

Lab: 以 SSH 方式登入到伺服器不需要輸入密碼

目的: Server1 使用者 user3 以及 user4

以 SSH 方式以使用者 max 身份登入到 Server2 不需要輸入密碼驗證

請於 Server2

```
#su - max -c "mkdir /home/max/.ssh" <建立.ssh 資料夾存放金鑰>
```

請於 Server1

```
#useradd -m user3 <新增使用者>
```

```
#useradd -m user4 <新增使用者>
```

```
server1:~ # su - user3 <切換為使用者 user3>
```

```
user3@server1:~> ssh-keygen -d <以 DSA 方式建立 ssh 金鑰>
```

Generating public/private dsa key pair.

Enter file in which to save the key (/home/user3/.ssh/id_dsa): <儲存位置:請輸入 Enter>

Created directory '/home/user3/.ssh'.

Enter passphrase (empty for no passphrase): <金鑰密碼:請輸入 Enter>

Enter same passphrase again: <金鑰密碼:請輸入 Enter>

Your identification has been saved in /home/user3/.ssh/id_dsa.

Your public key has been saved in /home/user3/.ssh/id_dsa.pub.

The key fingerprint is:

8d:e5:24:eb:98:71:f4:c6:01:96:fc:78:23:f8:d0:02 user3@server1

```
user3@server1:~> cd /home/user3/.ssh <切換到使用者家目錄下.ssh 目錄>
```

```
user3@server1:~/ssh> ls <應該會看到公鑰及私鑰>
```

```
id_dsa id_dsa.pub
```

將公鑰複製到 Server2

```
user3@server1:~/ssh> scp id_dsa.pub max@主機的 IP:/home/max/.ssh/authorized_keys
```

The authenticity of host '192.168.235.129 (192.168.235.129)' can't be established.

RSA key fingerprint is 10:a4:50:0f:00:06:98:e3:c2:56:d4:0e:3f:03:d1:65.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '192.168.235.129' (RSA) to the list of known hosts.

Password: <請輸入 max 的密碼>

```
id_dsa.pub 100% 1115 1.1KB/s 00:00
```

```
user3@server1:~/ssh> logout <登出>
```

接下來針對使用者 user4 來建立金鑰

```
server1:~ # su - user4
```

<切換為使用者 user4>

```
user4@server1:~> ssh-keygen -d
```

<以 DSA 方式建立 ssh 金鑰>

Generating public/private dsa key pair.

Enter file in which to save the key (/home/user4/.ssh/id_dsa):

<儲存位置:請輸入 Enter>

Created directory '/home/user4/.ssh'.

Enter passphrase (empty for no passphrase):

<金鑰密碼:請輸入 Enter>

Enter same passphrase again:

<金鑰密碼:請輸入 Enter>

Your identification has been saved in /home/user4/.ssh/id_dsa.

Your public key has been saved in /home/user4/.ssh/id_dsa.pub.

The key fingerprint is:

c8:0c:56:cb:6c:7a:1f:1d:5f:e8:6e:09:83:f0:0b:81 user4@server1

```
user4@server1:~> cd /home/user4/.ssh/ <切換到使用者家目錄下.ssh 目錄>
```

將公鑰複製到 Server2

```
user4@server1:~/.ssh> ssh-copy-id -i /home/user4/.ssh/id_dsa.pub max@主機的 IP
```

The authenticity of host '192.168.3.128 (192.168.3.128)' can't be established.

RSA key fingerprint is 4e:52:bf:ad:59:bf:59:33:af:62:d2:c7:72:40:78:e0.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '192.168.3.128' (RSA) to the list of known hosts.

Password:

<請輸入 max 的密碼>

Now try logging into the machine, with "ssh 'max@192.168.3.128'", and check in:

```
.ssh/authorized_keys
```

to make sure we haven't added extra keys that you weren't expecting.

測試:

請於 Server2 上面觀察

```
#cat /home/max/.ssh/authorized_keys
```

請於 Server1 上面

以 user3 及 user4 身份

```
ssh max@主機的 IP
```

或是

```
ssh -l max 主機的 IP
```

Lab:

ssh 只接受 key 驗證, 不接受密碼驗證, 並只接受 SSH Version2 連線



Client (**Server1**):

之前練習已經有做過 key 驗證

```
#su - user4
```

<切換使用者 user4>

```
>ssh -l max 遠端主機的 IP
```

<當初有交換 max 的 key 驗證,故不要求提供密碼>

```
遠端> exit
```

<登出遠端,回到本機>

```
>ssh -l root 遠端主機的 IP
```

<當初沒有交換 root 的 key 驗證,故要求提供密碼>

<此時除了 key 驗證還有密碼驗證>

請於 Server (**Server2**) :

修改相關設定

```
#vi /etc/ssh/sshd_config
```

<修改相關設定>

```
UsePAM no
```

```
PasswordAuthentication no
```

```
Protocol 2
```

```
#rcsshd restart
```

<重新啟動 sshd>

測試

請於 Client 端

```
#su - user4
```

<切換使用者 user4>

```
>ssh -l root 遠端主機的 IP
```

<當初沒有交換 root 的 key 驗證,直接拒絕>

請將設定回復預設值

```
#vi /etc/ssh/sshd_config
```

<修改相關設定>

```
UsePAM yes
```

```
PasswordAuthentication no
```

```
Protocol 2
```

```
#rcsshd restart
```

<重新啟動 sshd>