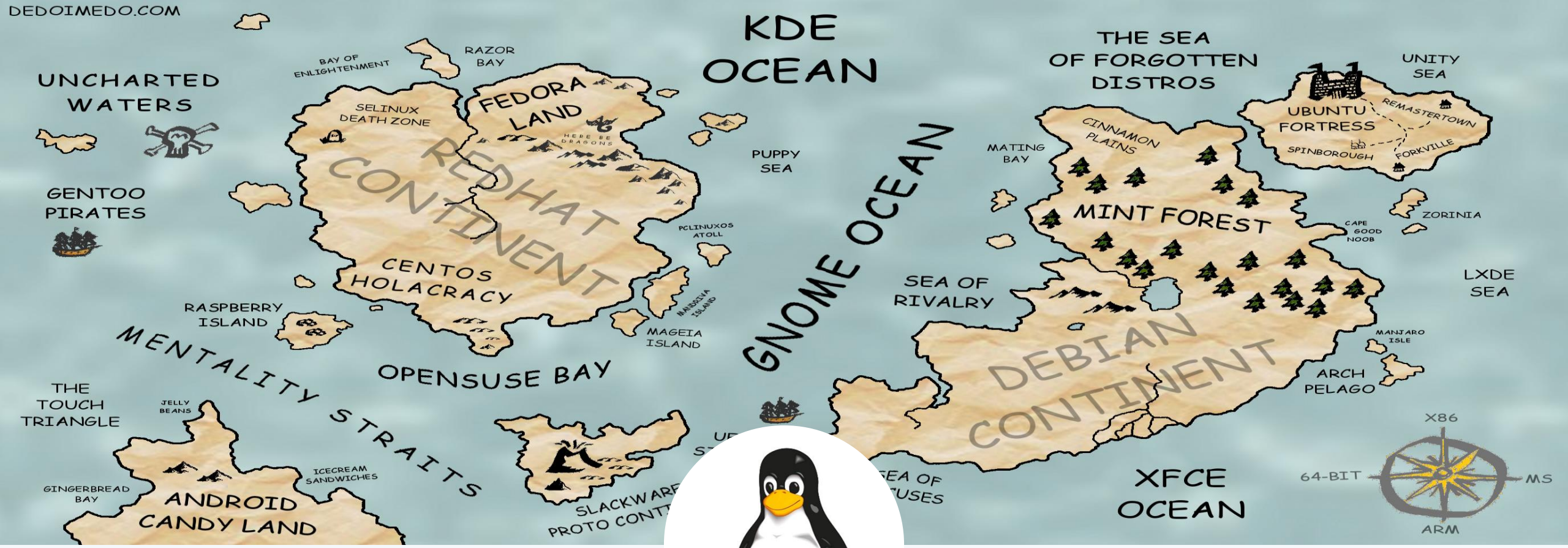



# 用户身份与文件权限

任课教师：刘遄 www.LinuxProbe.com

# 课程概述

01 **用户身份与能力**
User Identity And Capabilities

02 **文件权限与归属**
Document Authority And Ownership

03 **文件的特殊权限**
Special Permissions For Files

04 **文件的隐藏属性**
Hidden Properties Of Files

05 **文件访问控制列表**
File Access Control List

06 **su命令与sudo服务**
Su Command And Sudo Service

# 前言

01 Linux是一个多用户、多任务的操作系统，具有很好的稳定性与安全性，在幕后保障Linux系统的安全则是一系列复杂的配置工作。

02 文件的所有者、所属组以及其他人可对文件进行的读（r）、写（w）、执行（x）等操作，如何在Linux系统中添加、删除、修改用户账户信息。

03 使用SUID、SGID与SBIT特殊权限更加灵活地设置系统权限，来弥补对文件设置一般操作权限时所带来的不足。

04 隐藏权限能够给系统增加一层隐形的防护层，让黑客最多只能查看关键日志信息，而不能篡改或删除。

05 文件访问控制列表（Access Control List，ACL）可以进一步让单一用户、用户组对单一文件或目录进行特殊的权限设置，让文件具有能满足工作需求的最小权限。

