用户切换和用户状态命令

内容提要

1. 理解 su 和 sudo 的不同
2. 掌握 su 和 sudo 的使用
3. 学会使用 id groups newgrp 等命令

用户切换命令

系统管理员应该养成良好的习惯：以一个普通用户登录系统进行不同操作，当需要超级用户身份进行系统管理时再切换超级用户执行系统管理命令。有如下两种方式：

- su
  - 直接切换为超级用户
  - 普通用户要切换为超级用户必须知道超级用户的口令
  - 适用于系统中只有单个系统管理员的情况
- sudo
  - 直接使用 sudo 命令前缀执行系统管理命令
  - 执行系统管理命令时无需知道超级用户的口令，使用普通用户自己的口令即可
  - 由于执行系统管理命令时无需知晓超级用户口令，所以适用于系统中有多个系统管理员的情况，因为这样不会泄露超级用户口令。当然系统只有单个系统管理员时也可以使用。

su

su 用于切换当前用户到指定的用户账号，命令的格式如下：

```
su [-|-p] [-c command] [username]
```

其中：

- **-**：在切换当前用户时切换用户工作环境
- **-p**：在切换当前用户时不切换用户工作环境，即保持当前用户工作环境，此为缺省值
- **-c command**：以指定的用户身份执行命令 command
- **username**：为要切换的用户，省略时表示 root

例如：

```
# 切换为超级用户，不切换用户身份
[osmond@cnetos5 ~]$ su
Password:                                       # 输入超级用户口令
[root@cnetos5 osmond]# env|egrep 'USER|LOGNAME|PATH|MAIL'
USER=osmond
PATH=/usr/kerberos/sbin:/usr/kerberos/bin:/usr/local/bin:/bin:/usr/bin:/home/osmond/bin
MAIL=/var/spool/mail/osmond
LOGNAME=osmond
[root@cnetos5 osmond]# exit
# 切换为超级用户 root，同时切换用户身份
[osmond@cnetos5 ~]$ su -
Password:                                       # 输入超级用户口令
[root@cnetos5 ~]# env|egrep 'USER|LOGNAME|PATH|MAIL'
USER=root
MAIL=/var/spool/mail/root
PATH=/usr/kerberos/sbin:/usr/kerberos/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin
LOGNAME=root
[root@cnetos5 ~]# exit
```

```
[osmond@cnetos5 ~]$
# 切换为普通用户 crq，同时切换用户身份
[osmond@cnetos5 ~]$ su - crq
Password:                                       # 输入用户 crq 的口令
[crq@cnetos5 ~]$
[crq@cnetos5 ~]$ exit
# 以超级用户身份和环境执行命令
[osmond@cnetos5 ~]$ su - -c 'tail -1 /etc/shadow'
Password:                                       # 输入超级用户口令
qul0m:!!:13862:0:99999:7:::
[osmond@cnetos5 ~]$
```

sudo

sudo 简介

sudo [http://www.proxyserve.net/index.php?q=aHR0cDovL3d3dy5zdWRvLndzL3N1ZG8vc3Vkby5odG1s] (su "do") 允许系统管理员（root）为几个用户或组委派权利，使之能运行部分或全部由 root （或另一个）用户执行的命令。sudo 设计者的宗旨是：给用户尽可能少的权限但仍允许完成他们的工作。sudo 是设置了 SUID 位的执行文件。

sudo 具有以下特点：

- sudo 能够限制指定用户在指定主机上运行某些命令。
- sudo 可以提供日志，忠实地记录每个用户使用sudo做了些什么，并且能将日志传到中心主机或者日志服务器。
- sudo 为系统管理员提供配置文件，允许系统管理员集中地管理用户的使用权限和使用的主机。它默认的存放位置是 /etc/sudoers。
- sudo 使用时间戳文件来完成类似"检票"的系统。当用户执行 sudo 并且输入密码后，用户获得了一张默认存活期为5分钟的"入场券"（默认值可以在编译的时候改变）。超时以后，用户必须重新输入密码。

用户执行 sudo 的执行过程：

1. 在 /var/run/sudo/$HOME 目录中查找时间戳文件
   I. 若时间戳已过期，提示用户输入自己的口令
      a. 若口令输入错误则退出 sudo 的执行
      b. 若口令输入正确则继续 sudo 的执行过程
   II. 若文件存在继续 sudo 的执行过程
2. 读取配置文件 /etc/sudoers，判断用户是否具有执行此 sudo 命令的权限
   I. 若有权限执行则执行 sudo 后面的命令
   II. 若无权执行则退出 sudo 的执行

sudo 命令的格式

sudo 命令的格式为：

```
sudo -V | -h | -k | -l | -v
sudo [-Hb] [-u username|#uid] { -i | -s | <command> }
```

