



# LAB: Deploying a Website on AWS EC2

NGUYEN CONG LUC

[nguyencongluc.82@gmail.com](mailto:nguyencongluc.82@gmail.com)

[Luc Nguyen | LinkedIn](#)

0329206845

## MỤC LỤC

<i>Phần 1. Tạo Cloud Server .....</i>	<i>3</i>
<b>1.1 Yêu cầu.....</b>	<b>3</b>
<b>1.2 Tạo Cloud VPS với EC2 của AWS.....</b>	<b>3</b>
<b>1.3 Gắn Elastic IP cho VPS để có Ipv4 cố định.....</b>	<b>10</b>
<b>1.4 Cấu hình để SSH.....</b>	<b>17</b>
1.4.1 SSH với file .pem .....	17
1.4.2 SSH với public key .....	20
<i>Phần 2. Cấu hình để gửi source code web từ client qua server.....</i>	<i>23</i>
<b>2.1 Yêu cầu.....</b>	<b>23</b>
<b>2.2 Tạo user, thư mục cho user và phân quyền.....</b>	<b>23</b>
<b>2.3 Cấu hình để gửi source code web từ client qua server.....</b>	<b>24</b>
2.3.1 Tìm hiểu về FTP, FTPS và SFTP .....	24
2.3.2 Sử dụng SFTP(Nên dùng) .....	24
2.3.3 Sử dụng FTP (Không nên dùng vì không mã hóa file).....	31
2.3.4 Tiến hành upload source code lên server(Áp dụng SFTP để bảo mật).....	34
<i>Phần 3. Cài đặt Web server Apache, DNS Record và Deploy website .....</i>	<i>35</i>
<b>3.1 Cấu hình DNS Record .....</b>	<b>35</b>
<b>3.2 Cài đặt Apache Server.....</b>	<b>35</b>
<b>3.3 Tạo VirtualHost cho user nguyencongluc .....</b>	<b>36</b>
<b>3.4 Kiểm tra website đã deploy .....</b>	<b>37</b>
<i>Phần 4. Thêm SSL cho trang web.....</i>	<i>38</i>
<b>4.1 Cài đặt Cerrbot và lấy chứng chỉ SSL .....</b>	<b>38</b>
<b>4.2 Kiểm tra SSL trên website .....</b>	<b>39</b>

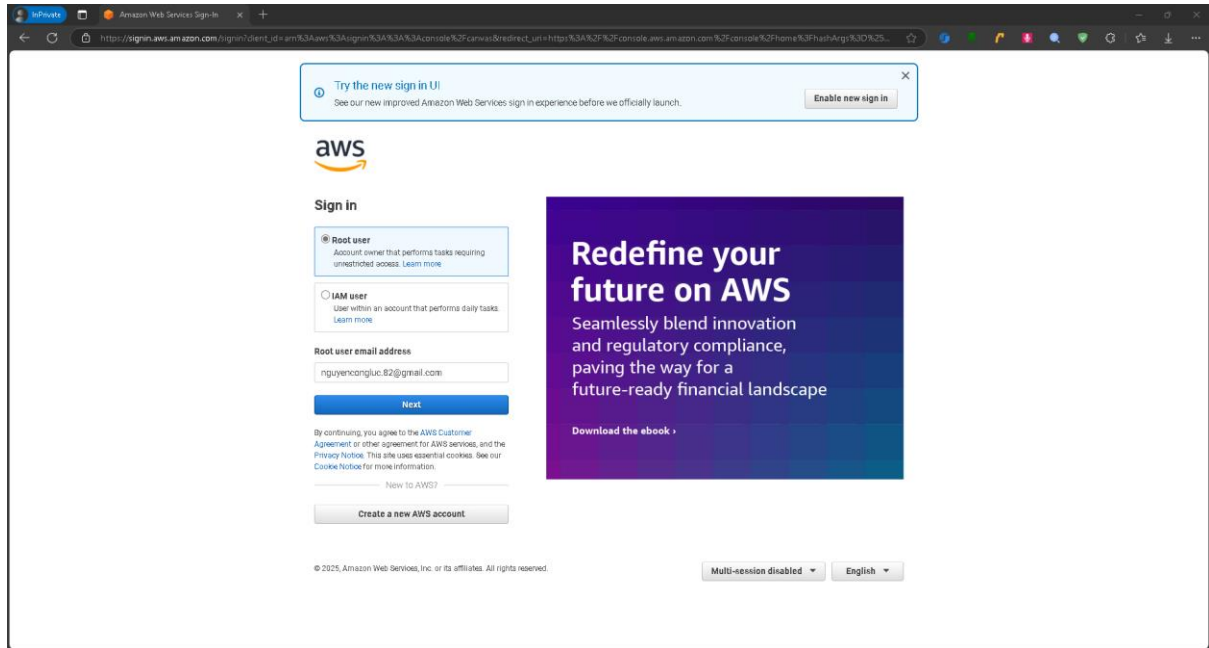
# Phần 1. Tạo Cloud Server

## 1.1 Yêu cầu

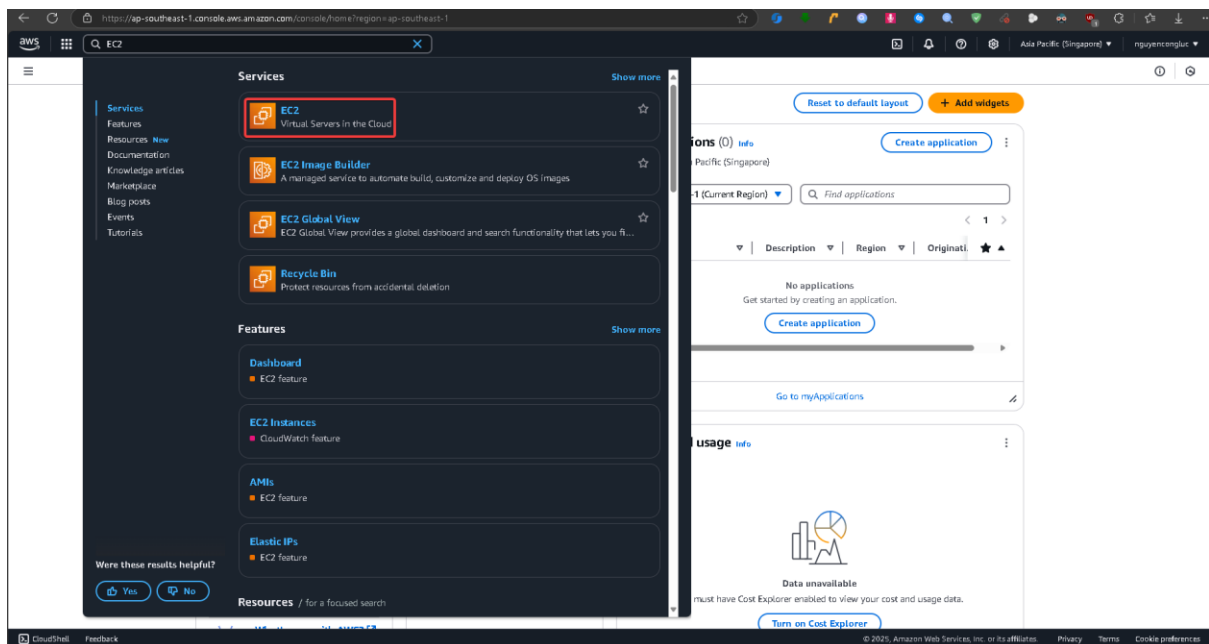
- Tạo VPS Ubuntu để lưu trữ source code

## 1.2 Tạo Cloud VPS với EC2 của AWS

- EC2 là 1 Amazon Web Services, cho phép người dùng thuê máy tính ảo để chạy các ứng dụng máy tính của riêng họ với khả năng nâng cấp rất dễ dàng trên cloud
- Login với user root và email



- Search từ khóa EC2



## - Æn launch instance

The screenshot shows the AWS Management Console for the Asia Pacific (Singapore) region. The left sidebar contains navigation links for EC2 resources. The main content area displays the 'Launch instance' button, which is highlighted with a red box. Other visible elements include the 'Resources' section showing a table of EC2 resources, the 'Service health' section indicating that the service is operating normally, and the 'Account attributes' section showing the default VPC and settings. The 'Launch instance' button is located under the 'Launch instance' section, which also includes a 'Migrate a server' button.

## - Đặt tên cho instance, chọn OS và instance type, ưu tiên chọn các lựa chọn free:

The screenshot shows the 'Launch instance' wizard in the AWS Management Console. The 'Name and tags' section has a text input field for the instance name, which is highlighted with a red box. The 'Application and OS Images (Amazon Machine Image)' section shows a list of AMIs, with 'Ubuntu Server 24.04 LTS (HVM), EBS General Purpose (SSD) Volume Type' selected and highlighted with a red box. The 'Instance type' section shows a list of instance types, with 't2.micro' selected and highlighted with a red box. The 'Summary' section on the right shows the configuration details, including the instance name, AMI, instance type, and storage. A 'Free tier eligible' badge is visible next to the selected AMI and instance type. The 'Launch instance' button is highlighted with a red box.

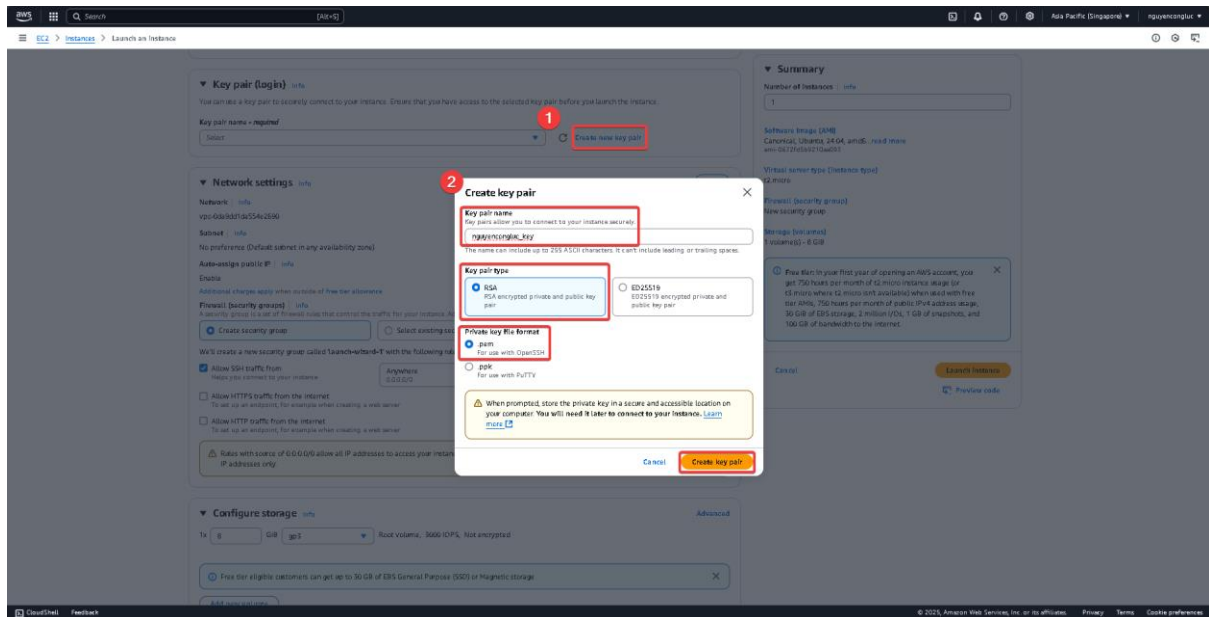
- Tạo key pair để SSH từ xa:

Key pair name: Tên file key

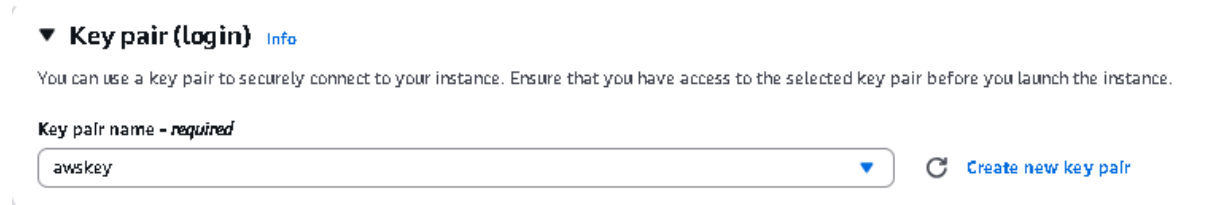
Key pair type: Nên chọn RSA

Privated key file format: để sử dụng ssh qua openssh, sử dụng format .pem

Sau khi chọn Create key pair->Trình duyệt sẽ tự download file .pem về máy, và chỉ cho phép download 1 lần duy nhất, nếu như lỡ xóa file pem cần phải tạo file pem mới và cài lại theo hướng dẫn phần 1.4 SSH



Có thể tạo nhiều key tên khác nhau (nguyenconglac\_key, awskey,...) và chọn key mình thích



- Cấu hình network settings, có thể để mặc định

▼ Network settings

Info

VPC - required

Info

vpc-0da9dd1da554e2690

172.31.0.0/16

(default)

↻

Subnet

Info

No preference

↕

↻ Create new subnet

Auto-assign public IP

Info

Enable

↕

Additional charges apply

when outside of free tier allowance

Firewall (security groups)

Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group

☐ Select existing security group

Security group name - required

launch-wizard-1

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_-./!@#\$%^&\*~

Description - required

Info

launch-wizard-1 created 2025-03-08T02:02:08.726Z

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Remove

Type

Info

ssh

↕

Protocol

Info

TCP

Port range

Info

22

Source type

Info

Anywhere

↕

Source

Info

🔍 Add CIDR, prefix list or security group

0.0.0.0/0

✕

Description - optional

Info

e.g. SSH for admin desktop

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

✕

Add security group rule

▼ Network settings

Info

Network

Info

vpc-0da9dd1da554e2690

Subnet

Info

No preference (Default subnet in any availability zone)

Auto-assign public IP

Info

Enable

Additional charges apply

when outside of free tier allowance

Firewall (security groups)

Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group

☐ Select existing security group

We'll create a new security group called 'launch-wizard-1' with the following rules:

☒ Allow SSH traffic from

Helps you connect to your instance

Anywhere

0.0.0.0/0

↕

☒ Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

☒ Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

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

✕

Edit

- Trong Configure storage tăng dung lượng volume thành max 30GB nếu như không sử dụng Cloud server nào khác

▼ **Configure storage** [Info](#)

1x

GiB

▼

Root volume, 3000 IOPS, Not encrypted

❗

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

×

Add new volume

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

🔄

Click refresh to view backup information

↻

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

[Edit](#)

- Trong phần Advanced details để mặc định

### ▼ **Advanced details** [Info](#)

- Check summary sau đó chọn launch instance:

▼ **Summary**

Number of instances

[Info](#)

Software image (AMI)

Canonical, Ubuntu, 24.04, amd64...[read more](#)

ami-0672fd5b9210a3d93

Virtual server type (Instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 30 GiB

❗

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

×

[Cancel](#)

Launch Instance

📄

[Preview code](#)

Chú ý Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

750 giờ/tháng sử dụng instance t2.micro (hoặc t3.micro nếu t2.micro không khả dụng) với AMI(amazon machine image) miễn phí.

