Központi azonosítás lehetőségei

Mátó Péter <atya@fsf.hu>

Néhány alapvető fogalom

- Hozzáférés vezérlés – Access Control
- Azonosítás - Idetify
- Hitelesítés - Authentication
- Feljogosítás – Authorization

Azonosítási módszerek

- Tud valamit - jelszó, PIN...
- Van valamije - csipkártya, telefon...
- Valami ő maga - retina, ujjlenyomat, aláírás...

Több faktoros azonosítás

- Egy módszer, több faktor – csipkártya
- Egymás után több azonosítás

Modern jogosultság kezelés

- Ezen a területen van még mit behozni a szabad szoftver rendszereknek
- Csoport vagy szerepkör alapú
- Központilag kezelt felhasználók
- Jogosultságok központi elosztása
  - Általában szerepkör alapján
  - Kényelmes és hatékony

Egy kis történelem

- Kezdetben vala a passwd
- Aztán jövé a shadow
- Node, minden alkalmazásba külön-külön be kellett építeni
  - felesleges plusz munka
  - felesleges hibalehetőség
  - hibák!
- És akkor eljövé a PAM maga

PAM - Pluggable authentication modules

- moduláris – kényelmes fejlesztés
- rugalmas – könnyen adoptálható
- egységes – minden alrendszer ugyanúgy használja, konfigurálja
- átlátszó – a felhasználó nem veszi észre
- sokrétű – nagyon sok alkalmazást és azonosítási módszert támogat

Központi AA előnyei

- Kényelmesebb használat, egy jelszó
- Bármely megadott munkaállomás használható
- Minden gép előtt ugyanazt kapja a felhasználó

Központi AA veszélyei

- A jelszó megszerzése mindenhová bejuttathatja a támadót
- Nem titkosított protokollok (ftp, pop3...)

Hálózati AA módszerei

- Hálózati hitelesítési módszerek
  - Kerberos - SSO
  - LDAP/LDAPS
- Hálózati feljogosítási módszerek
  - LDAP/LDAPS
- Hálózati adatbázisok
  - NSS LDAP

