第 3 章

远 程 登 录

Chapter 3

远程登录是管理远程主机的基础。远程登录方式分为文本界面和图形界面两种。文本界面包括 Telnet 和 SSH 两种远程访问方式，Telnet 访问由于采用明文传输数据，因此并不安全，已被逐渐淘汰；而 SSH 访问则采用加密方式传输数据，因此更加安全，并已被广泛采用。

本章主要学习 Linux 的文本界面远程登录方式 Telnet 和 SSH 以及图形界面远程登录。

本章的学习目标如下。

(1) 文本界面远程登录：掌握 Telnet 和 SSH 服务端的安装、配置和启动，客户端的安装和连接；掌握远程传输命令 scp。

(2) 图形界面远程登录：掌握 VNC 服务端的安装、配置和启动，客户端的安装和连接。

3.1 文本界面远程登录

文本界面远程登录包括 Telnet 和 SSH。Telnet 为明文传输数据，并不安全，已被逐渐淘汰。SSH 为加密传输数据，更加安全，已被广泛使用。

3.1.1 Telnet

Telnet 协议是 TCP/IP 协议集中的一员，是远程登录服务的标准协议，它为用户提供了在本地主机上操作远程主机的方式。

表 3.1 为各节点的网络配置。

表 3.1 各节点的网络配置

节　　点	主 机 名	IP 地址和子网掩码
Telnet 服务器	centos-s	192.168.0.251/24
Telnet 客户机	centos-c	192.168.0.1/24

步骤 1：在服务器端安装 Telnet。

```
[root@centos-s ~]# yum -y install telnet-server
```

步骤 2：在服务器端启动 Telnet 服务。

```
[root@centos-s ~]# systemctl start telnet.socket
```

步骤 3：设置服务器防火墙以放行 Telnet 服务。

```
[root@centos-s ~]# firewall-cmd --permanent --add-service=telnet
[root@centos-s ~]# firewall-cmd --reload
```

步骤 4：安装 Telnet 客户端。

```
[root@centos-c ~]# yum -y install telnet
```

步骤 5：在客户机上利用 Telnet 登录服务器。

```
[root@centos-c ~]# telnet 192.168.0.251
Trying 192.168.0.251...
Connected to 192.168.0.251.
Escape character is '^]'.

Kernel 3.10.0-1127.el7.x86_64 on an x86_64
centos-s login: test
// 输入用户名
Password:
// 输入密码
Last login: Mon Mar  8 07:44:21 on :0
[test@centos-s ~]$
```

注意：对于 Telnet 远程访问方式来说默认不允许用户 root 远程登录。

```
[root@centos-c ~]# telnet 192.168.0.251
Trying 192.168.0.251...
Connected to 192.168.0.251.
Escape character is '^]'.

Kernel 3.10.0-1062.el7.x86_64 on an x86_64
centos-s login: root
Password:
Login incorrect
```

如果需要用户 root 远程登录，在服务器端将以下内容添加到文件/etc/securetty 并重新启动服务 Telnet。

```
[root@centos-s ~]# vi /etc/securetty
pts/0
pts/1
pts/2
pts/3
[root@centos-s ~]# systemctl restart telnet.socket
```

3.1.2 SSH

SSH(Secure Shell)是一种能够以安全的方式提供远程登录的协议，也是目前远程管理

Linux 的首选方式。

SSH 提供两种安全验证的方法。

(1) 基于密码的验证。用账户和密码来验证登录。

(2) 基于密钥的验证。需要在本地生成密钥对,然后把密钥对中的公钥上传至服务器;而在登录时需与服务器中的公钥进行比较。

基于密钥的验证由于不需要每次访问时验证密码,所以更安全。

Linux 的典型 SSH 服务端软件有 sshd,其配置文件位于/etc/ssh/sshd_config 中,常用字段和含义见表 3.2。

表 3.2 sshd 服务配置文件中常用字段和含义

字 段	含 义
Port 22	sshd 服务监听的端口
ListenAddress 0.0.0.0	sshd 服务监听的 IP 地址
Protocol1/2	SSH 协议版本号
HostKey /etc/ssh/ssh_host_key	SSH 协议版本为 1 时,DES 私钥存放的位置
HostKey /etc/ssh/ssh_host_rsa_key	SSH 协议版本为 2 时,RSA 私钥存放的位置
HostKey /etc/ssh/ssh_host_dsa_key	SSH 协议版本为 2 时,DSA 私钥存放的位置
PermitRootLogin yes/no	是否允许用户 root 登录
StrictModes yes/no	当远程用户的私钥改变时是否直接拒绝连接
MaxAuthTries 6	最大密码尝试次数
MaxSessions 10	最大会话数
PasswordAuthentication yes/no	是否允许基于密码的验证
PermitEmptyPasswords no/yes	是否允许空密码登录

