

## 项目 3 配置网络和使用 ssh 服务-实训任务指导书 (3-3)

### 任务 3-5 配置远程控制任务

在 centos7 系统中，已经默认安装并启用了 sshd 服务程序，**防火墙默认策略允许 SSH 服务，不需要配置**。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 系统的首选方式。想要使用 SSH 协议来远程管理 Linux 系统，则需要部署配置 sshd 服务程序。sshd 是基于 SSH 协议开发的一款远程管理服务程序，不仅使用起来方便快捷，而且能够提供了以下两种安全验证的方法。配置远程控制项目，实现如下子任务。

1. 实现基于口令的验证—用账户和密码来验证登录。
2. 在配置的 sshd 服务中，设置禁止以 root 管理员的身份远程登录到服务器。
- 3: 配置基于密钥验证方式，并进行远程登录验证
- 4: 使用远程传输命令 scp，并进行远程登录验证。

sshd 服务配置文件中包含的重要参数如表 2-1 所示。

参 数	作 用
Port 22	默认的 sshd 服务端口
ListenAddress 0.0.0.0	设定 sshd 服务器监听的 IP 地址
Protocol 2	SSH 协议的版本号
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	设定是否允许 root 管理员直接登录
StrictModes yes	当远程用户的私钥改变时直接拒绝连接
MaxAuthTries 6	最大密码尝试次数
MaxSessions 10	最大终端数
PasswordAuthentication yes	是否允许密码验证
PermitEmptyPasswords no	是否允许空密码登录 (很不安全)

子任务 1：配置基于口令的验证 sshd 服务，并使用账户和密码来进行远程登录验证。

准备工作：

1. 可恢复到快照 1
2. 需要两台虚拟机（只有一台的同学可利用当前的克隆一台虚拟机）

具体实训操作步骤：

1、分别设置两台虚拟机的主机名和 IP 地址，一台做服务器，一台做客户机，需特别注意两台虚拟机的网络配置方式一定要一致，此案例两台网络均设置为桥接模式。（桥接模式，相当于把物理主机设为交换机）

配置如下：

①角色为服务器的虚拟机，为方便使用主机名设为 server7-1，IP 地址配置为 192.168.10.1/24。网络模式设置为桥接模式（配置完可重启网络生效）



②角色为客户端的虚拟机，为方便使用主机名设为 client7-2，IP 地址配置为 192.168.10.20/24。网络模式设置为桥接模式（配置完可重启网络生效）



③分别使用 nmcli 命令修改服务器和客户端虚拟机的主机名为 server7-1 和 client7-2

●打开服务器虚拟机使用如下命令修改主机名

```
[ root@192 ~ ] # nmcli general hostname server7-1
[ root@192 ~ ] # hostname
server7-1
```

Exit 退出当前用户登录后，重新打开终端，主机名生效，如下图

```
[ root@server7-1 ~ ] # ifconfig
ens33: flags=4163<UP, BROADCAST, RUNNING, MULTICAST> mtu 1500
    inet 192.168.10.1 netmask 255.255.255.0 broadcast 192.168.10.255
    inet6 fe80::6c88:2ce8:cf5:9ba6 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:32:c1:32 txqueuelen 1000 (Ethernet)
    RX packets 203480 bytes 296534991 (282.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 65718 bytes 3989013 (3.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

●打开客户端虚拟机使用如下命令修改主机名

```
[ root@localhost ~ ] # nmcli general hostname client7-2
[ root@localhost ~ ] # hostname
client7-2
```

Exit 退出当前用户登录后，重新打开终端，主机名生效，如下图

```
root@client7-2 ~]# ifconfig
ens33: flags=4163<UP, BROADCAST, RUNNING, MULTICAST> mtu 1500
    inet 192.168.10.20 netmask 255.255.255.0 broadcast 192.168.10.255
    inet6 fe80::b9bc:46be:e31d:dd38 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:0f:dc:75 txqueuelen 1000 (Ethernet)
    RX packets 203300 bytes 281588823 (268.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 95759 bytes 5783378 (5.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

2. 本案例中防火墙默认策略允许 SSH 服务，不需要配置，但要会查看

```
[root@server7-1 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: dhcpv6-client http ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

3. 在客户端，使用账户和密码进行远程登录口令验证，命令格式为：

“ssh [参数] 主机 IP 地址”。要退出登录则执行 exit 命令，

①登录服务器的 root 用户，如下图：

