



## BÁO CÁO THỰC HÀNH

**Bài thực hành số 02: Quản lý và triển khai hạ tầng AWS và ứng dụng microservices với Terraform, CloudFormation, GitHub Actions, AWS CodePipeline và Jenkins**

Môn học: NT548

Lớp: NT548.P11.MMCL

### THÀNH VIÊN THỰC HIỆN (Nhóm 21):

STT	Họ và tên	MSSV
1	Lê Triệu Vĩ	21522785
2	Lý Thế Nguyên	21552389
3		

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

Source code câu 1: <https://github.com/just-vile/NT548-Lab2.git>

Source code câu 2: <https://github.com/just-vile/NT548-Lab2-Cloudformation.git>

Source code câu 3: <https://github.com/just-vile/Multi-Tier-MicroService-Application-Deployment.git>, branch: latest

## 1. Câu 1

a. Mục 1

Sử dụng Checkov để scan từng module ở local:

The screenshot shows a developer's workspace with the following details:

- EXPLORER**: Shows the project structure under **UNTITLED (WORKSPACE)**, including **1st 2024-2025**, **.venv**, **Capstone**, **Data Analysis**, **DevOps** (selected), **Books**, **Lab2**, **Labs**, **NT548-Lab-2**, **.github**, **.terraform**, **modules**, and **ec2** (selected). The **main.tf** file is open in the editor.
- OUTLINE**: Shows the structure of the **main.tf** file, including resources for **aws\_instance** (public and private instances) and **aws\_vpc**.
- TIMELINE**: Shows the history of changes made to the files.
- TERMINAL**: Displays the command output of `checkov . -d modules/ec2`, showing the scan results for the `variables.tf` and `variables.tftf` files.
- Prisma Cloud**: Shows the status "By Prisma Cloud | version: 3.2.281" and an update available message.

**Code Editor Content (main.tf):**

```
1st 2024-2025 > DevOps > NT548-Lab-2 > modules > ec2 > main.tf ...  
1 resource "aws_instance" "public_instance" {  
2   # checkov:skip=CKV_AWS_135  
3   # checkov:skip=CKV_AWS_79  
4   # checkov:skip=CKV_AWS_8  
5   # checkov:skip=CKV_AWS_126  
6   # checkov:skip=CKV2_AWS_41  
7   ami           = var.public_instance_ami  
8   instance_type = var.instance_type  
9   subnet_id     = var.public_subnet_id  
10  security_groups = [var.public_security_group_id]  
11  key_name      = var.ssh_key_name  
12  
13  tags = {  
14    Name = "Public EC2 Instance"  
15  }  
16 }  
17  
18 resource "aws_instance" "private_instance" {  
19   # checkov:skip=CKV_AWS_135  
20   # checkov:skip=CKV_AWS_79  
21   # checkov:skip=CKV_AWS_8  
22   # checkov:skip=CKV_AWS_126  
23   # checkov:skip=CKV2_AWS_41  
24   ami           = var.private_instance_ami  
25   instance_type = var.instance_type  
26   subnet_id     = var.private_subnet_id  
27   security_groups = [var.private_security_group_id]  
28   key_name      = var.ssh_key_name  
29  
30   tags = {  
31     Name = "Private EC2 Instance"  
32   }  
33 }
```

**Terminal Output (checkov scan results):**

```
D:\Learning Space\1st 2024-2025\DevOps\NT548-Lab-2>c:/users/asus/appdata\roaming\python\python312\scripts\checkov.cmd -d modules\ec2  
2024-11-09 17:02:51,767 [ThreadPoolEx] [WARNI] [ArmLocalGraph] created 0 vertices  
2024-11-09 17:02:51,767 [ThreadPoolEx] [WARNI] [ArmLocalGraph] created 0 edges  
[ terraform framework ]: 100% | [3/3], Current File Scanned=modules\ec2\variables.tf  
[ secrets framework ]: 100% | [3/3], Current File Scanned=modules\ec2\variables.tftf
```

**Prisma Cloud Status:**

```
By Prisma Cloud | version: 3.2.281  
Update available      -> 3.2.283  
Run pip3 install -U checkov to update
```

**terraformer scan results:**

Passed checks: 4, Failed checks: 0, Skipped checks: 10

Ở module EC2, Checkov detect một vài lỗi, tuy nhiên, phần lớn đều không liên quan đến yêu cầu ở Lab 1, nên em đã comment lại trong code để Checkov skip qua.

# Bài thực hành số 02: Quản lý và triển khai hạ tầng AWS và ứng dụng microservices với Terraform, CloudFormation, GitHub Actions, AWS CodePipeline và Jenkins



Các lỗi mà nhóm đã skip:

```
Check: CKV_AWS_126: "Ensure that detailed monitoring is enabled for EC2 instances"
    SKIPPED for resource: aws_instance_public_instance
    Suppress comment: No comment provided
    File: \main.tf:1-16
    Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-logging-policies/ensure-that-detailed-monitoring-is-enabled-for-ec2-instances
Check: CKV_AWS_135: "Ensure that EC2 is EBS optimized"
    SKIPPED for resource: aws_instance_public_instance
    Suppress comment: No comment provided
    File: \main.tf:1-16
    Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-general-policies/ensure-that-ec2-is-ebs-optimized
Check: CKV_AWS_79: "Ensure Instance Metadata Service Version 1 is not enabled"
    SKIPPED for resource: aws_instance_public_instance
    Suppress comment: No comment provided
    File: \main.tf:1-16
    Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-general-policies/bc-aws-general-31
Check: CKV_AWS_8: "Ensure all data stored in the Launch configuration or instance Elastic Blocks Store is securely encrypted"
    SKIPPED for resource: aws_instance_public_instance
    Suppress comment: No comment provided
    File: \main.tf:1-16
    Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-general-policies/general-13
Check: CKV_AWS_126: "Ensure that detailed monitoring is enabled for EC2 instances"
    SKIPPED for resource: aws_instance_private_instance
    Suppress comment: No comment provided
    File: \main.tf:18-33
    Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-logging-policies/ensure-that-detailed-monitoring-is-enabled-for-ec2-instances
Check: CKV_AWS_135: "Ensure that EC2 is EBS optimized"
    SKIPPED for resource: aws_instance_private_instance
    Suppress comment: No comment provided
    File: \main.tf:18-33
    Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-general-policies/ensure-that-ec2-is-ebs-optimized
Check: CRV_AWS_79: "Ensure Instance Metadata Service Version 1 is not enabled"
    SKIPPED for resource: aws_instance_private_instance
    Suppress comment: No comment provided
    File: \main.tf:18-33
    Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-general-policies/bc-aws-general-31
Check: CKV_AWS_8: "Ensure all data stored in the Launch configuration or instance Elastic Blocks Store is securely encrypted"
    SKIPPED for resource: aws_instance_private_instance
    Suppress comment: No comment provided
    File: \main.tf:18-33
    Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-general-policies/general-13
Check: CKV2_AWS_41: "Ensure an IAM role is attached to EC2 instance"
    SKIPPED for resource: aws_instance_public_instance
```

Tương tự với các module khác ...

## Module nat\_gateway

```
D:\Learning Space\1st 2024-2025\DevOps\NT548-Lab-2>c:\users\asus\appdata\roaming\python\python312\scripts\checkov.cmd -d modules\nat_gateway
2024-11-09 17:03:57,940 [ThreadPoolEx] [WARNI] [ArmLocalGraph] created 0 vertices
2024-11-09 17:03:57,942 [ThreadPoolEx] [WARNI] [ArmLocalGraph] created 0 edges
[ terraform framework ]: 100%          [[3/3], Current File Scanned=modules\nat_gateway\variables.tf
[ secrets framework ]: 100%          [[3/3], Current File Scanned=modules\nat_gateway\variables.tf
[ secrets framework ]: 67%           [[2/3], Current File Scanned=modules\nat_gateway\variables.tf

[{"id": "CKV2_AWS_19", "check": "CKV2_AWS_19: \"Ensure that all EIP addresses allocated to a VPC are attached to EC2 instances\"", "status": "PASSED", "resource": "aws_eip.nat_eip", "file": "\main.tf:1-3", "guide": "https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/ensure-that-all-eip-addresses-allocated-to-a-vpc-are-attached-to-ec2-instances"}, {"id": "CKV2_AWS_41", "check": "CKV2_AWS_41: \"Ensure an IAM role is attached to EC2 instance\"", "status": "SKIPPED", "resource": "aws_instance_public_instance", "file": "\main.tf:1-16", "guide": "https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-general-policies/general-13"}]

By Prisma Cloud | version: 3.2.281
Update available      -> 3.2.283
Run pip3 install -U checkov to update

terraform scan results:
Passed checks: 1, Failed checks: 0, Skipped checks: 0

Check: CKV2_AWS_19: "Ensure that all EIP addresses allocated to a VPC are attached to EC2 instances"
    PASSED for resource: aws_eip.nat_eip
    File: \main.tf:1-3
    Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/ensure-that-all-eip-addresses-allocated-to-a-vpc-are-attached-to-ec2-instances
```

## Module route\_table

```
D:\Learning Space\1st 2024-2025\DevOps\NT548-Lab-2>c:\users\asus\appdata\roaming\python\python312\scripts\checkov.cmd -d modules\route_table
2024-11-09 17:07:23,911 [ThreadPoolEx] [WARNI] [ArmLocalGraph] created 0 vertices
2024-11-09 17:07:23,911 [ThreadPoolEx] [WARNI] [ArmLocalGraph] created 0 edges
[ terraform framework ]: 100%          [[3/3], Current File Scanned=modules\route_table\variables.tf
[ secrets framework ]: 100%          [[3/3], Current File Scanned=modules\route_table\variables.tf
[ secrets framework ]: 67%           [[2/3], Current File Scanned=modules\route_table\variables.tf

[{"id": "CKV2_AWS_19", "check": "CKV2_AWS_19: \"Ensure that all EIP addresses allocated to a VPC are attached to EC2 instances\"", "status": "PASSED", "resource": "aws_eip.nat_eip", "file": "\main.tf:1-3", "guide": "https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/ensure-that-all-eip-addresses-allocated-to-a-vpc-are-attached-to-ec2-instances"}, {"id": "CKV2_AWS_41", "check": "CKV2_AWS_41: \"Ensure an IAM role is attached to EC2 instance\"", "status": "SKIPPED", "resource": "aws_instance_public_instance", "file": "\main.tf:1-16", "guide": "https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-general-policies/general-13"}]

By Prisma Cloud | version: 3.2.281
Update available      -> 3.2.283
Run pip3 install -U checkov to update

terraform scan results:
Passed checks: 4, Failed checks: 0, Skipped checks: 0
```



## Module security\_group

```
D:\Learning Space\1st 2024-2025\DevOps\NT548-Lab-2>c:\users\asus\appdata\roaming\python\python312\scripts\checkov.cmd -d modules\security_group
2024-11-09 17:14:55,094 [ThreadPoolEx] [WARNI] [ArmLocalGraph] created 0 vertices
2024-11-09 17:14:55,094 [ThreadPoolEx] [WARNI] [ArmLocalGraph] created 0 edges
[ terraform framework ]: 100%|[██████████|[[3/3], Current File Scanned=modules\security_group\variables.tf
[ secrets framework ]: 100%|[██████████|[[3/3], Current File Scanned=modules\security_group\variables.tftf

By Prisma Cloud | version: 3.2.281
Update available      -> 3.2.283
Run pip3 install -U checkov to update

terraform scan results:

Passed checks: 13, Failed checks: 0, Skipped checks: 5

Check: CKV_AWS_23: "Ensure every security group and rule has a description"
    PASSED for resource: aws_security_group.public_sg
    File: \main.tf:1-23
    Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/networking-31


```

## Các lỗi đã skip ở module Security Group

```
Check: CKV_AWS_24: "Ensure no security groups allow ingress from 0.0.0.0:0 to port 22"
    SKIPPED for resource: aws_security_group.private_sg
    Suppress comment: No comment provided
    File: \main.tf:1-23
    Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/networking-1-port-security

Check: CKV_AWS_24: "Ensure no security groups allow ingress from 0.0.0.0:0 to port 22"
    SKIPPED for resource: aws_security_group.private_sg
    Suppress comment: No comment provided
    File: \main.tf:25-47
    Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/networking-1-port-security

Check: CKV2_AWS_5: "Ensure that Security Groups are attached to another resource"
    SKIPPED for resource: aws_security_group.public_sg
    Suppress comment: No comment provided
    File: \main.tf:1-23
    Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/ensure-that-security-groups-are-attac
    hed-to-ec2-instances-or-elastic-network-interfaces-enis

Check: CKV2_AWS_5: "Ensure that Security Groups are attached to another resource"
    SKIPPED for resource: aws_security_group.private_sg
    Suppress comment: No comment provided
    File: \main.tf:25-47
    Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/ensure-that-security-groups-are-attac
    hed-to-ec2-instances-or-elastic-network-interfaces-enis

Check: CKV2_AWS_5: "Ensure that Security Groups are attached to another resource"
    SKIPPED for resource: aws_security_group.default_sg
    Suppress comment: No comment provided
    File: \main.tf:49-56
    Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/ensure-that-security-groups-are-attac
    hed-to-ec2-instances-or-elastic-network-interfaces-enis

PS D:\Learning Space\1st 2024-2025\DevOps\NT548-Lab-2\modules> |
```

## Module subnet:

```
D:\Learning Space\1st 2024-2025\DevOps\NT548-Lab-2>c:\users\asus\appdata\roaming\python\python312\scripts\checkov.cmd -d modules\subnet
2024-11-09 17:17:37,349 [ThreadPoolEx] [WARNI] [ArmLocalGraph] created 0 vertices
2024-11-09 17:17:37,349 [ThreadPoolEx] [WARNI] [ArmLocalGraph] created 0 edges
[ terraform framework ]: 100%|[██████████|[[3/3], Current File Scanned=modules\subnet\variables.tf
[ secrets framework ]: 100%|[██████████|[[3/3], Current File Scanned=modules\subnet\variables.tftf
[ secrets framework ]: 67%|[██████████|[[2/3], Current File Scanned=modules\subnet\variables.tftf

By Prisma Cloud | version: 3.2.281
Update available      -> 3.2.283
Run pip3 install -U checkov to update

terraform scan results:

Passed checks: 1, Failed checks: 0, Skipped checks: 1

Check: CKV_AWS_130: "Ensure VPC subnets do not assign public IP by default"
    PASSED for resource: aws_subnet.private_subnet
    File: \main.tf:12-19
    Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/ensure-vpc-subnets-do-not-assign-publ
    ic-ip-by-default

Check: CKV_AWS_130: "Ensure VPC subnets do not assign public IP by default"
    SKIPPED for resource: aws_subnet.public_subnet
    Suppress comment: No comment provided
    File: \main.tf:1-10
    Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/ensure-vpc-subnets-do-not-assign-publ
    ic-ip-by-default
```

Tạo thư mục .github/workflow. Sau đó tạo file deploy.yaml để tự động hóa quá trình triển khai terraform với github actions.

```

1  name: 'Terraform Infrastrucuture Deployment with Checkov Scan'
2
3  on:
4    push:
5      branches:
6        - main
7    pull_request:
8      branches:
9        - main
10
11 env:
12   AWS_ACCESS_KEY_ID: ${{ secrets.aws_access_key }}
13   AWS_SECRET_ACCESS_KEY: ${{ secrets.aws_secret_key }}
14   AWS_REGION: us-east-1
15   TF_VAR_region: us-east-1

```



Triển khai trên branch main, cập nhật AWS key trong section secret trên Github.

