

用户维持

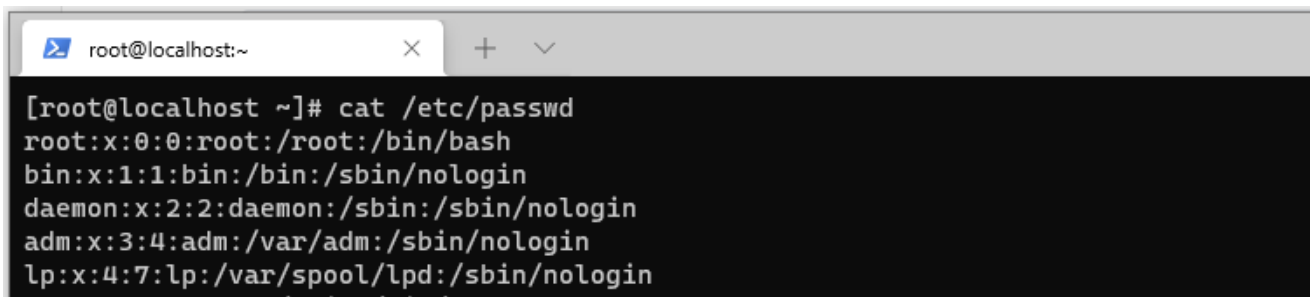
特权用户维持

用户文件介绍

在Linux系统中,存在着两个特殊的文件 `/etc/passwd` 和 `/etc/shadow` 这两个文件中存储着用户名和加密后的密码. 在目前大多数Linux系统中,将加密后的用户密码存放在`/etc/shadow`中但是 `/etc/shadow` 只能root用户查看

一、`/etc/passwd`介绍

用户名: 密码: UID (用户ID) : GID (组ID) : 描述性信息: 主目录: 默认Shell



```
root@localhost:~  
[root@localhost ~]# cat /etc/passwd  
root:x:0:0:root:/root:/bin/bash  
bin:x:1:1:bin:/bin:/sbin/nologin  
daemon:x:2:2:daemon:/sbin:/sbin/nologin  
adm:x:3:4:adm:/var/adm:/sbin/nologin  
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
```

(1) 用户名

用户名, 就是一串代表用户身份的字符串, 用户名仅是为了方便用户记忆, Linux 系统是通过 UID 来识别用户身份, 分配用户权限的。 `/etc/passwd` 文件中就定义了用户名和 UID 之间的对应关系。

(2) 密码

"x" 表示此用户设有密码, 但不是真正的密码, 真正的密码保存在 `/etc/shadow` 文件中, 在早期的 UNIX 中, 这里保存的就是真正的加密密码串, 但由于所有程序都能读取此文件, 非常容易造成用户数据被窃取。虽然密码是加密的, 但是采用暴力破解的方式也是能够进行破解的。因此, 现在 Linux 系统把真正的加密密码串放置在 `/etc/shadow` 文件中, 此文件只有 root 用户可以浏览和操作, 这样就最大限度地保证了密码的安全。

(3) UID

UID, 也就是用户 ID。每个用户都有唯一的一个 UID, Linux 系统通过 UID 来识别不同的用户。实际上, UID 就是一个 0~65535 之间的数, 不同范围的数字表示不同的用户身份

UID范围	用户身份
0	超级用户。UID 为 0 就代表这个账号是管理员账号。在 Linux 中，如何把普通用户升级成管理员呢？只需把其他用户的 UID 修改为 0 就可以了，这一点和 Windows 是不同的。不过不建议建立多个管理员账号。
1~1000	系统用户（伪用户）。也就是说，此范围的 UID 保留给系统使用。其中，1~99 用于系统自行创建的账号；100~499 分配给有系统账号需求的用户。其实，除了 0 之外，其他的 UID 并无不同，这里只是默认 500 以下的数字给系统作为保留账户，只是一个公认的习惯而已。
1000~65535	普通用户。通常这些 UID 已经足够用户使用了。但不够用也没关系，2.6.x 内核之后的 Linux 系统已经可以支持 232 个 UID 了。

(4) GID

全称“Group ID”，简称“组ID”，表示用户初始组的组 ID 号。在建立用户jack 的同时，就会建立jack 组作为jack 用户的初始组。刚刚的 jack 用户除属于初始组 jack 外，我又把它加入了 bob 组，那么jack 用户同时属于 jack 组和 bob 组，其中 jack是初始组，bob 是附加组。

