上午 2.5 小时 rhcsa，下午 4 小时 rhce。上午时间充裕，下午时间相对紧张，下午我用 2 小时做完所有题目，半小时检查测试，预计学生很难在 4 小时内作为所有 20 道题。考试题目可以选择简体中文，但是建议中英文切换着看，有些地方翻译的不严谨，且中文断句上有问题，某些地方少个逗号意思就变了。

上午 rhcsa 考试内容：

一台虚拟机 system1,网络环境为 desktopX.example.com（172.250.X.0/24）,有一个禁止网络 xjxx.com (172.10.0.0/24)

0. 首先需要进入需要重置 Root 密码为 ooxxbalabala，然后按要求设置 system1 的网络和主机名，正常连接网络后才能看到后续的试题。
1. 配置 SELinux 环境，将 system1 的 SELinux 设为 enforcing 模式。
2. 按照要求建立 Yum 软件仓库配置文件后续如果按转软件包需要这个 Yum 仓库为默认仓库。
3. 调整指定 LVM 的卷及其上文件系统大小。
4. 按要求创建用户组及多个用户，设置用户的候选组，设置用户的默认 shell。
5. 按要求设置文件及目录权限，会用到文件 acl 权限。
6. 设置用户的计划任务 cron。
7. 设置带 sgid 的目录权限。
8. 按指定要求安装升级内核，保证 grub2 启动时为默认项目。
9. 使用 LDAP 作为本地用户认证方式，需要设置域、服务器位置和下载 key。
10. 设置 NTP 服务，同步指定服务器时间。NTP 服务器程序改为 chrony。
11. 配置和 LDAP 用户认证配合的 autofs 自动目录挂接。
12. 用户配置，和创建用户题目类似，创建指定 uid 或 gid 的用户。
13. 创建新的指定大小的 swap 分区，需要写入 fstab 自动开机挂接，分区的时候注意，后面还要创建新 LVM 卷的时候还需要一个分区。
14. 查找属于特定用户或组的文件，并将其拷贝到指定目录。
15. 在文件中查找指定的字符串，将其输出到指定文件。
16. 创建指定目录的压缩的归档文件，例如 backup.tar.bz2。
17. 创建指定大小的逻辑卷，需要自己创建分区、物理卷、逻辑卷组和逻辑卷。逻辑卷组是指定特殊 PE 大小的。

下午 rhce 考试内容：

两台虚拟机 system1 和 system2。system1 是服务器，主要设置 system1；system2 可以看作是客户端，但一些题目是两台虚拟机都要配置完成。

1. 配置 system1 和 sysytm2 上的 SELinux 环境为 enforcing
   编辑/etc/selinux/config ,修改 SELINUX=enforcing
2. 配置 system1 和 system2 上的 SSH 访问控制，拒绝一个 xjxx.com (172.10.0.0/24)网段的访问
   编写 firewall-cmd 规则或使用 firewall-config 配置一条 Rich Rule，Reject 那个网段
3. 配置基本 samba 配置和 multiuser smb 配置，这是多道题，包括在 system1 上配置 samba 的工作组，设置共享目录和共享权限；system2 上只是 multiuser 方式自动挂接。
   （1） 服务端#semanage fcontext –a –t samba_share_t '/dirpath/(/.*)？'
   （2） [dirname]
   path = /dirpath

write list = username

（3） 配置服务端 firewalld

#firewall-cmd –permanent –add-service=samba

（4） 服务端启动 smb 和 nmb 服务

#systemctl enable smb nmb

#systemctl start smb nmb

（5） 客户端/etc/fstab 中加入

//server_name/path /mount_dir cifs cred=/multiuser.txt_path,multiuser,sec=ntlmssp 0 0

（6） Multiuser.txt 文件样式如下

username=username

password=password

4. 基本 nfs 配置和 security nfs 配置，这是两道题，包括 system1 的简单 sec=system 导出和基于 sec=krb5p 的认证导出；system2 的基于 nfs-secure 的自动挂机。

（1） 服务端安装 nfs-secure-server，客户端安装 nfs-secure

（2） 把下载的 keytab 文件命名为/etc/krb5.keytab

（3） 服务端启动 nfs-sercure-server.service,客户端启动 nfs-secure.service

（4） 服务器端导出项目 sec=krb5p,在/etc/sysconfig/nfs 中配置 RPCNFSDARGS=”-V 4.2”, 客户端 fstab 中需要写 defaults,v4.2,sec=krb5p

