



BÁO CÁO THỰC HÀNH

Bài thực hành 01: Dùng Terraform và CloudFormation 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 xx):

STT	Họ và tên	MSSV
1	Lâm Bảo Duy	20521231
2	Hồ Hải Dương	21520202
3		

Điểm tự đánh giá
10

ĐÁNH GIÁ KHÁC:

Tổng thời gian thực hiện	3 tuần
Link GitHub	
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

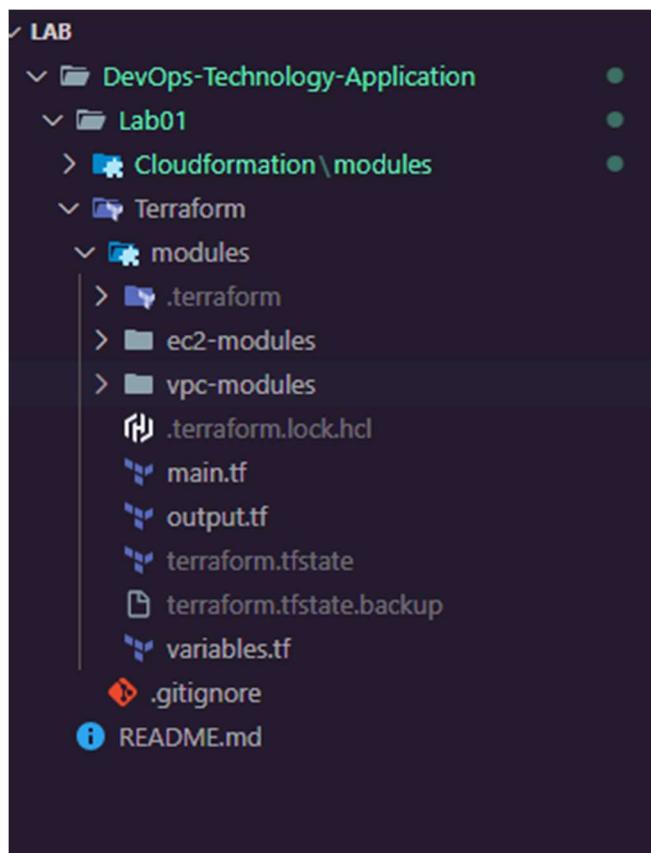
MỤC LỤC

BÁO CÁO CHI TIẾT	3
1. Quản lý và triển khai hạ tầng AWS sử dụng Terraform.	3
a. Cấu trúc thư mục	3
b. Source code cho VPC modules	3
c. Source code cho EC2 modules.....	8
d. Gọi modules VPC và EC2 để tạo instances.	9
e. Triển khai tự động bằng terraform và xem kết quả trên AWS Console.	10
f. Tiến hành SSH Public instance và Private Instance để kiểm tra kết quả.....	15
2. Quản lý và triển khai hạ tầng AWS sử dụng CloudFormation.	17
a. Source code CloudFormation.....	17
a.1. Resources vpc.yaml	17
a.2. Resource ec2.yaml.....	20
a.3. Resource main.yaml.....	21
b. Triển khai và quản lý hạ tầng tự động với CloudFormation.....	22
b.1. Tạo S3 Bucket và upload các file	22
b.2. Tạo Stack trong CloudFormation	23
b.3. Xem chi tiết thông tin của Stack	24
b.4. Kiểm tra tài nguyên được tạo từ CloudFormation	27
b.5. Kiểm tra kết nối SSH tới EC2	29
c. Tiến hành SSH và kiểm tra kết quả.....	30

BÁO CÁO CHI TIẾT

1. Quản lý và triển khai hạ tầng AWS sử dụng Terraform.

a. Cấu trúc thư mục



Hình 1.1: Cấu trúc thư mục cho Terraform viết bằng modules.

- Trong thư mục modules sẽ có 2 thư mục là ec2-modules và vpc-modules và 3 file cấu hình chính gồm main.tf, variables.tf và output.tf. 3 file này sẽ dùng để gọi các modules từ vpc và ec2 để khởi tạo instance.
- Trong ec2-modules sẽ có 3 file gồm main.tf code các dịch vụ cho VPC, bao gồm cả Subnet, Interet Gateway, Route Tables, Security Group, variables.tf để lưu trữ các biến và output.tf để trả về những giá trị mong muốn trong resource.
- Tương tự, vpc-modules cũng sẽ có 3 file, main.tf dùng để code các resource tạo instance EC2, variables.tf để lưu trữ các biến và output.tf để trả về những giá trị mong muốn trong resource.

b. Source code cho VPC modules



```

1 // AWS VPC
2 resource "aws_vpc" "vpc" {
3   cidr_block      = var.vpc_id
4   enable_dns_hostnames = true
5   enable_dns_support  = true
6
7   tags = {
8     Name = "labi_vpc"
9   }
10 }
11
12 // AWS Internet gateway
13 resource "aws_internet_gateway" "igw" {
14   vpc_id = aws_vpc.vpc.id
15
16   tags = {
17     Name = "labi_internet_gateway"
18   }
19 }
20
21 // AWS Public Subnet
22 resource "aws_subnet" "public_subnet" {
23   vpc_id          = aws_vpc.vpc.id
24   cidr_block      = var.public_subnet_cidr
25   availability_zone = var.availability_zone
26   map_public_ip_on_launch = "true"
27
28   tags = {
29     Name = "labi_public_subnet"
30   }
31 }
32
33 // AWS Private Subnet
34 resource "aws_subnet" "private_subnet" {
35   vpc_id          = aws_vpc.vpc.id
36   cidr_block      = var.private_subnet_cidr
37   availability_zone = var.availability_zone
38   map_public_ip_on_launch = "false"
39
40   tags = {
41     Name = "labi_private_subnet"
42   }
43 }
44
45 # AWS Default Security Group for VPC
46 resource "aws_security_group" "default_sg" {
47   name        = "default_ec2_sg"
48   description = "Default Security Group for EC2"
49   vpc_id      = aws_vpc.vpc.id
50
51   ingress {
52     from_port    = 0
53     to_port      = 0
54     protocol     = "-1"
55   }
56
57   egress {
58     from_port    = 0
59     to_port      = 0
60     protocol     = "-1"
61     cidr_blocks = ["0.0.0.0/0"]
62   }
63
64   tags = {
65     Name = "labi_default_security_group"
66   }
67 }

```

Hình 1.2: Tạo các resource cho module VPC

- Trong VPC modules sẽ có các resource bao gồm:

- o aws_vpc: Tạo 1 VPC trên AWS

- aws_internet_gateway: Tạo Internet Gateway trên AWS và gắn với VPC dùng để cho phép các tài nguyên bên trong có thể truy cập Internet.
- aws_subnet: Tạo public subnet để kết nối với Internet Gateway và private Subnet để sử dụng NAT kết nối ra bên ngoài và gắn với VPC
- aws_security_group: Tạo Security Group mặc định cho VPC

```
69  resource "aws_eip" "nat" {
70    domain = "vpc"
71  }
72
73 // AWS Nat Gateway
74 resource "aws_nat_gateway" "nat_gw" {
75   allocation_id = aws_eip.nat.id
76   subnet_id     = aws_subnet.public_subnet.id
77   depends_on    = [aws_internet_gateway.igw]
78 }
79
```

Hình 1.2: Tạo các resource cho module VPC (tt)

- aws_eip: Elastic IP, tạo 1 IP tĩnh cho NAT gateway
- aws_internet_gateway: Tạo Gateway cho AWS và gắn với VPC dùng để cho phép các tài nguyên trong Private Subnet có thể truy cập Internet.

```

80  # AWS Public Route Table
81 resource "aws_route_table" "rtb_public" {
82    vpc_id = aws_vpc.vpc.id
83
84    route {
85      cidr_block = "0.0.0.0/0"
86      gateway_id = aws_internet_gateway.igw.id
87    }
88
89    tags = {
90      Name = "lab1_public_route_table"
91    }
92  }
93
94 // AWS Private Route table
95 resource "aws_route_table" "rtb_private" {
96   vpc_id = aws_vpc.vpc.id
97
98   route {
99     cidr_block      = "0.0.0.0/0"
100    nat_gateway_id = aws_nat_gateway.nat_gw.id
101  }
102
103  tags = {
104    Name = "lab1_private_route_table"
105  }
106}
107
108 # Connect Public Subnet with Internet Gateway
109 resource "aws_route_table_association" "public-association" {
110   subnet_id      = aws_subnet.public_subnet.id
111   route_table_id = aws_route_table.rtb_public.id
112 }
113
114 # Connect Private Subnet with NAT Gateway
115 resource "aws_route_table_association" "private-association" {
116   subnet_id      = aws_subnet.private_subnet.id
117   route_table_id = aws_route_table.rtb_private.id
118 }

```

Hình 1.3: Tạo các resource cho module VPC (tt)

