```
[ec2-user@ip-10-0-1-17 ~]$ ls
sample.txt
[ec2-user@ip-10-0-1-17 ~]$
```

i-038fe620fb367048f (rootlinuxbastion)
Public IPs: 23.23.13.38 Private IPs: 10.0.1.17

Step 7. Since we don't have the public ip we are unable to connect it from aws console, we will connect it from public subnet



Instance summary for i-0af3fa665157fbf10 (linuxprivate) [Info](#)
Updated less than a minute ago

Instance ID	Public IPv4 address	Private IPv4 addresses
i-0af3fa665157fbf10 (linuxprivate)	-	10.0.2.131
IPv6 address	Instance state	Public IPv4 DNS
-	Running	-
Hostname type	Private IP DNS name (IPv4 only)	Elastic IP addresses
IP name: ip-10-0-2-131.ec2.internal	ip-10-0-2-131.ec2.internal	-
Answer private resource DNS name	Instance type	AWS Compute Optimizer finding
-	t2.micro	Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto-assigned IP address	VPC ID	Auto Scaling Group name
-	vpc-08043d342756457e2 (My-Custom-vpc)	-
IAM Role	Subnet ID	
-	subnet-0b327234fe94dc34e (My-Custom-subnet-private1-us-east-1a)	

[Details](#) [Security](#) [Networking](#) [Storage](#) [Status checks](#) [Monitoring](#) [Tags](#)

Step 8. In order to connect it from public subnet we need to have the private key inside the public subnet file system, make a key.pem file

The screenshot shows a terminal window titled "Instance details | EC2 | us-east-1 | EC2 Instance Connect | us-east-1" with the URL "us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh". The terminal interface includes a top navigation bar with AWS services like EC2, Billing, RDS, EFS, VPC, and IAM, and a bottom status bar with "CloudShell" and "Feedback". The main area of the terminal shows a command-line session:

```
fec2-user@ip-10-0-1-17 ~]$ vi key.pem
```

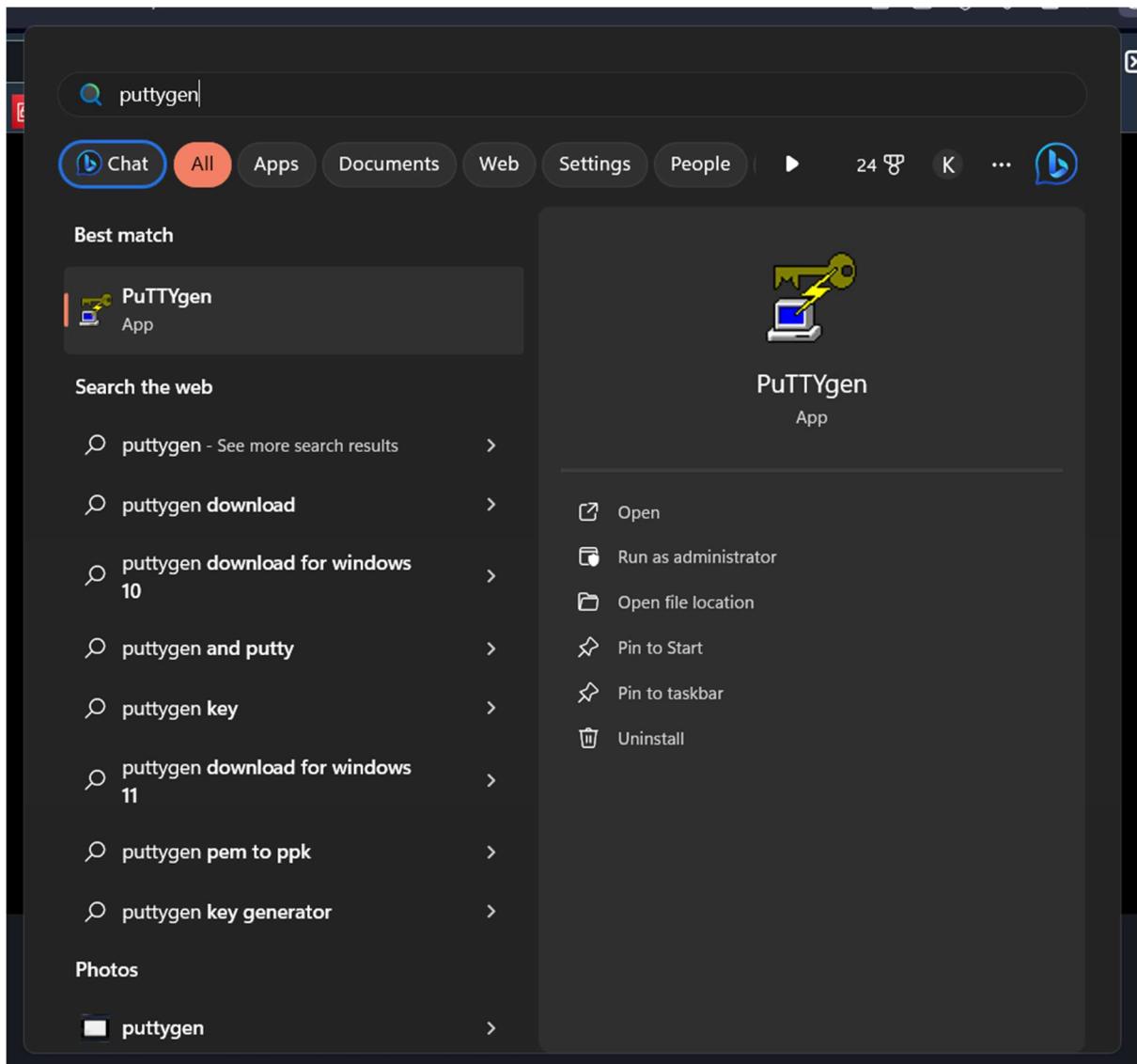
Below the terminal, a status bar displays the instance information:

i-038fe620fb367048f (rootlinuxbastion)
PublicIPs: 23.23.13.38 PrivateIPs: 10.0.1.17

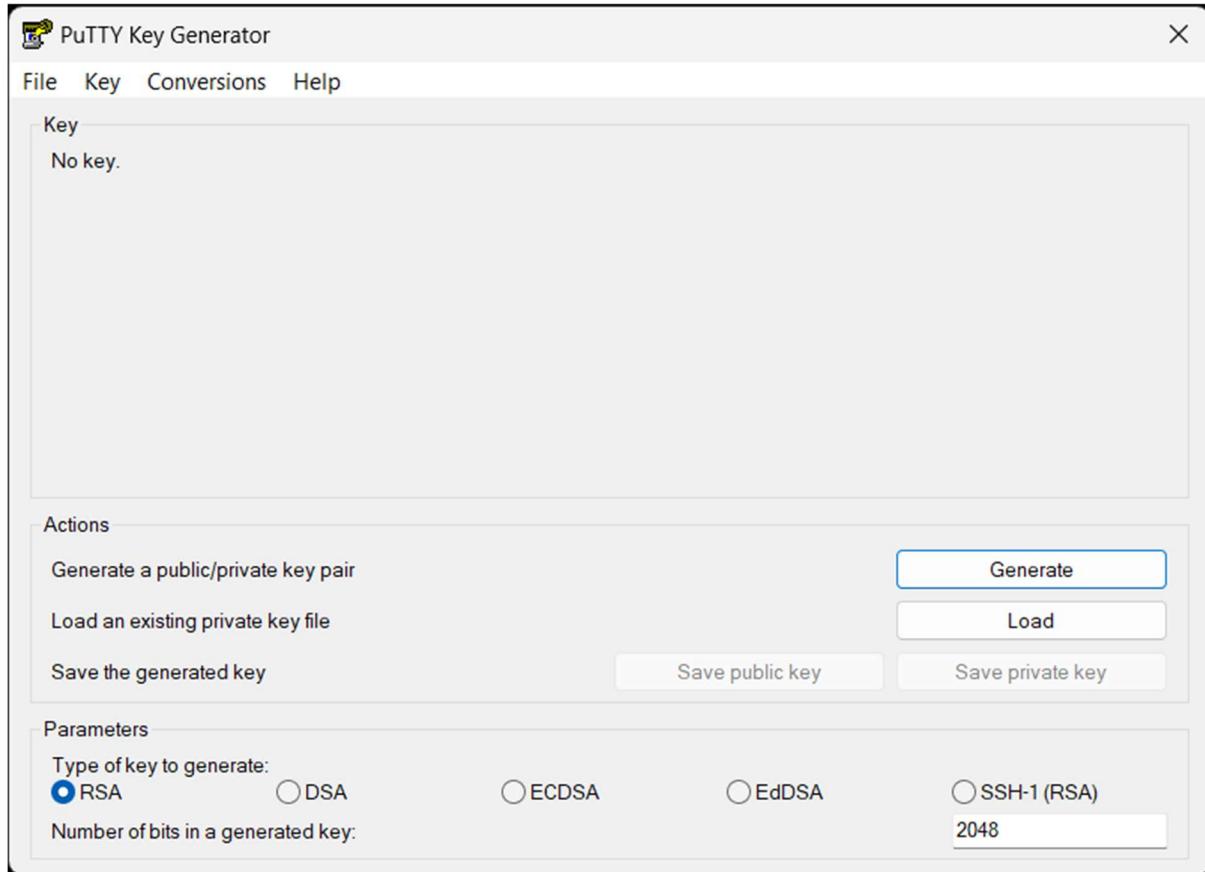
At the bottom right of the terminal window, there are links for "CloudShell", "Feedback", "© 2023, Amazon Web Services India Private Limited or its affiliates.", "Privacy", "Terms", and "Cookie preferences".

Step 9. If you are a windows user you need to convert your ppk file to pem file by using putty gen tool

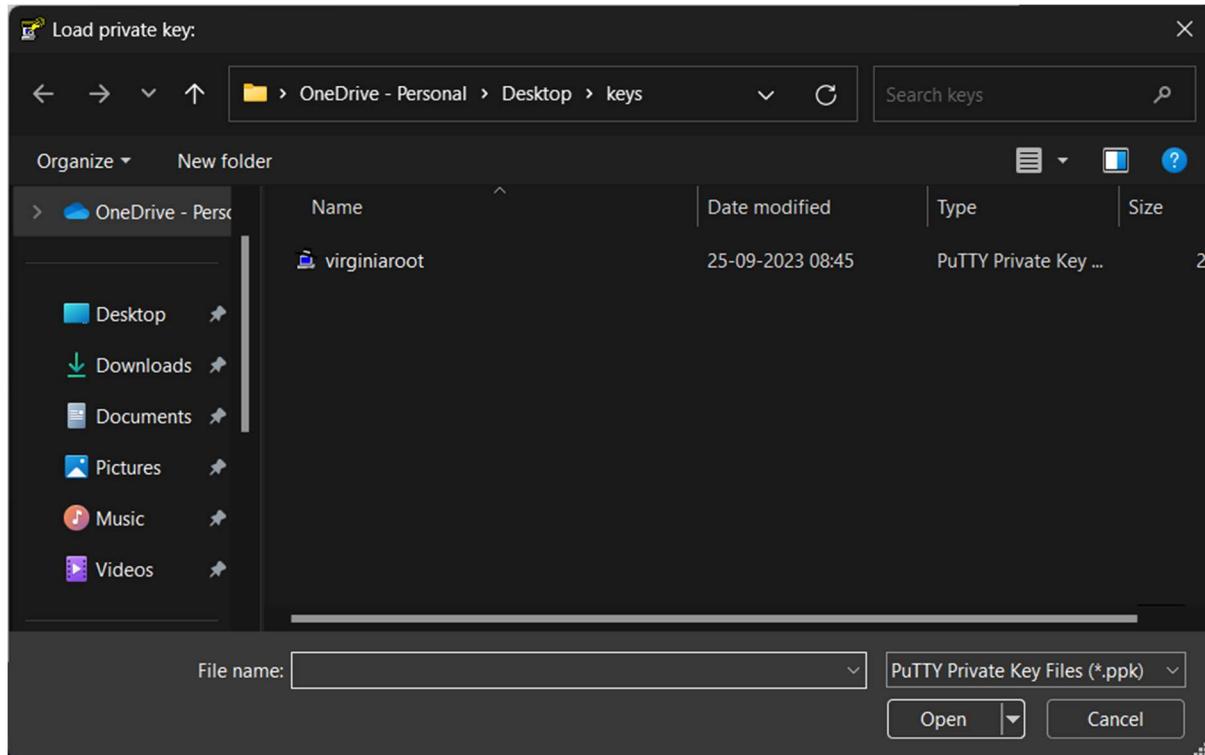
Open putty gen tool and load the ppk private key file



