8 权限管理

8.1 ACL权限

8.1.1 ACL权限简介与开启

1. acl权限简介 独立于所有者、所属组和其他人等权限
2. 查看分区acl权限是否开启

- df -h #查询分区
- dumpe2fs -h /dev/vda1 #dumpe2fs命令是查询指定分区详细文件系统信息的命令
- 选项：
  - -h 仅显示超级块中信息，而不显示磁盘块组的详细信息

3. 临时开启分区acl权限

- mount -o remount, acl / #重新挂载根分区，并挂载加入acl权限

4. 永久开启分区acl权限

- vi /etc/fstab
  - UUID=c2ca6f57-b15c-43ea-bca0-f239083d8bd2 / ext4 defaults,acl 1 1 #加入acl
- mount -o remount / #重新挂载文件系统或重启动系统，使修改生效

8.1.2 查看与设定ACL权限

1. 查看ACL命令

- getfacle 文件名 #查看acl权限

2. 设定ACL权限命令

- setfacl [选项] 文件名
- 选项：
  - -m 设定ACL权限
  - -x 删除指定的ACL权限
  - -b 删除所有的ACL权限
  - -d 设定默认ACL权限
  - -k 删除默认ACL权限
  - -R 递归设定ACL权限

```
useradd zhangsan
useradd lisi
useradd st
groupadd tgroup
mkdir /project
chown root:tgroup /project/
chmod 770 /project/
setfacl -m u:st:rx /project/
# 给用户st赋予r-x权限，使用"u：用户名：权限"格式
```

3. 给用户组设定ACL权限

- groupadd tgroup2
- setfacl -m g：tgroup2:rwx /project/ #为组tgroup2分配ACL权限。使用"g：组名：权限"格式

8.1.3 最大有效权限与删除ACL权限

1. 最大有效权限mask

- mask是用来指定最大有效权限的。如果我给用户赋予了ACL权限，是需要和mask的权限"相与"才能得倒用户的真正权限

2. 修改最大有效权限

- setfacl -m m:rx 文件名 #设定mask权限为r-x，使用"m：权限"格式

3. 删除acl权限

- setfacl -x u:用户名 文件名 #删除指定用户的acl权限
- setfacl -x g:组名 文件名 #删除指定用户组的acl权限

8.1.4 默认ACL权限和递归ACL权限

1. 递归ACL权限

- 针对目录下已有的文件
- 递归是指父目录在设定ACL权限时，所有的字文件和子目录也会拥有相同的ACL权限。
- setfacl -m u:用户名:权限 -R 目录名(目录也是文件)

2. 默认ACL权限

- 针对目录下新建的文件
- 默认ACL权限的作用是如果给父目录设定了默认ACL权限，那么父目录中的所有新建的字文件都会继承父目录的ACL权限。
- setfacl -m d:u:用户名:权限 目录名

8.2 文件特殊权限

8.2.1 SetUID

1. **SetUID的功能**

- 只有**可以执行的二进制程序**才能设定SUID权限
- 命令执行者要对该程序拥有x(执行)权限
- 命令执行者在执行该程序时获得该程序文件属主的身份(在执行程序的过程中灵魂附体为文件的属主)
- SetUID权限只在该程序执行过程中有效，也就是说身份改变只在程序执行过程中有效

2. passwd命令拥有SetUID权限(rws)，所以普通用户可以修改自己的密码

- ll /usr/bin/passwd

3. cat命令没有SetUID权限，所以普通用户不能查看/etc/shadow文件内容

- ll /bin/cat

4. **设定SetUID的方法**

- 4代表SUID
  - chmod 4755 文件名
  - chmod u+s 文件名

5. **危险**的SetUID

- 关键目录应该严格控制写权限。比如“/”、“/usr”等
- 用户的密码设置要严格遵守密码三原则
- 对系统中默认应该具有SetUID权限的文件作一列表，定时检查有没有这之外的文件被设置了SetUID权限

