SSH原理深度解析

—— 原理解析与应用技巧分享

关于SSH的一些声音

“SSH有啥好讲的？”

“SSH不就是一个Linux登陆么？”

“SSH还需要配置？”

“原来SSH可以长期保持连接”

“SSH安全性原来是这样保证的。”

“SSH核心技术居然中了2项图灵奖！！”

“.....”

报　告 人：郝伟

报告日期：2022年6月16日 (星期四)

报告时间：18:00-18:30

腾讯会议：594-695-631

面向听众：需要使用SSH的技术人员

北京华云安信息技术有限公司

目 录

CONTENTS

01 1 简介

SSH基本信息介绍

02 2 工作原理

SSH连接通信和加密等工作原理

03 3 配置文件

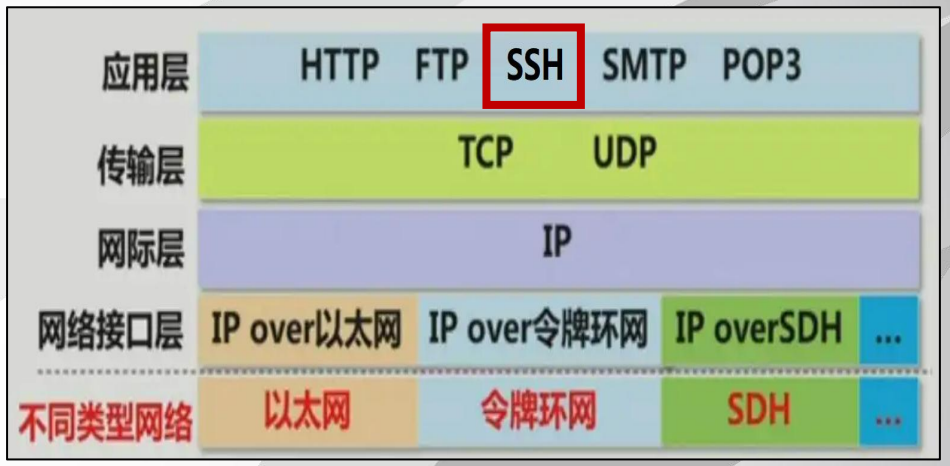
~/.ssh 目录中的文件作用

04 4 常用操作

SSH常用操作方法与技巧

SSH简介

- SSH(Secure SHell) 是一种常用的网络通信协议。
- SSH 是一种建立在应用层上用于提供可靠的消息信道。
- SSH 能够有效防止远程过程中的信息泄露。
- SSH最初是UNIX系统上，后来又迅速扩展到其他操作平台。
- SSH客户端适用于多种平台，几乎所有UNIX平台—包括HP-UX、Linux、AIX、Solaris、Digital UNIX、Irix等平台，当前Windows10,11也都整合了SSH。