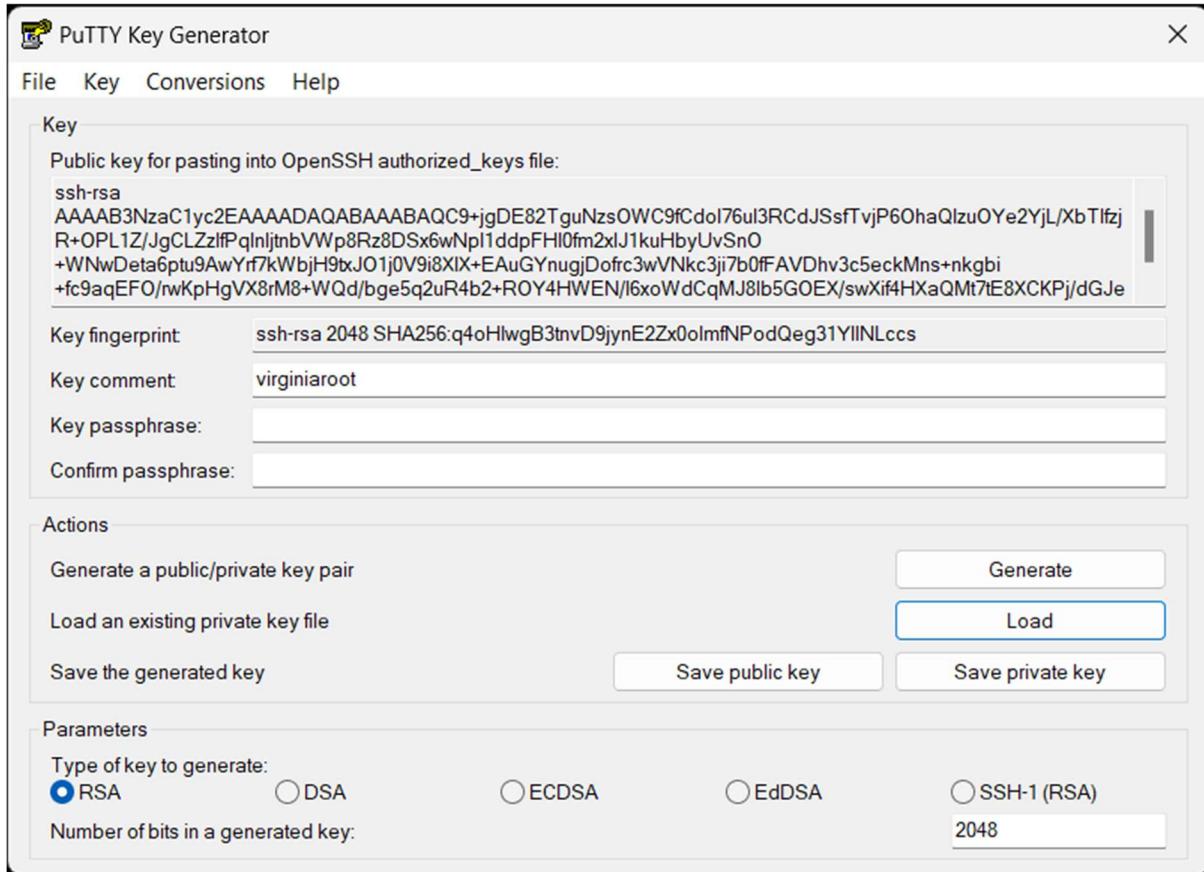
Step 10. Open putty gen tool



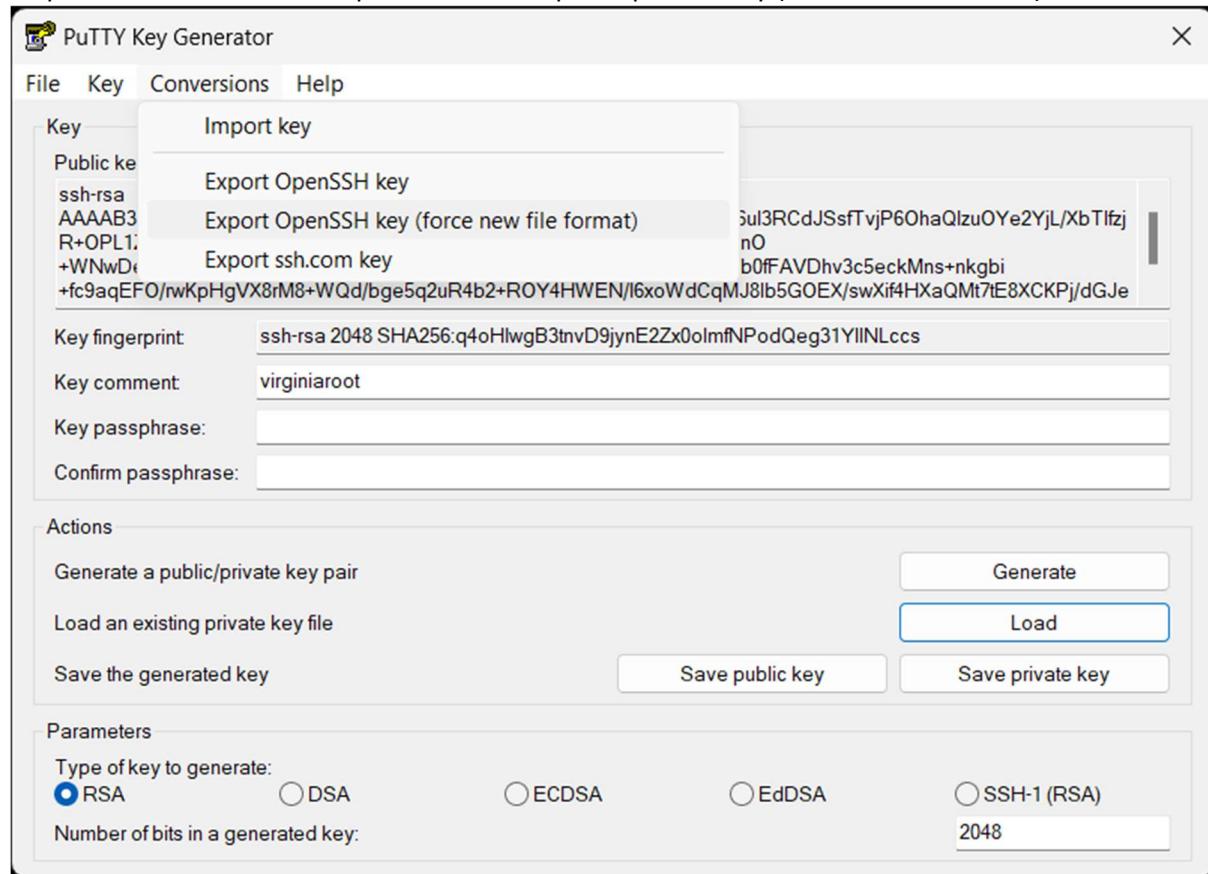
Step 11. load your ppk file



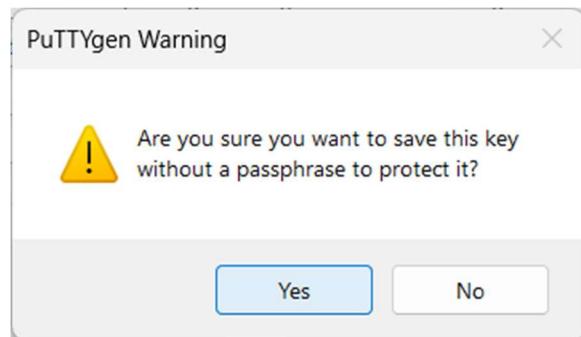
step 12.



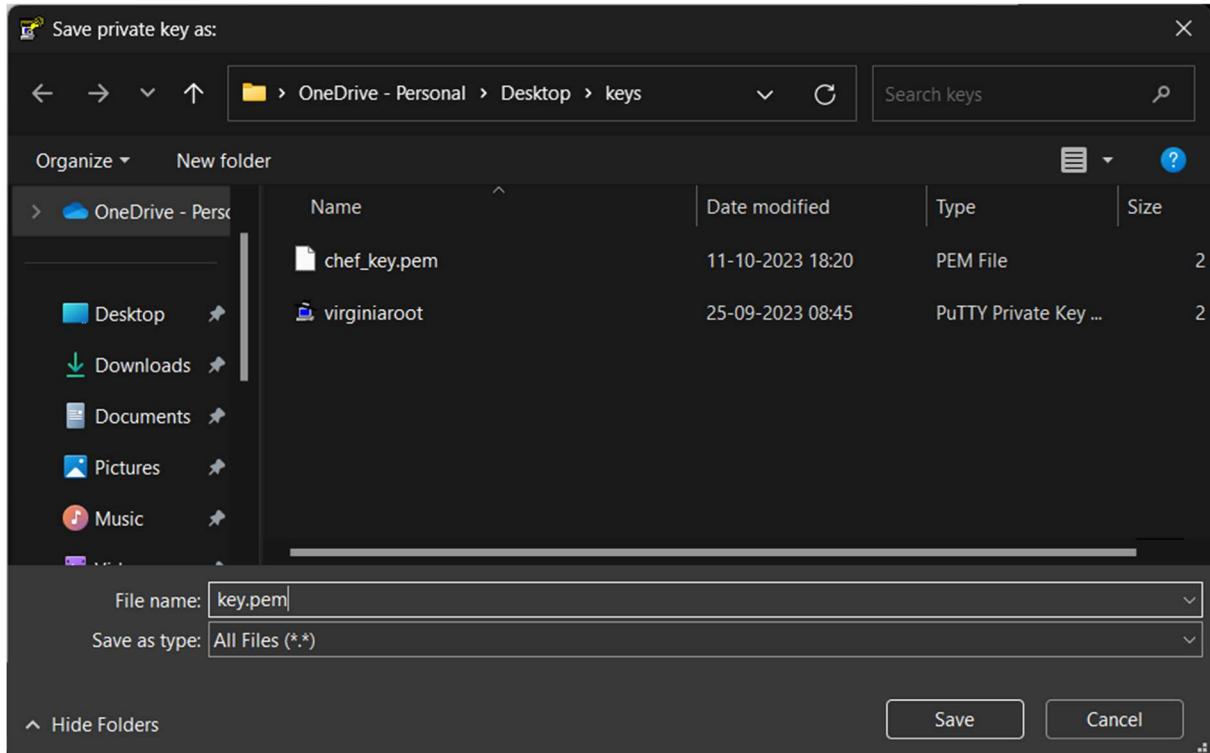
step 13. Under conversions options choose export OpenSSH key (force new file format)



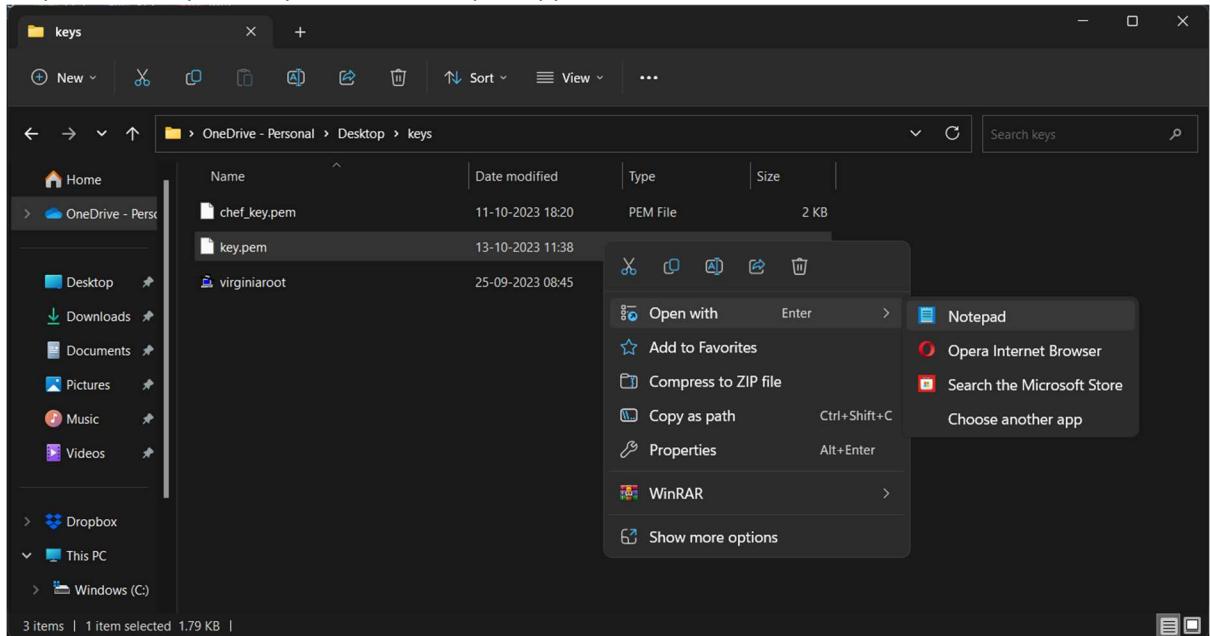
step 14. click yes, save it without passphrase



