牛犇

学习资料链接地址：

正式课程笔记：码云

https://gitee.com/niubenlinux/nsd2107

昨日习题：

案例1:为虚拟机配置以下静态地址参数

– 主机名:nb.tedu.cn

[root@nb ~]# hostnamectl set-hostname nb.tedu.cn

案例2:指定yum软件源

1. 将光驱设备挂载到/os/centos目录，以/os/centos目录作为其访问点

2. 利用/os/centos目录提供光盘内容作为软件源，构建本地Yum仓库

3. 安装软件包gcc

[root@A ~]# **mkdir -p /os/centos**

[root@A ~]#  **mount /dev/cdrom /os/centos**

[root@A ~]#  **ls /os/centos**

[root@A ~]# **rm -rf /etc/yum.repos.d/\***

[root@A ~]# **vim /etc/yum.repos.d/dvd.repo**

**[centos]**

**name=centos7**

**baseurl=file:///os/centos**

**enabled=1**

**gpgcheck=0**

[root@A ~]# **yum -y install gcc**

案例3:tar制作/释放归档压缩包（zcf、ztf、zxf、jcf、jtf、jxf、cf、tf）

首先创建/root/boothome/与/root/usrsbin/目录

1）备份/boot、/home这两个文件夹，保存为bh.tar.gz文件

2）查看bh.tar.gz文件内包含哪些内容

3）将bh.tar.gz释放到文件夹/root/boothome/下

4）备份/usr/sbin目录，保存为usr.tar.bz2文件

5）查看usr.tar.bz2文件内包含哪些内容

6）将usr.tar.bz2释放到/root/usrsbin/文件夹下

[root@A ~]# mkdir /root/boothome /root/usrsbin

[root@A ~]# tar -zcf /opt/bh.tar.gz /home /boot

[root@A ~]# ls /opt

[root@A ~]# tar -xf /opt/bh.tar.gz -C /root/boothome

[root@A ~]# tar -jcf /opt/usr.tar.bz2 /usr/sbin

[root@A ~]# ls /opt

[root@A ~]# tar -xf /opt/usr.tar.bz2 -C /root/usrsbin

案例4：添加并测试用户账号

1）创建一个名为stu01的用户账号

2）检查/etc/passwd、/etc/shadow文件的最后一行

3）检查/home/新增加的宿主目录（家目录）

4）为用户stu01设置一个密码（123456）

[root@A ~]# useradd stu01

[root@A ~]# grep stu01 /etc/passwd

[root@A ~]# grep stu01 /etc/shadow

[root@A ~]# ls /home

[root@A ~]# echo 123456 | passwd --stdin stu01

案例5：添加账号时设置不同属性

1）新建用户zh01，宿主目录位于/opt/zh01

2）新建账号sys01，将UID设为1234，登录Shell设为/sbin/nologin

3）为用户sys01设置密码，并测试是否能够登录

4）新建用户admin，附加组设为adm、root

[root@A ~]# **useradd -d /opt/zh01 zh01**

[root@A ~]# **grep zh01 /etc/passwd**

[root@A ~]# **useradd -u 1234 -s /sbin/nologin sys01**

[root@A ~]# **echo 123 | passwd --stdin sys01**

[root@A ~]# **grep sys01 /etc/passwd**

[root@A ~]# **useradd -G adm,root admin**

案例6：passwd设置密码

1）交互式给用户zh01设置密码123456

