

Dr. Mileff Péter

# UNIX/LINUX OPERÁCIÓS RENDSZER ÜZEMELTETÉSE

6. ELŐADÁS

Miskolci Egyetem  
Általános Informatikai Tanszék

## Felhasználók adminisztrációja...

## A felhasználó törlése

- A felhasználó törlése kézzel:
  - Törölni kell a felhasználó bejegyzését az `/etc/passwd` állományból,
  - shadow jelszó használata esetén az `/etc/shadow` állományból is.
  - Ha az `/etc/group` állomány tartalmaz rá vonatkozó bejegyzéseket, akkor azt is el kell távolítanunk.
- Ezzel a felhasználó megszűnt létezni, de
  - azonban még további állományai lehetnek a rendszerben.
  - Alapértelmezett esetben a home jegyzék tartalma, és a levelesládája (általában `/var/spool/mail/<login név>`).
- Automatikus törlés:
  - A `userdel` parancs segítségével.
    - `(userdel -r <login név>)`

## Felhasználó váltás

- Van lehetőség a felhasználók közötti váltásra is.
- Ezt az `su` paranccsal tehetjük meg:

**su - (felhasználónév)**

- Példa: `# su - superman`
- Amennyiben a rendszergazda felhasználóra szeretnénk váltani:
  - akkor elég az `su` parancsot önmagában alkalmazni paraméter nélkül.
  - Mindkét esetben a rendszer kéri a váltani kívánt user kódját.

## Felhasználók tulajdonságainak megváltoztatása

- Bármely felhasználó tulajdonságai megváltoztathatók.
  - A root vagy a user által.
- **1. A héj megváltoztatása:** beállítható, hogy a belépés után melyik héj induljon el a user számára.
  - **Parancs:** `chsh` (*change shell*)
- Körültekintőnek kell lennünk a héjprogram megválasztásakor
  - Ha olyan héjat választunk, amely nem létezik, vagy nem működik megfelelően, akkor kizárhatjuk magunkat a rendszerből.
  - A chsh program segít nekünk ebben.

5

## Felhasználók tulajdonságainak megváltoztatása

- Mielőtt megváltoztatná a beállítást:
  - a chsh ellenőrzi, hogy létezik-e a program, amelyet héjként használni akarunk,
  - és azt is megvizsgálja, hogy szerepel-e a `/etc/shells` állományban.
  - Csak olyan programokat állíthatnak be, amelyek szerepelnek a `/etc/shells` állományban.
- **Példa:**

```
# chsh -s /bin/csh
Changing shell for luke.
Password:
Shell changed.
```

6

## Felhasználók tulajdonságainak megváltoztatása

- A root bármely felhasználó héjprogramját beállíthatja.
- Ez lehetőséget teremt arra is, hogy az interaktív hozzáférést megtiltsa a felhasználó számára.
  - Ha olyan héjprogramot állít be, ami nem működik héjként, a felhasználó nem tud parancsokat kiadni, nem tud a számítógépre bejelentkezni.
- **Az interaktív bejelentkezés tiltására általában a `/sbin/nologin` programot szokás használni.**
  - Ha ezt állítjuk be a user számára, akkor nem tud bejelentkezni.
- Egyéb szolgáltatásokat elérhet:
  - Pl.: ftp használat, levelek olvasása, stb.

7

## Felhasználók tulajdonságainak megváltoztatása

- Példa az interaktív bejelentkezés letiltására:
 

```
# chsh -s /bin/nologin
Changing shell for luke.
Shell changed.
```

8

## Felhasználók tulajdonságainak megváltoztatása

### 2. Személyes adatok megváltoztatása:

- Program: **chfn**
  - Megváltoztatja a user személyes adatait
  - (név, munkahelyi szobaszám, munkahelyi telefonszám és otthoni telefonszám).
- A rendszergazda bármely user személyes adatait megváltoztathatja

chfn [kapcs.] [felhnev]

*Kapcsoló*

*Jelentés*

-f név

A felhasználó nevének megváltoztatása

-o iroda

A felhasználó irodájának megváltoztatása.

-w telefon

A felhasználó irodai telefonszámának megváltoztatása.

-h telefon

A felhasználó otthoni telefonszámának megváltoztatása.

9

## Felhasználók tulajdonságainak megváltoztatása

### 3. Egyéb adatok megváltoztatása:

- Parancs: **usermod**
- Használat:** a felhasználó saját jegyzékének, elsődleges csoportjának és néhány egyéb adatának megváltoztatása.

usermod [kapcs.] felhnev

- Példa: # usermod -g (csoport) felhasználó

10

## Csoportok adminisztrációja

- A csoportok adminisztrálására hasonló segédprogramok.
- Pl.: a **groupadd**, **groupdel**, **groupmod**
  - új csoportok létrehozása, illetve törlése.
- Rendszer-csoportok létrehozása:
  - groupadd -r** kapcsolóval
- Jelentése:**
  - a group azonosító kisebb lesz a normál azonosítóknál.

