Ubuntu 环境下 SSH 的安装及使用

1. ssh 简介及工作机制

Secure Shell（缩写为 SSH），由 IETF 的网络工作小组（Network Working Group）所制定；SSH 为一项创建在应用层和传输层基础上的安全协议，为计算机上的 Shell（壳层）提供安全的传输和使用环境。

最初的 SSH 协议是由芬兰的一家公司的研究员 Tatu Ylönen 于 1995 年设计开发的，但是因为受版权和加密算法等等的限制，现在很多人都转而使用 OpenSSH。OpenSSH 是 SSH 的替代软件包，而且是开放源代码和免费的。

SSH 分为两部分：客户端部分和服务端部分。

服务端是一个守护进程(demon)，他在后台运行并响应来自客户端的连接请求。服务端一般是 sshd 进程，提供了对远程连接的处理，一般包括公共密钥认证、密钥交换、对称密钥加密和非安全连接。

客户端包含 ssh 程序以及像 scp（远程拷贝）、slogin（远程登陆）、sftp（安全文件传输）等其他的应用程序。

他们的工作机制大致是本地的客户端发送一个连接请求到远程的服务端，服务端检查申请的包和 IP 地址再发送密钥给 SSH 的客户端，本地再将密钥发回给服务端，自此连接建立。刚才所讲的只是 SSH 连接的大致过程，SSH 1.x 和 SSH 2.x 在连接协议上还有着一些差异。

SSH 被设计成为工作于自己的基础之上而不利用超级服务器(inetd)，虽然可以通过 inetd 上的 tcpd 来运行 SSH 进程，但是这完全没有必要。启动 SSH 服务器后，sshd 运行起来并在默认的 22 端口进行监听（你可以用 # ps -waux | grep sshd 来查看 sshd 是否已经被正确的运行了）如果不是通过 inetd 启动的 SSH，那么 SSH 就将一直等待连接请求。当请求到来的时候 SSH 守护进程会产生一个子进程，该子进程进行这次的连接处理。

但是因为受版权和加密算法的限制，现在很多人都转而使用 OpenSSH。OpenSSH 是 SSH 的替代软件，而且是免费的，

SSH 分客户端 openssh-client 和 openssh-server。如果只是想登陆别的机器的 SSH 只需要安装 openssh-client（ubuntu 有默认安装，如果没有则 sudoapt-get install openssh-

client），如果要使本机开放 SSH 服务就需要安装 openssh-server。

2. 安装客户端

```
sudo apt-get install ssh  或者 sudo apt-get installopenssh-client

ssh-keygen
```

根据提示按回车，(按回车设置默认值)

按缺省生成 id_rsa 和 id_rsa.pub 文件，分别是私钥和公钥。

说明：如果 sudo apt-get insall ssh 出错，无法安装可使用 sudo apt-get install openssh-client 进行安装。

假定服务器 IP 为 192.168.1.103，服务器上用户为 learningx；

用 ssh 登录服务器的命令为：

```
ssh  learningx@192.168.1.103
```

按照提示输入服务器密码即可远程连接。

3. 安装服务端

Ubuntu 缺省没有安装 SSH Server，使用以下命令安装：

```
sudo apt-get install openssh-server
```

然后确认 sshserver 是否启动了：（或用“netstat -tlp”命令）

```
ps -e|grep ssh
```

如果只有 ssh-agent 那 ssh-server 还没有启动，需要/etc/init.d/ssh start，如果看到 sshd 那说明 ssh-server 已经启动了。

如果没有则可以这样启动：

```
sudo/etc/init.d/ssh start
```

到这里 OpenSSH Server 就算安装好了。