11.1 遠端連線伺服器



遠端連線伺服器對我們來說，可是一項很有用的工具啊！可能會有安全性的問題吶！

11.1.1 什麼是遠端連線伺服器



遠端連線伺服器在提供你由遠端透過文字或圖形介面的方式來登入系統，讓你在遠端的工作機前面登入Linux主機以取得可操控主機之介面(shell)，而登入後的操作感覺上就像坐在系統前面一樣。

11.1.2 有哪些可供登入的類型？



那麼目前遠端連線伺服器的主要類型有哪些？如果以登入的連線介面來分類，基本上有文字介面與圖形介面兩種：

* 文字介面明碼： telnet, rsh等為主，目前非常少用；
* 文字介面密碼： ssh為主，已經取代上述的 telnet, rsh 等明碼方式；
* 圖形介面： Xdmcp, VNC, RDP 等較為常見

在文字介面登入的連線伺服器，主要有以『明碼』傳送資料的telnet伺服器，及以加密技術進行資料加密再傳送的SSH伺服器！telnet由於是使用明碼來傳送資料，資料很容易遭到有心人士的擷取！至於圖形介面的連線伺服器，目前很常見的圖形連線伺服器，就是VNC(Virtual Network Computing)，透過VNC server/client軟體來進行連接。

|  |  |
| --- | --- |
| **Tips:** 圖形介面最大的優點是『圖形』！不過圖形傳送，傳輸的資料量大，所以速度與安全性都有待考量。因此建議將圖形介面的遠端登入伺服器開放在內部網域(LAN)就好了！ |  |

資料傳送的明碼與密碼

明碼就是：『當資料封包在網路上傳輸時，該資料封包的內容為資料的原始格式』，使用telnet登入遠端主機時得要輸入帳號密碼，那是以原本的資料格式傳輸，所以如果被類似[tcpdump](http://linux.vbird.org/linux_server/0140networkcommand.php#tcpdump)之類的監聽軟體擷取資料，那帳密就有可能被竊取！因此目前通常都希望使用可以將這些在網路上面跑的資料加密的技術，以增加資料在Internet上面傳送的安全性！

11.2 文字介面連線伺服器： SSH 伺服器



SSH是**S**ecure **SH**ell protocol的簡寫(安全的殼程式協定)，它可以透過資料封包加密技術，將等待傳輸的封包加密後再傳輸到網路上，因此資料訊息當然就比較安全！特別注意：SSH協定在預設的狀態中，本身就提供兩個伺服器功能：

1. 一個就是類似telnet的遠端連線使用shell的伺服器，亦即是俗稱的ssh；
2. 另一個就是類似FTP服務的sftp-server！提供更安全的FTP服務。

11.2.1 連線加密技術簡介

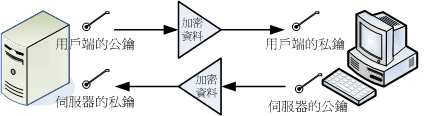


目前常見的網路封包加密技術是藉由所謂的『非對稱金鑰系統』來處理的。透過兩把不一樣的公鑰與私鑰(Public and Private Key)進行加密與解密。這兩把鑰匙是加解密的功用，在同一個方向的連線中，這兩把鑰匙當然是需要成對的：

* 公鑰(public key)：提供給遠端主機進行資料加密的行為，就是**大家都能取得你的公鑰來將資料加密**的意思；
* 私鑰(private key)：遠端主機使用你的公鑰加密的資料，在本地端使用私鑰來進行解密。**私鑰是不能夠外流的！只能保護在自己的主機上。**

每部主機都應該有自己的金鑰(公鑰與私鑰)，且公鑰用來加密而私鑰用來解密，其中私鑰不可外流。因為網路連線是雙向的，每個人應該都要有對方的『公鑰』！在用戶端與伺服器端的相對連線方向上，應該有如下的加密動作：