表 3.3 所示为各节点的网络配置。

表 3.3 各节点的网络配置

节 点	主 机 名	IP 地址和子网掩码
SSH 服务器	centos-s	192.168.0.251/24
SSH 客户机	centos-c	192.168.0.1/24

1. 基于密码的验证进行 SSH 登录

步骤 1:在服务器上安装 SSH 服务端。

Linux 已经默认安装并启动 SSH 服务端程序 sshd。

步骤 2:在客户机上利用 SSH 登录服务器。

Linux 已经默认安装 SSH 客户端程序 ssh。命令 ssh 的语法格式如下:

```
ssh [选项] 远程主机地址
```

以普通用户 test 进行 SSH 登录。

```
[root@centos-c ~]# ssh test@192.168.0.251
The authenticity of host '192.168.0.251 ( 192.168.0.251) ' can't be established.
ECDSA key fingerprint is SHA256:JjFeFasmZ0pCSIsp4bXpC/UU0qnxZN5itQUh1JGFO2w.
ECDSA key fingerprint is MD5:c3:a7:97:85:a0:7a:62:0e:16:e1:3d:bf:2c:2e:34:b5.
```

```
Are you sure you want to continue connecting ( yes/no ) ? yes
Warning: Permanently added '192.168.0.251' ( ECDSA ) to the list of known hosts.
test@192.168.0.251's password:
// 输入普通用户 test 的密码
Last login: Mon Mar  8 07:44:21 2021
[test@centos-s ~]$
```

以用户 root 进行 SSH 登录。

```
[root@centos-c ~]# ssh root@192.168.0.251
root@192.168.0.251's password:
// 输入用户 root 的密码
Last login: Sun Mar 14 19:22:35 2021
[root@centos-s ~]#
```

如果禁止用户 root 进行 SSH 登录就可以减少被暴力破解用户 root 密码的可能性。可在服务端的配置文件第 38 行处,去掉 # 号,并把 yes 改为 no。

```
[root@centos-s ~]# vi /etc/ssh/sshd_config
PermitRootLogin no
```

重新启动服务 sshd 使配置文件生效。

```
[root@centos-s ~]# systemctl restart sshd
```

当用户 root 进行 SSH 登录时被拒绝。

```
[root@centos-c ~]# ssh root@192.168.0.251
root@192.168.0.251's password:
Permission denied, please try again.
// 无论输入的密码是否正确,均提示“权限被拒绝”。
```

