Felhasználói adminisztráció

Felhasználói adatbázisok

A felhasználók adatainak tárolása többféleképpen történhet:

- Kevés felhasználó esetén szöveges állományban:
  - /etc/passwd
  - /etc/shadow
  - /etc/group
  - /etc/gshadow
- Több felhasználó esetén adatbázis-kiszolgáló használatával
- Nagyméretű hálózat estén pedig központi nyilvántartással

Felhasználók adatai

Felhasználók adatai a /etc/passwd állományban vannak eltárolva. Ebben a szöveges állományban minden sor pontosan egy felhasználó adatait tartalmazza kettőspontokkal elválasztva.

A mezők tartalma:

1) Felhasználói név.
2) Kódolt jelszó helye. Ma már csak egy „x” jelzi a helyét.
3) Felhasználói azonosító (UID).
4) A felhasználó elsődleges csoportja (GID).
5) Egyéb adatok vesszővel elválasztva. (GECOS információk)
6) A felhasználó saját könyvtárának abszolút elérési útja.
7) A felhasználó által használt héjprogram.

Csoportok adatai

Csoportok adatai a /etc/group állományban vannak eltárolva. Ebben a szöveges állományban minden sor pontosan egy csoport adatait tartalmazza kettőspontokkal elválasztva.

A mezők tartalma:

1) A csoport neve.
2) A csoporthoz tartozó jelszó helye. Ma már csak egy „x” jelzi a helyét.
3) A csoport azonosítója (GID).
4) A csoporthoz tartozó felhasználók nevei, vesszővel elválasztva.

Az árnyékjelszó rendszer

A felhasználói adatokat tároló szöveges állományok tartalmát bármely felhasználó megtekintheti. Ezért a felhasználók kódolt jelszavait egy sokkal védettebb állományban, a /etc/shadow-ban tárolja a rendszer.

A mezők jelentése:

1) A felhasználó neve.
2) A kódolt jelszó
3) Az utolsó jelszóváltoztatás napja(1970.január.1-óta eltelt napok számával jelölve).
4) Két jelszóváltoztatás közötti maximális idő napokban.
5) Két jelszóváltoztatás közötti minimális idő napokban.
6) A jelszó lejárata előtt hány nappal kap a felhasználó figyelmeztetést.
7) A jelszó lejárata után hány nappal kerül kitiltásra a felhasználó a rendszerből.

Felhasználók létrehozása

adduser „felhasználónév”

Felhasználók hozzáadására használható egyszerű program. Bejegyzéseket hoz létre a rendszer passwd és group állományaiban. Ezen kívül még létrehozza az új felhasználó könyvtárát is, odamásolja az alapértelmezett konfigurációs állományokat a /etc/skel könyvtárból .

Az adduser.conf fájl tartalma

/etc/adduser.conf

Tartalma:

- Alapértelmezett shell (DSHELL)
- Alapértelmezett home könyvtár (DHOME)
- Csoportosítás a /home-ban (GROUPHOMES)
- Csoportosítás a /home-ban (LETTERHOMES)
- Mintakönyvtár (SKEL)
- Azonosítók tartománya a rendszer szintű és a normál felhasználók számára
- Új felhasználóhoz jöjjön-e létre új csoport (USERGROUPS)
- Alapértelmezett csoport (USERS_GID)
- Új felhasználó könyvtárának jogai (DIR_MODE)
- Egyéb csoportok (EXTRA_GROUPS)
- A felhasználó és a csoportnevek karakterválasztéka(NAME_REGEX)

Felhasználók adatainak megjelenítése

getent <adatbázis> <kulcsszó>

A getent parancs megjeleníti különböző rendszerszintű adatbázisok tartalmát .

```
root@debian:/home/jambor# getent passwd jambor
jambor:x:1000:1000:Jambor Zoltan,,,:/home/jambor:/bin/bash
root@debian:/home/jambor# getent shadow jambor
jambor:$6$QDwg/Wqo$P6mBJvKP8fYgZHT7XHf9GjwHkgu6e29r6D4c92BRoAENYuHfqUEABXnyRAUmm
5SW3udAKnYfZKiyGYAmBgZ9Y.:17070:0:99999:7:::
root@debian:/home/jambor# _
```

