

作者@@老马

整理时间：2023-12

RHCSA考试

请查阅以下重要配置信息，以了解考试环境相关的信息。

考试时间3小时。

请注意，考试过程中不能与其他考生交流，您也不得连接到其他考生的主机，测验系统及其网络会受到监控，不当使用可导致成绩判为零分。

请执行下方列出的任务。在开始操作前，您不妨先通读整个列表。这些项目将使用一个分数来评分，这些任务的总分为 300 分，您必须达到 210 分或以上才能获得认证。

重要配置信息

在考试期间，除了您就坐位置的台式机之外，还将使用多个虚拟系统。您不具有台式机系统的 root 访问权，但具有对虚拟系统的完整 root 访问权。

系统信息

在本考试期间，您将操作下列虚拟系统：

系统	IP地址
servera.lab.example.com	172.25.250.10
serverb.lab.example.com	172.25.250.11

- 您使用的系统属于 DNS 域 `lab.example.com`。
- 该域中的所有系统都位于 `172.25.250.0/24` 子网中。
- 针对这些系统列出的 IP 地址是应该分配给系统的地址。您可能需要为一个或两个系统配置网络，以便能够通过上述地址访问您的地址。

帐户信息

- `servera` 的 `root` 已经设置为 `redhat`。
- 除非另有指定，否则这将是用于访问其他系统和服务的密码。
- 除非另有指定，否则应将该密码用于您创建的什么问题帐户或者需要设置密码的任意服务。

镜像仓库信息

- 仓库地址: `registry.lab.example.com`
- 登录信息:
 - 用户名: `admin`
 - 密码: `redhat321`

其他信息

- 您可以通过 SSH 或控制台访问考试系统（参见下文所述）。请注意，SSH 访问权可能取决于您解答其他考试项目的情况。
- 如果您需要在系统上安装其他软件，可以使用位于以下地址的存储库：
 - http://content.example.com/rhel9.0/x86_64/dvd/BaseOS
 - http://content.example.com/rhel9.0/x86_64/dvd/AppStream

重要评测信息

您的系统会在重新引导后进行评测：

- 因此务必确保您实施的的所有配置和服务在重新引导后仍然保留。
- 服务必须在没有人工干预的情况下启动。
- 本次考试使用的所有虚拟实例都必须能够重新引导至适当的多用户目标，而无需任何人工辅助。在无法引导或无法进行无人干预引导的系统上完成的所有操作都将为零分。

虚拟系统管理

考试期间，您可以随时关闭或重新引导虚拟机系统。您可以从虚拟系统本身进行这项操作，也可以从物理系统控制虚拟系统。要从物理系统访问或控制考试系统，单击桌面上 VM 控制台图标。这会显示一个表格，包含每个虚拟机系统的对应按钮，单击特定虚拟机系统的按钮将弹出一个菜单，包含用来控制该系统的选项：

- **启动节点VM**：如果指定的虚拟系统未在运行，该选项将启动指定系统。如果系统已经在运行-则该选项无任何作用。
- **重新引导节点VM**：正常关闭考试虚拟系统，然后重启。
- **关闭节点VM**：正常关闭指定虚拟系统。
- **关闭节点VM电源**：立即关闭指定虚拟系统。
- **控制台**：这将打开一个窗口，用于连接到指定虚拟系统的控制台。请注意，如果将焦点移动到此窗口，控制台将抓住您的鼠标。要恢复鼠标，同时键入 Ctrl+Alt。

- **重建节点VM**：将当前VM还原为原始状态。系统将弹出一个单独的窗口，要求您确认操作。
警告!!! 您在VM上完成的所有操作都将丢失。仅当系统无法使用时才应使用这个功能。在使用这个功能之前，确保关闭VM。

答题小技巧

1. 仔细检查鼠标和键盘，特别是鼠标右键和中间。
2. 尽可能使用tab键补全。
3. 考试过程中用到的名称、路径等字符串，使用复制粘贴。
4. 保持终端清洁，每做完一个题目，执行clear命令或使用快捷键CTRL+L清屏。
5. 根据需要，打开多个终端，例如查看帮助。

练习环境准备

将文件 `rhcsa9_prepare.sh`、`rhcsa9-exam200.zip` 上传到foundation0上root用户家目录，然后执行以下命令：

```
1 [root@foundation0 ~]# chmod +x rhcsa9_prepare.sh
2 [root@foundation0 ~]# /root/rhcsa9_prepare.sh
3 Reset all VMs:
4   wait for classroom running ..... DONE
5   wait for bastion running ..... DONE
6   wait for workstation running ..... DONE
7   wait for utility running ..... DONE
8   wait for servera running ..... DONE
9   wait for serverb running ..... DONE
10 Prepare foundation ..... DONE
11 Prepare classroom ..... DONE
12 Prepare servera ..... DONE
13 Prepare serverb ..... DONE
14 Check exam environment ..... DONE
15
16 -----
17     按 Super 键，搜索 EXAM，打开试题，按回车键开始答题
18 -----
```

脚本执行完成后开始做题。

练习题

开始之前

考试时，主机 `servera` 和 `serverb` 的 `root` 账户不能远程登录。

解除方法如下，以 `servera` 为例：

```
1 ## 单击左上角 active-->搜索 servera关键字-->打开 servera虚拟机 console
2 # 登录主机 用户名：root 密码：redhat
3 Red Hat Enterprise Linux 9.0 (Plow)
4 Kernel 5.14.0-70.13.1.el9_0.x86_64 on an x86_64
5
6 Activate the web console with: systemctl enable --now cockpit.socket
7
8 laoma login: `root`
9 Password: `redhat`
10 Last login: Mon Dec 18 13:06:38 on tty1
11 [root@servera ~]# vi /etc/ssh/sshd_config
12 #搜索/Root, 找到 PermitRootLogin prohibit-password行, 并在该行下面新添加一
    行
13 PermitRootLogin yes
14
15 # 重启 sshd 服务
16 [root@laoma ~]# systemctl restart sshd
```

servera

在 `servera.lab.example.com` 上完成以下任务。

1. 配置网络设置

将 `servera` 配置为具有以下网络配置：

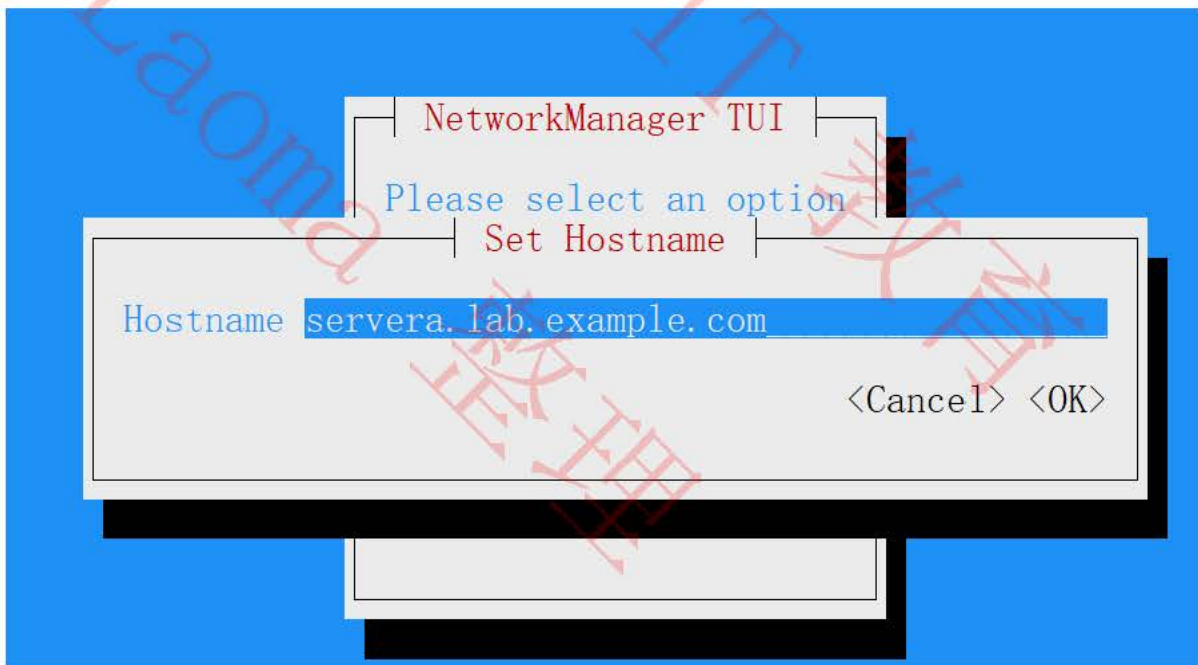
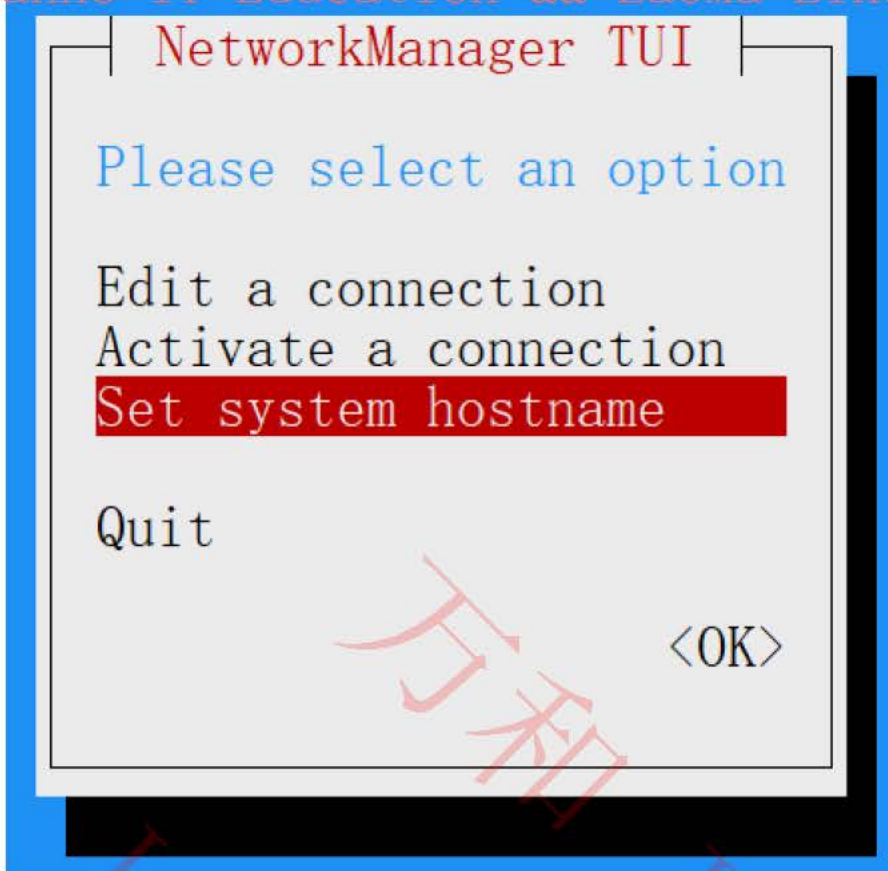
- 主机名： `servera.lab.example.com`
- IP地址： `172.25.250.10`
- 子网掩码： `255.255.255.0`
- 网关： `172.25.250.254`
- 名称服务器： `172.25.250.220`