其中：

- **-V**：显示版本信息，并退出。
- **-h**：显示帮助信息。
- **-l**：显示当前用户（执行 sudo 的使用者）的权限，只有在 /etc/sudoers 里的用户才能使用该选项。
- **-v**：延长密码有效期限5分钟。
- **-k**：将会强迫使用者在下一次执行 sudo 时问密码（不论有没有超过 5 分钟）。
- **-H**：将环境变数中的 $HOME 指定为要变更身份的使用者家目录（如不加 -u 参数就是 /root ）。
- **-b**：在后台执行指令。
- **-u username|#uid**：以指定的用户作为新的身份。身略此参数表示以 root 的身份执行指令。
- **-i**：模拟一个新用户身份的初始 Shell。

- **-s**：执行环境变量 $SHELL 所指定的 shell ，或是 /etc/passwd 里所指定的 shell。
- **command**：为以新用户身份要执行的命令。

配置 sudo

默认情况下，只有 root 用户可以使用 sudo 命令。要分派其他用户使用 sudo 命令，需要修改配置文件 /etc/sudoers，下面是 CentOS 默认的 配置文件 /etc/sudoers：

```
# cat /etc/sudoers |egrep -v ^#|egrep -v ^$
Cmnd_Alias NETWORKING = /sbin/route, /sbin/ifconfig, /bin/ping, \
/sbin/dhclient, /usr/bin/net, /sbin/iptables, /usr/bin/rfcomm, \
/usr/bin/wvdial, /sbin/iwconfig, /sbin/mii-tool
Cmnd_Alias SOFTWARE = /bin/rpm, /usr/bin/up2date, /usr/bin/yum
Cmnd_Alias SERVICES = /sbin/service, /sbin/chkconfig
Cmnd_Alias LOCATE = /usr/sbin/updatedb
Cmnd_Alias STORAGE = /sbin/fdisk, /sbin/sfdisk, /sbin/parted, /sbin/partprobe, \
/bin/mount, /bin/umount
Cmnd_Alias DELEGATING = /usr/sbin/visudo, /bin/chown, /bin/chmod, /bin/chgrp
Cmnd_Alias PROCESSES = /bin/nice, /bin/kill, /usr/bin/kill, /usr/bin/killall
Cmnd_Alias DRIVERS = /sbin/modprobe
Defaults    requiretty
Defaults    env_reset
Defaults    env_keep = "COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR \
                        LS_COLORS MAIL PS1 PS2 QTDIR USERNAME \
                        LANG LC_ADDRESS LC_CTYPE LC_COLLATE LC_IDENTIFICATION \
                        LC_MEASUREMENT LC_MESSAGES LC_MONETARY LC_NAME  \
                        LC_NUMERIC LC_PAPER LC_TELEPHONE LC_TIME LC_ALL \
                        LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY"
root    ALL=(ALL)       ALL
```

root 用户可以使用如下命令修改 sudo 的配置文件 /etc/sudoers ：

```
# visudo
```

上面的命令将启动 vi 编辑文件 /etc/sudoers。之所以使用 visudo 有两个原因：一是它能够防止两个用户同时修改它；二是它也能进行有限的语法检查。

/etc/sudoers 文件的语法相对复杂，详细说明请参见其手册 man sudoers，下面做简单说明：

/etc/sudoers 中的特殊字符和保留字：

- 以 # 开始的行为注释行
- 保留字 ALL 表示所有
- % 后的名字表示组名
- ! 表示逻辑非
- 行末的 \ 为续行符
- 下面的字符作为一个词的一部分(例如,一个用户名或者一个主机名)出现时必需使用反斜线("\")来转义:"@","!","=",":", ",", "(", ")", "\"

/etc/sudoers 的组成部分：

1. 别名定义部分：包括 User_Alias, Host_Alias, Runas_Alias, Cmnd_Alias
2. 配置选项部分：由 Defaults 设置
3. 权限分配部分：这是整个配置文件的核心部分，其格式为：

```
User    Host = (Runas)                  Cmnd
用户     主机 = (可切换的其他用户)          可执行的命令
```