06 如何使用su命令与sudo服务让普通用户具备管理员的权限，这不仅能够满足日常的工作需求，还可以确保系统的安全性。


# 用户身份与能力

User Identity And Capabilities

# 用户身份与能力

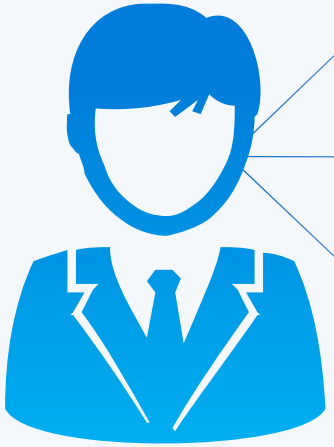
01 在Linux的学习过程中如果使用普通用户身份进行操作，则在配置服务之后出现错误时很难判断是系统自身的问题还是因为权限不足而导致的；这无疑会给大家的学习过程徒增坎坷。

02 更何况我们的实验环境是使用VMware虚拟机软件搭建的，可以将安装好的系统设置为一次快照，这样即便系统彻底崩溃了，也可以在5秒的时间内快速还原出一台全新的系统，而不用担心数据丢失。

03 很多图书或培训机构的老师会讲到，Linux系统中的管理员就是root。这其实是错误的，Linux系统的管理员之所以是root，并不是因为它的名字叫root，而是因为该用户的身份号码即UID（User IDentification）的数值为0。

04 在Linux系统中，UID就像我们的身份证号码一样具有唯一性，因此可通过用户的UID值来判断用户身份。

# 用户身份



1 **管理员UID为0**
系统的管理员用户。

2 **系统用户UID为1～999**
Linux系统为了避免因某个服务程序出现漏洞而被黑客提权至整台服务器，默认服务程序会由独立的系统用户负责运行，进而有效控制被破坏范围。

