openEuler

用户和群组

课程介绍

- 用户和用户组管理是系统安全管理的重要组成部分，本章主要介绍openEuler提供的用户管理和组管理命令，以及为普通用户分配特权的方法。

- 学完本课程后，您将能够：能够在linux系统中创建用户、用户组及相关管理；设置文件的权限；掌握不同用户间切换

目录

CONTENT

openEuler

用户的基础概念

Linux是一个多用户的操作系统：

大家想象一下，我们是一个管理团队，共同维护一组服务器，难道每个人都能够被赋予管理员权限吗？显然是不行的，因为不是所有的数据都可以对每位管理员公开，而且如果在运维团队中有某位管理员对 Linux 不熟悉，那么赋予他管理员权限的后果可能是灾难性的。
因此，越是对安全性要求高的服务器，越需要建立合理的用户权限等级制度和服务器操作规范。
Linux 是多用户多任务操作系统，换句话说，Linux 系统支持多个用户在同一时间内登陆，不同用户可以执行不同的任务，并且互不影响。

例如，某台 Linux 服务器上有 4 个用户，分别是 root、www、ftp 和 mysql，在同一时间内，root 用户可能在查看系统日志、管理维护系统；www 用户可能在修改自己的网页程序；ftp 用户可能在上传软件到服务器；mysql 用户可能在执行自己的 SQL 查询，每个用户互不干扰，有条不紊地进行着自己的工作。与此同时，每个用户之间不能越权访问，比如 www 用户不能执行 mysql 用户的 SQL 查询操作，ftp 用户也不能修改 www 用户的网页程序。

用户：

用户是能够获取系统资源的权限的集合；

每个用户都会分配一个特有的id号-uid。

用户UID

UID指的是用户的ID（User ID），一个用户UID标示一个给定用户，UID是用户的唯一标示符，通过UID可以区分不同用户的类别（用户在登录系统时是通过UID来区分用户，而不是通过用户名来区分）：

超级用户

也称为root用户，它的**UID为0**，超级用户拥有系统的完全控制权，可以进行修改、删除文件等操作，也可以运行各种命令，所以在使用root用户时要十分谨慎；

普通用户

普通用户:也称为一般用户，它的**UID为1000-60000**之间，普通用户可以对自己目录下的文件进行访问和修改，也可以对经过授权的文件进行访问；

虚拟用户

虚拟用户：也称为系统用户，它的**UID为1-999**之间，虚拟用户最大的特点是不提供密码登录系统，它们的存在主要是为了方便系统的管理。

区分用户类别

通过查看不同用户UID来区分用户的类别为超级用户、普通用户或是虚拟用户。

查看UID命令：id [option] [user_name]。

相关参数：

```
-a          ignore, for compatibility with other versions
 -Z, --context  print only the security context of the process
 -g, --group    print only the effective group ID
 -G, --groups   print all group IDs
 -n, --name     print a name instead of a number, for -ugG
 -r, --real     print the real ID instead of the effective ID, with -ugG
 -u, --user     print only the effective user ID
 -z, --zero     delimit entries with NUL characters, not whitespace;
```

示例：

```
[root@localhost ~]# id -a
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

管理用户

在Linux系统中，每个普通用户都有一个账号，包括用户名、密码和主目录等信息。除此之外，还有一些系统本身创建的特殊用户，具有特殊的存在意义，其中最重要的用户就是管理员账户，默认的用户名为root（也就是超级用户）。通过操作命令行能够对用户文件进行创建、修改、删除更改密码等操作。

与用户账号信息有关的文件如下：

/etc/passwd：用户账号信息文件。
/etc/shadow：用户账号信息加密文件。
/etc/group：组信息文件。
/etc/default/useradd：定义默认设置文件。
/etc/login.defs：系统广义设置文件。
/etc/skel：默认的初始配置文件目录。

创建用户 - useradd

useradd命令可用来创建用户账号，并保存在/etc/passwd文件中。

语法：useradd [options] user_name。

其中的命令选项说明如下：

-u 指定用户UID

-o 配合“-u”属性，允许UID重复

-g 指明用户所属基本组，既可为用户组名，也可为GID（该组必须已存在）

-d 指定用户的home目录，并自动创建用户home目录

-s 指明用户的默认shell程序

-D 显示或更改默认配置

创建用户 - 示例

创建一个用户user：

命令为：useradd user

