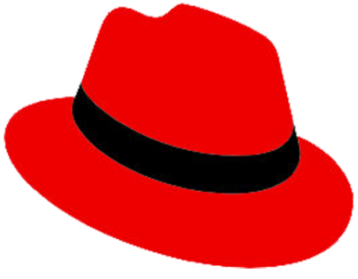
Red Hat

RH124 红帽系统管理 I

RH124-05-管理本地Linux用户和组



Red Hat

一、用户和组

什么是用户？

系统中的每个进程（运行进程）都作为一个**特定用户**运行。每个文件归一个特定用户所有。对文件和目录的访问受到用户的限制。与运行进程相关的用户可确定该进程可访问的文件和目录。

命令：**id**

该命令用于显示有关当前已登录用户的信息。也可以通过在用户名中传递作为id的首个参数来请求有关其他用户的基本信息。

命令：**ls -l**

查看某一文件或目录相关联的用户。第三列显示用户名。

查看进程信息

- 要查看进程可使用命令**ps -aux**
- 默认为仅显示当前shell中的进程

选项：

- a：查看与某一终端相关的所有进程
- u：查看与进程相关的用户

/etc/passwd文件

默认情况下，系统使用简单的“平面文件”**/etc/passwd**文件存储有关本地用户的信息。

[root@desktop ~]grep tom /etc/passwd

tom:x:501:501::/home/tom:/bin/bash

账户名：密码：UID：GID：描述：家目录：所使用的shell

passwd文件详细

- username：是UID到名称的一种映射，便于用户使用
- password：以前是以加密格式保存密码的位置。现在密码存储在/etc/shadow中
- UID：用户ID，标识用户的编号
- GID：用户的主要组ID编号
- GECOS：可以是任意文本，通常包含用户的实际名字
- /home/dir：用户的个人数据和配置文件的位置
- shell：用户登录时运行的程序。

什么是组？

与用户一样，组也有名称和编号（GID）。本地组在/**etc/group**中定义

主要组：

- 每个用户都有且只有一个主要组
- 对于本地用户，主要组通过/etc/passwd第三个字段的GID定义
- 通常，用户创建的新文件归主要组所有。
- 通常，新建用户的主要组名称与用户名相同。用户是此用户专用组（UPG）的唯一成员。

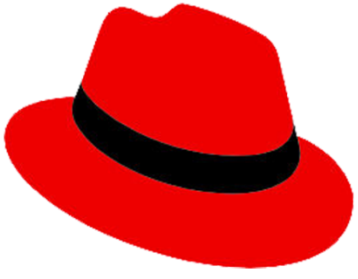
补充组（附加组）：

- 用户可以是0个或多个补充组的成员
- 属于本地补充组成员的用户列在/etc/group中组条目的最后一个字段

组文件

/etc/group中的每一行代表一个组，用：隔开不同项

- group_name：组名
- password：组密码（一般不用）
- GID ：组身份编号
- user_list：组成员列表



Red Hat

二、获得超级用户访问权限

root用户

- root用户是具有系统全部权限的用户，要执行诸如安装或删除软件以及管理系统文件和目录等任务，必须将特权升级到root用户
- 建议管理员在以普通用户登陆，仅在需要时升级到root用户特权

su

su命令可以让用户切换至另一个用户账户。如果未指定账户名，则意味着使用root账户。当作为普通用户调用时，系统将提示输入要切换到的账户的密码。作为root用户调用时，则无需输入账户密码。

命令：su [-] username

- su　username：会启动non-login shell
- su – username：自动login shell

区别：

su – 会将shell环境设置为如同以该用户身份完全登陆一样，而su仅以该用户身份使用当前的环境设置启动shell

使用sudo提升权限

sudo命令可以使用户根据**/etc/sudoers**文件中的设置，而被允许以root或其他用户身份运行命令。与su之类的工具不同，sudo要求输入其**自己的密码**以进行身份验证，这样可让管理员将细微的权限交给用户来委派系统管理任务，而无需交出root密码。

