10. Linux实操篇-组管理和权限管理

10.1 Linux组基本介绍

在Linux系统中，每个用户都必须归属于一个组，无法独立于组外。同时，每个文件都涉及所有者、所在组以及其它组这三个概念。

1. **所有者**：通常指创建文件的用户，谁创建了该文件，谁就是文件的所有者。
2. **所在组**：当用户创建文件后，文件的所在组默认就是该用户所属的组。
3. **其它组**：除文件所有者和所在组的用户之外，系统中的其他用户都属于文件的其它组。
4. **改变用户所在的组**：用户所属的组可以在添加用户时指定，也可由root用户利用管理权限进行更改。

10.2 文件 / 目录所有者

10.2.1 查看文件的所有者

要查看文件的所有者，可使用`ls -ahl`指令。该指令会以长格式列出文件的详细信息，其中包含文件所有者的相关信息。

10.2.2 修改文件所有者

修改文件所有者的指令为`chown 用户名 文件名`。例如，若使用 root 用户创建了一个文件`apple.txt`，之后想要将其所有者修改为`tom`，则执行`chown tom apple.txt`即可。

10.3 组的创建

10.3.1 基本指令

创建组的基本指令是`groupadd 组名`。

10.3.2 应用实例

1. 若要创建一个名为`monster`的组，只需在终端输入`groupadd monster`。
2. 若要创建一个用户`fox`，并将其添加到`monster`组中，可使用`useradd -g monster fox`指令。

10.4 文件 / 目录所在组

10.4.1 查看文件 / 目录所在组

查看文件或目录所在组的基本指令同样是`ls -ahl`。通过该指令列出的文件信息中，可明确文件或目录所属的组。例如，使用`fox`用户创建一个文件后，通过`ls -ahl`指令查看该文件的详细信息，就能确定该文件属于`fox`用户所在的组。

10.4.2 修改文件 / 目录所在的组

1. **基本指令**：修改文件或目录所在组的指令为`chgrp 组名 文件名`。
2. **应用实例**：首先使用 root 用户创建文件`orange.txt`，查看该文件当前所属的组（默认为 root 组），然后创建一个名为`fruit`的组，即`groupadd fruit`。最后，使用`chgrp fruit orange.txt`指令将`orange.txt`文件的所在组修改为`fruit`组。

10.5 其它组

除文件的所有者和所在组的用户之外，系统中的其他用户都属于文件的其它组。这意味着对于一个文件，除了创建它的用户及其所属组的成员，其他所有用户都被归为其它组，他们对文件的访问权限由文件的权限设置决定。

10.6 改变用户所在组

10.6.1 改变用户所在组

改变用户所在组的指令为`usermod -g 新组名 用户名`。此外，`usermod -d 目录名 用户名`可用于改变该用户登录的初始目录，但需注意用户需要具备进入新目录的权限。

10.6.2 应用实例

若要将用户`zwj`从原来所在的组修改到`wudang`组，在终端输入`usermod -g wudang zwj`即可完成操作。

10.7 权限的基本介绍

通过`ls -l`指令列出的文件信息中，每个文件的权限信息以 10 个字符表示。例如，对于文件`-rwxrw-r-- 1 root root 1213 Feb 2 09:39 abc`，其各字符含义如下：

1. **第 0 位**：确定文件类型。`d`表示目录，类似于 Windows 的文件夹；`-`表示普通文件；`l`表示链接，相当于 Windows 的快捷方式；`c`表示字符设备文件，如鼠标、键盘；`b`表示块设备，如硬盘。
2. **第 1 - 3 位**：确定所有者（该文件的所有者）拥有该文件的权限，这一组权限称为`User`权限。
3. **第 4 - 6 位**：确定所属组（与用户同组的）拥有该文件的权限，这一组权限称为`Group`权限。
4. **第 7 - 9 位**：确定其他用户拥有该文件的权限，这一组权限称为`Other`权限。

10.8 rwx 权限详解，难点

10.8.1 rwx 作用到文件

1. **[r] 代表可读 (read)**：表示用户可以读取文件内容，进行查看操作。
2. **[w] 代表可写 (write)**：意味着用户可以修改文件内容，但需要注意的是，拥有对文件的写权限并不代表可以删除该文件。删除一个文件的前提条件是对该文件所在的目录拥有写权限。
3. **[x] 代表可执行 (execute)**：表示该文件可以被执行，前提是该文件具有可执行的格式和内容。

