



一、系统管理部分（参考答案）

快速重置 RHCSA 练习环境，请执行：

```
[root@room9pc13.tedu.cn ~]# rht-vmctl reset classroom //先重置资源服务器
[root@room9pc13.tedu.cn ~]# rht-vmctl reset server //再重置虚拟机
```

#####

00a、重设 root 密码

- 1) 重启虚拟机 server，出现 GRUB 启动菜单时按 e 键进入编辑状态
- 2) 找到 linux16 所在行，末尾添加 **rd.break console=tty0**，按 Ctrl+x 键进入恢复模式
- 3) 以可写方式挂载硬盘中的根目录，并重设 root 密码：

```
switch_root:/# mount -o remount,rw /sysroot //以可读写方式重新挂载根系统
switch_root:/# chroot /sysroot/ //切换到根系统
sh-4.2# echo redhat | passwd --stdin root //修改 root 口令为指定的字符串
sh-4.2# touch /.autorelabel //标记下一次启动重做 SELinux 标记
sh-4.2# exit
switch_root:/# reboot
```

00b、配置主机名、IP 地址/掩码/默认网关/DNS 地址

```
[root@server0 ~]# hostnamectl set-hostname server0.example.com
[root@server0 ~]# nmcli connection show //获取连接名
[root@server0 ~]# nmcli connection modify "连接名" ipv4.method manual ipv4.addresses
"172.25.0.11/24 172.25.0.254" ipv4.dns 172.25.254.254
[root@server0 ~]# nmcli connection modify "连接名" connection.autoconnect yes
[root@server0 ~]# nmcli connection up "连接名"
```

#####

01. 为您的系统指定一个默认的软件仓库

```
[root@server0 ~]# yum-config-manager --add http://content.example.com/rhel7.0/x86_64/dvd //添加指定软件源
[root@server0 ~]# vim /etc/yum.conf
gpgcheck=0 //找到此行，把原来的 1 改为 0，不检查软件签名
[root@server0 ~]# yum repolist //确认配置结果
```

02. 配置一个用户帐户

```
[root@server0 ~]# useradd -u 3456 athena
[root@server0 ~]# echo tomato | passwd --stdin athena
```

03. 管理用户账号、组账号

```
[root@server0 ~]# groupadd teachers
```



```
[root@server0 ~]# useradd -G teachers jerry
[root@server0 ~]# useradd -G teachers tom
[root@server0 ~]# useradd -s /sbin/nologin huloo

[root@server0 ~]# echo tomato | passwd --stdin jerry
[root@server0 ~]# echo tomato | passwd --stdin tom
[root@server0 ~]# echo tomato | passwd --stdin huloo
```

04. 复制文件并配置文件权限

```
[root@server0 ~]# cp /etc/fstab /var/tmp/fstab
[root@server0 ~]# setfacl -m u:jerry:rw /var/tmp/fstab
[root@server0 ~]# setfacl -m u:tom:- /var/tmp/fstab
```

05. 创建共用目录

```
[root@server0 ~]# mkdir /home/rhcedir

[root@server0 ~]# chown :teachers /home/rhcedir
[root@server0 ~]# chmod ug=rwx,o=rwx /home/rhcedir
[root@server0 ~]# chmod g+s /home/rhcedir
```

06. 配置 cron 计划任务

```
[root@server0 ~]# systemctl restart crond
[root@server0 ~]# systemctl enable crond

[root@server0 ~]# crontab -e -u jerry
30 10 * * * /bin/echo haha > /tmp/jerry.log
```

07. 升级 Linux 系统内核

```
[root@f0 ~]# LANG= firefox http://classroom/content/rhel7.0/x86\_64/errata/Packages/
//从浏览器访问所给的地址，找到内核 rpm 文件的下载地址
//如果 Firefox 右键菜单乱码，请添加 LANG= 改运行环境

[root@server0 ~]# yum -y install http://.../kernel-3.10.0-123.1.2.el7.x86\_64.rpm
//请耐心等待安装完成，千万不要强行中断!!!

[root@server0 ~]# reboot //重启以使新内核生效
[root@server0 ~]# uname -r
3.10.0-123.1.2.el7.x86_64 //确认新内核版本
```