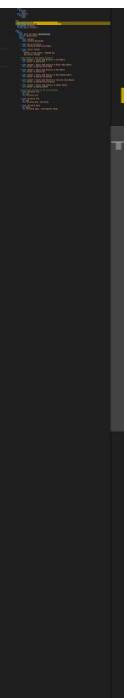
Name	Last updated
AWS_ACCESS_KEY	1 hour ago
AWS_SECRET_KEY	1 hour ago

File deploy.yaml sẽ setup Terraform, tải Checkov và thực hiện scan trên từng modules.

```

17 jobs:
18   build:
19     name: Build and Deploy Infrastructure
20     runs-on: ubuntu-latest
21     steps:
22       - name: Checkout
23         uses: actions/checkout@v2
24
25       - name: Set up Terraform
26         uses: hashicorp/setup-terraform@v1
27
28       - name: Install Checkov
29         run:
30           - python3 -m pip install --upgrade pip
31           - pip install checkov
32
33       # Run Checkov on each module directory
34       - name: Checkov - Static Code Analysis on EC2 Module
35         run: checkov -d modules/ec2
36
37       - name: Checkov - Static Code Analysis on Route Table Module
38         run: checkov -d modules/route_table
39
40       - name: Checkov - Static Code Analysis on VPC Module
41         run: checkov -d modules/vpc
42
43       - name: Checkov - Static Code Analysis on NAT Gateway Module
44         run: checkov -d modules/nat_gateway
45
46       - name: Checkov - Static Code Analysis on Security Group Module
47         run: checkov -d modules/security_group
48
49       - name: Checkov - Static Code Analysis on Subnet Module
50         run: checkov -d modules/subnet

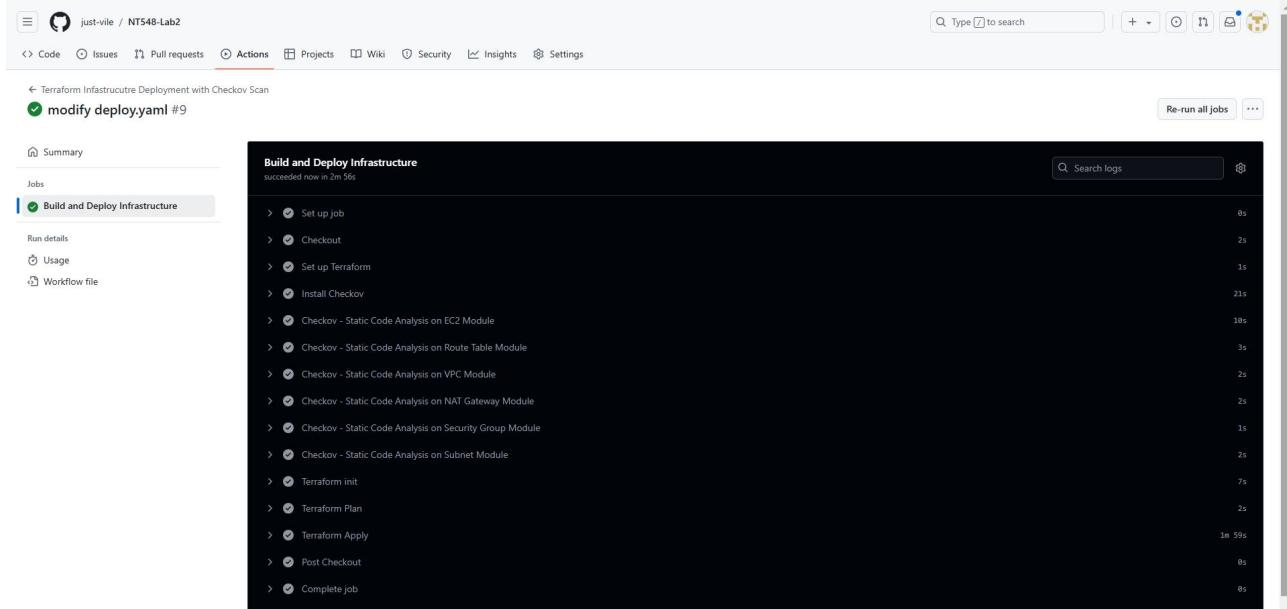
```



Sau đó sẽ khởi tạo và tự động deploy lên AWS.

```
52 # Initialize Terraform in the root directory
53 - name: Terraform init
54   id: init
55   run: terraform init
56
57 - name: Terraform Plan
58   id: plan
59   run: terraform plan -out=tfplan
60
61 - name: Terraform Apply
62   id: apply
63   run: terraform apply --auto-approve tfplan
64
```

Kết quả:



Instances (5) <a href="#">Info</a>		Last updated	<a href="#">Connect</a>	Instance state	Actions	<a href="#">Launch instances</a>	<a href="#">Edit</a>
<a href="#">Find Instance by attribute or tag (case-sensitive)</a>							
	Name		Instance ID	Instance state	Instance type	Status check	Alarm status
<input type="checkbox"/>	i-0d69b3ccd228e43e7	<a href="#">Running</a>	t2.medium	<a href="#">2/2 checks passed</a>	<a href="#">View alarms</a>	<a href="#">+</a>	us-east-1
<input type="checkbox"/>	single-instance	<a href="#">Running</a>	t2.medium	<a href="#">2/2 checks passed</a>	<a href="#">View alarms</a>	<a href="#">+</a>	us-east-1
<input type="checkbox"/>	Public EC2 Instance	<a href="#">Running</a>	t2.micro	<a href="#">2/2 checks passed</a>	<a href="#">View alarms</a>	<a href="#">+</a>	us-east-1
<input type="checkbox"/>	Private EC2 Instance	<a href="#">Running</a>	t2.micro	<a href="#">2/2 checks passed</a>	<a href="#">View alarms</a>	<a href="#">+</a>	us-east-1
<input type="checkbox"/>	i-0b733dee307b06c78	<a href="#">Running</a>	t2.medium	<a href="#">2/2 checks passed</a>	<a href="#">View alarms</a>	<a href="#">+</a>	us-east-1

Các cấu hình vẫn y như Lab 1.

## 2. Câu 2

### a. Mục 1



Trước tiên, ta tạo một role để tránh xảy ra xung đột khi Pipeline chạy:

<a href="#">Cloud Control API</a>	Full access	All resources	None
<a href="#">CloudFormation</a>	Full access	All resources	None
<a href="#">CloudWatch Logs</a>	Limited: Write	Multiple	None
<a href="#">CodeBuild</a>	Full access	All resources	None
<a href="#">CodeDeploy</a>	Full access	All resources	None
<a href="#">CodePipeline</a>	Full access	All resources	None
<a href="#">EC2</a>	Full access	All resources	None
<a href="#">IAM</a>	Full access	All resources	None
<a href="#">S3</a>	Full access	All resources	None

Đặt tên là ‘Group21-CodeBuild-Role’

Vào IAM, sau đó tạo một Git Credential để truy cập CodeCommit.

### Generate credentials

Your new credentials are available.

**Save your user name and password or download the credentials file.**

This is the only time you can view the password or download it. You cannot recover it later. However, you can reset your password at any time.

You can use these credentials when connecting from your local computer, or from tools that require a static user name and password. [Learn more](#)

User name  
 user\_cli-at-590184125844

Password  
 \*\*\*\*\* [Show](#)

[Download credentials](#) [Close](#)

Khi clone Repo trên CodeCommit về, sẽ bắt ta đăng nhập bằng Git Credentials trên.



## Git Credential Manager



### Git Credential Manager

Enter your credentials for 'https://git-codecommit.us-east-1.amazonaws.com/v1/repos/Group21-Lab2'

Continue

```
PS D:\Learning Space\1st 2024-2025\DevOps\NT548-LAB2> git clone https://git-codecommit.us-east-1.amazonaws.com/v1/repos/Group21-Lab2
Cloning into 'Group21-Lab2'...
warning: You appear to have cloned an empty repository.
PS D:\Learning Space\1st 2024-2025\DevOps\NT548-LAB2> |
```

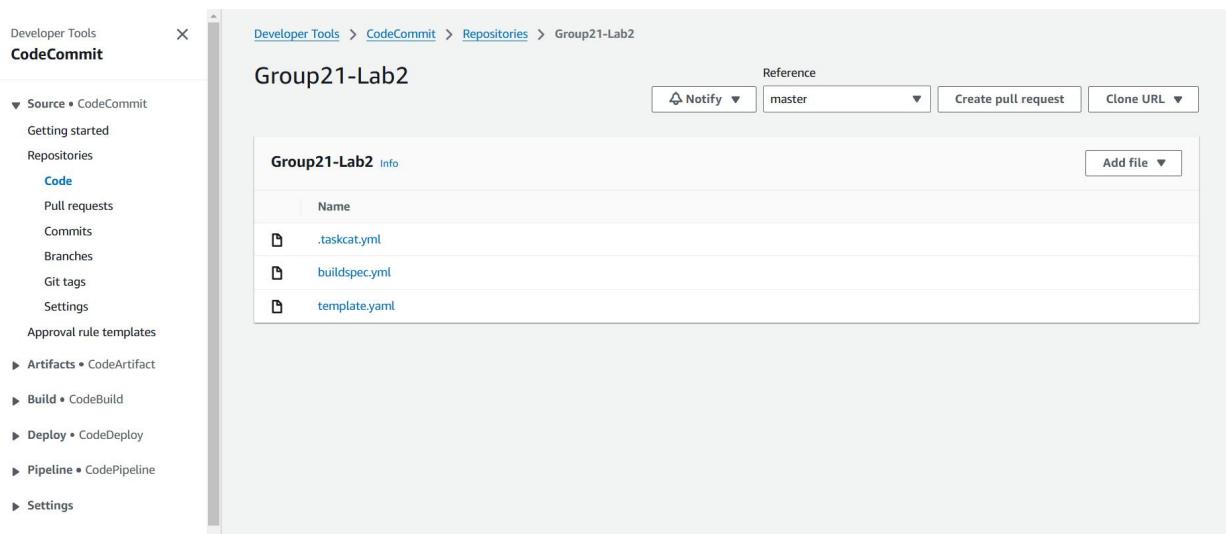
Push code từ Local lên CodeCommit.

```
PS D:\Learning Space\1st 2024-2025\DevOps\NT548-LAB2\Group21-Lab2> git add .
PS D:\Learning Space\1st 2024-2025\DevOps\NT548-LAB2\Group21-Lab2> git commit -m 'first commit'
[master (root-commit) 7c052df] first commit
 3 files changed, 229 insertions(+)
  create mode 100644 .taskcat.yml
  create mode 100644 buildspec.yml
  create mode 100644 template.yaml
PS D:\Learning Space\1st 2024-2025\DevOps\NT548-LAB2\Group21-Lab2> git push
Enumerating objects: 5, done.
Counting objects: 100% (5/5), done.
Delta compression using up to 16 threads
Compressing objects: 100% (5/5), done.
Writing objects: 100% (5/5), 1.57 KiB | 1.57 MiB/s, done.
Total 5 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
remote: Validating objects: 100%
To https://git-codecommit.us-east-1.amazonaws.com/v1/repos/Group21-Lab2
 * [new branch]      master -> master
PS D:\Learning Space\1st 2024-2025\DevOps\NT548-LAB2\Group21-Lab2> |
```

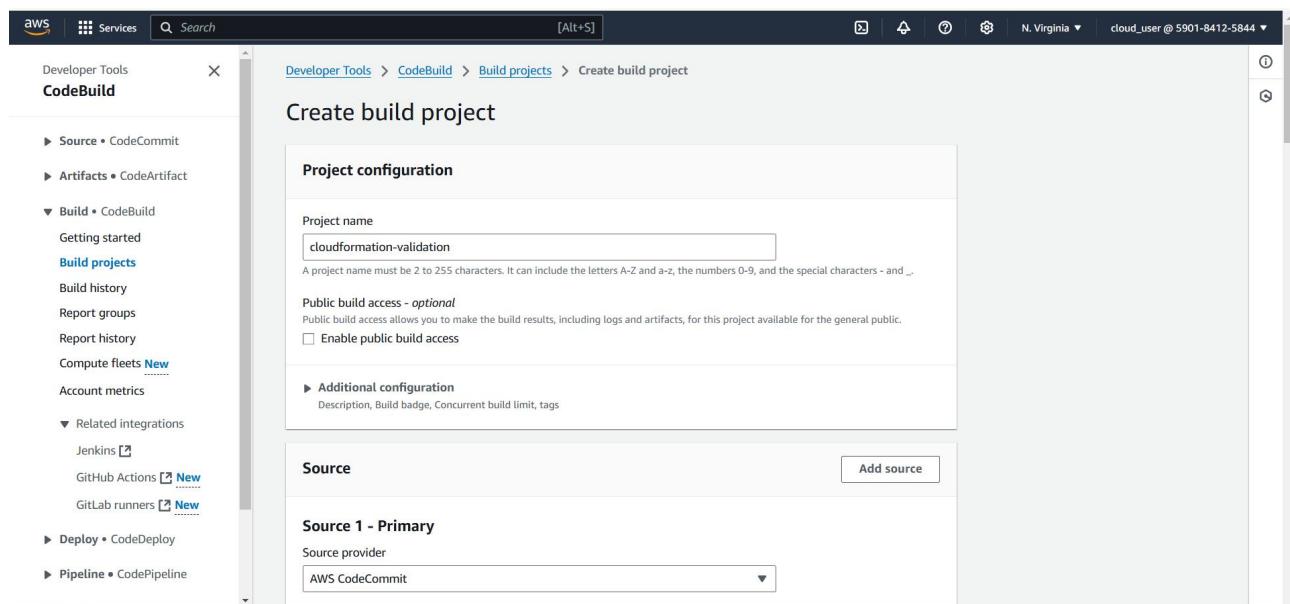
# Bài thực hành số 02: Quản lý và triển khai hạ tầng AWS và ứng dụng microservices với Terraform, CloudFormation, GitHub Actions, AWS CodePipeline và Jenkins

6

Đã push thành công lên CodeCommit.