10.8.2 rwx 作用到目录

1. **[r] 代表可读 (read)**：用户可以使用`ls`命令读取目录内容，查看目录下包含的文件和子目录。
2. **[w] 代表可写 (write)**：用户可以对目录内的文件和子目录进行创建、删除以及重命名操作。
3. **[x] 代表可执行 (execute)**：用户可以使用`cd`命令进入该目录。

10.9 文件及目录权限实际案例

对于`ls -l`中显示文件信息`-rwxrw-r-- 1 root root 1213 Feb 2 09:39 abc`：

1. 权限解读
    - 第一个字符`-`表示这是一个普通文件。

- 其余字符每 3 个一组，分别代表不同用户的权限。第一组`rwx`表示文件拥有者的权限是读、写和执行；第二组`rw-`表示与文件拥有者同一组的用户的权限是读、写但不能执行；第三组`r--`表示不与文件拥有者同组的其他用户的权限是读，不能写和执行。

2. **权限数字表示**：在 Linux 中，权限可以用数字来表示，其中`r = 4`，`w = 2`，`x = 1`。因此，`rwx = 4 + 2 + 1 = 7`，不同的权限组合可以通过数字相加来表示。例如，上述文件权限`rwxrw-r--`用数字表示为`764`。

3. 其他信息
   - `1`表示文件的硬连接数（对于文件而言）或目录的子目录数（对于目录而言）。
   - `root`表示文件的所有者为 root 用户。
   - `root`表示文件的所在组为 root 组。
   - `1213`表示文件大小为 1213 字节，如果是文件夹，通常显示为 4096 字节。
   - `Feb 2 09:39`表示文件的最后修改日期。
   - `abc`为文件名。

10.10 修改权限 - chmod

10.10.1 基本说明

通过`chmod`指令，可以修改文件或者目录的权限。

10.10.2 第一种方式：+、-、= 变更权限

在这种方式中，使用`u`表示所有者，`g`表示所有组，`o`表示其他人，`a`表示所有人（即`u`、`g`、`o`的总和）。

1. **设置权限**：例如，`chmod u=rwx,g=rx,o=x 文件/目录名`，表示给文件的所有者赋予读、写、执行权限，给所在组赋予读、执行权限，给其他组赋予执行权限。
2. **增加权限**：`chmod o+w 文件/目录名`，表示给其他组增加写权限。
3. **去除权限**：`chmod a - x 文件/目录名`，表示去除所有人的执行权限。

10.10.3 第二种方式：通过数字变更权限

由于`r = 4`，`w = 2`，`x = 1`，所以`rwx = 4 + 2 + 1 = 7`。例如，`chmod u=rwx,g=rx,o=x 文件目录名`，相当于`chmod 751 文件/目录名`。

10.10.4 案例演示

1. 若要给`abc`文件的所有者赋予读写执行权限，给所在组赋予读执行权限，给其它组赋予读执行权限，可使用`chmod u=rwx,g=rx,o=rx abc`。
2. 若要给`abc`文件的所有者除去执行权限，增加组写权限，可使用`chmod u - x,g + w abc`。
3. 若要给`abc`文件的所有用户添加读权限，可使用`chmod a + r abc`。
4. 若要将`/home/abc.txt`文件的权限修改成`rwxr - xr - x`，使用数字方式则为`chmod 755 /home/abc.txt`。

10.11 修改文件所有者 - chown

10.11.1 基本介绍

1. **修改所有者**：`chown newowner 文件/目录`，用于改变文件或目录的所有者。
2. **同时修改所有者和所在组**：`chown newowner:newgroup 文件/目录`，可以同时改变文件或目录的所有者和所在组。
3. **递归修改**：当需要对目录及其下所有子文件或目录递归生效时，使用`-R`选项。例如，`chown -R newowner 目录名`，会将该目录及其下所有文件和子目录的所有者都修改为`newowner`。

10.11.2 案例演示

1. 若要将`/home/abc.txt`文件的所有者修改成`tom`，执行`chown tom /home/abc.txt`。
2. 若要将`/home/test`目录下所有的文件和目录的所有者都修改成`tom`，执行`chown -R tom /home/test`。

