Мениджмънт на потребители и групи

Thursday, August 27, 2020 4:38 PM

Полезно е да знаем кои файлове да променяме с цел мениджмънт на настройките на потребителските акаунти.

Потребителските профили се складират в /etc/passwd
Това което можем да видим от там са:

Името на акаунта	evgeni
Потребителски идентификационен номер	1006
Домашната директория	/home/evgeni
Обикновената черупка	/bin/bash

Паролите и възрастта на акаунтите се запазва в	/etc/shadow

Обикновени настройки на потребителите	/etc/login.def

Обикновената черупка и домашната директория в	/etc/default/useradd

В /etc/default/useradd се уточнява и skeletal или skel директориятa. Чиито предмет е да съдържа файловете които са копирани във всяка нова потребителска директория автоматично.

Процеса по създаването на потребителски акаунт

useradd

Ако напишем useradd в конзолата (черупката, интерпретатора) ще видим:

sudo useradd

```
Usage: useradd [options] LOGIN
       useradd -D
       useradd -D [options]

Options:
  -d, --home-dir HOME_DIR       home directory of the new account
  -D, --defaults                print or change default useradd configuration
  -e, --expiredate EXPIRE_DATE  expiration date of the new account
  -f, --inactive INACTIVE       password inactivity period of the new account
  -g, --gid GROUP               name or ID of the primary group of the new
                                account
  -G, --groups GROUPS           list of supplementary groups of the new
                                account
  -h, --help                    display this help message and exit
  -k, --skel SKEL_DIR           use this alternative skeleton directory
  -K, --key KEY=VALUE           override /etc/login.defs defaults
  -l, --no-log-init             do not add the user to the lastlog and
                                faillog databases
  -m, --create-home             create the user's home directory
  -M, --no-create-home          do not create the user's home directory
  -N, --no-user-group           do not create a group with the same name as
                                the user
  -o, --non-unique              allow to create users with duplicate
                                (non-unique) UID
  -p, --password PASSWORD       encrypted password of the new account
  -r, --system                  create a system account
  -R, --root CHROOT_DIR         directory to chroot into
  -P, --prefix PREFIX_DIR       prefix directory where are located the /etc/* files
```

```
-s, --shell SHELL           login shell of the new account
-u, --uid UID               user ID of the new account
-U, --user-group            create a group with the same name as the user
-Z, --selinux-user SEUSER   use a specific SEUSER for the SELinux user mapping
    --extrausers            Use the extra users database
```

https://unix.stackexchange.com/questions/4460/why-is-debian-not-creating-the-wheel-group-by-default
https://serverfault.com/questions/367559/how-to-add-a-user-without-knowing-the-encrypted-form-of-the-password

useradd bob

cat /etc/passwd | grep bob

```
cat /etc/passwd | grep bob
bob:x:1007:1007::/home/bob:/bin/sh
```

Четвъртата колона показва първичното потребителско групово ID което се генерира автоматично.
Можем да направим препратка с това число към /etc/group файла

```
cat /etc/group | grep bob
bob:x:1007:
```

Сега ще погледнем паролата и старостта на акаунта в /etc/shadow

```
sudo cat /etc/shadow | grep bob
bob:!:18517:0:99999:7:::
```

Ако погледнем целият файл ще забележим, че паролите седят във втората колона.
Но там има удивителни знаци, в зависимост от операционната система може да е един или два.
Това посочва, че потребителят няма парола. Това означава, че потребителят не може да се логне.

Нека му сложим някаква парола за да може да се логне:

```
sudo passwd bob
New password:
Retype new password:
passwd: password updated successfully
```

Сега погледнете shadow файла отново спрямо потребителя:

```
sudo cat /etc/shadow | grep bob
bob:$6$NLK.WPFDsI3Fxuri$QqHd19Sah6F8F/auFhx3B2EBmno2.DhYIz32xCYrrZ4m3LfjiG3C7iCf2396jHdBSy/50Y.WSwSVV0z
GchWOi.:18517:0:9
9999:7:::
```

*Виждаме, че паролата вече е криптирана.

(Ако ползвате CLI на Windows
sudo useradd pesho -m -d /home/pesho -s /bin/bash => не е конфигуриран да взима обикновените настройки

Препоръчва се adduser.
)

Сега нека му погледнем неговата домашна директория:

```
ls -lah
total 8.0K
drwxr-xr-x 1 bob bob 4.0K Sep 13 02:06 .
drwxr-xr-x 1 root root 4.0K Sep 13 02:06 ..
-rw------- 1 bob bob 5 Sep 13 02:06 .bash_history
-rw-r--r-- 1 bob bob 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 bob bob 3.7K Feb 25 2020 .bashrc
-rw-r--r-- 1 bob bob 807 Feb 25 2020 .profile
```

Ако искаме да изтрием потребителя можем просто да:

userdel bob - това не маха папката му в /home

За да я махнете:

userdel -r bob със sudo

Като го изтриете:

cat /etc/passwd | grep bob и няма да е там

Ако искате да дадете sudo привилегии на потребител използвайте групата wheel

```
sudo useradd petar -m -d /home/petar -s /bin/bash
sudo passwd petar
```

sudo usermod -aG wheel petar

За можем да променяме настройки на потребителите ще трябва да ползваме usermod .