2）采用--stdin方式将用户zh01的密码设为654321

[root@A ~]# passwd zh01

[root@A ~]# echo 654321 | passwd --stdin zh01

案例7：usermod修改用户

1）新建一个用户zh03，将宿主目录设为/opt/home03，并设置密码

2）设置zh03密码为redhat

3）将用户zh03的宿主目录改为/home/zh03

4）将用户sys01的登录Shell改为/bin/bash

[root@A ~]# useradd -d /opt/home03 zh03

[root@A ~]# grep zh03 /etc/passwd

[root@A ~]# echo redhat | passwd --stdin zh03

[root@A ~]# usermod -d /home/zh03 zh03

[root@A ~]# grep zh03 /etc/passwd

[root@A ~]# usermod -s /bin/bash sys01

案例8：组账号基本管理

1）新建组账号stugrp

2）为stugrp组添加三个成员用户（user01、root、zhangsan）

3）从stugrp组删除一个成员（user01）

[root@A ~]# **groupadd stugrp**

[root@A ~]# **useradd user01**

[root@A ~]# **useradd zhangsan**

[root@A ~]# **gpasswd -M 'user01,root,zhangsan' stugrp**

[root@A ~]# **grep stugrp /etc/group**

[root@A ~]# **gpasswd -d user01 stugrp**

[root@A ~]# **grep stugrp /etc/group**

案例9: vim文本编辑器练习，命令模式下的基本操作

1）将/etc/passwd的前20行,写入到文件/opt/pass20.txt

2）将/etc/shadow的前10行,追加写入到文件/opt/pass20.txt

2）利用/opt/pass20.txt，进项如下操作：

– 命令模式下移动光标：键盘上下左右键、Home键、End键

– 命令模式下行间跳转：到全文的第一行（1G或gg）、到全文的最后一行（G）、到全文的第10行（10G）

– 命令模式下复制、粘贴：

复制1行（yy）、复制3行（3yy）

粘贴到当前行之后（小写p）

– 命令模式下删除：

删除单个字符（x）

删除到行首（d^）、删除到行尾（d$）

删除1行（dd）、删除3行（3dd）

– 命令模式下查找关键词：

搜索（/word）切换结果（n、N）

– 补充：在命令模式下大写的C，可以删除光标之后，并且进入插入模式

一、环境的准备

还原快照，开启CentOS7虚拟机，利用root进行登录

* **构建本地Yum仓库**

[root@localhost ~]# mkdir /nsd30

[root@localhost ~]# mount /dev/cdrom /nsd30

[root@localhost ~]# ls /nsd30

[root@localhost ~]# rm -rf /etc/yum.repos.d/\*

[root@localhost ~]# vim /etc/yum.repos.d/dvd.repo

[haha]

name=xixi

baseurl=file:///nsd30

enabled=1

gpgcheck=0

[root@localhost ~]# yum -y install xorg-x11-apps

二、基本权限与归属

* 访问权限
  + 读取：允许查看内容-**r**ead
  + 写入：允许修改内容-**w**rite
  + 可执行：允许运行和切换-e**x**cute

对于文本文件：

r读取权限：cat、less、grep、head、tail

w写入权限：vim、> 、 >>

x可执行权限：Shell与Python

* 归属关系
  + 所有者(属主)：拥有此文件/目录的用户-**u**ser
  + 所属组(属组)：拥有此文件/目录的组-**g**roup
  + 其他用户：除所有者、所属组以外的用户-**o**ther