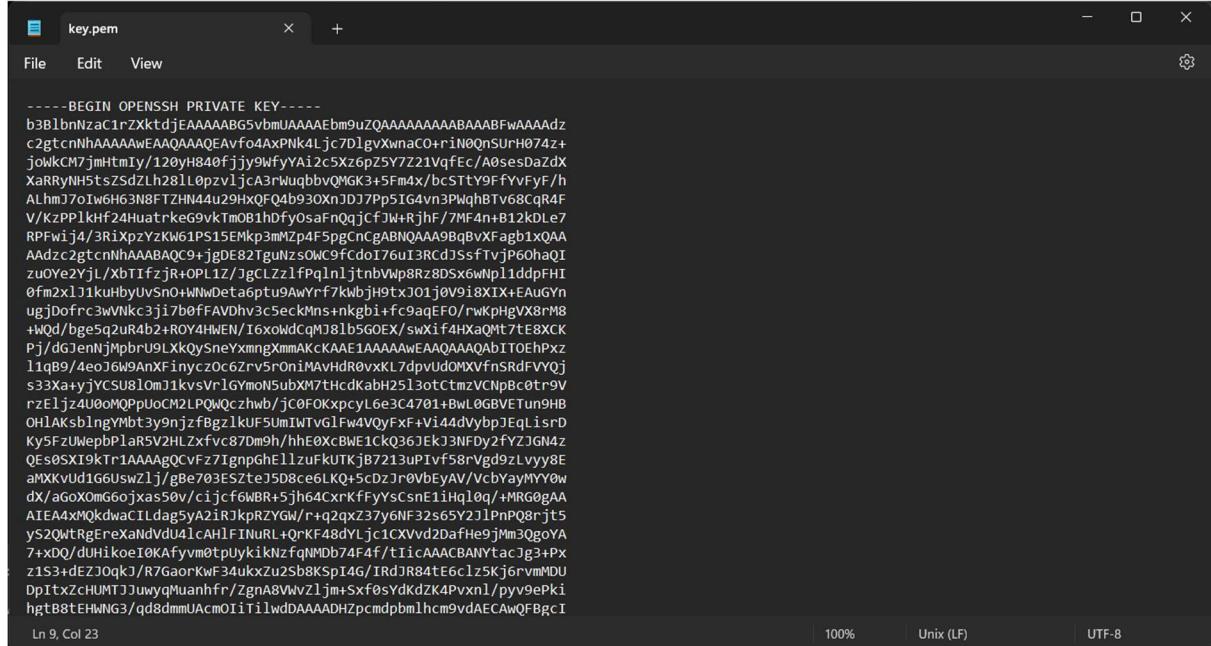
step 15. Save it as key.pem file



step 16. Now open the pem file in notepad app



step 17. Copy the content to clipboard

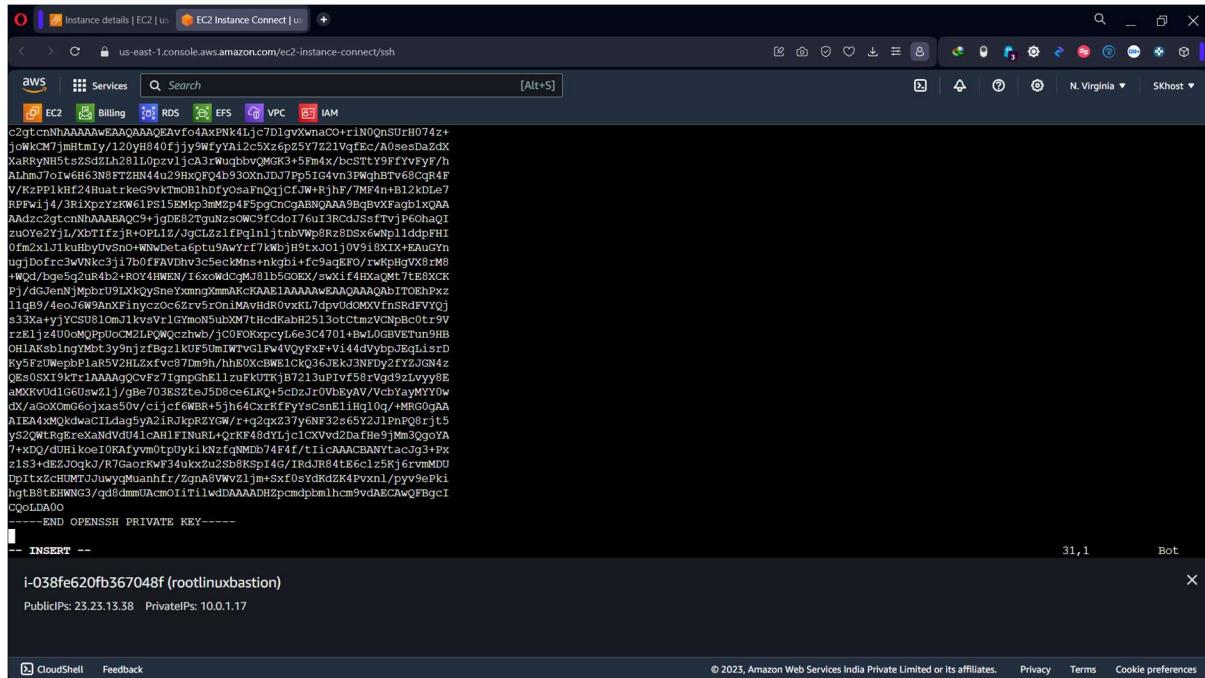


```
-----BEGIN OPENSSH PRIVATE KEY-----  
b3B1bnNzaC1rZXktbjEAAAAABG5bmUAAAAEb9uZQAAAAAAAAAABAAABFwAAAAdz  
c2gtcnhAAAAAwEAQAAAQEAvfo4AxPK4Ljc7DlxvKwnaCo+r+iN0QnsUrH074z+  
j0WkCM7jmhtmIy/120yh840fjjy9WfyYAi25xz6pZ5Y7Z21VqfEc/A0sesdaZdx  
XaRRyNH5tsZsdLh281l0pzv1ja3rWuqbbvQMGK3+5Fm4x/bcS1tY9FfyFyF/h  
ALhmJ7oIw6HG3NBFTZHN44u29HXQF04b930XnJDJ7Pp5IG4vn3PWhhBTv68CqR4F  
V/KzPPlkhF24Huatrkeg9vkTm0B1hbffyosafnqqjcfW+rjhF/_MF4+n+B12kDLe7  
RPfwij4/3RixpzyzKW61PS15Mkp3mZp4f5pgCncaBNQAA9BqbvFagb1xQA  
AAczc2gtcnhAAAABAc9+jgDE82tgUnzs0WC9fcdo176u13RcdJssfTvjp6OhaQI  
zu0Ye2yjl/XbTIfzjR+OPL1z/JgCLZz1fPg1n1jtnbWp8Rz8DsxewNplddpFHI  
0fUm2x1j1kuHbyUvSn0+NwNDea6ptu9AwYrf7kWbjH9txJ01j0V9i8IX+EAuGYN  
ugjDofrc3wNkc3ji7boffFAVDhv3cSeckMns+nkgbi+fc9aqEFO/rwKpHgVx8rm8  
+WQd/bge5q2uR4b2+ROY4HWEN/I6xowdcqM18lb5GOEX/swxf4HxaQmt7tE8XCK  
Pj/dGJenNjMpbru9LXkQysneXmnngXmmAkKAEE1AAAAbEAAQAAAQAbITOEhPxz  
11qB9/4eoJ6w9AnxFinyczo6Grv5On1MAvHdR0vxxL7dpUd0MXVfnSrdfVYoj  
s33Xa+tyjYCSU8lOm1jkvsVrlgymonSubxM7tHcdkabH2513otCtmzVCNpbC0tr9V  
rzEljz4U0oMQPpuoCM2LPQWQczhwb/jc0FOKxpcyL6e3C4701+BwL0GBVETun9HB  
OHIAKsb1ngYmbt3y9njzfbgZ1kuF5UmiWITvgfIwf4QyFx+f+vi44dybpJeqLisrD  
Ky5FzUWeppb1aRSV2HLZxfvc870m9h/hhE0xCBWE1CkQ36JEk13NFdy2fyZJGN4z  
QEs0SX19kTr1AAAAGQCFz7IgnpHe11zuFkUTKjB721suPiVvf58rVgd9zLyv8E  
aMXKVUD1G6Uszw1j/gB703ES2teJ5D8ce6LQ+5cDzJr0vbEyAV/VcbYayMYY0w  
dx/agoX0m6ojxass50v/cijcf6WBt-5jh64cxrKFfYyScsnE11hql0q/+MRG0gAA  
AIEA4xMqdwaCILdag5yA2iRjKpRYGw/r+q2qxZ37y6NF32s65Y2JlpnPQ8rjt5  
ys2QwtggEreXaNdvd41cAH1fInurl+QrKF48dYLj1cCXvd2dahfieqjMm3QgoYA  
7+xDQ/dUHicoeI0KAfym0tpuYikhnZfqNNDb74F4f/ticAAACBANYtacJg3+Px  
z1S3+dEZ0qk/JR7GaorKwf34ukxZu2Sb8KSpI4G/IRdJR84tE6clz5Kj0rvvMDU  
DpitxCHUMTJjuwygMuahfr/ZgnA8WwZ1jm+Sxf0sydkdzK4Pvxnl/pyv9ePki  
hgtB8tEHWN63/qd8dmmmuAcmmoIi1ilwdAAAAADHZpcmdpbmllhcm9vdAECAwQFBgcI
```

Ln 9, Col 3

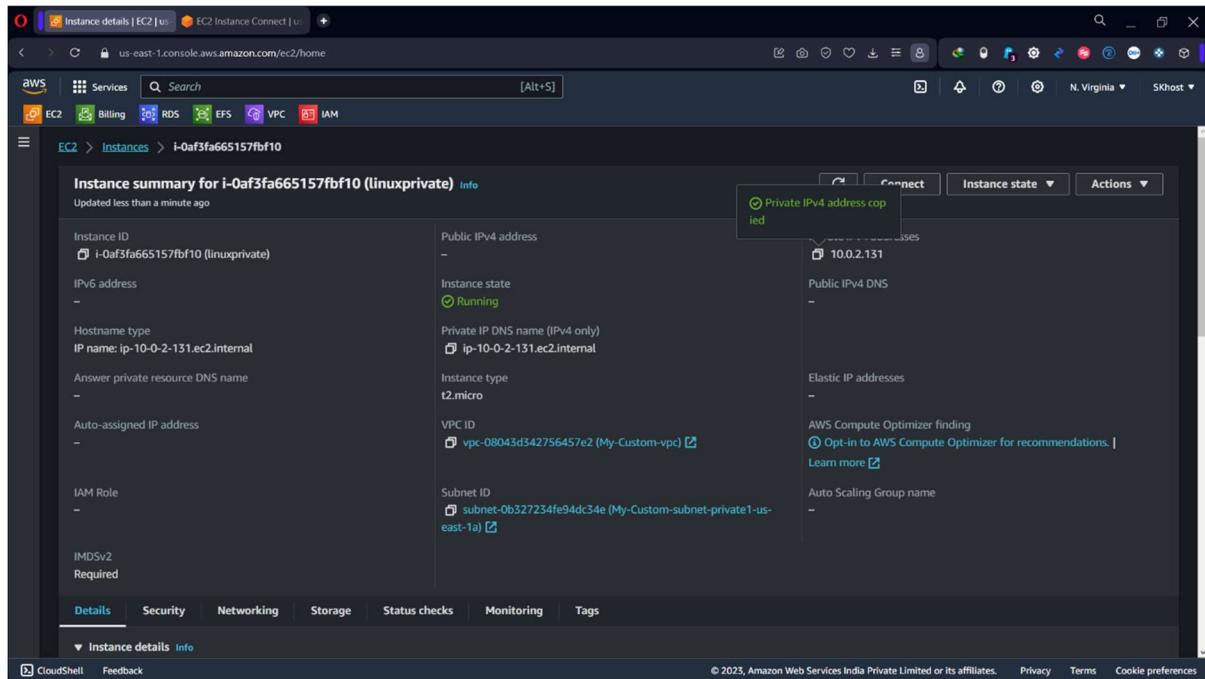
100% | Unix (LF) | UTF-8

step 18. paste the content on vi key.pem file inside public subnet ec2 terminal and save the file