```
[root@localhost ~]# ssh 192.168.10.1
The authenticity of host '192.168.10.1 (192.168.10.1)' can't be established.
ECDSA key fingerprint is SHA256:Pw0T6UHxllukiTlIxiVbiEQ8gpUDSzVbDxRKTJsPtW8.
ECDSA key fingerprint is MD5:65:62:86:7d:b4:17:45:f7:1b:6e:ab:d7:f9:4c:c0:11.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '192.168.10.1' (ECDSA) to the list of known hosts.
Authentication failed.
[root@localhost ~]# ssh 192.168.10.1
root@192.168.10.1's password:
Last login: Sat Apr 9 08:47:14 2022
[root@server7-1 ~]#
```

此处请输入“yes”，不要输入“y”

此处请输入 root 密码

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '192.168.10.1' (ECDSA) to the list of known hosts.

root@192.168.10.1's password: 此处输入远程主机 root 管理员的密码

说明：客户端第一次登录服务器，会提醒要求获取服务器端证书的钥匙 key，本钥匙能实现服务器和客户端认证加密访问，默认证书加密算法为 RSA。

②登录服务器的任意一用户，包括 root 用户和普通用户

命令格式可以使用：ssh 用户名@主机名 IP，如下图：

```
[ root@client7- 2 ~]# ssh root@192.168.10.1
root@192.168.10.1's password:
Last login: Sat Apr  9 09:29:57 2022 from 192.168.10.20
[ root@server7- 1 ~]# exit
登出
Connection to 192.168.10.1 closed.
[ root@client7- 2 ~]# ssh dm@192.168.10.1
dm@192.168.10.1's password:
Last login: Sat Apr  9 09:31:32 2022 from 192.168.10.20
[ dm@server7- 1 ~]$ exit
登出
Connection to 192.168.10.1 closed.
```

子任务 2：在以上配置的 sshd 服务中，禁止以 root 管理员的身份远程登录到服务器，并进行远程登录验证。禁止以 root 管理员的身份远程登录，可以大大降低被黑客暴力破解密码的概率。

具体实训操作步骤：

(1) server7-1 服务器上，修改 sshd 服务的主配置文件

/etc/ssh/sshd\_config

在 server7-1 SSH 服务器上，首先使用 vim 文本编辑器打开 sshd 服务的主配置文件，然后把第 38 行 #PermitRootLogin yes 参数前的井号 (#) 去掉，并把参数值 yes 改成 no，这样就不再允许 root 管理员远程登录了。记得最后保存文件并退出。

```
[root@RHEL7-1 ~]# vim /etc/ssh/sshd_config
```

```
37 #LoginGraceTime 2m
38 PermitRootLogin no
39 #StrictModes yes
40 #MaxAuthTries 6
41 #MaxSessions 10
42
: wq
```

### (2) 重启 sshd 服务程序，并设置 sshd 服务开机即启动

一般的服务程序并不会在配置文件修改之后立即获得最新的参数。如果想让新配置文件生效，则需要手动重启相应的服务程序。最好也将这个服务程序加入到开机启动项中，这样系统在下次启动时，该服务程序便会自动运行，继续为用户提供服务。

```
[ root@server7- 1 ~]# systemctl restart sshd
[ root@server7- 1 ~]# systemctl enable sshd
```

(3) 在 client7-2 客户机上测试，当 root 管理员再来尝试访问 sshd 服务程序时，系统会提示不可访问的错误信息。Root 用户被禁止登录，但普通用户可以正常登录

```
[root@client7-2 ~]# ssh root@192.168.10.1
root@192.168.10.1's password:
Permission denied, please try again.
root@192.168.10.1's password:
Permission denied, please try again.
root@192.168.10.1's password:
Permission denied (publickey, gssapi-keyex, gssapi-with-mic, password).
[root@client7-2 ~]# ssh dm@192.168.10.1
dm@192.168.10.1's password:
Last login: Sat Apr 9 11:15:03 2022 from 192.168.10.20
[dm@server7-1 ~]$
```

### 子任务 3：配置基于密钥验证方式，并进行远程登录验证。

在生产环境中使用密码进行口令验证存在着被暴力破解或嗅探截获的风险。对可靠性比较高的服务器，可能不知道服务器账号密码。这时就需要密钥对验证，也就是证书验证加密，需要创建公钥私钥对。如果正确配置了密钥验证方式，那么 sshd 服务程序将更加安全。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，并与服务器中的公钥进行比较；该方式相较来说更安全。加密是对信息进行编码和解码的技术，在传输数据时，如果担心被他人监听或截获，就可以在传输前先使用公钥对数据加密处理，然后再行传送。这样，只有掌握私钥的用户才能解密这段数据，除此之外的其他人即便截获了数据，一般也很难将其破译为明文信息。

#### 具体实训操作步骤：

下面使用密钥验证方式，以用户 student 身份登录 SSH 服务器，具体配置如下。

(1) 在服务器虚拟机 server7-1，创建新用户 student，并设置密码。

