教学环境介绍

• 每个学员机上有三台预先配置好的虚拟机

– server —— 作为练习用服务器

– desktop —— 作为练习用客户机

– classroom —— 提供网关/DNS/软件素材等资源

优先开启classroom虚拟机

真机上,进行还原三台机器:

[student@room9pc01 ~]$ rht-vmctl reset classroom

[student@room9pc01 ~]$ rht-vmctl reset server

[student@room9pc01 ~]$ rht-vmctl reset desktop

虚拟机server root的密码redhat

虚拟机desktop root的密码redhat

虚拟机server:

1.查看系统版本:RHEL7.0

2.查看eth0网卡IP地址:172.25.0.11/24

3.查看主机名:server0.example.com

虚拟机desktop:

1.查看系统版本:RHEL7.0

2.查看eth0网卡IP地址:172.25.0.10/24

3.查看主机名:desktop0.example.com

###################################################

真机进行远程管理虚拟机

1.真机ping两台虚拟机

[student@room9pc01 ~]$ ping 172.25.0.11

[student@room9pc01 ~]$ ping 172.25.0.10

2.真机执行命令: ssh 用户@对方的IP地址

Ctrl + shift + t:开启新的终端

[student@room9pc01 ~]$ ssh root@172.25.0.11

[student@room9pc01 ~]$ ssh root@172.25.0.10

-X(大写):可以在远程管理时,开启对方的图形程序

[root@server0 ~]# exit

登出

Connection to 172.25.0.11 closed.

[student@room9pc01 ~]$ ssh -X root@172.25.0.11

[root@server0 ~]# firefox #火狐浏览器,开启对方的图形程序

[root@server0 ~]# firewall-config #图形防火墙配置程序

3.简化复杂的命令

为真机设置永久别名: ~/.bashrc #新开一个终端

[student@room9pc01 ~]$ vim /home/student/.bashrc

# .bashrc

alias gos='ssh -X root@172.25.0.11'

alias god='ssh -X root@172.25.0.10'

新开一个终端进行验证:

[student@room9pc01 ~]$ gos

[student@room9pc01 ~]$ god

###################################################

权限和归属

基本权限

• 访问方式(权限)

– 读取:允许查看内容-read r

– 写入:允许修改内容-write w

– 可执行:允许运行和切换-execute x

对于文本文件:

r: cat head less

w: vim > >>

x: Shell脚本

• 权限适用对象(归属)

– 所有者:拥有此文件/目录的用户-user u

– 所属组:拥有此文件/目录的组-group g

– 其他用户:除所有者、所属组以外的用户-other o

• 使用 ls -l 命令

– ls -ld 文件或目录...

以-开头:文本文件 以d开头:目录 以l开头:快捷方式

[root@server0 ~]# ls -ld /etc/

[root@server0 ~]# ls -l /etc/passwd

[root@server0 ~]# ls -l /etc/shadow

[root@server0 ~]# ls -ld /home/student

[root@server0 ~]# ls -ld /tmp

Permission denied :权限不足

####################################################

• 使用 chmod 命令

– chmod [-R] 归属关系+-=权限类别 文档...

