



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 Vĩ	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 (<i>nếu có</i>) + 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 Terraform

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

The screenshot shows the AWS EC2 Key Pairs page. A success message at the top says "Successfully created key pair". Below it is a table with three rows:

Name	Type	Created	Fingerprint	ID
rsa_keypair	rsa	2024/10/09 15:42 GMT+7	06:4a:eb:a5:73:a9:33:35:17:25:29:ab:eb:c0:...	key-0d5c59...
ssh_rsa_keypair	rsa	2024/10/09 16:09 GMT+7	67:5b:89:c9:fced:d8:93:b1:d8:c5:b0:97:68:6...	key-0b15c7...
custom-key	rsa	2024/10/09 14:10 GMT+7	6a:73:60:7b:f2:13:60:26:9f:b1:3b:8c:55:6d:5...	key-07d6b...

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

PS D:\Learning Space\1st 2024-2025\DevOps\Labs\Lab1> **terraform apply**
var.key_name
The name of the existing key pair to use for SSH access

Enter a value: ssh_rsa_keypair

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

```
module.route_table.aws_nat_gateway.nat: Still creating... [30s elapsed]
module.route_table.aws_nat_gateway.nat: Still creating... [40s elapsed]
module.route_table.aws_nat_gateway.nat: Still creating... [50s elapsed]
module.route_table.aws_nat_gateway.nat: Still creating... [1m0s elapsed]
module.route_table.aws_nat_gateway.nat: Still creating... [1m10s elapsed]
module.route_table.aws_nat_gateway.nat: Still creating... [1m20s elapsed]
module.route_table.aws_nat_gateway.nat: Still creating... [1m30s elapsed]
module.route_table.aws_nat_gateway.nat: Still creating... [1m40s elapsed]
module.route_table.aws_nat_gateway.nat: Creation complete after 1m48s [id=nat-03dd117aaca2cc7ab]
module.route_table.aws_route.private_route_nat: Creating...
module.route_table.aws_route.private_route_nat: Creation complete after 2s [id=r-rtb-0047ddcdff8b23cff1080289494]

Apply complete! Resources: 17 added, 0 changed, 0 destroyed.
```

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

VPC:

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

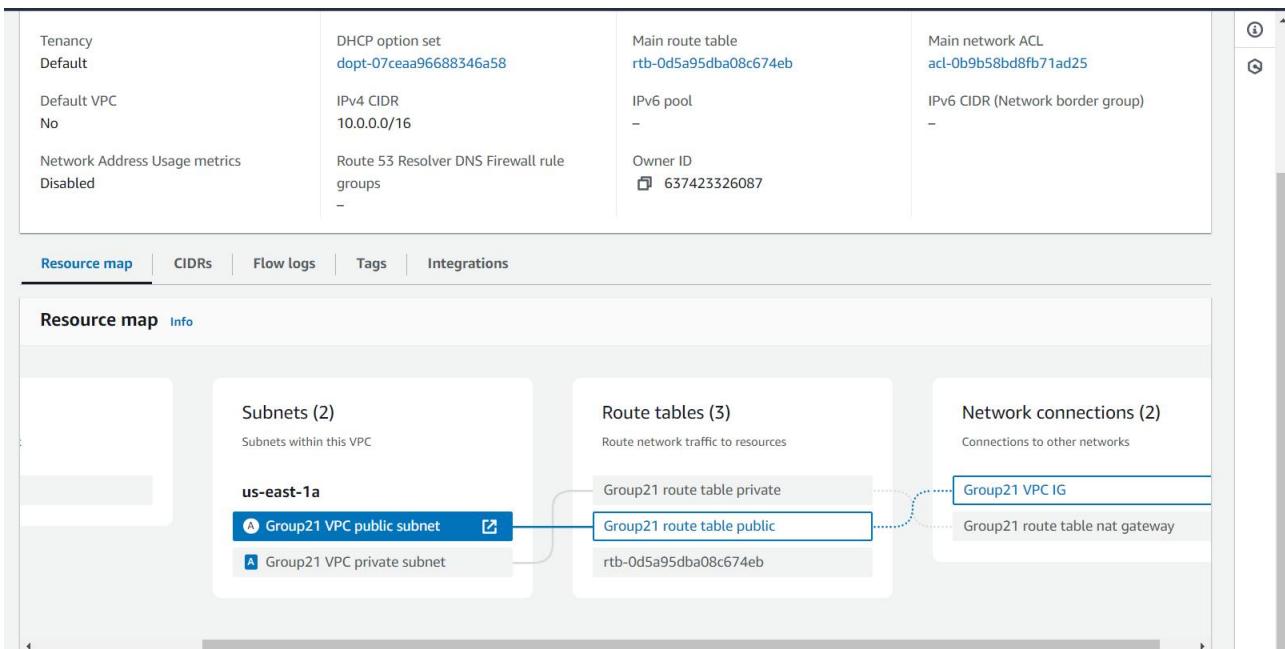


- **VPC:** Tạo một VPC chứa các thành phần sau (3 điểm):

- 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

Your VPCs (1/3) Info						
		Actions		Create VPC		
Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP opt	
<input checked="" type="checkbox"/> Group21 VPC main	vpc-0c8f821f6394c085f	Available	10.0.0.0/16	-	dopt-07ce	Edit
<input type="checkbox"/> -	vpc-05b9780b2132c29d8	Available	172.31.0.0/16	-	dopt-07ce	Edit
<input type="checkbox"/> Samsung-VPC	vpc-08af53cd9d154cd8c	Available	10.0.0.0/16	-	dopt-07ce	Edit

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 gateways (1/3) Info						
		Actions		Create internet gateway		
Name	Internet gateway ID	State	VPC ID	Owner		
<input type="checkbox"/> -	igw-0bbf53ad982c9613	Attached	vpc-05b9780b2132c29d8	637423326087		
<input type="checkbox"/> Samsung-igw	igw-0bee8b8b2dfcc59fc	Attached	vpc-08af53cd9d154cd8c Samsung-VPC	637423326087		
<input checked="" type="checkbox"/> Group21 VPC IG	igw-0d5d93bbff3a987f0	Attached	vpc-0c8f821f6394c085f Group21 VPC...	637423326087		

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

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



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 Groups (3/6) Info					
Name		Security group ID	Security group name	VPC ID	Description
<input type="checkbox"/>	-	sg-0cb1a6a57170b0e96	default	vpc-05b9780b2132c29d8	default VPC security group
<input checked="" type="checkbox"/>	Group 21 public se...	sg-0b69688a80608a294	public-sg	vpc-0cf8f821f6394c085f	Allow SSH access
<input checked="" type="checkbox"/>	Group21 VPC s...	Edit Name Group21 VPC security group	terraform-202410091257298426000...	vpc-0cf8f821f6394c085f	Managed by Terraform
<input checked="" type="checkbox"/>	Group 21 private s...		terraform-202410091257357432000...	vpc-0cf8f821f6394c085f	Managed by Terraform
<input type="checkbox"/>	-	default	vpc-0cf8f821f6394c085f	vpc-08af33cd9d154cd8c	default VPC security group
<input type="checkbox"/>	-	default	vpc-08af33cd9d154cd8c	vpc-08af33cd9d154cd8c	default VPC security group

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.

Route tables (2/6) Info					
Last updated 7 minutes ago C Actions Create route table					
Name		Route table ID	Explicit subnet associations	Edge associations	Main
<input type="checkbox"/>	Samsung-route-table	rtb-00603be5782cb09d6	subnet-019531f10fc6569...	-	No
<input checked="" type="checkbox"/>	Group21 route table private	rtb-0047ddcdff8b23cff	subnet-02642821669e62...	-	No
<input checked="" type="checkbox"/>	Group21 route table public	rtb-0fd143e35118dbd98	subnet-0ff31f8cc89928c6...	-	No
<input type="checkbox"/>	-	rtb-07a36e9b302c73416	-	-	Yes
<input type="checkbox"/>	-	rtb-0d5a95dba08c674eb	-	-	Yes
<input type="checkbox"/>	-	rtb-027cc54c06a8a6761	-	-	Yes

Các route tables đã được khởi tạo thành công!