- aws_route_table: Tạo public và private Route Table, gắn vào VPC, public route table định tuyến thông qua internet gateway và private route table định tuyến thông qua NAT Gateway
- aws_route_table_association: Tạo liên kết giữa giữa public subnet và public route tables, private subnet và private route tables.

```
96  # AWS Public EC2 Security group
97  resource "aws_security_group" "public_ec2_sg" {
98    name      = "public_ec2_sg"
99    description = "Public Security Group for EC2"
100   vpc_id     = aws_vpc.vpc.id
101
102   ingress {
103     from_port  = 22
104     to_port    = 22
105     protocol   = "tcp"
106     cidr_blocks = ["0.0.0.0/0"]
107   }
108
109   egress {
110     from_port  = 0
111     to_port    = 0
112     protocol   = "-1"
113     cidr_blocks = ["0.0.0.0/0"]
114   }
115
116   tags = {
117     Name = "lab1_public_security_group"
118   }
119 }
120
121 # AWS Private EC2 Security group
122 resource "aws_security_group" "private_ec2_sg" {
123   name      = "private_ec2_sg"
124   description = "Private Security Group for EC2"
125   vpc_id     = aws_vpc.vpc.id
126
127   ingress {
128     from_port      = 22
129     to_port        = 22
130     protocol       = "tcp"
131     security_groups = [aws_security_group.public_ec2_sg.id]
132   }
133
134   egress {
135     from_port      = 0
136     to_port        = 0
137     protocol       = "-1"
138     cidr_blocks   = ["0.0.0.0/0"]
139   }
140
141   tags = {
142     Name = "lab1_private_security_group"
143   }
144 }
```

Hình 1.4: Tạo các resource cho module VPC (tt)

- aws_security_group: Tạo các rules cho EC2 instances
 - public security group: cho phép port 22 để SSH và nhận tất cả các IP, có thể thay đổi cidr bằng IP cá nhân để giới hạn rules và tăng cường bảo mật
 - private security group: cho phép port 22 để SSH từ public EC2 instance.

c. Source code cho EC2 modules.

```

1 resource "aws_instance" "public_ec2_instace" {
2   ami           = var.ami
3   instance_type = var.instance_type
4   subnet_id    = var.public_subnet_id
5   security_groups = [var.public_security_groups]
6
7   tags = {
8     Name = "lab1_public_ec2_instance"
9   }
10 }
11
12 resource "aws_instance" "private_ec2_instace" {
13   ami           = var.ami
14   instance_type = var.instance_type
15   subnet_id    = var.private_subnet_id
16   security_groups = [var.private_security_groups]
17
18   tags = {
19     Name = "lab1_privte_ec2_instance"
20   }
21 }
```

Hình 1.5: Tạo các resource cho module EC2

- Tạo public và private instance cho EC2, tham số truyền vào gồm:
 - o ami: chỉ định hệ điều hành cho instance
 - o instance_type: loại instance ví dụ như t2.micro
 - o subnet_id: truyền subnet id tương ứng, private subnet với private instance và public subnet với public instance
 - o security_group: truyền vào public security group với public instance để cho phép instance có thể truy cập được internet, truyền vào private security group chỉ cho phép truy cập thông qua ssh từ public instance.

d. Gọi modules VPC và EC2 để tạo instances.

```

1  provider "aws" {
2    region = "us-east-1"
3  }
4
5  module "vpc" {
6    source = "./vpc-modules"
7
8    vpc_id           = "10.0.0.0/16"
9    public_subnet_cidr = "10.0.1.0/24"
10   private_subnet_cidr = "10.0.2.0/24"
11   availability_zone   = "us-east-1a"
12 }
13
14 module "ec2" {
15   source          = "./ec2-modules"
16   key_name        = "customkey"
17   ami             = "ami-005fc0f236362e99f"
18   instance_type   = "t2.micro"
19   public_subnet_id = module.vpc.public_subnet_id
20   public_security_groups = module.vpc.public_sg
21   private_subnet_id  = module.vpc.private_subnet_id
22   private_security_groups = module.vpc.private_sg
23 }

```

Hình 1.6: Gọi các modules để triển khai instance

- Cung cấp region cho provider AWS
- Module VPC và EC2 sẽ truyền các biến và giá trị dựa trên các variables được tạo trong file main của các modules tương ứng
- VPC Module:
 - o source: chỉ định source cho module VPC
 - o vpc_id: gán id cho vpc là 10.0.0.0/16
 - o public_subnet_cidr: gán public subnet cho VPC là 10.0.1.0/24
 - o private_subnet_cidr: gán private subnet cho VPC là 10.0.2.0/24
 - o availability_zone: gán availability zone cho VPC là us-east-1a
- EC2 module:
 - o source: chỉ định source cho module EC2
 - o key_name: tham chiếu đến keypair trên AWS để ssh
 - o ami: chỉ định ami để xác định hệ điều hành cho instance
 - o instance type: t2.micro
 - o public_subnet_id, private_subnet_id: truyền subnet từ module VPC để tạo instance tương ứng
 - o public_security_group, private_security_group: truyền security group từ module VPC để tạo các instance tương ứng

e. Triển khai tự động bằng terraform và xem kết quả trên AWS Console.

```
Enter a value. yes

aws_key_pair.my_key_pair: Creating...
module.vpc.aws_eip.nat: Creating...
module.vpc.aws_vpc.vpc: Creating...
aws_key_pair.my_key_pair: Creation complete after 2s [id=custom-key]
module.vpc.aws_eip.nat: Creation complete after 3s [id=eipalloc-004d5bbe0133e8f2d]
module.vpc.aws_vpc.vpc: Still creating... [10s elapsed]
module.vpc.aws_vpc.vpc: Creation complete after 16s [id=vpc-07f00e297bf3f8c76]
module.vpc.aws_internet_gateway.igw: Creating...
module.vpc.aws_subnet.public_subnet: Creating...
module.vpc.aws_subnet.private_subnet: Creating...
module.vpc.aws_security_group.default_sg: Creating...
module.vpc.aws_security_group.public_ec2_sg: Creating...
module.vpc.aws_internet_gateway.igw: Creation complete after 2s [id=igw-0fe5ba5b8e73378ec]
module.vpc.aws_route_table.rtb_public: Creating...
module.vpc.aws_subnet.private_subnet: Creation complete after 2s [id=subnet-0effff5bf856bb7f2c]
module.vpc.aws_route_table.rtb_public: Creation complete after 3s [id=rtb-02f78766171f30e18]
module.vpc.aws_security_group.default_sg: Creation complete after 5s [id=sg-06e5d5c6ea96528a2]
module.vpc.aws_security_group.public_ec2_sg: Creation complete after 6s [id=sg-095f979f183945a6d]
module.vpc.aws_security_group.private_ec2_sg: Creating...
module.vpc.aws_subnet.public_subnet: Still creating... [10s elapsed]
module.vpc.aws_security_group.private_ec2_sg: Creation complete after 5s [id=sg-03b4c7aae18a47d74]
module.ec2.aws_instance.private_ec2_instance: Creating...
module.vpc.aws_subnet.public_subnet: Creation complete after 13s [id=subnet-06891fe59950aa064]
module.vpc.aws_route_table_association.public-association: Creating...
module.vpc.aws_nat_gateway.nat_gw: Creating...
module.ec2.aws_instance.public_ec2_instance: Creating...
module.vpc.aws_route_table_association.public-association: Creation complete after 1s [id=rtbassoc-06b9a33a9c84f21a9]
module.ec2.aws_instance.private_ec2_instance: Still creating... [10s elapsed]
module.vpc.aws_nat_gateway.nat_gw: Still creating... [10s elapsed]
module.ec2.aws_instance.public_ec2_instance: Still creating... [10s elapsed]
module.ec2.aws_instance.private_ec2_instance: Creation complete after 16s [id=i-0b68979d1d6e25594]
module.ec2.aws_instance.public_ec2_instance: Creation complete after 16s [id=i-0ce12a45534afaf2e]
module.vpc.aws_nat_gateway.nat_gw: Still creating... [20s elapsed]
module.vpc.aws_nat_gateway.nat_gw: Still creating... [30s elapsed]
module.vpc.aws_nat_gateway.nat_gw: Still creating... [40s elapsed]
module.vpc.aws_nat_gateway.nat_gw: Still creating... [50s elapsed]
module.vpc.aws_nat_gateway.nat_gw: Still creating... [1m0s elapsed]
module.vpc.aws_nat_gateway.nat_gw: Still creating... [1m10s elapsed]
module.vpc.aws_nat_gateway.nat_gw: Still creating... [1m20s elapsed]
module.vpc.aws_nat_gateway.nat_gw: Still creating... [1m30s elapsed]
module.vpc.aws_nat_gateway.nat_gw: Creation complete after 1m38s [id=nat-0444b81cc21fe9fa6]
module.vpc.aws_route_table.rtb_private: Creating...
module.vpc.aws_route_table.rtb_private: Creation complete after 3s [id=rtb-09cd97e519b64c7e1]
module.vpc.aws_route_table_association.private-association: Creating...
module.vpc.aws_route_table_association.private-association: Creation complete after 1s [id=rtbassoc-0af6b9b9d0f6ad054]

Apply complete! Resources: 16 added, 0 changed, 0 destroyed.

In 127. Col 21 (144 selected)
```

Hình 1.7: Triển khai các hạ tầng tự động bằng Terraform.

- Tiến hành triển khai hạ tầng với:
 - o terraform init → terraform plan → terraform apply
 - o Các hạ tầng sẽ được triển khai tự động, tạo và trả về các kết quả ID của các Resource.
- Sau khi sử dụng terraform apply và trả về kết quả complete. Kiểm tra các hạ tầng trên AWS console.

Your VPCs (2) Info							Last update 20 minutes ago
<input type="checkbox"/> Name VPC ID State IPv4 CIDR IPv6 ... DHCP option set Main route table Main network ACL							
<input type="checkbox"/>	–	ypc-07ed10898f08dcc8d	Available..	172.31.0.0/16	–	dopt-07446a1761f2...	rtb-0de339d28f100459e
<input type="checkbox"/>	lab1_vpc	ypc-07f00e297bf3f8c76	Available..	10.0.0.0/16	–	dopt-07446a1761f2...	rtb-0e396101b92683589

Hình 1.8: Triển khai các hạ tầng tự động (tt).

