

- [建立 Windows Server](#)
 - [建立 EC2 實例](#)
 - [設置 Advanced details](#)
 - [補充說明 User data 的設置](#)
 - [補充說明 User data 的 CMD 指令](#)
 - [補充說明 User data 其他規範](#)
 - [建立並預覽指令](#)
 - [使用圖形化介面建立實例](#)
 - [使用 CLI 建立實例](#)
 - [準備紀錄用文檔](#)
 - [準備 AWS CLI 環境所需配置](#)
 - [進行 AWS CLI 環境配置](#)
 - [檢查 AWS CLI 設置已完成](#)
 - [取得實例連線的帳號與密碼](#)
 - [連線](#)
 - [關於使用 AWS CLI 建立實例的錯誤](#)
 - [驗證 base64 編碼](#)
 - [重新編輯 User Data](#)
 - [關於生成實例的錯誤處理](#)
 - [手動 安裝 XAMPP](#)

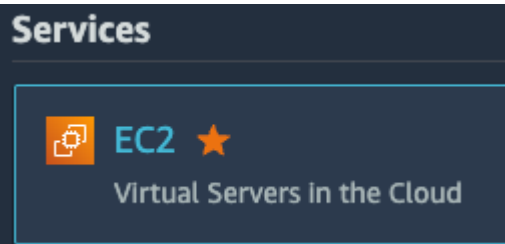
建立 Windows Server

使用 *Learner Lab* 資源建立一個 Windows Server 的 EC2 實例，將在後續步驟中用於作為網站伺服器

建立 EC2 實例

進入 AWS 主控台

1. 進入 EC2。



2. 點擊 **Launch instance**，任意命名如 **MyInstance1018**。

Name and tags [Info](#)

Name

MyInstance1018

3. OS 選擇 **Windows**，Amazon Machine Image 選用 **Microsoft Windows Server 2022 Base**。

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system applications) required to launch your instance. Search or Browse for AMIs if you for below

Recents | **Quick Start**

Amazon Linux 	macOS 	Ubuntu 	Windows 	Red Hat
-------------------------	------------------	-------------------	--------------------	--------------------

Amazon Machine Image (AMI)

Microsoft Windows Server 2022 Base ami-0324a83b82023f0b3 (64-bit (x86)) Virtualization: hvm ENA enabled: true Root device type: ebs
--

4. 在 Instance type 部分，選擇 **t2.micro** 即可，這裡為了提升效能，所以選擇 **t3.large**。

Instance type

t3.large

Family: t3 2 vCPU 8 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0832 USD per Hour
On-Demand Windows base pricing: 0.1108 USD per Hour
On-Demand RHEL base pricing: 0.112 USD per Hour
On-Demand SUSE base pricing: 0.1395 USD per Hour

Additional costs apply for AMIs with pre-installed software

5. 點擊 **Create new key pair** 建立新的 Key pair；命名 **MyKey1018**，其餘採用預設；點擊右下角 **Create key pair** 完成建立，此時會自動下載同名密鑰文件到本地電腦。

Create key pair

×

Key pair name

Key pairs allow you to connect to your instance securely.

Mykey1018

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ RSA
RSA encrypted private and public key pair

☐ ED25519
ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

Cancel

Create key pair

6. Firewall (security groups) 的設定全部點選，也就是開啟 HTTPS 及 HTTP 的進站規則。

Firewall (security groups) Info

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

☒ Create security group

☐ Select existing security group

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

☒ Allow RDP 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

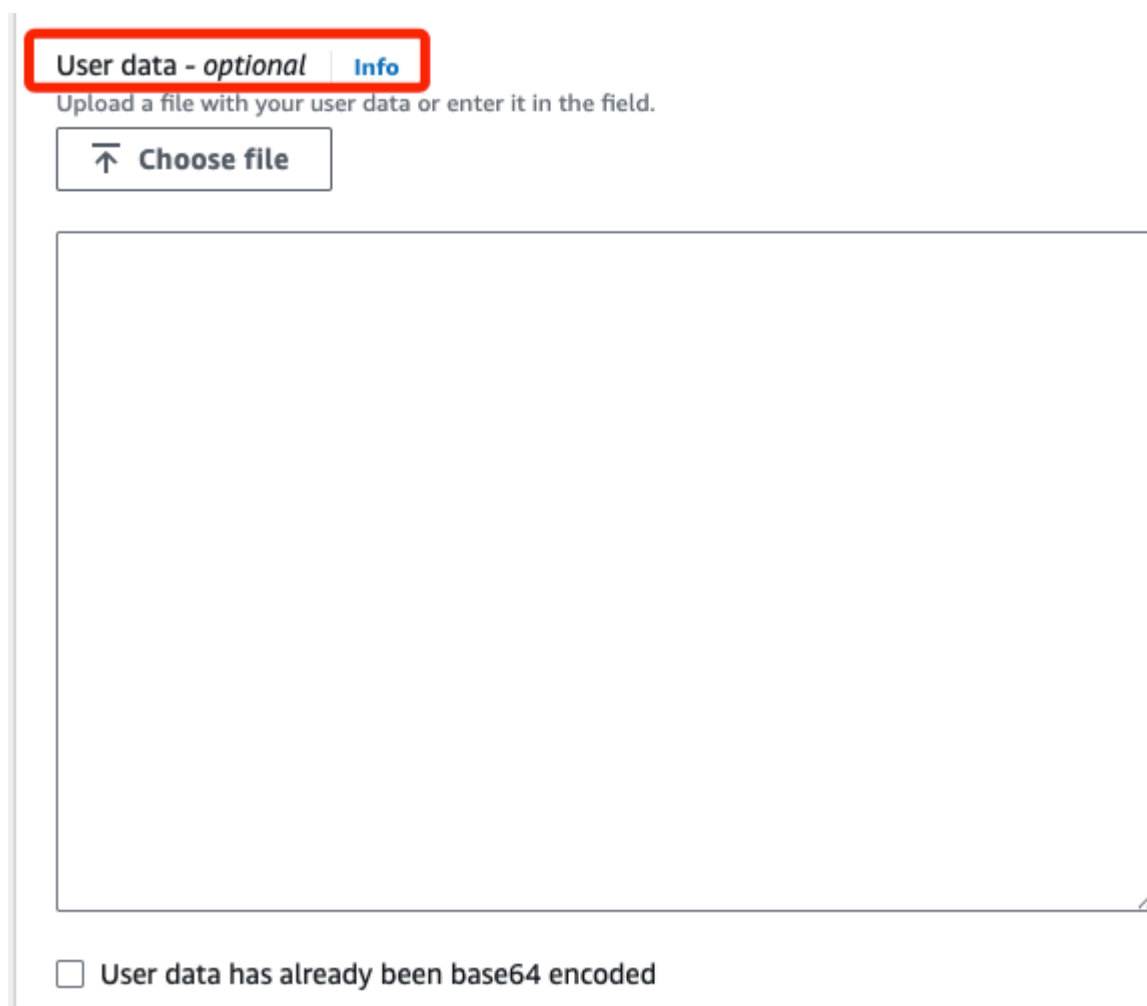
☒ Allow HTTP traffic from the internet

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

設置 Advanced details


以下列舉 *User data* 的設定值，在這裡僅安裝 *Python*。

1. 展開 *Advanced details* 並滑動到該區塊最下方會看到 *User data*，可用於自動化伺服器配置，節省手動安裝和設定的時間；特別注意，*User data* 預設有 *16KB* 的大小限制，並且只會在實例第一次啟動時執行，如果想讓指令每次重啟時都執行，需要將腳本放入 *C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\.*。



User data - optional [Info](#)

Upload a file with your user data or enter it in the field.

 Choose file

☐ User data has already been base64 encoded

2. 這裡僅先嘗試安裝指定版本的 *Python*，安裝後將 *Python* 加入環境變數路徑，最後刪除安裝檔；在 *Powershell* 中使用 *Invoke-WebRequest* 下載 *XAMPP*，相關指引與規範可參考 [官網](#)。

```
<powershell>
# 下載並安裝 Python
Invoke-WebRequest -Uri
"https://www.python.org/ftp/python/3.10.0/python-3.10.0-amd64.exe" -
OutFile "C:\python-installer.exe"
Start-Process -FilePath "C:\python-installer.exe" -ArgumentList "/quiet
InstallAllUsers=1 PrependPath=1" -Wait
Remove-Item -Path "C:\python-installer.exe"
</powershell>
```

補充說明 **User data** 的設置

對於其他可透過 **PowerShell** 指令預先安裝的項目做簡單說明；特別說明，這些指令在實例啟動後皆可在 **Powershell** 中運行，假如使用 AWS 圖形化介面建立實例，也可以寫在 **User data** 中。

1. 在實例啟動時自動更新。

```
<powershell>
Install-WindowsUpdate -AcceptAll -AutoReboot
</powershell>
```

2. 安裝 **Google Chrome**。

```
<powershell>
Invoke-WebRequest -Uri
"https://dl.google.com/chrome/install/375.126/chrome_installer.exe" -
OutFile "C:\chrome_installer.exe"
Start-Process -FilePath "C:\chrome_installer.exe" -ArgumentList
"/silent /install" -Wait
Remove-Item -Path "C:\chrome_installer.exe"
</powershell>
```