8.2.2 SetGID

1. SetGID针对**文件**的作用

- 只有可执行的二进制程序才能设置SGID权限
- 命令执行者要对该程序拥有x(执行)权限
- 命令执行在执行程序的时候，组身份升级为该程序文件的**属组**
- SetGID权限同样只在该程序执行过程中有效，也就是说组身份改变只在程序执行过程中有效

2. SetGID针对**目录**的作用

- 普通用户必须对此目录拥有r和x权限，才能进入此目录
- 普通用户在此目录中的有效组会变成此目录的**属组**
- 若普通用户对此目录拥有w权限时，新建的文件的默认属组是这个目录的属组

3. 设定SetGID

- 2代表SGID
  - chmod 2755 文件名
  - chmod g+s 文件名

4. 取消SetGID

- chmod 755 文件名
- chmod g-s 文件名

8.3.3 Sticky BIT

1. SBIT粘着位作用

- 1代表SBIT
- 粘着位目前只对**目录**有效
- 普通用户对该目录拥有w和x权限，即普通用户可以在此目录拥有写入权限
- 如果没有粘着位，因为普通用户拥有w权限，所以可以删除此目录下所有文件，包括其他用户建立的文件。一旦赋予了粘着位，除了root可以删除所有文件，普通用户就算拥有w权限，也只能删除自己建立的文件，但是不能删除其他用户建立的文件

2. 设置粘着位

- chmod 1755 目录名
- chmod o+t 目录名

3. 取消粘着位

- chmod 777 目录名
- chmod o-t 目录名

8.3 文件系统属性chattr权限

1. chattr命令格式

- chattr [+-=] [选项] 文件或目录名
- [+-=]
  - + 增加权限
  - - 删除权限
  - = 等于某权限
- 选项：
  - i #如果对文件设置i属性，那么不允许对文件进行删除、改名，也不能添加和修改数据；如果对目录设置i属性，那么只能修改目录下文件的数据，但不允许建立和删除文件
  - a #如果对文件设置a属性，那么只能在文件中增加数据，但是不能删除也不能修改数据；如果对目录设置a属性，那么只允许在目录中建立和修改文件，但是不允许删除
- 对root也生效

2. 查看文件系统属性

- lsattr 选项 文件名
- 选项：
  - -a 显示所有文件和目录
  - -d 若目标是目录，仅列出目录本身对属性，而不是子文件的

8.4 系统命令sudo权限

1. sudo权限

- root把本来只能超级用户执行的命令赋予普通用户执行。
- sudo的操作对象是**系统命令**。

2. sudo使用

- visudo #实际上修改的是/etc/sudoers文件
- root ALL=(ALL) ALL
- #用户名 **被管理(访问)的主机地址**=(可使用的身份) 授权命令(绝对路径)
- %wheel ALL=(ALL) ALL
- #%组名 被管理的主机地址=(可使用的身份) 授权命令(绝对路径)

3. 授权sc用户可以重启服务器

- visudo
- sc ALL= /sbin/shutdown -r now

4. 普通用户执行sudo赋予的命令

- su -sc
- sudo -l#查看可以使用的sudo命令
- sudo /sbin/shutdown -r now #普通用户执行sudo赋予的命令

9 文件系统管理

9.1回顾分区和文件系统

1. 分区类型

- **主分区**：总共最多只能有4个
- **扩展分区**：
  - 最多只能有1个，也算做主分区的一种
  - 主分区+扩展分区最多有4个
  - 但是扩展分区不能存储数据和格式化，必须再划分成逻辑分区才能使用
  - 逻辑分区
- **逻辑分区**:
  - 是在扩展分区中划分
  - 如果是IDE硬盘，Linux最多支持59个逻辑分区
  - 如果是SCSI硬盘，Linux最多支持11个逻辑分区

2. 分区表示方法

- 注：1、2、3、4这四个分区号只能给主分区和扩展分区使用，逻辑分区只能从5开始

分区	分区设备文件名
主分区1	/dev/sda1
主分区2	/dev/sda2
主分区3	/dev/sda3
扩展分区	/dev/sda4
逻辑分区1	/dev/sda5
逻辑分区2	/dev/sda6
逻辑分区3	/dev/sda7