```
[ root@server7- 1 ~]# useradd student
[ root@server7- 1 ~]# passwd student
更改用户 student 的密码 。
新的 密码 :
重新输入新的 密码 :
passwd : 所有的身份验证令牌已经成功更新。
[ root@server7- 1 ~]# █
```

(2) 在客户端主机 client7-2 中生成“密钥对”。查看公钥 id\_rsa.pub 和私钥 id\_rsa。

①使用 ssh-keygen -t rsa 命令生成“密钥对”

(-t rsa 指定加密算法，也可省略，默认即此加密算法)

```

[root@client7-2 ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
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: QINY8tflkNl6cZ+sY220xUVl93xtbVwVUdCzbHkmUXA root@client7-2
The key's randomart image is:
+--[RSA 2048]-----+
| .o..o .+. o0E|
| .o.. oo+o . .*0|
| . o ...o o.+#|
| . . . . *B*|
| S. +.=|
| + +|
| . o|
+-----[SHA256]-----+

```



以上语句说明:

- rsa : 非对称加密算法
- Generating public/private rsa key pair. 创建公钥私钥对
- /root/.ssh/id\_rsa 默认文件的保存路径
- Enter passphrase (**empty** for no passphrase): 保护私钥密码, 可直接按回车键使用空密码 (或设置密钥的密码), 使用空密码, 可以不需要输入用户名和密码, 直接登录远程服务器, 前提是证书文件上传服务器。

②进入.ssh目录, 查看公钥和私钥信息

```

[root@client7-2 ~]# cd .ssh/
[root@client7-2 .ssh]# ll
总用量 12
-rw-----. 1 root root 1675 4月 9 12:44 id_rsa
-rw-r--r--. 1 root root 396 4月 9 12:44 id_rsa.pub
-rw-r--r--. 1 root root 174 4月 9 09:28 known_hosts

```

## ●查看公钥信息

```
[root@client7-2 ~]# cat /root/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDTN95fQYxcT0CYTSXUIw6b5nPiQVLI4
hP4M+UBczo0YvAdNPY0CSQuQL1oos39L3TEbhHy8nornI7DNzGSLRSsTkVj3qbNsT0yYzU
GD9mn0ZSyhkNrso/00RME54jg68QYh/5u/sjRjDyDqZ+r5sMTz1QneQ2vA50cJAoVk8yNs
0wNbUA+0b0XPAWwnci/GbMrPW4XrSsgEFai/feuev5Frdrp0SkwTFcULVQ7ZtugggqN7mLC
5bR1AP16wF8V2sMx8Rb38pPRvl3lTDAceCYRvwFKiGNqz07dgD0xp0dBLNPnu4czn9rjNN
61bTllK31Kg2qqumTClb7zCx7vzw7D root@client7-2
```

## ●查看私钥信息

