RHCSA部分

关于密码破解，在上午的考试中需要我们自己安装图形化界面和破解root密码，root的密码按照题目的要求来进行修改。可以使用单用户模式或者使用上课讲的rd.break都可以。

rd.break方法：

删除 console=ttys0,115200n8这句话 在最后加入rd.break

进入交换模式以后输入下列指令：

mount -o remount,rw /sysroot

chroot /sysroot

passwd 密码

touch /.autorelabel

exit

reboot

图形化界面安装：

考试的时候可能需要自己安装图形化界面，如果在startx无法启动图形化的情况下可以是下面的命令进行安装：

yum –y install xorg\*

yum –y install gnome\*

yum –y install glx\*

startx后者init 5

密码修完完成，注意此处是修改的你考试用的虚拟机密码，而不是物理机密码。

关于IP地址的设置，请查看考题的其他信息里面可以看到虚拟机应该设置的IP地址信息，和主机名信息。

hostnamectl set-hostname station.domain11.example.com

nmcli connection modify eno16777736 ipv4.method manual

nmcli connection modify eno16777736 ipv4.addresses '172.24.11.10/24 172.24.11.254'

nmcli connection modify eno16777736 ipv4.dns '172.24.11.250'

nmcli connection up eno16777736

nmcli con show eno16777736 | grep ipv4

host server.domain11.example.com

route -n

IP地址也可以使用nm-connection-editor图形化界面进行修改。

修改完成以上信息以后就可以开始正式做题了。

rhel7进入单用户方式和重置密码方式发生了较大变化，GRUB由b引导变成了ctrl+x引导。

重置密码主要有rd.break和init两种方法。

rd.break方法：

1. 启动的时候，在启动界面，相应启动项，内核名称上按“e”；

2. 进入后，找到linux16开头的地方，按“end”键到最后，输入rd.break，按ctrl+x进入；

3. 进去后输入命令mount，发现根为/sysroot/，并且不能写，只有ro=readonly权限；

4. mount -o remount,rw /sysroot/，重新挂载，之后mount，发现有了r,w权限；

5. chroot /sysroot/ 改变根；

6. passwd

7. touch /.autorelabel 这句是为了selinux生效

8. ctrl+d 退出

9. 然后reboot

至此，密码修改完成

init方法：

1. 启动系统，并在GRUB2启动屏显时，按下e键进入编辑模式。

2. 在linux16/linux/linuxefi所在参数行尾添加以下内容：init=/bin/sh

3. 按Ctrl+x启动到shell。

4. 挂载文件系统为可写模式：mount –o remount,rw /

5. 运行passwd,并按提示修改root密码。

6. 如何之前系统启用了selinux，必须运行以下命令，否则将无法正常启动系统：touch /.autorelabel

7. 运行命令exec /sbin/init来正常启动，或者用命令exec /sbin/reboot重启

1. 配置SELINUX使其工作在enforcing模式下

解法：

getenforce //查看模式

setenforce 1 //设置为enforcing模式

getenforce //查看

vim /etc/selinux/config //永久修改

selinux=enforcing

：wq

重启

然后使用sestatus命令查看

1. 为您的系统配置一个默认的软件仓库

一个YUM 源已经提供了在

http://server.domain11.example.com/pub/x86\_64/Server,配置你的系统，并且能正常使用。

解法：

vim/etc/yum.reopos/base.repo

[base]

name=base

baseurl= http://server.domain11.example.com/pub/x86\_64/Server

gpgcheck=0

enable=1

保持退出

yum list进行验证，能列出软件包信息就是正确的。Yum 配置不正确会导致后面一些题目做不出来。

1. 调整逻辑卷的大小

调整逻辑卷vo的大小，它的文件系统大小应该为290M.确保这个文件系统的内容完整。注：分区很少能精确到和要求的大小相同，因此在范围270M到320M之间都是可以接受的

