账户和权限

任何一个系统都是通过账户和密码判断当前使用者身份，系统安全的第一步就是账户管理

在Linux或Unix系统中用户是基于用户的UID数值进行判断身份

0 代表是管理员用户

1--499 代表程序用户，一般管理员管理，安装软件包的时候会自动创建，不用于系统登录只用于管理某个服务用

500-- 代表普通用户，管理员创建可以分配给其他用户用于登录系统用的，用户管理管理的就是普通用户

在7的系统中，0代表root用户，1--499系统用户500--999代表程序用户，1000--才是普通用户

在GUI登录界面，显示登录的只能是普通用户，管理员和程序用户都不会显示

组分为基本组和附加组：组自身没有基本组和附加组区别，当用户添加至组的时候可以以这个组为基本组或附加组

基本组：用户只能加入一个基本组，而且必须加入，唯一性，捆绑用户，当任何用户创建文件或文件夹的时候默认拥有者是自己，拥有组是自己的主要组（基本组），建议以人员少的组为主要组，人员多的为附加组，这个是基于安全性方面的考虑

附加组：用户可以加入任意附加组，有也可以没有也行，多少个都无所谓，任意性

useradd 创建用户的命令

-u 指定用户的UID数值，如果不指定，默认以最后一个用户+1，默认只能是普通用户的UID

-g 指定用户的基本组，如果不指定，默认会创建一个和用户同名的组做基本组

-G 指定用户的附加组，如果不指定，默认没有附加组

-d 指定用户的宿主目录，如果不指定，默认会在/home目录下创建一个和用户同名的文件夹

-s 指定用户的shell，用户通过shell来控制服务器，服务器通过shell反馈结果给用户，cat /etc/shells查看当前系统支持的shell，/bin/bash是在Linux系统中默认使用的shell，/sbin/nologin非交互式shell，对于系统中大部分程序用户以及远程访问本地服务（不需要本地登录）一般都是这个shell

-M 不创建用户的宿主目录，和-d不能同时用

-m 创建用户的宿主目录，默认有该选项（Solaris系统默认没有该选项）

-e 指定用户的过期时间，如果不指定，默认永不过期

useradd zhangsan 默认属性创建zhangsan用户

useradd -u 1000 -g bin -G wheel -d /lisi -s /sbin/nologin -e 2018-1-1 lisi 定义了用户的各种属性

id zhangsan 测试用户是否存在

UID要求唯一，每个用户都是唯一的

/etc/passwd 这个记录了系统中所有账户的信息，该文件以:为分隔符，划分了七段内容，每段内容可以参考man 5 passwd有详解，最后一段是shell，可以看到UID小于500基本上都是/sbin/nologin

/etc/shadow 这个是记录了系统中所有账户的密码信息，该文件以:为分隔符，划分了九段内容，每段可以参考man 5 shadow有详解

passwd 命令，可以修改和设置用户的密码信息，如果不设置密码，默认情况下所有账户都是不能登录系统，新建账户必须创建密码，否则拒绝登录

usermod 修改一个已存在的账户的信息，支持useradd中的很多选项

userdel 删除一个已存在的账户，建议添加-r选项，会删除用户的宿主目录以及用户邮件文件

groupadd 创建一个组，可以使用-g指定组的GID编号

groupdel 删除一个组，如果有用户以该组为基本组，不允许删除

Linux系统中默认只有root一个管理员，其他用户添加至root组仅能查看root组可以查看的文件而已，没有特殊权限（修改IP），如果希望创建第二个管理员，可以创建一个账户，设置账户的密码，将用户的UID改为0即可，这个账户登录系统后提示也是root

Linux中权限的管理：

Linux中只有三个权限r（读）、w（写）、x（执行），x权限一般只有文件夹才具备，可以使用cd命令或者鼠标双击打开文件夹，如果没有x权限直接报错，文件不需要x权限，只有把文件当做程序运行（脚本）才需要x权限