Kế tiếp, ta sẽ tạo một Build Project bằng CodeBuild, tên project là 'cloudformation-validation', source là từ CodeCommit khi nãy.



**Source 1 - Primary**

Source provider

AWS CodeCommit

Repository

Group21-Lab2

Reference type

Choose the source version reference type that contains your source code.

Branch

Git tag

Commit ID

Branch

Choose a branch that contains the code to build.

master

Commit ID - optional

Choose a commit ID. This can shorten the duration of your build.

Source version [Info](#)

refs/heads/master

7c052dfe first commit

► Additional configuration

Git clone depth, Git submodules

File build là ‘buildspec.yml’: thực hiện tải về cfn-lint và taskcat, sau đó scan file template để kiểm tra tính đúng đắn của nó, cuối cùng nó sẽ output ra file template.yaml:

```
1st 2024-2025 / DevOps / NT548-Lab2-CloudFormation / buildspec.yml
1 version: 0.2
2
3 phases:
4   install:
5     runtime-versions:
6       python: 3.8
7     commands:
8       - pip install cfn-lint
9       - pip install taskcat
10  pre_build:
11    commands:
12      - echo "Linting CloudFormation template"
13      - cfn-lint template.yaml
14  build:
15    commands:
16      - echo "Testing CloudFormation template with Taskcat"
17      - taskcat test run
18
19 artifacts:
20   files:
21     - template.yaml
```

Chọn ‘Use a buildspec file’, và nhập đường dẫn là file ‘buildspec.yml’

**Buildspec**

**Build specifications**

Insert build commands  
Store build commands as build project configuration

Use a buildspec file  
Store build commands in a YAML-formatted buildspec file

**Buildspec name - optional**  
By default, CodeBuild looks for a file named buildspec.yml in the source code root directory. If your buildspec file uses a different name or location, enter its path from the source root here (for example, buildspec-two.yml or configuration/buildspec.yml).

buildspec.yml

## Khởi tạo Build Project thành công.

**Project created**  
You have successfully created the following project: cloudformation-validation

Developer Tools > CodeBuild > Build projects > cloudformation-validation

**cloudformation-validation**

Actions Create trigger Edit Clone Debug build Start build with overrides Start build

**Configuration**

Source provider	AWS CodeCommit	Primary repository	Group21-Lab2	Artifacts upload location	Service role
Public builds	Disabled	arn:aws:iam::590184125844:role/service-role/codebuild-cloudformation-validation-service-role			

Build history Batch history Project details Build triggers Metrics

**Build history**

Tiếp đến ta sẽ tạo một Pipeline, tên là 'Group21-Pipeline', tạo một role là 'Group21-PipelineRole' (để mặc định cũng được).

Step 3  
Add source stage  
Step 4  
Add build stage  
Step 5  
Add deploy stage  
Step 6  
Review

**Pipeline name**  
Enter the pipeline name. You cannot edit the pipeline name after it is created.  
**Group21-Pipeline**  
No more than 100 characters

**Pipeline type**  
You can no longer create V1 pipelines through the console. We recommend you use the V2 pipeline type with improved release safety, pipeline triggers, parameterized pipelines, and a new billing model.

**Execution mode**  
Choose the execution mode for your pipeline. This determines how the pipeline is run.  
 Superseded  
A more recent execution can overtake an older one. This is the default.  
 Queued (Pipeline type V2 required)  
Executions are processed one by one in the order that they are queued.  
 Parallel (Pipeline type V2 required)  
Executions don't wait for other runs to complete before starting or finishing.

**Service role**  
 New service role  
Create a service role in your account  
 Existing service role  
Choose an existing service role from your account

**Role name**  
Group21-PipelineRole  
Type your service role name  
 Allow AWS CodePipeline to create a service role so it can be used with this new pipeline

Source là từ CodeCommit, branch master.

Source provider: AWS CodeCommit

Repository name: Group21-Lab2

Branch name: master

Change detection options:

- Amazon CloudWatch Events (recommended)
- AWS CodePipeline

Output artifact format:

- CodePipeline default
- Full clone

Enable automatic retry on stage failure

## Sử dụng Build Project khi này

Build provider: Other build providers

AWS CodeBuild

Project name: cloudformation-validation

Environment variables - optional

Add environment variable

Build type:

- Single build
- Batch build

Region: US East (N. Virginia)

Input artifacts

Chọn ‘Deploy action provider’ là AWS Cloudformation, CREATE\_UPDATE, tên stack là ‘Group21-Stack’, TemplatePath là file template.yaml từ BuildArtifact, sử dụng Role ‘Group21-CodeBuild-Role’ vừa nãy tạo.

## Step 4: Add deploy stage

Deploy action provider

Deploy action provider

AWS CloudFormation

ActionMode

CREATE\_UPDATE

StackName

Group21-Stack

TemplatePath

BuildArtifact::template.yaml

RoleArn

arn:aws:iam::590184125844:role/Group21-CodeBuild-Role

Configure automatic rollback on stage failure

Enabled

Enable automatic retry on stage failure

Disabled

The screenshot shows the AWS CloudFormation 'Deploy provider' configuration screen. The provider is set to 'AWS CloudFormation'. The Region is 'US East (N. Virginia)'. The input artifact is 'BuildArtifact' (defined by Build). The action mode is 'Create or update a stack'. The stack name is 'Group21-Stack'. The template is 'template.yaml'.

## Chạy Pipeline vừa tạo.

The screenshot shows the AWS CodePipeline console. In the top left, there's a sidebar titled "Developer Tools" with "CodePipeline" selected. The main content area has a green header bar with the text "Success" and "Congratulations! The pipeline Group21-Pipeline has been created." Below this, the navigation path is "Developer Tools > CodePipeline > Pipelines > Group21-Pipeline". The pipeline name "Group21-Pipeline" is displayed prominently. To its right are buttons for "Edit", "Stop execution", "Clone pipeline", and a yellow "Release change" button. The pipeline type is listed as "V2" and the execution mode as "QUEUED". The main body of the page shows the first stage, "Source", which is currently "In progress". A pipeline execution ID is provided: f515bdbb-71ad-4c64-9c5d-033990dae0fa. Below this, there are buttons for "View details", "Disable transition", and "Start rollback". The "Build" stage is shown below, with the status " Didn't Run" and a "Start rollback" button.

Source stage chạy thành công.

Source	
Pipeline execution ID:	<a href="#">f515bdbb-71ad-4c64-9c5d-033990dae0fa</a>
Source	<a href="#">AWS CodeCommit</a>
 Succeeded	- 4 minutes ago
<a href="#">7c052dfe</a>	
<a href="#">View details</a>	

Ở Build Stage, cfn-lint đã scan file template.yaml và output 'Success'

# Bài thực hành số 02: Quản lý và triển khai hạ tầng AWS và ứng dụng microservices với Terraform, CloudFormation, GitHub Actions, AWS CodePipeline và Jenkins

15

Tương tự đối với Taskcat, chạy lên ‘taskcat test run’ và output ‘Success’

Action execution details

Action name: Build Status: In progress

```
275 [INFO] : status: CREATE_IN_PROGRESS
276 [stack @ tCaT-cloudformation-template-test-default-2c480b676dc74d8e8cba9150efc29039
277 [region: us-east-1
278 [status: CREATE_IN_PROGRESS
279 [stack @ tCaT-cloudformation-template-test-default-2c480b676dc74d8e8cba9150efc29039
280 [region: us-east-1
281 [status: CREATE_IN_PROGRESS
282 [stack @ tCaT-cloudformation-template-test-default-2c480b676dc74d8e8cba9150efc29039
283 [region: us-east-1
284 [status: CREATE_IN_PROGRESS
285 [stack @ tCaT-cloudformation-template-test-default-2c480b676dc74d8e8cba9150efc29039
286 [region: us-east-1
287 [status: CREATE_IN_PROGRESS
288 [stack @ tCaT-cloudformation-template-test-default-2c480b676dc74d8e8cba9150efc29039
289 [region: us-east-1
290 [status: CREATE_IN_PROGRESS
291 [INFO] : r stack @ tCaT-cloudformation-template-test-default-2c480b676dc74d8e8cba9150efc29039
292 [INFO] : { region: us-east-1
293 [INFO] : l status: CREATE_COMPLETE
294 [INFO] : Reporting on arn:aws:cloudformation:us-east-1:590184125844:stack/tCaT-cloudformation-template-test-default-2c480b676dc74d8e8cba9150efc29039/59044060-a0cf-11ef-bda3-0affff5c24b0d
295 [INFO] : Deleting stack: arn:aws:cloudformation:us-east-1:590184125844:stack/tCaT-cloudformation-template-test-default-2c480b676dc74d8e8cba9150efc29039
296 [stack @ tCaT-cloudformation-template-test-default-2c480b676dc74d8e8cba9150efc29039
297 [region: us-east-1
298 [status: DELETE_IN_PROGRESS
299 [stack @ tCaT-cloudformation-template-test-default-2c480b676dc74d8e8cba9150efc29039
```

Done

Action execution details

Action name: Build Status: Succeeded

```
333 [INFO] : Will not delete bucket created outside of taskcat group21-taskcat
334
335 [Container] 2024/11/12 08:41:42.337861 Phase complete: BUILD State: SUCCEEDED
336 [Container] 2024/11/12 08:41:42.337887 Phase context status code: Message:
337 [Container] 2024/11/12 08:41:42.378083 Entering phase POST_BUILD
338 [Container] 2024/11/12 08:41:42.382000 Phase complete: POST_BUILD State: SUCCEEDED
339 [Container] 2024/11/12 08:41:42.382015 Phase context status code: Message:
340 [Container] 2024/11/12 08:41:42.454819 Expanding base directory path: .
341 [Container] 2024/11/12 08:41:42.456367 Assembling file list
342 [Container] 2024/11/12 08:41:42.456380 Expanding .
343 [Container] 2024/11/12 08:41:42.457926 Expanding file paths for base directory .
344 [Container] 2024/11/12 08:41:42.457936 Assembling file list
345 [Container] 2024/11/12 08:41:42.457939 Expanding template.yaml
346 [Container] 2024/11/12 08:41:42.459413 Found 1 file(s)
347 [Container] 2024/11/12 08:41:42.460615 Set report auto-discover timeout to 5 seconds
348 [Container] 2024/11/12 08:41:42.460697 Expanding base directory path: .
349 [Container] 2024/11/12 08:41:42.462089 Assembling file list
350 [Container] 2024/11/12 08:41:42.462100 Expanding .
351 [Container] 2024/11/12 08:41:42.463972 Expanding file paths for base directory .
352 [Container] 2024/11/12 08:41:42.463984 Assembling file list
353 [Container] 2024/11/12 08:41:42.463988 Expanding **/*
354 [Container] 2024/11/12 08:41:42.466022 No matching auto-discover report paths found
355 [Container] 2024/11/12 08:41:42.466038 Report auto-discover file discovery took 0.005422 seconds
356 [Container] 2024/11/12 08:41:42.466048 Phase complete: UPLOAD_ARTIFACTS State: SUCCEEDED
357 [Container] 2024/11/12 08:41:42.466053 Phase context status code: Message:
```

Done

Build stage chạy thành công.

**Build** Succeeded

Pipeline execution ID: [f515bdbb-71ad-4c64-9c5d-033990dae0fa](#)

**Build**

[AWS CodeBuild](#)

**Succeeded** - Just now

[View details](#)

[7c052dfe](#) Source: first commit

[Start rollback](#)

## Bài thực hành số 02: Quản lý và triển khai hạ tầng AWS và ứng dụng microservices với Terraform, CloudFormation, GitHub Actions, AWS CodePipeline và Jenkins

Khi chạy đến Deploy stage thì phải update lại trust policy:

The screenshot shows the AWS IAM 'Trust policy updated' page. It displays the JSON code for a trust policy:

```

1- [{
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Principal": {
7-         "Service": "cloudformation.amazonaws.com"
8-       },
9-       "Action": "sts:AssumeRole"
10-    }
11-  ]
12-]

```

Deploy stage chạy thành công!

The screenshot shows the AWS CodePipeline 'Deploy' stage status. It indicates 'Succeeded' and provides a Pipeline execution ID: [3ae39194-d67d-4b87-8d3f-5f4d69c18762](#). A green checkmark icon is visible on the right.

Các Cloudformation stack đã được khởi tạo.