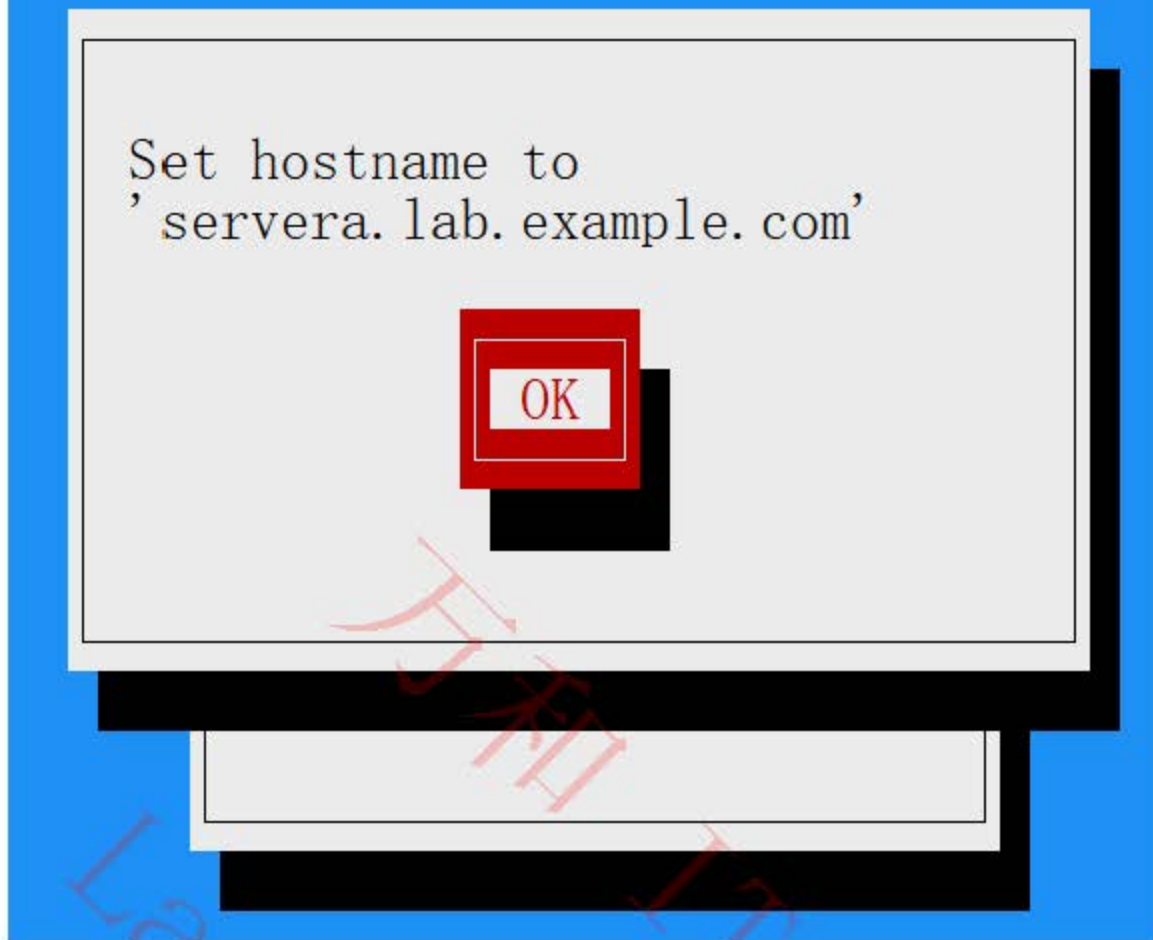
解答：

方法一：图形界面设置

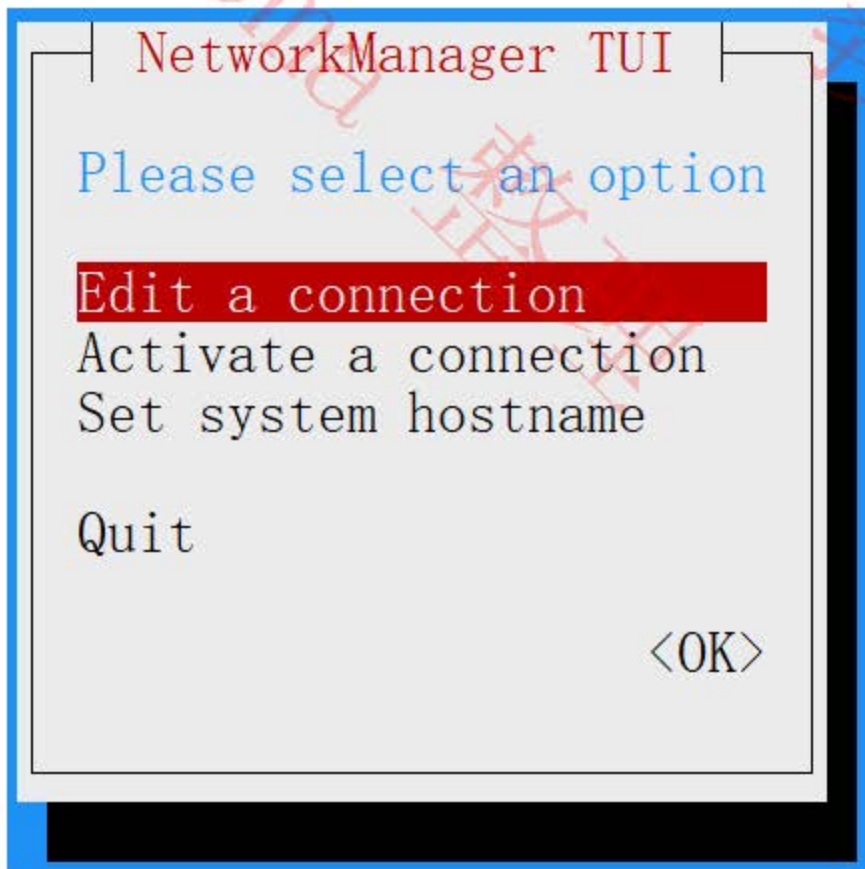
```
1 [root@laoma ~]# nmtui
```

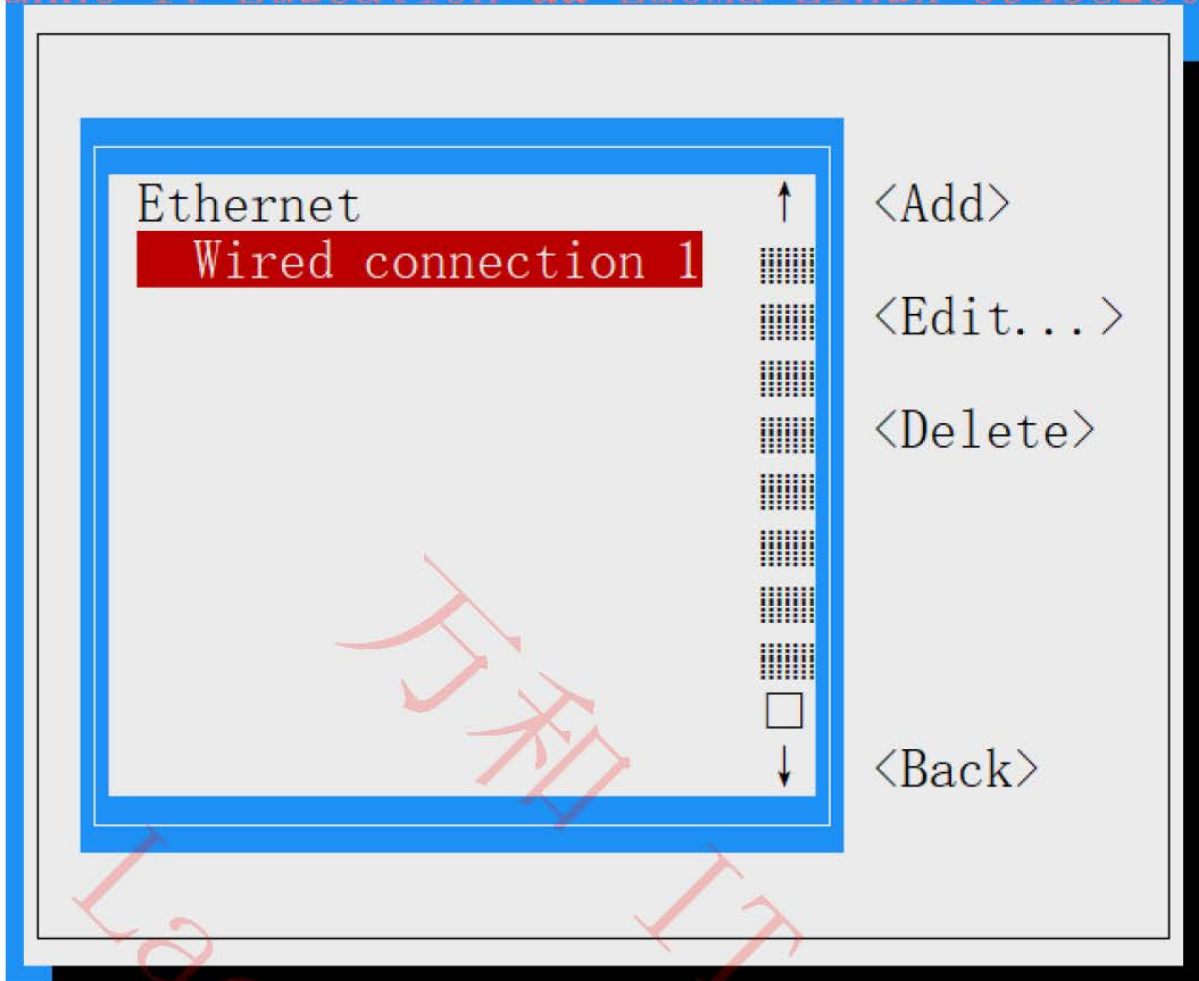
设置主机名