- Một VPC mới được tạo bởi Terraform với các giá trị được cấu hình:
 - o IPv4 CIDR là 10.0.0/16

<input type="checkbox"/>	lab1_private_subnet	subnet-0efff5bf856bb7f2c	Available	vpc-07f00e297bf3f8c76 lab1_vpc	10
<input type="checkbox"/>	-	subnet-0295a9ad8a70d29e4	Available	vpc-07ed10898f08dcc8d	11
<input type="checkbox"/>	-	subnet-0868d43f2fbfd39b7	Available	vpc-07ed10898f08dcc8d	11
<input type="checkbox"/>	lab1_public_subnet	subnet-06891fe59950aa064	Available	vpc-07f00e297bf3f8c76 lab1_vpc	10

Hình 1.9: Triển khai các hạ tầng tự động (tt).

- Hai Subnet mới được tạo và gán với VPC ID lab1_vpc với các giá trị:
 - o IPv4 CIDR của public subnet là 10.0.1.0/24, private subnet là 10.0.2.0/24

Elastic IP addresses (1)						
Actions ▾ Allocate						
	Name	Allocated IPv4 addr...	Type	Allocation ID	Reverse DNS record	Associated instance ID
<input type="checkbox"/>	-	3.217.74.138	Public IP	eipalloc-004d5bbe0133e8f2d	-	-

Hình 1.10: Triển khai các hạ tầng tự động (tt).

- Elastic IP được tạo để gán cho NAT Gateway với các giá trị được cấu hình:
 - o Allocated IPv4 address: Địa chỉ IP tĩnh 3.217.74.138 được tạo để gán cho NAT để private subnet có thể kết nối được internet
 - o Allocation ID tương ứng ID cấu hình bởi terraform ở hình 1.7
 - o Private IP: là 10.0.1.209

NAT gateways (1) Info						
Actions ▾ Create NAT gateway						
◀ 1 ▶ ⌂						
NAT gateway ID	Con...	State	Stat...	Primary public I...	Primary pri...	VPC
nat-0444b81cc21fe9fa6	Public	Available.	-	3.217.74.138	10.0.1.209	eni-02a... vpc-07f00e297bf3f8c76 / lab1_vpc subnet-06891fe59950aa064 / lab1_public_subnet

Hình 1.11: Triển khai các hạ tầng tự động (tt).

- NAT Gateway được tạo với các giá trị được cấu hình:
 - o Primary Public IP: 3.217.74.138 và Private Private IP: là 3.217.74.138 được tạo bởi EIP
 - o NAT gateway ID tương ứng với ID cấu hình bởi Terraform hình 1.7
 - o NAT Gateway được gán với lab1_vpc đã tạo
 - o Subnet: gán với lab1_public_subnet để có thể kết nối với Internet bằng NAT.

Internet gateways (2) Info					
Search					
	Name	Internet gateway ID	State	VPC ID	Owner
<input type="checkbox"/>	-	igw-0c878678f22aa49a2	Attached	vpc-07ed10898f08dcc8d	339713068874
<input type="checkbox"/>	lab1_internet_gate...	igw-0fe5ba5b8e73378ec	Attached	vpc-07f00e297bf3f8c76 lab1_vpc	339713068874

Hình 1.12: Triển khai các hạ tầng tự động (tt).

- Internet Gateway được tạo để kết nối với Internet với các giá trị được cấu hình:
 - o Internet Gateway ID tương ứng với ID cấu hình bởi Terraform hình 1.7
 - o Gateway được gán với lab1_vpc đã tạo

Route tables (4) Info						Last updated 21 minutes ago	Actions	C
<input type="checkbox"/>	Name	Route table ID	Explicit subnet associations	Edge...	Main	VPC	Owner ID	C
<input type="checkbox"/>	lab1_private_route_table	rtb-09cd97e519b64c7e1	subnet-0e8ff5bf856bb7f2c / lab1_private_subnet	-	No	vpc-07f00e297bf3f8c76 lab1_vpc	339713068874	Actions
<input type="checkbox"/>	lab1_public_route_table	rtb-02f78766171f30e18	subnet-0e891fe59950aa064 / lab1_public_subnet	-	No	vpc-07f00e297bf3f8c76 lab1_vpc	339713068874	Actions

Hình 1.12: Triển khai các hạ tầng tự động (tt).

- Public và Private route table được với các giá trị được cấu hình:
 - o Public và Private Route Table ID tương ứng với ID cấu hình bởi Terraform hình 1.7
 - o Các route table gán với lab1_vpc đã tạo
 - o Subnet association: liên kết public route table với public subnet và private route table với private subnet

Security Groups (5) Info						Actions	Exp
<input type="checkbox"/>	Name	Security group ID	Security group na...	VPC ID	Description		
<input type="checkbox"/>	-	sg-0cbc5d94e1b942fa	default	vpc-07ed10898f08dcc8d	default VPC security group		
<input type="checkbox"/>	lab1_public_security_group	sg-095f979f183945a6d	public_ec2_sg	vpc-07f00e297bf3f8c76	Public Security Group for EC2		
<input type="checkbox"/>	lab1_private_security_group	sg-03b4c7aae18a47d74	private_ec2_sg	vpc-07f00e297bf3f8c76	Private Security Group for EC2		
<input type="checkbox"/>	lab1_default_security_group	sg-06e5d5c6ea96528a2	default_ec2_sg	vpc-07f00e297bf3f8c76	Default Security Group for EC2		
<input type="checkbox"/>	-	sg-0281555accfd8914f	default	vpc-07f00e297bf3f8c76	default VPC security group		

Hình 1.13: Triển khai các hạ tầng tự động (tt).

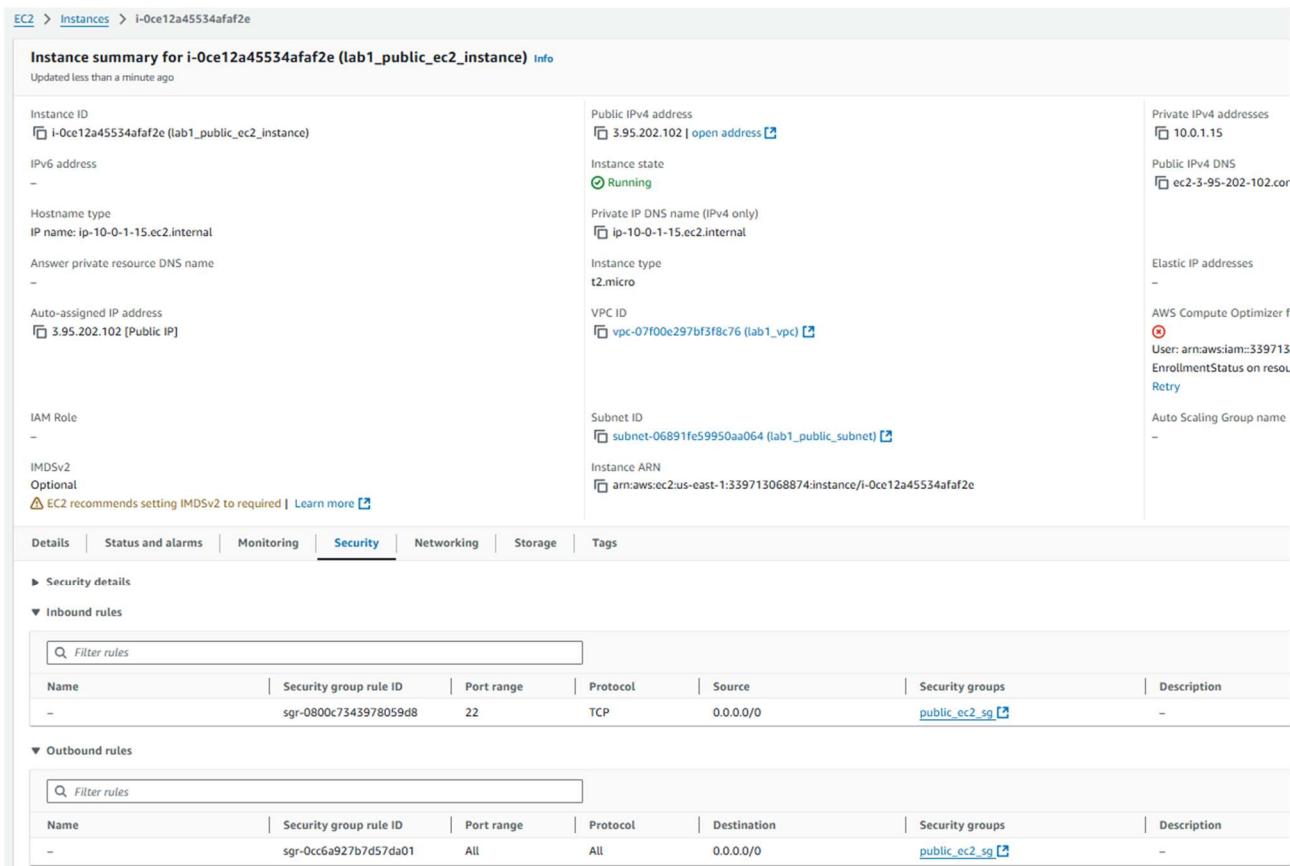
- Các Security group được tạo để thiết lập các rules với các giá trị được cấu hình:
 - o Public, Private, Default Security Group gồm được gán với lab1_vpc đã tạo

Instances (2) Info													Last updated less than a minute ago	Actions	Launch instances
<input type="checkbox"/>	Name	Instance ID	Instance state	Instanc...	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitor...	Security group name		
<input type="checkbox"/>	lab1_public_ec2_instance	i-0ce12a45534afaf2e	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-3-95-202-102.com...	3.95.202.102	-	-	disabled	public_ec2_sg		
<input type="checkbox"/>	lab1_private_ec2_instance	i-0b68979d1d6e25594	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-	-	-	-	disabled	private_ec2_sg		

Hình 1.14: Triển khai các hạ tầng tự động (tt).