Stack name	Status	Created time	Description
<a href="#">Group21-Stack</a>	<span>✓ CREATE_COMPLETE</span>	2024-11-12 15:41:48 UTC+0700	Create VPC, Subnets, Security Groups, Internet and NAT Gateways, Route Tables, and EC2 Instances
<a href="#">lab02group05</a>	<span>✓ CREATE_COMPLETE</span>	2024-11-12 15:01:01 UTC+0700	Template to create a VPC, Subnets, Internet Gateway, NAT Gateway, EC2 instances
<a href="#">cfst-1449-a1843f1a6e15027d9d1aee248b392b9d9c60ef15603b06e811d0ae8a33c04ca5</a>	<span>✓ CREATE_COMPLETE</span>	2024-11-12 12:41:17 UTC+0700	-

Instances (2/9) <a href="#">Info</a>		Last updated less than a minute ago	<a href="#">C</a>	<a href="#">Connect</a>	<a href="#">Instance state ▾</a>	<a href="#">Actions ▾</a>	<a href="#">Launch instances</a>	<a href="#">...</a>
<input type="text"/> Find Instance by attribute or tag (case-sensitive)				<a href="#">All states ▾</a>				
<a href="#">Instance state = running</a> <a href="#">X</a>		<a href="#">Clear filters</a>		< 1 > <a href="#">...</a>				
—	Name <a href="#">🔗</a>	▼	Instance ID	Instance state	▼	Instance type	▼	Status check
<input checked="" type="checkbox"/>	PrivateEC2Instance		i-0469f58a58106ef28	<span>Running</span> <a href="#">Q</a> <a href="#">Q</a>	t2.micro	<span>2/2 checks passec</span>	<a href="#">View alarms</a> <a href="#">+</a>	us-east
<input type="checkbox"/>			i-059acb3bea9f7b801	<span>Running</span> <a href="#">Q</a> <a href="#">Q</a>	t2.medium	<span>2/2 checks passec</span>	<a href="#">View alarms</a> <a href="#">+</a>	us-east
<input checked="" type="checkbox"/>	PublicEC2Instance		i-0269ddc6cffb89c07	<span>Running</span> <a href="#">Q</a> <a href="#">Q</a>	t2.micro	<span>2/2 checks passec</span>	<a href="#">View alarms</a> <a href="#">+</a>	us-east
<input type="checkbox"/>	single-instance		i-01a89996da578ead4	<span>Running</span> <a href="#">Q</a> <a href="#">Q</a>	t2.medium	<span>2/2 checks passec</span>	<a href="#">View alarms</a> <a href="#">+</a>	us-east
<input type="checkbox"/>	Public Instance group 12		i-072d5a0a623185fff	<span>Running</span> <a href="#">Q</a> <a href="#">Q</a>	t2.micro	<span>Initializing</span>	<a href="#">View alarms</a> <a href="#">+</a>	us-east
<input type="checkbox"/>			i-01ee8337daf2ec153	<span>Running</span> <a href="#">Q</a> <a href="#">Q</a>	t2.medium	<span>2/2 checks passec</span>	<a href="#">View alarms</a> <a href="#">+</a>	us-east
<input type="checkbox"/>	PublicEC2Instance		i-0849c0613f2665f91	<span>Running</span> <a href="#">Q</a> <a href="#">Q</a>	t2.micro	<span>2/2 checks passec</span>	<a href="#">View alarms</a> <a href="#">+</a>	us-east
<input type="checkbox"/>	PrivateEC2Instance		i-014328ad0a1430b52	<span>Running</span> <a href="#">Q</a> <a href="#">Q</a>	t2.micro	<span>2/2 checks passec</span>	<a href="#">View alarms</a> <a href="#">+</a>	us-east

### 3. Câu 3

Đầu tiên, tạo một Jenkins Server bằng terraform, sau đó tải các package cần thiết để triển khai Docker, Kubernetes, EKS, Jenkins, Trivy và SonarQube.

The screenshot shows a Visual Studio Code interface with the following details:

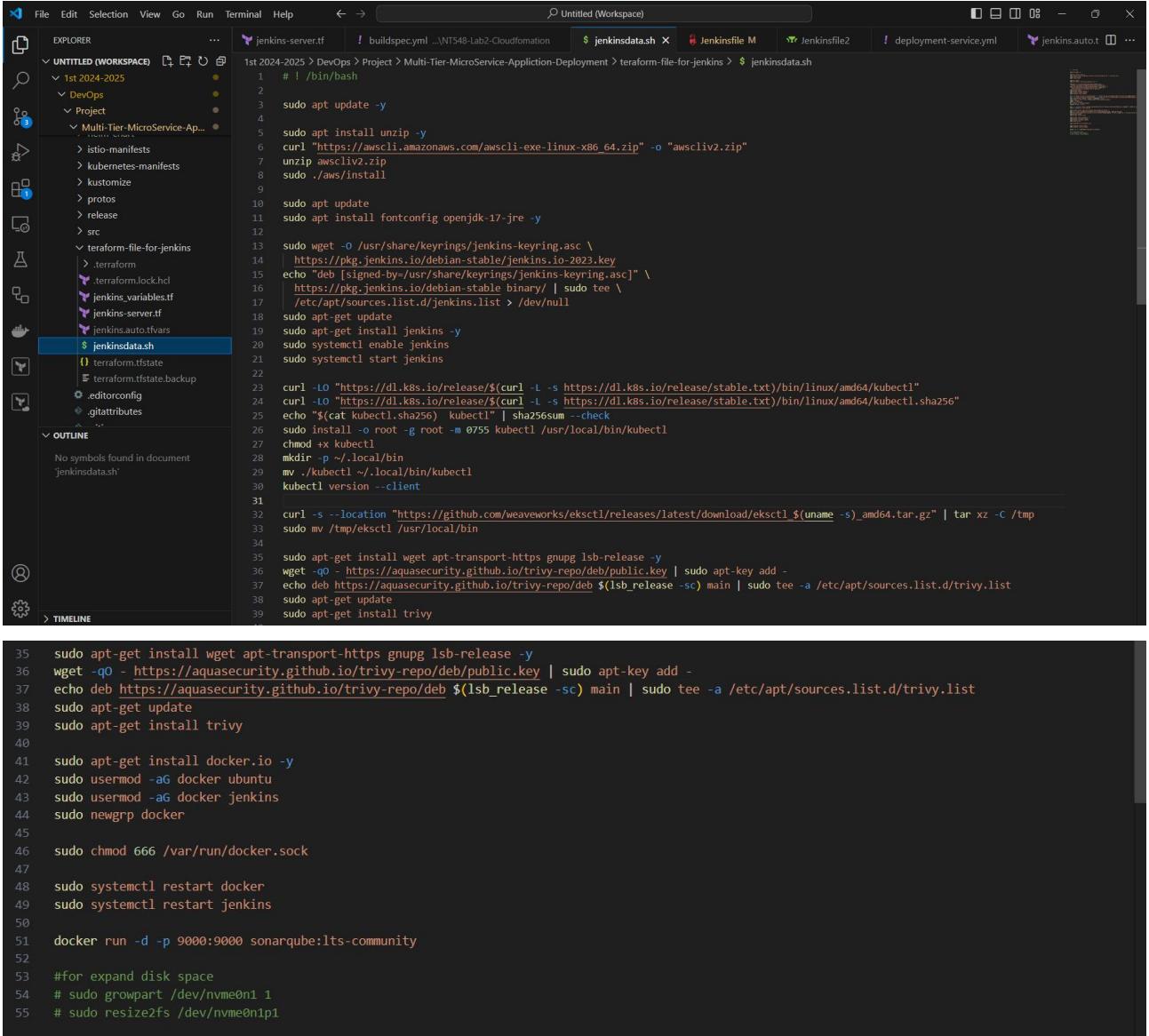
- File Explorer:** On the left, it displays the project structure under "UNTITLED (WORKSPACE)". The "jenkins-server.tf" file is currently selected.
- Code Editor:** The main area shows the Terraform configuration for the Jenkins server. It includes resources for an AWS instance, security group, and ingress rules.
- Terminal:** At the bottom, the terminal shows the command "terraform apply" being run, with output indicating the creation of various AWS resources like security groups and instances.

```
provider "aws" {
  region = var.region
}

resource "aws_instance" "tf-jenkins-server" {
  ami           = var.ami
  instance_type = var.instance_type
  key_name      = var.mykey
  vpc_security_group_ids = [aws_security_group.tf-jenkins-sec-gr.id]
  iam_instance_profile = aws_iam_instance_profile.tf-jenkins-server-profile.name
  ebs_block_device {
    device_name = "/dev/xvda"
    volume_type = "gp2"
    volume_size = 16
  }
  tags = {
    Name = var.jenkins-server-tag
    server = "Jenkins"
  }
  user_data = templatefile("./jenkinsdata.sh", {})
}

resource "aws_security_group" "tf-jenkins-sec-gr" {
  name = var.jenkins_server_secgr
  tags = [
    {Name = var.jenkins_server_secgr}
  ]
  ingress {
    from_port   = 80
    protocol   = "tcp"
    to_port     = 80
    cidr_blocks = ["0.0.0.0/0"]
  }
  ingress {
    from_port   = 22
    protocol   = "tcp"
    to_port     = 22
    cidr_blocks = ["0.0.0.0/0"]
  }
}
```

## Bài thực hành số 02: Quản lý và triển khai hạ tầng AWS và ứng dụng microservices với Terraform, CloudFormation, GitHub Actions, AWS CodePipeline và Jenkins



The screenshot shows a code editor interface with multiple tabs open. The main tab contains a shell script for Jenkins setup, which includes commands for updating packages, installing AWS CLI, and configuring Jenkins. Below this, another section of the script continues with package management and configuration steps for Docker and Trivy.

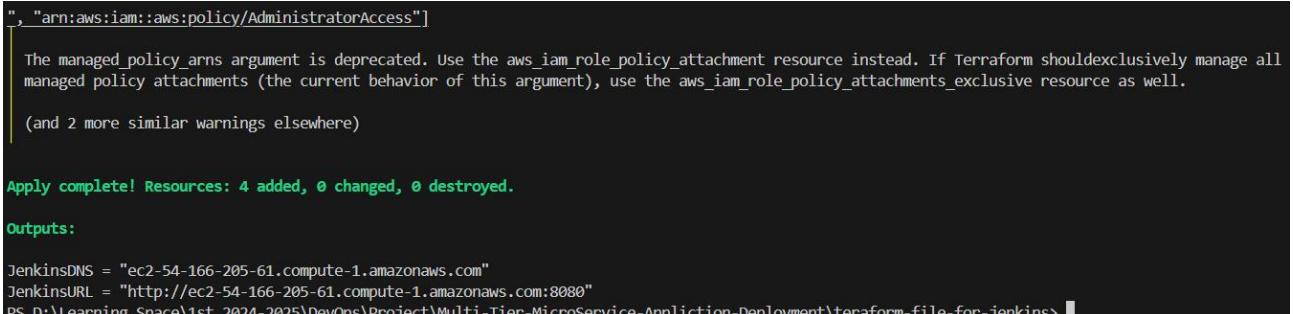
```

1st 2024-2025 > DevOps > Project > Multi-Tier-MicroService-Application-Deployment > terraform-file-for-jenkins > $ jenkinsdata.sh
1 #!/bin/bash
2
3 sudo apt update -y
4
5 sudo apt install unzip -y
6 curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
7 unzip awscliv2.zip
8 sudo ./aws/install
9
10 sudo apt update
11 sudo apt install fontconfig openjdk-17-jre -y
12
13 sudo wget -O /usr/share/keyrings/jenkins-keyring.asc \
14 https://pkg.jenkins.io/debian-stable/jenkins.io-2023.key
15 echo "deb [signed-by=/usr/share/keyrings/jenkins-keyring.asc] " \
16 https://pkg.jenkins.io/debian-stable binary/ | sudo tee \
17 /etc/apt/sources.list.d/jenkins.list > /dev/null
18 sudo apt-get update
19 sudo apt-get install jenkins
20 sudo systemctl enable jenkins
21 sudo systemctl start jenkins
22
23 curl -LO "https://dl.k8s.io/release/$(curl -L -s https://dl.k8s.io/release/stable.txt)/bin/linux/amd64/kubectl"
24 curl -LO "https://dl.k8s.io/release/$(curl -L -s https://dl.k8s.io/release/stable.txt)/bin/linux/amd64/kubectl.sha256"
25 echo "$(cat kubectl.sha256) kubectl" | sha256sum --check
26 sudo install -o root -g root -m 0755 kubectl /usr/local/bin/kubectl
27 chmod +x kubectl
28 mkdir -p ~/.local/bin
29 mv ./kubectl ~/.local/bin/kubectl
30 kubectl version --client
31
32 curl -s --location "https://github.com/weaveworks/eksctl/releases/latest/download/eksctl_$(uname -s)_amd64.tar.gz" | tar xz -c /tmp
33 sudo mv /tmp/eksctl /usr/local/bin
34
35 sudo apt-get install wget apt-transport-https gnupg lsb-release -y
36 wget -qO - https://aquasecurity.github.io/trivy-repo/deb/public.key | sudo apt-key add -
37 echo deb https://aquasecurity.github.io/trivy-repo/deb $(lsb_release -sc) main | sudo tee -a /etc/apt/sources.list.d/trivy.list
38 sudo apt-get update
39 sudo apt-get install trivy
40
41 sudo apt-get install docker.io -y
42 sudo usermod -aG docker ubuntu
43 sudo usermod -aG docker jenkins
44 sudo newgrp docker
45
46 sudo chmod 666 /var/run/docker.sock
47
48 sudo systemctl restart docker
49 sudo systemctl restart jenkins
50
51 docker run -d -p 9000:9000 sonarqube:lts-community
52
53 #for expand disk space
54 # sudo growpart /dev/nvme0n1 1
55 # sudo resize2fs /dev/nvme0n1p1

```

Lần lượt gõ terraform init, terraform plan và terraform apply.

Triển khai Jenkins Server thành công, IP public là 54.166.205.61.