解法—加法

df –hT

lvextend -L +100M /dev/vg0/vo

lvscan

xfs\_growfs /home/ //home为LVM挂载的目录 这步仅仅是在我们练习的环境中需要做，考试的时候是EXT4不需要此步骤。

resize2fs /dev/vg0/vo //考试的时候用这条命令进行更新就可以了。

df –hT

解法—减法

e2fsck –f /dev/vg0/vo

umount /home

resize2fs /dev/vg0/vo 最终要求的分区容量 如100M

lvreduce –l 100M /dev/vg0/vo

mount /dev/vg0/vo /home

df -hT

1. 创建用户账号

创建下面的用户、组和组成员关系

名字为adminuser 的组

用户natasha，使用adminuser 作为附属组

用户harry，也使用adminuser 作为附属组

用户sarah，在系统商不能访问可交互的SHELL，且不是adminuser 的成员，natasha，harry，sarah密码都是redhat

解法：

groupadd adminuser

useradd natasha –G adminuser

useradd haryy –G adminuser

useradd sarah –s /sbin/nologin

passwd 用户名 //来修改密码

id natasha //查看用户组

1. 配置/var/tmp/fstab的权限

复制文件/etc/fstab到/var/tmp/fstab

配置/var/tmp/fstab的权限如下：

文件/var/tmp/fstab所有者是ROOT

文件/var/tmp/fstab属于root组

文件/var/tmp/fstab不能被任何用户执行

用户natasha可读和可写/var/tmp/fstab

用户harry不能读写/var/tmp/fstab

所有其他用户（现在和将来的）具有读/var/tmp/fstab的能力。

解法：

cp /etc/fstab /var/tmp/

ll /var/tmp/fstab 查看所有者

setfacl –m u:natasha:rw- /var/tmp/fstab

setfacl –m u:haryy:--- /var/tmp/fstab

使用getfacl /var/tmp/fstab查看权限

1. 配置一个cron任务

用户natasha必须配置一个cron job，当地时间每天14：23运行，执行：

\*/bin/echo hiya

解法：

crontab –e –u natasha

23 14 \* \* \* /bin/echo hiya

crontab –l –u natasha 查看

1. 创建一个共享目录

创建一个共享目录/home/admins，使之具有下面的特性：

/home/admins 所属组为adminuser

这个目录对组adminuser的成有具有可读、可写和可执行。

在/home/ admins创建的任何文件所属组自动设置为adminuser。

解法：

mkdir /home/admins

chgrp -R adminuser /home/admins

chmod g+w /home/admins

chmod g+s /home/admins

1. 安装内核的升级

从http://server.domain11.example.com/pub/updates安装适合的内核更新。下面的要求必须满足：

更新的内核作为系统启动的默认内核

原来的内核在系统启动的时候依然有效和可引导

解法：

使用浏览器打开题目给的网址，并下载内核文件，到根或者家目录。

uname -r 查看当前内核版本

rpm –ivh kernel-\*.rpm

vi /boot/grub/grub.conf 查看

1. 绑定到外部验证服务器

系统server.domain11.example.com提供了一个LDAP的验证服务，你的系统应该按下面的要求绑定到这个服务：

验证服务的基准DN是dc=example,dc=com

LDAP用于提供账户信息和验证信息

连接应用使用位于

http://server.domain11.example.com/pub/EXAMPLE-CA-CERT的证书加密

当正确的配置后，ldapuser1可以登录你的系统，但是没有HOME目录，直到你完成autofs题目的ldapuser1的密码是password

解法：

yum -y install auth\*

system-config-authentication

将user account database 修改为ldap，根据题目要求填写 DN和LDAP SERVER，use TLS to encrypt connections打钩，在download ca 中写入

http://server.domain11.example.com/pub/EXAMPLE-CA-CERT。authentication metod选择ldap password。

Id ldapuser1 查看有没有学习到用户

注：这题中只要能搜索到用户即可，用户密码不需要设置。

1. 配置NTP

配置你的系统使它server.domain11.example.com的一个NTP用户

解法：

System-config-date 需安装

Synchronize date and time over the network 打钩

删除默认的NTP server

添加一个NTP server 地址为：server.domain11.example.com

1. 配置autofs

配置autofs自动挂在LDAP用户的家目录，如下要求

server.domain11.example.com使用NFS共享了home给你的系统。这个文件系统包含了预先配置 好的用户ldapuserX的home目录

ldapuserX的home目录是

server.domain11.example.com /home/guests/ldapuser

ldapuserX的home目录应该自动挂载到本地/home/guests下面的ldapuserX

home目录必须对用户具有可写权限

ldapuser1的密码是password

解法：

yum install –y autofs

mkdir /home/rehome

vi /etc/auto.master

/home/rehome /etc/auto.ldap

保存退出

cp /etc/auto.misc /etc/auto.ldap

vi /etc/auto.ldap

ldapuserX -fstype=nfs,rw server.domain11.example.com:/home/guests/

保存退出

systemctl start autofs

systemctl enable autofs

su – ldapuserX 测试

如果以上写法在考试的时候无法创建文件或者命令提示符是-bash-4.2$这样的话可能存在多级目录也需要将server.domain11.example.com:/home/guests/

