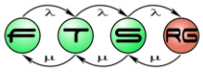
Intelligens rendszerfelügyelet

Címtár szolgáltatások

Szatmári Zoltán
Tóth Dániel



Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

Utolsó módosítás: 2011. 03. 09. by Zee

Előző és következő részek tartalmából

- Modellezés
- Felhasználókezelés
  - Alapjai, hitelesítés (OPRE)
  - Engedélyezés (OPRE)
  - **Központosított felhasználókezelés, címtárak**

Tartalom

- **A felhasználókezelés nehézségei**
- Címtár szolgáltatások
  - LDAP
  - Active Directory

DEMO Felhasználókezelés nehézségei

- Sok rendszer
- Sok felhasználó (minden rendszeren külön-külön)
- Kitör a káosz
  - Elburjánzó felhasználói fiókok
  - Szétszinkronizálódó jelszavak
  - Webes alkalmazásnak, VPN-nek is kéne beléptetés, teljesen más rendszert használnak…

VPN, SSH, WP, Accounts, DNS

Megoldások a káoszra

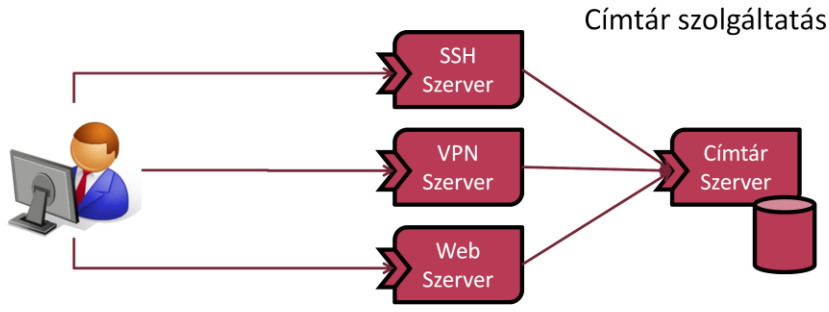
- Elburjánzó felhasználói fiókok
  → felhasználói életciklus kezelésére eljárásrend
- Sok rendszer igényel hitelesítést
  → **központosított felhasználói adattár**

Címtár (directory) szolgáltatás

- Definíció:
  - nyilvános adattár
  - „intelligens” címjegyzék (phone directory)
- Tárolt adatok
  - felhasználó adatai (e-mail címek, különböző fajta nevek, azonosítók, ...)
  - számítógépek adatai
  - biztonsági információk
  - bármi egyéb

Címtár szolgáltatás hitelesítésre

Hogy fogja ez megoldani a hitelesítést?



Beléptetés *minden esetben* a címtárban tárolt felhasználói adatok lekérdezésével történik.

Hogy néz ki egy címtár?

- Speciális adatbázis struktúra
  - szigorúan hierarchikus (általában objektum-orientált)
- Domináns műveletek:
  - keresés
  - olvasás
  - batch jellegű hozzáadás / módosítás

User
+ ID + Name + Real Name + Personal data… + Shared Secret (Password, etc.) + Private Datastore path

Címtárak fejlődéstörténete

- DNS (Domain Name Service)
- NIS (Network Information System)
  - volt Sun Yellow Pages (Sun Microsystems, 1988, SunOS 4.0)
- A korszerűbbek
  - X.500 / LDAP
  - Active Directory

Tartalom

- A felhasználókezelés nehézségei
- Címtár szolgáltatások
  - **LDAP**
  - Active Directory

Lightweight Directory Access Protocol (LDAP)

Kibocsátó: Internet Engineering Task Force (IETF)
Legutóbbi verzió: LDAPv3 – RFC 4510, 2006
Cél: elosztott címtárszolgáltatások megvalósítása, elérése