- Public và Private Instance được với các giá trị được cấu hình:
 - o Instance type: t2.micro
 - o Availability zone: us-east-1a
 - o Public EC2 gán với Public Security Group

- Private EC2 gán với Private Security Group



Hình 1.15: Cấu hình chi tiết của Public EC2

- Các IP của Public EC2 bao gồm Instance ID, VPC ID, Subnet ID, Security Group ID, ... tương tự với ID đã được cấu hình bởi terraform ở hình 1.7
- Public IPv4: 3.95.202.102, Private IPv4: 10.0.1.15
- Security Group allow port 22 cho phép SSH từ một source IP cụ thể, có thể thay thế Source bằng IP cá nhân.

Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
-	sgr-0d749f8d9016a8c10	22	TCP	sg-095f979f183945a6d	private_ec2_sg	-

Name	Security group rule ID	Port range	Protocol	Destination	Security groups	Description
-	sgr-03ec5725e9da0f708	All	All	0.0.0.0/0	private_ec2_sg	-

Hình 1.16: Cấu hình chi tiết private EC2 instance

- Các IP của Private EC2 bao gồm Instance ID, VPC ID, Subnet ID, Security Group ID, ... tương tự với ID đã được cấu hình bởi terraform ở hình 1.7
- Private IPv4: 10.0.2.148
- Security Group allow port 22 cho phép SSH từ Source Public Security Group, có nghĩa là Private EC2 chỉ có thể truy cập Internet thông qua Public EC2

f. Tiến hành SSH Public instance và Private Instance để kiểm tra kết quả

```
Bao Duy@DESKTOP-QE2KJE6 MINGW64 /d/lab-nt548/lab/DevOps-Technology-Application/Lab01/Terraform/modules (dev)
$ ssh -i ~/.ssh/id_rsa ubuntu@3.95.202.102
The authenticity of host '3.95.202.102 (3.95.202.102)' can't be established.
N OPENSSH PRIVATE KEY-----
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-10-0-1-15:~$ ping google.com
PING google.com (172.253.122.100) 56(84) bytes of data.
64 bytes from bh-in-f100.1e100.net (172.253.122.100): icmp_seq=1 ttl=106 time=1.81 ms
64 bytes from bh-in-f100.1e100.net (172.253.122.100): icmp_seq=2 ttl=106 time=1.48 ms
64 bytes from bh-in-f100.1e100.net (172.253.122.100): icmp_seq=3 ttl=106 time=1.95 ms
64 bytes from bh-in-f100.1e100.net (172.253.122.100): icmp_seq=4 ttl=106 time=1.97 ms
```

Hình 1.18: SSH tới Public EC2 Instance

- SSH với Public EC2 Instance bằng lệnh:
 - ssh -i ~/.ssh/id_rsa ubuntu@3.95.202.102
 - Trong đó:
 - o id_rsa: là private key
 - o ubuntu là hệ điều hành được tạo dựa trên ami
 - o 3.95.202.102 là IP Public của Public EC2 Instance
- Sau khi kết nối thành công thì console sẽ hiển thị ubuntu@ip-10-0-1-15
 - o 10.0.1.15 chính là IP Private của Public EC2 Instance
- Ping tới google.com và thành công kết nối tới Internet.

```
ubuntu@ip-10-0-1-15:~/ssh$ ssh -i id_rsa ubuntu@10.0.2.148
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-1015-aws x86_64)

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

 System information as of Thu Oct 10 08:14:47 UTC 2024

 System load: 0.0 Processes: 101
 Usage of /: 21.1% of 7.57GB Users logged in: 0
 Memory usage: 20% IPv4 address for eth0: 10.0.2.148
 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-10-0-2-148:~$ ping google.com
PING google.com (142.251.167.139) 56(84) bytes of data.
64 bytes from ww-in-f139.1e100.net (142.251.167.139): icmp_seq=1 ttl=57 time=2.74 ms
64 bytes from ww-in-f139.1e100.net (142.251.167.139): icmp_seq=2 ttl=57 time=2.28 ms
64 bytes from ww-in-f139.1e100.net (142.251.167.139): icmp_seq=3 ttl=57 time=2.00 ms
64 bytes from ww-in-f139.1e100.net (142.251.167.139): icmp_seq=4 ttl=57 time=2.45 ms
64 bytes from ww-in-f139.1e100.net (142.251.167.139): icmp_seq=5 ttl=57 time=2.19 ms
64 bytes from ww-in-f139.1e100.net (142.251.167.139): icmp_seq=6 ttl=57 time=2.20 ms
64 bytes from ww-in-f139.1e100.net (142.251.167.139): icmp_seq=7 ttl=57 time=1.80 ms
```

Hình 1.18: Kiểm tra kết nối

- Tạo file id_rsa và copy private key vào trong đó, cấp quyền read write cho private key sau đó tiến hành ssh từ public EC2 bằng lệnh:
 - o ssh -i ~/ssh/id_rsa ubuntu@10.0.2.148
- Trong đó:
 - o id_rsa là private key
 - o ubuntu là hệ điều hành được tạo dựa trên ami
 - o 10.0.2.148 là IP Private của Private EC2 Instance
- Sau khi kết nối thành công thì console sẽ hiển thị ubuntu@ip-10-0-2-148
 - o Ssh thành công từ Public EC2 vào Private EC2.
- Ping tới google.com và thành công kết nối tới Internet.

2. Quản lý và triển khai hạ tầng AWS sử dụng CloudFormation.

a. Source code CloudFormation

a.1. Resources *vpc.yaml*

Tạo một VPC để triển khai EC2, kết nối được ra internet thông qua Internet Gateway và NAT Gateway:

- aws_vpc: Tạo một VPC với CIDR block 10.0.0.0/16.
- aws_internet_gateway: Tạo Internet Gateway để các tài nguyên trong VPC có thể kết nối với Internet.
- aws_subnet: Tạo subnet công cộng và riêng tư, kết nối với Internet Gateway và NAT Gateway.
- aws_route_table: Tạo bảng định tuyến cho cả subnet công cộng và riêng tư.
- aws_nat_gateway: Sử dụng Elastic IP để tạo NAT Gateway cho kết nối từ subnet riêng tư ra Internet.

```

21  Resources:
22  MyVPC:
23    Type: AWS::EC2::VPC
24  Properties:
25    CidrBlock: !Ref VpcCIDR
26    EnableDnsSupport: true
27    EnableDnsHostnames: true
28  Tags:
29    - Key: Name
30    Value: !Sub "${Environment}_VPC"
31
32  PublicSubnet:
33    Type: AWS::EC2::Subnet
34  Properties:
35    VpcId: !Ref MyVPC
36    CidrBlock: !Ref PublicSubnetCIDR
37    AvailabilityZone: !Ref AvailabilityZone
38    MapPublicIpOnLaunch: true
39  Tags:
40    - Key: Name
41    Value: !Sub "${Environment}_PublicSubnet"
42
43  PrivateSubnet:
44    Type: AWS::EC2::Subnet
45  Properties:
46    VpcId: !Ref MyVPC
47    CidrBlock: !Ref PrivateSubnetCIDR
48    AvailabilityZone: !Ref AvailabilityZone
49  Tags:
50    - Key: Name
51    Value: !Sub "${Environment}_PrivateSubnet"
52
53  InternetGateway:
54    Type: AWS::EC2::InternetGateway
55  Properties:
56  Tags:
57    - Key: Name
58    Value: ${Environment}_InternetGateway
59
60  AttachGateway:
61    Type: AWS::EC2::VPCGatewayAttachment
62  Properties:
63    VpcId: !Ref MyVPC
64    InternetGatewayId: !Ref InternetGateway
65

```

Hình 2.1: Resources vpc.yaml

```

66  PublicRouteTable:
67    Type: AWS::EC2::RouteTable
68    Properties:
69      VpcId: !Ref MyVPC
70      Tags:
71        - Key: Name
72          Value: "${Environment}_PublicRouteTable"
73
74  PublicRoute:
75    Type: AWS::EC2::Route
76    DependsOn: AttachGateway
77    Properties:
78      RouteTableId: !Ref PublicRouteTable
79      DestinationCidrBlock: "0.0.0.0/0"
80      GatewayId: !Ref InternetGateway
81
82  PublicSubnetRouteTableAssociation:
83    Type: AWS::EC2::SubnetRouteTableAssociation
84    Properties:
85      SubnetId: !Ref PublicSubnet
86      RouteTableId: !Ref PublicRouteTable
87
88  PrivateRouteTable:
89    Type: AWS::EC2::RouteTable
90    Properties:
91      VpcId: !Ref MyVPC
92      Tags:
93        - Key: Name
94          Value: !Sub "${Environment}_PrivateRouteTable"
95
96  NatEIP:
97    Type: AWS::EC2::EIP
98    Properties:
99      Tags:
100        - Key: Name
101          Value: custom_NatEIP
102
103 NatGateway:
104   Type: AWS::EC2::NatGateway
105   Properties:
106     AllocationId: !GetAtt NatEIP.AllocationId
107     SubnetId: !Ref PublicSubnet
108     Tags:
109       - Key: Name
110         Value: !Sub "${Environment}_NatGateway"