VPC > Route tables > rtb-0fd143e35118dbd98																					
rtb-0fd143e35118dbd98 / Group21 route table public																					
Actions																					
Details Info																					
<table border="1"><tr><td>Route table ID rtb-0fd143e35118dbd98</td><td>Main <input type="checkbox"/> No</td><td>Explicit subnet associations subnet-0ff31f8cc89928c67 / Group21 VPC public subnet</td><td>Edge associations -</td><td colspan="2" rowspan="4"></td></tr></table>						Route table ID rtb-0fd143e35118dbd98	Main <input type="checkbox"/> No	Explicit subnet associations subnet-0ff31f8cc89928c67 / Group21 VPC public subnet	Edge associations -												
Route table ID rtb-0fd143e35118dbd98	Main <input type="checkbox"/> No	Explicit subnet associations subnet-0ff31f8cc89928c67 / Group21 VPC public subnet	Edge associations -																		
Routes																					
Routes (2)																					
<table border="1"><tr><th colspan="2">Filter routes</th><th>Both</th><th>Edit routes</th></tr><tr><th>Destination</th><th>Target</th><th>Status</th><th>Propagated</th></tr><tr><td>0.0.0.0/0</td><td>igw-0d5d93bbff3a987f0</td><td><input checked="" type="checkbox"/> Active</td><td>No</td></tr><tr><td>10.0.0.0/16</td><td>local</td><td><input checked="" type="checkbox"/> Active</td><td>No</td></tr></table>						Filter routes		Both	Edit routes	Destination	Target	Status	Propagated	0.0.0.0/0	igw-0d5d93bbff3a987f0	<input checked="" type="checkbox"/> Active	No	10.0.0.0/16	local	<input checked="" type="checkbox"/> Active	No
Filter routes		Both	Edit routes																		
Destination	Target	Status	Propagated																		
0.0.0.0/0	igw-0d5d93bbff3a987f0	<input checked="" type="checkbox"/> Active	No																		
10.0.0.0/16	local	<input checked="" type="checkbox"/> Active	No																		

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

The screenshot shows the AWS Route Tables page for a private route table. Key details include:

- Route table ID: rtb-0047ddcddf8b23cff
- Main: No
- Owner ID: 637423326087
- VPC: vpc-0c8f821f6394c085f | Group21 VPC main
- Explicit subnet associations: subnet-02642821669e62acd / Group21 VPC private subnet
- Edge associations: -

The "Routes" tab is selected, showing two entries:

Destination	Target	Status	Propagated
0.0.0.0/0	nat-03dd117aaaca2cc7ab	Active	No
10.0.0.0/16	local	Active	No

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**).

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

6

```
ASUS@LAPTOP-Z99D0RSV 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:zQR1kDIRKDDVmxxYtFFS1wfkxk65RGxpv1gGEKe+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.

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