3 **普通用户UID从1000开始**
是由管理员创建的用于日常工作的用户。

**需要注意的是，UID是不能冲突的，而且管理员创建的普通用户的UID默认是从1000开始的（即使前面有闲置的号码）。**

# 用户组

## 用户组

为了方便管理属于同一组的用户，Linux系统中还引入了用户组的概念。

通过使用用户组号码（GID，Group IDentification），可以把多个用户加入到同一个组中，从而方便为组中的用户统一规划权限或指定任务。

## 基本用户组

在Linux系统中创建每个用户时，将自动创建一个与其同名的基本用户组，而且这个基本用户组只有该用户一个人。

如果该用户以后被归纳到其他用户组，则这个其他用户组称之为扩展用户组。

一个用户只有一个基本用户组，但是可以有多个扩展用户组，从而满足日常的工作需要。

**注：**基本用户组就像是原生家庭，是在创建账号（出生）时就自动生成的；而扩展用户组则像工作单位，为了完成工作，需要加入到各个不同的群体中，这是需要手动添加的。

# 用户能力

## id命令

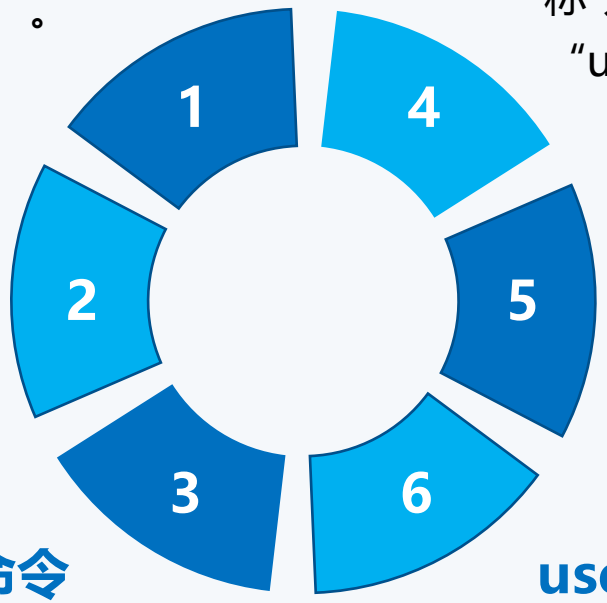
id命令用于显示用户的详细信息，语法格式为“id用户名”。

## useradd命令

useradd命令用于创建新的用户账户，语法格式为“useradd [参数] 用户名”。

## groupadd命令

groupadd命令用于创建新的用户组，语法格式为“groupadd [参数] 群组名”。




## usermod命令

usermod命令用于修改用户的属性，英文全称为“user modify”，语法格式为“usermod [参数] 用户名”。

## passwd命令

passwd命令用于修改用户的密码、过期时间等信息，英文全称为“password”，语法格式为“passwd [参数] 用户名”。

## userdel命令

userdel命令用于删除已有的用户账户，英文全称为“user delete”，语法格式为“userdel [参数] 用户名”。

# useradd命令中的参数以及作用

| 参数 | 作用 |
| --- | --- |
| -d | 指定用户的家目录（默认为/home/username） |
| -e | 账户的到期时间，格式为YYYY-MM-DD. |
| -u | 指定该用户的默认UID |
| -g | 指定一个初始的用户基本组（必须已存在） |
| -G | 指定一个或多个扩展用户组 |
| -N | 不创建与用户同名的基本用户组 |
| -s | 指定该用户的默认Shell解释器 |

# usermod命令中的参数以及作用

| 参数 | 作用 |
| --- | --- |
| -c | 填写用户账户的备注信息 |
| -d –m | 参数-m与参数-d连用，可重新指定用户的家目录并自动把旧的数据转移过去 |
| -e | 账户的到期时间，格式为YYYY-MM-DD |
| -g | 变更所属用户组 |
| -G | 变更扩展用户组 |
| -L | 锁定用户禁止其登录系统 |
| -U | 解锁用户，允许其登录系统 |
| -s | 变更默认终端 |
| -u | 修改用户的UID |

# passwd命令中的参数以及作用

| 参数 | 作用 |
| --- | --- |
| -l | 锁定用户，禁止其登录 |
| -u | 解除锁定，允许用户登录 |
| --stdin | 通过标准输入修改用户密码，如echo "NewPassWord" \| passwd --stdin Username |
| -d | 使该用户可用空密码登录系统 |
| -e | 强制用户在下次登录时修改密码 |
| -S | 显示用户的密码是否被锁定，以及密码所采用的加密算法名称 |