2. 基于密钥验证的 SSH 登录

步骤 1:在客户机端生成密钥并查看密钥。

```
[root@centos-c ~]# ssh-keygen
// 生成 SSH 密钥
Generating public/private rsa key pair.
Enter file in which to save the key ( /root/.ssh/id_rsa ) :
// 输入密钥的存储路径
Enter passphrase ( empty for no passphrase ) :
// 输入密钥的密码,按 Enter 键则为空密码
Enter same passphrase again:
// 再次输入密钥的密码
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
```

```
The key fingerprint is:
SHA256:bPDGuLw+u2kX+Ag3NFoZg5HBh/Cd/5DHrKAZwqTNziM root@centos-c
The key's randomart image is:
+---[RSA 2048]----+
|  .oo *          |
|   .=.+.         |
|  . ..++         |
| *    =B +       |
|. = .+ooS +      |
| o .o=+=.=       |
|E + ooo+...      |
| . .  +oo        |
|    o *=         |
+----[SHA256]-----+
[root@centos-c ~]# cat /root/.ssh/id_rsa
// 查看 SSH 私钥
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAt3RZydsVAYji1Nb6I5YMIQw9FT9EIhKsXrKxR2azpVhxieny
3ec1bgYbDFjzAA0Ex3vCYDLtryqrXclm5bzI8I6mmelK2bw/iT+LqmAFtWTOG82B
xCvvZeQ+NS3MkczYhhmo5Gql5mQClxek8lMm9RRjrmVwddmBzy7FNcTIl1s7nHNi
v3yVibgFK/e/KLgdIw5wnAIjp7/FaT+dJ11iIymAG5awTWEPgc8sT3m9MHyCRKoV
aInSEMKvAT+TZFnNbiojId8dylBEMYlkYxkSrVL0298YDLwqoW6/joEByshgOnsx
S3bnU0qrY7JZBt6YAYWfejgQhh24Wy+45yMctQIDAQABAoIBACUtRfjbFeGuvNEH
E7/ca27TDRneLU9+W0IBkl122Zb7Wl7pcxc3AKPgRuD0saHkAYDveo+GIpap3fpu
kxShclMVhXuRRGLlfDazEvme5elBmWcW+WIoySXr4BNkyZ0OVx6t2oUXe7E5uTCn
UPzujumBjUXNNsIbJuw2fS6NR10sfu/Oz38OiJryndkgyIVJmd/KI+6Fa38g9wvB
OBMrPJh1LKhs4hfvTpwCFyoy+th2OXvdVJ3+xpunhD/nvwf7mk0VSgbDr3hHjlu0
t8Bln5Z5UhBFbBMZRKttNtaIKuoYag4KggKy5S/YqB2/W8c6aIpWuR/dYJXE7JPS
EnCLqQECgYEA5CChTAS0tEx9Ko0xgV5pa2sn8Zrhnd1RqjTuxMHcA/iFeY5K38K3
IocQ8R8/9J6x1iQ+a5IaYzGwv9Xo6CV8HKjMK1BoFZ5aQpnrc/h+zlHhhGFmwr/N
5Z5I143k3w1amBaaFKr/aaz4OJH1gmotL2W9NVW/oX0+D/Mi3Dc37HUCgYEAzd5w
li7M5eUFLNrm+mukbeE6I3iIb/XKm1XF8r0lT9TUdo0cu8QY9ldjPyxAjGHj7K3Z
gZCD0KryPzaEvS1Z+Xcscl8vZikWoKtQsVghGbyh/ADjnWaUfO/WCsfS3rYKOFqw
Pz3ucW8Uv3OWEJnp6PhR+d6k86rqD1zWrFT5Z0ECgYEAt4Cb3pdGeGWypUDQGp1E
NVkL12fbpm253C0aB4FdJoCJdV8FUXrCb26wLRUTEAV7TaL35vWubi4xXA6Ie/xz
GmaZXRofr4wiVMKVSEMSVYo92ouy6mL5D4REWcfU26tVPVOo+4kVTP8K6A5Yq2AX
GrI/AaEJNbCV9KSCXRu5y2UCgYEAn7x/+VfY7myUZmh3nkkVbZi7xrgIjW7WxU55
aE5w/A90x4PYjqyqfcHypRrN/t8ZvhRq10htruRlUL0Zo7vju1hH6XqHyaoJ/6LN
2r05+cFOor2B3yiwAH0LxJOlv97Z8T4U0Q1ZzTRWkfK6tqjmQTkkSlACB3tPX5o2
i8LnPcECgYEArNZkBXw5KqFzCJ58STjaiqsvl+dAkx6BRJxgywbcq+GpYO7MyKng
+nZNAlv6VT3DOgyCu0b1P5LP/DOpDbXY8uly64CZh4wDNBjO6ZsygRA7e9im1drE
CC+Ej0RZ7o36WXmFZqLozqCB7ZwLDNkoapPavslsJfGTstFNAhYx2ZY=
-----END RSA PRIVATE KEY-----
[root@centos-c ~]# cat /root/.ssh/id_rsa.pub
// 查看 SSH 公钥
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC3dFnJ2xUBiOLU1vojlgwhDD0VP0QiEqxesrFHZr
OlWHGJ6fLd5zVuBhsMWPMADQTHe8JgMu2vKqtdyWblvMjwjqaZ6UrZvD+JP4uqYAW1ZM4bzYHEK+
9l5D41LcyRzNiGGajkaqXmZAKXF6TyUyb1FGOuZXB12YHPLsU1xMiXWzucc2K/fJWJuAUr978ouB0
jDnCcAiOnv8VpP50nXWIjKYAblrBNYQ+BzyxPeb0wfIJEqhVoidIQwq8BP5NkWc1uKiMh3x3KUEQx
iWRjGRKtUvTb3xgMvCqhbr+OgQHKyGA6ezFLdudTSqtjslkG3pgBhZ96OBCGHbhbL7jnIxy1 root@
centos-c
```

