OpenSSL 和 OpenSSH 源码升级过程

版本	日期	作者	说明
1.0	2020.07.06	雷殊隐	N/A

1. 简要描述

本文描述了在 Centos 操作系统上，升级 OpenSSL 版本至 1.1.1.g，升级 OpenSSH 版本至 8.2p1 的详细过程。升级目的是实现后续开发测试环境版本与客户机环境一致。本文主要参考了博客*升级 openssh 到 openssh-8.0p1 版本*，但本文环境与原博客所述环境略有不同，因此部分命令需要修改。主要有几个步骤：

(1) 使用 yum 升级 OpenSSH 和 OpenSSL；
(2) 安装和配置 telnet 服务；
(3) 安装和升级相关依赖包（gcc、pre-dvel 等）；
(4) 下载相应版本 OpenSSL 源码和 OpenSSH 源码；
(5) 编译安装新版本的 OpenSSL 和 OpenSSH；
(6) 测试。

2. 准备工作

（1）先使用 yum 升级 OpenSSH 和 OpenSSL 到较高版本，但该方式往往不能升级到最新版本。此后安装 telnet Sever。依次使用命令为：

序号	命令	说明
1	ssh -V	查看 OpenSSH 和 OpenSSL 版本
2	yum update openssh -y	升级 OpenSSH
3	yum install xinetd telnet-server -y	安装 telnet-server 以及 xinetd

（2）配置 telnet 服务。首先配置 telnet 登录的终端类型，在/etc/securetty 文件末尾增加一些 pts 终端。然后启动 telnet 服务，并设置开机自动启动。最后将与服务器的连接方式切换到 telnet 方式登录，以后的操作都在 telnet 终端下操作，防止 ssh 连接意外中断造成升级失败。依次使用命令为：

序号	命令	说明
1	vim /etc/securetty	增加： pts/0 pts/1 pts/2 pts/3
2	systemctl enable xinetd systemctl enable telnet.socket systemctl start telnet.socket systemctl start xinetd	启动 telnet 服务； 设置开机自启动
3	在 XShell 中切换连接方式为 Telnet	N/A

（3）安装相关依赖包，下载相应版本 OpenSSL 源码和 OpenSSH 源码。主要包括 pam、zilib、和编译相关依赖包和。依次使用命令为：

序号	命令	说明
1	yum install -y gcc gcc-c++ glibc make autoconf openssl openssl-devel pcre-devel pam-devel	安装编译相关包
2	yum install -y pam* zlib*	安装 pam 和 zilib
3	https://openbsd.hk/pub/OpenBSD/OpenSSH/portable/ https://ftp.openssl.org/source/	下载源码

3. OpenSSL 升级

此步骤中，首先解压源码文件，备份相关文件。然后编译安装新版本的 OpenSSL、最后配置软链接并加载新配置。依次使用命令为：

序号	命令	说明
1	mkdir /data/tools -p cd /data/tools/ tar xfz openssl-1.1.1g.tar.gz	创建文件夹并解压源码
2	mv /usr/bin/openssl /usr/bin/openssl_bak mv /usr/include/openssl /usr/include/openssl_bak	备份相关文件（如果存在）
3	cd /data/tools/openssl-1.1.1g/ ./config shared && make && make install echo $?	编译源码 echo 结果为 0 表示编译成功
4	ln -s /usr/local/ssl/bin/openssl /usr/bin/openssl ln -s /usr/local/ssl/include/openssl /usr/include/openssl	配置软链接
5	echo "/usr/local/ssl/lib" >> /etc/ld.so.conf /sbin/ldconfig	加载新配置

若报错：openssl: error while loading shared libraries: libssl.so.1.1: cannot open shared object file: No such file or directory;

解决办法为新增如下软链接：

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

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

4. OpenSSH 升级

首先删除原先SSH的配置文件和目录，然后编译安装，最后修改sshd_config，设置开机自启动并启动服务。依次按如下命令进行：

序号	命令	说明
1	rm -rf /etc/ssh/*	删除原先 SSH 配置
2	./configure --prefix=/usr/ --sysconfdir=/etc/ssh --with-openssl-includes=/usr/local/ssl/include --with-ssl-dir=/usr/local/lib64/ --with-zlib --with-md5-passwords --with-pam && make && make install	编译源码
3	vim /etc/ssh/sshd_config	修改配置文件： PermitRootLogin yes
4	cp -a contrib/redhat/sshd.init /etc/init.d/sshd cp -a contrib/redhat/sshd.pam /etc/pam.d/sshd.pam chmod +x /etc/init.d/sshd chkconfig --add sshd systemctl enable sshd	复制相关文件 （此步骤或可以省略）
5	mv /usr/lib/systemd/system/sshd.service /data/	移走原先的 sshd 服务
6	chkconfig sshd on	设置 sshd 开机自启动

5. 测试启停服务

最后对新版本的 sshd 测试启停服务。依次执行命令如下：

序号	命令	说明
1	systemctl stop sshd netstat -lntp	停用 sshd
2	systemctl start sshd netstat -lntp	启动 sshd
3	systemctl restart sshd netstat -lntp	重启 sshd

注：若更新版本后连接报错：Permission denied，可尝试关闭 SELinux 服务。