说明：

- 在 Cmnd 部分之前可以使用 NOPASSWD: 参数，表示不用输入密码即可执行 Cmnd
- (Runas) 部分可以省略，省略时表示 (root) ，即表示仅能切换为 root 用户身份
- 四个部分均可设置多个项目，每个项目用逗号间隔
- 四个部分均可使用别名定义来简化配置，即用 User_Alias 定义用户别名、用 Host_Alias 定义主机别名、用 Runas_Alias

定义切换用户别名、用 Cmnd_Alias 定义命令别名。别名必须使用大些字母。这些别名语句的格式为：

```
User_Alias USER_ALIAS_NAME = user1, user2, ......
Host_Alias HOST_ALIAS_NAME = host1, host2, ......
Runas_Alias RUNAS_ALIAS_NAME = runas1, runas2, ......
Cmnd_Alias COMMAND_ALIAS_NAME = cmnd1, cmnd2, ......
```

下面给出一些配置片段：

```
# 让 osmond 用户和 wheel 组的成员可以在任何主机上以任何人的身份运行任何命令。
osmond ALL = (ALL) ALL
%wheel ALL = (ALL) ALL

# 专职系统管理员(millert,mikef和dowdy)可以在任何主机上执行任何命令而不需要进行身份验证。
User_Alias FULLTIMERS = millert, mikef, dowdy
FULLTIMERS ALL = NOPASSWD: ALL

# 兼职系统管理员(bostley,jwfox和crawl)可以在任何主机上运行任何命令,
# 但他们首先必须进行身份验证(因为这个条目没有NOPASSWD标签)。
User_Alias PARTTIMERS = bostley, jwfox, crawl
PARTTIMERS ALL = ALL

# 兼职管理员(jalala, sonar和huge)可以在任何主机上运行 BROWSE、PROCESSES、USERS 中的命令
# 同时可以修改除了 root 用户之外的所有用户口令
User_Alias       PARTTIMERS2 = jalala, sonar , huge
Cmnd_Alias      BROWSE = /bin/ls, /bin/cd, /bin/cat
Cmnd_Alias      PROCESSES = /bin/nice, /bin/kill, /usr/bin/kill, /usr/bin/killall
Cmnd_Alias      USERS = /usr/sbin/useradd [A-z]*,/usr/sbin/userdel -r [A-z]*
PARTTIMERS2 ALL=USERS,PROCESSES,BROWSE,/usr/bin/passwd [A-z]*, !/usr/bin/passwd root

# 允许sys 组的成员运行 networking, software, service 等管理命令
Cmnd_Alias NETWORKING = /sbin/route, /sbin/ifconfig, /bin/ping, \
/sbin/dhclient, /usr/bin/net, /sbin/iptables, /usr/bin/rfcomm, \
/usr/bin/wvdial, /sbin/iwconfig, /sbin/mii-tool
Cmnd_Alias SOFTWARE = /bin/rpm, /usr/bin/up2date, /usr/bin/yum
Cmnd_Alias SERVICES = /sbin/service, /sbin/chkconfig
Cmnd_Alias LOCATE = /usr/sbin/updatedb
Cmnd_Alias STORAGE = /sbin/fdisk, /sbin/sfdisk, /sbin/parted, /sbin/partprobe, \
/bin/mount, /bin/umount
Cmnd_Alias DELEGATING = /usr/sbin/visudo, /bin/chown, /bin/chmod, /bin/chgrp
Cmnd_Alias PROCESSES = /bin/nice, /bin/kill, /usr/bin/kill, /usr/bin/killall
Cmnd_Alias DRIVERS = /sbin/modprobe
%sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, \
PROCESSES, LOCATE, DRIVERS

# WEBMASTERS(will, wendy,和 wim)中的用户都能够在主机www上
# 以www的身份执行任何命令，或者使用 su www 命令
User_Alias     WEBMASTERS = will, wendy, wim
WEBMASTERS www = (www) ALL, (root) /usr/bin/su www
```

