**Morning**

1. 基本权限

-权限的类别

1）对于文本文件的作用：

读取：允许查看内容-read （cat less head tail）

写入：允许修改内容-write （vim 保存）

可执行：允许运行和切换-execute

1. 对于目录的作用：

r权限：ls

w权限：rm/mv/cp/mkdir/touch/等更改目录内容的操作（子目录权限）

x权限：cd

-权限使用对象（归属）

所有者：拥有此文件/目录的用户-user

所属组：拥有此文件/目录的组-group

其他用户：除所有者、所属组以外的用户-other

-查看文件或目录权限（ls -l）

ls -l(-ld) 文件或目录

- rw- r-- r-- . （字段）

1）-开头代表文本文件、d开头代表目录、-l开头代表快捷方式

2）分别为所有者、所属组、其他用户的权限（顺序固定为rwx）

3）. 无acl策略 +设置acl策略

-设置基本权限（chmod）

chmod [-R] 归属关系+-=权限类别 文档 #-R递归权限

例：chmod u-w,go+r /dir1 #所有者取消写，组/其他添加读

chmod ugo=--- /dir1 #任何人取消所有权限

-Linux判断用户具备的权限

1. 查看用户对于文档处于什么身份
2. 查看相应身份的权限

Permission denied：权限不足

-设置文档归属（chown）

chown gjq /nsd01 #更改所有者

chown :grp1 /nsd01 #更改所属组

chown gjq:grp1 /nsd01 #更改所有者及所属组

用户加入组的权限需要注销才生效

权限冲突时：所有者>所属组>其他人（匹配即停止）

**Afternoon**

1、附加权限（特殊权限）

-Set GID：目录下新增的文档自动设置与父目录相同的属组

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

[root@server0 ~]# ls -ld /data/test

drwxrws---. 2 zhangsan tarena 6 9月 7 19:34 /data/test

#附加在属组的x位，S表示只有附加权限，s表示执行&附加权限。

1. acl访问控制列表

-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

-getfacl 命令

-R递归 -m设置acl -x删除acl -b清空acl

setfacl -m u:gjq:rx /nsd02 #给gjq用户设置rx权限

setfacl -m u:gjq:--- /nsd02 #去掉gjq用户的所有权限

setfacl -m g:grp1:rx /nsd02 #给grp1组设置rx权限

setfacl -m u:gjq:rx -m g:grp1:rx /nsd02 #一次性设置多个acl策略

setfacl -x u:gjq /nsd02 #删除用户gjq的acl策略

setfacl -b /nsd02 #清空该文档所有acl策略

1. LDAP认证

-作用：主要实现网络用户认证，达到用户的集中管理。

-网络用户：由LDAP服务器提供用户名、密码信息。

-服务端：LDAP服务器 虚拟机classroom

-客户端：虚拟机server

1. 安装sssd软件包，与LDAP沟通的软件包
2. 安装authconfig-gtk图形的工具，配置sssd软件包
3. 运行authconfig-gtk

LDAP搜索基础DN（B）：dc=example,dc=com

LDAP服务器(S)：classroom.example.com

勾选TLS加密，使用证书加密：http://classroom.example.com/pub/example-ca.crt

1. 重启服务，开机自启

systemctl restart sssd

systemctl enable sssd

1. 验证服务

grep ldapuser0 /etc/passwd 未找到命令

id ldapuser0 有用户ID信息

1. 家目录漫游

-NFS（Network File System）共享服务端：虚拟机classroom

由NFS服务器将指定的文件夹共享给客户机

-NFS共享客户端

1. 查看NFS资源

showmount -e 服务器地址

结果：/home/guests 172.25.0.0/255.255.0.0

2）挂载NFS共享目录

mount classroom.example.com:/home/guests /home/guests

#必须保证挂载目录与NFS服务器的家目录一致

3）访问此共享

**作业**

案例1:指定yum软件源

为 server0 指定可用的 yum 软件源

– YUM软件库的地址为 http://classroom.example.com/content/rhel7.0/x86\_64/dvd/

– 将此配置为虚拟机 server0 的默认软件仓库

– 确认可用的仓库列表

– 利用yum仓库安装xeyes

#安装完xeyes，rpm -q xeyes显示无安装

xeyes的软件包名不叫xeyes

案例2：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3：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

案例4: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

案例5：绑定到LDAP验证服务

– 使用系统 classroom.example.com 提供的LDAP服务

– 验证服务的基本DN是：dc=example,dc=com

– 账户信息和验证信息都是由 LDAP 提供的

– 连接要使用证书加密，证书可以在下面的链接下载：

– 确认本地可以识别ldapuser0用户

案例6：访问NFS共享

– 查看classroom.example.com的NFS共享

– 将classroom.example.com的NFS共享目录，挂载到本地/home/guests