用法：

sudo 授权命令

密码验证：

初次执行sudo命令时，验证当前用户密码。

不需要验证目标用户的密码。

配置sudo授权：

visudo或者vim /etc/sudoers

/etc/sudoers

格式：

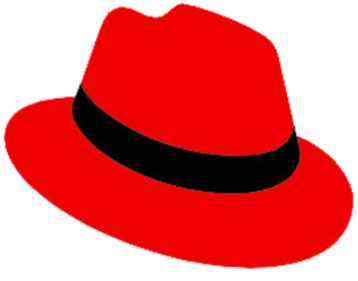
用户　主机名=（运行身份）　命令程序列表

实例：

david　ALL=（root）　/sbin/useradd

注：默认切换到root用户，默认需要验证密码

上述命令表示，david默认可以在任何主机中使用root用户执行useradd命令。



Red Hat

三、管理本地用户账户

useradd

命令：**useradd**

- 不带选项运行，useradd username 会为/etc/passwd中的所有字段设置合理的默认值，默认情况下，useradd不设置任何有效密码，**用户也必须要设定密码后才能登陆**
- 一些默认值从**/etc/login.defs**文件中读取。

useradd-常用选项

- -u：指定用户UID
- -e：设置用户失效时间
- -d：指定家目录
- -g：创建用户时候指定基本组
- -G：创建用户时候指定附加组
- -s ： 为用户指定登录的shell

usermod（修改用户的属性）

命令：usermod

参数：

- -g，--gid：为用户指定主要组
- -G，--groups：为用户指定一组补充组
- -a，--append：与-G选项搭配使用（-aG），将用户附加到所给的补充组，而不将该用户从其他组删除
- -d，--home：为用户指定新的主目录
- -m，--move：将用户主目录移动到新的位置。必须与-d搭配使用
- -s，--shell：为用户账户指定新的登陆shell
- -L，--lock：锁定用户账户
- -U，--unlock：解锁用户账户

usermod变更组成员资格

实例：

- usermod **–g** student student
  更改用户的主要组
- usermod **–aG** wheel elvis
  elvis将用户添加到补充组

userdel

命令：userdel

userdel username：可将用户从/etc/passwd中删除，但默认情况下保留主目录不变

userdel –r username：同时删除用户和其主目录

实例：

useradd prince
userdel prince //ls –l /home查看
useradd bob
userdel –r bob //ls –l /home查看

id和passwd

命令：id

- id：将显示用户信息，包括用户的UID编号和组成员资格
- id username：显示username的用户信息，包括用户的UID编号和组成员资格

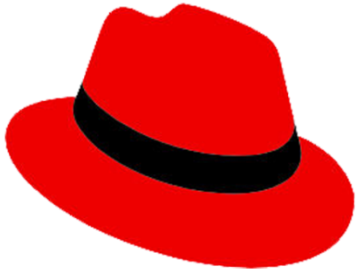
命令：passwd

- passwd username：设置用户的初始密码或更改用户密码
- root用户可以将密码设置为任何值。如果密码不符合最低建议标准，系统显示消息；不过之后会提示要求重新键入新密码，所有令牌也会成功更新

UID范围

特定的UID编号和编号范围供红帽Linux用于特殊目的

- UID 0：始终分配至超级用户root
- UID 1-200：是一系列“系统用户”，静态分配给红帽的系统进程
- UID 201-999：是一系列“系统用户”，供文件系统中没有自己的文件的系统进程使用。通常在安装需要他们的软件时，从可用池中动态分配他们。
- UID 1000+：供分配给普通用户的范围