```
[root@client7-2 .ssh]# cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAOzfeX0GMXEzgmE0l1CM0m+Zz4kFSyJeIT+DPLAXM6DmLwHTT
2NAkkLkC9aKLN/S90xG4R8vJ6K5y0wzcxki0UrE5FY96mzbEzsmM1Bg/ZpzmUsoZ
Da7KP9DkTB0eI40vEGIf+bv7IOSXWHamfq+bDE89UJ3kNrw0dHCQKFZPMjbdDsDW1
APjmlzwFsJ3IvxmzKz1uF60rIBBWov33rnr+Ra3adEpMEXFC1U02bboIIKje5i
wuW0dQD9esBfFdrDMfEW9/KTOb5d5UwwHHgmEb8BSohjas903YA9MaTnQSzT57uH
M5/a4zTetW05ZSt9SoNqqrpkwpW+8wse7880wwIDAQABAoIBABrc3SRCQuauRFY6
YZhESSRcv9pDspKeaxC1p9DMmA3k27hDY3oMpsndLdotrQUV1FqWw1gm0+yi2xZV
gXKaZopyy3fJgq9g3NDR40RKPS4AwG5BE8SguUo6d/6Q9CjSI56yzBxH4x30KG1w
OaYFEXQUU9j/67lmW3RFqJ/osjPRdf9rJwL7JAR1U/eI6fwLXKC0/NTGgcQDxArR
d/Bpb070VSoPTdKtFgpWpFIXNnsAit7SuRtUGKwJ60SpJYFP0Ntmi4L/kLT1xROS
vXYvo5i/fqIlIq07biUpLmxWIPTsdt9Yo1FLuIbd7noJm6ZK2EMPmCNX3XR9pstt
JhvDjLkCgYEA9ZFGcM9p4FmLpNwTsAWhNSSEjFQImSmVKQOMDvBbeDq/Z3rEYGQs
d4rlEP4e0FWv8RdVM/hKSdGLZ9IYw/L80QPPxZgnhm7Q0qxI9yNKPFLvXjx4MqCQ
HsK7MBJZ3QCkwH9kzXpNOV80gpfZsCkshfpu5KYI0hVp8jyEJhqqSR8CgYEA3DEF
PonDoyfGm5S1bT9IznQcFV249XDfe8X73PTWn/W1wPLf8hutGq2Yh0dfSYJR51uV
KVKh7bui09yfd/OJL56XicdjfoUowgVjGEPvDGjP0dcfjZC3a8tKXLRE42aK2XTS
2brTApZpFynzjqSfdawqK7DY13YwpMhXz09vMd0CgYA9BCfYh/DqydUk1Xoe1odD
yRswMxsf03E4i6UVYSuZKB+++oYo3TsfS0e53SptHP1mjKghdCQhS3Ip5c45gfrH
hIbvteq8QHSqpBxNK/uaGZFYfPXwvmyQ+BnCzAyAGVTWb9EALU+AonncgRaZ6uEh
0SSss4R/yipVAixju2HwSQKBgHXJu1Zy97alpna/nDXurpHSRtufITwav1JE3LCc
QNuc4zduNSIccANfbcKgCXcXQZ0Tvr02000lfKFPeb9hyrIwkjvf73dU4DK6EwJ+
```

```
BLiMsJ3uWDCwg44kV4kz3c4PoqMk/U3/xLUTpPABPwrFQY//IyfwGG9aCDd9/Isn
oQH5AoGBAN5hpYUiJgmrNXA5kQHKHDe1ZB1StdXn6yU0FMwKsts/LbKmCDyeCZ54
fM20MAyW/YkWrUiNK7CH5nMtYDKD4s4xWkxejLGS3D7WiWS5cRceD8xQTeKPRgbV
RgAwBNkN5kmZZik+t5HkyJ7hdzfTiZuQv+8EDHBexE9zqcZQN253
-----END RSA PRIVATE KEY-----
```

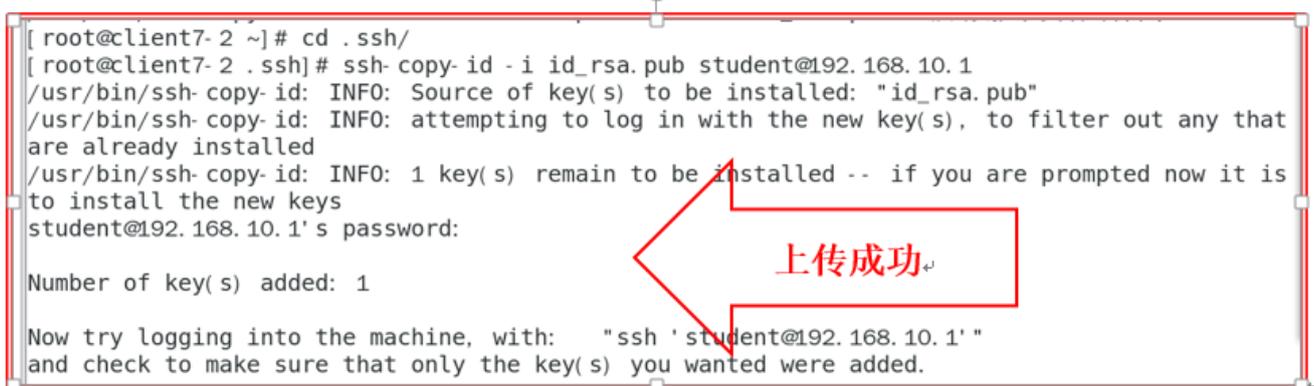
(3) 把客户端主机 client7-2 中生成的公钥文件传送至远程主机的 student 用户，因为 root 用户已禁止登录。

①进入客户端主机 client7-2 的 .ssh 目录，使用 ssh-copy-id -i id\_rsa.pub student@192.168.10.1 命令，上传公钥文件到服务器。

