

RHCE 7 答题参考(下午)

考试环境说明 ——

真实机(无 root 权限): foundation.groupX.example.com 虚拟机 1(有 root 权限): system1.groupX.example.com 虚拟机 2(有 root 权限): system2.groupX.example.com 考试服务器(提供 DNS/YUM/认证/素材...):

server1. groupX. example. com, host. groupX. example. com

练习环境说明 ——

真实机(无 root 权限): foundationX. example. com 虚拟机 1(有 root 权限): serverX. example. com 虚拟机 2(有 root 权限): desktopX. example. com

1. 配置 SELinux

试题概述:

确保 SEL inux 处于强制启用模式。

解题参考:

```
      [root@serverX ~]# vim /etc/selinux/config
      //永久配置

      SELINUX=enforcing
      //临时配置

      [root@serverX ~]# setenforce
      //临时配置

      [root@serverX ~]# getenforce
      //查看结果

      Enforcing
```

2. 配置 SSH 访问

试题概述:

按以下要求配置 SSH 访问:

- □ 用户能够从域 example. com 内的客户端 SSH 远程访问您的两个虚拟机系统
- □ 在域 my133t.org 内的客户端不能访问您的两个虚拟机系统

解题参考:

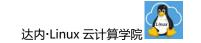
```
[root@serverX ~]# vim /etc/ssh/sshd_config
.....
DenyUsers *@<mark>*.my133t.org</mark> *@<mark>172.34.0.*</mark> //此题也可由防火墙解决
[root@serverX ~]# systemct| restart sshd
```

3. 自定义用户环境(别名设置)

试题概述:

在系统 system1 和 system2 上创建自定义命令为 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。





解题参考:

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

[root@serverX ~] # source /etc/bashrc //或重登录后生效
[root@serverX ~] # qstat //确认别名可用
```

4. 配置防火墙端口转发

试题概述:

```
在系统 system1 配置端口转发,要求如下:
```

- □ 在 172. 25. 0. 0/24 网络中的客户机,访问 system1 的本地端口 5423 将被转发到 80
- □ 此设置必须永久有效

解题参考:

5. 配置链路聚合

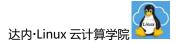
试题概述:

在 server0. example. com 和 desktop0. example. com 之间按以下要求配置一个链路:

- □ 此链路使用接口 eth1 和 eth2
- □ 此链路在一个接口失效时仍然能工作:
- □ 此链路在 server0 使用下面的地址 172. 16. 3. 20/255. 255. 255. 0
- □ 此链路在 desktop0 使用下面的地址 172.16.3.25/255.255.255.0
- □ 此链路在系统重启之后依然保持正常状态

```
[root@serverX ~] # nmcli connection add con-name team0 type team ifname team0 config
'{ "runner":{ "name":"activebackup" } }'
                                                        //建立新的聚合连接
                                                 teamO-p1 type team-slave ifname eth1
[root@serverX ~]# nmcli connection add con-name
master team0
                                                        //指定成员网卡1
[root@serverX ~] # nmcli connection add con-name
                                                 team0-p2 type team-slave ifname eth2
                                                        //指定成员网卡 2
master team0
[root@serverX ~]# nmcli
                                 modify
                                                    ipv4. method
                                                                  manual ipv4. addresses
                           con
                                           team0
"<mark>172. 16. 3. 20/24</mark>" connection. autoconnect yes
                                                        //为聚合连接配置 IP 地址
[root@serverX ~]# nmcli con modify team0-p1 connection.autoconnect yes
```





```
[root@serverX ~]# nmcli con modify team0-p2 connection.autoconnect yes
//允许成员连接自动启用
[root@serverX ~]# nmcli connection up team0 //激活聚合连接
[root@serverX ~]# teamdctl team0 state //确认连接状态
```

6. 配置 IPv6 地址

试题概述:

```
在您的考试系统上配置接口 eth0 使用下列 IPv6 地址:
   □ system1 上的地址应该是 2003:ac18::305/64
   □ system2 上的地址应该是 2003:ac18::306/64
   □ 两个系统必须能与网络 2003: ac18/64 内的系统通信
   □ 地址必须在重启后依旧生效
   □ 两个系统必须保持当前的 IPv4 地址并能通信
解题参考:
[root@serverX ~]# nmcli connection show
                                                   //获知连接名称
NAME
                                             TYPE
                                                          DEVICE
System eth0
           5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03
                                             802-3-ethernet
[root@serverX ~] # nmcli connection modify "System eth0" ipv6. method manual \
   ipv6. addresses 2003:ac18::305/64
[root@serverX ~] # nmcli connection up "System eth0"
//为两个系统设置固定主机名,避免误操作
[root@serverX ~] # hostnamectI set-hostname server0.example.com
```

7. 配置本地邮件服务

试题概述:

在系统 server0 上配置邮件服务,满足以下要求:

[root@desktopX ~] # hostnamect| set-hostname desktop0.example.com

- 口 这些系统不接收外部发送来的邮件
- □ 在这些系统上本地发送的任何邮件都会自动路由到 smtp0. example. com
- □ 从这些系统上发送的邮件显示来自于 desktop0. example. com

您可以通过发送邮件到本地用户 student 来测试您的配置,系统server1.groupX.example.com 已经配置把此用户的邮件转到下列 URL: http://server1.groupX.example.com/received_mail/3

解题参考:

[练习环境: lab smtp-nullclient setup]

```
[root@serverX ~]# vim /etc/postfix/main.cfrelayhost = [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
```



8. 通过 Samba 发布共享目录

试题概述:

- 在 server0 上通过 SMB 共享/common 目录:
- □ 您的 SMB 服务器必须是 STAFF 工作组的一个成员
- □ 共享名必须为 common
- □ 只有 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 harry 必须能够读取共享中的内容,如果需要的话,验证的密码是 migwhisk

解题参考:

```
[root@serverX ~]# yum -y install
[root@serverX ~]# mkdir /common
[root@serverX ~]# setsebool -P samba_export_all_rw=on
                                                       //取消 SELinux 限制
[root@serverX ~] # useradd harry ; pdbedit -a harry
                                                       //启用共享账号并设密码 migwhisk
[root@serverX ~]# vim /etc/samba/smb.conf
[global]
                                                       //修改此行,指定工作组名
   workgroup = STAFF
[common]
   path = /common
   hosts allow = 172.25.0.0/24
                                                       //只允许指定网域访问
[root@serverX ~]# systemctl restart smb
[root@serverX ~]# systemctl enable smb
```

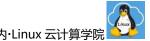
9. 配置多用户 Samba 挂载

试题概述:

在 server0 通过 SMB 共享目录/devops,并满足以下要求:

- 口 共享名为 devops
- □ 共享目录 devops 只能被 example.com 域中的客户端使用
- □ 共享目录 devops 必须可以被浏览
- □ 用户 ken ji 必须能以读的方式访问此共享, 该问密码是 atenorth
- □ 用户 chihiro 必须能以读写的方式访问此共享,访问密码是 atenorth
- 山 此共享永久挂载在 desktop0. example. com 上的/mnt/dev 目录,并使用用户 kenji 作为认证,任何用户可以通过用户 chihiro 来临时获取写的权限





解题参考:

```
在 server0 上:
```

```
[root@serverX ~]# mkdir /devops
[root@serverX ~]# useradd kenji ; pdbedit -a kenji
[root@serverX ~] # useradd chihiro ; pdbedit -a chihiro
[root@serverX ~]# setfacl -m u:chihiro:rwx /devops/
[root@serverX ~]# vim /etc/samba/smb.conf
[devops]
   path = /devops
   write list = chihiro
   hosts allow = 172.25.0.0/24
                                                         //只允许指定网域访问
[root@serverX ~]# systemctl restart smb
```

在 desktop0 上:

```
[root@desktopX ~]# yum -y install samba-client cifs-utils
[root@desktopX ~]# smbclient -L serverX
                                                    //查看对方提供了哪些共享
                                                    //无需密码,直接按 Enter 键确认
[root@desktopX ~]# mkdir /mnt/dev
[root@desktopX ~]# vim /etc/fstab
//serverX.example.com/devops
                                                  /mnt/dev
                                                                                 cifs
username=kenji,password=atenorth,multiuser,sec=ntlmssp, netdev 0 0
[root@desktopX ~]# mount -a
```

验证多用户访问(在 desktop0 上):普通用户切换为 chihiro 身份即可读写