# userdel命令中的参数以及作用

| 参数 | 作用 |
| --- | --- |
| -f | 强制删除用户 |
| -r | 同时删除用户及用户家目录 |


# 文件权限与归属

Document Authority And Ownership

# 文件权限


1

**可读（r）**

“可读”表示能够读取目录内的文件列表；

2

**可写（w）**

“可写”表示能够在目录内新增、删除、重命名文件；

3

**可执行（x）**

“可执行”则表示能够进入该目录。

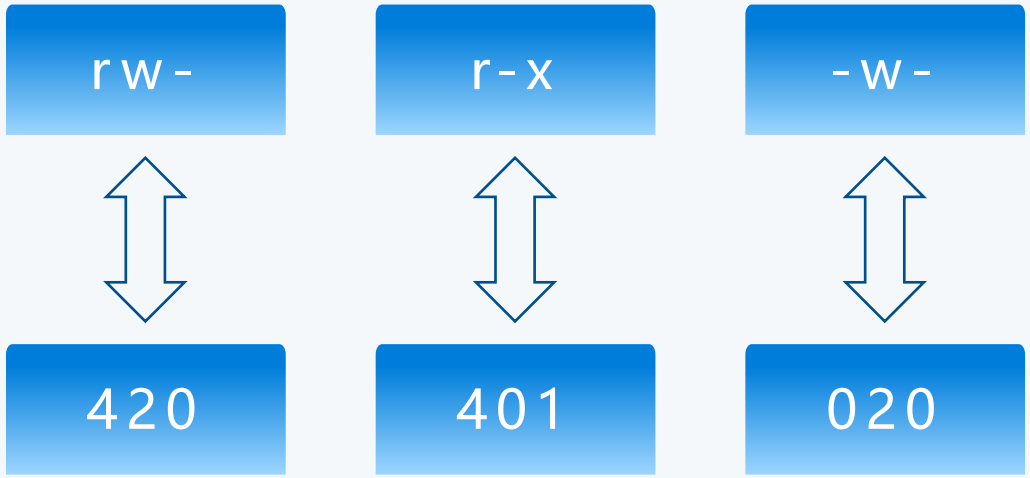
# 可读、可写、可执行权限对应的命令在文件和目录上的区别

| | 文件 | 目录 |
|---|---|---|
| 可读（r） | cat | ls |
| 可写（w） | vim | touch |
| 可执行（x） | ./script | cd |

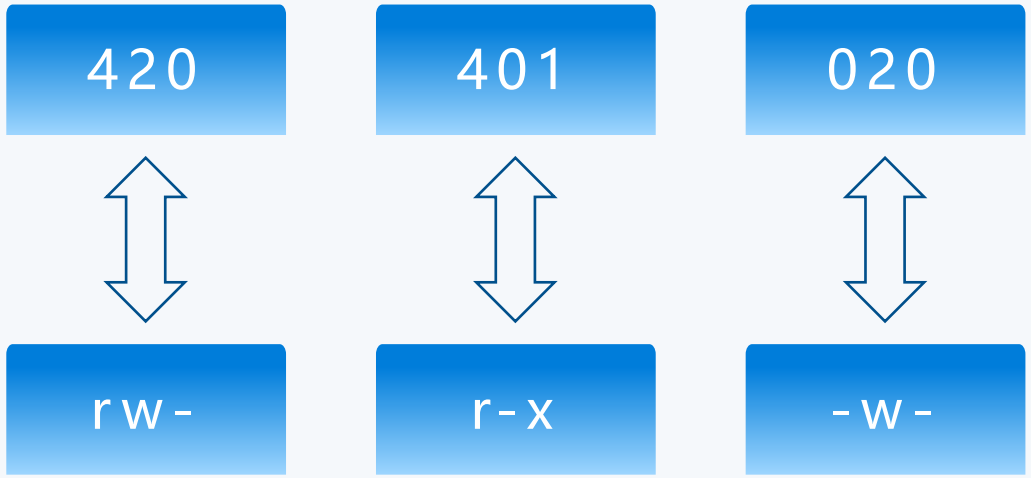
# 文件权限的字符与数字表示

| 权限项 | 可读 | 可写 | 可执行 | 可读 | 可写 | 可执行 | 可读 | 可写 | 可执行 |
|---|---|---|---|---|---|---|---|---|---|
| 字符表示 | r | w | x | r | w | x | r | w | x |
| 数字表示 | 4 | 2 | 1 | 4 | 2 | 1 | 4 | 2 | 1 |
| 权限分配 | 文件所有者 | | | 文件所属组 | | | 其他用户 | | |

# 转换示意图




字符表示权限与数字表示权限的转换示意图




数字与字符权限转换示意图

# 常见的文件类型

1. 普通文件（-）
2. 目录文件（d）
3. 链接文件（l）
4. 管道文件（p）
5. 块设备文件（b）
6. 字符设备文件（c）。

普通文件的范围特别广泛，比如纯文本信息、服务配置信息、日志信息以及Shell脚本等，都属于普通文件。几乎在每个目录下都能看到普通文件（-）和目录文件（d）的身影。块设备文件（b）和字符设备文件（c）一般是指硬件设备，比如鼠标、键盘、光驱、硬盘等，在/dev/目录中最为常见。应该很少有人会对鼠标、键盘进行硬件级别的管理吧。