的写法变为server.domain11.example.com:/home/guests/ldapuserX就可以了。何为多级目录也就是题目给的/home/guests/ldapuserX下面还有一个ldapuserX的目录这个目录才是真正的目录。

1. 配置一个用户账号

创建一个用户iar，uid是3400.这个用户的密码是redhat

解法：

useradd –u 3400 iar

passwd iar

1. 添加一个swap分区

为你的系统额外添加一个大小为500M的交换分区，这个交换分区在系统启动的时候应该能自动挂载。不要移除和修改你系统上现有的交换分区。

解法：

fdisk –cu /dev/vda 以扩展分区的方式来做，不要做主分区。

partx –a /dev/vda

mkswap /dev/vdax

swapon /dev/vdax

swapon –s

vi /etc/fstab

/dev/vdax swap swap defaults 0 0

mount -a

1. 查找文件

找到所有者是iar的文件，并把题目拷贝到/root/findresults目录

解法：

useradd iar 可以使用id iar 看是否有用户，有则不需要创建

mkdir /root/findresults

find / -user iar –exec cp -rfp {} /root/findresults \;

ls /root/findresults

1. 查找一个字符串

在/usr/share/dict/words内找出所有包含字符串seismic的列，然后把这些列依照原来的次序拷贝到/root/lines.txt内,在此档内不存在空行，所有的行必须是/usr/share/dict/words中原有行的精确复制。

解法：

grep seismic /usr/share/dict/words > /root/lines.txt

1. 创建名为/root/backup.tar.bz2的备份文件，其中包含/usr/local的内容，tar必须使用bzip2压缩。

cd /usr/local

tar –jcvf /root/backup.tar.bz2 \*

mkdir /test

tar –jxvf /root/backup.tar.bz2 –C /test/ 解压看下类容是不是和/usr/local里面的一样

如果题目要求使用gzip压缩就把-j换成-z即可

1. 创建一个逻辑卷

按照下面的要求创建一个新的逻辑卷

逻辑卷的命名为database,属于卷组的datastore,且大小为50个PE。

在卷组datastore的逻辑卷每个扩展的大小为16MB

使用ext3格式化这个新的逻辑卷，此逻辑卷在系统启动的时候应该自动挂载到/mnt/database

解法：

fdisk –cu /dev/vda 创建一个1G的分区根据情况修改

partx –a /dev/vda

pvcreate /dev/vdax

vgcreate datastore /dev/vdax –s 16M

lvcreate – l 50 –n database datastore

mkfs.ext3 /dev/datastore/database

mkdir /mnt/database

mount /dev/datastore/database /mnt/database/

df –Th

vi /etc/fstab

/dev/datastore /database /mnt/database/ ext3 defaults 0 0

mount –a

重启检查所有题目要求。

RHCE部分

1. 配置SELINUX

修改selinux的状态为Enforcing模式

使用VIM /etc/selinux

解法：

getenforce 查看当前SELINUX模式

setenforce 1 将selinux临时设置为enforcing模式

vim /etc/selinux/config

SELINUX=enforcing

:wq

getenforce

enforcing

2. **配置SSH访问**

按以下要求配置SSH访问：

1. 用户能够从域group3.example.com内的客户端通过SSH远程访问您的两个虚拟机系统

2. 在域my133t.org内的客户端不能访问您的两个虚拟机系统

解法1：

修改/etc/hosts.allow文件

添加一行 sshd: 172.24.11.

修改/etc/hosts.deny文件

添加一行 sshd: 172.25.0.

两台都需要配置

解法2：

添加防火墙策略

firewall-cmd –zone=block --add-source=172.25.11.0/24 --permanent

firewall-cmd –reload

两台都需要配置

3. **自定义用户环境：**

在系统 system1 和 system2 上创建自定义命名名为qstat 此自定义命令将执行以下命令：

/bin/ps – Ao pid,tt,user,fname,rsz

此命令对系统中所有用户有效

解法：

vim /etc/bashrc //重启保持有效

alias qstat=’/bin/ps –Ao pid,tt,user,fname,rsz’