```
[root@localhost ~]# useradd user
```

执行完该命令后，没有任何提示，表明用户建立成功。这时并没有设置用户的口令，请使用passwd命令修改用户的密码，没有设置密码的新账号不能登录系统。

通过cat /etc/passwd命令查看是否创建成功，显示用户user已创建。

```
[root@localhost ~]# cat /etc/passwd

dbus:x:980:980:System Message Bus:/:/usr/sbin/nologin
test:x:1000:1000::/home/test:/bin/bash
test02:x:1001:1001::/home/test02:/bin/bash
user:x:1002:1004::/home/user:/bin/bash
```

修改用户 - usermod

usermod可用来修改用户账号的各类信息。

语法：usermod [options] user_name。

其中部分命令选项说明如下：

-u 修改用户UID

-g 修改用户所属用户组

-l 修改用户账号名称

-d 修改用户home目录

-s 修改用户默认shell程序

具体参数详细介绍可以使用 usermod --help或usermod -h查询

删除用户 - userdel

userdel用于删除指定的用户以及与该用户相关的文件。

语法：userdel [options] user_name。

其中的命令选项说明如下：

-f 强制删除用户账号，即使用户当前处于登录状态

-r 删除用户，同时删除与用户相关的所有文件

-h 显示命令的帮助信息

（userdel命令用于删除指定的用户以及用户相关的文件，实际上是对系统的用户账号文件进行了修改）

修改用户密码 - passwd

passwd用来修改用户的密码。

语法：passwd [OPTION...] user_name。

其中的命令选项说明如下：

-n 设置修改密码最短天数

-x 设置修改密码最长天数

-w 设置用户在密码过期前多少天收到警告信息

-i 设置密码过期多少天后禁用账户

-d 删除用户密码

-S 显示用户密码信息

（root用户可以修改任何用户的密码，普通用户只能修改自身的密码）

用户组的基础概念

用户组是具有相同特征用户的逻辑集合。简单的理解，有时我们需要让多个用户具有相同的权限，比如查看、修改某一个文件的权限，一种方法是分别对多个用户进行文件访问授权，如果有 10 个用户的话，就需要授权 10 次，那如果有 100、1000 甚至更多的用户呢?

显然，这种方法不太合理。最好的方式是建立一个组，让这个组具有查看、修改此文件的权限，然后将所有需要访问此文件的用户放入这个组中。那么，所有用户就具有了和组一样的权限，这就是用户组。

将用户分组是 Linux 系统中对用户进行管理及控制访问权限的一种手段，通过定义用户组，很多程序上简化了对用户的管理工作。

用户组特点:
具有相同特性用户的逻辑集合，通过组的形式使得具有相同特性的多个用户能够拥有相同的权限，便于管理;

每一个用户都拥有自己的私有组;

同一组内的所有用户可以共享该组下的文件;

每一个用户组都会被分配一个特有的id号-gid。

用户组GID

用户组ID（Group ID，简称为GID）和用户UID类似，作为唯一标识符来标示系统中的一个用户组：

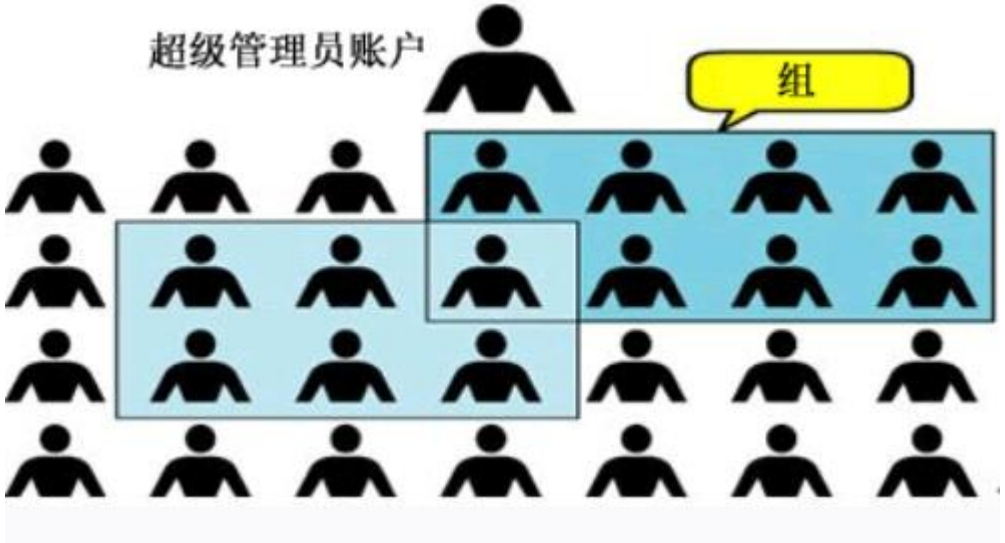
在添加账户时，默认情况下会同时建立一个与用户同名且UID和GID相同的组；

GID与UID都会将0赋予给超级用户或者具有超级用户的用户组（也就是root用户组）；

系统会预留一些较前的GID给虚拟用户（也称为系统用户）。

可以通过输入命令行id [option] [user_name]，查看用户组gid以及每个用户组下拥有的用户数量。

用户和用户组的关系



一对一：一个用户可以存在一个用户组中，作为组中的唯一成员；

一对多：一个用户可以存在多个用户组中，该用户具有多个组的共同权限；

多对一：多个用户可以存在一个用户组中，这些用户具有和组相同的权限；

多对多：多个用户可以存在多个用户组中，其实就是以上三种关系的扩展。

管理用户组

随着用户的不断增多，用户权限的把控变得复杂繁重，对系统的安全管理产生负面影响，用户组的加入，使得每一个用户至少属于一个用户组，从而便利了权限管理。

用户和用户组管理是系统安全管理的重要组成部分，通过操作命令行能够对用户组文件进行创建、修改、删除以及关联用户等操作.

创建组 - groupadd

groupadd可用来创建一个新的用户组，并将新用户组信息添加到系统文件中。

语法： groupadd [options] group_name

其中的命令选项说明如下：

-f 如果组已存在，则成功退出

-g 为新用户组所使用的GID

-h 显示此帮助信息并退出

-o 允许创建有重复 GID 的组

-p 为新用户组使用此加密过的密码

-r 创建一个系统账户

修改组 - groupmod

groupmod可用来更改群组识别码或者名称。

语法：groupmod [options] group_name

其中的命令选项说明如下：

-g 修改为要使用的GID

-h 显示此帮助信息并退出

-n 修改为要使用的组名称

-o 允许使用重复的 GID

-p 更改密码(加密过的)

删除组 - groupdel

Groupdel可用来删除用户组，但若是用户组中包含一些用户，需先删除掉用户后再

删除用户组：

语法：groupdel [options] group_name

其中的命令选项说明如下：

-f 即便是用户的主组也继续删除

-h 显示此帮助信息并退出

（groupdel命令用于从系统中删除组，需要注意的是，若是在组中仍然包括某些用户，此时需要先删除这些用户后，才能删除组）

关联用户和组 - gpasswd

gpasswd可以用来添加或删除用户到组中。

语法：gpasswd [option] group_name。