步骤 2：在客户机端上载公钥到服务器。

```
[root@centos-c ~]# ssh-copy-id test@192.168.0.251
/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
test@192.168.0.251's password:
// 输入服务器的用户密码

Number of key( s ) added: 1

Now try logging into the machine, with:   "ssh 'test@192.168.0.251'"
and check to make sure that only the key( s ) you wanted were added.
```

步骤 3：在客户机上以 SSH 方式登录服务器。

```
[root@centos-c ~]# ssh test@192.168.0.251
Last login: Sun Mar 14 19:28:03 2021 from 192.168.0.1
[test@centos-s ~]$
```

如果要禁止基于密码，即只能基于密钥的验证进行 SSH 登录，需要在服务端的配置文件第 65 行处，将 yes 改为 no。

```
[root@centos-s ~]# vi /etc/ssh/sshd_config
PasswordAuthentication no
```

重新启动服务 sshd 使配置文件生效。

```
[root@centos-s ~]# systemctl restart sshd
```

客户端基于密码的验证进行 SSH 登录被拒绝。

```
[root@centos-c ~]# ssh root@192.168.0.251
Permission denied( publickey,gssapi-keyex,gssapi-with-mic ) .
```

3. 远程传输命令

远程传输命令 scp(Secure Copy)是一个基于 SSH 协议在网络上进行安全传输文件的命令。命令 scp 有上载文件和下载文件两种语法格式。

(1) 上载文件。

```
scp [选项] 本地路径/文件 远程主机地址:远程路径/文件
```

(2) 下载文件。

```
scp [选项] 远程主机地址:远程路径/文件 本地路径/文件
```

scp 命令常用选项含义见表 3.4。

表 3.4 scp 命令常用选项含义

选项	含　义
-v	显示详细的连接进度
-p	指定远程主机的 sshd 端口号
-r	用于传送文件夹
-6	使用 IPv6 协议

【例 3.1】 在客户机上创建文件并上载到服务器。

```
[root@centos-c ~]# echo "This is a file created by the Client." > centos-c.txt
// 客户机创建文件
[root@centos-c ~]# scp /root/centos-c.txt 192.168.0.251:/root/centos-c.txt
// 客户机上载文件到服务器
root@192.168.0.251's password:
centos-c.txt                                  100%   38    32.7KB/s   00:00
```

【例 3.2】 在服务器端创建文件并在客户机端下载。

```
[root@centos-s ~]# echo "This is a file created by the Server." > centos-s.txt
// 在服务器端创建文件
[root@centos-c ~]# scp 192.168.0.251:/root/centos-s.txt /root/centos-s.txt
// 在客户机端下载服务器的文件
root@192.168.0.251's password:
centos-s.txt                                  100%   38    22.2KB/s   00:00
```

3.2 图形界面远程登录

以图形界面方式远程登录的软件包括 VNC 等。

表 3.5 所示为各节点的网络配置。

表 3.5 各节点的网络配置

节　点	主　机　名	IP 地址和子网掩码
VNC 服务器	centos-s	192.168.0.251/24
VNC 客户机 Linux	centos-c	192.168.0.1/24
VNC 客户机 Windows		192.168.0.2/24

1. 配置 VNC 服务器

步骤 1：在服务器上安装 VNC 服务端。

```
[root@centos-s ~]# yum -y install tigervnc-server
```

步骤 2：在服务器上创建 VNC 服务密码。

```
[root@centos-s ~]# vncpasswd
Password:
Verify:
Would you like to enter a view-only password(y/n)? n
```

```
// 选择是否输入仅浏览模式密码,即 VNC 连接后只能进行查看而不能进行其他操作。
A view-only password is not used
```

步骤 3：在服务器上启动 VNC 服务。

```
[root@centos-s ~]# vncserver

New 'centos-s:1 ( root ) ' desktop is centos-s:1

Creating default startup script /root/.vnc/xstartup
Creating default config /root/.vnc/config
Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/centos-s:1.log
```