:wq

source /etc/bashrc

alias 看是否有qstat

qstat 执行

两台都要做

4. **配置端口转发**

在系统system1 配置端口转发，要求如下：

1. 在172.24.11.0/24网络中的系统，访问system1的本地端口5423将被转发到80

2. 此设置必须永久有效

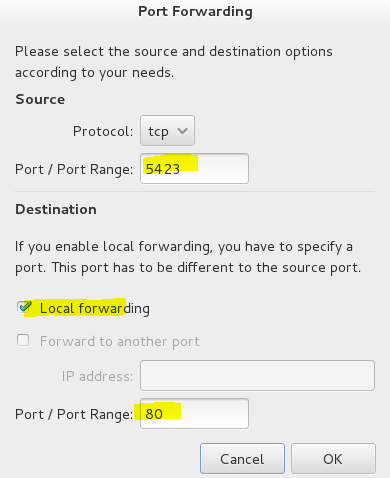
解法：

使用图形化界面进行配置

在CLI中使用firewall-config 开启图形化界面

将configuration:下拉菜单调整为permanent

在public区域中的port forward中添加一个策略



systemctl restart firewalld.service 重装载防火墙策略

5. **配置链路聚合**

**在**systeml. group3.example.com和system2. group3.example.com之间按以下要求配置一个链路：

1. 此链路使用接口eth1和eth2
2. 此链路在一个借口失效时仍然能工作
3. 此链路在systeml使用下面的地址172.16.3.20/255.255.255.0
4. 此链路在system2使用下面的地址172.16.3.25/255.255.255.0
5. 此链路在系统重启之后依然保持正常状态

如果不记得name如何写可以在/var/share/doc/team-1.9/example\_configs/查看例子。

nmcli connection add con-name team0 type team ifname team0 config '{"runner":{"name":"activebackup"}}'

nmcli con modify team0 ipv4.addresses '172.16.11.25/24'

nmcli connection modify team0 ipv4.method manual

nmcli connection add type team-slave con-name team0-p1 ifname eth1 master team0

nmcli connection add type team-slave con-name team0-p2 ifname eth2 master team0

nmcli connection up team0

nmcli con up team0-p1

nmcli con up team0-p2

6. **配置IPV6地址**

在您的考试系统上配置接口eth0 使用下列IPV6地址：

1. system1上的地址应该是2003：acl8：：305/64
2. system2上的地址应该是2003：acl8：：30a/64
3. 两个系统必须能与网络2003：acl8/64内的系统通信
4. 地址必须在重启后依然生效
5. 两个系统必须保持当前的IPV4地址并能通信

解法：

nmcli con mod eth0 ipv6.addresses “2003:ac18::305/64”

nmcli con mod eth0 ipv6.method manual

systemctl restart network

nmcli con mod eth0 ipv6.addresses “2003:ac18::30a/64”

nmcli con mod eth0 ipv6.method manual

systemctl restart network

ping6 2003:ac18::30a

7. **配置本地邮件服务**

在系统 system1 和 system2 上配置邮件服务，满足以下要求：

1. 这些系统不接受外部发送来的邮件
2. 在这些系统上本地发送的任何邮件都会自动路由到rhgls.domain11.example.com
3. 从这些系统上发送的邮件显示来自于rhgls.domain11.example.com
4. 您可以通过发送邮件到本地用户’authur’来测试您的配置，系统rhgls.domain11.example.com
5. 已经配置把此用户的邮件转到下列URL rhgls.domain11.example.com/received\_mail/11

解法：

postconf -e local\_transport=err:XX

vim /etc/postfix/main.cf

relayhost=[rhgls.domain11.exmaple.com]

postconf -e myorigin=domain11.example.com

systemctl restart postfix

echo aaa | mail -S hello dave

在浏览器中打开rhgls.domain11.example.com/received\_mail/11

8.通过SMB共享目录

在system1上配置SMB服务

您的SMB服务器必须是STAFF工作组一个成员

共享 /common 目录共享名必须为common

只有domain11.example.com域内的客户端可以访问common共享

common必须是可以浏览的

用户andy必须能够读取共享中的内容，需要需要的话，验证密码是redhat

解法：

system1:

yum -y install samba samba-client

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

firewall-cmd --add-service=mountd –permanent

systemctl restart firewalld

vim /etc/samba/smb.conf

workgroup = STAFF

[common]

path = /common

hosts allow = 172.24.11.

browseable = yes

:wq

mkdir /common

chcon –R –t samba\_share\_t /common/

smbpasswd -a andy

systemctl start smb

systemctl enable samba

system2:

yum install –y cifs-utils samba-client

9. **配置多用户SMB挂载**

在systeml共享通过SMB目录/devops满足下列要求：

1. 共享名为devops
2. 共享目录devops只能被domain11.example.com域中的客户端使用
3. 共享目录devops必须可以被浏览
4. 用户silene必须能以读的方式访问此共享，访问密码是redhat
5. 用户akira必须能以读写的方式访问此共享，访问密码是redhat
6. 此共享永久挂载在system2. domain11.example.com上的/mnt/dev用户，并使用用户silene作为认证任何用户可以通过用户akira来临时获取写的权限