```
[root@client7-2 ~]# cd .ssh/
[root@client7-2 .ssh]# ssh-copy-id -i id_rsa.pub student@192.168.10.1
/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
student@192.168.10.1's password:

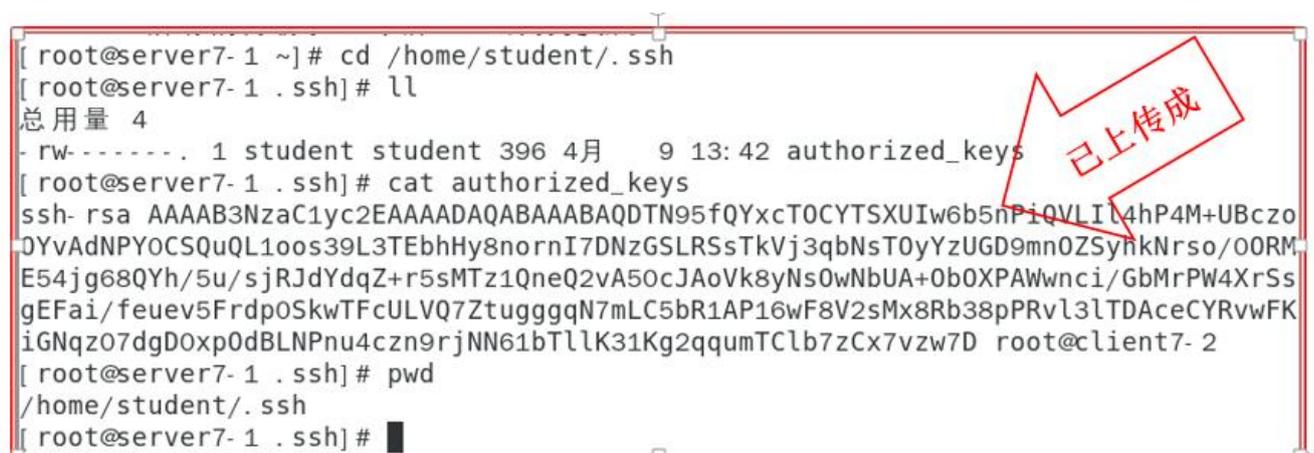
Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'student@192.168.10.1'"
and check to make sure that only the key(s) you wanted were added.
```



②到服务器主机 server7-1，查看客户端主机的公钥文件是否已传当前服务器。可见 authorized\_keys 即客户端主机上传的公钥信息。

```
[root@server7-1 ~]# cd /home/student/.ssh
[root@server7-1 .ssh]# ll
总用量 4
-rw----- 1 student student 396 4月  9 13:42 authorized_keys
[root@server7-1 .ssh]# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDTN95fQYxcT0CYTSXUIw6b5nPiQVLI4hP4M+UBczo
DYvAdNPY0CSQuQL1oos39L3TEbhHy8nornI7DNzGSLRSsTkVj3qbNsT0yYzUGD9mn0ZSynkNrso/0ORM
E54jg68QYh/5u/sjRjdYdqZ+r5sMTz1QneQ2vA50cJAoV8yNs0wNbUA+0b0XPAWwnci/GbMrPW4XrSs
gEFai/feuev5Frdp0SkwTFcULVQ7ZtugggqN7mLC5bR1AP16wF8V2sMx8Rb38pPRvl3lTDAceCYRvwFK
iGNqz07dgD0xp0dBLNPnu4czn9rjNN61bTllK31Kg2qqumTClb7zCx7vz7D root@client7-2
[root@server7-1 .ssh]# pwd
/home/student/.ssh
[root@server7-1 .ssh]#
```



(4) 在服务器 server7-1 中，修改 SSH 服务的主配置文件 /etc/ssh/sshd\_config，只允许密钥验证，拒绝传统的口令验证方式。设置 65 行，使其将 “PasswordAuthentication yes” 改为 “PasswordAuthentication no”。

记得在修改配置文件后保存并重启 sshd 服务程序。

