

Kết nối EC2

cuong@techmaster.vn

4 cách khác nhau để kết nối vào EC2 instance

1. EC2 Instance Connect

- Dễ nhất, chỉ cần dùng trình duyệt

2. Session Manager

- Root hoặc admin account có thể quản lý truy cập đến qua Session Manager

3. SSH Client

- Dùng SSH client kết nối, yêu cầu phải có key pairs

4. EC2 Serial Connect

- Dùng chuẩn serial, chứ không yêu cầu SSH, giúp user xem được toàn bộ quá trình boot up của EC2
- Yêu cầu EC2 instance type là Nitro based
- Nếu chỉ xem boot log thì có thể thay thế bằng Get system log

EC2 Instance Connect

- Dễ nhất
- Không cần phải cấu hình nhiều
- Không cần dùng SSH
- Nhược điểm: không upload file tải file, đồng bộ thư mục

EC2 > Instances > i-06562eeb173a6057d > Connect to instance

Connect to instance [Info](#)

Connect to your instance i-06562eeb173a6057d (Spot T2.micro) using any of these options

EC2 Instance Connect

Session Manager


SSH client

EC2 Serial Console

Instance ID

 i-06562eeb173a6057d (Spot T2.micro)

Public IP address

 175.41.155.168

User name

ec2-user

Connect using a custom user name, or use the default user name ec2-user for the AMI used to launch the instance.



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


Cancel

Connect

Session Manager



- Không yêu cầu SSH key hay bastion host (*server whose purpose is to provide access to a private network from an external network*)
- Session được mã hoá bằng Key Management Service Key, không dùng key pair (*Sessions are secured using an AWS Key Management Service key*)
- Dùng Session Manager để quản lý: start – terminate session
- Không upload file, tải file hay đồng bộ thư mục được

Ưu điểm của Session Manager là root account hoặc IAM user có admin role có thể xem các session đang kết nối và có thể terminate

 Services

Search for services, features, blogs, docs, and more

[Option+S]

  Singapore minhuong

AWS Systems Manager X

Quick Setup

▼ Operations Management

Explorer

OpsCenter

CloudWatch Dashboard

PHD

Incident Manager New

▼ Application Management

Application Manager New

AppConfig

Parameter Store

▼ Change Management

Change Manager New

Automation

Change Calendar


Maintenance Windows


[AWS Systems Manager](#) > Session Manager

Session Manager

Sessions Session history Preferences

Sessions

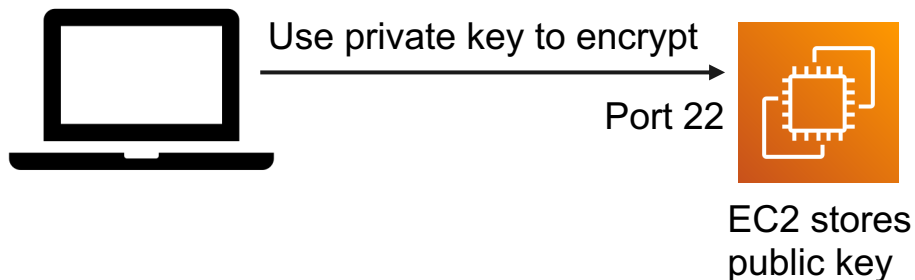
 Terminate Start session

	Session ID	Owner	Instance ID	Document name	Reason	Start date	Status
<input type="radio"/>	root-09eabeb3a6b57e97c	arn:aws:iam::952317537183:root	i-06562eeb173a6057d			Sat, 05 Feb 2022 10:54:00 GMT	 Connect

Tất cả các session kết nối sẽ hiện ra ở đây

SSH Client

- EC2 phải chạy SSHd và có public key trong keypair
- Client: máy tính của chúng ta cần có phần mềm SSH client.
 - Mac, Linux mặc định có sẵn SSH
 - Windows: Putty hoặc Hyper.js
 - Cần phải dùng private key trong keypair
- Copy file dùng scp
- Đồng bộ thư mục dùng rsync



Key pair – cặp public/private key

- Nhiều instance có thể dùng chung 1 key pair. Tiện nhưng bảo mật kém.
- Mỗi instance dùng 1 key pair khác nhau. Quản lý phức tạp nhưng bảo mật cao
- Người dùng tải về private key của key pair. Nếu mất không thể lấy lại key pair. Muốn truy cập vào instance sẽ phải gán key pair mới vào instance rất phức tạp

AWS

Services

Search for services, features, blogs, docs, and more

[Option+5]

New EC2 Experience

Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances New

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances New

Dedicated Hosts

Capacity Reservations

Images

AMIs New

AMI Catalog

Elastic Block Store

Volumes New

Snapshots New

Lifecycle Manager New

Network & Security

Security Groups

Elastic IPs

Hostname type

IP name: ip-172-31-29-216.ap-southeast-1.compute.internal

Instance type

t2.micro

AWS Compute Optimizer finding

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

Private IP DNS name (IPv4 only)

ip-172-31-29-216.ap-southeast-1.compute.internal

Elastic IP addresses

-

IAM Role

AmazonSSMRoleForInstancesQuickSetup

Answer private resource DNS name

IPv4 (A)

