openssh升级

重要，使用新的客户端成功连接前，千万不要断开**ssh**连接，否则就接不上了；确定升级完成、新的客户端可以连接后才断开，请确保电脑连接了电源，网络畅通

升级openssl

openssl https://www.openssl.org/source/

```
# 下载源代码
wget https://www.openssl.org/source/openssl-3.3.1.tar.gz

# 解压缩
tar -xvzf openssl-3.3.1.tar.gz

# 安装依赖
yum install perl-IPC-Cmd

# 配置
./config --prefix=/usr/local/openssl --openssldir=/usr/local/openssl
# --prefix=/usr/local/openssl 安装目录
# --openssldir=/usr/local/openssl 配置目录

# 编译
make -j$(nproc)

# 测试，非必要，测试失败不意味着编译安装会失败
make test

# 安装，openssl将被安装到 /usr/local/openssl
make install

# 验证版本
/usr/local/openssl/bin/openssl version
```

openssl **/usr/local/openssl** 。可能提示找不到 libcrypto.so.3 库，需要建立共享库搜寻路径

```
# □□□□□□□□□□
echo "/usr/local/openssl/lib64" | sudo tee /etc/ld.so.conf.d/openssl.conf

# □□□□□□□□□□
ldconfig
```

openssh□□

openssh □□□□□ https://cdn.openbsd.org/pub/OpenBSD/OpenSSH/portable/

```
# □□sshd□□
ssh -V
sshd -V

# □□□□□□ssh□□□
# https://cdn.openbsd.org/pub/OpenBSD/OpenSSH/portable/
# 2025□9□23□
wget https://cdn.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-10.0p2.tar.gz

# □□□□□
tar -xvzf openssh-10.0p2.tar.gz

# □□GCC□□□
yum install gcc

# □□zlib□□
yum install zlib-devel

# □□pam□□
yum install pam-devel

# □□□□□□□
cp -a /etc/ssh/ /etc/ssh_bak/

# □□□□□(□□□□□□□SSH□□□□□□ssl□□□□□□□□□)
./configure --prefix=/usr --sysconfdir=/etc/ssh --with-md5-passwords --with-pam --with-zlib
```

此时还可能提示openssl不存在、版本太低，如果本机没有openssl，则参见openssl升级

```
# 查看openssl版本
openssl version

# 查看openssl位置
which openssl

查看openssl库文件位置
ldd /usr/bin/openssl

# 指定openssh需要使用的openssl库文件位置
./configure --prefix=/usr --sysconfdir=/etc/ssh --with-md5-passwords --with-pam --with-zlib --
with-ssl-dir=/usr/local/openssl

# 编译并安装
make -j$(nproc)

make install

# 验证ssh版本
ssh -V
sshd -V

# 验证配置文件正确性
/usr/sbin/sshd -t -f /etc/ssh/sshd_config

# 修改配置文件权限，如果验证配置文件正确性语句出错的话
chmod 0600 /etc/ssh/ssh_host_rsa_key
chmod 0600 /etc/ssh/ssh_host_ecdsa_key
chmod 0600 /etc/ssh/ssh_host_ed25519_key

# 修改配置文件，如果验证配置文件正确性语句出错的话
vi /etc/ssh/sshd_config

# 修个sshd_config配置文件，启用以下两个配置
UsePAM yes
PermitRootLogin yes
# 修个sshd_config配置文件，禁用以下四个配置
```

```
#GSSAPIAuthentication yes
#GSSAPICleanupCredentials no
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no
#GSSAPIEnablek5users no

# 重启sshd服务,
systemctl restart sshd

# 此时可能重启失败,使用journalctl -xe 查看错误信息,一般是提示找不到 libcrypto.so.3 库
# 将库建立软连接到共享库目录
ln -s /usr/local/openssl/lib64/libcrypto.so.3 /usr/lib64/libcrypto.so.3

# 重启sshd服务卡主,修改服务通知类型为simple
vi /usr/lib/systemd/system/sshd.service
# Type=simple

systemctl daemon-reload
# 重启sshd服务
systemctl restart sshd

# 禁用ssh客户端
vi /etc/ssh/ssh_config
```

升级完成后,旧版的xshell提示,找不到匹配的host key算法,这是旧版xhsell的bug,需要升级xshell

直接在服务器使用ssh命令连接到其他机器报错: /etc/ssh/ssh_config line 59: Unsuppor "gssapiauthentication"

```
# 修改配置文件,是ssh,不是sshd
vi /etc/ssh/ssh_config

# 注释本行
# GSSAPIAuthentication yes
```

版本号 #24
创建于 30 十一月 2023 02:40:58
由 董列涛 更新于 2 四月 2026 05:31:28