Red Hat

四、管理本地组账户

groupadd

groupadd groupname如果不带选项，则使用/etc/login.defs文件中指定范围内的下一个可用GID

- -g：用于指定具体的GID
- -r：使用/etc/login.defs文件中所列有效系统GID编号范围内的GID创建系统组

注意：

由于用户专用组（GID 1000以上）是自动创建的，因此通常建议预备一系列GID编号待用于补充组。较高的范围可以避免与系统组（GID0-999）产生冲突

groupmod修改现有组

groupmod用于将组名更改为GID映射。

选项：

- -n：用于指定新的名称
- -g：用于指定新的GID

实例：

- groupmod –n javaapp appusers
- groupmod –g 6000 ateam

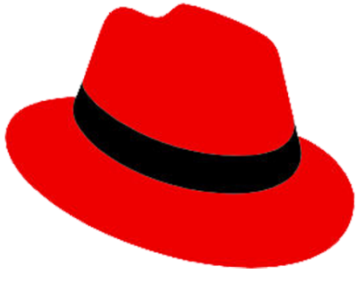
groupdel删除组

实例：

- groupdel javaapp

注意：

如果组是任何现有用户的**主要组**，则它不能被删除。与userdel一样，请检查所有文件系统，确保不遗留由该组拥有的任何文件



Red Hat

五、管理用户密码

密码策略

- 以前加密密码存储在全局可读的**/etc/passwd**中。后来将密码移动到**/etc/shadow**中
- 用户尝试登录时，系统在/etc/shadow中查询用户的条目，如果匹配则用户键入了正确的密码。

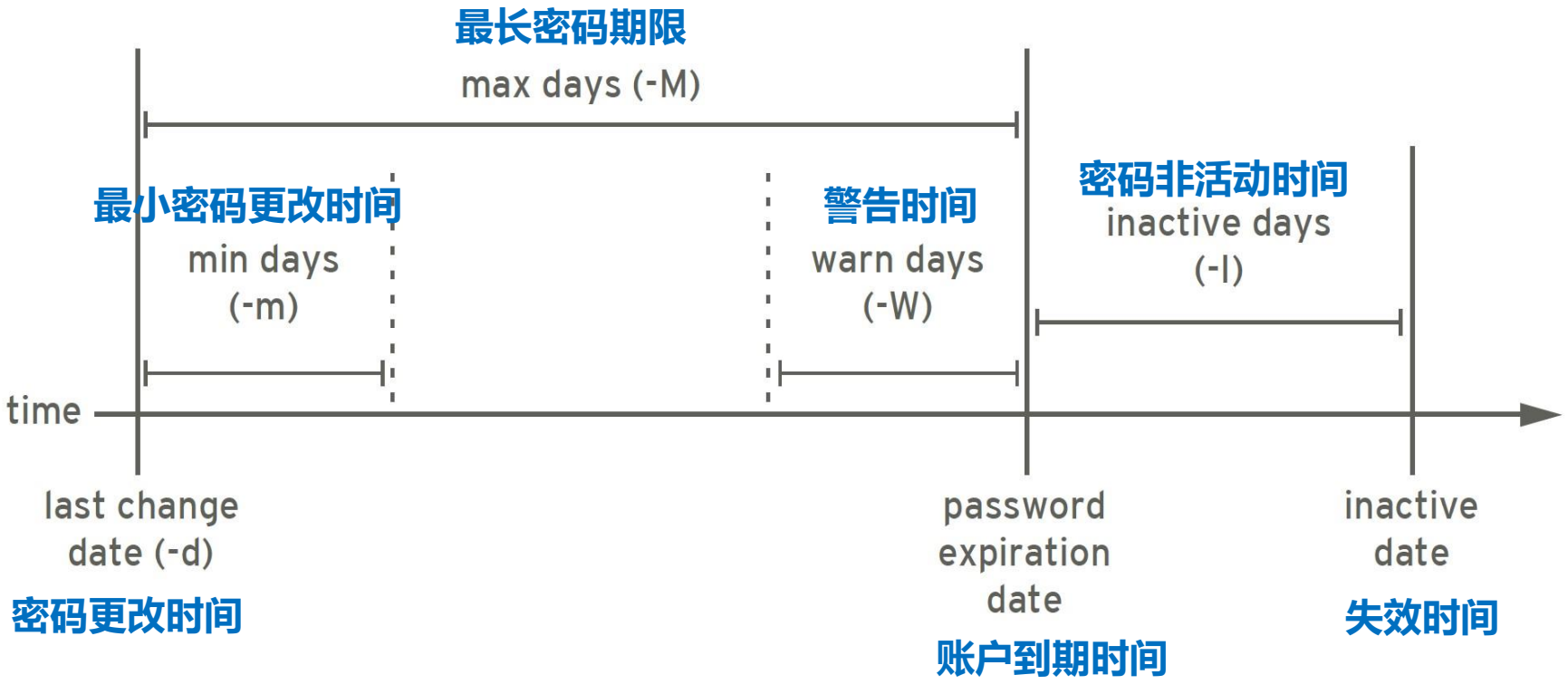
shadow文件详解

root用户的密码配置：

root:6vACL6866bGlMZ7Sh$nvstpNvQQVO.J79kH.oiD9tQBTTiYQ4C708P30BH/uWOaAF2j2V7/Dhnm9LkO3c6qLPGVJQGA8ZnwQt6ILUxW/:18037:0:99999:7:::

- **name**：登陆名称，必须是系统中的有效账户
- **passwd**：已加密的密码。密码字段开头为感叹号时，表示改密码被锁定
- **lastchange**：最近一次更改密码的日期，以距离1970年1月1日的天数表示
- **minage**：可以更改密码前的最少天数，如果为0则表示“无最短期限要求”
- **maxage**：必须更改密码前的最多天数
- **warning**：密码即将到期的警告期。以天数表示，0表示不提供警告
- **inactive**：账户在密码到期后保持活动的天数，在这期限内，用户依然可以登录系统并更改密码。在指定天数过后，账户被锁定，变为不活动
- **expire**：账户到期日期，以距离1970年1月1日的天数表示
- **blank**：预留字段，供未来使用

密码时间


最长密码期限
max days (-M)
最小密码更改时间
min days
(-m)
警告时间
warn days
(-W)
密码非活动时间
inactive days
(-I)
time
last change
date (-d)
密码更改时间
password
expiration
date
账户到期时间
inactive
date
失效时间

chage-修改密码时间策略

修改密码的时间策略：

chage -d 修改密码的时间戳

chage -E 设置密码过期日期（设置99999永不过期）

chage -l 查看密码信息

chage -I 密码更改的缓冲期

chage -M 密码更改的天数

chage -m 两次密码修改的间隔时间

chage -W 密码更改的警告天数

格式：

chage **-m** 0 **-M** 90 **-W** 7 **-I** 14 username

chage **-d** 0 username：强制在下次登录时更新密码

chage **-l** username：列出用户名的当前设置

chage **-E** YYYY-MM-DD：将在指定的日期使账户到期

随堂练习

1、创建下面的用户、组和组成员关系:

创建名字为adminuser 的组，并制定GID为5000；

创建用户natasha，使用adminuser 作为附属组；

创建用户harry，也使用adminuser 作为附属组；

创建用户sarah，设置为不能登录的SHELL（/sbin/nologin）；

natasha，harry，sarah密码都是redhat ；（echo redhat |passwd - -stdin user）

将natasha用户添加到wheel补充组。（wheel组在系统中默认就有无需自 行创建）

2、切换到harry用户，尝试使用useradd创建用户tom；

尝试使用sudo useradd创建用户tom；

切换到root用户，使用visudo修改配置文件，允许harry使用root权限执行所有操作。再次切换到harry用户，用sudo命令创建tom用户；

查看/etc/passwd 及 /etc/group 验证上面创建的用户和组是否在文件里面。

3、修改harry的密码过期时间为2019-8-1（ chage **-E** YYYY-MM-DD ）并强制harry用户在下次登录时修改密码（chage **–d** 0 username ）；

注销系统，使用harry用户进行登录验证。


WISDOM NET