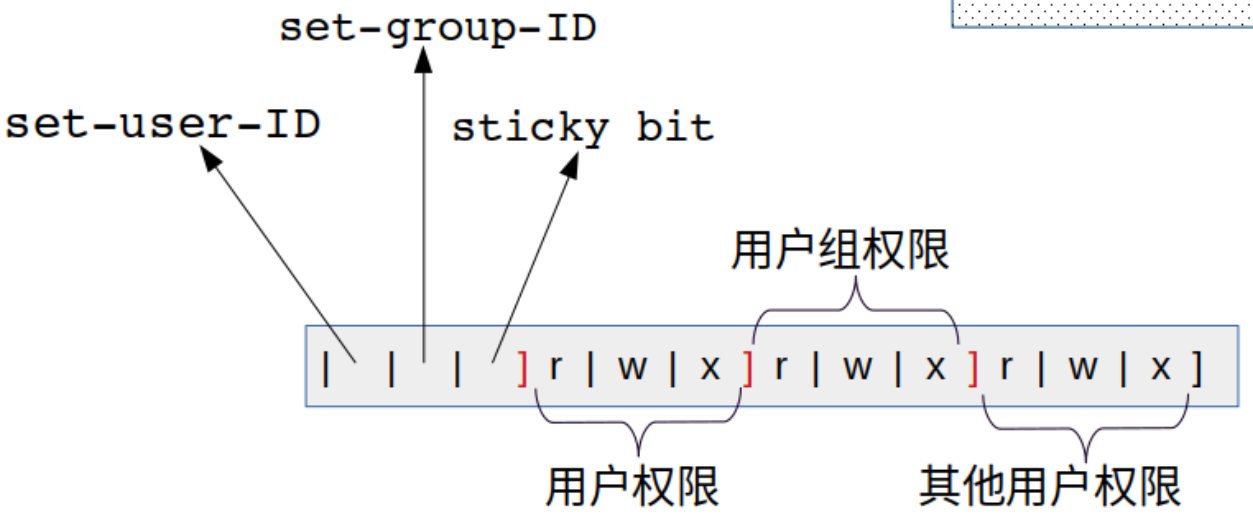
Linux 基础

第 11 讲 用户与权限更多细节

权限控制标志位

用于权限控制的 12 个标志位



除了开始的 3 个特殊标志位，
后面 3 个一组，从左到右分别表示可读，可写，可执行。

set-user-ID 标志位

- 它的出现是为了解决一个重要问题：用户如何修改自己的密码?

如何修改密码

- 修改密码的命令是 `passwd`。
- 保存用户密码的文件是 `/etc/shadow`。
- `passwd` 命令修改密码会涉及到修改 `/etc/shadow` 文件。
- 但是此文件只有 `root` 用户才可以修改。

解决方案

- 问题的解决不是给所有用户都具备 `/etc/shadow` 文件的写权限。
- 而是通过设置 `passwd` 命令所属用户为 `root`，并设置 `set-user-ID` 标志位。
- 这样其他用户在运行 `passwd` 时就好像是 `root` 在执行。

是否可以修改其他用户密码

- 除了 root 用户，其他用户使用 passwd 只能修改自己的密码。
- passwd 命令知道谁在运行程序，它通过系统调用 getuid 可以获取用户的 ID，只会修改对应用户 ID 的密码。

set-group-ID

- 类似的， set-group-ID 标志位表示，用户在运行程序时，就像是所属组的用户在执行。
- 相当于用户获取了所属组的权限。

sticky 位

- sticky 位对文件和目录有不同的作用，对于文件来说，主要是早期的 Unix 系统要在有限的内存中运行多个程序，会把暂时不需要的放到 swap 分区中，但是现在操作系统都使用虚拟内存。
- 对于目录来说， sticky 位可以允许所有用户都可以在目录下创建文件，但是只能删除自己的文件， Linux 内核中的 /tmp 目录作为临时文件存放目录就使用了 sticky 位。

