TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

BÁO CÁO THỰC HÀNH

Bài thực hành số 1: Dùng Terraform và CloudFormation để quản lý và triển khai hạ tầng AWS

Môn học: Công nghệ DevOps và Ứng dụng

Lớp: NT548.P11.MMCL

THÀNH VIÊN THỰC HIỆN (Nhóm 21):

STT	Họ và tên	MSSV
1	Lê Triệu Vỉ	21522785
2	Lý Thế Nguyên	21522389

Điểm tự đánh giá
9

ĐÁNH GIÁ KHÁC:

Tổng thời gian thực hiện	
Phân chia công việc	
Ý kiến *(nếu có)* + Khó khăn + Đề xuất, kiến nghị	

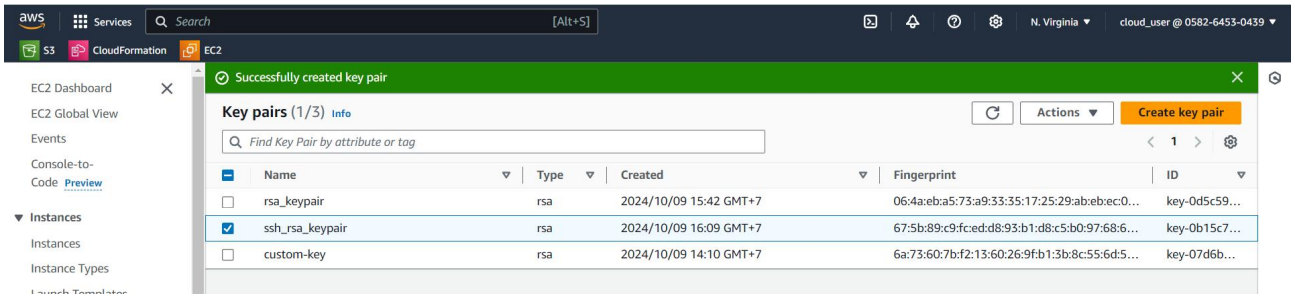
Phần bên dưới của báo cáo này là báo cáo chi tiết của nhóm thực hiện

A. BÁO CÁO CHI TIẾT

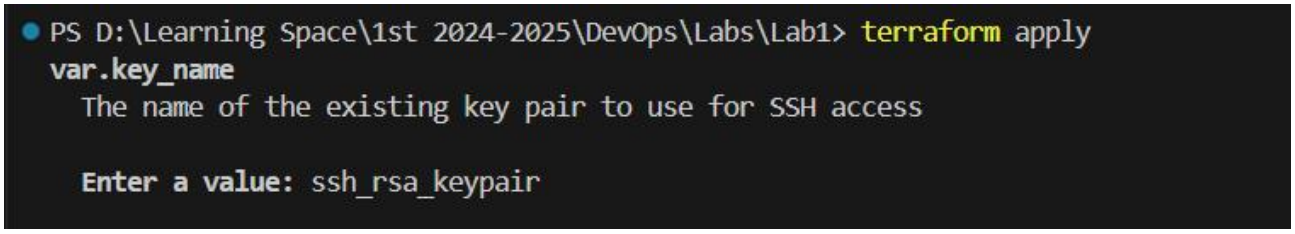
CHI TIẾT SOURCE CODE: https://github.com/just-vile/NT548-Labs.git

Quản lý và triển khai hạ tầng AWS bằng Teraform

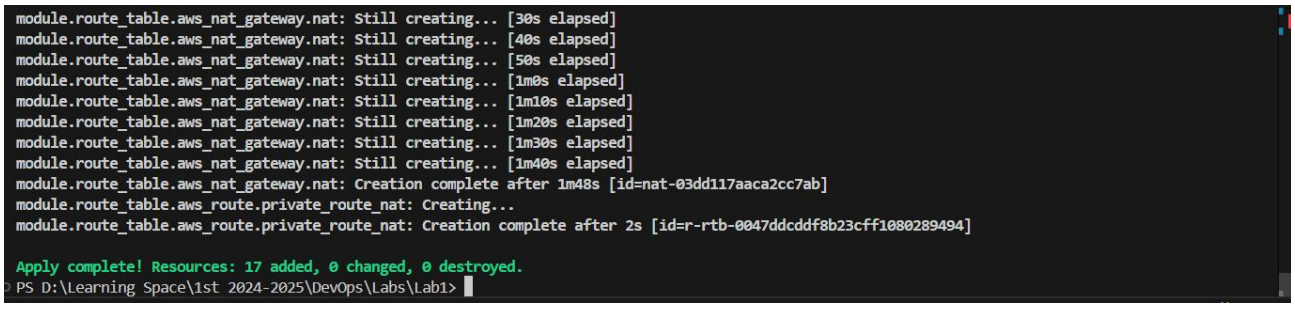
Đầu tiên, tạo cặp keypair từ AWS Dashboard, sau đó tải file key .pem về máy.



Sau đó, khởi tạo 'terraform init' rồi 'terraform apply' (source code trong file GitHub)



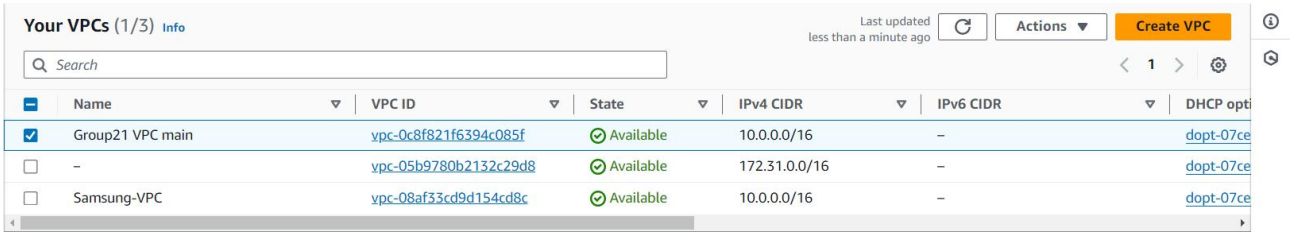
Nhập keypair cần sử dụng cho SSH. Khởi tạo các dịch vụ thành công!



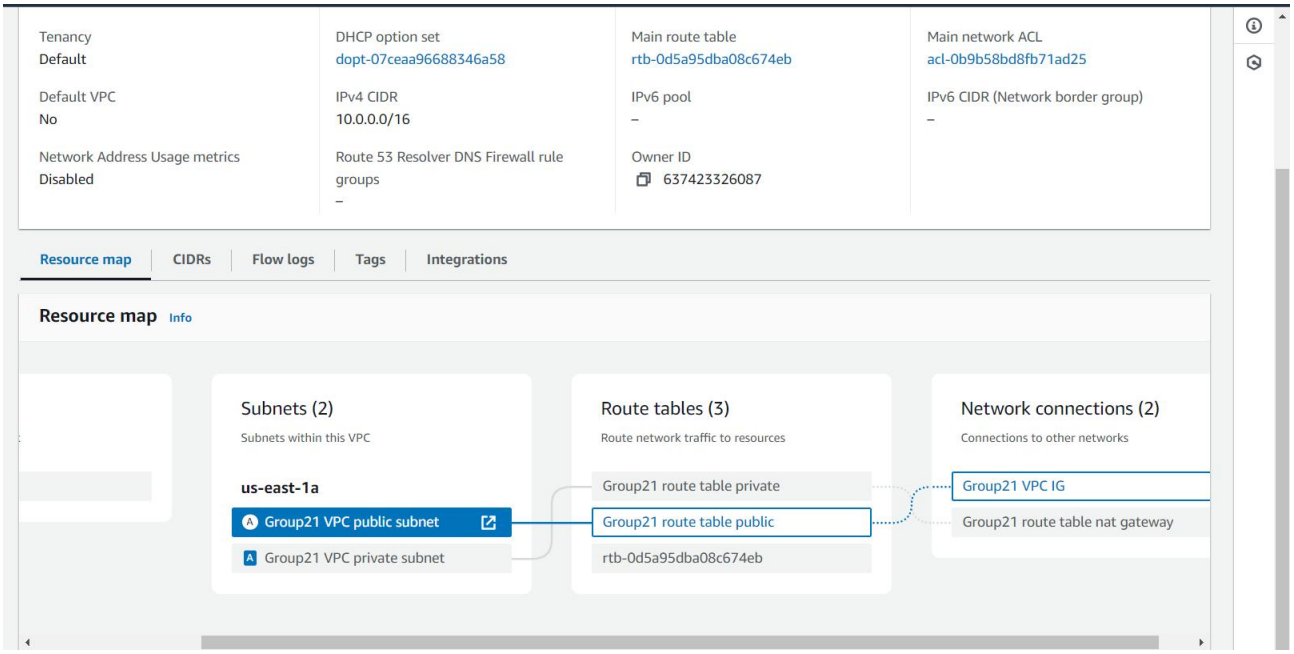
Ta sẽ kiểm tra chi tiết từng dịch vụ đã triển khai.