Linux中权限对象，默认一个文件或文件夹有一个UID和一个GID，可以使用ls -l查看

每个用户有一个UID和若干个GID（基本组和附加组）

如果用户的UID和文件的UID一致，认为用户是文件或文件夹的拥有者，如果UID不一致再次检查GID，如果用户的GID有任何一个能够和文件或文件夹的GID一致，认为是文件或文件夹的拥有组，如果GID都不能一致，认为是其他人

权限默认在Linux使用ugo表示，ls -l中看到的前面10个字符中后面9个代表三类用户三个权限，前三个代表拥有者，中间三个代表拥有组，最后三个代表其他人，第一个字符代表的是文件类型

权限第二种表示方式使用3位八进制数字表示，r（4），w（2），x（1），分别将拥有者（u），拥有组（g），其他人（o）自己的三个权限位加起来就是得到三个八进制数字

touch test.txt 创建测试文件

ls test.txt

chmod 777 test.txt

ls test.txt

chmod 000 test.txt

ls test.txt

chmod 123 test.txt

ls test.txt

chmod 456 test.txt

ls test.txt

chmod u+w test.txt

ls test.txt

chmod g-x test.txt

ls test.txt

chmod o= test.txt

ls test.txt

umask 查看当前用户反掩码，当用户创建文件或文件夹的时候默认以最大权限减去umask数值就得到新建文件或文件夹的权限，文件夹是777 ，文件是666

单独设置某个用户或组的权限可以参考setfacl命令

chown 修改拥有者或拥有组

chown 用户名 文件或文件夹 修改属主

chown :组名 文件或文件夹 修改属组

chown 用户名:组名 文件或文件夹 同时修改拥有者和拥有组

chmod和chown都支持-R选项，文件夹中递归，不仅会修改文件夹自身的属性同时也会将所有子目录或文件全部修改

软件包安装

rpm 红帽包管理，红帽做的软件包，源码包安装需要配置和编译再安装，rpm将编译的工作提前完成，安装只需要一条命令即可，很多Linux和Unix都支持RPM，安装光盘中有绝大多数的RPM包

使用光驱，确保虚拟机设置中，CD/DVD的已连接是选中

mkdir /media/cdrom

mount /dev/cdrom /media/cdrom 挂载光驱到指定目录

ls /media/cdrom/Packages 该目录是光盘中所有的RPM包的位置

rpm -q vsftpd 查询vsftpd软件是否已安装

rpm -ivh /media/cdrom/Packages/vsftpd-\* 安装软件包

rpm -q vsftpd

rpm -e vsftpd 卸载软件包

RPM包安装过程中可能会涉及依赖关系，被依赖的软件包需要先安装，如果依赖关系比较复杂，安装软件变得非常困难，可能需要花费大量时间在寻找依赖关系上。yum可以自动帮助用户解决依赖关系

CentOS系统默认情况下yum可用，会通过互联网连接CentOS官方网站下载软件更新，也可以换其他更新源，如果服务器不能上网

本地更新源配置：

mkdir /etc/yum.repos.d/bak 创建一个目录放置以前更新源

mv /etc/yum.repos.d/Cent\* /etc/yum.repos.d/bak 移动以前更新源文件至备份目录下

自己创建本地更新源文件

vim /etc/yum.repos.d/local.repo 位置固定，名称任意，必须以.repo结尾

写入下面内容：

[local] 内容随意，本地记录唯一即可

name=This is my repo 描述信息，随意写

baseurl=file:///media/cdrom 定义更新源位置，光驱就是一个更新源

enabled=1 是否启用该记录，1为启用0为禁用

gpgcheck=0 是否验证签名，0为禁用，1为启用，如果是1的话需要再定义gpgkey

yum install gcc-c++ 可以自动解决依赖关系

cat /etc/yum.conf 记录了yum主配置文件，可以看到更新源应该放置的位置，最后两行