3. 安裝 **XAMPP**，設定為 **靜默模式**，安裝完畢刪除安裝檔案，然後使用 **Start-Process** 指令批次啟動 **XAMPP** 管理的 **Apache** 和 **MySQL** 服務。

```
<powershell>
Invoke-WebRequest -Uri
"https://sourceforge.net/projects/xampp/files/XAMPP%20Windows/8.2.12/xam
mpp-windows-x64-8.2.12-0-VS16-installer.exe/download" -OutFile
"C:\xampp-installer.exe"

Start-Process -FilePath "C:\xampp-installer.exe" -ArgumentList "--mode
unattended --unattendedmodeui none --prefix C:\xampp" -Wait

Remove-Item -Path "C:\xampp-installer.exe"

Start-Process -FilePath "C:\xampp\apache_start.bat" -Wait
Start-Process -FilePath "C:\xampp\mysql_start.bat" -Wait
</powershell>
```

4. 安裝 **IIS** 網頁伺服器。

```
<powershell>
Install-WindowsFeature -name Web-Server -IncludeManagementTools
</powershell>
```

補充說明 **User data** 的 **CMD** 指令

1. 更新防火牆規則。

```
<persist>
rem 啟動 Apache 和 MySQL
cd C:\xampp
apache_start.bat
mysql_start.bat

rem 設定防火牆規則，允許 HTTP (80)，HTTPS (443) 和 MySQL (3306) 的入站連接
netsh advfirewall firewall add rule name="Allow HTTP" dir=in
action=allow protocol=TCP localport=80
netsh advfirewall firewall add rule name="Allow HTTPS" dir=in
action=allow protocol=TCP localport=443
netsh advfirewall firewall add rule name="Allow MySQL" dir=in
action=allow protocol=TCP localport=3306
```

```
</persist>
```

2. 指定腳本在每次啟動實例時都執行。

```
<persist>true</persist>
```

補充說明 **User data** 其他規範

1. 若運行多項功能，只需要添加一次 **Section** 語句。
2. **User data** 腳本有預設的執行時間限制，如果腳本過長或過於複雜，某些命令可能無法完全執行。

建立並預覽指令

1. 點擊 **Launch instance** 之前，下方有個 **Preview code**，先點擊查看；右側會顯示指令預覽，這裡先做紀錄，之後再來透過指令重新建立一次。

Launch instance

 **Preview code**

2. 包含了三個部分，分別是 **CreateSecurityGroup**、**AuthorizeSecurityGroupIngress**、**RunInstances**。

EC2 / Launch Instances

Last updated Sat Oct 19 2024 00:20:10 GMT+0800 (台北標準時間)

CreateSecurityGroup

```
aws ec2 create-security-group --group-name "launch-wizard-1" --description "launch-wizard-1 created 2024-10-18T16:13:57.43Z" --vpc-id "vpc-0c46350047f5fa6e4"
```

AuthorizeSecurityGroupIngress

```
aws ec2 authorize-security-group-ingress --group-id "sg-0324a83b820e1e1e1" --protocol "tcp" --port "3389" --vpc-id "vpc-0c46350047f5fa6e4" --cidr "0.0.0.0/0"
```

RunInstances

```
aws ec2 run-instances --image-id "ami-0324a83b820e1e1e1" --instance-type "t3.large" --key-name "MyKey1018" --network-interface-public-address "true" --device-index "0" --groups ["sg-0324a83b820e1e1e1"] --tag-specifications [{"Resource": "instance", "Tags": [{"Key": "Name", "Value": "MyInstance1"}]}
```

3. **CreateSecurityGroup** 區塊預設會建立名為 **launch-wizard-1** 的安全群組，並附加到指定的 **VPC**。

CreateSecurityGroup

```
aws ec2 create-security-group --group-name "launch-wizard-1" --description "launch-wizard-1 created 2024-10-19T07:52:39.490Z" --vpc-id "vpc-0c46350047f5fa6e4"
```

4. **AuthorizeSecurityGroupIngress** 會自動依據安全群組為 ID 為 **sg-preview-1** 的安全群組設置入口規則 (**Ingress Rules**)，也可稱為 **進站規則 (Inbound Rules)**。

AuthorizeSecurityGroupIngress

```
aws ec2 authorize-security-group-ingress --group-id "sg-preview-1" --i
p-permissions '{"IpProtocol":"tcp","FromPort":3389,"ToPort":3389,"IpRange
s":[{"CidrIp":"0.0.0.0/0"}]}' '{"IpProtocol":"tcp","FromPort":443,"ToPort":443
,"IpRanges":[{"CidrIp":"0.0.0.0/0"}]}' '{"IpProtocol":"tcp","FromPort":80,"ToP
ort":80,"IpRanges":[{"CidrIp":"0.0.0.0/0"}]}'
```

5. **RunInstances** 進行啟動 EC2 實例；這段指令很長，會依據各項設定自動生成。

RunInstances

```
aws ec2 run-instances --image-id "ami-0324a83b82023f0b3" --instanc
e-type "t3.large" --key-name "MyKey1018" --user-data "PHBvd2Vyc2h1bG
w+Ckluc3RhbgWtV2luZG93c1VwZGF0ZSA0QWNjZXB0QWxsIC1BdXRvUmV
ib290CgpJbnZva2UtV2ViUmVxdWVzdCA0VXJpIChodHRwczovL3d3dy5weX
Rob24ub3JnL2Z0cC9weXRob24vMy4xMC4wL3B5dGhvb2JlEwLjAtYW1k
NjQuZXh1IAtT3V0RmlsZSAiQzpccl0aG9uLWluc3Rhbgxlc15leGUIClN0YXJ
OLVByb2Nlc3MgLUZpbGVQYXRoICh0aWwweXRob24taW5zdGFsbGVyLmV4
ZS1lcl1Fv73Vt7W50TG1zdCAiIl3F1aWV0IFluc3RhbgxRbGxVc2Vvcz0xIFRv7
```

6. 點擊 **Download** 下載語法備用。

 Copy

 Download

使用圖形化介面建立實例

1. 點擊 **Launch instance**。

Launch instance

 Preview code

2. 沒特殊狀況就會顯示 **Success**，但這僅是完成設定，實例尚未完成啟動，回到 EC2 清單查看。

A green rectangular box with a red border. Inside, on the left, is a white checkmark icon followed by the word "Success" in white. Below this, in smaller white text, is the message "Successfully initiated launch of instance (i-0190c32abd7526432)".

✓ **Success**
Successfully initiated launch of instance (i-0190c32abd7526432)

使用 CLI 建立實例

使用相同的設置所下載的語法文件 `console-to-code.txt` 在本地的終端機中運行，並藉此比較相同設置卻出現的錯誤日誌；透過 CLI 建立實例時出現了錯誤，特別是在處理 `User data` 部分。

1. 首先建立安全群組並取得 ID，特別注意，假如是再次運行並沿用現有安全群組，可查詢安全群組 ID 即可。
2. 第二段語句是設定安全群組的入站規則，將 ID 填入範例語句中即可運行；同樣的，假如沿用現有安全群組，可視狀況進行設定。
3. 建立實例，這裡要將安全群組 ID 填入，假如需要再次建立，需對實例名稱重新定義；特別注意最後一個參數 `--count`，預設建立一個實例，假如要批次建立可在這填入數值。
4. 若希望輸出會自動顯示，不需要手動逐頁查看，可在指令尾端加上參數 `--no-paginate`，這指令會顯示所有輸出，且在執行完畢後自動返回命令行。

```
--no-paginate
```

準備紀錄用文檔

接下來會有一些資訊需要記錄備用，在一般正式的 Lab 中會建議使用 Cloud9 做紀錄，但這個 Lab 並未授權，請自行使用任意文件編輯器做紀錄。

1. 建立文檔後，先貼上以下內容，這將用於建立終端機視窗的 區域變數；其中 Username 及 Shared_Name_of_Drive_C 已填入預設的內容 Administrator、C_Drive，若沿用則無需更改。

```
# 第一部分：複製 AWS CLI 貼上，格式不重要，稍後會直接覆蓋
[default]
aws_access_key_id=
aws_secret_access_key=
aws_session_token=

# 第二部分：在操作步驟中逐一複製
Instance_ID=
Public_IPv4_address=
Security_groups=
Username=Administrator
Password=''
Shared_Name_of_Drive_C=C_Drive

# 第三部分：建立環境變數
export AWS_ACCESS_KEY_ID=$aws_access_key_id
export AWS_SECRET_ACCESS_KEY=$aws_secret_access_key
export AWS_SESSION_TOKEN=$aws_session_token
```

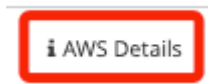
2. 延續前一點，文件底部三行是終端機指令，用於建立環境變數提供 AWS CLI 及 AWS SDK 使用，在後續步驟複製後即可在終端機內貼上運行。

```
# 第三部分：建立環境變數
export AWS_ACCESS_KEY_ID=$aws_access_key_id
export AWS_SECRET_ACCESS_KEY=$aws_secret_access_key
export AWS_SESSION_TOKEN=$aws_session_token
```

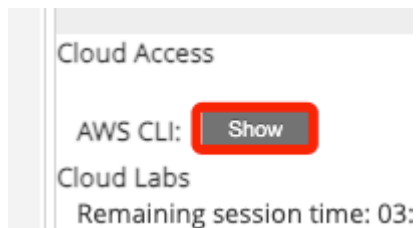
準備 AWS CLI 環境所需配置

在等待實例初始化同時，可先進行 CLI 環境設置

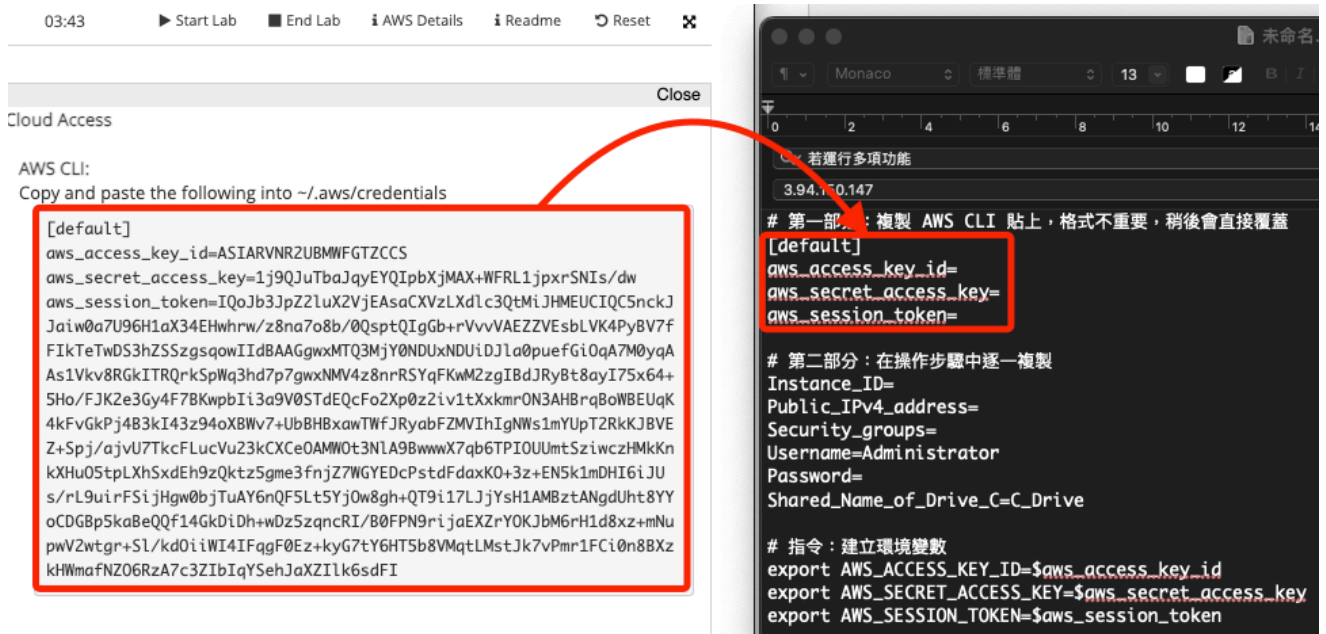
1. 回到 Lab 主頁面，點擊右上角的文字圖標！ **AWS Details**。



2. 在 **AWS CL** 尾端點擊 **Show** 展開內容。



3. 複製展開後的內容，這是 AWS CLI 所需資訊，包含 ID、Key、Token；貼到前面步驟所建立的文檔中。



4. 直接覆蓋原本 **第一部分** 的內容即可，貼上時特別注意尾端不要添加多餘的空格或換行符號，因為後續將直接用於建立環境變數。


```
# 複製 AWS CLI 貼上
[default]
aws_access_key_id=ASIARVNR2UBMY47YXSP4

aws_secret_access_key=Zt70Qh8p1l7ZtETpkoSD6l0cCIzgbGYlq9jIngLs

aws_session_token=IQoJb3JpZ2luX2VjEPj////////
wFaCXVzLXdlc3Q0tMiJGMEQCIcPd1F7FFnWJWeHy+YqExNfL5/
McDizaskl1bFzpbUbAiAMMyN+napk8eH2h7UaHE815hCAsttZz0hFHdJEzmcFYyqjAghhEAAaDDExNDcyNjQ0N
TE0NSIMzzVeysEzAJrxIn2SKoACIEfaUrcXbE/ydqa5BX+q5ubT6VMtc9hby4WEuTasDlCozlKaakJaypki/
AuRT7hIz0scA2b2ndpRfDZQZ3axkR5wh6v65kLDfzPGarGaa/T73mruZWf/
dX2efq4y04CuJerdFe1Vkt4BnPkA5pRwCXkwhwUd9nQIGPyi fvIbcJYERPX1ZUC3KQ9iEibZ583WLnI4dQlNpo
H0IjctJ3AxIN+XGSIQ6uHrFn+OGQA/bgH+j5HHmb06P1d83ZZPuGQR9vg/WqPA7LIZ/k1AvMoBD+Bce9D5ch/
Yszvkl+MrqVW3BpsZ0dLcheagSwcmRBjW0mVadoVx+Pzv4DzTUozUk4DDnqc+4BjaeAVTCeZPoF3M7kzbimG/
YrHy3zFEiPlqZLPCXRtljYYznWg/00FKz7Zlmlj/
pFx2BZ9Es6Eu0QTMyaW9l3kTb6buwTou15JxWdC0qxH96Z6k0TU1NIT0Vy5SsIhrqtKE1IIElmZxl0rn8RHbcl
vEW+uqyZQqT8/86B5hsktrKk50Iu7BUDN9+tER5JrEFf6G3LyJV7JCdayXqZ7mV/RFY
```

5. 先將第一部分指令從 `[default]` 以下進行複製並貼在終端機中。

```
(envAWS) samhsiao@SamdeMac-mini ~ % aws_access_key_id=ASIARVNR2UBMWFGTZCCS
aws_secret_access_key=1j9QJuTbaJqyEYQIpbXjMAX+WFRL1jpxrSNIIs/dw
aws_session_token=IQoJb3JpZ2luX2VjEAsaCXVzLXdlc3Q0tMiJHMEUCIQC5nckJJaiw0a7U96H1aX
34EHwhrw/z8na7o8b/0QsptQIGGb+rVvvVAEZZVESbLVK4PyBV7fFIkTeTwDS3hZSSzsqowIIdBAAGg
wxMTQ3MjY0NDUxNDUiDJla0puefGi0qA7M0yqAAs1Vkv8RGkITRqrkSpWq3hd7p7gwxNMV4z8nrRSYqF
KwM2zgIBdJRyBt8ayI75x64+5Ho/FJK2e3Gy4F7BKwpbIi3a9V0STdEQcFo2Xp0z2iv1tXxkmrON3AHB
rqBowBEUqK4kFvGkPj4B3kI43z94oXBWv7+UbBHBxawTwfJRYabFZMVIhIgNws1mYUpT2RkKJBVEZ+Sp
j/ajvU7TkcFLucVu23kCXCeOAMW0t3NlA9BwwwX7qb6TPIOUmtSziwcZHMkKnkXH05tpLXhSxdEh9z
Qktz5gme3fnjZ7WGYEDcPstdFdaxK0+3z+EN5k1mDHI6iJUs/rL9uirFSijHgw0bjTuAY6nQF5Lt5Yj0
w8gh+QT9i17LJjYsH1AMBztANGdUht8YYoCDGBp5kaBeQQf14GkDiDh+wDz5zqncRI/B0FPN9rijaEXZ
rYOKJbM6rH1d8xz+mNupwV2wtgr+Sl/kd0iIW4IFqgF0Ez+kyG7tY6HT5b8VMqtLMstJk7vPmr1FCi0
n8BXzkHwmafNZO6RzA7c3ZiBiqYSehJaXZiIk6sdFI
(envAWS) samhsiao@SamdeMac-mini ~ %
```

6. 接著複製第三部分在終端機中運行；這是透過 `export` 指令加上符號 `$` 來引用第一部分的 **區域變數** 進行環境變數設置；特別注意，因為暫時未使用 AWS SDK，所以不對其他變數進行設置，僅針對 CLI 中會使用到的這三個變數進行設置。

```
export AWS_ACCESS_KEY_ID=$aws_access_key_id
export AWS_SECRET_ACCESS_KEY=$aws_secret_access_key
export AWS_SESSION_TOKEN=$aws_session_token
```

7. 特別說明 **變數或環境變數** 的生命週期，皆僅限於當前終端視窗，關閉視窗這些變數就會被刪除；在新的工作視窗若需要使用這些變數，必須重新執行以下區塊的指令。

```
# 建立變數
[default]

aws_access_key_id=ASIARVNR2UBMSQJ5BM67
aws_secret_access_key=37IyUsNaZ3G0X3D8FCamXbFVG9Bt8+J4viYGvGKF
aws_session_token=IQoJb3JpZ2luX2VjEAMaCXVzLXdlc3Q0tMiJHMEUCTH4z1rPAUyybV0HXyPJJ6eIx2MpQ4Fv8/
uPmKcVt1avNAiEA8QWvPrL4vc3yb0V+N04vjCdIj3QHf4PS0FYwmfKVMWoqowIIbBAAGgwMTQ3MjY0NDUxNDUiDIebjqVLHtzKxqXQbiq
AAhInlda5UFgDLEpTnTzcfz12+grBVeWXT/61yLwrxr3G6xhRn2kfMnf4iD05444RIML5VinJdlIKKfrvHIn+NcF69koZ5Vkung/
ysX4+ljhOCzVdW8cRoFdXm3Nh4gofKrUS3h0WePLXFkbXicOHJlNCi8I77Lm6JFPP7B8mW1NpCTVWNptuTbySEj0kTU39+jgpmdbARsu8/
Tawru9n2C7zQ58BPIHsboACn2bFqM0a9/
Wrw24DRIiRtnyXlnYxb9sJs2qqFLi5WxMW9GoJUcKvNqh3rn744nvYaN096AzfdrlpgeD6BcxIj7FxfbigTQZ8nPrZpIqzpfG/0lZ/
CkwrtPRuAY6n0HFvWbDYs1ga4PkGYbqaRXA0oIXvGpWQ0GRPftFA6ALheLkLBbn/
EkZUdULNwKxky1FPryBkiYw8cf4ongI7YfYBVo5Gb8vHdlkAvmSIqCQ1dV47P+EnhSPPhmFuHaWaGBBsi.c0vIhdnMZFApW5DKxJbpL8Z
ZJRjCivYk1045UrVw4mLuuFPdiYulc35gIHesPtYb8J0tWCSqoev

# 建立環境變數
export AWS_ACCESS_KEY_ID=$aws_access_key_id
export AWS_SECRET_ACCESS_KEY=$aws_secret_access_key
export AWS_SESSION_TOKEN=$aws_session_token
```

進行 AWS CLI 環境配置

在 Lab 環境中可以省略這個步驟

1. 特別說明，因為 **環境變數** 的優先權是在 **設定檔** 之前，而在 Lab 中 一定要透過環境變數設定 **Token** 進行授權，而 **TOKEN** 一但設定後必須與環境變數中的 **ID** 和 **KEY** 相對應才會生效；假如沒有找到對應的設定則會讀取 `~/.aws` 中的授權資訊，但是在 `~/.aws` 中無法設定 Token，所以在 Lab 環境是將無法這樣配置的。

```
aws configure
```

```
(envAWS) samhsiao@SamdeMac-mini ~ % aws configure
AWS Access Key ID [*****BTHJ]: ASIARVNR2UBMSQJ5BM67
AWS Secret Access Key [*****L1uL]: tS8jZOypjv
BYdmlf
Default region name [us-east-1]:
Default output format [json]:
(envAWS) samhsiao@SamdeMac-mini ~ %
```

2. 這些文檔的具體位置是在 `~/.aws` 中，此處暫不贅述。

```
(envAWS) samhsiao@SamdeMac-mini ~ % cd ~/.aws
(envAWS) samhsiao@SamdeMac-mini .aws % tree

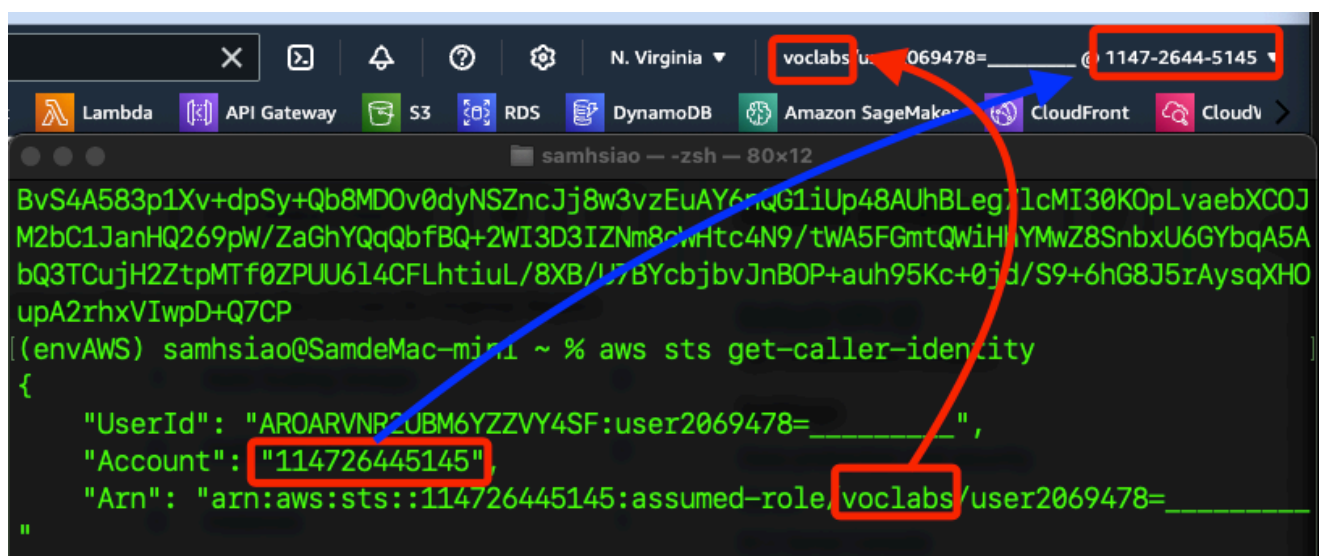
.
├── config
├── credentials
├── sso
│   └── cache
│       ├── 456eb0b848876425acbbae9be0a5de33a24a96a5.json.tmp-74a9d07e
│       ├── aws-toolkit-vscode-client-id-us-east-1-178deade4420b9a4a9a43e8c4f6a2
│       ├── dc9f57167065a547049d7c12da566d1fec3.json
│       └── aws-toolkit-vscode-client-id-us-east-1-d4a6d74660e1188d28597f1c746b8
│           35e69ede3e1ac7527dcdbd1d31f16109623.json
└── 3 directories, 5 files
```

檢查 AWS CLI 設置已完成

運行以下基本指令來確認設置

1. 確認當前用戶。

```
aws sts get-caller-identity
```



2. 返回的結果中會顯示角色的 資源名稱 (ARN)，在這就是 **voclabs**；特別注意，其中 **user2069478** 是當前 AWS 會話中的一個具體 用戶身份，附加在 **voclabs** 角

色之下，用來追蹤和標識用戶的操作。

```
(envAWS) samhsiao@SamdeMac-mini ~ % aws sts get-caller-identity
{
  "UserId": "AROARVNR2UBM6YZZVY4SF:user2069478=_____",
  "Account": "114726445145",
  "Arn": "arn:aws:sts::114726445145:assumed-role/voclabs/user2069478=_____"
}
(envAWS) samhsiao@SamdeMac-mini ~ %
```

3. 列出角色的附加權限。

```
aws iam list-attached-role-policies --role-name voclabs
```

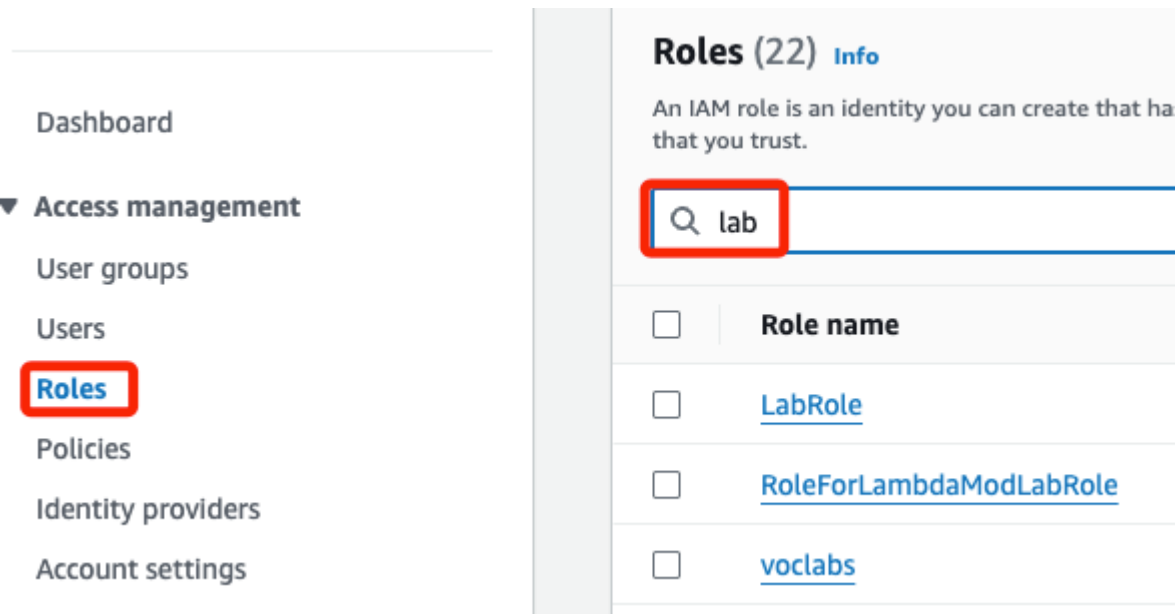
```
{
  "AttachedPolicies": [
    {
      "PolicyName": "voc-cancel-cred",
      "PolicyArn": "arn:aws:iam::114726445145:policy/voc-cancel-cred"
    }
  ]
}
```

4. 檢查該角色的內嵌策略。

```
aws iam list-role-policies --role-name voclabs
```

```
(envAWS) samhsiao@SamdeMac-mini ~ % aws iam list-role-policies --role-name voclabs
{
  "PolicyNames": [
    "Pvoclabs"
  ]
}
```

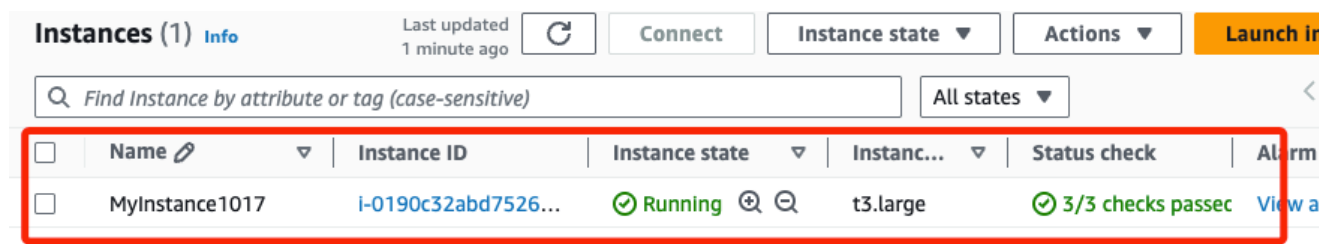
5. 關於跟 Lab 相關的角色，可進入主控台查看如下；具體點擊查看可以知道，Lab 環境對於角色的授權相當有限，此處不做贅述。



取得實例連線的帳號與密碼

回到 EC2 實例，這時應該已經完成 *Status check*，特別注意，並非以 *Instance state* 的 *Running* 作為確認資訊，而是要確認實例已經功過檢查。

1. 務必確認所有狀態都已完成。



2. 勾選實例，先複製下方 *ID* 及 *IP* 到紀錄中；特別注意，*ID* 並不包含尾端括號及括號內字串，點擊複製圖標時，也不會將其複製，此後不再贅述。

Table with 4 columns: ☒, Name, Instance ID, Instance state.

<input checked="" type="checkbox"/>	MyInstance1017	i-0190c32abd7526...	Running
-------------------------------------	----------------	---------------------	---------

i-0190c32abd7526432 (MyInstance1017)

Details | Status and alarms | Monitoring | Security | Net

▼ Instance summary Info

Instance ID
i-0190c32abd7526432 (MyInstance1017)

Public IPv4 address
44.205.11.13 | open

3. 接著切換到 **Security** 頁籤，複製 **Security groups** 的 ID 到紀錄中。

Table with 4 columns: ☒, Name, Instance ID, Instance state.

<input checked="" type="checkbox"/>	MyInstance1017	i-0190c32abd7526...	Running
-------------------------------------	----------------	---------------------	---------

i-0190c32abd7526432 (MyInstance1017)

Details | Status and alarms | Monitoring | **Security** | Net

▼ Security details


IAM Role
-

Owner ID
114726445145





Security groups
sg-08cee57891d0276ed (launch-wizard-2)

4. 接著點擊上方頁籤中的 **Connect**。

Instances (1/1) [Info](#)

Last updated less than a minute ago  **Connect** Instance state ▼ Action

Find Instance by attribute or tag (case-sensitive)


<input checked="" type="checkbox"/>	Name 	Instance ID	Instance state
<input checked="" type="checkbox"/>	win20241017	i-0114836e36c8d7e9d	 Running  

5. 切換到 **RDP client** 頁籤，點擊下方 **Get password**。

Connect to instance [Info](#)


Connect to your instance i-0114836e36c8d7e9d (win20241017) using any of these options

Session Manager **RDP client** EC2 serial console


Instance ID
 i-0114836e36c8d7e9d (win20241017)

Connection Type


☒ **Connect using RDP client**
Download a file to use with your RDP client and retrieve your password.


☐ Connect using Fleet Manager
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#) 

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:


 **Download remote desktop file**

When prompted, connect to your instance using the following username and password:

Public DNS
 ec2-52-87-159-155.compute-1.amazonaws.com

Username [Info](#)
 Administrator ▼

Password **Get password**

 If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

6. 點擊 **Upload private key file** 上傳密鑰，選取前面步驟下載到本地的密鑰文件 ***.pem**，選取後點擊右下角 **Decrypt password** 將 **Private Key** 解密成密碼。

Private key

Either upload your private key file or copy and paste its contents into the field below.

↑ Upload private key file

✓ MyKey20241017.pem
1.674KB

Private key contents - optional

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAtQHGVv5Y7TytbU1P/r3GhcV1oxNRozZ/a4yJbAxx3a9wZJxL
gGN4vuOwAkIfMQEqnoxvHDibvnlqcM+EkxNfF5ERgpHfBul8CfeRtivdpTnDuWui
HuIFV+RtLLJVyskn4sIFOW3gPFRVWvYQKiNaYQTvISrOOy2AhlqfNmiiirOEE3Hy
OZAW09ODS+njTQU3E74A0MoSnnzRWNIYoZEYJdNltlKZClBss7yaQ/sWkBz//8MO
Nicjrl/MxFLRqAyXuFNP4CfroKny6P6CT1kRZZOmds9Yi1EbwQNx5qnZOEIU/d8r
7w7kTh12VVohql698FBaBFQKEHiODO9rl+7oTQIDAQABAoIBABa0o0m0XDlePC8S
3K8K5UVQkMILIT+FDZTTK0XnhXzcjg/A32O6lqHzc9fErZ77E3q5CToUC81n86c1
```

Cancel

Decrypt password

7. 解密後可看到這組密碼是可讀的；紀錄其中 Username、Password。

Session Manager

RDP client

EC2 serial console

Instance ID

📄 i-0114836e36c8d7e9d (win20241017)

Connection Type

☒ Connect using RDP client

Download a file to use with your RDP client and retrieve your password.

☐ Connect using Fleet Manager

To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#) 📄

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

↓ Download remote desktop file

When prompted, connect to your instance using the following username and password:

Public DNS

📄 ec2-52-87-199-155.compute-1.amazonaws.com

Username [Info](#)

📄 Administrator ▼

Password

📄 5=W\$wwgGzkSOx1Lh=2xk}wD3o4YDnCJG

📘 If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

8. 至此 第二部分 也完全填補完成，複製後貼到終端機運行一次。

```
# 第二部分：在操作步驟中逐一複製
Instance_ID=i-00b830b4e66fe2705
Public_IPv4_address=3.216.126.33
Security_groups=sg-02cef58f67e93c0fc
Username=Administrator
Password=LKZV5*XU)UIY3IMGI@t6fE4&lel8(Z5X
Shared_Name_of_Drive_C=C_Drive
```

9. 特別說明，解密後的密碼有時會包含括號)、驚嘆號 ! 等特殊字元，這些字元作為指令運行時會被解析為特殊符號；所以在密碼的部分使用單引號 ' ' 將字串包覆，特別注意，要使用單引號而不是雙引號。

```
# 第二部分：在操作步驟中逐一複製
Instance_ID=i-00e0861b9bedb37cc
Public_IPv4_address=3.94.132.156
Security_groups=sg-00e795396d1621e15
Username=Administrator
Password='8;duyy)x=EW2wLQqXcEMJJwHl=rOsVrP'
Shared_Name_of_Drive_C=C_Drive
```

10. 點擊 Download remote desktop file 下載連線遠端桌面所需連結。

Instance ID


 i-0114836e36c8d7e9d (win20241017)

Connection Type

☒ Connect using RDP client

Download a file to use with your RDP client and retrieve your password.

☐ Connect using Fleet Manager

To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#) 

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

 **Download remote desktop file**

When prompted, connect to your instance using the following username and password:


Public DNS

 ec2-52-87-199-155.compute-1.amazonaws.com

Username [Info](#)

 Administrator ▼

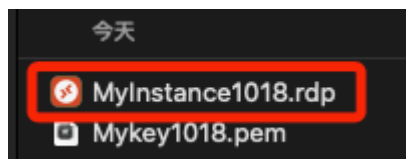
Password [Get password](#)

 If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

連線

以下步驟可能因為使用的遠端工具不同而不同

1. 點擊下載的 *.rdp 文件進行連線；這是一個與實例同名的文件。



2. 勾選並點擊 連線。



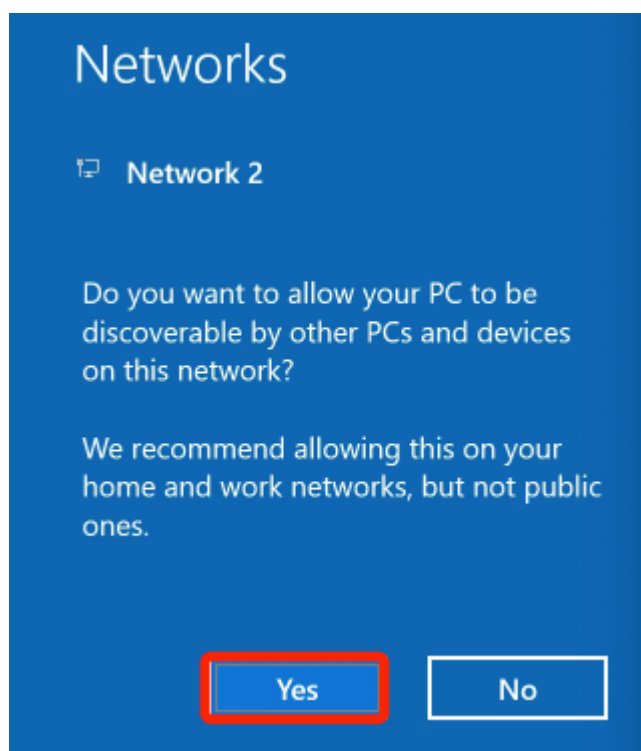
3. 輸入密碼並勾選 **記住我**，然後點擊 **確認**。



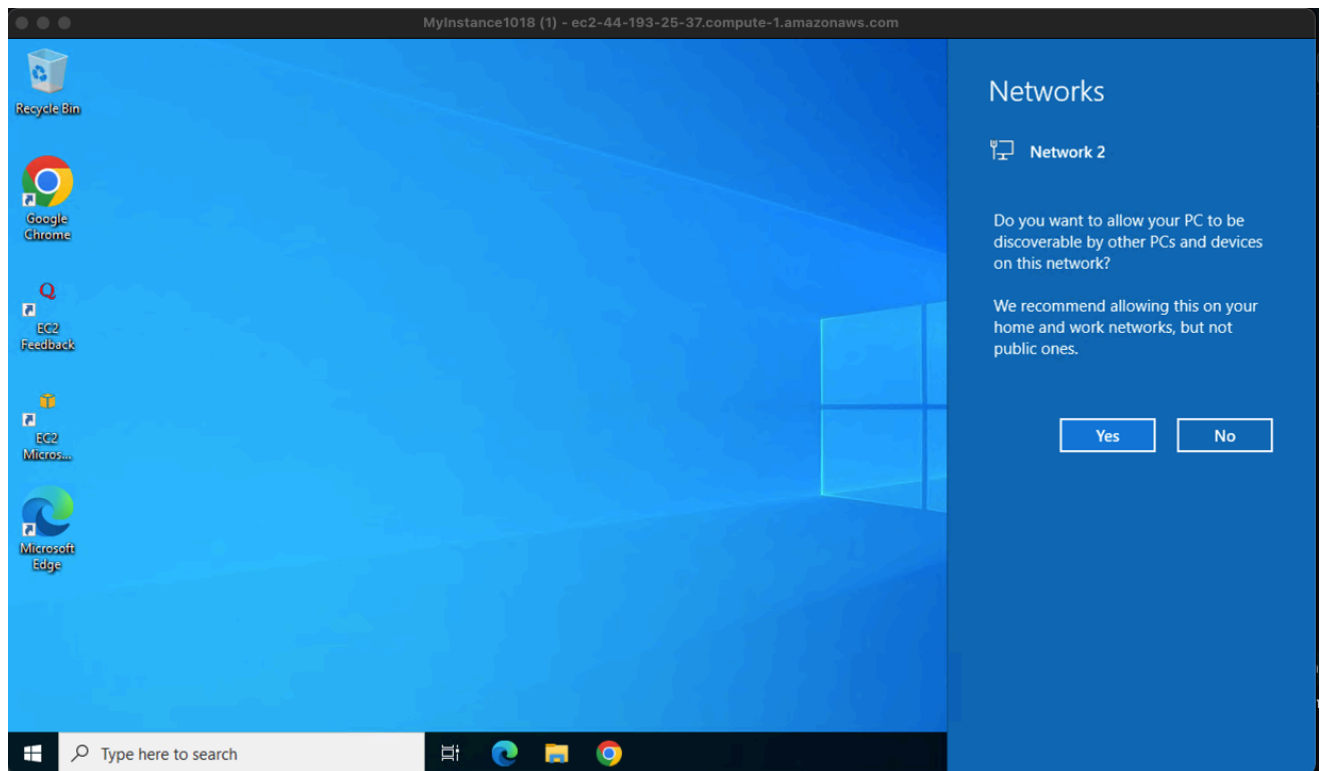
4. 勾選 **不要再詢問** 後點擊 **是**。



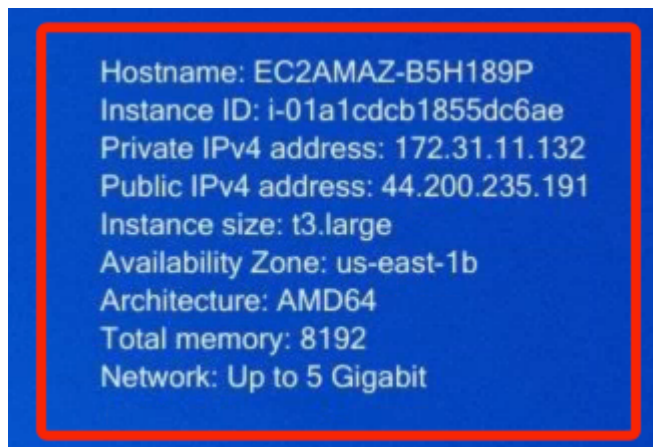
5. 進入到桌面，會詢問是否允許其他設備在網路上發現這台電腦，點擊 **YES** 即可。



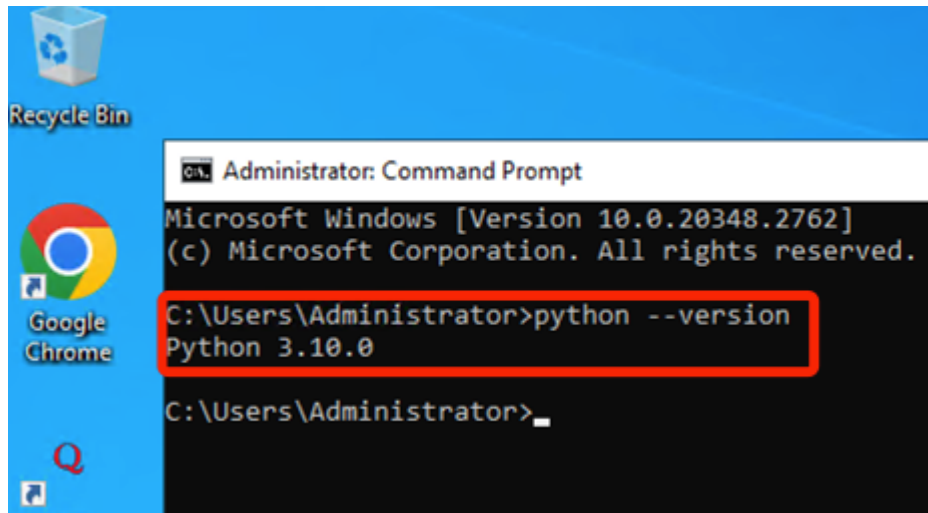
6. 假如在 **User data** 還寫入了其他應用如 **Chrome** 等的安裝指令時，啟動就會看到桌面捷徑。



7. 畫面右側會有詳細連線資訊。



8. 開啟 Windows 的 CMD，透過指令 `python --version` 驗證 Python 版本以確定完成安裝。



關於使用 AWS CLI 建立實例的錯誤

1. 使用 CLI 建立並登入伺服器後，透過查詢 Python 版本會發現 Python 並未順利完成安裝，這就代表 User Data 並未順利進行。

```
C:\Users\Administrator>python --version
'python' is not recognized as an internal or external command,
operable program or batch file.
```

2. 觀察實例日誌文檔顯示，系統在解析 User Data 時先嘗試 YAML 格式失敗，然後退回至 XML 格式也失敗；日誌文檔位置在 C:\ProgramData\Amazon\EC2Launch\log\ 中。

```
Failed to unmarshal user data as YAML: yaml: unmarshal errors:
line 1: cannot unmarshal !!str `PHBvd2V...` into task.UserDataSchema
0xc00009d3f8
```

驗證 base64 編碼

透過反向編碼驗證

1. 在前面步驟中，因為輸入的指令是 明文 的，下方這個勾選框可以不用選。

☐ User data has already been base64 encoded

2. 在點擊 **Preview code** 後，在預覽視窗中可看到所生成的指令自動將 Powershell 指令轉換成 base64 編碼。

Launch instance

 Preview code

3. 實例建立後，卻會在日誌中會看到如下的訊息表示 User Data 被編碼成為 Base64 格式，但沒有使用 Base64 解碼來解析它。

```
2024-10-20 19:48:59 Warning: No XML or YAML user data detected. If XML or YAML user data is intended, check for typos or refer to documentation (https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2launch-v2-settings.html#ec2launch-v2-example-user-data): %!w(*fmt.wrapError=&{Failed to unmarshal user data as YAML: yaml: unmarshal errors: [line 1: cannot unmarshal !!str `PHBvd2V...` into task.UserDataSchema 0xc0000b3158}]})
```

4. 進一步透過指令從指定的實例中取得解碼後的 User Data 並儲存在變數 **UserDataDecoded** 中；特別注意，取回的內容雖已成功解碼，但仍是 Base64 編碼的形式保存在變數中。

```
USER_DATA_DECODE=$(aws ec2 describe-instance-attribute --instance-id $Instance_ID --attribute userData --query "UserData.Value" --output text | base64 --decode)
```

5. 透過解碼來查看內容，可以確認內容是正確的，但是 AWS 卻無法順利解析，這應該是 AWS 的一個 Bug。

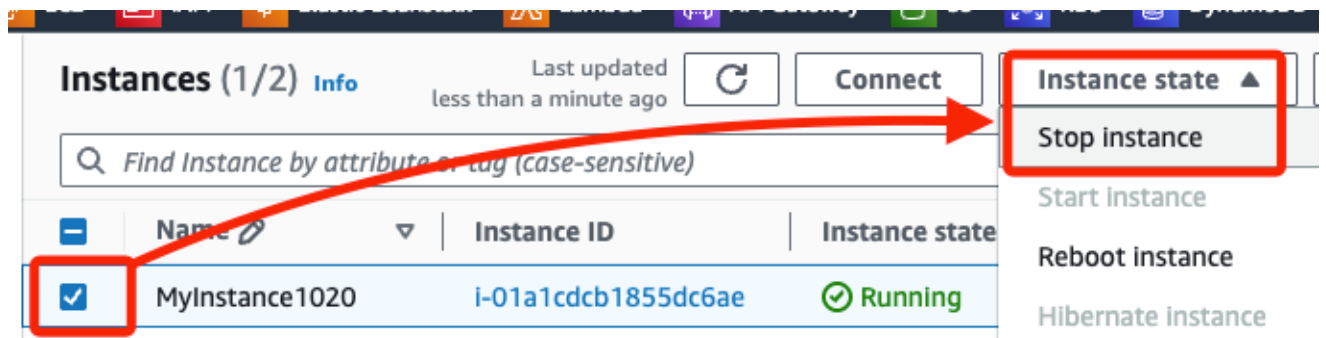
```
echo $USER_DATA_DECODE | base64 --decode
```

```
(envAWS) samhsiao@SamdeMac-mini ~ % echo $USER_DATA_DECODE | base64 --decode
<powershell>
# 下載並安裝 Python
Invoke-WebRequest -Uri "https://www.python.org/ftp/python/3.10.0/python-3.10.0-amd64.exe" -OutFile "C:\python-installer.exe"
Start-Process -FilePath "C:\python-installer.exe" -ArgumentList "/quiet InstallAllUsers=1 PrependPath=1" -Wait
Remove-Item -Path "C:\python-installer.exe"
</powershell>%
(envAWS) samhsiao@SamdeMac-mini ~ %
```

重新編輯 User Data

特別注意，這裡無法透過編輯 **User Data** 進行修正，因為在預設情況下，**User Data** 只會在首次啟動時執行；如需在每次啟動皆運行 **User Data** 需添加語句 `<persist>true</persist>`；同理，當 **User Data** 只運行一次時，對其進行編輯後重啟並不會生效，所以有修改需求時，需在建立實例時便預先寫入語句 **User data**；以下僅就修改方式做補充說明，另外，實例並無重啟的功能，所謂的重啟泛指停止之後再啟動。

1. 首先，系統會要求停止啟動中的實例才允許進行編輯。



2. 展開 **Actions** 選單，在 **Instance setting** 中點擊 **Edit user data**。

Instances (1/1) Info Last updated 3 minutes ago [Refresh] [Connect] [Instance state] [Actions] [Launch]

Find Instance by attribute or tag (case-sensitive) All state

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instanc...
<input checked="" type="checkbox"/>	MyInstance1017	i-0190c32abd7526...		

i-0190c32abd7526432 (MyInstance1017)

Details Status and alarms Monitoring

▼ Instance summary Info

Instance ID
I-0190c32abd7526432 (MyInstance1017)

IPv6 address
-

Hostname type
IP name: ip-172-31-15-238.ec2.internal

Public IP address
-

Instance state
Stopped

Private IP address
ip-172-31-15-238

Private IPv4 addresses
172.31.15.238

Public IPv4 DNS
-

Actions dropdown menu:

- Attach to Auto Scaling Group
- Change termination protection
- Change stop protection
- Change shutdown behavior
- Change auto-recovery behavior
- Change instance type
- Change CPU options
- Change Nitro Enclaves
- Change credit specification
- Change resource based naming options
- Modify instance placement
- Modify Capacity Reservation settings
- Edit user data**
- Allow tags in instance metadata

Instance settings:

- Networking
- Security
- Image and templates
- Monitor and troubleshoot
- Tags

3. 使用預選的 **Modify user data text** 選項以編輯方式進行修正，將更新代碼填寫在下方輸入框中，完成後點擊 **Save**。

New user data
This user data will replace the current user data

☒ **Modify user data as text**
Add your user data below

☐ **Modify user data by importing a file**
Description of importing a file and what will happen to it

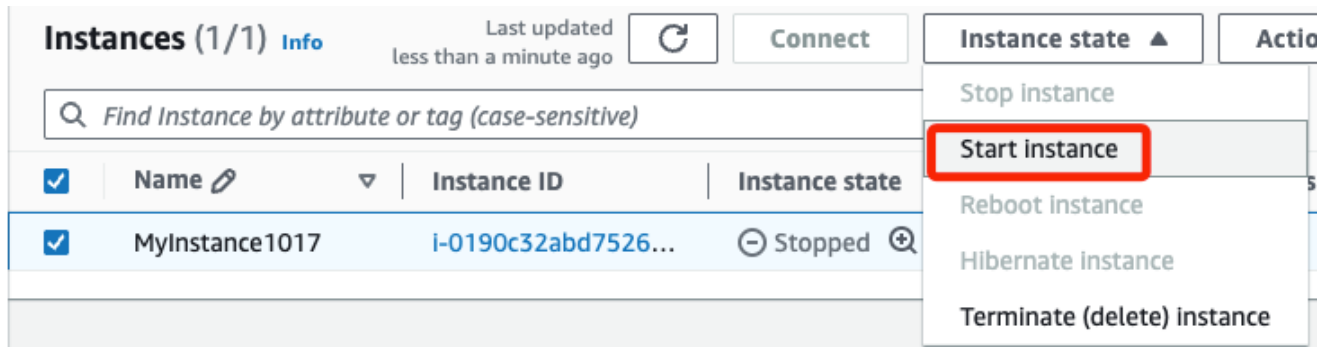
```
</powershell>

<persist>
@echo off
curl -L -o C:\xampp-installer.exe https://sourceforge.net/projects/xampp/files/XAMPP%20Windows/8.0.30/xampp-windows-x64-8.0.30-0-VS16-installer.exe/download
```

☐ Input is already base64-encoded

Cancel **Save**

4. 重新啟動實例。



5. 實例重啟之後必須下載新的 **remote desktop file** 進行連線。

You can connect to your Windows instance using
running the RDP shortcut file below:



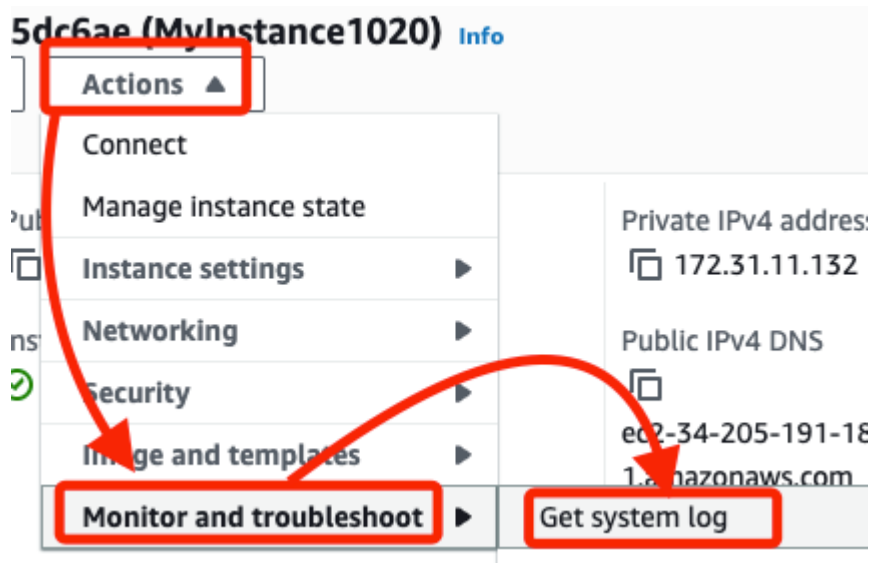
關於生成實例的錯誤處理

可積極地進行例外捕捉，或在錯誤發生後觀察日誌

1. 在 **PowerShell** 中可加入 **例外捕捉** 語句進行錯誤處理，確保初始化過程不會因為錯誤而中斷，以下就安裝 **Python** 作為示範，加入 **try...catch** 拋出可能的錯誤。

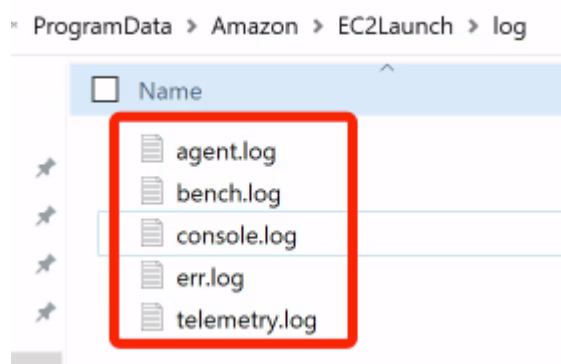
```
try {
    Invoke-WebRequest -Uri
    "https://www.python.org/ftp/python/3.10.0/python-3.10.0-amd64.exe" -
    OutFile "C:\python-installer.exe"
    Start-Process -FilePath "C:\python-installer.exe" -ArgumentList
    "/quiet InstallAllUsers=1 PrependPath=1" -Wait
    Remove-Item -Path "C:\python-installer.exe"
} catch {
    Write-Host "Python 安裝失敗: $_"
}
```


2. 若要在日誌中查看實例運行，展開 **Actions** 選單，在 **Monitor and troubleshoot** 中點擊 **Get system log** 可查看實例運行的紀錄文件。



3. 安裝完成後，可在實例的檔案管理中在以下路徑查看日誌，其中 **agent.log**、**bench.log**、**console.log** 皆紀錄了部分 **User Data** 相關資訊；其中 **agent** 說明 **EC2Launch agent** 操作，**bench** 部分紀錄系統與網路資源，**console** 部分是紀錄控制台訊息。

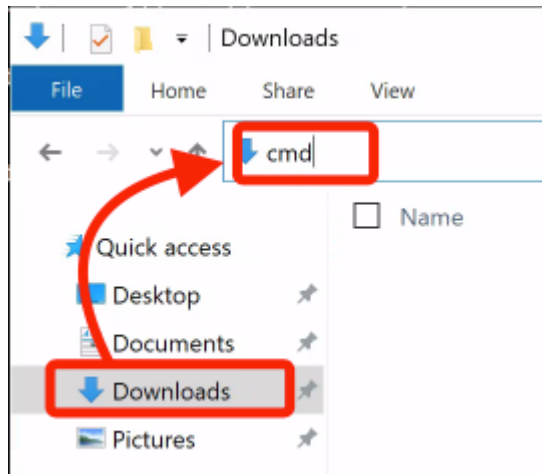
C:\ProgramData\Amazon\EC2Launch\log\



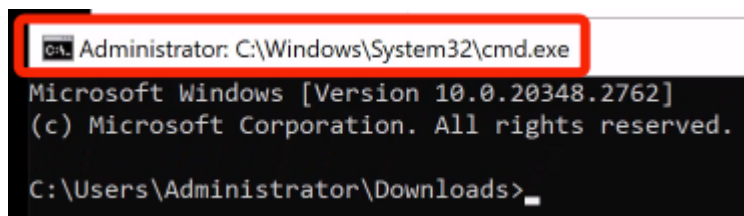
手動 安裝 XAMPP

使用 CMD 指令在 Windows 伺服器中安裝 XAMPP 來管理 Apache 服務

1. 進入 Windows 伺服器的檔案總管，在 **Downloads** 資料夾的路徑欄中輸入 **cmd** 開啟 CMD。

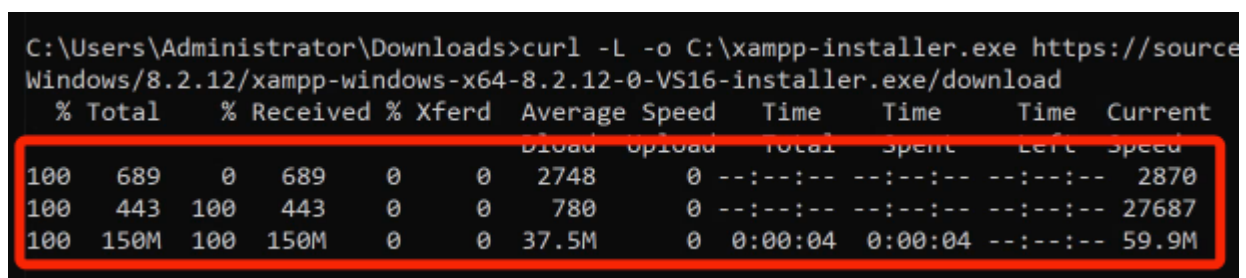


2. 預設就會使用 **Administrator** 身份開啟，CMD 所在路徑就是 **Downloads**。



3. 接著使用指令下載 XAMPP 安裝程式；版本資訊可參考 [官網](#)，這裡下載的是 **8.2.12**。