解法：

system1：

mkdir /devops

chcon -R -t samba\_share\_t /devops/

chmod o+w /devops/

vim /etc/samba/smb.conf

[devops]

path = /devops

hosts allow = 172.24.11.

browseable = yes

writable = no

write list = akira

:wq

systemctl restart smb

smbpasswd -a silene

smbpasswd -a akira

system2：

mkdir /mnt/dev

smbclient -L /system1/ -U silene

vim /etc/fstab

//system1/devops /mnt/dev cifs defaults,multiuser,username=silene,password=redhat,sec=ntlmssp 0 0

df –hT

测试：

在system2上切换到akira用户，进入到/mnt/dev下 查看文件

su akira

cd /mnt/dev

ls

cifscreds add system1

touch 1

10. **配置NFS服务**

在system1配置NFS服务，要求如下：

1. 以只读的方式共享目录/public同时只能被domain11.example.com域中的系统访问
2. 以读写的方式共享目录/protected需要通过Kerberos安全加密，您可以使用下面URL提供的密钥

http://host.domain11.example.com/materials/nfs\_server.keytab

1. 目录/protected应该包含名为project.拥有人为deepak的子目录
2. 用户deepak 能以读写方式访问/protected/project

解法：

system1:

vim /etc/exports

/protected 172.24.11.0/24(rw,sync,sec=krb5p)

/public 172.24.11.0/24(ro,sync)

wget -O /etc/krb5.keytab <http://host.domain11.example.com/materials/nfs_server.keytab>

vim /etc/sysconfig/nfs

RPCNFSDARGS="-V 4.2 "

:wq

systemctl restart nfs

systemctl start nfs-secure-server

systemctl enable nfs-secure-server

exportfs –ra

showmount –e

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

firewall-cmd --add-service=rpc-bind –permanent

firewall-cmd --add-service=mountd–permanent

systemc tl restart fiewalld

mkdir -p /protected/project

chown deepak /protected/project/

ll /protected/

chcon -R -t public\_content\_t /protected/project/

11. **挂载一个NFS共享**

在system2上挂载一个system1.domain11.example.com的NFS共享,并符合下列要求：

1. /public挂载在下面的目录上/mnt/nfsmount
2. /protected挂载在下面的目录上/mnt/nfssecure并使用安全的方式，密钥下载URL如下：[http://host.domain11.example.com](http://host.domain11.example.com/)/materials/nfs\_client.keytab
3. 用户deepak能够在/mnt/nfssecure/project上创建文件
4. 这些文件系统在系统启动时自动挂线

解法：

system2:

showmount -e system1

mkdir -p /mnt/nfsmount

vim /etc/fstab

system1:/public /mnt/nfsmount nfs defaults 0 0

mount –a

df –h

mkdir /mnt/nfssecure

wget -O /etc/krb5.keytab <http://host.domain11.example.com/materials/nfs_client.keytab>

vim /etc/fstab

system1:/protected /mnt/nfssecure nfs defaults,sec=krb5p,v4.2 0 0

:wq

mount -a

12. **实现一个 web 服务器**

在 system1 上配置一个站点 http://systeml. domain11.example.com/ 然后执行下述步骤：

1. 从 http://rhgls. domain11.example.com/materials/station.html下载文件，并且将文件重名为 index.html 不要修改此文件的内容, 将文件 index.html 拷贝到您的 web服务器的 DocumentRoot 目录下