VPC ID

vpc-05a1bad64ba6d2b3d

Subnet ID

subnet-0b29ed1d7811313fc

Details

Security

Networking

Storage

Status checks

Monitoring

Tags

Instance details

Info

Platform

Amazon Linux (Inferred)

Platform details

Linux/UNIX

Launch time

Sat Feb 05 2022 11:08:00 GMT+0700 (Indochina Time) (about 1 hour)

Stop-hibernate behavior

disabled

State transition reason

-

State transition message

-

AMI ID

ami-07f179dc333499419

AMI name

amzn2-ami-kernel-5.10-hvm-2.0.20220121.0-x86_64-gp2

AMI location

amazon/amzn2-ami-kernel-5.10-hvm-2.0.20220121.0-x86_64-gp2

AMI Launch index

0

Credit specification

standard

Usage operation

RunInstances

Monitoring

disabled

Termination protection

Disabled

Lifecycle

spot

Key pair name

khueaws

Kernel ID

-

RAM disk ID

-

Mỗi EC2 được gắn 1 Key pair

Launch Templates
Spot Requests
Savings Plans
Reserved Instances New
Dedicated Hosts
Capacity Reservations

▼ Images

AMIs New
AMI Catalog

▼ Elastic Block Store

Volumes New
Snapshots New
Lifecycle Manager New

▼ Network & Security

Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces

Key pairs (2) Info



Actions ▼

Create key pair

Filter key pairs



1



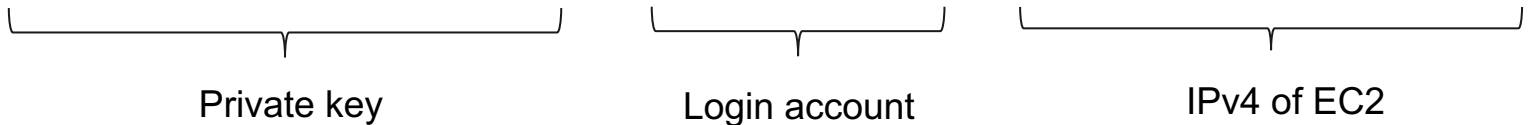
<input type="checkbox"/>	Name ▼	Type ▼	Fingerprint ▼	ID ▼
<input type="checkbox"/>	cuongec2	rsa	ed:fc:9d:e2:37:14:f5:1a:...	key-0d4c8c14c624ce912
<input type="checkbox"/>	khueaws	rsa	f9:30:b0:b5:6d:5a:7d:8...	key-0b36bf71fb48c1438



Chỉ có thể xóa hoặc tạo mới key pairs
Không thể tải lại key pairs

SSH

```
ssh -i "khueaws.cer" ec2-user@175.41.155.168
```



The diagram illustrates the components of the SSH command `ssh -i "khueaws.cer" ec2-user@175.41.155.168`. Brackets are placed under each part of the command, with a vertical line pointing down to a descriptive label:





- `-i "khueaws.cer"` is labeled "Private key".
- `ec2-user@` is labeled "Login account".
- `175.41.155.168` is labeled "IPv4 of EC2".



```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@                WARNING: UNPROTECTED PRIVATE KEY FILE!                @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0777 for 'khueaws.cer' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
key_load_private: bad permissions
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@                WARNING: UNPROTECTED PRIVATE KEY FILE!                @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0777 for 'khueaws.cer' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "khueaws.cer": bad permissions
```

Cách xử lý là gõ lệnh

```
$ chmod 400 hueaws.cert
```

chmod 400 hạn chế quyền chỉ có owner mới được đọc

 chmodcommand.com/chmod-400/   

 CHMOD Calculator 

Chmod 400

Chmod calculator allows you to quickly generate permissions in numerical and symbolic formats. All options are included (recursive, sticky, etc). You'll be ready to copy paste your chmod command into your terminal in seconds.

	Owner Rights (u)	Group Rights (g)	Others Rights (o)
Read (4)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Write (2)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Execute (1)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☐ Verbose ⓘ

☐ Changes ⓘ

☐ Silent ⓘ

☒ Default ⓘ

Extra chmod command options

☒ Recursive ⓘ

☐ Preserve-Root ⓘ

☐ Reference File ⓘ

☐ Setuid ⓘ

☐ Setgid ⓘ

☐ Sticky Bit ⓘ

EC2 Serial Console

- Chỉ hỗ trợ Nitro instance type
- Giao diện web như Instance Connect và Session Manager
- Sử dụng giao thức serial để kết nối EC2, không cần SSH. Nếu SSH không khởi động được trong EC2 thì phải chuyển qua dùng serial console
- Xem được toàn bộ quá trình khởi động EC2