Felhasználók létrehozása II.

adduser „felhasználónév”

Kapcsolói:

- --home kvt. A felhasználó saját könyvtárának megadása.
- --ingroup csop. A felhasználó elsődleges csoportja.
- --add_extra_groups A felhasználóhoz hozzáadja az alapértelmezett másodlagos csoportokat.
- --shell héj A felhasználóhoz tartozó parancsértelmező beállítása.
- --gecos felhaszn. egyéb adatok
- --disabled-login új jelszó létrehozásáig nem léphet be a felhasználó (!)
- --disabled-password nem készül jelszó de a belépés -pl. SSH-n keresztül- lehetséges (*)
- --system rendszer szintű felhasználó jön létre. Extra jog nincs.

Felhasználók törlése

deluser „felhasználónév”

Kapcsolói:

--remove-home A parancs a felhasználó saját könyvtárát is törli.

Felhasználó törlése adott csoportból:

deluser <felhasználónév> <csoport név>

Felhasználók adatainak módosítása

usermod „felhasználónév

Kapcsolói:

-d kvt. A felhasználó saját könyvtárának megváltoztatása.
-g csop. A felhasználó elsődleges csoportjának megváltoztatása.
-G csoportok A felhasználó másodlagos csoportjai vesszővel elválasztva.
-l „felhasználónév” Felhasználónév megváltoztatása.
-s héj A felhasználóhoz tartozó parancsértelmező megváltoztatása.

Felhasználó hozzáadása csoporthoz:

adduser <felhasználó név> <csoport>

Csoportok kezelése

addgroup <csoport név> Csoport létrehozása

groupadd <csoport név> Csoport létrehozása

groupdel <csoport név> Csoport törlése

Felhasználó kitiltása a rendszerből

passwd -l <username> ideiglenes kitiltás

passwd -u <username> jelszó újraaktiválása

passwd -d <username> jelszó törlése

passwd -S <username> jelszó állapotának megjelenítése

Felhasználó kitiltása a rendszerből

```
root@debian:/home/p# passwd -l jambor
passwd: password expiry information changed.
root@debian:/home/p# getent shadow jambor
jambor:!$6$QDwg/Wqo$P6mBJvKP8fYgZHT7XHf9GjwHkgu6e29r6D4c92B
m5SW3udAKnYfZKiyGYAmBgZ9Y.:17070:0:99999:7:::
root@debian:/home/p# passwd -S jambor
jambor L 09/26/2016 0 99999 7 -1
root@debian:/home/p# passwd -u jambor
passwd: password expiry information changed.
root@debian:/home/p# getent shadow jambor
jambor:$6$QDwg/Wqo$P6mBJvKP8fYgZHT7XHf9GjwHkgu6e29r6D4c92BR
5SW3udAKnYfZKiyGYAmBgZ9Y.:17070:0:99999:7:::
root@debian:/home/p# passwd -S jambor
jambor P 09/26/2016 0 99999 7 -1
root@debian:/home/p# passwd -d jambor
passwd: password expiry information changed.
root@debian:/home/p# passwd -S jambor
jambor NP 09/26/2016 0 99999 7 -1
root@debian:/home/p# getent shadow jambor
jambor::17070:0:99999:7:::
```

LibreOffice®

open source™

Felhasználói jelszavak kezelése

chage parancs

chage -l <felhasználó név> listázza a felhasználóhoz tartozó jelszó paramétereket.

chage -M <napok száma> <felhasználó név> beállítja a jelszó lejárati idejét, ami után a felhasználónak meg kell azt változtatnia.

chage -E <dátum> <felhasználónév> a megadott dátum (vagy napok száma) után a felhasználó már nem fog tudni hozzáférni a rendszerhez. A -1 értékkel törölhető a beállítás.

chage -I <napok száma> <felhasználó név> inaktivitási idő. Ha a felhasználó nem használja a rendszert. A -1 értékkel törölhető.