```
ubuntu@ip-10-0-1-33: ~
GNU nano 7.2
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEakI4hA4uUZKymdgSwrAMrmktzOgu0tQEkwz3ruCwm2R99eOSy
vCiqoj180pHURhxW2nX4b1IObvADHNzXG3CERh+0IWTR+rIJLYH5X3/gc7wXCV+j
zx8xhAIckhfw/5Pga4+CpmARDJQEAnPIhJJpUEzes3Sx6PgIlgxLMZEa2SyErT35
lZR7/uz8NuIYOabvdjw5a11Y/Xw9891HhSasfbUE8A+Y5f/zLPQ4szLFox2Sbs4W
0t681+i/TDENC1EqQV501EPh6uKeuBjyYZ0WL+7Za/E+kjHWYxfKTEAnQUqHiRpB
WH1/QHxLQP1DJwYVw14k3g0Afbl81KrveuXvGwIDAQABAoIBACXBSXQg16B3y35V
mUNEDLZe8Hh/qDICVKpL204ev2ZEKERUDy6/vD474wcoWXNuC2U1E9W8jgfIH2A
XJppF9Ms4qI6L/G3YFhHczdzMc9o1+e12BX3wroExyuNHz/RgrL1J52Gx80uN6Hg
VcXya5kyipP6baE4bx2p11Ya3RVNe9YYQ0AVdjpJjaCxsURxrjpNC5G+a7YxW9Mc
C2eTsLFhNFbZ5P3B2IgUzElkIN5F0tLiypFCDyAPa/19n5vXZdA1JbdFxZZc3Tym
GRpQmnHTi/d6gEpOi17rmZIPv5SXNVRgpb503TFcQPg9CaNkwcr0+ga9p1UZYhT
k3v+6tkCgYEAwynuVznPv0Xt84YYNYV5wtQQjSwkk3XwjAA0IupJ87tXxTJw35W
f6gBcPxMxxWcPifXo65sHFD+7MpQPwPh2RE04KmKkU2VnpVrqLB0BrVPnupJLSV
8gXmZ7MJKsoE6BVh1q1c5EYz53eQGVZNjrh0uVAfxNuXwpzdLRo1iUCgYEAvZ2h
ycHCSf8rsYn1VT+7dQRabAVV583iRLeRmJYMEuWzDs0bjt/4NGQ/9kTxegH3Gv6R
JPi/u6Ep+4hcRqm4my5xJBTGu4CQuq8utqaS001aqpyr1JPwTtP87XBpDIYBtzfL
WVmNTjxSQXk0GM2KHVcwfp0Lc3USo01Lr75jD8CgYBd26aRaF1tvS6Itw6jhSPU
GLSNKZXZrIw33Ek2mXjjUy/M2ItMG8tCYFX8x6BiDUR91tPjqzTmWhgPJQHGjjd
icSb6y2G38ca80VKLm6jRKRVXmdkDa0nLgs2x/WarH1bnBznf4xzBAgmQ2v7o303
M9Xp2yLNdjzx1D9oHvnk0QKBgC+m67/ed8tM21g0yXjxGVUhEPBQrvQgY5rNX00v
gb1GCKfR198/LgtMn15vmRgGYmlgTG20Lcsjh391F2uSv5gQJdLhfcg1WR/0crjo
R8FEw8pYsT4tJ51H4Spys504IbnX0f1scIVS14EoypTpIqqY/NCMGQ3hy1Ynn2Lu
D5zVAoGAXPkZVADE+6GSaRz2rippOLxkk+vq0CA/Ddnbnjh8ieZTEDCEZSRLG8J
emw8Tsy4gIE6P9K9Fw/u0w4USDwUH4Zc90rpIuTnwnCQpE2A6x5fsbrNPBnIqfM+
ke9xvjwUYdpY5MV752F4I99bpitK06+Gb0jGBJnTMcohXuvL99c=
-----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:~$
```

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



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).

Security Groups (2/6) Info					
		Actions		Create security group	
Name	Security group ID	Security group name	VPC ID	Description	
-	sg-0cb1a6a57170b0e96	default	vpc-05b9780b2132c29d8	default VPC securit	
<input checked="" type="checkbox"/> Group 21 public se...	sg-0b69688a80608a294	public-sg	vpc-0c8f821f6394c085f	Allow SSH access fr	
<input type="checkbox"/> Group21 VPC secu...	sg-03afc798d83310489	terraform-202410091257298426000...	vpc-0c8f821f6394c085f	Managed by Terraf	