08. 绑定到 LDAP 验证服务

```
[root@server0 ~]# yum -y install sssd
[root@server0 ~]# authconfig-tui //使用简易配置工具
```

根据提示完成用户和认证方式设置 ——

User Information: [*] Use LDAP

Authentication Method: [*] Use LDAP Authentication

根据提示选中 [*] Use TLS, 并设置下列参数 ——

Server: classroom.example.com

Base DN: dc=example,dc=com

提示下载证书到 /etc/openldap/cacerts 目录时, 另开一终端执行:

```
[root@server0 ~]# cd /etc/openldap/cacerts/
[root@server0 ~]# wget http://classroom.example.com/pub/example-ca.crt
```

然后回到 authconfig-tui 工具确认, 稍等片刻即可。

```
[root@server0 ~]# systemctl restart sssd
[root@server0 ~]# systemctl enable sssd

[root@server0 ~]# id ldapuser0 //验证 LDAP 用户
uid=170(ldapuser0) gid=170(ldapuser0) groups=170(ldapuser0)
```

09. 配置 autofs 按需挂载

```
[root@server0 ~]# yum -y install autofs

[root@server0 ~]# vim /etc/auto.master //设置监控点（主目录的上一层）
/home/guests /etc/guests.rule //由 guests.rule 文件给出具体挂载策略

[root@server0 ~]# vim /etc/guests.rule //配置挂载策略
ldapuser0 -rw classroom.example.com:/home/guests/ldapuser0

[root@server0 ~]# systemctl start autofs
[root@server0 ~]# systemctl enable autofs

[root@server0 ~]# su - ldapuser0 -c 'pwd' //验证结果
/home/guests/ldapuser0
```

10. 配置 NTP 网络时间客户端

```
[root@server0 ~]# vim /etc/chrony.conf
#server 0.rhel.pool.ntp.org iburst //注释掉默认的 server 配置,
#server 1.rhel.pool.ntp.org iburst
#server 2.rhel.pool.ntp.org iburst
#server 3.rhel.pool.ntp.org iburst
server classroom.example.com iburst //添加新的配置
[root@server0 ~]# systemctl restart chronyd
[root@server0 ~]# systemctl enable chronyd

[root@server0 ~]# timedatectl //查看状态
NTP enabled: yes //检查 NTP 是否已经启用
```



11. 查找文件

```
[root@server0 ~]# mkdir /root/results //确认已提前建好目录
[root@server0 ~]# find / -user student -type f -exec cp -p {} /root/results/ \;
```

12. 查找文本内容

```
[root@server0 ~]# grep 'tasia' /usr/share/dict/words > /root/wlist
```

13. 创建一个归档

```
[root@server0 ~]# tar -jcpf /root/backup.tar.bz2 /usr/local/
```

14. 创建一个逻辑卷

注(1): 考试时直接操作磁盘/dev/vda (包含 Linux 系统), 使用剩余空间完成考题要求

注(2): 练习时需要自行处理/dev/vdb, 模拟成“已使用部分空间+剩余空间”的磁盘练习环境

0) 练习环境的磁盘环境准备

```
[root@server0 ~]# fdisk /dev/vdb
Command (m for help): n //新建
Partition type:
  p   primary (0 primary, 0 extended, 4 free)
  e   extended
Select (default p): p //主分区
Partition number (1-4, default 1): 1 //分区编号 1
First sector (2048-20971519, default 2048): //起始位置默认
Last sector, +sectors or +size[K,M,G] (2048-20971519, default 20971519): +200M //结束位置+200MiB
Partition 1 of type Linux and of size 200 MiB is set
Command (m for help): n //新建
Select (default p): p //主分区
Partition number (2-4, default 2): 2 //分区编号 2
First sector .. .: //起始位置默认
Last sector, .. .: +2000M //结束位置+2000MiB
Partition 2 of type Linux and of size 2 GiB is set
Command (m for help): n //新建
Select (default p): p //主分区
Partition number (3,4, default 3): 3 //分区编号 3
First sector .. .: //起始位置默认
Last sector, .. .: +1000M //结束位置+1000MiB
Partition 3 of type Linux and of size 1000 MiB is set
Command (m for help): p //确认分区结果
  Device Boot      Start         End      Blocks    Id  System
/dev/vdb1          2048        411647        204800    83  Linux
/dev/vdb2        411648        4507647        2048000    83  Linux
/dev/vdb3        4507648        6555647        1024000    83  Linux
Command (m for help): w //保存分区结果
```



```
[root@server0 ~]# partprobe /dev/vdb //刷新分区表

[root@server0 ~]# vgcreate systemvg /dev/vdb1 //创建卷组
Physical volume "/dev/vdb1" successfully created
Volume group "systemvg" successfully created

[root@server0 ~]# lvcreate -n vo -L 180M systemvg //创建逻辑卷
Logical volume "vo" created

[root@server0 ~]# lvscan //确认结果
ACTIVE          '/dev/systemvg/vo' [180.00 MiB] inherit

[root@server0 ~]# mkfs.ext3 /dev/systemvg/vo //格式化
```

