

# OpenSSH伺服器

---

- OpenSSH簡介
  - OpenSSH安裝
  - OpenSSH組態設定
  - 用戶端連接
-



# OpenSSH簡介

---

# OpenSSH包含套件

---

- **sshd**：執行OpenSSH的伺服器軟體，它會監聽來自用戶端的連線要求，而當sshd收到任何要求後，就會執行身份驗證以服務用戶端。
  - **ssh**：這是屬於用戶端的程式，它可用來登入其他主機，或是在其他主機上執行程式，有時也稱為slogin。
  - **scp**：在主機間執行安全性複製工作的程式
  - **ssh-keygen**：可用來產生Pubkey 驗證金鑰，也就是RSA或DSA的主機及使用者驗證金鑰。
-

# OpenSSH包含套件

---

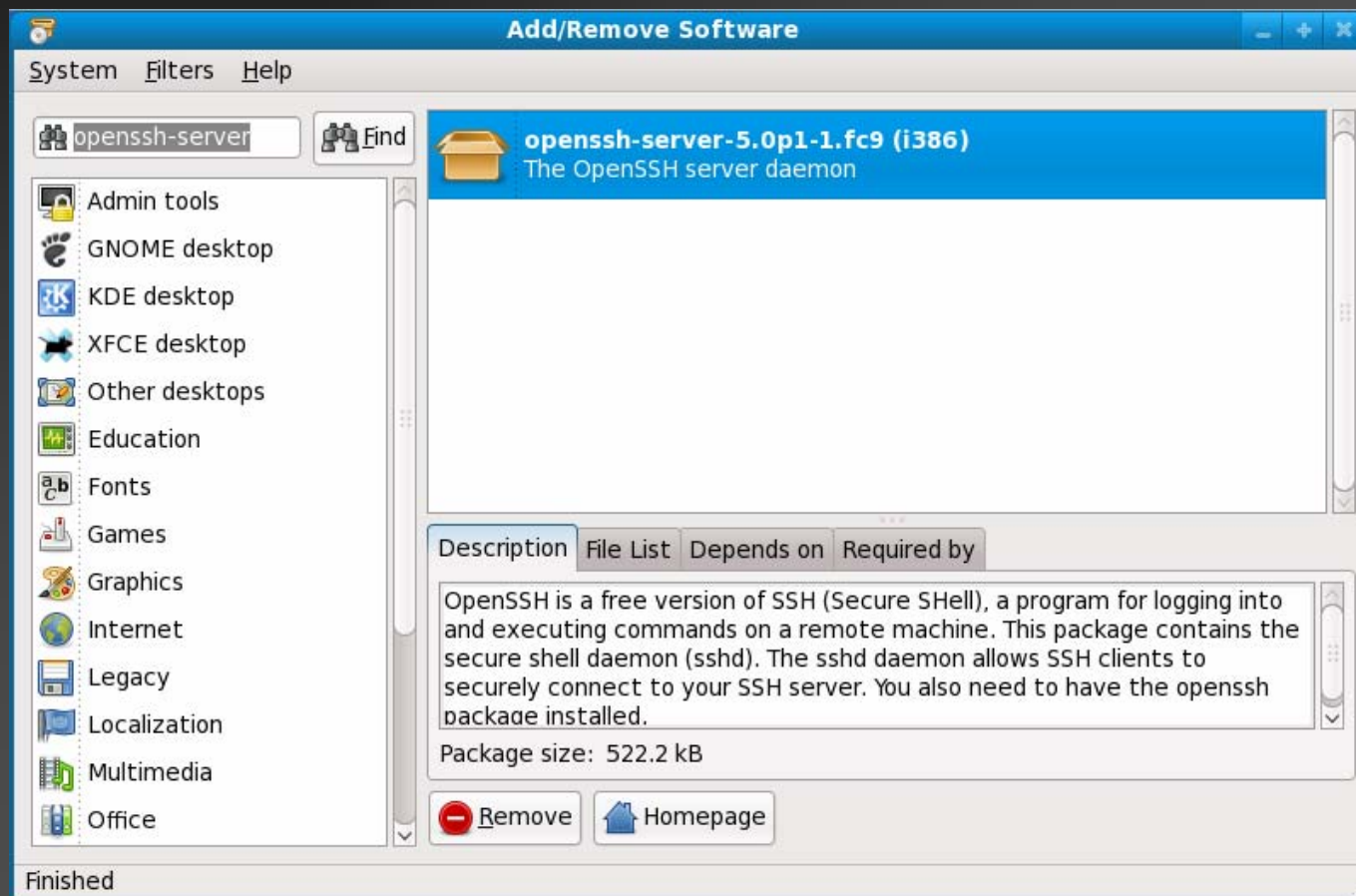
- `ssh-agent`：它的功能是儲存驗證用的RSA金鑰
  - `ssh-add`：用來產生新的金鑰
  - `sftp-server`：SFTP伺服器軟體
  - `sftp`：安全性的FTP程式
  - `ssh-keyscan`：集中管理ssh公開金鑰軟體
  - `ssh-keysign`：在主機驗證時的ssh說明程式
-



# OpenSSH安裝

---

# 安裝OpenSSH伺服器





# OpenSSH組態設定

---

# /etc/ssh/sshd\_config中的重要選項

- **Port**：指定sshd監聽的連接埠號碼，預設值為22。
- **Protocol**：指定sshd支援的SSH通訊協定版本，預設值為「2,1」（多重版本編號間需以逗號區隔）。
- **ListenAddress**：指定sshd監聽的位址，此處可以使用IPv4或IPv6位址，預設值為「0.0.0.0」（所有的IPv4位址）和「::」（所有的IPv6位址）。
- **ServerKeyBits**：定義SSHv1的伺服器金鑰長度，此處的最小值為512，而預設值為768個位元。
- **LogLevel**：設定記錄檔內容的詳細程度（記錄層級），可用的選項有：QUIET、FATAL、ERROR、INFO（預設）、VERBOSE、DEBUG、DEBUG1、DEBUG2和DEBUG3等。

# /etc/ssh/sshd\_config中的**重要選項**

- **LoginGraceTime**：在此設定時間內，若是使用者無法成功進行登入，則伺服器將中斷此次的連接，若設為0表示沒有時間的限制，預設值為600秒。
- **PermitRootLogin**：是否允許以「root」帳號進行登入，預設值為yes。
- **PasswordAuthentication**：是否允許密碼驗證的功能，預設值為yes。
- **PermitEmptyPasswords**：若允許密碼驗證，則可在此設定是否允許使用者使用空白密碼登入，預設值為no。
- **ChallengeResponseAuthentication**：是否啓用Challenge Response的驗證方法，預設值為yes。

# /etc/ssh/sshd\_config重要選項

- **KerberosAuthentication**：是否啓用Kerberos驗證，預設值爲no。
- **KerberosOrLocalPasswd**：在啓用此選項後，若是無法通過Kerberos 驗證，則密碼的正確性將由本地的機制來決定，例如/etc/passwd，預設值爲yes。
- **PrintMotd**：指定sshd是否在使用者登入後，顯示/etc/motd檔案的內容，預設值爲yes。
- **PrintLastLog**：指定sshd是否顯示使用者上次登入的時間及日期，預設值爲yes。
- **UseLogin**：是否允許在交談式登入階段使用login指令，預設值爲no。
- **KeepAlive**：指定伺服器是否傳送TCP keepalive訊息給用戶端，若是啓用此選項，則任何閒置的用戶端都將收到警示訊息，除非之間的連線已中斷，預設值爲yes。
- **Compression**：是否啓用檔案壓縮功能，預設值爲yes。



# 用戶端連接



# 以ssh指令登入遠端主機

---

## ssh指令語法

ssh 主機名稱或IP位址

---

# 以sftp指令與遠端主機傳輸檔案

---

## sftp指令語法

sftp 帳號名稱@主機名稱或IP位址

---

# 以scp指令與遠端主機傳輸檔案

---

## scp指令語法

scp 本地檔案 使用者名稱@遠端主機名稱或IP位址：/遠端檔案名稱

---