**1\_Admin05权限和归属ACL**

**一 教学环境介绍**

1.1 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

优先虚拟机classroom开机

1.2真机上使用rht-vmctl辅助工具

]# rht-vmctl reset classroom #先重置资源服务器

]# rht-vmctl reset server #重置server

]# rht-vmctl reset desktop #再重置答题虚拟机

1.3虚拟机server: root用户密码为redhat

查看系统版本:RHEL7

查看主机名:server0.example.com

查看eth0网卡IP地址:172.25.0.11/24

1.4 虚拟机desktop: root用户密码为redhat

查看系统版本:RHEL7

查看主机名:desktop0.example.com

查看eth0网卡IP地址:172.25.0.10/24

1.5利用真机进行远程管理虚拟机

真机能够与虚拟机通信

[student@room9pc01 ~]$ ping 172.25.0.11

[student@room9pc01 ~]$ ping 172.25.0.10

远程管理命令: ssh 用户名@对方的IP地址

[student@room9pc01 ~]$ ssh root@172.25.0.11

[student@room9pc01 ~]$ ssh root@172.25.0.10

ctrl + shift + t :在一个窗口中,新开一个终端

-X(大写)：远程管理时，开启对方的图形程序

[root@server0 ~]# exit

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

[root@server0 ~]#　firefox #火狐浏览器

[root@server0 ~]#　firewall-config #防火墙工具

1.6 常见提示:dconf桌面服务报错,与远程管理无关

(process:30405): dconf-WARNING \*\*: failed to commit changes

to dconf: 无法连接：拒绝连接

**二 补充:为真机设置永久别名**

配置文件: ~/.bashrc[为当前用户设置alias]

配置文件: ~/.bashrc #每开一个新的终端生效

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

alias gos='ssh -X root@172.25.0.11'

alias god='ssh -X root@172.25.0.10'

真机:开启一个新的终端验证

[student@room9pc01 ~]$ gos

[student@room9pc01 ~]$ god

**三 权限和归属**

**3.1 基本权限**

基本权限的类别

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

**对目录文件:**

**r:能够 ls 浏览此目录内容**

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

**x:能够 cd 切换到此目录**

**对文本文件:**

**r: cat less head tail**

**w: vim > >>**

**x: Shell脚本**

**3.2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

**3.3查看权限**

使用 ls -l 命令

ls -ld 文件或目录...

以 d 开头为目录

以 - 开头为文本文件

以 l 开头为快捷方式

**3.4 使用 chmod 命令**

chmod [-R] 归属关系+-=权限类别 文档...

-R:递归设置权限

**3.5 Linux判定一个用户拥有的权限 匹配及停止**

判断用户的身份:所有者>所属组>其他人

查看相应权限位的权限

Permission denied :权限不足

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

使用户lisi能够在此目录下创建子目录 su - lisi

chmod o+w /nsddir/

使用户lisi不能够在此目录下创建子目录

chmod o-w /nsddir/

使用户lisi能够修改readme.txt文件内容

chmod o+w /nsddir/readme.txt

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/

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

**3.6设置文档归属**

3.6.1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...**

利用root用户新建/nsd06目录，并进一步完成下列操作

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

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

使用户gelin02能进入、查看此目录内容

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

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

设置权限,让lisi用户可以读取/etc/shadow文件内容,有几种办法?

1.利用其他人:

chmod o+r /etc/shadow

2.利用所属组:

chown :lisi /etc/shadow

chmod g+r /etc/shadow

3.利用所有者:

chown lisi /etc/shadow

chmod u+r /etc/shadow

4.利用ACL策略

setfacl -m u:lisi:r /etc/shadow

**四 附加权限(特殊权限)**

**4.1 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,

自动继承父目录所属组身份

**4.2 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 ~]# cp /usr/bin/mkdir /usr/bin/hahadir

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

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

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

[root@server0 ~]# su - lisi

[lisi@server0 ~]$ /usr/bin/mkdir test

[lisi@server0 ~]$ /usr/bin/hahadir nsd

[lisi@server0 ~]$ ls -l

[lisi@server0 ~]$ exit

**4.3 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)

**五 acl访问控制列表**

**5.1 acl策略的作用**

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

无法实现更精细的控制

**5.2 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

**5.3使用 getfacl、setfacl 命令**

**getfacl 文档...** #查看文档acl设置

**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:用户名 文档...** #删除文档的用户ACL

**setfacl [-R] -b 文档...** #清除所有ACL

]# mkdir /nsd14

]# setfacl -m u:lisi:rwx /nsd14

]# setfacl -m u:dc:rx /nsd14

]# setfacl -m u:genlin01:rwx /nsd14

]# setfacl -m u:genlin02:--- /nsd14 #设置无任何权限

]# getfacl /nsd14

]# setfacl -x u:genlin02 /nsd14 #删除指定ACL策略

]# getfacl /nsd14

]# setfacl -x u:genlin01 /nsd14 #删除指定ACL策略

]# getfacl /nsd14

]# setfacl -b /nsd14 #清除所有的ACL策略

]# getfacl /nsd14

\*