3. 文件系统

- ext2
  - 最大支持16TB的分区和最大2TB的文件
- ext3
  - 最大支持16TB的分区和最大2TB的文件
  - 支持日志功能
- ext4
  - 最大支持1EB的分区和最大16TB的文件

9.2 文件系统常用命令

9.2.1 文件系统命令

1. **df**

- 功能描述：文件系统查看命令，**统计文件系统的占用情况**
- 命令格式：df[选项] [挂载点]
- 选项：
  - -a 显示所有文件系统信息，包括特殊文件系统，如/proc、/sysfs
  - -h 使用习惯单位显示容量，如KB、MB、GB等
  - -T 显示文件系统类型
  - -m 以MB为单位显示容量
  - -k 以KB为单位显示容量

2. **du**

- 功能描述：**统计目录或文件大小**
- 命令格式：du [选项] [目录或文件名]
- 选项：
  - -a 显示每个子文件的磁盘占用量。默认只统计字目录的磁盘占用量
  - -h 使用习惯单位显示磁盘占用量，如KB、MB、GB等
  - -s 统计总占用量，而不列出字目录和子文件的占用量
- **df命令和du命令的区别**
  - df命令是从文件系统考虑的，不光要考虑文件占用的空间，还要统计被命令或程序占用的空间(最常见的就是文件已经删除，但是程序并没有释放空间)
  - du命令是面向文件的，只会计算文件或者目录占用的空间

3. **fsck**

- 功能描述：**文件系统修复命令**
- 命令格式：fsck [选项] 分区设备文件名
- 选项：
  - -a 不用显示用户提示，自动修复文件系统
  - -y 自动修复，和-a作用一致。不过有些文件系统只支持-y

4. **dump2fs**

- 功能描述：**显示磁盘状态命令**
- 命令格式：dumpe2fs 分区设备文件名

9.2.2 挂载命令

1. mount [-l]

- **查询**系统中已经挂载的设备，-l会显示卷标名称

2. mount -a

- 依据配置文件/etc/fstab的内容，**自动挂载**

3. 挂载命令格式：mount [-t 文件系统] [-L 卷标名] \ [-o 特殊选项] 设备文件名 挂载点

- 选项：
  - -t 文件系统：加入文件系统类型来指定挂载的类型，可以以ext3、ext4、vfat(32)、fat(16)、iso9660等文件系统
  - -L 卷标名(别名)：挂载指定卷标等分区，而不是安装设备文件名挂载
  - -o 特殊选项：可以指定挂载的额外选项(前者为系统默认)
  - defaults 定义默认值，相当于rw、suid、dev、exec、auto、mouser、async这七个选项
  - atime/natime 更新访问时间/不更新访问时间(访问分区时，是否更新文件的访问时间)
  - async/sync 异步/同步
  - auto/noauto 自动/手动(mount -a命令执行时，是否会自动安装/etc/fstab文件内容挂载)
  - exec/noexec 执行/不执行(设定是否允许在文件系统中执行可执行文件)
  - rw/ro 读写/只读(文件系统挂载时，是否具有读写权限)
  - suid/nosuid 具有/不具有SUID权限(设定文件系统是否具有SUID和SGID的权限)
  - user/nouser 允许/不允许普通用户挂载(设定文件系统是否允许普通用户挂载)
  - remount 重新挂载已经挂载的文件系统，一般用于指定修改特殊权限
  - usrquota 写入代表文件系统支持用户磁盘配额，默认不支持
  - grpquota 写入代表文件系统支持组磁盘配额，默认不支持

9.2.3 挂载光盘和U盘

9.2.4 支持NTFS文件系统

9.3 fdisk分区

1. 查询硬盘

- fdisk -l

2. 使用fdisk命令分区

- fdisk /dev/sdb

3. 重新读取分区表

- **partprobe**(最好在每次分区后使用)

4. 格式化分区

- mkfs -t ext4 /dev/sdb1

5. 建立挂载点并挂载

- mkdir /disk1
- mount /dev/sdb1 /disk1/

9.4 分区自动挂载和/etc/fstab文件修复

9.5 分配swap分区