X.500

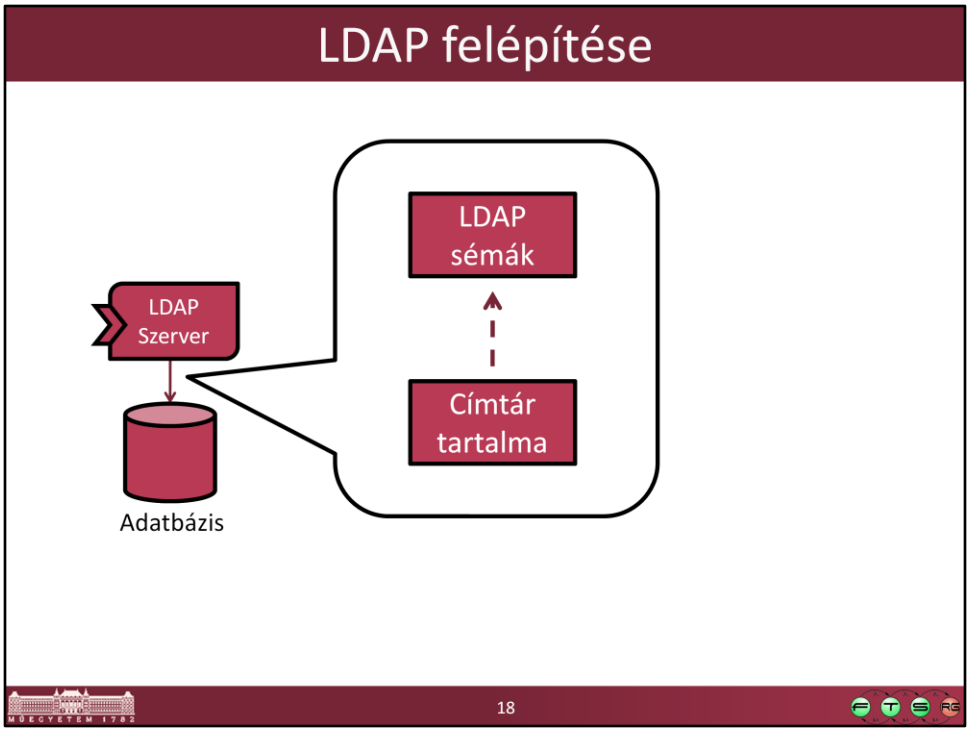
- ISO/OSI X.500 egy szabványcsalád
  - Eredetileg X.400-as levelezés támogatására
- Alapfogalmak: X.500
  - Modellek: X.501
  - Hitelesítés: X.509 (Tovább él az SSL certificate-ekben)
  - Attribútumok: X.520
  - Osztályok: X.521
  - Elérési protokoll: X.519
- Ennek része a DAP (Directory Access Protocol)
  - Az ISO/OSI hálózati szolgáltatásokra épül → TCP/IP-re nem jó!
  - Az IETF kézbe vette a dolgot → Ebből lett az LDAP

LDAP

- **LDAP**: **L**ightweight **D**irectory **A**ccess **P**rotocol
- **L**, mint pehelysúlyú: az X.500 kódnevű protokollcsalád könnyített változata.
- **D**, mint címtárszolgáltatás: elsősorban egy számítógépes hálózat felhasználóit és erőforrásait tartalmazó adatbázis közvetítésére szolgál
- **A**, mint elérés: támogatja az adatok frissítését, törlését, beszúrását és lekérdezését
- **P**, mint az elektronikus kommunikáció egyik nyelve: egy TCP/IP felett megvalósított bináris protokoll

Alaptulajdonságok és fogalmak

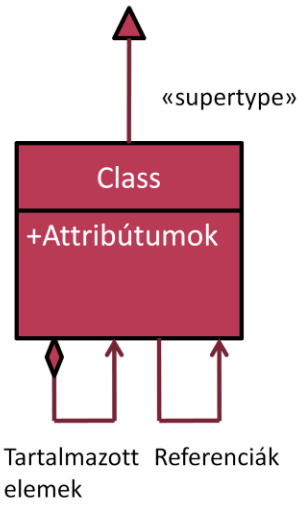
- Hierarchikus felépítés (**directory tree**)
- Csomópontok, bejegyzések (**entries**)
- Objektum-orientált szemlélet
- Kitüntetett attribútum
  (**relative distinguished name - rdn**)
- Megkülönböztető név (**distinguished name - dn**)
- Többértékű attribútumok



Séma: metamodellje a tárolt adatoknak

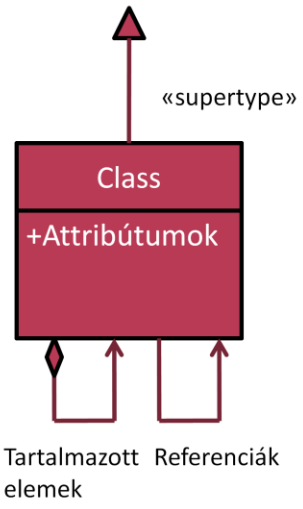
Ez határozza meg, hogy milyen típusú adatokat tárolunk benne és azok között milyen kapcsolat lehet.