圖 11.2-1、公鑰與私鑰在進行資料傳輸時的角色示意圖



如上圖所示，在用戶端的角度，首先要取得伺服器端的公鑰，然後將自己的公鑰發送給伺服器端，最終在用戶端上面的金鑰會是『伺服器的公鑰加上用戶端我自己的私鑰』組成的。

11.2.2 啟動 SSH 服務



在Linux系統中預設已含SSH的所有需要的軟體了！這包含了可以產生密碼等協定的[OpenSSL](http://www.openssl.org" \t "_blank)軟體與[OpenSSH](http://www.openssh.com/" \t "_blank)軟體！目前的Linux Distributions中是預設啟動SSH的，直接啟動SSH daemon(sshd)，所以手動可以這樣啟動：

|  |
| --- |
| [root@www ~]# /etc/init.d/sshd restart  [root@www ~]# netstat -tlnp | grep ssh  Active Internet connections (only servers)  Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name  tcp 0 0 :::22 :::\* LISTEN 1539/sshd |

SSH不但提供了shell給我們使用，亦即是ssh protocol的主要目的，同時亦提供了一個較為安全的FTP server，亦即是 ssh-ftp server當成是FTP來使用！所以sshd可以同時提供shell與ftp！而且都是架構在port 22上面的呢！

11.2.3 ssh 用戶端連線程式 - Linux 用戶



Linux的預設情況已經有底下的所有指令，不必安裝額外的軟體！底下就來介紹一下這些指令吧！



ssh ：直接登入遠端主機的指令

SSH在client端使用的是ssh指令，一般的用法可以使用底下的方式：

|  |
| --- |
| [root@www ~]# ssh [-f] [-o 參數項目] [-p 非正規埠口] [帳號@]IP [指令]  選項與參數：  -f ：需要配合後面的 [指令]，不登入遠端主機直接發送一個指令過去而已；  -o 參數項目：主要的參數項目有：  ConnectTimeout=秒數 ：連線等待的秒數，減少等待的時間  StrictHostKeyChecking=[yes|no|ask]：預設是 ask，若要讓 public key  主動加入 known\_hosts ，則可以設定為 no 即可。  -p ：如果你的 sshd 服務啟動在非正規的埠口 (22)，需使用此項目；  [指令] ：不登入遠端主機，直接發送指令過去。但與 -f 意義不太相同。  # 1. 直接連線登入到對方主機的方法 (以登入本機為例)：  [root@www ~]# ssh 127.0.0.1  The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.  RSA key fingerprint is eb:12:07:84:b9:3b:3f:e4:ad:ba:f1:85:41:fc:18:3b.  Are you sure you want to continue connecting (yes/no)? yes  Warning: Permanently added '127.0.0.1' (RSA) to the list of known hosts.  root@127.0.0.1's password: <==在這裡輸入 root 的密碼即可！  Last login: Mon Jul 25 11:36:06 2011 from 192.168.1.101  [root@www ~]# exit <==離開這次的 ssh 連線  # 由於 ssh 後面沒有加上帳號，因此預設使用當前的帳號來登入遠端伺服器 |

一般使用ssh登入遠端主機，都會填寫『ssh 帳號@主機IP』的格式，意思是說，使用該主機的某帳號登入。但是使用『ssh 主機IP』的格式，那會以本地端電腦的帳號來嘗試登入遠端。如果近端與遠端具有相同的帳號，那麼不寫帳號也沒有關係。但為了以後習慣著想，還是一開始就使用類似email的方式來登入遠端主機！

上面訊息中，開頭RSA的那行後面接的是遠端伺服器的公鑰指紋碼，如果確定該指紋碼沒問題，就要輸入yes來將該指紋碼寫入伺服器公鑰記錄檔(~/.ssh/known\_hosts)，以方便未來比對該伺服器的正確性之用。注意是要寫yes，單純輸入Y或y是不會被接受的～由於該主機的公鑰已經被記錄，因此未來重複使用ssh登入此主機時，就不會出現這個指紋碼提示了。

|  |
| --- |
| # 2. 使用 student 帳號登入本機  [root@www ~]# ssh student@127.0.0.1  student@127.0.0.1's password:  [student@www ~]$ exit  # 由於加入帳號，因此切換身份成為 student 了！另外，因為 127.0.0.1 曾登入過，  # 所以就不會再出現提示你要增加主機公鑰的訊息囉！  # 3. 登入對方主機執行過指令後立刻離開的方式：  [root@www ~]# ssh student@127.0.0.1 find / &> ~/find1.log  student@localhost's password:  # 此時你會發現怎麼畫面卡住了？這是因為上頭的指令會造成，你已經登入遠端主機，  # 但是執行的指令尚未跑完，因此你會在等待當中。那如何指定系統自己跑？  # 4. 與上題相同，但是讓對方主機自己跑該指令，你立刻回到近端主機繼續工作：  [root@www ~]# ssh -f student@127.0.0.1 find / &> ~/find1.log  # 此時你會立刻登出 127.0.0.1 ，但 find 指令會自己在遠端伺服器跑喔！ |

上述的範例當中，第4個範例最有用！如果想要讓遠端主機進行關機的指令，如不加上-f的參數，那會等待對方主機關機完畢再將踢出連線，加上-f就很重要～因為你會指定遠端主機自己跑關機，而不需要在空空等待。例如：『ssh -f root@some\_IP shutdown -h now』之類的指令囉。

伺服器公鑰記錄檔：~/.ssh/known\_hosts

當你登入遠端伺服器時，本機會主動的用接收到的伺服器的public key去比對~/.ssh/known\_hosts有無相關的公鑰，然後進行底下的動作：

* 若接收的公鑰尚未記錄，則詢問使用者是否記錄。若要記錄(回答yes的那個步驟)則寫入~/.ssh/known\_hosts且繼續登入的後續工作；若不記錄(回答no)則不寫入該檔案，並且離開登入工作；
* 若接收到的公鑰已有記錄，則比對記錄是否相同，若相同則繼續登入動作；若不相同，則出現警告資訊，且離開登入的動作。這是用戶端的自我保護功能，避免你的伺服器是被別人偽裝的。

模擬 FTP 的檔案傳輸方式： sftp

ssh是登入遠端伺服器進行工作，如果只想從遠端伺服器下載或上傳檔案呢？那就要使用sftp或scp。這兩個指令也是用ssh的通道(port 22)，只是模擬成FTP與複製的動作。sftp的用法與ssh很相似，只是ssh是用在登入而sftp在上傳/下載檔案。

|  |
| --- |
| [root@www ~]# sftp student@localhost  Connecting to localhost...  student@localhost's password: <== 這裡請輸入密碼啊！  sftp> exit <== 這裡就是在等待你輸入 ftp 相關指令的地方了！ |

進入到 sftp 之後，那就跟在一般 FTP 模式下的操作方法沒有兩樣了！底下我們就來談一談，sftp這個介面下的使用指令吧！

|  |  |
| --- | --- |
| 針對遠方伺服器主機 (Server) 之行為 | |
| 變換目錄到 /etc/test 或其他目錄 | cd /etc/test cd PATH |
| 列出目前所在目錄下的檔名 | ls dir |
| 建立目錄 | mkdir directory |
| 刪除目錄 | rmdir directory |
| 顯示目前所在的目錄 | Pwd |
| 更改檔案或目錄群組 | chgrp groupname PATH |
| 更改檔案或目錄擁有者 | chown username PATH |
| 更改檔案或目錄的權限 | chmod 644 PATH 其中，644 與權限有關！回去看基礎篇！ |
| 建立連結檔 | ln oldname newname |
| 刪除檔案或目錄 | rm PATH |
| 更改檔案或目錄名稱 | rename oldname newname |
| 離開遠端主機 | exit (or) bye (or) quit |
| 針對本機 (Client) 之行為(都加上 l, L 的小寫 ) | |
| 變換目錄到本機的 PATH 當中 | lcd PATH |
| 列出目前本機所在目錄下的檔名 | Lls |
| 在本機建立目錄 | Lmkdir |
| 顯示目前所在的本機目錄 | Lpwd |
| 針對資料上傳/下載的行為 | |
| 將檔案由本機上傳到遠端主機 | put [本機目錄或檔案] [遠端] put [本機目錄或檔案] 如果是這種格式，則檔案會放置到目前遠端主機的目錄下！ |
| 將檔案由遠端主機下載回來 | get [遠端主機目錄或檔案] [本機] get [遠端主機目錄或檔案] 若是這種格式，則檔案會放置在目前本機所在的目錄當中！可以使用萬用字元，例如： get \* get \*.rpm 亦是可以的格式！ |

sftp在Linux下，如果不考慮圖形介面，那麼他已經可以取代FTP了！

|  |  |
| --- | --- |
| 例題：假設localhost為遠端伺服器，且伺服器上有student這個使用者。你想要 (1)將本機的/etc/hosts上傳到 student家目錄，並 (2)將student的.bashrc複製到本機的/tmp下，該如何透過sftp達成？  答：   |  | | --- | | [root@www ~]# sftp student@localhost  sftp> lls /etc/hosts <==先看看本機有沒有這個檔案  /etc/hosts  sftp> put /etc/hosts <==有的話，那就上傳吧！  Uploading /etc/hosts to /home/student/hosts  /etc/hosts 100% 243 0.2KB/s 00:00  sftp> ls <==有沒有上傳成功？看遠端目錄下的檔名  hosts  sftp> ls -a <==那有沒有隱藏檔呢？  . .. .bash\_history .bash\_logout  .bash\_profile .bashrc .mozilla hosts  sftt> lcd /tmp <==切換本機目錄到 /tmp  sftp> lpwd <==只是進行確認而已！  Local working directory: /tmp  sftp> get .bashrc <==沒問題就下載吧！  Fetching /home/student/.bashrc to .bashrc  /home/student/.bashrc 100% 124 0.1KB/s 00:00  sftp> lls -a <==看本地端檔案檔名  . .font-unix keyring-rNd7qX .X11-unix  .. .gdm\_socket lost+found scim-panel-socket:0-root  .bashrc .ICE-unix mapping-root .X0-lock  sftp> exit <==離開吧！ | |

檔案異地直接複製： scp

通常使用sftp是因為可能不知道伺服器上面有什麼檔名的檔案存在，如果已經知道伺服器上的檔案檔名了，那麼最簡單的檔案傳輸則是透過scp這個指令喔！最簡單的scp用法如下：

|  |
| --- |
| [root@www ~]# scp [-pr] [-l 速率] file [帳號@]主機:目錄名 <==上傳  [root@www ~]# scp [-pr] [-l 速率] [帳號@]主機:file 目錄名 <==下載  選項與參數：  -p ：保留原本檔案的權限資料；  -r ：複製來源為目錄時，可以複製整個目錄 (含子目錄)  -l ：可以限制傳輸的速度，單位為 Kbits/s ，例如 [-l 800] 代表傳輸速限 100Kbytes/s  # 1. 將本機的 /etc/hosts\* 全部複製到 127.0.0.1 上面的 student 家目錄內  [root@www ~]# scp /etc/hosts\* student@127.0.0.1:~  student@127.0.0.1's password: <==輸入 student 密碼  hosts 100% 207 0.2KB/s 00:00  hosts.allow 100% 161 0.2KB/s 00:00  hosts.deny 100% 347 0.3KB/s 00:00  # 檔名顯示 進度 容量(bytes) 傳輸速度 剩餘時間  # 你可以仔細看，出現的訊息有五個欄位，意義如上所示。  # 2. 將 127.0.0.1 這部遠端主機的 /etc/bashrc 複製到本機的 /tmp 底下  [root@www ~]# scp student@127.0.0.1:/etc/bashrc /tmp |

其實上傳或下載的重點是那個冒號(:)！連接在冒號後面的就是遠端主機的檔案。因此，如果冒號在前，代表的就是從遠端主機下載下來，如果冒號在後，則代表本機資料上傳啦！而如果想要複製目錄的話，那麼可以加上-r的選項！

|  |
| --- |
| 例題：假設本機有個檔案檔名為/root/dd\_10mb\_file，這個檔案有10MB。假設你想要上傳到127.0.0.1的/tmp，而且你在127.0.0.1上面有root這個帳號的使用權。但由於頻寬很寶貴，因此你只想要花費100Kbyes/s 的傳輸量給此一動作，那該如何下達指令？  答：由於預設不存在這個檔案，因此我們得先使用dd來建立一個大檔案：  dd if=/dev/zero of=/root/dd\_10mb\_file bs=1M count=10  由於是上傳資料，觀察-l的選項中，速率用的是bit，轉成容量的bytes需要乘上8倍，因此指令就要這樣下達：  scp -l 800 /root/dd\_10mb\_file root@127.0.0.1:/tmp |

11.2.4 ssh 用戶端連線程式 - Windows 用戶



與Linux不同，Windows預設沒有ssh的用戶端程式，所有的程式都要下載其他第三方軟體。常見的軟體有pietty, psftp及filezilla等。

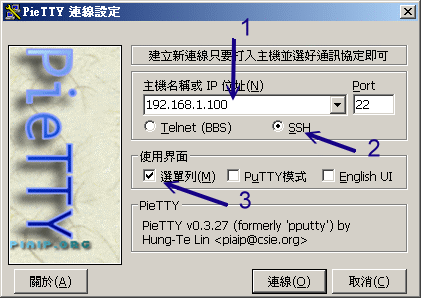
直接連線的pietty

在 Linux 底下想要連接SSH伺服器，可以直接利用[ssh](http://linux.vbird.org/linux_server/0310telnetssh.php" \l "ssh)這個指令，在Windows下就得要使用pietty或putty：

* putty 官方網站：[http://www.chiark.greenend.org.uk/~sgtatham/putty/](http://www.chiark.greenend.org.uk/~sgtatham/putty/" \t "_blank)
* pietty 官方網站：[http://www.csie.ntu.edu.tw/~piaip/pietty/](http://www.csie.ntu.edu.tw/~piaip/pietty/" \t "_blank)

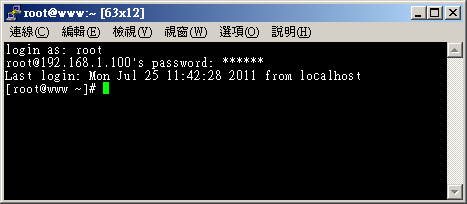
在putty的官方網站上有很多的軟體可以使用的，包括putty/pscp/psftp等等。他們分別對應了ssh/scp/sftp這三個指令就是了。在下載pietty完成後，雙擊該檔案，就會出現如下的畫面囉：

圖 11.2-3、pietty 的啟動畫面示意圖



在上圖中箭頭為1的地方請填寫相關的主機名稱或者是IP，箭頭2選擇SSH，至於箭頭3的地方，鳥哥比較喜歡選單出現的樣式，因為可以直接修改一些pietty的環境設定值，所以鳥哥是選擇選單啦！按下『連線』後，就會出現如下等待登入與輸入帳/密資料的畫面：

圖 11.2-4、pietty 的登入與使用畫面示意圖

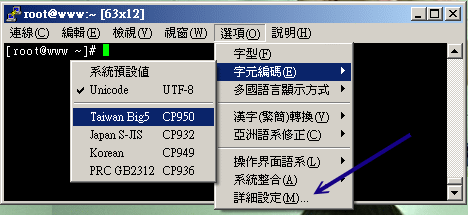


這個圖示會讓你以為是在主機前面工作吧！而且上頭還有選單可以隨時調整類似字形、字體、字元編碼等等的重要環境參數。 尤其是字元編碼的問題，有時候你會發現開啟檔案時，竟然畫面當中會有亂碼而不是正常的中文顯示，那就是編碼的問題。要解決這個問題時，你必須要牢記下面的三個跟語系編碼有關的資料要相同才行：

* 文字檔案本身在存檔時所挑選的語系；
* Linux程式(如bash軟體)本身所使用的語系(可用LANG變數調整)；
* pietty所使用的語系。

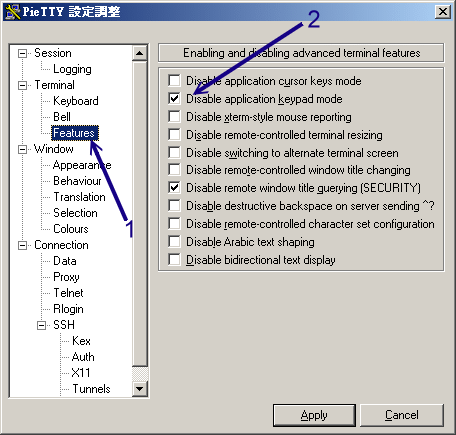
我們知道Linux本身的編碼可以透過LANG這個變數來調整，那該如何調整pietty的中文編碼呢？你可以透過圖11.2-4選單列當中的『選項』來處理，如下所示：

圖 11.2-5、調整 pietty 的語系編碼方式 (與中文較相關)



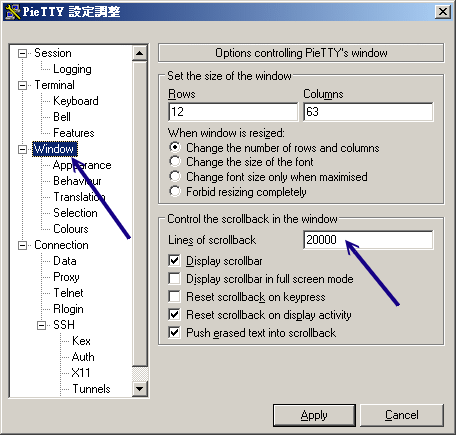
在『選項』的『字元編碼』裡面可以挑選big5(cp950)或者是unicode(utf8)的中文編碼，讓它符合你的Linux與檔案所儲存的資料格式，那中文字就OK的啦！如果想要作更細部的設定時，可以選擇圖11.2-5上頭最底下的那個『詳細設定』項目， 就會出現如下圖示。其中更為重要的是『鍵盤右側的數字鍵想要生效』時，可以按照下圖的指示來啟動數字鍵的功能：

圖 11.2-6、pietty 軟體環境詳細設定，與鍵盤右側數字鍵相關者



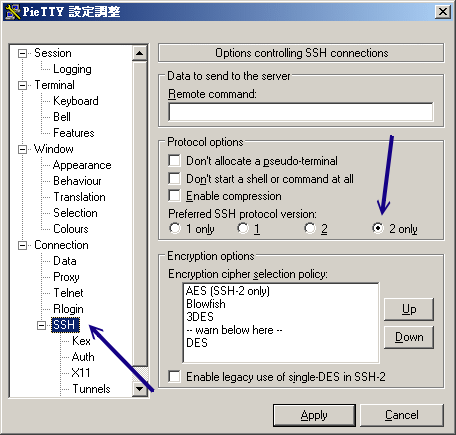
將上圖中箭頭2所指的那個項目勾選起來且按下『Apply』之後，你鍵盤右側的數字鍵才能夠正常的使用呢，否則按右側數字鍵會是亂碼。可以調整pietty捲軸的記憶行數，這樣當資料太多時，你依舊可以調整捲軸來查閱之前的資料。設定的方法如下：