VPC:

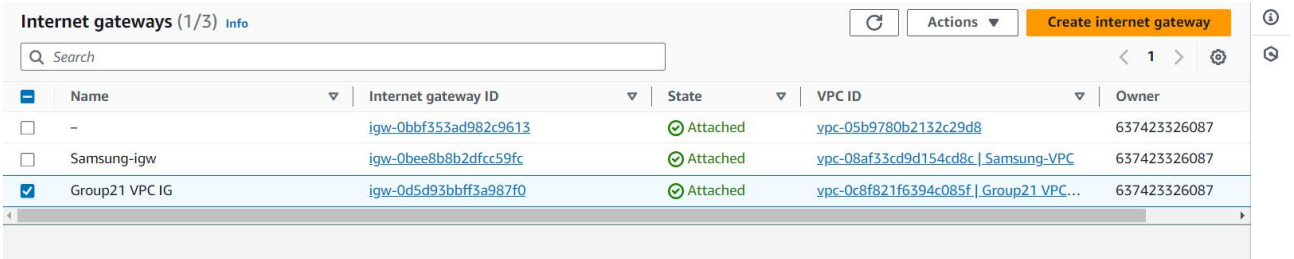
- **VPC:** Tạo một VPC chứa các thành phần sau (3 điểm):
  - Subnets: Bao gồm cả Public Subnet (kết nối với Internet Gateway) và Private Subnet (sử dụng NAT Gateway để kết nối ra ngoài).
  - Internet Gateway: Kết nối với Public Subnet để cho phép các tài nguyên bên trong có thể truy cập Internet.
  - Default Security Group: Tạo Security Group mặc định cho VPC



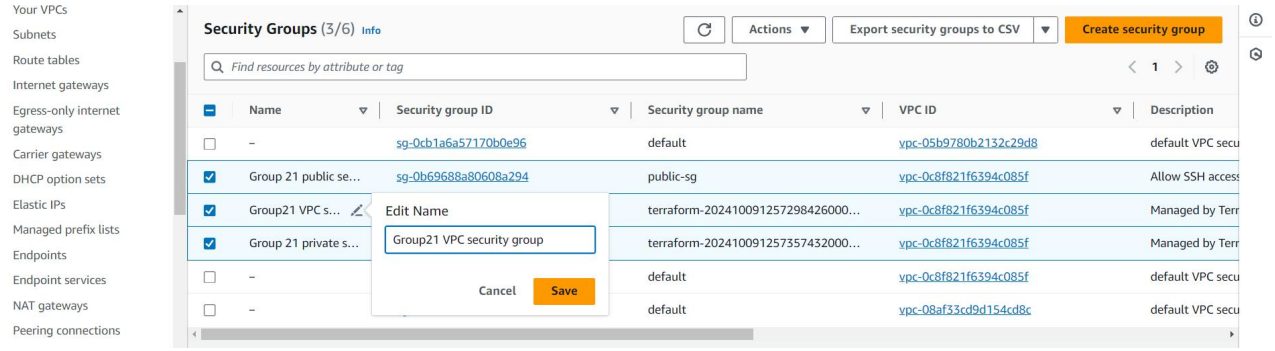
VPC đã được khởi tạo thành công.



Kiểm tra các connections trong VPC thì thấy public subnet kết nối ra internet gateway, còn private subnet thì kết nối đến NAT Gateway để kết nối ra ngoài.



Internet gateway đã được khởi tạo để kết nối ra ngoài.

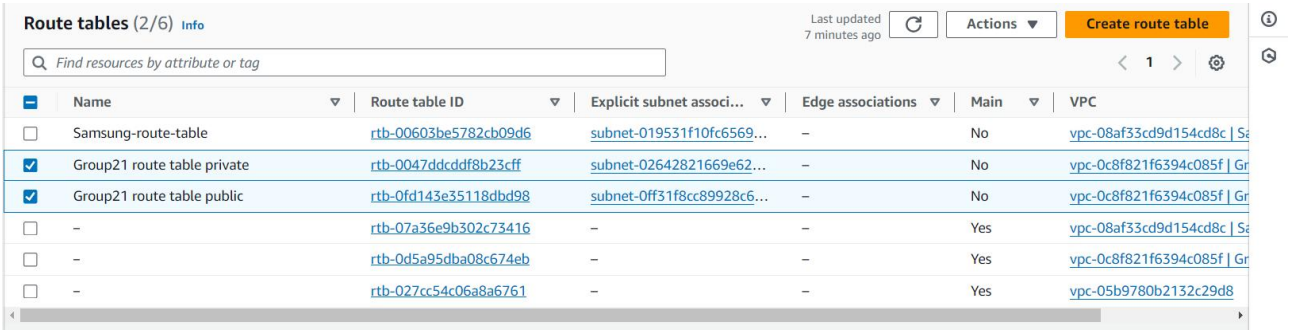


Security Group mặc định cho VPC.

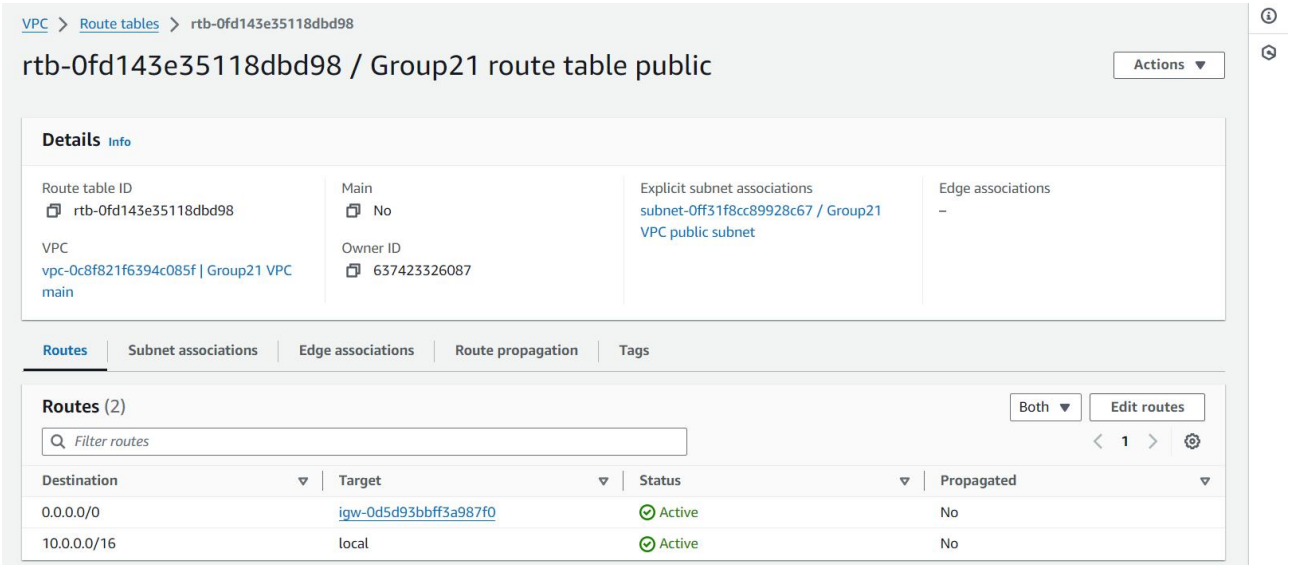
Vậy các VPC đã được cấu hình thành công!

Route Table:

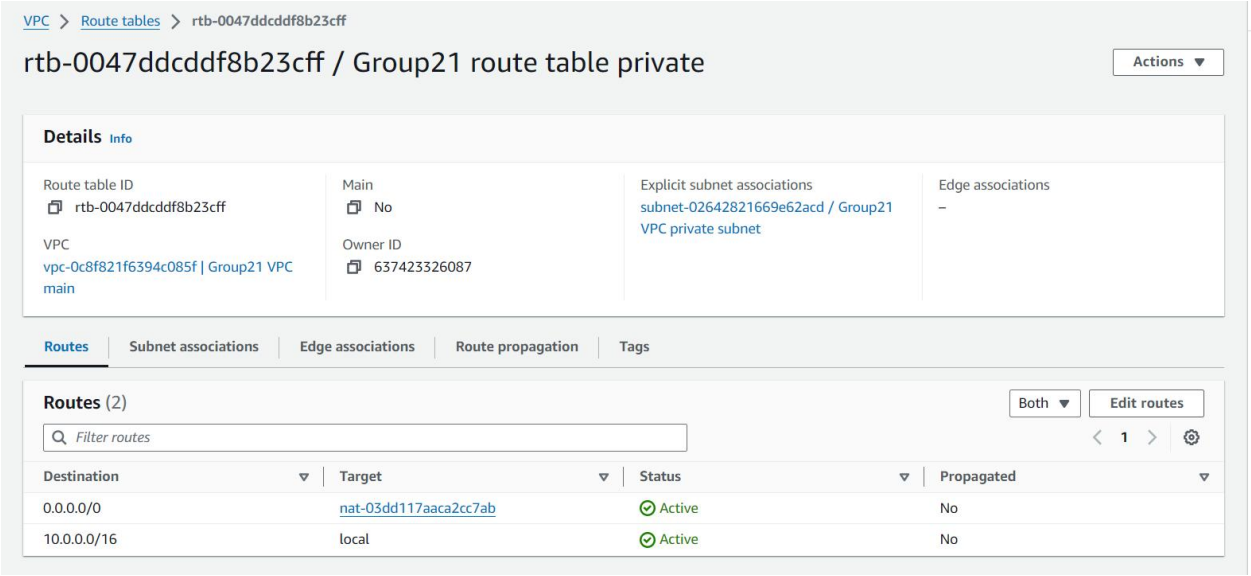
- **Route Tables:** Tạo Route Tables cho Public và Private Subnet (2 điểm):
  - Public Route Table: Định tuyến lưu lượng Internet thông qua Internet Gateway.
  - Private Route Table: Định tuyến lưu lượng Internet thông qua NAT Gateway.



Các route tables đã được khởi tạo thành công!



Public Route Table định tuyến lưu lượng thông qua Internet Gateway.



Private Route Table định tuyến lưu lượng thông qua NAT Gateway.

Vậy các Route Table đã được cấu hình thành công!

NAT Gateway:

- **NAT Gateway:** Cho phép các tài nguyên trong Private Subnet có thể kết nối Internet mà vẫn bảo đảm tính bảo mật (1 điểm).

```
ubuntu@ip-10-0-2-16:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=2.78 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=2.01 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=1.76 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=2.01 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.761/2.139/2.782/0.384 ms
ubuntu@ip-10-0-2-16:~$
```

Từ private EC2 instance, ta có thể kết nối đến internet. Kết nối đều đi qua NAT Gateway nên tính bảo mật vẫn sẽ được đảm bảo.

Vậy NAT Gateway đã được cấu hình thành công!