2. 来自于 group3.example.com 域的客户端可以访问此web服务

3. 来自于 my133t.org域的客户端拒绝访问此web服务

解法：

yum groupinstall httpd\* -y

systemctl start httpd

systemctl enable httpd

vim /etc/httpd/conf/httpd.conf

/ServerName

ServerName server1.domain11.example.com:80

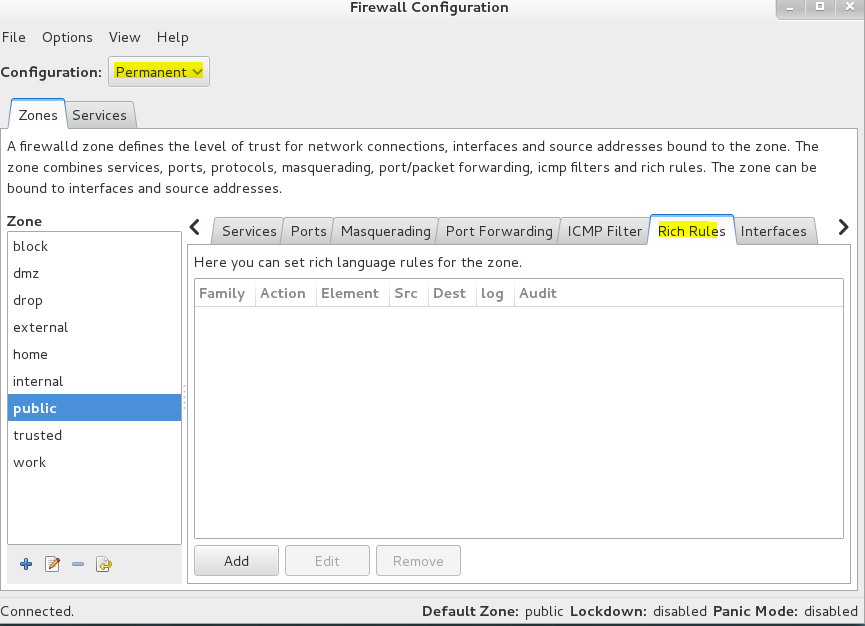
systemctl restart httpd

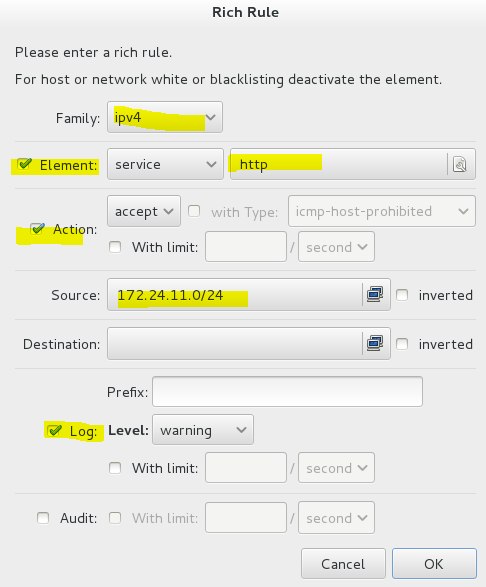
#restorecon -R /var/www/html/ ->恢复SELinux文件属性即恢复文件的安全上下文

wget -O index.html <http://rhgls.domain11.example.com/materials/station.html>

firewall-config

systemctl restart firewalld





13. **配置安全web服务**

为站点http://systeml.domain11.example.com配置TLS加密一个已签名证书从http://host.domain11.example.com/materials/system1.crt获取 此证书的密钥从http://host.domain11.example.com/materials/system1.key获取 此证书的签名授权信息从http://host.domain11.example.com/materials/domain11.crt获取

解法：

<virtualhost \*:80>

documentroot /var/www/html

servername system1.domain11.example.com

</virtualhost>

<virtualhost \*:443>

documentroot /var/www/html

servername system1.domain11.example.com

SSLEngine on

SSLCertificateFile /etc/pki/tls/certs/server1.crt

SSLCertificateKeyFile /etc/pki/tls/private/server1.key

SSLCertificateChainFile /etc/pki/tls/certs/domain11.crt

<virtualhost>

systemctl restart httpd

firewall-cmd --add-service=https –permanent

systemctl restart firewalld

14：**配置虚拟主机**

在system1 上扩展您的web服务器，为站点

[http://www.domain11.example.com](http://www.domain11.example.com/)

创建一个虚拟主机，然后执行下述步骤：

1. 设置DocumentRoot为/var/www/virtual
2. 从 http://rhgls.domain11.example.com/materials/www.html
3. 下载文件重名为index.html 不要对文件index.html 中的内容做任何修改
4. 将文件index.html 放到虚拟主机的DocumentRoot的目录下
5. 确保andy用户能够在/var/www/virtual目录下创建文件

注意：原始站点http://systeml.domian11.example.com/ 必须仍然能够访问，名称服务器domain11.example.com提供对主机名www.domain11.example.com的域名解析。

解法：

mkdir –p /var/www/ virtual

cd /var/www/ virtual

wget –O index.html <http://rhgls.domain11.example.com/materials/www.html>

vim /etc/httpd/conf/httpd.conf

<virtualhost \*:80>

documentroot /var/www/virtual

servername www.domain11.example.com

</virtualhost>

setfacl -m u:andy:rwx /var/www/virtual

su andy

touch /var/www/virtual/11.html

15. **配置web内容的访问**

在您的system1 上的web服务器的DocumentRoot目录下 创建一个名为private的目录，要求如下：

1. 从http://rhgls.domain11.example.com/materials/private.html 下载一个文件副本到这个目录，并且重命名为index.html.
2. 不要对这个文件的内容做任何修改
3. 从system1 上，任何人都可以浏览private的内容，但是从其它系统不能访问这个目录的内容