网络层次结构

目 录

CONTENTS

01 1 简介

SSH基本信息介绍

02 **2 工作原理**

SSH连接通信和加密的工作原理

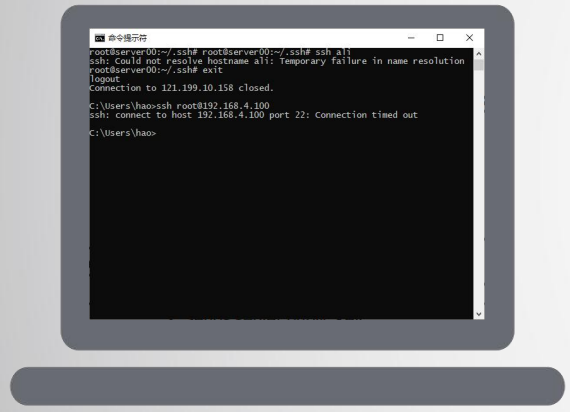
03 3 配置文件

~/.ssh 目录中的文件作用

04 4 常用操作

SSH常用操作方法与技巧

SSH 登陆原理



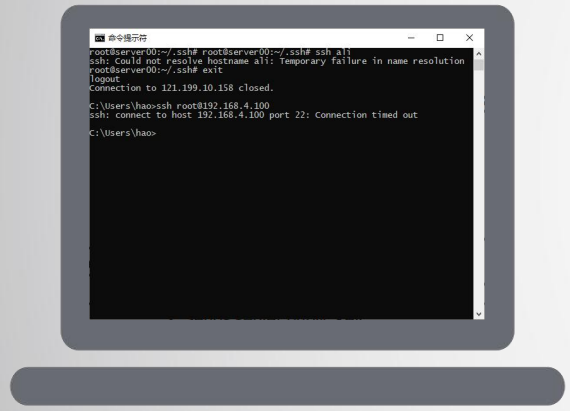
SSH Client

1. 客户端也服务器尝试初始化连接
2. 发送使用公钥加密的消息
3. 返回使用私钥解密的消息
4. 验证通过后沟通通信与连接通道参数
5. 用户登陆到服务器进行相关操作

SSH Server

SSH 远程命令执行原理

输入命令显示执行结果



SSH Client

1. 发送命令

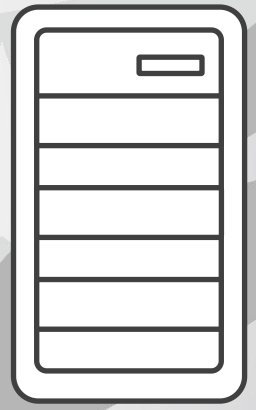
2. 服务器端执行并返回执行结果

3. 客户端显示与可交互操作同步

4. 执行完退出

5. 发出退出消息后断开连接

执行输入命令并返回结果



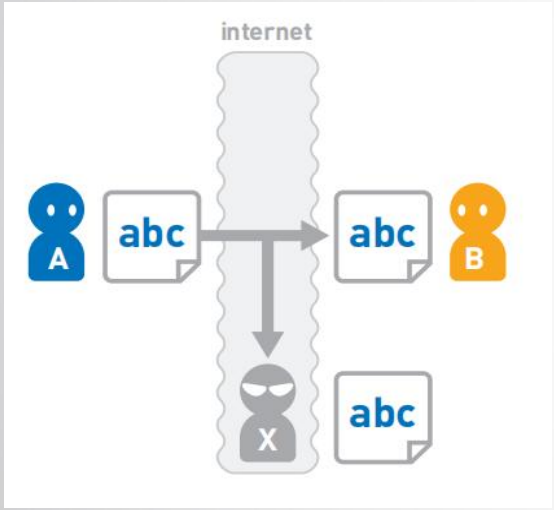
SSH Server

SSH加密原理 核心技术获得了2项图灵奖

- 接入认证
  - 即身份验证，指服务器对接入者进行身份验证，只有已授权用户才可以登陆。这个过程可以理解为我们在参加一些重要活动时的入场安检。
  - 身份验证有两种方式用户名密码登陆和非对称密钥（常用RSA，获2002年图灵奖）登陆。
- 通信加密
  - 通信过程使用对称算法（如AES）进行加密。
  - 在对称加密的密钥生成与交换算法使用 DH 算法（2015年图灵奖）。

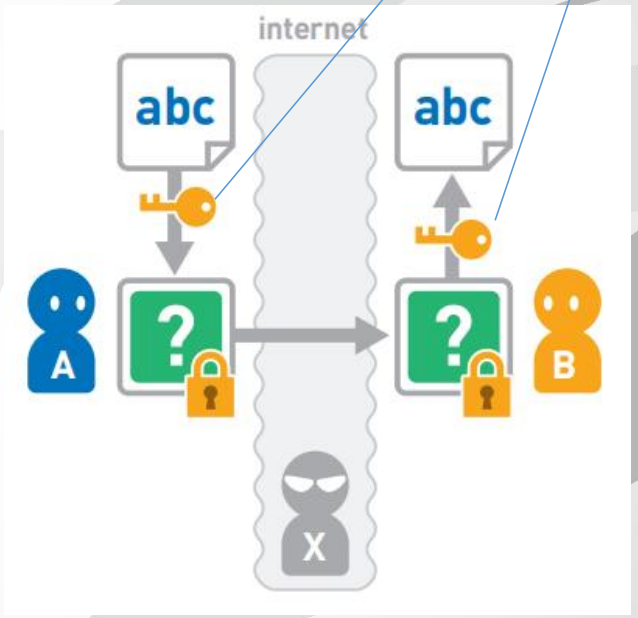
历届图灵奖获奖名单， https://baike.baidu.com/item/%E5%9B%BE%E7%81%B5%E5%A5%96