sudo 使用举例

```
[crq@cnetos5 ~]$ sudo -V                # 显示当前 sudo 的软件版本
Sudo version 1.6.8p12
[crq@cnetos5 ~]$ sudo tail /etc/shadow        # 首次运行 sudo 命令

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password:                                   # 输入 crq 用户自己的口令
crq is not in the sudoers file.  This incident will be reported.
# 因为 crq 用户未在 /etc/sudoers 文件中，所以未能执行 tail 命令
[crq@cnetos5 ~]$
```

```
# 以 root 用户身份执行命令
[osmond@cnetos5 ~]$ sudo touch /root/sudotest
Password:                                   # 输入 osmond 用户自己的口令
[osmond@cnetos5 ~]$ ls /root/sudotest
ls: /root/sudotest: Permission denied
```

```
[osmond@cnetos5 ~]$ sudo ls -l /root/sudotest
# 5 分钟之内再使用 sudo 命令无需再输入口令
-rw-r--r-- 1 root root 0 Dec 19 01:51 /root/sudotest
# 以其他用户身份执行命令
[osmond@cnetos5 ~]$ sudo -u crq touch /home/crq/sudotest
[osmond@cnetos5 ~]$ ls -l /home/crq/sudotest
ls: /home/crq/sudotest: Permission denied
[osmond@cnetos5 ~]$ sudo ls -l /home/crq/sudotest
-rw-r--r-- 1 crq crq 0 Dec 19 01:53 /home/crq/sudotest
# 显示当前用户 osmond 的 sudo 权限
[osmond@cnetos5 ~]$ sudo -l
User osmond may run the following commands on this host:
    (ALL) ALL
# 以 root 用户身份执行子shell
[osmond@cnetos5 ~]$ sudo -s
[root@cnetos5 ~]#
[root@cnetos5 ~]# exit
[osmond@cnetos5 ~]$
```

用户状态命令

常用的用户状态命令包括：whoami、id、groups、newgrp 等。

- whoami：用于显示当前用户的名称
- groups：用于显示指定用户所属的组
- id：用户显示用户身份
- newgrp：用户转换用户的当前组到指定的附加组，用户必须属于该组才可以进行

下面给出这些命令的使用举例：

```
# 创建一个新组staff
[root@cnetos5 ~]# groupadd staff
# 将用户crq 加入staff 附加组，并为其设置口令
[root@cnetos5 ~]# usermod -G staff crq
# 显示当前用户的名称
[root@cnetos5 ~]# whoami
root
# 显示当前用户所属的组
[root@cnetos5 ~]# groups
root bin daemon sys adm disk wheel
# 显示指定用户所属的组
[root@cnetos5 ~]# groups crq
crq : crq staff
# 显示用户当前的uid、gid和用户所属的组列表
[root@cnetos5 ~]# id
uid=0(root) gid=0(root) groups=0(root),1(bin),
2(daemon),3(sys),4(adm),6(disk),10(wheel)

#切换当前用户到crq（超级用户切换到普通用户无需口令），同时切换用户工作环境
[root@cnetos5 ~]# su - crq
[crq@cnetos5 ~]$
# 显示用户当前的uid、gid和用户所属的组列表
[crq@cnetos5 ~]$ id
uid=504(crq) gid=504(crq) groups=504(crq),3001(staff)
# 创建一个新文件，并查看其用户和组
[crq@cnetos5 ~]$ touch abc
[crq@cnetos5 ~]$ ll abc
-rw-rw-r-- 1 crq crq 0 Dec 19 02:13 abc
# 切换用户的当前组到指定的附加组staff
[crq@cnetos5 ~]$ newgrp staff
# 显示用户当前的uid、gid和用户所属的组列表
[crq@cnetos5 ~]$ id
uid=504(crq) gid=3001(staff) groups=504(crq),3001(staff)
# 创建一个新文件，并查看其用户和组（比较abc和xyz的组）
[crq@cnetos5 ~]$ touch xyz
[crq@cnetos5 ~]$ ll
total 0
-rw-rw-r-- 1 crq crq   0 Dec 19 02:13 abc
-rw-r--r-- 1 crq staff 0 Dec 19 02:14 xyz
# 返回上一次 crq 的登录
[crq@cnetos5 ~]$ exit
exit
```

```
# 返回上一次root的登录
[crq@cnetos5 ~]$ exit
logout
[root@cnetos5 ~]#
```

参考

- 掌握sudo的使用 [http://www.proxyserve.net/index.php?q=aHR0cDovL2Jsb2cuY2hpbmF1bml4Lm5ldC91LzEyNTkyL3Nob3dhcnRfMjM4OTc5Lmh0bWw%3D]
- sudoers中文man文档 [http://www.proxyserve.net/index.php?q=aHR0cDovL3d3dy5sZWZ0d29ybGQubmV0L3dlbnpoYW5nL3Nob3cvMTU0My5odG1s]
- 显示源文件
- 登录