LDAP séma



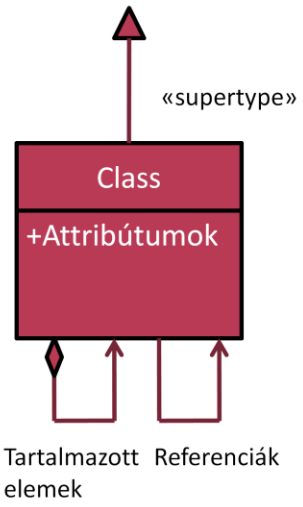
- Statikus
  - Működés közben nem változik
  - Konfigurációs fájlokban adják meg (ASN.1 formátumban)
- Szabványos
  - Van számos többé-kevésbe de facto szabvány séma
  - Pl. core, cosine (X.500), java, nis, inetorgperson

LDAP séma



- Minden elemnek van egy azonosítója (OID)
  - osztálynak és attribútumnak is
    - Pl.: inetOrgPerson 2.16.840.1.113730.3.2.2
  - álnevek használata
    - Pl.: uid és userid
- Van öröklés az osztályok között
- Attribútumok
  - lehetnek kötelezőek, opcionálisak,
  - van multiplicitásuk is (lista)
- A referenciák valójában string attribútumok (hogy lehet ez?)

LDAP séma

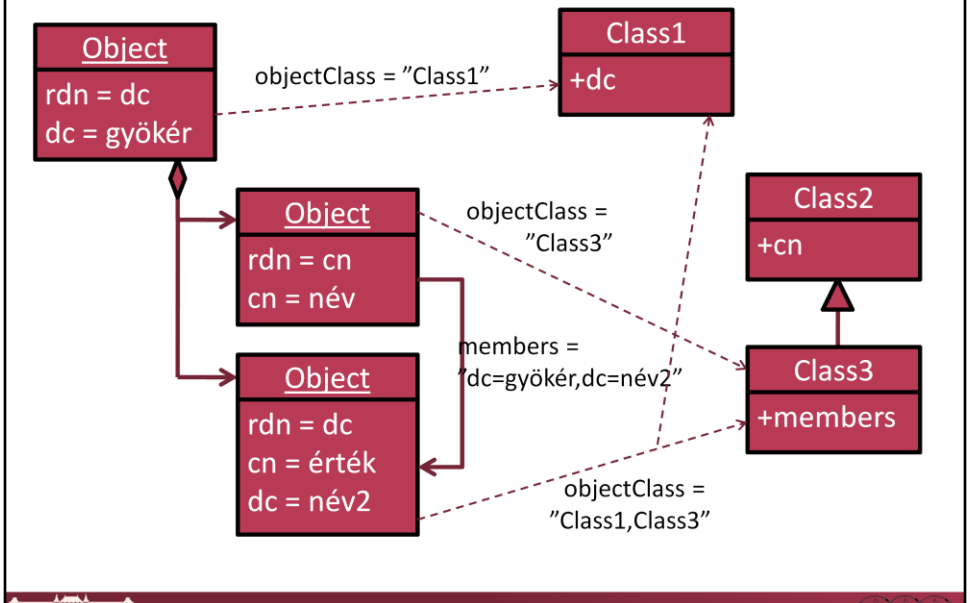


- Osztályok típusai
  - Absztrakt
    - Alapvető struktúra kialakítása
    - A felhasználó számára nincs releváns információja.
    - Pl.: top
  - Strukturális
    - Alapvető tulajdonságokat ad meg
    - Egymást kizáró osztályok
    - Pl.: person és group
  - Kiegészítő
    - Egyes sémák kiegészítésére
    - Pl.: inetOrgPerson, PosixAccount