1) 综合所有需要磁盘空间的题目，规划分区方案（此步结果用于 14、15、16 题）

```
[root@server0 ~]# fdisk /dev/vdb
Command (m for help): n //新建
Partition type:
  p   primary (3 primary, 0 extended, 1 free)
  e   extended
Select (default e): e //扩展分区
Selected partition 4
First sector (6555648-20971519, default 6555648): //起始位置默认
Last sector, +sectors or +size{K,M,G} .. .): //结束位置默认

Command (m for help): n //新建
First sector (6557696-20971519, default 6557696): //起始位置默认
Last sector, +sectors or +size{K,M,G} .. .): +500M //结束位置 +500MiB (卷组扩容用)
Partition 5 of type Linux and of size 500 MiB is set

Command (m for help): n //新建
First sector (7583744-20971519, default 7583744): //起始位置默认
Last sector, +sectors or +size{K,M,G} .. .): +2000M //结束位置 +2000MiB (自定义卷组用)
Partition 6 of type Linux and of size 2 GiB is set

Command (m for help): n //新建
First sector (11681792-20971519, default 11681792): //起始位置默认
Last sector, +sectors or +size{K,M,G} .. .): +512M //结束位置 +512MiB (交换分区用)
Partition 7 of type Linux and of size 512 MiB is set

Command (m for help): p
  Device Boot      Start         End      Blocks   Id  System
... ..
/dev/vdb4          6555648      20971519      7207936    5  Extended
/dev/vdb5          6557696       7581695       512000   83  Linux
/dev/vdb6          7583744     11679743     2048000   83  Linux
/dev/vdb7         11681792     12730367      524288   83  Linux

Command (m for help): w //保存分区更改
[root@server0 ~]# partprobe /dev/vdb //刷新分区表

[root@server0 ~]# reboot //重启一次!! 确保新分区表生效
```



2) 新建卷组

```
[root@server0 ~]# vgcreate -s 16MiB datastore /dev/vdb6 //创建时指定 PE 大小
```

3) 新建逻辑卷

```
[root@server0 ~]# lvcreate -l 50 -n database datastore
```

4) 格式化及挂载使用

```
[root@server0 ~]# mkfs.ext3 /dev/datastore/database
[root@server0 ~]# mkdir /mnt/database
[root@server0 ~]# vim /etc/fstab
/dev/datastore/database /mnt/database ext3 defaults 0 0
[root@server0 ~]# mount -a
```

15. 逻辑卷扩容

1) 检查 vo 逻辑卷的大小，及所在卷组

```
root@server0 ~]# lvscan
ACTIVE                '/dev/systemvg/vo' [180.00 MiB] inherit
```

2) 为卷组扩容（若 vo 所在卷组的剩余空间足够，可以直接 lvextend 扩逻辑卷）

```
[root@server0 ~]# vgextend systemvg /dev/vdb5 //将预备好的分区 vdb5 扩展到卷组
```

3) 扩展逻辑卷

```
[root@server0 ~]# lvextend -L 300MiB /dev/systemvg/vo //扩展逻辑卷
[root@server0 ~]# resize2fs /dev/systemvg/vo //更新逻辑卷大小
```

16. 添加新的 swap 分区

```
[root@server0 ~]# mkswap /dev/vdb7 //格式化预备好的分区 vdb7
[root@server0 ~]# vim /etc/fstab
/dev/vdb7 swap swap defaults 0 0

[root@server0 ~]# swapon -a
[root@server0 ~]# swapon -s //查看交换分区信息
```