<input checked="" type="checkbox"/> Group 21 private s...	sg-0f86859225e94b12e	terraform-202410091257357432000...	vpc-0c8f821f6394c085f	Managed by Terraf	
<input type="checkbox"/> -	sg-09640edb50726a3e	default	vpc-0c8f821f6394c085f	default VPC securit	
<input type="checkbox"/> -	sg-0f556e308c7f70fbf	default	vpc-08af33cd9d154cd8c	default VPC securit	

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

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

6

The screenshot shows the AWS Security Groups console for a security group named "public-sg". The "Details" section displays the following information:

Security group name: public-sg	Security group ID: sg-0b69688a80608a294	Description: Allow SSH access from a specific IP	VPC ID: vpc-0c8f821f6394c085f
Owner: 637423326087	Inbound rules count: 1 Permission entry	Outbound rules count: 1 Permission entry	

Below the details, there are tabs for "Inbound rules", "Outbound rules", and "Tags". The "Inbound rules" tab is selected, showing one rule:

rule...	IP version	Type	Protocol	Port range	Source	Description
zeadb6cd	IPv4	SSH	TCP	22	58.187.185.59/32	-

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

The screenshot shows the AWS Security Groups console for a security group named "terraform-20241009125735743200000004". The "Details" section displays the following information:

Security group name: terraform-20241009125735743200000004	Security group ID: sg-0f86859225e94b12e	Description: Managed by Terraform	VPC ID: vpc-0c8f821f6394c085f
Owner: 637423326087	Inbound rules count: 1 Permission entry	Outbound rules count: 1 Permission entry	

Below the details, there are tabs for "Inbound rules", "Outbound rules", and "Tags". The "Inbound rules" tab is selected, showing one rule:

rule...	IP version	Type	Protocol	Port range	Source	Description
-	-	SSH	TCP	22	sg-0b69688a80608a2...	-

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

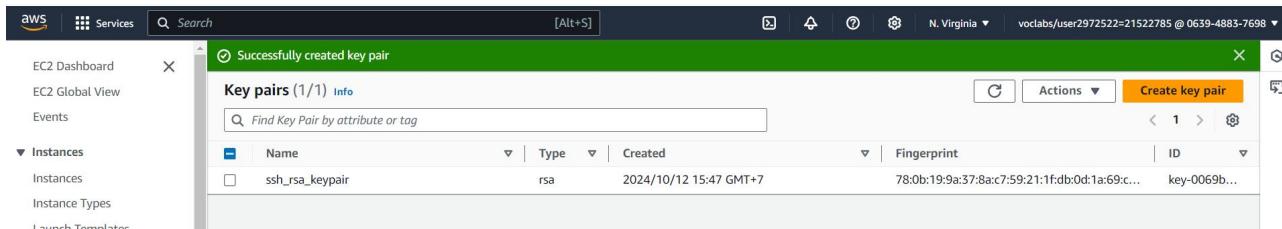
```
PS D:\Learning Space\1st 2024-2025\DevOps\Labs\Lab1_CloudFormation> aws s3 mb s3://grouptwentyonebucket
● make bucket: grouptwentyonebucket
PS D:\Learning Space\1st 2024-2025\DevOps\Labs\Lab1_CloudFormation> aws s3 cp main.yaml s3://grouptwentyonebucket
upload: .\main.yaml to s3://grouptwentyonebucket/main.yaml
● 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 http://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 clouformation stack ‘group21-vpc-stack’ với template url là S3 bucket trên.