圖 11.2-7、調整畫面可以記憶的行數，可讓用戶回去看較多之前的畫面



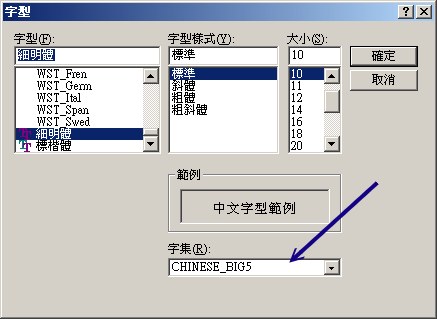
調整完這些常用的資料後，再來這是最重要的：『你要以哪一個版本的SSH演算法登入？』前面說過，我們預設是以version2 來登入的，所以這裡我們可以調整為2那個項目！這樣每次登入都會以version 2的模式登入主機了！

圖 11.2-8、設定登入伺服器時使用的 ssh 演算法版本



整個pietty的使用與相關設定流程就是這樣！如此一來你就可以在Windows上面以SSH的協定，登入遠端的Linux主機嚕！目前pietty已經支援中文！不過需要修改一下字元集，選擇[圖11.2-5](http://linux.vbird.org/linux_server/0310telnetssh.php#fig11.2-5)『選項』內的『字型』就會出現如下圖示：

圖 11.2-9、選擇中文的字形與編碼



將(1)字型設定為細明體、(2)字集設定為『Big5』，如此一來，你的 pietty 就支援中文的輸入囉！

上面我們作的這些設定值都記錄在Windows 的登錄檔當中！你可以在 Windows 的系統當中，在『開始』-->『執行』後，出現的框框內輸入『regedit』，之後會出現一個大視窗。請在左邊的畫面當中選擇『HKEY\_CURRENT\_USER --> Software --> SimonTatham --> PuTTY --> Sessions』，就可以看到你的設定值囉！這樣也就可以儲存你的設定值囉～



使用 sftp-server 的功能： psftp

在 putty 的官方網站上也提供 psftp 這支程式。這一支程式的重點則在使用 sftp-server。使用的方式可以直接點選 psftp 這個檔案，讓他直接啟動，則會出現下面的圖樣：

|  |
| --- |
| psftp: no hostname specified; use "open host.name" to connect  psftp> |

這個時候可以填入你要連接上去的主機名稱，例如我的區域內網路192.168.100.254 這部主機：

|  |
| --- |
| psftp: no hostname specified; use "open host.name" to connect  psftp> open 192.168.100.254  login as: root  root@192.168.100.254's password:  Remote working directory is /root  psftp> <== 這裡就在等待你輸入 FTP 的指令了！ |

呵呵！這樣就登入主機啦！很簡單吧！然後其他的使用方式跟前面提到的[sftp](http://linux.vbird.org/linux_server/0310telnetssh.php" \l "sftp)一樣哩！加油的使用吧！

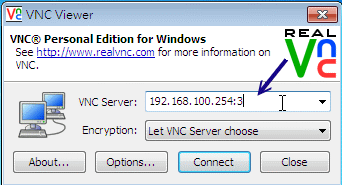
圖形化介面的 sftp 用戶端軟體： Filezilla

SSH所提供的sftp功能能利用圖形介面的軟體呢？就是有用的Filezilla！Filezilla是圖形介面的一個FTP用戶端軟體！

用戶端程式： realvnc

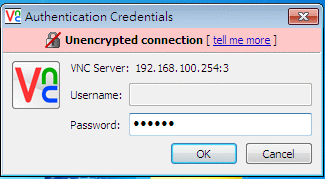
vnc client軟體不少，比較熟悉的是realvnc公司出的GNU自由軟體！在連結(<http://www.realvnc.com/download.html>)下載到最簡單的版本，是不用錢的自由軟體版本。直接執行vnc-viewer軟體，然後就會看到如下的畫面：

圖 11.4-3、Windows Real VNC 用戶端連線示意圖



如上圖所示，你在 server 欄位填上 IP:port 的資料即可，然後按下『OK』吧！

圖 11.4-4、Windows Real VNC 用戶端連線示意圖



由於 VNC server 需要的僅是連線的 VNC 密碼而已，因此上圖中的Username可以不用填，老實說，這個程式它也不會讓你填～ 呵呵！填完按下『OK』即可！接下來就會出現正確的畫面囉！