11

## /etc/passwd fájl

- A Unix/Linux rendszerek alapvető felhasználói adatbázisa a **/etc/passwd**.
  - szöveges fájl, jelszófájlnek nevezik.
  - Felsorolja az összes érvényes felhasználói nevet és a hozzájuk kapcsolt információkat.
- Felépítése:**
  - minden felhasználói névhez egy sor tartozik,
  - és 7, kettősponttal elválasztott mezőre oszlik.

12

## /etc/passwd fájl

- ⊙ 1. Felhasználói név (username).
- ⊙ 2. Titkosított jelszó.
- ⊙ 3. Felhasználói azonosító szám (uid).
- ⊙ 4. Csoportazonosító szám (gid).
- ⊙ 5. Teljes név, vagy egyéb leírás.
- ⊙ 6. Home jegyzék.
- ⊙ 7. Bejelentkezési burok (login shell), azaz a bejelentkezéskor futtatandó program.

### Példa:

```
root:HhziK643GFhujMM:0:0:Rendszergazda:/root:/bin/bash
```

```
luke:K3xcO1Qnx8LFN:2332:1999:LukeSkywalker:/home/luke:/usr/local/bin/bash
```

13

## /etc/passwd fájl

- ⊙ A rendszer minden felhasználója olvashatja a jelszófájlt,
  - így pl. megismerhetik a többi felhasználó nevét.
  - még a jelszó is mindenki számára elérhető.
    - De csak egy titkosított változata.
- ⊙ Azonban a titkosítás feltörhető
  - különösen gyenge jelszavak esetén.
  - Ezért nem jó ötlet, hogy itt vannak a titkosított jelszavak.
- ⊙ Sok Linux rendszer rendelkezik az árnyék jelszó (shadow password) lehetőségével:
  - a titkosított jelszó ekkor egy külön fájlban, a **/etc/shadow**-ban van, melyet csak a root olvashat.

14

## /etc/shadow fájl

- ⊙ Ekkor a /etc/passwd fájl csak egy speciális jelet tartalmaz a második mezőben.
- ⊙ Minden program, amely egy felhasználót azonosít, el kell érje az árnyék jelszófájlt.
  - A szokásos programok elérhetnek a jelszón kívül minden információt az eredeti jelszófájlból, de magát a jelszót nem.
- ⊙ Felépítése: az /etc/passwd file-hoz hasonlóan:
  - ez is egy egyszerű szöveges állomány,
  - mindegyik felhasználó egy sort foglal el.
  - Itt is kettőspont választja el az adatmezőket.

15

## Árnyék jelszó példa

- ⊙ Árnyék fájl esetén a korábbi passwd bejegyzés a következőre módosul:

```
root:x:0:0:Rendszergazda:/root:/bin/bash
luke:x:2332:1999:Luke Skywalker:/home/luke:/usr/local/bin/bash
```

### Az /etc/shadow tartalma ekkor:

```
root:$1$q59x0VBc9KL$J:14435:0:Rendszergazda::::
luke:$6$2j6Geq78PU$Hdj1FVC:14437:1999:0::::37:
```

16

## Bejelentkezés a rendszerbe...

17

## Általános áttekintés

- ◉ Egy felhasználó többféleképpen is bejelentkezhet:
  - A legegyszerűbb eset:
    - a számítógép előtt ülve valamelyik karakteres munkafelületen gépelik be a felhasználói nevüket és a jelszavukat.
  - A felhasználók bejelentkezhetnek grafikus felületen is.
  - A bejelentkezés történhet számítógép-hálózaton keresztül is.
- ◉ A Unix rendszerek bejelentkezési folyamata többé-kevésbé megegyezik
  - a bejelentkezés általában hasonlóképpen megy végbe minden UNIX/Linux rendszeren.

18

## A klasszikus bejelentkezés folyamata...

19

## Üzenetek a bejelentkezéskor

- ◉ A bejelentkezés előtt a **/etc/issue** állomány tartalmát írja ki a rendszer a helyi képernyőre.
- ◉ Távoli bejelentkezés esetén:
  - a felhasználó képernyőjén a **/etc/issue.net** állomány tartalma jelenik meg.
- ◉ **Céljuk:** a rendszergazda a bejelentkezéshez szükséges információk kiírására használhatja.
- ◉ /etc/issue.net állományban:
  - gyakran helyeznek el a számítógépre, a rajta található operációs rendszerre vonatkozó információkat.
  - biztonsági szempontból nem szerencsés
    - mert így a támadó információkat szerezhet a számítógépen futtatott szoftverrendszerrel.

20

## Üzenetek a bejelentkezéskor

- ◉ Továbbá, a **/etc/motd** állomány tartalma a sikeres bejelentkezés után jelenik meg
  - akkor, amikor a felhasználói hitelesítés megtörtént.
- ◉ A rendszerre jellemző információkat inkább ebbe az állományba tesszük,
  - Mert csak azok látják, akik érvényes névvel és jelszóval rendelkeznek.
- ◉ A misztikus MOTD rövidítés mögött a „napi hír” (*message of the day*) kifejezés áll.