二、综合应用部分（参考答案）

快速重置 RHCE 练习环境，请执行：

```
[root@room9pc13.tedu.cn ~]# rht-vmctl reset classroom //先重置资源服务器
[root@room9pc13.tedu.cn ~]# rht-vmctl reset server //再重置虚拟机 1
[root@room9pc13.tedu.cn ~]# reset desktop //再重置虚拟机 2
```

01. 配置 SELinux

```
[root@server0 ~]# vim /etc/selinux/config //配置开机自动开启 SELinux
SELINUX=enforcing
[root@server0 ~]# setenforce 1 //临时开启 SELinux
[root@server0 ~]# getenforce //查看结果
Enforcing
```

02. 配置 SSH 访问控制

```
[root@server0 ~]# vim /etc/ssh/sshd_config
...
DenyUsers *@*.unknown.org *@172.34.0.* //网段地址以考试说明为准
[root@server0 ~]# systemctl restart sshd
```

03. 自定义用户环境（别名设置）

```
[root@server0 ~]# vim /etc/bashrc
alias qstat='/bin/ps -Ao pid,tt,user,fname,rsz'

[root@server0 ~]# su - student //切换为任意现有用户
[student@server0 ~]$ qstat //测试执行别名 qstat 都可用
```

04. 配置防火墙端口转发

```
[root@server0 ~]# systemctl restart firewalld
[root@server0 ~]# systemctl enable firewalld
```

//调整防火墙信任区域（设为 trusted），简化对后续各种服务的防护

```
[root@server0 ~]# firewall-cmd --set-default-zone=trusted
```

//阻止未授权网络 unknown.org 的网段

```
[root@server0 ~]# firewall-cmd --permanent --add-source=172.34.0.0/24 --zone=block
```

//实现端口 5423 => 80 端口转发

```
[root@server0 ~]# firewall-cmd --permanent --zone=trusted --add-forward-
port=port=5423:proto=tcp:toport=80
[root@server0 ~]# firewall-cmd --reload
```



05. 配置链路聚合

1) 新建聚合链接

```
[root@server0 ~]# nmcli connection add con-name team0 type team ifname team0 config '{ "runner": { "name": "activebackup" } }' //建立主连接
[root@server0 ~]# nmcli connection add con-name team0-p1 type team-slave ifname eth1 master team0 //指定成员网卡 1
[root@server0 ~]# nmcli connection add con-name team0-p2 type team-slave ifname eth2 master team0 //指定成员网卡 2
[root@server0 ~]# nmcli con modify team0 ipv4.method manual ipv4.addresses "172.16.3.20/24" connection.autoconnect yes //为聚合连接配置 IP 地址
```

2) 设置自动连接 (通常情况下, 默认是已经设置好的)

```
[root@server0 ~]# nmcli con modify team0 connection.autoconnect yes
[root@server0 ~]# nmcli con modify team0-p1 connection.autoconnect yes
[root@server0 ~]# nmcli con modify team0-p2 connection.autoconnect yes
```

3) 激活连接并检查

```
[root@server0 ~]# nmcli connection up team0 //激活聚合连接
[root@server0 ~]# teamdctl team0 state //确认连接状态
```

注(1): 此考点在 desktop0 的配置与 server0 几乎完全相同 (只是 IP 地址不一样)。

06. 配置 IPv6 地址

```
[root@server0 ~]# nmcli connection show //获知 eth0 的连接名称
NAME          UUID                                  TYPE          DEVICE
System eth0    5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03 802-3-ethernet eth0

[root@server0 ~]# nmcli connection modify "连接名" ipv6.method manual \
    ipv6.addresses 2003:ac18::305/64
[root@server0 ~]# nmcli connection up "连接名"
```

07. 配置本地邮件服务

1) 在虚拟机 server0 上

```
[root@server0 ~]# hostnamectl set-hostname server0.example.com //正确设置静态主机名, 避免邮箱域识别错误

[root@server0 ~]# vim /etc/postfix/main.cf //调整邮件服务配置
relayhost = [smtp0.example.com] //后端邮件服务器
inet_interfaces = loopback-only //仅本机
myorigin = desktop0.example.com //发件来源域
mynetworks = 127.0.0.0/8, [::1]/128 //信任网络
mydestination = //此行的值设为空

[root@server0 ~]# systemctl restart postfix
[root@server0 ~]# systemctl enable postfix

[root@server0 ~]# echo 'I am king.' | mail -s 'Test1' student //在 server0 发测试邮件
```