解法：

mkdir /var/www/virtual/private

mkdir /var/www/html/private

cd /var/www/virtual/private

wget -O index.html http://rhgls.domain11.example.com/materials/private.html

cd /var/www/html/private

wget -O index.html http://rhgls.domain11.example.com/materials/private.html

<Directory "/var/www/html/private">

AllowOverride none

Require all denied

Require local

</Directory>

<Directory "/var/www/virtual/private">

AllowOverride none

Require local

Require all denied

</Directory>

16，**实现动态WEB 内容**

在 system1 上配置提供动态web内容，要求如下：

1. 动态内容由名为 dynamic.domain11.example.com 的虚拟主机提供
2. 虚拟主机侦听在端口 8909
3. 从 [http://rhgls](http://rhgls/).domain11.example.com/materials/webapp.wsgi 下载一个脚本，然后放在适当的位置，无论如何不要求修改此文件的内容
4. 客户端访问 http:// dynamic.domain11example.com:8909/ 时，应该接收到动态生成的web页面
5. 此 http:// dynamic.domain11.example.com:8909/ 必须能被 domain11.example.com 域内的所有系统访问

解法：

yum -y install mod\_wsgi

vim /etc/httpd/conf/httpd.conf

Listen 80

Listen 8909

<virtualhost \*:8909>

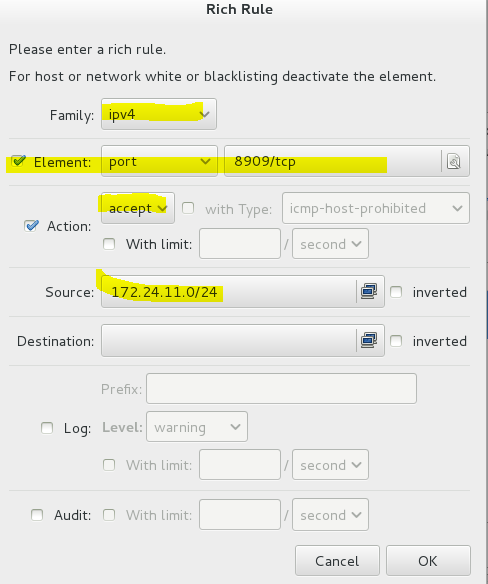
servername dynamic.domain11.example.com

WSGIScriptAlias / /var/www/html/webapp.wsgi //注意大小写

</virtualhost>

cd /var/www/html

wget http://rhgls.domain11.example.com/materials/webapp.wsgi



systemctl restart firewalld

semanage port -a -t http\_port\_t -p tcp 8909

systemctl restart httpd

17. **创建一个脚本**

在system1上创建一个名为/root/foo.sh的脚本，让其提供下列特性：

1. 当运行/root/foo.sh redhat,输出为fedora
2. 当运行/root/foo.sh fedora,输出为redhat
3. 当没有任何参数或者参数不是redhat或者fedora时，其错误输出产生以下的信息：/root/foo.sh redhat:fedora

解法:

cd ~

vim foo.sh

#~/bin/bash

case $1 in

redhat)

echo fedora

;;

fedora)

echo redhat

;;

\*)

echo 'root/foo.sh redhat:fedora'

esac

:wq

chmod +x foo.sh

./foo.sh redhat

./foo.sh fedora

./foo.sh 1

18. **创建一个添加用户的脚本**

在system1上创建一个脚本，名为/root/mkusers ,此脚本能实现为系统system1创建本地用户，并且这些用户的用户名来自一个包含用户名列表的文件，同时满足下列要求：

1. 此脚本要求提供一个参数，此参数就是包含用户名列表的的文件
2. 如果没有提供参数，此脚本应该给出下面的提示信息Usage：/root/mkusers然后退出并返回相应的值
3. 如果提供一个不存在的文件名，此脚本应该给出下面的提示信息Input file not found 然后退出并返回相应的值
4. 创建的用户登录shell为/bin/false
5. 此脚本不需要为用户设置密码
6. 您可以从下面的URL中获取用户名列表作为测试用http://rhgls. domain11.example.com/materials/ userlist

解法：

vim mkusers.sh //注意空格

#! /bin/bash

if [ $# -eq 0 ];then

echo 'Usage:/root/mkusers'

exit 1

fi

if [ ! -f $1 ]; then

echo 'Input file not found'

exit

fi

while read line

do

useradd -s /bin/false $line

done < $1

:wq

chmod +x mkusers.sh

wget http://rhgls.domain11.example.com/materials/userlist

./mkusers.sh userlist

id 用户名 查看用户是否添加

然后测试文件不存在和没有输入参数的情况是否符合题目要求

19. **配置ISCSI服务端**

配置system1提供一个ISCSI 服务磁盘名为

iqn.2014-09.com.example.domain11:system1 并符合下列要求：

1. 服务端口为3260
2. 使用iscsi\_store作其后端卷 其大小为3G
3. 此服务职能被system2.domian11.example.com访问