```
curl -L -o C:\xampp-installer.exe  
https://sourceforge.net/projects/xampp/files/XAMPP%20Windows/8.2.12/xam  
pp-windows-x64-8.2.12-0-VS16-installer.exe/download
```



4. 使用無人值守模式自動化部署、安裝 **XAMPP** 到 **C:\xampp** 目錄；**unattended** 模式下安裝過程不會提示用戶進行任何輸入或確認；**無人值守** 模式對於自動化部署來

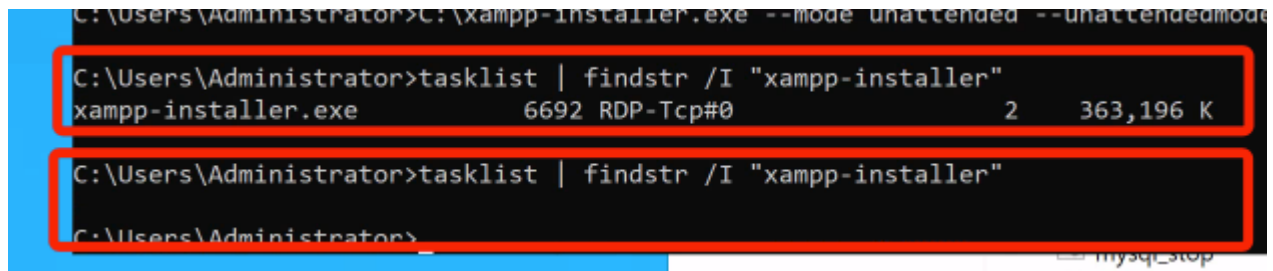
說非常實用，安裝會在完全無需手動的看框下使用預設選項進行。

```
C:\xampp-installer.exe --mode unattended --unattendedmodeui none --  
prefix C:\xampp
```

5. 因為畫面不會有任何顯示，若要查詢安裝進度，需查看 **安裝進程是否結束** 來確定安裝是否完成；這個過程約略需要五分鐘，甚至更多。

```
tasklist | findstr /I "xampp-installer"
```

6. 直到確認進程消失代表安裝已經結束，然後再繼續後續步驟。



```
C:\Users\Administrator>C:\xampp-installer.exe --mode unattended --unattendedmode  
C:\Users\Administrator>tasklist | findstr /I "xampp-installer"  
xampp-installer.exe        6692  RDP-Tcp#0           2    363,196 K  
C:\Users\Administrator>tasklist | findstr /I "xampp-installer"  
C:\Users\Administrator>
```

7. 刪除安裝檔案。

```
del C:\xampp-installer.exe
```

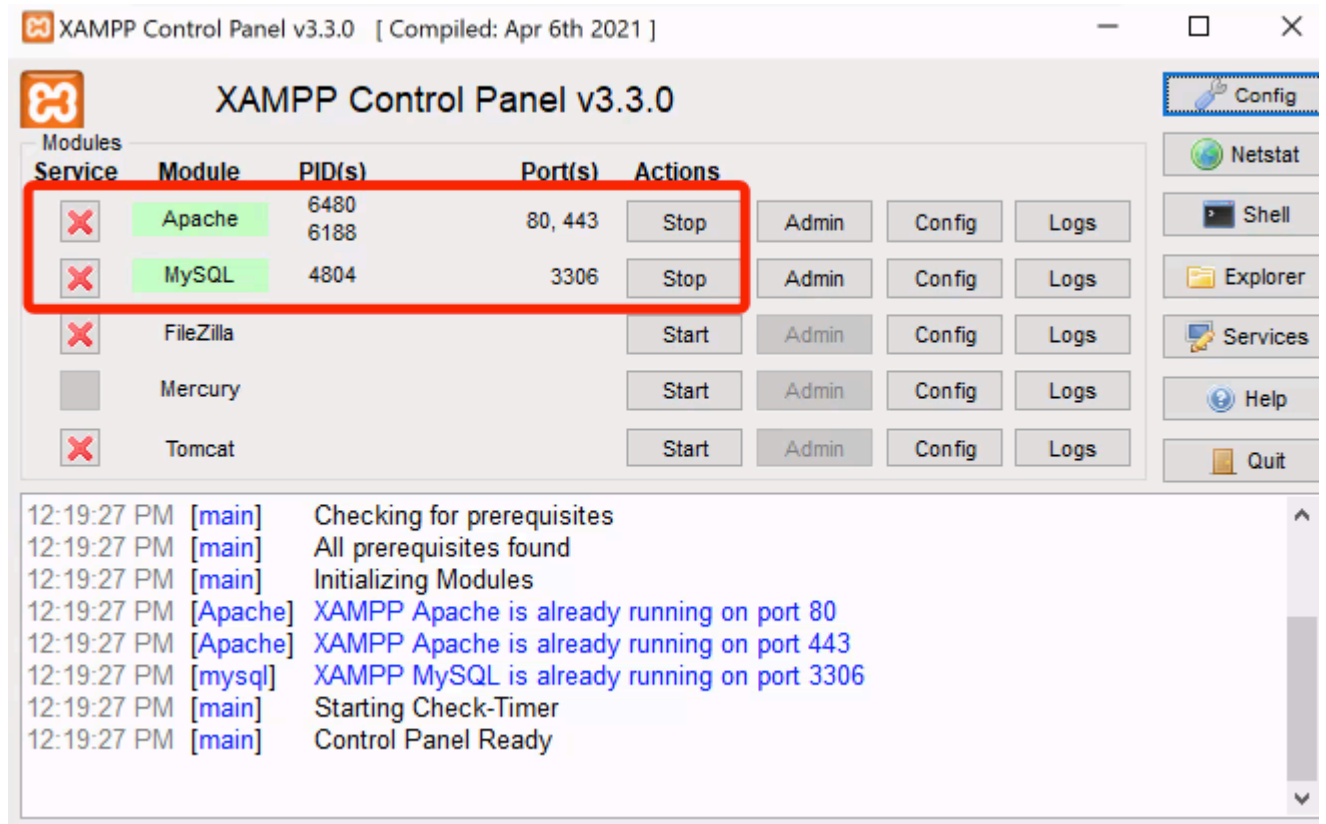
8. 啟動 Apache 和 MySQL 服務；使用 **start** 指令載不阻塞終端的情況下同時啟動以下兩個服務，**""** 是提供給 **start** 指令的終端機空標題；**/min** 參數來最小化批次運行，這樣第二個指令視窗不會等待使用者按下 **ENTER**。

```
start /min "" C:\xampp\apache_start.bat  
start /min "" C:\xampp\mysql_start.bat
```

9. 啟動 XAMPP 應用。

```
start "" C:\xampp\xampp-control.exe
```

10. 應用程式視窗，可看到兩個服務已經啟動，並且顯示了運行端口。



END