21

## Na és hogyan történik a beléptetés?

- ◉ A felhasználó beléptetését Unix rendszereken a **login program** végzi.
  - Az, hogy mi indítja a login programot, az egyes Unix/Linux rendszereken változó.
- ◉ A login fő feladatai:
  - a felhasználó azonosítása
  - és a felhasználó alapértelmezett héjprogramjának elindítása az azonosítás után.

22

## Na és hogyan történik a beléptetés?

- ◉ A login ezt a feladatot a következő lépések elvégzésével látja el:
- ◉ **1.** Ha a login program indulásakor még nem ismert a felhasználó felhasználói neve, a login megkérdezi.
- ◉ **2.** Ha az adott felhasználó bejelentkezése jelszóhoz kötött, a login megkérdezi a jelszót.
  - A jelszó begépelésekor a képernyőn *semmi* nem jelenik meg,
  - hogy ne lehessen kikélni a jelszót és azt sem, hogy az hány karakterből áll.

23

## Na és hogyan történik a beléptetés?

- ◉ **3.** Ha a bejelentkezés minden feltétele adott,
  - a login elindítja az azonosított felhasználó alapértelmezett héjprogramját.
  - A héjprogram elindítását a program úgy végzi, hogy az már az azonosított felhasználó nevében fusson, az azonosított felhasználó jogaival rendelkezzen.
- ◉ **4.** Ezek után a login vár, amíg a héj fut.
  - Amikor a felhasználó kilép a héjból, a login is kilép, hogy az őt indító program tudja, új felhasználó jelentkezhet be.

24

## Na és hogyan történik a beléptetés?

- A login a Unix rendszereken néhány apró feladatot is elvégez:
  - ha a **/etc/nologin** állomány létezik, akkor csak a rendszergazda léphet be.
  - Minden más felhasználó belépési kérelmét elutasítja a login,
  - az elutasítást a **/etc/nologin** tartalmának kiírásával jelezve.
  - Ha tiltás okát egyszerűen bele kell írni.

- **Példa:**

```
# echo "Karbantartás miatt a szerver nem üzemel!" > etc/nologin
```

25

## Na és hogyan történik a beléptetés?

- A login bejelentkezéskor megvizsgálja:
  - a **/var/spool/mail/** jegyzékben van-e a felhasználó felhasználói nevével megegyező nevű állomány.
  - Ha igen, akkor az 0 hosszúságú-e?
  - Ha nem 0 a hossza az állománynak, akkor kiírja a képernyőre, hogy a felhasználónak olvasatlan levele van.
- A levéltovábbító alrendszer a beérkezett elektronikus leveleket a **/var/spool/mail/** jegyzékben tárolja.
  - minden felhasználó számára egy állomány van fenntartva.
  - A levelezőprogram az olvasott elektronikus leveleket eltávolítja innen, így ha az állomány nem üres, a felhasználónak olvasatlan levele van.

26

## Na és hogyan történik a beléptetés?

- **Csendes login:**

- Ha a felhasználó a **.hushlogin** (*hush*, csendes, nyugodt) rejtett állományt elhelyezi a saját könyvtárában,
- akkor a belépéskor a login nem ellenőrzi a levelesládát,
- és nem írja ki az utolsó belépés időpontját.

27

## Na és hogyan történik a beléptetés?

- A login következő feladata a **bejelentkezés naplózása**.
  - A Unix rendszerek a **/var/log/wtmp** és **/var/log/utmp** állományokban rögzítik a felhasználók bejelentkezéseit,
  - így a login is ezekben az állományokban rögzíti a bejelentkezéseket és a kilépéseket.
  - A **w** és a **who** programok is ezt a nyilvántartást használják a pillanatnyilag belépett felhasználók listájának kiírására.

28

## Na és hogyan történik a beléptetés?

- A login szerencsés esetben túljutva ezeken az adminisztratív feladatokon:
  - elindítja a felhasználó héj programját,
  - azaz kiolvassa a felhasználói nyilvántartásból, hogy milyen héjat használ a felhasználó, és elindítja azt.
- Bonyolult:
  - sajnos héj indítása korántsem egyszerű folyamat.
  - Tovább bonyolítja a helyzetet az, hogy UNIX rendszereken sokféle héj létezik és ezek viselkedése már induláskor különbözhet.

29

## A héj indulása...

30

## A héj indulása

- A Linux rendszerekben a legelterjedtebb héj a BASH héj.
  - Sok felhasználónak a BASH az alapértelmezett héjprogramja.
- A BASH alapjában véve **három üzemmóddal rendelkezik**, háromféleképpen indulhat el:
  - **1. Beléptető héj üzemmód (login shell mode):**
    - ez az üzemmód kimondottan a belépéskor való indításra készült erőforrás-takarékossági okokból; akkor szokásos használni, amikor a felhasználó belépésekor alapértelmezett héjként indul a BASH.

31

Köszönöm a figyelmet!

32