```

Hình 2.2: Resources vpc.yaml

```

112  PrivateRoute:
113    Type: AWS::EC2::Route
114    Properties:
115      RouteTableId: !Ref PrivateRouteTable
116      DestinationCidrBlock: "0.0.0.0/0"
117      NatGatewayId: !Ref NatGateway
118
119  PrivateSubnetRouteTableAssociation:
120    Type: AWS::EC2::SubnetRouteTableAssociation
121    Properties:
122      SubnetId: !Ref PrivateSubnet
123      RouteTableId: !Ref PrivateRouteTable
124
125  PublicEC2SecurityGroup:
126    Type: AWS::EC2::SecurityGroup
127    Properties:
128      GroupDescription: Allow SSH access from specific IP
129      VpcId: !Ref MyVPC
130      SecurityGroupIngress:
131        - IpProtocol: tcp
132          FromPort: 22
133          ToPort: 22
134          CidrIp: !Ref PublicIP
135      Tags:
136        - Key: Name
137          Value: !Sub "${Environment}_PublicEC2SecurityGroup"
138
139  PrivateEC2SecurityGroup:
140    Type: AWS::EC2::SecurityGroup
141    Properties:
142      GroupDescription: Allow SSH access from Public EC2 instance
143      VpcId: !Ref MyVPC
144      SecurityGroupIngress:
145        - IpProtocol: tcp
146          FromPort: 22
147          ToPort: 22
148          SourceSecurityGroupId: !Ref PublicEC2SecurityGroup
149      Tags:
150        - Key: Name
151          Value: !Sub "${Environment}_PrivateEC2SecurityGroup"

```

Hình 2.3: Resources vpc.yaml

a.2. Resource ec2.yaml

Tạo hai EC2 instance, 1 public và 1 private, để kiểm tra kết nối và truy cập vào resource VPC.

- Public EC2 instance: Có thể truy cập từ Internet.
- Private EC2 instance: Chỉ có thể truy cập từ Public EC2 qua mạng nội bộ.
- Security Group: Được tạo để bảo vệ các EC2 instance, với các quy tắc bảo mật cho phép hoặc ngăn cản các kết nối từ ngoài vào.

```

25 Resources:
26   CustomKeyPair:
27     Type: 'AWS::EC2::KeyPair'
28     Properties:
29       KeyName: MyKeyValuePair
30       PublicKeyMaterial: |
31         ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQCX0f7o18ixX7fDMDODwD
32         0NdEprkrK5qbG9cQ/MMC5X4zOcw0n9hIue5BhExh0S7EpXCIhTIIsPXdav
33         IUTtaXiY4g9EI76F96U0LIwVgdvpJ+44arqmDCoa3A3qgpWYBQhTkBsdlM
34         tg3rLZ5familcHxGS47hEf7hvIH10wSToJUb7I2PHQbwD8Q+Me8/X/Ij
35         d4/ynlbwYppHTwe0gttgWEfROh4YWxqPAU43Lk7sEety9Kwxs1CorVbygL
36         HB6bGb75rGoUqlgmXOfTRBT9bCFILU/lPlXQXJr70CSixqGsULpIuanRFg
37         nVvwb7P2wmczgtcI51LGVObNUQKmTpcD Bao Duy@DESKTOP-QE2KJE6
38
39
40   PublicEC2Instance:
41     Type: AWS::EC2::Instance
42     Properties:
43       InstanceType: !Ref INSTANCETYPE
44       KeyName: !Ref CustomKeyPair
45       ImageId: !Ref AMI
46       SubnetId: !Ref PublicSubnetId
47       SecurityGroupIds:
48         - !Ref PublicEC2SecurityGroup
49     Tags:
50       - Key: Name
51       | Value: !Sub "${Environment}_PublicEC2Instance"
52
53   PrivateEC2Instance:
54     Type: AWS::EC2::Instance
55     Properties:
56       InstanceType: !Ref INSTANCETYPE
57       KeyName: !Ref CustomKeyPair
58       ImageId: !Ref AMI
59       SubnetId: !Ref PrivateSubnetId
60       SecurityGroupIds:
61         - !Ref PrivateEC2SecurityGroup
62     Tags:
63       - Key: Name
64       | Value: !Sub "${Environment}_PrivateEC2Instance"

```

Hình 2.4: Resources ec2.yaml

a.3. Resource main.yaml

Tạo file main.yaml giúp các stack con dễ dàng và có tổ chức, giảm thiểu rủi ro khi có nhiều thành phần trong hệ thống.

main.yaml đóng vai trò là file chính, sử dụng nested stack để kết nối các template con vpc.yaml và ec2.yaml. Giúp chia nhỏ cấu trúc hạ tầng, dễ quản lý và cập nhật từng phần.

```

4  Parameters:
5    VpcCIDR:
6      Type: String
7      Default: "192.168.0.0/16"
8    PublicSubnetCIDR:
9      Type: String
10     Default: "192.168.1.0/24"
11    PrivateSubnetCIDR:
12      Type: String
13      Default: "192.168.2.0/24"
14    AvailabilityZone:
15      Type: String
16      Default: "us-east-1a"
17    BucketName:
18      Type: String
19      Default: "labil3bucketnhom14"
20
21 Resources:
22   VPCStack:
23     Type: AWS::CloudFormation::Stack
24     Properties:
25       TemplateURL: !Sub "https://${BucketName}.s3.amazonaws.com/vpc.yaml"
26       Parameters:
27         VpcCIDR: !Ref VpcCIDR
28         PublicSubnetCIDR: !Ref PublicSubnetCIDR
29         PrivateSubnetCIDR: !Ref PrivateSubnetCIDR
30         AvailabilityZone: !Ref AvailabilityZone
31
32   EC2Stack:
33     Type: AWS::CloudFormation::Stack
34     Properties:
35       TemplateURL: !Sub "https://${BucketName}.s3.amazonaws.com/ec2.yaml"
36       Parameters:
37         VPCId: !GetAtt VPCStack.Outputs.VPCId
38         PublicSubnetId: !GetAtt VPCStack.Outputs.PublicSubnetId
39         PrivateSubnetId: !GetAtt VPCStack.Outputs.PrivateSubnetId
40         PublicEC2SecurityGroup: !GetAtt VPCStack.Outputs.PublicSgId
41         PrivateEC2SecurityGroup: !GetAtt VPCStack.Outputs.PrivateSgId
42
43 Outputs:
44   VPCId:
45     Value: !GetAtt VPCStack.Outputs.VPCId
46   PublicSubnetId:
47     Value: !GetAtt VPCStack.Outputs.PublicSubnetId
48   PrivateSubnetId:
49     Value: !GetAtt VPCStack.Outputs.PrivateSubnetId
50   PublicEC2InstanceId:
51     Value: !GetAtt EC2Stack.Outputs.PublicEC2InstanceId
52   PrivateEC2InstanceId:
53     Value: !GetAtt EC2Stack.Outputs.PrivateEC2InstanceId

```

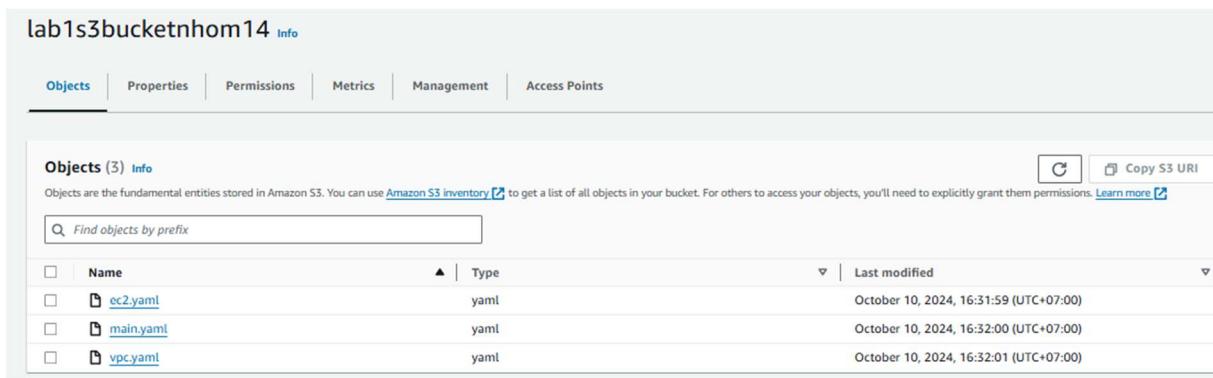
Hình 2.5: Code main.yaml

b. Triển khai và quản lý hạ tầng tự động với CloudFormation

b.1. Tạo S3 Bucket và upload các file

Tạo một S3 Bucket để lưu trữ các file yaml, sau đó upload các file vpc.yaml, ec2.yaml, và main.yaml.

⇒ Sử dụng S3 để quản lý các file CloudFormation, đảm bảo việc triển khai các tài nguyên AWS có thể truy xuất đúng các file cần thiết.