```
[root@desktopX ~]# su - student
                                                  //切换到普通用户
[student@desktopX ~]$ cifscreds add -u chihiro serverX //向服务器提交用户认证凭据
Password:
                                                  //提供 Samba 用户 chihiro 的密码
[student@desktopX ~]$ touch /mnt/dev/b.txt
                                                  //确认有写入权限(新建文件)
```

10. 配置 NFS 共享服务

试题概述:

在 server0 配置 NFS 服务,要求如下:

- □ 以只读的方式共享目录/public, 同时只能被 example.com 域中的系统访问
- □ 以读写的方式共享目录/protected, 能被 example.com 域中的系统访问
- □ 访问/protected 需要通过 Kerberos 安全加密, 您可以使用下面 URL 提供的密钥: http://classroom/pub/keytabs/serverX.keytab
- □ 目录/protected 应该包含名为 project 拥有人为 krishna 的子目录
- □ 用户 krishna 能以读写方式访问/protected/project

解题参考:

[练习环境: lab nfskrb5 setup]

```
[root@serverX ~]# mkdir -p /public /protected/project
[root@serverX ~]# chown | IdapuserO | /protected/project/
```





11. 挂载 NFS 共享

试题概述:

在 system2 上挂载一个来自 server0. exmaple. com 的共享,并符合下列要求:

- □ /public 挂载在下面的目录上/mnt/nfsmount
- □ /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: http://classroom/pub/keytabs/desktopX.keytab
- □ 用户 Idapuser0 能够在/mnt/nfssecure/project 上创建文件
- □ 这些文件系统在系统启动时自动挂载

解题参考:

[练习环境: lab nfskrb5 setup]

```
[root@desktopX ~]# mkdir -p /mnt/nfsmount /mnt/nfssecure
[root@desktopX ~]# wget -0 /etc/krb5.keytab <mark>http://classroom/pub/keytabs/desktop0.keytab</mark>
[root@desktopX ~]# systemctl start nfs-secure
                                                         //启用安全 NFS 的客户端服务
[root@desktopX ~] # systemctl enable nfs-secure
[root@desktopX ~] # showmount -e server0
                                                         //查看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@desktopX ~]# vim /etc/fstab
                               /mnt/nfsmount
                                                                          0
serverX.example.com:/public
                                               nfs
                                                    netdev
serverX. example. com:/protected
                               /mnt/nfssecure
                                                     sec=krb5p, _netdev
                                               nfs
                                      //若服务器有 NFS 版本要求, 挂载时可添加类似 v4 的参数
[root@desktopX ~]# mount -a
[root@desktopX ~] # ssh | IdapuserO@desktopO
                                                             //SSH 登入以获取通行证
                                                             //密码 kerberos (练习环境)
IdapuserX@desktopX's password:
[IdapuserX@desktopX ~]$ touch /mnt/nfssecure/project/a.txt
                                                             //写入测试
```



12. 实现一个 web 服务器

试题概述:

为 http://server0.example.com 配置 Web 服务器:

- □ 从 http://classroom/pub/materials/station.html -0 index.html 下载一个主页文件,并将该文件重命名为 index.html
- 口 将文件 index. html 拷贝到您的 web 服务器的 DocumentRoot 目录下
- □ 不要对文件 index. html 的内容进行任何修改
- □ 来自于 example.com 域的客户端可以访问此 Web 服务
- □ 来自于 my133t. org 域的客户端拒绝访问此 Web 服务

解题参考:

13. 配置安全 web 服务

试题概述:

为站点 http://server0.example.com 配置 TLS 加密:

- □ 一个已签名证书从 http://classroom/pub/server0.crt 获取
- □ 此证书的密钥从 http://classroom/pub/tls/private/server0.key 获取
- □ 此证书的签名授权信息从 http://classroom/pub/tls/certs/example-ca.crt 获取

[root@serverX private]# systemctl restart httpd

14. 配置虚拟主机

试题概述:

在 system1 上扩展您的 web 服务器,为站点 http://www0.example.com 创建一个虚拟主机,然后执行下述步骤:

- □ 设置 DocumentRoot 为/var/www/virtual
- □ 从 http://classroom/pub/materials/www.html 下载文件并重命名为 index.html
- □ 不要对文件 index. html 的内容做任何修改
- □ 将文件 index. html 放到虚拟主机的 DocumentRoot 目录下
- □ 确保 harry 用户能够在/var/www/virtual 目录下创建文件

注意:原始站点 http://server0.example.com 必须仍然能够访问,名称服务器classroom.example.com 提供对主机名 www0.example.com 的域名解析。

解题参考:

15. 配置 web 内容的访问

试题概述:

在您的 server0 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:

- □ 从 http://classroom/pub/materials/private.html 下载一个文件副本到这个目录, 并且得命名为 index.html
- 口 不要对这个文件的内容做任何修改
- □ 从 system1 上,任何人都可以浏览 private 的内容,但是从其他系统不能访问这个目录的内容