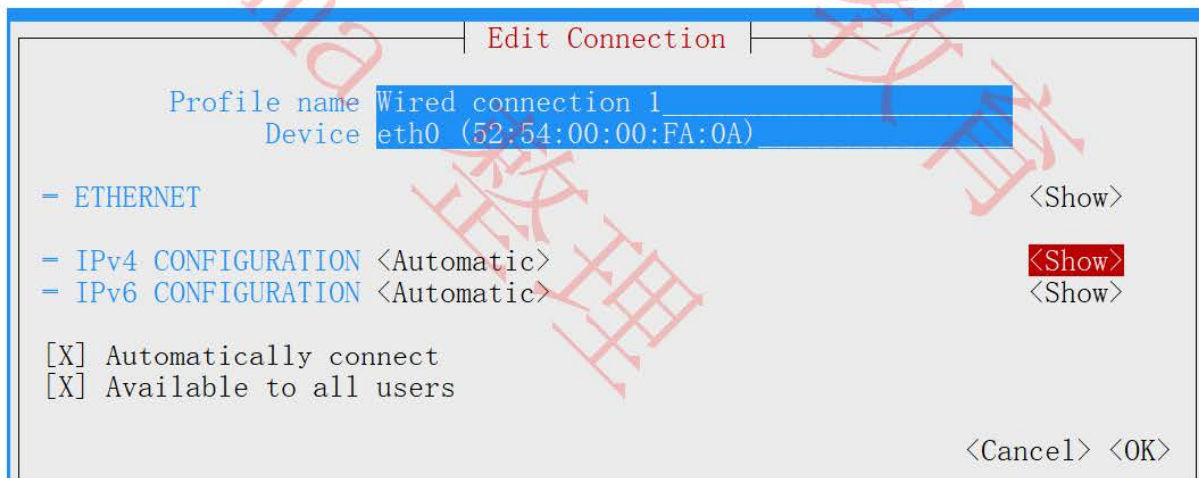


设置网络

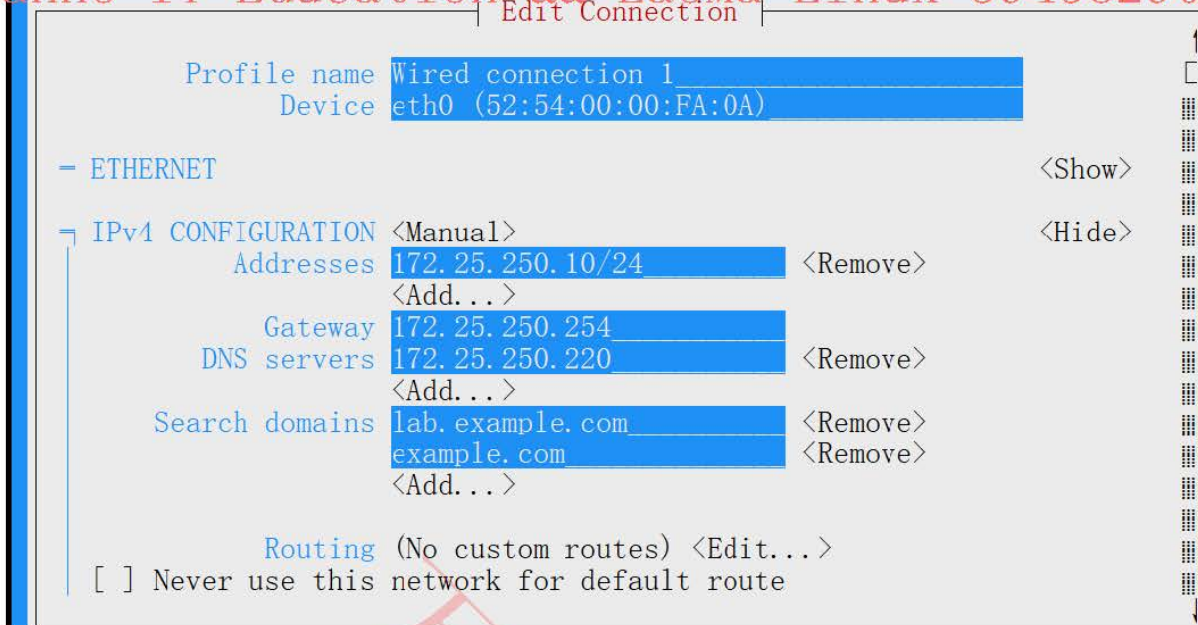




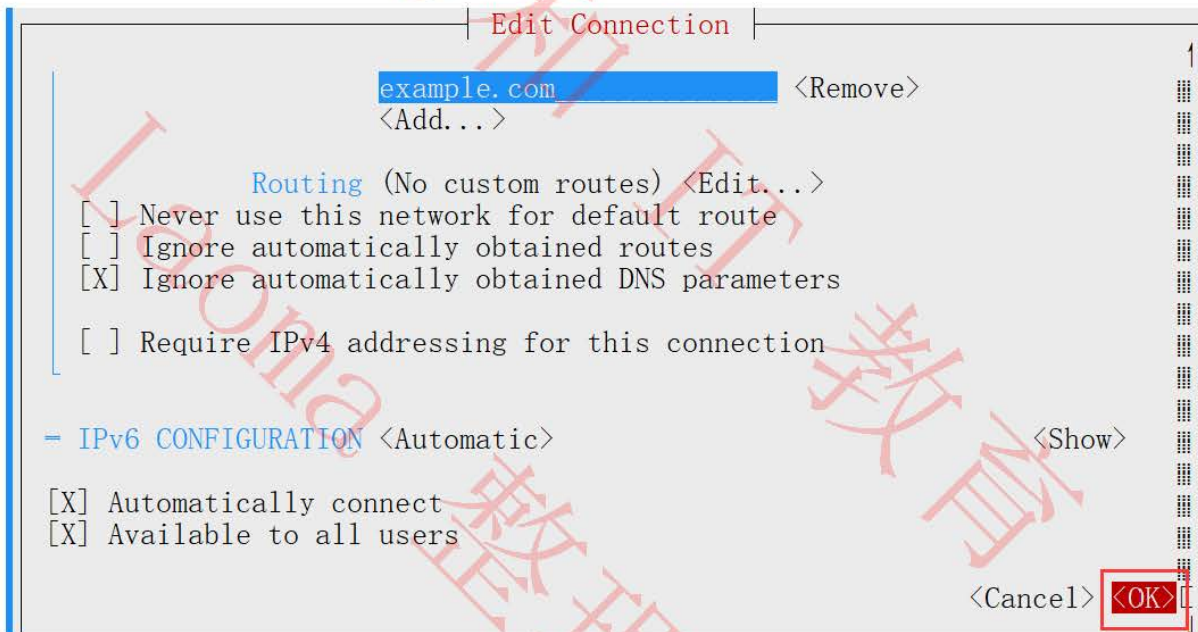
考试是配置界面如下图:



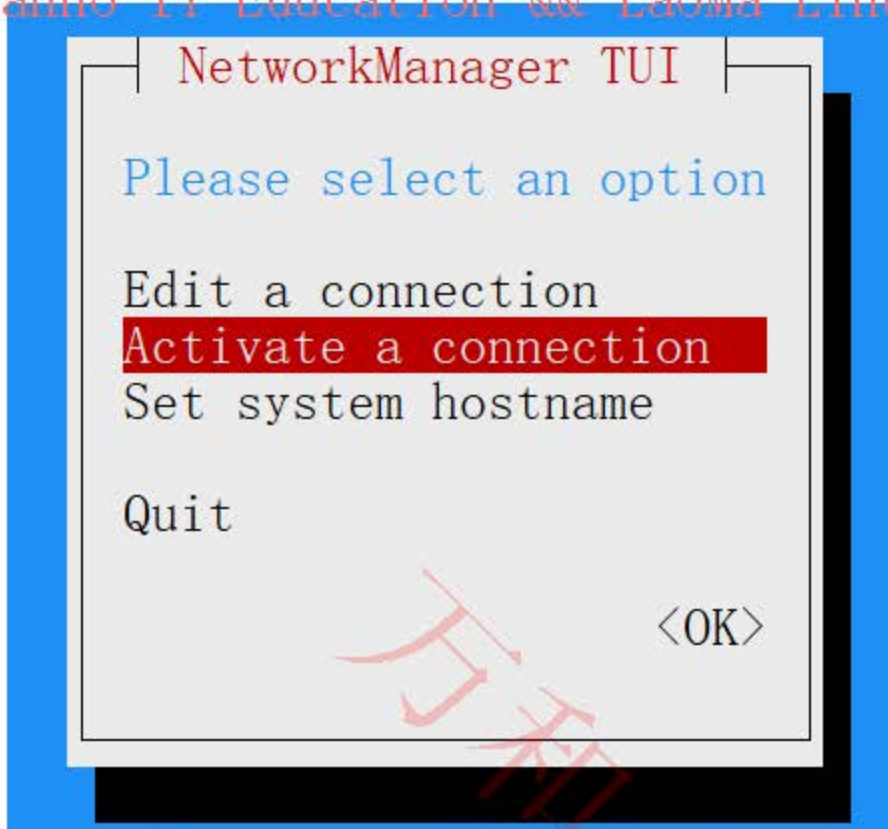
配置后效果如下:



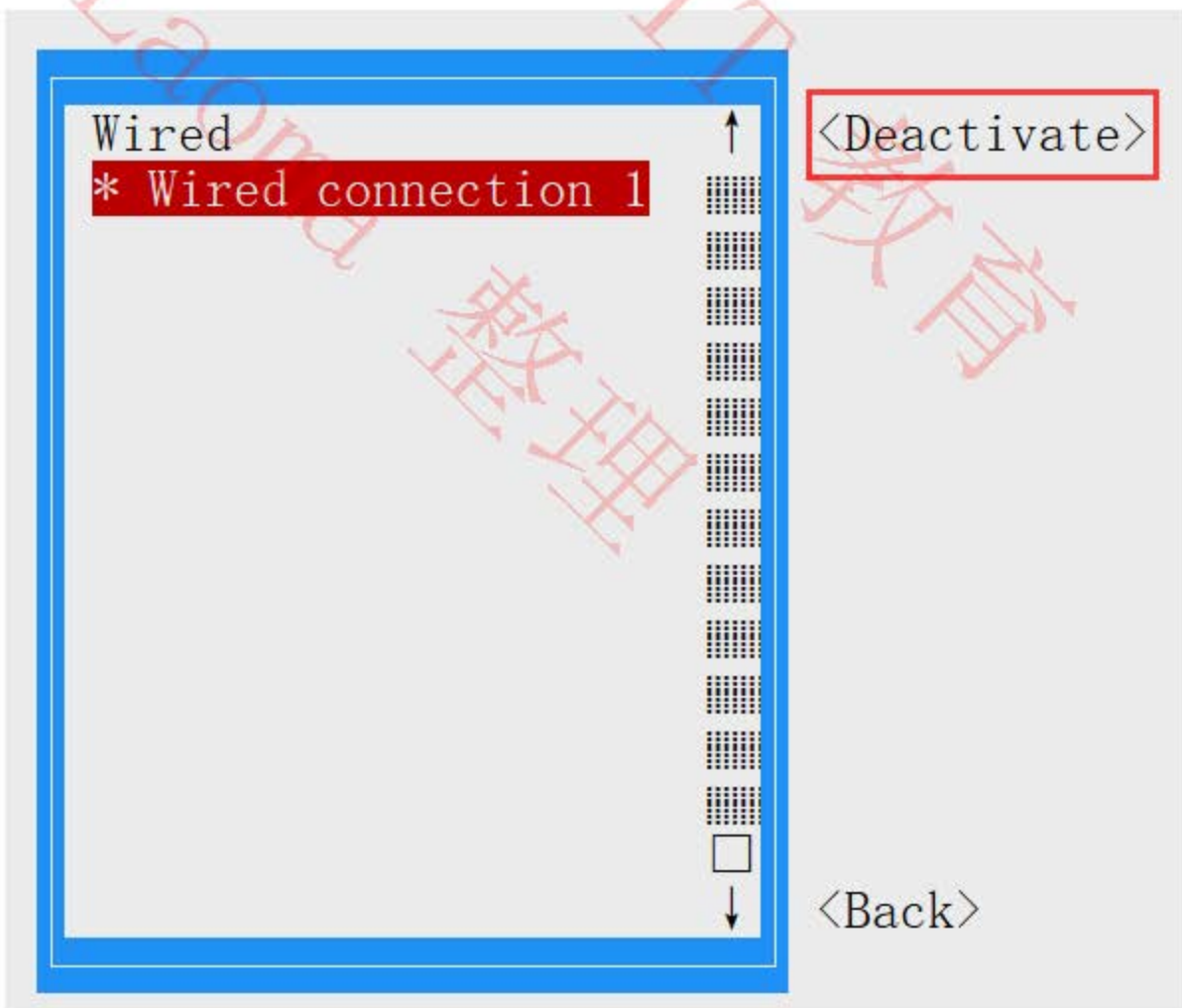
找到最下方OK，回车。

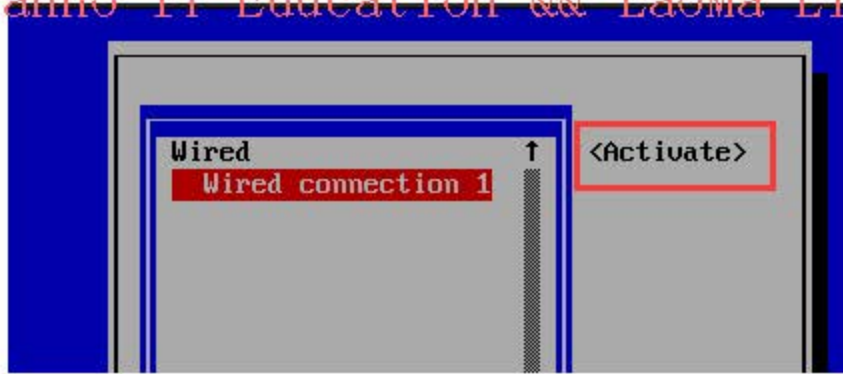


回到激活界面



取消激活 (Deactivate), 并再次激活 (Activate)。





方法二：命令行设置

设置主机名

```

1 [root@laoma ~]# hostnamectl set-hostname servera.lab.example.com
2
3 # 查看主机名
4 [root@servera ~]# hostnamectl
5     Static hostname: servera.lab.example.com
6         Icon name: computer-vm
7         Chassis: vm
8         Machine ID: f874df04639f474cb0a9881041f4f7d4
9         Boot ID: 67392cf28d44494eb8e2f5b46ff7cc30
10        Virtualization: kvm
11        Operating System: Red Hat Enterprise Linux 8.2 (ootpa)
12        CPE OS Name: cpe:/o:redhat:enterprise_linux:8.2:GA
13        Kernel: Linux 4.18.0-193.el8.x86_64
14        Architecture: x86_64

```

设置网络

```

1 [root@servera ~]# nmcli connection modify "wired connection 1"
   ipv4.method manual ipv4.addresses 172.25.250.10/24 ipv4.gateway
   172.25.250.254 ipv4.dns 172.25.250.220
2
3 # 激活网络
4 [root@servera ~]# nmcli connection up "wired connection 1"

```

主机网络配置完成后，通过ssh登录到servera验证。

```

1 # 查看ip地址和网关
2 [root@servera ~]# ip -br a
3 lo                UNKNOWN          127.0.0.1/8 ::1/128
4 eth0              UP               172.25.250.10/24
                   fe80::c38a:ac39:36a1:a43c/64
5 [root@servera ~]# ip r
6 default via 172.25.250.254 dev eth0 proto static metric 100
7 172.25.250.0/24 dev eth0 proto kernel scope link src 172.25.250.10
   metric 100
8
9 # 查看DNS

```

```
10 [root@servera ~]# nslookup servera
11 Server:      172.25.250.220
12 Address:    172.25.250.220#53
13
14 Name:      servera.lab.example.com
15 Address: 172.25.250.10
```

2. 配置 yum 仓库

- 配置您的系统从 http://content.example.com/rhel9.0/x86_64/dvd/BaseOS 和 http://content.example.com/rhel9.0/x86_64/dvd/AppStream 获取软件。
- 将这些 YUM 存储库设置为默认存储库。

解答:

```
1 # 创建.repo结尾文件，系统中可能未安装vim工具
2 [root@servera ~]# vi /etc/yum.repos.d/laoma.repo
3 [BaseOS]
4 name=BaseOS
5 baseurl=http://content.example.com/rhel9.0/x86_64/dvd/BaseOS
6 enabled=1
7 gpgcheck=0
8 [AppStream]
9 name=AppStream
10 baseurl=http://content.example.com/rhel9.0/x86_64/dvd/AppStream
11 enabled=1
12 gpgcheck=0
```

验证

```
1 # 生成仓库缓存
2 [root@servera ~]# dnf makecache
3
4 # 安装系统中不存在的软件，例如vim
5 [root@servera ~]# dnf install -y vim
```

3. 调试 SELinux

非标准端口 82 上运行的 Web 服务器在提供内容时遇到问题。根据需要调试并解决问题，使其满足以下条件:

- 系统上的 Web 服务器能够提供 `/var/www/html` 中所有现有的 HTML 文件 (注: 不要删除或以其他方式改动现有的文件内容)
- Web 服务器在端口 82 上提供此内容
- Web 服务器在系统启动时自动启动

解答:

```
1 # 安装软件 setroubleshoot-server 软件, 才能查看到 selinux 日志
2 # 考试环境未安装该软件, 所以默认无法查看到 selinux 日志
3 [root@servera ~]# dnf install -y setroubleshoot-server
4
5 # 设置服务开机启动并启动httpd服务
6 [root@servera ~]# systemctl enable httpd --now
7 Created symlink /etc/systemd/system/multi-
  user.target.wants/httpd.service →
  /usr/lib/systemd/system/httpd.service.
8 Job for httpd.service failed because the control process exited with
  error code.
9 See "systemctl status httpd.service" and "journalctl -xe" for details.
10
11 # 启动报错
12 [root@servera ~]# systemctl status httpd.service | cat
13 • httpd.service - The Apache HTTP Server
14   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled;
  vendor preset: disabled)
15   Active: failed (Result: exit-code) since Mon 2023-12-18 12:18:06
  EST; 28s ago
16   Docs: man:httpd.service(8)
17   Process: 8542 ExecStart=/usr/sbin/httpd $OPTIONS -DFOREGROUND
  (code=exited, status=1/FAILURE)
18   Main PID: 8542 (code=exited, status=1/FAILURE)
19   Status: "Reading configuration..."
20   CPU: 163ms
21
22 Dec 18 12:18:06 servera.lab.example.com systemd[1]: Starting The Apache
  HTTP Server...
23 Dec 18 12:18:06 servera.lab.example.com httpd[8542]: (13)Permission
  denied: AH00072: make_sock: could not bind to address [::]:82
24 Dec 18 12:18:06 servera.lab.example.com httpd[8542]: (13)Permission
  denied: AH00072: make_sock: could not bind to address 0.0.0.0:82
25 .....
26
27 # 查看 /var/log/messages, 82端口SELinux标签有误
28 [root@servera ~]# tail /var/log/messages
29 .....
```

```
30 Dec 18 12:18:16 servera setroubleshoot[8546]: SELinux is preventing
/usr/sbin/httpd from name_bind access on the tcp_socket port
82.#012#012***** Plugin bind_ports (99.5 confidence) suggests
*****#012#012If you want to allow /usr/sbin/httpd to
bind to network port 82#012Then you need to modify the port
type.#012Do#012# semanage port -a -t PORT_TYPE -p tcp 82#012 where
PORT_TYPE is one of the following: http_cache_port_t, http_port_t,
jboss_management_port_t, jboss_messaging_port_t, ntop_port_t,
puppet_port_t.#012#012***** Plugin catchall (1.49 confidence) suggests
*****#012#012If you believe that httpd should be
allowed name_bind access on the port 82 tcp_socket by default.#012Then
you should report this as a bug.#012You can generate a local policy
module to allow this access.#012Do#012allow this access for now by
executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-
httpd#012# semodule -X 300 -i my-httpd.pp#012
31
32 # 根据上面的提示设置82端口标签
33
34 [root@servera ~]# semanage port -a -t http_port_t -p tcp 82
35 [root@servera ~]# semanage port -l|grep 80
36
37 # 再次启动服务
38 [root@servera ~]# systemctl start httpd
39
40 # 验证服务状态
41 [root@servera ~]# systemctl is-enabled httpd
42 enabled
43 [root@servera ~]# systemctl is-active httpd
44 active
45
46 # 防火墙放行82端口，据说不放行不扣分
47 [root@servera ~]# firewall-cmd --add-port=82/tcp
48 success
49 [root@servera ~]# firewall-cmd --add-port=82/tcp --permanent
50 success
51
52 # 查看防火墙配置
53 [root@servera ~]# firewall-cmd --list-ports
54 82/tcp
55
56 # 测试物理机 foundation0 访问 web 服务，正常
57 [kiosk@foundation0 ~]$ curl http://servera.lab.example.com:82
58
59 # 查看 web 主目录中文件名
60 [root@servera ~]# ls /var/www/html/
61 file1 file2
62
63 # 访问 file1 和 file2
64 [kiosk@foundation0 ~]$ curl http://servera.lab.example.com:82/file1
65 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
66 <html><head>
67 <title>403 Forbidden</title>
```

```

68 </head><body>
69 <h1>Forbidden</h1>
70 <p>You don't have permission to access this resource.</p>
71 </body></html>
72 [kiosk@foundation0 ~]$ curl http://servera.lab.example.com:82/file2
73 hello laowang
74
75 # 查看日志，确定文件SELinux标签有误
76 [root@servera ~]# tail /var/log/messages
77 .....
78 Dec 18 12:21:48 servera setroubleshoot[8802]: SELinux is preventing
    /usr/sbin/httpd from getattr access on the file
    /var/www/html/file1.#012#012***** Plugin restorecon (92.2 confidence)
    suggests *****#012#012If you want to fix the
    label. #012/var/www/html/file1 default label should be
    httpd_sys_content_t.#012Then you can run restorecon. The access attempt
    may have been stopped due to insufficient permissions to access a
    parent directory in which case try to change the following command
    accordingly.#012Do#012# /sbin/restorecon -v
    /var/www/html/file1#012#012***** Plugin public_content (7.83
    confidence) suggests *****#012#012If you want to treat
    file1 as public content#012Then you need to change the label on file1
    to public_content_t or public_content_rw_t.#012Do#012# semanage
    fcontext -a -t public_content_t '/var/www/html/file1'#012# restorecon -
    v '/var/www/html/file1'#012#012***** Plugin catchall (1.41 confidence)
    suggests *****#012#012If you believe that httpd
    should be allowed getattr access on the file1 file by default.#012Then
    you should report this as a bug.#012You can generate a local policy
    module to allow this access.#012Do#012allow this access for now by
    executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-
    httpd#012# semodule -X 300 -i my-httpd.pp#012
79
80 # 根据提示恢复标签
81 [root@servera ~]# restorecon -RV /var/www/html/
82
83 # 再次访问测试
84 [kiosk@foundation0 ~]$ curl http://servera.lab.example.com:82/file1
85 hello laoma

