

SSH (Secure Shell) 用于服务器登录和各种加密通信。能对操作者进行认证 (authentication) 和授权 (authorization)。明文的网络协议可以套用在它里面，从而实现加密。默认端口 22

SSH 作为加密通信的中介，充当两台服务器之间的通信加密跳板，使得原本不加密的通信变成加密通信。这个功能称为端口转发 (port forwarding) 又称 SSH 隧道 (tunnel)

功能

远程登录：通过 SSH 可以安全地登录到远程服务器，并在该服务器上执行命令。

文件传输：使用基于 SSH 的工具（如 SCP 和 SFTP）可以在本地和远程系统之间安全地传输文件。

端口转发：允许将不安全的 TCP 连接转换为安全的 SSH 连接，保护数据传输的安全性。

原理

加密：SSH 使用对称加密、非对称加密和哈希函数来确保通信的安全性。

对称加密：用于加密大部分数据流，双方使用相同的密钥进行加密和解密。

非对称加密：用于生成会话密钥，验证服务器的身份，并在客户端和服务端之间建立安全连接。

哈希函数：用于验证数据完整性，确保数据未被篡改。

认证方式：

密码认证：最常见的方式，用户输入用户名和密码进行登录。

公钥认证：更安全的方式，用户生成一对公钥和私钥。将公钥添加到服务器上的 `~/.ssh/authorized_keys` 文件中，然后使用私钥进行身份验证。

双因素认证 (2FA) 结合密码和一次性验证码（通常通过手机应用生成）来增加安全性。

组件

`ssh` 用于登录远程服务器。

`scp` 用于在本地和远程系统之间安全复制文件。

`sftp` 类似于 FTP 但使用 SSH 协议进行文件传输。

`ssh-keygen` 用于生成、管理和转换认证密钥。

`ssh-agent` 和 `ssh-add` 用于管理私钥，简化公钥认证过程。

部署

```
#安装
sudo apt-get -y install openssh-server
#启动
sudo systemctl start ssh
#查看SSH状态
sudo systemctl status ssh

#防火墙设置
sudo ufw allow ssh
```

#修改服务端口

```
sudo ufw allow 22/tcp
```

#修改SSH配置

```
sudo systemctl restart ssh
```

#查看日志

```
cat /var/log/auth.log | grep ssh
```

```
tail -f /var/log/auth.log | grep ssh
```

```
sudo grep "Failed password" /var/log/auth.log
```

从远程服务器下载文件到本地

```
scp <用户名>@<ssh服务器地址>:<文件> <本地文件路径>
```

```
scp root@127.20.36.88:~/test.txt ~/Desktop
```

从远程服务器下载文件夹到本地

```
scp -r <用户名>@<ssh服务器地址>:<文件夹名> <本地路径>
```

```
scp -r root@127.20.36.88:~/test ~/Desktop
```

从本地上传文件到服务器上

```
scp <本地文件名> <用户名>@<ssh服务器地址>:<上传保存路径>
```

从本地上传文件夹到服务器上

```
scp -r <本地文件夹名> <用户名>@<ssh服务器地址>:<上传保存路径>
```

From:

<https://www.sujj.wiki/> - 落月思君归

Permanent link:

<https://www.sujj.wiki/doku.php?id=%E8%BD%AF%E4%BB%B6:ssh&rev=1758396141>Last update: **2025/09/21 03:22**