NSD ADMIN DAY05

1 案例1：访问练习用虚拟机

1.1 问题

学会在教学环境中访问练习用虚拟机，主要完成以下事项：

1. 快速重置教学虚拟机环境
2. 通过“虚拟系统管理器”访问虚拟机
3. 通过 ssh -X 远程访问 server 的命令行

1.2 方案

为了方便学员练习所学实验案例，教学环境的CentOS真机已经部署为基于KVM技术的虚拟化服务器，并且预先提供了3个虚拟机：server、desktop、classroom。

1.3 步骤

实现此案例需要按照如下步骤进行。

步骤一：快速重置教学虚拟机环境

按照顺序先重置classroom，再依次重置server、desktop；如果只是做Linux管理员技术部分的练习，只需要重置classroom、server就可以。

```
[root@room9pc13 ~]# rht-vmctl reset classroom        //先重置资源服务器
[root@room9pc13 ~]# rht-vmctl reset server           //再重置练习用虚拟机
[root@room9pc13 ~]# rht-vmctl reset desktop
```

步骤二：通过“虚拟系统管理器”访问虚拟机

这种方式的优势是，即使虚拟机的IP地址或防火墙配置有误，仍然可以访问；不足的地方是，比较占用系统资源、不方便传递文本信息（复制粘贴）。

直接从桌面双击“虚拟系统管理器”图标，找到classroom、server等虚拟机，双击打开运行即可。

步骤三：通过 ssh -X 远程登录到 server 的命令行

重置过的练习环境已预先配置好网络，并且为从真机访问答题用虚拟机提前配置了SSH密钥验证，因此直接执行快速登录（ssh -X root@目标主机地址）即可。

```
[root@room9pc13 ~]# ssh -X root@server0.example.com
[root@server0 ~]# hostname
server0.example.com
```

注意ssh添加了-X选项（大写字母X），这是为了在执行远程主机的图形程序时，能够将图形界面在客户机上显示，方便用户操作。例如，连接到server0以后，运行对方的网卡配置工具nm-connection-editor，其程序窗口会直接显示在客户机的图形桌面上。

2 案例2：配置附加权限

2.1 问题

本例要求创建一个某个组的用户共享使用的目录 /home/admins，满足以下要求：

1. 此目录的组所有权是 adminuser
2. adminuser 组的成员对此目录有读写和执行的权限，除此以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）
3. 在此目录中创建的文件，其组的所有权会自动设置为属于 adminuser 组

2.2 方案

使目录的属组能够向下自动继承，只要对这个目录设置Set GID附件权限即可。

2.3 步骤

实现此案例需要按照如下步骤进行。

步骤一：创建目录并调整权限

1）新建文件夹

```
[root@server0 ~]# mkdir  /home/admins
```

2）调整并确认权限

```
[root@server0 ~]# chown  :adminuser /home/admins
[root@server0 ~]# chmod  ug=rwx,o-rwx  /home/admins
[root@server0 ~]# chmod  g+s  /home/admins

[root@server0 ~]# ls  -ld  /home/admins/
drwxrws---. 2 root adminuser 6 12月 23 23:13 /home/admins/
```

步骤二：验证目录的特性

1）在此目录下新建一个文件

```
[root@server0 ~]# touch  /home/admins/a.txt
```

2）查看新建文件的归属，其属组应该与父目录相同

```
[root@server0 ~]# ls -lh /home/admins/a.txt
-rw-r--r--. 1 root adminuser 0 12月 23 23:17 /home/admins/a.txt
```

3 案例3：配置文档的访问权限

3.1 问题

本例要求将文件 /etc/fstab 拷贝为 /var/tmp/fstab，并调整文件 /var/tmp/fstab的权限，满足以下要求：

1. 此文件的拥有者是 root
2. 此文件属于 root 组
3. 此文件对任何人都不可执行
4. 用户 natasha 能够对此文件执行读和写操作
5. 用户 harry 对此文件既不能读，也不能写
6. 所有其他用户（当前的和将来的）能够对此文件进行读操作

3.2 方案

针对个别用户的权限策略，使用setfacl命令进行设置。

3.3 步骤

实现此案例需要按照如下步骤进行。

步骤一：复制文件

1）使用cp命令进行复制

```
[root@server0 ~]# cp /etc/fstab /var/tmp/fstab
```

2）确认复制后的权限

```
[root@server0 ~]# ls -l /var/tmp/fstab
-rw-r--r--. 1 root root 313 12月 23 23:01 /var/tmp/fstab
```

说明已经满足案例要求的前三条和最后一条。

步骤二：调整权限

1）增加额外的访问控制策略

```
[root@server0 ~]# setfacl -m u:natasha:rw /var/tmp/fstab
[root@server0 ~]# setfacl -m u:harry:--- /var/tmp/fstab
```

2）确认结果

```
[root@server0 ~]# getfacl  /var/tmp/fstab
getfacl: Removing leading '/' from absolute path names
# file: var/tmp/fstab
# owner: root
# group: root
user::rw-
user:natasha:rw-
user:harry:---
group::r--
mask::rw-
other::r--

[root@server0 ~]#
```