```

4. 创建用户帐户

创建下列用户、组和组成员资格：

- 名为 `sysmgrs` 的组
- 用户 `natasha`，作为次要组从属于 `sysmgrs`
- 用户 `harry`，作为次要组还从属于 `sysmgrs`
- 用户 `sarah`，无权访问系统上的交互式shell且不是 `sysmgrs` 的成员
- `natasha`、`harry` 和 `sarah` 的密码应当都是 `redhat`

解答:

```
1 # 创建组 sysmgrs
2 [root@servera ~]# groupadd sysmgrs
3
4 # 创建用户 natasha
5 [root@servera ~]# useradd -G sysmgrs natasha
6
7 # 创建用户 harry
8 [root@servera ~]# useradd -G sysmgrs harry
9
10 # 创建用户 sarah
11 [root@servera ~]# useradd -s /sbin/nologin sarah
12
13 # 设置用户密码方法一
14 [root@servera ~]# passwd natasha
15 Changing password for user natasha.
16 New password: `redhat`
17 BAD PASSWORD: The password is shorter than 8 characters
18 Retype new password: `redhat`
19 passwd: all authentication tokens updated successfully.
20
21 # 设置用户密码方法二
22 [root@servera ~]# echo redhat | passwd --stdin harry
23 Changing password for user harry.
24 passwd: all authentication tokens updated successfully.
25 [root@servera ~]# echo redhat | passwd --stdin sarah
26 Changing password for user sarah.
27 passwd: all authentication tokens updated successfully.
28
29 ## 验证用户信息, 以natasha为例
30 # ssh登录, 测试密码
31 [kiosk@foundation0 ~]$ ssh natasha@servera
32
33 # 验证用户组信息
34 [natasha@servera ~]$ id natasha
35 uid=2003(natasha) gid=2004(natasha) groups=2004(natasha),2003(sysmgrs)
36
37 # 验证用户bash信息
38 [natasha@servera ~]$ grep sarah /etc/passwd
39 sarah:x:2005:2006:~/home/sarah:/sbin/nologin
```

5. 配置 cron 作业

题型1: 配置 cron 作业, 该作业每天 14:23 (当地时间) 以 natasha 用户身份执行以下命令:

```
1 /bin/echo hiya
```

解答:

```

1 # 验证crond服务状态
2 [root@servera ~]# systemctl is-enabled crond.service
3 enabled
4 [root@servera ~]# systemctl is-active crond.service
5 active
6
7 # 添加cron作业，内容格式可以参考/etc/crontab
8 [root@servera ~]# crontab -u natasha -e
9 23 14 * * * /bin/echo hiya
10
11 # 验证文件内容
12 [root@servera ~]# crontab -u natasha -l
13 23 14 * * * /bin/echo hiya

```

题型2: 配置 cron 作业，该作业每隔 2 分钟以 natasha 用户身份执行以下命令：

```
1 logger "EX200 in progress"
```

解答:

```

1 # 添加cron作业，内容格式可以参考/etc/crontab
2 [root@servera ~]# crontab -u natasha -e
3 */2 * * * * logger "EX200 in progress"

```

6. 创建协作目录

创建具有以下特征的协作目录 `/home/managers`：

- `/home/managers` 的组所有权是 `sysmgrs`。
- 目录应当可被 `sysmgrs` 的成员读取、写入和访问，但任何其他用户不具这些权限。
- `/home/managers` 中创建的文件自动将组所有权设置到 `sysmgrs` 组。

解答:

```

1 # 创建目录
2 [root@servera ~]# mkdir /home/managers
3
4 # 更改目录所属组
5 [root@servera ~]# chgrp sysmgrs /home/managers
6
7 # 设置目录组权限和其他用户权限
8 [root@servera ~]# chmod g=rwx,o=- /home/managers
9
10 # 设置组特殊权限
11 [root@servera ~]# chmod g+s /home/managers
12

```


32

```

=====
33  ^* sidecar.lab.example.com      8   6   37   44   +83us[ -999us] +/-
    1747us

```

8. 配置 autofs

以按照如下所述自动挂载远程用户的主目录：

- `classroom.example.com` (172.25.254.254) NFS导出 `/rhome` 到您的系统。此文件系统包含为用户 `laoma` 预配置的主目录。
- `laoma` 的主目录是 `classroom.example.com:/rhome/laoma`。
- `laoma` 的主目录应自动挂载到本地 `/rhome` 下的 `/rhome/laoma`。
- 主目录必须可供其用户写入。
- `laoma` 的密码是 `redhat`。

解答：

```

1  # 安装软件包
2  [root@servera ~]# yum install -y autofs
3
4  ## 修改配置文件
5  [root@servera ~]# vim /etc/auto.master
6  # 在文件末尾增加一行
7  /rhome /etc/auto.laoma
8
9  ## 准备配置文件/etc/auto.laoma, 参考/etc/auto.misc文件
10 [root@servera ~]# cp /etc/auto.misc /etc/auto.laoma
11 [root@servera ~]# vim /etc/auto.laoma
12 laoma -fstype=nfs,rw,sync classroom.example.com:/rhome/laoma
13
14 # 设置服务autofs开机自启, 并启动服务
15 [root@servera ~]# systemctl enable autofs --now
16
17 # 验证自动挂载
18 [root@servera ~]# ssh laoma@servera
19 laoma@servera's password: `redhat`
20 .....
21 [laoma@servera ~]$ pwd
22 /rhome/laoma
23 [laoma@servera ~]$ df /rhome/laoma/
24 Filesystem                1K-blocks    Used Available Use%
   Mounted on
25 classroom.example.com:/rhome/laoma 51699712 2048640 49651072   4%
   /rhome/laoma

```

9. 配置用户帐号

配置用户 `xiaozhang`，其用户ID为 `3533`。此用户的密码应当为 `redhat`。

解答：

```
1 # 判断用户 xiaozhang 是否存在
2 [root@servera ~]# id xiaozhang
3 id: 'xiaozhang': no such user
4
5 # 如果不存在，使用以下命令添加账户
6 [root@servera ~]# useradd -u 3533 xiaozhang
7
8 # 如果存在，并且用户id不是3533使用以下命令更改
9 [root@servera ~]# usermod -u 3533 xiaozhang
10
11 # 设置密码
12 [root@servera ~]# echo redhat | passwd --stdin xiaozhang
```

10. 查找文件

查找用户 `jacques` 所有的所有文件并将其副本放入 `/root/findfiles` 目录。

解答：

```
1 # 确保目录/root/findfiles存在
2 [root@servera ~]# mkdir /root/findfiles
3
4 # 查找文件
5 [root@servera ~]# find / -user jacques -exec cp -a {} /root/findfiles/
6 \;
7 find: '/proc/27744/task/27744/fd/7': No such file or directory
8 find: '/proc/27744/task/27744/fdinfo/7': No such file or directory
9 find: '/proc/27744/fd/8': No such file or directory
10 find: '/proc/27744/fdinfo/8': No such file or directory
11 # 以上报错不用理会
12
13 # 验证查找结果
14 [root@servera ~]# ls /root/findfiles
15 jacques1 jacques2 jacques3 jacques4 jacques5 jacquesdir
```

11. 查找字符串

- 查找文件 `/usr/share/doc/words/readme.txt` 中包含字符串 `crosswords` 的所有行。将所有这些行的副本按原始顺序放在文件 `/root/list` 中。
- `/root/list` 不得包含空行，且所有行必须是 `/usr/share/doc/words/readme.txt` 中原始行的确切副本。

解答:

```

1 # 使用grep过滤，并重定向到目标文件
2 [root@servera ~]# grep crosswords /usr/share/doc/words/readme.txt >
   /root/list
3
4 # 查看查找到的内容
5 [root@servera ~]# cat /root/list
6 113,809 official crosswords
7 4,160 official crosswords delta
8 when combined with the 113,809 crosswords file, it produces the

```

12. 创建存档

创建一个名为 `/root/backup.tar.gz` 的tar存档，其应包含 `/usr/local` 的内容。该 tar 存档必须使用 `gzip` 进行压缩。

解答:

```

1 # 根据题目要求打包成特定压缩包，man tar查找压缩参数
2 [root@servera ~]# tar -czf /root/backup.tar.gz /usr/local/
3 tar: Removing leading `/' from member names
4
5 # 验证压缩包内容
6 [root@servera ~]# tar -tf /root/backup.tar.gz
7 usr/local/
8 usr/local/bin/
9 .....

