

# RHCE模拟练习v3.0 1.5h

## [环境信息]

模拟环境：server0、desktop0

root密码：redhat

example.com: 172.25.0.0/24

cracker.com: 172.24.3.0/24

YUM: [http://content.example.com/rhel7.0/x86\\_64/dvd](http://content.example.com/rhel7.0/x86_64/dvd)

==server/desktop==

# lab nfskrb5 setup //仅模拟环境

1. 配置server0和desktop0 YUM
2. 配置server0和desktop0上的SELinux环境为enforcing
3. 配置server0和desktop0上的访问控制，拒绝cracker.com域中的主机访问SSH
4. server0和desktop0针对所有用户创建自定义命令psnew，执行该命令是将执行ps -Ao user,pid,ppid,command
5. 配置server0服务器SMB，工作组为STAFF，共享目录/smb1，共享名smb1，只有example.com域中主机访问共享smb1，smb1必须可浏览；用户ldapuser1必须能够读取共享中的内容，密码tianyun。
6. 配置server0服务器samba，共享目录/smb2，共享名smb2，只有example.com域中主机访问。用户ldapuser1读取，ldapuser2读写，密码都为tianyun；desktop0以multiuser方式自动挂接到/mnt/smb2

## 7. 配置server0 NFS服务

以只读的方式共享目录/nfs1，只能被example.com域中主机访问；

以读写的方式共享目录/nfs2，能被example.com域中主机访问

访问/nfs2需要Kerberos安全加密，密钥为 `http://classroom.example.com/pub/keytabs/server0.keytab`

目录/nfs2应包含名为private拥有者为ldapuser5的子目录，用户ldapuser5能以读写的方式访问/nfs2/private

## 8. 配置desktop0挂载NFS

/nfs1挂载到/mnt/nfs1

/nfs2挂载到/mnt/nfssecure，并使用安全的方式，密钥为：

`http://classroom.example.com/pub/keytabs/desktop0.keytab`

ldapuser5用户能在/mnt/nfssecure/private上创建文件

## 9. 配置server0和desktop0上的链路聚合，使用接口eth1、eth2。当一个接口失效时仍然能够工作。

server0: 192.168.0.1/255.255.255.0

desktop0: 192.168.0.2/255.255.255.0

## 10. 配置server0端口转发，从172.25.10.0/24网段访问server0端口6666/tcp时，转发到80/tcp

## 11. 配置server0和desktop0上的IPv6，使用接口eth0，相互可以ping通，原IPv4仍然有效。

server0: 2012:ac18::1205/64

desktop0: 2012:ac18::120a/64

## 12. 配置server0和desktop0邮件服务

server0和desktop0不接收外部邮件

本地发送的邮件会路由到 smtp.example.com

本地发送的邮件显示来自 example.com

可以通过发送邮件到本地用户ldapuser0来测试配置，可通过[http://smtp.example.com/received\\_mail/0](http://smtp.example.com/received_mail/0)查看

### 13. 配置server0 iSCSI 服务端

提供iscsi磁盘名为 iqn.2017-04.com.tianyun:server0

使用iscsi\_store作为其后端卷，其大小为2G

此服务只能被desktop0.example.com访问

提供服务的端口为3260

### 14. 配置desktop0 iSCSI 客户端

自动连接 iqn.2017-04.com.tianyun:server0

创建大小为500M的分区，格式化为 ext4文件系统，自动挂载到/mnt/iscsidisk

### 15. 配置server0 web服务，http://www0.example.com

网页：<http://classroom.example.com/content/exam/webs/www.html>，命名index.html，勿修改内容

将index.html拷贝到 DocumentRoot 目录下；

来自example.com域的客户端可以访问web服务；

来自cracker.com域的客户端拒绝访问web服务。

### 16. 配置server0 安全的web服务

网站<https://www0.example.com> 启用TLS加密。

已签名证书 <http://classroom/pub/tls/certs/www0.crt>

此证书的密钥 <http://classroom/pub/tls/private/www0.key>

此证书的授权信息从<http://classroom/pub/example-ca.crt>获取

#### 17. 配置server0 虚拟主机，<http://server0.example.com>

DocumentRoot 为 `/var/www/virtual`

网页：<http://classroom.example.com/pub/webs/server.html>，命名index.html，勿修改内容

将index.html拷贝到虚拟机 DocumentRoot 目录下；

确保ldapuser5用户能够在 `/var/www/virtual`下创建文件；

原始网站 <http://www0.example.com> 必须仍能访问

#### 18. 配置server0 web内容访问

在server0的 web服务器的DocumentRoot目录下创建目录private

网页：<http://classroom.example.com/content/exam/webs/private.html>，命名为index.html，勿修改内容

从server0 任何人可以浏览private的内容，但从其它系统不能访问该目录的内容。

#### 19. 配置server0 实现动态web内容

动态内容由 [webapp0.example.com](http://webapp0.example.com) 虚拟主机提供

虚拟机监听端口为 8888/tcp

Python application <http://classroom.example.com/content/exam/webs/webapp.wsgi>

放置在适当的位置，勿修改脚本中的内容

客户端访问<http://webapp0.example.com:8888>时能接收到动态内容

20. 配置server0 Shell script , /root/script1.sh。

执行/root/script1.sh foo , 输出bar

执行/root/script1.sh bar 输出foo

没有任何参数时, 输出 Usage /root/script1.sh bar|foo

21. 配置server0 添加用户脚本： /root/batchusers

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；

如果没有参数, 应给出提示 Usage: /root/batchusers userfile 然后退出返回相应的值；

如果提供一个不存在的文件名, 应给出提示消息 Input file not found 然后退出返回相应的值；

设置/bin/false为添加用户默认shell。

22. 配置server0 Mariadb数据库

1) 安装Mariadb

2) 配置root户只能从本地登录, 密码为tianyun

3) 禁用匿名用户访问

4) 创建数据库Concats

5) 导入数据到Concats , <http://classroom.example.com/content/exam/mariadb/mariadb.dump>

6) 授权Luigi用户可以从本地以select方式访问数据库Concats中的表, 密码tianyun。

7) 按要求实现单表查询, 提交结果

8) 按要求实现多表查询, 提交结果