2) 在虚拟机 desktop0 上

注(1): 考试时 desktop0 的配置与 server0 完全相同(后端邮件服务器由考场提供, 无需考生配置)

注(2): 练习时需在 desktop0 上执行 `lab smtp-nullclient setup`, 将其配置为后端邮件服务器

```
[root@desktop0 ~]# hostnamectl set-hostname desktop0.example.com
//正确设置静态主机名, 避免邮箱域识别错误
[root@desktop0 ~]# mail -u student
//练习时在 desktop0 应能收到测试邮件
...
//考试时访问题目给出的网址, 应能看到测试邮件
```

08. 配置默认 web 站点

```
[root@server0 ~]# yum -y install httpd
[root@server0 ~]# vim /etc/httpd/conf.d/00-default.conf //添加第一个(默认)虚拟主机
<VirtualHost *:80>
    ServerName server0.example.com
    DocumentRoot /var/www/html
</VirtualHost>
[root@server0 ~]# cd /var/www/html/
[root@server0 html]# wget http://classroom/pub/materials/station.html -O index.html
[root@server0 html]# systemctl restart httpd
[root@server0 html]# systemctl enable httpd
```

09. 配置虚拟主机

```
[root@server0 ~]# mkdir /var/www/virtual

[root@server0 ~]# cd /var/www/virtual/
[root@server0 virtual]# wget http://classroom/pub/materials/www.html -O index.html

[root@server0 virtual]# vim /etc/httpd/conf.d/01-www0.conf
<VirtualHost *:80>
    ServerName www0.example.com
    DocumentRoot /var/www/virtual
</VirtualHost>

[root@server0 virtual]# chown -R hary /var/www/virtual/
[root@server0 virtual]# systemctl restart httpd
```

10. 配置安全 web 服务

1) 安装 mod_ssl 软件包

```
[root@server0 ~]# yum -y install mod_ssl
```

2) 下载并部署网站证书、密钥、根证书

```
[root@server0 ~]# cd /etc/pki/tls/certs/
[root@server0 certs]# wget http://classroom/pub/example-ca.crt //部署网站证书
[root@server0 certs]# wget http://classroom/pub/tls/certs/server0.crt //部署根证书

[root@server0 certs]# cd /etc/pki/tls/private/
[root@server0 private]# wget http://classroom/pub/tls/private/server0.key //部署网站密钥
```



3) 调整虚拟 Web 主机配置 ssl.conf

```
[root@server0 private]# vim /etc/httpd/conf.d/ssl.conf
<VirtualHost _default_:443>
    DocumentRoot "/var/www/html"           //设置站点根目录
    ServerName server0.example.com:443     //设置站点名称
    ... ..                                  //搜 localhost, 找到并修改以下行
    SSLCertificateFile /etc/pki/tls/certs/server0.crt
    SSLCertificateKeyFile /etc/pki/tls/private/server0.key
    SSLCACertificateFile /etc/pki/tls/certs/example-ca.crt
</VirtualHost>

[root@server0 private]# systemctl restart httpd
```

11. 配置 web 内容的访问

```
[root@server0 ~]# mkdir /var/www/html/private
[root@server0 ~]# cd /var/www/html/private/
[root@server0 private]# wget http://classroom/pub/materials/private.html -O index.html

[root@server0 private]# vim /etc/httpd/conf.d/00-default.conf
... ..
<Directory /var/www/html/private>
    Require ip 127.0.0.1 ::1 172.25.0.11 //仅允许本机 IP 访问
</Directory>

[root@server0 private]# systemctl restart httpd
```

12. 实现动态 WEB 内容

```
[root@server0 ~]# yum -y install mod_wsgi
[root@server0 ~]# mkdir /var/www/webapp0

[root@server0 ~]# cd /var/www/webapp0
[root@server0 webapp0]# wget http://classroom/pub/materials/webinfo.wsgi

[root@server0 webapp0]# vim /etc/httpd/conf.d/02-alt.conf
Listen 8909
<VirtualHost *:8909>
    ServerName webapp0.example.com
    DocumentRoot /var/www/webapp0
    WSGIScriptAlias / /var/www/webapp0/webinfo.wsgi
</VirtualHost>

[root@server0 webapp0]# semanage port -a -t http_port_t -p tcp 8909 //突破 SELinux 限制
[root@server0 webapp0]# systemctl restart httpd
```

