一、账户与安全

Linux系统对账号与组的管理是通过ID号来实现的，在登录时输入用户名与对应的密码，操作系统会将用户名转化为ID号后再判断该账号是否存在，并对比密码是否匹配。Linux中，用户ID号被称为UID，组ID号被称为GID。其中，UID为0，代表超级管理员，也就是通常所说的root账号，1~499之间的ID系统会预留下来。这样我们创建的普通用户ID号会从500算起。

Linux操作系统中的组分为基本组与附加组，一个用户同一时刻仅可以加入一个基本组中，但可以同时加入多个附加组。默认在创建用户时，系统默认会自动创建同名的组，并设置用户加入该基本组中。

1.创建账户及组

使用系统命令useradd可以创建我们需要的账户，groupadd命令用来创建组账户。需要注意的是，创建账户及组时需要有管理员权限。

① **useradd [选项] 用户名称**

选项：

-c 设置账号描述信息，一般为账号全称。

-d 设置账号home目录，默认为/home/用户名

-e 设置账户的失效日期，格式为YYYY-MM-DD

-g 设置账户的基本组

-G 设置账户的附加组，多个附加组中间用逗号隔开

-M 不创建账号home目录，一般与-s结合使用

-s 设置账户的登录shell，默认为bash

-u 指定账户UID

基本组：如果没有指定用户组，创建用户的时候系统会默认同时创建一个和这个用户名同名的组，这个组就是基本组，不可以把用户从基本组中删除。在创建文件时，文件的所属组就是用户的基本组。

附加组：除了基本组之外，用户所在的其他组，都是附加组。用户是可以从附加组中被删除的。

用户不论为与基本组中还是附加组中，就会拥有该组的权限。一个用户可以属于多个附加组。但是一个用户只能有一个基本组。

② **groupadd [选项] 组名称**

-g 设置组ID号

③ 查看所有用户及用户组

cat /etc/group

返回的格式为：若干条记录，group_name:passwd:GID:user_list

第一字段：用户组名称； 第二字段：用户组密码； 第三字段：GID 第四字段：用户列表，每个用户之间用,号分割；本字段可以为空；如果字段为空表示用户组为GID的用户名；只显示附加组成员，基本组成员不显示。

cat /etc/passwd

返回的格式为：若干条记录，
login_name:passwd:UID:GID:user_name:home_directory:shell

第一个字段（login_name）：注册名，用于区分不同的用户。在同一系统中注册名是唯一的。linux中区分大小写 第二个字段（passwd）：系统口令来验证用户的合法性。超级用户root或某些高级用户可以使用系统命令passwd来更改系统中所有用户的口令，普通用户也可以在登录后使用passwd命令来更改自己的口令。通常将passwd文件中的口令字段使用一个“x”来代替，将/etc/shadow作为真正的口令文件，用于保存个人口令在内的数据。 第三个字段（UID）：UID是数值，是Linux系统中唯一的用户标识，用于区别不同的用户。 第四个字段（GID）：这是当前用户的缺省工作组标识，或者是在useradd时指定的用户组。 第五个字段（user_name）：在useradd时通过-c指定的用户信息。 第六个字段（home_directory）：该字段定义了个人用户的主目录，当用户登录后，它的shell将把该目录作为用户的工作目录 第七个字段（shell）：命令解释程序，shell是当用户登录系统时运行的程序名称，通常是一个shell程序的全路径名。/bin/bash为可登陆系统shell，/sbin/nologin表示账户无法登陆系统。

cat /etc/shadow

第一个字段为用户名，第二个字段为密码（未设置密码时为!!，设置密码后加密显示），第三个字段为上次修改密码的时间距离1970-01-01有多少天，第四个字段为密码最短有效天数（密码至少使用多少天，0代表无限制），第五个字段为密码最长有效天数（默认为99999天，可以理解为永不过期），第六个字段为密码过期后的宽限天数（默认过期提前7天警告，但进入警告日期后认可以使用旧密码登录系统），第七个字段为密码过期后的宽限天数（密码过期后，预留几天给账户修改密码，此时已无法使用旧密码登录系统），第八个字段为账户失效日期（从1970-01-01起多少天后账户失效），第九个字段暂时保留未使用。