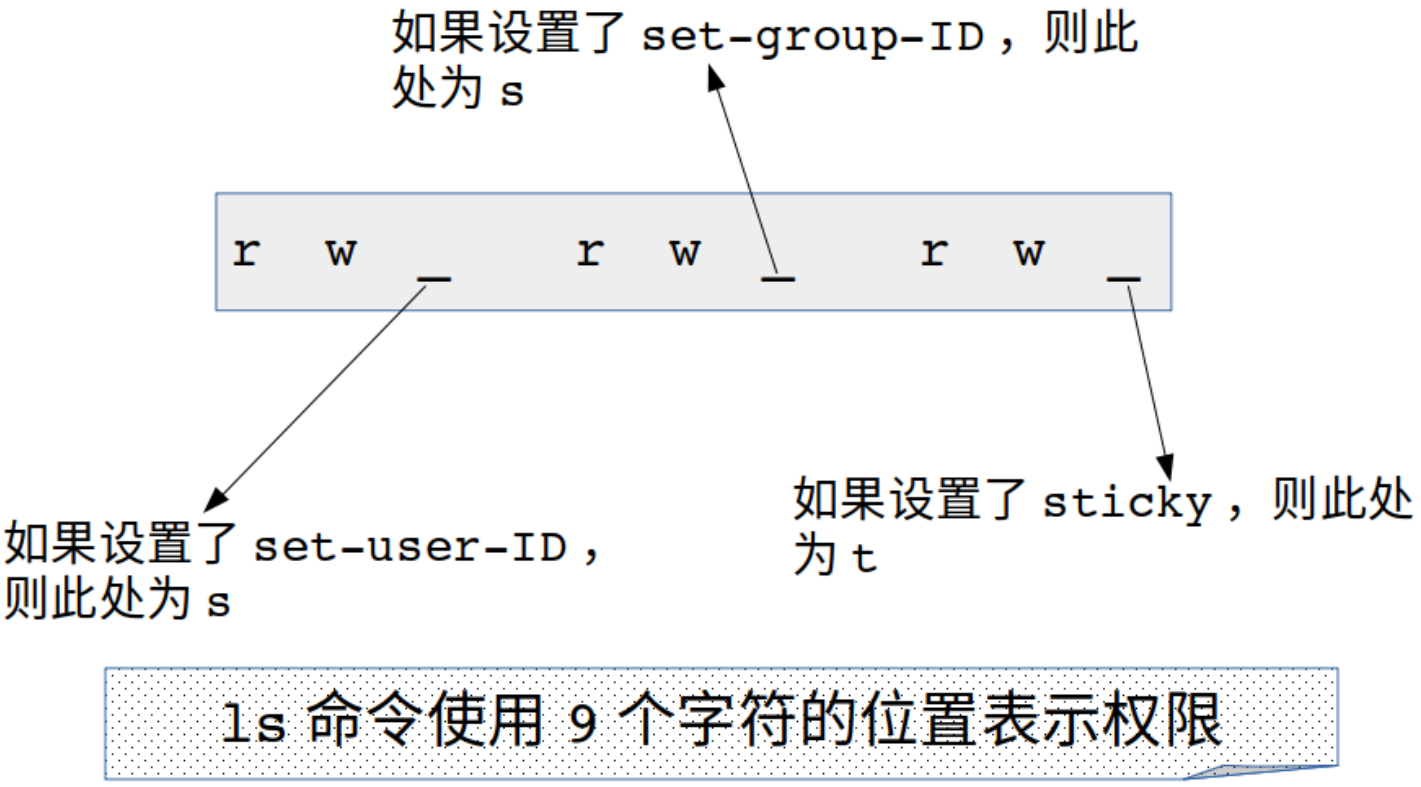
如何设置 sticky 位

- 使用命令 chmod：

  使用八进制数字： `chmod 1777 tmp/`

  使用字符： `chmod o+wt tmp/`
- 需要配合可写权限，否则其他用户也无法创建文件。

ls 命令是如何显示权限的



系统用户和普通用户

- 普通用户一般可以登录并会在登录后运行一个 `shell`。
- 系统用户往往不可登录，它们的存在是为了给程序一个身份去运行。
- 比如 `PostgreSQL` 数据库使用 `postgres` 用户运行，此用户需要安装数据库时创建。

创建系统用户组和系统用户

- 创建系统用户 servg:

```
sudo --system servg
```

- 创建系统用户 servtest：

```
sudo adduser servtest --system \
--disabled-login --disabled-password \
--no-create-home --ingroup servg
```

表示折行并继续，
此处是为了调整格式。

以指定用户的身份运行程序

- 以用户 servtest 的身份运行 rmdir：

```
sudo -u servtest rmdir tmp/ht
```


tmp/ht 不属于 servtest 用户

```
rmdir: 删除 'tmp/ht' 失败：权限不够
```

练习

- 创建系统用户组： brain。
- 创建系统用户 helloworld 属于组 brain。
- 使用用户 helloworld 的身份在当前位置创建目录 data，并在 data 中创建文件 list.log。
- 在 data 中创建 tmp 目录，给 tmp 设置 sticky 位允许其他用户在此目录创建文件。

* 文件访问控制列表

- 如果需要针对某一个或一些用户设置权限，这种细粒度的划分需要使用访问控制列表（ACL）实现。
- Linux 提供了两个命令： setfacl, getfacl

* 文件访问控制列表

- 设置用户 oklinux 对当前用户下的 tmp/images 目录具备写权限:

  ```
  setfacl -m u:oklinux:w tmp/images
  ```

- 查看访问控制列表:

  ```
  getfacl tmp/images
  ```

* 文件访问控制列表

- 移除 oklinux 用户的访问控制列表：

```
setfacl -x u:oklinux tmp/images
```