（5） 配置服务端 firewalld

#firewall-cmd –permanent –add-service=nfs

5. 配置聚合链路，需要在 system1 和 system2 上配置 eth1 和 eth2 任意一个设备损坏网络都可以正常访问。

（1） 使用 nm-connection-editor 配置 team，按要求添加 Team，配置 connection name 和 ip ，在 Team 标签中添加 Ethernet， 配置 team slave 设备，不要忘了 Genera 标签中的 Auto connect 。复制 Device Mac address 有风险，建议在配置文件中添加 DEVICE=所对应的设备。

（2） 在 Team 配置中 JSON config 框中填入

{“runner”: {“name”: “activebackup”}}

（3） 使用# teamdctl team0 state 查看一下状态，同时 ping 一下测试

6. 端口转发配置，配置 system1 上的某个端口转发到本地的 80 端口。

（1） 直接使用 firewall-cmd 或 firewall-config 配置转发规则

（2） 需要注意 Zone，在默认 Zone 中配置，或修改默认 Zone。

（3） 配置 firewall-configure 时需要注意 Configuration 需要设置为 Permanent，配置后需要 Options->Reload Firewalld

7. IPV6 配置，system1 和 system2 都要配置 eth0 上的 ipv6 地址，并且可以相互 ping 通。

（1） 使用 nm-connection-edit 配置设备的 ipv6 属性

（2） 使用 ping6 测试

8. 邮件系统配置，system1 和 system2 上都要配置 postfix 为 null client 状态，会有一个测试网页查看转发后的邮件。

（1） 配置邮件系统为 null client 状态，也就是个群发邮件服务器

配置/etc/postfix/main.cf 配置文件，修改或添加如下配置

Inet_interfaces=loopback-only

mydestination= (此处为空)

relayhost=[smtp.desktopX.example.com]
myorigin=desktopX.example.com
mynetworks=127.0.0.0/8 [::1]/128
local_transport=error:local delivery diskabled
如果忘记了可以参考配置文件：
/usr/share/doc/postfix-x-x-x/README_FILES/STANDARD_CONFIGURATION_README
文件中 null client 配置部分，另外开个终端看着然后用 postconf 设置。
不要忘记用 mail 发邮件确认，通过浏览器检测一下，题目里会有提示。

9. Iscsi 配置，服务端和客户端，这是两道题。system1 配置 iscsi target，system2 配置 iscsi initiator。需要现在 system1 上分区，创建 pv、vg、lv，然后 iscsi 导出 lv。system2 上导出 iscsi 后要分区、创建文件文件系统，然后自动挂接到 system2 本地目录。

（1） 服务端配置，安装 targetcli，分区，启动 target.service 服务，使用 firewalld 打开 3260/tcp 端口，输入 targetcli 进入 iscsi 配置界面
/backstores/block create $diskname $diskpath
/iscsi create $iqn_name
/iscsi/$iqn/tpg/luns create /backstores/block/$diskname
/iscsi/$iqn/tpg/acls create $initiator_iqn
/iscsi/$iqn/tpg/portals create $localip 3260
saveconfig
exit

（2） 客户端配置，安装 iscsi-initiator-utils，配置/etc/iscsi/initiatorname.iscsi 文件，修改 InitiatorName=为$initiator_iqn，启动 iscsi.service 。使用 iscsiadm 去配置管理 iscsi，使用 lsblk 查看是否正常，在 fstab 里需要写_netdev 作为参数。

10. Web 服务，需要在 system1 上配置三个虚拟主机，分别是正常的 http://station.desktopX.example.com 、https://station.desktopX.example.com 和 http://dynamic.desktopX.example.com:8998 。配置不允许访问的 xjxx.com (172.10.0.0/24) 的网段，设置目录访问权限。从指定位置所需要的 ssl 相关密钥、index.html 文件和动态页面 webapp.wsgi。目录要自己建、防火墙规则要自己写、安全上下文要自己配、httpd 安全监听端口要自己添加。
不要忘了 systemctl enable httpd ; systemctl start httpd ; firewall-cmd –permanent –add-service=http 和其他端口

