SSH

1. SSH证书介绍

Secure Shell (SSH) 是一个允许两台电脑之间通过安全的连接进行数据交换的网络协议。通过加密保证了数据的保密性和完整性。SSH采用公钥加密技术来验证远程主机，以及(必要时)允许远程主机验证用户。

1. 生成证书
2. 通过git，生成CA，即一对密钥
3. 运用命令

ssh-keygen -t rsa -b 4096 -f host\_ca -C host\_ca

生成签发服务器证书的密钥,即host\_ca（私钥）和 host\_ca.pub（公钥）

1. 运用命令

ssh-keygen -f ~/.ssh/ssh\_host\_rsa\_key -b 4096 -t rsa

生成服务器的密钥，即ssh\_host\_rsa\_key（私钥）和 ssh\_host\_rsa\_key.pub（公钥）

1. 运用命令

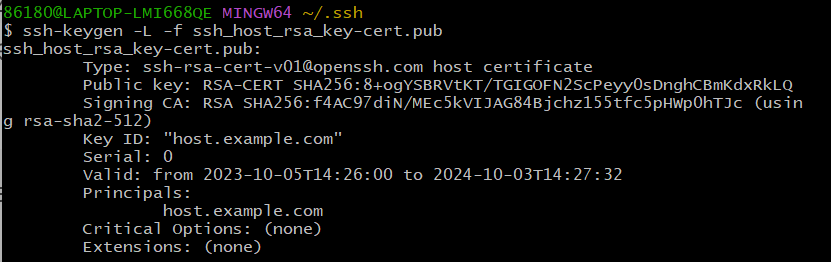
ssh-keygen -s host\_ca -I host.example.com -h -n host.example.com -V +52w ssh\_host\_rsa\_key.pub

生成服务器证书ssh\_host\_rsa\_key-cert.pub

1. 各字段意义
2. 在git命令行中，使用命令

ssh-keygen -L -f ssh\_host\_rsa\_key-cert.pub

查看证书的细节



1. 解析各字段含义：
   1. ssh\_host\_rsa\_key-cert.pub：这是证书文件的名称
   2. Type: ssh-rsa-cert-v01@openssh.com host certificate：证书的类型是SSH RSA服务器证书，使用了OpenSSH的标准v01格式。
   3. Public key: RSA-CERTSHA256:8+ogYSBRVtKT/TGIGOFN2ScPeyy0sDnghCBmKdxRkLQ：这是证书的公钥部分，使用SHA256算法进行哈希处理得到的指纹。
   4. Signing CA: RSA SHA256:f4AC97diN/MEc5kVIJAG84Bjchz155tfc5pHWp0hTJc (using rsa-sha2-512)：这是签发该证书的CA（证书颁发机构）的公钥信息，使用SHA256和rsa-sha2-512算法进行哈希处理得到的指纹。
   5. Key ID: "host.example.com"：证书的键ID字段，用于指示证书所属的实体或主机的标识。
   6. Serial: 0：证书的序列号。
   7. Valid: from 2023-10-05T14:26:00 to 2024-10-03T14:27:32：证书的有效期，从2023年10月5日14:26:00到2024年10月3日14:27:32。
   8. Principals：host.example.com被授权使用此证书的主机名称。
   9. Critical Options: (none)：关键选项，没有定义任何关键选项。
   10. Extensions: (none)：扩展字段，没有定义任何扩展信息。
2. 公钥算法
3. 这个证书使用的公钥算法是RSA（Rivest-Shamir-Adleman）。RSA是一种非对称加密算法，其中包含两个密钥：私钥和公钥。在这个证书中，ssh-rsa-cert-v01@openssh.com 表明使用了RSA算法生成的证书。RSA在SSH中广泛使用，用于建立安全的加密连接和进行身份验证。它能够实现数据的加密和数字签名，确保通信的机密性和完整性。
4. 除了RSA，SSH还支持其他的公钥算法，如DSA（Digital Signature Algorithm）、ECDSA（Elliptic Curve Digital Signature Algorithm）和EdDSA（Edwards-curve Digital Signature Algorithm）。
5. RSA加密流程：

①生成密钥对：

选择两个不同的质数：p 和 q。

计算 n = p \* q。

计算 λ(n) = lcm(p-1, q-1)。

选择一个整数 e，满足 1 < e < λ(n)，且 e 和 λ(n) 互质。

计算 d，满足 (d \* e) mod λ(n) = 1。 （可以使用扩展欧几里得算法来找到 d 的值。）

②加密：

假设要加密的消息为 m。

使用接收方的公钥 (n, e)。

计算密文 c = (m^e) mod n。

③解密：

使用私钥 (n, d)。

计算明文 m = (c^d) mod n。