CentOS 丛书目录 — 系统管理 — 网络服务 — 应用部署

口令管理和口令时效

内容提要

1. 学会使用passwd命令设置用户口令
2. 学会使用passwd命令管理用户口令
3. 学会使用chage命令修改口令时效

使用 passwd 命令管理口令

创建了用户账户之后，还要给新用户设置口令。设置用户口令的命令是 passwd [http://www.proxyserve.net/index.php?q=aHR0cDovL21hbi5jeC9wYXNzd2Q%3D]，命令格式是：

```
passwd [选项] [用户登录名]
```

选项	说明
-d	删除口令。仅管理员才能使用。
-k	设置只有在口令过期失效后方能更新。
-l	锁定用户账户。
-u	解除已锁定账户。
-S	列出口令的状态信息。

1. 在输入口令时，屏幕上不会回显。口令的选取至少用六个字符，最好大小写字母和数字及特殊字符搭配使用，尽量不要用英文单词作口令。
2. 只有管理员账户（root）可以更改其他用户的口令，普通用户只能更改自己的口令，且在更改口令之前，系统会要求用户输入现在的口令。
3. 超级用户也可以使用不带任何参数的 passwd 命令修改自己的口令。

举例：

1、创建新用户 jason，显示口令状态，为其设置口令

```
#  useradd jason
#  passwd -S jason
jason LK 2007-12-14 0 99999 7 -1 (Password locked.)
#  passwd jason
Changing password for user jason.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

2、用户jason 自己要更改自己的口令，可以这样操作：

```
$ passwd
Changing password for user osmond.
Changing password for osmond
(current) UNIX password:
```

```
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
$
```

3、超级用户可以使用如下命令进行用户口令管理，例如：

```
#  passwd -S jason         # 显示口令状态
jason PS 2007-12-15 0 99999 7 -1 (Password set, MD5 crypt.)
#  passwd -l jason         # 锁定用户 jason
Locking password for user jason.
passwd: Success
#  passwd -S jason         # 显示口令状态
jason LK 2007-12-15 0 99999 7 -1 (Password locked.)
#  passwd -u jason         # 解除对用户 jason 的锁定
Unlocking password for user jason.
passwd: Success.
#  passwd -S jason         # 显示口令状态
jason PS 2007-12-15 0 99999 7 -1 (Password set, MD5 crypt.)
#  passwd -d jason         # 清空 jason 的口令
Removing password for user jason.
passwd: Success
#  passwd -S jason         # 显示口令状态
jason NP 2007-12-15 0 99999 7 -1 (Empty password.)
#  passwd jason            # 重新设置用户 jason 的口令
Changing password for user jason.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
#  passwd -S jason         # 显示口令状态
jason PS 2007-12-15 0 99999 7 -1 (Password set, MD5 crypt.)
```

口令时效

目前已有更强大的硬件大大地缩短了利用自动运行的程序来猜测口令的时间。口令时效是系统管理员用来防止机构内不良口令的一种技术。防止口令被攻击的方法就是要经常地改变口令。为安全起见，要求用户定期改变他们的口令是明智之举。口令时效意味着过了一段预先设定的时间后，用户会被提示创建一个新口令。它所根据的理论是，如果用户被强制定期改变口令，某个破译的口令对入侵者来说就只有有限的利用机会。这种用来强制用户在一段时间之后更改口令的机制称为口令时效。

设置新添用户的口令时效

通过编辑 /etc/login.defs，可以指定几个参数，来设置口令实效的默认设定：

```
# Password aging controls:
#
#   PASS_MAX_DAYS   Maximum number of days a password may be used.
#   PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#   PASS_MIN_LEN    Minimum acceptable password length.
#   PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_MIN_LEN    5
PASS_WARN_AGE   7
```

- PASS_MAX_DAYS：设定在多少天后要求用户修改口令。默认口令时效的天数为99999，即关闭了口令时效。更明智的设定一般是60天（每2个月）强制更改一次口令。
- PASS_MIN_DAYS：设定在本次口令修改后，下次允许更改口令之前所需的最少天数。
- PASS_MIN_LEN ：设定口令的最小字符数。
- PASS_WARN_AGE：设定在口令失效前多少天开始通知用户更改口令（一般在用户刚刚登陆系统时就会收到警告通知）。

也可以编辑 /etc/default/useradd 文件中 INACTIVE 和 EXPIRE 的设置。

```
# The number of days after a password expires until the account
# is permanently disabled
# INACTIVE=-1
#
# The default expire date
# EXPIRE=
```

- INACTIVE：指明在口令失效后多久时间内，如果口令没有进行更改，则将账户更改为失效状态。默认值为 -1，即关闭了口令时效。更明智的设定一般是60天（每2个月）强制更改一次口令。
- EXPIRE：为设置所有新用户设定一个口令失效的明确时间（具体格式为"YYYY-MM-DD"）。

设置已存在用户的口令时效

对系统已存在用户设置口令时效是通过 chage [http://www.proxyserve.net/index.php?q=aHR0cDovL21hbi5jeC9jaGFnZQ%3D%3D] 命令来管理的。chage命令的格式是：

```
chage [选项] [用户登录名]
```

选项	说明
-m days	指定用户必须改变口令所间隔的最少天数。如果值为 0，口令就不会过期。(PASS_MIN_DAYS)
-M days	指定口令有效的最多天数。当该选项指定的天数加上-d选项指定的天数小于当前的日期，用户在使用该账号前就必须改变口令。(PASS_MAX_DAYS)
-d days	指定自从1970年1月1日起，口令被改变的天数。
-I days	指定口令过期后，账号被锁前不活跃的天数。如果值为0，账号在口令过期后就不会被锁。
-E date	指定账号被锁的日期，日期格式为YYYY-MM-DD。若不用日期，也可以使用自1970年1月1日后经过的天数。
-W days	指定口令过期前要警告用户的天数。(PASS_WARN_AGE)
-l	列出指定用户当前的口令时效信息，以确定账号何时过期。

举例：

1、要求用户jason两天内不能更改口令，并且口令最长的存活期为30天，并在口令过期前5天通知jason。

```
#  chage -m 2 -M 30 -W 5 jason
```

2、可以使用如下命令查看用户jason当前的口令时效信息。

```
#  chage -l jason
Last password change                                    : Dec 15, 2007
Password expires                                        : Jan 14, 2008
Password inactive                                       : never
Account expires                                         : never
```

```
Minimum number of days between password change          : 2
Maximum number of days between password change          : 30
Number of days of warning before password expires       : 5
```

1. 也可以使用chage <用户名>进入交互模式修改用户的口令时效。
2. 使用chage命令实质上是修改影子口令文件/etc/shadow中的与口令时效相关的字段值。
3. chage命令仅仅适用于本地系统账户，对LDAP账号和数据库账号不起作用。

制定一项策略，定义多长时间一个口令必须进行更改，然后强制执行该策略，是非常不错的一个做法。在解雇了某个雇员后，口令时效策略会保证该雇员不可能在被解雇3个月后发现他的口令依然可用。即使系统管理员忽略了删除他的帐号，该帐号也会因口令时效策略而被自动锁定。当然，这一点并不能成为不及时删除该雇员帐号的理由，但是这个策略的确提供了一层额外的安全防护，尤其是在过去常常忽视及时清理帐号的情况下。

- 显示源文件
- 登录