# 操作步骤 （Ubuntu 1604 server）

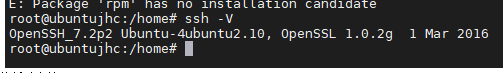
## 版本说明

zlib-1.2.7> zlib-1.2.11（目标版本）

OpenSSL 1.0.2g > OpenSSL 1.1.1l（目标版本）

OpenSSH 7.2p2 > OpenSSH -8.8p1（目标版本）

升级前目标版本查询：

****

**前提条件：**

**使用的虚拟机在安装过程中安装了openssh server，版本是7.7p2，但是虚拟机中缺少gcc、make等编译功能，离线升级的情况下，需要通过镜像文件配置apt本地源。**

**具体步骤如下：**

**将镜像挂载到虚拟机**

**以VMware Workstation为例，打开“虚拟机设置”，点击“CD/DVD”选项，将 “设备状态”中的“已连接”勾选上。然后选择下方“使用ISO镜像文件”，点击浏览，选择与虚拟机操作系统相同的系统镜像文件即可。**

**进行iso挂载**

**# 执行下面三条命令进行iso挂载**

**## 如果这一步有报错找不到CD-rom，可以将上一步的CD/DVD删掉重新添加一次，重启系统再执行下面命令**

**mkdir /media/cdrom**

**#mount 挂载镜像到本地目录**

**mount -t iso9660 -o loop /dev/sr0 /media/cdrom (或者：mount -t auto /dev/cdrom /media/cdrom)**

**#备注：**

**#/dev/cdrom 与 /dev/sr0都是系统文件名，两个在光盘挂载时是一样的，所以用哪个都行。/media/cdrom是挂载点，是自定义的。**

**#如果用完想退出光盘镜像文件的话，必须先解除挂载。umount命令加系统文件名或挂载点，如umount /dev/sr0**

**#添加本地目录到软件源**

**sudo apt-cdrom -m -d=/media/cdrom add**

**查看apt源地址**

**cat /etc/apt/sources.list 注释在线源**

**如果不用在线的软件源，则将其他的注释掉只保留本地源即可。**

**#进行本地库依赖更新**

**apt-get update**

**安装gcc、make**

**apt install gcc**

**apt install make**

## step 1 、升级前提说明：（参考）

1、升级OpenSSH后，原有公钥失效，信任关系需要重新配置；

2、升级过程需要停止sshd服务，会导致ssh和sftp无法使用；

4、升级需要关闭防火墙服务；

5、升级需要关闭selinux服务；

7、升级过程中需要刷新lib库：ldconfig -v；

8、升级顺序：顺序是zlib库-> openssl -> openssh；

9、升级需要gcc、make、perl、zlib、zlib-devel、pam、pam-devel；

## step 2、安装包准备

1. 下载软件包

zlib-1.2.11下载链接：http://www.zlib.net/zlib-1.2.11.tar.gz

OpenSSL 1.1.1lo下载链接：https://www.openssl.org/source/openssl-1.1.1l.tar.gz

OpenSSH -8.8p1下载链接：https://cloudflare.cdn.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-8.8p1.tar.gz

2、创建上传目录

通过WinSCP 上传到home文件夹下

说明：

Ubuntu Winscp 连接方式

1、刚开始winscp 以root账号登录，一直拒绝访问，以一般用户登录，权限不够。

2、在虚拟机中执行sudo passwd root,修改密码，以刚修改的密码来登录winscp即可。

3、vi /etc/ssh/sshd\_config，修改PermitRootLogin without-password 为PermitRootLogin yes 。

4、重启

## step 3、正式开始升级openssh

升级顺序：zlib库-> openssl -> openssh

1、停止sshd服务

systemctl stop sshd

#service ssh stop

systemctl is-active sshd

2、卸载系统里原有Openssh

查看系统原有openssh包

ps -e | grep ssh #查询SSH相关进程

service sshd stop #停止SSH服务

apt purge openssl #卸载openssl相关组件

#卸载openssh相关组件

apte-get remove openssh-server openssh-client

#删除原ssh配置目录

#rm  -rf  /etc/ssh

service ssh status #查询SSH服务状态

3、编译安装zlib

解压安装zlib

cd /home/

tar -xzvf zlib-1.2.11.tar.gz

cd zlib-1.2.11

./configure –prefix=/usr/local/zlib

make&&make install

验证zlib安装是否成功

cd /usr/local/zlib

ll

要包含include、lib、share上个目录。

编辑配置文件/etc/ld.so.conf.d/zlib.conf

vi /etc/ld.so.conf.d/zlib.conf

加入如下内容后保存退出

/usr/local/zlib/lib

刷新库文件

ldconfig -v，刷新库文件，加载刚才编译安装的zlib生成的库文件

ldconfig -v

4、升级OpenSSL

解压安装openssl包

cd /home/

tar -xzvf openssl-1.1.1l.tar.gz

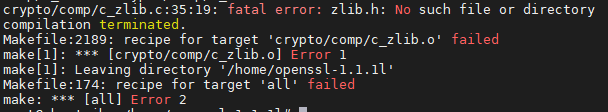
编译openssl

cd openssl-1.1.1l

./config shared zlib （配置时调用zlib库）

Make

如果有问题：



在/home/zlib-1.2.11执行

cp zutil.h /usr/local/include

cp zutil.c /usr/local/include

make install

创建ssl相关软连接

ln -s /usr/local/ssl/bin/openssl /usr/bin/openssl

ln -s /usr/local/ssl/include/openssl /usr/include/openssl

编辑配置文件/etc/ld.so.conf.d/ssl.conf 可不执行

vi /etc/ld.so.conf.d/ssl.conf

加入如下内容后保存退出

/usr/local/ssl/lib

刷新库文件

ldconfig -v，刷新库文件，加载刚才编译安装的ssl生成的库文件

ldconfig -v

查看openssl版本

openssl version -a

当出现问题：

openssl: error while loading shared libraries: libssl.so.1.1: cannot open shared object file

查找一下libssl.so.1.1的位置，然后连接到/usr/lib64/libssl.so.1.1即可。如下我的位置是在/usr/local/lib64/libssl.so.1.1，连接到/usr/lib64/libssl.so.1.1就可以了。

# find / -name libssl.so.1.1

/usr/local/lib64/libssl.so.1.1

# ln -s /usr/local/lib64/libssl.so.1.1 /usr/lib64/libssl.so.1.1

# ln -s /usr/local/lib64/libcrypto.so.1.1 /usr/lib64/libcrypto.so.1.1

# openssl version -a

OpenSSL 1.1.1l 24 Aug 2021

5、升级OpenSSH

重命名原有配置文件

解压openssh

tar -xzvf openssh-8.8p1.tar.gz

cd openssh-8.8p1/

./configure --prefix=/usr/local/openssh --sysconfdir=/etc/ssh --with-ssl-dir=/usr/local/ssl --mandir=/usr/share/man --with-zlib=/usr/local/zlib

上面为一行。

make

make install

验证openssh版本

/usr/local/openssh/bin/ssh -V

设置sshd服务开机自动启动

拷贝配置文件

cp /home/openssh-8.8p1/contrib/redhat/sshd.init /etc/init.d/sshd

修改配置文件权限

chmod u+x /etc/init.d/sshd

添加sshd服务，开机启动

Systemctl enable sshd #设定指定服务开机开启

替换配置文件

cp /home/openssh-8.8p1/sshd\_config /etc/ssh/sshd\_config

编辑sshd\_config文件

将subsystem sftp路径变更为实际路径/usr/local/openssh/libexec/sftp-server

vi /etc/ssh/sshd\_config

#Subsystem sftp /usr/libexec/sftp-server

注释掉，换为如下一句：

Subsystem sftp /usr/local/openssh/libexec/sftp-server

拷贝命令

cp /usr/local/openssh/sbin/sshd /usr/sbin/sshd

拷贝sshd命令至/usr/bin/

cp /usr/local/openssh/bin/ssh /usr/bin/

ssh -V

拷贝ssh-keygen

cp /usr/local/openssh/bin/ssh-keygen /usr/bin/ssh-keygen

修改配置文件/etc/ssh/sshd\_config

vi /etc/ssh/sshd\_config

PasswordAuthentication yes #取消这一行注释

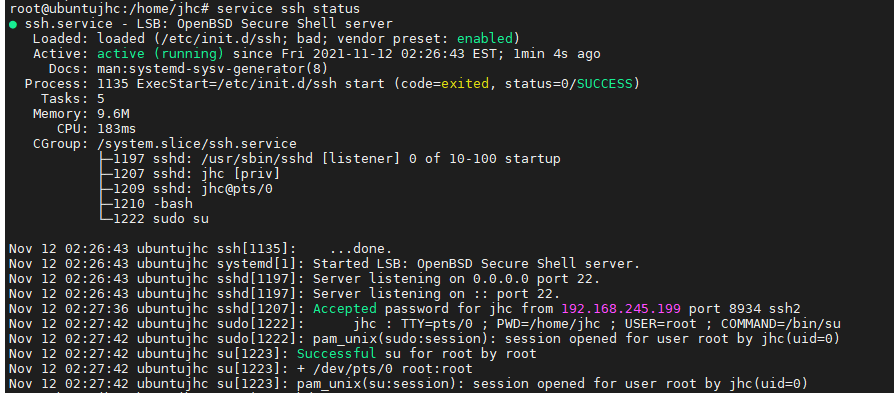
PermitRootLogin yes #添加PermitRootLogin yes行

重启sshd服务

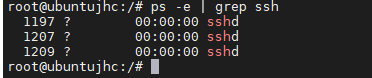
service ssh restart

service ssh start

安装后结果：







备注：

1、当出现Failed to start SYSV: OpenSSH server daemon.报错时或者It is recommended that your private key files are NOT accessible by others.

This private key will be ignored这个提示时：

# cd /etc/ssh

# chmod 600 file（给上面报错提到的文件添加权限）

2、若出现Unit ssh.service is masked.

使用Systemctl unmask ssh命令。解除冻结。

3、若出现 ssh 的状态为active(exited)

使用/etc/init.d/ssh start命令，启动成功

4、有需要的话修改 config 文件，取消对Port 22 端口的注释

vi /etc/ssh/sshd\_config

ssh 默认 22端口

打开注释掉的或者加上

Port 22

5、./config shared --prefix=/usr/local/ssl