解法：

fdisk /dev/sda

partprobe /dev/sda

yum install -y targetcli\\*

targetcli

cd backstores/

block/ create block1 /dev/sda3

cd /iscsi

create iqn.2014-09.com.example.domain11:system1

cd iqn.2014-09.com.example.domain11:system1/

cd tpg1/

acls/ create iqn.2014-09.com.example.domain11:system

luns/ create /backstores/block/block1

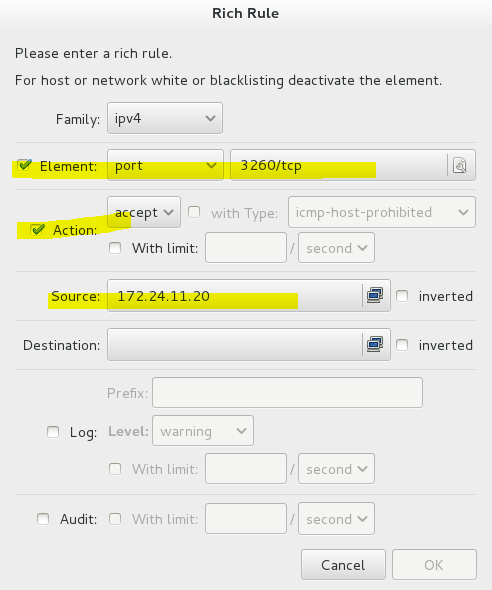
portals/ create system1.domain11.example.com

exit

systemctl start target

systemctl enable target

firewall-config



systecmctl restart firewalld

20. **配置ISCISI的客户端**

配置system2使其能链接在system1上提供的

iqn.2014-09.com.example.domain11:system1并符合以下要求：

1. ISCISI设备在系统启动的期间自动加载
2. 块设备ISCISI上包含一个大小为2100MIB的分区，并格式化为ext4
3. 此分区挂载在/mnt/data上 同时在系统启动的期间自动挂载

解法：

yum install -y iscsi-initiator-utils.i686

vim /etc/iscsi/initiatorname.iscsi

InitiatorName=iqn.2014-09.com.example.domain11:system

systemctl start iscsid

systemctl is-active iscsid

iscsiadm --mode discoverydb --type sendtargets --portal 172.24.11.10 –discover

iscsiadm --mode node --targetname iqn.2014-09.com.example.domain11:system1 --portal 172.24.11.10:3260 –login

fdisk –l

fdisk /dev/sdb

mkfs.ext4 /dev/sdb1

partprobe

mkdir /mnt/data

vim /etc/fstab

/dev/sdb1 /mnt/data ext4 \_netdev 0 0

21. **配置一个数据库**

在 system1上创建一个Maria DB数据库，名为Contacts，并符合以下条件：

1. 数据库应该包含来自数据库复制的内容，复制文件的URL为

http://rhgls.domain11.example.com/materials/users.mdb

1. 数据库只能被 localhost 访问
2. 除了root用户，此数据库只能被用户Luigi查询，此用户密码为 redhat
3. root 用户的密码为 redhat，同时不允许空密码登录

解法：

yum install -y mariadb\*

systemctl start mariadb

systemctl enable mariadb

cd /

wget http://rhgls.domain11.example.com/materials/users.mdb

mysql

create database Contacts;

show databases;

use Contacts

source /users.mdb

show tables;

grant select on Contacts .\* to Luigi@'localhost' identified by 'redhat';

exit

mysqladmin -uroot -p password 'redhat' 两个回车

mysql -uroot –p 密码输入redhat

mysql -uLuigi –p 密码输入redhat

22. **数据库查询**

在系统 system1 上使用数据库 Contacts ，并使用相应的SQL 查询以回答下列问题：

1. 密码是 tangerine 的人的名字？
2. 有多少人的姓名是 John 同时居住在 Santa Clara ？

mysql –uroot –p

show tables; 查看表结构

desc 表名; 查看表字段

select bid,password from pass where password='tangerine'; //查密码的ID号

select \* from name where aid='3' ; //通过密码id找名字

select \* from name where firstname='John'; //查找同名的人

select \* from loc where loction='Santa Clara'; //查找住在同一城市的人