EC2 Instances:

- **EC2:** Tạo các instance trong Public và Private Subnet, đảm bảo Public instance có thể truy cập từ Internet, còn Private instance chỉ có thể truy cập từ Public instance thông qua SSH hoặc các phương thức bảo mật khác (2 điểm).

```
ASUS@LAPTOP-299D0RSV MINGW64 /d/Learning Space/1st 2024-2025/DevOps/Labs/Lab1
$ ssh -i ssh_rsa_keypair.pem ubuntu@54.208.58.235
The authenticity of host '54.208.58.235 (54.208.58.235)' can't be established.
ED25519 key fingerprint is SHA256:zQRIkDIRKDDVmxYtFFSlWfkxk65RGxxpV1gGEKe+fN4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '54.208.58.235' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Wed Oct  9 13:14:04 UTC 2024

  System load:  0.0               Processes:             104
  Usage of /:   22.8% of 6.71GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for enX0: 10.0.1.33
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-1-33:~$
```

Sử dụng keypair vừa rồi để ssh đến public instance.

```
ubuntu@ip-10-0-1-33:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=1.63 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=1.96 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=2.36 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.633/1.984/2.363/0.298 ms
ubuntu@ip-10-0-1-33:~$
```

Public instance có thể connect ra internet.

Để public instance có thể connect đến private instance thì ta sẽ tạo file key ở public instance.

ubuntu@ip-10-0-1-33: ~

```
 GNU nano 7.2
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAkI4hA4uUZKymdgSwrAMrmktzOguOtQEKwz3ruCWm2R99eOSy
vCiqOj180pHURHxW2nX4b1IObvaDHNzXG3CERh+OIWTR+rIJLYH5X3/gc7wXCV+j
zx8xhAIckhfw/5Pga4+CpmARDJQEAnPIhJJpUEzes3Sx6PgIlgxLMZEa2SyErT35
lZR7/uz8NuIYOabvdjw5a11Y/Xw989lHhSasfbUE8A+Y5f/zLPQ4szLFox2Sbs4W
Ot68l+i/TDEnC1EqQV5O1EPh6uKeuBjyYZOWL+7Za/E+kjHWYxfKTEAnQUqHiRpB
WH1/QHxLQPlDJwYVw14k3g0AfbL81KrveuXvGwIDAQABAoIBACXBSXQgl6B3y35V
mUNEDLZe8Hh/qDICVKpL2O4ev2ZEKERUDy6/vD474wcoWXWNuC2U1E9W8jgfIH2A
XJppF9Ms4qI6L/G3YFhHczdzMc9ol+e12BX3wroExyuNHz/RgrL1J52Gx8OuN6Hg
VcXya5kyipP6baE4bx2pllYa3RVNe9YYQOAVdjpJjaCxsURxrjpNC5G+a7YxW9Mc
C2eTsLFhNFbZ5P3B2IgUzElkIN5FOtLiypFCDyAPa/l9n5vXZdA1JbdFxZZc3Tym
GRpQmnHTi/d6gEpOi17rmZIPv5SXNVRgpb5O3TFcQPgL9CaNkwcrO+ga9p1UZYhT
k3v+6tkCgYEAwynuVZnPvOXt84YYNYV5WtQQOjSwkk3XWjAAOIupJ87tXxTJw35W
f6gBcPxMxxWcPifXo65sHFD+7MpQPwPh2REO4KmKkU2VnpVrqlLBOBrVPnupJLSV
8gXmZ7MJKsoE6BVh1q1c5EYz53eQGVZNgjrhOuVAFxNuXWpxdLRo1iUCgYEAvZ2h
ycHCSf8rsYn1VT+7dQRabAVV583iRLeRmJYMEuWzDsObJt/4NGQ/9kTxegH3Gv6R
JPi/u6Ep+4hcRqm4my5xJBTGu4CQUq8utqaSOOlaqpyr1JPwTtP87XBpDIYBtZfL
WVmnTjxSQXkOGM2KHVcwfPuOLc3USoO1Lr75jD8CgYBd26aRaF1tvS6ItW6jHsPU
GLSNKZXZZrIw33Ek2mXJjUy/M2ItMG8tCYFX8x6BiDUR91tPjqzTmWhgPJQHGjjd
icSb6y2G38ca8OVKLm6jRKRVXmdkDaOnLgs2x/WarHlbnBznf4xzBAgmQ2v7o3O3
M9Xp2yLNdjzXlD9oHvNkOQKBgC+m67/ed8tM21gOyXjxGVUhEPBQrvQgY5rNXOOv
gb1GCKfRl98/LgtMnl5vmRgGYmlgTG2OLcsjh391F2uSv5gQJdLhfcglWR/Ocrjo
R8FEw8pYsT4tJ5lH4Spys5O4IbnXOf1scIVS14EoypTpIqqY/NCMGQ3hylYnn2Lu
D5zVAoGAXPkZVADE+6GSaRz2rippOLxkK+vqOcA/Ddnbnjh8ieZTVEDCEZSRLG8J
emw8Tsy4gIE6P9K9Fw/uOW4USDwUH4Zc9OrpIuTnwnCQpE2A6x5fsbrNPBnIqfM+
ke9xvjwUYdpY5MV752F4I99bpiTKO6+GbOjGBJnTMcohXuvL99c=
-----END RSA PRIVATE KEY-----
```

Copy file key vào public instance.

```
ubuntu@ip-10-0-1-33:~$ chmod 400 ssh_rsa_keypair.pem
ubuntu@ip-10-0-1-33:~$ ssh -i ssh_rsa_keypair.pem ubuntu@10.0.2.16
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Wed Oct  9 13:17:37 UTC 2024

  System load:  0.08              Processes:             105
  Usage of /:   22.8% of 6.71GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for enX0: 10.0.2.16
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-2-16:~$
```

Cấp quyền 'chmod 400' cho file key. Ta có thể kết nối đến private instance thông qua public instance.

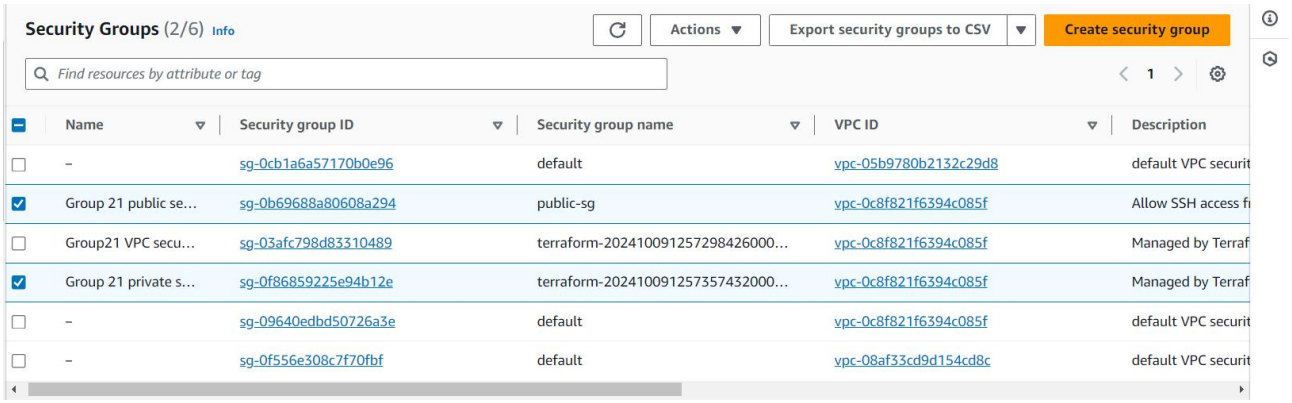
Ngoài ra, theo yêu cầu thì chỉ có public instance mới có thể connect đến private instance, nên từ máy cá nhân, ta không thể connect đến private instance.

```
ASUS@LAPTOP-299D0RSV MINGW64 /d/Learning Space/1st 2024-2025/DevOps/Labs/Lab1
$  ssh -i ssh_rsa_keypair.pem ubuntu@10.0.2.16
ssh: connect to host 10.0.2.16 port 22: Connection timed out

ASUS@LAPTOP-299D0RSV MINGW64 /d/Learning Space/1st 2024-2025/DevOps/Labs/Lab1
$
```

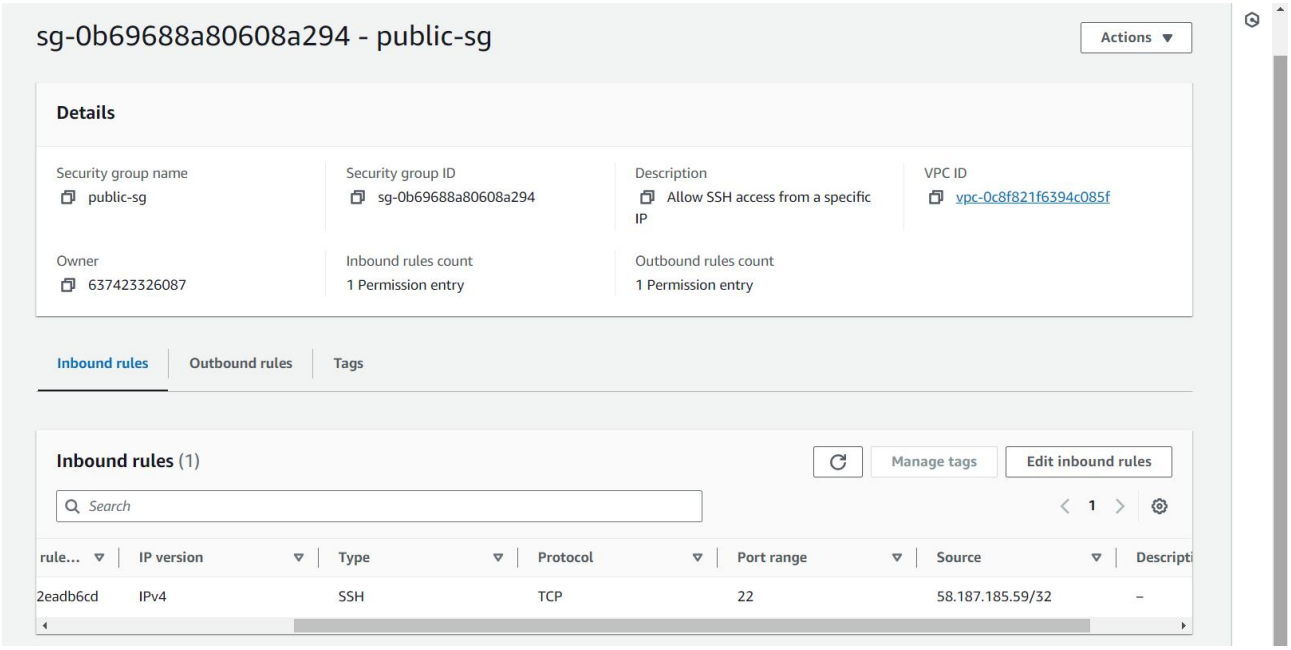
Vậy các instance đã được cấu hình thành công.