Tạo keypair trên AWS Console.



Các Stacks đã được tạo thành công.

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

11

Stack name	Status	Created time	Description
group21-vpc-stack-EC2Stack-1JF3D013SAZFP	CREATE_COMPLETE	2024-10-12 15:50:26 UTC+0700	Create EC2 Instances in Public and Private Subnets
group21-vpc-stack-GatewayStack-1LAPC4N5JAAR	CREATE_COMPLETE	2024-10-12 15:50:14 UTC+0700	Create Internet Gateway and NAT Gateway
group21-vpc-stack-SecurityGroupStack-403Y7UKFF5JA	CREATE_COMPLETE	2024-10-12 15:50:03 UTC+0700	Create Security Groups for EC2 Instances
group21-vpc-stack-SubnetStack-1NLXQRADLIHTW	CREATE_COMPLETE	2024-10-12 15:50:03 UTC+0700	Create Public and Private Subnets
group21-vpc-stack-VPCStack-EZSSBKA1532E	CREATE_COMPLETE	2024-10-12 15:49:40 UTC+0700	Create VPC
group21-vpc-stack	CREATE_COMPLETE	2024-10-12 15:49:38 UTC+0700	Main CloudFormation template to call separate module stacks.

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.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP opt
MyVPC	vpc-0f9c21b70c4273e53	Available	10.0.0.0/16	-	dopt-0b1b
-	vpc-0bf99e22cfe8a4df8	Available	172.31.0.0/16	-	dopt-0b1b

Chi tiết các Subnets trong VPC.

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

The screenshot shows the AWS VPC dashboard with the 'Resource map' tab selected. The diagram illustrates the network topology: a central VPC connected to two Subnets (us-east-1a and us-east-1b) via two Route tables (PublicRouteTable and PrivateRouteTable). Each subnet is connected to one of two Network interfaces: MyInternetGateway or MyNATGateway.

Các Subnets đã được tạo thành công.

The screenshot shows the AWS VPC dashboard with the 'Subnets' table selected. The table lists eight subnets, with 'PrivateSubnet' and 'PublicSubnet' being the ones currently selected (indicated by a checked checkbox). Other subnets listed are not selected.

Name	Subnet ID	State	VPC	IPv4 CIDR
-	subnet-0be8a0fa3db630cd0	Available	vpc-0bf99e22cfe8a4df8	172.31.16.0/20
-	subnet-0762b2846b2f22d99	Available	vpc-0bf99e22cfe8a4df8	172.31.32.0/20
PrivateSubnet	subnet-0dd25e2a02d557920	Available	vpc-0f9c21b70c4273e53 MyVPC	10.0.2.0/24
-	subnet-0286b0ea57cfab53c	Available	vpc-0bf99e22cfe8a4df8	172.31.48.0/20
-	subnet-05293120009fdca4a	Available	vpc-0bf99e22cfe8a4df8	172.31.80.0/20
-	subnet-0963ea22ee018fc8	Available	vpc-0bf99e22cfe8a4df8	172.31.0.0/20
-	subnet-04627d09a2627ea3e	Available	vpc-0bf99e22cfe8a4df8	172.31.64.0/20
PublicSubnet	subnet-0da7f6f8bf6b0ce83	Available	vpc-0f9c21b70c4273e53 MyVPC	10.0.1.0/24

Public Subnet được nối đến internet gateway

The screenshot shows the AWS VPC dashboard with the 'Route table' configuration for the PublicRouteTable. The table lists two routes: one to the 'local' target and another to the internet gateway 'igw-02bddd5f0e2ed8dd1'.

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-02bddd5f0e2ed8dd1

Private Subnet được nối đến NAT Gateway để kết nối Internet

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

The screenshot shows the AWS VPC dashboard. A new VPC named "MyVPC" has been created. Key details include:

- Availability Zone ID:** us-east-1a2
- Network ACL:** acl-056159f08bc858db3
- Auto-assign customer-owned IPv4 address:** No
- IPv6 CIDR reservations:** -
- Resource name DNS AAAA record:** Disabled
- VPC:** vpc-0f9c21b70c4273e53 | MyVPC
- Route table:** rtb-0fda88bc10c9fa7d8 | PrivateRouteTable
- Auto-assign public IPv4 address:** No
- Outpost ID:** -
- Hostname type:** IP name
- Owner:** 063948837698
- Auto-assign IPv6 address:** No
- IPv4 CIDR reservations:** -
- Resource name DNS A record:** Disabled

Internet Gateway đã được tạo

The screenshot shows the AWS VPC dashboard. A new Internet Gateway named "MyInternetGateway" has been created. Key details include:

- Name:** MyInternetGateway
- Internet gateway ID:** igw-02bdd5f0e2ed8dd1
- State:** Attached
- VPC ID:** vpc-0f9c21b70c4273e53 | MyVPC
- Owner:** 063948837698

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.