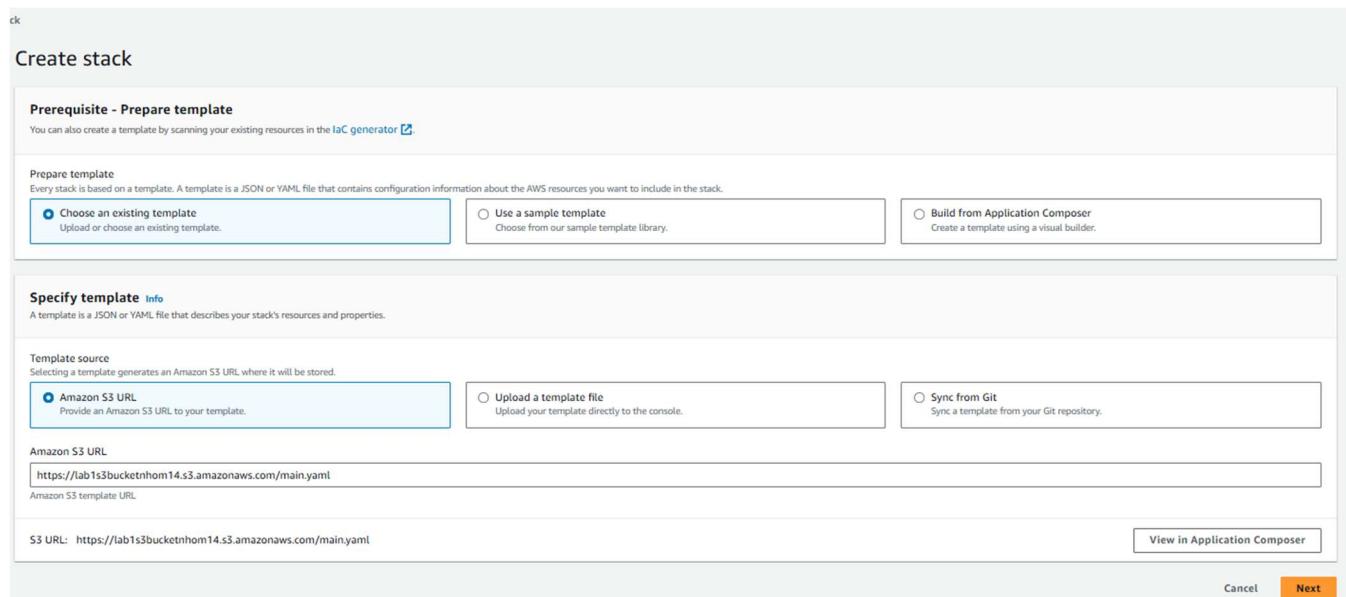
Hình 2.6: Tạo Bucket.

b.2. Tạo Stack trong CloudFormation

Tạo stack trong CloudFormation, chọn file main.yaml từ S3 để bắt đầu triển khai.

CloudFormation sẽ tự động tạo các tài nguyên từ các file nested stack như VPC, EC2 instances, và Security Groups.

⇒ Tự động triển khai hạ tầng thông qua CloudFormation, giúp tiết kiệm thời gian và đảm bảo cấu hình nhất quán.



Hình 2.7: Tạo Stack trên CloudFormation

Specify stack details

Provide a stack name

Stack name
nhom14-stack
Stack name must be 1 to 128 characters, start with a letter, and only contain alphanumeric characters. Character count: 12/128.

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

AvailabilityZone
us-east-1a

BucketName
lab1s3bucketnhom14

PrivateSubnetCIDR
192.168.2.0/24

PublicSubnetCIDR
192.168.1.0/24

VpcCIDR
192.168.0.0/16

Hình 2.8: Thông tin chi tiết của Stack lấy từ main.yaml

The screenshot shows the AWS CloudFormation console interface. On the left, there's a sidebar with a list of stacks. One stack, 'nhom14-stack', is selected and expanded, showing its nested stacks: 'nhom14-stack-EC2Stack-CWLTCFA2MJYC' and 'nhom14-stack-VPCStack-W1ETBV8CGQBW', both of which are in a 'CREATE_COMPLETE' state. On the right, the main panel is titled 'nhom14-stack' and shows the 'Events' tab. It lists 8 events from 2024-10-10 at 16:36 UTC+0700, detailing the creation of various resources like EC2Stack, VPCStack, and nested stacks, all in a 'CREATE_COMPLETE' status.

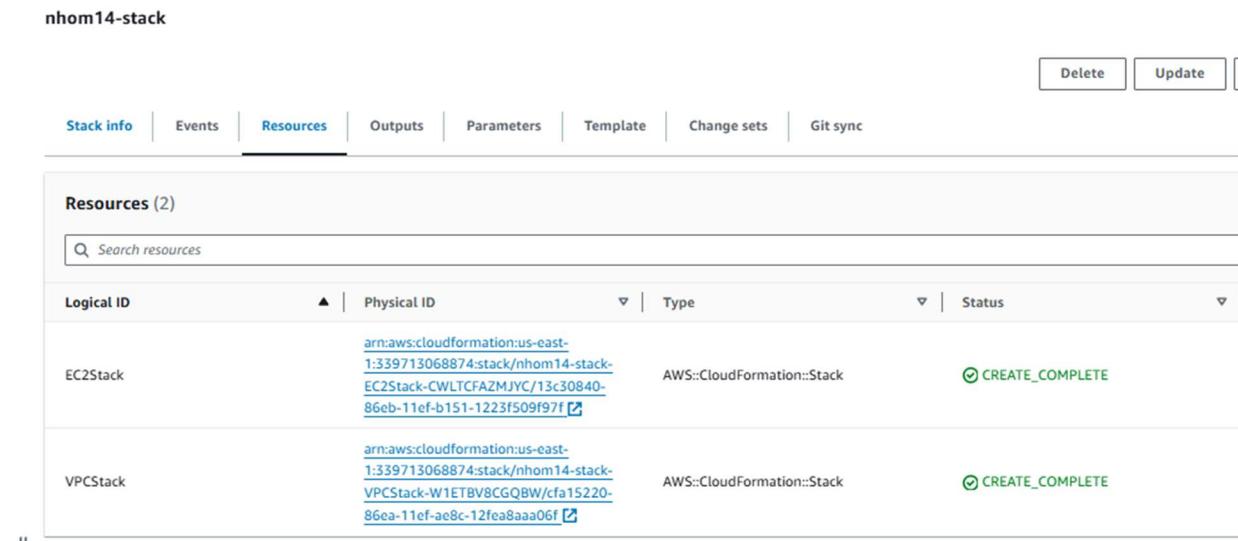
Timestamp	Logical ID	Status
2024-10-10 16:36:30 UTC+0700	nhom14-stack	CREATE_COMPLETE
2024-10-10 16:36:29 UTC+0700	EC2Stack	CREATE_COMPLETE
2024-10-10 16:36:08 UTC+0700	EC2Stack	CREATE_IN_PROGRESS
2024-10-10 16:36:07 UTC+0700	EC2Stack	CREATE_IN_PROGRESS
2024-10-10 16:36:06 UTC+0700	VPCStack	CREATE_COMPLETE
2024-10-10 16:34:13 UTC+0700	VPCStack	CREATE_IN_PROGRESS
2024-10-10 16:34:13 UTC+0700	nhom14-stack	CREATE_IN_PROGRESS
2024-10-10 16:34:10 UTC+0700		CREATE_IN_PROGRESS

Hình 2.9: Tạo stack thành công với EC2 và VPC nested

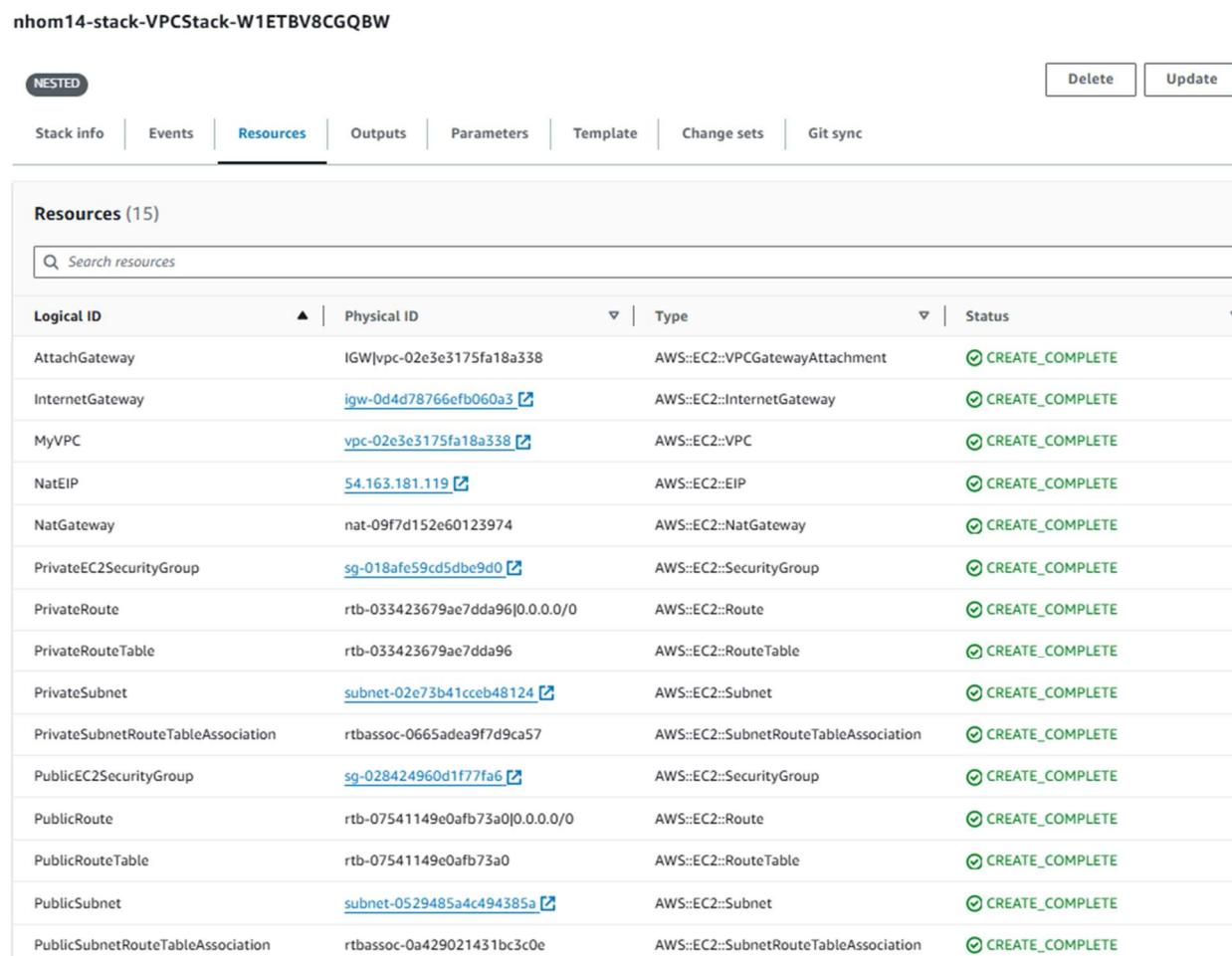
b.3. Xem chi tiết thông tin của Stack

Sau khi stack được tạo thành công, có thể xem các tài nguyên được tạo bao gồm VPC ID, Public Subnet ID, Private Subnet ID, và EC2 instance ID.