750 giờ/tháng sử dụng địa chỉ IPv4 công khai, không đc dùng IP mà không gắn instance.

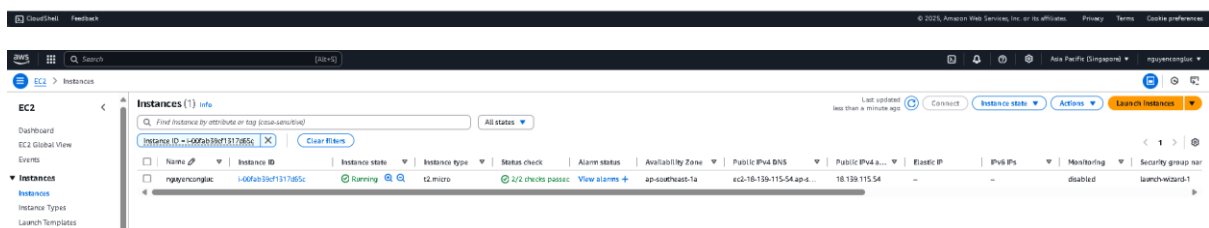
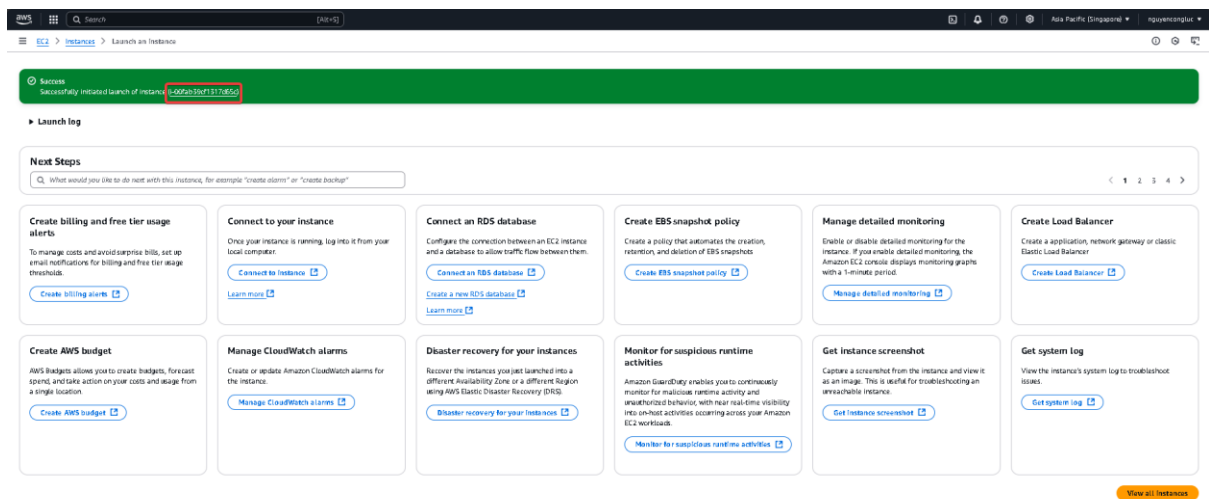
30 GB lưu trữ EBS (gp2/gp3).

2 triệu I/O trên EBS (Các thao tác thêm xóa sửa xuất trong server)

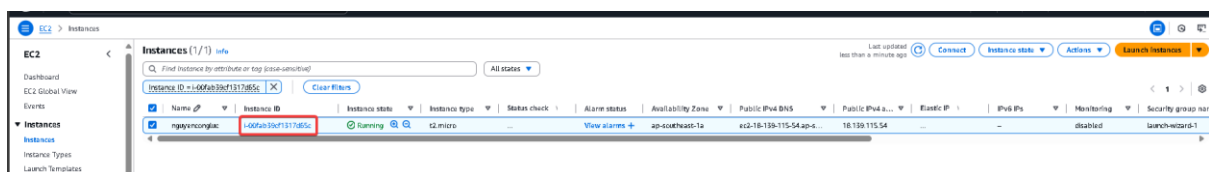
1 GB dung lượng snapshot.

100 GB băng thông ra ngoài internet.

- Đã tạo thành công



- Tiến hành truy cập server:





Instance summary for i-00fab39cf1317d65c (nguyencongluc) info

Updated less than a minute ago

Instance ID: i-00fab39cf1317d65c

Public IPv4 address: 18.139.115.54 | open address

Instance state: Running

Private IP DNS name (IPv4 only): ip-172-31-27-54-ap-southeast-1-compute.internal

Instance type: c2.micro

VPC ID: vpc-669808106554e269c

Subnet ID: subnet-679af1556e4babf5

Instance ASN: amazon-aws-i2-ap-southeast-1-46932545792 instance/i-00fab39cf1317d65c

Private IPv4 address: 172.31.27.54

Public IPv4 DNS: ip-18-139-115-54-ap-southeast-1-compute.amazonaws.com | open address

Elastic IP address: -

AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Auto Scaling Group name: -

Managed: false

Connect to Instance info

Connect to your instance i-00fab39cf1317d65c (nguyencongluc) using any of these options:

EC2 Instance Connect | Session Manager | SSH client | EC2 serial console

Instance ID: i-00fab39cf1317d65c (nguyencongluc)

Connection Type:

☒ Connect using EC2 Instance Connect  
Connect using the EC2 Instance Connect browser-based client, with a public (IPv4 or IPv6) address.

☐ Connect using EC2 Instance Connect Endpoint  
Connect using the EC2 Instance Connect browser-based client, with a private (IPv4 address and a VPC endpoint).

Public IPv4 address: 18.139.115.54

IPv6 address: -

Username: ubuntu

Note: In most cases, the default username, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

Cancel | Connect

CloudShell | Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. | Privacy | Terms | Cookie preferences

aws | Search | [Alt+S] | Asia Pacific (Singapore) | nguyencongluc

```
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1024-aws x86_64)

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

System information as of Mon Mar 17 07:25:28 UTC 2025

System load:  0.08          Processes:    112
Usage of /:   8.1% of 28.02GB Users logged in: 2
Memory usage: 22%          IPv4 address for enX0: 172.31.27.54
Swap usage:   0%

* Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.
  https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.
99 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

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

Last login: Mon Mar 17 06:39:04 2025 from 27.64.59.225
ubuntu@ip-172-31-27-54:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enX0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:05:89:ac:59:7b brd ff:ff:ff:ff:ff:ff
    inet 172.31.27.54/20 metric 100 brd 172.31.31.255 scope global dynamic enX0
        valid_lft 2794sec preferred_lft 2794sec
    inet6 fe80::51:89ff:feac:597b/64 scope link
        valid_lft forever preferred_lft forever
ubuntu@ip-172-31-27-54:~$ curl ifconfig.io
18.141.58.92
ubuntu@ip-172-31-27-54:~$ |
```

i-00fab39cf1317d65c (nguyencongluc)  
PublicIPs: 18.141.58.92 PrivateIPs: 172.31.27.54

### 1.3 Gắn Elastic IP cho VPS để có Ipv4 cố định

- Mặc định EC2 Instance sẽ có IP V4 động và IP sẽ bị thay đổi mỗi khi shutdown máy.

Vậy nên nếu cần IP cố định cho Instance thì tạo thêm Elastic IP để gắn thêm tuy nhiên sẽ tốn phí theo h nếu mua riêng, chỉ free khi tạo và gắn kèm vào Instance đang có Free Tier. Quá trình tạo và gắn phải thực hiện nhanh bởi nếu tạo mà không gắn vào instance free đã tạo thì cũng đã bị tính phí theo giờ rồi.

- Để tạo Elastic IP address vào Network & Security->Elastic IPs-> Allocate Elastic IP address

The screenshot displays the AWS Management Console interface for Elastic IP addresses. The left-hand navigation pane shows the 'Network & Security' section expanded, with 'Elastic IPs' selected and marked with a red circle containing the number '1'. The main content area is titled 'Elastic IP addresses' and features a search bar with the placeholder text 'Find resources by attribute or tag'. Below the search bar, a table header is visible with columns for 'Name', 'Allocated IPv4 addr...', and 'Type'. The table currently shows 'No Elastic IP addresses found in this Region'. A red circle with the number '2' highlights the 'Allocate Elastic IP address' button in the top right corner. At the bottom of the console, a notification banner suggests viewing IP address usage and recommendations to release unused IPs with a link to 'Public IP insights'.

- Allocate theo các giá trị mặc định đề xuất:

aws

Search

[Alt+S]

Asia Pacific (Singapore)

nguyencongluc

EC2 > Elastic IP addresses > Allocate Elastic IP address

Allocate Elastic IP address

Elastic IP address settings

Public IPv4 address pool

☒ Amazon's pool of IPv4 addresses

☐ Public IPv4 address that you bring to your AWS account with BYOIP. (option disabled because no pools found) [Learn more](#)

☐ Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. (option disabled because no customer owned pools found) [Learn more](#)

☐ Allocate using an IPv4 IPAM pool (option disabled because no public IPv4 IPAM pools with AWS service as EC2 were found)

Network border group

ap-southeast-1

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. [Learn more](#)

Create accelerator

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags

Cancel

Allocate

CloudShell

Feedback

Privacy

Terms

Cookie preferences

© 2025, Amazon Web Services, Inc. or its affiliates.

- IPv4 sẽ xuất hiện khi tạo thành công:

aws [Search] [Alt+S] Asia Pacific (Singapore) nguyentongluc

EC2

- Dashboard
- EC2 Global View
- Events

▼ Instances

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

▼ Images

- AMIs
- AMI Catalog

▼ Elastic Block Store

- Volumes
- Snapshots
- Lifecycle Manager

▼ Network & Security

- Security Groups
- Elastic IPs**
- Placement Groups
- Key Pairs
- Network Interfaces

▼ Load Balancing

- Load Balancers
- Target Groups
- Trust Stores

▼ Auto Scaling

- Auto Scaling Groups

Settings

✓ Elastic IP address allocated successfully.  
Elastic IP address 52.77.48.176

Associate this Elastic IP address

Elastic IP addresses (1)

Find resources by attribute or tag

Public IPv4 address : 52.77.48.176 Clear filters

<input type="checkbox"/>	Name	Allocated IPv4 address	Type	Allocation ID
<input type="checkbox"/>	-	52.77.48.176	Public IP	eipalloc-0d4934

View IP address usage and recommendations to release unused IPs with [Public IP insights](#)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- Nếu muốn chọn IP đẹp, dễ nhớ thì có thể xóa rồi tạo lại, tuy nhiên theo thời điểm làm lab này thì EC2 chỉ cấp cho 3 IP khác nhau cho dù random có nhiều lần hơn nữa.

- Chỉnh sửa lại Name IP nếu cần để phân biệt với nhiều IP khác (EC2 cho phép tạo tối đa 5 Elastic IPs) và click vào đây IP để vào cài đặt:

## Elastic IP addresses (1/1)

Find resources by attribute or tag			
<input checked="" type="checkbox"/>	Name	Allocated IPv4 addr...	Type
<input checked="" type="checkbox"/>	IP Instance NguyenCongLuc	52.77.48.176	Public IP

- Click vào Associate Elastic IPaddress để gắn Instance

aws

Search

[Alt+S]

Asia Pacific (Singapore)

nguyencongluc

EC2 > Elastic IP addresses > 52.77.48.176

EC2

Dashboard

EC2 Global View

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Load Balancing

Load Balancers

Target Groups

Trust Stores

52.77.48.176

Actions

Associate Elastic IP address

Summary

Allocated IPv4 address

52.77.48.176

Allocation ID

eipalloc-08640f163c6fb3c38

Association ID

-

Associated instance ID

-

Network interface ID

-

Public DNS

-

Address pool

Amazon

Type

Public IP

Reverse DNS record

-

Scope

VPC

Private IP address

-

Network interface owner account ID

-

NAT Gateway ID

-

Network border group

ap-southeast-1

Tags(1)

Manage tags

Key

Value

Name

IP Instance NguyenCongLuc

CloudShell

Feedback

Privacy

Terms

Cookie preferences

© 2025, Amazon Web Services, Inc. or its affiliates.