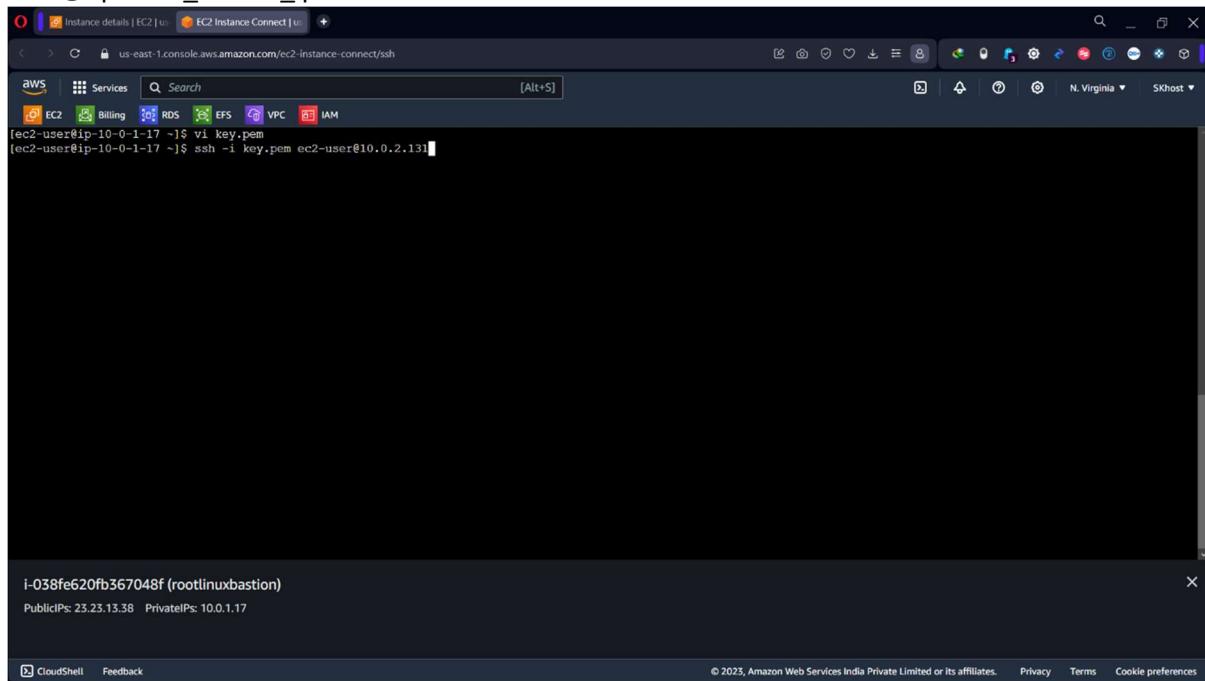


```
c2gtcmnhAAAAAwEAAQAAQAvfc44xNW4Ijc7DlgyWnaO+riN0nSURH074z+joWkCM7jmlmly/120yB840fjjy9WfyYai2c5Xz6pZ5Y7Z21VqfEc/A0sesDa2dXxaRvN5tsz3d1h281LopvJlCa3rWucpbvQmG3+5m4x/besTUV9FfVryFy/hAlIm7j0iW663N8FT2RN4u259XQrQb530XnJb7Tp51G4vn3WghbRv68cgR4FV/k2PP1khf24HufrkeG9vXm081hDiyosfaMrQjcfJW-Rhf/MFm+812kdLe7KpFW1j4/sR1xpz1zrkw1ps15wMcpSmwz45pqcn9AbnQAAA9bq9vxFaqbj1XJAADz2gtcmnhAAAQc9+jgD8z7guNs0C9ycdo16u1RCdJSsITVjP6OhaQ1zuYg2tj1/xbT1TzjR+oPL1z/Jgc1zz1fPg1nltnbvWp8Rz8DSxwNp1ldpPHI0fm2x1JkuuJdvsn0-WNWeptuAWY1f7kbjH9txJ0t0V918IX+EaUgynug)Defrcs3WNKc3j17b0FAVfhv35eckMns-nkgbi+fc9aqbFO/rwKphgvX8rm8+wg_dbe5g2+0YAHEN/16xowdcmJ81b5gOBX/swX1f4HXaQMT7LEBXCKP/dJenjhMprt91LXQySmrxmngXmaKcKAe1AAAAwEAAQAAQabiTOehPxz11gB9/4eoJGWAnXhinyzoc6zr5vzOnMAVihs0vx17dpvcdMXvfn5rdFVYqj33Xa+vjYCSU81lOm1kvsvrlgYm0n5ubM7thcdKab12513otCtmzvCNpBc0tr9VrzB1z400oMoPp1oCMLBzQzchzbw/iC0FOK9pcy16e3C4701+BwL0GBVETun9HB0HIAKsblmYMt3y9njzBgz1kUF5UmIWTVGLFw4VqyFxF+V144dvbypEqLijsrDKy+FzUWepbplarSV2HLzxvc87l7Sh/hhE0xCBWE1CKQ36.EKJNFdy2FYJGN4zQE50SX19KT1AAAAGqcVcz7IgpnpGhEl1zuuKuTKtjb7213uIrvf58rVgd9zIvvyy8EaMKVb1l6GUwsZLj/gb703ES52le5D8ce6LKQ+5cDzJr0VbhyV/VcbhyayMY0wDX/aGoxXmG6jxas15v0+ciJcf6WBr+5jh64CxrkffryyscsnEl1hql0g/+MRG0gAATEA1xQJQdwacILIdag7y21RzpkRZYGW/r+q2pxZ37y6Nz2s65Y2J1PnPQ8rjt5yS20WtrgfreXaNUVdU41CAII1INuRI+QrkF48dyLj1c1CXVvd2DafHe9JmM3QgoYA7+xDj/DUHikoeIOKAfvym0tpuykiKnzfQmND874F4f/ticAACBANYtacJg3+Pxz1s3+dE2JQyk/R7GaorKw34ukxu2s8KSp14G/IRduR84tE6c1z5K16rvMDUbpItxzCHUMTJJuwyMuahrz/Zgn8@WwZl1j+sxf0sYdKdZK4pxvn1/pv9ePkihgTBtEHWNG3/qd8dmnUAcmOti7iIwdDAAADH2pcmdphbmhc9vdACAwQFBgcICQ0LDAO0-----END OPENSSH PRIVATE KEY-----  
-- INSERT --  
i-038fe620fb367048f (rootlinuxbastion)  
Public IPs: 23.23.13.38 Private IPs: 10.0.1.17  
CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences
```

step 19. You need to copy the private ip address to clipboard



step 20. connect the private subnet from public subnet via ssh , ssh -l <pemkey>ec2-user@<private_subnet_ip>

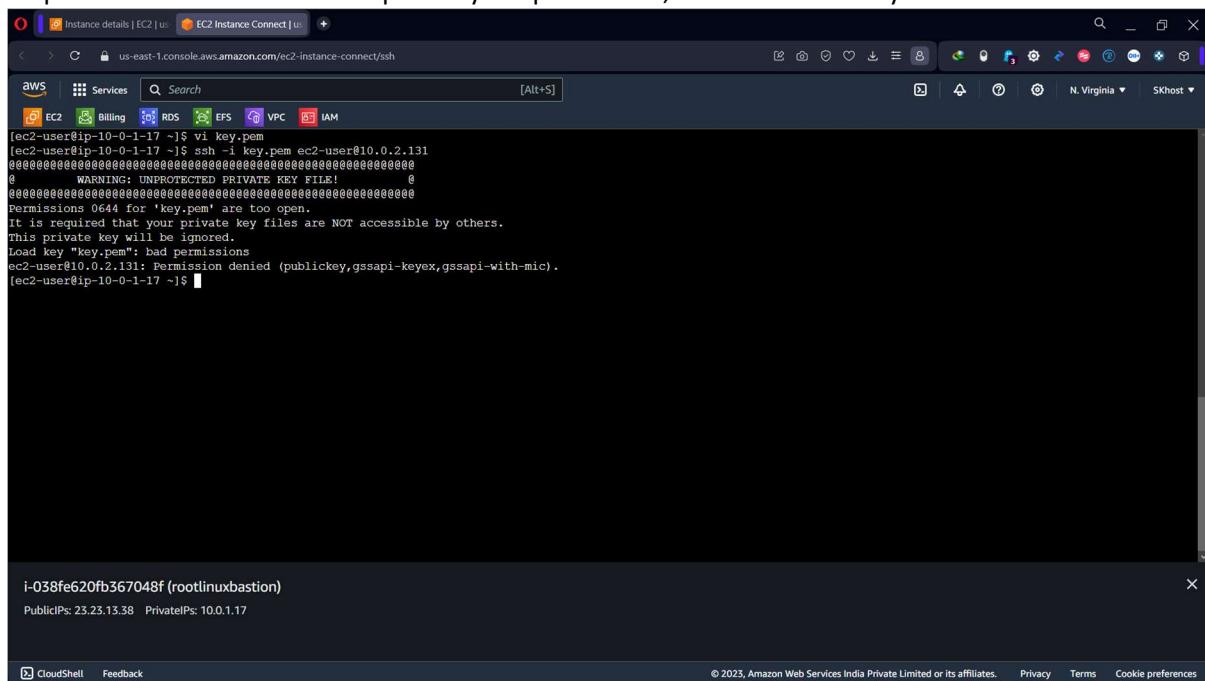


The screenshot shows a browser window for EC2 Instance Connect. The address bar is "us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh". The AWS navigation bar includes EC2, Billing, RDS, EFS, VPC, and IAM. The main area is a terminal window with the following content:

```
(ec2-user@ip-10-0-1-17 ~]$ vi key.pem
(ec2-user@ip-10-0-1-17 ~]$ ssh -i key.pem ec2-user@10.0.2.131
```

At the bottom of the terminal, it says "i-038fe620fb367048f (rootlinuxbastion)". Below the terminal, it shows "PublicIPs: 23.23.13.38 PrivateIPs: 10.0.1.17".

step 21. The error is due to the pem key file permission, it should have only read access