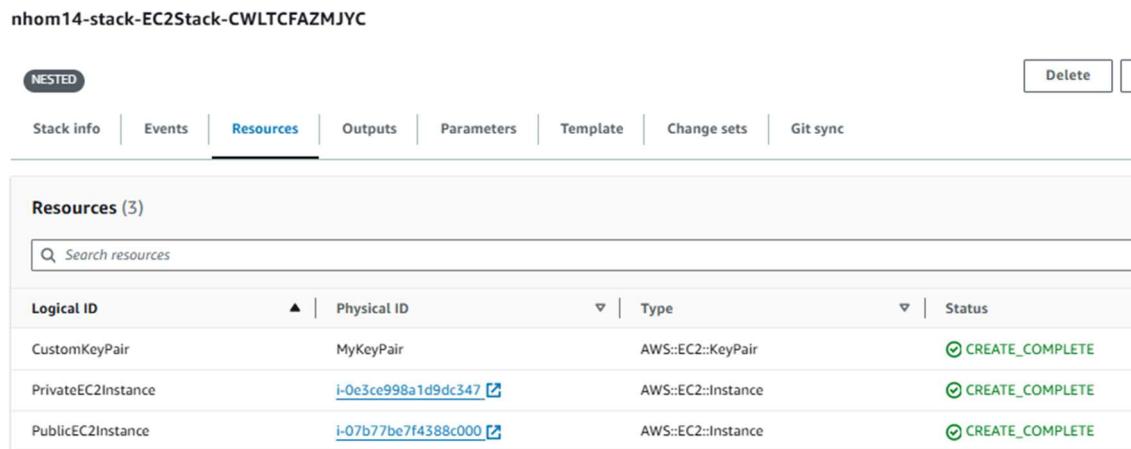
⇒ Kiểm tra rằng các tài nguyên đã được tạo thành công và đã có ID riêng để quản lý sau khi stack được triển khai hoàn tất.



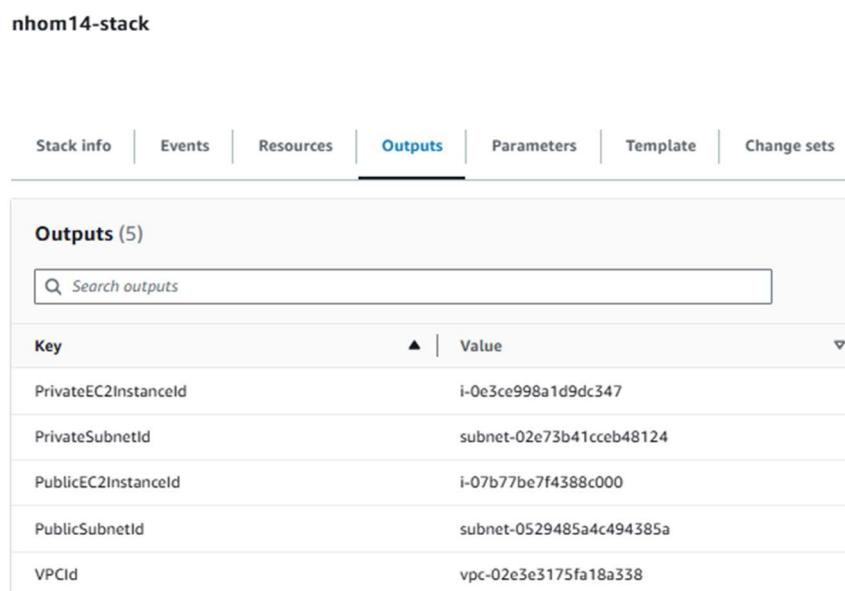
Hình 2.10: Resources chính nhom14-stack



Hình 2.11: Resource VPC được tạo từ nhom14-stack



Hình 2.12: Resource EC2 được tạo từ nhom14-stack



Hình 2.13: Output chính của nhom14-stack

Key	Value	Description
PrivateSgId	sg-018afe59cd5dbe9d0	-
PrivateSubnetId	subnet-02e73b41cceb48124	-
PublicSgId	sg-028424960d1f77fa6	-
PublicSubnetId	subnet-0529485a4c494385a	-
VPCId	vpc-02e3e3175fa18a338	-

Hình 2.14: Output của VPC được tạo từ nhom14-stack

Key	Value
PrivateEC2InstanceId	i-0e3ce998a1d9dc347
PublicEC2InstanceId	i-07b77be7f4388c000

Hình 2.15: Output của EC2 được tạo từ nhom14-stack

b.4. Kiểm tra tài nguyên được tạo từ CloudFormation

⇒ Kiểm tra tất cả các tài nguyên đã được tạo thành công và hoạt động đúng cách. Việc kiểm tra giúp đảm bảo tính toàn vẹn của hệ thống.

Kiểm tra VPC để đảm bảo đã được tạo thành công và có ID hợp lệ:

Your VPCs (2) Info									
Search									
		Name	VPC ID	State	IPv4 CIDR	IPv6 ...	DHCP option set	Main route table	Main network ACL
<input type="checkbox"/>	\$({Enviro... vpc-02e3e3175fa18a338	Available...	192.168.0.0/16	-	dopt-07446a1761f2...	rtb-040ab120b7b2ca445	acl-05a3376f412d59954		

Hình 2.16: VPC được tạo bởi CloudFormation

Kiểm tra các subnet (public và private) được tạo bên trong VPC:

Bài thực hành 01: Dùng Terraform và CloudFormation quản lý và triển khai hạ tầng AWS

subnet-0529485a4c494385a		vpc-02e3e3175fa18a338 ...	192.168.1.0/24	-	-	249	us-east-1a	use1-az2	us-east-1	rtb-07541149e0afb73a0 ...
subnet-00a6ef550bbcd0fc7		vpc-07ed10898f08dcc8d	172.31.0.0/20	-	-	4091	us-east-1d	use1-az1	us-east-1	-
subnet-02e73b41ccb48124		vpc-02e3e3175fa18a338 ...	192.168.2.0/24	-	-	250	us-east-1a	use1-az2	us-east-1	rtb-033423679ac7dd961 ...

Hình 2.17: Subnet được tạo bởi CloudFormation

Kiểm tra Internet Gateway để đảm bảo nó hoạt động và được gắn vào VPC:

Internet gateways (2) Info						
	Name	Internet gateway ID	State	VPC ID	Owner	
<input type="checkbox"/>	-	igw-0c878678f22aa49a2		vpc-07ed10898f08dcc8d	339713068874	
<input type="checkbox"/>	\$(Enviro...)	igw-0d4d78766fb060a3		vpc-02e3e3175fa18a338 ...	339713068874	

Hình 2.18: Internet Gateway được tạo bởi CloudFormation

Kiểm tra Elastic IP được tạo và gắn vào NAT Gateway:

Elastic IP addresses (1)									
	Name	Allocated IPv4 ...	Type	Allocation ID	Reverse DNS record	Associated instance ID	Private IP addr...		
<input type="checkbox"/>	custom_NatEIP	54.163.181.119	Public IP	eipalloc-066ed3bc927f4e787	-	-	192.168.1.248		
<input type="checkbox"/>	\$(Enviro...)	nat-09f7d152e601239...	Public		54.163.181.119	192.168.1.248	eni-096...	vpc-02e3e3175fa18a338 /...	subnet-0529485a4c494385a /...