- Chọn Resource type là Instance (Lưu ý: Nếu liên kết Elastic IP với một Instance đã có Elastic IP được liên kết, Elastic IP được liên kết trước đó sẽ bị hủy liên kết, nhưng địa chỉ cũ đó vẫn sẽ được phân bổ cho tài khoản (Vẫn sẽ tính phí)

)

aws

Search

[Alt+S]

Asia Pacific (Singapore)

nguyencongluc

[EC2](#) > [Elastic IP addresses](#) > [52.77.48.176](#) > Associate Elastic IP address

### Associate Elastic IP address

Choose the instance or network interface to associate to this Elastic IP address (52.77.48.176)


**Elastic IP address: 52.77.48.176**

**Resource type**  
Choose the type of resource with which to associate the Elastic IP address.  
☒ Instance  
☐ Network interface

**⚠**

If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. [Learn more](#)

If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address. [↗](#)

**Instance**  
 

**Private IP address**  
The private IP address with which to associate the Elastic IP address.

**Reassociation**  
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.  
☐ Allow this Elastic IP address to be reassociated

[Cancel](#) [Associate](#)

CloudShell [Feedback](#)

[Privacy](#) [Terms](#) [Cookie preferences](#)

© 2025, Amazon Web Services, Inc. or its affiliates.

- Trong Instance chọn ID đã có sẵn:

**Instance**

Q i-00fab39cf1317d65c X

i-00fab39cf1317d65c (nguyencongluc) - running

- Và chọn Privated Ip đã có sẵn:

**Private IP address**  
The private IP address with which to associate the Elastic IP address.

Q 172.31.27.54 X

172.31.27.54

- Ấn Associate để hoàn tất

aws Search [Alt+S] Asia Pacific (Singapore) nguyencongluc

EC2 > Elastic IP addresses > 52.77.48.176 > Associate Elastic IP address

**Associate Elastic IP address**  
Choose the instance or network interface to associate to this Elastic IP address (52.77.48.176)

**Elastic IP address: 52.77.48.176**

**Resource type**  
Choose the type of resource with which to associate the Elastic IP address.

☒ Instance  
☐ Network interface

**Instance**  
Q i-00fab39cf1317d65c X

**Private IP address**  
The private IP address with which to associate the Elastic IP address.  
Q 172.31.27.54 X

**Reassociation**  
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.

☐ Allow this Elastic IP address to be reassociated

Cancel Associate

- Kết quả thành công:

EC2

Dashboard

EC2 Global View

Events

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Load Balancing

Load Balancers

Target Groups

Trust Stores

Elastic IP addresses

52.77.48.176

Elastic IP address associated successfully.  
Elastic IP address 52.77.48.176 has been associated with instance i-00fab39cf1317d65c.

52.77.48.176

Actions

Associate Elastic IP address

Summary

Allocated IPv4 address  
52.77.48.176

Allocation ID  
eipalloc-08640f163c6fb3c38

Association ID  
eipassoc-070f0c2c9bc6eac94

Associated instance ID  
i-00fab39cf1317d65c

Network interface ID  
eni-0eb607b09e3579bdd

Public DNS  
ec2-52-77-48-176.ap-southeast-1.compute.amazonaws.com

Address pool  
Amazon

Type  
Public IP

Reverse DNS record  
-

Scope  
VPC

Private IP address  
172.31.27.54

Network interface owner account ID  
469232545782

NAT Gateway ID  
-

Network border group  
ap-southeast-1

Tags(1)

Manage tags

1

Key | Value

Name | IP Instance NguyenCongLuc

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy Terms Cookie preferences

- Kiểm tra trong Instance và thấy đã cập nhật Public IPv4 là 52.77.48.176:

EC2

Dashboard

EC2 Global View

Events

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Load Balancing

Load Balancers

Target Groups

Trust Stores

Instances (1/1)

Last updated less than a minute ago

Connect

Instance state

Actions

Launch instances

Find Instance by attribute or tag (case-sensitive)

All states

1

2

nguyencongluc

i-00fab39cf1317d65c

Running

t2.micro

2

i-00fab39cf1317d65c (nguyencongluc)

Details

Status and alarms

Monitoring

Security

Networking

Instance summary

Instance ID  
i-00fab39cf1317d65c

IPv6 address  
-

Hostname type  
IP name: ip-172-31-27-54.ap-southeast-1.compute.internal

Public IPv4 address  
52.77.48.176 open address

Instance state  
Running

Private IP DNS name (IPv4 only)  
ip-172-31-27-54.ap-southeast-1.compute.internal

Private IPv4 addresses  
172.31.27.54

Public IPv4 DNS  
ec2-52-77-48-176.ap-southeast-1.compute.amazonaws.com open address

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy Terms Cookie preferences



- Ngoài ra có thể check tại terminal và thấy được kết quả:

```
aws [Alt+S] [Search] [Settings] Asia Pacific (Singapore) nguyencongluc

Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1024-aws x86_64)

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

System information as of Mon Mar 24 07:12:37 UTC 2025

System load:  0.08      Processes:      105
Usage of /:   8.4% of 28.02GB   Users logged in: 0
Memory usage: 23%      IPv4 address for enx0: 172.31.27.54
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

102 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

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

Last login: Mon Mar 24 07:13:05 2025 from 3.0.5.36
ubuntu@ip-172-31-27-54:~$ curl ifconfig.io
52.77.48.176
```

## 1.4 Cấu hình để SSH

### 1.4.1 SSH với file .pem

- Sử dụng file pem mà trình duyệt đã tự động tải xuống sau khi thêm key pair để SSH, AWS chỉ cho phép 1 user duy nhất có quyền truy cập vào file .pem để ssh. Vì thế cần đảm bảo file .pem chỉ có 1 user sử dụng, nếu không sẽ có lỗi như ảnh (Bản chất file .pem vẫn là 1 private key)

```
C:\Users\Nguyen Cong Luc>ssh -i "C:\Users\Nguyen Cong Luc\.ssh\awskey.pem" ubuntu@ec2-18-139-115-54.ap-southeast-1.compute.amazonaws.com
Bad permissions. Try removing permissions for user: UNKNOWN\UNKNOWN (S-1-5-21-772653804-3857895930-4180330516-1027) on file C:/Users/Nguyen
Cong Luc/.ssh/awskey.pem.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: UNPROTECTED PRIVATE KEY FILE!
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions for 'C:\Users\Nguyen Cong Luc\.ssh\awskey.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "C:\Users\Nguyen Cong Luc\.ssh\awskey.pem": bad permissions
ubuntu@ec2-18-139-115-54.ap-southeast-1.compute.amazonaws.com: Permission denied (publickey).
```

+Trên window để gỡ bỏ các user khác đang sử dụng, chỉ để user chính, thực hiện các lệnh sau:

```
icacls.exe "C:\Users\Nguyen Cong Luc\.ssh\awskey.pem" /reset
```

```
icacls.exe "C:\Users\Nguyen Cong Luc\.ssh\awskey.pem" /grant:r "%username%:(R)"
```

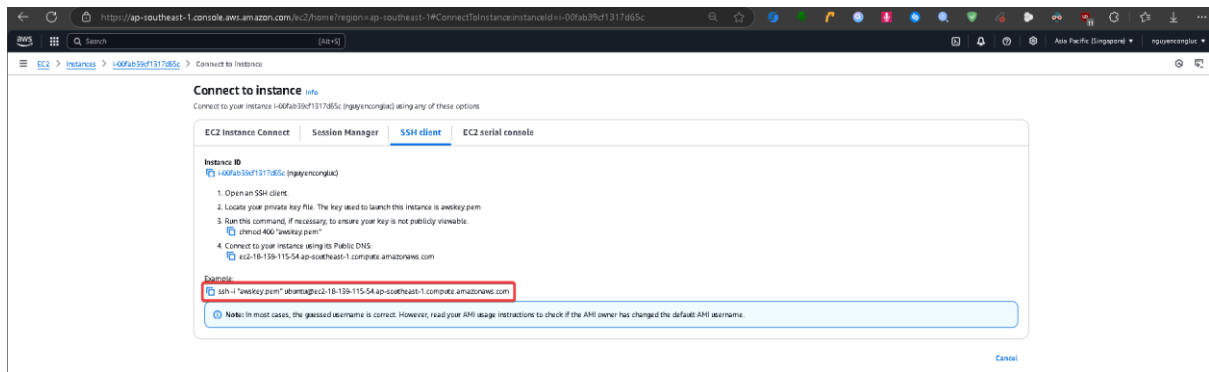
```
icacls.exe "C:\Users\Nguyen Cong Luc\.ssh\awskey.pem" /inheritance:r
```

```
C:\Users\Nguyen Cong Luc>icacls.exe "C:\Users\Nguyen Cong Luc\.ssh\awskey.pem" /reset
processed file: C:\Users\Nguyen Cong Luc\.ssh\awskey.pem
Successfully processed 1 files; Failed processing 0 files

C:\Users\Nguyen Cong Luc>icacls.exe "C:\Users\Nguyen Cong Luc\.ssh\awskey.pem" /grant:r "%username%:(R)"
processed file: C:\Users\Nguyen Cong Luc\.ssh\awskey.pem
Successfully processed 1 files; Failed processing 0 files

C:\Users\Nguyen Cong Luc>icacls.exe "C:\Users\Nguyen Cong Luc\.ssh\awskey.pem" /inheritance:r
processed file: C:\Users\Nguyen Cong Luc\.ssh\awskey.pem
Successfully processed 1 files; Failed processing 0 files
```

- Lấy lệnh ssh:



ssh -i "awskey.pem" ubuntu@ec2-18-141-58-92.ap-southeast-1.compute.amazonaws.com trong cmd đã cài openssh hoặc các tool ssh tương tự:

```
ubuntu@ip-172-31-27-54: ~  
Connection to ec2-18-139-115-54.ap-southeast-1.compute.amazonaws.com closed.  
D:\Job\System Admin\Lab\myOthersLab>ssh -i "awskey.pem" ubuntu@ec2-18-139-115-54.ap-southeast-1.compute.amazonaws.com  
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1021-aws x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/pro  
  
System information as of Sat Mar  8 04:44:52 UTC 2025  
  
System load:  0.0          Processes:            108  
Usage of /:   6.1% of 28.02GB  Users logged in:     1  
Memory usage: 21%          IPv4 address for enX0: 172.31.27.54  
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  
  
Last login: Sat Mar  8 04:43:41 2025 from 116.102.137.84  
ubuntu@ip-172-31-27-54:~$
```

\* Trường hợp file pem bị xóa thì cần phải tạo file pem mới, vì aws chỉ generate ra 1 lần

**EC2** > Key pairs

**Key pairs (1/3)** Info

Find Key Pair by attribute or tag

	Name	Type	Created
<input type="checkbox"/>	awskey	rsa	2025/03/08 09:25 GMT
<input type="checkbox"/>	nguyencongluc_key	rsa	2025/03/08 09:21 GMT
<input type="checkbox"/>	aws	rsa	2025/03/08 09:24 GMT

**Create key pair** (2)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- Chỉnh sửa thông tin theo mẫu dưới đây:

**Create key pair** Info

**Key pair**  
A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

**Name**  
awskey (1)  
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

**Key pair type** Info  
☒ RSA (2) ☐ ED25519

**Private key file format**  
☒ .pem (3) For use with OpenSSH  
☐ .ppk For use with PuTTY

**Tags - optional**  
No tags associated with the resource.  
[Add new tag](#)  
You can add up to 50 more tags.

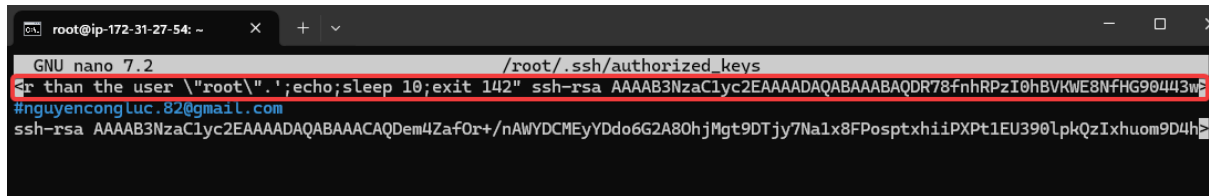
[Cancel](#) **Create key pair** (4)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- File pem là private key, phải generating ra public key rồi thêm vào server: `ssh-keygen -y -f "C:\Users\Nguyen Cong Luc\.ssh\hihi.pem"`

```
PS C:\Users\Nguyen Cong Luc\.ssh> ssh-keygen -y -f "C:\Users\Nguyen Cong Luc\.ssh\hihi.pem"
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQ91YjYGVXWQA2L9ud70xu1UWkIjrzXq6w7kYj6afQ7RKjt+9oAieFwXyVUGdjQUpjNIITX23N5K0PnkSye
8BMh0/SZ0CL714qVnuSs6iZ0afBhn6qZmRq+m2LRsPmEm75JAqkxLTg8jw9VEXYAs3fz/np3PpPtFzHkHi2ao8R75yU71tMnJ4aMjy0nwKGQgeANIHwAnvvQ
Vg5x1b7CgGBWobuffkFwXcINobCMvFLIqsXEWIhGz3b2zK1r0u8LetXCoP8F9RDC2U0CCVvjGktuGyUo05g4IIIOGq7Lg2IdVsgfaznGUNyHgljNPgbByxF
QSFARkk1s7Uo1LQPRt
```

