利用公鑰進行檔案傳輸使用說明

OscarLi@nchc.narl.org.tw

利用 SSH 的公鑰認證可以免除重複輸入密碼的不便，特別是當您需要建立一個自動化的工作流程作業時。目前台灣杉一號高速計算主機上的檔案傳輸節點(xdata1, xdata2)均提供 SSH 連線服務，因此可以利用 SSH 服務內建的公鑰認證機制，來達成免密碼登入。本說明文件將針對用戶連線過程使用的 Windows 與 Linux 作業系統，分別提供設定範例。

Windows 用戶端(使用 WinSCP 程式)免密碼連線 xdata 節點方式

首先 請在 Taiwania1 的登入節點，利用 ssh-keygen 指令產生一組公私鑰對。

```
[username@clogin1 ~]$ cd .ssh/
[username@clogin1 .ssh]$ pwd
/home/username/.ssh

[username@clogin1 .ssh]$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/username/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/username/.ssh/id_dsa.
Your public key has been saved in /home/username/.ssh/id_dsa.pub.
The key fingerprint is:
c7:b1:23:8a:29:45:56:24:eb:4c:dc:b2:7c:40:dd:76 username@clogin1
The key's randomart image is:
+--[ DSA 1024]----+
|        ooo.     |
|      o =. o E   |
|       O .. ..   |
|      B +    . o |
|       * . S =   |
|      . + . o .  |
|     . o .       |
|      .          |
```

```
|                         |
+-----------------+
[username@clogin1 .ssh]$
```

此時帳號家目錄下的.ssh 目錄內會產生 id_dsa 與 id_dsa.pub 檔案。

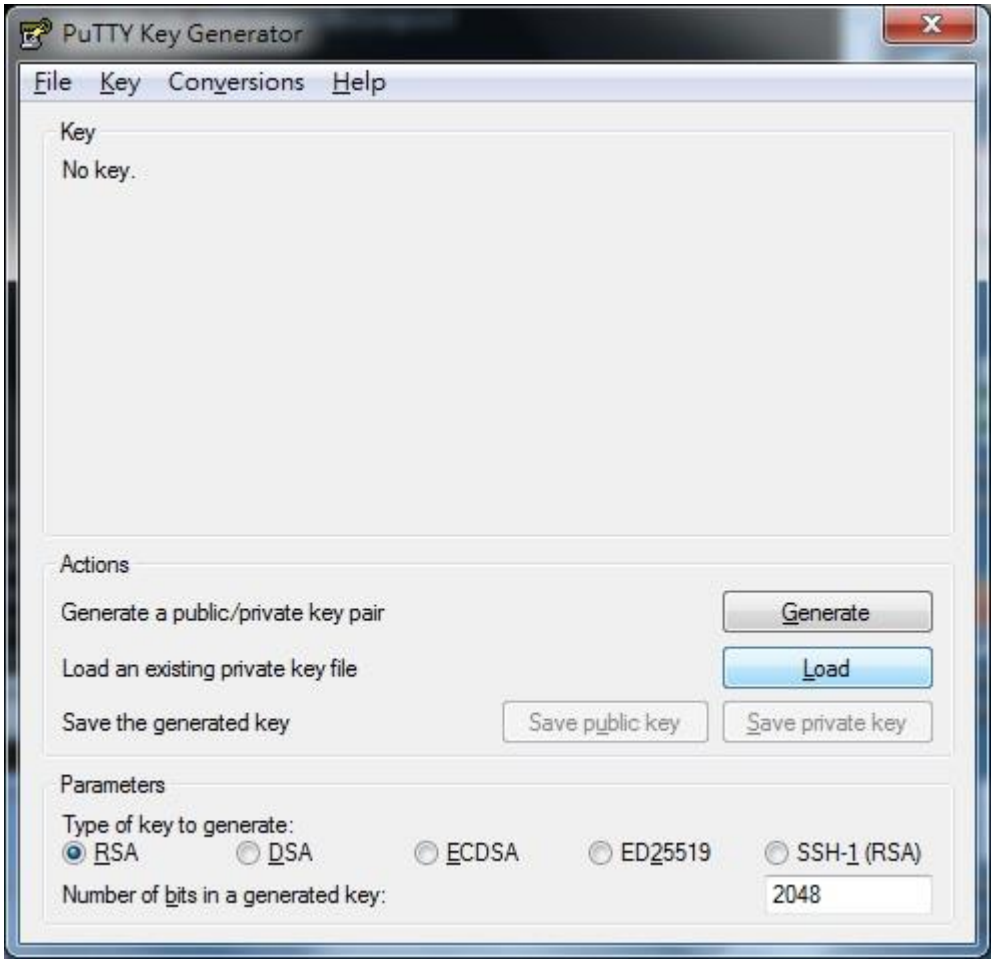
```
[username@clogin1 .ssh]$ ls -al
total 24
drwx------    2 username TRI107044 4096 Nov    8 09:22 .
drwx------ 68 username TRI107044 4096 Nov    8 09:01 ..
-rw-------    1 username TRI107044    668 Nov    8 09:22 id_dsa
-rw-r--r--    1 username TRI107044    606 Nov    8 09:22 id_dsa.pub
-rw-------    1 username TRI107044    227 May    7    2018 id_ecdsa
-rw-------    1 username TRI107044    178 May    7    2018 id_ecdsa.pub
```

請將 id_dsa.pub 內容附加到 authorized_keys 檔案內

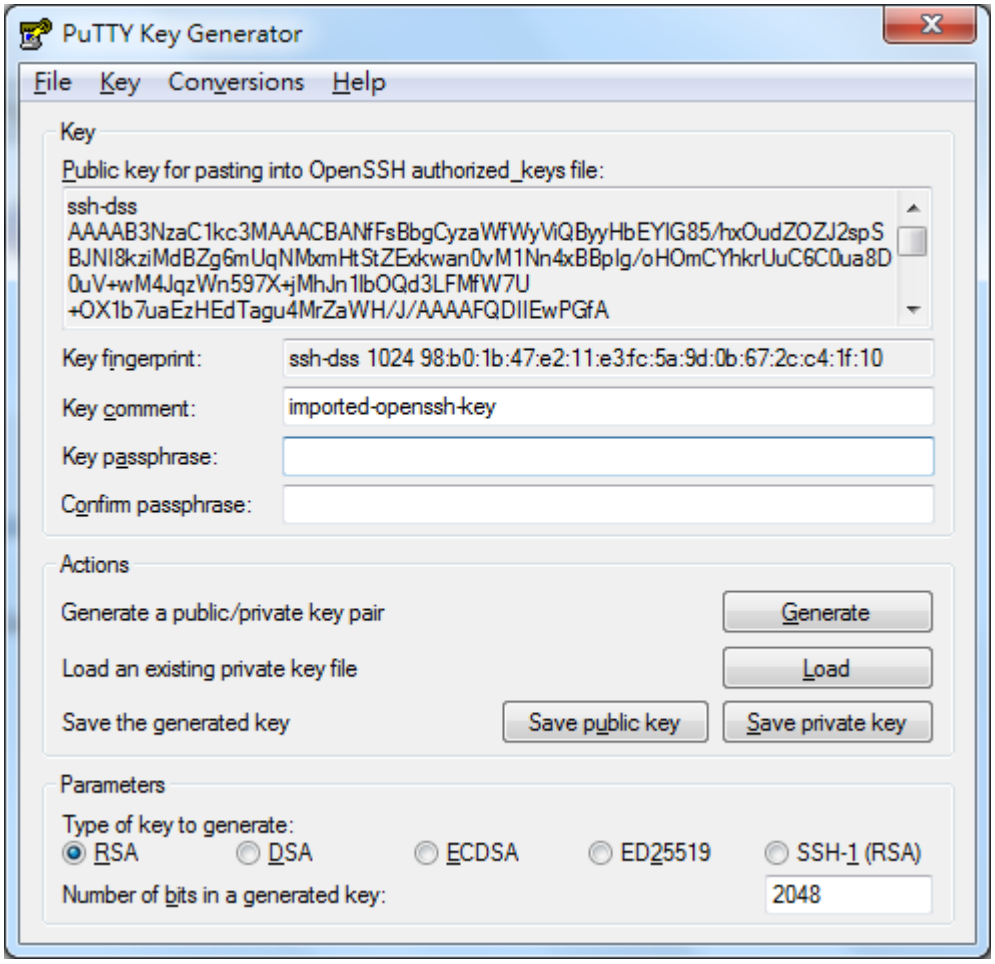
```
[username@clogin1 .ssh]$ cat id_dsa.pub >> authorized_kyes
```

並將 id_dsa 私鑰檔案，使用 WinSCP 程式下載傳回到你自己的 Windows 電腦。

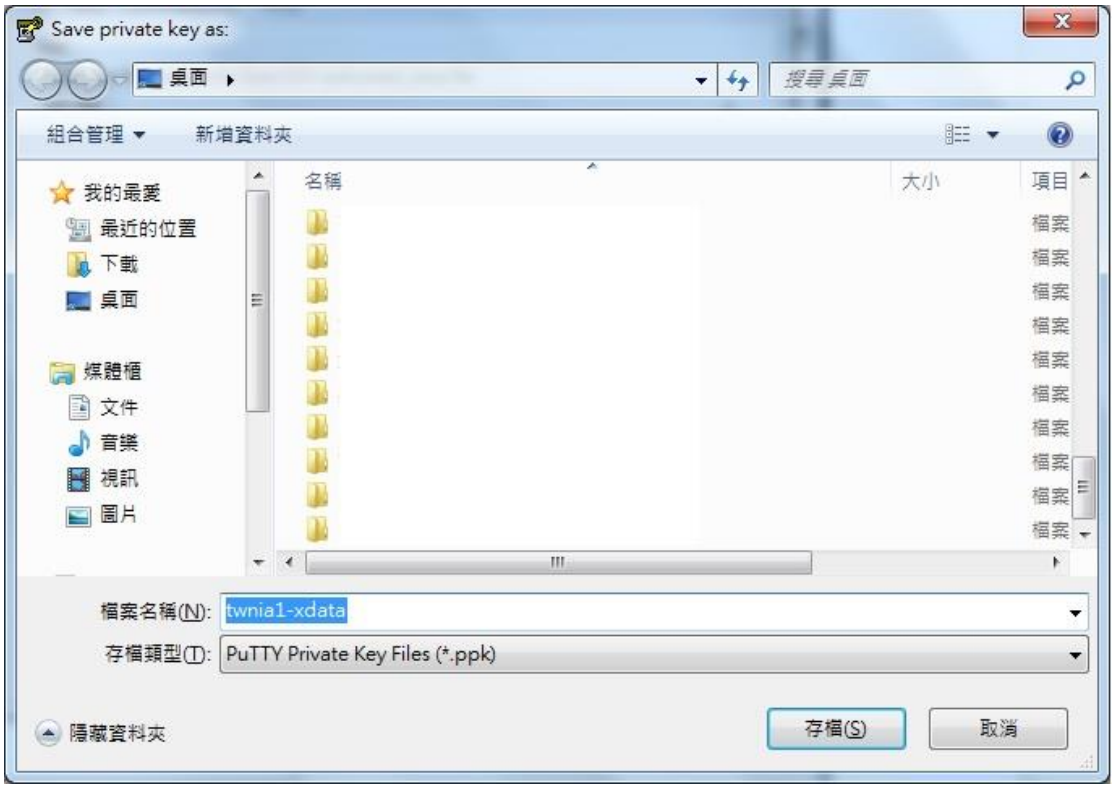
再請至 https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html 下載 puttygen 程式，開啟 puttygent 程式之後點選 Load 載入 id_dsa 檔案。



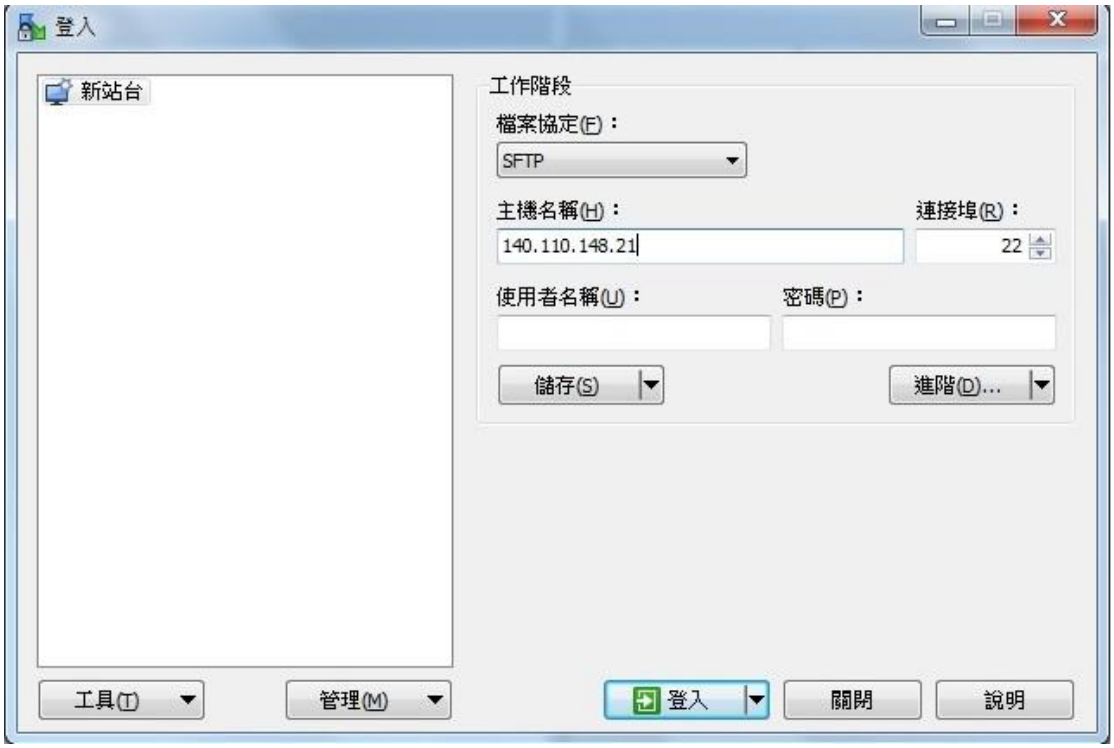
完成 Load 動作，此時建議您加上密碼(Key passphrase\Confirm passphrase)保護您即將要產生的 twnia1-xdata.ppk 檔案。



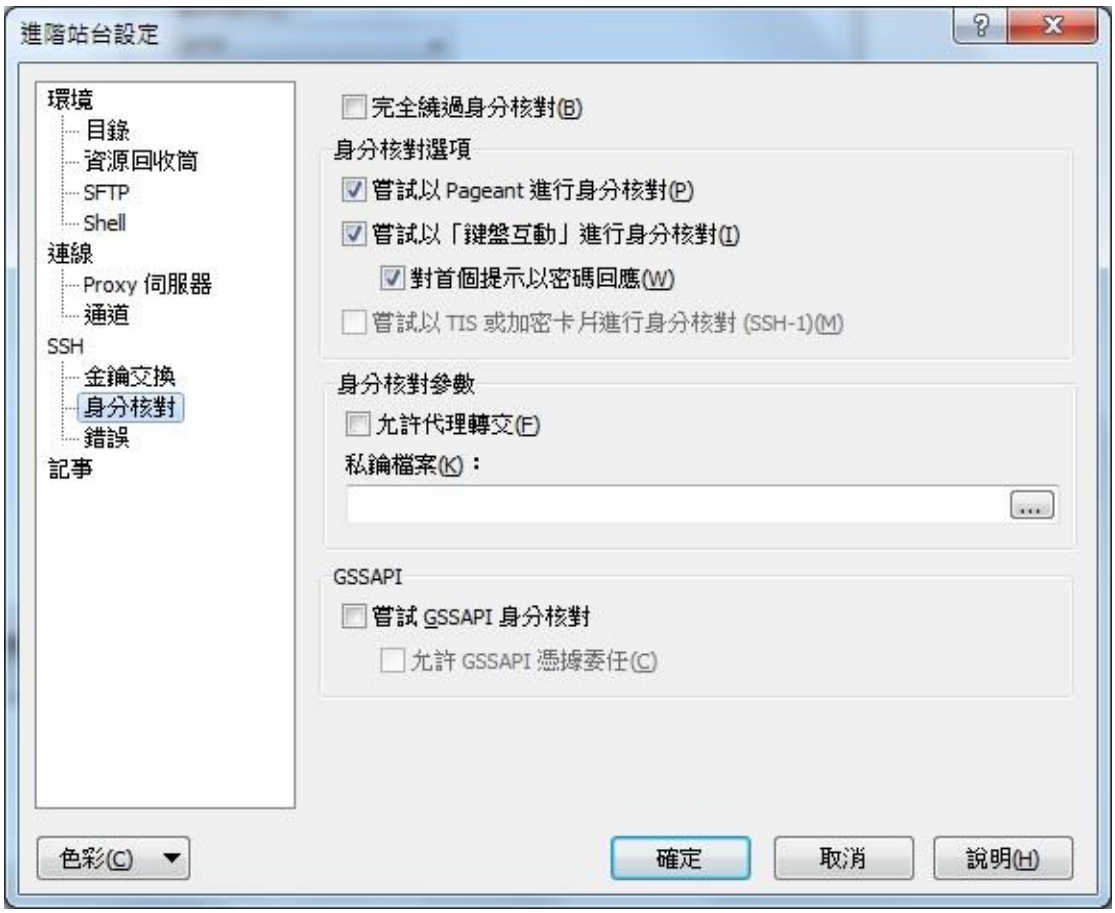
再選擇 Save private key 儲存成 twnia1-xdata.ppk 檔案，之後請妥善保護好 twnia1-xdata.ppk 檔案。

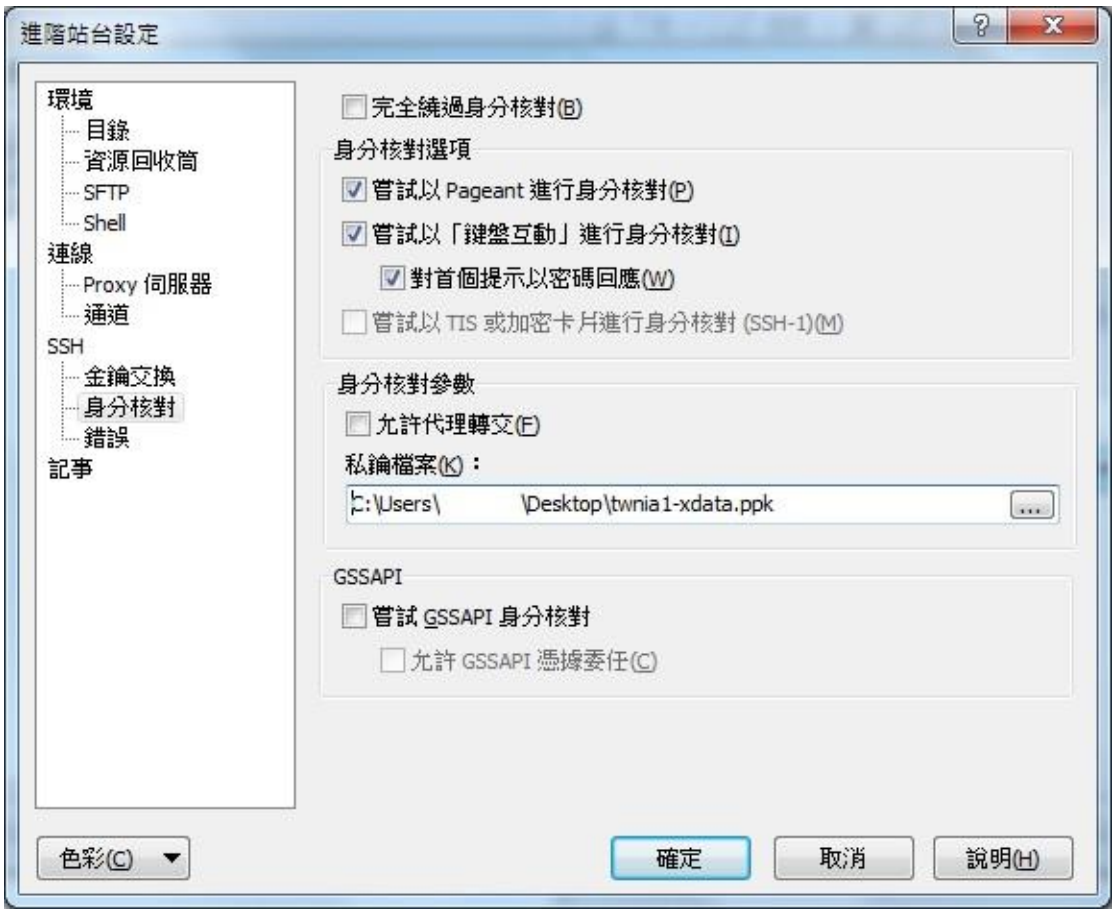


開啟 WinSCP 程式，輸入欲連線的 IP 網址。

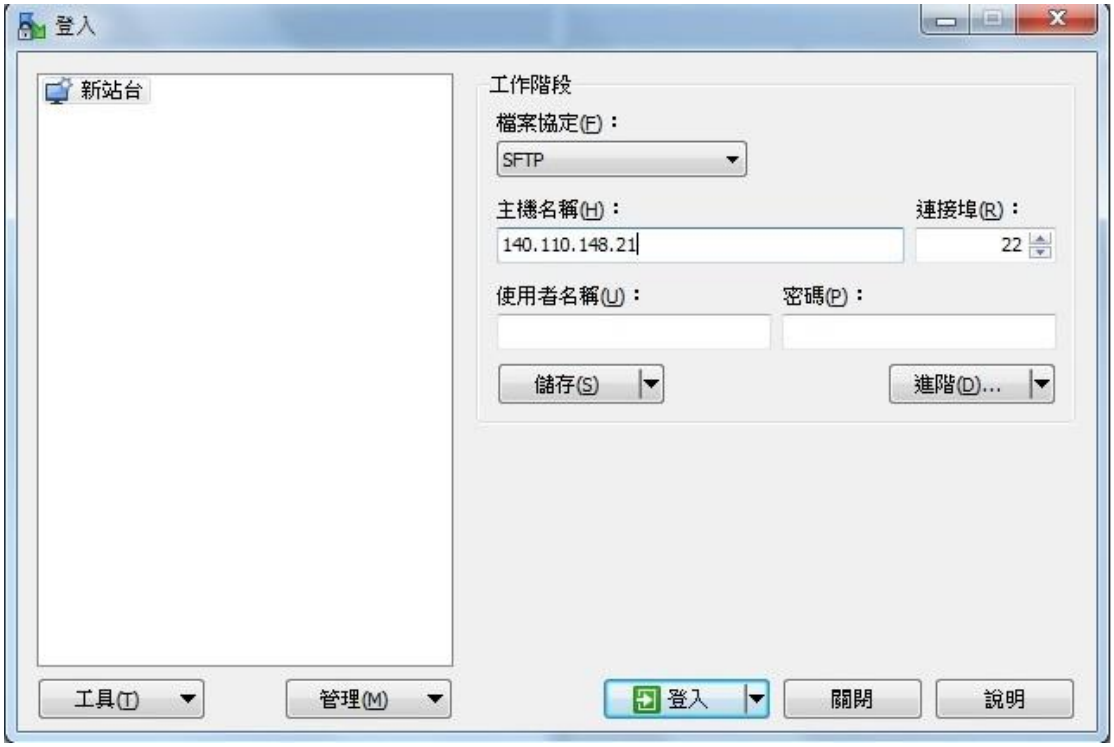


按下進階，選擇 SSH/身份核對，瀏覽選取已經建立私鑰檔案 twnia1-xdata.ppk。


進階站台設定
環境
目錄
資源回收筒
SFTP
Shell
連線
Proxy 伺服器
通道
SSH
金鑰交換
身分核對
錯誤
記事
完全繞過身分核對(B)
身分核對選項
嘗試以 Pageant 進行身分核對(P)
嘗試以「鍵盤互動」進行身分核對(I)
對首個提示以密碼回應(W)
嘗試以 TIS 或加密卡片進行身分核對 (SSH-1)(M)
身分核對參數
允許代理轉交(F)
私鑰檔案(K)：
...
GSSAPI
嘗試 GSSAPI 身分核對
允許 GSSAPI 憑據委任(C)
色彩(C)
確定
取消
說明(H)



回到 WinSCP 登入畫面，使用者名稱欄只輸入帳號，按下登入即可免輸入密碼登入到 xdata1，去執行檔案上傳與檔案下傳。



Linux 用戶端免密碼連線 xdata 節點方式

請於您自己的 Linux 主機，先使用 ssh-keygen 指令產生公鑰與私鑰。

```
[username@linux ~]$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/username/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/username/.ssh/id_dsa.
Your public key has been saved in /home/username/.ssh/id_dsa.pub.
The key fingerprint is:
f1:f2:fb:d7:2c:a3:e5:6e:47:f6:85:6f:88:74:98:7a username@linux
The key's randomart image is:
+--[ DSA 1024]----+
|                 |
|                 |
|        .        |
|       o         |
|      S . o .    |
|       o + o +   |
|      .o o.Bo    |
|     ..Eo* B     |
|      .oo=o=     |
+-----------------+

[username@linux ~]$ ls –al .ssh/
total 20
drwx------  2 username n0000000 4096 Nov  5 17:18 .
drwx------ 10 username n0000000 4096 Aug  8  2016 ..
-rw-------  1 username n0000000  668 Nov  5 17:18 id_dsa
-rw-r--r--  1 username n0000000  606 Nov  5 17:18 id_dsa.pub
-rw-r--r--  1 username n0000000  396 Nov  5 17:17 known_hosts
```

利用 ssh-copy-id 指令將公鑰 id_dsa.pub 傳送到 Taiwania1 的檔案傳輸節點，這一個過程 Password:會需要輸入你的帳號與密碼(要附加 OTP 碼) 。

```
[username@linux ~]$ ssh-copy-id -i ~/.ssh/id_dsa.pub username@140.110.148.21
```

```
Password:
Now try logging into the machine, with "ssh 'username@140.110.148.21'", and
check in:

    .ssh/authorized_keys

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

[username@linux ~]$
```

完成上述 ssh-copy-id 指令，接下來的後續連線，就可以免密碼對檔案傳輸節點進行遠端操作與檔案傳輸。

```
[username@linux ~]$ ssh username@140.110.148.21 "date"
Mon Nov  5 17:23:06 CST 2018

[username@linux ~]$ ssh username@140.110.148.21 "hostname"
xdata1

[username@linux ~]$ ssh username@140.110.148.22 "hostname"
xdata2

[username@linux ~]$ scp ~/data0 username@140.110.148.21:~/cptest.data0
data0                                         100%   35     8.6KB/s   00:00

[username@linux ~]$ scp ~/data1 username@140.110.148.22:~/cptest.data1
data1                                         100%   35    18.4KB/s   00:00
```

當有大量檔案上下傳時，建議也可以再結合 rsync 同步複製指令，讓只有異動的部分更新，減少傳輸的時間。

(完)