(5) 描述性信息

这个字段并没有什么重要的用途，只是用来解释这个用户的意义而已。

(6) 主目录

也就是用户登录后有操作权限的访问目录，通常称为用户的主目录。

(7) 默认的Shell

Shell 就是 Linux 的命令解释器，是用户和 Linux 内核之间沟通的桥梁。linux 系统默认使用的命令解释器是 bash (/bin/bash)

二、/etc/shadow介绍

/etc/shadow 文件，用于存储 Linux 系统中用户的密码信息，又称为“影子文件”。前面介绍了 /etc/passwd 文件，由于该文件允许所有用户读取，易导致用户密码泄露，因此 Linux 系统将用户的密码信息从 /etc/passwd 文件中分离出来，并单独放到了此文件中。/etc/shadow 文件只有 root 用户拥有读权限，其他用户没有任何权限，这样就保证了用户密码的安全性。

用户名：加密密码：最后一次修改时间：最小修改时间间隔：密码有效期：密码需要变更前的警告天数：密码过期后的宽 限时间：账号失效时间：保留字段
--

```
root@localhost:~  
[root@localhost ~]# cat /etc/shadow  
root:$6$VPeZTWUwabJQBgPP$nC4s.cCHR03es8je4kEsSPdCBvTLcJVJvJ.0bq2ciRkhd  
kuJ3tH8a7.WvU2qyyNA9souUmfr8aHj/i65PWxaU1::0:99999:7:::  
bin:!:17632:0:99999:7:::  
daemon:!:17632:0:99999:7:::  
adm:!:17632:0:99999:7:::  
lp:!:17632:0:99999:7:::
```

(1) 用户名 同 /etc/passwd 文件的用户名有相同的含义。

(2) 加密密码 这里保存的是真正加密的密码。目前 Linux 的密码采用的是 SHA512 散列加密算法，原来采用的是 MD5 或 DES 加密算法。SHA512 散列加密算法的加密等级更高，也更加安全。注意，这串密码产生的乱码不能手工修改，如果手工修改，系统将无法识别密码，导致密码失效。很多软件透过这个功能，在密码串前加上 "!"、"" 或 "x" 使密码暂时失效。所有伪用户的密码都是 "!!" 或 ""，代表没有密码是不能登录的。当然，新创建的用户如果不设定密码，那么它的密码项也是 "!!"，代表这个用户没有密码，不能登录。

(3) 最后一次修改时间 此字段表示最后一次修改密码的时间，可是，为什么 root 用户显示的是 15775 呢？这是因为，Linux 计算日期的时间是以 1970 年 1 月 1 日作为 1 不断累加得到的时间，到 1971 年 1 月 1 日，则为 366 天。这里显示 15775 天，也就是说，此 root 账号在 1970 年 1 月 1 日之后的第 15775 天修改的 root 用户密码。

(4) 最小修改时间间隔 最小修改间隔时间，也就是说，该字段规定了从第 3 字段（最后一次修改密码的日期）起，多长时间之内不能修改密码。如果是 0，则密码可以随时修改；如果是 10，则代表密码修改后 10 天之内不能再次修改密码。此字段是为了针对某些人频繁更改账户密码而设计的。

(5) 密码有效期 经常变更密码是个好习惯，为了强制要求用户变更密码，这个字段可以指定距离第 3 字段（最后一次更改密码）多长时间内需要再次变更密码，否则该账户密码进行过期阶段。该字段的默认值为 99999，也就是 273 年，可认为是永久生效。如果改为 90，则表示密码被修改 90 天之后必须再次修改，否则该用户即将过期。管理服务时，通过这个字段强制用户定期修改密码。

(6) 密码需要变更前的警告天数 与第 5 字段相比较，当账户密码有效期快到时，系统会发出警告信息给此账户，提醒用户 "再过 n 天你的密码就要过期了，请尽快重新设置你的密码！"。该字段的默认值是 7，也就是说，距离密码有效期的第 7 天开始，每次登录系统都会向该账户发出 "修改密码" 的警告信息。

(7) 密码过期后的宽限天数

也称为“口令失效日”，简单理解就是，在密码过期后，用户如果还是没有修改密码，则在此字段规定的宽限天数内，用户还是可以登录系统的；如果过了宽限天数，系统将不再让此账户登陆，也不会提示账户过期，是完全禁用。比如说，此字段规定的宽限天数是 10，则代表密码过期 10 天后失效；如果是 0，则代表密码过期后立即失效；如果是 -1，则代表密码永远不会失效。