（1） 配置普通的 http-vhost
在/etc/httpd/conf.d/目录下创建配置问题 wwwX.conf
<VirtualHost *:80>
ServerName wwwX.example.com
ServerAlias wwwX
DocumentRoot /srv/wwwX.example.com/www
CustomLog “logs/wwwX.example.com.log” combined
</VirtualHost>
<Directory /srv/wwwX.example.com/www>
Require all granted
</Directory>
配置/srv/wwwX.example.com/www 的 Selinux 权限
restorecon –vvFR /srv

配置是有问题查看/usr/share/doc/httpd-x.x.x/httpd-vhosts.conf 配置模板

（2） 配置 https 的 vhost

```
<VirtualHost *:443>
  ServerName wwwX.example.com
  SSLEngine on
  SSLProtocal all –SSLv2 –SSLv3
  SSLCipherSuite HIG:MEDIUM:!aNull:!MD5
 SSLHonorCipherOrder on
 SSLCerficateFile /etc/pki/tls/certs/wwwX.crt
 SSLCerficateKeyFile /etc/pki/tls/private/wwwX.key
 SSLCerticateChainFile /etc/pki/tls/certs/example-ca.crt
 DocumentRoot /srv/wwwX/www
</VirtualHost>
<Directory /srv/wwwX/www>
    Requrie all granted
</Directory>
```

配置/srv/wwwX.example.com/www 的 Selinux 权限

```
 # restorecon –vvFR /srv
```

下载 wwwX.crt、wwwX.key、example-ca.crt 到相应的目录下，注意权限。

（3） Wsgi dynamic web

首先安装 mod_wsgi 软件包

在原有 DocumentRoot 的行替换为 WSGIScriptAlias

```
WSGIScriptAliase / /srv/weappX/www/webapp.wsgi
```

其他都和配置 http-vhost 和 https-vhost 都一样

重启 httpd.service 服务

（4） 如果需要监听其他端口请在/etc/httpd/conf.d/wwwX.conf 中加入

```
Listen  $port
```

如果是 https 协议，需加入

```
Listen $port https
```

新的监听端口需要额外操作

```
#semanger port –a –t http_port_t –p tcp $port
#firewall-cmd –permanent –add-port=$port/tcp
#firewall-cmd --reload
```

11. Shell script 编程，两道题。在 system1 上编写，需要按指定的文件名，建议配置可执行权限。

（1） 输入 bar 显示 foo，输入 foo 显示 bar，输入其他显示 Usage

精简脚本 foo.sh

```
#!/bin/bash
case $1 in
        bar )       echo “foo” ;;
        foo )       echo “bar” ;;
        *)          echo “Usage bala bala” ;;
esac
#chmod +x foo.sh
```

（2） 批量添加用户，根据指定文件作为参数添加用户，需要判断是否存在参数和用户文件是否存在，需要错误推出和退出返回值。设置/bin/false 为添加用户默认 shell。

精简脚本 mkuser

```
#!/bin/bash
[ ! $# -eq 1 ] && echo " Usage bala bala" && exit 1
[ ! –f $1 ] && echo " False bala bala" && exit 1
while read addusername ; do
  adduser –s /bin/false $addusername 2>&1 >/dev/null
done <  $1
```

12. Mariadb 数据库操作，这是两道题目。在 system1 上完成并且保证只能在 system1 上使用 mariadb。创建指定的数据库和用户，并且给用户适当的权限。使用指定文件导入数据库，多表查询数据取出数据填入考试页面然后提交。

（1） 安装 Mariadb

```
#yum groupinstall mariadb mariadb-client -y
```

（2） 配置 Mariadb root 用户只能本地登录

```
#systemctl enable mariadb ; systemctl start mariadb
#mysql_secure_installation  ( 按题目要求配置 root 的密码、关闭支持远程连接和是否删除测试库)
```

（3） 导入数据库 Concacts，授权 Luigi 用户可以 select 访问数据库

```
#mysql
MariaDB [(noe)]>create database Concacts;
#mysql –u root Concacts < mariadb.dumpfile
MariaDB [(noe)]>grant select on Concacts.* to Luigi@'%' identified by "password";
```

（4） 数据库查询，将查询结果提交

```
MariaDB [(noe)]> use database_name;
MariaDB [(noe)]> select * from table_A, table_B where table_A.item=table_B.item and table_A.item like "balabala";
```