The screenshot shows the AWS Security Groups page. Four default security groups are listed:

Name	Security group ID	Security group name	VPC ID	Description
-	sg-0cb99542881ccf05b	default	vpc-0f9c21b70c4273e53	default VPC security group
PublicEC2Security...	sg-0c14b02fce314b224	group21-vpc-stack-SecurityGroupStac...	vpc-0f9c21b70c4273e53	Allow SSH from specific IP
PrivateEC2Security...	sg-044873f60921d0e13	group21-vpc-stack-SecurityGroupStac...	vpc-0f9c21b70c4273e53	Allow SSH from Public EC...
-	sg-011fc4df6576f814f	default	vpc-0bf99e22fce8a4df8	default VPC security group

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

Name	Route table ID	Explicit subnet associations	Main	VPC
PublicRouteTable	rtb-0d938ef7ffa90ae10	subnet-0da7f6fb6b0ce...	-	vpc-0f9c21b70c4273e53 MyVPC
PrivateRouteTable	rtb-0fda88bc10c9fa7d8	subnet-0dd25e2a02d557...	-	vpc-0f9c21b70c4273e53 MyVPC
-	rtb-078e09d756033d0e6	-	Yes	vpc-0bf99e22cfe8a4df8
-	rtb-0d01f6ba81e5827da	-	Yes	vpc-0f9c21b70c4273e53 MyVPC

Public Route table kết nối ra internet gateway

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0d938ef7ffa90ae10	No	subnet-0da7f6fb6b0ce83 / PublicSubnet	-
VPC	Owner ID		
vpc-0f9c21b70c4273e53 MyVPC	063948837698		

Routes		Subnet associations		Edge associations		Route propagation		Tags	
Both									
Filter routes									
Destination	Target	Status				Propagated			
0.0.0.0	igw-02bdd5f0e2ed8dd1	Active				No			
10.0.0.0/16	local	Active				No			

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

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0fda88bc10c9fa7d8	No	subnet-0dd25e2a02d557920 / PrivateSubnet	-
VPC	Owner ID		
vpc-0f9c21b70c4273e53 MyVPC	063948837698		

Routes		Subnet associations		Edge associations		Route propagation		Tags	
Both									
Filter routes									
Destination	Target	Status				Propagated			
0.0.0.0	nat-0340e088d81bd15e1	Active				No			
10.0.0.0/16	local	Active				No			

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:

The screenshot shows the AWS EC2 Instance Summary page for an instance named i-02e47a740b24ee476. The instance is running in a Public Subnet (subnet-0da7f6fb6b0ce83) and has a Public IPv4 address of 3.87.14.134. It is an t2.micro instance type. The instance is connected via a VPC ID (vpc-0f9c21b70c4275e53). The instance ARN is arn:aws:ec2:us-east-1:063948837698:instance/i-02e47a740b24ee476.

Private EC2 instance:

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

The screenshot shows the AWS CloudShell interface with the following details:

- Instance summary for i-01070ec653a5734e2 (PrivateEC2Instance)**
- Public IPv4 address:** -
- Private IPv4 addresses:** 10.0.2.243
- Instance state:** Running
- Private IP DNS name (IPv4 only):** ip-10-0-2-243.ec2.internal
- Instance type:** t2.micro
- VPC ID:** vpc-0f9c21b70c4273e53 (MyVPC)
- Subnet ID:** subnet-0dd25e2a02d557920 (PrivateSubnet)
- Instance ARN:** arn:aws:ec2:us-east-1:063948837698:instance/i-01070ec653a5734e2
- AWS Compute Optimizer finding:** Opt-in to AWS Compute Optimizer for recommendations.
- Elastic IP addresses:** -
- Auto Scaling Group name:** -