# 文件的特殊权限

Special Permissions For Files

# 文件的特殊权限

## SUID

SUID是一种对二进制程序进行设置的特殊权限，能够让二进制程序的执行者临时拥有所有者的权限（仅对拥有执行权限的二进制程序有效）。

## SGID

SGID特殊权限有两种应用场景：当对二进制程序进行设置时，能够让执行者临时获取文件所属组的权限；当对目录进行设置时，则是让目录内新创建的文件自动继承该目录原有用户组的名称。

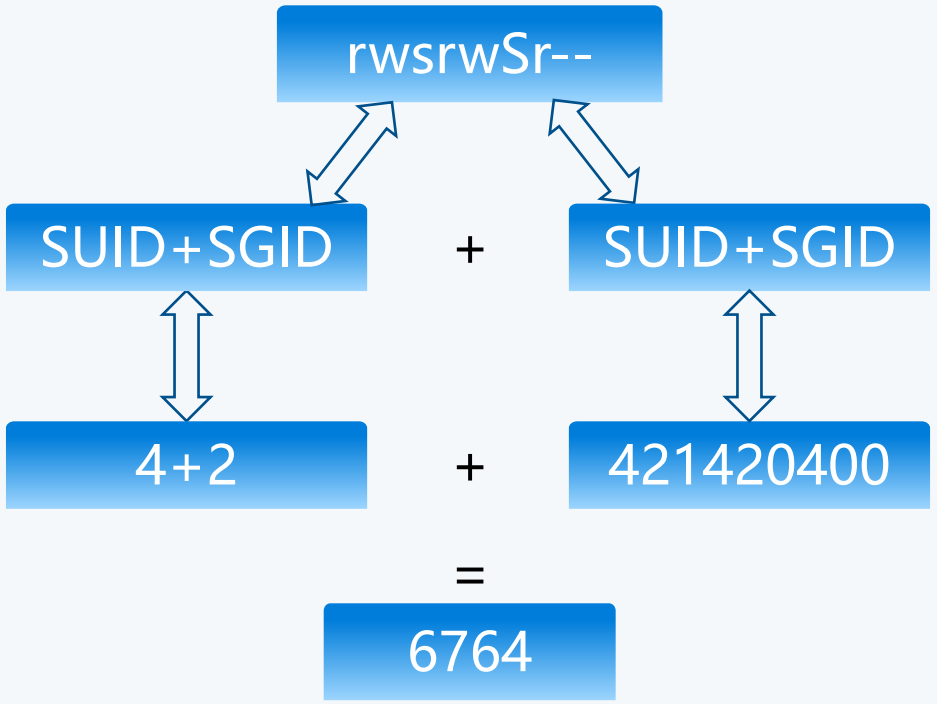
## SBIT

SBIT特殊权限位可确保用户只能删除自己的文件，而不能删除其他用户的文件。换句话说，当对某个目录设置了SBIT粘滞位权限后，那么该目录中的文件就只能被其所有者执行删除操作了。