对称加密



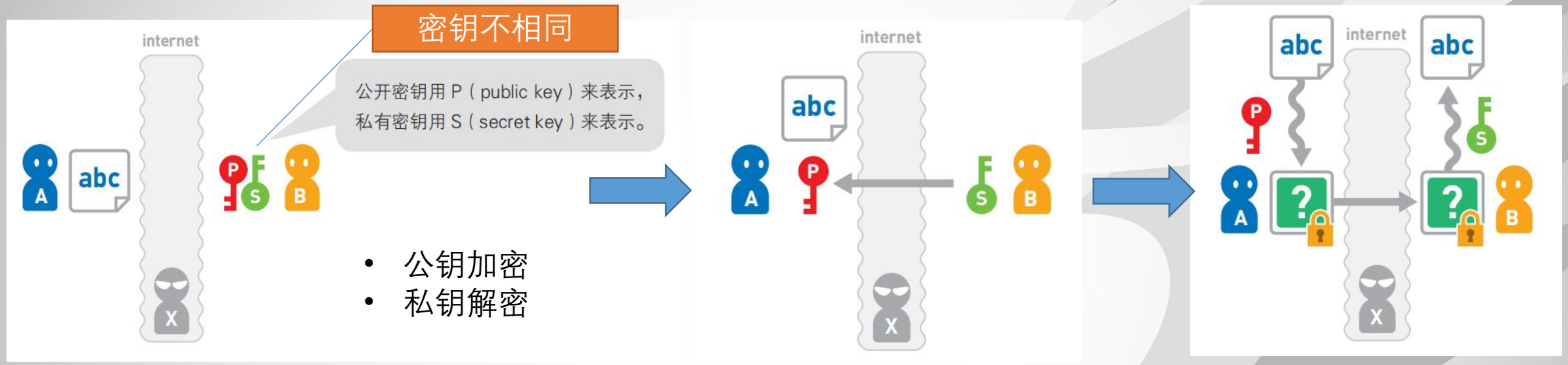
直接通信

加密



对称加密通信

非对称加密



简介

实现公开密钥加密的算法有很多，如RAS算法、椭圆曲线加密算法等，其中最为著名并被广泛使用的是RSA算法。RSA算法由其开发者Rivest、Shamir、Adleman的首字母命名而来，三人在2002年获得了图灵奖，其贡献程度可见一斑。