Tárolt jelszavak titkosítása

/etc/pam.d/common-passwd (közvetlenül szerkeszthető)

```
password        [success=1 default=ignore]      pam_unix.so obscure sha512
```

/etc/shadow

```
jambor $6$0z5a1OKm$/.ANhzlOL29oWjTl2TOvvpEQLSICB1xyA.U8aSkefvIdmJWtAMIxCjqxhSUtg
Fhdg4RvnEKsX/ODwiaG6umZl0:17097:0:99999:7:::
```

1	MD5	22 karakter
2a	BlowFish	
5	SHA256	43 karakter
6	SHA512	86 karakter

A hash-elés megváltoztatása után ki kell adni a

chage -d 0 <felhasználónév>

parancsot. Ezzel a felhasználót kényszerítjük jelszavának megváltoztatására!

LibreOffice®

open source™

A sudo program

A sudo program segítségével másokra bízhatjuk a rendszerfelügyelet egy részét anélkül, hogy teljes rendszergazdai hozzáférést adnánk.

/etc/sudoers fájl

Szerkeszteni a visudo paranccsal lehetséges. (apt-get install sudo)

A sudo program

```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/
sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

A sudo program

A sudoers sorok formája:

<felhasználó> <gép>= (<felhasználó név>) <parancs>

Magyarázat:

Első oszlop: a sudo felhasználó azonosítója

Második oszlop: gépek amelyeken érvényes a bejegyzés

Harmadik oszlop (zárójelben): az a felhasználó akinek a nevében a sudo parancsot hajthat végre.

Negyedik oszlop: mely parancsokat hajthatja végre a felhasználó

A sudo program

Példák:

root ALL=(ALL:ALL) ALL A rootnak mindent szabad

jambor ALL=(ALL:ALL) /sbin/ifconfig jambor felhasználó megtekintheti az ip paramétereket az interfészeken.

jambor ALL=(ALL:ALL) NOPASSWD: /sbin/ifconfig nem kér jelszót

jambor ALL=(ALL:ALL) NOPASSWD: /usr/bin/apt-get update jambor felhasználó tudja frissíteni a csomaglistákat (jelszó megadása nélkül...)

A sudo program

Példák:

```
# User alias specification
User_Alias APTMASTERS=joska,pista,jambor
# Cmnd alias specification
Cmnd_Alias APT=/usr/bin/apt-get update,/usr/bin/apt-get upgrade,/usr/bin/apt-get
 install *
```

```
jambor  ALL=(ALL:ALL) /sbin/ifconfig
jambor ALL=(ALL) NOPASSWD: /sbin/ifconfig
APTMASTERS ALL=(ALL:ALL) NOPASSWD: APT
```

A felhasználói quóta EXT4 fájlrendszereken

A quóta segítségével szabályozhatjuk, hogy a felhasználók mekkora tárterületet használhatnak maximálisan adataik tárolására.

Ext4 fájlrendszert alkamazó rendszereken ez a következőképp működik:

1) A rendszermag minden írási művelet előtt ellenőrzi a felhasználó számára rendelkezésre álló tárterületet a nyilvántartásból.
2) Ha az íráshoz szükséges lemezterület nem áll rendelkezésre, a művelet hibaüzenettel leáll.
3) Ha rendelkezésre áll a megfelelő lemezterület, az írási művelet végrehajtásra kerül.
4) A rendszermag az újonnan felhasznált lemezterülettel frissíti a nyilvántartást.

A felhasználói quóta EXT4 fájlrendszereken

Lemezkorlátot a rendszer minden partíciójára külön-külön létre kell hozni (vagy csak arra amelyikre akarjuk...).

Az előzőekben említett nyilvántartás valójában két állomány, amit célszerű az adott partíció gyökerében elhelyezni (csatolási pont).

Alapesetben a rendszerpartíció (/) gyökerében el kell helyezni egy aquota.user és egy aquota.group állományokat. Mindezeket meg kell ismételi a felhasználói fiókokat tartalmazó partíción is (/home).

Az imént létrehozott állományok a felhasználók és a csoportok lemezhasználatát tartalmazzák. A fenti állományok jogait 600 jogosultságra kell állítani. Tulajdonos természetesen a root.

A quóta kezdeti beállítása

Quóta használatához az adott partíció(ka)t a megfelelő módon kell beilleszteni a rendszerbe. Ehhez a /etc/fstab állományt a megfelelő módon kell módosítani.