[-R]:递归设置权限

[root@server0 ~]# mkdir /nsd01

[root@server0 ~]# ls -ld /nsd01

[root@server0 ~]# chmod u-w /nsd01

[root@server0 ~]# ls -ld /nsd01

[root@server0 ~]# chmod g+w /nsd01

[root@server0 ~]# ls -ld /nsd01

[root@server0 ~]# chmod o=--- /nsd01

[root@server0 ~]# ls -ld /nsd01

[root@server0 ~]# chmod u=rwx,g=rx,o=rx /nsd01

[root@server0 ~]# ls -ld /nsd01

[root@server0 ~]# chmod ugo=rwx /nsd01

[root@server0 ~]# ls -ld /nsd01

[root@server0 ~]# mkdir -p /opt/aa/bb/cc

[root@server0 ~]# ls -ld /opt/aa

[root@server0 ~]# chmod -R o=--- /opt/aa

[root@server0 ~]# ls -ld /opt/aa

[root@server0 ~]# ls -ld /opt/aa/bb/

[root@server0 ~]# ls -ld /opt/aa/bb/cc/

#####################################################

Linux判断用户具备的权限 匹配及停止

1.判断用户角色 顺序:所有者>所属组>其他人

2.查看相应角色权限位

目录的 r 权限:能够 ls 浏览此目录内容

目录的 w 权限:能够执行 rm/mv/cp/mkdir/touch/等更改目录内容的操作

目录的 x 权限:能够 cd 切换到此目录

以root用户新建/nsddir目录，在此目录下新建readme.txt文件

并进一步完成下列操作

1）使用户lisi能够在此目录下创建子目录 切换用户 su - lisi

chmod o+w /nsddir/

2）使用户lisi不能够在此目录下创建子目录

chmod o-w /nsddir/

3）使用户lisi能够修改readme.txt文件内容

chmod o+w /nsddir/readme.txt

4）调整此目录的权限，使所有用户都不能cd进入此目录

chmod u-x,g-x,o-x /nsddir/

5）为此目录及其下所有文档设置权限 rwxr-x---

chmod -R u=rwx,g=rx,o=--- /nsddir/

　　　-R：递归设置权限，目录下及目录下所有

####################################################

• 使用 chown 命令

– chown [-R] 属主 文档...

– chown [-R] :属组 文档...

– chown [-R] 属主:属组 文档...

[root@server0 ~]# mkdir /nsd03

[root@server0 ~]# ls -ld /nsd03

[root@server0 ~]# groupadd tedu

[root@server0 ~]# chown lisi:tedu /nsd03

[root@server0 ~]# ls -ld /nsd03

[root@server0 ~]# chown student /nsd03

[root@server0 ~]# ls -ld /nsd03

[root@server0 ~]# chown :root /nsd03

[root@server0 ~]# ls -ld /nsd03

###################################################

利用root用户新建/nsd06目录，并进一步完成下列操作

1）将属主设为gelin01，属组设为tarena组

[root@server0 /]# useradd gelin01

[root@server0 /]# useradd gelin02

[root@server0 /]# groupadd tarena

[root@server0 /]# chown gelin01:tarena /nsd06

2）使用户gelin01对此目录具有rwx权限

除属主与属组之外的人，对此目录无任何权限

[root@server0 /]# chmod o=--- /nsd06

3）使用户gelin02能进入、查看此目录内容

[root@server0 /]# gpasswd -a gelin02 tarena

4）将gelin01加入tarena组, 将nsd06目录的权限设为rw-r-x---

再测试gelin01用户能否进入此目录

[root@server0 /]# gpasswd -a gelin01 tarena

[root@server0 /]# chmod u=rw,g=rx /nsd06

####################################################

附加权限(特殊权限)