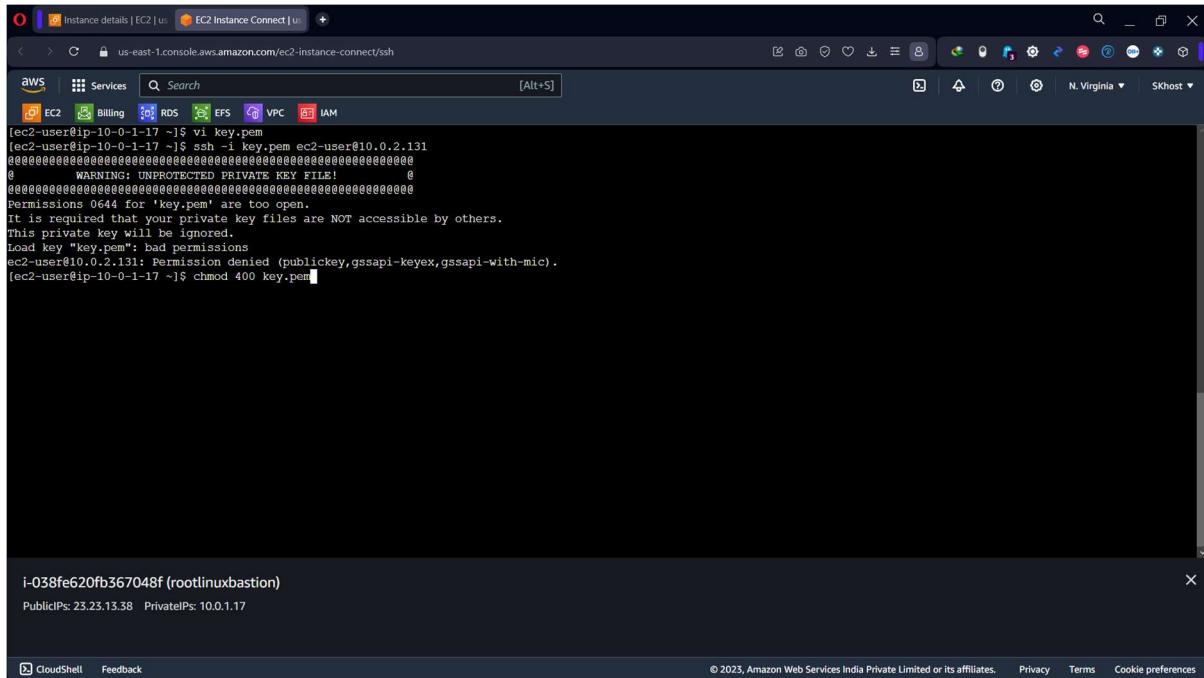


The screenshot shows a browser window for EC2 Instance Connect. The address bar is "us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh". The AWS navigation bar includes EC2, Billing, RDS, EFS, VPC, and IAM. The main area is a terminal window with the following content:

```
(ec2-user@ip-10-0-1-17 ~]$ vi key.pem
(ec2-user@ip-10-0-1-17 ~]$ ssh -i key.pem ec2-user@10.0.2.131
@@@@@@@WARNING: UNPROTECTED PRIVATE KEY FILE!
Permissions 0644 for 'key.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "key.pem": bad permissions
ec2-user@10.0.2.131: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
(ec2-user@ip-10-0-1-17 ~]$
```

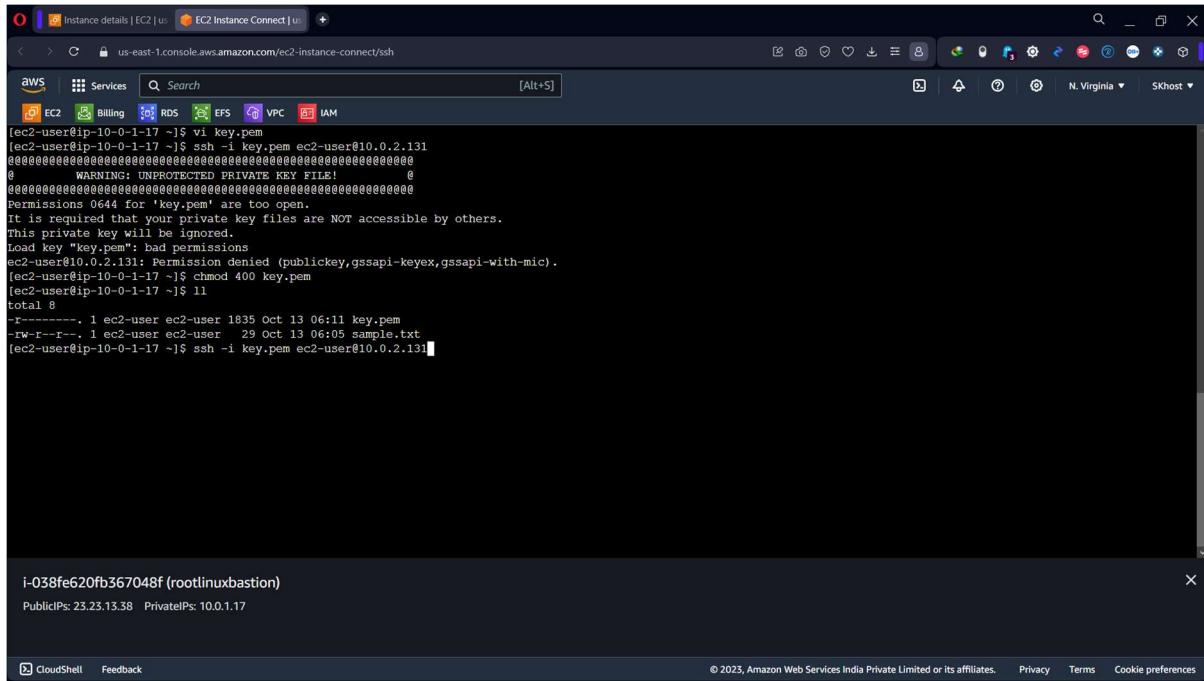
At the bottom of the terminal, it says "i-038fe620fb367048f (rootlinuxbastion)". Below the terminal, it shows "PublicIPs: 23.23.13.38 PrivateIPs: 10.0.1.17".

Step 22. Change the pem key file permission to read only access



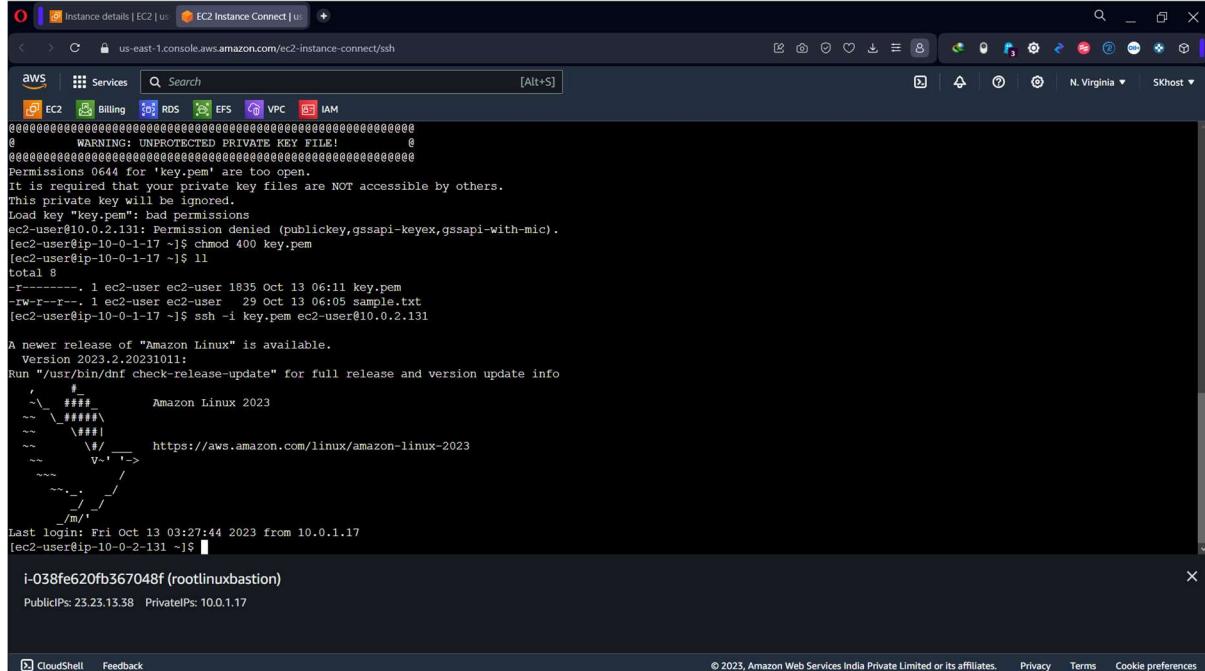
```
[ec2-user@ip-10-0-1-17 ~]$ vi key.pem
[ec2-user@ip-10-0-1-17 ~]$ ssh -i key.pem ec2-user@10.0.2.131
@@@@@@@WARNING: UNPROTECTED PRIVATE KEY FILE! @@@@
Permissions 0644 for 'key.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "key.pem": bad permissions
ec2-user@10.0.2.131: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[ec2-user@ip-10-0-1-17 ~]$ chmod 400 key.pem
```

step 23. Try to ssh into private subnet again



```
[ec2-user@ip-10-0-1-17 ~]$ vi key.pem
[ec2-user@ip-10-0-1-17 ~]$ ssh -i key.pem ec2-user@10.0.2.131
@@@@@@@WARNING: UNPROTECTED PRIVATE KEY FILE! @@@@
Permissions 0644 for 'key.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "key.pem": bad permissions
ec2-user@10.0.2.131: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[ec2-user@ip-10-0-1-17 ~]$ chmod 400 key.pem
[ec2-user@ip-10-0-1-17 ~]$ ll
total 8
-r-----. 1 ec2-user ec2-user 1835 Oct 13 06:11 key.pem
-rw-r--r--. 1 ec2-user ec2-user 29 Oct 13 06:05 sample.txt
[ec2-user@ip-10-0-1-17 ~]$ ssh -i key.pem ec2-user@10.0.2.131
```

step 24. Now we have successfully logged in as ec2-user at private subnet



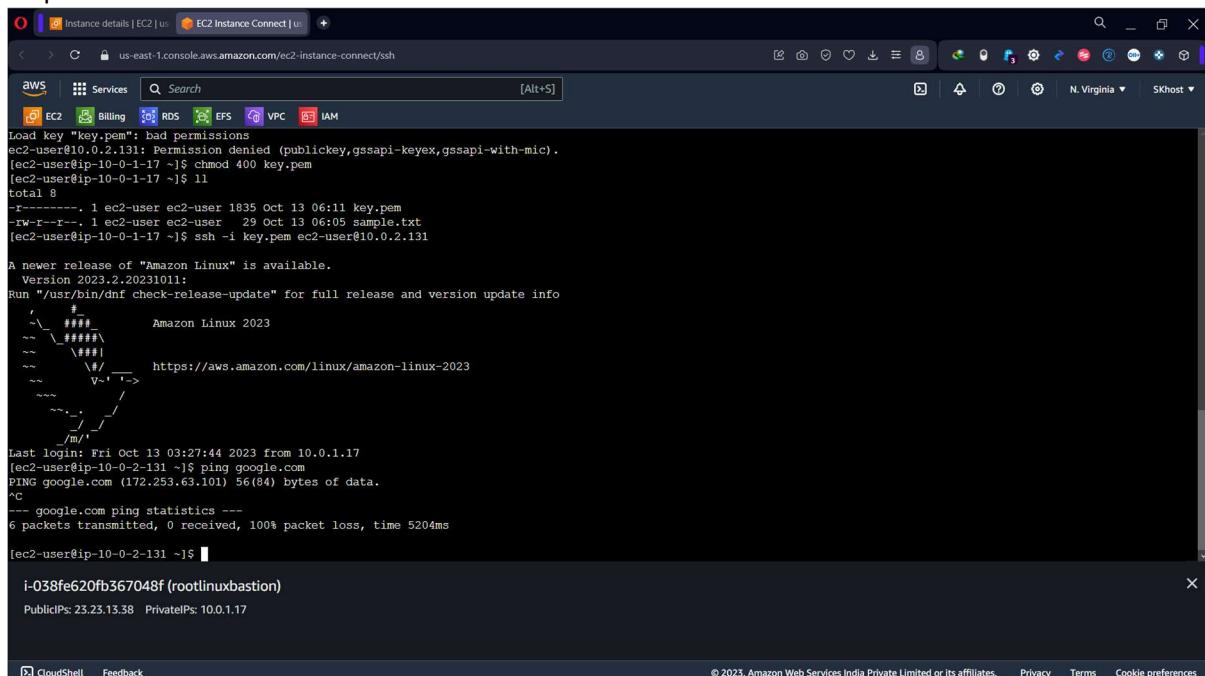
The screenshot shows the AWS CloudShell interface. The title bar says "Instance details | EC2 | us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh". The main area displays a terminal session:

```
WARNING: UNPROTECTED PRIVATE KEY FILE!
Permissions 0644 for 'key.pem' are too open.
it is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "key.pem": bad permissions
ec2-user@10.0.2.131: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[ec2-user@ip-10-0-1-17 ~]$ chmod 400 key.pem
[ec2-user@ip-10-0-1-17 ~]$ ll
total 8
-r----- 1 ec2-user ec2-user 1835 Oct 13 06:11 key.pem
-rw-r--r-- 1 ec2-user ec2-user 29 Oct 13 06:05 sample.txt
[ec2-user@ip-10-0-1-17 ~]$ ssh -i key.pem ec2-user@10.0.2.131

A newer release of "Amazon Linux" is available.
Version 2023.2.20231011:
Run "/usr/bin/dnf check-release-update" for full release and version update info
      _\###_
     /###\ Amazon Linux 2023
    /###\###\_____
   /###\###\###\_____
  /###\###\###\###\_____
 /###\###\###\###\###\_____
/###\###\###\###\###\###\_____
Last login: Fri Oct 13 03:27:44 2023 from 10.0.1.17
[ec2-user@ip-10-0-2-131 ~]$
```