```
[root@serverX ~]# mkdir /var/www/html/private
[root@serverX ~]# cd /var/www/html/private/
[root@serverX private]# wget http://classroom/pub/materials/private.html -0 index.html
```



```
[root@serverX private]# vim /etc/httpd/conf. d/00-default.conf
<Directory /var/www/html/private>
       Require ip 127.0.0.1 ::1 172.25.X.11
                                                         //仅允许本机 IP 访问
</Directory>
[root@serverX private]# systemctl restart httpd
```

16. 实现动态 WEB 内容

`_	Ľ	PI	1	0.7	٠	Ŀ	
77	ı	题	h	P.Y.	٦/	ı۸	
м	v	化八	. 1	Ŋι	٠.	Ŀ	

试题概述:						
在 system1 上配置提供动态 Web 内容,要求如下:						
口 动态内容由名为 webapp0. example. com 的虚拟主机提供						
□ 虚拟主机侦听在端口 8909						
□ 从 http://classroom/pub/materials/webinfo.wsgi 下载一个脚本,然后放在适当的位置,无论如何不要修改此文件的内容						
□ 客户端访问 http://web0.example.com:8909 可接收到动态生成的 Web 页						
□ 此 http://webapp0.example.com:8909/必须能被 example.com 域内的所有系统访问						
解题参考:						
[root@serverX ~]# yum -y install mod_wsgi						
[root@serverX ~]# mkdir /var/www/webapp0						
[root@serverX ~]# cd /var/www/webapp0						
[root@serverX webapp0]# wget http://classroom/pub/materials/webinfo.wsgi						
[root@serverX webapp0]# vim /etc/httpd/conf.d/02-alt.conf						
Listen 8909						
<pre><virtualhost *:8909=""></virtualhost></pre>						
ServerName webapp0 example com						

[root@serverX webapp0]# semanage port -a -t http_port_t -p tcp 8909 //开启非标准端口 [root@serverX webapp0]# systemctl restart httpd

17. 创建一个脚本

</VirtualHost>

DocumentRoot /var/www/webapp0

WSGIScriptAlias / /var/www/webapp0/webinfo.wsgi

试题概述:

在 system1 上创建一个名为/root/foo. sh 的脚本, 让其提供下列特性: □ 当运行/root/foo. sh redhat, 输出为 fedora □ 当运行/root/foo. sh fedora, 输出为 redhat

□ 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

```
[root@serverX ~]# 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
fi
[root@serverX ~]# chmod +x /root/foo.sh
```

18. 创建一个添加用户的脚本

试题概述:

在 system1 上创建一个脚本, 名为/root/batchusers, 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的文件, 同时满足下列要求:

- □ 此脚本要求提供一个参数,此参数就是包含用户名列表的文件
- □ 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
- □ 创建的用户登陆 Shell 为/bin/false, 此脚本不需要为用户设置密码
- □ 您可以从下面的 URL 获取用户名列表作为测试用: http://classroom/pub/materials/userlist

解题参考:

```
[root@serverX ~]# wget -0 /root/userlist http://classroom/pub/materials/userlist
[root@serverX ~]# vim /root/batchusers
#!/bin/bash
if [ $# -eq 0 ] ; then
        echo "Usage: /root/batchusers <userfile>"
        exit 1

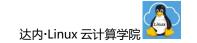
fi
if [ ! -f $1 ] ; then
        echo "Input file not found"
        exit 2

fi
for name in $(cat $1)
do
        useradd -s /bin/false $name
done
[root@serverX ~]# chmod +x /root/batchusers
```

19. 配置 iSCSI 服务端

试题概述:

配置 system1 提供 iSCSI 服务, 磁盘名为 ign. 2016-02. com. example:server0, 并符合



下列要求:

- □ 服务端口为 3260
- □ 使用 iscsi_store 作其后端卷, 其大小为 3GiB
- □ 此服务只能被 desktop0. example. com 访问

解题参考:

1) 准备磁盘空间

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

2) 安装、配置 iSCSI 磁盘