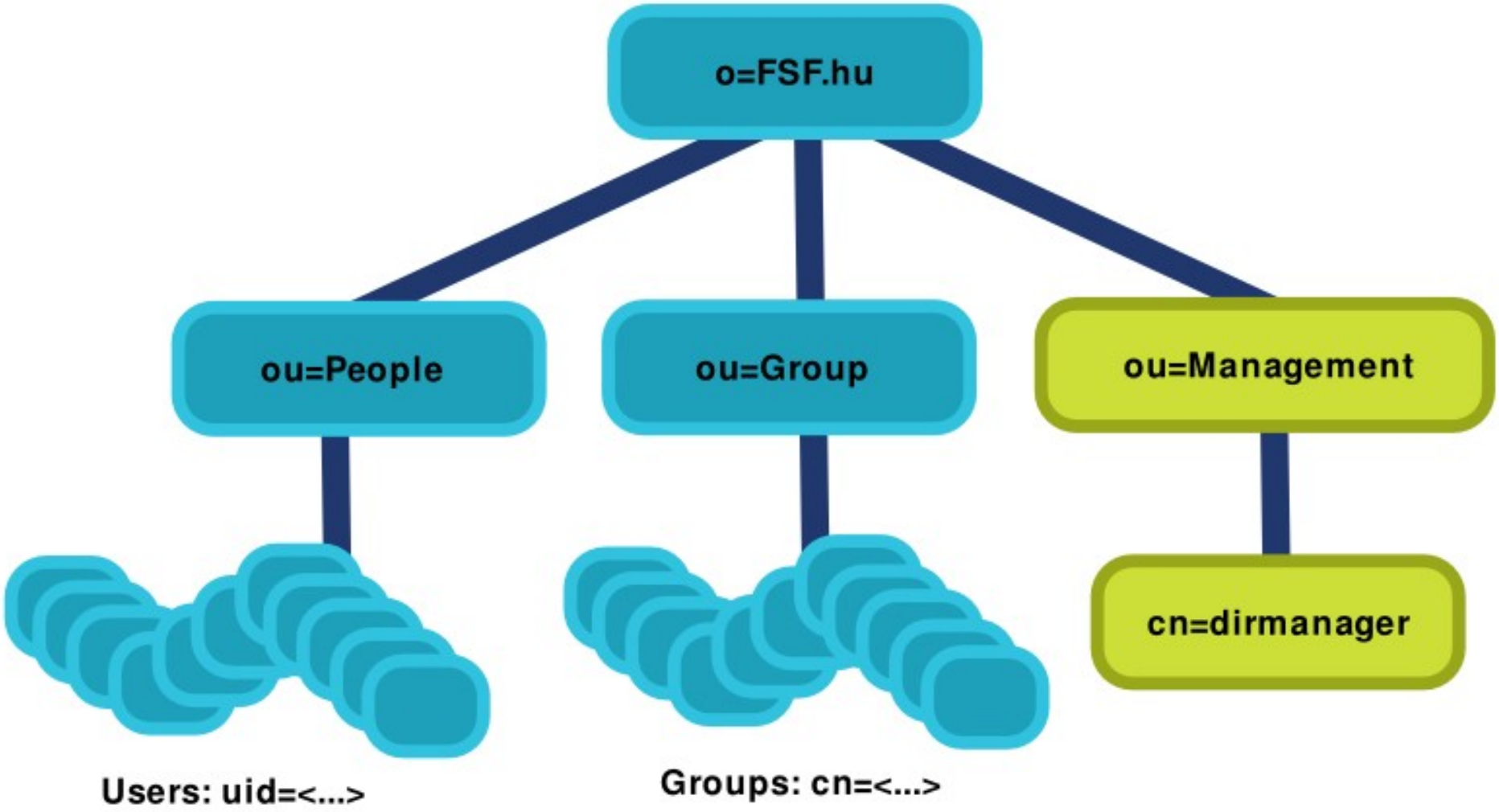
Felhasználás feltételei

- PAM támogatás szükséges
- Vagy közvetlenül be kell építeni a rendszerbe a Kerberos/LDAP támogatást
- Eltér az alapértelmezettől, így bonyolítja a rendszerek adminisztrációját
- A felhasználó adminisztrációs eszközök általában még nem támogatják

Az LDAP-ban tárolt információk

- A felhasználó adatai – posixAccount, shadowAccount objektumban
- A felhasználó jelszava - userPassword attribútumban
- A csoportok adatai - posixGroup objektumban

Az LDAP fa felépítése



A posixAccount osztály

```
dn: uid=atya,ou=People,o=FSF.hu
uid: atya
cn: Peter MATO
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
userPassword: {SSHA}4Tz5EVerD6RNggLSG37dbdUNqSINXvcW
shadowLastChange: 11226
shadowMax: 99999
shadowWarning: 7
shadowFlag: 134538484
loginShell: /bin/bash
uidNumber: 1492
gidNumber: 200
homeDirectory: /home/atya
gecos: Peter MATO
```

