RHCSA 系列（三）：如何管理 RHEL7 的用户和组

2015-9-10 10:56 收藏: 11

原文：http://www.tecmint.com/rhcsa-exam-manage-users-and-groups/ 作者： Gabriel Cánepa
译文：LCTT https://linux.cn/article-6187-1.html 译者： xiqingongzi

和管理其它Linux服务器一样，管理一个 RHEL 7 服务器要求你能够添加、修改、暂停或删除用户帐户，并且授予他们执行其分配的任务所需的文件、目录、其它系统资源所必要的权限。

RHCSA: 用户和组管理 – Part 3

管理用户帐户

如果想要给RHEL 7 服务器添加账户，你需要以root用户执行如下两条命令之一：

```
# adduser [new_account]
# useradd [new_account]
```

当添加新的用户帐户时，默认会执行下列操作。

- 它/她的主目录就会被创建(一般是"/home/用户名"，除非你特别设置)
- 一些隐藏文件 如 `.bash_logout`，`.bash_profile` 以及 `.bashrc` 会被复制到用户的主目录，它们会为用户的回话提供环境变量。你可以进一步查看它们的相关细节。
- 会为您的账号添加一个邮件池目录。
- 会创建一个和用户名同样的组（LCTT 译注：除非你给新创建的用户指定了组）。

用户帐户的全部信息被保存在 `/etc/passwd` 文件。这个文件以如下格式保存了每一个系统帐户的所有信息(字段以":"分割)

```
[username]:[x]:[UID]:[GID]:[Comment]:[Home directory]:[Default shell]
```

- `[username]` 和 `[Comment]` 其意自明，就是用户名和备注
- 第二个'x'表示帐户的启用了密码保护(记录在 `/etc/shadow` 文件)，密码用于登录 `[username]`
- `[UID]` 和 `[GID]` 是整数，它们表明了 `[username]` 的用户ID 和所属的主组ID

最后。

- `[Home directory]` 显示 `[username]` 的主目录的绝对路径
- `[Default shell]` 是当用户登录系统后使用的默认shell

另外一个你必须要熟悉的重要的文件是存储组信息的 `/etc/group` 。和 `/etc/passwd` 类似，也是每行一个记录，字段由":"分割

```
[Group name]:[Group password]:[GID]:[Group members]
```

- `[Group name]` 是组名
- 这个组是否使用了密码 (如果是"x"意味着没有)
- `[GID]` : 和 `/etc/passwd` 中一样
- `[Group members]` :用户列表，使用","隔开。里面包含组内的所有用户

添加过帐户后，任何时候你都可以通过 usermod 命令来修改用户账户信息，基本的语法如下:

```
# usermod [options] [username]
```

相关阅读

- **15 'useradd' 命令示例 <http://www.tecmint.com/add-users-in-linux/>**
- **15 'usermod' 命令示例 <http://www.tecmint.com/usermod-command-examples/>**

示例1：设置帐户的过期时间

如果你的公司有一些短期使用的帐户或者你要在有限时间内授予访问，你可以使用 `--expiredate` 参数 ，后加YYYY-MM-DD 格式的日期。为了查看是否生效，你可以使用如下命令查看

```
# chage -l [username]
```

帐户更新前后的变动如下图所示

修改用户信息

示例 2: 向组内追加用户

除了创建用户时的主用户组，一个用户还能被添加到别的组。你需要使用 -aG或 -append -group 选项，后跟逗号分隔的组名。

示例 3: 修改用户主目录或默认Shell

如果因为一些原因，你需要修改默认的用户主目录(一般为 /home/用户名)，你需要使用 -d 或 -home 参数，后跟绝对路径来修改主目录。

如果有用户想要使用其它的shell来取代默认的bash(比如zsh)。使用 usermod ，并使用 -shell 的参数，后加新的shell的路径。

示例 4: 展示组内的用户

当把用户添加到组中后，你可以使用如下命令验证属于哪一个组

```
# groups [username]
# id [username]
```

下面图片的演示了示例2到示例4

添加用户到额外的组

在上面的示例中:

```
# usermod --append --groups gacanepa,users --home /tmp --shell /bin/sh tecmint
```

