

第8章 Linux实操篇-用户管理

8.1 基本介绍

Linux系统作为一个多用户多任务的操作系统，允许多个用户同时使用系统资源，并执行多个任务。在这样的环境中，任何想要使用系统资源的用户，都必须先向系统管理员申请一个账号。通过这个账号，用户能够以特定的身份进入系统，从而被系统识别和管理，确保系统资源的合理分配与使用安全。

8.2 添加用户

8.2.1 基本语法

在Linux系统中，添加用户的基本指令为 `useradd 用户名`。该指令会按照系统默认设置，创建一个新用户。

8.2.2 应用案例

例如，要添加一个名为 `milan` 的用户，只需在终端输入 `useradd milan`。执行该指令后，系统会自动创建一个与用户名 `milan` 同名的用户，且默认该用户的家目录位于 `/home/milan`。

8.2.3 细节说明

- 家目录的自动创建：**当用户创建成功后，系统会自动创建一个与用户同名的家目录。家目录是用户在系统中存储个人文件和配置的地方，为用户提供了独立的工作空间。例如，`milan` 用户的家目录 `/home/milan`，只有 `milan` 用户及其所属组具有相应的访问权限。
- 指定家目录：**若要为新创建的用户指定特定的家目录，可以使用 `useradd -d 指定目录 新的用户名` 这一指令。例如，想要将新用户 `newuser` 的家目录指定为 `/data/newuser_home`，则在终端输入 `useradd -d /data/newuser_home newuser`。这种方式适用于有特殊存储需求或对用户目录结构有特定规划的场景。

8.3 指定 / 修改密码

8.3.1 基本语法

为用户指定或修改密码的基本语法是 `passwd 用户名`。通过该指令，系统会提示用户输入新密码，并进行相应的设置。

8.3.2 应用案例

若要给 `milan` 用户指定密码，在终端输入 `passwd milan`。系统会提示输入新密码，输入密码时，屏幕上不会显示输入的字符，以确保密码的安全性。输入完成后，系统会要求再次确认密码，确认无误后，密码设置成功。

另外，在操作过程中，若需要查看当前用户所在的目录，可以使用 `pwd` 指令。该指令会在终端输出当前用户的工作目录路径。例如，在为 `milan` 用户设置密码的过程中，若想确认当前所处的目录位置，输入 `pwd`，即可得知当前所在的目录。

8.4 删除用户

8.4.1 基本语法

删除用户的基本语法有两种：

- `userdel 用户名`：该指令用于删除指定的用户，但会保留用户的家目录。
- `userdel -r 用户名`：此指令不仅会删除用户，还会将用户的主目录及其所有内容一并删除。

8.4.2 应用案例

1. **保留家目录删除用户**：若要删除 `milan` 用户，但保留其家目录，在终端输入 `userdel milan`。执行该指令后，`milan` 用户将从系统中删除，但 `/home/milan` 目录及其内容将依然存在。
2. **删除用户及主目录**：例如，要删除用户 `tom` 及其主目录，在终端输入 `userdel -r tom`。系统会将 `tom` 用户的所有信息从系统中删除，并同时删除 `/home/tom` 目录及其包含的所有文件和子目录。

8.4.3 细节说明

关于是否保留家目录的讨论：一般情况下，建议保留用户的家目录。因为家目录中可能包含用户的重要数据和个人配置文件，保留家目录可以在需要时方便数据的恢复或后续的分析。例如，若用户在未来可能需要重新创建，或者需要从其原有的数据中获取某些信息，保留家目录就显得尤为重要。但在某些情况下，如用户数据不再有价值或需要彻底清理系统空间时，可以选择删除用户及其主目录。

8.5 查询用户信息指令

8.5.1 基本语法

查询用户信息的基本语法是 `id 用户名`。通过该指令，系统会返回指定用户的详细信息，包括用户标识号、组标识号、所属组等。

8.5.2 应用实例

例如，要查询 `root` 用户的信息，在终端输入 `#id root`。系统会输出类似如下的信息：`uid=0(root) gid=0(root) groups=0(root)`。其中，`uid` 表示用户标识号，`gid` 表示组标识号，`groups` 列出了该用户所属的组。

8.5.3 细节说明

当查询的用户不存在时，系统会返回“无此用户”的提示信息。这表明系统中没有找到与输入用户名匹配的用户记录，可能是由于用户名输入错误或该用户确实未在系统中创建。

8.6 切换用户

8.6.1 介绍

在操作 Linux 系统时，有时当前用户的权限可能不足以完成某些任务。此时，可以通过 `su -` 指令，切换到具有更高权限的用户，例如切换到 `root` 用户。`root` 用户拥有系统的最高权限，能够执行系统管理的各种操作。