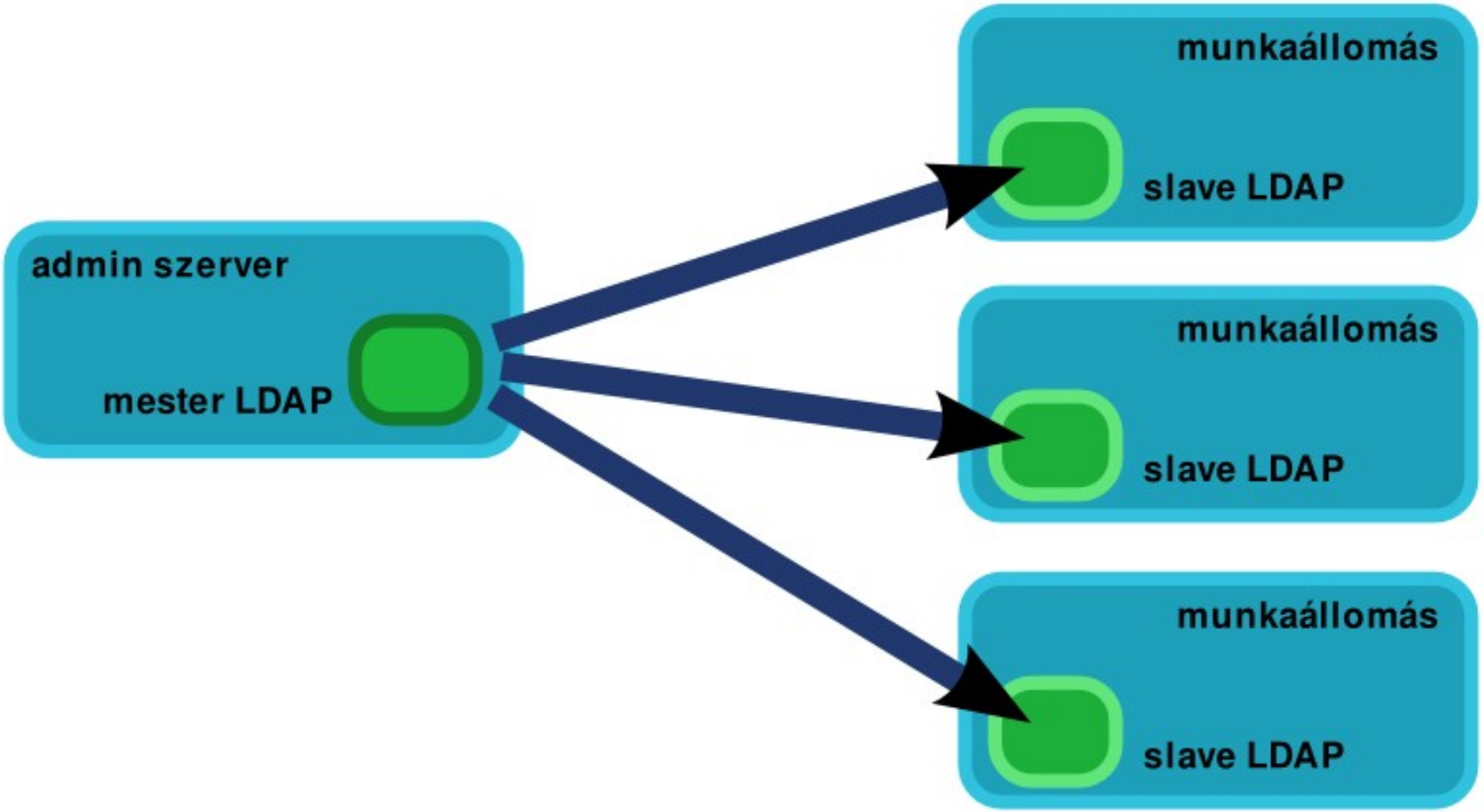
A posixGroup osztály

```
dn: cn=users,ou=Group,o=FSF.hu
objectClass: top
objectClass: posixGroup
cn: admins
gidNumber: 200
```

Az OpenLDAP beállításai

- rootdn, rootpw tilos!
- include nis.schema
- Óvatos jogosultság beállítások
- Legalább egy replika, de megbízható környezetben szerencsésebb mindenhová
- A replikákat rendszeresen ellenőrizni kell
- Rendszeres mentés

Az LDAP szerverek elosztott működése



Felhasználók migrációja

- migrationtools használatával
- Felhasználók adminisztrációja
  - jelenleg kézi munkát igényel
  - használható LDAP böngésző
  - írhatunk adminisztrációs scripteket

Fájl szervíz

- Felhasználók saját adatai
  - Egyben felcsatoljuk automatikusan
  - Belépéskor csatolódik - pam_mount
  - Samba LDAP hiteletsítéssel
- Csoport alapon hozzáférhető könyvtárak

Lehetőségek, tippek

- Fél-vékony kliensek
  - a rendszer a helyi diszken
  - adatok hálózati fájlrendszeren
- Központi konfiguráció kezelés
- Központi frissítéskezelés
- Központi mentési rendszer

Köszönöm a figyelmet