Security Groups:

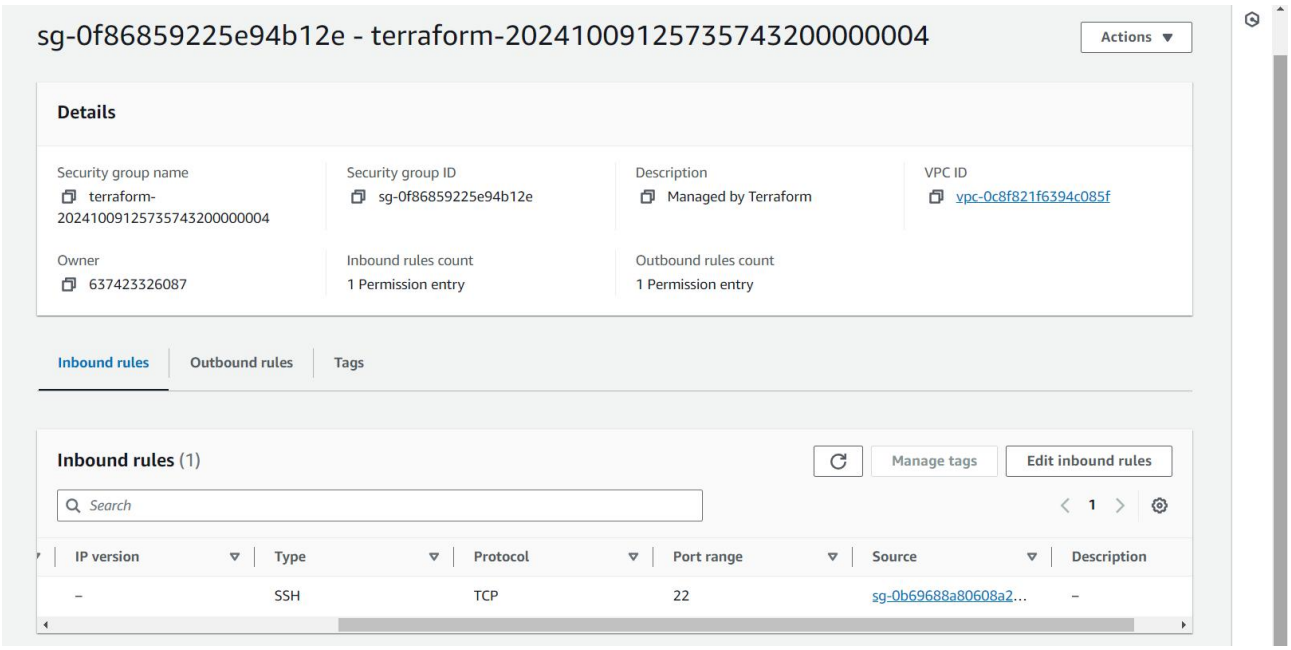
- **Security Groups**: Tạo các Security Groups để kiểm soát lưu lượng vào/ra của EC2 instances (2 điểm):
  - Public EC2 Security Group: Chỉ cho phép kết nối SSH (port 22) từ một IP cụ thể (hoặc IP của người dùng).
  - Private EC2 Security Group: Cho phép kết nối từ Public EC2 instance thông qua port cần thiết (SSH hoặc các port khác nếu có nhu cầu).



Các SG được cấu hình gồm có public SG và private SG được tạo thành công.



Check Inbound rules của public SG thì thấy chỉ cho phép SSH từ IP máy cá nhân.



Check Inbound rules của private SG thì thấy chỉ cho phép SSH từ public instance (ở trên 'Source' là public SG).

Vậy các SG đã được cấu hình thành công.

Quản lý và triển khai hạ tầng AWS bằng CloudFormation

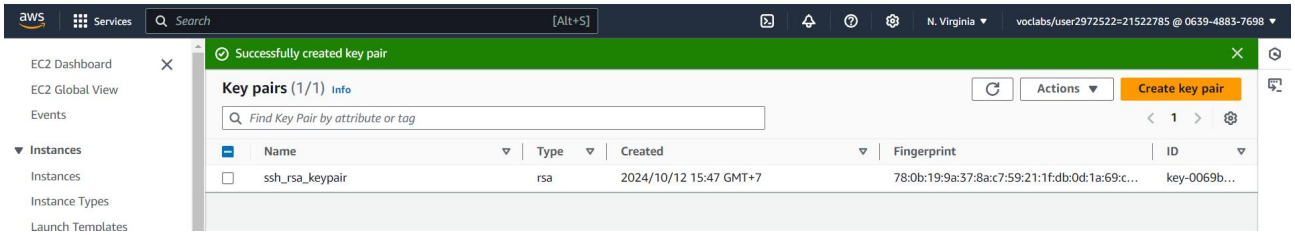
```
PS D:\Learning Space\1st 2024-2025\DevOps\Labs\Lab1_CloudFormation> aws s3 mb s3://grouptwentyonebucket
make_bucket: grouptwentyonebucket
PS D:\Learning Space\1st 2024-2025\DevOps\Labs\Lab1_CloudFormation> aws s3 cp main.yaml s3://grouptwentyonebucket
upload: .\main.yaml to s3://grouptwentyonebucket/main.yaml
PS D:\Learning Space\1st 2024-2025\DevOps\Labs\Lab1_CloudFormation> aws s3 cp vpc.yaml s3://grouptwentyonebucket
upload: .\vpc.yaml to s3://grouptwentyonebucket/vpc.yaml
PS D:\Learning Space\1st 2024-2025\DevOps\Labs\Lab1_CloudFormation> aws s3 cp subnets.yaml s3://grouptwentyonebucket
upload: .\subnets.yaml to s3://grouptwentyonebucket/subnets.yaml
PS D:\Learning Space\1st 2024-2025\DevOps\Labs\Lab1_CloudFormation> aws s3 cp gateway.yaml s3://grouptwentyonebucket
upload: .\gateway.yaml to s3://grouptwentyonebucket/gateway.yaml
PS D:\Learning Space\1st 2024-2025\DevOps\Labs\Lab1_CloudFormation> aws s3 cp route_tables.yaml s3://grouptwentyonebucket
upload: .\route_tables.yaml to s3://grouptwentyonebucket/route_tables.yaml
PS D:\Learning Space\1st 2024-2025\DevOps\Labs\Lab1_CloudFormation> aws s3 cp security_groups.yaml s3://grouptwentyonebucket
upload: .\security_groups.yaml to s3://grouptwentyonebucket/security_groups.yaml
PS D:\Learning Space\1st 2024-2025\DevOps\Labs\Lab1_CloudFormation> aws s3 cp ec2_instances.yaml s3://grouptwentyonebucket
upload: .\ec2_instances.yaml to s3://grouptwentyonebucket/ec2_instances.yaml
PS D:\Learning Space\1st 2024-2025\DevOps\Labs\Lab1_CloudFormation>
```

Khởi tạo một S3 bucket ‘grouptwentyonebucket’, sau đó copy các file .yaml vào bucket ấy.

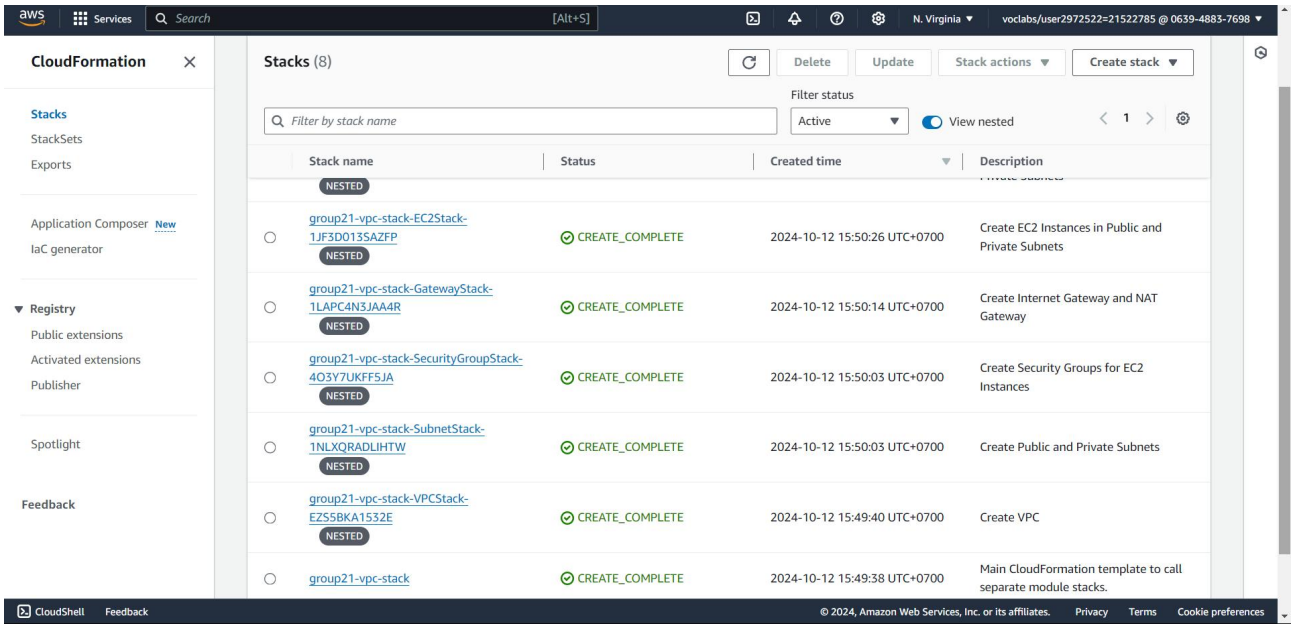
```
PS D:\Learning Space\1st 2024-2025\DevOps\Labs\Lab1_CloudFormation> aws cloudformation create-stack --stack-name group21-vpc-stack --template-url htt
ps://grouptwentyonebucket.s3.amazonaws.com/main.yaml --capabilities CAPABILITY_NAMED_IAM
{
    "StackId": "arn:aws:cloudformation:us-east-1:063948837698:stack/group21-vpc-stack/8f8edb30-8875-11ef-a0eb-0e3b23bfaf07"
}

PS D:\Learning Space\1st 2024-2025\DevOps\Labs\Lab1_CloudFormation>
```

Khởi tạo một cloudformation stack ‘group21-vpc-stack’ với template url là S3 bucket trên.