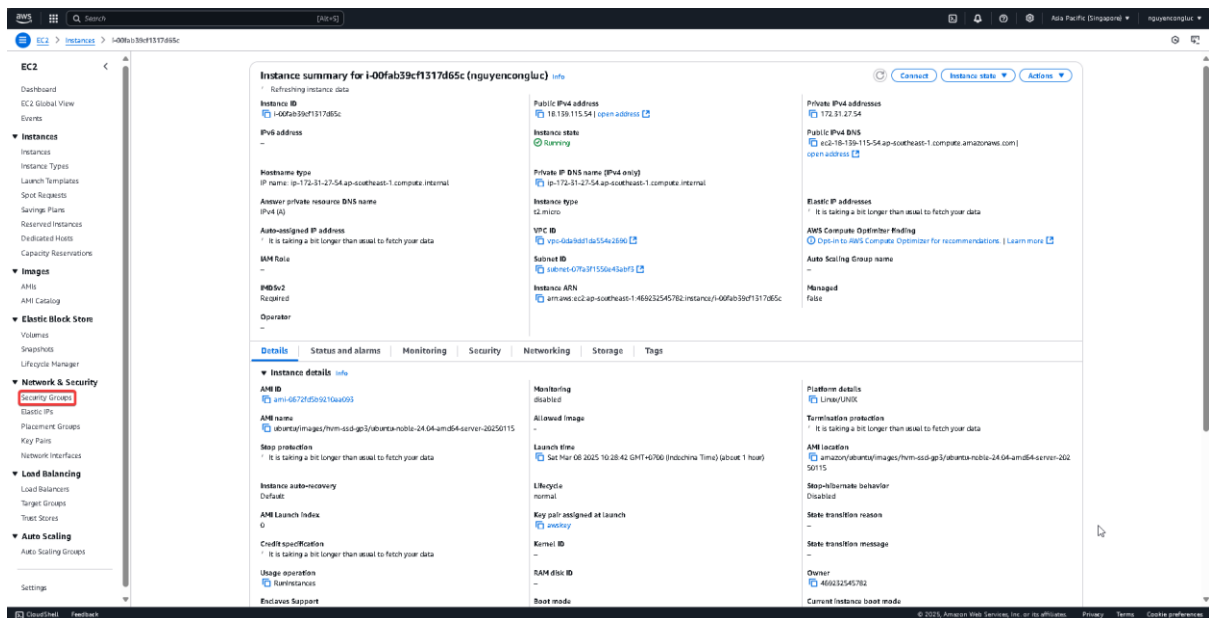
- Sau đó thêm vào vào trong `~/.ssh/authorizedkeys` của server



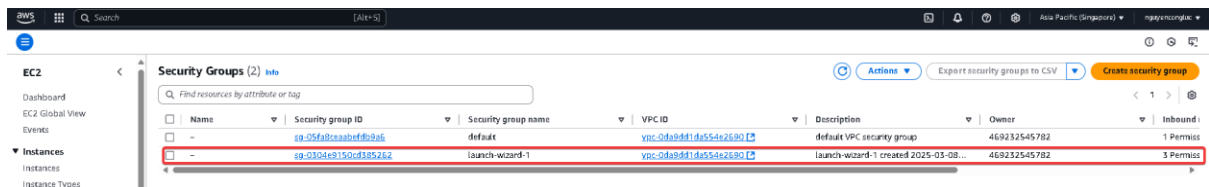
```
GNU nano 7.2 /root/.ssh/authorized_keys
r than the user \"root\".';echo;sleep 10;exit 142" ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQ91YjYGVXWQA2L9ud70xu1UWkIjrzXq6w7kYj6afQ7RKjt+9oAieFwXyVUGdjQUpjNIITX23N5K0PnkSye
#nguyencongluc.82@gmail.com
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQDem4ZafOr+/nAWYDCMEYDdo6G2A80hjMgt9DTjy7Na1x8FPosptxhiiPXpt1EU390lpkQzIxhuom9D4H
```

## 1.4.2 SSH với public key

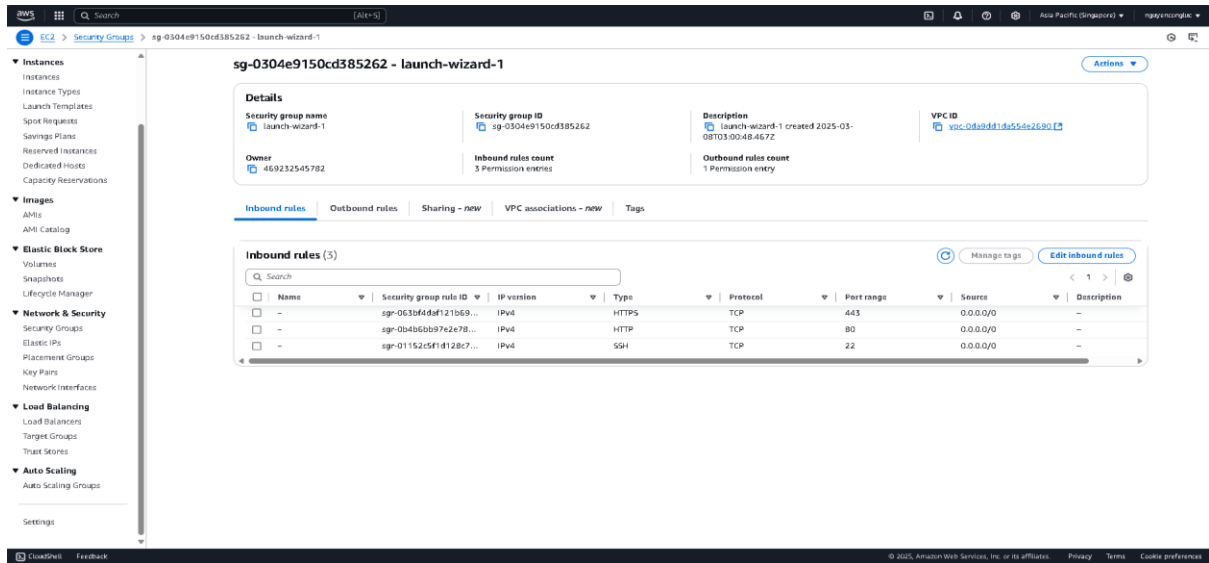
- Cấu hình để có thể ssh bằng IP và port



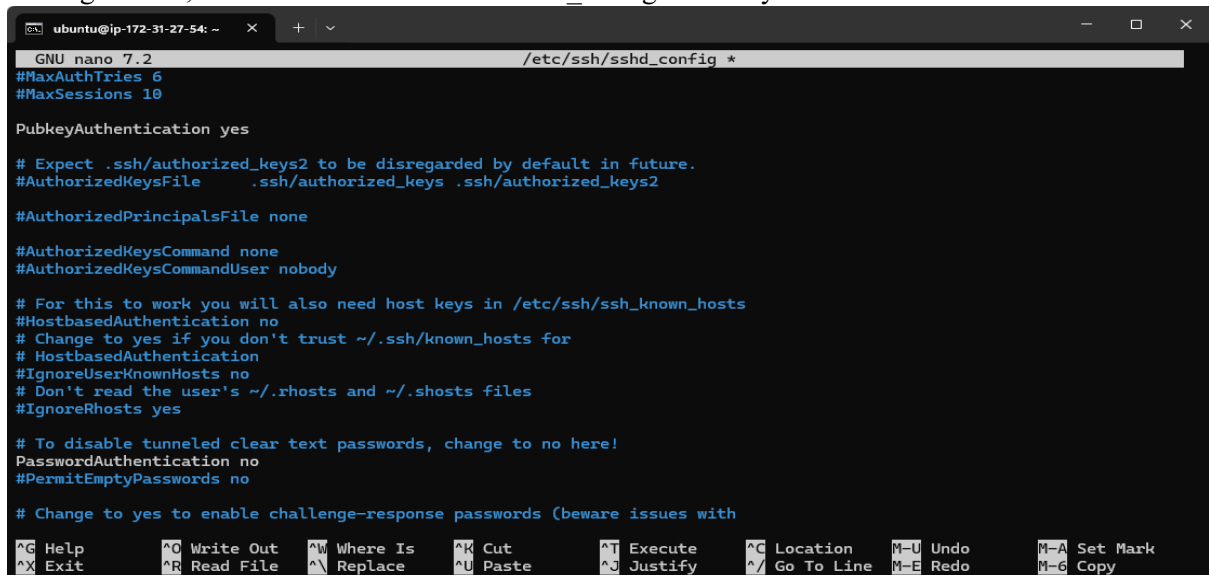
- EC2 > Network & Security > Security Groups -> Click vào các security group name để kiểm tra



- Check các port dưới đây đã mở chưa



- Trong file ssh, cấu hình file nano /etc/ssh/sshd\_config dưới đây



- Thêm public key vào server với lệnh:

```
curl https://raw.githubusercontent.com/lucskyost/vHost/refs/heads/main/authorized_keys >>
~/.ssh/authorized_keys
```

```
root@ip-172-31-27-54:~# curl https://raw.githubusercontent.com/lucskyost/vHost/refs/heads/main/authorized_keys >> ~/.ssh/authorized_keys
```

- Restart lại dịch vụ: sudo systemctl restart ssh

```
root@ip-172-31-27-54:~# sudo systemctl restart ssh
```

- Kết quả ssh thành công với public key:

```
root@ip-172-31-27-54: ~  
PS C:\Users\Nguyen Cong Luc\.ssh> ssh -i "C:\Users\Nguyen Cong Luc\.ssh\id_rsa" root@18.141.58.92  
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1024-aws x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/pro  
  
System information as of Mon Mar 17 07:37:20 UTC 2025  
  
System load:  0.0          Processes:            113  
Usage of /:   8.1% of 28.02GB Users logged in:        2  
Memory usage: 22%          IPv4 address for enX0: 172.31.27.54  
Swap usage:   0%  
  
* Ubuntu Pro delivers the most comprehensive open source security and  
  compliance features.  
  
  https://ubuntu.com/aws/pro  
  
Expanded Security Maintenance for Applications is not enabled.  
  
99 updates can be applied immediately.  
To see these additional updates run: apt list --upgradable  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
Last login: Mon Mar 17 06:53:14 2025 from 27.64.59.225  
root@ip-172-31-27-54:~#
```

## Phần 2. Cấu hình để gửi source code web từ client qua server

### 2.1 Yêu cầu

- Deploy 1 Website html-javascripts đơn giản

### 2.2 Tạo user, thư mục cho user và phân quyền

- Thêm user với lệnh: adduser nguyenciluc

```
root@ip-172-31-27-54:~# adduser nguyenciluc
info: Adding user `nguyenciluc' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `nguyenciluc' (1001) ...
info: Adding new user `nguyenciluc' (1001) with group `nguyenciluc (1001)' ...
info: Creating home directory `/home/nguyenciluc' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for nguyenciluc
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
info: Adding new user `nguyenciluc' to supplemental / extra groups `users' ...
info: Adding user `nguyenciluc' to group `users' ...
```

- Tạo thư mục, chỉnh sửa chủ sở hữu và phân quyền

```
root@ip-172-31-27-54:~# mkdir -p /home/nguyenciluc/public_html
```

```
root@ip-172-31-27-54:~# chown -R nguyenciluc:nguyenciluc /home/nguyenciluc/
```

```
root@ip-172-31-27-54:~# chmod -R 775 /home/nguyenciluc/
```

```
root@ip-172-31-27-54:~# mkdir -p /home/nguyenciluc/public_html
root@ip-172-31-27-54:~# chown -R nguyenciluc:nguyenciluc /home/nguyenciluc/
root@ip-172-31-27-54:~# chmod -R 775 /home/nguyenciluc/
```

- Thêm quyền sudo cho user nguyenciluc (Nên có nếu muốn làm việc lâu dài với 1 user)

```
root@ip-172-31-27-54:/# sudo usermod -aG sudo nguyenciluc
```

```
root@ip-172-31-27-54:/# groups nguyenciluc
```

```
root@ip-172-31-27-54:/# sudo usermod -aG sudo nguyenciluc
root@ip-172-31-27-54:/# groups nguyenciluc
nguyenciluc : nguyenciluc sudo users
```

## 2.3 Cấu hình để gửi source code web từ client qua server

### 2.3.1 Tìm hiểu về FTP, FTPS và SFTP

- FTP (File Transfer Protocol): Giao thức truyền file không mã hóa, dùng port 20/21, cần dịch vụ FTP (như vsftpd), dễ bị nghe lén, tốc độ nhanh nhất.

- FTPS: FTP với mã hóa SSL/TLS, vẫn dùng port 20 và 21, an toàn hơn FTP nhưng phức tạp hơn trong cấu hình, tốc độ nhanh sau FTP.

- Trong FTP và FTPS:

+ Port 21: Kênh điều khiển (control channel) - dùng để gửi lệnh (ví dụ: liệt kê thư mục, tải file).

+ Port 20: Kênh dữ liệu (data channel) - dùng để truyền file hoặc danh sách thư mục trong chế độ Active Mode.

Trong Passive Mode, port 20 không được dùng; thay vào đó, server mở một port ngẫu nhiên (>1023) do client yêu cầu.

Tiêu chí	Active Mode	Passive Mode
Ai khởi tạo dữ liệu	Server (port 20)	Client
Cổng dữ liệu	Port 20	Port ngẫu nhiên
Tường lửa/NAT	Khó hoạt động	Thân thiện hơn
Phức tạp cấu hình	Đơn giản hơn	Cần mở dải cổng

=> Active Mode: Dùng trong mạng nội bộ không có tường lửa/NAT, hoặc khi client có IP công khai và server không bị giới hạn port 20.

