

云服务器远程运维实战

技术栈：CentOS 7、银河麒麟、openEuler、SSH、SCP、VNC、腾讯云

项目目标：

掌握云服务器全生命周期管理（申请→配置→运维）。

实现安全的远程访问与文件传输。

技术实现：

云环境搭建：

腾讯云申请 ECS 实例，配置安全组（放行 SSH 22 端口、HTTP 80 端口）。

初始化系统：更新 YUM 源、关闭非必要服务、配置防火墙（firewalld）。

SSH 安全优化：

生成 RSA 密钥对，禁用密码登录，防止暴力破解。

使用 SCP 命令实现 Linux/Windows 跨平台文件同步。

远程管理扩展：

安装 TigerVNC 服务端，配置 GNOME 桌面环境供图形化运维。

关键问题与解决：

问题 1：VNC 连接黑屏。

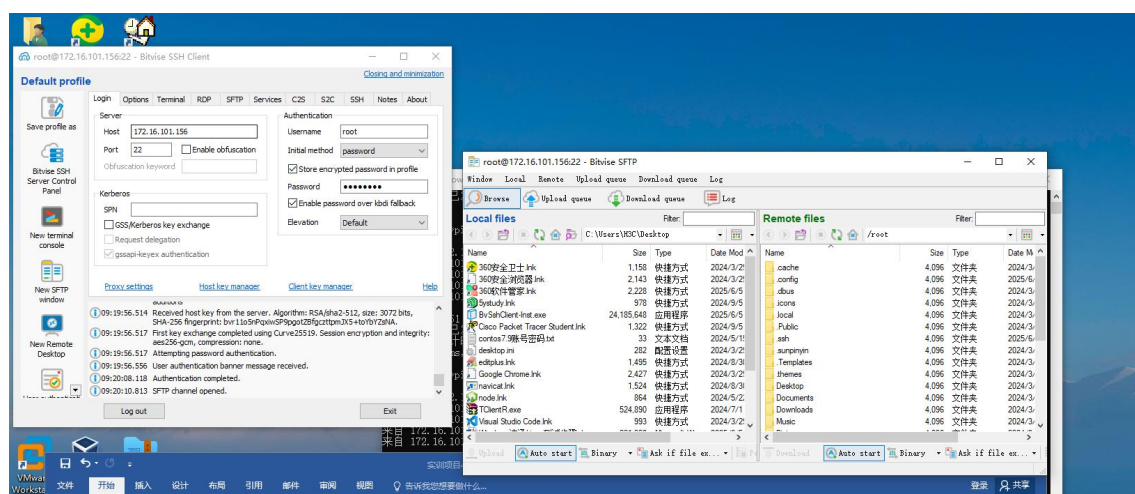
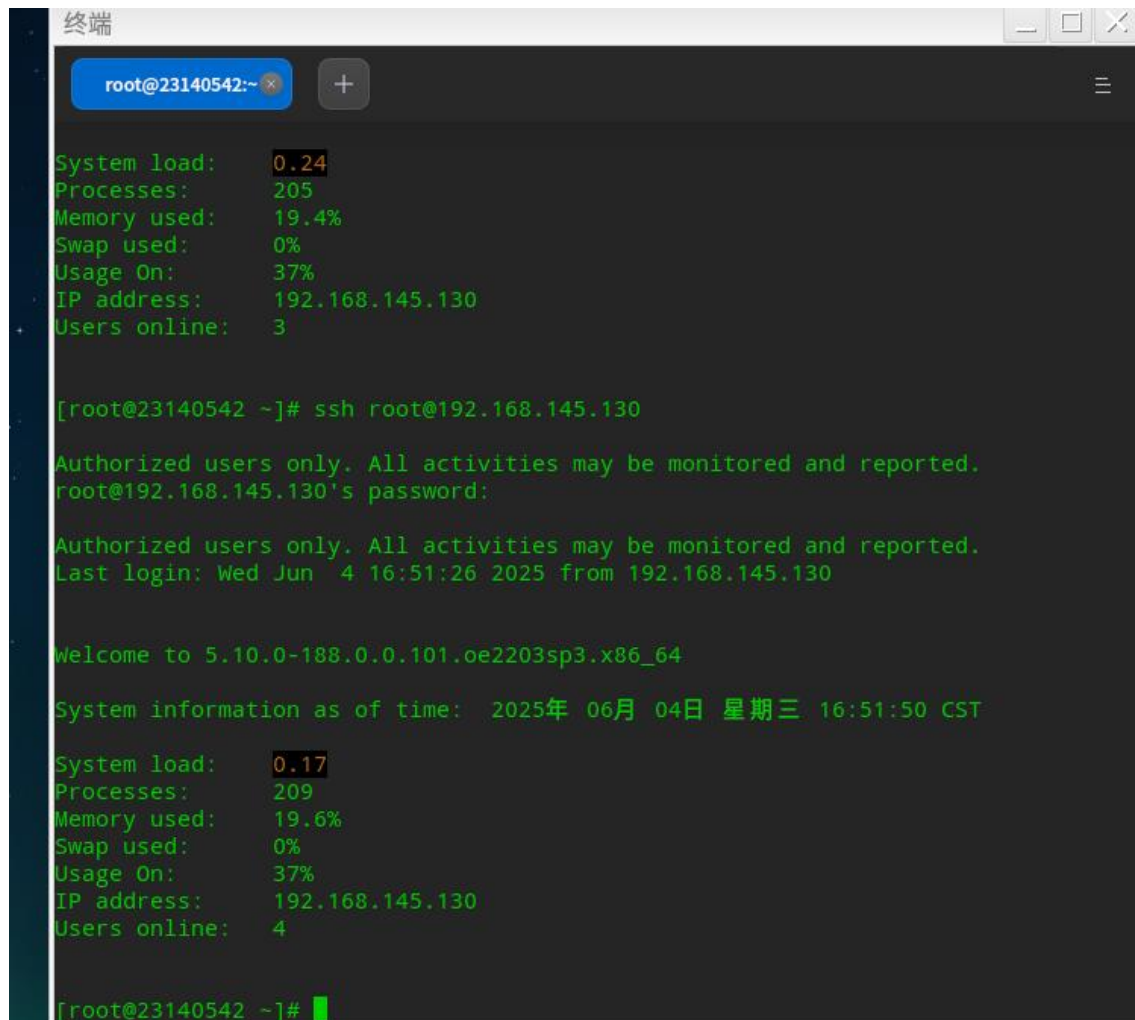
解决：检查 ~/.vnc/xstartup 配置，修正 GNOME 启动参数。