Tạo keypair trên AWS Console.



Các Stacks đã được tạo thành công.

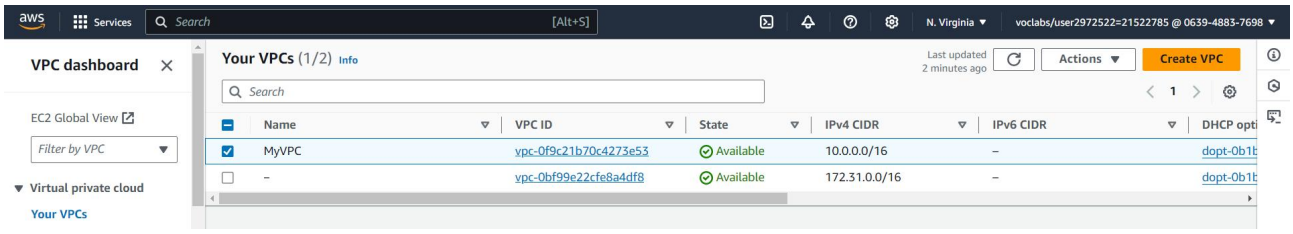


Ta sẽ kiểm tra chi tiết từng dịch vụ đã triển khai. Hầu hết các dịch vụ đều đã được khởi tạo tương tự như khi sử dụng Terraform.

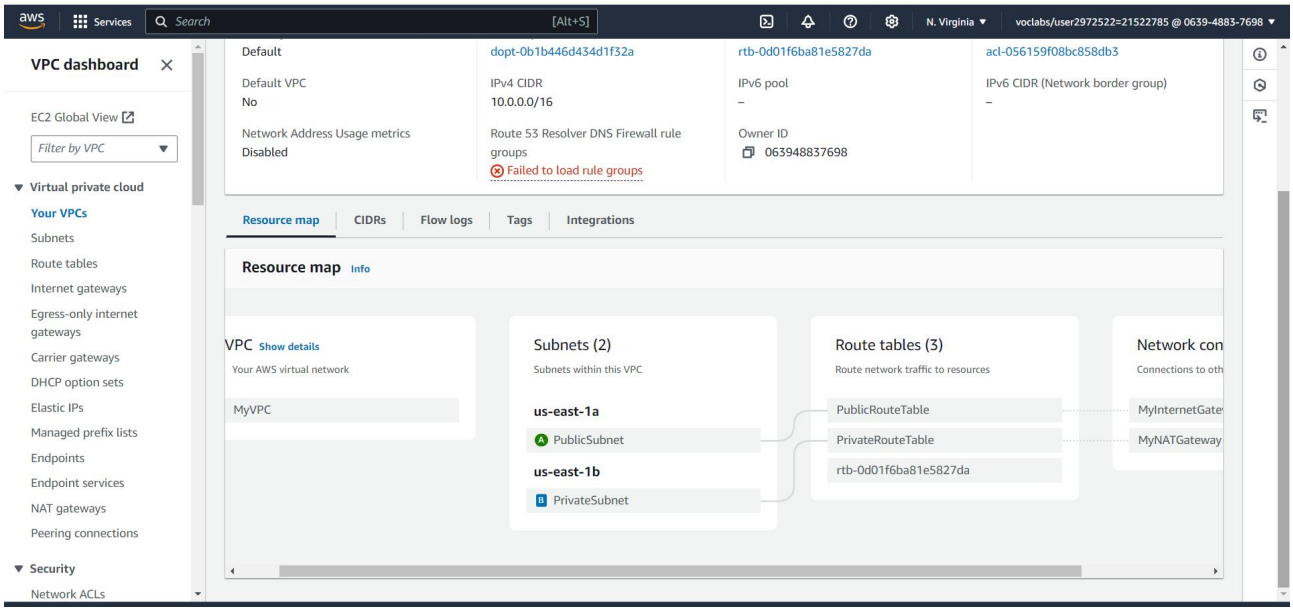
VPC:

- **VPC:** Tạo một VPC chứa các thành phần sau (3 điểm):
  - Subnets: Bao gồm cả Public Subnet (kết nối với Internet Gateway) và Private Subnet (sử dụng NAT Gateway để kết nối ra ngoài).
  - Internet Gateway: Kết nối với Public Subnet để cho phép các tài nguyên bên trong có thể truy cập Internet.
  - Default Security Group: Tạo Security Group mặc định cho VPC

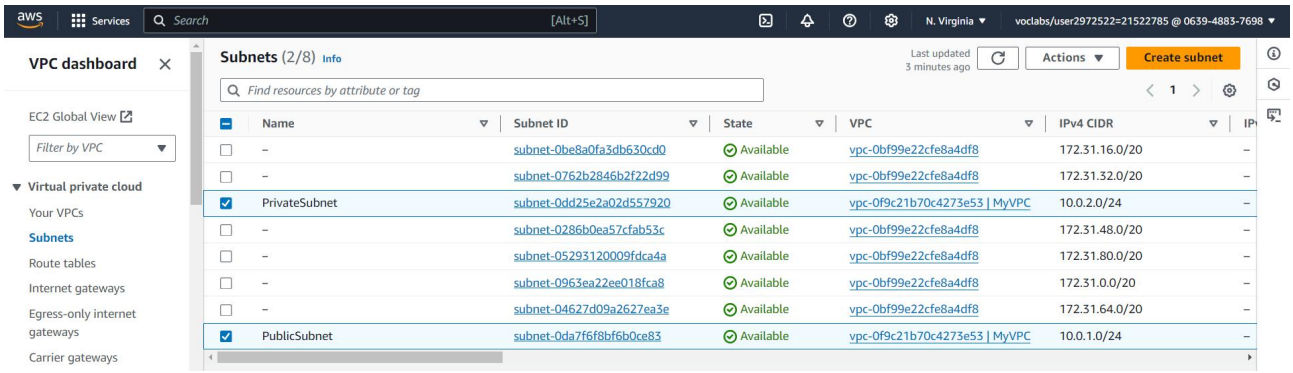
VPC đã được tạo thành công.



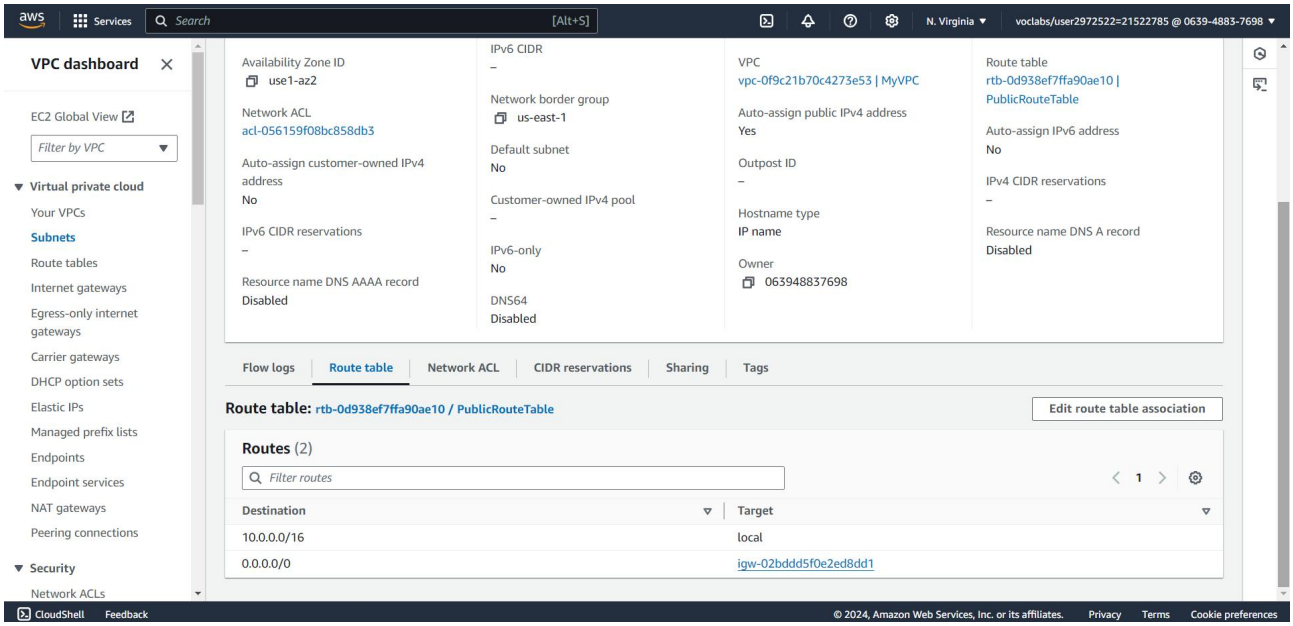
Chi tiết các Subnets trong VPC.