Голяма част от синтаксиса на usermod е като на useradd

usermod
Usage: usermod [options] LOGIN

Options:
```
  -c, --comment COMMENT         new value of the GECOS field
  -d, --home HOME_DIR           new home directory for the user account
  -e, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -f, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
  -g, --gid GROUP               force use GROUP as new primary group
  -G, --groups GROUPS           new list of supplementary GROUPS
  -a, --append                  append the user to the supplemental GROUPS
                                mentioned by the -G option without removing
                                the user from other groups
  -h, --help                    display this help message and exit
  -l, --login NEW_LOGIN         new value of the login name
  -L, --lock                    lock the user account
  -m, --move-home               move contents of the home directory to the
                                new location (use only with -d)
  -o, --non-unique              allow using duplicate (non-unique) UID
  -p, --password PASSWORD       use encrypted password for the new password
  -R, --root CHROOT_DIR         directory to chroot into
  -P, --prefix PREFIX_DIR       prefix directory where are located the /etc/* files
  -s, --shell SHELL             new login shell for the user account
  -u, --uid UID                 new UID for the user account
  -U, --unlock                  unlock the user account
  -v, --add-subuids FIRST-LAST  add range of subordinate uids
  -V, --del-subuids FIRST-LAST  remove range of subordinate uids
  -w, --add-subgids FIRST-LAST  add range of subordinate gids
  -W, --del-subgids FIRST-LAST  remove range of subordinate gids
  -Z, --selinux-user SEUSER     new SELinux user mapping for the user account
```

sudo useradd ivelina -m -d /home/ivelina -s /bin/bash
sudo passwd ivelina
sudo cat /etc/shadow

cat /etc/group | grep audio

groupadd audio ако я нямате

sudo usermod -a -G audio ivelina

cat /etc/group | grep audio

sudo usermod -L ivelina --> за да заключим акаунта

cat /etc/shadow и ще видите че има удивителна преди паролата и.

sudo usermod -U ivelina за да отключите потребителя

cat /etc/shadow удивителната липсва, защото отключихме акаунта

sudo usermod -s /sbin/nologin ivelina

Ако ползвате сървър бихте могли да я спрете от логване по този начин.

cat /etc/passwd | grep ivelina и ще видите, че нейната черупка е променена

Как бихте обърнали процеса?

*
sudo usermod -s /bin/bash ivelina

Групи

Групите са важна част от Linux системата, но имат един голям недостатък -> те не могат да бъдат загнездени, това което имам в предвид е, че няма група в групата.

sudo groupadd -g 1050 accounting

cat /etc/group | grep accounting и ще я видите

Ако искаме да променим номера на групата:

sudo groupmod -g 1051 accounting

Това ще промени номера на групата, проверка:

cat /etc/group | grep accounting

Ако искате да добавите потребител в групата:

sudo gpasswd -a username accounting

Можем да направим така, че потребителите да принадлежат в група:

sudo usermod -a -G groupname username

За да изтрием група:

sudo groupdel groupname

Проверка:

cat /etc/group

Повечето потребителски акаунти в линукс използват номера от 500 до 1000 или 1000+.

В зависимост как системата е била нагласена.
Можем да видим как е нагласена в /etc/login.defs файла.

less /etc/login.defs

/uid

И ще видите, че в centos е сложено:

```
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                 1000
GID_MAX                 60000
```

Под 1000 са системни акаунти и обикновено не са логин акаунти, ще познаете това по

awk -F: '($3<1000){print $1}' /etc/passwd

Ще покаже всичките само по име.

Може да ги познаете също по последната колона:

Логин потребителите ще са със /bin/bash, а системните:
/bin/false
/sbin/nologin

Можем да имаме логин потребители които могат да включат едно персонализано софтуеърче.
Като сложим апликацията в края на техният потребител.
В момента на логване ще стартира апликацията.

Имайте в предвид, че полицата на SE-Linux трябва да бъде променена за да могат да го правят.