其中的命令选项说明如下：

-a 向组 GROUP 中添加用户 USER

-d 从组 GROUP 中添加或删除用户

-M 设置组 GROUP 的成员列表

-A 设置组的管理员列表

-r 移除组 GROUP 的密码

-R 向其成员限制访问组 GROUP

-Q 要 chroot 进的目录

OpenEuler中用户关联的文件

openEuler下涉及到管理用户信息的文件一般有以下两种：

- /etc/passwd：用户账号信息文件。

  在这个文件中，保存着系统中所有用户的主要信息，每一行代表着一个记录；

  每一行用户记录中定义了用户各个方面的相关属性。

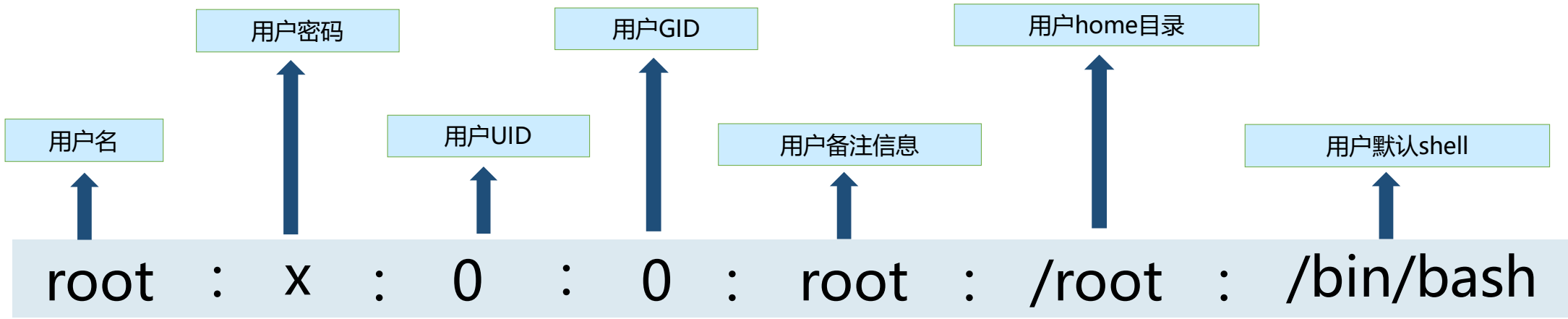
- /etc/shadow：用户账号信息加密文件（又称为“影子文件”）

  用于存储系统中用户的密码信息；

  由于/etc/passwd文件允许所有用户读取，容易导致密码泄露，因此将密码信息从该文件中分离出来，单独放置在/etc/shadow文件中。

/etc/passwd文件

/etc/passwd文件每一行由七个字段的数据组成，且字段之间用“:”隔开



Linux中的shell，是指一个面向用户的命令接口，表现形式为一个可以又用户登录的界面，Linux的shell有很多种sh, csh, ksh, tcsh, bash等

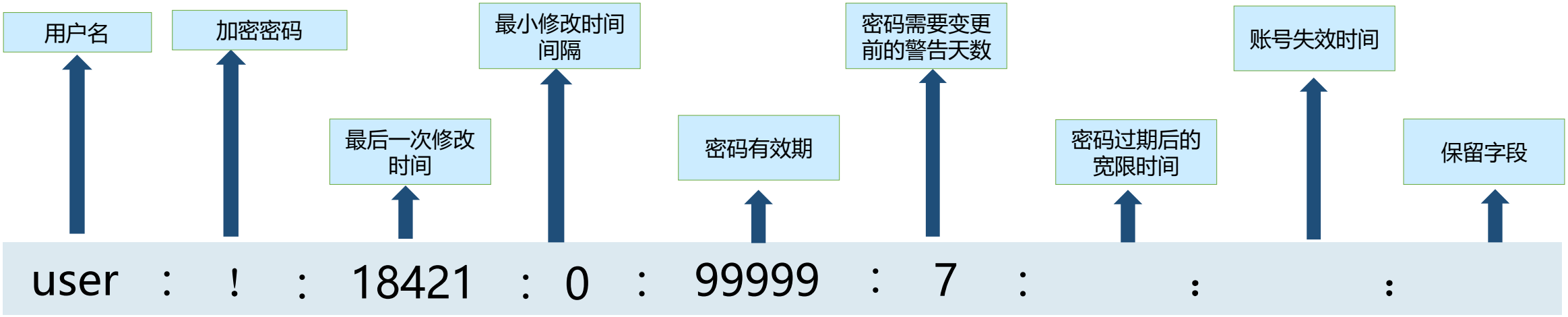
(shell是建立在内核的基础上，且面向于用户的一种表现形式)

/etc/shadow文件

/etc/shadow文件只有超级用户（root用户）具有读权限，其他用户均没有权限，从而保证了用户密码的安全性。

密码在经由/etc/shadow保护后，在/etc/passwd文件的用户记录中只会以“X”的形式呈现。

与/etc/passwd文件相似，每一行记录代表一个用户，且以“:”隔开，不同之处在于/etc/passwd中每行记录被分为九个字段。



openEuler中用户组关联的文件

openEuler下涉及到管理用户组信息的文件一般有以下两种：

- /etc/group：组信息文件。

  在这个文件中，保存着用户组的所有信息，每一行记录代表一个用户组；

  将用户分组是对用户进行管理及控制访问权限的一种手段，每个用户都属于一个用户组；一个组中可以有多个用户，一个用户也可以属于不同的组。

- /etc/gshadow：组信息加密文件。

  在这个文件中，会保存用户组加密信息，比如说用户组管理密码就保存在此（与/etc/shadow文件相似）；

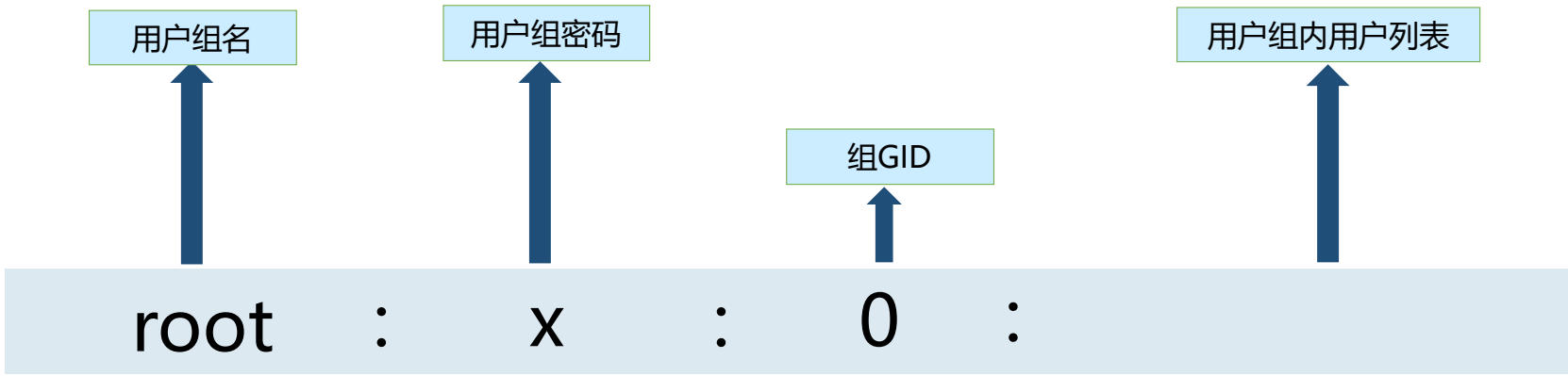
  与/etc/group文件互补，对于大型服务器来说，拥有很多用户和组，此时会针对这些用户和组来生成一些复杂的权限模型，此时设置并管理密码就显得尤为重要。

/etc/group文件

/etc/group文件每一行由四个字段的数据组成，且字段之间用“:”隔开。例如：