(8) 账号失效时间

同第 3 个字段一样，使用自 1970 年 1 月 1 日以来的总天数作为账户的失效时间。该字段表示，账号在此字段规定的时间之外，不论你的密码是否过期，都将无法使用！该字段通常被使用在具有收费服务的系统中。

(9) 保留 这个字段目前没有使用，等待新功能的加入。

特权用户维持

田间特权用户及时添加的用户和 root 拥有相同的权限，也就是在添加用户的时候将 UID 更改为 0，使用 useradd 命令创建用户

用法: useradd [选项] 登录 useradd -D useradd -D [选项]

选项:

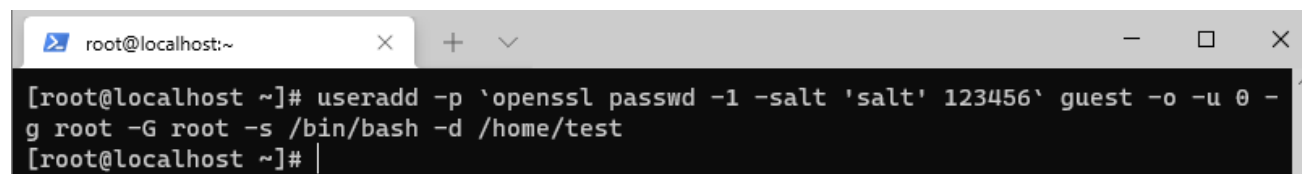
-b, --base-dir BASE_DIR	新账户的主目录的基目录
-c, --comment COMMENT	新账户的 GECOS 字段
-d, --home-dir HOME_DIR	新账户的主目录
-D, --defaults	显示或更改默认的 useradd 配置
-e, --expiredate EXPIRE_DATE	新账户的过期日期
-f, --inactive INACTIVE	新账户的密码不活动期
-g, --gid GROUP	新账户主组的名称或 ID
-G, --groups GROUPS	新账户的附加组列表
-h, --help	显示此帮助信息并推出
-k, --skel SKEL_DIR	使用此目录作为骨架目录
-K, --key KEY=VALUE	不使用 /etc/login.defs 中的默认值
-l, --no-log-init	不要将此用户添加到最近登录和登录失败数据库
-m, --create-home	创建用户的主目录
-M, --no-create-home	不创建用户的主目录
-N, --no-user-group	不创建同名的组
-o, --non-unique	允许使用重复的 UID 创建用户
-p, --password PASSWORD	加密后的新账户密码
-r, --system	创建一个系统账户
-R, --root CHROOT_DIR	chroot 到的目录
-s, --shell SHELL	新账户的登录 shell
-u, --uid UID	新账户的用户 ID
-U, --user-group	创建与用户同名的组
-Z, --selinux-user SEUSER	为 SELinux 用户映射使用指定 SEUSER

添加普通用户

```
# 创建一个用户名guest, 密码123456的普通用户
useradd -p `openssl passwd -1 -salt 'salt' 123456` guest
# useradd -p 方法 `` 是用来存放可执行的系统命令, "$()"也可以存放命令执行语句
useradd -p "$(openssl passwd -1 123456)" guest
# chpasswd方法
useradd guest;echo 'guest:123456'|chpasswd
# echo -e方法
useradd test;echo -e "123456\n123456\n" |passwd test
```

添加超级用户:

```
# 创建一个用户名guest, 密码123456的root用户
useradd -p `openssl passwd -1 -salt 'salt' 123456` guest -o -u 0 -g root -G root -s
/bin/bash -d /home/test
```



```
root@localhost:~
[root@localhost ~]# useradd -p `openssl passwd -1 -salt 'salt' 123456` guest -o -u 0 -g root -G root -s /bin/bash -d /home/test
[root@localhost ~]#
```

Windows PowerShell

版权所有 (C) Microsoft Corporation。保留所有权利。

尝试新的跨平台 PowerShell <https://aka.ms/pscore6>

PS C:\Users\DaoEr> **ssh** guest@192.168.41.134

guest@192.168.41.134's password:

Last login: Thu Mar 24 14:31:01 2022 from 192.168.41.1

[root@localhost ~]# whoami

root