13. 通过 Samba 发布共享目录

```
[root@server0 ~]# yum -y install samba
[root@server0 ~]# mkdir /common
[root@server0 ~]# setsebool -P samba_export_all_rw=on //取消 SELinux 限制
```



```
[root@server0 ~]# useradd harry //此账号考试时或已提供
[root@server0 ~]# pdbedit -a harry //启用共享账号 harry、设置密码
[root@server0 ~]# vim /etc/samba/smb.conf
[global]
    workgroup = STAFF //修改此行，指定工作组名
[common]
    path = /common
    hosts allow = 172.25.0.0/24 //只允许指定网段访问
[root@server0 ~]# systemctl restart smb nmb
[root@server0 ~]# systemctl enable smb nmb
```

注(1)：为安全起见，建议直接调整共享目录的安全属性（而不调整全局布尔值）

```
[root@server0 ~]# semanage fcontext -a -t samba_share_t '/common(/.*)?'
[root@server0 ~]# restorecon -R /common //设置目录 SELinux 属性
```

14. 配置多用户 Samba 挂载

1) 在虚拟机 server0 上

```
[root@server0 ~]# mkdir /devops //若无目录，应提前建好
[root@server0 ~]# useradd kenji //此账号考试时默认应已提供
[root@server0 ~]# pdbedit -a kenji //启用共享账号 kenji、设置密码
[root@server0 ~]# useradd chihiro //此账号考试时默认应已提供
[root@server0 ~]# pdbedit -a chihiro //启用共享账号 chihiro、设置密码
[root@server0 ~]# setfacl -m u:chihiro:rwX /devops/ //设置写入权限

[root@server0 ~]# vim /etc/samba/smb.conf
[devops]
    path = /devops
    write list = chihiro
    hosts allow = 172.25.0.0/24 //只允许指定网段访问
[root@server0 ~]# systemctl restart smb nmb //重启
```

注(1)：为安全起见，建议直接调整共享目录的安全属性（而不调整全局布尔值）

```
[root@server0 ~]# semanage fcontext -a -t samba_share_t '/devops(/.*)?'
[root@server0 ~]# restorecon -R /devops //设置目录 SELinux 属性
```

2) 在虚拟机 desktop0 上

```
[root@desktop0 ~]# yum -y install samba-client cifs-utils
[root@desktop0 ~]# smbclient -L server0 //检查对方提供了哪些共享
... //无需密码，直接按 Enter 键确认
[root@desktop0 ~]# mkdir /mnt/dev //创建好挂载点
[root@desktop0 ~]# vim /etc/fstab
//server0.example.com/devops /mnt/dev cifs
username=kenji,password=atenorth,multiuser,sec=ntlmssp,_netdev 0 0
[root@desktop0 ~]# mount -a //检查挂载配置
```

3) 验证结果（在 desktop0 上）

```
[root@desktop0 ~]# su - student //切换到普通用户
[student@desktop0 ~]$ cifscreds add -u chihiro server0 //临时切换为 chihiro 身份
Password: //提供 Samba 用户 chihiro 的密码
```



```
[student@desktop0 ~]$ touch /mnt/dev/b.txt //确认有写入权限（新建文件）
```

注(2)：为安全起见，建议不要将密码直接存入/etc/fstab 文件

```
[root@desktop0 ~]# vim /etc/fstab
//server0.example.com/devops /mnt/dev cifs
credentials=/root/smb.pass,multiuser,sec=ntlmssp,_netdev 0 0

[root@desktop0 ~]# vim /root/smb.pass
username=kenji
password=atenorth
```