=> Passive Mode: Dùng trong hầu hết các trường hợp hiện đại (client sau NAT, server trên cloud như EC2), vì dễ vượt qua tường lửa và phổ biến hơn.

- SFTP (Secure File Transfer Protocol): Truyền file qua SSH (port 22), mã hóa toàn bộ, không cần dịch vụ FTP riêng, đơn giản và bảo mật cao. Quá trình mã hóa và giải mã của SSH tạo thêm chi phí xử lý so với FTPS nên tốc độ nhanh sau FTP, FTPS tuy nhiên không đáng kể, bù lại có mã hóa mạnh, cơ chế bắt tay phức tạp đảm bảo bảo mật cao.

### 2.3.2 Sử dụng SFTP(Nên dùng)

- SFTP (Secure File Transfer Protocol) là giao thức truyền file an toàn, dựa trên SSH (port 22) để truyền file an toàn, mã hóa toàn bộ dữ liệu, không cần dịch vụ FTP riêng. Nó cho phép chuyển file giữa client và server một cách bảo mật, chỉ cần SSH chạy trên server và tài khoản được cấu hình key hoặc mật khẩu.

- Tạo file `.ssh/authorized_keys` nếu chưa có cho user `nguyencongluc` muốn SFTP vào:

```
root@ip-172-31-27-54:~# mkdir -p /home/nguyencongluc/.ssh
```

```
root@ip-172-31-27-54:~# touch /home/nguyencongluc/.ssh/authorized_keys
```

```
root@ip-172-31-27-54:~# mkdir -p /home/nguyencongluc/.ssh
root@ip-172-31-27-54:~# touch /home/nguyencongluc/.ssh/authorized_keys
```



- Thiết lập đặc quyền nếu chưa có:

```
root@ip-172-31-27-54:~# chmod 700 /home/nguyencongluc/.ssh/
```

```
root@ip-172-31-27-54:~# chmod 600 /home/nguyencongluc/.ssh/authorized_keys
```

```
root@ip-172-31-27-54:~# sudo chown -R nguyencongluc:nguyencongluc /home/nguyencongluc/
```

```
root@ip-172-31-27-54:~# chmod 700 /home/nguyencongluc/.ssh/
root@ip-172-31-27-54:~# chmod 600 /home/nguyencongluc/.ssh/authorized_keys
```

```
root@ip-172-31-27-54:~# sudo chown -R nguyencongluc:nguyencongluc /home/nguyencongluc/
```

- Download public key và thêm vào:

curl

```
https://raw.githubusercontent.com/lucskyost/vHost/refs/heads/main/authorized_keys
>> /home/nguyencongluc/.ssh/authorized_keys
```

```
root@ip-172-31-27-54:~# curl https://raw.githubusercontent.com/lucskyost/vHost/refs/heads/main/authorized_keys >> /home/nguyencongluc/.ssh/authorized_keys
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100  780    100  780    0    0  1087      0  --:--:-- --:--:-- --:--:-- 1087
```

- Kiểm tra Security Group trên AWS

Vào AWS Console > EC2 > Security Groups > Chọn Security Group của instance.

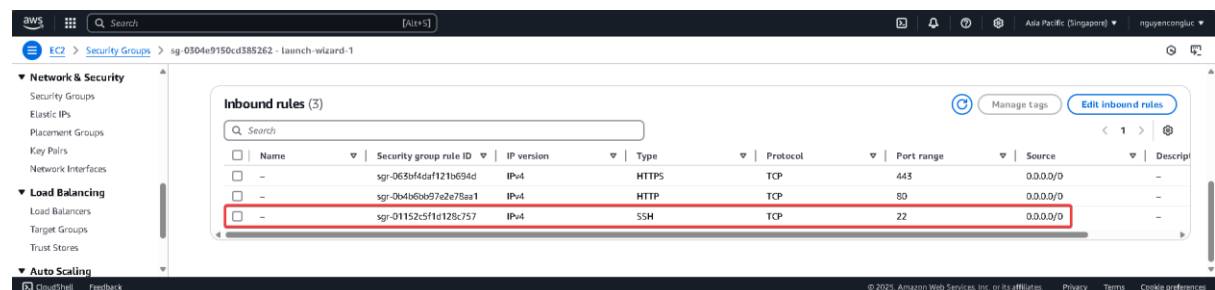
Đảm bảo có rule:

Type: SSH

Protocol: TCP

Port Range: 22

Source: Anywhere (0.0.0.0/0) hoặc IP máy.



- Cấu hình WinSCP trên Windows:

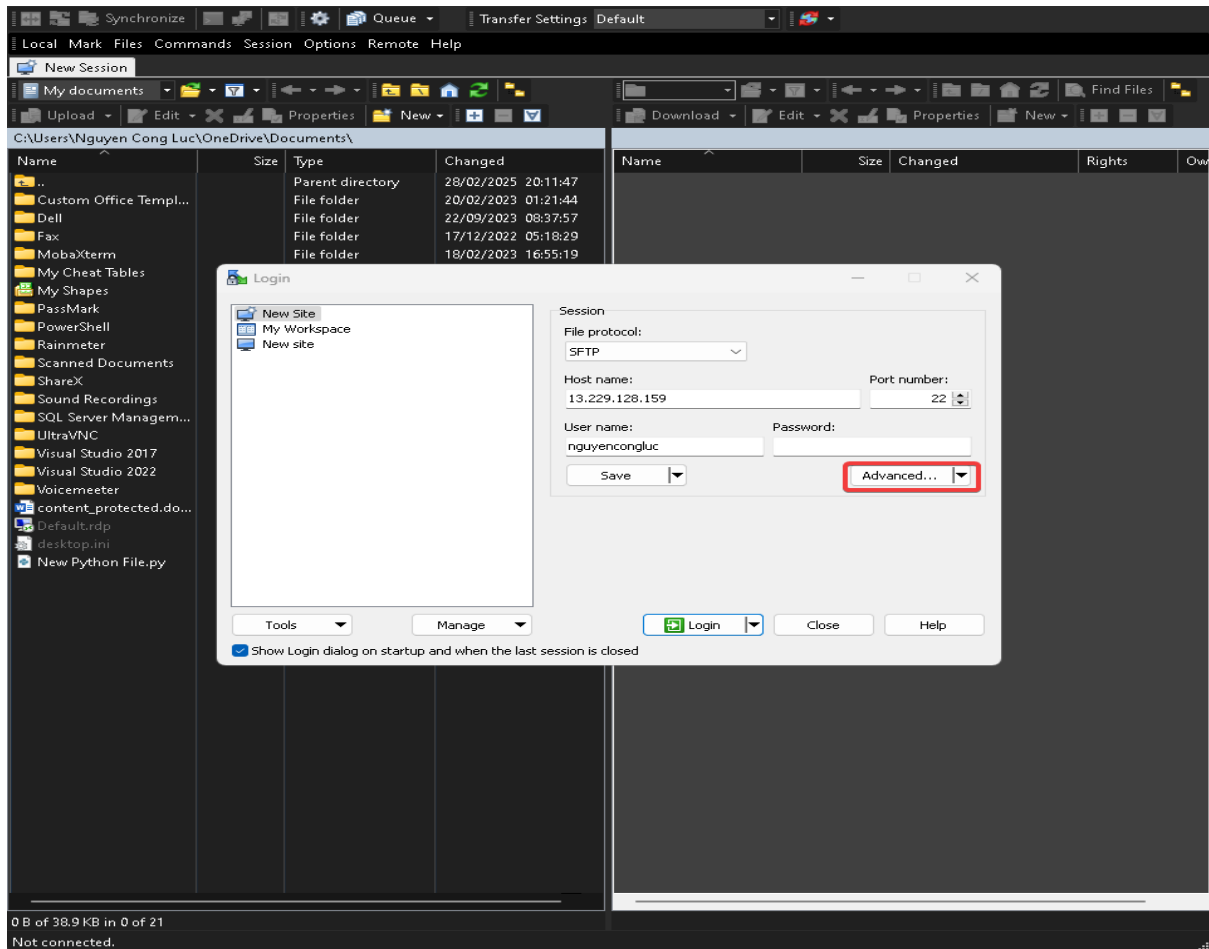
+Mở WinSCP và tạo kết nối mới:

File Protocol: SFTP

Host name: IP hiện tại của instance (ví dụ: 13.229.128.159).

Port number: 22

Username: nguyenciluc , Password không cần

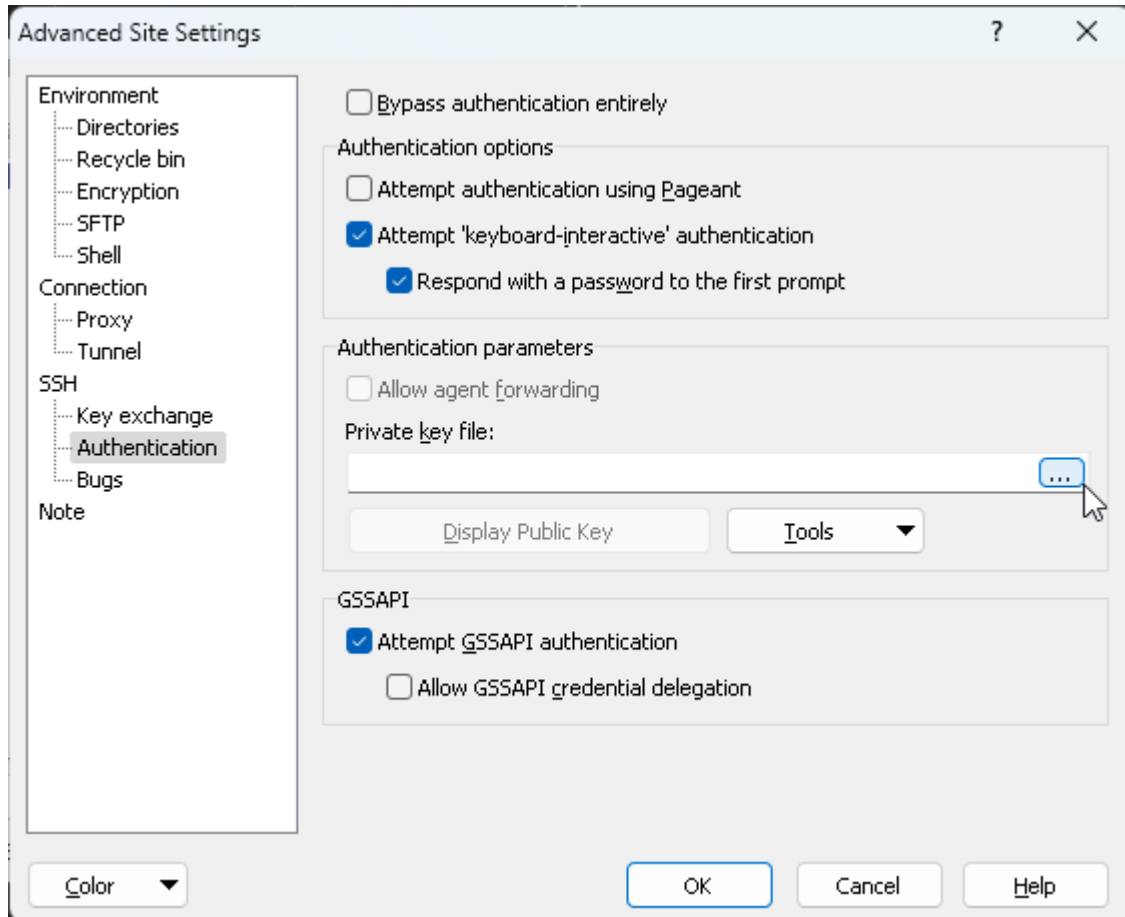


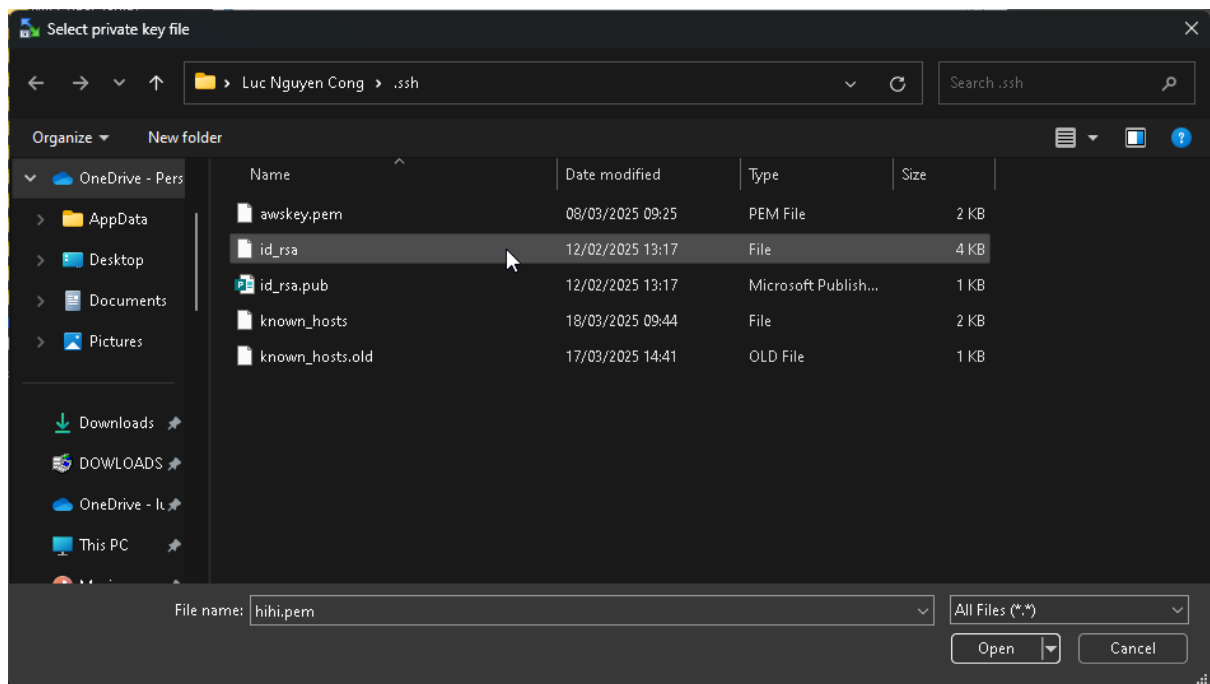
+ Trong tab Advanced:

SSH > Authentication:

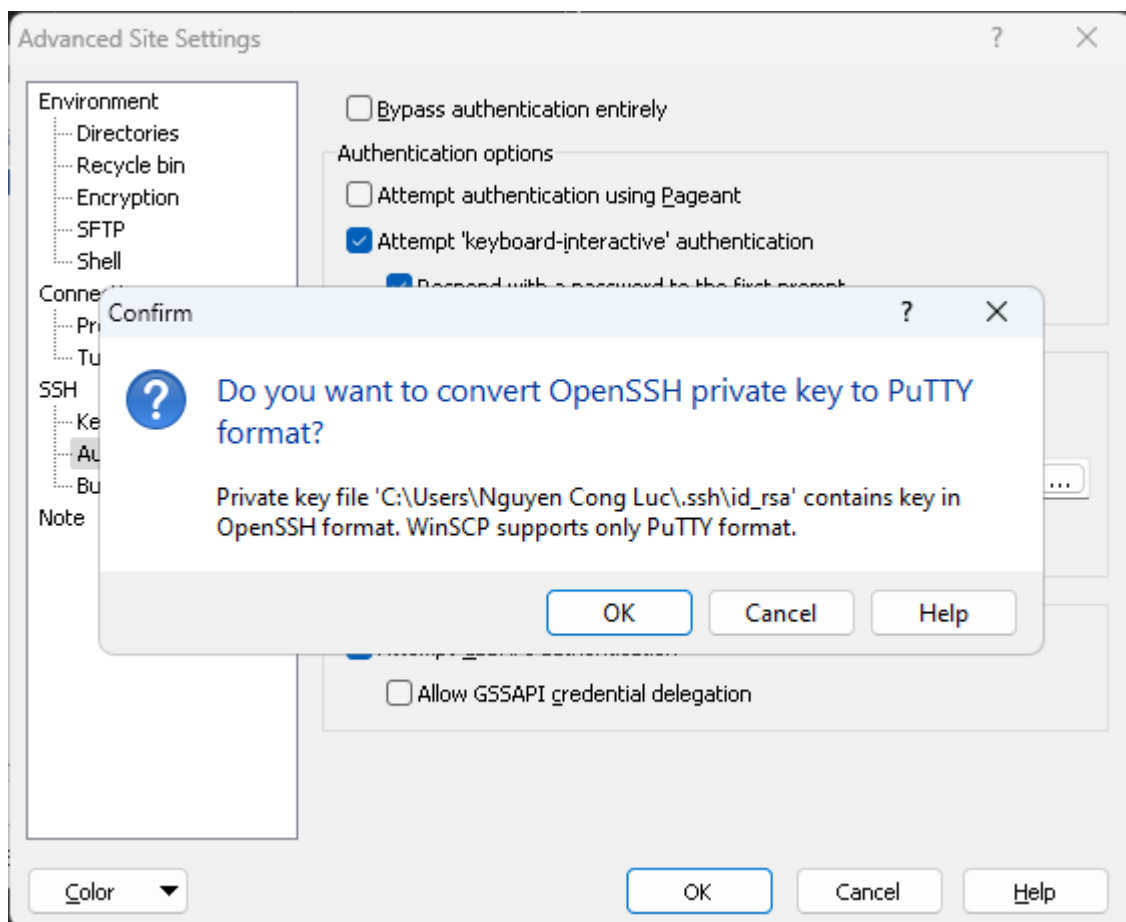
Bỏ chọn "Allow agent" và "Attempt authentication using Pageant" nếu không dùng PuTTY.

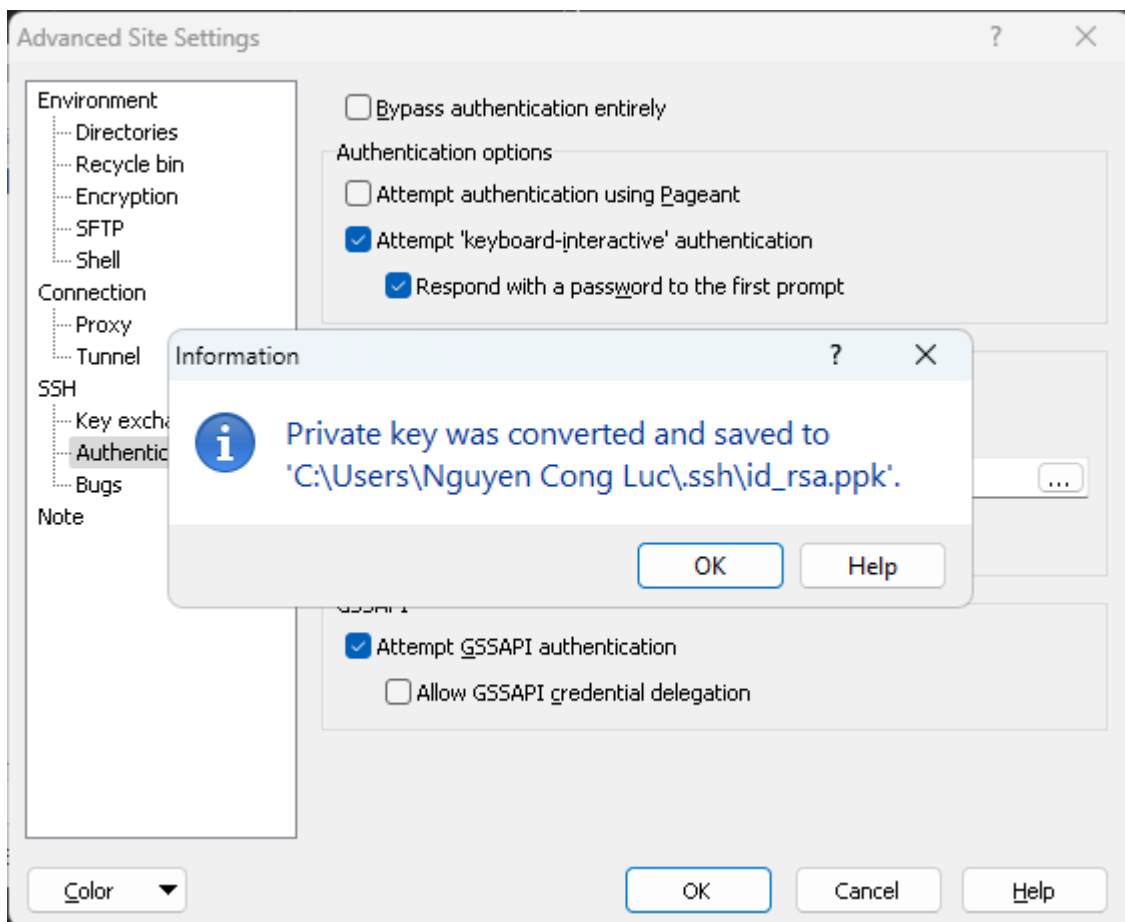
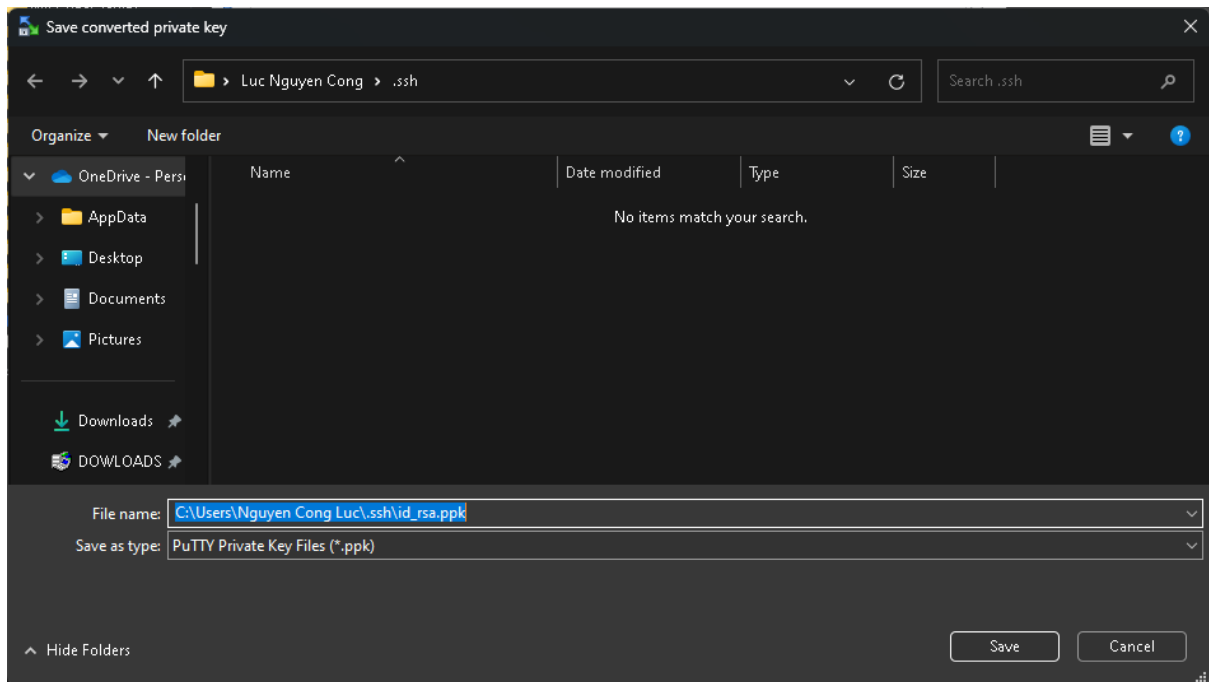
Tại "Private key file", nhấn nút "..." và chọn file .pem của bạn.