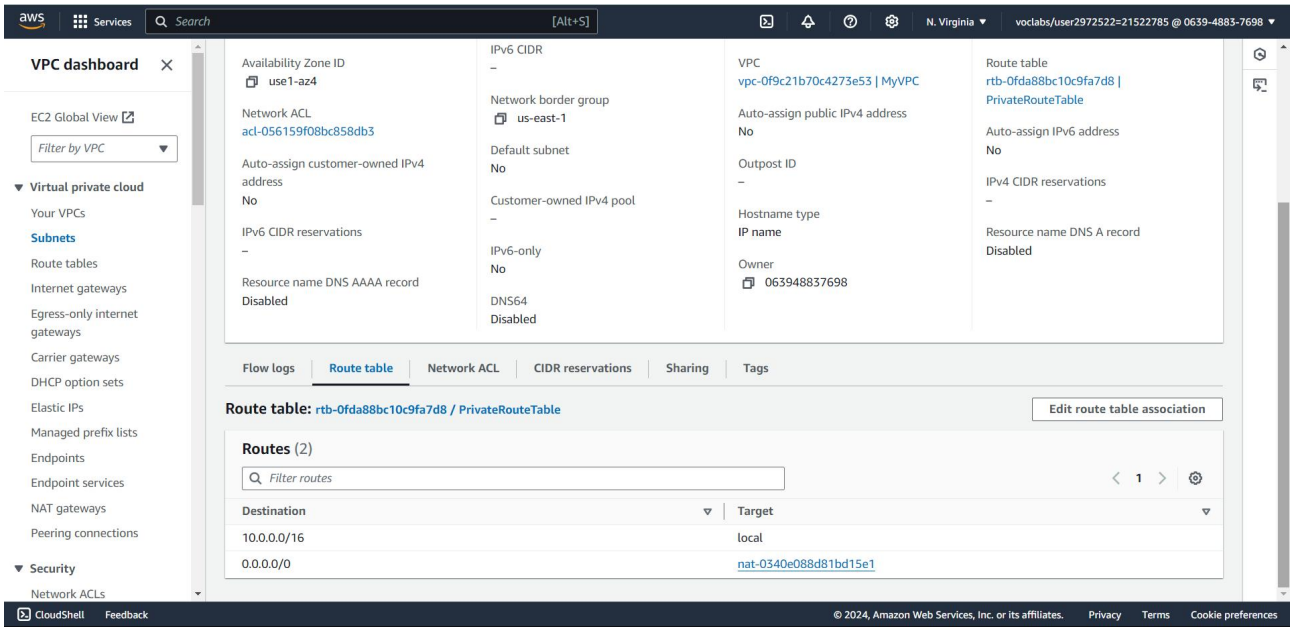
Các Subnets đã được tạo thành công.



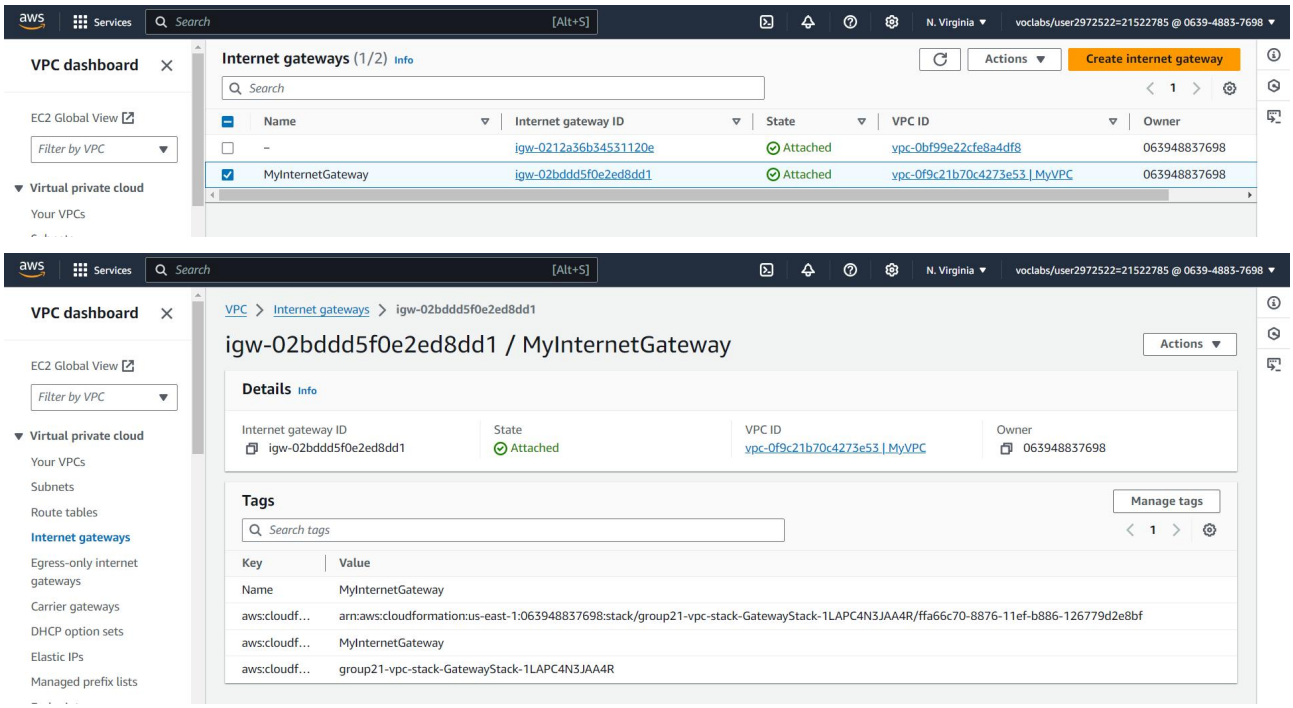
Public Subnet được nối đến internet gateway



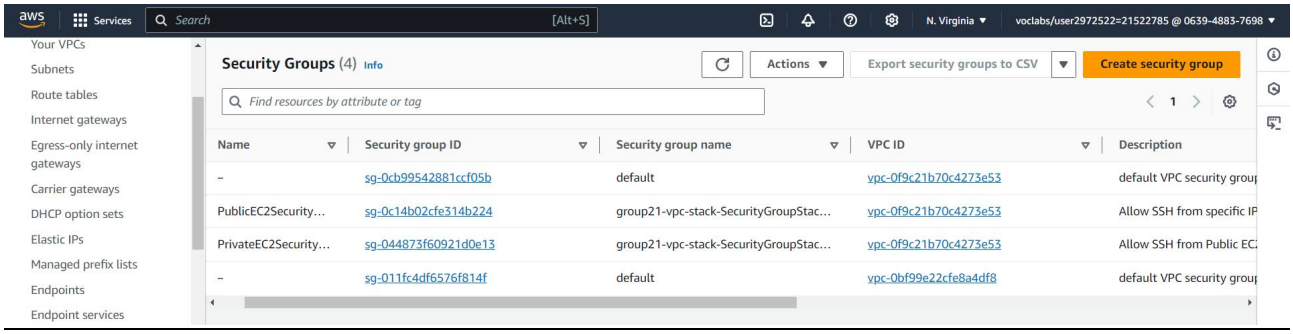
Private Subnet được nối đến NAT Gateway để kết nối Internet



Internet Gateway đã được tạo



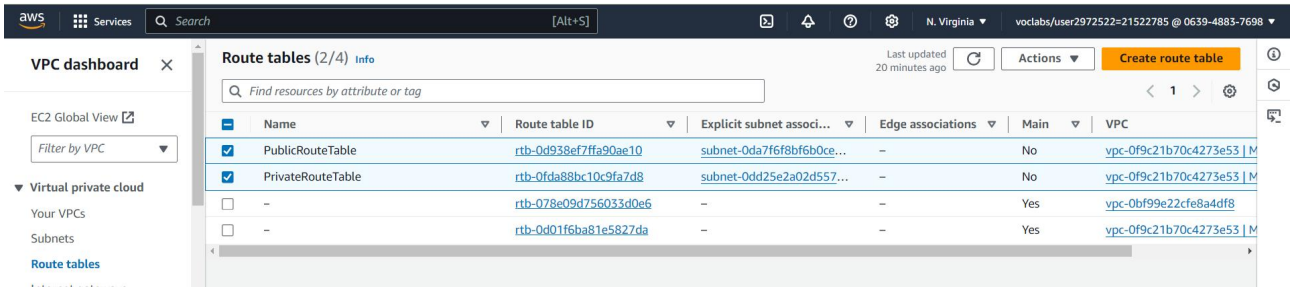
Các default security groups được tạo mặc định cho VPC, không hiểu sao em thử tạo Default security group cho VPC nhưng dính lỗi :D.



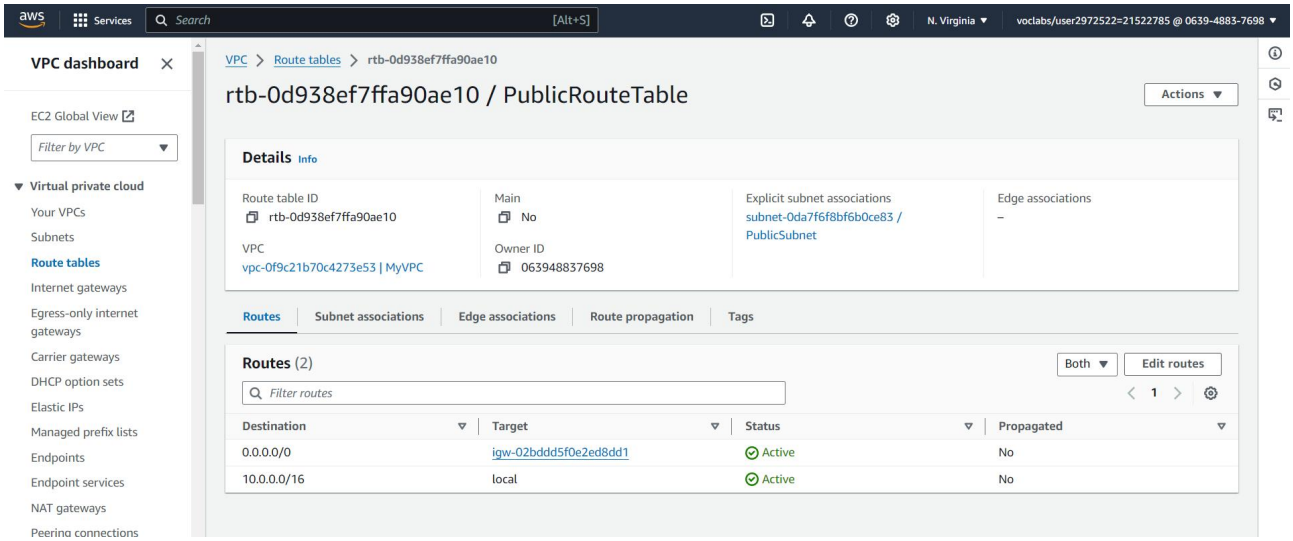
Route Table:

- **Route Tables:** Tạo Route Tables cho Public và Private Subnet (2 điểm):
  - Public Route Table: Định tuyến lưu lượng Internet thông qua Internet Gateway.
  - Private Route Table: Định tuyến lưu lượng Internet thông qua NAT Gateway.

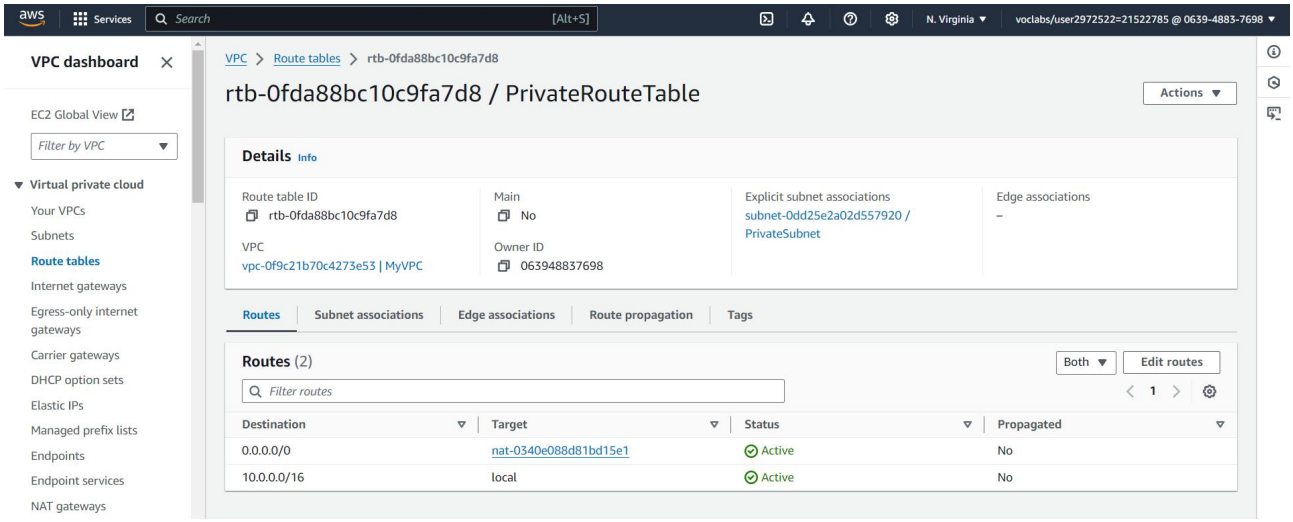
Các Route tables đã được tạo thành công



Public Route table kết nối ra internet gateway



Private Route table sử dụng NAT Gateway kết nối ra Internet.



NAT Gateway:

- **NAT Gateway:** Cho phép các tài nguyên trong Private Subnet có thể kết nối Internet mà vẫn bảo đảm tính bảo mật (1 điểm).

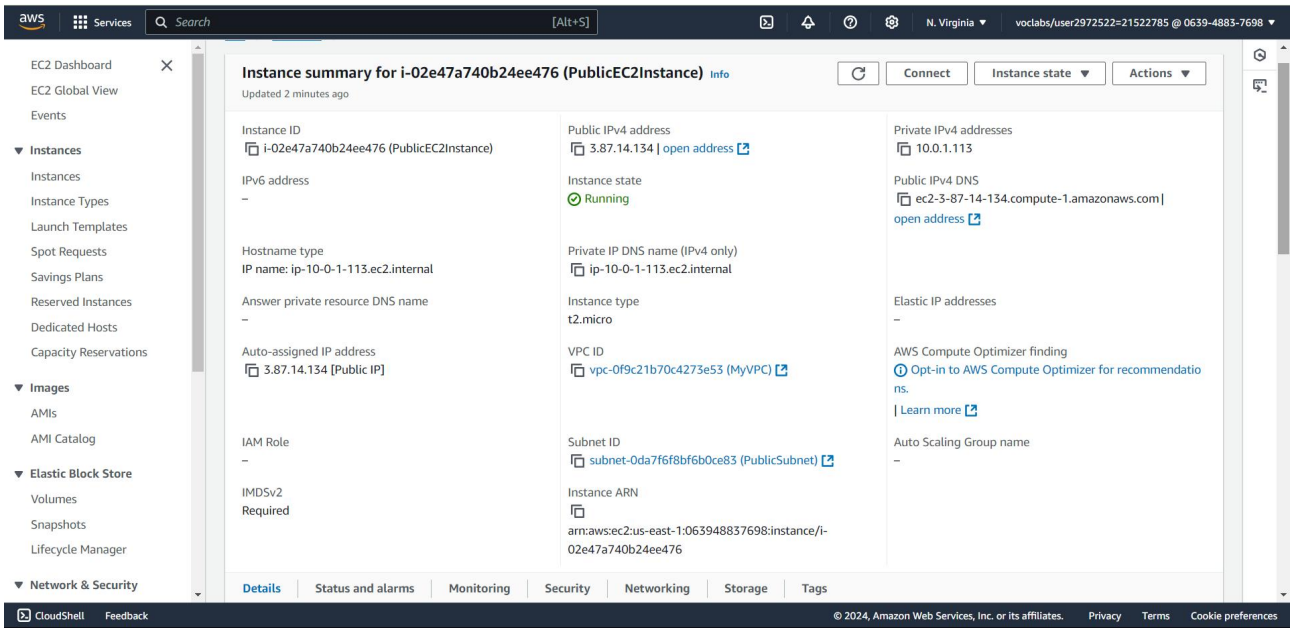
Private instance có thể truy cập internet thông qua NAT Gateway nên sẽ đảm bảo tính bảo mật cho private instance.

```
ubuntu@ip-10-0-2-243:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=57 time=2.24 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=57 time=1.56 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=57 time=1.88 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.557/1.891/2.235/0.276 ms
ubuntu@ip-10-0-2-243:~$
```

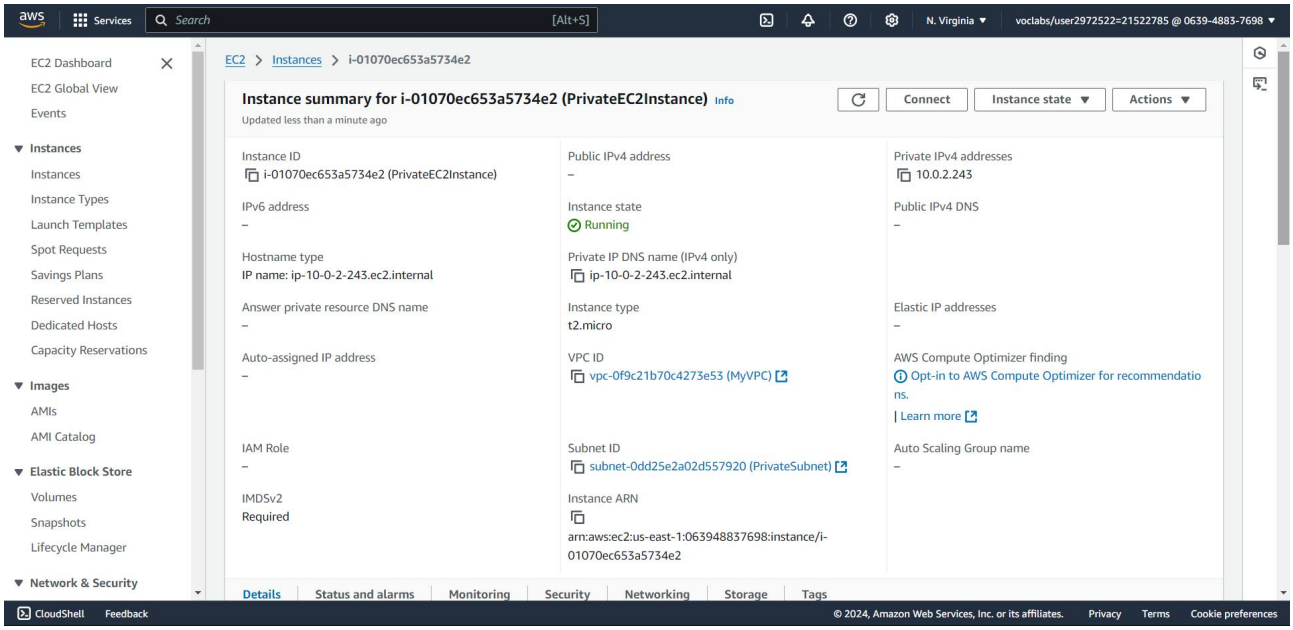
EC2 Instances:

- **EC2:** Tạo các instance trong Public và Private Subnet, đảm bảo Public instance có thể truy cập từ Internet, còn Private instance chỉ có thể truy cập từ Public instance thông qua SSH hoặc các phương thức bảo mật khác (2 điểm).