zhangsan（所有者） zhangsan(所属组) 1.txt

* 执行 ls -l或者ls -ld 命令查看

以-开头：文本文件

以d开头：目录

以l开头：快捷方式

[root@localhost ~]# ls -ld /etc/

[root@localhost ~]# ls -l /etc/passwd

[root@localhost ~]# ls -ld /root

[root@localhost ~]# ls -ld /tmp #有特殊权限

[root@localhost ~]# ls -l /etc/shadow

[root@localhost ~]# useradd zhangsan

[root@localhost ~]# ls -ld /home/zhangsan

三、修改权限

* chmod命令
  + 格式：chmod [ugoa] [+-=][rwx] 文件...
* 常用命令选项
  + -R：递归修改权限

]# mkdir /nsd10

]# ls -ld /nsd10

]# chmod u-w /nsd10 #所有者去掉w权限

]# ls -ld /nsd10

]# chmod u+w /nsd10 #所有者加上w权限

]# ls -ld /nsd10

]# chmod g+w /nsd10 #所属组加上w权限

]# ls -ld /nsd10

]# chmod g=r /nsd10 #所属组重新定义权限

]# ls -ld /nsd10

]# chmod a=rwx /nsd10 #a表示所有人

]# ls -ld /nsd10

]# chmod u=---,g=rx,o=rwx /nsd10

]# ls -ld /nsd10

-R：递归修改权限

[root@localhost ~]# mkdir -p /opt/aa/bb/cc

[root@localhost ~]# chmod -R o=--- /opt/aa

[root@localhost ~]# ls -ld /opt/aa

[root@localhost ~]# ls -ld /opt/aa/bb

[root@localhost ~]# ls -ld /opt/aa/bb/cc

* **Linux中判断用户具备的权限：**

1. 查看用户，对于该数据所处的身份，顺序所有者>所属组>其他人，原则是**匹配即停止**
2. 查看相应身份的权限位

对于**目录**：

读取权限：查看目录内容

写入权限：能够创建、删除、修改等目录的**内容**

执行权限：能够cd切换到此目录下

**案例1：设置基本权限**

**1）以root身份新建/nsddir1/目录，在此目录下新建readme.txt文件**

[root@localhost ~]# mkdir /nsddir1

[root@localhost ~]# echo 123456 > /nsddir1/readme.txt

[root@localhost ~]# cat /nsddir1/readme.txt

**2）使用户zhangsan能够修改readme.txt文件内容课**

[root@localhost ~]# chmod o+w /nsddir1/readme.txt

**3）使用户zhangsan不可以修改readme.txt文件内容**

[root@localhost ~]# chmod o-w /nsddir1/readme.txt

**4）使用户zhangsan能够在此目录下创建/删除子目录**

[root@localhost ~]# chmod o+w /nsddir1/

**5）调整此目录的权限，使任何用户都不能进入，然后测试用户zhangsan是否还能修改readme.txt（测试结果不能，对父目录没有权限）**

[root@localhost ~]# chmod a-x /nsddir1/

**6）为此目录及其下所有文档设置权限 rwxr-x---**

[root@localhost ~]# chmod -R u=rwx,g=rx,o=--- /nsddir1/

**四、修改归属关系**

* chown命令 chmod
  + chown 属主 文件...
  + chown 属主:属组 文件...
  + chown :属组 文件...
* 常用命令选项
  + -R：递归修改归属关系

]# **mkdir /nsd15**

]# **ls -ld /nsd15**

]# **groupadd tmooc**  #创建组tmooc

]# **chown lisi:tmooc /nsd15** #修改所有者与所属组

]# **ls -ld /nsd15**

]# **chown zhangsan /nsd15**  #仅修改所有者

]# **ls -ld /nsd15**

]# **chown :root /nsd15** #仅修改所属组

]# **ls -ld /nsd15**

案例2：归属关系练习

**1）利用root的身份新建/tarena目录，并进一步完成下列操作**

[root@localhost ~]# mkdir /tarena

**2）将/tarena属主设为gelin01，属组设为tmooc组**

[root@localhost ~]# useradd gelin01

[root@localhost ~]# groupadd tmooc

[root@localhost ~]# chown gelin01:tmooc /tarena

**3）使用户gelin01对此目录具有rwx权限，除去所有者与所属组之外的用户对此目录无任何权限**

[root@localhost ~]# chmod o=--- /tarena

**4）使用户gelin02能进入、查看此目录**

[root@localhost ~]# useradd gelin02

[root@localhost ~]# gpasswd -a gelin02 tmooc

**5）将gelin01加入tmooc组，将tarena目录的权限设为450，测试gelin01用户能否进入此目录**

[root@localhost ~]# gpasswd -a gelin01 tmooc

[root@localhost ~]# chmod 450 /tarena

* **权限利用数字方式表示**
* 权限位的8进制数表示
  + r、w、x分别对应4、2、1，后3组分别求和

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **分组** | User权限 | | | Group权限 | | | Other权限 | | |
| **字符** | r | w | x | r | - | x | r | - | x |
| **数字** | 4 | 2 | 1 | 4 | 0 | 1 | 4 | 0 | 1 |
| **求和** | **7** | | | **5** | | | **5** | | |

[root@localhost ~]# **mkdir /nsd14**

[root@localhost ~]# **ls -ld /nsd14**

[root@localhost ~]# **chmod 700 /nsd14**

[root@localhost ~]# **ls -ld /nsd14**

[root@localhost ~]# **chmod 007 /nsd14**

[root@localhost ~]# **ls -ld /nsd14**

[root@localhost ~]# **chmod 750 /nsd14**

[root@localhost ~]# **ls -ld /nsd14**

[root@localhost ~]# **chmod 755 /nsd14**

[root@localhost ~]# **ls -ld /nsd14**

五、附加权限(特殊权限)

* **粘滞位**，Sticky Bit 权限
  + 占用其他人（Other）的 x 位
  + 显示为 t 或 T，取决于其他人是否有 x 权限
  + 适用于目录，用来限制用户滥用写入权
  + 在设置了t权限的文件夹下，即使用户有写入权限，也不能删除或改名其他用户文档