At the bottom, it says "i-038fe620fb367048f (rootlinuxbastion)" and "PublicIPs: 23.23.13.38 PrivateIPs: 10.0.1.17".

step 25. Private subnet don't have internet access



The screenshot shows the AWS CloudShell interface. The title bar says "Instance details | EC2 | us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh". The main area displays a terminal session:

```
Load key "key.pem": bad permissions
ec2-user@10.0.2.131: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[ec2-user@ip-10-0-1-17 ~]$ chmod 400 key.pem
[ec2-user@ip-10-0-1-17 ~]$ ll
total 8
-r----- 1 ec2-user ec2-user 1835 Oct 13 06:11 key.pem
-rw-r--r-- 1 ec2-user ec2-user 29 Oct 13 06:05 sample.txt
[ec2-user@ip-10-0-1-17 ~]$ ssh -i key.pem ec2-user@10.0.2.131

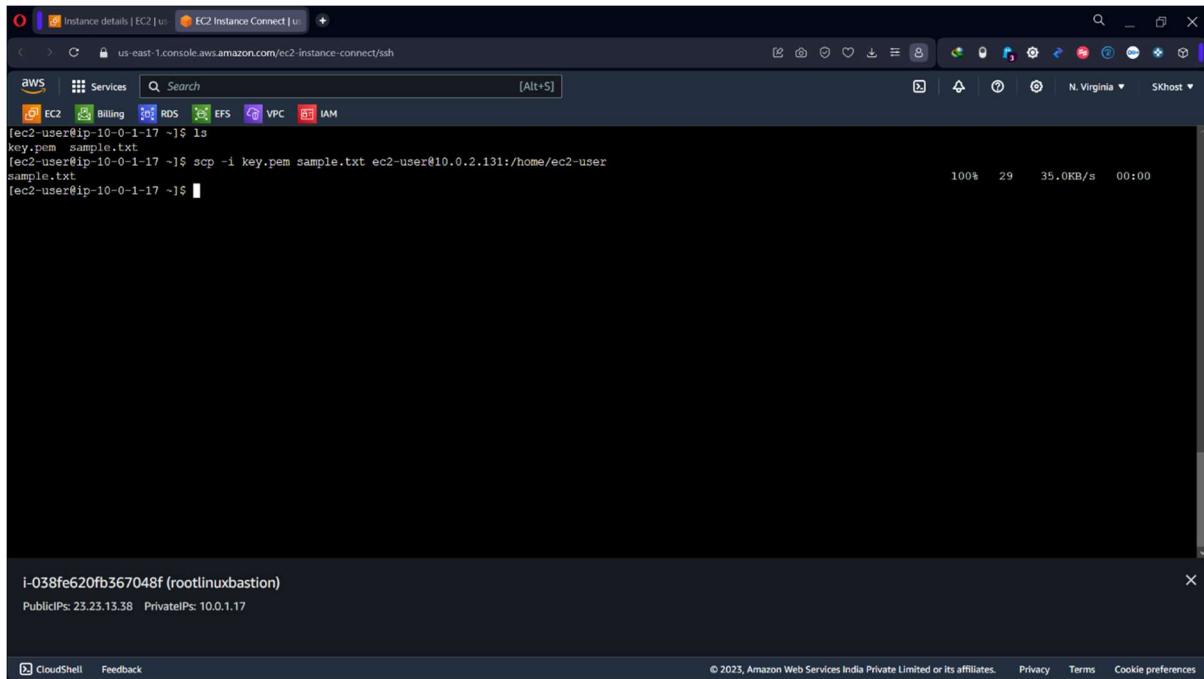
A newer release of "Amazon Linux" is available.
Version 2023.2.20231011:
Run "/usr/bin/dnf check-release-update" for full release and version update info
      _\###_
     /###\ Amazon Linux 2023
    /###\###\_____
   /###\###\###\_____
  /###\###\###\###\_____
 /###\###\###\###\###\_____
/###\###\###\###\###\###\_____
Last login: Fri Oct 13 03:27:44 2023 from 10.0.1.17
[ec2-user@ip-10-0-2-131 ~]$ ping google.com
PING google.com (172.253.63.101) 56(84) bytes of data.
^C
--- google.com ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5204ms

[ec2-user@ip-10-0-2-131 ~]$
```

At the bottom, it says "i-038fe620fb367048f (rootlinuxbastion)" and "PublicIPs: 23.23.13.38 PrivateIPs: 10.0.1.17".

step 26. exit the private subnet and come back to public subnet ,

now we will copy the sample.txt file from public instance to private instance using below commands at destination /home/ec2-user

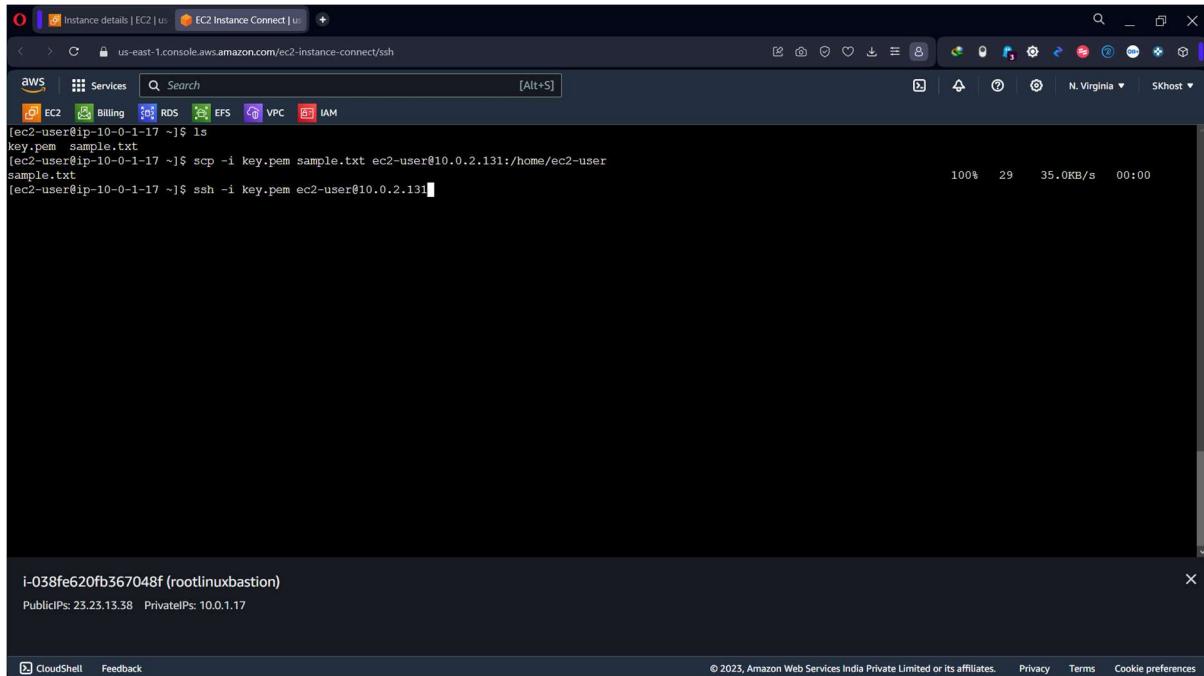


```
[ec2-user@ip-10-0-1-17 ~]$ ls
key.pem sample.txt
[ec2-user@ip-10-0-1-17 ~]$ scp -i key.pem sample.txt ec2-user@10.0.2.131:/home/ec2-user
sample.txt
[ec2-user@ip-10-0-1-17 ~]$
```

i-038fe620fb367048f (rootlinuxbastion)
Public IPs: 23.23.13.38 Private IPs: 10.0.1.17

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

step 27. The file have been copied

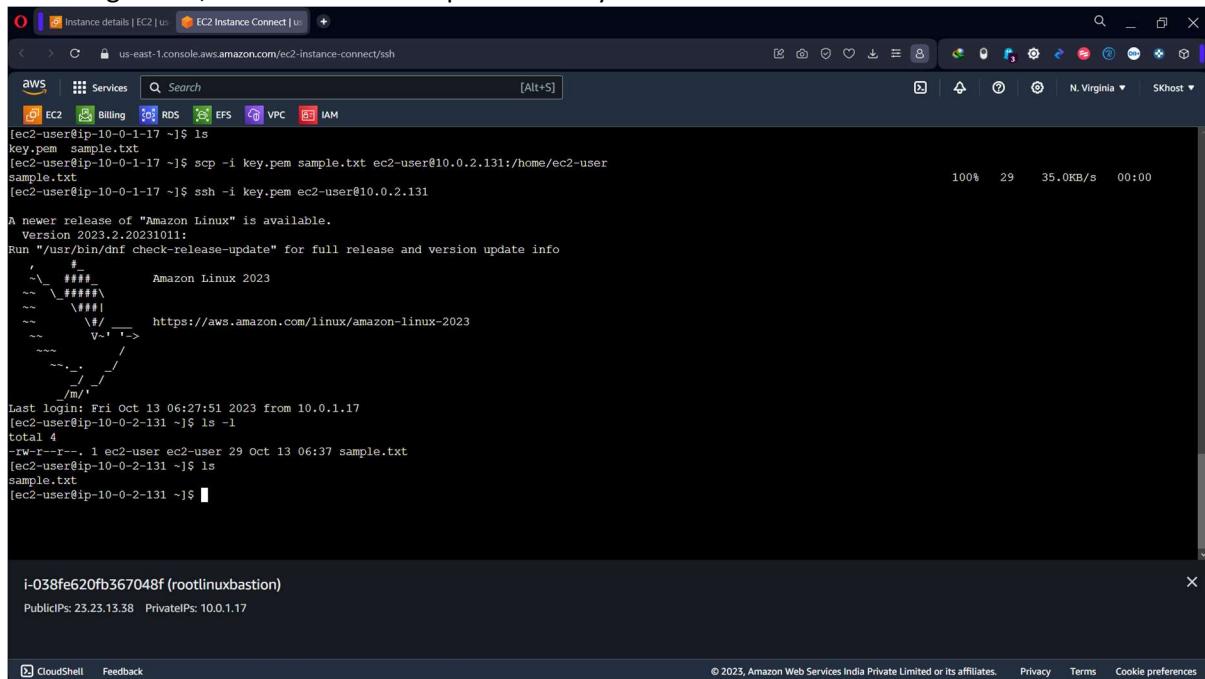


```
[ec2-user@ip-10-0-1-17 ~]$ ls
key.pem sample.txt
[ec2-user@ip-10-0-1-17 ~]$ scp -i key.pem sample.txt ec2-user@10.0.2.131:/home/ec2-user
sample.txt
[ec2-user@ip-10-0-1-17 ~]$ ssh -i key.pem ec2-user@10.0.2.131
```

i-038fe620fb367048f (rootlinuxbastion)
Public IPs: 23.23.13.38 Private IPs: 10.0.1.17

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

step 28. ssh into private instance like previously and check the location if the copied file has been reflecting or not, the file has been copied correctly.