问题 2：SCP 传输速度慢。

解决：启用 SSH 压缩选项（-C），速度提升 30%。

1. 安全 Shell (SSH) (操作结果截图)

- 1) 在 Linux 系统上使用 SSH 登录
- 2) 在 Windows 系统上使用 SSH 登录



2. 文件拷贝

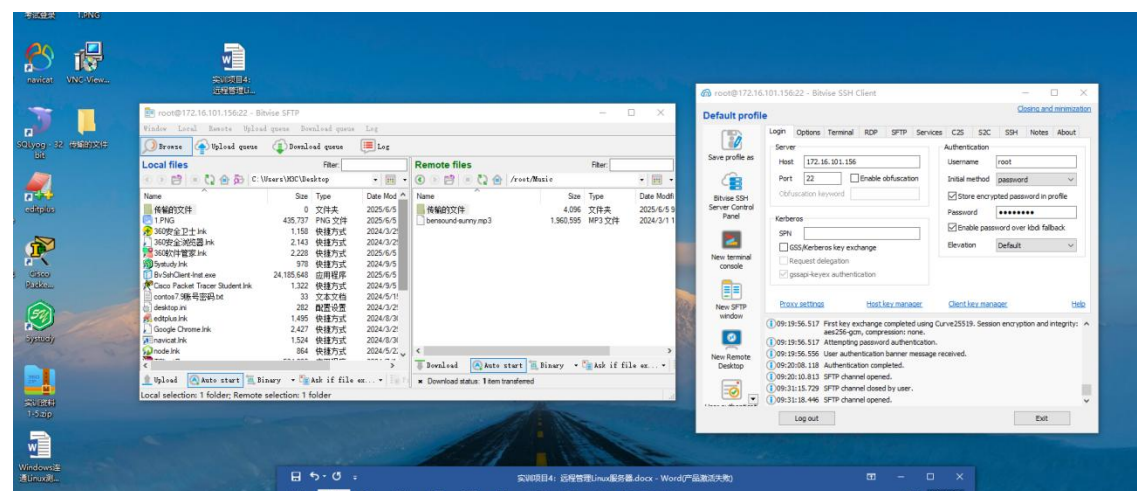
1) 在 Linux 系统间传输文件---scp 命令

```
[root@23140542 ~]# scp /etc/passwd root@192.168.145.130:/tmp/

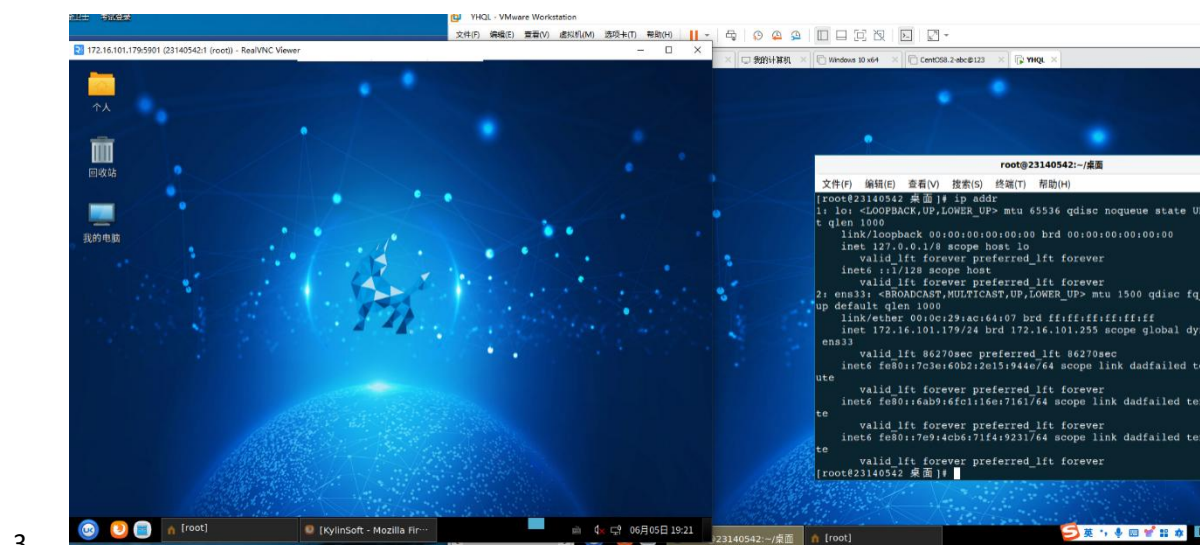
Authorized users only. All activities may be monitored and reported.
root@192.168.145.130's password:
passwd                                100% 2207      5.7MB/s   00:00
[root@23140542 ~]# scp root@192.168.145.130:/etc/passwd /root/

Authorized users only. All activities may be monitored and reported.
root@192.168.145.130's password:
passwd                                100% 2207      8.8MB/s   00:00
[root@23140542 ~]#
```

2) 在 Windows 和 Linux 系统间传输文件



2. 用 VNC 远程桌面管理 Linux 服务器



3.

```
root@23140542:~/桌面
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
[root@23140542 桌面]# vncserver :1

New '23140542:1 (root)' desktop is 23140542:1

Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/23140542:1.log

[root@23140542 桌面]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:ac:64:07 brd ff:ff:ff:ff:ff:ff
    inet 172.16.101.179/24 brd 172.16.101.255 scope global dynamic noprefixroute ens33
        valid_lft 86270sec preferred_lft 86270sec
    inet6 fe80::7c3e:60b2:2e15:944e/64 scope link dadfailed tentative noprefixroute
    inet6 fe80::6ab9:6fc1:16e:7161/64 scope link dadfailed tentative noprefixroute
    inet6 fe80::7e9:4cb6:71f4:9231/64 scope link dadfailed tentative noprefixroute
[root@23140542 桌面]#
```

5.配置 SSH 密钥认证

实验 1: 在 server20 上实现密钥认证登录 server10

```
[root@23140542 ~]# 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:jRwsAaKIxl+qrQlj0o90FlqBW8+44VSlShUzRk1I8U root@23140542
The key's randomart image is:
+---[RSA 3072]-----+
| .o.++B=          |
|+. ..+oEo         |
|=. . o. o         |
|O=. . o +         |
|+.oo   S .        |
|o +=.             |
|.*Oo .            |
|+**=.             |
|=ooo+             |
+---[SHA256]-----+
[root@23140542 ~]# ssh-copy-id root@192.168.145.130
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/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 t
he new keys

Authorized users only. All activities may be monitored and reported.
root@192.168.145.130's password:
```



```

/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

Authorized users only. All activities may be monitored and reported.
root@192.168.145.130's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'root@192.168.145.130'"
and check to make sure that only the key(s) you wanted were added.

[root@23140542 ~]# ssh root@192.168.145.130

Authorized users only. All activities may be monitored and reported.
root@192.168.145.130's password:

Authorized users only. All activities may be monitored and reported.
Last login: Wed Jun  4 16:51:50 2025 from 192.168.145.130

Welcome to 5.10.0-188.0.0.101.oe2203sp3.x86_64

System information as of time: 2025年 06月 04日 星期三 17:24:52 CST

System load:      0.37
Processes:        214
Memory used:      21.7%
Swap used:        0%
Usage On:         39%
IP address:       192.168.145.130
Users online:     5

[root@23140542 ~]# ls /root/.ssh
authorized_keys  id_rsa  id_rsa.pub  known_hosts  known_hosts.old
[root@23140542 ~]#

```

腾讯云申请 ECS 实例，配置安全组（放行 SSH 22 端口、HTTP 80 端口）。
实现安全的远程访问与文件传输。