The terminal window shows the results of a Terraform apply command. It indicates that 4 resources were added, and provides the IP address of the Jenkins server (54.166.205.61) and its URL (http://ec2-54-166-205-61.compute-1.amazonaws.com:8080).

```

", "arn:aws:iam::aws:policy/AdministratorAccess"]

The managed_policy_arns argument is deprecated. Use the aws_iam_role_policy_attachment resource instead. If Terraform should exclusively manage all managed policy attachments (the current behavior of this argument), use the aws_iam_role_policy_attachments_exclusive resource as well.

(and 2 more similar warnings elsewhere)

Apply complete! Resources: 4 added, 0 changed, 0 destroyed.

Outputs:

JenkinsDNS = "ec2-54-166-205-61.compute-1.amazonaws.com"
JenkinsURL = "http://ec2-54-166-205-61.compute-1.amazonaws.com:8080"
PS D:\Learning_Space\1st 2024-2025\DevOps\Project\Multi-Tier-MicroService-Application-Deployment\terraform-file-for-jenkins>

```

## Bài thực hành số 02: Quản lý và triển khai hạ tầng AWS và ứng dụng microservices với Terraform, CloudFormation, GitHub Actions, AWS CodePipeline và Jenkins

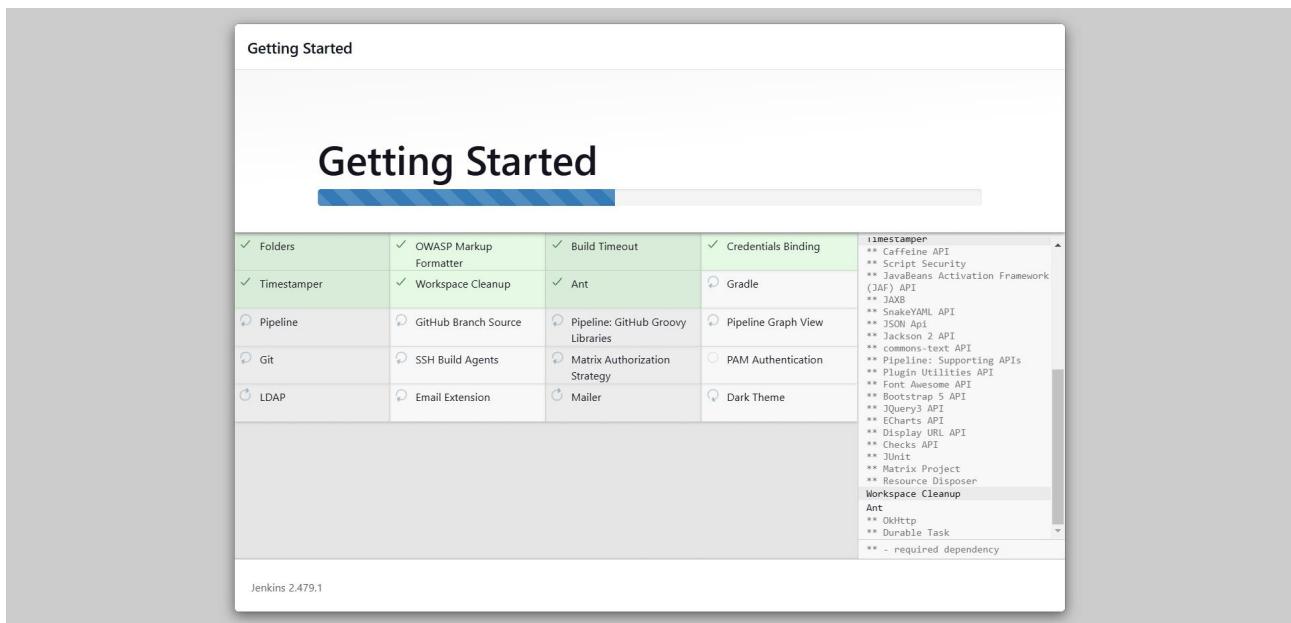
The screenshot shows the AWS EC2 Instances page. On the left sidebar, under the 'Instances' section, 'Instances' is selected. The main content area displays a table titled 'Instances (1/1) info'. A single row is shown for an instance named 'Jenkins Server' with the instance ID 'i-02f7bbb5678b21ea2'. The instance state is 'Running' and the instance type is 'm5.large'. The status check shows 'Initializing' and the alarm status is 'View alarms'. The availability zone is 'us-east-1'. Below the table, a detailed view for the instance 'i-02f7bbb5678b21ea2 (Jenkins Server)' is expanded, showing details like Public IPv4 address (54.166.205.61), Private IPv4 addresses (172.31.39.121), and Public IPv4 DNS.

Truy cập vào Jenkins bằng địa chỉ <PublicIP>:8080, và vào path bên dưới để lấy mật khẩu.

The screenshot shows a browser window with the URL 'http://54.166.205.61:8080/login?from=%2F'. The page title is 'Getting Started' and the main heading is 'Unlock Jenkins'. It instructs the user to copy the password from the file '/var/lib/jenkins/secrets/initialAdminPassword'. Below this, there is a text input field labeled 'Administrator password' with a placeholder 'Enter your password here'. At the bottom right is a 'Continue' button. Below the page content, a terminal session shows the password being read from the file:

```
ubuntu@ip-172-31-39-121:~$ cat /var/lib/jenkins/secrets/initialAdminPassword
cat: /var/lib/jenkins/secrets/initialAdminPassword: Permission denied
ubuntu@ip-172-31-39-121:~$ sudo cat /var/lib/jenkins/secrets/initialAdminPassword
43f45ead94614c0a889b748ceba68bb9
ubuntu@ip-172-31-39-121:~$ |
```

Tải về một số plugins.



Tạo Admin User.

The screenshot shows the Jenkins 'Create First Admin User' form. It has five input fields:

- Username: jenkins
- Password: ..... (redacted)
- Confirm password: ..... (redacted)
- Full name: jenkins
- E-mail address: (empty field)

At the bottom, there are two buttons: 'Skip and continue as admin' and 'Save and Continue'. The 'Save and Continue' button is highlighted with a blue border.

Jenkins 2.479.1

# Bài thực hành số 02: Quản lý và triển khai hạ tầng AWS và ứng dụng microservices với Terraform, CloudFormation, GitHub Actions, AWS CodePipeline và Jenkins

21

The screenshot shows the Jenkins dashboard with the following sections:

- Left sidebar:** Includes links for "New Item", "Build History", "Manage Jenkins", and "My Views".
- Welcome to Jenkins!**: A central heading with a brief introduction.
- Start building your software project**: A section with links to "Create a job", "Set up a distributed build", "Set up an agent", "Configure a cloud", and "Learn more about distributed builds".
- Build Queue**: A box stating "No builds in the queue."
- Build Executor Status**: A box showing "0/2" available executors.
- Bottom right:** Links for "REST API" and "Jenkins 2.479.1".

## Tải về một số Plugins.

<input checked="" type="checkbox"/>	<a href="#">SonarQube Scanner</a> 2.17.2	External Site/Tool Integrations Build Reports	8 mo 26 days ago
	This plugin allows an easy integration of <a href="#">SonarQube</a> , the open source platform for Continuous Inspection of code quality.		
<input checked="" type="checkbox"/>	<a href="#">Docker</a> 1.7.0	Cloud Providers Cluster Management docker	28 days ago
	This plugin integrates Jenkins with <a href="#">Docker</a>		
<input checked="" type="checkbox"/>	<a href="#">Docker Commons</a> 445.v6b_646c962a_94	Library plugins (for use by other plugins) docker	4 days 17 hr ago
	Provides the common shared functionality for various Docker-related plugins.		
<input checked="" type="checkbox"/>	<a href="#">Docker Pipeline</a> 580.vc0c340686b_54	pipeline DevOps Deployment docker	5 mo 24 days ago
	Build and use Docker containers from pipelines.		
<input checked="" type="checkbox"/>	<a href="#">CloudBees Docker Build and Publish</a> 1.4.0	Build Tools docker	2 yr 2 mo ago
	This plugin enables building Dockerfile based projects, as well as publishing of the built images/repos to the docker registry.		
<input checked="" type="checkbox"/>	<a href="#">Kubernetes Client API</a> 6.10.0-240.v57880ce8b_0b_2	kubernetes Library plugins (for use by other plugins)	9 mo 20 days ago
	Kubernetes Client API plugin for use by other Jenkins plugins.		
<input checked="" type="checkbox"/>	<a href="#">Kubernetes Credentials</a> 190.v03c305394deb_	kubernetes credentials	1 mo 25 days ago
	Common classes for Kubernetes credentials		
<input checked="" type="checkbox"/>	<a href="#">Kubernetes</a> 4296.v20a_7e4d77cf6	Cloud Providers Cluster Management kubernetes Agent Management	6 days 23 hr ago
	This plugin integrates Jenkins with <a href="#">Kubernetes</a>		
<input checked="" type="checkbox"/>	<a href="#">Kubernetes CLI</a> 1.12.1	kubernetes	1 yr 2 mo ago
	Configure kubectl for Kubernetes		
<input checked="" type="checkbox"/>	<a href="#">Kubernetes Credentials Provider</a> 1.262.v2670ef7ea_0c5	kubernetes credentials	8 mo 16 days ago
	Provides a read only credentials store backed by Kubernetes.		

# Bài thực hành số 02: Quản lý và triển khai hạ tầng AWS và ứng dụng microservices với Terraform, CloudFormation, GitHub Actions, AWS CodePipeline và Jenkins

22

The screenshot shows the Jenkins interface with the title 'Jenkins'. In the top right, there are icons for notifications, security, and user status, followed by 'jenkins' and 'log out'. Below the title is a search bar with the placeholder 'Search (CTRL+K)'. Underneath the search bar is a navigation menu with 'Dashboard', 'Manage Jenkins', and 'Plugins'. The 'Plugins' section is active. On the left, there's a sidebar with 'Updates', 'Available plugins', 'Installed plugins' (which is selected and highlighted in grey), 'Advanced settings', and 'Download progress'. A search bar at the top of the main content area has the text 'eks'. The main content shows a table with columns 'Name' and 'Enabled'. One row is visible: 'EKS Token Plugin 0.0.2', which is enabled (indicated by a checked checkbox). There is also a link 'Report an issue with this plugin'.

Đăng nhập vào SonarQube với tài khoản admin:admin.

The screenshot shows a browser window with the URL 'http://54.166.205.61:9000/sessions/new?return\_to=%2F'. The page title is 'Log in to SonarQube'. It features two input fields: one for 'admin' and one for a password (represented by four asterisks). Below the fields are 'Log in' and 'Cancel' buttons. The browser's address bar shows the URL, and the toolbar includes standard icons like back, forward, and search.

```
ubuntu@ip-172-31-39-121:~$ eksctl create cluster --name=my-eks2 \
--region=us-east-1 \
--zones=us-east-1a,us-east-1b \
--without-nodegroup
2024-11-12 09:46:17 [ℹ] eksctl version 0.194.0
2024-11-12 09:46:17 [ℹ] using region us-east-1
2024-11-12 09:46:17 [ℹ] subnets for us-east-1a - public:192.168.0.0/19 private:192.168.64.0/19
2024-11-12 09:46:17 [ℹ] subnets for us-east-1b - public:192.168.32.0/19 private:192.168.96.0/19
2024-11-12 09:46:17 [ℹ] using Kubernetes version 1.38
2024-11-12 09:46:17 [ℹ] creating EKS cluster "my-eks2" in "us-east-1" region with
2024-11-12 09:46:17 [ℹ] if you encounter any issues, check CloudFormation console or try 'eksctl utils describe-stacks --region=us-east-1 --cluster=my-eks2'
2024-11-12 09:46:17 [ℹ] Kubernetes API endpoint access will use default of {publicAccess=true, privateAccess=false} for cluster "my-eks2" in "us-east-1"
2024-11-12 09:46:17 [ℹ] CloudWatch logging will not be enabled for cluster "my-eks2" in "us-east-1"
2024-11-12 09:46:17 [ℹ] you can enable it with 'eksctl utils update-cluster-logging --enable-types={SPECIFY-YOUR-LOG-TYPES-HERE (e.g. all)} --region=us-east-1 --cluster=my-eks2'
2024-11-12 09:46:17 [ℹ] default addons vpc-cni, kube-proxy, coredns were not specified, will install them as EKS addons
2024-11-12 09:46:17 [ℹ]
2 sequential tasks: { create cluster control plane "my-eks2",
  2 sequential sub-tasks: {
    1 task: { create addons },
    wait for control plane to become ready,
  }
}
2024-11-12 09:46:17 [ℹ] building cluster stack "eksctl-my-eks2-cluster"
2024-11-12 09:46:17 [ℹ] deploying stack "eksctl-my-eks2-cluster"
```

Tạo một Cluster tên 'my-eks2'

## Bài thực hành số 02: Quản lý và triển khai hạ tầng AWS và ứng dụng microservices với Terraform, CloudFormation, GitHub Actions, AWS CodePipeline và Jenkins

```
ubuntu@ip-172-31-39-121:~$ eksctl utils associate-iam-oidc-provider \
--region us-east-1 \
--cluster my-eks2 \
--approve
2024-11-12 10:01:37 [+] will create IAM Open ID Connect provider for cluster "my-eks2" in "us-east-1"
2024-11-12 10:01:37 [-] created IAM Open ID Connect provider for cluster "my-eks2" in "us-east-1"
ubuntu@ip-172-31-39-121:~$ eksctl create nodegroup --cluster=my-eks2 \
--region=us-east-1 \
--name=node2 \
--node-type=t3.medium \
--nodes=3 \
--nodes-min=2 \
--nodes-max=3 \
--node-volume-size=20 \
--ssh-public-key=mykey \
--managed \
--asg-access \
--external-dns-access \
--full-ecr-access \
--appmesh-access \
--alb-ingress-access
2024-11-12 10:01:44 [+] will use version 1.30 for new nodegroup(s) based on control plane version
2024-11-12 10:01:45 [+] nodegroup "node2" will use "" [AmazonLinux2/1.30]
2024-11-12 10:01:45 [+] 1 nodegroup (node2) was included (based on the include/exclude rules)
2024-11-12 10:01:45 [+] will create a CloudFormation stack for each of 1 managed nodegroups in cluster "my-eks2"
2024-11-12 10:01:45 [+] 2 sequential tasks: { fix cluster compatibility, 1 task: { 1 task: { create managed nodegroup "node2" } } }
[+]
2024-11-12 10:01:45 [+] checking cluster stack for missing resources
2024-11-12 10:01:45 [+] cluster stack has all required resources
2024-11-12 10:01:45 [+] building managed nodegroup stack "eksctl-my-eks2-nodegroup-node2"
2024-11-12 10:01:45 [+] deploying stack "eksctl-my-eks2-nodegroup-node2"
2024-11-12 10:01:45 [+] waiting for CloudFormation stack "eksctl-my-eks2-nodegroup-node2"
2024-11-12 10:02:15 [+] waiting for CloudFormation stack "eksctl-my-eks2-nodegroup-node2"
2024-11-12 10:03:05 [+] waiting for CloudFormation stack "eksctl-my-eks2-nodegroup-node2"
2024-11-12 10:04:26 [+] waiting for CloudFormation stack "eksctl-my-eks2-nodegroup-node2"
2024-11-12 10:04:26 [+] no tasks
2024-11-12 10:04:26 [-] created 0 nodegroup(s) in cluster "my-eks2"
```

Liên kết OIDC với với Cluster 'my-eks2' và tạo một nodegroup cho cluster 'my-eks2', gồm 3 node EC2 (t3.medium) với cấu hình chi tiết bên trên.

Stack name	Status	Created time	Description
<a href="#">eksctl-my-eks2-nodegroup-node2</a>	<span>CREATE_COMPLETE</span>	2024-11-12 17:01:45 UTC+0700	EKS Managed Nodes (SSH access: false) [created by eksctl]
<a href="#">eksctl-my-eks2-cluster</a>	<span>CREATE_COMPLETE</span>	2024-11-12 16:46:17 UTC+0700	EKS cluster (dedicated VPC: true, dedicated IAM: true) [created and managed by eksctl]

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
my-eks2-node2-Node	i-0b6ed4243e82b5366	<span>Running</span>	t3.medium	<span>3/3 checks passed</span>	<a href="#">View alarms +</a>	us-east-1
my-eks2-node2-Node	i-0baef501130a3d355	<span>Running</span>	t3.medium	<span>3/3 checks passed</span>	<a href="#">View alarms +</a>	us-east-1
my-eks2-node2-Node	i-01de46c7cb0c2d3e4	<span>Running</span>	t3.medium	<span>3/3 checks passed</span>	<a href="#">View alarms +</a>	us-east-1
Jenkins Server	i-02f7bb5678b21ea2	<span>Running</span>	m5.large	<span>3/3 checks passed</span>	<a href="#">View alarms +</a>	us-east-1

The screenshot shows the 'Tokens of Administrator' section in SonarQube. A new token named 'T' has been generated for 30 days. The token value is displayed in a yellow-highlighted box with a 'Copy' button. Below the table, a note states: 'Embedded database should be used for evaluation purposes only. The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine.'