```
root@debian:~# cat /etc/fstab
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/sda2 during installation
UUID=12ff5993-3268-43e6-addc-ad165a9e6e7a /               ext4    errors=remount
-ro,usrquota,grpquota 0       1
# /home was on /dev/sda3 during installation
UUID=9716f12f-d23f-4093-812b-9c041c03a009 /home           ext4    defaults,usrqu
ota,grpquota        0       2
# swap was on /dev/sda1 during installation
UUID=e29fddaa-772b-4971-b21a-86c29f08d47b none            swap    sw
  0       0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0
```

A quóta beállítása

Szükséges telepíteni a quota csomagot:

apt-get install quota

A quotacheck paranccsal a nyilvántartás ellenőrzését, javítását, és előkészítését tudjuk elvégezni.

Kapcsolói:

- -v Folyamatosan kiírja hol tart a munkában.
- -u Csak felhasználói lemezkorlát kezelése.
- -g Csak csoport lemezkorlát kezelése.
- -c Ne foglalkozzon a meglévő nyilvántartással.
- -M Írásra beillesztett állományrendszer kezelése.

Példa : quotacheck -c -M /home

A quóta beállítása

A lemezkorlát figyelésének és nyilvántartásának bekapcsolására a quotaon parancs szolgál. Kikapcsolás a quotaoff paranccsal történik.

A quotaon kapcsolói:

-u A felhasználókra vonatkozó korlát bekapcsolása.

-g A csoportokra vonatkozó korlát bekapcsolása.

-p A lemezkorlát állapotának kiíratása.

-f A lemezkorlát kikapcsolása.

Példa: quotaon -p /

Lemezkorlát felhasználóhoz rendelése

A felhasználókhoz történő lemezquóta beállítására az edquota parancs szolgál. Példa: edquota diak

A parancs után az adott felhasználó nevét kell megadni. Ezek után megnyílik egy állomány amit szerkeszteni lehet. Az állomány sorai a quóta használatára engedélyezett partíciókat tartalmazzák.

Hat oszlopa van. Első három a blocks (blokkok) jelenlegi állását valamint a soft és hard limitjeit tartalmazzák, a második három a csomópontokra (inodes) vonatkozó hasonló információkat tartalmazzák.

A soft limit átléphető a hard limit nem. A blokkok mérete 1 kB.

Mintafelhasználó használata lemezkorlát beállításához

Sok felhasználó esetén macerás lehet a beállítás ezért lehetőség van egy felhasználó quótájának beállításait mintaként használni akár script segítségével is.

Erre a műveletre a setquota parancs szolgál.

Kapcsolói:

- -u felhasználó lemezkorlátjának beállítása.
- -g Csoport lemezkorlátjának beállítása.
- -p felh Felhasználó mintaként való használata.

Példa:

```
setquota -p mintafelhasznalo felhasznalo /home
```

Lemezkorlát ellenőrzése

Adott felhasználó lemezkorlátjának ellenőrzésére a quota parancs szolgál.

Kapcsolói:

- -g Felhasználói csoport ellenőrzése.
- -q Azon felhasználók kilistázása akik átlépték a soft limitet.

Példa: quota diak

Jelentést a lemezkorlát állásáról a repquota parancsal kaphatunk.

Példa: repquota -s /home

A türelmi időt az edquota -t paranccsal tudjuk megváltoztatni szerkesztéssel.

LibreOffice®

open source™