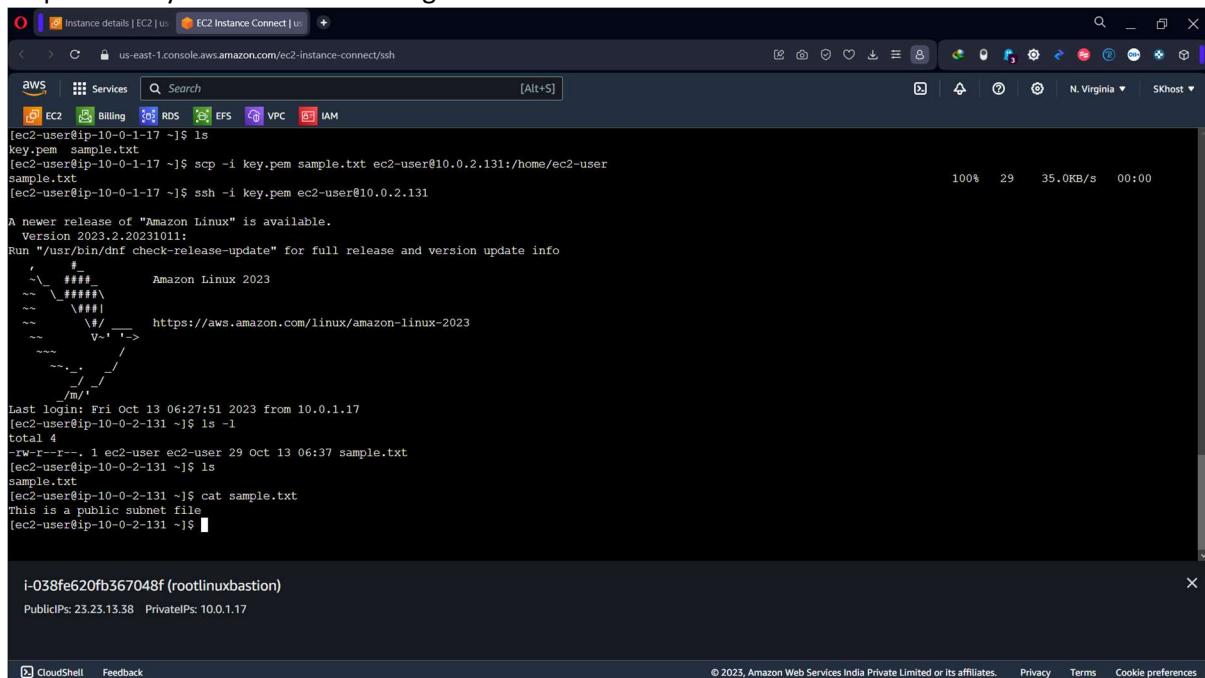


```
[ec2-user@ip-10-0-1-17 ~]$ ls
key.pem sample.txt
[ec2-user@ip-10-0-1-17 ~]$ scp -i key.pem sample.txt ec2-user@10.0.2.131:/home/ec2-user
sample.txt
[ec2-user@ip-10-0-1-17 ~]$ ssh -i key.pem ec2-user@10.0.2.131
A newer release of "Amazon Linux" is available.
Version 2023.2.20231011:
Run "/usr/bin/dnf check-release-update" for full release and version update info
      # 
      # Amazon Linux 2023
      # \###\
      #  \/
      #   V-->
      #   /
      #   / \
      #   /m/
Last login: Fri Oct 13 06:27:51 2023 from 10.0.1.17
[ec2-user@ip-10-0-2-131 ~]$ ls -l
total 4
-rw-r--r-- 1 ec2-user ec2-user 29 Oct 13 06:37 sample.txt
[ec2-user@ip-10-0-2-131 ~]$ ls
sample.txt
[ec2-user@ip-10-0-2-131 ~]$ 
```

i-038fe620fb367048f (rootlinuxbastion)
PublicIPs: 23.23.13.38 PrivateIPs: 10.0.1.17

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

step 29. Verify the file content using cat command



```
[ec2-user@ip-10-0-1-17 ~]$ ls
key.pem sample.txt
[ec2-user@ip-10-0-1-17 ~]$ scp -i key.pem sample.txt ec2-user@10.0.2.131:/home/ec2-user
sample.txt
[ec2-user@ip-10-0-1-17 ~]$ ssh -i key.pem ec2-user@10.0.2.131
A newer release of "Amazon Linux" is available.
Version 2023.2.20231011:
Run "/usr/bin/dnf check-release-update" for full release and version update info
      # 
      # Amazon Linux 2023
      # \###\
      #  \/
      #   V-->
      #   /
      #   / \
      #   /m/
Last login: Fri Oct 13 06:27:51 2023 from 10.0.1.17
[ec2-user@ip-10-0-2-131 ~]$ ls -l
total 4
-rw-r--r-- 1 ec2-user ec2-user 29 Oct 13 06:37 sample.txt
[ec2-user@ip-10-0-2-131 ~]$ ls
sample.txt
[ec2-user@ip-10-0-2-131 ~]$ cat sample.txt
This is a public subnet file
[ec2-user@ip-10-0-2-131 ~]$ 
```

i-038fe620fb367048f (rootlinuxbastion)
PublicIPs: 23.23.13.38 PrivateIPs: 10.0.1.17

CloudShell Feedback © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

step 30. The private subnet is unable to access the internet

A screenshot of the AWS CloudShell interface. The terminal window shows the command `ping google.com` being run. The output indicates a failed ping attempt:

```
[ec2-user@ip-10-0-2-131 ~]$ ping google.com
PING google.com (172.253.115.100) 56(84) bytes of data.
^C
--- google.com ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3158ms
[ec2-user@ip-10-0-2-131 ~]$
```

The CloudShell interface includes tabs for CloudShell and Feedback, and a footer with copyright information and links to Privacy, Terms, and Cookie preferences.

step31. Go to private subnet instance dashboard in aws console

A screenshot of the AWS EC2 Instances dashboard. The left sidebar shows navigation options like EC2 Dashboard, EC2 Global View, Events, Instances, Images, and Elastic Block Store. The main panel displays the instance summary for an instance named `i-0af3fa665157fbf10 (linuxprivate)`. Key details shown include:

Attribute	Value
Instance ID	<code>i-0af3fa665157fbf10 (linuxprivate)</code>
IPv6 address	-
Hostname type	IP name: <code>ip-10-0-2-131.ec2.internal</code>
Answer private resource DNS name	-
Auto-assigned IP address	-
IAM Role	-
IMDSv2 Required	-
Public IPv4 address	-
Instance state	Running
Private IP DNS name (IPv4 only)	<code>ip-10-0-2-131.ec2.internal</code>
Instance type	t2.micro
VPC ID	<code>vpc-08043d342756457e2 (My-Custom-vpc)</code>
Subnet ID	<code>subnet-0b327234fe94dc34e (My-Custom-subnet-private1-us-east-1a)</code>
Private IPv4 addresses	<code>10.0.2.131</code>
Public IPv4 DNS	-
Elastic IP addresses	-
AWS Compute Optimizer finding	<code>Opt-in to AWS Compute Optimizer for recommendations.</code>
Auto Scaling Group name	-

The bottom of the screen shows standard AWS footer links for CloudShell, Feedback, and cookie preferences.

step 32. We have not attached any gateway to the private routable for private subnet

The screenshot shows the AWS VPC Route Tables page. On the left, there's a sidebar with options like EC2 Global View, Virtual private cloud (Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, Peering connections), Security (Network ACLs), CloudShell, and Feedback.

The main content area shows a route table named "rtb-030aa83d37c89e3aa / My-Custom-rtb-private". The "Details" tab is selected, showing the following information:

Route table ID	rtb-030aa83d37c89e3aa	Main	No	Explicit subnet associations	subnet-0b327234fe94dc34e / My-Custom-subnet-private1-us-east-1a	Edge associations	-	
VPC	vpc-08043d342756457e2 My-Custom-vpc	Owner ID	617040060013					

Below the details, there are tabs for Routes, Subnet associations, Edge associations, Route propagation, and Tags. The Routes tab shows one route:

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

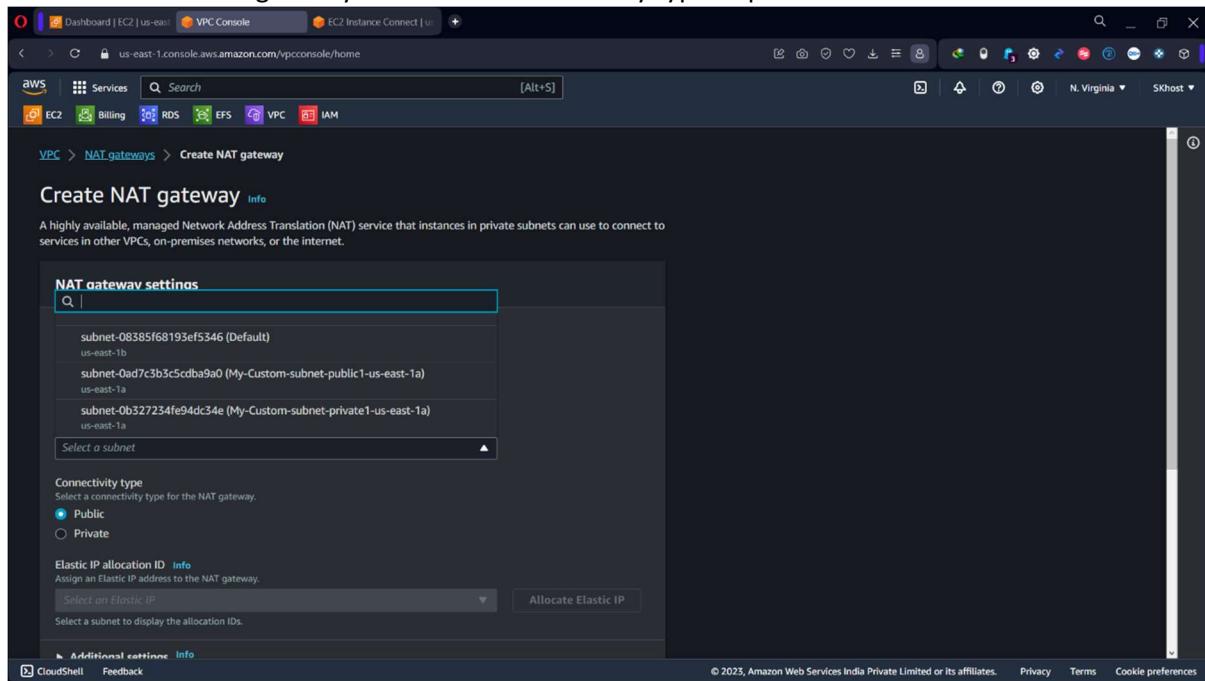
step 33. create a natgateway for private subnet and attach it to private routable

The screenshot shows the AWS NAT Gateways page. On the left, there's a sidebar with options like EC2 Global View, Virtual private cloud (Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, Peering connections), Security (Network ACLs, Security groups), DNS firewall (Rule groups, Domain lists), and Network Firewall (Firewalls, Firewall policies, Network Firewall rule groups, TLS inspection configurations).

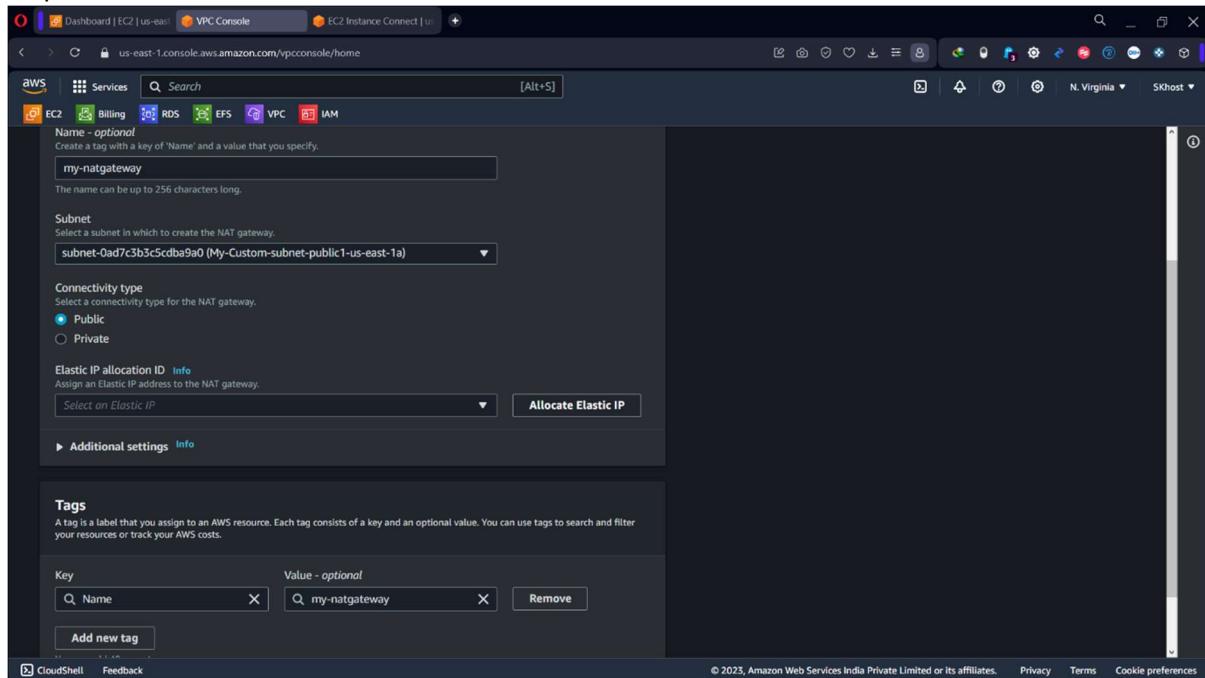
The main content area shows a table titled "NAT gateways" with the following columns: Name, NAT gateway ID, Connectivit..., State, State message, Primary public I..., Primary priv... The table currently displays "No NAT gateways".