[root@localhost ~]# **mkdir /home/public**

[root@localhost ~]# **chmod 777 /home/public**

[root@localhost ~]# **ls -ld /home/public**

[root@localhost ~]# **chmod o+t /home/public**

[root@localhost ~]# **ls -ld /home/public**

* Set GID权限(SGID)
  + 占用属组（Group）的 x 位
  + 显示为 s 或 S，取决于属组是否有 x 权限
  + 对目录有效
  + 在一个具有SGID权限的目录下，**新建**的文档会**自动继承**此目录的属组身份

]# **mkdir /nsd18**

]# **chown :tmooc /nsd18**

]# **ls -ld /nsd18**

]# **mkdir /nsd18/abc01**

]# **ls -ld /nsd18/abc01**

]# **chmod g+s /nsd18** #赋予SGID特殊权限

]# **ls -ld /nsd18**

]# **mkdir /nsd18/abc02**

]# **ls -ld /nsd18/abc02**

**六、ACL策略管理**

* 文档归属的局限性：
  + 任何人只属于三种角色：属主、属组、其他人
  + 针对特殊的人实现更精细的控制
* acl访问策略作用：
  + **能够对个别用户、个别组设置独立的权限**
  + 大多数挂载的EXT3/4、XFS文件系统默认已支持
* setfacl命令
* 格式：setfacl [选项] u:用户名:权限 文件...

setfacl [选项] g:组名:权限 文件...

* 常用命令选项
* -m：修改ACL策略
* -x：清除指定的ACL策略
* -b：清除所有已设置的ACL策略
* -R：递归设置ACL策略

]# **mkdir /nsd19**

]# **chmod 770 /nsd19**

]# **ls -ld /nsd19**

]# **su - dc**

]$ **cd /nsd19**

-bash: cd: /nsd19: 权限不够

]$ **exit**

]# **setfacl -m u:dc:rx /nsd19** #单独赋予dc权限

]# **getfacl /nsd19**  #查看ACL策略

]# **su - dc**

]$ **cd /nsd19**

]$ **pwd**

]$ **exit**

ACL命令的练习：

]# **mkdir /nsd22**

]# **setfacl -m u:dc:rx /nsd22**

]# **setfacl -m u:zhangsan:rwx /nsd22**

]# **setfacl -m u:lisi:rx /nsd22**

]# **setfacl -m u:gelin01:rwx /nsd22**

]# **getfacl /nsd22**

]# **setfacl -x u:zhangsan /nsd22**#删除指定用户ACL

]# **getfacl /nsd22**

]# **setfacl -x u:dc /nsd22** #删除指定用户ACL

]# **getfacl /nsd22**

]# **setfacl -b /nsd22** #清除目录所有ACL策略

]# **getfacl /nsd22**

* -R：递归设置ACL策略

[root@nb /]# **setfacl -Rm u:tc:rx /opt/aa**

**七、补充内容**

* **ACL策略-黑名单的使用（单独拒绝某些用户）**

]# **setfacl -m u:lisi:--- /home/public/**

]# **getfacl /home/public/**

* **附加权限SUID权限**
  + 占用属主（User）的 x 位
  + 显示为 s 或 S，取决于属主是否有 x 权限
  + 仅对可执行的程序有意义
  + 当其他用户执行带SUID标记的程序时，具有此程序属主的身份和相应权限



这不是一把普通的剑！！

[root@localhost ~]# which mkdir

/usr/bin/mkdir

[root@localhost ~]# /usr/bin/mkdir /opt/abc01

[root@localhost ~]# ls /opt/

[root@localhost ~]# cp /usr/bin/mkdir /usr/bin/hahadir

[root@localhost ~]# ls -l /usr/bin/hahadir

[root@localhost ~]# /usr/bin/hahadir /opt/abc02

[root@localhost ~]# ls /opt/

[root@localhost ~]# chmod u+s /usr/bin/hahadir

[root@localhost ~]# ls -l /usr/bin/hahadir

[root@localhost ~]# su - zhangsan

[zhangsan@localhost ~]$ /usr/bin/mkdir zs01

[zhangsan@localhost ~]$ ls -l

[zhangsan@localhost ~]$ /usr/bin/hahadir zs02

[zhangsan@localhost ~]$ ls -l

* **文件/目录的默认权限**
* 新建文件/目录的默认权限
  + 一般文件默认均不给 x 执行权限
  + 其他取决于 **umask(权限掩码)** 设置
  + 新建目录默认权限为755
  + 新建文件默认权限为644