```

补充说明:

- 如果使用 `bzip2` 压缩，则使用选项 `-j`，而且需要手动安装 `bzip2` 软件包。
- 如果使用 `xz` 压缩，则使用选项 `-J`。

13. 创建一个容器镜像

- 以 `contsvc` 用户身份，构建名为 `ascii2pdf` 的镜像。
- 容器文件位于 <http://materials.example.com/laoma/Containerfile>，不要修改文件内容。

解答:

```

1 # 安装 podman
2 [root@servera ~]# dnf install -y podman
3
4 # 必须通过 ssh 方式登录，禁止使用 su 或者 sudo 切换用户
5 [root@servera ~]# ssh contsvc@servera
6

```

```

7 # 下载并查看容器文件
8 [contsv@servera ~]$ wget
http://materials.example.com/laoma/Containerfile
9 [contsv@servera ~]$ cat Containerfile
10 FROM registry.lab.example.com/ubi8/pdf-tools
11 MAINTAINER laoma@example.com
12 CMD /bin/sh /opt/ascii2pdf.sh
13
14 # 登录容器仓库并下载镜像
15 [contsv@servera ~]$ podman login -u admin registry.lab.example.com
16 Password: `redhat321`
17 Login succeeded!
18 [contsv@servera ~]$ podman pull registry.lab.example.com/ubi8/pdf-
tools
19
20 # 构建镜像
21 [contsv@servera ~]$ podman build -t ascii2pdf .
22 STEP 1/3: FROM registry.lab.example.com/ubi8/pdf-tools
23 STEP 2/3: MAINTAINER laoma@example.com
24 --> 51051cdf5f7
25 STEP 3/3: CMD /bin/sh /opt/ascii2pdf.sh
26 COMMIT ascii2pdf
27 --> ee8299d5a12
28 Successfully tagged localhost/ascii2pdf:latest
29 ee8299d5a12bf185e3ced52a759159087a0f5b3f90979290d5b58656dc97bb4a
30
31 # 验证
32 [contsv@servera ~]$ podman images localhost/ascii2pdf
33 REPOSITORY          TAG          IMAGE ID      CREATED      SIZE
34 localhost/ascii2pdf latest       ee8299d5a12b 49 seconds ago 235 MB

```

14. 将容器配置为服务

创建一个无根容器作为 systemd 服务自动启动，要求如下：

- 使用 `contsv` 用户，配置一个 systemd 服务
- 容器名称为 `ascii2pdf`
- 使用刚创建的镜像 `ascii2pdf`
- 该服务命名为 `container-ascii2pdf`，并在系统重启时自动启动
- 将服务配置为在启动时：
 - 自动将 `/opt/files` 挂载到容器 `/opt/input-txt` 下；
 - 自动将 `/opt/progress` 挂载到容器 `/opt/output-pdf` 下；

如果服务工作正常，则放入本地 `/opt/files` 目录中的文本文档将会被转换为 pdf 文档，并存放到本地 `/opt/progress` 目录。

解答:

```
1 # 准备容器目录
2 [root@servera ~]# mkdir /opt/files /opt/progress
3 [root@servera ~]# chown contsvc:contsvc /opt/files /opt/progress
4
5 ## 设置允许用户service随服务器一起启动
6 [contsvc@servera ~]$ loginctl enable-linger
7 # 验证
8 [contsvc@servera ~]$ loginctl show-user contsvc |tail -1
9 Linger=yes
10
11 # 创建容器
12 [contsvc@servera ~]$ podman run -d --name ascii2pdf \
13 -v /opt/files:/opt/input-txt:Z \
14 -v /opt/progress:/opt/output-pdf:Z \
15 localhost/ascii2pdf
16
17 # 验证
18 [contsvc@servera ~]$ podman ps
19 CONTAINER ID IMAGE COMMAND CREATED
20 250023a9d663 localhost/ascii2pdf:latest /bin/sh -c /bin/s... 2
21 seconds ago Up 2 seconds ago ascii2pdf
22
23 # 查找user unit配置目录
24 [contsvc@servera ~]$ man systemd.unit
25
26 # 准备unit目录和文件
27 [contsvc@servera ~]$ mkdir -p ~/.config/systemd/user/
28 [contsvc@servera ~]$ cd ~/.config/systemd/user/
29 [contsvc@servera user]$ podman generate systemd --name ascii2pdf --
30 files --new
31 /home/contsvc/.config/systemd/user/container-ascii2pdf.service
32
33 # 通知systemd读取用户unit文件
34 [contsvc@servera user]$ systemctl --user daemon-reload
35
36 # 强制删除容器
37 [contsvc@servera user]$ podman rm ascii2pdf --force
38
39 # 设置用户单元开机启动并立刻启动
40 [contsvc@servera user]$ systemctl --user enable container-
41 ascii2pdf.service --now
42
43 # 验证当前是否处于运行状态, 以及开机是否自动启动
44 [contsvc@servera user]$ systemctl --user status container-
45 ascii2pdf.service
46
47 # 创建文本文件验证
48 [contsvc@servera user]$ echo hello > /opt/files/f1.txt
```

```
45 [contsv@servera user]$ ls /opt/progress/
46 f1.pdf
```

附加题

说明：考试时会随机考其中1-2题。

15. 添加 sudo 免密操作

允许 `sysmgrs` 组成员 `sudo` 时不需要密码。

解答：

```
1 [root@servera ~]# visudo
2 .....
3 # %wheel          ALL=(ALL)        NOPASSWD: ALL
4 # 参考wheel组添加如下记录
5 %sysmgrs          ALL=(ALL)        NOPASSWD: ALL
6
7 # 验证
8 [root@servera ~]# su - natasha
9 [natasha@servera ~]$ sudo tail /var/log/messages
```

16. 配置创建新用户的密码策略

- 创建新用户时，默认密码策略为：20 天后密码会过期。

```
1 [root@servera ~]# vim /etc/login.defs
2 ...
3 # 修改以下参数值为20
4 PASS_MAX_DAYS    20
5
6 # 验证
7 [root@servera ~]# useradd dog
8 [root@servera ~]# chage -l dog
9 Last password change           : Dec 18, 2023
10 Password expires               : Jan 07, 2024
11 Password inactive             : never
12 Account expires               : never
13 Minimum number of days between password change : 0
14 Maximum number of days between password change : 20
15 Number of days of warning before password expires : 7
16 [root@servera ~]# userdel -r dog
```

17. 创建脚本

题型1: 创建一个名为 `myresearch` 的脚本

- 该脚本放置在 `/usr/local/bin` 下
- 该脚本用来查找 `/usr` 下所有小于 `50k`、大于 `30k`、且具有设置SUID权限的文件，将这些文件清单保存在文件 `/root/myfiles` 中。

解答:

```

1 [root@servera ~]# vim /usr/local/bin/myresearch
2 #!/bin/bash
3 find /usr -size +30k -size -50k -perm -4000 > /root/myfiles
4
5 # 如果题目要求就是将找到的文件副本保存到/root/myfiles中，则脚本内容如下：
6 #!/bin/bash
7 mkdir /root/myfiles
8 find /usr -size -50k -size +30k -perm -4000 -exec cp -a {}
  /root/myfiles \;
9
10 [root@servera ~]# chmod +x /usr/local/bin/myresearch
11 [root@servera ~]# /usr/local/bin/myresearch
12
13 # 验证
14 [root@servera ~]# cat /root/myfiles

```

题型2: 配置一个应用

配置应用 `ex200`，要求如下：当以用户 `natasha` 执行 `ex200` 时，它将显示消息：

```
1 welcome to Pandora
```

解答:

```

1 [root@servera ~]# vim /usr/local/bin/ex200
2 #!/bin/bash
3 echo "welcome to Pandora"
4
5 [root@servera ~]# chmod +x /usr/local/bin/ex200
6 [root@servera ~]# su - natasha
7 [pandora@servera ~]$ ex200
8 welcome to Pandora

```

18. 默认文件权限

- **题型1:** 配置用户 `laoma`，确保创建的文件和目录权限如下：
 - 创建文件默认权限是 `r--r--r--`
 - 创建目录默认权限是 `r-xr-xr-x`

解答:

```
1 [laoma@servera ~]$ vim ~/.bashrc
2 # 文件末尾最后添加
3 umask 222
```

- **题型2:** 配置所有用户:

- 创建文件默认权限: 拥有组和其他人不具有任何权限。

解答:

```
1 [root@servera ~]# vim /etc/bashrc
2 # 或者
3 [root@servera ~]# vim /etc/profile
4 # 文件末尾最后添加
5 umask 077
```