Могат да се инсталират и черупки които са ограничени като например:

rsh, rbash, bash --restricted, rksh и ksh -r

https://stackoverflow.com/questions/74844/bash-or-kornshell-ksh

За много дистрибуции имаме специален акаунт който се казва wheel, но често се намира в групата на администраторите.

less /etc/security/access.conf

Това са неговите привилегии:

```
#-:ALL EXCEPT wheel shutdown sync:LOCAL
#
# Same, but make sure that really the group wheel and not the user
# wheel is used (use nodefgroup argument, too):
#
#-:ALL EXCEPT (wheel) shutdown sync:LOCAL
#
# Disallow non-local logins to privileged accounts (group wheel).
#
#-:wheel:ALL EXCEPT LOCAL .win.tue.nl
```

Дава ни например всички потребители които са в групата да могат да изключват хоста.
Също не локалните логини в wheel акаунта са ограничени.

Нека видим sudo конфигурацията:

sudo visudo

```
## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL

## Same thing without a password
```

```
# %wheel      ALL=(ALL)      NOPASSWD: ALL
```

Тук виждаме, че всички потребители в wheel могат да пускат комади с високи привилегии.

Не е рядко системите да бъдат хакнати поради слаби пароли.
Администраторите могат да имплементират полици които да, изискват минимален брой знаци и различни видове знаци.

Линукс има кредитна система която афектира позволените знаци в парола.

Например:

Minimum password length =9 Lowercase credit =1 Effective minimum password length = 8	tqbfjotl
Minimum password length =9 Lowercase credit =1 Uppercase credit =1 Effective minimum password length = 7	Tqbfjot
Minimum password length =9 Lowercase credit =1 Uppercase credit =1 Digit credit =1 Effective minimum length password length =6	Tq8fjo

Паролната конфигурационна полица съдържа настройки за:

Уникални знаци, минимален брой знаци, цифри, знаци с главна буква, малка, и др.
Това включва пунктуация. Също има опции за минимален брой различни знаци и класове, повторения на знаците и дали да провери коментираното поле в /etc/passwd с цел проверка за подобни пароли с други потребители.

Броя на знаци които не трябва да са като в старата парола	difok = 5
Минималната дължина на новата паролата имайте в предвид, че кредитите ще извадят от това число, ако ползвате кредите ще ползвате един като ваш желан минимум.	minlen =9
Максимален кредит за ползването на цифри, ако е по малко от 0 ще бъде минималната бройка цифри.	dcredit =1
Максимален брой кредити които са за големи знаци, ако е отрицателно ще е минимален брой главни букви.	ucredit=1
Максимален брой кредити за малки знаци, ако е под 0 ще е минимален брой знаци с малка буква.	lcredit =1
Максимален брой кредити за пунктуационни знаци, под нулата минималният им брой други знаци	ocredit =1
Минимален брой изискани класове от знаци ако сложите 4 ще иска от 4рите	minclass =1
Максималното повторение на еднакви последователни знаци; 0 за да го спрете	maxrepeat =0
Ако искаме да държим потребител от имането на много цифри или букви едни до други = спираме го с 0	maxclassrepeat = 0
Проверка с коментари по дълги от 3 знака в обратна или нормална форма 0 за да го спрем.	gecoscheck=0

cat /etc/security/pwdquality.conf там се намират отгоре изброените.

sudo passwd --expire username ще принуди потребителя да си смени паролата.

!
Става и със:

sudo chage -d 0 username ---> където с -d обявяваме след колко дни - 0 означава веднага като zero day
sudo chage -l username показва всички полици
Лист на полицата за паролата на потребителя

```
  -d, --lastday LAST_DAY       set date of last password change to LAST_DAY
  -E, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -h, --help                   display this help message and exit
  -I, --inactive INACTIVE      set password inactive after expiration
                               to INACTIVE
  -l, --list                   show account aging information
  -m, --mindays MIN_DAYS       set minimum number of days before password
                               change to MIN_DAYS
  -M, --maxdays MAX_DAYS       set maximum number of days before password
                               change to MAX_DAYS
  -R, --root CHROOT_DIR        directory to chroot into
  -W, --warndays WARN_DAYS     set expiration warning days to WARN_DAYS
```

chage -l показва информация за потребителя и необходимостта дали трябва да си смени паролата.

sudo chage -d -1 -I -1 -m 0 -M 99999 -E -1 ivelina безвъзвратно променя всичко по старому.

Тоест връща обикновенни политически настройки на потребителя.

Индивидуални потребителски настройки

usermod

-d, --home <homedir>	Specifies user's home directory
-g <group id> /-u <user id>	Changes primary group or user id
-G <groups>	Specifies supplemental groups
-a	Combined with -G, appends users to supplemental group list
-l <login name>	Change user's login name
-L	Lock account
-U	Unlock account
-s <shell>	Specifies shell

Пример с промяна на потребителско име:

След като във клипа не ми се получи, потърсих правилното решение и се оказа, че имам неправилен синтаксис. Правилният е:

sudo usermod –l newusername oldusername