Truy cập EC2 public instance từ máy cá nhân.

```
ubuntu@ip-10-0-1-113:~ $ ssh -i ./ssh_rsa_keypair.pem ubuntu@3.87.14.134
The authenticity of host '3.87.14.134 (3.87.14.134)' can't be established.
ED25519 key fingerprint is SHA256:ZyCyOprK4L0zJwF9hAYDTArAhv4tBBhdwRo1S07p8BA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '3.87.14.134' (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 Sat Oct 12 09:25:48 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: 10.0.1.113
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-10-0-1-113:~$ |
```

Truy cập internet từ public instance.

```
ubuntu@ip-10-0-1-113:~$ 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=117 time=1.53 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=1.34 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=1.22 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.221/1.363/1.527/0.125 ms
^Cubuntu@ip-10-0-1-113:~$ |
```

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.

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

The screenshot shows the AWS Management Console interface for the VPC section. On the left, there's a navigation pane with options like Virtual private cloud, Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, and Managed prefix lists. The main content area is titled "Security Groups (2/4) Info". It contains a table with columns: Name, Security group ID, Security group name, VPC ID, and Description. The table shows four entries:

Name	Security group ID	Security group name	VPC ID	Description
-	sg-0cb99542881ccf05b	default	vpc-0f9c21b70c4273e53	default VPC secu
<input checked="" type="checkbox"/> PublicEC2Security...	sg-0c14b02cf314b224	group21-vpc-stack-SecurityGroupStack...	vpc-0f9c21b70c4273e53	Allow SSH from :
<input checked="" type="checkbox"/> PrivateEC2Security...	sg-044873f60921d0e13	group21-vpc-stack-SecurityGroupStack...	vpc-0f9c21b70c4273e53	Allow SSH from I
-	sg-011fc4df6576f814f	default	vpc-0bf99e22cf8a4df8	default VPC secu

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

This screenshot shows the detailed view of the "PublicEC2SecurityGroup". The "Details" tab is selected, displaying information such as the security group name, ID, owner, and counts of inbound and outbound rules. The "Inbound rules" tab is active, showing one rule that allows SSH (TCP port 22) from the IP 42.112.228.59/32.

Security group name	Security group ID	Description	VPC ID
group21-vpc-stack-SecurityGroupStack-AO3Y7UKFF5JA-PublicEC2SecurityGroup-X2NsK77rj8oN	sg-0c14b02cf314b224	Allow SSH from specific IP	vpc-0f9c21b70c4273e53

Owner	Inbound rules count	Outbound rules count
063948837698	1 Permission entry	1 Permission entry

Inbound rules (1)						
Security group rule...	IP version	Type	Protocol	Port range	Source	
sgr-09886f03b133c0b48	IPv4	SSH	TCP	22	42.112.228.59/32	

Private SG chỉ cho phép SSH từ public EC2 instance:

This screenshot shows the detailed view of the "PrivateEC2SecurityGroup". The "Details" tab is selected, displaying information such as the security group name, ID, owner, and counts of inbound and outbound rules. The "Inbound rules" tab is active, showing one rule that allows SSH (TCP port 22) from the security group sg-0c14b02cf314b224.

Security group name	Security group ID	Description	VPC ID
group21-vpc-stack-SecurityGroupStack-AO3Y7UKFF5JA-PrivateEC2SecurityGroup-FSSREKc2OapD	sg-044873f60921d0e13	Allow SSH from Public EC2	vpc-0f9c21b70c4273e53

Owner	Inbound rules count	Outbound rules count
063948837698	1 Permission entry	1 Permission entry

Inbound rules (1)						
Security group rule...	IP version	Type	Protocol	Port range	Source	
0f5071093e6cf303f	-	SSH	TCP	22	sg-0c14b02cf314b224...	