```
[[root@server7-1 student]]# vim /etc/ssh/sshd_config
```

```
64 #PermitEmptyPasswords no
65 PasswordAuthentication no
66 # Change to no to disable s/key passwords
67 #ChallengeResponseAuthentication yes
:wq
```

---

```
[root@server7-1 student]# systemctl restart sshd
```

(5) 在客户端 client7-2 上尝试使用 student 用户远程登录到服务器，此时无须输入密码也可成功登录。

①使用 student 用户远程登录到服务器，此时无须输入密码也可成功登录。因为公钥私钥对匹配，确认验证成功。

**思考：使用 dm 用户远程登录到服务器，此时不能登录，为什么？**

```
[root@client7-2 ~]# ssh student@192.168.10.1
[student@server7-1 ~]$ exit
登出
Connection to 192.168.10.1 closed.
[root@client7-2 ~]# ssh dm@192.168.10.1
Permission denied (publickey, gssapi-keyex, gssapi-with-mic).
[root@client7-2 ~]#
```

②利用 ifconfig 命令可查看到 ens33 的 IP 地址是 192.168.10.1，也即服务器 server7-1 的网卡和 IP 地址，说明已成功登录到了远程服务器 RHEL 7-1 上。

```
[student@server7-1 ~]$ ifconfig
```

```
[root@client7-2 ~]# ssh student@192.168.10.1
Last login: Sat Apr  9 14:29:15 2022 from 192.168.10.20
[student@server7-1 ~]$ ifconfig
ens33: flags=4163<UP, BROADCAST, RUNNING, MULTICAST> mtu 1500
    inet 192.168.10.1 netmask 255.255.255.0 broadcast 192.168.10.255
    inet6 fe80::6c88:2ce8:cf5:9ba6 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:32:c1:32 txqueuelen 1000 (Ethernet)
    RX packets 205032 bytes 296797330 (283.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 66123 bytes 4043674 (3.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

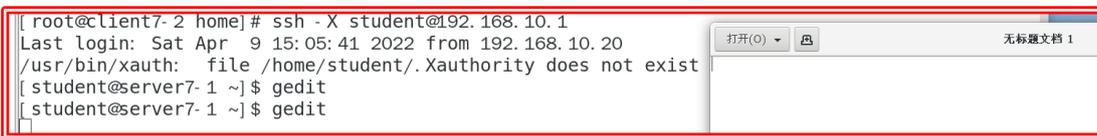
lo: flags=73<UP, LOOPBACK, RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 463 bytes 44522 (43.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
```

此时使用普通用户 student 登录，项目执行中可使用 su - root 切换到 root 用户，或使用 sudo root 命令的格式，执行 root 的权限。

```
[root@client7-2 home]# ssh student@192.168.10.1
Last login: Sat Apr 9 14:35:14 2022 from 192.168.10.20
[student@server7-1 ~]$ su - root
密码:
上一次登录: 六 4月 9 11:10:51 CST 2022从 192.168.10.20pts/1 上
最后一次失败的登录: 六 4月 9 13:28:00 CST 2022从 192.168.10.20ssh: notty 上
最有一次成功登录后有 5 次失败的登录尝试。
[root@server7-1 ~]#
```

此 SSh 配置实现了远程字符界面的访问，如果想实现远程图形界面的访问，可使用参数-X

```
[root@client7-2 home]# ssh -X student@192.168.10.1
```



●在客户机 client7-2 上，使用账户和密码进行远程登录服务器成功后，使用命令 firefox <http://192.168.10.1> 访问服务上的 Apache 服务器。

```
[student@server7-1 ~]$ firefox http://192.168.10.1
Running without a11y support!
```



welcome to myweb

(6) 在服务器 server7-1 上查看 client7-2 客户机的公钥是否传送成功。本案例成功传送。