如果想要从组内删除用户，取消 `--append` 选项，并使用 `--groups` 和你要用户属于的组的列表。

示例 5: 通过锁定密码来停用帐户

如果想要关闭帐户，你可以使用 -l(小写的L)或 -lock 选项来锁定用户的密码。这将会阻止用户登录。

示例 6: 解锁密码

当你想要重新启用帐户让它可以继续登录时，使用 -u 或 –unlock 选项来解锁用户的密码，就像示例5 介绍的那样

```
# usermod --unlock tecmint
```

下面的图片展示了示例5和示例6：

锁定上锁用户

示例 7:删除组和用户

如果要删除一个组，你需要使用 groupdel ，如果需要删除用户 你需要使用 userdel (添加 -r 可以删除主目录和邮件池的内容)。

```
# groupdel [group_name]          # 删除组
# userdel -r [user_name]         # 删除用户，并删除主目录和邮件池
```

如果一些文件属于该组，删除组时它们不会也被删除。但是组拥有者的名字将会被设置为删除掉的组的GID。

列举，设置，并且修改标准 ugo/rwx 权限

著名的 **ls 命令 <http://linux.cn/article-5349-1.html>** 是管理员最好的助手. 当我们使用 -l 参数, 这个工具允许您以长格式（或详细格式)查看一个目录中的内容。

而且，该命令还可以用于单个文件中。无论哪种方式，在“ls”输出中的前10个字符表示每个文件的属性。

这10个字符序列的第一个字符用于表示文件类型：

- – (连字符): 一个标准文件
- d: 一个目录
- l: 一个符号链接
- c: 字符设备（将数据作为字节流，例如终端）
- b: 块设备（以块的方式处理数据，例如存储设备）

文件属性的接下来的九个字符，分为三个组，被称为文件模式，并注明读（r）、写（w）、和执行（x）权限授予文件的所有者、文件的所有组、和其它的用户（通常被称为“世界”）。

同文件上的读取权限允许文件被打开和读取一样，如果目录同时有执行权限时，就允许其目录内容被列出。此外，如果一个文件有执行权限，就允许它作为一个程序运行。

文件权限是通过chmod命令改变的，它的基本语法如下：

```
# chmod [new_mode] file
```

new_mode 是一个八进制数或表达式，用于指定新的权限。随意试试各种权限看看是什么效果。或者您已经有了一个更好的方式来设置文件的权限，你也可以用你自己的方式自由地试试。

八进制数可以基于二进制等价计算，可以从所需的文件权限的文件的所有者、所有组、和世界组合成。每种权限都等于2的幂（R = 2^2，W = 2^1，x = 2^0），没有时即为0。例如：

文件权限

在八进制形式下设置文件的权限，如上图所示

```
# chmod 744 myfile
```

请用马上来对比一下我们以前的计算，在更改文件的权限后，我们的实际输出为：

长列表格式

示例 8: 寻找777权限的文件

出于安全考虑，你应该确保在正常情况下，尽可能避免777权限（任何人可读、可写、可执行的文件）。虽然我们会在以后的教程中教你如何更有效地找到您的系统的具有特定权限的全部文件，你现在仍可以组合使用ls 和 grep来获取这种信息。

在下面的例子，我们会寻找 /etc 目录下的777权限文件。注意，我们要使用第二章：文件和目录管理 <https://www.linux.cn/article-6155-1.html> 中讲到的管道的知识：

```
# ls -l /etc | grep rwxrwxrwx
```

查找所有777权限的文件

示例 9: 为所有用户指定特定权限

shell脚本，以及一些二进制文件，所有用户都应该有权访问（不只是其相应的所有者和组），应该有相应的执行权限（我们会讨论特殊情况下的问题）：

```
# chmod a+x script.sh
```

注意: 我们可以使用表达式设置文件模式，表示用户权限的字母如“u”，组所有者权限的字母“g”，其余的为“o” ，同时具有所有权限为“a”。权限可以通过 `+` 或 `-` 来授予和收回。

为文件设置执行权限

长目录列表还用两列显示了该文件的所有者和所有组。此功能可作为系统中文件的第一级访问控制方法：

检查文件的所有者和所有组

改变文件的所有者，您应该使用chown命令。请注意，您可以在同时或分别更改文件的所有组：

```
# chown user:group file
```

你可以更改用户或组，或在同时更改两个属性，但是不要忘记冒号区分，如果你想要更新其它属性，让另外的部分为空：

```
# chown :group file             # 仅改变所有组
# chown user: file              # 仅改变所有者
```

示例 10:从一个文件复制权限到另一个文件

如果你想“克隆”一个文件的所有权到另一个，你可以这样做，使用–reference参数，如下：

```
# chown --reference=ref_file file
```

ref_file的所有信息会复制给 file

复制文件属主信息

设置 SETGID 协作目录

假如你需要授予在一个特定的目录中拥有访问所有的文件的权限给一个特定的用户组，你有可能需要使用给目录设置setgid的方法。当setgid设置后，该眞实用户的有效GID会变成属主的GID。

因此，任何访问该文件的用户会被授予该文件的属组的权限。此外，当setgid设置在一个目录中，新创建的文件继承组该目录的组，而且新创建的子目录也将继承父目录的setgid权限。

```
# chmod g+s [filename]
```

要以八进制形式设置 setgid，需要在基本权限前缀以2。

```
# chmod 2755 [directory]
```

总结

扎实的用户和组管理知识，以及标准和特殊的 Linux权限管理，通过实践，可以帮你快速解决 RHEL 7 服务器的文件权限问题。

我向你保证，当你按照本文所概述的步骤和使用系统文档(在本系列的第一章 回顾基础命令及系统文档 <http://www.tecmint.com/rhcsa-exam-reviewing-essential-commands-system-documentation/> 中讲到)，你将掌握基本的系统管理的能力。

请随时使用下面的评论框让我们知道你是否有任何问题或意见。

---

via: http://www.tecmint.com/rhcsa-exam-manage-users-and-groups/ <http://www.tecmint.com/rhcsa-exam-manage-users-and-groups/>

作者：Gabriel Cánepa <http://www.tecmint.com/author/gacanepa/> 译者：xiqingongzi <https://github.com/xiqingongzi> 校对：wxy <https://github.com/wxy>

本文由 LCTT <https://github.com/LCTT/TranslateProject> 原创翻译，Linux中国 <file:///root/github/my-notes/Manual/Linux.cn/RHCSA/RHCSA%E7%B3%BB%E5%88%973%E5%A6%82%E4%BD%95%E7%AE%A1%E7%90%86%20RHEL7%20%E7%9A%84%E7%94%A8%E6%88%B7%E5%92%8C.html> 荣誉推出

> 原文：http://www.tecmint.com/rhcsa-exam-manage-users-and-groups/ <http://www.tecmint.com/rhcsa-exam-manage-users-and-groups/>
>
> 作者： Gabriel Cánepa
>
> 译文：LCTT <http://lctt.github.io/> https://linux.cn/article-6187-1.html <https://linux.cn/article-6187-1.html> 译者： xiqingongzi

体验环境

本文导航

相关阅读

RHCSA

- RHCSA 系列（四）：编辑文本文件及分析文本 2015-9-16
- RHCSA 系列（七）：使用 ACL（访问控制列表）和挂载 Samba/NFS 共享 2015-9-22
- RHCSA 系列（八）：加固 SSH，设定主机名及启用网络服务 2015-9-23
- RHCSA 系列（九）：安装、配置及加固一个 Web 和 FTP 服务器 2015-9-24
- RHCSA 系列（十）：Yum 包管理、Cron 自动任务计划和监控系统日志 2015-9-26
- RHCSA 系列（十一）：使用 firewalld 和 iptables 来控制网络流量 2015-9-29