Set GID

• 附加在属组的 x 位上

– 属组的权限标识会变为 s

– 适用于目录,Set GID可以使目录下新增的文档自动设

置与父目录相同的属组

– 让子文档自动继承父目录的所属组身份

[root@server0 ~]# mkdir /nsd08

[root@server0 ~]# ls -ld /nsd08

[root@server0 ~]# chown :tedu /nsd08 #修改所属组

[root@server0 ~]# ls -ld /nsd08

[root@server0 ~]# mkdir /nsd08/abc01

[root@server0 ~]# ls -ld /nsd08/abc01

[root@server0 ~]# chmod g+s /nsd08 #设置Set GID权限

[root@server0 ~]# ls -ld /nsd08

[root@server0 ~]# mkdir /nsd08/abc02

[root@server0 ~]# ls -ld /nsd08/abc02

[root@server0 ~]# touch /nsd08/1.txt

[root@server0 ~]# ls -ld /nsd08/1.txt

/nsd/2018-6-5.txt

/nsd/2018-6-6.txt

/nsd/2018-6-7.txt

/nsd/2018-6-8.txt

/nsd/2018-6-9.txt

[root@server0 ~]# chmod o=--- /nsd

[root@server0 ~]# groupadd caiwu

[root@server0 ~]# chown :caiwu /nsd

[root@server0 ~]# chmod g+s /nsd

####################################################

Set UID

• 附加在属主的 x 位上

– 属主的权限标识会变为 s

– 适用于可执行文件,Set UID可以让使用者具有文件属主的身份及部分权限

[root@server0 ~]# /usr/bin/mkdir /opt/haha

[root@server0 ~]# ls /opt/

[root@server0 ~]# cp /usr/bin/mkdir /usr/bin/xixidir

[root@server0 ~]# ls /usr/bin/xixidir

[root@server0 ~]# /usr/bin/xixidir /opt/abc

[root@server0 ~]# ls /opt/

[root@server0 ~]# chmod u+s /usr/bin/xixidir

[root@server0 ~]# ls -l /usr/bin/xixidir

[root@server0 ~]# su - dc

[dc@server0 ~]$ /usr/bin/mkdir dc01

[dc@server0 ~]$ ls -l

[dc@server0 ~]$ /usr/bin/xixidir dc02

[dc@server0 ~]$ ls -l

[dc@server0 ~]$ exit

###################################################

Sticky Bit

• 附加在其他人的 x 位上

– 其他人的权限标识会变为 t

– 适用于开放 w 权限的目录,可以阻止用户滥用 w 写入

权限(禁止操作别人的文档)

[root@server0 ~]# mkdir /home/public

[root@server0 ~]# chmod ugo=rwx /home/public

[root@server0 ~]# ls -ld /home/public

[root@server0 ~]# chmod o+t /home/public/

[root@server0 ~]# ls -ld /home/public

#################################################

acl访问控制列表

• acl访问策略

– 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

[root@server0 ~]# mkdir /nsd09

[root@server0 ~]# ls -ld /nsd09

[root@server0 ~]# chmod o=--- /nsd09

[root@server0 ~]# ls -ld /nsd09

[root@server0 ~]# su - lisi

[lisi@server0 ~]$ cd /nsd09

-bash: cd: /nsd09: Permission denied

[lisi@server0 ~]$ exit

[root@server0 ~]# setfacl -m u:lisi:rx /nsd09 #设置ACL

[root@server0 ~]# getfacl /nsd09 #查看ACL权限

[root@server0 ~]# su - lisi

[lisi@server0 ~]$ cd /nsd09

[lisi@server0 nsd09]$ pwd

[lisi@server0 nsd09]$ exit

[root@server0 ~]#

####################################################

使用 getfacl、setfacl 命令

– getfacl 文档...

– setfacl [-R] -m u:用户名:权限类别 文档...

– setfacl [-R] -m g:组名:权限类别 文档...

– setfacl [-R] -x u:组名 文档... #删除指定ACL策略

– setfacl [-R] -b 文档... #删除所有ACL策略

[root@server0 ~]# mkdir /nsd11

[root@server0 ~]# setfacl -m u:lisi:rwx /nsd11

[root@server0 ~]# setfacl -m u:dc:rx /nsd11

[root@server0 ~]# setfacl -m u:zhangsan:rwx /nsd11

[root@server0 ~]# setfacl -m u:gelin01:rwx /nsd11

setfacl: Option -m: 无效的参数 near character 3

[root@server0 ~]# id gelin01

id: gelin01: no such user

[root@server0 ~]# useradd gelin01

[root@server0 ~]# setfacl -m u:gelin01:rwx /nsd11

[root@server0 ~]# getfacl /nsd11

[root@server0 ~]# setfacl -x u:dc /nsd11 #删除指定ACL

[root@server0 ~]# getfacl /nsd11

[root@server0 ~]# setfacl -b /nsd11 #删除所有ACL

[root@server0 ~]# getfacl /nsd11

####################################################