```
[root@server7-1 student]# cat /home/student/.ssh/authorized_keys
```

```
[root@server7-1 student]# cat /home/student/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDTN95fQYxcTOCYTSXUIw6b5nPiQVLI14hP4M+UBczo
0YvAdNPY0CSQuQL1oos39L3TEbhHy8nornI7DNzGSLRSsTkVj3qbNsT0yYzUGD9mn0ZSyhkNrso/0ORM
E54jg68QYh/5u/sjRjYdqZ+r5sMTz1QneQ2vA50cJAoV8yNs0wNbUA+0b0XPAWwnci/GbMrPW4XrSs
gEFai/feuev5Frpd0SkwTFcULVQ7ZtugggqN7mLC5BR1AP16wF8V2sMx8Rb38pPRv13lTDAceCYRvwFK
iGNqzO7dgdOxp0dBLNPnu4czn9rjNN61bTlK31Kg2qqumTClb7zCx7vzW7D root@client7-2
[root@server7-1 student]#
```



**子任务 4: 使用远程传输命令 scp，并进行远程登录验证。** 远程传输命令 scp (secure copy) 是一个基于 SSH 协议在网络之间进行安全传输的命令，其格式为 “scp [参数] 本地文件 远程帐户@远程 IP 地址:远程目录”。

参数	作用
-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

具体实训步骤:

1. 在服务器 server7-1 上 root 目录下创建文件 myweb.txt，并向远程客户主机 client7-2 (192.168.10.20) 上传此文件。

```
[root@server7-1 ~]# echo "Welcome to smile.com" > mytest.txt
```

```
[root@server7-1 ~]# scp /root/mytest.txt 192.168.10.20:/home
```

```
[root@server7-1 ~]# echo "Welcome to smile.com" > mytest.txt
[root@server7-1 ~]# ll
总用量 12
-rw-r--r-- 1 root root 1898 2月 23 17:00 anaconda-ks.cfg
-rw-r--r-- 1 root root 1926 2月 23 09:05 initial-setup-ks.cfg
-rw-r--r-- 1 root root 21 4月 9 14:53 mytest.txt
drwxr-xr-x 2 root root 6 2月 23 09:06 公共
drwxr-xr-x 2 root root 6 2月 23 09:06 模板
drwxr-xr-x 2 root root 6 2月 23 09:06 视频
drwxr-xr-x 2 root root 147 2月 28 15:22 图片
drwxr-xr-x 2 root root 6 2月 23 09:06 文档
drwxr-xr-x 2 root root 46 3月 1 08:15 下载
drwxr-xr-x 2 root root 6 2月 23 09:06 音乐
drwxr-xr-x 2 root root 6 3月 1 08:23 桌面
[root@server7-1 ~]# scp /root/mytest.txt 192.168.10.20:/home
The authenticity of host '192.168.10.20 (192.168.10.20)' can't be established.
ECDSA key fingerprint is SHA256:PwOT6UHxllukiT1IxiVbiEQ8gpUDSzVbDxRkTJsPtw8.
ECDSA key fingerprint is MD5:65:62:86:7d:b4:17:45:f7:1b:6e:ab:d7:f9:4c:c0:11.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.10.20' (ECDSA) to the list of known hosts.
root@192.168.10.20's password:
mytest.txt                               100% 21      7.0KB/s   00:00
[root@server7-1 ~]# █
```

2. 在客户主机 client7-2 (192.168.10.20) 上, 进入 home 目录查看传输的 mytest.txt 文件已经接收到。

```
[ root@client7- 2 ~]# cd /home
[ root@client7- 2 home]# ll
总用量 4
drwx- - - - - . 5 dm    dm    107 3月   4 16:00 dm
-rw- r- - r- - . 1 root  root   21 4月   9 14:54 mytest.txt
[ root@client7- 2 home]#
```

3. root@192.168.10.20's password: 此处输入远程服务器中 root 管理员的密码, 可以把远程主机的系统版本信息文件下载过来, 这样就无须先登录远程主机, 再进行文件传送了, 也就省去了很多周折。

```
[root@server7-1 ~]# scp 192.168.10.20:/etc/redhat-release /root
```

root@192.168.10.20's password: 此处输入远程服务器中 root 管理员的密码

```
[root@server7-1 ~]# cat redhat-release
```

```
[ root@server7- 1 ~]# scp 192.168.10.20:/etc/redhat-release /root
root@192.168.10.20's password:
redhat-release                               100%  37    2.7KB/s   00:00
[ root@server7- 1 ~]# cat redhat-release
CentOS Linux release 7.9.2009 (Core)
[ root@server7- 1 ~]# █
```

### 子任务 5:

1. 了解使用 window 的一些远程登录小工具, 如 Xshell, SCRT, winscp 等实现 SSH 远程登录。
2. 了解 linux 中使用 VNC 实现图形界面的远程管理, 详见课本的微视频。