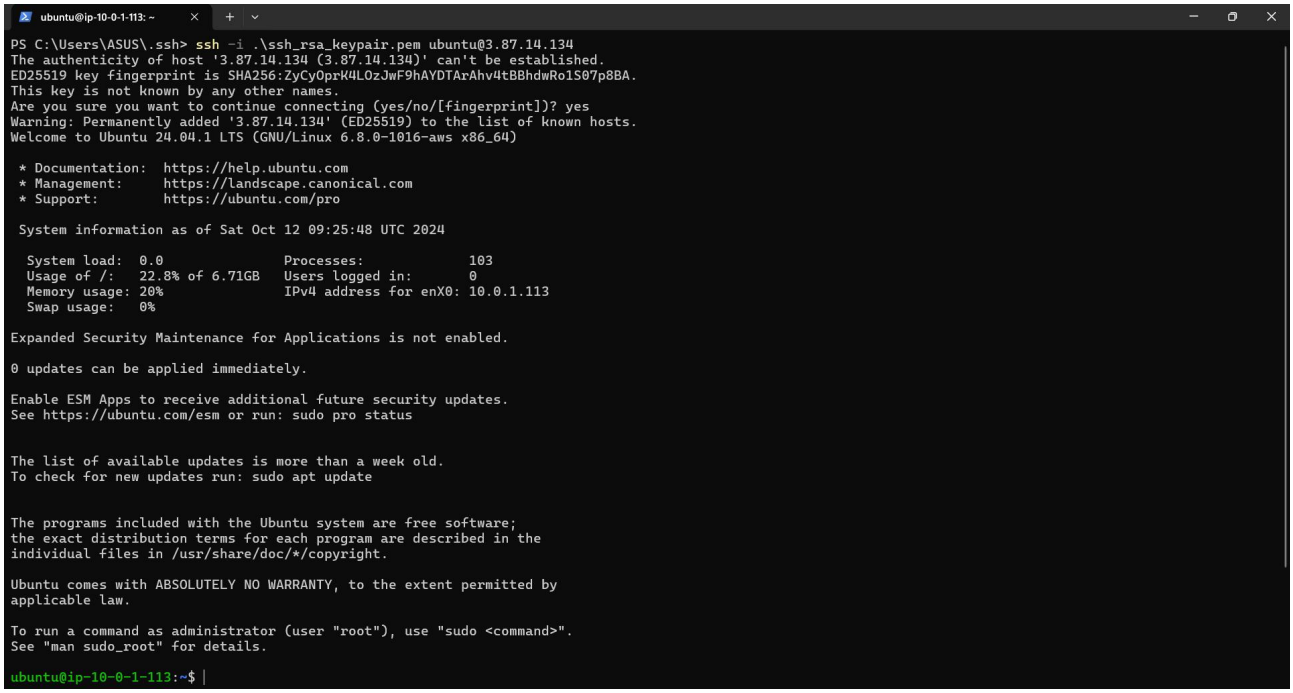
Public EC2 instance:



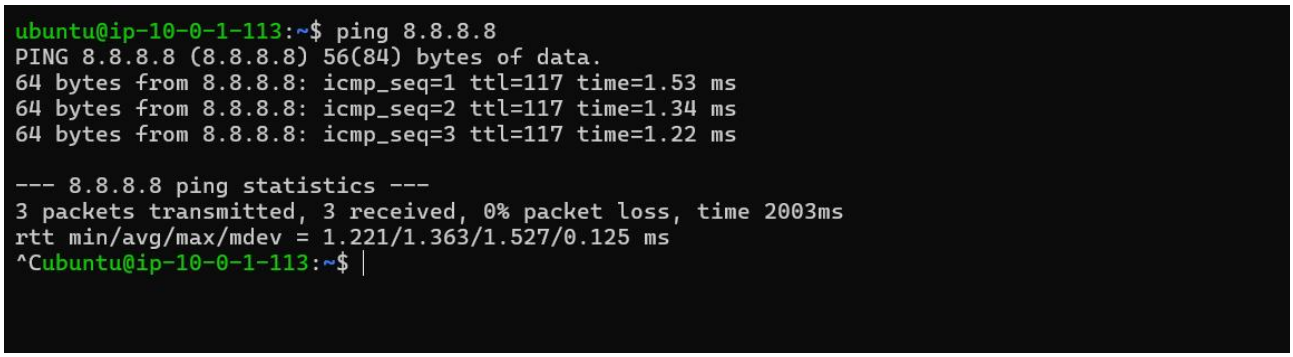
Private EC2 instance:



Truy cập EC2 public instance từ máy cá nhân.



Truy cập internet từ public instance.



Truy cập Private instance từ Public instance:

```
ubuntu@ip-10-0-1-113:~$ chmod 400 ssh_rsa_keypair.pem
ubuntu@ip-10-0-1-113:~$ ssh -i ssh_rsa_keypair.pem ubuntu@10.0.2.243
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sat Oct 12 09:29:51 UTC 2024

  System load:  0.0               Processes:             103
  Usage of /:   22.8% of 6.71GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for enX0: 10.0.2.243
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-2-243:~$
```

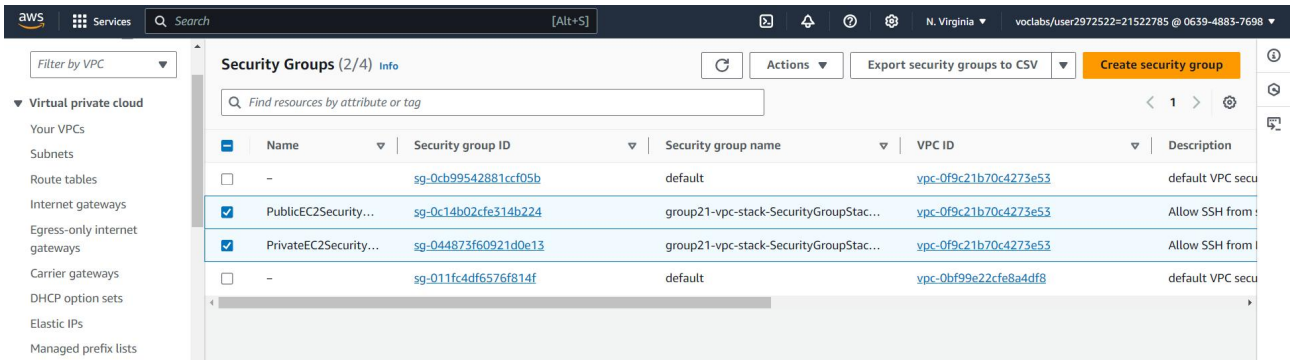
Truy cập internet từ private instance:

```
ubuntu@ip-10-0-2-243:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=57 time=2.24 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=57 time=1.56 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=57 time=1.88 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.557/1.891/2.235/0.276 ms
ubuntu@ip-10-0-2-243:~$
```

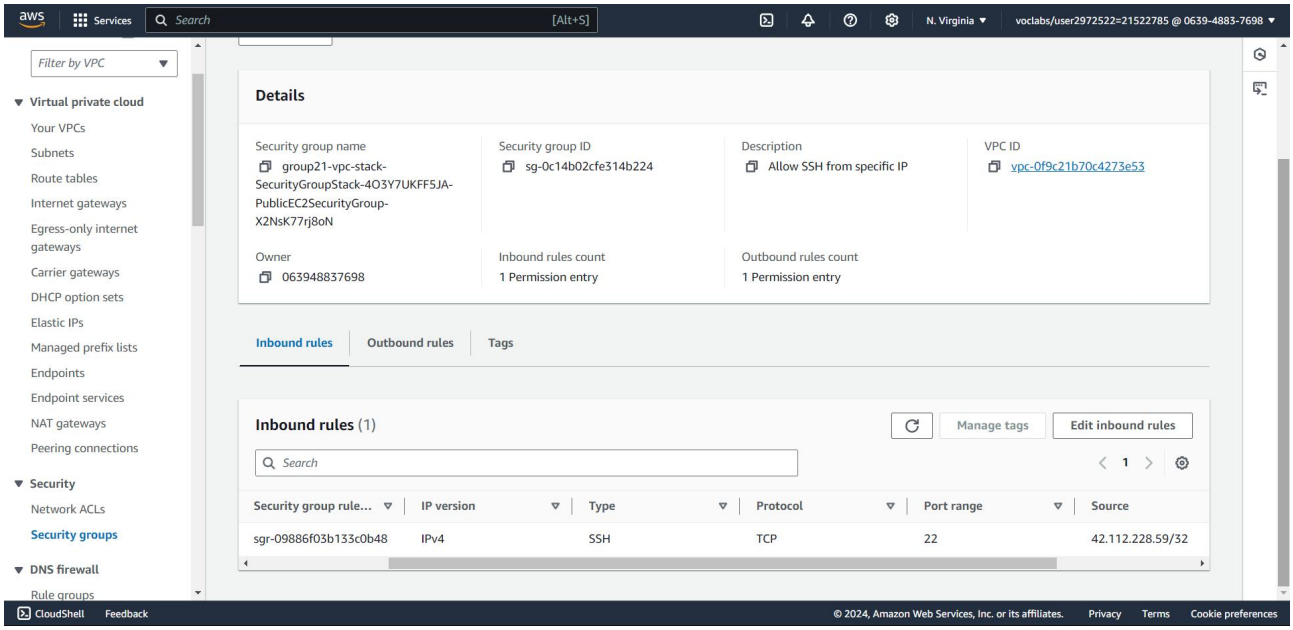
Security Groups:

- **Security Groups**: Tạo các Security Groups để kiểm soát lưu lượng vào/ra của EC2 instances (2 điểm):
    - Public EC2 Security Group: Chỉ cho phép kết nối SSH (port 22) từ một IP cụ thể (hoặc IP của người dùng).
    - Private EC2 Security Group: Cho phép kết nối từ Public EC2 instance thông qua port cần thiết (SSH hoặc các port khác nếu có nhu cầu).

Các security groups đã được khởi tạo.



Public SG chỉ cho phép kết nối SSH từ máy cá nhân:



Private SG chỉ cho phép SSH từ public EC2 instance: