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]----+

000.	
o =. o E	
O	
B + . o	
* . S =	
.+.0.	
.	



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	e@clogin1 .ssh]\$ ls -al			
total 24				
drwx	2 username TRI107044	4096 Nov	8 09:22 .	
drwx	68 username TRI107044 4	1096 Nov	8 09:01	
-rw	1 username TRI107044	668 Nov	8 09:22 id	dsa
-rw-rr	1 username TRI107044	606 Nov	8 09:22 id_	_dsa.pub
-rw	1 username TRI107044	227 May	7 2018 i	d_ecdsa
-rw	1 username TRI107044	178 May	7 2018 i	d_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。

le Key Conversions Help	
Key No key.	
Actions Generate a public/private key pair	Generate
Actions Generate a public/private key pair	Generate
Actions Generate a public/private key pair Load an existing private key file	<u>G</u> enerate Load
Actions Generate a public/private key pair Load an existing private key file Save the generated key	Generate Load Save public key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters	Generate Load Save public key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters Type of key to generate:	Generate Load Save public key Save private key CDSA © ED25519 © SSH-1 (RSA)



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。

😴 PuTTY Key Generat	or		×
<u>File K</u> ey Con <u>v</u> ersio	ns <u>H</u> elp		
Key			
Public key for pasting in	nto OpenSSH authorize	d_keys file:	
ssh-dss AAAAB3NzaC1kc3MA BJNI8kziMdBZg6mUq QuV+wM4JqzWn597X +OX1b7uaEzHEdTagu	AACBANfFsBbgCyzaW NMxmHtStZExkwan0v +ijMhJn11bOQd3LFMfW u4MrZaWH/J/AAAAFC	/fWyViQByyHbEYIG85// M1Nn4xBBplg/oHOmC\ /7U QDIIEwPGfA	nxOudZOZJ2spS /hkrUuC6C0ua8D
Key fingerprint:	ssh-dss 1024 98:b0:18	p:47:e2:11:e3:fc:5a:9d:0	b:67:2c:c4:1f:10
Key comment:	imported-openssh-key		
Key p <u>a</u> ssphrase:			
Confirm passphrase:			
Actions			
Generate a public/priva	ate key pair		<u>G</u> enerate
Load an existing private	e key file		Load
Save the generated ke	у	Save p <u>u</u> blic key	<u>S</u> ave private key
Parameters			
Type of key to generate <u>R</u> SA <u></u>	e: <u>)</u> SA © <u>E</u> CD:	SA © ED <u>2</u> 5519) SSH- <u>1</u> (RSA)
Number of <u>b</u> its in a gen	erated key:		2048

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。

-	- ↓ 搜尋 桌面	Q
	8	•••
^	大小	項目
		檔案
		福案
		檔案
		檔案
		福案
		檔案
		福案 、
III		
		Ŧ
*.ppk)		·
	存檔(5)	取消
		 ✓ 4 按章 真面 第 ★.ppk) 存楣(S)

開啟 WinSCP 程式,輸入欲連線的 IP 網址。

ず 新站台	工作階段 檔案協定(E): SFTP ▼	
	主機名稱(出):	連接埠(R):
	140.110.148.21	22 🛓
	使用者名稱(山):	密碼(P):

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。

環境 □ 目錄 □ SFTP □ Shell 連線 □ Proxy 伺服器 □ 通道 SSH □ 金鑰交換 □ 自分核對 □ 錯誤 記事	 完全繞過身分核對(g) 身分核對邏項 『嘗試以 Pageant 進行身分核對(g) 『嘗試以「謹盤互動」進行身分核對(g) 『嘗試以「IS 或加密卡 片進行身分核對 (SSH-1)(M) 當試以 TIS 或加密卡 片進行身分核對 (SSH-1)(M) 身分核對參數 ① 尤許代理轉交(p) 私論檔案(K):
色彩(2) ▼	確定 取消 說明田

環境 目錄	□ 完全繞過身分核對個)
	身分核對選項
SFTP	☑ 嘗試以 Pageant 進行身分核對(P)
Shell	☑ 嘗試以「鍵盤互動」進行身分核對①
建禄 Proxy 伺服器	☑ 對首個提示以密碼回應(₩)
通道 SSH	□ 嘗試以 TIS 或加密卡 片進行身分核對 (SSH-1)(M)
金鑰交換	身分核對參數
	允許代理轉交(F)
記事	私論檔案化:
	12: \Users\ \Desktop\twnia1-xdata.ppk
	GSSAPI
	III 嘗試 GSSAPI 身分核對
	□

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。

5 量入		
₩ 新站台	工作階段 檔案協定(E): SFTP 主機名稱(H): 140.110.148.21] 使用者名稱(U): 密函 儲存(S) ▼	連接埠(R): 22 彙 嗎(P): 進階(D) ↓
	各理(M) ▼ □ 登入 ▼	關閉 說明

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]----+

.
О
S. o.
o + o +
.o o.Bo
Eo* B
.00=0=

-----+

[username	e@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-rr	1 username n0000000	606 Nov	5	17:18 id	_dsa.pu
-rw-rr	1 username n0000000	396 Nov	5	17:17 kn	iown_h

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 517:23:06 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)