Hình 2.19: Elastice IP và NAT được tạo bởi CloudFormation

Kiểm tra NAT Gateway, đảm bảo rằng các tài nguyên trong subnet riêng tư có thể truy cập Internet thông qua NAT Gateway:

Security Groups (5) Info									
	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count	
<input type="checkbox"/>	-	sg-0cbbc5d94e1b942fa	default	vpc-07ed10898f08dcc8d	default VPC security group	339713068874	1 Permission entry	1 Permission entry	
<input type="checkbox"/>	\$(Envir...)	sg-028424960d1177fa6	rnhom14-stack-VPCStack...	vpc-02e3e3175fa18a338	Allow SSH access from specifi...	339713068874	1 Permission entry	1 Permission entry	
<input type="checkbox"/>	-	sg-0baaa3882f81789cc5	default	vpc-01ee68157a742c9a2	default VPC security group	339713068874	1 Permission entry	1 Permission entry	
<input type="checkbox"/>	\$(Envir...)	sg-018afe59cd5dbe9d0	rnhom14-stack-VPCStack...	vpc-02e3e3175fa18a338	Allow SSH access from Public ...	339713068874	1 Permission entry	1 Permission entry	
<input type="checkbox"/>	-	sg-0496e7d7b4a46b7da	default	vpc-02e3e3175fa18a338	default VPC security group	339713068874	1 Permission entry	1 Permission entry	

Hình 2.20: Security Group được tạo bởi CloudFormation

Kiểm tra Route Table để đảm bảo các lưu lượng mạng được định tuyến đúng thông qua Internet Gateway và NAT Gateway:

Route tables (4) Info								
	Name	Route table ID	Explicit subnet associations	Edge... Type	Main	VPC	Owner ID	
<input type="checkbox"/>	\${Enviro...}	rtb-07541149e0afb73a0	subnet-0529485a4c494385a / ...	-	No	vpc-02e3e3175fa18a338 ...	339713068874	
<input type="checkbox"/>	-	rtb-040ab120b7b2ca445	-	-	Yes	vpc-02e3e3175fa18a338 ...	339713068874	
<input type="checkbox"/>	\${Enviro...}	rtb-033423679ae7dda96	subnet-02e73b41cce8124 / ...	-	No	vpc-02e3e3175fa18a338 ...	339713068874	
<input type="checkbox"/>	-	rtb-0de339d28f100459e	-	-	Yes	vpc-07ed10898f08dcc8d	339713068874	

Hình 2.21: Route Table được tạo bởi CloudFormation

b.5. Kiểm tra kết nối SSH tới EC2

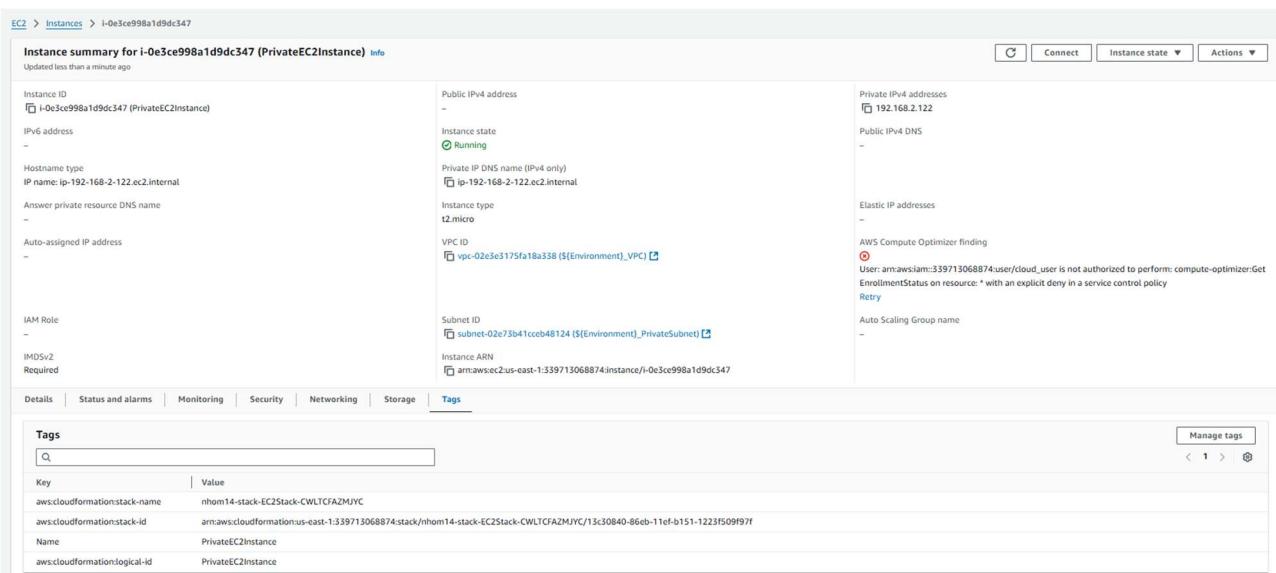
⇒ Kiểm tra kết nối giữa các EC2 instances, đảm bảo các EC2 được triển khai đúng với cấu hình bảo mật. Public EC2 có thể truy cập từ bên ngoài và Private EC2 chỉ có thể truy cập qua mạng nội bộ từ Public EC2, đảm bảo tính bảo mật của hệ thống.

Instances (2) Info														
	Name	Instance ID	Instance state	Instanc...	Status check	Alarm status	Availability...	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitor...	Security group name	Key name
<input type="checkbox"/>	PublicEC2Instance	i-07b77be7f4388c000	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-52-90-238-1...	52.90.238.165	-	-	disabled	rhom14-stack-VPCStack-...	MyKeyPair
<input type="checkbox"/>	PrivateEC2Instance	i-0e3ce998a1d9dc347	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-	-	-	-	disabled	rhom14-stack-VPCStack-...	MyKeyPair

Hình 2.22: Public EC2 và Private EC2 được tạo bởi CloudFormtaion

EC2 > Instances > i-07b77be7f4388c000 (PublicEC2Instance) Info													
Instance summary for i-07b77be7f4388c000 (PublicEC2Instance) Info													
Updated less than a minute ago													
Instance ID i-07b77be7f4388c000 (PublicEC2Instance)													
Public IPv4 address 52.90.238.165 [open address]													
IPv6 address -													
Hostname type IP name: ip-192-168-1-239.ec2.internal													
Answer private resource DNS name -													
Auto-assigned IP address 52.90.238.165 [Public IP]													
IAM Role -													
IMDSv2 Required													
Details Status and alarms Monitoring Security Networking Storage Tags													
Tags													
Manage tags													
Key Value													
Name PublicEC2Instance													
aws:cloudformation:logical-id PublicEC2Instance													
aws:cloudformation:stack-name rhom14-stack-EC2Stack-CWLTCFAZMJYC													
aws:cloudformation:stack-id arn:aws:cloudformation:us-east-1:339713068874:stack/rhom14-stack-EC2Stack-CWLTCFAZMJYC/13c30840-86eb-11ef-b151-1223f509f9f7													

Hình 2.23: Public EC2 với Tags được tạo bởi CloudFormation



Hình 2.24: Private EC2 với Tags được tạo bởi CloudFormation

c. Tiến hành SSH và kiểm tra kết quả

Sử dụng lệnh SSH để kết nối đến máy chủ Ubuntu (với địa chỉ IP là 52.90.238.165). Khóa riêng tư id_rsa được sử dụng để xác thực kết nối.

Máy chủ xác thực và chấp nhận kết nối, hiển thị thông tin: Ubuntu Server 20.04.1 LTS, thông tin bộ nhớ, IP (192.168.1.239), số tiến trình đang chạy, và tài nguyên hệ thống.

Thực hiện ping google.com để kiểm tra kết nối ra ngoài internet và thành công.

```
Bao_Duy@DESKTOP-QE2KJE6 MINGW64 /d/lab-nt548/lab/DevOps-Technology-Application/Lab01/C1
$ ssh -i ~/.ssh/id_rsa ubuntu@52.90.238.165
The authenticity of host '52.90.238.165 (52.90.238.165)' can't be established.
ED25519 key fingerprint is SHA256:ZjrUoqsy5lHAFxZyTsh2+Kv+43LG02b0qJM56PctQ1c.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '52.90.238.165' (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 Thu Oct 10 09:47:54 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: 192.168.1.239
  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-192-168-1-239:~$ ping google.com
PING google.com (142.251.16.138) 56(84) bytes of data.
64 bytes from bl-in-f138.1e100.net (142.251.16.138): icmp_seq=1 ttl=105 time=2.74 ms
64 bytes from bl-in-f138.1e100.net (142.251.16.138): icmp_seq=2 ttl=105 time=2.03 ms
64 bytes from bl-in-f138.1e100.net (142.251.16.138): icmp_seq=3 ttl=105 time=1.97 ms
64 bytes from bl-in-f138.1e100.net (142.251.16.138): icmp_seq=4 ttl=105 time=1.94 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.937/2.172/2.744/0.332 ms
ubuntu@ip-192-168-1-239:~$
```

Hình 2.25: SSH tới public EC2

Chuyển đến thư mục SSH, sau đó tạo file khóa riêng tư (id_rsa) và gán quyền chỉ đọc cho người sở hữu bằng “touch id_rsa” và “chmod 600 id_rsa”

Sử dụng private key id_rsa để kết nối đến server với địa chỉ IP là 192.168.2.122

Sau khi server cho phép kết nối thì hiển thị các thông tin về tài nguyên hệ thống.

```
ubuntu@ip-192-168-1-239:~$ cd ~/.ssh/
ubuntu@ip-192-168-1-239:~/ssh$ touch id_rsa
ubuntu@ip-192-168-1-239:~/ssh$ chmod 600 id_rsa
ubuntu@ip-192-168-1-239:~/ssh$ ssh -i ~/ssh/id_rsa ubuntu@192.168.2.122
The authenticity of host '192.168.2.122 (192.168.2.122)' can't be established.
ED25519 key fingerprint is SHA256:8gvbfIrc5WhSpMkk4Uw+I3glnb/+uLP4PpypsIBZQA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.122' (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 Thu Oct 10 09:50:45 UTC 2024

System load: 0.0          Processes:      104
Usage of /: 22.9% of 6.71GB Users logged in: 0
Memory usage: 20%          IPv4 address for enx0: 192.168.2.122
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-192-168-2-122:~$
```

Hình 2.26: SSH tới private EC2