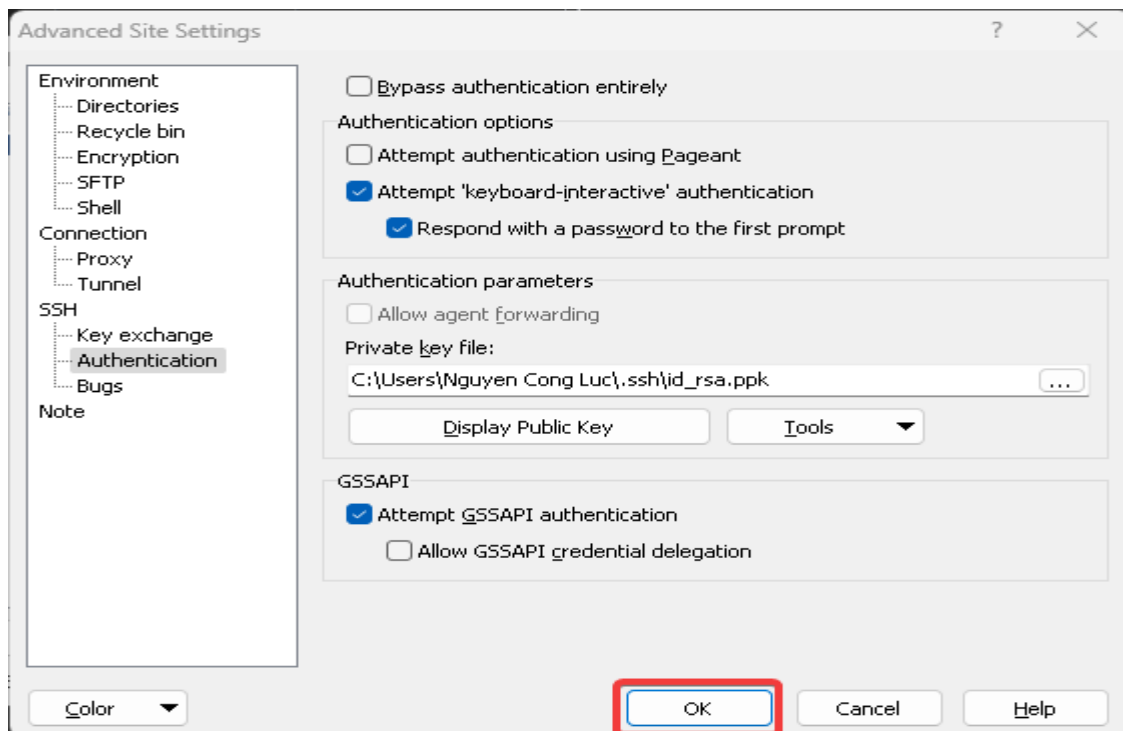




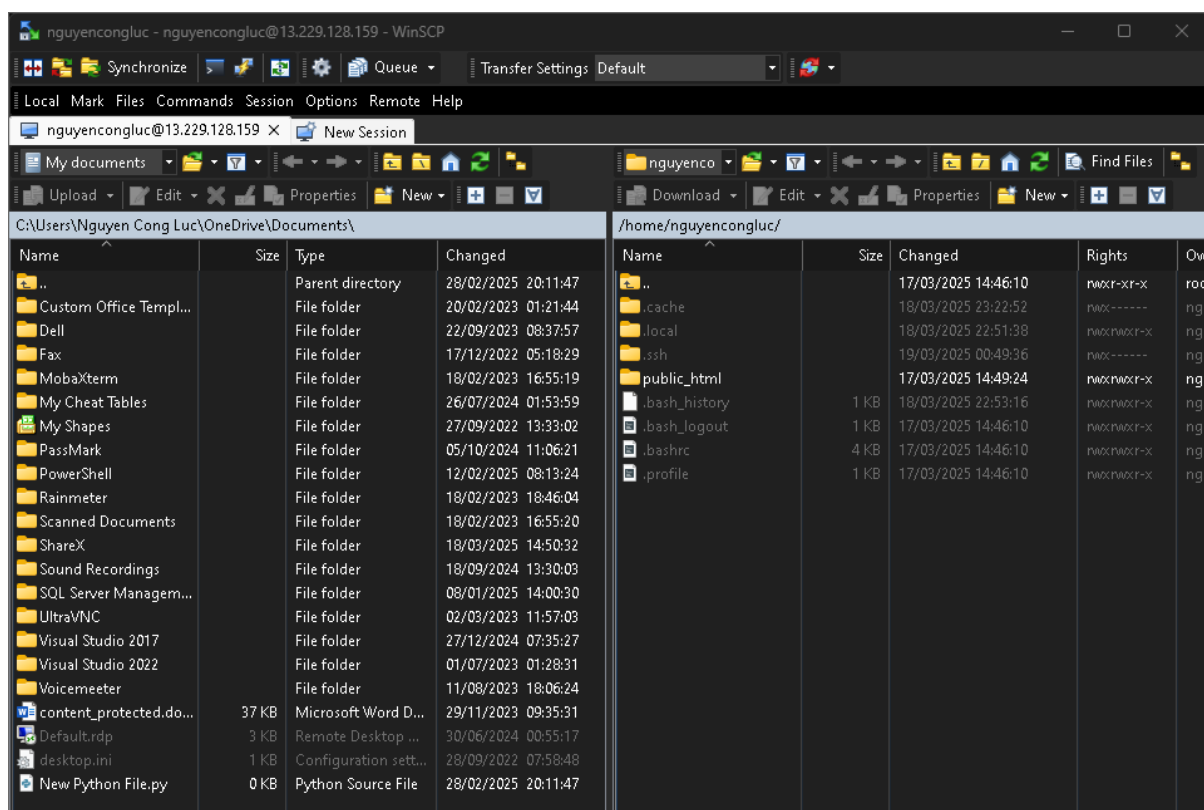
- Nếu WinSCP yêu cầu chuyển đổi file .pem sang định dạng .ppk (PuTTY format), nhấn OK để chuyển đổi và lưu file .ppk, sau đó chọn file .ppk vừa tạo.







- Kết quả khi SFTP vào thành công:



### 2.3.3 Sử dụng FTP (Không nên dùng vì không mã hóa file)

- Cần cài đặt VSFTPD nếu chưa có:

```
sudo apt update
```

```
sudo apt install vsftpd
```

```
root@ip-172-31-27-54:~# sudo apt update
Hit:1 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
102 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@ip-172-31-27-54:~# sudo apt install vsftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
vsftpd is already the newest version (3.0.5-0ubuntu3.1).
0 upgraded, 0 newly installed, 0 to remove and 102 not upgraded.
```

- sudo nano /etc/vsftpd.conf

Thêm mới hoặc chỉnh sửa các nội dung sau:

```
# Tắt đăng nhập ẩn danh
```

```
anonymous_enable=NO
```

```
# Cho phép ghi file (upload)
```

```
write_enable=YES
```

```
GNU nano 7.2 /etc/vsftpd.conf *
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (:::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
```

- Khởi động lại VSFTPD

`sudo systemctl restart vsftpd`

`sudo systemctl enable vsftpd` (Lệnh để vsftpd tự khởi động sau khi reboot server)

- Check trạng thái: `sudo systemctl status vsftpd`

```
root@ip-172-31-27-54:~# sudo systemctl restart vsftpd
sudo systemctl enable vsftpd
Synchronizing state of vsftpd.service with SysV service script with /usr/lib/systemd/systemd-sysv-inst
all.
Executing: /usr/lib/systemd/systemd-sysv-install enable vsftpd
root@ip-172-31-27-54:~# sudo systemctl restart vsftpd
root@ip-172-31-27-54:~# sudo systemctl enable vsftpd
Synchronizing state of vsftpd.service with SysV service script with /usr/lib/systemd/systemd-sysv-inst
all.
Executing: /usr/lib/systemd/systemd-sysv-install enable vsftpd
root@ip-172-31-27-54:~# sudo systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: enabled)
   Active: active (running) since Tue 2025-03-18 03:32:50 UTC; 7s ago
     Main PID: 2170 (vsftpd)
        Tasks: 1 (limit: 1129)
       Memory: 716.0K (peak: 872.0K)
          CPU: 6ms
       CGroup: /system.slice/vsftpd.service
               └─2170 /usr/sbin/vsftpd /etc/vsftpd.conf

Mar 18 03:32:50 ip-172-31-27-54 systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Mar 18 03:32:50 ip-172-31-27-54 systemd[1]: Started vsftpd.service - vsftpd FTP server.
```

- Cập nhật Security Group trên AWS

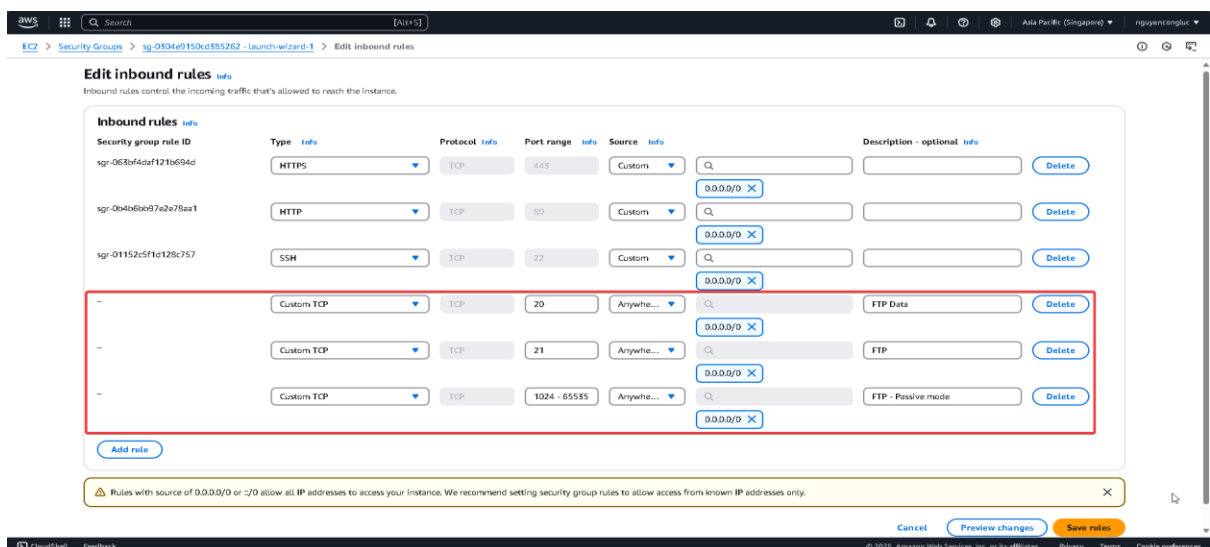
Vào AWS Console > EC2 > Security Groups > Chọn Security Group của instance.

Chỉnh sửa inbound rules để mở các port cần thiết:

+Port 21 (FTP): Để kết nối FTP.

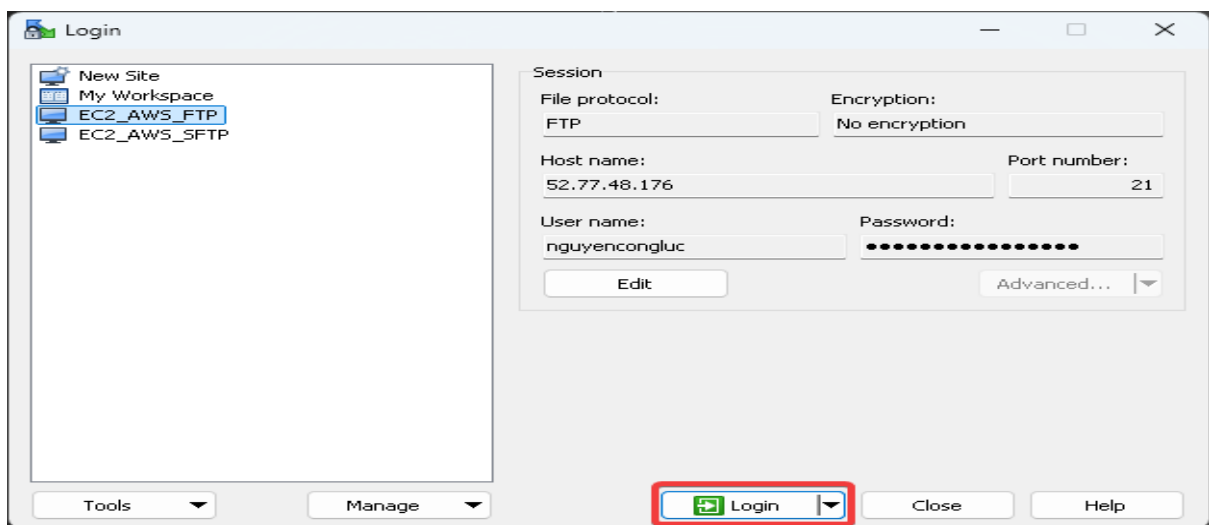
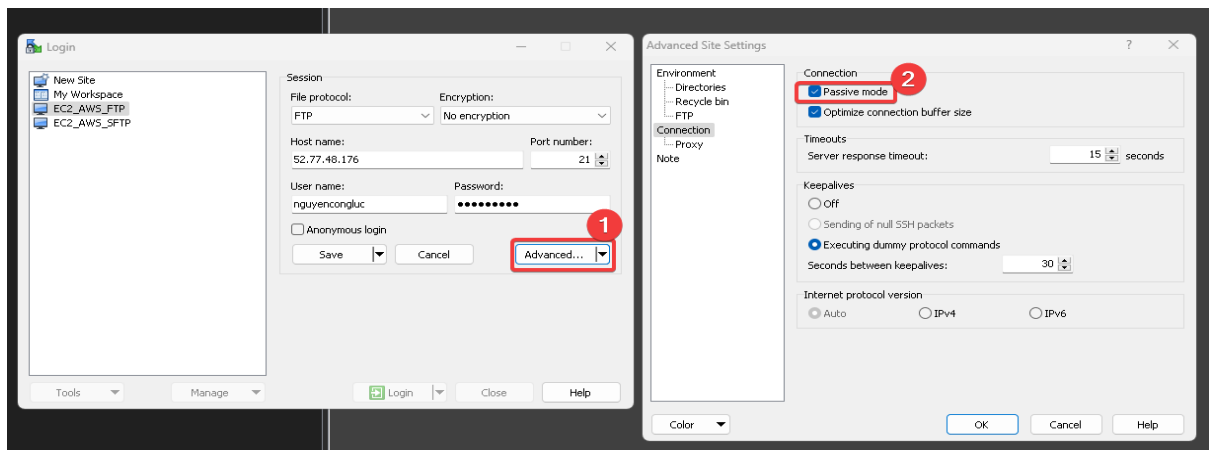
+Port 20 (FTP Data): Dùng cho truyền dữ liệu (nếu dùng active mode).

+Port 1024-65535: Dải port cho passive mode (nên sử dụng). Passive Mode không yêu cầu client mở port ngoài port điều khiển (21) để khởi tạo kết nối, trong khi Active Mode đòi hỏi client mở port ngẫu nhiên cho server kết nối ngược.