10.12 修改文件 / 目录所在组 - chgrp

10.12.1 基本介绍

`chgrp newgroup 文件/目录`用于改变文件或目录的所在组。

10.12.2 案例演示

1. 若要将`/home/abc.txt`文件的所在组修改成`shaolin`（少林），首先需要创建`shaolin`组，即`groupadd shaolin`，然后执行`chgrp shaolin /home/abc.txt`。
2. 若要将`/home/test`目录下所有的文件和目录的所在组都修改成`shaolin`（少林），执行`chgrp -R shaolin /home/test`。

10.13 最佳实践 - 警察和土匪游戏

10.13.1 游戏场景设定

在这个场景中，有`police`（警察）和`bandit`（土匪）两个阵营。其中，`jack`和`jerry`属于警察阵营，`xh`和`xq`属于土匪阵营。

10.13.2 操作步骤

1. **创建组**：使用`groupadd police`和`groupadd bandit`分别创建警察组和土匪组。
2. 创建用户并分组
   - 使用`useradd -g police jack`和`useradd -g police jerry`将`jack`和`jerry`添加到警察组。
   - 使用`useradd -g bandit xh`和`useradd -g bandit xq`将`xh`和`xq`添加到土匪组。
3. 文件权限设置
   - `jack`登录后创建一个文件`jack.txt`，并设置权限为自己可以读（`r`）写（`w`），本组人可以读（`r`），其它组没有任何权限，即`vim jack.txt`创建文件后，执行`chmod 640 jack.txt`。
   - `jack`修改该文件权限，使其它组人可以读，本组人可以读写，执行`chmod o=r,g=r jack.txt`。
4. 用户组变更及测试
   - `xh`投靠警察，使用`usermod -g police xh`将`xh`从土匪组变更到警察组。

- 测试 `xh` 和 `xq` 对 `jack.txt` 文件的读写权限。由此可以得出结论，如果要对目录内的文件进行操作，需要对该目录具有相应权限。

2. 课后练习

练习要求

1. **创建组**：建立两个组，分别为 `神仙(sx)` 和 `妖怪(yg)`。
2. 创建用户并分组
   - 建立四个用户，分别为 `唐僧`、`悟空`、`八戒`、`沙僧`。
   - 为每个用户设置密码。
   - 将 `悟空` 和 `八戒` 放入 `妖怪` 组，将 `唐僧` 和 `沙僧` 放入 `神仙` 组。
3. 文件操作及权限设置
   - 用 `悟空` 建立一个文件 `monkey.java`，并在文件中输出 `i am monkey`。
   - 给 `八戒` 对该文件赋予读（`r`）写（`w`）权限。
   - `八戒` 修改 `monkey.java`，加入一句话 `i am pig`。
   - 确保 `唐僧` 和 `沙僧` 对该文件没有权限。
4. 用户组变更及文件修改
   - 将 `沙僧` 放入 `妖怪` 组。
   - 让 `沙僧` 修改 `monkey.java` 文件，加入一句话 `我是沙僧，我是妖怪!`。
5. **文件夹权限测试**：深入讨论和测试文件夹 `rwx` 权限的细节，即 `x` 表示可以使用 `cd` 命令进入该目录；`r` 表示可以使用 `ls` 命令将目录的内容显示出来；`w` 表示可以在该目录中删除或者创建文件。

10.15 课堂练习 2

10.15.1 练习步骤

1. **创建用户**：用 root 用户登录，使用 `useradd mycentos` 创建用户 `mycentos`，并使用 `passwd mycentos` 为其设定密码。
2. 创建目录和文件
   - 用 `mycentos` 登录，在主目录下使用 `mkdir -p test/t11/t1` 创建多级目录 `test/t11/t1`。
   - 在 `t1` 目录中使用 `vim aa` 建立一个文本文件 `aa`，并编辑其内容为 `ls –al`。
3. 修改文件权限并执行
   - 使用 `chmod +x aa` 改变 `aa` 的权限为可执行文件。
   - 运行该文件 `./aa`，该文件会将当前目录下的文件列表信息输出。
4. 删除目录和用户
   - 使用 `rm -rf test/t11/t1` 删除新建立的目录 `test/t11/t1`。
   - 使用 `userdel -r mycentos` 删除用户 `mycentos` 及其主目录中的内容。
5. 系统设置
   - 将 Linux 系统设置成进入到图形界面的运行模式，在 CentOS 7 及之后的系统中，使用 `systemctl set - default graphical.target`。
   - 可以选择重新启动 Linux 系统，使用 `reboot` 命令；或者关机，使用 `shutdown -h now` 命令。