At the bottom, there's a section titled "Select a NAT gateway" with three small icons.

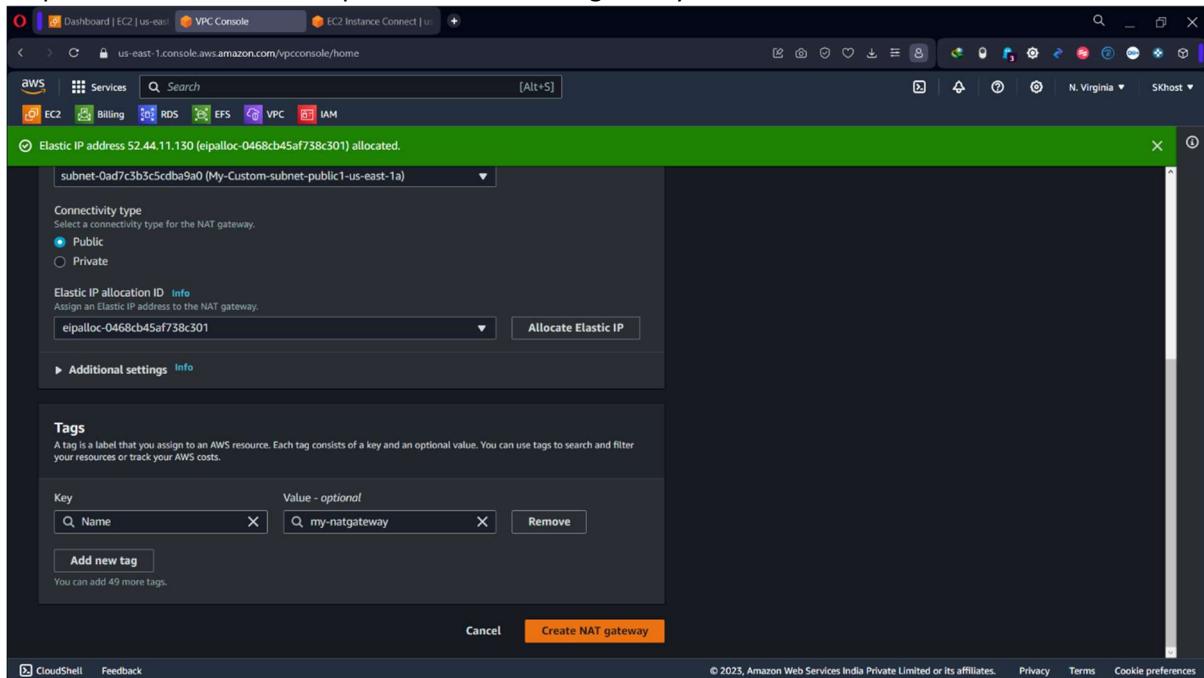
step 34. choose public subnet , since the natgateway needs a connection to the internet and public subnet have internetgateway and choose connectivity type as public



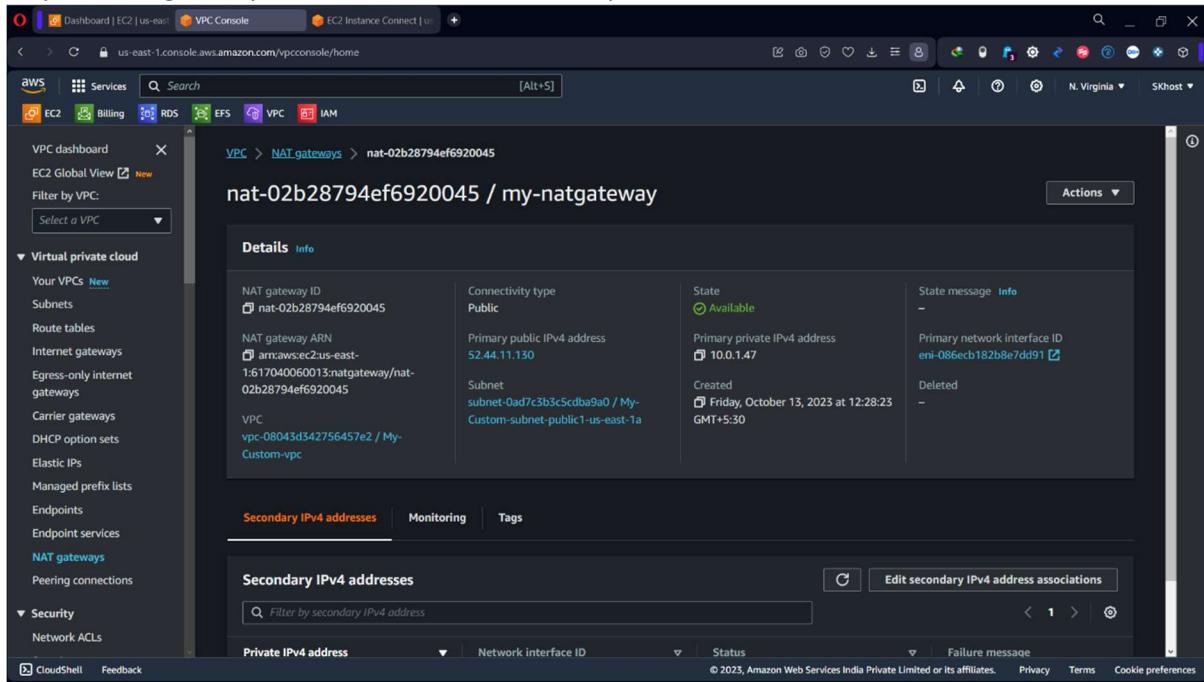
step 35.



step 36. Allocate an elastic ip address for the natgateway



step 37. NAT gateway has been created successfully



step 38. Go to private route table

The screenshot shows the AWS VPC Console interface. On the left, there's a sidebar with navigation links for EC2 Global View, Virtual private cloud (Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, Peering connections), Security (CloudShell, Feedback), and a CloudWatch Metrics section.

The main content area displays a route table named "rtb-030aa83d37c89e3aa / My-Custom-rtb-private". The "Details" tab is selected, showing the following information:

Route table ID	rtb-030aa83d37c89e3aa	Main	No	Explicit subnet associations	subnet-0b327234fe94dc34e / My-Custom-subnet-private1-us-east-1a	Edge associations	-
VPC	vpc-08043d342756457e2 My-Custom-vpc	Owner ID	617040060013				

Below the details, there are tabs for Routes, Subnet associations, Edge associations, Route propagation, and Tags. The Routes tab shows one route entry:

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

step 39. Attach the NAT gateway by editing the routes

The screenshot shows the "Edit routes" page for the same route table. The top navigation bar and sidebar are identical to the previous screenshot.

The main content area shows the "Edit routes" table with two entries:

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
Q 0.0.0.0/0	NAT Gateway	-	No

Below the table are buttons for "Add route" (which has been clicked), "Cancel", "Preview", and "Save changes".

step 40. Now we got internet access for private subnet

```
Instance details | EC2 | us-east-1 | VPC Console | EC2 Instance Connect | us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh [Alt+S] Services Search [Alt+S] EC2 Billing RDS EFS VPC IAM N. Virginia SKhost [CloudShell Feedback] © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences
```

```
[ec2-user@ip-10-0-2-131 ~]$ ping google.com
PING google.com (172.253.63.113) 56(84) bytes of data.
64 bytes from bi-in-f113.le100.net (172.253.63.113): icmp_seq=1 ttl=102 time=3.70 ms
64 bytes from bi-in-f113.le100.net (172.253.63.113): icmp_seq=2 ttl=102 time=2.63 ms
64 bytes from bi-in-f113.le100.net (172.253.63.113): icmp_seq=3 ttl=102 time=2.69 ms
64 bytes from bi-in-f113.le100.net (172.253.63.113): icmp_seq=4 ttl=102 time=2.66 ms
64 bytes from bi-in-f113.le100.net (172.253.63.113): icmp_seq=5 ttl=102 time=2.62 ms
64 bytes from bi-in-f113.le100.net (172.253.63.113): icmp_seq=6 ttl=102 time=2.63 ms
64 bytes from bi-in-f113.le100.net (172.253.63.113): icmp_seq=7 ttl=102 time=2.71 ms
64 bytes from bi-in-f113.le100.net (172.253.63.113): icmp_seq=8 ttl=102 time=3.64 ms
64 bytes from bi-in-f113.le100.net (172.253.63.113): icmp_seq=9 ttl=102 time=2.95 ms
^C
--- google.com ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8013ms
rtt min/avg/max/mdev = 2.622/2.915/3.696/0.414 ms
[ec2-user@ip-10-0-2-131 ~]$
```

i-038fe620fb367048f (rootlinuxbastion)
PublicIPs: 23.23.13.38 PrivateIPs: 10.0.1.17

step 41. we want to create a dedicated private security group for the private subnet

```
EC2 | us-east-1 | Connect to instance | EC2 Instance Connect | AWS Create NAT Gateway | us-east-1.console.aws.amazon.com/ec2/home [CloudShell Feedback] © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences
```

New EC2 Experience [Tell us what you think](#)

EC2 Dashboard
EC2 Global View
Events

Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations

Images
AMIs
AMI Catalog

Elastic Block Store
Volumes
Snapshots
Lifecycle Manager

EC2 > Security Groups > sg-033558ec8c3464cb5 - privatesg

sg-033558ec8c3464cb5 - privatesg Actions ▾

Details

Security group name privatesg	Security group ID sg-033558ec8c3464cb5	Description privatesg for private instance	VPC ID vpc-08045d342756457e2
Owner 617040060013	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules Outbound rules Tags

Inbound rules (1/1)

Name	Security group rule...	IP version	Type	Protocol	Port range
-	sgr-009f31452d81be1cb	IPv4	All ICMP - IPv4	ICMP	All

step 42. edit the inbound rules of private security group, so that private instance should be connected to internet via public instance and no other way for security purpose

The screenshot shows the AWS EC2 console with the URL us-east-1.console.aws.amazon.com/ec2/home. The navigation bar includes links for Connect to instance | EC2, EC2 Instance Connect | UI, and AWS Create NAT Gateway. The main menu has options like AWS, Services, Search, EC2, Billing, RDS, EFS, VPC, and IAM. The EC2 service is selected. Below the menu, the breadcrumb trail shows EC2 > Security Groups > sg-033558ec8c3464cb5 - privatesg > Edit inbound rules. The title is "Edit inbound rules" with an "Info" link. A sub-header states: "Inbound rules control the incoming traffic that's allowed to reach the instance." The main content area is titled "Inbound rules" with an "Info" link. It displays two rules:

Security group rule ID	Type Info	Protocol Info	Port range	Source Info	Description - optional Info
sgr-009f31452d81be1cb	All ICMP - IPv4	ICMP	All	Custom	<input type="text" value="103.172.209.121/32"/> X
-	SSH	TCP	22	Custom	<input type="text" value="10.0.1.0/24"/> X

At the bottom, there are buttons for "Add rule", "Cancel", "Preview changes", and "Save rules". The footer includes links for CloudShell, Feedback, and copyright information: © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences.