# 操作步骤 （CentOS 7）

## 版本说明

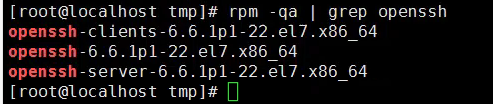
zlib-1.2.7> zlib-1.2.11（目标版本）

OpenSSL 1.0.1e > OpenSSL 1.1.1lo（目标版本）

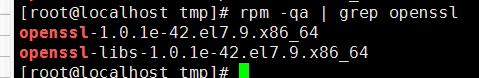
OpenSSH 6.6.1p1 > OpenSSH -8.8p1（目标版本）

升级前目标版本查询：

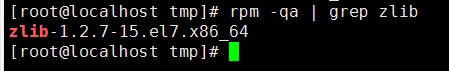
Openssh



Openssl



Zlib



## step 1 、升级前提说明：

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；

3、升级OpenSSH影响的业务有：QDG同步、Mediation及现场自己写的同步脚本等；

4、升级需要关闭防火墙服务；

5、升级需要关闭selinux服务；

6、升级前需要开启telnet，防止升级失败，系统无法登录，对应的防火墙需要开启23端口，安装需要telnet相关包（推荐通过系统ISO安装）

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 3、关闭防火墙和selinux

systemctl status firewalld.service

检查防火墙状态，如果在运行停掉。

systemctl stop firewalld.service

关闭开机自启动

systemctl disable firewalld

## step 4 、验证selinux是否关闭

getenforce

如果未关闭，关闭之

setenforce 0

上面只是临时关闭了，重启后不生效。下面改配置文件，使永久生效。

vi /etc/selinux/config

修改：

SELINUX=disabled

保存退出。

step 5、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

## step 6、开启telnet （非必须）

临时开启telnet服务，用于升级ssh，同时方总升级ssh过程中主机无法登录。

1、挂载操作系统镜像

2、安装ftp所需系统包

yum -y install xinetd telnet telnet-server

3、改/etc/pam.d/login配置文件

编辑/etc/pam.d/login，注释掉下面这行，允许root用户通过telnet登陆：

#auth [user\_unknown=ignore success=ok ignore=ignore default=bad] pam\_securetty.so

4、编辑/etc/securetty

编辑/etc/securetty，添加超级用户登陆设备。

备份/etc/securetty文件：

cp /etc/securetty /etc/securetty.bak

添加超级用户登陆设备至/etc/securetty文件：

echo "pts/1" >> /etc/securetty

echo "pts/2" >> /etc/securetty

echo "pts/3" >> /etc/securetty

echo "pts/4" >> /etc/securetty

echo "pts/5" >> /etc/securetty

echo "pts/6" >> /etc/securetty

echo "pts/7" >> /etc/securetty

echo "pts/8" >> /etc/securetty

echo "pts/9" >> /etc/securetty

echo "pts/10" >> /etc/securetty

echo "pts/11" >> /etc/securetty

5、编辑/etc/pam.d/remote

编辑/etc/pam.d/remote，注释下列这行，开启root用户远程登陆：

vi /etc/pam.d/remote

#auth required pam\_securetty.so

6、重启telnet和xinetd服务

PS：telnet服务依赖于xinetd服务。

systemctl start telnet.socket

systemctl start xinetd

PS：如果开启了防火墙，需要将23端口（系统默认23为telnet端口）添加到防火墙允许的端口的列表中。

7、开启telnet和xinetd开机自动启动

systemctl enable xinetd.service

systemctl enable telnet.socket

8、验证开机启动

systemctl list-unit-files |grep telnet

systemctl list-unit-files |grep xinetd

## step 7、安装openssh升级依赖包 （离线升级不需要）

yum -y install gcc make perl zlib zlib-devel pam pam-devel

检查相关依赖包是否安装

rpm -qa | egrep "gcc|make|perl|zlib|zlib-devel|pam|pam-devel"

## step 8、正式开始升级openssh

升级顺序：zlib库-> openssl -> openssh

1、停止sshd服务

systemctl stop sshd

systemctl is-active sshd

2、卸载系统里原有Openssh

查看系统原有openssh包

rpm -qa | grep openssh

根据上面查询出的结果，卸载系统里原有Openssh

rpm -e openssh --nodeps

rpm -e openssh-server --nodeps

rpm -e openssh-clients --nodeps

验证

rpm -qa | grep openssh

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

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 test

make install

重命名现有文件目录

mv /usr/bin/openssl /usr/bin/openssl.OFF

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

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

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

mv /etc/ssh /etc/ssh.bak

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

chkconfig --add sshd

验证开机启动

chkconfig --list|grep sshd

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

PS：如果不允许root用户远程直接登录，这里配置为PermitRootLogin no；

重启sshd服务

service sshd restart

systemctl is-active sshd

查看22端口监听

netstat -an |grep LISTEN|grep :22

安装后结果：



备注：

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）