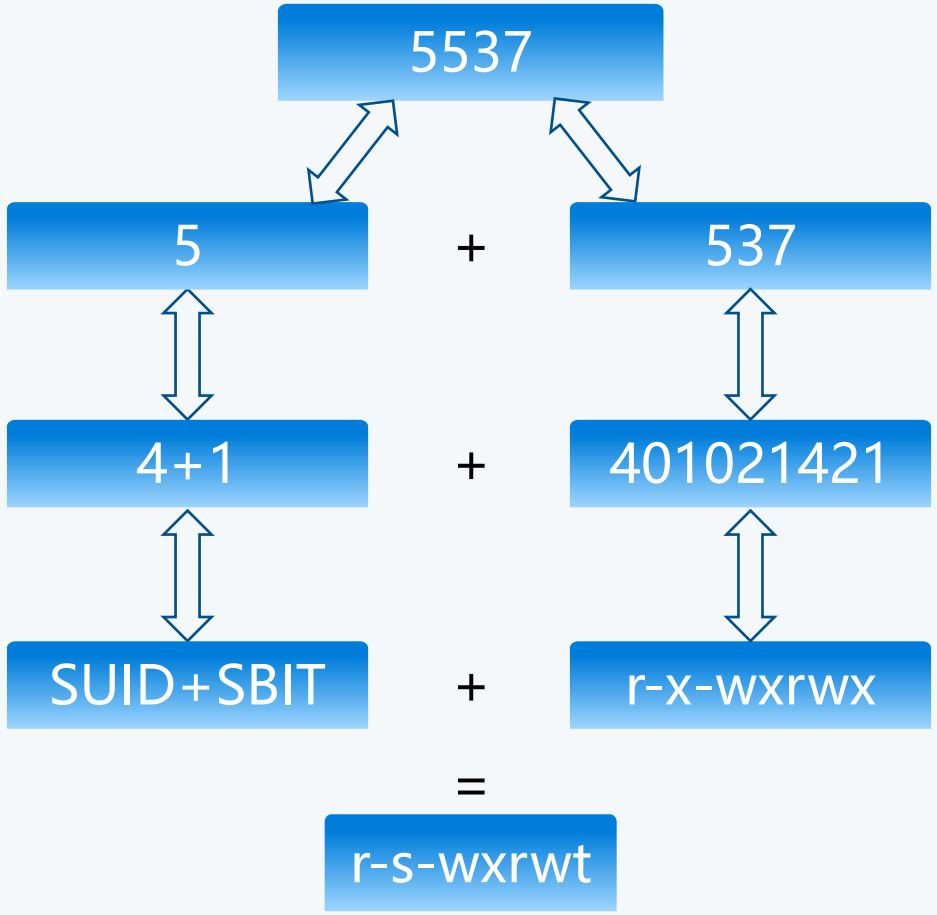
# SUID、SGID、SBIT特殊权限的设置参数

| 参数 | 作用 |
| --- | --- |
| u+s | 设置SUID权限 |
| u-s | 取消SUID权限 |
| g+s | 设置SGID权限 |
| g-s | 取消SGID权限 |
| o+t | 设置SBIT权限 |
| o-t | 取消SBIT权限 |

# 文件的特殊权限




将权限的字符表示法转换为数字表示法




将权限的数字表示法转换为字符标识法


# 文件的隐藏属性

Hidden Properties Of Files

# 文件的隐藏属性

01

## chattr命令

chattr命令用于设置文件的隐藏权限，英文全称为change attributes，语法格式为“chattr [参数] 文件名称”。

02

## lsattr命令

lsattr命令用于查看文件的隐藏权限，英文全称为“list attributes”，语法格式为“lsattr [参数] 文件名称”。

# chattr命令中的参数及其作用

| 参数 | 作用 |
| --- | --- |
| i | 无法对文件进行修改；若对目录设置了该参数，则仅能修改其中的子文件内容而不能新建或删除文件 |
| a | 仅允许补充（追加）内容，无法覆盖/删除内容（Append Only） |
| S | 文件内容在变更后立即同步到硬盘（sync） |
| s | 彻底从硬盘中删除，不可恢复（用零块填充原文件所在的硬盘区域） |
| A | 不再修改这个文件或目录的最后访问时间（Atime） |
| b | 不再修改文件或目录的存取时间 |
| D | 检查压缩文件中的错误 |
| d | 使用dump命令备份时忽略本文件/目录 |
| c | 默认将文件或目录进行压缩 |
| u | 当删除该文件后依然保留其在硬盘中的数据，方便日后恢复 |
| t | 让文件系统支持尾部合并（tail-merging） |
| x | 可以直接访问压缩文件中的内容 |