步骤 4：设置服务器防火墙以放行 VNC 服务。

```
[root@centos-s ~]# firewall-cmd --permanent --add-service=vnc-server
[root@centos-s ~]# firewall-cmd --reload
```

2. 配置 VNC 客户机 Linux

步骤 1：在客户机 Linux 上安装 VNC 客户端。

```
[root@centos-c ~]# yum -y install tigervnc
```

步骤 2：在客户机 Linux 上运行 VNC 客户端。在桌面上方的工具栏左侧选择 Applications→Internet→TigerVNC Viewer 命令，如图 3.1 所示。

图 3.1 在客户机 Linux 上运行 VNC 客户端

步骤 3：输入 VNC 服务器的地址。

在 VNC server 文本框中输入 VNC 服务器的地址，并单击 Connect 按钮，如图 3.2 所示。

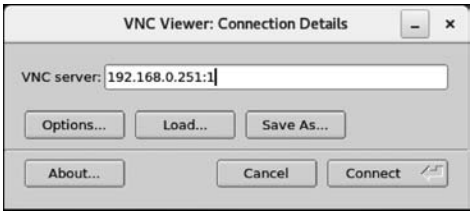

图 3.2　输入 VNC 服务器的地址

步骤 4：输入 VNC 服务器的密码。

在 Password 文本框中输入 VNC 服务器的密码，并单击 OK 按钮，如图 3.3 所示。

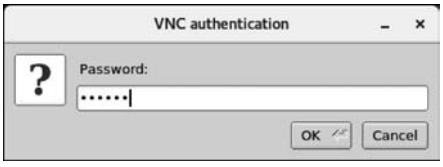

图 3.3　输入 VNC 服务器的密码

步骤 5：连接成功后，在 VNC 客户端系统窗口显示服务器的图形界面，如图 3.4 所示。

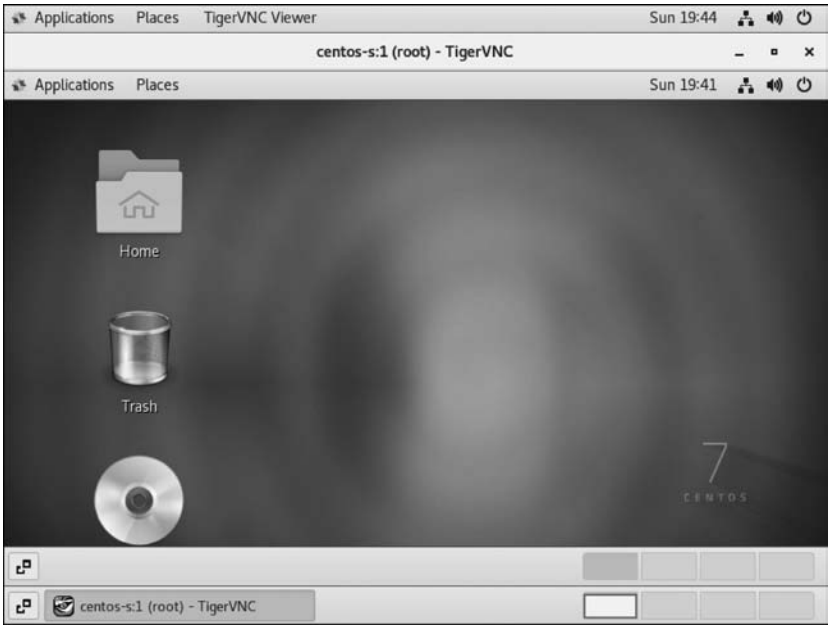

图 3.4　Linux 客户端连接成功

3. 配置 VNC 客户机 Windows

步骤 1：下载和运行 VNC Windows 客户端，在 Server 文本框中输入 VNC 服务器的地址，如图 3.5 所示。

图 3.5 输入 VNC 服务器的地址

步骤 2：输入 VNC 服务器的密码。在 Password 文本框中输入 VNC 服务器的密码，并单击 OK 按钮，如图 3.6 所示。

图 3.6 输入 VNC 服务器的密码

步骤 3：连接成功后，在 VNC 客户端系统窗口显示服务器的图形界面，如图 3.7 所示。

图 3.7 Windows 客户端连接成功