[root@localhost ~]# umask

0022

[root@A ~]# umask -S

u=rwx,g=rx,o=rx

课后习题：

案例1：chmod权限设置

1）以root用户新建/nsddir/目录，在该目录下新建文件readme.txt

2）使用户zhangsan能够在/nsddir/目录下创建/删除子目录

3）使用户zhangsan能够修改/nsddir/readme.txt文件的容

案例2：chown归属设置

1）新建/tarena1目录

a）将属主设为gelin01，属组设为tarena组

b）使用户gelin01对此目录具有rwx权限，其他人对此目录无任何权限

2）使用户gelin02能进入、查看/tarena1文件夹（提示：将gelin02加入所属组）

3）新建/tarena2目录

a）将属组设为tarena

b）使tarena组的任何用户都能在此目录下创建、删除文件

4）新建/tarena/public目录

a）使任何用户对此目录都有rwx权限

b）拒绝zhangsan进入此目录，对此目录无任何权限（提示ACL黑名单）

**案例3:权限设置**

1. **创建文件夹/data/test,设置目录的访问权限，使所有者和所属组具备读写执行的权限；其他人无任何权限。**

[root@A ~]# mkdir -p /data/test

[root@A ~]# chmod 770 /data/test

1. **递归修改文件夹/data/test的归属使所有者为zhangsan，所属组为tarena。**

[root@A ~]# chown -R zhangsan:tarena /data/test

[root@A ~]# ls -ld /data/test

1. **请实现在test目录下，新建的所有子文件或子目录的所属组都会是tarena。**

[root@A ~]# chmod g+s /data/test

[root@A ~]# mkdir /data/test/abc

[root@A ~]# ls -ld /data/test/abc

**4、为lisi创建ACL访问权限，使得lisi可以查看/etc/shadow文件**

[root@A ~]# setfacl -m u:lisi:r /etc/shadow

[root@A ~]# getfacl /etc/shadow

案例4:虚拟机 上操作

将文件 /etc/fstab 拷贝为 /var/tmp/fstab，并调整文件 /var/tmp/fstab权限

满足以下要求：

– 此文件的拥有者是 root

– 此文件对任何人都不可执行

– 用户 natasha 能够对此文件执行读和写操作

– 用户 harry 对此文件既不能读，也不能写

案例5:虚拟机上操作

创建一个共用目录 /home/admins，要求如下：

– 此目录的所属组是 adminuser

– adminuser 组的成员对此目录有读写和执行的权限，并且其他用户没有任何权限

– 在此目录中创建的文件，其所属组会自动设置为 属于 adminuser 组

参考答案

案例1：chmod权限设置

1）以root用户新建/nsddir/目录，在该目录下新建文件readme.txt

2）使用户zhangsan能够在/nsddir/目录下创建/删除子目录

3）使用户zhangsan能够修改/nsddir/readme.txt文件的容

[root@A ~]# mdkir /nsddir

[root@A ~]# echo haha >> /nsddir/readme.txt

[root@A ~]# chmod o+w /nsddir

[root@A ~]# su - zhangsan

[zhangsan@A ~]$ mkdir /nsddir/zhangsan

[zhangsan@A ~]$ ls /nsddir

[zhangsan@A ~]$ exit

[root@A ~]# chmod o+w /nsddir/readme.txt

[root@A ~]# su - zhangsan

[zhangsan@A ~]$ echo xixi >> /nsddir/readme.txt

[zhangsan@A ~]$ cat /nsddir/readme.txt

[zhangsan@A ~]$ exit

案例2：chown归属设置

1）新建/tarena1目录

a）将属主设为gelin01，属组设为tarena组

b）使用户gelin01对此目录具有rwx权限，其他人对此目录无任何权限

[root@A ~]# mkdir /tarena1

[root@A ~]# useradd gelin01

[root@A ~]# groupadd tarena

[root@A ~]# chown gelin01:tarena /tarena1

[root@A ~]# ls -ld /tarena1

[root@A ~]# chmod o=--- /tarena1

[root@A ~]# ls -ld /tarena1

2）使用户gelin02能进入、查看/tarena1文件夹（提示：将gelin02加入所属组）

[root@A ~]# useradd gelin02

[root@A ~]# gpasswd -a gelin02 tarena

[root@A ~]# id gelin02

[root@A ~]# su - gelin02

[gelin02@A ~]$ cd /tarena1

[gelin02@A tarena1]$ cd /tarena1

[gelin02@A tarena1]$ ls

[gelin02@A tarena1]$ exit

3）新建/tarena2目录