19. 在容器中执行命令

在容器 `ascii2pdf` 中执行命令 `echo Hello world`

解答:

```
1 [contsvc@servera ~]$ podman exec ascii2pdf echo Hello world
```

serverb

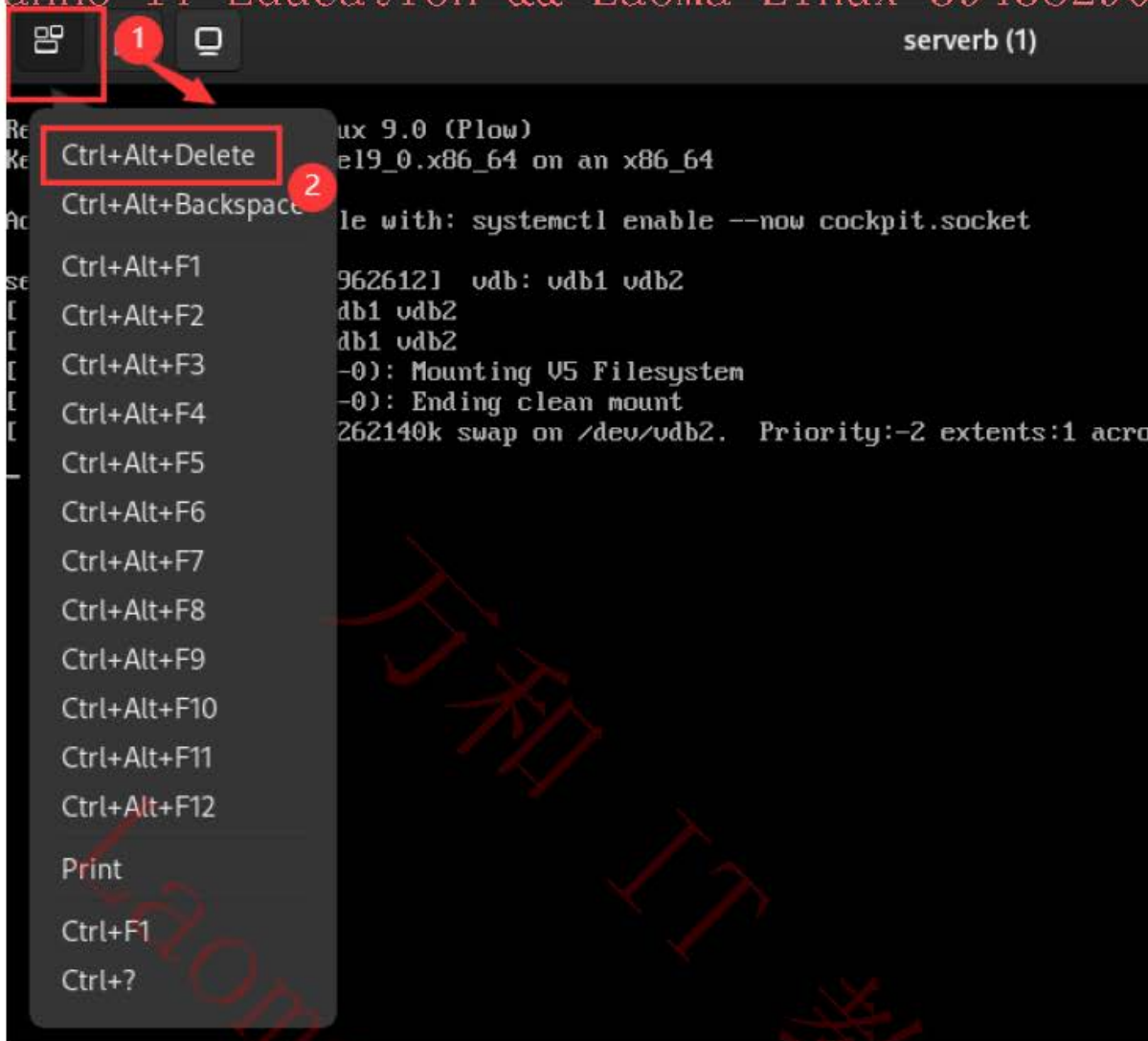
在 `serverb.lab.example.com` 上完成以下任务。

1. 设置 root 密码

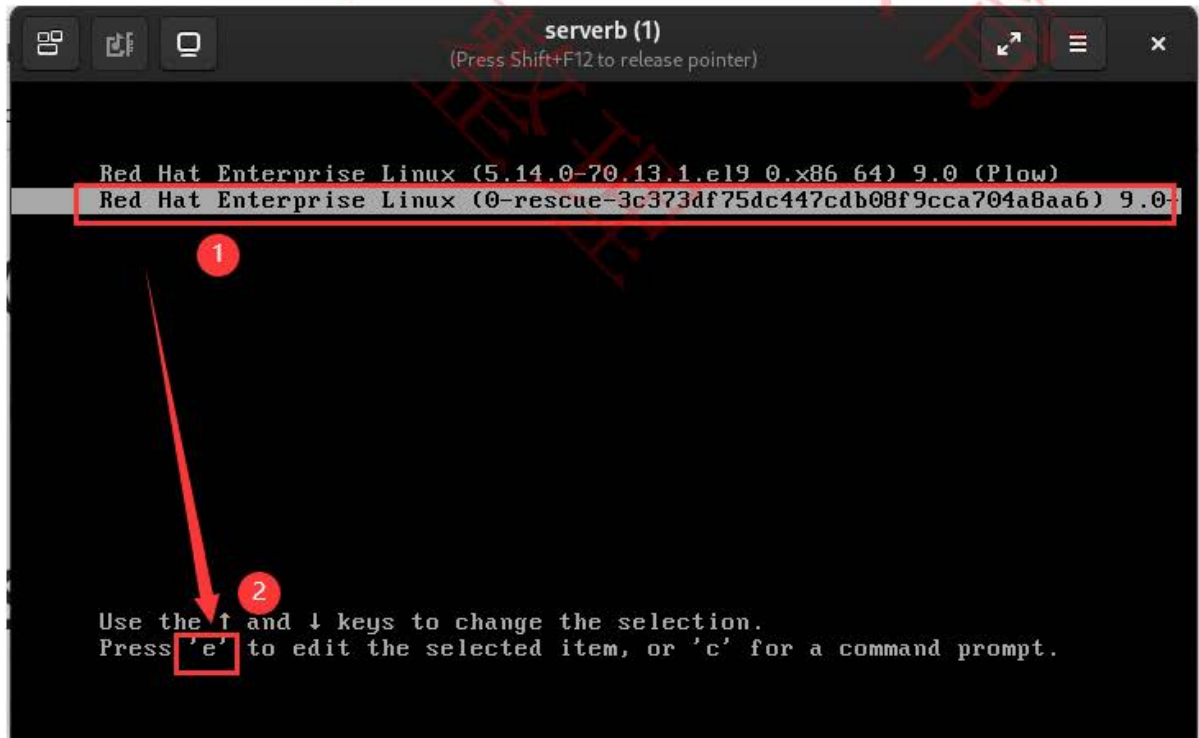
将 `root` 密码设置为 `redhat`。您需要获得系统访问权限才能进行此操作。

解答:

通过 `serverb` 终端左上角图标, 重启 `serverb`



在系统菜单界面，通过上下方向键选择带有 `rescue` 行，并按 `e` 进行编辑。



在 `linux` 行末尾，添加 `rd.break`，然后 `Ctrl+x` 启动。

```

serverb (1)

load_video
set gfx_payload=keep
insmod gzio
linux ($root)/vmlinuz-0-rescue-3c373df75dc447cdb08f9cca704a8aa6 root=UUID=fb53\
5add-9799-4a27-b8bc-e8259f39a767 console=tty0 console=ttyS0,115200n8 no_timer_\
check net.ifname=0 rd.break
initrd ($root)/initramfs-0-rescue-3c373df75dc447cdb08f9cca704a8aa6.img

Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
discard edits and return to the menu. Pressing Tab lists
possible completions.

```

启动后界面如下:

```

1 .....
2
3 Generating "/run/initramfs/rdsosreport.txt"
4
5
6 Entering emergency mode. Exit the shell to continue.
7 Type "journalctl" to view system logs.
8 You might want to save "/run/initramfs/rdsosreport.txt" to a USB stick
9 or /boot
10 after mounting them and attach it to a bug report.
11 # 按回车继续
12 Press Enter for maintenance
13 (or press Control-D to continue): `回车`
14
15 # 以读写方式重新挂载/sysroot
16 sh-5.1# mount -o rw,remount /sysroot/
17
18 # 切换 root目录
19 sh-5.1# chroot /sysroot/
20
21 # 设置root密码
22 sh-5.1# echo redhat | passwd --stdin root
23
24 # 创建/.autorelabel, 确保系统重启后对用户相关文件重新打标签
25 sh-5.1# touch /.autorelabel
26
27 # 退出两次
28 sh-5.1# exit
29 exit

```

SELinux打标签完成后，重启系统。

```
[ 161.317073] XFS (dm-0): Ending clean mount
[ 161.608385] audit: type=1404 audit(1702923042.686:4): enforcing=0 old_enforcing=1 auid=4294967295 ses=4294967295 enabled=1 old-enabled=1 lsm=selinux res=1
[ 158.745022] selinux-autorelabel[821]: *** Warning -- SELinux targeted policy relabel is required.
[ 158.751395] selinux-autorelabel[821]: *** Relabeling could take a very long time, depending on file
[ 158.765965] selinux-autorelabel[821]: *** system size and speed of hard drives.
[ 176.635418] selinux-autorelabel[827]: Relabeling / /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /laoma /run /sys /sys/fs/cgroup /sys/fs/pstore /sys/kernel/debug /sys/kernel/tracing
[ 207.389343] selinux-autorelabel[1178]: Warning no default label for /dev/mqueue
[ 207.419233] selinux-autorelabel[827]: Cleaning up labels on /tmp
[ 210.596339] watchdog: watchdog0: watchdog did not stop!
[ 210.627483] systemd-shutdown[1]: Using hardware watchdog 'iTCO_wdt', version 0, device /dev/watchdog0
[ 210.643087] systemd-shutdown[1]: Watchdog running with a timeout of 10min.
[ 210.756229] systemd-shutdown[1]: Syncing filesystems and block devices.
[ 210.770478] systemd-shutdown[1]: Sending SIGTERM to remaining processes...
[ 210.872123] systemd-journald[748]: Received SIGTERM from PID 1 (systemd-shutdown).
[ 210.918195] systemd-shutdown[1]: Sending SIGKILL to remaining processes...
[ 210.928934] systemd-shutdown[1]: Unmounting file systems.
```

使用新密码登录即可。

```
1 Red Hat Enterprise Linux 9.0 (Plow)
2 Kernel 5.14.0-70.13.1.el9_0.x86_64 on an x86_64
3
4 Activate the web console with: systemctl enable --now cockpit.socket
5
6 serverb login: `root`
7 Password: `redhat`
8 Last login: Mon Dec 18 14:06:38 on tty1
9 [root@serverb ~]#
```

2. 配置 yum 仓库

- 配置您的系统从 http://content.example.com/rhel9.0/x86_64/dvd/BaseOS 和 http://content.example.com/rhel9.0/x86_64/dvd/AppStream 获取软件。
- 将这些 YUM 存储库设置为默认存储库。

解答：

```
1 # 直接从 servera 节点拷贝文件
2 [root@serverb ~]# scp root@servera:/etc/yum.repos.d/laoma.repo /etc/yum.repos.d/
```

3. 设置逻辑卷大小

将逻辑卷 `laomalv` 及其文件系统的大小调整到 `230MiB`。确保文件系统内容保持不变。

注：分区大小很少与请求的大小完全相同，因此可以接受范围为 `217MiB` 到 `243MiB` 的大小。

解答：

```

1 # 查看文件系统大小
2 [root@serverb ~]# df -h |grep laomalv
3 /dev/mapper/laomavg-laomalv 123M 7.6M 116M 7% /laoma
4
5 # 查看逻辑卷大小
6 [root@serverb ~]# lvs
7   LV      VG      Attr      LSize   Pool Origin Data%  Meta%  Move Log
8   Cpy%Sync Convert
9   laomalv laomavg -wi-ao---- 128.00m
10
11 # 查看卷组空间是否够扩容，剩余124m，足够扩容
12 [root@serverb ~]# vgs
13   VG      #PV #LV #SN Attr   VSize   VFree
14   laomavg  1   1   0 wz--n- 252.00m 124.00m
15
16 # 逻辑卷和文件系统一起扩容，其中-r选项代表文件系统一起扩展。
17 [root@serverb ~]# lvextend -rL 230M /dev/mapper/laomavg-laomalv
18
19 # 验证扩展结果
20 [root@serverb ~]# df -h /laoma
21 Filesystem                Size      Used Avail Use% Mounted on
22 /dev/mapper/laomavg-laomalv 227M    8.5M  219M   4% /laoma
23
24 [root@serverb ~]# lvs
25   LV      VG      Attr      LSize   Pool Origin Data%  Meta%  Move Log
26   Cpy%Sync Convert
27   laomalv laomavg -wi-ao---- 232.00m