Name	Type	Project	Last use	Created	Expiration
T	User		Never	November 12, 2024	December 12, 2024

Quay lại với SonarQube, chọn vào Admininstration -> Token -> Generate Token.

The screenshot shows the 'New credentials' form in Jenkins. A secret text credential named 'sonar-token' is being created. The 'Kind' is set to 'Secret text', 'Scope' is 'Global (Jenkins, nodes, items, all child items, etc)', and the 'ID' is 'sonar-token'. The 'Create' button is visible at the bottom.

Vào Jenkins, Manage Jenkins -> Credentials -> Global Credentials, tạo một secret text với token vừa tạo, đặt id là 'sonar-token'.

# Bài thực hành số 02: Quản lý và triển khai hạ tầng AWS và ứng dụng microservices với Terraform, CloudFormation, GitHub Actions, AWS CodePipeline và Jenkins

25

New credentials

Kind

Username with password

Scope ?

Global (Jenkins, nodes, items, all child items, etc)

Username ?

levi2708

Treat username as secret ?

Password ?

.....

ID ?

docker-cred

Description ?

Create

Tương tự như trên, tạo một Username with password với tài khoản mật khẩu của Docker.

Amazon Elastic Kubernetes Service

Clusters

Amazon EKS Anywhere

Enterprise Subscriptions New

Related services

Amazon ECR

AWS Batch

Console settings

Documentation

Submit feedback

Cluster info Info

Status Active

Kubernetes version Info 1.30

Support period Standard support until July 28, 2025

Provider EKS

Networking

VPC Info vpc-Oda54dfdafacb1aa6

Subnets subnet-029c5892ae1b1826, subnet-0b3a8a53637555976, subnet-04566cf7237369162, subnet-0053981f50848c2fc

Cluster IP address family Info IPv4

Service IPv4 range Info 10.100.0.0/16

Cluster security group Info sg-0078f045b4ac6a043

API server endpoint access Info Public

Additional security groups Info sg-0290ea3c35492eac4

Public access source allowlist 0.0.0.0/0 (open to all traffic)

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws Services Search [Alt+S]

VPC > Security Groups > sg-0290ea3c35492eac4 - eksctl-my-eks2-cluster-ControlPlaneSecurityGroup-X5ESEoNuiFsy > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range	Source Info	Description - optional Info
-	All traffic	All	All	Anywhere	0.0.0.0/0

Add rule

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel Preview changes Save rules

Trước khi vào bước tiếp theo, ta cần chỉnh lại inbound rules ở Additional security group của 'my-eks2'.

Tạo một namespace tên là 'webapps'

```
ubuntu@ip-172-31-39-121:~$ kubectl create namespace webapps
namespace/webapps created
ubuntu@ip-172-31-39-121:~$ kubectl get namespace
NAME      STATUS   AGE
default   Active   49m
kube-node-lease   Active   49m
kube-public   Active   49m
kube-system   Active   49m
webapps     Active   16s
ubuntu@ip-172-31-39-121:~$ |
```

Tạo một ServiceAccount tên là Jenkins cho namespace webapps.

```
ubuntu@ip-172-31-39-121:~$ nano sa.yaml
ubuntu@ip-172-31-39-121:~$ nano sa.yaml
ubuntu@ip-172-31-39-121:~$ |
```

```
ubuntu@ip-172-31-39-121: ~      X + v
GNU nano 7.2
apiVersion: v1
kind: ServiceAccount
metadata:
  name: jenkins
  namespace: webapps
```

```
ubuntu@ip-172-31-39-121:~$ kubectl apply -f sa.yaml
serviceaccount/jenkins created
ubuntu@ip-172-31-39-121:~$ |
```

Tạo một role tên là ‘app-role’ cho namespace webapps.

Các rules bao gồm:

Các API mặc định của Kubernetes cùng với vài API khác như apps, autoscaling, ...

Danh sách các tài nguyên mà Role có thể truy cập như pods, configmaps, ...

Danh sách các hành động Role thực hiện như get, list, create, ...

```
ubuntu@ip-172-31-39-121:~$ nano rol.yaml
ubuntu@ip-172-31-39-121:~$ |
```



```
GNU nano 7.2                                     rol.yaml *
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: app-role
  namespace: webapps
rules:
- apiGroups:
  - ""
  - apps
  - autoscaling
  - batch
  - extensions
  - policy
  - rbac.authorization.k8s.io
  resources:
  - pods
  - configmaps
  - deployments
  - daemonsets
  - componentstatuses
  - events
  - endpoints
  - horizontalpodautoscalers
  - ingress
  - jobs
  - limitranges
  - namespaces
  - nodes
  - persistentvolumes
  - persistentvolumeclaims
  - resourcequotas
  - replicases
  - replicationcontrollers
  - serviceaccounts
  - services
  verbs:
  - get
  - list
  - watch
  - create
```

```
ubuntu@ip-172-31-39-121:~$ kubectl apply -f rol.yaml
role.rbac.authorization.k8s.io/app-role created
ubuntu@ip-172-31-39-121:~$ |
```

Tạo một RoleBinding tên là app-rolebinding cho namespace webapps.

Gán quyền của Role ‘app-role’ cho ServiceAccount ‘jenkins’ trong namespace webapps, nghĩa là SA ‘jenkins’ sẽ có tất cả quyền được xác định trong ‘app-role’.

```
ubuntu@ip-172-31-39-121:~$ nano bind.yaml|
```

```
ubuntu@ip-172-31-39-121: ~ + - 
GNU nano 7.2
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: app-rolebinding
  namespace: webapps
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: app-role
subjects:
- namespace: webapps
  kind: ServiceAccount
  name: jenkins
```

```
ubuntu@ip-172-31-39-121:~$ kubectl apply -f bind.yaml
rolebinding.rbac.authorization.k8s.io/app-rolebinding created
ubuntu@ip-172-31-39-121:~$ |
```

Tạo một secret chứa token của ServiceAccount ‘jenkins’, tên là mysecretname.

```
ubuntu@ip-172-31-39-121:~$ nano sec.yaml
ubuntu@ip-172-31-39-121:~$ |
```

```
ubuntu@ip-172-31-39-121: ~ + - 
GNU nano 7.2
apiVersion: v1
kind: Secret
type: kubernetes.io/service-account-token
metadata:
  name: mysecretname
  annotations:
    kubernetes.io/service-account.name: jenkins
```

```
ubuntu@ip-172-31-39-121:~$ kubectl apply -f sec.yaml -n webapps
secret/mysecretname created
ubuntu@ip-172-31-39-121:~$ |
```

Ta có thể lấy token đó bằng cách dùng câu lệnh bên dưới:

Lưu vào trong credentials của Jenkins, id là k8s-token-webapps.

 Jenkins

Dashboard > Manage Jenkins > Credentials > System > Global credentials (unrestricted) >

## New credentials

Kind

Secret text

Scope ?

Global (Jenkins, nodes, items, all child items, etc)

Secret

.....

ID ?

k8s-token-webapps

Description ?

.....

Create

Copy đoạn URL của EKS server endpoint rồi lưu vào credentials của Jenkins.

The screenshot shows the AWS EKS service page for a cluster named "eks". The left sidebar includes links for Clusters, Amazon EKS Anywhere, Enterprise Subscriptions, and Related services (Amazon ECR, AWS Batch). The main content area displays cluster information: Status (Active), Kubernetes version (1.30), Support period (Standard support until July 28, 2025), and Provider (EKS). Below this, tabs for Overview, Resources, Compute, Networking, Add-ons, Access, Observability, Upgrade insights, and Update history are visible. The Details section shows the endpoint (https://67FBD3D51BE6C68A23FDA36D74A5892.gr7.us-east-1.eks.amazonaws.com), OpenID Connect provider URL (https://oidc.eks.us-east-1.amazonaws.com/id/67FBD3D51BE6C68A23FDA36D74A5892D), Certificate authority (base64 encoded string), Cluster IAM role ARN (arn:aws:eks:us-east-1:730335451237:role/eksctl-my-eks-2-cluster-ServiceRole-bCM2k6j9DwDwW), and Platform version (eks.18).

# Bài thực hành số 02: Quản lý và triển khai hạ tầng AWS và ứng dụng microservices với Terraform, CloudFormation, GitHub Actions, AWS CodePipeline và Jenkins

30

The screenshot shows the Jenkins interface for creating new credentials. The 'Kind' dropdown is set to 'EKS Token Credentials'. The 'ID' field contains 'eks-server-url'. The 'Description' field is empty. The 'Cluster Name' field contains 'https://67FBD3D51BE6C68A23FDA36D74A5892D.gr7.us-east-1.eks.amazonaws.com'. The 'Region' dropdown is set to 'us-gov-west-1'. A 'Create' button is visible at the bottom.

Tất cả các Credentials đã tạo

The screenshot shows the Jenkins interface displaying a list of global credentials. There are four entries: 'sonar-token' (Secret text), 'docker-cred' (Username with password), 'k8s-token-webapps' (Secret text), and 'eks-server-url' (EKS Token Credentials). A '+ Add Credentials' button is located at the top right of the table header.

ID	Name	Kind	Description
sonar-token	sonar-token	Secret text	
docker-cred	levi2708/********	Username with password	
k8s-token-webapps	k8s-token-webapps	Secret text	
eks-server-url	eks-server-url	EKS Token Credentials	

Tạo SonarQube Scanner bằng cách vào Manage Jenkins -> tools.

The screenshot shows the Jenkins interface for managing tools. Under 'SonarQube Scanner installations', there is a form to add a new installation. The 'Name' field is 'sonar'. The 'Install automatically?' checkbox is checked. Under 'Install from Maven Central', the 'Version' dropdown is set to 'SonarQube Scanner 6.2.1.4610'. An 'Add Installer' button is at the bottom.

Vào Manage Jenkins -> System, sau đó tạo một Jenkins server với IP là <PublicIP>:9000, với token là 'sonar-token' đã tạo trước đó.

The screenshot shows the Jenkins System configuration page under the 'Manage Jenkins' section. In the 'SonarQube installations' section, there is a single entry named 'sonar'. The 'Name' field contains 'sonar', the 'Server URL' field contains 'http://54.166.205.61:9000', and the 'Server authentication token' dropdown contains 'sonar-token'. There is also a '+ Add' button and an 'Advanced' dropdown.

Tạo Pipeline tên là '10-Tier', các cấu hình đều để mặc định, sau đó paste Jenkinsfile vào phần Script.

### New Item

Enter an item name

10-Tier

Select an item type



**Freestyle project**

Classic, general-purpose job type that checks out from up to one SCM, executes build steps serially, followed by post-build steps like archiving artifacts and sending email notifications.



**Pipeline**

Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.



**Multi-configuration project**

Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.



**Folder**

Creates a container that stores nested items in it. Useful for grouping things together. Unlike view, which is just a filter, a Folder creates a separate namespace, so you can have multiple things of the same name as long as they are in different folders.



**Multibranch Pipeline**

OK

Đoạn script sẽ checkout nhánh 'latest' từ Github repo đã cho. Sử dụng SonarQube để scan và trả về kết quả ở SonarQube server.

```
1st 2024-2025 > DevOps > Project > Multi-Tier-MicroService-Application-Deployment > Jenkinsfile2
 1 pipeline {
 2   agent any
 3   environment{
 4     SCANNER_HOME= tool 'sonar-scanner'
 5   }
 6   stages {
 7     stage('git checkout') {
 8       steps {
 9         git branch: 'latest', url: 'https://github.com/just-vile/Multi-Tier-MicroService-Application-Deployment.git'
10       }
11     }
12     stage('SonarQube') {
13       steps {
14         withSonarQubeEnv('sonar') {
15           sh '''
16             $SCANNER_HOME/bin/sonar-scanner -Dsonar.projectKey=10-Tier -Dsonar.ProjectName=10-Tier -Dsonar.java.binaries=.
17             ...
18           '''
19         }
20       }
21     }
22   }
}
```