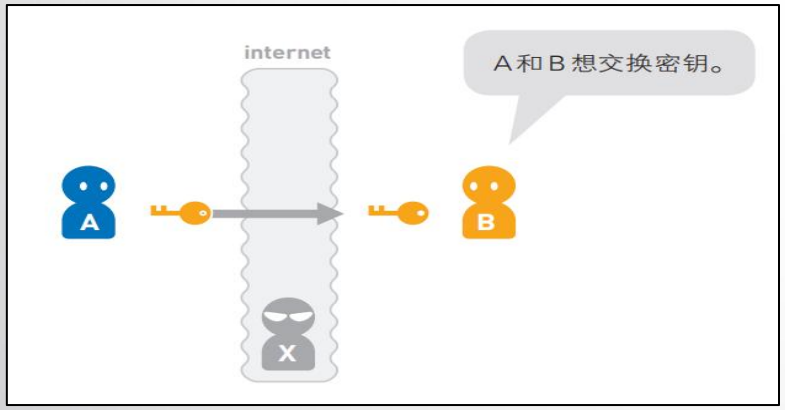
Diffie-Hellman 密钥交换算法

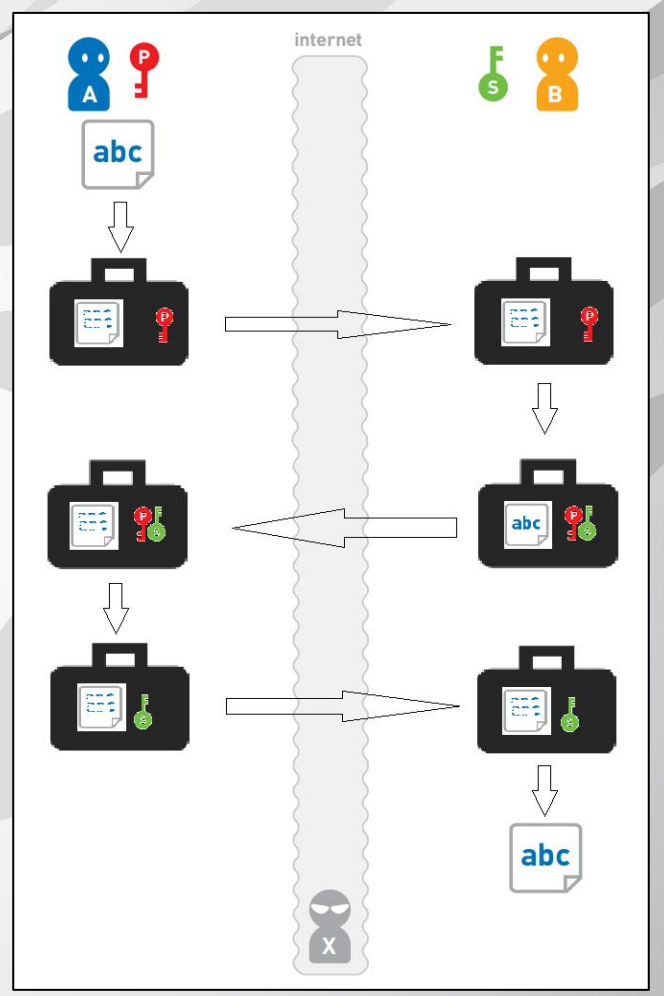
- **算法目的**

  利用大素数分解难题，在保证安全的前提下，交换生成密钥。
  如分解仅15位的大数 999896028823019 就很困难。
  而256bit的位长就有77位（2^256=1.16E+77）

- **基本原理**

  1. AB通过公共因子k，分别提出大素数 p 和 q;
  2. 只交换 p*q的乘积和k
  3. 通过欧拉公式推导出对方的q和p，从而完成密钥交换。





密钥交换示意图

注1：DH算法由 Whitfield Diffie 和Martin Hellman 提出，两人在 2015 年获得了图灵奖。
注2：详细原则参见 https://blog.csdn.net/weixin_43145361/article/details/105770539
注3：有专门收集素数的网站，如https://www.haomeili.net/ZhiShu/big?TotalCount=5046500&PageIndex=1

密码登陆

- 基本命令
  - ssh user@ip
  - 示例 ssh root@192.168.4.100
- 使用非默认端口
  - 默认端口为 22，登陆时可以省略
  - 修改后的端口 ssh root@192.168.4.100 -p 1022

密钥登陆

1. 使用 ssh-keygen 生成密钥对

   此命令会生成一对密钥，默认名称为 id_rsa.pub (公钥) 和 id_rsa (私钥)。

2. 使用 ssh-copy-id 上传公钥

```
(base) haowei@Haos-MacBook-Pro-2021-M1-Pro .ssh % ssh-copy-id -i id_rsa.pub sp
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
parallels@10.211.55.4's password:

Number of key(s) added:        1

Now try logging into the machine, with:   "ssh 'sp'"
and check to make sure that only the key(s) you wanted were added.
```

目 录

CONTENTS

01 1 简介

SSH基本信息介绍

02 2 工作原理

SSH连接通信和加密等工作原理

03 **3 配置文件**

~/.ssh 目录中的文件作用

04 4 常用操作

SSH常用操作方法与技巧

~/.ssh 目录

在 ~/.ssh 目录下会有以下文件

- config 用户配置文件
- known_hosts 已经连接过的主机
- authorized_keys 已经授权的密钥
- id_rsa 默认的私钥

config 文件

```
Host hfmaster
  HostName  192.168.4.100
  User root
  ServerAliveInterval 60
  ServerAliveCountMax 10
  IdentityFile ~/.ssh/ida_ras
  Port 10714

Host ali_s1
  HostName 121.199.10.158
```

known_hosts 文件

用于记录已经登陆过的主机列表

记录格式为:

目标机器IP + 目标公钥类型和内容

以下为一个示例文件

```
PS C:\Users\Administrator> cat .\.ssh\known_hosts
192.168.4.100 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFxJfxR2giSYyAIZSctXHFuaKepA3nc+aVfal93aJKBr56ZL24XJdvo6pEKS/ioF2OK0tcay7leqDg8JIgcThgI=
192.168.4.101 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGYJFDx0SIMVpYrwG3Exk8EWfrVFXBj3eKV69RX9ahPDO76DxHBN9hTY0tLGyjEBKFTuPQbIm/o0PZD1lw3fVNM=
192.168.4.102 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAeclRn8oZdDBexZU6vldvqWOijf0mkZX4ebh2XPgWBJUWnmSaTqMiByVGQAfV6kUbstGanjM3n8nWkoqyGpPF4=
192.168.4.103 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLBcfkRJkLTtzOOBsU/Sc1+jQWOEBTM+S+6CRHto+xGycBMtSkmqwXpFMupr1lhsayidH2HeRiRUilHL5Zyw0Sg=
192.168.4.104 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFyNpPmKp3vFyCV0SbOmcT4oyHqrP1OMF26GRhh9jXiIVy023gR4BpQWXX2DX+jylCRMf2V3Xd2UyE5WfOBfrbQ=
121.199.10.158 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBE903Eqy01RRaMH5933piD8TPSvI6TfTRQRBBxsbq6AYwTJ2b8YiBE+yW5yax62GVHQZXyUJ3sm5XFdGyeADyuc=
121.199.10.158 ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPSHLFZR6peWfcgCpeMii/zvCerVqRWEZdekap5pjJD7
192.168.2.21 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMke1PX4H5cbPKSfpyOw4CIBEgSUiYuD4Dr4lUWEjHnFNGulKiRrnLMvSgiAKyR3AvRY6jPXX5gPg3s6XVAlrBo=
192.168.2.30 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMke1PX4H5cbPKSfpyOw4CIBEgSUiYuD4Dr4lUWEjHnFNGulKiRrnLMvSgiAKyR3AvRY6jPXX5gPg3s6XVAlrBo=
PS C:\Users\Administrator>
```

authorized_keys 文件

用于记录已经授权的客户端列表

记录格式为:

客户端公钥 + 帐号名@机器名

以下为一个示例文件

```
root@server00:~# cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCsypaf6S5i5xw9RPV88/K27+hP7LPMd2qP5OGjSOLo/ThMKH7SCTVNP0QOfIT/xw7pNWJO/bqfUIrlbzF2UqeihQ00BscVb1sBQItOMbiK/TpqMqQ4KgBKFkgP9IL
fPVdDVjcYNWk+sWyRf9Z9LdrtG3zzPbNA+Vi+cRpubCeekiu2+bgorQ9pUqzTEgIOqUlmCSxiMpM3W0ND1Z7i9BpbE3baEv7BoOsw5FIxoseUGI+wBkwQXJZSr263Se/ZhMnjH9QdlR4J0bdub6jJKS82loq9V2Y+bO
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC9koQeIbf+bJEIlE9VdqSl3W/TbdjF8/2UMZjBYBK4wSUieqAVXXT1S999OHEtyHplmPLy3cvixl3q3RjEuTLwGaFJdDqAmC5dCWop3b5fhmEikSXALt2kKNXXjrM
3HjX035dBK8uNko5EzjqecoXN/wv41aF7nX8Y16K3Xaipr2hljqBGomAC6THaB2Bcz0Vi2ZVEdePboPuPrdMdjSqdxmjqIZcO0DZWv3xb07vxiBVFR8LULErQA6Inpff1L7NIyTwNrLHvsQL/WUTBbMhyJzrAtqz/j1
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCyX4PdQSXREi1ImGaalFVKzQoexdB1LVs2eJvp2j7kykUINv/gxgOO+tZtBP8fSKqiQSm0jUEnGTWqlR9KnZp4Xe6Jt2yN+AazCmfYDyjkjIcNe/cvfBC4ExL5D6d
ntsLkMHOljrPqVnvtcpuzxWI3/miIv4/FUGMyTKn1meRm4OyLiwyKUy0Q7RBiybsazpX7H0nccDRmb1HSB/3jm1O8te4D0/lfIPcUWbg0MHuRl1CHsxhqAjyACxlPiTOCnwFo4ol7tY0F9krm5ZAzLGXJp6+Ofcb/Ww
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDg7zHmKFgLHTRBPp+z4l2RJiOcYwRG3y5eucdbyTPu91DltRqMEelGESZn/fkrHCAQ7Xv7iDgW+VN57en+gyU2NaQ8upRVatUwEY8au6r/susgGJz9BYB9Ouoh9Lx
oxFOduoX3Iz4Xfvmd3K9cZcpw3W4EpyNmBOPYEiCkQoClTW2taaF+i8IWbvtf+yp6Z8tNgUfvMKD8PPSJqXZoISpeTC/ubhbnNVrzffpXAJBQEqhPod6Vjnn2DrYsyx4eI9kFM3qtMdvS5uQOlnTzHm3NF2lH/JBSMB
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDDXn8FDVzB8Q4aaneBVOep2bLNI1PozI4MgM4af62+oYlPYOETabI+cHSFqS6sFTIS2ay5mvAPPxr8A8deZvnCUmCNgOmYrIis1QeBMf7aQuuBu2YkGXa4Y8OnHuN
BUSOwYWSjZu6Hm7f8FOY0Vk3nozjDdTd+mIvC6OLov34Qoim5k845i3E7REpgUXoExaGlw0kETY5ukNlGX4C/xzHA6rDWeO00VbPMw8n9FjfqWPeOdbCHTSYDzQ1X91a6himy9iWIp5Vk6gEsJO2YkF7aTTbvhUb0rT
```

目 录

CONTENTS

01 1 简介

SSH基本信息介绍

02 2 工作原理

包括连接、通信和加密等工作原理。

03 3 配置文件

~/.ssh 目录中的文件作用

04 **4 常用操作**

SSH常用操作方法与技巧

指定端口登陆

- SSH默认端口为 22，在登陆时可以省略，也可以使用-p指定，如以下两条命令等价：
  - ssh root@192.168.4.100
  - ssh root@192.168.4.100 -p 22
- 修改登陆端口

  为了提高系统安全，在公网的主机往往会修改登陆端口号，减少来自默认端口的攻击。

  1. 登陆目标服务器
  2. 编辑 **/etc/ssh/sshd_confi**g 添加 Port=端口号，如将登陆端口修改为45： **Port=45**
  3. 重启ssh：**systemctl restart sshd** # 或使用命令 service sshd restart
  4. 查看ssh端口是否更改成功 **netstat -ntlp**

