Linux服务器的初步配置流程

作者： [阮一峰](http://www.ruanyifeng.com/)

日期： [2014年3月14日](http://www.ruanyifeng.com/blog/2014/03/)

开发网站的时候，常常需要自己配置Linux服务器。

本文记录配置Linux服务器的初步流程，也就是系统安装完成后，下一步要做的事情。这主要是我自己的总结和备忘，如果有遗漏，欢迎大家补充。

下面的操作针对Debian/Ubuntu系统，其他Linux系统也类似，就是部分命令稍有不同。



第一步：root用户登录

首先，使用root用户登录远程主机（假定IP地址是128.199.209.242）。

ssh root@128.199.209.242

这时，命令行会出现警告，表示这是一个新的地址，存在安全风险。键入yes，表示接受。然后，就应该可以顺利登入远程主机。

接着，修改root用户的密码。

passwd

第二步：新建用户

首先，添加一个用户组（这里假定为admin用户组）。

addgroup admin

然后，添加一个新用户（假定为bill）。

useradd -d /home/bill -s /bin/bash -m bill

上面命令中，参数d指定用户的主目录，参数s指定用户的shell，参数m表示如果该目录不存在，则创建该目录。

接着，设置新用户的密码。

passwd bill

将新用户（bill）添加到用户组（admin）。

usermod -a -G admin bill

接着，为新用户设定sudo权限。

visudo

visudo命令会打开sudo设置文件/etc/sudoers，找到下面这一行。

root ALL=(ALL:ALL) ALL

在这一行的下面，再添加一行。

root ALL=(ALL:ALL) ALL

bill ALL=(ALL) NOPASSWD: ALL

上面的NOPASSWD表示，切换sudo的时候，不需要输入密码，我喜欢这样比较省事。如果出于安全考虑，也可以强制要求输入密码。

root ALL=(ALL:ALL) ALL

bill ALL=(ALL:ALL) ALL

然后，先退出root用户的登录，再用新用户的身份登录，检查到这一步为止，是否一切正常。

exit

ssh bill@128.199.209.242

第三步：SSH设置

首先，确定本机有SSH公钥（一般是文件~/.ssh/id\_rsa.pub），如果没有的话，使用ssh-keygen命令生成一个（可参考我写的[SSH教程](http://www.ruanyifeng.com/blog/2011/12/ssh_remote_login.html" \t "_blank)）。

在本机上另开一个shell窗口，将本机的公钥拷贝到服务器的authorized\_keys文件。

cat ~/.ssh/id\_rsa.pub | ssh bill@128.199.209.242 'mkdir -p .ssh && cat - >> ~/.ssh/authorized\_keys'

# 或者在服务器端，运行下面命令

echo "ssh-rsa [your public key]" > ~/.ssh/authorized\_keys

然后，进入服务器，编辑SSH配置文件/etc/ssh/sshd\_config。

sudo cp /etc/ssh/sshd\_config ~

sudo nano /etc/ssh/sshd\_config

在配置文件中，将SSH的默认端口22改掉，可以改成从1025到65536之间的任意一个整数（这里假定为25000）。

Port 25000

然后，检查几个设置是否设成下面这样，确保去除前面的#号。

Protocol 2

PermitRootLogin no

PermitEmptyPasswords no

PasswordAuthentication no

RSAAuthentication yes

PubkeyAuthentication yes

AuthorizedKeysFile .ssh/authorized\_keys

UseDNS no

上面主要是禁止root用户登录，以及禁止用密码方式登录。

接着，在配置文件的末尾，指定允许登陆的用户。

AllowUsers bill

保存后，退出文件编辑。

接着，改变authorized\_keys文件的权限。

sudo chmod 600 ~/.ssh/authorized\_keys && chmod 700 ~/.ssh/

然后，重启SSHD。

sudo service ssh restart

# 或者

sudo /etc/init.d/ssh restart

下面的一步是可选的。在本机~/.ssh文件夹下创建config文件，内容如下。

Host s1

HostName 128.199.209.242

User bill

Port 25000

最后，在本机另开一个shell窗口，测试SSH能否顺利登录。

ssh s1

第四步：运行环境配置

首先，检查服务器的区域设置。

locale

如果结果不是en\_US.UTF-8，建议都设成它。

sudo locale-gen en\_US en\_US.UTF-8 en\_CA.UTF-8

sudo dpkg-reconfigure locales

然后，更新软件。

sudo apt-get update

sudo apt-get upgrade

最后，再根据需要，做一些安全设置，比如搭建防火墙，关闭HTTP、HTTPs、SSH以外的端口，再比如安装Fail2Ban，详细可参考这篇[《Securing a Linux Server》](http://spenserj.com/blog/2013/07/15/securing-a-linux-server/)。

（完）