

NSD ADMIN DAY07

1. [案例1：Linux管理员 综合测试](#)

1 案例1：Linux管理员 综合测试

1.1 问题

根据本文提供的练习步骤完成所有练习案例。

1.2 方案

开始练习之前，先依次重置虚拟机环境。

```
01. [root@room9pc13 ~]# rht-vmtl reset classroom
02. [root@room9pc13 ~]# rht-vmtl reset server
```

1.3 步骤

实现此案例需要按照如下步骤进行。

步骤01：配置一个用户

案例概述：

创建一个名为alex的用户，用户ID是 3456。密码是flectrag

```
01. [root@server0 ~]# useradd -u 3456 alex
02. [root@server0 ~]# echo flectrag | passwd --stdin alex
```

步骤02：创建用户账号和组

案例概述：

创建下列用户、组以及和组的成员关系：

- 一个名为adminuser的组
- 一个名为natasha的用户，其属于adminuser，这个组是该用户的从属组
- 一个名为harry的用户，属于adminuser，这个组是该用户的从属组
- 一个名为sarah的用户，其在系统中没有可交互的shell，并且不是adminuser组的成员用户
- natasha、harry、和sarah的密码都要设置为flectrag

```
01. [root@server0 ~]# groupadd adminuser //添加组 Top
02.
03. [root@server0 ~]# useradd -G adminuser natasha //添加用户
```

```
04. [root@server0 ~]# useradd -G adminuser harry
05. [root@server0 ~]# useradd -s /sbin/nologin sarah
06.
07. [root@server0 ~]# echo flectrag | passwd --stdin natasha //设置密码
08. [root@server0 ~]# echo flectrag | passwd --stdin harry
09. [root@server0 ~]# echo flectrag | passwd --stdin sarah
```

步骤03：配置文件 /var/tmp/fstab 的权限

案例概述：

拷贝文件/etc/fstab到/var/tmp/fstab，配置文件/var/tmp/fstab的权限：

- 文件/var/tmp/fstab的拥有者是root用户
- 文件/var/tmp/fstab属于root组
- 文件/var/tmp/fstab对任何人都不可执行
- 用户natasha 能够对文件/var/tmp/fstab执行读和写操作
- 用户harry 对文件/var/tmp/fstab既不能读，也不能写
- 所有其他用户（当前的和将来的）能够对文件/var/tmp/fstab进行读操作

```
01. [root@server0 ~]# cp /etc/fstab /var/tmp/fstab //复制文件
02. [root@server0 ~]# setfacl -m u:natasha:rw /var/tmp/fstab //添加个别用户权限
03. [root@server0 ~]# setfacl -m u:harry:- /var/tmp/fstab
```

步骤04：配置一个 cron 任务

案例概述：

为用户natasha配置一个定时任务，每天在本地时间14:23时执行以下命令：

/bin/echo hiya

解题参考：

```
01. [root@server0 ~]# systemctl restart crond
02. [root@server0 ~]# systemctl enable crond
03.
04. [root@server0 ~]# crontab -e -u natasha
05. 23 14 * * * /bin/echo hiya
```

步骤05：创建一个共享目录

案例概述：

创建一个共享目录/home/admins，特性如下：

- /home/admins目录的组所有权是adminuser

[Top](#)

- adminuser组的成员对目录有读写和执行的权限。除此之外的其他所有用户没有任何权限（root 用户能够访问系统中的所有文件和目录）
- 在/home/admins目录中创建的文件，其组所有权会自动设置为属于adminuser组
- [注]此处所谓的共享目录并不是指网络共享，只是某个组成员共用

解题参考：

```
01. [ root@server0 ~] # mkdir /home/admins
02. [ root@server0 ~] # chown :adminuser /home/admins
03. [ root@server0 ~] # chmod ug+rw, o-rwx /home/admins //调整权限
04. [ root@server0 ~] # chmod g+s /home/admins //设置Set UID权限
```