移除首次登陆提醒

- 第1次登陆会出现以下提示信息
  如果目标是首次登陆，则系统会给出提示并询问是否要连接。

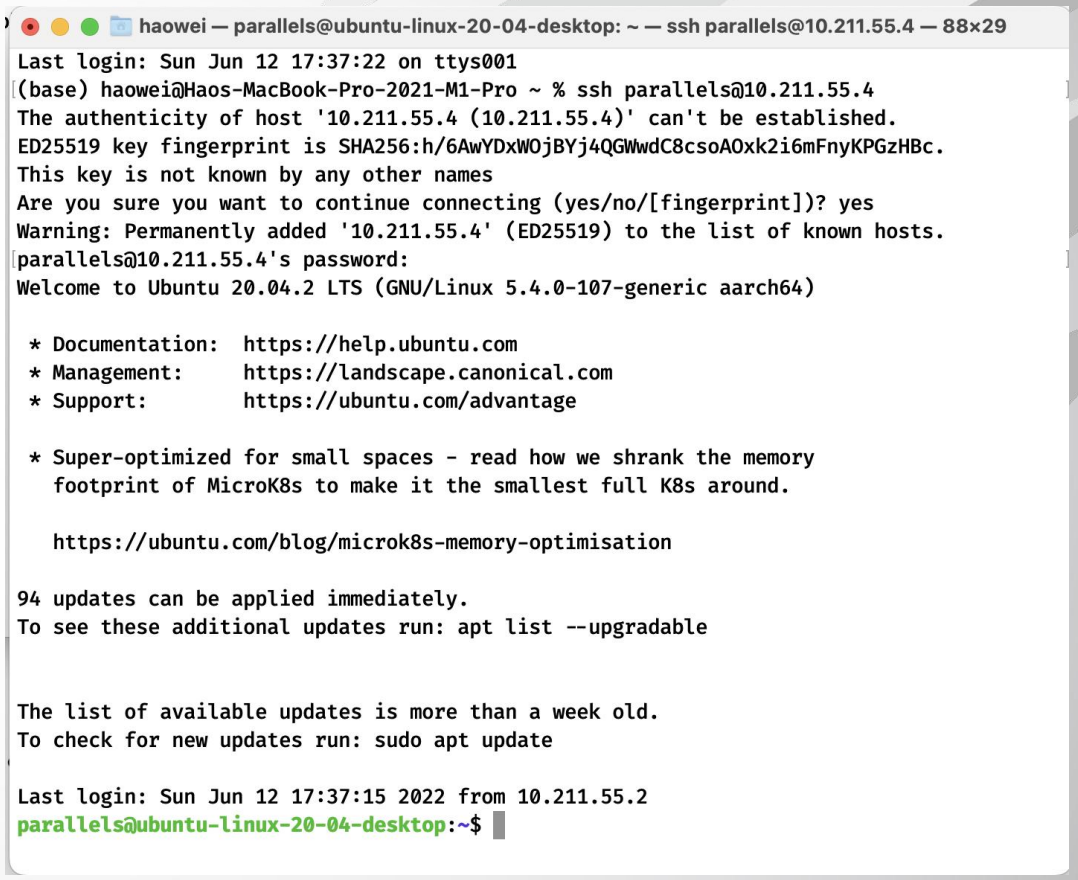
```
(base) haowei@Haos-MacBook-Pro-2021-M1-Pro ~ % ssh parallels@10.211.55.4
The authenticity of host '10.211.55.4 (10.211.55.4)' can't be established.
ED25519 key fingerprint is SHA256:h/6AwYDxWOjBYj4QGWwdC8csoAOxk2i6mFnyKPGzHBc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.211.55.4' (ED25519) to the list of known hosts.
parallels@10.211.55.4's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-107-generic aarch64)
```

- 通过命令关闭提示
  在自动化脚本中，为了避免输入，可用 **-o StrictHostKeyChecking=no** 关闭系统访问，如下所示：

```
(base) haowei@Haos-MacBook-Pro-2021-M1-Pro ~ % ssh parallels@10.211.55.4 -o
StrictHostKeyChecking=no
Warning: Permanently added '10.211.55.4' (ED25519) to the list of known hosts.
parallels@10.211.55.4's password:
```

- 删除已经登陆记录
  已登陆的主机会记录在 ~/.ssh/known_hosts 中，消息格式如下所示：

```
10.211.55.4 ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGnrhtbSXOPBgbhmiDF7h4Ua4iHDAy2vyzTam9+Et6w6ZscHok/5r04DUf5Xb65Go5qX3m/yllsZE1FfZ3Yt/sQ=
```



避免长时间登陆掉线

若一个SSH连接长时间没有收到操作，就会主动断开连接并提示“Write failed: Broken pipe”。 解决此问题的方法很多，现提供以下三种处理方法：

临时方法：在登陆命令中添加参数 `-o ServerAliveInterval=60`

```
$ ssh -o ServerAliveInterval=60 user@sshserver
```

- 在config中进行配置

```
Host hfmaster
HostName  192.168.4.100
User root
ServerAliveInterval 60
ServerAliveCountMax 10
IdentityFile ~/.ssh/ida_ras
Port 10714
```

- 在服务器端配置
  在服务器的 `/etc/ssh/sshd_config` 中添加如下内容：

```
ClientAliveInterval 60
ClientAliveCountMax 10
```

谢谢！