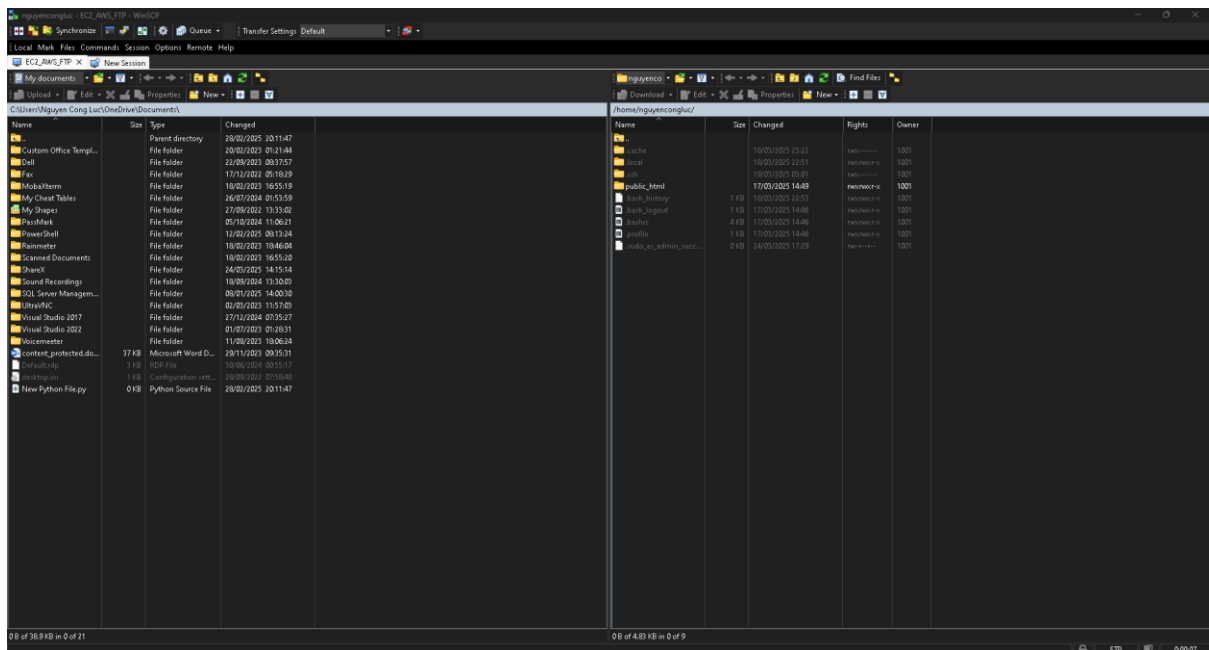




- Thực hiện mở FTP với WinSCP:



- Kết quả FTP thành công:



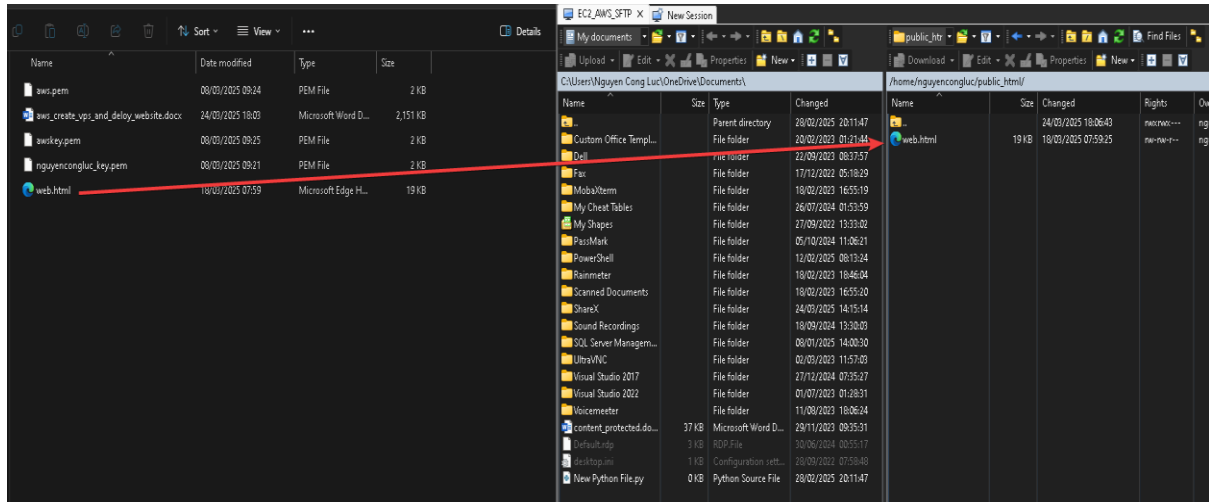
### 2.3.4 Tiến hành upload source code lên server(Áp dụng SFTP để bảo mật)

- Theo mặc định trên Ubuntu, Apache ưu tiên các tên file sau (theo thứ tự):

index.html>index.htm>index.php

Vì vậy, để file HTML được tự động hiển thị khi truy cập domain hoặc IP mà không cần chỉ định tên file thì nên đặt tên file code gốc là index.html

- Trong WinSCP thực hiện kéo file index.html vào



## Phần 3. Cài đặt Web server Apache, DNS Record và Deloy website

### 3.1 Cấu hình DNS Record

- Yêu cầu tiên quyết là đã mua domain, sau đó vào web nhà cung cấp domain để chỉnh sửa DNS record, trỏ domain về IP của server chứa website.

**Manage DNS records**  
These records define how your domain behaves. Common uses include pointing your domain at web servers or configuring email delivery for your domain.

Type A	Name @	Points to 52.77.48.176	TTL 60	<b>Add Record</b>
-----------	-----------	---------------------------	-----------	-------------------

- Kiểm tra domain đã trỏ về IP chưa: nslookup nguyencongluc.site

```
C:\Users\Nguyen Cong Luc>nslookup nguyencongluc.site
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:     nguyencongluc.site
Address:  52.77.48.176
```

### 3.2 Cài đặt Apache Server

- Sử dụng lệnh:

apt update

apt install apache2 -y

systemctl enable apache2 (Bật tự khởi động lại server khi reboot server)

systemctl start apache2 (Khởi động server)

- Kiểm tra: systemctl status apache2

```
root@ip-172-31-27-54:~# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
root@ip-172-31-27-54:~# systemctl start apache2
root@ip-172-31-27-54:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Mon 2025-03-24 11:35:47 UTC; 57s ago
     Docs: https://httpd.apache.org/docs/2.4/
    Main PID: 33098 (apache2)
      Tasks: 55 (limit: 1129)
    Memory: 5.3M (peak: 5.6M)
       CPU: 39ms
    CGroup: /system.slice/apache2.service
            └─33098 /usr/sbin/apache2 -k start
              └─33101 /usr/sbin/apache2 -k start
                └─33102 /usr/sbin/apache2 -k start

Mar 24 11:35:47 ip-172-31-27-54 systemd[1]: Starting apache2.service - The Apache HTTP Server...
Mar 24 11:35:47 ip-172-31-27-54 systemd[1]: Started apache2.service - The Apache HTTP Server.
```

### 3.3 Tạo VirtualHost cho user nguyenciluc

- Gán quyền quản lý thư mục cho user của apache

```
sudo chown -R www-data:www-data /home/nguyenciluc/public_html sudo chmod -R 755 /home/nguyenciluc/public_html
```

- Lấy IP V4 Private trong VM, vì đây là IP Apache dùng để lắng nghe trên giao diện mạng nội bộ chứ không phải Elastic IP được gắn vào. Chạy lệnh: ip a

```
root@ip-172-31-27-54:/home/nguyenciluc/public_html# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enX0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:05:89:ac:59:7b brd ff:ff:ff:ff:ff:ff
    inet 172.31.27.54/20 metric 100 brd 172.31.31.255 scope global dynamic enX0
        valid_lft 2131sec preferred_lft 2131sec
    inet6 fe80::5:89ff:feac:597b/64 scope link
        valid_lft forever preferred_lft forever
```

- Cấu hình file config apache2 cho website nguyenciluc.site bằng cách tạo file cấu hình cho site1.nguyenciluc.site:

```
sudo nano /etc/apache2/sites-available/nguyenciluc.site.conf
```

```
<VirtualHost 172.31.27.54:80>
```

```
    ServerName nguyenciluc.site
```

```
    DocumentRoot /home/nguyenciluc/public_html
```

```
    <Directory /home/nguyenciluc/public_html>
```

```
        AllowOverride All
```

```
        Require all granted
```

```
    </Directory>
```

```
</VirtualHost>
```

```
GNU nano 7.2 /etc/apache2/sites-available/nguyenciluc.site.conf
<VirtualHost 172.31.27.54:80>
    ServerName nguyenciluc.site
    DocumentRoot /home/nguyenciluc/public_html
    <Directory /home/nguyenciluc/public_html>
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>
```

- Kích hoạt Virtual Host:

```
sudo a2ensite nguyenciluc.site.conf
```

- Khởi động lại Apache:

```
sudo systemctl restart apache2
```

### 3.4 Kiểm tra website đã deploy

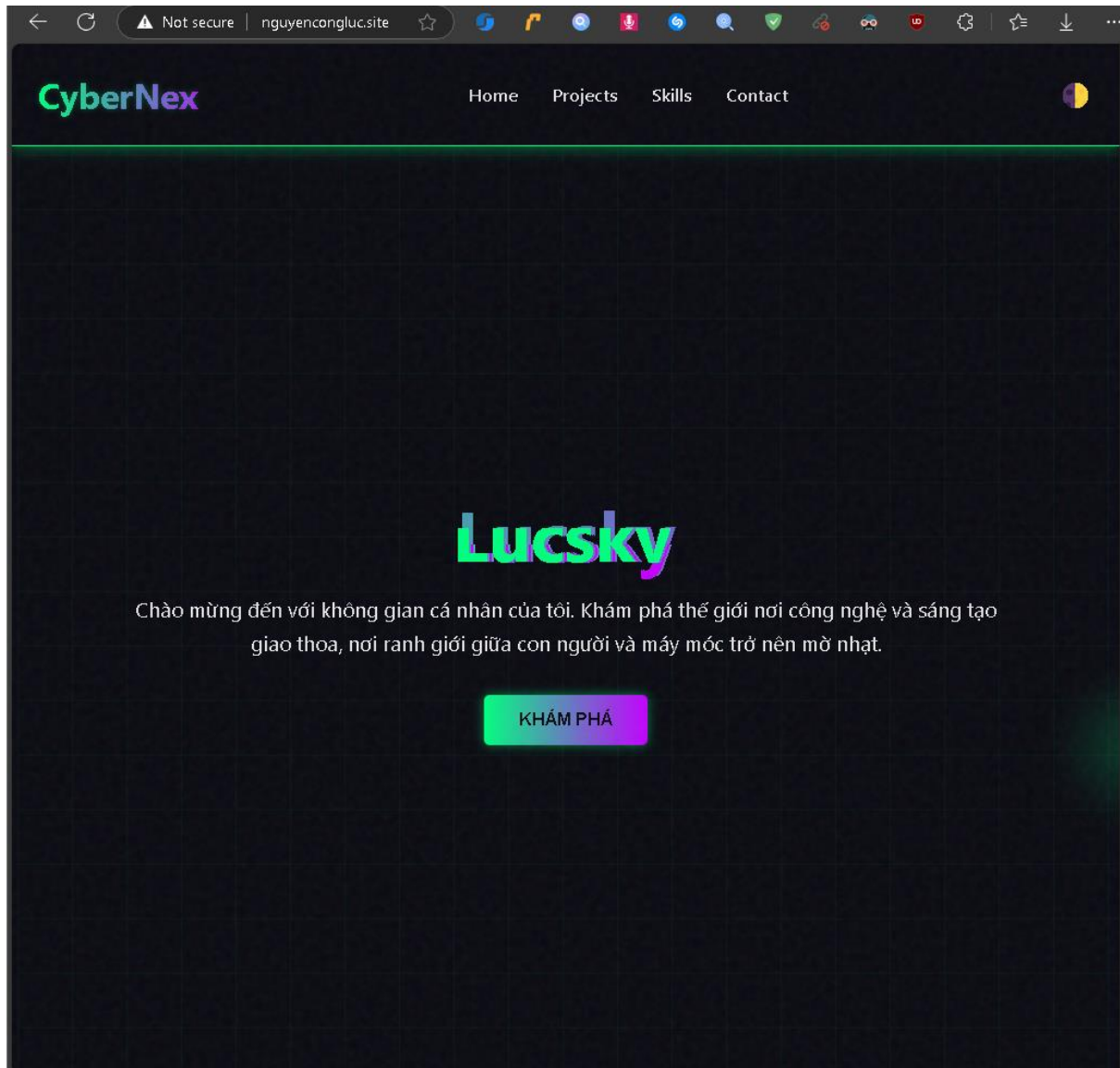
- Truy cập:

<http://nguyencongluc.site/> (nếu DNS đã trở về 52.77.48.176)

hoặc

<http://52.77.48.176/>.

Virtual Host đã hoạt động.



## Phần 4. Thêm SSL cho trang web

### 4.1 Cài đặt Certbot và lấy chứng chỉ SSL

- Để lấy chứng chỉ SSL bắt buộc phải có cấu hình website chạy được ở http: 80, sau đó thực hiện lệnh sau để lấy chứng chỉ cho từng site (Nhấn phím 1 nếu có để tạo SSL mới):

- Cài đầy đủ gói cần thiết để Certbot tích hợp với Apache. Tải về cerbot: `sudo apt install certbot python3-certbot-apache -y`

```
root@ip-172-31-27-54:~# sudo apt install certbot python3-certbot-apache -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
certbot is already the newest version (2.9.0-1).
python3-certbot-apache is already the newest version (2.9.0-1).
0 upgraded, 0 newly installed, 0 to remove and 102 not upgraded.
```

- Chạy lại lệnh Certbot để tạo chứng chỉ:

`sudo certbot --apache -d nguyencongluc.site`

```
root@ip-172-31-27-54:~# sudo certbot --apache -d nguyencongluc.site
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
(Enter 'c' to cancel): nguyencongluc.82@gmail.com

-----
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.5-February-24-2025.pdf. You must
agree in order to register with the ACME server. Do you agree?
-----
(Y)es/(N)o: Y

-----
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the web,
EFF news, campaigns, and ways to support digital freedom.
-----
(Y)es/(N)o: Y
Account registered.
Requesting a certificate for nguyencongluc.site

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/nguyencongluc.site/fullchain.pem
Key is saved at: /etc/letsencrypt/live/nguyencongluc.site/privkey.pem
This certificate expires on 2025-06-22.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

Deploying certificate
Successfully deployed certificate for nguyencongluc.site to /etc/apache2/sites-available/nguyencongluc
.site-le-ssl.conf
Congratulations! You have successfully enabled HTTPS on https://nguyencongluc.site

-----
If you like Certbot, please consider supporting our work by:
* Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
* Donating to EFF: https://eff.org/donate-le
-----
```

## 4.2 Kiểm tra SSL trên website

- Website đã có SSL:

