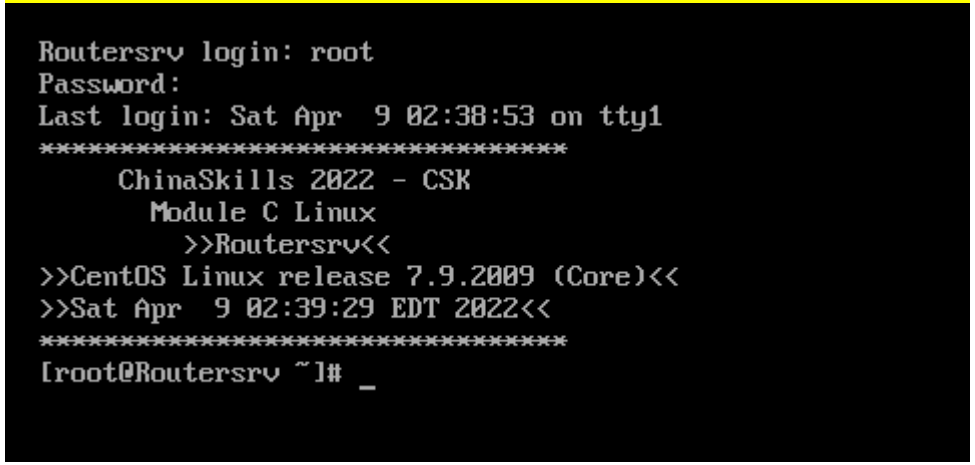
C 模块 Linux 部署评分标准（300）

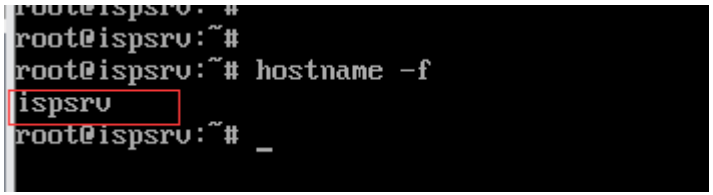
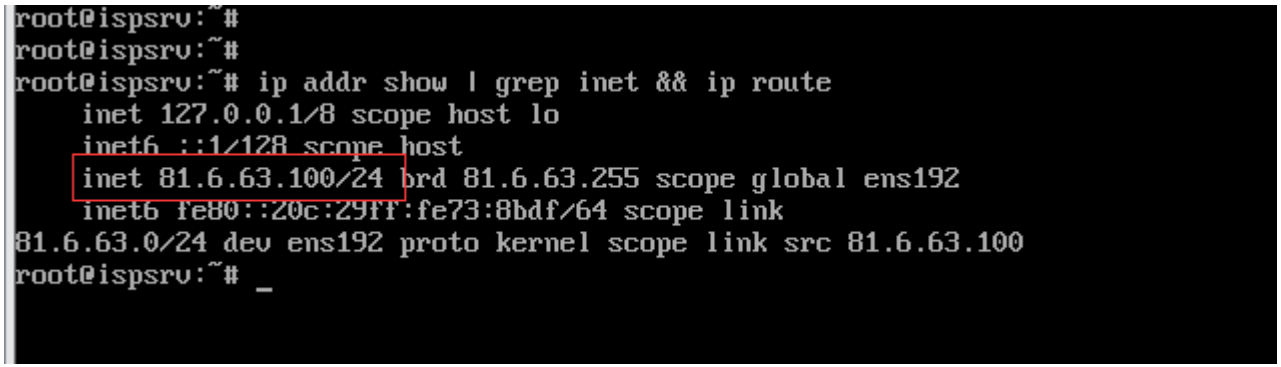
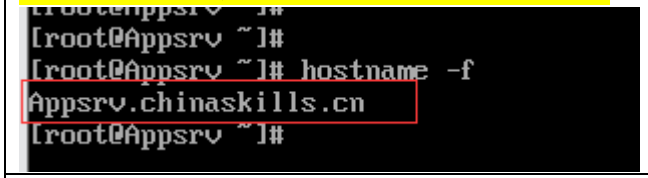
要求：使用下面指令查看其运行状态，并使用 FSCapture 截图软件进行截图，将输入结果的截图插入到文档中；
注：

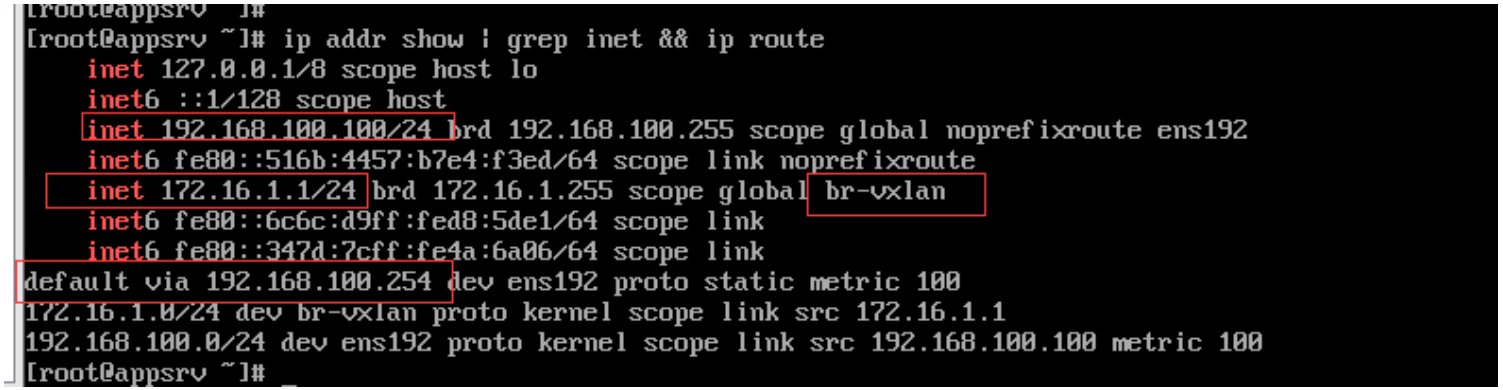
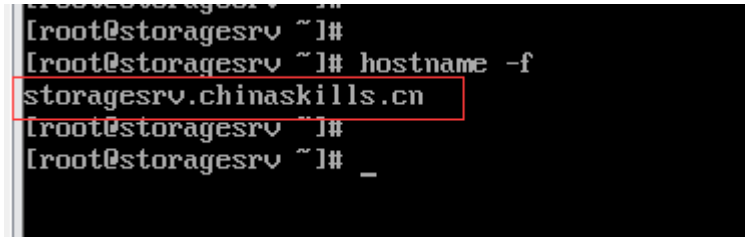
✧ 答题卡中如果整个大题没有截图则整个大题不得分，未使用抓图工具截图的或**截图不完整不清晰**，则不给分。

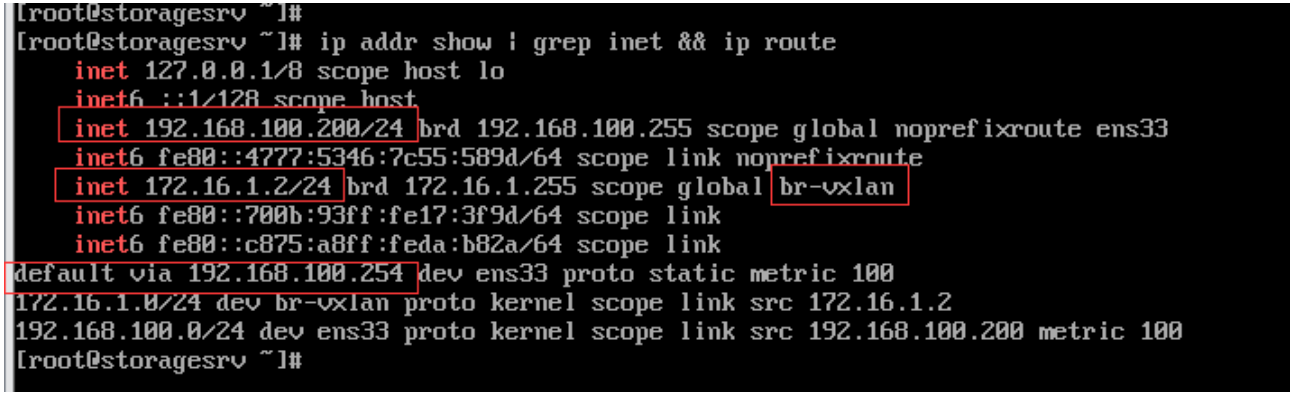
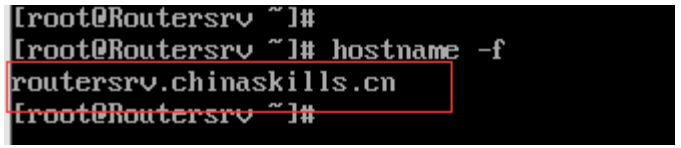
基础分（2 分）

评分要点	分值	评分
1、本地登录提示信息（在任意设备上进行本地登录）	2 分	
评分要点：本地登录提示信息（在任意设备上进行本地登录）（评分要点：在不同的机器上截图，登录提示信息中会显示对应的主机，提示信息存在版本信息，存在日期和时间信息。特别注意，该信息是在登录成功过后弹出！）  		

网络地址规划（31 分）

评分要点	分值	评分
1、ISPSRV：（1）域名（执行指令：hostname -f）；【1 分】	1 分	
（评分要点：主机名信息，大小写不要求。） 		
1、ISPSRV：（2）网络地址/掩码/网关(执行指令：ip addr show | grep inet && ip route)；【每个点 1 分，共 3 分】	3 分	
（评分要点：检查是否存在 81.6.63.100/24 的地址信息，掩码为 24 位，不存在默认路由，无 default 字样。） 		
2、APPSRV：（1）域名（执行指令：hostname -f）；【1 分】	1 分	
（评分要点：主机名等信息，大小写不要求。） 		
2、APPSRV：（2）网络地址/掩码/网关(执行指令：ip addr show | grep inet && ip route)；【每个点 1 分，共 4 分】	4 分	
（评分要点：检查是否存在 192.168.100.100/24 的地址信息，存在 172.16.1.1/24 的 br-vxlan 网桥，存在默认路由，网		

关为 192.168.100.254。）  		
3、STORAGESRV：（1）域名（执行指令：hostname -f）；【1 分】	1 分	
（评分要点：主机名等信息，大小写不要求。）  		
3、STORAGESRV：(2)网络地址/掩码/网关(执行指令：ip addr show | grep inet && ip route)；【每个点 1 分，共 4 分】	4 分	
（评分要点：检查是否存在 192.168.100.200/24 的地址信息，存在地址为 172.16.1.2，名称为 br-vxlan 网桥，存在默认路由，网关为 192.168.100.254。）		

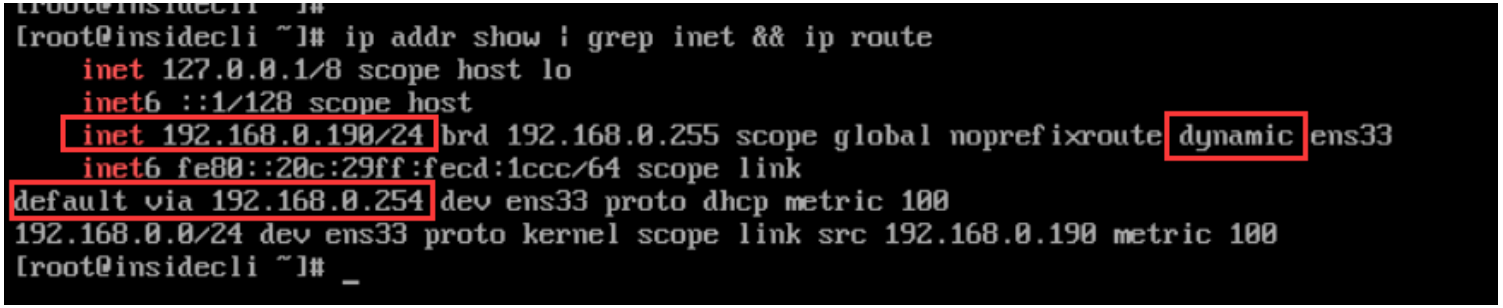
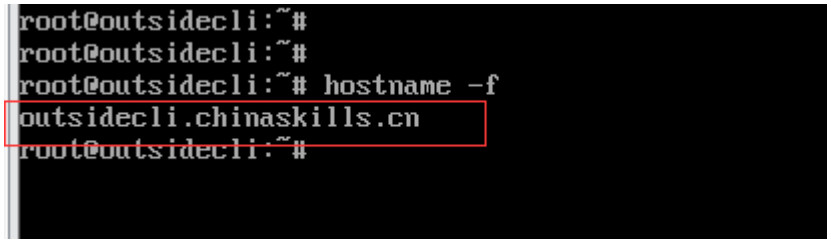
		
4、ROUTERSRV：（1）域名（执行指令：hostname -f）；【1 分】	1 分	
（评分要点：主机名等信息，大小写不要求。） 		
4、ROUTERSRV：（2）网络地址/掩码/网关(执行指令：ip addr show | grep inet && ip route)；【每个点 1 分，共 5 分】	5 分	
（评分要点：检查是否存在 81.6.63.254/24，192.168.100.254/24，192.168.0.254/24，172.16.0.X/24，不存在默认路由，无 default 字样。）		

```
[root@routersrv ~]#
[root@routersrv ~]# ip addr show | grep inet && ip route
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
    inet 192.168.100.254/24 brd 192.168.100.255 scope global noprefixroute ens33
    inet6 fe80::5def:b99a:f3f0:ba86/64 scope link noprefixroute
    inet 192.168.0.254/24 brd 192.168.0.255 scope global noprefixroute ens36
    inet6 fe80::9ada:a9a7:69e3:4bd6/64 scope link noprefixroute
    inet 81.6.63.254/24 brd 81.6.63.255 scope global noprefixroute ens37
    inet6 fe80::686d:356a:49f:61e3/64 scope link noprefixroute
    inet 172.16.0.1/24 brd 172.16.0.255 scope global tun0
    inet6 fe80::ad1d:4d34:a550:906a/64 scope link flags 800
81.6.63.0/24 dev ens37 proto kernel scope link src 81.6.63.254 metric 102
172.16.0.0/24 dev tun0 proto kernel scope link src 172.16.0.1
192.168.0.0/24 dev ens36 proto kernel scope link src 192.168.0.254 metric 101
192.168.100.0/24 dev ens33 proto kernel scope link src 192.168.100.254 metric 100
[root@routersrv ~]# _
```

5、INSIDECLI：（1）域名（执行指令：hostname -f）；【2 分】；	2 分	
（评分要点：主机名等信息，大小写不要求。）		

```
[root@insidecli ~]#
[root@insidecli ~]#
[root@insidecli ~]# hostname -f
insidecli.chinaskills.cn
[root@insidecli ~]# _
```

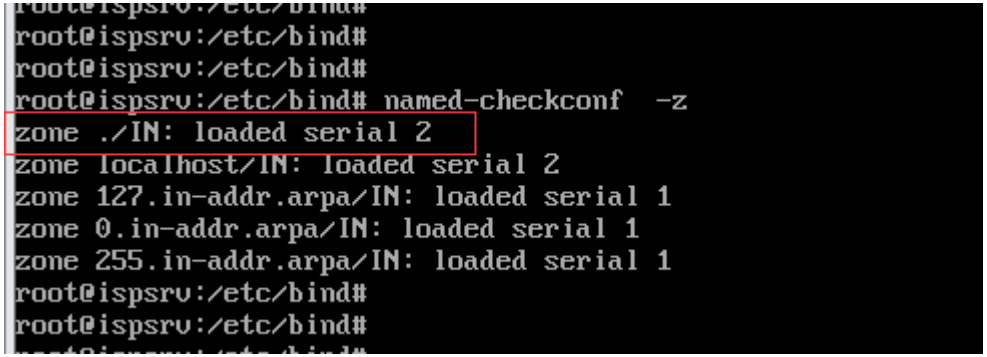
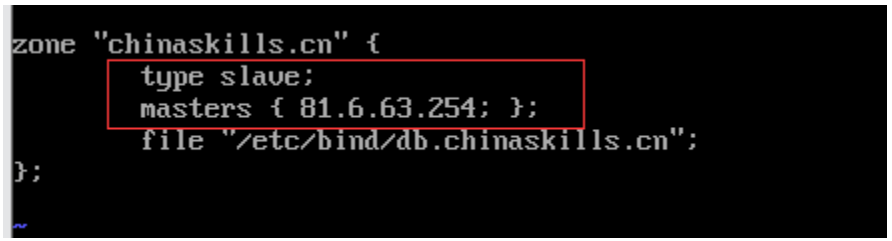
5、INSIDECLI：（2）网络地址/掩码/网关(执行指令：ip addr show | grep inet && ip route)；【每个点 1 分，共 3 分】	3 分	
（评分要点:检查是否存在 192.168.0.190/24 的地址信息,并且地址通过动态 dynamic 获取,默认网关为 192.168.0.254。）		

		
6、OUTSIDECLI：（1）域名（执行指令：hostname -f）；【1 分】	1 分	
（评分要点：主机名等信息，大小写不要求。） 		
6、OUTSIDECLI：（2）网络地址/掩码/网关(执行指令：ip addr show | grep inet && ip route)；【每个点 1 分，共 5 分】	5 分	
（评分要点：存在 81.6.63.110 /24，172.16.0.X/24 地址信息，存在 192.168.0.0/24 和 192.168.100.200/24 的路由，没有默认路由信息，无 default 字样。）		

```
root@outsidecli:~# ip addr show | grep inet && ip route
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
    inet 81.6.63.110/24 brd 81.6.63.255 scope global ens33
    inet6 fe80::20c:29ff:fedb:c9a/64 scope link
    inet 172.16.0.2/24 brd 172.16.0.255 scope global tun0
    inet6 fe80::cf30:c07e:921:99a2/64 scope link stable-privacy
81.6.63.0/24 dev ens33 proto kernel scope link src 81.6.63.110
172.16.0.0/24 dev tun0 proto kernel scope link src 172.16.0.2
192.168.0.0/24 via 172.16.0.1 dev tun0
192.168.100.200 via 172.16.0.1 dev tun0
root@outsidecli:~#
```

ISPSRV 工作任务（15 分）

评分要点	分值	评分
1、DNS：（1）安装 BIND9（执行指令：systemctl status bind9）；【6 分】	6 分	
（评分要点：bind9 服务征程运行“active（running）；运行目录为 -t /var/named/chroot ；注意如果不是 /var/named/chroot 该小题不得分。） root@ispsrv:/var/named/chroot# root@ispsrv:/var/named/chroot# systemctl status bind9 ● bind9.service - BIND Domain Name Server Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled) Active: active (running) since Mon 2022-08-08 14:11:35 CST; 14s ago Docs: man:named(8) Process: 2720 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS) Main PID: 2721 (named) Tasks: 7 (limit: 2281) Memory: 14.5M CGroup: /system.slice/bind9.service └─2721 /usr/sbin/named -u bind -t /var/named/chroot		
1、DNS：（2）根域服务器搭建；【2 分】	2 分	

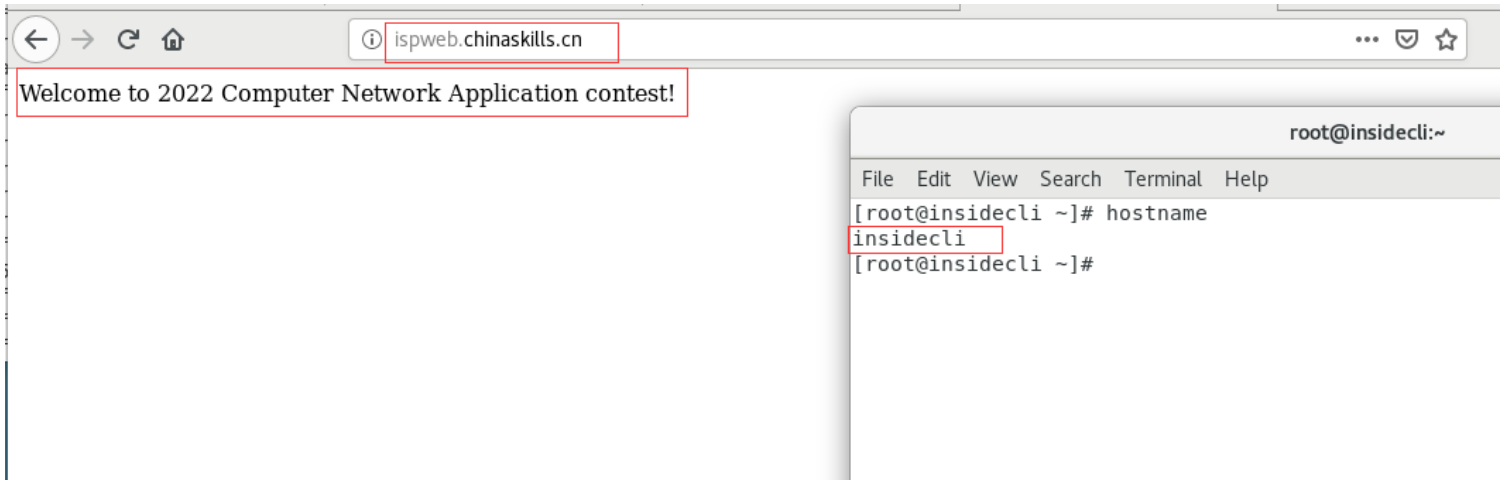
（评分要点：存在“zone ./IN loaded serial 2”） 		
1、DNS：（3）正向区域“chinaskills.cn”搭建。【2 分】	2 分	
（评分要点：type 类型为 slave，masters 设置为 81.6.63.254）； 		
2、WEB：（1）安装 nginx（执行指令：systemctl status nginx）；【1 分】	1 分	
（评分要点：nginx 服务状态运行“active（running）”）		

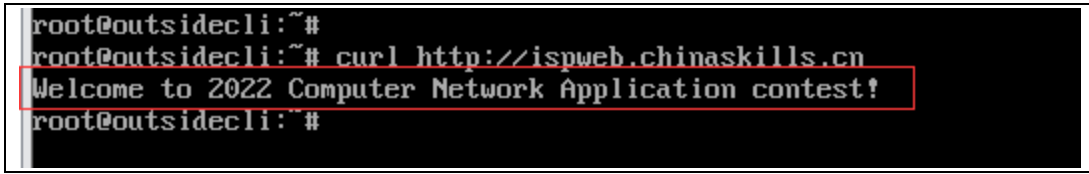
```
root@ispsrv:~#
root@ispsrv:~# systemctl  status  nginx.service
* nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2022-04-09 14:41:10 CST; 18min ago
     Docs: man:nginx(8)
  Process: 743 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCE
  Process: 804 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
 Main PID: 806 (nginx)
    Tasks: 9 (limit: 2308)
   Memory: 12.2M
   CGroup: /system.slice/nginx.service
           |-806 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
           |-807 nginx: worker process
           |-808 nginx: worker process
           |-809 nginx: worker process
           |-810 nginx: worker process
           |-811 nginx: worker process
           |-812 nginx: worker process
           |-813 nginx: worker process
           `-814 nginx: worker process
```

2、WEB：（2）客户端测试（使用 insidecli 网页访问 ispweb.chinaskills.cn 站点，并且要携带命令行输入 hostname 的界面。然后在 outsidecli 上使用 curl http://ispweb.chinaskills.cn）；【4 分】

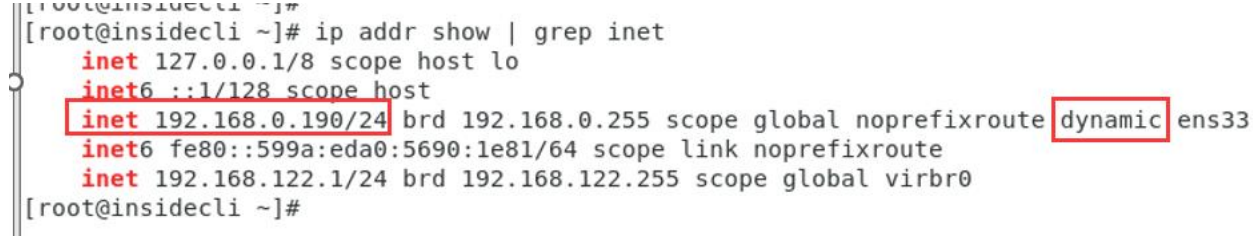
4 分

(评分要点：insidedecli 能够正常访问 ispweb.chinaskills.cn，outsidecli 通过 curl http://ispweb.chinaskills.cn 能够正常显示网页内容。如果 inside 没有携带 hostname 或者 hostname 的主机名不是 insidecli 扣 2 分)



ROUTERSRV 工作任务（40 分）

评分要点	分值	评分
1、DHCP 中继：（1）在 insidecli 上使用 ip addr show | grep inet 查看 insidecli 获取正确的 IP 地址【1 分】；（2）cat /etc/resolv.conf 获取正确的 DNS【1 分】;（3）ip route 查看 GW 地址。【1 分】	3 分	
（1）获取正确 IP（评分要点：能看到客户端的地址为 192.168.0.190，而且是 dynamic 获取。）  （2）DNS(评分要点：能看到 dns 服务器是 192.168.100.100)  （3）网关(评分要点：存在默认路由，而且下一跳是 192.168.0.254)		

```
[root@insidecli ~]# ip route
default via 192.168.0.254 dev ens192 proto dhcp metric 100
192.168.0.0/24 dev ens192 proto kernel scope link src 192.168.0.190 metric 100
192.168.122.0/24 dev virbr0 proto kernel scope link src 192.168.122.1
[root@insidecli ~]#
```

2、ROUTING：开启路由转发，使用 sysctl –p 命令查询；【2 分】	2 分	
（评分要点：查询结果为 net.ipv4.ip_forward = 1，不满足不得分。）		

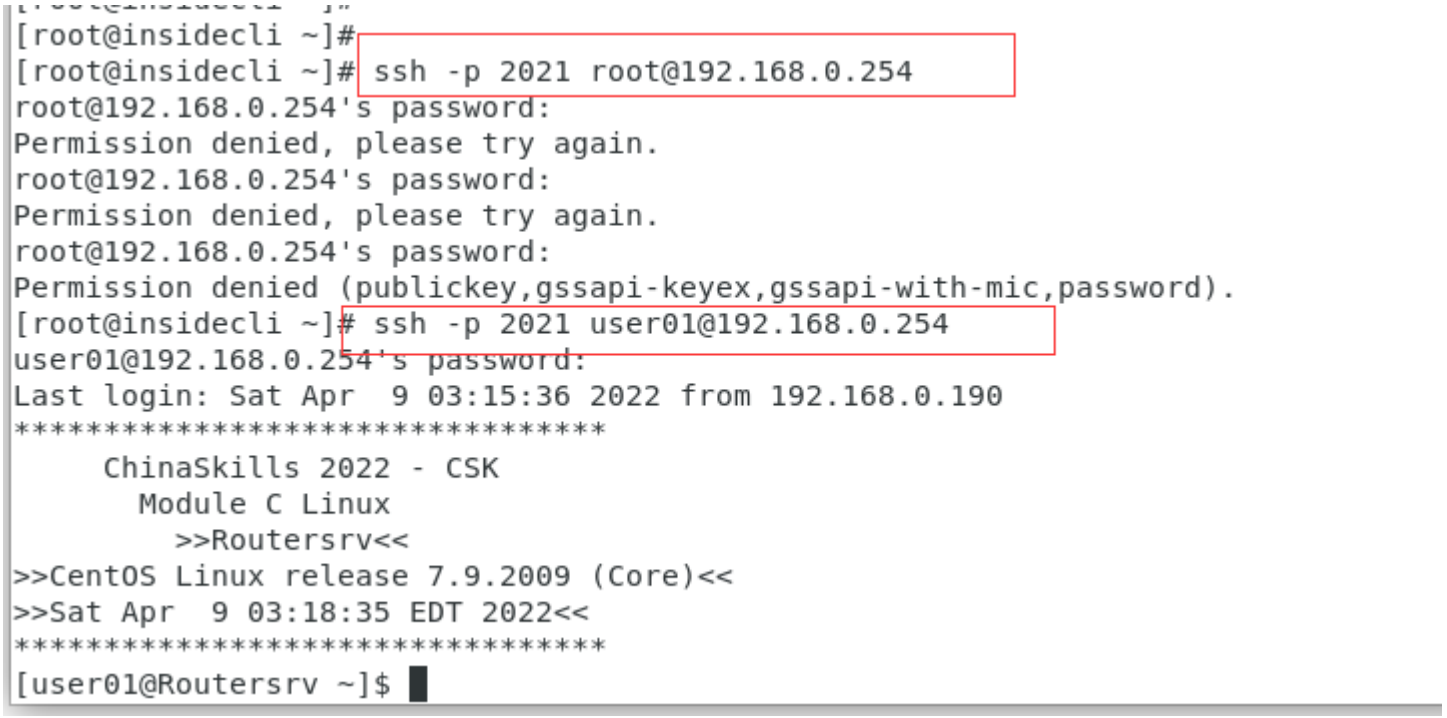
```
[root@Routersrv ~]#
[root@Routersrv ~]# sysctl  -p
net.ipv4.ip_forward = 1
[root@Routersrv ~]# _
```

3、SSH:（1）查看 SSH 服务状态；【1 分】	1 分	
（评分标准：能看到服务状态为 running 即可）		

```
[root@Routersrv ~]#
[root@Routersrv ~]#
[root@Routersrv ~]# systemctl  status  sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-04-08 11:44:15 EDT; 15h ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 10523 (sshd)
   CGroup: /system.slice/sshd.service
           └─10523 /usr/sbin/sshd -D
```

3、SSH:（2）查看 SSH 监听端口(ss -ntpl |grep ssh)；【1 分】	1 分	
（评分标准：显示监听端口号为 2021 即可）		

```
[root@Routersrv ~]#
[root@Routersrv ~]#
[root@Routersrv ~]# ss -ntpl | grep  ssh
LISTEN     0      128          *:2021                     *:*                   users:(("sshd",pid=12579,fd=3))
LISTEN     0      128       [::]:2021                  [::]:*                   users:(("sshd",pid=12579,fd=4))
[root@Routersrv ~]#
```

3、SSH:（3）测试 SSH 登录用户(使用 insidecli 先用 root 用户登录 routersrv，然后再使用 user01 用户登录)；【2 分】	2 分	
(评分要点:先使用 root 用户进行 ssh 登录，显示 permission denied，失败三次后弹出，再使用 user01 用户登录 ssh，成功。) 		
3、SSH：（4）安全测试(使用 user01 用户连续登录失败 3 次，然后再登录一次后截图。)；【4 分】	4 分	
(评分要点:先失败三次，然后自动弹出，再一次登录后显示连接超时。)		

```
[root@insidecli ~]#
[root@insidecli ~]# ssh -p 2021 user01@192.168.0.254
user01@192.168.0.254's password:
Permission denied, please try again.
user01@192.168.0.254's password:
Permission denied, please try again.
user01@192.168.0.254's password:
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@insidecli ~]# ssh -p 2021 user01@192.168.0.254
ssh: connect to host 192.168.0.254 port 2021: Connection timed out
[root@insidecli ~]#
```

3、SSH:（5）查看 SSH 日志 tail -f /var/log/ssh.log；【2 分】	2 分	
（评分标准：能够显示源 IP，源端口号即可，源端口号是随机的。）		

```
[root@Routersrv ~]#
[root@Routersrv ~]# tail -f /var/log/ssh.log
Apr  9 03:18:35 routersrv sshd[12653]: Accepted password for user01 from 192.168.0.190 port 44130 ssh2
Apr  9 03:18:37 routersrv sshd[12622]: Failed password for invalid user root from 192.168.0.190 port 44124 ssh2
Apr  9 03:18:37 routersrv sshd[12622]: Connection closed by 192.168.0.190 port 44124 [preauth]
Apr  9 03:19:53 routersrv sshd[12655]: Received disconnect from 192.168.0.190 port 44130:11: disconnected by user
Apr  9 03:19:53 routersrv sshd[12655]: Disconnected from 192.168.0.190 port 44130
Apr  9 03:19:58 routersrv sshd[12717]: Failed password for user01 from 192.168.0.190 port 44132 ssh2
Apr  9 03:20:01 routersrv sshd[12717]: Failed password for user01 from 192.168.0.190 port 44132 ssh2
Apr  9 03:20:03 routersrv sshd[12717]: Failed password for user01 from 192.168.0.190 port 44132 ssh2
Apr  9 03:20:03 routersrv sshd[12717]: Connection closed by 192.168.0.190 port 44132 [preauth]
Apr  9 03:20:11 routersrv sshd[12719]: Failed password for user01 from 192.168.0.190 port 44134 ssh2




Apr  9 03:22:47 routersrv sshd[12739]: Failed password for user01 from 192.168.0.190 port 44138 ssh2
Apr  9 03:22:50 routersrv sshd[12739]: Failed password for user01 from 192.168.0.190 port 44138 ssh2
Apr  9 03:22:53 routersrv sshd[12739]: Failed password for user01 from 192.168.0.190 port 44138 ssh2
Apr  9 03:22:53 routersrv sshd[12739]: Connection closed by 192.168.0.190 port 44138 [preauth]
Apr  9 03:26:19 routersrv sshd[12749]: Failed password for user01 from 192.168.0.190 port 44142 ssh2
Apr  9 03:26:19 routersrv sshd[12749]: Connection closed by 192.168.0.190 port 44142 [preauth]
Apr  9 03:26:20 routersrv sshd[12751]: Accepted password for user01 from 192.168.0.190 port 44144 ssh2
```

4、IPTABLES：SNAT（在 routersrv 上执行指令：iptables -t nat -nvL POSTROUTING）；【2 分】	2 分	
（评分要点：存在源为 192.168.0.0/24 和 192.168.100.0/24 的 MASQUERADE 规则，其他参数不做评判标准。）		

```
[root@Routersrv ~]#
[root@Routersrv ~]# iptables -t nat -nvL POSTROUTING
Chain POSTROUTING (policy ACCEPT 161K packets, 10M bytes)
 pkts bytes target     prot opt in     out     source               destination
    2   134 MASQUERADE  all  --  *      ens256  192.168.100.0/24     0.0.0.0/0
   11   732 MASQUERADE  all  --  *      ens256  192.168.0.0/24       0.0.0.0/0
[root@Routersrv ~]# _
```

4、IPTABLES：（2）DNAT（在 routersrv 上执 行指令：iptables -t nat -nvL PREROUTING）；**【2 分】**	2 分	
（评分要点：存在目的地为 81.6.63.254 的 DNAT 规则，规则中至少需要存在 udp53，tcp53、tcp80、tcp443、tcp465、tcp993。）		

```
[root@Routersrv ~]#
[root@Routersrv ~]# iptables -t nat -nvL  PREROUTING
Chain PREROUTING (policy ACCEPT 199K packets, 13M bytes)
 pkts bytes target     prot opt in     out     source               destination
    4   240 DNAT       tcp  --  *      *       81.6.63.0/24         81.6.63.254          multiport dports 53,80,443,465,993 to:192.168.100.100
    0     0 DNAT       tcp  --  *      *       81.6.63.0/24         81.6.63.254          multiport dports 20,21,137,138,139,444,445,3358 to:192.168.100.200
  875 63004 DNAT       udp  --  *      *       81.6.63.0/24         81.6.63.254          udp dpt:53 to:192.168.100.100
[root@Routersrv ~]#
[root@Routersrv ~]#
```

4、IPTABLES：（3）默认链拒绝流量通行（在 routersrv 上执行指令：iptables -nL	grep Chain）；**【1 分】**	1 分	
（评分要点：INPUT 、OUTPUT 和 FORWARD 链的默认规则为 DROP）		

```
[root@Routersrv ~]#
[root@Routersrv ~]# iptables -nL | grep Chain
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy DROP)
```

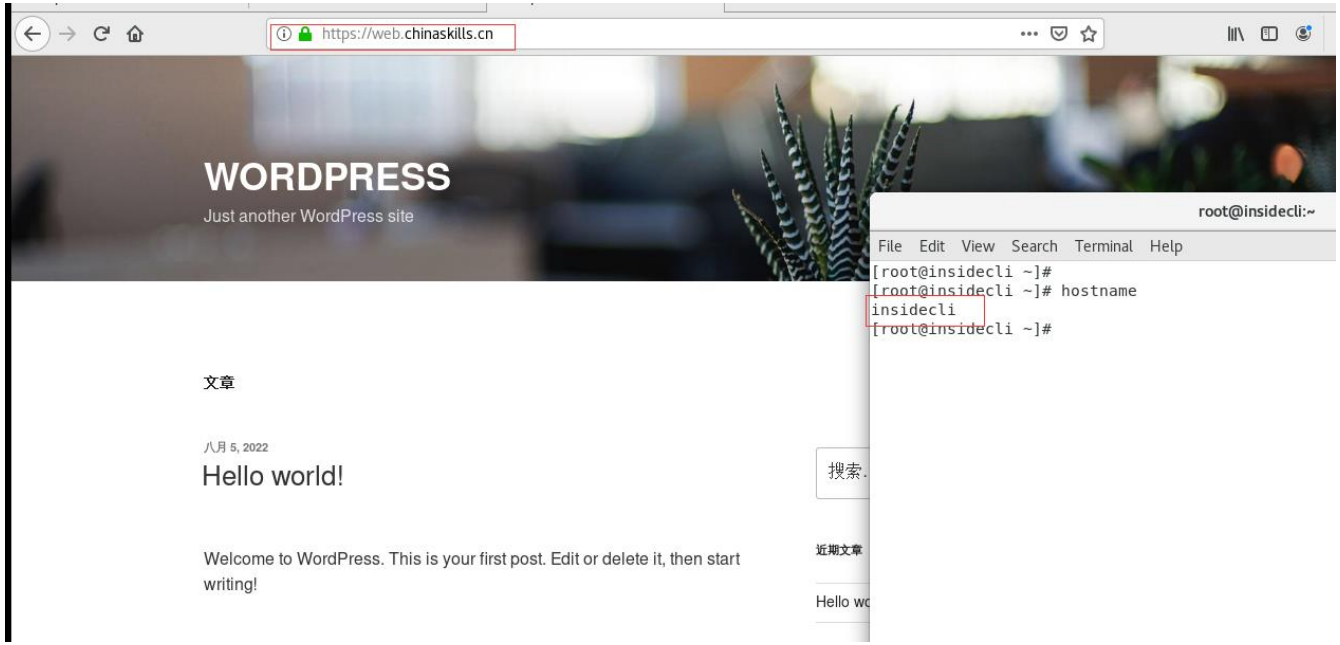
4、IPTABLES：（4）放行必要流量（在 routersrv 上执行：iptables -nL）;**【2 分】**	2 分	
（评分要点：INPUT 链至少需要放行 tcp2021，tcp1194，udp67， 流量。FORWARD 链至少需要放行 tcp 20,21,53,80,433,465,993 udp53 流量。）		

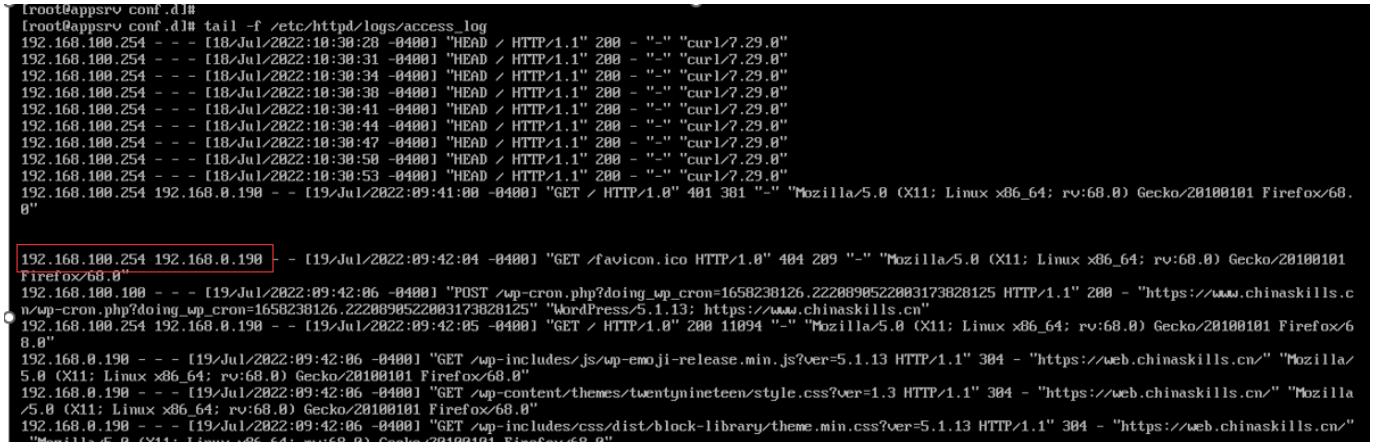
```
[root@routersrv ~]#
[root@routersrv ~]# iptables -nL
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 67,68
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 1194,2021

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 53,80,443,465,993,20,
21,137,138,139,444,445,4500:5000
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:53

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 67,68
[root@routersrv ~]# _
```

5、Web Proxy：（1）检查 nginx 服务状态（routersrv 执行 systemctl status nginx）；【1 分】	1 分	
（评分要点：服务状态为 running 即可得分）		

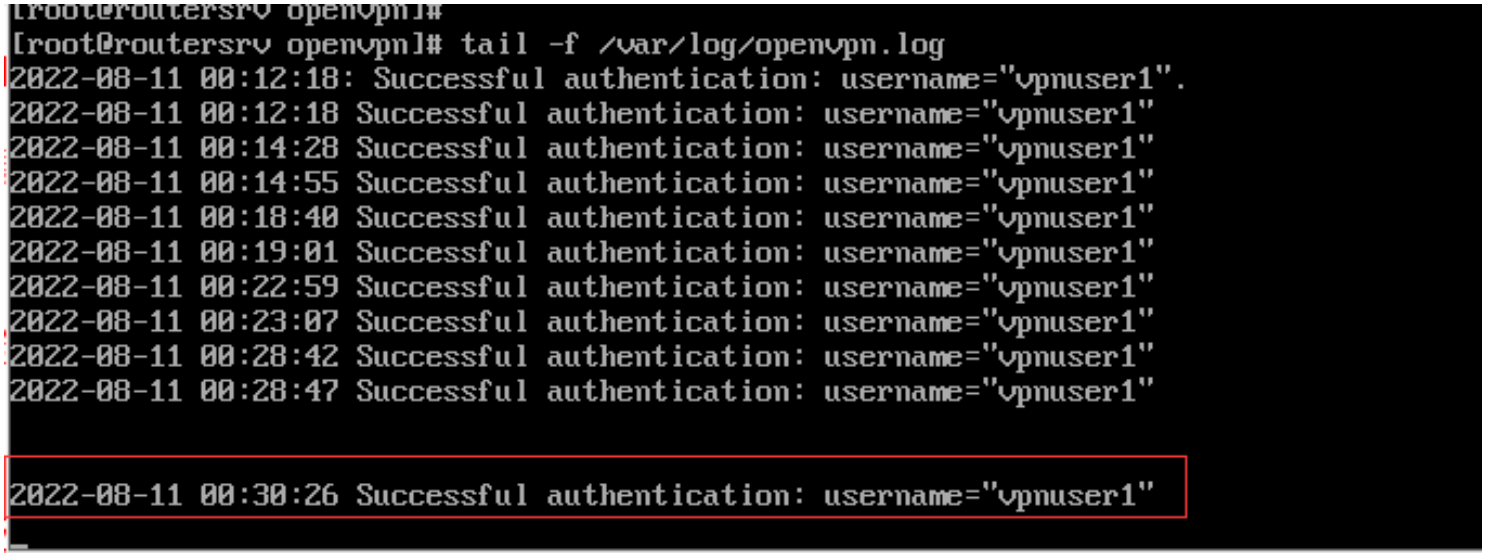
```
[root@Routersrv ~]#
[root@Routersrv ~]# systemctl  status  nginx.service
● nginx.service - The nginx HTTP and reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2022-04-08 02:54:02 EDT; 24h ago
 Main PID: 8691 (nginx)
   CGroup: /system.slice/nginx.service
           ├─8691 nginx: master process /usr/sbin/nginx
           ├─8692 nginx: worker process
           ├─8693 nginx: worker process
           ├─8694 nginx: worker process
           ├─8695 nginx: worker process
           ├─8696 nginx: worker process
           ├─8697 nginx: worker process
           ├─8698 nginx: worker process
           ├─8699 nginx: worker process
           └─8700 nginx: cache manager process
```

5、Web Proxy：（2）客户端访问测试（使用 insidecli 访问 web.chinaskills.cn,并且携带在终端输入 hostname 的截图）；【2 分】	2 分	
（评分要点：通过 web.chinaskills.cn 能访问到 www.chinaskills.cn 页面的内容，www.chinaskills.cn 是 wordpress 主页面，而且有绿色带锁的标志，如果不携带 hostname 的截图或者 hostname 截图主机名不是 insidecli 本题不得分）		

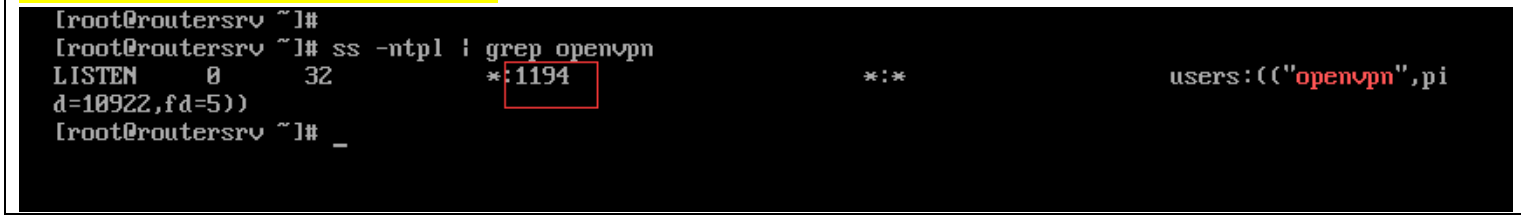


5、Web Proxy：（3）检查网页日志（appsrv 执行 tail -f /etc/httpd/logs/access_log）；【2 分】	2 分	
（评分要点：能够看到代理服务器 IP 和客户端真实 IP 即可得分，例如 192.168.100.254 192.168.0.190 的地址。第二个地址必须是 192.168.0.190，第一个地址可以是 192.168.100.254 或 192.168.0.254） 		

5、Web Proxy：（4）测试服务器监控脚本(routersrv 先执行网页检测脚本，appsrv 执行 tail -f /etc/httpd/logs/access_log)；【3 分】	3 分	
(评分要点：每三秒作为一次间隔。进行网页监测，如图所示的 11:42:28 - 11:42:31 - 11:42:34) 192.168.100.254 - - - [09/Apr/2022:11:42:28 -0400] "GET / HTTP/1.1" 200 11039 "-" "curl/7.29.0" 192.168.100.254 - - - [09/Apr/2022:11:42:31 -0400] "GET / HTTP/1.1" 200 11039 "-" "curl/7.29.0" 192.168.100.254 - - - [09/Apr/2022:11:42:34 -0400] "GET / HTTP/1.1" 200 11039 "-" "curl/7.29.0"		
6、OPENVPN：（1）测试 VPN 用户验证（在 outsidecli 上执行 systemctl restart openvpn@client；然后输入用户密码截图；然后再执行 systemctl status openvpn@client)；【每个点 2 分，共 6 分】	6 分	
（评分要点：用户认证后，能看到服务状态为 running，而且显示 Initialzation Sequence Completed） root@outsidecli:~# root@outsidecli:~# systemctl restart openvpn@client Enter Auth Username: vpnuser1 Enter Auth Password: ****** root@outsidecli:~# root@outsidecli:~# systemctl status openvpn@client * openvpn@client.service - OpenVPN connection to client Loaded: loaded (/lib/systemd/system/openvpn@.service; enabled-runtime; vendor preset: enabled) Active: active (running) since Thu 2022-08-11 00:28:42 CST; 30s ago Docs: man:openvpn(8) https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage https://community.openvpn.net/openvpn/wiki/HOWTO Main PID: 22003 (openvpn) Status: "Initialization Sequence Completed" Tasks: 1 (limit: 2281) Memory: 904.0K CGroup: /system.slice/system-openvpn.slice/openvpn@client.service `-22003 /usr/sbin/openvpn --daemon ovpn-client --status /run/openvpn/client.status 10 --cd /etc/openvpn --config /etc Aug 11 00:28:44 outsidecli ovpn-client[22003]: Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key Aug 11 00:28:44 outsidecli ovpn-client[22003]: ROUTE: default_gateway=UNDEF Aug 11 00:28:44 outsidecli ovpn-client[22003]: TUN/TAP device tun0 opened Aug 11 00:28:44 outsidecli ovpn-client[22003]: TUN/TAP TX queue length set to 100 Aug 11 00:28:44 outsidecli ovpn-client[22003]: do_ifconfig, tt->did_ifconfig_ipv6_setup=0 Aug 11 00:28:44 outsidecli ovpn-client[22003]: /sbin/ip link set dev tun0 up mtu 1500 Aug 11 00:28:44 outsidecli ovpn-client[22003]: /sbin/ip addr add dev tun0 172.16.0.2/24 broadcast 172.16.0.255 Aug 11 00:28:44 outsidecli ovpn-client[22003]: /sbin/ip route add 192.168.0.0/24 via 172.16.0.1 Aug 11 00:28:44 outsidecli ovpn-client[22003]: /sbin/ip route add 192.168.100.200/32 via 172.16.0.1 Aug 11 00:28:44 outsidecli ovpn-client[22003]: Initialization Sequence Completed lines 1-23/23 (END)		
6、OPENVPN：（2）然后查看 VPN 日志（routersrv 执行 tail -f /var/log/openvpn.log）；【2 分】	2 分	
（评分要点：存在登陆成功的条目，和题目要求格式一致即可得分）		



6、OPENVPN：（3）查看 VPN 端口号（routersrv 执行 ss -ntpl | grep openvpn）；【2 分】	2 分	
（评分要点：监听 TCP1194 即可得分）		



APPSRV 工作任务（95 分）

评分要点	分值	评分
1、SSH：（1）安装和监听端口设置（在 appsrv 上执行：ss -nltp | grep ssh）；【1 分】	1 分	
（评分要点：sshd 程序监听 tcp2101 端口）		

```
[root@appsrv ~]#
[root@appsrv ~]# ss -ntpl | grep ssh
LISTEN     0      128          *:2101                     *:*                   users:(("sshd",pid=82487,fd=3))
LISTEN     0      128       [::]:2101                  [::]:*                   users:(("sshd",pid=82487,fd=4))
[root@appsrv ~]#
```

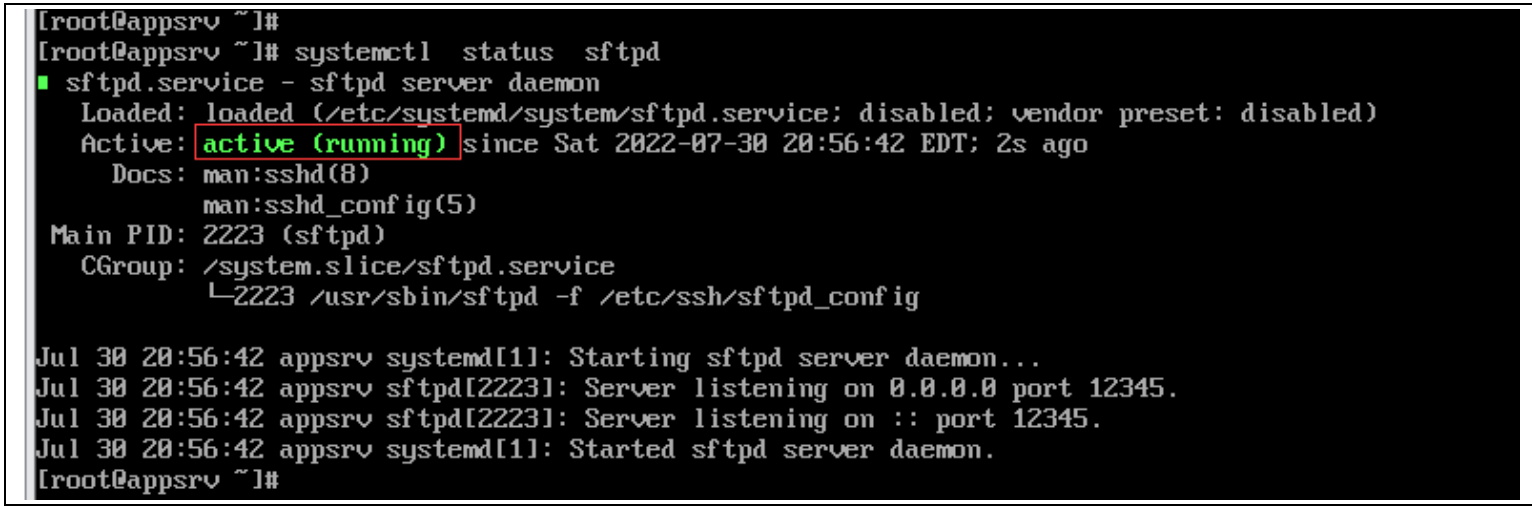
1、SSH：（2）访问限制（在 storagesrv 上执行指令：ssh -p 2101 root@192.168.100.100）；【2 分】	2 分	
（评分要点：返回结果为 Connection reset by peer）		

```
[root@storagesrv ~]#
[root@storagesrv ~]# ssh -p 2101 root@192.168.100.100
ssh_exchange_identification: read: Connection reset by peer
[root@storagesrv ~]#
```

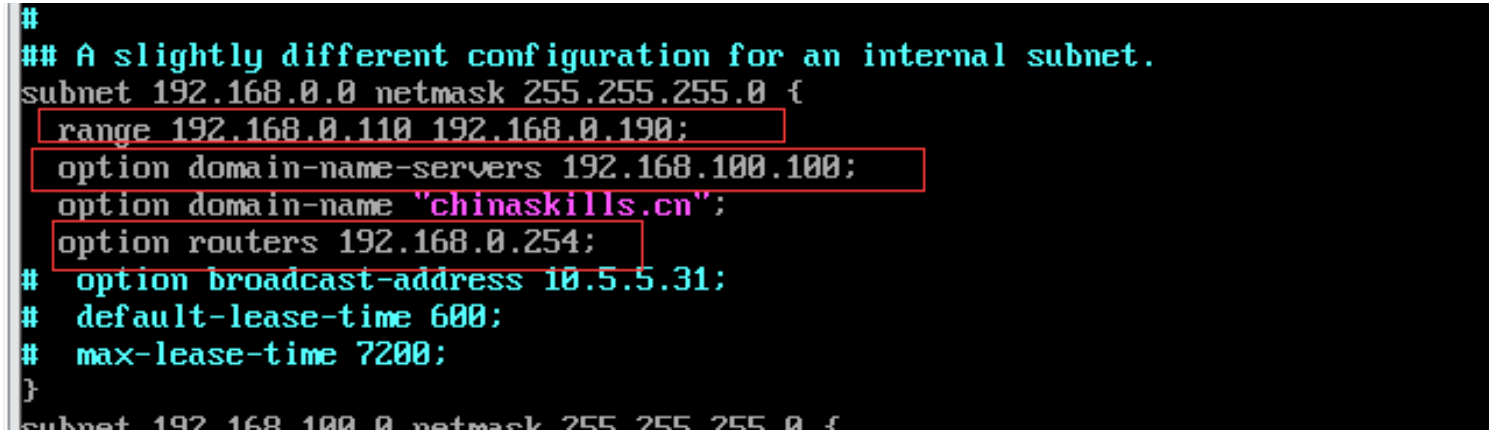
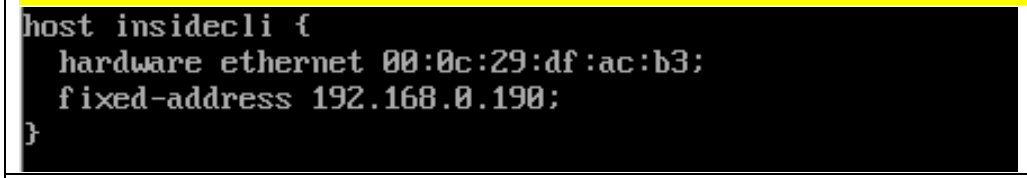
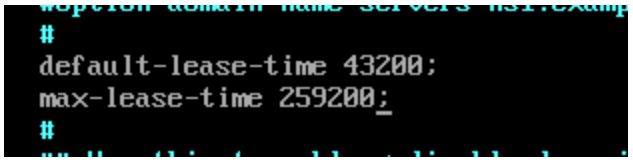
1、SSH：（3）免密登录（InsideCli 的 cskadmin 用户环境上执行指令：ssh -p 2101 root@192.168.100.100）；【2 分】	2 分	
（评分要点：Insidecli 可以进行 SSH 免密登录，并且成功）		

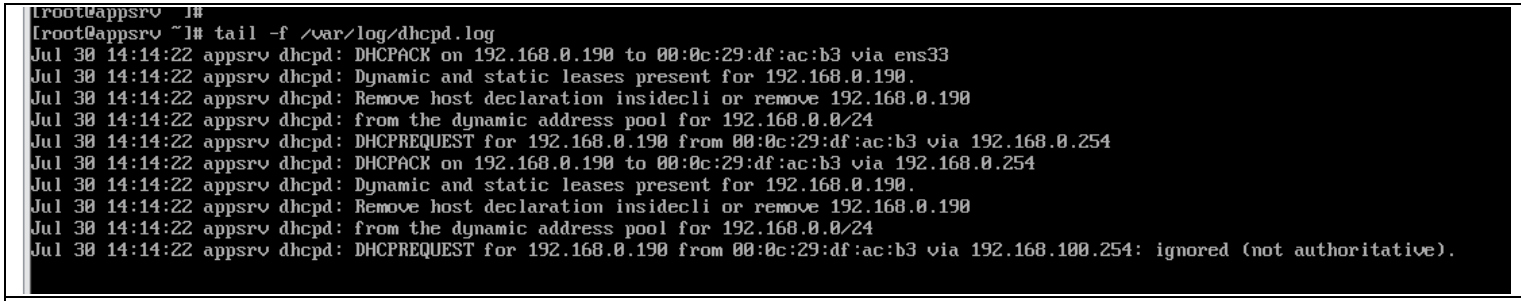
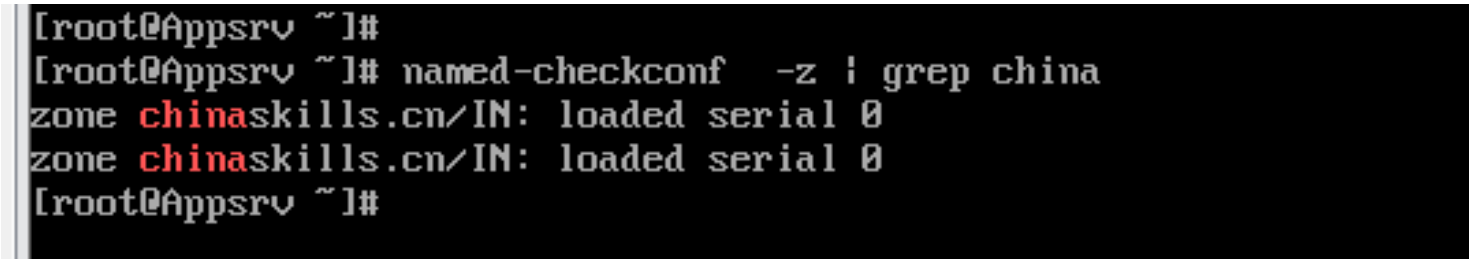
```
[cskadmin@insidecli ~]$ ssh -p 2101 root@192.168.100.100
Last login: Tue Jul 19 05:01:03 2022 from 192.168.0.190
**************************
   ChinaSkills 2022 - CSK
     Module C Linux
     >>appsrv<<
     >>CentOS Linux release 7.9.2009 (Core)<<
>>Tue Jul 19 09:53:01 EDT 2022<<
**************************
[root@appsrv ~]#
```

1、SSH：（4）分离 SFTP（appsrv 执行 systemctl status sftpd）；【3 分】	3 分	
（评分要点：状态显示为 running 得分）		



1、SSH：（5）SFTP 端口号（appsrv 执行 ss -ntpl	grep sftpd）；【2 分】	2 分	
（评分要点：监听端口号为 54321 得分） 		
2、DHCP：（1）客户端地址范围、DNS 选项、网关选项（查看 DHCP 配置文件，截取相关的部分配置即可）；【4 分】	4 分	
（评分要点：范围在 192.168.0.110-192.168.0.190，DNS 设置为：192.168.100.100，网关设置为 192.168.0.254）		

		
2、DHCP:（2）分配固定地址（查看 DHCP 配置文件，截取固定地址分配的配置即可）；【2 分】	2 分	
（评分要点：存在 fixed-address 192.168.0.190；和 hardware ethernet 即可） 		
2、DHCP:（3）查看租约时间（查看 DHCP 配置文件中租约时间的配置）；【2 分】	2 分	
（评分要点：默认租约时间为 43200 秒，最大租约时间为 259200 秒） 		
2、DHCP:（4）查看日志信息（在 appsrv 执行指令：tail -f /var/log/dhcpd.log）；【2 分】	2 分	
（评分要点：存在日志信息即可得分）		

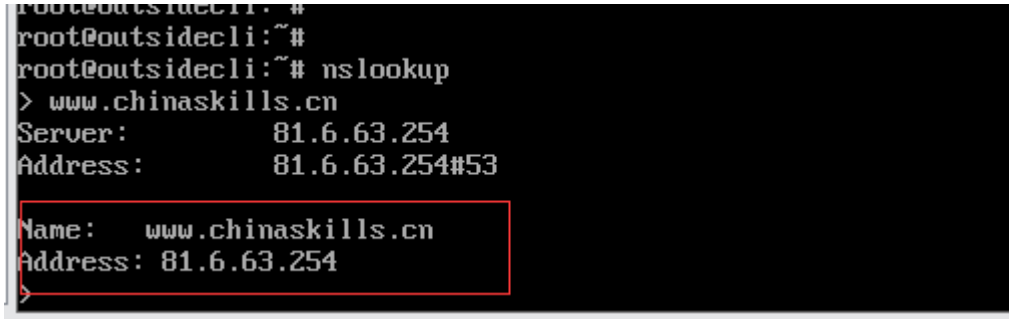
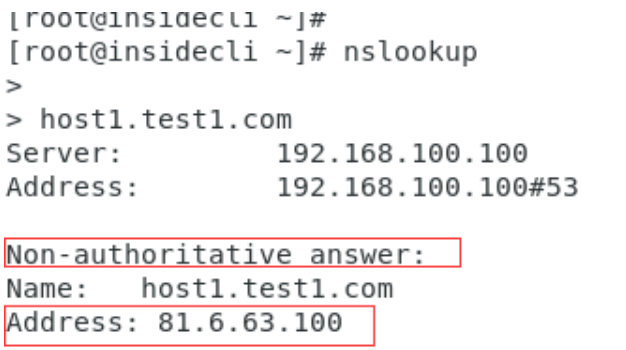
		
3、DNS：（1）chinaskills.cn 域解解析（在 appsrv 上执行指令：named-checkconf -z | grep china）；【2 分】	2 分	
（评分要点:在 appsrv 上执行指令：named-checkconf -z | grep china，存在 2 条 chinaskills.cn 即可） 		
3、DNS：（2）A 记录；(在 insidecli 上进入 nslookup 解析视图，分别解析 www.chinaskills.cn、 download.chinaskills.cn 和 mail.chianskills.cn)；【3 分】	3 分	
（评分要点：www、download、mail 主机均解析到 192.168.100.100，一条解析记录 1 分）		

```
[root@insidecli ~]#
[root@insidecli ~]# nslookup
> www.chinaskills.cn
Server:         192.168.100.100
Address:        192.168.100.100#53

Name:   www.chinaskills.cn
Address: 192.168.100.100
> download.chinaskills.cn
Server:         192.168.100.100
Address:        192.168.100.100#53

Name:   download.chinaskills.cn
Address: 192.168.100.100
> mail.chinaskills.cn
Server:         192.168.100.100
Address:        192.168.100.100#53

Name:   mail.chinaskills.cn
Address: 192.168.100.100
>
```

3、DNS：（3）MX 记录（在 insidecli 上执行指令：host -t MX chinaskills.cn 192.168.100.100）；【1 分】	1 分	

（评分要点：chinaskills.cn 的 MX 解析解析到 mail.chinaskills.cn.主机）

```
[root@insidecli ~]#
[root@insidecli ~]# host -t MX chinaskills.cn 192.168.100.100
Using domain server:
Name: 192.168.100.100
Address: 192.168.100.100#53
Aliases:

chinaskills.cn mail is handled by 10 mail.chinaskills.cn.
```

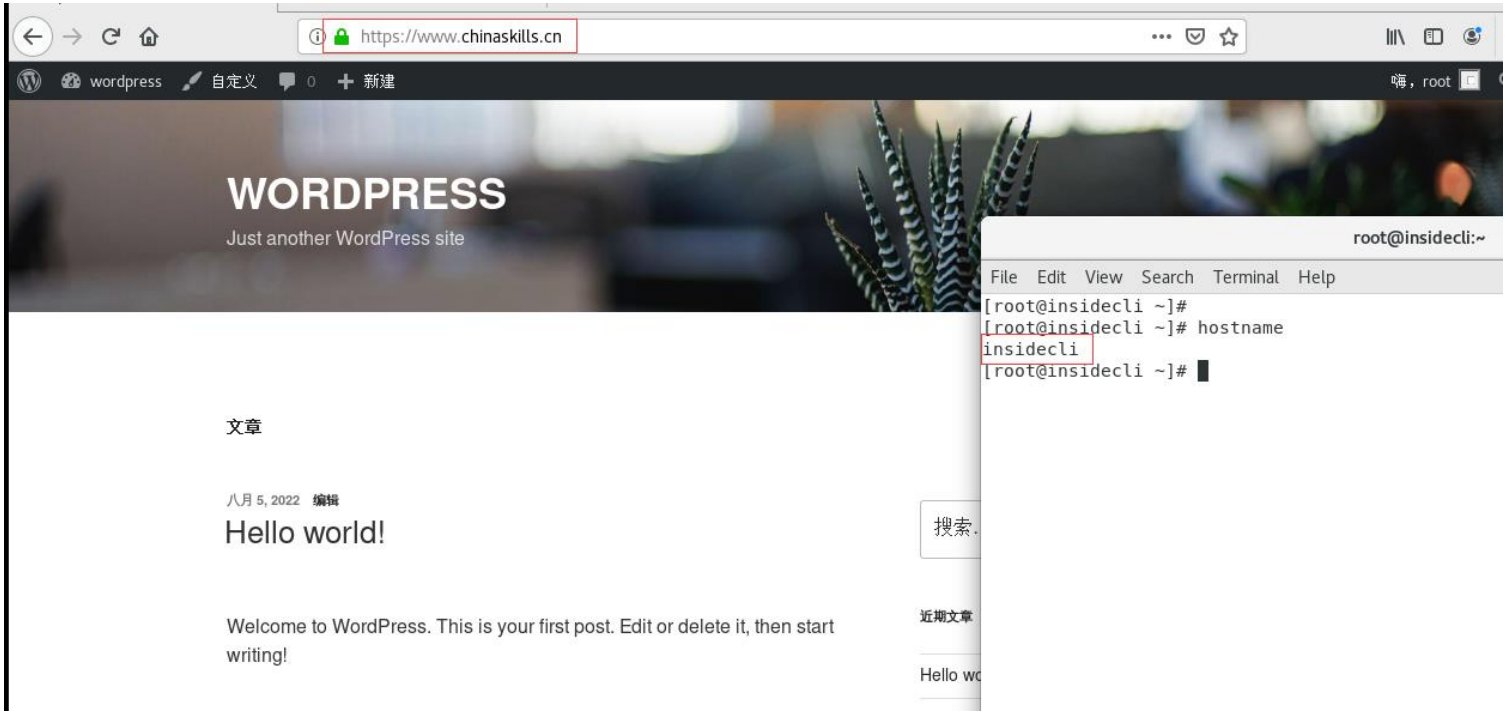
3、DNS：（4）内外网解析（在 outsidecli 上进入 nslookup 视图解析 www.chinaskills.cn）；【2 分】	2 分	
（评分要点：在 outsidecli 进入 nslookup 视图解析 www.chinaskills.cn 域名，结果为 81.6.63.254。）  		
3、DNS：（5）上游 DNS 设置（在 insidecli 上进入 nslookup 视图解析 host1.test1.com）；【2 分】	2 分	
（评分要点：，均显示 Non-authoritative answer，并解析到 81.6.63.100 的地址。）  		
3、DNS：（6）隐藏 DNS 版本（在 insidecli 上执行 nslookup -q=txt -class=CHAOS version.bind 192.168.100.100）；【2 分】	2 分	
（评分要点：版本显示 unknow）		

<table>
<tr><td> 
</td><td></td><td></td></tr>
<tr><td>4、httpd：（1）安装 apache2（执行指令：systemctl status httpd）；【1 分】</td><td>1 分</td><td></td></tr>
<tr><td>（评分要点：httpd 服务征程运行“active（running）”）
 
</td><td></td><td></td></tr>
<tr><td>4、httpd：（2）网站根目录（在 appsrv 上执行指令：cat /etc/fstab | grep webdata；然后使用 vim 查看 wordpress 站点的 wp-config.php 配置内容）；【5 分】</td><td>5 分</td><td></td></tr>
<tr><td>（评分要点：cat /etc/fstab | grep webdata 能看到挂载源为 192.168.100.200:/webdata，挂载点为 /webdata 得 2 分；wordpress 配置文件每个标记点匹配得 1 分）
 
</td><td></td><td></td></tr>
</table>

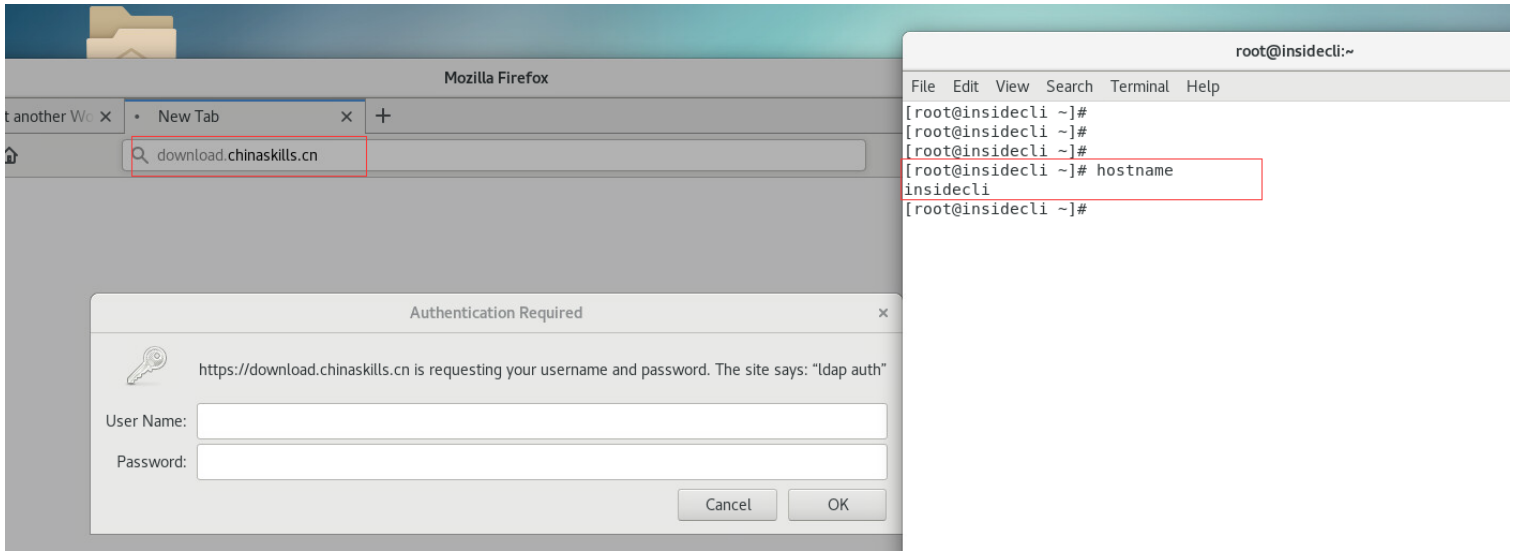
```
*/

// ** MySQL ■ ■  - ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ** //
/** WordPress■ ■ ■ ■ ■ ■  */
define('DB_NAME', 'wordpress');

/** MySQL■ ■ ■ ■ ■ ■  */
define('DB_USER', 'root');

/** MySQL■ ■ ■ ■ ■  */
define('DB_PASSWORD', 'root@123');

/** MySQL■ ■  */
define('DB_HOST', '192.168.100.200');

/** ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■  */
define('DB_CHARSET', 'utf8');

/** ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■  */
define('DB_COLLATE', '');
```

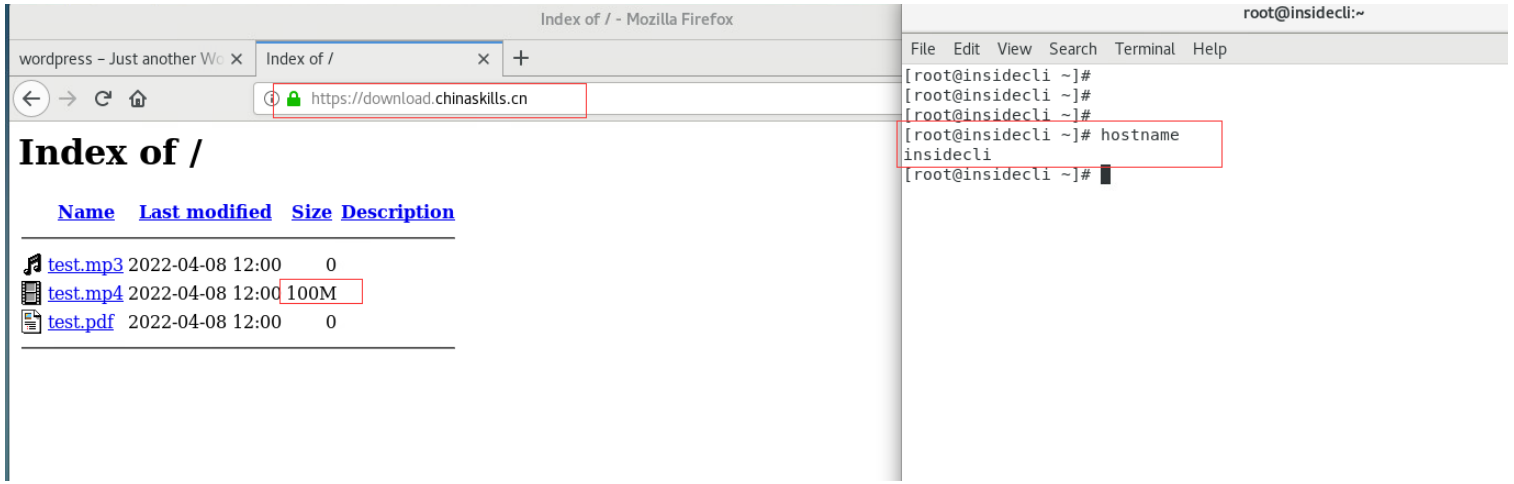
4、httpd：（3）运行用户（appsrv 上执行 id webuser && ps aux | grep webuser）；【2 分】	2 分	
（评分要点：在 appsrv 上执行：id webuser && ps aux | grep webuser，webuser 的 uid 需要小于 1000，大于 1000 不得分。显示 httpd 的进程由 webuser 运行。每个点 1 分）		

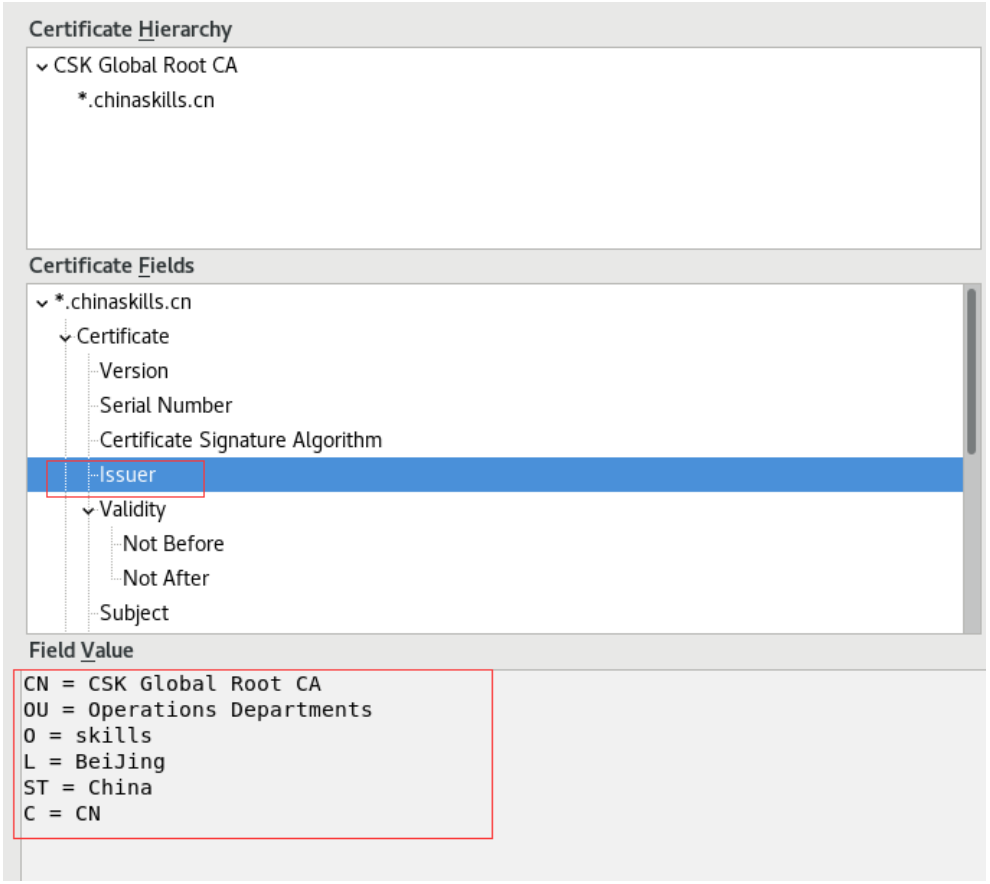
```
[root@appsrv ~]# id webuser && ps aux | grep webuser
uid=666(webuser) gid=1001(webuser) groups=1001(webuser)
webuser    96251  0.0  1.0 512180 10084 ?        S    09:41   0:00 /usr/sbin/httpd -DFOREGROUND
webuser    96252  0.0  2.0 527768 20828 ?        S    09:41   0:00 /usr/sbin/httpd -DFOREGROUND
webuser    96253  0.0  1.7 516892 16988 ?        S    09:41   0:00 /usr/sbin/httpd -DFOREGROUND
webuser    96254  0.0  1.0 512180 10080 ?        S    09:41   0:00 /usr/sbin/httpd -DFOREGROUND
webuser    96255  0.0  1.0 512180 10080 ?        S    09:41   0:00 /usr/sbin/httpd -DFOREGROUND
webuser    96287  0.0  0.9 512180  9576 ?        S    09:42   0:00 /usr/sbin/httpd -DFOREGROUND
webuser    96296  0.0  0.8 512040  8328 ?        S    09:42   0:00 /usr/sbin/httpd -DFOREGROUND
webuser    96297  0.0  0.8 512040  8328 ?        S    09:42   0:00 /usr/sbin/httpd -DFOREGROUND
webuser    96298  0.0  0.8 512040  8328 ?        S    09:42   0:00 /usr/sbin/httpd -DFOREGROUND
webuser    96299  0.0  0.8 512040  8328 ?        S    09:42   0:00 /usr/sbin/httpd -DFOREGROUND
root       97439  0.0  0.0 112808   968 tty1     S+   10:04   0:00 grep --color=auto webuser
[root@appsrv ~]#
```

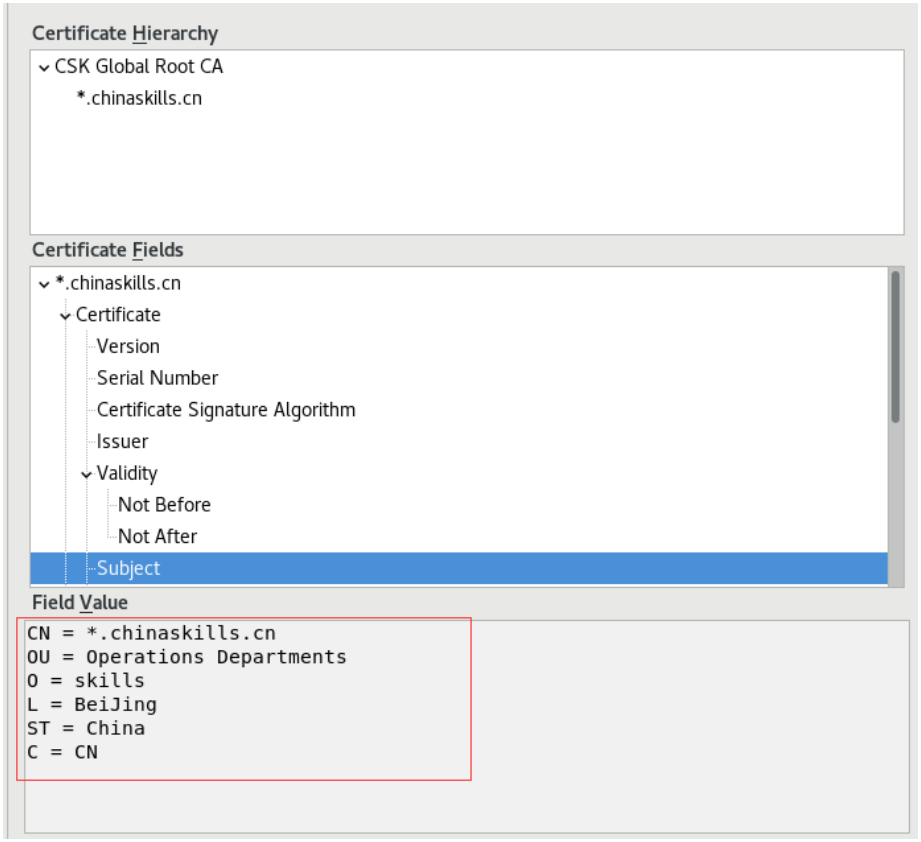
4、httpd：（4）限制内存（在 appsrv 上执行：cat /etc/systemd/system/multi-user.target.wants/httpd.service | grep memory）；【2 分】	2 分	
（评分要点：，存在下图标记的配置即可得分） 		
4、httpd：（5）www 网页内容（在 insidecli 上使用浏览器访问 www.chinaskills.cn 站点，打开终端输入 hostname 后，一起截图）；【4 分】	4 分	
（评分要点：显示出 wordpress 主页面，得 4 分；URL 中小锁必须为绿色，不为绿色本题都不得分，如果不携带 hostname 或者 hostname 不是 insidecli 扣 2 分） 		
4、httpd：（6）download 网站身份认证及网站内容【4 分】	4 分	
（评分要点：（1）在 insidecli 上输入 download.chinaskills.cn 网址，弹出输出用户名和密码框；【1 分】（2）输入		

LDAP 上设置的三个用户中的一个 zsuser/ lsusr/ wuusr 和相应的密码，成功登录该网站；【1 分】（3）download 站点页面列出目录文件，存在 test.mp3\test.mp4\test.pdf 文件，其它多余文件不作判断；【1 分】且 test.mp4 文件大小为 100M。【1 分】注意 download 页面也要有一个绿色的锁，没有的话本题不得分。如果不携带 hostname 或者 hostname 不是 insidecli 扣 2 分）

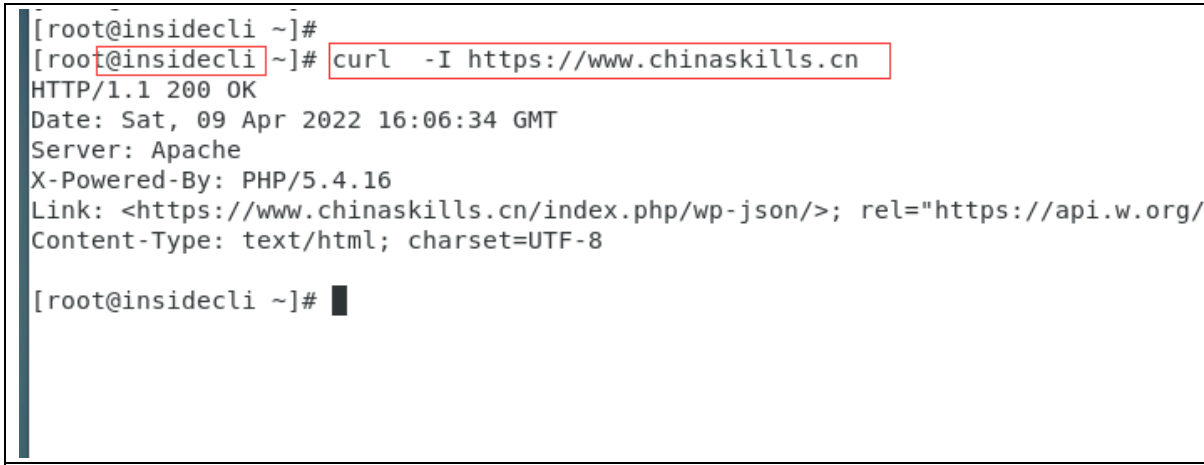


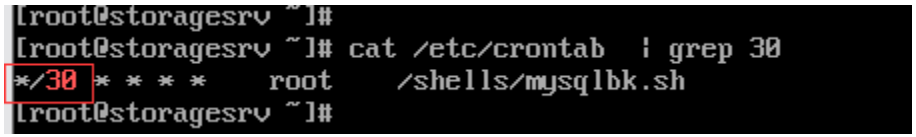
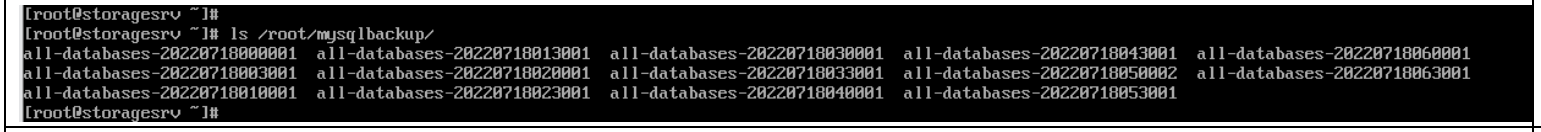


4、httpd：（7）证书信息；【4 分】	4 分	
（评分要点：在 insidecli 上使用浏览器访问 www.chinaskills.cn 站点后，打开证书，查看证书使用者信息。，证书使用者信息需要严格匹配。两个证书的信息和下图中标记严格匹配即可。每个证书匹配得 2 分，共 4 分）  		

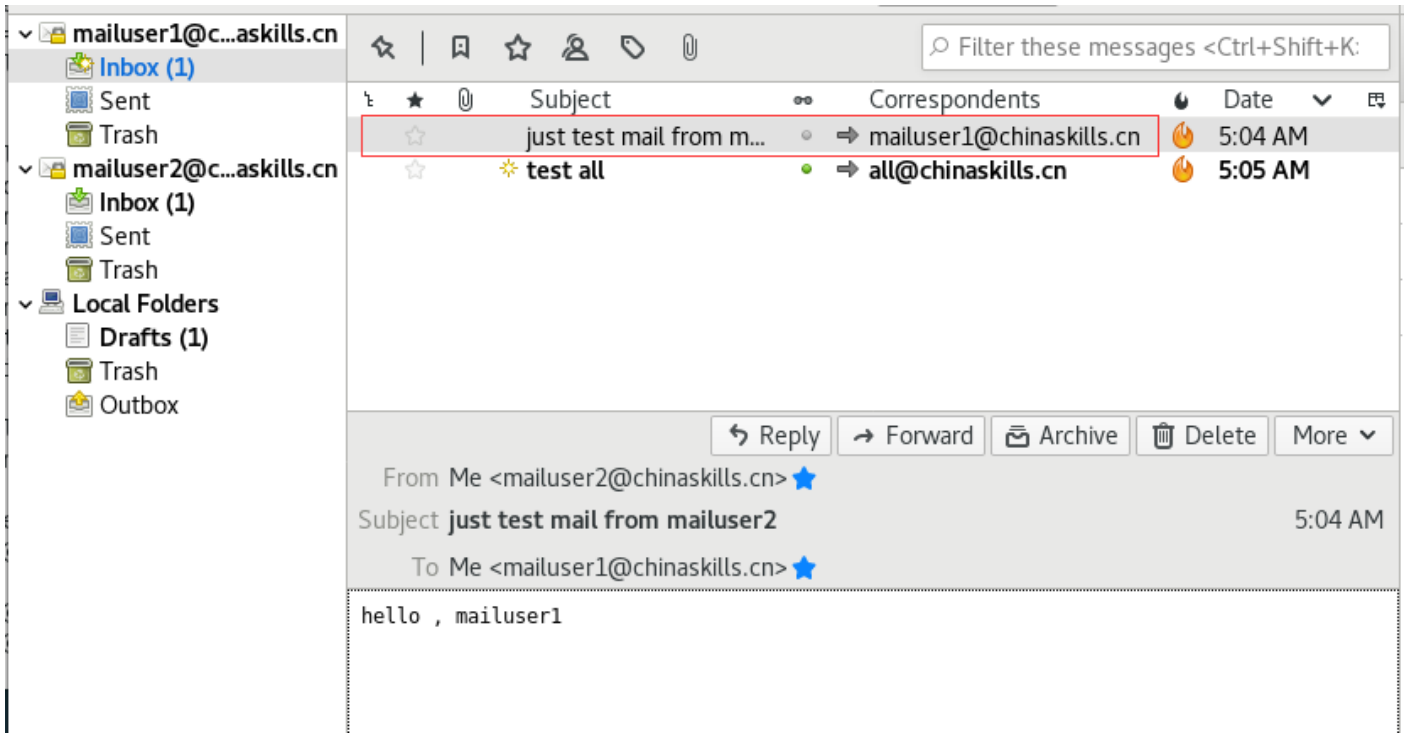


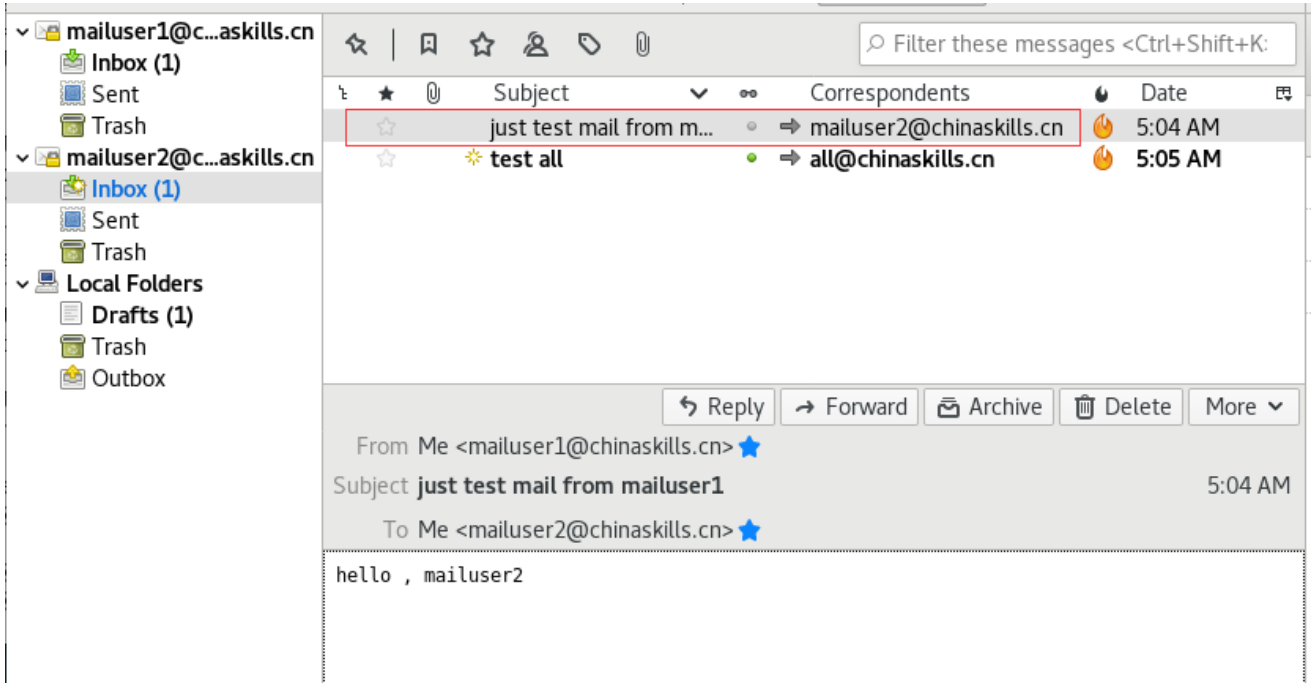
4、httpd：（8）无证书警告（在 insidecli 上执行：curl -I https://www.chinaskills.cn）；**【2 分】**	2 分	
（评分要点：curl 指令不允许使用-k 参数，访问 https 站点不提示任何的证书提示信息）		

		
4、httpd：（9）http 跳转 https（在 insidecli 上执行：curl -I http://www.chinaskills.cn）；**【2 分】**	2 分	
（评分要点：能看到 Location：https://www.chinaskills.cn） 		
4、httpd：（9）不显示非安全系统信息;【1 分】	1 分	
（评分要点：download 站点的任何页面不存在任何的系统版本以及 web 服务器的版本信息）		

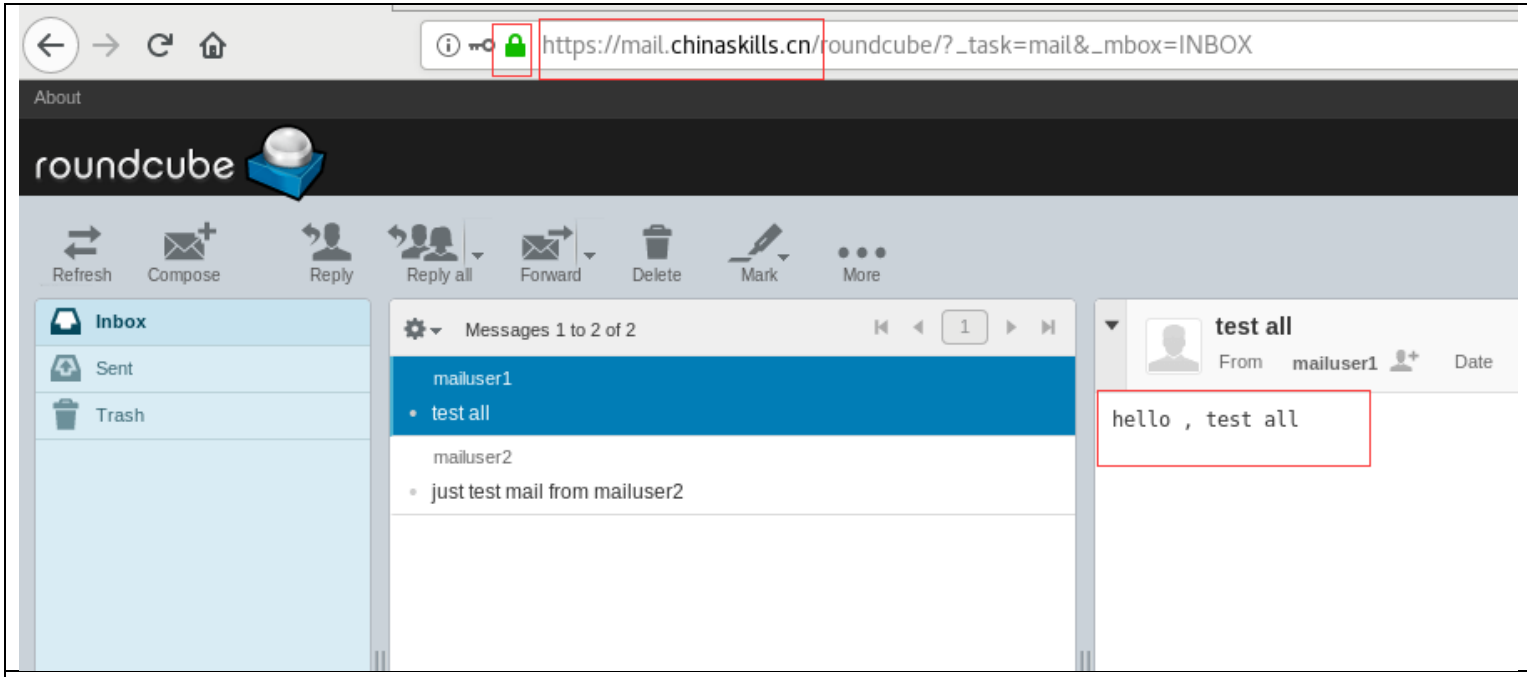
5、数据库备份:（1）测试数据库备份脚本（使用 vim 查看数据库脚本的编写）；【2 分】	2 分	
（评分要点：能看到 mysqldump 关键字 和 --all-databases 即可得分。） 		
5、数据库备份:（2）查看定时任务（执行命令 cat /etc/crontab | grep 30）；【2 分】	2 分	
（评分要点:能看到第一个* 为 */30 即可） 		
5、数据库备份:（3）查看备份文件(执行命令 ls /root/mysqlbackup)；【1 分】	1 分	
（评分要点：只要存在文件名为 all-databases-年月日，精确到秒即可得分。） 		
6、MAIL：（1）启用 IMAPS 和 SMTPS，禁止非安全 IMAP\SMTP(在 appsrv 上执行指令：ss -nltp | grep -E	2 分	

“master|dovecot”，）；【2 分】		
（评分要点：监听端口在仅允许 465 和 993 端口，出现其他端口不得分） 		
6、MAIL：（2）邮件用户（通过 postfixadmin 的网页查看 appsrv 上的虚拟用户）；【4 分】	4 分	
（评分要点：通过 postfixadmin 查看 appsrv 上的虚拟用户，邮箱数为 99 即可得分） 		
6、MAIL：（3）测试邮件（在 insidecli 上使用 thunderbird 登录邮箱客户端，从 mailuser1 和 mailuser2 分别向对方发送邮件）；【6 分】	6 分	
（评分要点：在 insidecli 上使用 thunderbird 登录邮箱客户端，从 mailuser1 和 mailuser2 分别向对方发送邮件，收件箱中查看邮件接收成功）		


mailuser1@c...askills.cn
Inbox (1)
Sent
Trash
mailuser2@c...askills.cn
Inbox (1)
Sent
Trash
Local Folders
Drafts (1)
Trash
Outbox
Filter these messages <Ctrl+Shift+K:
Subject
Correspondents
Date
just test mail from m...
mailuser1@chinaskills.cn
5:04 AM
test all
all@chinaskills.cn
5:05 AM
Reply
Forward
Archive
Delete
More
From Me <mailuser2@chinaskills.cn>
Subject just test mail from mailuser2
5:04 AM
To Me <mailuser1@chinaskills.cn>
hello , mailuser1



6、MAIL：（4）广播邮件（insidecli 通过网页查看广播邮箱，使用 mailuser1 用户登录）；【4 分】	4 分	
（评分要点：通过网页查看广播邮箱，使用 mailuser1 用户登录，网页有绿色的小锁，而且能查看到广播邮箱）		

		
7、CA：根证书路径和根证书信息（在 appsrv 上执行指令：openssl x509 -text -in /csk-rootca/csk-ca.pem -noout | grep Subject）；【5 分】	5 分	
（评分要点：在 appsrv 上执行指令：openssl x509 -text -in /csk-rootca/csk-ca.pem -noout | grep Subject，6 个信息点都对才能得分） [root@appsrv ~]# [root@appsrv ~]# openssl x509 -text -in /csk-rootca/csk-ca.pem -noout | grep Subject Subject: C=CN, ST=China, L=BeiJing, O=skills, OU=Operations Departments, CN=CSK Global Root CA Subject Public Key Info: X509v3 Subject Key Identifier: [root@appsrv ~]#		
8、网桥 VXLAN 服务：（1）查看 appsrv 和 storagesrv 上的 vxlan 网桥（分别在 appsrv 和 storagesrv 执行 brctl show）；【每个 4 分，共 8 分】	8 分	
（评分要点：能看到网桥为 br-vxlan，接口为 vxlan10）		

<table>
<tr><td>

```
[root@appsrv ~]#
[root@appsrv ~]# brctl  show
bridge name     bridge id               STP enabled     interfaces
br-vxlan                8000.367d7c4a6a06       no              vxlan10
[root@appsrv ~]#
```

```
[root@storagesrv ~]# brctl  show
bridge name     bridge id               STP enabled     interfaces
br-vxlan                8000.ca75a8dab82a       no              vxlan10
[root@storagesrv ~]#
```

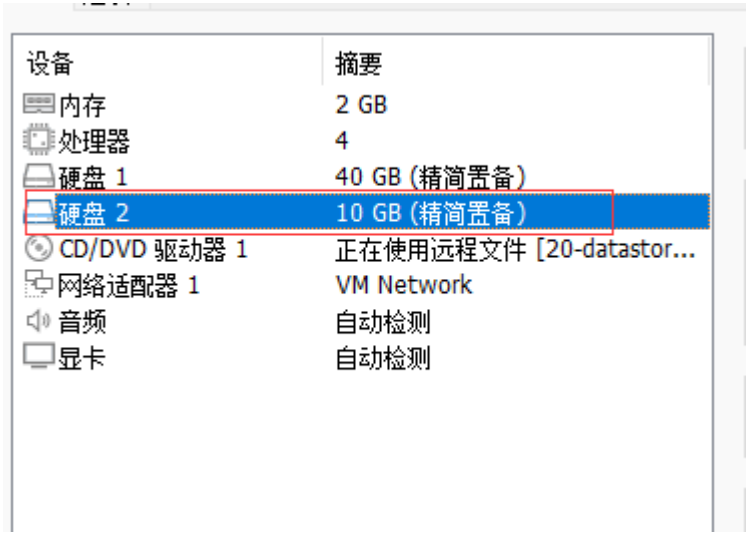
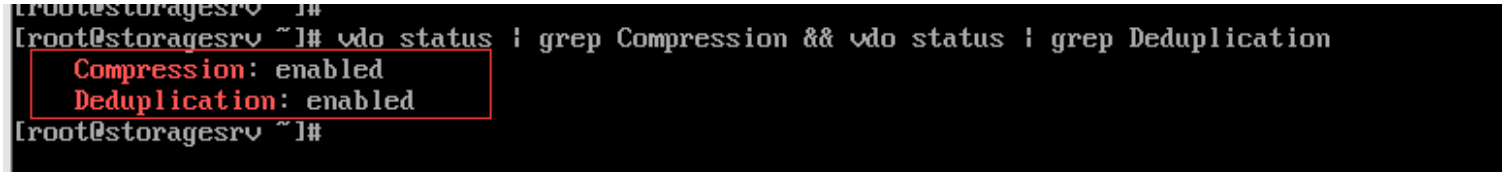
</td><td></td><td></td></tr>
<tr><td>8 网桥 VXLAN 服务：（2）appsrv 测试 vxlan 隧道连通性（使用 ping -I 172.16.1.1 172.16.1.2）；【2 分】</td><td>2 分</td><td></td></tr>
<tr><td>（评分要点：能够 ping 通即可）

```
[root@appsrv ~]#
[root@appsrv ~]# ping -I 172.16.1.1 172.16.1.2
PING 172.16.1.2 (172.16.1.2) from 172.16.1.1 : 56(84) bytes of data.
64 bytes from 172.16.1.2: icmp_seq=1 ttl=64 time=0.200 ms
64 bytes from 172.16.1.2: icmp_seq=2 ttl=64 time=0.163 ms
64 bytes from 172.16.1.2: icmp_seq=3 ttl=64 time=0.178 ms
^C
--- 172.16.1.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.163/0.180/0.200/0.018 ms
[root@appsrv ~]#
```

</td><td></td><td></td></tr>
</table>

STORAGESRV 工作任务（80 分）

评分要点	分值	评分
1、（1）磁盘管理：查看新加磁盘（右击虚拟机属性查看）；【1 分】	1 分	
（评分要点：看到一块大小为 10G 的硬盘即可）		

<table>
<tr><td> 
</td><td></td><td></td></tr>
<tr><td>1、磁盘管理：（2）查看 vdo 重删和压缩（vdo status | grep Compression && vdo status | grep Deduplication）；【2 分】</td><td>2 分</td><td></td></tr>
<tr><td>（评分要点：能看到压缩和重删 都是 enable 即可，每个 1 分）
 
</td><td></td><td></td></tr>
<tr><td>1、磁盘管理：（3）查看挂载（在 storagesrv 上执行指令：df -Th）；【3 分】</td><td>3 分</td><td></td></tr>
<tr><td>（评分要点：看到文件系统是 ext4，大小为 148G（150G 左右即可），挂载点为/vdodata；每个 1 分）</td><td></td><td></td></tr>
</table>

```
[root@storagesrv dev]#
[root@storagesrv dev]# df -Th
Filesystem                Type      Size  Used Avail Use% Mounted on
devtmpfs                  devtmpfs  894M     0  894M   0% /dev
tmpfs                     tmpfs     910M     0  910M   0% /dev/shm
tmpfs                     tmpfs     910M   10M  900M   2% /run
tmpfs                     tmpfs     910M     0  910M   0% /sys/fs/cgroup
/dev/mapper/centos-root   xfs        39G  4.9G   34G  13% /
/dev/sr0                  iso9660   9.5G  9.5G     0 100% /mnt/cdrom
/dev/mapper/centos-home   xfs        19G   37M   19G   1% /home
/dev/sda1                 xfs      1014M  185M  830M  19% /boot
tmpfs                     tmpfs     182M     0  182M   0% /run/user/0
/dev/mapper/snapvg-snapsrc ext4      4.8G   20M  4.6G   1% /snap
/dev/mapper/vdodisk       ext4      148G   61M  140G   1% /vdodata
[root@storagesrv dev]#
[root@storagesrv dev]#
```

2、SSH：（1）查看 SSH 服务（在 storagesrv 上执行指令：systemctl status sshd）；【1 分】 | 1 分

（评分要点：状态为 running 即可得分）

```
[root@storagesrv ~]#
[root@storagesrv ~]# systemctl  status  sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2022-04-09 11:16:26 EDT; 22s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 23536 (sshd)
   CGroup: /system.slice/sshd.service
           └─23536 /usr/sbin/sshd -D

Apr 09 11:16:26 storagesrv systemd[1]: Starting OpenSSH server daemon...
Apr 09 11:16:26 storagesrv sshd[23536]: Server listening on 0.0.0.0 port 3358.
Apr 09 11:16:26 storagesrv sshd[23536]: Server listening on :: port 3358.
Apr 09 11:16:26 storagesrv systemd[1]: Started OpenSSH server daemon.
```

2、SSH:（2）查看 ssh 端口监听(ss -ntpl | grep ssh)；【1 分】 | 1 分

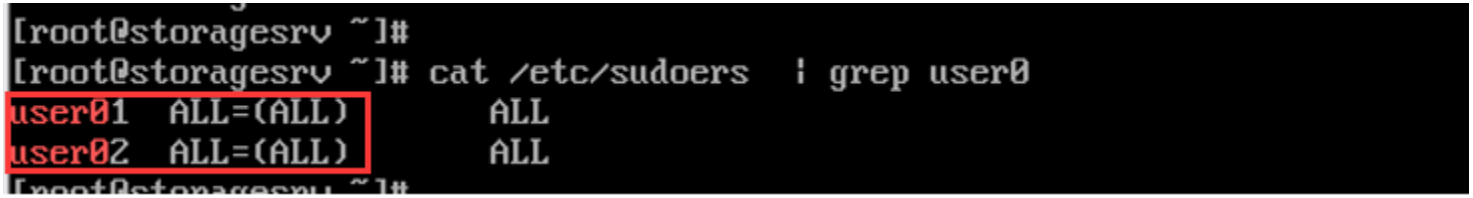
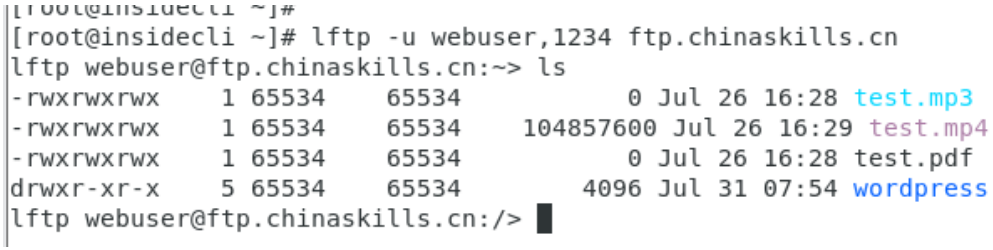
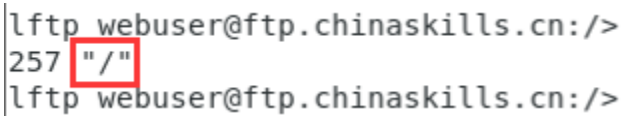
（评分要点：ssh 的监听端口是 2022 即可）

```
[root@storagesrv ~]# ss -ntpl | grep ssh
LISTEN     0      128          *:2022                     *:*                   users:(("sshd",pid=4
3072,fd=3))
LISTEN     0      128       [::]:2022                  [::]:*                   users:(("sshd",pid=4
3072,fd=4))
[root@storagesrv ~]#
```

2、SSH：（3）测试 ssh 用户访问（在 insidecli 上分别使用 user01、user02、root 用户通过 SSH 来登录 storagesrv）；【3 分】	3 分	
（评分要点：user01 和 user02 都可以正常登录，root 用户无法登录，失败提示 permission denied，失败三次后自动退出）		

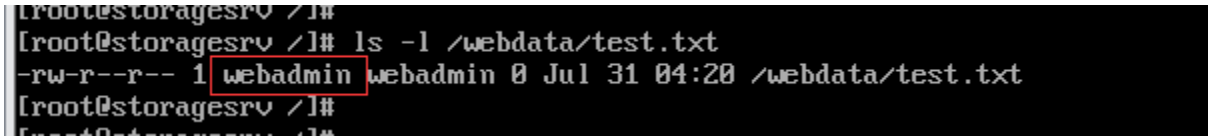
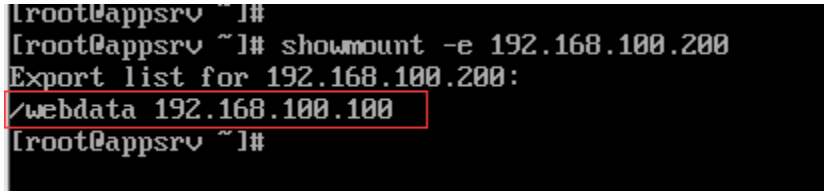
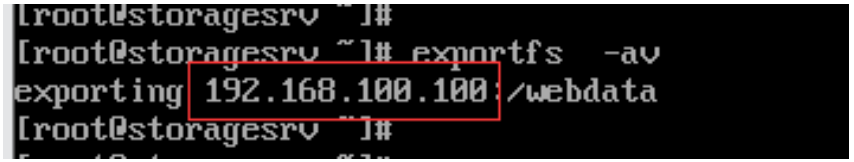
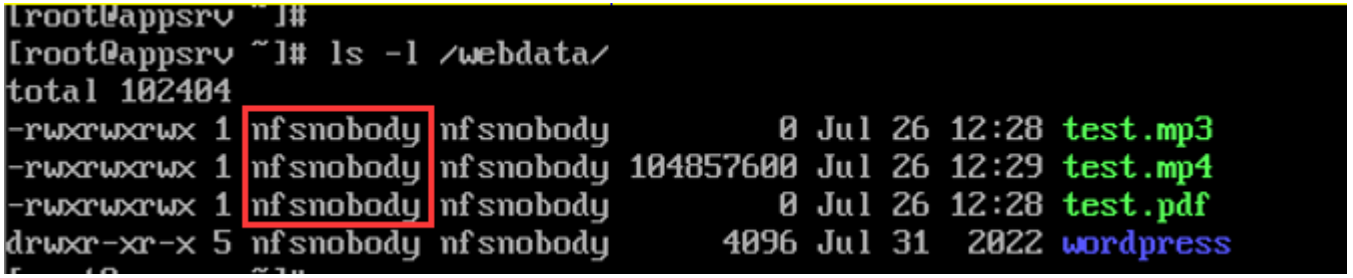
```
[root@insidecli ~]#
[root@insidecli ~]# ssh -p 3358 user01@192.168.100.200
user01@192.168.100.200's password:
Last failed login: Sat Apr  9 11:19:11 EDT 2022 from 192.168.0.190 on ssh:notty
There were 2 failed login attempts since the last successful login.
Last login: Sat Apr  9 11:15:08 2022
[user01@storagesrv ~]$ exit
logout
Connection to 192.168.100.200 closed.
[root@insidecli ~]# ssh -p 3358 user02@192.168.100.200
user02@192.168.100.200's password:
[user02@storagesrv ~]$ exit
logout
Connection to 192.168.100.200 closed.
[root@insidecli ~]# ssh -p 3358 root@192.168.100.200
root@192.168.100.200's password:
Permission denied, please try again.
root@192.168.100.200's password:
Permission denied, please try again.
root@192.168.100.200's password:
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@insidecli ~]#
```

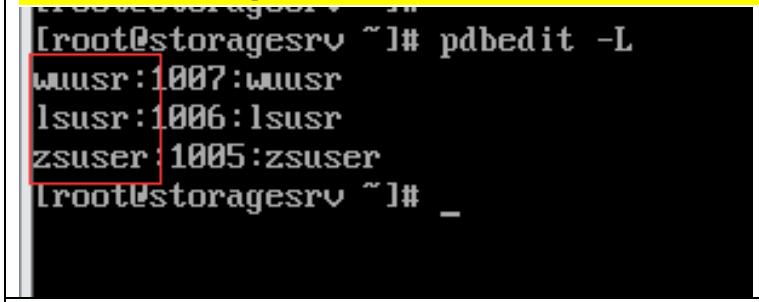
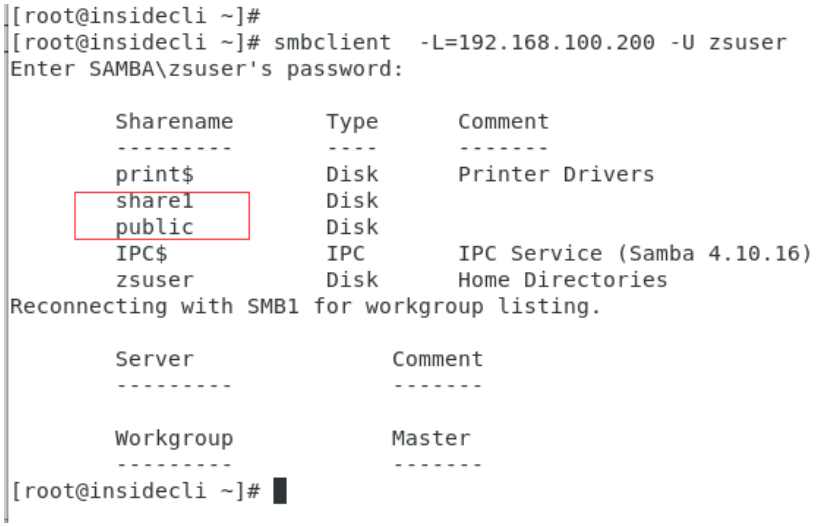
2、SSH：（4）查看 sudo 组用户（在 storagesrv 上执行指令：cat /etc/sudoers | grep user0）；【2 分】	2 分	
（评分标准：存在 user01 和 user02 对应的的信息即可得分，每个 1 分）		

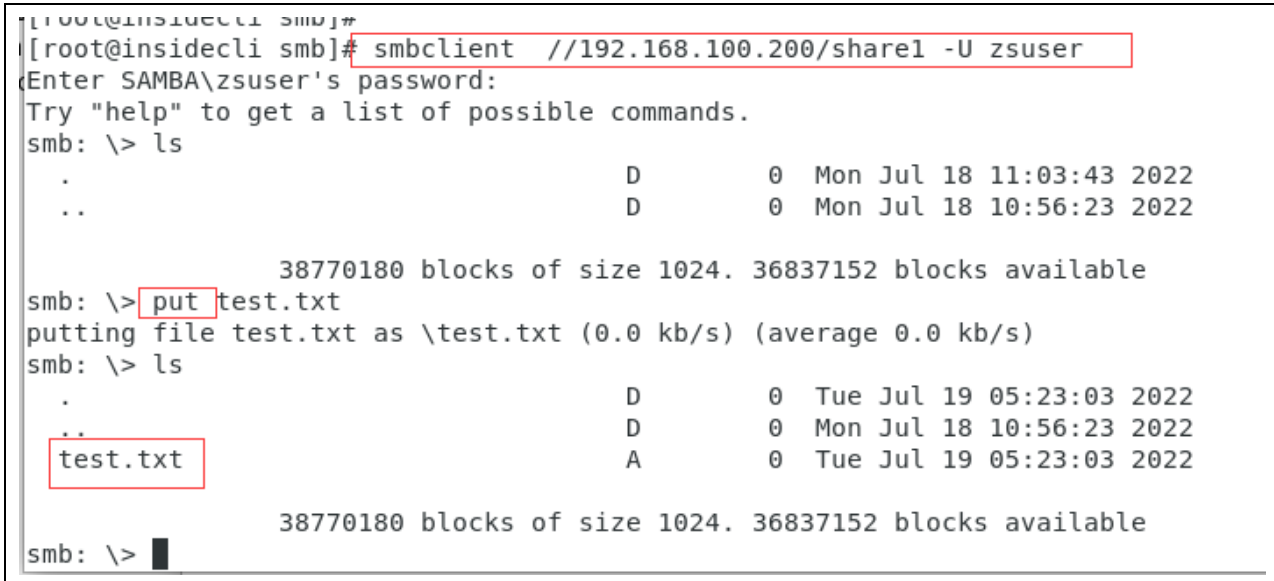
		
3、VSFTPD：（1）测试 ftps（insidecli 使用 lftp -u webuser,密码 ftp.chinaskills.cn 登录，然后使用 ls 截图）；【2 分】	2 分	
（评分要点：FTP 登陆后能够查看 文件内容，不报 SSL 错误即可） 		
3、VSFTPD：（2）quote pwd 查看 chroot；【2 分】	2 分	
（评分要点：显示为 “/”） 		
3、VSFTPD：（3）测试 ftp 文件上传权限(分别上传 test.doc,test.docx,test.xlsx,test.txt 文件,然后 ls)；【4 分】	4 分	
（评分要点：上传 test.doc、test.docx、test.xlsx 后缀文件会提示错误 550 代码，如果不是 550 错误则不得分，每个 1 分，【3 分】；上传 test.txt 成功，并且 ls 能够显示【1 分】）		

```
lftp webuser@ftp.chinaskills.cn:/> put test.doc
put: Access failed: 550 Permission denied. (test.doc)
lftp webuser@ftp.chinaskills.cn:/> put test.docx
put: Access failed: 550 Permission denied. (test.docx)
lftp webuser@ftp.chinaskills.cn:/>
lftp webuser@ftp.chinaskills.cn:/> put test.xlsx
put: Access failed: 550 Permission denied. (test.xlsx)
lftp webuser@ftp.chinaskills.cn:/>
lftp webuser@ftp.chinaskills.cn:/> put test.txt
lftp webuser@ftp.chinaskills.cn:/>
lftp webuser@ftp.chinaskills.cn:/> ls
-rwxrwxrwx    1 65534    65534           0 Jul 26 16:28 test.mp3
-rwxrwxrwx    1 65534    65534   104857600 Jul 26 16:29 test.mp4
-rwxrwxrwx    1 65534    65534           0 Jul 26 16:28 test.pdf
-rw-r--r--    1 1001     1001            0 Jul 31 08:20 test.txt
drwxr-xr-x    5 65534    65534        4096 Jul 31 07:54 wordpress
```

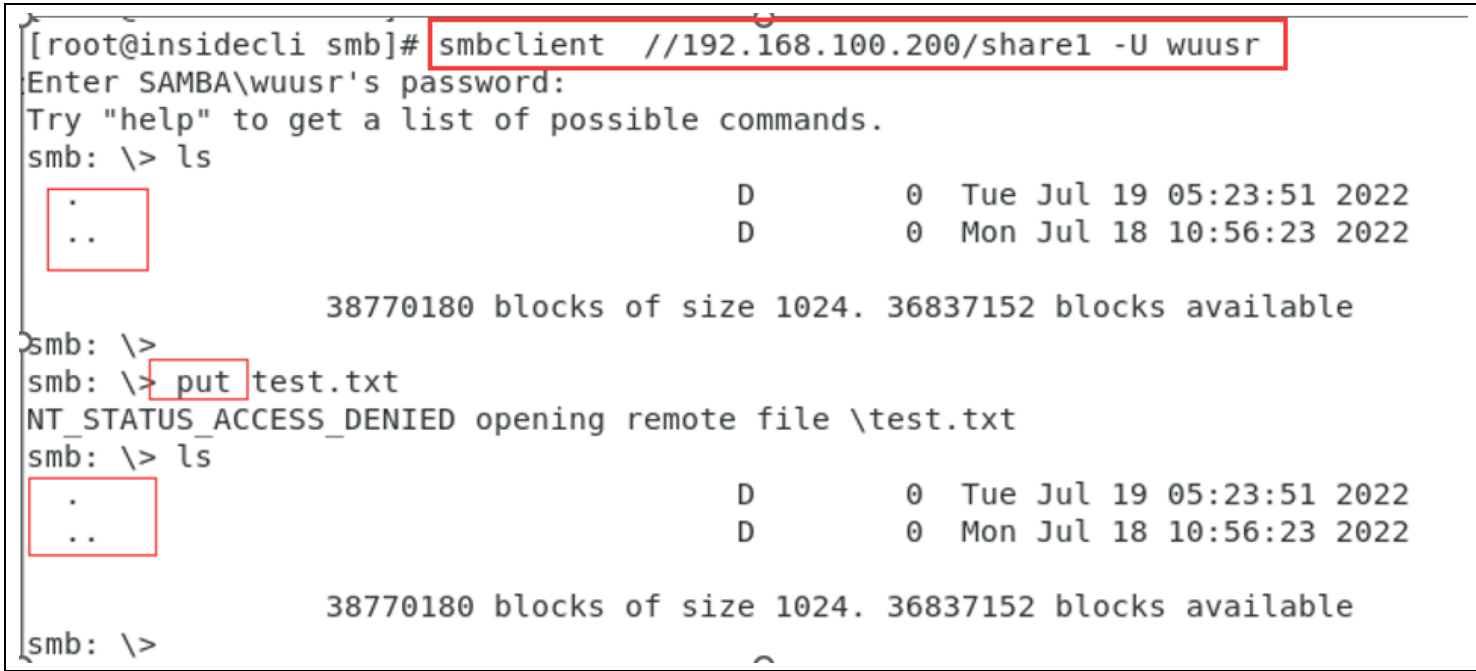
3、VSFTPD：（4）查看 vsftp 配置文件中限速限制的配置（在 storagesrv 上执行指令：cat /etc/vsftpd/vsftpd.conf|grep rate）；【1 分】	1 分	
（评分要点：显示出 local_max_rate=100000 即可，如果显示的是其它关键字则不得分。）		
3、VSFTPD：（5）测试 ftp 中同一个 IP 地址登录（insidecli 上通过 lftp -u webuser，密码 ftp.chinaskills.cn 打开三个终端，第三个终端执行 ls 命令后截图）【1 分】	1 分	
（评分要点：打开第三个终端输入 ls 后显示 delying before reconnect，显示其它不得分；）		
3、VSFTPD：（6）查看端口范围（截取配置文件中相关配置）；【2 分】	2 分	
（评分要点：和截图中配置信息一致即可得分）		
3、VSFTPD：（7）测试匿名用户（storagesrv 执行 ls -l /webdata/test.txt）；【3 分】	3 分	

（评分要点：之前上传的 test.txt 的文件所属者为 webadmin 即可得分） 		
4、NFS：（1）共享目录（在 appsrv 上执行指令：showmount -e 192.168.100.200）；【2 分】	2 分	
(评分要点：在 appsrv 上执行 showmount -e 192.168.100.200，存在/webdata 即可) 		
4、NFS：（2）仅允许 AppSrv 访问（在 storagesrv 上执行指令：exportfs -av）；【2 分】	2 分	
(评分要点：storagesrv 上执行 exportfs -av，能看到 192.168.100.100 的地址即可。) 		
4、NFS：（3）访问身份（在 appsrv 上执行指令：ls -l /webdata）；【3 分】	3 分	
（评分要点：在 appsrv 上执行 ls -l /webdata； test.mp3, test.mp4, test.pdf 得所有者都是 nfsnobody 即可得分，每个 1 分） 		

5、SAMBA：（1）samba 用户创建（在 storagesrv 上执行指令：pdbedit -L）；【3 分】	3 分	
（评分要点：通过 pdbedit -L 查询出存在 zsuser, lsusr, wuusr 用户，每个 1 分） 		
5、SAMBA：（2）文件共享（在 insidecli 执行指令：smbclient -L=192.168.100.200 -U zsuser）；【2 分】	2 分	
（评分要点：在 insidecli 上查询发布出来的目录(smbclient -L=192.168.100.200 -U zsuser)，，有 share1 和 public 即可得分，其它不做评判，每个 1 分） 		
5、SAMBA：（3）share1 目录的用户权限管理（使用 zsuser 测试；用户登录后先进行 ls，然后上传 test.txt;最后再进行 ls 之后在截图）；【1 分】	1 分	
（评分要点：zsuser 可以上传文件并成功查看）		



5、SAMBA：（4）share1 目录的用户权限管理（wuusr 测试；用户登录后先进行 ls，然后上传 test.txt;最后再进行 ls 之后在截图）；【1 分】	1 分	
（评分要点：wuusr 上传文件提示 access_denied，上传文件失败）		

		
5、SAMBA：（5）share1 目录的用户权限管理（lsusr 测试；用户登录后先进行 ls，然后上传 test.txt;最后再进行 ls 之后在截图）；【1 分】	1 分	
（评分要点：lsusr 上传文件提示 access_denied，上传文件失败）		

<table>
<tr>
<td>
<pre>
[root@insidecli smb]# smbclient //192.168.100.200/share1 -U lsusr
Enter SAMBA\lsusr's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .   D   0 Tue Jul 19 05:23:51 2022
  ..   D   0 Mon Jul 18 10:56:23 2022

                38770180 blocks of size 1024. 36837124 blocks available
smb: \> put test.txt
NT_STATUS_ACCESS_DENIED opening remote file \test.txt
smb: \> ls
  .   D   0 Tue Jul 19 05:23:51 2022
  ..   D   0 Mon Jul 18 10:56:23 2022

                38770180 blocks of size 1024. 36837124 blocks available
smb: \>
</pre>
</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5、SAMBA：（6）public 目录的用户权限管理（使用 smbclient //192.168.100.200/public -U anonymous，登录后上传 test.txt 进行测试）；【2 分】</td>
<td>2 分</td>
<td></td>
</tr>
<tr>
<td>（评分要点：anonymous 可以上传文件，通过 ls 也能查看到上传的文件）</td>
<td></td>
<td></td>
</tr>
</table>

```
[root@insidecli smb]# smbclient  //192.168.100.200/public -U anonymous
Enter SAMBA\anonymous's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Jul 19 05:22:38 2022
  ..                                  D        0  Mon Jul 18 10:56:23 2022

                38770180 blocks of size 1024. 36837144 blocks available
smb: \> put test.txt
putting file test.txt as \test.txt (0.0 kb/s) (average 0.0 kb/s)
smb: \> ls
  .                                   D        0  Tue Jul 19 05:25:25 2022
  ..                                  D        0  Mon Jul 18 10:56:23 2022
  test.txt                            A        0  Tue Jul 19 05:25:25 2022

                38770180 blocks of size 1024. 36837144 blocks available
smb: \>
```

**6、LDAP：（1）查询 LDAP 中的 chinaskills.cn 目录（在 storagesrv 上执行指令：ldapsearch -x -b “dc=chinaskills,dc=cn	grep “dn: dc”）；【3 分】**	3 分	

（评分要点：存在 dc=chinaskills, dc=cn 即可得分）
`[root@storagesrv ~]# ldapsearch  -x -b "dc=chinaskills,dc=cn" | grep "dn: dc"`
`dn: dc=chinaskills,dc=cn`
`[root@storagesrv ~]#`		

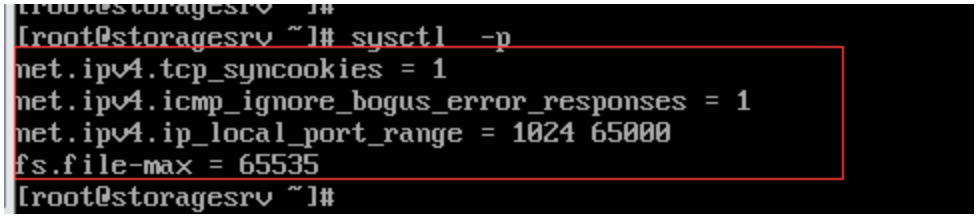
6、LDAP：（2）ldap 用户（在 storagesrv 上执行指令：ldapsearch -x -b “dc=chinaskills,dc=cn	grep “dn: uid”）；**【3 分】**	3 分	

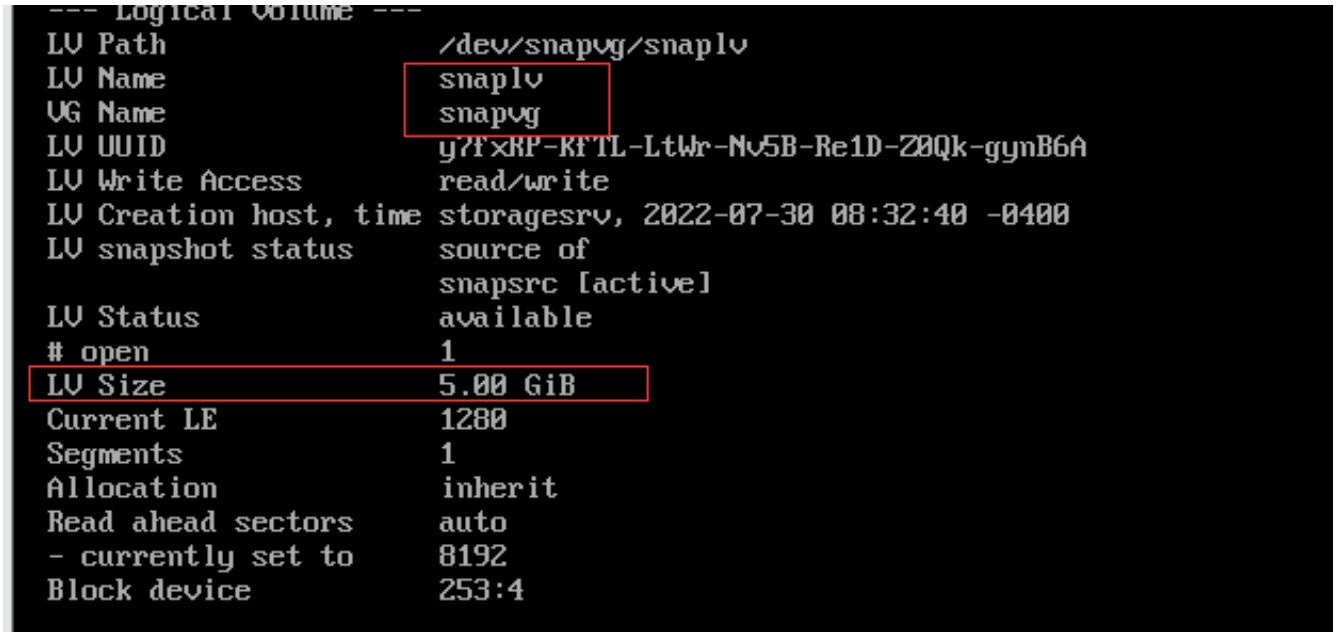
（评分要点：存在用户 zsuser，lsusr，wuusr 即可，每个用户 1 分）
`[root@storagesrv ~]# ldapsearch -x -b "dc=chinaskills,dc=cn" | grep "dn: uid"`
`dn: uid=zsuser,ou=users,dc=chinaskills,dc=cn`
`dn: uid=lsusr,ou=users,dc=chinaskills,dc=cn`
`dn: uid=wuusr,ou=users,dc=chinaskills,dc=cn`
`[root@storagesrv ~]#`		

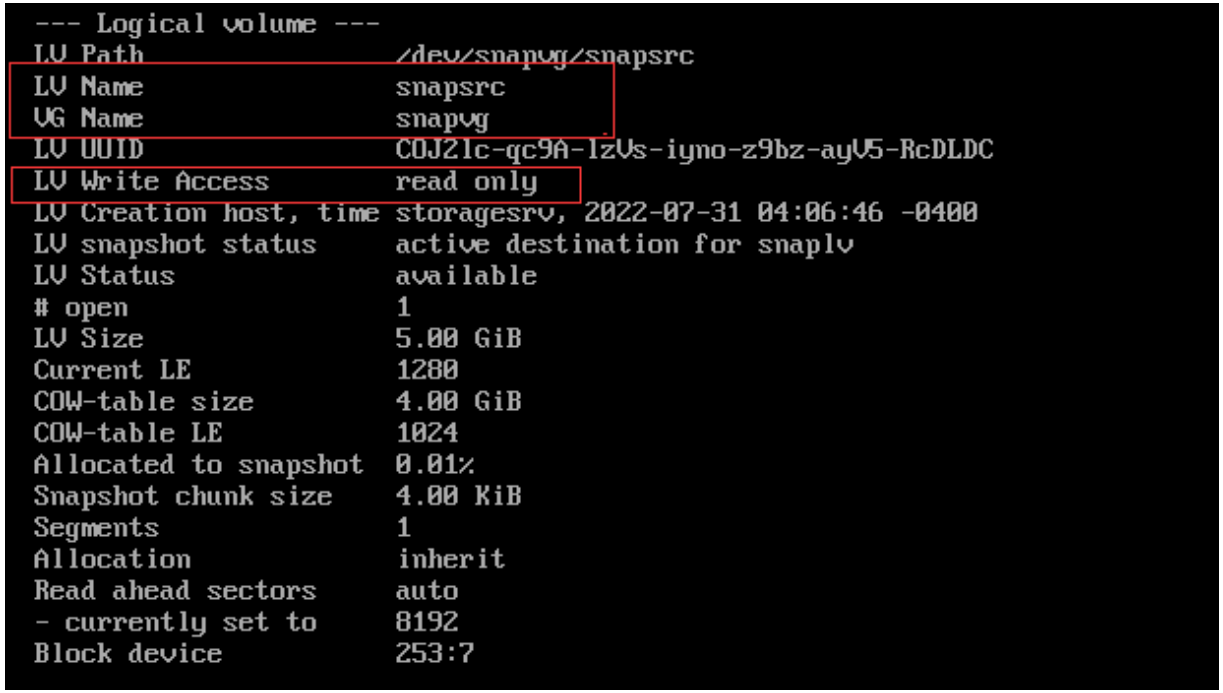
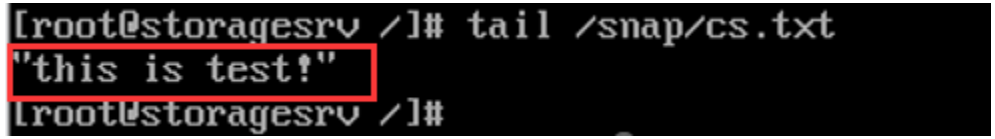
**6、LDAP：（3）ldap 用户组（storagesrv 执行指令：ldapsearch -x -b “dc=chinaskills,dc=cn	grep “dn: cn”）；【2 分】**	2 分	

（评分要点：存在 cn=ldsgp 的用户组即可得分） [root@storagesrv ~]# ldapsearch -x -b "dc=chinaskills,dc=cn" | grep "dn: cn" dn: cn=ldsgp,ou=users,dc=chinaskills,dc=cn [root@storagesrv ~]#		
7、Shell 脚本：（1）运行 userAdd.sh 脚本后截图（在 storagesrv 上执行指令 /shells/userAdd.sh lifei）；【1 分】	1 分	
（评分要点：运行 shell 脚本后，提示 adding new entry 即可） [root@storagesrv shells]# ./userAdd.sh lifei User lifei password set to none. adding new entry "uid=lifei,ou=users,dc=chinaskills,dc=cn"		
7、Shell 脚本：（2）查看 ldap 用户 lifei 的情况（在 storagesrv 上执行指令：ldapsearch -x -b “dc=chinaskills,dc=cn | grep “dn: uid=lifei”）；【2 分】	2 分	
（评分要点：存在 dn: uid=lifei 这一行信息即可得分） [root@storagesrv shells]# ldapsearch -x -b "dc=chinaskills,dc=cn" | grep "dn: uid=lifei" dn: uid=lifei,ou=users,dc=chinaskills,dc=cn [root@storagesrv shells]# _		
7、Shell 脚本：（3）查看 samba 用户（在 storagesrv 执行指令：pdbedit -L | grep lifei）；【2 分】	2 分	
（评分要点：存在 lifei 用户即可） [root@storagesrv ~]# pdbedit -L | grep lifei lifei:1008: [root@storagesrv ~]#		
8、Cockpit：（1）查看 cockpit 运行状态（systemctl status cockpit）；【1 分】	1 分	
（评分要点：看到服务状态为 running 即可）		

8、cockpit:（2）通过网页查看 cockpit 监测的服务器状态页面；【4 分】	4 分	
（评分要点：网页中能看到主机名是 storagesrv 即可）		

9、系统优化（在 storagesrv 上执行指令：sysctl -p）；【8 分】	8 分	
（评分要点：存在标记出信息即可，顺序不分先后，每个 2 分） 		

10、磁盘快照：（1）查看 snaplv 逻辑卷信息（lvdisply 截取 snaplv 相关信息）；**【3 分】**	3 分	
（评分要点：标记出匹配即可得分，每个 1 分）  		
10、磁盘快照：（2）查看 snapsrc（lvdisply 截取 snapsrc 相关信息）；【4 分】	4 分	
（评分要点：标记出匹配即可得分；read only 2 分，其它每点 1 分）		

		
10、磁盘快照：（3）测试磁盘快照（挂载快照后；执行 tail /snap/cs.txt）；【2 分】	2 分	
（评分要点:能够正常查看 cs.txt 的信息，内容为“this is test!”） 		

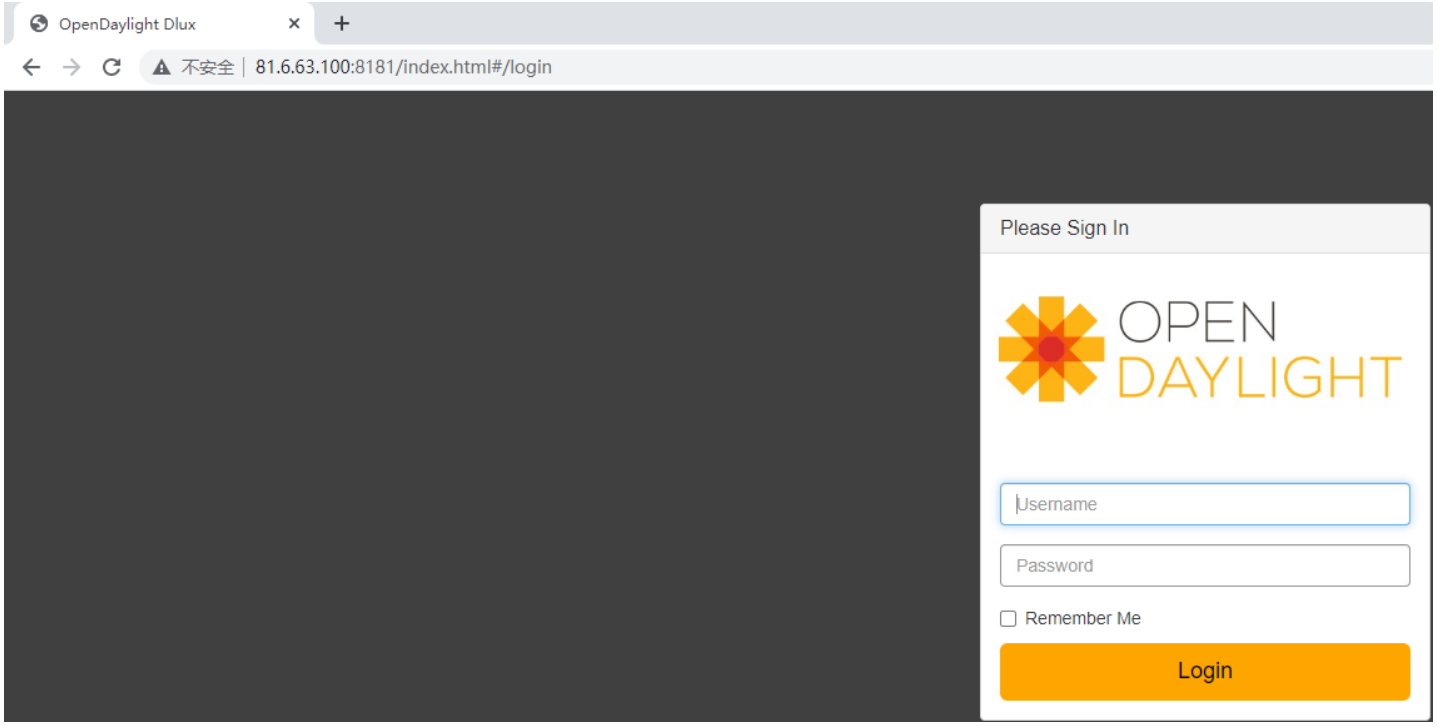
OUTSIDECLI & INSIDECLI 工作任务（2 分）

评分要点	分值	评分
1、基本配置：安装测试工具（在 outsidecli 或 insidecli 上执行指令（随便一个客户机即可）；whereis nslookup dig firefox curl ssh smbclient lftp ping）；【2 分】	2 分	

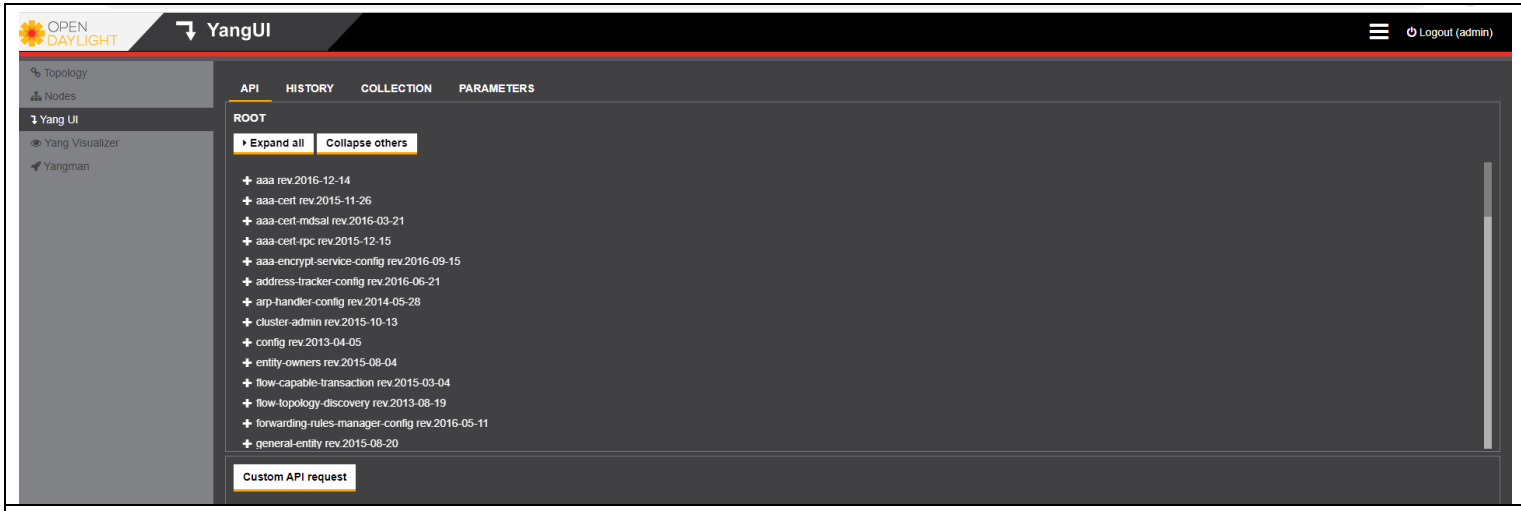
（评分要点：在 outsidecli 或 insidecli 上执行指令（任意一个客户端即可）：whereis nslookup dig firefox curl ssh smbclient lftp ping,所有指令均存在对应的路径信息，完全匹配得分） [root@insidecli ~]# whereis nslookup dig firefox curl ssh smbclient lftp ping nslookup: /usr/bin/nslookup /usr/share/man/man1/nslookup.1.gz dig: /usr/bin/dig /usr/share/man/man1/dig.1.gz firefox: /usr/bin/firefox /usr/lib/firefox /usr/lib64/firefox /etc/firefox /usr/share/man/man1/firefox.1.gz curl: /usr/bin/curl /usr/share/man/man1/curl.1.gz ssh: /usr/bin/ssh /etc/ssh /usr/share/man/man1/ssh.1.gz smbclient: /usr/bin/smbclient /usr/share/man/man1/smbclient.1.gz lftp: /usr/bin/lftp /usr/lib64/lftp /etc/lftp.conf /usr/share/man/man1/lftp.1.gz ping: /usr/bin/ping /usr/share/man/man8/ping.8.gz [root@insidecli ~]#		

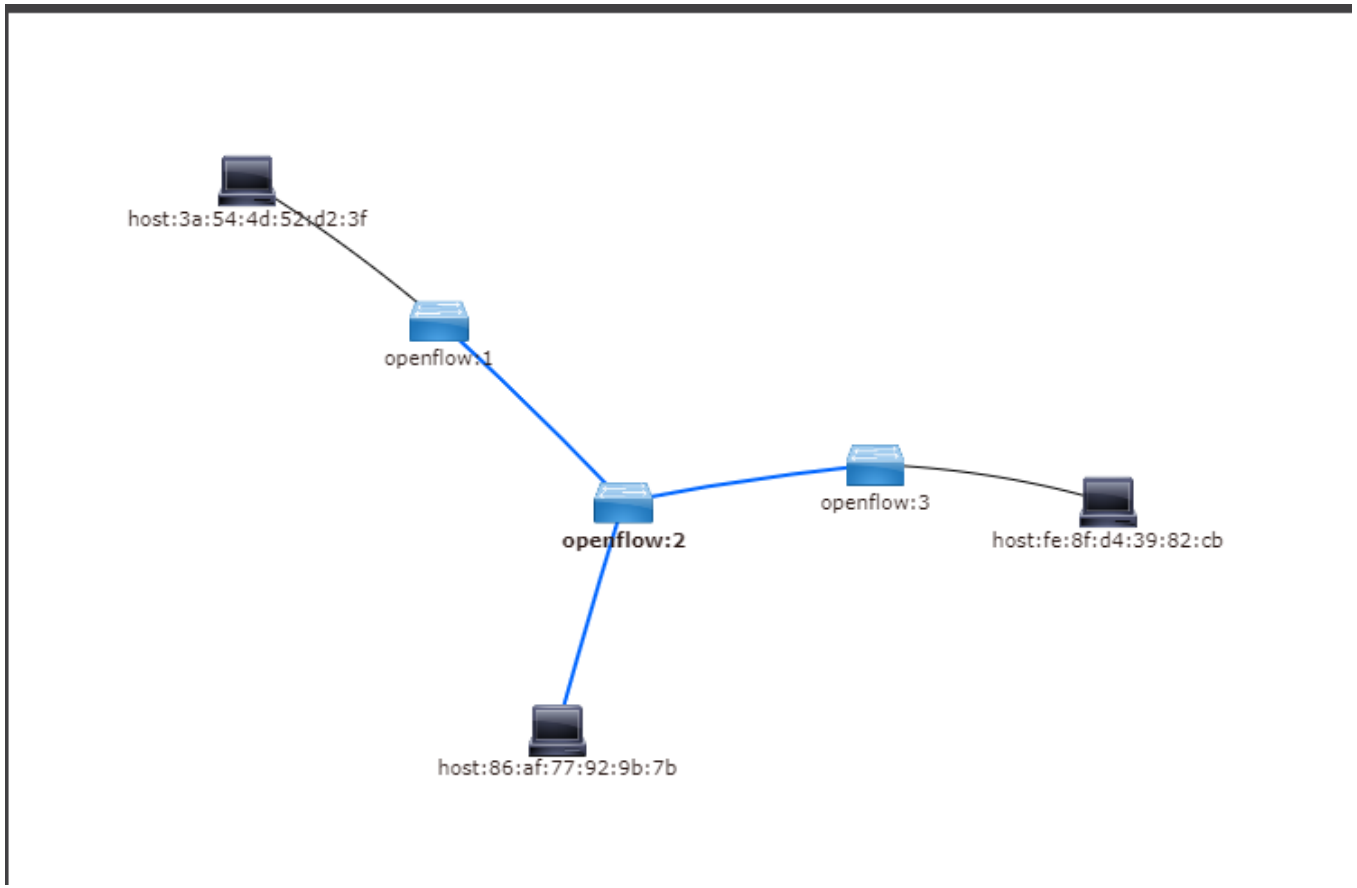
SDN 服务部署（35 分）

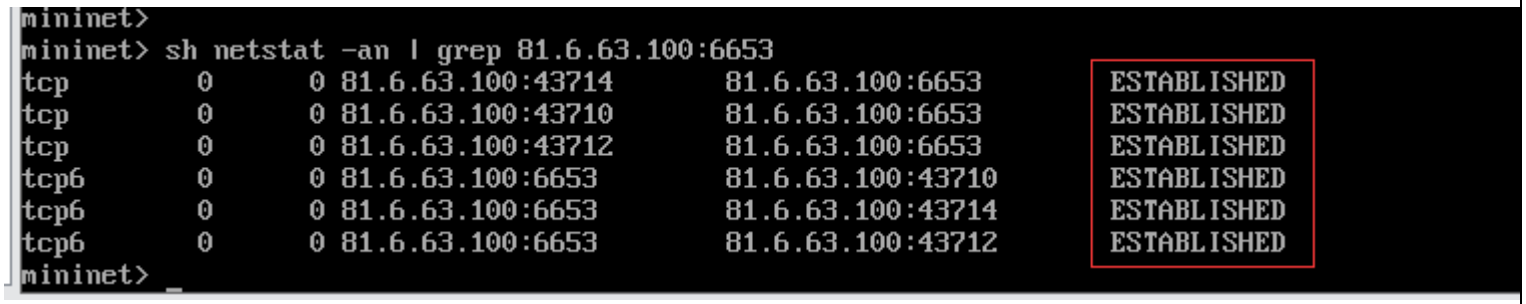
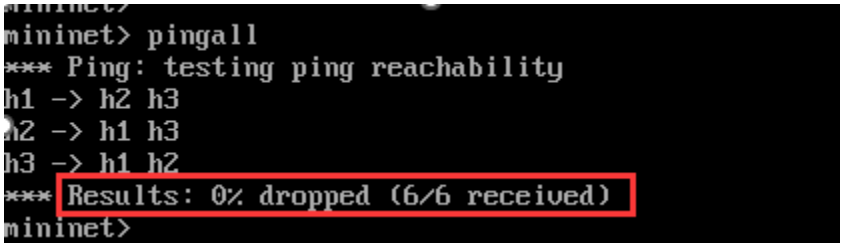
评分要点	分值	评分
在 ODL 主机上，opendaylight-user@root>输入：feature:list | grep odl-mdsal-apidocs 获取结果；【3 分】	3 分	
（评分要点：能看到一个 X 标记即可） opendaylight-user@root>feature:list | grep odl-mdsal-apidocs odl-mdsal-apidocs | 1.5.0-Carbon | x | odl-controller-1.5.0-Carbon | Op enDaylight :: MDSAL :: APIDOCS opendaylight-user@root>		
在 ODL 主机上，opendaylight-user@root>输入：feature:list | grep odl-l2switch-switch-ui 获取结果；【3 分】	3 分	
（评分要点：能看到一个 X 标记即可） opendaylight-user@root> opendaylight-user@root>feature:list | grep odl-l2switch-switch-ui odl-l2switch-switch-ui | 0.5.0-Carbon | x | l2switch-0.5.0-Carbon | Op enDaylight :: L2Switch :: Switch opendaylight-user@root>		
评分要点	分值	评分
谷歌浏览器访问 URL 地址，并通过默认账号进入管理界面，登录界面和通过默认账号进入管理界面分别截 1 张图；【6 分】	6 分	
（评分要点：能正常显示该页面即可，得 3 分）		

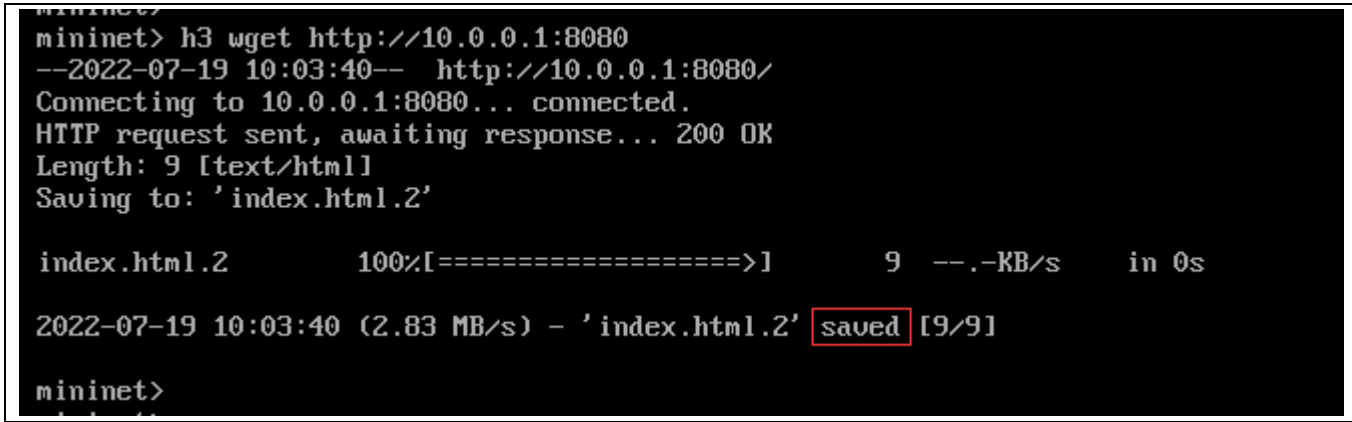


（评分要点：能正常显示该页面即可，得 3 分）

		
登录 ODL 管理界面，查看 topology 界面，截图拓扑示意图；【3 分】	3 分	

		
在 ODL 主机上通过 mininet> sh netstat -an |grep 81.6.63.100:6653 并截图 【5 分】	5 分	
（评分要点：存在 6 个 established 即可）		

		
通过 OVS 下发流表前，在 ODL 主机上的 mininet 模式下，执行 mininet> pingall 并截图获取主机直接 ping 测试；【5 分】	5 分	
（评分要点：能够全通即可） 		
通过 OVS 下发流表后，在 ODL 主机上的 mininet 模式下，执行 mininet> pingall 并截图获取主机之间的 ping 测试；【5 分】	5 分	
（评分要点：H1 只能和 H3 互通，其他都无法互通） 		
mininet> h3 wget http://10.0.0.1:8080【5 分】	5 分	
（评分要点：存在 saved 关键字即可得分）		


mininet> h3 wget http://10.0.0.1:8080
--2022-07-19 10:03:40-- http://10.0.0.1:8080/
Connecting to 10.0.0.1:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9 [text/html]
Saving to: 'index.html.2'
index.html.2   100%[===================>]   9 --.-KB/s   in 0s
2022-07-19 10:03:40 (2.83 MB/s) - 'index.html.2' saved [9/9]
mininet>