# openssh 升级

**要先升级openssl（前提）**

./configure --help 可查看支持的编译参数

**9.0不支持以下参数**

configure: WARNING: unrecognized options: --with-openssl-includes, --with-md5-passwords

#!/bin/bash  
export PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin  
  
if [ $UID -ne 0 ]; then  
echo "Superuser privileges are required to run this script."  
exit 1  
fi  
  
log\_err() {  
 printf "[$(date +'%Y-%m-%dT%H:%M:%S')]: \033[31mERROR: $@ \033[0m\n"  
}  
  
log\_info() {  
 printf "[$(date +'%Y-%m-%dT%H:%M:%S')]: \033[32mINFO: $@ \033[0m\n"  
}  
  
log\_warning() {  
 printf "[$(date +'%Y-%m-%dT%H:%M:%S')]: \033[33mWARNING: $@ \033[0m\n"  
}  
  
sh\_path=$(cd `dirname $0`;pwd)  
LOGDIR=/var/log/init\_record  
if [ ! -d ${LOGDIR} ];then mkdir -vp ${LOGDIR}; fi  
  
upgrade\_openssh () {  
 log\_info "[-] update\_openssh Configuring..." |tee -a ${LOGDIR}/${log\_name}  
 #yum -y install gcc gcc-c++ glibc make autoconf openssl openssl-devel pcre-devel pam-devel |tee -a ${LOGDIR}/${log\_name}  
 #yum install -y zlib\* pam\* zlib\* |tee -a ${LOGDIR}/${log\_name}  
 mv /etc/ssh{,.bak}  
 tar xf ${opensshVer}.tar.gz  
  
  
 #先备份  
 mv /usr/sbin/sshd{,.bak}   
 mv /usr/bin/ssh{,.bak}  
 mv /usr/bin/ssh-keygen{,.bak}  
 #拷贝文件  
 \cp -av /usr/local/openssh/bin/ssh /usr/bin/ssh |tee -a ${LOGDIR}/${log\_name}  
 \cp -av /usr/local/openssh/bin/ssh-keygen /usr/bin/ssh-keygen |tee -a ${LOGDIR}/${log\_name}  
 \cp -av /usr/local/openssh/sbin/sshd /usr/sbin/sshd |tee -a ${LOGDIR}/${log\_name}  
 #查看openssh当前版本  
 ssh -V |tee -a ${LOGDIR}/${log\_name}  
 #重新启动openssh服务  
 #先停止服务  
 systemctl disable sshd --now |tee -a ${LOGDIR}/${log\_name}  
 #备份文件  
 mv /usr/lib/systemd/system/sshd.service{,.bak}   
 #重载守护进程  
 systemctl daemon-reload |tee -a ${LOGDIR}/${log\_name}  
 #复制配置文件   
 cd ${sh\_path}/${opensshVer}  
 cp -av contrib/redhat/sshd.init /etc/init.d/sshd |tee -a ${LOGDIR}/${log\_name}  
 cp -av contrib/redhat/sshd.pam /etc/pam.d/sshd.pam |tee -a ${LOGDIR}/${log\_name}  
 #\cp -av /etc/ssh.bak/sshd\_config /etc/ssh/ |tee -a ${LOGDIR}/${log\_name}  
 grep ^[a-Z] /etc/ssh.bak/sshd\_config|egrep -v "Subsystem|AuthorizedKeysFile" >> /etc/ssh/sshd\_config  
 #添加设置  
 chkconfig --add sshd |tee -a ${LOGDIR}/${log\_name}  
 #重新开启服务  
 systemctl enable sshd --now |tee -a ${LOGDIR}/${log\_name}  
 systemctl restart sshd  
 cd ${sh\_path}  
 log\_info "[\*] update\_openssh successful!" |tee -a ${LOGDIR}/${log\_name}  
}  
  
check\_openssh(){  
 log\_name=check\_openssh.log  
 succ\_num=$(grep successful ${LOGDIR}/${log\_name}|wc -l)  
 if [ ! -f ${LOGDIR}/${log\_name} -o ${succ\_num} -eq 0 ];then  
 while true;do  
 curl https://mirrors.aliyun.com/openssh/portable/ > dwopenssh.log 2>&1  
 num=$(grep openssh-.\*tar.gz dwopenssh.log|grep -v asc|wc -l)  
 if [ ${num} -le 0 ];then   
 echo "未获取到最新版本，将继续尝试下载，请耐心等待！" |tee -a ${LOGDIR}/${log\_name}  
 else   
 echo "获取到最新版本,开始下载！" |tee -a ${LOGDIR}/${log\_name}  
 opensshVer=$(grep openssh-.\*tar.gz dwopenssh.log|grep -v asc|tail -n1|awk -F'"' '{print $4}'| awk -F . '{print $1"."$2}')  
 while true;do  
 wget --no-check-certificate https://mirrors.aliyun.com/openssh/portable/${opensshVer}.tar.gz |tee -a ${LOGDIR}/${log\_name}  
 if [ "$?" != 0 ];then  
 echo "未下载成功，将继续尝试下载，请耐心等待！" |tee -a ${LOGDIR}/${log\_name}  
 else   
 echo "下载成功,开始部署！" |tee -a ${LOGDIR}/${log\_name}  
 upgrade\_openssh  
 break  
 fi  
 done  
 break  
 fi  
 done  
 else  
 log\_info "[\*] update\_openssh Configuration already!...!"  
 fi  
}  
  
main (){  
 check\_openssh  
}  
  
main "$@"