# 文件访问控制列表

File Access Control List

# 文件访问控制列表

## setfacl命令

setfacl命令用于管理文件的ACL权限规则，英文全称为“set files ACL”，语法格式为“setfacl [参数] 文件名称”。

## getfacl命令

getfacl命令用于查看文件的ACL权限规则，英文全称为“get files ACL”，语法格式为“getfacl [参数] 文件名称”。

| 参数 | 作用 |
| --- | --- |
| -m | 修改权限 |
| -M | 从文件中读取权限 |
| -x | 删除某个权限 |
| -b | 删除全部权限 |
| -R | 递归子目录 |

setfacl命令中的参数以及作用


# su命令与sudo服务

Su Command And Sudo Service

# su命令与sudo服务

01 授权原则：在保证普通用户完成相应工作的前提下，尽可能少地赋予额外的权限。

02 sudo命令用于给普通用户提供额外的权限，语法格式为“sudo [参数] 用户名”。

03 使用sudo命令可以给普通用户提供额外的权限来完成原本只有root管理员才能完成的任务，可以限制用户执行指定的命令，记录用户执行过的每一条命令，集中管理用户与权限（/etc/sudoers），以及可以在验证密码后的一段时间无须让用户再次验证密码。

| 参数 | 作用 |
| --- | --- |
| -h | 列出帮助信息 |
| -l | 列出当前用户可执行的命令 |
| -u用户名或UID值 | 以指定的用户身份执行命令 |
| -k | 清空密码的有效时间，下次执行sudo时需要再次进行密码验证 |
| -b | 在后台执行指定的命令 |
| -p | 更改询问密码的提示语 |

setfacl命令中的参数以及作用

# su命令与sudo服务

**谁可以使用 允许使用的主机 = （以谁的身份） 可执行命令的列表**

| 谁可以使用 | 允许使用的主机 | 以谁的身份 | 可执行命令的列表 |
| --- | --- | --- | --- |
| 稍后要为哪位用户进行命令授权。 | 可以填写ALL表示不限制来源的主机，亦可填写如192.168.10.0/24这样的网段限制来源地址，使得只有从允许网段登录时才能使用sudo命令。 | 可以填写ALL表示系统最高权限，也可以是另外一位用户的名字。 | 可以填写ALL表示不限制命令，亦可填写如/usr/bin/cat这样的文件名称来限制命令列表，多个命令文件之间用逗号（,）间隔。 |

# 复习题

✓ **1．在RHEL 8系统中，root管理员是谁?**

答：是UID为0的用户，是权限最大、限制最小的管理员。

✓ **2．如何使用Linux系统的命令行来添加和删除用户?**

答：添加和删除用户的命令分别是useradd与userdel。

✓ **3．若某个文件的所有者具有文件的读/写/执行权限，其余人仅有读权限，那么用数字法表示应该是什么?**

答：所有者权限为rwx，所属组和其他人的权限为r--，因此数字法表示应该是744。

✓ **4．某文件的字符权限为rwxrw-r--，那么对应的数字法权限应该是多少?**

答：数字法权限应该是764。

✓ **5．某链接文件的权限用数字法表示为755，那么相应的字符法表示是什么呢?**

答：在Linux系统中，不同文件具有不同的类型，因此这里应写成lrwxr-xr-x。

# 复习题

✓ **6．如果希望用户执行某命令时临时拥有该命令所有者的权限，应该设置什么特殊权限?**

答：特殊权限中的SUID。

✓ **7．若对文件设置了隐藏权限（+i参数），则意味着什么?**

答：无法对文件进行修改；若对目录设置了该参数，则仅能修改其中的子文件内容而不能新建或删除文件。

✓ **8．使用访问控制列表（ACL）来限制linuxprobe用户组，使得该组中的所有成员不得在/tmp目录中写入内容。**

答：想要设置用户组的ACL，则需要把u改成g，即setfacl -Rm g:linuxprobe:r-x /tmp。

✓ **9．当普通用户使用sudo命令时是否需要验证密码?**

答：系统在默认情况下需要验证当前登录用户的密码，若不想验证，可添加NOPASSWD参数。

祝同学们学习顺利，爱上Linux系统。