a）将属组设为tarena

b）使tarena组的任何用户都能在此目录下创建、删除文件

[root@A ~]# mkdir /tarena2

[root@A ~]# chown :tarena /tarena2

[root@A ~]# chmod g+w /tarena2

[root@A ~]# ls -ld /tarena2

[root@A ~]# useradd ceshi

[root@A ~]# gpasswd -a ceshi tarena

[root@A ~]# id ceshi

[root@A ~]# su - ceshi

[ceshi@A ~]$ mkdir /tarena2/ceshi

[ceshi@A ~]$ ls /tarena2

[ceshi@A ~]$ exit

4）新建/tarena/public目录

a）使任何用户对此目录都有rwx权限

b）拒绝zhangsan进入此目录，对此目录无任何权限

[root@A ~]# mkdir /tarena/public

[root@A ~]# chmod 777 /tarena/public

[root@A ~]# ls -ld /tarena/public

[root@A ~]# setfacl -m u:zhangsan:--- /tarena/public

[root@A ~]# su - zhangsan

[zhangsan@A ~]$ ls /tarena/public

[zhangsan@A ~]$ cd /tarena/public

[zhangsan@A ~]$ exit

案例3:权限设置

1、创建文件夹/data/test,设置目录的访问权限，使所有者和所属组具备读写执行的权限；其他人无任何权限。

2、递归修改文件夹/data/test的归属使所有者为zhangsan，所属组为tarena。

3、请实现在test目录下，新建的所有子文件或目录的所属组都会是tarena。

4、为lisi创建ACL访问权限，使得lisi可以查看/etc/shadow文件

[root@A ~]# mkdir /data/test

[root@A ~]# chmod u=rwx,g=rwx,o=--- /data/test 或者 chmod 770 /data/test

[root@A ~]# ls -ld /data/test

[root@A ~]# chown -R zhangsan:tarena /data/test

[root@A ~]# ls -ld /data/test

[root@A ~]# chmod g+s /data/test

[root@A ~]# mkdir /data/test/abc

[root@A ~]# ls -ld /data/test/abc

[root@A ~]# setfacl -m u:lisi:r /etc/shadow

[root@A ~]# getfacl /etc/shadow

[root@A ~]# su - lisi

[lisi@A ~]$ cat /etc/shadow

[lisi@A ~]$ exit

案例4:虚拟机 server0上操作

将文件 /etc/fstab 拷贝为 /var/tmp/fstab，并调整文件 /var/tmp/fstab权限

满足以下要求：

– 此文件的拥有者是 root

– 此文件对任何人都不可执行

– 用户 natasha 能够对此文件执行读和写操作

– 用户 harry 对此文件既不能读，也不能写

[root@A ~]# cp /etc/fstab /var/tmp/fstab

[root@A ~]# ls -l /var/tmp/fstab

[root@A ~]# setfacl -m u:natasha:rw /var/tmp/fstab

[root@A ~]# getfacl /var/tmp/fstab

[root@A ~]# su - natasha

[natasha@A ~]$ cat /var/tmp/fstab

[natasha@A ~]$ echo ceshi >> /var/tmp/fstab

[natasha@A ~]$ cat /var/tmp/fstab

[natasha@A ~]$ exit

[root@A ~]# setfacl -m u:harry:--- /var/tmp/fstab

[root@A ~]# getfacl /var/tmp/fstab

[root@A ~]# su - harry

[harry@A ~]$ cat /var/tmp/fstab

[harry@A ~]$ echo ceshi >> /var/tmp/fstab

[harry@A ~]$ exit

案例5:虚拟机操作

创建一个共用目录 /home/admins，要求如下：

– 此目录的所属组是 adminuser

– adminuser 组的成员对此目录有读写和执行的权限，并且其他用户没有任何权限

– 在此目录中创建的文件，其所属组会自动设置为 属于 adminuser 组

[root@A ~]# mkdir /home/admins

[root@A ~]# groupadd adminuser

[root@A ~]# chown :adminuser /home/admins

[root@A ~]# ls -ld /home/admins

[root@A ~]# chmod g+s /home/admins

[root@A ~]# ls -ld /home/admins

[root@A ~]# mkdir /home/admins/ceshi

[root@A ~]# ls -ld /home/admins/ceshi