8.6.2 基本语法

切换用户的基本语法为 `su - 切换用户名`。其中，`-` 选项的作用是切换用户的同时，将当前环境变量设置为目标用户的环境变量，包括工作目录、用户权限等。

8.6.3 应用实例

首先创建一个用户 `jack`，并为其指定密码。创建用户 `jack` 可使用 `useradd jack` 指令，然后使用 `passwd jack` 为其设置密码。完成后，若要从当前用户切换到 `jack` 用户，在终端输入 `su - jack`。此时，系统会提示输入 `jack` 用户的密码，输入正确后，即可成功切换到 `jack` 用户，终端的提示符也会相应改变，显示 `jack` 用户的相关信息。

8.6.4 细节说明

1. **权限切换与密码要求**：从权限高的用户切换到权限低的用户，不需要输入密码。例如，从 `root` 用户切换到普通用户 `jack`，在终端输入 `su - jack` 后，无需输入密码即可完成切换。反之，从权限低的用户切换到权限高的用户，则需要输入目标用户的密码。这是为了确保系统的安全性，防止未经授权的用户获取高权限。
2. **返回原用户**：当需要返回到原来的用户时，可以使用 `exit` 或 `logout` 指令。例如，在切换到 `jack` 用户后，若要回到之前的用户，在终端输入 `exit` 或 `logout`，即可退出 `jack` 用户的会话，返回原用户的环境。

8.7 查看当前用户 / 登录用户

8.7.1 基本语法

查看当前用户的基本语法有两种：`whoami` 和 `who am i`。这两种指令的功能相同，都用于在终端输出当前登录用户的用户名。

例如，在当前用户会话中，无论是普通用户还是 `root` 用户，输入 `whoami` 或 `who am i`，终端都会显示当前用户的用户名。这在需要确认当前操作身份的场景中非常有用，例如在执行某些敏感操作前，确认当前登录的用户是否具有相应的权限。

8.8 用户组

8.8.1 介绍

用户组类似于角色的概念，系统可以对具有共性或相同权限需求的多个用户进行统一的管理。通过将用户划分到不同的组，可以方便地对用户进行权限分配和管理。例如，将开发团队的所有成员划分到一个开发组，将运维团队的成员划分到运维组，然后为不同的组设置相应的权限，这样可以提高系统管理的效率和安全性。

8.8.2 新增组

新增组的指令为 `groupadd 组名`。在终端输入该指令，并指定要创建的组名，即可创建一个新的用户组。

例如，要创建一个名为 `developers` 的组，在终端输入 `groupadd developers`。执行该指令后，系统会创建一个名为 `developers` 的用户组，此时该组内没有任何成员。

8.8.3 删除组

删除组的基本语法是 `groupdel 组名`。在终端输入该指令，并指定要删除的组名，系统会删除指定的用户组。

例如，若要删除 `developers` 组，在终端输入 `groupdel developers`。需要注意的是，只有当组内没有用户时，才能成功删除该组。若组内还有用户，需要先将用户从组内移除，或者删除组内的用户，然后才能删除该组。

8.8.4 案例演示

1. **增加用户时直接指定组**：在创建用户时，可以直接将用户添加到指定的组中。使用的指令为 `useradd -g 用户组 用户名`。
2. **具体案例**：假设要创建一个用户 `zwj`，并将他直接指定到名为 `wudang` 的组中。首先，需要创建 `wudang` 组，使用 `groupadd wudang` 指令。然后，使用 `useradd -g wudang zwj` 指令创建用户 `zwj`，并将其添加到 `wudang` 组。这样，`zwj` 用户在创建的同时，就被添加到了 `wudang` 组中，拥有了该组的相关权限。

8.8.5 修改用户的组

修改用户所属组的基本语法是 `usermod -g 用户组 用户名`。通过该指令，可以将指定用户从原来的组移动到新的组中。

例如，先创建一个组 `mojiao`，使用 `groupadd mojiao`。然后，要将 `zwj` 用户放入到 `mojiao` 组中，在终端输入 `usermod -g mojiao zwj`。执行该指令后，`zwj` 用户将从原来的组（`wudang` 组）移动到 `mojiao` 组，其所属组的权限也相应发生改变。

8.9 用户和组相关文件

8.9.1 /etc/passwd 文件

`/etc/passwd` 文件是用户（user）的配置文件，用于记录用户的各种信息。该文件以文本形式存储，每行代表一个用户的信息，各字段之间用冒号（:）分隔。每行的含义如下：

