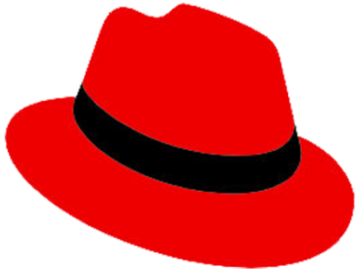
Red Hat

RH124 红帽系统管理 I

RH124-09-配置和保护OpenSSH服务



Red Hat

一、使用SSH访问远程命令行

SSH

- SSH 是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。
- SSH属于C/S架构，协议默认端口为22。
- SSH支持两种验证方式：

  1、密码验证（登录时需要输入用户名密码）

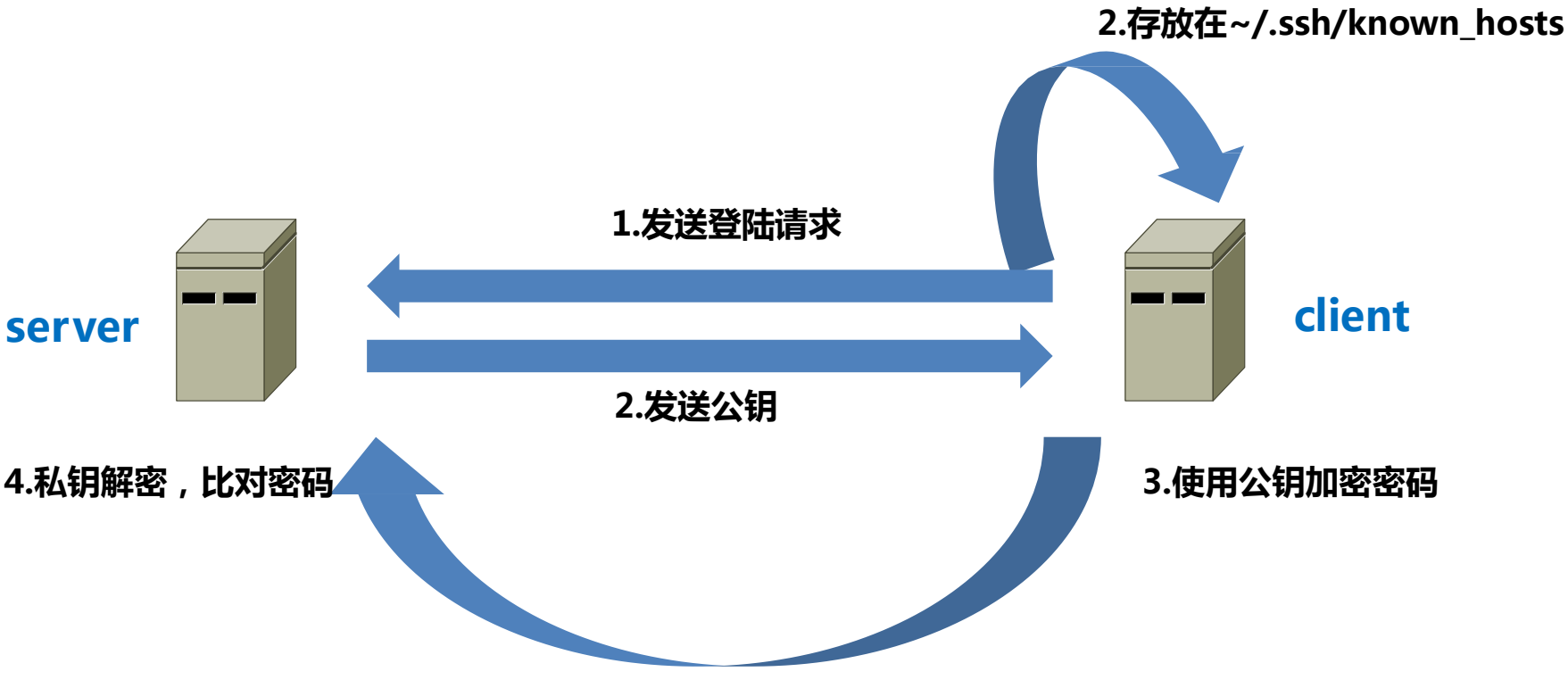
  2、秘钥验证（可以实现SSH的免密码登录）
- SSH进行远程登录的前提：

  1、网络可达

  2、ssh服务有开启

  3、密码验证需要对方的用户名和密码
- OpenSSH用于在远程系统上安全运行shell。

SSH密码验证


2.存放在~/.ssh/known_hosts
1.发送登陆请求
server
client
2.发送公钥
4.私钥解密，比对密码
3.使用公钥加密密码

基于SSH密码验证远程登录

- 以当前用户身份创建远程交互式shell：

  ssh remotehost

- 以其他用户身份登录到远程：

  ssh remoteuser@remotehost

- 检验命令：**w -f**

密钥位置

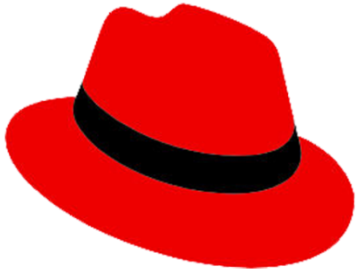
Server

私钥：/etc/ssh/**ssh_host_rsa_key**

公钥 ：/etc/ssh/**ssh_host_rsa_key.pub**

Client

~/.ssh/**known_hosts**（server给的公钥）



Red Hat

二、配置基于SSH密钥的身份认证

基于SSH密钥的身份验证

用户可以通过使用公钥身份验证进行ssh登陆身份验证。ssh允许用户使用**私钥-公钥**方案进行身份验证。这意味着将生成私钥和公钥两个密钥。

私钥文件用作身份验证凭据，像密码一样，必须妥善保管。

公钥复制到**用户希望登陆的系统**，用于验证私钥。公钥不需保密。拥有公钥的SSH服务器可以发布仅持有您私钥的系统才可解答的问题。这样您不必在每次访问系统时键入密码，但安全性任然能得到保障。

配置基于SSH密钥身份验证

配置基于SSH密钥身份验证

步骤：

1、client上生成公、私密钥对

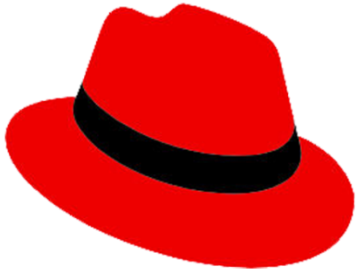
ssh-keygen

（生成私钥文件　~/.ssh/id_rsa）

（生成公钥文件　~/.ssh/id_rsa .pub）

2、把公钥拷贝到server上

ssh-copy-id -i ~/.ssh/id_rsa.pub 用户@server



Red Hat

三、自定义SSH服务配置

禁止root用户使用SSH登陆

配置文件：**/etc/ssh/sshd_config**

从安全角度而言，建议禁止root用户通过ssh直接登陆系统

1）修改配置文件

PermitRootLogin **no**

2）重启sshd服务

systemctl **restart** sshd

禁止使用SSH进行密码身份验证

仅允许基于密钥登陆远程命令行优点：

SSH密钥比一般的密码长，安全性更高

在首次设置后，启动远程shell访问更加便捷

1）编辑配置文件:/etc/ssh/sshd_config

PasswordAuthentication **no**

默认为打开密码身份验证的，将其改成no

2）重启服务

systemctl restart sshd


WISDOM NET