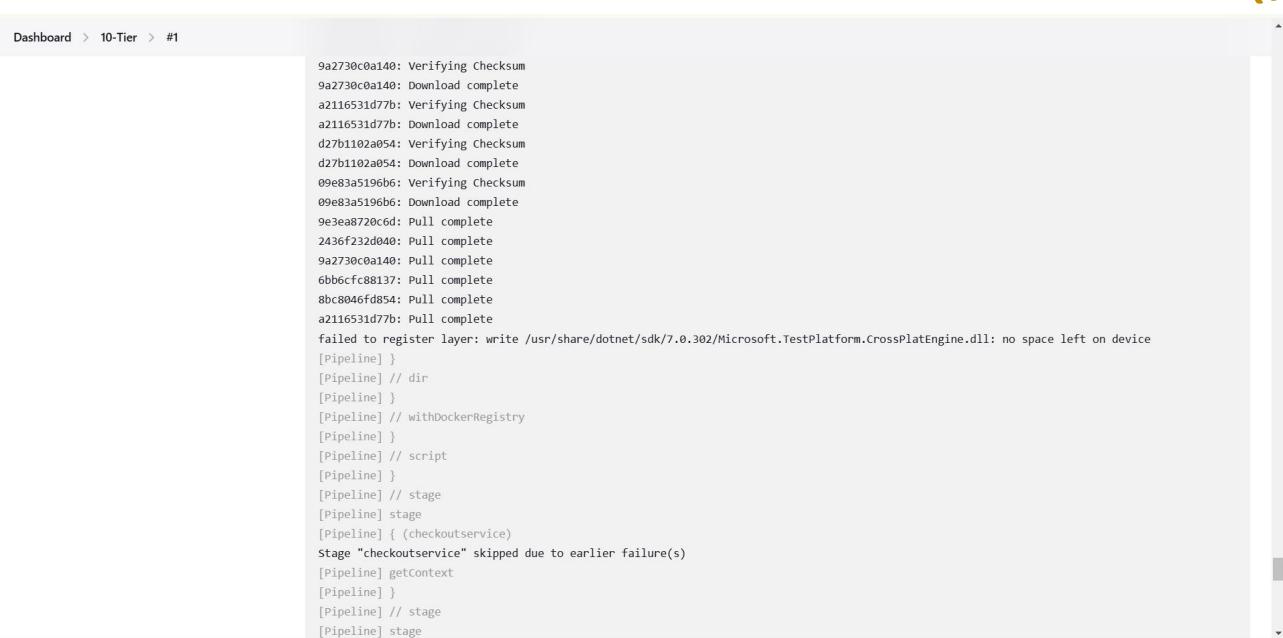
Kế tiếp sẽ sử dụng Docker để Containerize các service, sử dụng tài khoản đã lưu trước đó ở credentials của Jenkins.

```
23   stage('adservice'){
24     steps{
25       script{
26         withDockerRegistry(credentialsId: 'docker-cred', toolName: 'docker') {
27           dir('/var/lib/jenkins/workspace/10-Tier/src/adservice') {
28             sh 'docker build -t levi2708/adservice:latest .'
29             sh "docker push levi2708/adservice:latest"
30             sh "docker rmi levi2708/adservice:latest"
31           }
32         }
33       }
34     }
35   }
36
37   stage('cartservice'){
38     steps{
39       script{
40         withDockerRegistry(credentialsId: 'docker-cred', toolName: 'docker') {
41           dir('/var/lib/jenkins/workspace/10-Tier/src/cartservice/src') {
42             sh 'docker build -t levi2708/cartservice:latest .'
43             sh "docker push levi2708/cartservice:latest"
44             sh "docker rmi levi2708/cartservice:latest"
45           }
46         }
47       }
48     }
49   }
50
51   stage('checkoutservice'){
52     steps{
53       script{
54         withDockerRegistry(credentialsId: 'docker-cred', toolName: 'docker') {
55           dir('/var/lib/jenkins/workspace/10-Tier/src/checkoutservice/') {
56             sh 'docker build -t levi2708/checkoutservice:latest .'
57             sh "docker push levi2708/checkoutservice:latest"
58             sh "docker rmi levi2708/checkoutservice:latest"
59           }
50 }
```

Ở stage cuối cùng, nó sẽ deploy tài nguyên lên cụm EKS.

```
177   stage('K8-Deploy') {
178     steps {
179       script {
180         withKubeConfig(
181           caCertificate: '',
182           clusterName: 'my-eks2',
183           contextName: '',
184           credentialsId: 'k8s-token-webapps',
185           namespace: 'webapps',
186           restrictKubeConfigAccess: false,
187           serverUrl: 'eks-server-url'
188         ) {
189           sh 'kubectl apply -f deployment-service.yml'
190           sh 'kubectl get pods'
191           sh 'kubectl get svc'
192         }
193       }
194     }
195   }
196 }
197 }
```

Có vẻ như EC2 instance 'Jenkins Server' không đủ dung lượng để Docker có thể Containerize các Services của ứng dụng. Ta cần phải nâng dung lượng của nó.

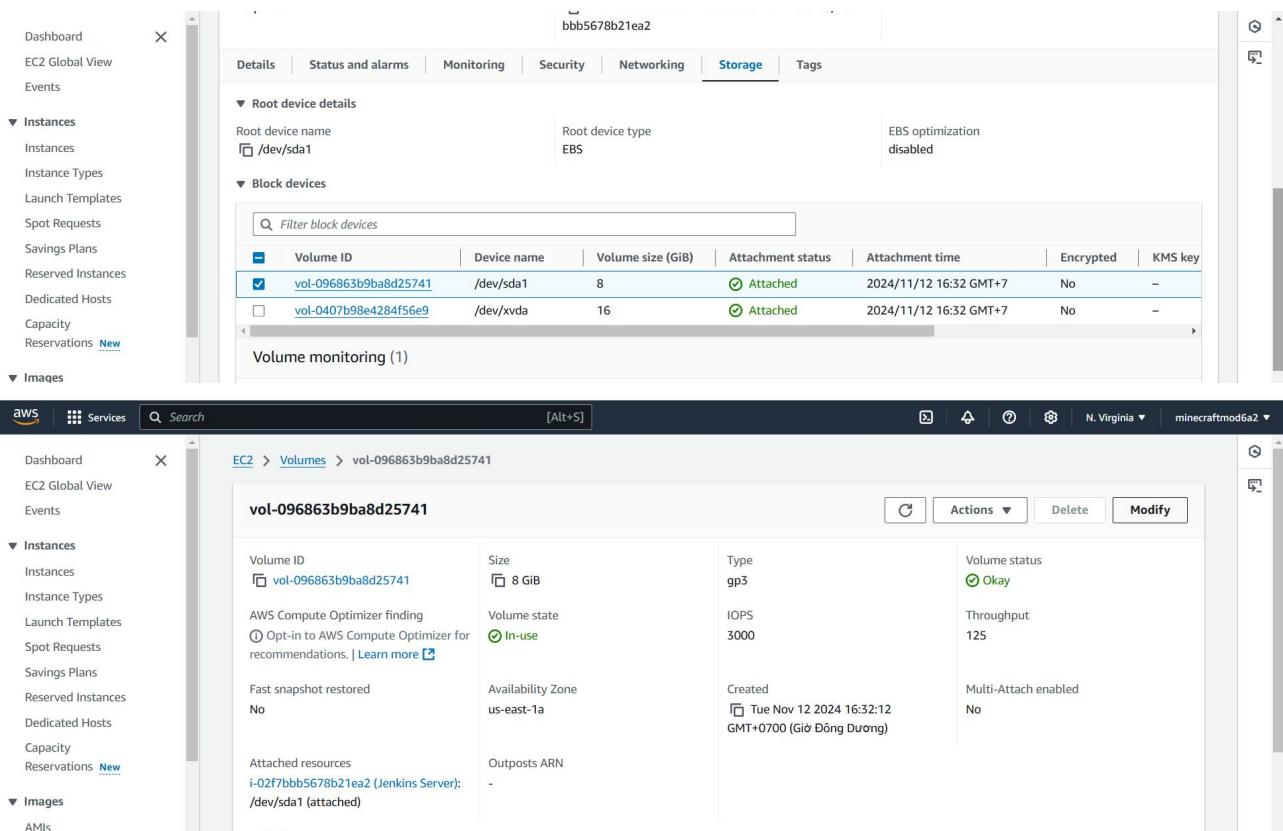


```

Dashboard > 10-Tier > #1
9a2730c0a140: Verifying Checksum
9a2730c0a140: Download complete
a2116531d77b: Verifying Checksum
a2116531d77b: Download complete
d27b1102a054: Verifying Checksum
d27b1102a054: Download complete
09e83a5196b6: Verifying Checksum
09e83a5196b6: Download complete
9e3ea8720c6d: Pull complete
2436f232d040: Pull complete
9a2730c0a140: Pull complete
6bb6cfc88137: Pull complete
8bc8046fd854: Pull complete
a2116531d77b: Pull complete
failed to register layer: write /usr/share/dotnet/sdk/7.0.302/Microsoft.TestPlatform.CrossPlatEngine.dll: no space left on device
[Pipeline]
[Pipeline] // dir
[Pipeline]
[Pipeline] // withDockerRegistry
[Pipeline]
[Pipeline] // script
[Pipeline]
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (checkoutservice)
Stage "checkoutservice" skipped due to earlier failure(s)
[Pipeline] getContext
[Pipeline]
[Pipeline] // stage
[Pipeline] stage

```

Vào Volume của Jenkins Server và nâng lên 16GB.



**Top Screenshot (Storage Tab):**

Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key
<a href="#">vol-096863b9ba8d25741</a>	/dev/sda1	8	Attached	2024/11/12 16:32 GMT+7	No	-
<a href="#">vol-0407b98e4284f56e9</a>	/dev/xvda	16	Attached	2024/11/12 16:32 GMT+7	No	-

**Bottom Screenshot (Volume Details):**

Volume ID	Size	Type	Volume status
<a href="#">vol-096863b9ba8d25741</a>	8 GiB	gp3	Okay
AWS Compute Optimizer finding	Volume state	IOPS	Throughput
<a href="#">Opt-in to AWS Compute Optimizer for recommendations.   Learn more</a>	In-use	3000	125
Fast snapshot restored	Availability Zone	Created	Multi-Attach enabled
No	us-east-1a	Tue Nov 12 2024 16:32:12 GMT+0700 (Giờ Đông Dương)	No
Attached resources	Outposts ARN		
<a href="#">i-02f7bbb5678b21ea2 (Jenkins Server): /dev/sda1 (attached)</a>	-		

## Bài thực hành số 02: Quản lý và triển khai hạ tầng AWS và ứng dụng microservices với Terraform, CloudFormation, GitHub Actions, AWS CodePipeline và Jenkins

The screenshot shows the AWS EC2 Modify volume interface. It displays the following details for a volume with ID vol-096863b9ba8d25741:

- Volume ID:** vol-096863b9ba8d25741
- Volume type:** General Purpose SSD (gp3)
- Size (GiB):** 16
- IOPS:** 3000
- Throughput (MiB/s):** 125

Sau đó gõ 2 câu lệnh này vào để mở rộng dung lượng.

```
ubuntu@ip-172-31-39-121:~$ sudo growpart /dev/nvme0n1 1
CHANGED: partition=1 start=2099200 old: size=14677983 end=16777182 new: size=31455199 end=33554398
ubuntu@ip-172-31-39-121:~$ sudo resize2fs /dev/nvme0n1p1
resize2fs 1.47.0 (5-Feb-2023)
Filesystem at /dev/nvme0n1p1 is mounted on /; on-line resizing required
old_desc_blocks = 1, new_desc_blocks = 2
The filesystem on /dev/nvme0n1p1 is now 3931899 (4k) blocks long.

ubuntu@ip-172-31-39-121:~$ |
```

Sau rất nhiều lần fail, Pipeline đã chạy thành công!

The Jenkins Pipeline Console shows the progress of Build #6. The pipeline stages are:

- git checkout
- SonarQube
- adservice
- cartservice
- checkoutservice
- currencyservice
- emailservice
- frontend
- loadgenerator
- paymentservice
- productcatalogservice
- recommendationservice
- shippingservice
- K8-Deploy** (highlighted in yellow)

The K8-Deploy stage details:

- Started 1 min 19 sec ago
- Queued 0 ms
- Took 2.3 sec
- Success
- View as plain text

The K8-Deploy stage tasks and their results:

Task	Type	Time
kubectl apply -f deployment-service.yml	Shell Script	1.6 sec
kubectl get pods	Shell Script	0.27 sec
kubectl get svc	Shell Script	0.27 sec

The kubectl get svc command output:

	NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
1	adservice	ClusterIP	10.100.17.251	<none>	9555/TCP	1s
2	cartservice	ClusterIP	10.100.37.220	<none>	7070/TCP	1s

# Bài thực hành số 02: Quản lý và triển khai hạ tầng AWS và ứng dụng microservices với Terraform, CloudFormation, GitHub Actions, AWS CodePipeline và Jenkins

35

Kết quả của SonarQube scan.

The screenshot shows the SonarQube interface for a project named "10-Tier". The top navigation bar includes "Projects", "Issues", "Rules", "Quality Profiles", "Quality Gates", "Administration", "Search for projects...", and "Create Project". The sidebar contains filters for Quality Gate (Passed: 1, Failed: 0), Reliability (A rating: 0, B rating: 0, C rating: 1, D rating: 0, E rating: 0), Security (Vulnerabilities: A rating: 0, B rating: 1, C rating: 0, D rating: 0, E rating: 0), and Security Review (Security Hotspots: A ≥ 80%: 0, B 70% - 80%: 0). The main dashboard displays the following metrics:

Metric	Value	Rating
Bugs	3	C
Vulnerabilities	1	B
Hotspots Reviewed	0.0%	E
Code Smells	1k	A
Coverage	0.0%	Red
Duplications	54.1%	Red
Lines	17k	M

A note states: "Embedded database should be used for evaluation purposes only. The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine." The bottom section shows the "Overview" tab selected, displaying the "QUALITY GATE STATUS" as "Passed" (All conditions passed) and various code quality measures:

Measure	Value	Rating
New Code	0 New Bugs	Reliability (A)
Overall Code	Started 2 hours ago	
New Vulnerabilities	0 New Vulnerabilities	Security (A)
New Security Hotspots	0 New Security Hotspots	Security Review (A)
Added Debt	0 Added Debt	Maintainability (A)
New Code Smells	0 New Code Smells	

## Bài thực hành số 02: Quản lý và triển khai hạ tầng AWS và ứng dụng microservices với Terraform, CloudFormation, GitHub Actions, AWS CodePipeline và Jenkins

**SonarQube Project Overview**

Passed  
All conditions passed.

Code Activity

Overall Code

3 Bugs (Reliability C)

1 Vulnerabilities (Security B)

8 Security Hotspots (0.0% Reviewed, Security Review E)

11d Debt (1k Code Smells, Maintainability A)

0.0% Coverage on 4.4k Lines to cover (Unit Tests)

54.1% Duplications on 17k Lines (22 Duplicated Blocks)

**Issues**

My Issues All

Filters

Issues in new code

- Type: Bug (3), Vulnerability (1), Code Smell (1k)
- Severity: Blocker (0), Critical (137), Major (87), Minor (803), Info (14)
- Scope: Resolution, Status, Security Category, Creation Date, Language, Rule

src/.../src/main/java/hipstershop/AdService.java

- Rename this field "MAX\_ADS\_TO\_SERVE" to match the regular expression "[a-zA-Z0-9]". (5 years ago, L46, convention)
- Replace this use of System.out or System.err by a logger. (4 years ago, L59, bad-practice, cert, owasp-a3)
- Replace this use of System.out or System.err by a logger. (6 years ago, L72, bad-practice, cert, owasp-a3)
- Remove this useless assignment to local variable "sleepTime". (6 years ago, L202, cert, cwe, unused)
- Remove this unused "sleepTime" local variable. (6 years ago, L202, unused)
- Remove this useless assignment to local variable "maxAttempts". (5 years ago, L203, cert, cwe, unused)
- Remove this unused "maxAttempts" local variable. (5 years ago, L203, unused)
- Complete the task associated to this TODO comment. (2 years ago, L205, cwe)

**Security Hotspots**

Assigned to me All

8 Security Hotspots to review

Review priority: MEDIUM

Permission (1)

Omitting "associate\_public\_ip\_address" allows network access from the Internet. Make sure it is safe here.