1. **用户名**：用户在系统中登录时使用的名称，是用户的唯一标识。
2. **口令**：这里显示的并非真正的密码，而是经过加密处理后的密码信息。在现代 Linux 系统中，真正的密码通常存储在 `/etc/shadow` 文件中，该字段主要用于兼容旧系统。
3. **用户标识号（UID）**：系统用于识别用户的唯一数字标识。每个用户都有一个唯一的 UID，其中 `root` 用户的 UID 为 0，普通用户的 UID 从 1000 开始（具体起始值可能因系统配置而异）。
4. **组标识号（GID）**：用户所属的主要组的标识号。用户可以同时属于多个组，但这里记录的是其主要组的 GID。
5. **注释性描述**：通常用于记录用户的一些描述信息，如用户的姓名、部门等，可用于系统管理和识别。
6. **主目录**：用户的家目录路径，是用户在系统中存储个人文件和配置的主要位置。
7. **登录 Shell**：用户登录系统后默认使用的 Shell 程序。Shell 是用户与操作系统内核进行交互的接口，常见的有 `bash`、`sh` 等。

8.9.2 /etc/shadow 文件

`/etc/shadow` 文件是口令的配置文件，用于存储用户密码的加密信息以及密码相关的策略设置。同样以文本形式存储，每行代表一个用户的信息，各字段之间用冒号（:）分隔。每行的含义如下：

1. **登录名**：与 `/etc/passwd` 文件中的用户名相对应，是用户登录系统时使用的名称。
2. **加密口令**：用户密码经过加密算法处理后的密文。系统在用户登录时，会将用户输入的密码进行加密，并与该字段的密文进行比对，以验证用户身份。
3. **最后一次修改时间**：表示密码最后一次修改的时间，以从 1970 年 1 月 1 日 00:00:00 UTC 到密码修改时间的天数来表示。
4. **最小时间间隔**：两次密码修改之间的最小天数。若设置为 0，则表示密码可以随时修改。
5. **最大时间间隔**：密码必须修改的最大天数。超过这个天数后，用户将被要求修改密码，否则将无法登录。
6. **警告时间**：在密码过期前多少天开始向用户发出警告信息，提示用户密码即将过期。

7. **不活动时间**：密码过期后，用户账号被禁用之前的天数。在这段时间内，用户仍可登录并修改密码，但登录时会收到密码过期的提示。
8. **失效时间**：用户账号失效的时间，以从 1970 年 1 月 1 日 00:00:00 UTC 到失效时间的天数来表示。超过这个时间后，用户账号将被禁用，无法再登录系统。
9. **标志**：保留字段，目前未被广泛使用，可用于未来扩展系统功能。

8.9.3 /etc/group 文件

/etc/group 文件是组（group）的配置文件，用于记录 Linux 系统中包含的组的信息。以文本形式存储，每行代表一个组的信息，各字段之间用冒号（:）分隔。每行的含义如下：

1. **组名**：组的名称，是组的唯一标识。
2. **口令**：与用户密码类似，这里存储的是组密码的加密信息。组密码用于让用户临时加入该组，一般较少使用。
3. **组标识号 (GID)**：系统用于识别组的唯一数字标识。每个组都有一个唯一的 GID。
4. **组内用户列表**：以逗号分隔的组内用户列表，列出了属于该组的所有用户。若该组没有用户，则该字段为空。

2. 课后练习

一、选择题

1. 在 Linux 系统中，添加用户 lisa 并指定其家目录为 /data/lisa_home，以下指令正确的是（ ）
A. `useradd -d /data/lisa_home lisa`
B. `useradd lisa -d /data/lisa_home`
C. `useradd -m /data/lisa_home lisa`
D. `useradd -s /data/lisa_home lisa`

答案：A

解析：指定用户家目录的语法是 `useradd -d 指定目录 新的用户名`，A 选项符合该语法。B 选项参数顺序错误；C 选项中 `-m` 用于自动创建家目录（即便指定了不存在的目录），并非指定目录位置；D 选项中 `-s` 用于指定用户登录 shell，不是指定家目录。

2. 以下关于删除用户的说法，正确的是（ ）
A. `userdel -r tom` 指令只会删除 tom 用户，保留其家目录
B. 使用 `userdel jack` 删除用户后，jack 的家目录也会被删除
C. 当用户组内还有用户时，可以直接删除该用户组
D. `userdel` 指令删除用户时，若不使用 `-r` 选项，默认保留用户家目录

答案：D

解析：`userdel -r tom` 会删除 tom 用户及其家目录，A 错误；`userdel jack` 只会删除 jack 用户，保留其家目录，B 错误；当用户组内有用户时，不能直接删除该组，需先移除组内用户，C 错误；`userdel` 不使用 `-r` 选项，默认保留用户家目录，D 正确。

3. 从普通用户 user1 切换到 root 用户，以下操作正确的是（ ）
A. 直接在终端输入 `su root`，无需输入密码
B. 在终端输入 `su - root`，并输入 root 用户密码
C. 在终端输入 `su - user1`，并输入 root 用户密码
D. 在终端输入 `su root -`，无需输入密码

答案：B

解析：从普通用户切换到 root 用户，需使用 `su - root` 指令，且要输入 root 用户密码，B 正确。从权限低的用户切换到权限高的用户需输入密码，A 错误；C 选项 `su - user1` 是切换到 user1 用户，不是 root 用户；D 选项 `su root -` 语法错误。

4. 查看当前登录用户的用户名，可以使用以下哪个指令（）

- A. `whoami`
- B. `id`
- C. `passwd`
- D. `pwd`

答案：A

解析：`whoami` 用于查看当前登录用户的用户名，A 正确。`id` 用于查询指定用户信息，`passwd` 用于指定或修改密码，`pwd` 用于显示当前用户所在目录，B、C、D 错误。

二、简答题

1. 请简述在 Linux 系统中，

```
/etc/passwd
```

文件每行各字段的含义。

参考答案

```
/etc/passwd
```

文件每行代表一个用户信息，各字段含义如下：

- **用户名**：用户登录系统使用的名称，是唯一标识。
- **口令**：加密后的密码信息（现代 Linux 系统中真正密码存于 `/etc/shadow` 文件，此字段主要用于兼容旧系统）。
- **用户标识号 (UID)**：系统识别用户的唯一数字标识，`root` 用户 UID 为 0，普通用户 UID 从 1000 开始（具体起始值因系统配置而异）。
- **组标识号 (GID)**：用户所属主要组的标识号。
- **注释性描述**：记录用户描述信息，如姓名、部门等，用于系统管理和识别。
- **主目录**：用户家目录路径，用于存储个人文件和配置。
- **登录 Shell**：用户登录后默认使用的 Shell 程序，如 `bash`、`sh` 等。

2. 现有一个用户

```
user2
```

，需要将其从

```
group1
```

组移动到

```
group2
```

组，应如何操作？并说明操作过程中涉及的指令及作用。

参考答案

：操作步骤如下：

- 使用 `usermod -g group2 user2` 指令。其中，`usermod` 是用于修改用户账号属性的命令，`-g` 选项用于指定用户所属的组，`group2` 是目标组名，`user2` 是要修改组的用户名。执行该指令后，`user2` 用户将从 `group1` 组移动到 `group2` 组，其所属组的权限也相应改变。

三、实操题

1. 在 Linux 系统中进行以下用户和用户组的操作：

- 创建一个名为 `finance` 的用户组。
- 创建一个用户 `emma`，并将其添加到 `finance` 组，同时指定 `emma` 的家目录为 `/home/finance/emma`。
- 为 `emma` 用户设置密码为 `123456`（实际操作中请使用安全密码）。
- 查看 `emma` 用户的信息，包括 UID、GID 等。
- 从当前用户切换到 `emma` 用户，然后再切换回原用户。

参考答案思路：

- 在终端输入 `groupadd finance`，创建 `finance` 用户组。
- 输入 `useradd -d /home/finance/emma -g finance emma`，创建用户 `emma` 并指定家目录和所属组。
- 输入 `passwd emma`，按照提示输入密码 `123456` 两次，为 `emma` 设置密码。
- 输入 `id emma`，查看 `emma` 用户的信息，包括 UID、GID 等。
- 输入 `su - emma`，输入 `emma` 用户密码，切换到 `emma` 用户；在 `emma` 用户会话中输入 `exit`，切换回原用户。

2. 假设你在 Linux 系统中误操作将用户

```
john
```

删除，但希望保留其家目录中的重要数据。已知

```
john
```

用户的家目录为

```
/home/john
```

，请尝试恢复

```
john
```

用户，并确保其能正常访问原家目录中的数据。

参考答案思路

- 首先，使用 `useradd -d /home/john john` 指令创建 `john` 用户，并指定其家目录为原目录。
- 由于原 `john` 用户的密码信息可能已丢失，使用 `passwd john` 指令为新创建的 `john` 用户设置新密码。
- 检查 `/home/john` 目录的权限设置，确保新创建的 `john` 用户对该目录及其内部文件有合适的访问权限。若权限不正确，可使用 `chown -R john:john /home/john` 指令，将目录及其内容的所有者和所属组设置为 `john`，并根据需要使用 `chmod` 指令调整目录和文件的权限，以确保 `john` 用户能正常访问原家目录中的数据。