```
[root@localhost ~]# cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:sanlock
```

/etc/group文件中相关字段的意义：

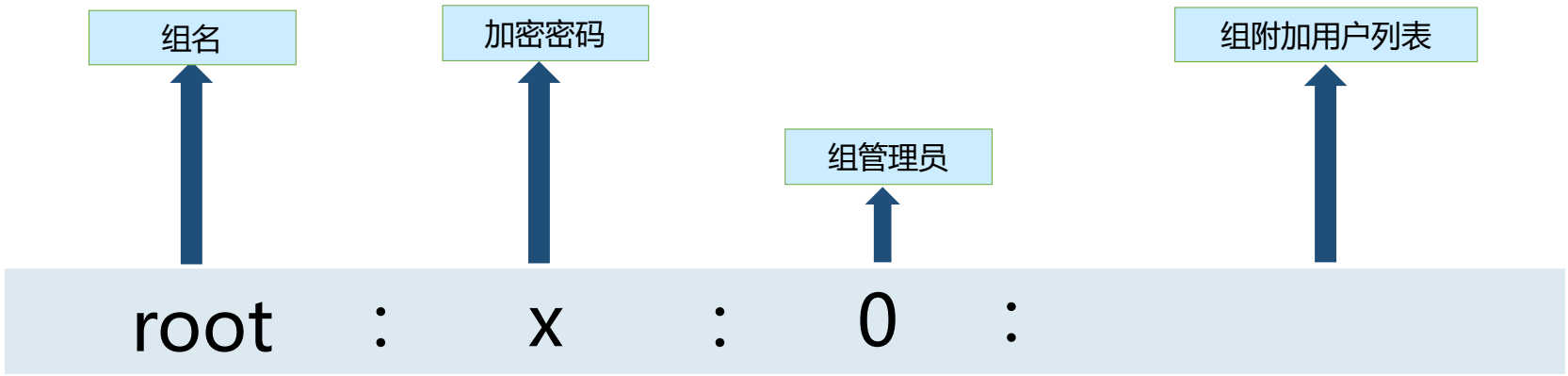


/etc/gshadow文件

/etc/gshadow文件每一行由四个字段的数据组成，且字段之间用“:”隔开。例如：

```
[root@localhost ~]# cat /etc/gshadow
root:::
bin:::
daemon:::
sys:::
adm:::
tty:::
disk:::sanlock
```

/etc/gshadow文件中相关字段的意义：



随堂测

- 1. 用户和用户组的关系,哪些是正确的？（多选题）

  A. 一对一
  B. 一对多
  C. 多对一
  D. 多对多

- 2. 以下哪一个命令可以创建新用户组？（单选题）

  A. groupadd
  B. groupmod
  C. Groupdel
  D. ls group

openEuler

目录

CONTENT

openEuler

权限概述

权限是操作系统用来限制对资源访问的一种机制，权限一般分为读、写、执行。

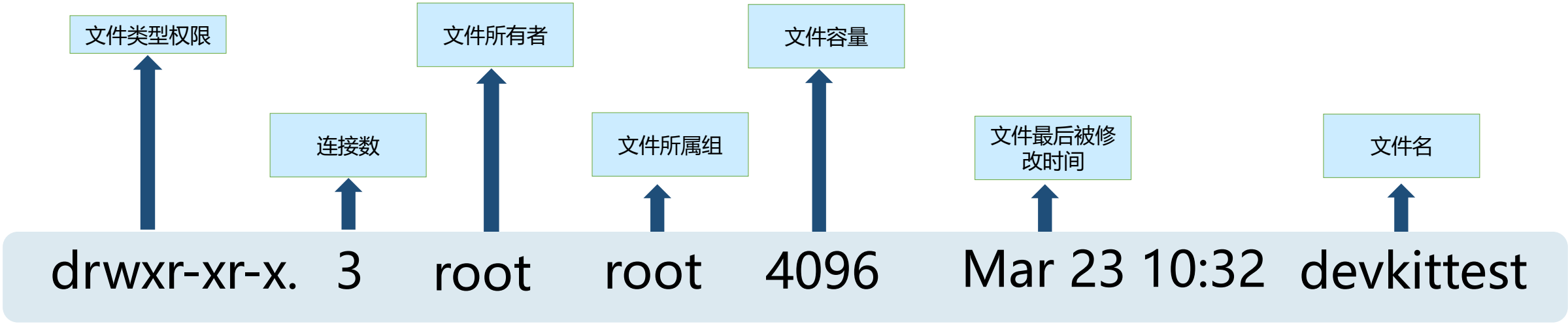
在Linux系统中，不同的用户所处的地位也不尽相同，不同地位的用户拥有不同的权限等级，为了保证系统的安全性，Linux系统针对不同用户的权限制定了不同的规则。

在Linux系统中，每个文件或目录都具有特定的访问权限、所属用户及所属组，通过这些规则可以限制什么用户、什么组可以对特定的文件执行什么样的操作。

权限示例

示例中通过ls –l命令可将文件权限的详细信息呈现出来，例如：

```
[root@localhost home]# ls -l
total 16
drwx------. 2 root root 16384 Jun  6 15:24 lost+found
```



权限位说明

在Linux中，每个文件或目录都有一组共有9个基础权限位，每三位字符分为一组，
它们分别是所属用户权限位，用户组权限位，其他用户权限位。最终形式"rw-r--r--"。

Linux正是通过这9个权限位来控制文件用户、用户组以及其他用户对文件的访问权限的。

位置	第123位	第456位	第789位
说明	所属用户的权限	所属用户组的权限	其他用户的权限

rwx权限的含义

位置	数字权限	权限含义
R(read)	4	读取权限
W(write)	2	写入权限
X(execut)	1	执行权限
-	0	没有权限

Linux系统中对文件和目录的权限含义区别：

位置	对文件的作用	对目录的作用
R(read)	具有读取。浏览文件内容权限	具有浏览目录及子目录权限
W(write)	具有修改，增加，删除文件内容权限	具有增加，删除或修改目录内文件的权限
X(execut)	具有执行文件权限	具有进入目录的权限

常用权限设置命令

- chmod命令：修改文件权限。

  Linux的文件调用权限分为三级：文件所有者、群组及其他，通过chmod命令可以控制文件被何人调用；
  使用权限：文件所有者。

- chown命令：修改文件属主属组（只允许管理员）。

  Linux做为多用户多任务系统，所有文件都有其所有者，通过chown可以将特定文件的所有者更改为指定用户或组；
  使用权限：管理员（root用户）。

- chgrp命令：修改文件属组。

  通过chgrp命令可以对文件或目录的所属群组进行更改；
  使用权限：管理员（root用户）。

- umask命令：遮罩码。

  通过umask命令可以指定在建立文件时进行权限掩码的预设；
  使用权限：管理员和普通用户。

修改文件权限 - chmod

chmod 更改文件或目录的权限

命令说明:

1.chmod 命令是用来改变文件或目录权限的命令
2.但是只有文件的属主和超级用户root才能够执行这个命令

命令格式:

chmod 支持两种修改权限的模式一种是字母表达，一种是数字表达

1）chmod [ugoa][-+=][rwx] 【文件或目录】

2）chmod |7|6|5|4|3|2|1| 【文件或目录】

用户位说明:
u 所属用户
g 所属组
o 其他用户
a 代表所有ugo

操作字符说明:
- 取消权限
+ 添加权限
= 取消所有的权限，赋予权限

根据配置场景，可以同时修改文件的一组权限，也可以只修改文件的某个权限。

修改文件权限chmod - 示例

同时修改测试文件usertxt的所有权限：

通过ls –l来查看为修改权限前测试文件usertxt的权限为；

```
[root@localhost ~]# ls –l
drwxr-xr-x.  2 root      root            4096 Apr 29 10:18 test1
```

使用chmod命令进行权限的修改：chmod 777 test1，再通过ls –l查看后发现权限已修改。

```
[root@localhost ~]# chmod 777 test1

[root@localhost ~]# ls –l
 drwxrwxrwx.  2 root      root            4096 Apr 29 10:18 test1
```

使用chmod命令进行权限的修改：chmod 777 test1，再通过ls –l查看后发现权限已修改。

```
[root@localhost ~]#  chmod a=r-- test1
[root@localhost ~]# ls –l
    dr--r--r--.  2 root      root            4096 Apr 29 10:18 test1
```

修改文件权限 - chown

利用chown可以将指定文件的所有者改为指定的用户或组。

语法：chown [OPTION]... [OWNER][:[GROUP]] FILE...

其中的命令选项说明如下：

-c：显示更改的部分的信息

-f：忽略错误信息

-h :修复符号链接

-v：显示详细的处理信息

-R：处理指定目录以及其子目录下的所有文件

根据配置场景，可以只修改属主，也可以只修改属组，亦可以同时修改属主属组。

修改文件权限chown - 示例

同时修改属主属组：

通过ls –l来查看为修改权限前测试文件usertxt的属主属组。

```
[root@localhost ~]# ls –l

drw-r--r--. 2 root    root       4096 Jun   8 11:10 usertxt
```

使用chown命令进行权限的修改： chown user: usergroup usertxt，再通过ls –l查看后发现权限已修改。

```
[root@localhost ~]# chown user:usergroup usertxt

[root@localhost ~]# ls -l
drw-r--r--. 2 user    usergroup    4096 Jun  8 11:10 usertxt
```

修改文件权限 - chgrp

chgrp可用来修改文件或目录的所属组。

语法：chgrp [OPTION]... GROUP FILE...

其中的命令选项说明如下：

-v：显示指令执行过程

-c：效果类似“-v”参数，但是只回报更改的部分

-f：不显示错误信息

-h：只修改符号连接的文件，而不对其他任何相关文件进行变动

-R：递归处理，即将指定目录下的所有文件及子目录一并处理

根据配置场景更改文件所属群组。

修改文件权限chgrp - 示例

更改文件所属组：

通过ls –l来查看为修改权限前测试文件usertxt的所属组。

```
[root@localhost ~]# ls –l
drw-r--r--. 2 user    usergroup  4096 Jun  8 11:10 usertxt
```

使用chgrp命令进行权限的修改： chgrp usergroup01 usertxt， 再通过ls –l查看后发现权限已修改。

```
[root@localhost ~]# chgrp usergroup01 usertxt
[root@localhost ~]# ls –l
drw-r--r--. 2 user    usergroup01  4096 Jun  8 11:10 usertxt
```

随堂测

1. 使用chmod命令修改test1文件权限：chmod 777 test1，修改后用户对文件权限是？（单选题）

   A. 可读

   B. 可写

   C. 可操作

   D. 可读可写可操作

2. 关于chgrp命令 的说法，哪个是正确的。（单选题）

   A. 控制文件被何人调用
   B. 可以对文件或目录的所属群组进行更改
   C. 将特定文件的所有者更改为指定用户或组
   D. 可以指定在建立文件时进行权限掩码的预设

目录

CONTENT

openEuler

其他管理权限

Linux中默认账户为普通用户，但是在更改系统文件或者执行某些命令时，都需要以root用户的权限才能进行，此时就需要将默认的普通用户更改为root用户。

在切换用户身份时，常常用到的命令有三种：

su：此命令在切换用户时，仅切换root用户身份，但shell环境仍为普通用户；

su –：此命令在切换用户时，用户身份和shell环境都会切换为root用户；

sudo：此命令可以允许普通用户执行管理员账户才能执行的命令。

命令 - su/su-

su可用来更改用户身份，但不会更改shell环境。

语法：su [options] [-] [<user> [<argument>...]]

其中的命令选项说明如下：

-m，-p：执行su时不会改变环境变量

-s：指定要执行的shell（bash csh tcsh 等）

-c：变更账号为USER的使用者并在执行完command后变为原使用者

-f：不需要读启动档，仅用于 csh 或 tcsh

etc...

命令 - sudo

sudo可允许普通用户执行root用户才能执行的任务。

语法：sudo –h | -K | -k | -V

其中的命令选项说明如下：

-h：显示版本号以及指令的使用说明

-k：使使用者在下次执行sudo时询问密码

-V：显示版本编号

-l：显示使用者的权限

-L：显示sudos设置

etc...

随堂测

1. 在openEuler中，默认情况下，以下哪个UID隶属于普通用户？（单选题）

   A. 0

   B. 300

   C. 900

   D. 1200

2. 以下哪一个命令可以用来查看用户和组相关联文件中的信息？（单选题）

   A. cat

   B. chmod

   C. clear

   D. chage

Thank you

openEuler