Weak Cryptography (6)

Review priority: LOW

Others (1)

8 of 8 shown

Status: To review Overall code

Security Hotspots Reviewed 0.0%

Omitting "associate\_public\_ip\_address" allows network access from the Internet. Make sure it is safe here.

Allowing public network access to cloud resources is security-sensitive. terraform:S6329

Status: TO REVIEW

This security hotspot needs to be reviewed to assess whether the code poses a risk.

Change status

Assignee: Not assigned

Where is the risk? What's the risk? Assess the risk How can I fix it?

terraform-file-for-jenkins/jenkins-server.tf

```

1 provider "aws" {
2   region = var.region
3 }
4
5 resource "aws_instance" "tf-jenkins-server" {
6   ami           = var.ami
7   instance_type = var.instance_type
8   key_name      = var.key_name
9   vpc_security_group_ids = [aws_security_group.tf-jenkins-sec-gr.id]
10  iam_instance_profile = aws_iam_instance_profile.tf-jenkins-server-profile.name
11
12  # Additional configuration...

```

Open in IDE Get Permalink

## Bài thực hành số 02: Quản lý và triển khai hạ tầng AWS và ứng dụng microservices với Terraform, CloudFormation, GitHub Actions, AWS CodePipeline và Jenkins

37

The screenshot shows the SonarQube interface for a '10-Tier' project. At the top, there's a navigation bar with links for Projects, Issues, Rules, Quality Profiles, Quality Gates, Administration, and a search bar. Below the navigation is a breadcrumb trail: 10-Tier / main. The main content area has tabs for Overview, Issues, Security Hotspots, Measures, Code (which is selected), and Activity.

**Risk Chart:** A bubble chart titled 'Risk' showing the relationship between Coverage (Y-axis, 0.0% to 80.0%) and Reliability (X-axis). The chart includes a legend for reliability ratings A through E. A large green circle at the top right represents 100% coverage and A-rated reliability.

**Code Metrics Table:** A table listing code metrics for various files and folders. The columns include Lines of Code, Bugs, Vulnerabilities, Code Smells, Security Hotspots, Coverage, and Duplications.

	Lines of Code	Bugs	Vulnerabilities	Code Smells	Security Hotspots	Coverage	Duplications
istio-manifests	73	0	0	0	0	—	0.0%
kubernetes-manifests	808	0	0	0	0	—	0.0%
kustomize	1,241	0	0	0	0	—	0.0%
release	732	0	0	0	0	—	0.0%
src	13,835	3	0	1,037	7	0.0%	66.9%
terraform-file-for-jenkins	107	0	1	0	1	—	0.0%
deployment-service.yml	660	0	0	0	0	—	0.0%

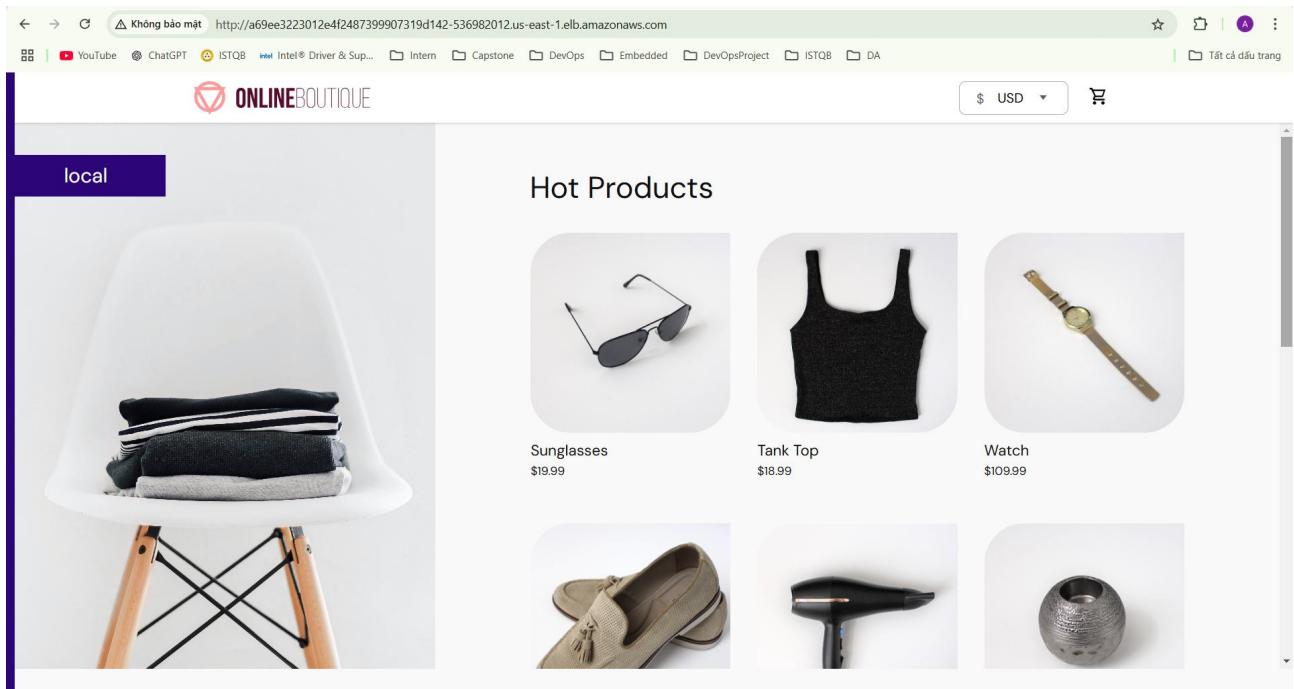
**Message Bar:** A yellow message bar at the bottom left states: 'Embedded database should be used for evaluation purposes only. The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine.'

Các pod của Kubernetes đã khởi tạo thành công.

```
ubuntu@ip-172-31-39-121:~$ kubectl get pods -n webapps
NAME                      READY   STATUS    RESTARTS   AGE
adservice-cdc698944-qrfw9   1/1    Running   0          3m
cartservice-6c46b9c7-nnb6l   1/1    Running   0          3m1s
checkoutservice-865b6987c6-nmbqf  1/1    Running   0          3m1s
currencyservice-76f9fc4456-dvvd4  1/1    Running   0          3m1s
emailservice-5c49dbbdd-gltjb   1/1    Running   0          3m1s
frontend-778ccfbff6-wqtbj   1/1    Running   0          3m1s
loadgenerator-655775b8b9-27mz6  1/1    Running   0          3m1s
paymentservice-cbd7cf6d8-45hbv  1/1    Running   0          3m1s
productcatalogservice-74658489bd-bn4cv  1/1    Running   0          3m1s
recommendationservice-5f4b894698-5f654  1/1    Running   0          3m1s
redis-cart-7d84f59b65-tnpqf   1/1    Running   0          3m
shippingservice-fb8fb7df8-n9zt7   1/1    Running   0          3m1s
ubuntu@ip-172-31-39-121:~$ |
```

```
ubuntu@ip-172-31-39-121:~$ kubectl get svc -n webapps
NAME           TYPE      CLUSTER-IP   EXTERNAL-IP
adservice      ClusterIP 10.100.17.251 <none>
cartservice    ClusterIP 10.100.27.229 <none>
checkoutservice ClusterIP 10.100.104.214 <none>
currencieservice ClusterIP 10.100.130.101 <none>
emailservice   ClusterIP 10.100.149.93 <none>
frontend       NodePort   10.100.31.65 <none>
frontend-external LoadBalancer 10.100.222.210 a69ee3223012e4f2487399907319d142-536982012.us-east-1.elb.amazonaws.com
paymentservice  ClusterIP 10.100.187.130 <none>
productcatalogservice ClusterIP 10.100.133.249 <none>
recommendationservice ClusterIP 10.100.58.138 <none>
redis-cart     ClusterIP 10.100.245.175 <none>
shippingservice ClusterIP 10.100.25.103 <none>
ubuntu@ip-172-31-39-121:~$ |
```

Ta có thể truy cập thông qua LoadBalancer IP.



Để tích hợp Trivy scan vào Pipeline, ta thêm các câu lệnh dưới đây vào từng services, nó sẽ được lưu lại ở Jenkins Server.

Đối với adservice.

```
23     stage('adservice'){
24         steps{
25             script{
26                 withDockerRegistry(credentialsId: 'docker-cred', toolName: 'docker') {
27                     dir('/var/lib/jenkins/workspace/10-Tier/src/adservice') {
28                         sh 'docker build -t levi2708/adservice:latest .'
29
30                         sh '''
31                             trivy image levi2708/adservice:latest > trivy_adservice_report.txt || true
32                             cat trivy_adservice_report.txt
33                         '''
34
35                         sh "docker push levi2708/adservice:latest"
36                         sh "docker rmi levi2708/adservice:latest"
37                     }
38                 }
39             }
40         }
41     }
```

Đối với cartservice và tương tự các service khác.

```

43     stage('cartservice'){
44         steps{
45             script{
46                 withDockerRegistry(credentialsId: 'docker-cred', toolName: 'docker') {
47                     dir('/var/lib/jenkins/workspace/10-Tier/src/cartservice/src/'){
48                         sh 'docker build -t levi2708/cartservice:latest .'
49
50                         sh '''
51                             trivy image levi2708/carservice:latest > trivy_carservice_report.txt || true
52                             cat trivy_carservice_report.txt
53                         '''
54
55                         sh "docker push levi2708/cartservice:latest"
56                         sh "docker rmi levi2708/cartservice:latest"
57                     }
58                 }
59             }
60         }
61     }
62 }
```

### Output của Trivy scan.

```

ubuntu@ip-172-31-39-121:/var/lib/jenkins/workspace/10-Tier/src$ cd currencyservice
ubuntu@ip-172-31-39-121:/var/lib/jenkins/workspace/10-Tier/src/currencyservice$ ls
Dockerfile client.js data genproto.sh package-lock.json package.json proto server.js trivy_currencyservice_report.txt
ubuntu@ip-172-31-39-121:/var/lib/jenkins/workspace/10-Tier/src/currencyservice$ cat trivy_currencyservice_report.txt

For OSS Maintainers: VEX Notice
-----
If you're an OSS maintainer and Trivy has detected vulnerabilities in your project that you believe are not actually exploitable, consider issuing a VEX (Vulnerability Exploitability eXchange) statement.
VEX allows you to communicate the actual status of vulnerabilities in your project, improving security transparency and reducing false positives for your users.
Learn more and start using VEX: https://aquasecurity.github.io/trivy/v0.57/docs/supply-chain/vex/repo#publishing-vex-documents

To disable this notice, set the TRIVY_DISABLE_VEX_NOTICE environment variable.

levi2708/currencyservice:latest (alpine 3.17.3)
=====
Total: 44 (UNKNOWN: 0, LOW: 4, MEDIUM: 38, HIGH: 2, CRITICAL: 0)



| Library | Vulnerability  | Severity | Status | Installed Version | Fixed Version                                                                                                                                        | Title                                                                                                                                 |
|---------|----------------|----------|--------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| busybox | CVE-2023-42363 | MEDIUM   | fixed  | 1.35.0-r29        | 1.35.0-r31                                                                                                                                           | busybox: use-after-free in awk<br><a href="https://avd.aquasec.com/nvd/cve-2023-42363">https://avd.aquasec.com/nvd/cve-2023-42363</a> |
|         | CVE-2023-42364 |          |        |                   |                                                                                                                                                      | busybox: use-after-free<br><a href="https://avd.aquasec.com/nvd/cve-2023-42364">https://avd.aquasec.com/nvd/cve-2023-42364</a>        |
|         | CVE-2023-42365 |          |        |                   |                                                                                                                                                      | busybox: use-after-free<br><a href="https://avd.aquasec.com/nvd/cve-2023-42365">https://avd.aquasec.com/nvd/cve-2023-42365</a>        |
|         | CVE-2023-42366 |          |        |                   | 1.35.0-r30<br>busybox: A heap-buffer-overflow<br><a href="https://avd.aquasec.com/nvd/cve-2023-42366">https://avd.aquasec.com/nvd/cve-2023-42366</a> |                                                                                                                                       |
|         | busybox-binsh  |          |        |                   | CVE-2023-42363                                                                                                                                       | 1.35.0-r31                                                                                                                            |
|         | CVE-2023-42364 |          |        |                   |                                                                                                                                                      | busybox: use-after-free                                                                                                               |


```

```

ubuntu@ip-172-31-39-121:/var/lib/jenkins/workspace/10-Tier/src$ cd frontend
ubuntu@ip-172-31-39-121:/var/lib/jenkins/workspace/10-Tier/src/frontend$ ls
Dockerfile deployment_details.go genproto.sh go.sum main.go money static trivy_frontend_report.txt
README.md genproto.go.mod handlers.go middleware.go rpc.go templates
ubuntu@ip-172-31-39-121:/var/lib/jenkins/workspace/10-Tier/src/frontend$ cat trivy_frontend_report.txt

For OSS Maintainers: VEX Notice
-----
If you're an OSS maintainer and Trivy has detected vulnerabilities in your project that you believe are not actually exploitable, consider issuing a VEX (Vulnerability Exploitability eXchange) statement.
VEX allows you to communicate the actual status of vulnerabilities in your project, improving security transparency and reducing false positives for your users.
Learn more and start using VEX: https://aquasecurity.github.io/trivy/v0.57/docs/supply-chain/vex/repo#publishing-vex-documents

To disable this notice, set the TRIVY_DISABLE_VEX_NOTICE environment variable.

levi2708/frontend:latest (alpine 3.18.0)
=====
Total: 45 (UNKNOWN: 0, LOW: 4, MEDIUM: 36, HIGH: 2, CRITICAL: 3)



| Library | Vulnerability  | Severity | Status | Installed Version | Fixed Version  | Title                                                                                                                                                                                   |           |
|---------|----------------|----------|--------|-------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| busybox | CVE-2022-48174 | CRITICAL | fixed  | 1.36.0-r9         | 1.36.1-r1      | busybox: stack overflow vulnerability in ash.c leads to arbitrary code execution<br><a href="https://avd.aquasec.com/nvd/cve-2022-48174">https://avd.aquasec.com/nvd/cve-2022-48174</a> |           |
|         | CVE-2023-42363 |          |        |                   |                | MEDIUM                                                                                                                                                                                  | 1.36.1-r7 |
|         |                |          |        |                   | CVE-2023-42364 |                                                                                                                                                                                         |           |


```