

SSH

SSH(Secure Shell) 是一个安全的网络协议，用于在计算机之间进行安全通信。它通过加密通道传输数据，防止窃听和篡改。SSH 通常用于远程登录和管理服务器。SSH 协议支持多种加密算法和认证方式，确保通信的安全性和完整性。SSH 还可以用于文件传输（SFTP）和端口转发等功能。SSH 是 Linux 和 Unix 系统上的标准工具，广泛应用于网络管理和系统维护。

- ssh 命令
- root 用户登录



ssh 默认端口是 **22**。ftp 21, http/https 80/443 是 IANA (Internet Assigned Numbers Authority) 定义的 TCP 和 UDP 端口 (Well-known port)。在 Linux 中，默认情况下，ssh 服务监听 22 端口。如果 22 端口被占用，可以配置 ssh 服务监听其他端口。例如，将 ssh 服务配置为监听 10022 端口。

SSH 配置

```
# vi /etc/ssh/sshd_config
```

SSH 端口

sshd_config 文件中的 **Port** 配置项指定了 ssh 服务监听的端口。默认情况下，该配置项设置为 22。如果希望更改端口，可以将该配置项的值修改为所需的端口号，例如 10022。

```
Port 10022
```

SSH 重启

Debian

```
# systemctl restart ssh
```

RHEL

```
# systemctl restart sshd
```

root   

!!! root      ,           

SSH 

```
# vi /etc/ssh/sshd_config
```

PermitRootLogin ☐ ☒

sshd_config `PermitRootLogin` `no` .

`PermitRootLogin` , `PermitRootLogin` `no` .

PermitRootLogin no

SSH Debian

```
# systemctl restart ssh
```

RHEL

```
# systemctl restart sshd
```