15. 配置 NFS 共享服务

注(1)：考试时 LDAP+Kerberos 环境预先已配置好，用户 ldapuser0 可以直接使用

注(2)：练习时需在 server0 上执行 lab nfskrb5 setup，由脚本快速配置好 LDAP+Kerberos 环境

```
[root@server0 ~]# mkdir -p /public /protected/project
[root@server0 ~]# chown ldapuser0 /protected/project/

[root@server0 ~]# wget -O /etc/krb5.keytab http://classroom/pub/keytabs/server0.keytab

[root@server0 ~]# vim /etc/exports
/public 172.25.0.0/24(ro)
/protected 172.25.0.0/24(rw,sec=krb5p)

[root@server0 ~]# systemctl start nfs-secure-server nfs-server //启用两个系统服务
[root@server0 ~]# systemctl enable nfs-secure-server nfs-server
```

16. 挂载 NFS 共享

注(1)：考试时 LDAP+Kerberos 环境预先已配置好，用户 ldapuser0 可以直接使用

注(2)：练习时需在 desktop0 上执行 lab nfskrb5 setup，由脚本快速配置好 LDAP+Kerberos 环境

```
[root@desktop0 ~]# mkdir -p /mnt/nfsmount /mnt/nfssecure
[root@desktop0 ~]# wget -O /etc/krb5.keytab http://classroom/pub/keytabs/desktop0.keytab

[root@desktop0 ~]# systemctl start nfs-secure //启用安全 NFS 的客户端服务
[root@desktop0 ~]# systemctl enable nfs-secure

[root@desktop0 ~]# showmount -e server0 //检查对方提供了哪些共享
Export list for server0:
/protected 172.25.0.0/24
/public 172.25.0.0/24

[root@desktop0 ~]# vim /etc/fstab
server0.example.com:/public /mnt/nfsmount nfs _netdev 0 0
server0.example.com:/protected /mnt/nfssecure nfs sec=krb5p,_netdev 0 0

[root@desktop0 ~]# mount -a //测试挂载配置

[root@desktop0 ~]# ssh ldapuser0@desktop0 //SSH 登入以领取通行证
ldapuser0@desktop0's password: //密码 kerberos（见考试说明）
[ldapuser0@desktop0 ~]$ touch /mnt/nfssecure/project/a.txt //写入测试
```



注(3)：为避免 desktop0 重启后挂载延迟，可以考虑做如下开机设置

```
[root@desktop0 ~]# chmod +x /etc/rc.d/rc.local //为开机脚本添加 x 权限
[root@desktop0 ~]# vim /etc/rc.d/rc.local //在文件末尾添加“补刀”操作
for i in {1..20}
do
    systemctl status nfs-secure || systemctl restart nfs-secure
    mount -a
    sleep 5
done &
```

17. 配置 iSCSI 服务端

1) 准备磁盘空间

```
[root@server0 ~]# fdisk /dev/vdb
Command (m for help): n // n 新建分区
Partition number (1-128, default 1): //接受默认分区编号
First sector (34-20971486, default 2048): //起始位置默认
Last sector, +sectors or +size {K, M, G, T, P} (2048-20971486, default 20971486): +3G
//结束位置设置 +3G
Command (m for help): w // w 保存分区更改
...
[root@server0 ~]# partprobe /dev/vdb //刷新分区表
```

2) 安装、配置 iSCSI 磁盘

```
[root@server0 ~]# yum -y install targetcli
[root@server0 ~]# targetcli
/> backstores/block create iscsi_store /dev/vdb1 //定义后端存储
/> /iscsi create iqn.2016-02.com.example:server0 //创建 iqn 对象
/> /iscsi/iqn.2016-02.com.example:server0/tpg1/acls create iqn.2016-02.com.example:desktop0
//授权客户机 (的 IQN)
/> /iscsi/iqn.2016-02.com.example:server0/tpg1/luns create /backstores/block/iscsi_store
//绑定存储
/> /iscsi/iqn.2016-02.com.example:server0/tpg1/portals create 172.25.0.11 3260
//指定监听地址 (本机 IP 及端口)
/> saveconfig //保存配置结果 (缺省)
/> exit
```

3) 启用 target 服务

```
[root@server0 ~]# systemctl restart target
[root@server0 ~]# systemctl enable target
```