习题

一、选择题

1. 在Linux系统中，若要创建一个名为“developers”的组，应使用以下哪个命令？
   A. `useradd developers`
   B. `groupadd developers`
   C. `chown developers`
   D. `chgrp developers`
2. 现有文件`test.txt`，其所有者为`user1`，所在组为`group1`。若要将该文件的所有者变更为`user2`，应使用的命令是？
   A. `chgrp user2 test.txt`
   B. `usermod -g user2 test.txt`
   C. `chown user2 test.txt`
   D. `groupadd user2 test.txt`
3. 执行`ls -l`命令后，显示某文件权限为`-rwxr - xr - x`。用数字表示该文件权限应为？
   A. 744
   B. 755
   C. 644
   D. 655
4. 以下关于文件权限的说法，正确的是？
   A. 对文件有写权限就一定能删除该文件
   B. 目录的执行权限意味着可以查看目录中的内容
   C. 文件的所有者一定能删除该文件
   D. 对文件所在目录有写权限才能删除该文件
5. 若要给文件`file.txt`的所有用户（所有者、所属组、其他用户）添加执行权限，应使用以下哪个命令？
   A. `chmod a + x file.txt`
   B. `chmod u + x,g + x,o + x file.txt`
   C. `chmod a = x file.txt`
   D. `chmod u=x,g=x,o=x file.txt`
6. 某用户创建了一个文件，该文件的所在组是？
   A. 该用户的主要组
   B. root 组
   C. 其他用户组
   D. 随机分配的组
7. 执行`usermod -g newgroup user1`命令的作用是？
   A. 将`user1`用户的主目录变更为`newgroup`
   B. 将`user1`用户添加到`newgroup`组
   C. 将`user1`用户从`newgroup`组移除
   D. 将`newgroup`组的组名变更为`user1`
8. 若要递归修改`/home/dir`目录及其所有子文件和子目录的所有者为`admin`，应使用的命令是？
   A. `chown admin /home/dir`
   B. `chown -R admin /home/dir`
   C. `chgrp -R admin /home/dir`
   D. `usermod -R admin /home/dir`
9. 以下文件类型中，`ls -l`命令输出的第一个字符为`d`的是？
   A. 普通文件
   B. 目录
   C. 链接文件
   D. 字符设备文件

10. 对于文件`-rw - r - - r - -`，其所属组的权限是？
    A. 可读、可写
    B. 可读
    C. 可写
    D. 不可读、不可写、不可执行

二、简答题

1. 简述 Linux 系统中文件所有者、所在组和其他组的概念。
2. 说明 `chmod` 命令两种修改权限方式的区别，并各举一例。
3. 为什么有时对文件有写权限却无法删除该文件？要删除文件需要满足什么条件？
4. 当执行`ls -l`命令看到文件权限为`-rwxrw - r - -`时，分别说明文件所有者、所属组和其他用户对该文件的权限。
5. 如何创建一个新组，并将一个新用户添加到该组中，同时设置该用户的登录初始目录？请写出具体步骤。

三、实操题

1. 请完成以下操作：
    - 创建一个名为 “sales” 的组。
    - 创建一个名为 “emma” 的用户，并将其添加到 “sales” 组，同时设置其初始登录目录为`/home/sales/emma`。
    - 以 “emma” 用户身份登录，在其主目录下创建一个名为 “report.txt” 的文件，并写入内容 “First sales report”。
    - 将 “report.txt” 文件的所有者变更为 “admin” 用户（假设 “admin” 用户已存在）。
    - 查看 “report.txt” 文件的权限信息，确保其所有者为 “admin”，所在组为 “sales”。
2. 现有一个目录`/data/files`，里面包含多个文件和子目录。请按照以下要求进行操作：
    - 将该目录及其所有内容的所有者变更为 “user1”，所在组变更为 “group1”。
    - 给 “user1” 用户对该目录及其所有内容具有读、写、执行权限；给 “group1” 组内成员对该目录及其所有内容具有读、执行权限；给其他用户对该目录及其所有内容仅具有读权限。
    - 创建一个新用户 “user2”，并将其添加到 “group1” 组。
    - 以 “user2” 用户身份登录，尝试进入`/data/files`目录，查看目录内容，并在该目录下创建一个新文件 “newfile.txt”。分析操作过程中可能出现的问题及原因，并给出解决方法。