步骤06：安装内核的升级

案例概述：

新版内核文件从以下地址获取：

http://classroom.example.com/content/rhel7.0/x86_64/errata/Packages/

- 升级你的系统的内核版本，同时要满足下列要求：
- 当系统重新启动之后升级的内核要作为默认的内核
- 原来的内核要被保留，并且仍然可以正常启动

解题参考：

```
01. [ root@server0 ~] # firefox \
02.   http://classroom.example.com/content/rhel7.0/x86_64/errata/Packages/
03.                                     //根据所给地址找到内核文件，复制其下载地址
04. [ root@server0 ~] # wget \
05.   http://classroom.example.com/content/rhel7.0/x86_64/errata/Packages/kernel-3.10.0-123.1.2.el7.x86_64.rpm
06. [ root@server0 ~] # rpm -ivh kernel-3.10*.rpm //安装新内核（耐心等待...）
07. [ root@server0 ~] # reboot //重启以使新内核生效
08. [ root@server0 ~] # uname -r
09. 3.10.0-123.1.2.el7.x86_64 //确认新内核版本
```

步骤07：绑定到外部验证服务

案例概述：

系统 classroom.example.com 提供了一个 LDAP 验证服务。您的系统需要按照以下要求绑定到这个服务上：

- 验证服务器的基本 DN 是：dc=example,dc=com
- 帐户信息和验证信息都是由 LDAP 提供的
- 连接要使用证书进行加密，证书可以在下面的链接中下载：
- <http://classroom.example.com/pub/example-ca.crt>

[Top](#)

- 当正确完成配置后，用户 ldapuser0 应该能够登录到您的系统中，但是没有主目录。当您完成 autofs 的题目之后，才能生成主目录
- 用户 ldapuser0 的密码是 password

解题参考：

```
01. [root@server0 ~]# yum -y install sssd
02. [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：

```
01. [root@server0 ~]# cd /etc/openldap/cacerts/ //进入CA机构证书目录
02. [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。

```
01. [root@server0 ~]# systemctl restart sssd
02. [root@server0 ~]# systemctl enable sssd
03. [root@server0 ~]# id ldapuser0 //验证LDAP用户可用
04. uid=1700(ldapuser0) gid=1700(ldapuser0) groups=1700(ldapuser0)
```

步骤08：家目录漫游

案例概述：

按照下述要求配置手动挂载 LDAP 用户的主目录：

- classroom.example.com (172.25.254.254) 通过 NFS 输出 /home/guests 目录到您的系统，这个文件系统包含了用户 ldapuser0 的主目录，并且已经预先配置好了
- ldapuser0 用户的主目录是 classroom.example.com:/home/guests/ldapuser0
- ldapuser0 的主目录应该挂载到本地的 /home/guests/ldapuser0 目录下
- 用户对其主目录必须是可写的
- ldapuser0 用户的密码是 password

[Top](#)

解题参考：

```
01. [root@server0 ~] # mkdir /home/guest/ldapuser0
02. [root@server0 ~] # mount classroom.example.com:/home/guests/ldapuser0 /home/gue
03.
04. [root@server0 ~] # su - ldapuser0 -c 'pwd' //验证结果
05. /home/guests/ldapuser0
```

步骤09：配置NTP网络时间客户端

案例概述：

配置您的系统，让其作为一个 classroom.example.com 的 NTP 客户端

解题参考：

```
01. [root@server0 ~] # yum -y install chrony
02. [root@server0 ~] # vim /etc/chrony.conf
03. #server 0.rhel.pool.ntp.org iburst //注释掉不可用server配置，
04. #server 1.rhel.pool.ntp.org iburst
05. #server 2.rhel.pool.ntp.org iburst
06. #server 3.rhel.pool.ntp.org iburst
07. server classroom.example.com iburst //添加新的配置
08. ...
09. [root@server0 ~] # systemctl restart chronyd
10. [root@server0 ~] # systemctl enable chronyd
```

步骤10：查找文件

案例概述：

找出所有用户student拥有的文件，并且把它们拷贝到/root/findfiles 目录中

解题参考：

```
01. [root@server0 ~] # mkdir /root/findfiles
02. [root@server0 ~] # find / -user student -type f -exec cp -p {} /root/findfiles/ \;
```

步骤11：查找一个字符串

案例概述：

在文件/usr/share/dict/words中查找到所有包含字符串seismic的行：

- 将找出的行按照原文的先后顺序拷贝到/root/wordlist文件中
- /root/wordlist文件不要包含空行，并且其中的所有行的内容都必须是 /usr/share/dict/words 文件中原始行的准确副本

[Top](#)

解题参考：

```
01. [root@server0 ~] # grep 'seismic' /usr/share/dict/words > /root/wordlist
```

步骤12：创建一个归档

案例概述：

创建一个名为 /root/backup.tar.bz2 的归档文件，其中包含 /usr/local 目录中的内容，tar 归档必须使用 bzip2 进行压缩

解题参考：

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