```

4. 添加交换分区

向您的系统添加一个额外的交换分区：

- 大小为 `756 MiB`。
- 应在系统启动时自动挂载。
- 不要删除或以任何方式改动系统上的任何现有交换分区。

解答：

```

1 # 查看系统中交换分区清单
2 [root@serverb ~]# swapon -s
3 Filename                    Type          Size          Used          Priority

```

```

4 /dev/vdb2 partition 262140 0 -2
5
6 # 查看硬盘分区，及剩余空间
7 [root@serverb ~]# lsblk
8 NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
9 vda                                  252:0    0   10G  0 disk
10 └─vda1                               252:1    0    1M  0 part
11 └─vda2                               252:2    0  200M  0 part /boot/efi
12 └─vda3                               252:3    0  500M  0 part /boot
13 └─vda4                               252:4    0   9.3G  0 part /
14 vdb                                  252:16   0    5G  0 disk
15 └─vdb1                               252:17   0  256M  0 part
16 | └─laomavg-laomalv                 253:0    0  232M  0 lvm  /laoma
17 └─vdb2                               252:18   0  256M  0 part [SWAP]
18
19 # 考试时，系统有2个硬盘vda和vdb，vda使用gpt分区，vdb未使用。
20
21 # 使用gdisk管理vdb磁盘
22 [root@serverb ~]# gdisk /dev/vdb
23 GPT fdisk (gdisk) version 1.0.7
24
25 Partition table scan:
26 MBR: protective
27 BSD: not present
28 APM: not present
29 GPT: present
30
31 Found valid GPT with protective MBR; using GPT.
32
33 # 使用p命令查看分区表信息
34 Command (? for help): p
35 .....
36 Number  Start (sector)    End (sector)  Size      code  Name
37     1            2048           526335     256.0 MiB   8E00  Linux LVM
38     2           526336          1050623     256.0 MiB   8200  Linux swap
39
40 # 使用n命令创建新分区
41 Command (? for help): `n`
42
43 # 分区号，使用默认值
44 Partition number (3-128, default 3): `回车`
45
46 # 分区起始位置，使用默认值
47 First sector (34-10485726, default = 1050624) or {+-}size{KMGTP}: `回车`
48
49 # 终止位置，使用 +756M
50 Last sector (1050624-10485726, default = 10485726) or {+-}size{KMGTP}:
51 `+756M`
52
53 # 指定分区类型 8200
54 Current type is 8300 (Linux filesystem)
55 Hex code or GUID (L to show codes, Enter = 8300): `8200`

```

```

55 changed type of partition to Linux swap
56
57
58 # 查看结果
59 Command (m for help): p
60 .....
61 Number  Start (sector)    End (sector)  Size      Code  Name
62     1             2048           526335      256.0 MiB   8E00   Linux LVM
63     2             526336         1050623      256.0 MiB   8200   Linux swap
64     3             1050624        2598911      756.0 MiB   8200   Linux swap
65
66 # 保存更改
67 Command (? for help): `w`
68
69 Final checks complete. About to write GPT data. THIS WILL OVERWRITE
70 EXISTING
71 PARTITIONS!!
72
73 # 输入 Y, 再次确认
74 Do you want to proceed? (Y/N): `Y`
75 OK; writing new GUID partition table (GPT) to /dev/vdb.
76 warning: The kernel is still using the old partition table.
77 The new table will be used at the next reboot or after you
78 run partprobe(8) or kpartx(8)
79 The operation has completed successfully.
80
81 # 刷新分区表
82 [root@serverb ~]# partprobe /dev/vdb
83 [root@serverb ~]# lsblk /dev/vdb
84 NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
85 vdb                  252:16  0    5G  0 disk
86 └─vdb1               252:17  0 256M  0 part
87  | └─laomavg-laoma1v 253:0   0 232M  0 lvm  /laoma
88  └─vdb2              252:18  0 256M  0 part [SWAP]
89  └─vdb3              252:19  0 756M  0 part
90
91 # 格式化 swap 分区
92 [root@serverb ~]# mkswap /dev/vdb3
93 setting up swap space version 1, size = 756 MiB (792719360 bytes)
94 no label, UUID=05a57aba-65c0-4450-b223-3e001a954fdf
95
96 # 设置新增 swap 分区开机自动激活
97 [root@serverb ~]# vim /etc/fstab
98 # 最后一行新增以下内容
99 UUID=05a57aba-65c0-4450-b223-3e001a954fdf none swap defaults 0 0
100
101 # 激活新分区
102 [root@serverb ~]# swapon -a
103
104 # 查看系统中交换分区清单
105 [root@serverb ~]# swapon -s
106
107 Filename                Type      Size      Used      Priority

```

106	/dev/vdb2	partition	262140	0	-2
107	/dev/vdb3	partition	774140	0	-3

5. 创建逻辑卷

根据如下要求，创建新的逻辑卷：

- 逻辑卷取名为 `qa`，属于 `qagroup` 卷组，大小为 60 个扩展块。
- `qagroup` 卷组中逻辑卷的扩展块大小应当为 16MiB。
- 使用 `vfat` 文件系统格式化新逻辑卷。该逻辑卷应在系统启动时自动挂载到 `/mnt/qa` 下。

解答：

```

1 # 计算新卷组容量至少是60*16=960MiB
2 # 准备一个容量为1G的分区
3
4 # 在vdb中新建分区
5 [root@serverb ~]# gdisk /dev/vdb
6 GPT fdisk (gdisk) version 1.0.7
7
8 Partition table scan:
9   MBR: protective
10  BSD: not present
11  APM: not present
12  GPT: present
13
14 Found valid GPT with protective MBR; using GPT.
15
16 # 新建分区
17 Command (? for help): `n`
18 Partition number (4-128, default 4): `回车`
19 First sector (34-10485726, default = 2598912) or {+}size{KMGT}: `回车`
20 Last sector (2598912-10485726, default = 10485726) or {+}size{KMGT}:
21 `+1G`
22 Current type is 8300 (Linux filesystem)
23 Hex code or GUID (L to show codes, Enter = 8300): `8E00`
24 Changed type of partition to 'Linux LVM'
25
26 # 保存更改
27 Command (? for help): `w`
28
29 Final checks complete. About to write GPT data. THIS WILL OVERWRITE
30 EXISTING
31 PARTITIONS!!
32
33 # 输入 Y，再次确认
34 Do you want to proceed? (Y/N): `Y`
35 OK; writing new GUID partition table (GPT) to /dev/vdb.

```

```
34 warning: The kernel is still using the old partition table.
35 The new table will be used at the next reboot or after you
36 run partprobe(8) or kpartx(8)
37 The operation has completed successfully.
38
39 # 刷新分区表
40 [root@serverb ~]# partprobe /dev/vdb
41 [root@serverb ~]# lsblk /dev/vdb
42 NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
43 vdb                                  252:16  0    5G  0 disk
44 └─vdb1                               252:17  0 256M  0 part
45   └─┌─laomavg-laomalv                253:0   0 232M  0 lvm  /laoma
46     └─vdb2                           252:18  0 256M  0 part [SWAP]
47     └─vdb3                           252:19  0 756M  0 part [SWAP]
48     └─vdb4                           252:20  0    1G  0 part
49
50
51 # 创建卷组，-s选项指定PE大小
52 # 如果该步骤忘记指定PE大小，可以使用vgremove删除vg后，重新创建vg
53 [root@serverb ~]# vgcreate qagroup /dev/vdb4 -s 16M
54 Physical volume "/dev/vdb4" successfully created.
55 Volume group "qagroup" successfully created
56
57 # 创建逻辑卷，-l选项指定le数量，-n指定逻辑卷名称
58 [root@serverb ~]# lvcreate -n qa -l 60 qagroup
59 Logical volume "qa" created.
60
61 # 查看逻辑卷信息
62 [root@serverb ~]# lvs
63 LV      VG      Attr      LSize   Pool Origin Data%  Meta%  Move Log
64 Cpy%Sync Convert
65 laomalv laomavg -wi-ao---- 232.00m
66 qa      qagroup -wi-a----- 960.00m
67
68 # 格式化逻辑卷
69 [root@serverb ~]# mkfs.vfat /dev/qagroup/qa
70 mkfs.fat 4.2 (2021-01-31)
71
72 # 创建挂载点
73 [root@serverb ~]# mkdir /mnt/qa
74
75 # 查看设备 UUID
76 [root@serverb ~]# blkid /dev/qagroup/qa
77 /dev/qagroup/qa: UUID="2CF5-5294" BLOCK_SIZE="512" TYPE="vfat"
78
79 # 设置永久挂载
80 [root@serverb ~]# vim /etc/fstab
81 # 最后一行新增以下内容
82 UUID="2CF5-5294" /mnt/qa vfat defaults 0 0
83
84 # 挂载文件系统
85 [root@serverb ~]# mount -a
```

```
85
86 # 验证
87 [root@serverb ~]# df -h /mnt/qa
88 Filesystem                Size  Used Avail Use% Mounted on
89 /dev/mapper/qagroup-qa    959M  4.0K  959M   1% /mnt/qa
```

6. 配置系统调优

为您的系统选择建议的 `tuned` 配置集并将它设为默认设置。

解答：

```
1 # 查看 tuned 服务自动状态
2 [root@serverb ~]# systemctl is-enabled tuned.service
3 enabled
4 [root@serverb ~]# systemctl is-active tuned.service
5 active
6
7 # 设定推荐 profile
8 [root@serverb ~]# tuned-adm auto_profile
9
10 # 查看系统推荐 profile
11 [root@serverb ~]# tuned-adm recommend
12 virtual-guest
13
14 # 查看系统当前 profile
15 [root@serverb ~]# tuned-adm active
16 Current active profile: virtual-guest
```

检查成绩

评分须知：

- 考试时，不提供评分脚本检查错误。
- 脚本评分不针对附加题评分。
- 确保 2 台虚拟机可以正常启动，再执行脚本 `grade` 评分。

如果无法启动，参照破解 `root` 密码过程，编辑 `/etc/fstab`，修正或者注释对应行，确保系统能正常启动。

```
1 [kiosk@foundation0 ~]$ grade
```