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 方式用 sles 身份登入到 Server2 ， 並且不需要輸入密碼驗證

Machine and HostName	IP
Server1 - linux-k73k	192.168.1.114
Server2 - linux-za1i	192.168.1.113

- 請於 Server2 建立 `.ssh` 資料夾來存放金鑰

```
linux-za1i:~ # su - sles -c "mkdir /home/sles/.ssh"
```

- 請於 Server1 內操作
  - 新增使用者 `user3` 和 `user4`

```
linux-k73k:~ # useradd -m user3
linux-k73k:~ # useradd -m user4
```

- 切換使用者 **user3** ，並以 **DSA** 方式建立 ssh 金鑰

```
linux-k73k:~ # su - user3
user3@linux-k73k:~> ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/user3/.ssh/id_dsa):   <儲存位置：請按
Enter>
Created directory '/home/user3/.ssh'.
Enter passphrase (empty for no passphrase):                      <金鑰密碼：請按
Enter>
Enter same passphrase again:                                     <金鑰密碼：請按
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:
SHA256:1A5lA4jQV5w5OyCL4XxnwOqGUiP9hwdNBskim1kLkXk user3@linux-k73k
The key's randomart image is:
+---[DSA 1024]----+
|.+.=.+ +o++      |
|= E O * =+ .     |
| % * O .oo.      |
|= X + +.oo       |
| = + =  S..      |
|o o o o          |
|..   o           |
|                 |
|                 |
+----[SHA256]-----+
```

- 請切換至使用者 → **user3** 家目錄底下 **.ssh** 目錄，應該會看到公鑰及私鑰

```
user3@linux-k73k:~> cd /home/user3/.ssh/
user3@linux-k73k:~/.ssh> ls
id_dsa  id_dsa.pub
```

- 請將 **user3 公鑰**複製到 Server2 後，請登出
  - 格式:
    `scp key_name.pub username@Server2_IP:/home/username/.ssh/authorized_keys`

```
user3@linux-k73k:~/.ssh> scp id_dsa.pub sles@192.168.1.113:/home/sles/.ssh/auth
orized_keys
The authenticity of host '192.168.1.113 (192.168.1.113)' can't be established.
ECDSA key fingerprint is SHA256:nLC+OEaJPMHqTDoRj+Qx4c2H/OdDaBXbh8YVwigawjI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.113' (ECDSA) to the list of known hosts.
Password:  <請輸入 sles 密碼>
id_dsa.pub                                    100%  606     0.6KB/s   00:00
user3@linux-k73k:~/.ssh> logout
```

- 請切換至使用者 → **user4** ， 並且以 **DSA** 方式建立 ssh 金鑰

```
linux-k73k:~ # su - user4
user4@linux-k73k:~> ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/user4/.ssh/id_dsa):   <儲存位置：請按
Enter>
Created directory '/home/user4/.ssh'.
Enter passphrase (empty for no passphrase):                      <金鑰密碼：請按
Enter>
Enter same passphrase again:                                     <金鑰密碼：請按
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:
SHA256:TYWH9lxZrcy4Bi8GAUEs15xWg7GGdv+Yj6kG/wQZq20 user4@linux-k73k
The key's randomart image is:
+---[DSA 1024]----+
|     o+=.=oo.  oo|
|    . o.B.+o. o .|
|     oo.=o.+ = . |
|     . o.B. + +  |
|        S.oo .   |
|      .o .o++    |
|      .oE.+o.    |
|       .o. +     |
|       ..o+ .    |
+----[SHA256]-----+
```

- 請切換至使用者 → **user4** 家目錄底下 **.ssh** 目錄，一樣會看到公鑰及私鑰

```
user4@linux-k73k:~> cd /home/user4/.ssh/
user4@linux-k73k:~/.ssh> ls
id_dsa  id_dsa.pub
```

- 請將 **user4 公鑰**複製到 Server2 後，請登出

- 格式:
  `ssh-copy-id -i /home/username/.ssh/id_dsa.pub username@Server2_IP`

```
user4@linux-k73k:~/.ssh> ssh-copy-id -i /home/user4/.ssh/id_dsa.pub sles@192.16
8.1.113
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/user4/.ssh
/id_dsa.pub"
The authenticity of host '192.168.1.113 (192.168.1.113)' can't be established.
ECDSA key fingerprint is SHA256:nLC+OEaJPMHqTDoRj+Qx4c2H/OdDaBXbh8YVwigawjI.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
 out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are promp
ted now it is to install the new keys
Password:  <請輸入 sles 密碼>

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'sles@192.168.1.113'"
and check to make sure that only the key(s) you wanted were added.
user4@linux-k73k:~/.ssh> exit
```

驗證測試

- 請於 Server2 上面觀察

```
linux-za1i:~ # cat /home/sles/.ssh/authorized_keys
```

- 請於 Server1 上面觀察

```
linux-k73k:~ # su - user3
user3@linux-k73k:~> ssh sles@192.168.1.113
Last login: Tue Nov 14 05:35:15 2017 from console
sles@linux-za1i:~>
```

```
linux-k73k:~ # su - user4
user4@linux-k73k:~> ssh -l sles 192.168.1.113
Last login: Tue Nov 14 07:26:40 2017 from 192.168.1.114
sles@linux-za1i:~>
```