```
[root@serverX ~] # yum -y install targetcli
[root@serverX ~]# targetcli
//定义后端存储
/> /iscsi create ign. 2016-02.com. example:server0
                                                     //创建 i an 对象
/> /iscsi/iqn. 2016-02. com. example:serverX/tpg1/acls_create_iqn. 2016-02. com. example:desktop0
                                                     //授权客户机(的 IQN)
/> /iscsi/iqn.2016-02.com.example:serverX/tpg1/luns create /backstores/block/iscsi_store
                                                         //绑定存储
/> /iscsi/iqn. 2016-02. com. example:serverX/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
[root@serverX ~]# systemct| restart target
[root@serverX ~]# systemctl enable target
```

20. 配置 iSCSI 客户端

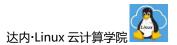
试题概述:

配置 system2 使其能连接 system1 上提供的 iqn. 2016-02. com. example:desktop0, 并符合以下要求:

- □ iSCSI 设备在系统启动的期间自动加载
- □ 块设备 iSCSI 上包含一个大小为 2100MiB 的分区, 并格式化为 ext4 文件系统
- □ 此分区挂载在/mnt/data 上,同时在系统启动的期间自动挂载

```
[root@desktopX ~]# yum -y install iscsi-initiator-utils
[root@desktopX ~]# vim /etc/iscsi/initiatorname.iscsi //设置本机 iqn 名称
InitiatorName=iqn. 2016-02. com. example:desktop0
[root@desktopX ~]# systemctl restart iscsid //起 iscsid 服务以读取 iqn 名称
[root@desktopX ~]# iscsiadm -m discovery -t st -p serverX //发现磁盘
```





```
[root@desktopX ~]# iscsiadm -m node -L all
                                                                //连接磁盘
[root@desktopX ~]# vim /var/lib/iscsi/nodes/iqn. 2016-02.com. example\:server0/*/default
node.conn[0].startup = automatic
                                                        //把 manual 改成 automatic
[root@desktopX ~]# systemctl enable iscsi
                                                        //将 iscsi 服务设开机自启
[root@desktopX ~]# IsbIk
                                                        //确认多出的磁盘,比如/dev/sda
[root@desktopX ~]# 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
                                                        // w 保存分区更改
Command (m for help): w
[root@desktopX ~]# partprobe /dev/sda
                                                        //刷新分区表
[root@desktopX ~]# mkfs.ext4 /dev/sda1
                                                        //按要求格式化分区
[root@desktopX ~]# mkdir /mnt/data
                                                        //创建挂载点
[root@desktopX ~]# blkid /dev/sda1
                                                        //找到分区 UUID
/dev/sda1: <mark>UUID="6ff20bb3-7543-4fa0-b4fa-bdc99a1e63ce"</mark>
[root@desktopX ~]# vim /etc/fstab
UUID="6ff20bb3-7543-4fa0-b4fa-bdc99a1e63ce" /mnt/data ext4 _netdev 0 0
[root@desktopX ~]# mount -a
[root@desktopX ~]# sync ; reboot -f
                                                    //先存盘再强制重启,避免关机卡死
```

21. 配置一个数据库

试题概述:

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

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://classroom/pub/materials/users.sql

数据库只能被 localhost 访问

除了 root 用户,此数据库只能被用户 Raikon 查询,此用户密码为 atenorth root 用户的密码为 atenorth,同时不允许空密码登陆。
```

解题参考:

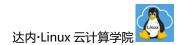
1) 安装、配置

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

2) 设密码、建库

```
[root@serverX ~]# mysqladmin -u root -p password 'atenorth' //设置密码
[root@serverX ~]# mysql -u root -p
```





22. 数据库查询(填空)

试题概述:

在系统 server0 上使用数据库 Contacts, 并使用相应的 SQL 查询以回答下列问题:

- □ 密码是 solicitous 的人的名字?
 -] 有多少人的姓名是 Barbara 同时居住在 Sunnyvale?

解题参考:

```
[root@serverX ~] # mysql -u root -p
Enter password:
MariaDB [Contacts]> USE Contacts;
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;

MariaDB [Contacts]> QUIT
```