cat /etc/gshadow

保存的是组账户密码文件。第一列为组账号名称，第二列为组密码（一般为管理员密码），第三列为组管理员，第四列为组成员（与/etc/group第四列相同）。

gpasswd admin 设置组密码

gpasswd -A mail admin 将mail账户设置为组admin的管理员

2.修改账户和组

① **passwd [选项] [账户名称]**

-l 锁定账户，仅root可使用此选项

--stdin 从文件或管道读取密码

-u 解锁账户

-d 快速清空账户密码，仅root可使用此选项

② **usermod [选项]** 账户名称

-d 修改账户home目录

-e 修改账户的失效日期

-g 修改账户所属基本组

-G 修改账户所属附加组

-s 修改账户登录shell

-u 修改账户UID

3.删除账户及组

① **userdel [选项]** 账户名称

-r 删除账户及相关文件

② **groupdel** 组名

4.文件及目录权限

linux权限主要分为读、写、执行三种控制，使用ls -l命令查看文件或目录信息时，系统会显示为r（读取权限）、w（写入权限）、x（执行权限）。ls -l的结果解释如下：

第一列的第一个字符代表文件类型：-代表普通文件，d代表目录，l代表链接文件，b或c代表设备。第二至第九个字符代表权限，三位一组分别为所有者的权限、所属组的权限、其他账户的权限。

第二列为链接数量或子目录个数（文件和目录这个数字的含义有所不同）。

第三列为文档所有者。

第四列为文档所属组。

第五列为容量。

第六列为最近文档被修改的月份。

第七列为文档最近被修改的日期。

第八列为文档最近被修改的时间。

第九列为文件或目录名称。

另外，可以用数字代表权限：4代表r，2代表w，1代表x。

① **chmod [选项] 权限 文件或目录**

选项：

--reference=RFILE 根据参考文档设置权限

-R 递归将权限应用于所有的子目录与子文件

权限：u代表所有者，g代表所属组，o代表其他用户，a代表所有人。

chmod u=rwx,g=rwx,o=rwx install.log： 表示给所有者rwx权限，所属组的rwx权限，其他用户rwx。

chmod g-x,o-rw install.log： 表示在原有基础上移除所属组的x权限，移除其他用户的rw权限。

chmod 700 install.log： 表示将权限修改为rwx------。

chmod --reference=install.log.syslog install.log： 表示以install.log.syslog为标准修改install.log的权限。

② **chown [选项] [所有者][:[所属组]] 文件或目录**

选项：

-R 递归将权限应用于所有的子目录和子文件

chown user2:mail install： 修改文件的所有者为user2，所属组为mail

chown :root install： 仅修改文件所属组为root

chown root install： 仅修改文件所属者为root

③ **ACL访问控制权限**

ACL访问控制表

二、计划任务

1.at 一次性计划任务

使用at制定一次性计划任务前需要确保atd服务是开启的，否则计划任务不会被执行，使用systemctl start atd开启服务，并使用systemctl enable atd确保该服务开机启动。

at

-m 当计划任务执行结束后发送邮件给用户

-l 查看用户计划任务

-d 删除用户计划任务

-c 查看at计划任务具体内容

2.cron周期性计划任务<对比Quartz>

使用cron制定计划任务前需要确保crond服务是开启的，否则计划任务不会被执行，使用systemctl start crond开启服务，并使用systemctl enable crond确保该服务开机启动。

crontab

-u 指定计划任务的用户，默认为当前用户

-l 查看计划任务

-r 删除计划任务

-e 编辑计划任务

-i 使用-r删除计划任务时，要求用户确认删除

命令格式为:

分 时 日 月 周 命令

分的取值范围是0~23

时的取值范围是0~23

日的取值范围是1~31

月的取值范围是1~12

周的范围是0~7，其中0和7都表示周日。

如果需要指定的是时间段，可以使用横杠（-）表示一段连续的时间，使用逗号（,）表示若干不连续的时间，使用星号（*）表示所有时间，用除号（/）表示间隔时间。

3.计划任务权限