18. 配置 iSCSI 客户端

```
[root@desktop0 ~]# yum -y install iscsi-initiator-utils
[root@desktop0 ~]# vim /etc/iscsi/initiatorname.iscsi //设置本机 iqn 名称
InitiatorName=iqn.2016-02.com.example:desktop0
[root@desktop0 ~]# systemctl restart iscsid //起 iscsid 服务以更新 iqn 名称

[root@desktop0 ~]# iscsiadm -m discovery -t st -p server0 //发现磁盘
```



```
[root@desktop0 ~]# iscsiadm -m node -L all //手动连接磁盘测试
[root@desktop0 ~]# systemctl enable iscsi //将 iscsi 服务设为开机自启
[root@desktop0 ~]# lsblk //确认多出的磁盘，比如/dev/sda

[root@desktop0 ~]# fdisk /dev/sda
Command (m for help): n // n 新建分区
Partition number (1-128, default 1): //接受默认分区编号
First sector (34-20971486, default 2048): //起始位置默认
Last sector, +sectors or +size {K, M, G, T, P} (2048-20971486, default 20971486): +2100M //结束位置设置 +2100M
Command (m for help): w // w 保存分区更改
.. ..
[root@desktop0 ~]# partprobe /dev/sda //刷新分区表
[root@desktop0 ~]# mkfs.ext4 /dev/sda1 //按要求格式化分区
[root@desktop0 ~]# mkdir /mnt/data //创建挂载点
[root@desktop0 ~]# vim /etc/fstab //提前用 blkid 找到分区 UUID
UUID="6ff20bb3-7543-4fa0-b4fa-bdc99a1e63ce" /mnt/data ext4 _netdev 0 0

[root@desktop0 ~]# mount -a
[root@desktop0 ~]# sync ; reboot -f //先存盘再强制重启，避免卡死
```

19. 编写简单脚本

```
[root@server0 ~]# vim /root/foo.sh
#!/bin/bash
if [ "$1" = "redhat" ] ; then
    echo "fedora"
elif [ "$1" = "fedora" ] ; then
    echo "redhat"
else
    echo "/root/foo.sh redhat|fedora" >&2 //将正常输出变为错误输出
    exit 2 //返回非零值
fi
[root@server0 ~]# chmod +x /root/foo.sh
```

20. 编写批量添加用户的脚本

```
[root@server0 ~]# vim /root/batchusers
#!/bin/bash
if [ $# -eq 0 ] ; then
    echo "Usage: /root/batchusers <userfile>"
    exit 1
fi
if [ ! -f $1 ] ; then
    echo "Input file not found"
    exit 2
fi
for name in $(cat $1)
do
    useradd -s /bin/false $name
done
[root@server0 ~]# chmod +x /root/batchusers
```



21. 配置一个数据库

1) 安装、配置

```
[root@server0 ~]# yum -y install mariadb-server mariadb
[root@server0 ~]# vim /etc/my.cnf
[mysqld]
skip-networking                                     //添加此行, 跳过网络
[root@server0 ~]# systemctl restart mariadb
[root@server0 ~]# systemctl enable mariadb
```

2) 设密码、建库

```
[root@server0 ~]# mysqladmin -u root password 'atenorth' //无密码情况下, 设新密码
[root@server0 ~]# mysql -u root -patenorth
MariaDB [(none)]> CREATE DATABASE Contacts;
MariaDB [(none)]> GRANT select ON Contacts.* to Raikon@localhost IDENTIFIED BY 'atenorth';
MariaDB [(none)]> DELETE FROM mysql.user WHERE Password=''; //删除空密码的账号
//!!注意: 设好 root 密码再做
MariaDB [(none)]> QUIT
```

3) 导入库

```
[root@server0 ~]# wget http://classroom/pub/materials/users.sql
[root@server0 ~]# mysql -u root -patenorth Contacts < users.sql
```

22. 数据库查询 (填空)

```
[root@server0 ~]# mysql -u root -patenorth
Enter password:
MariaDB [(none)]> USE Contacts; //选库
MariaDB [Contacts]> SHOW TABLES; //了解有哪些表
MariaDB [Contacts]> DESC XX 表名; //了解 XX 表有哪些列

MariaDB [Contacts]> SELECT name FROM base WHERE password='solicitous';
+-----+
| name |
+-----+
| James |
+-----+

MariaDB [Contacts]> SELECT count(*) FROM base,location WHERE base.name='Barbara' AND
location.city='Sunnyvale' AND base.id=location.id ;
1
MariaDB [Contacts]> QUIT
```

#####