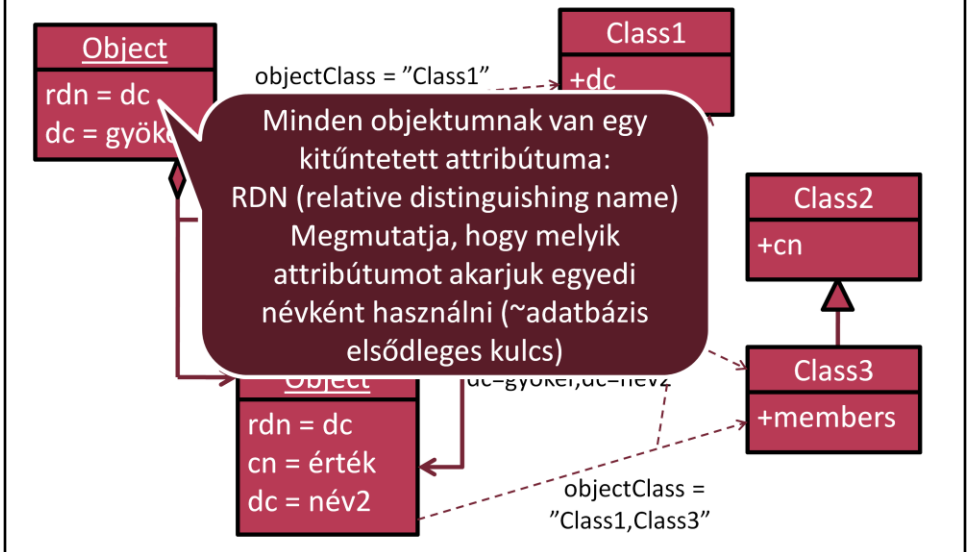
Példa osztály: Person

```
objectclass ( 2.5.6.6 NAME 'person'
        DESC 'RFC2256: a person'
        SUP top STRUCTURAL
        MUST ( sn $ cn )
        MAY ( userPassword $
            telephoneNumber $
            seeAlso $
            description )
)
```

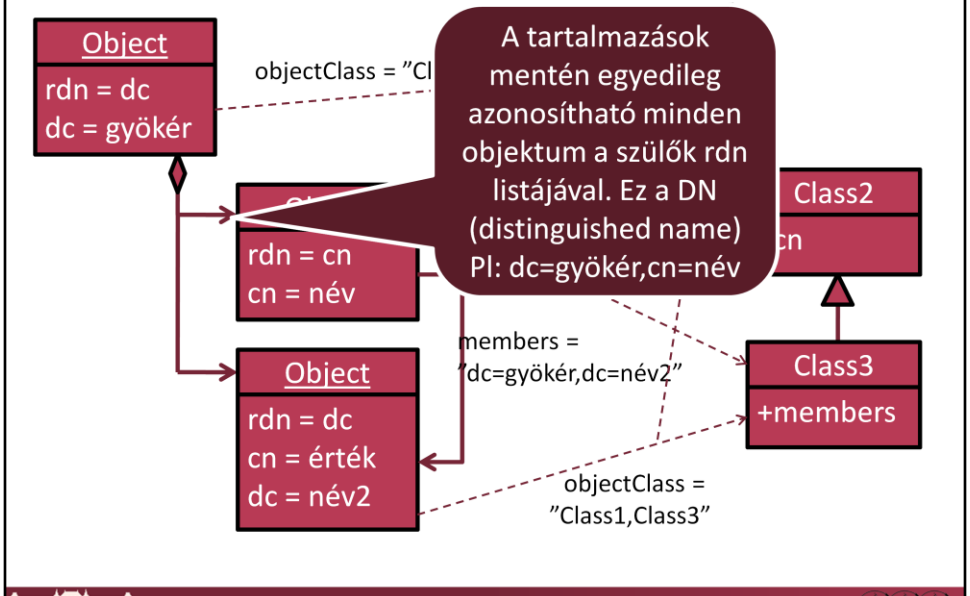
LDAP objektumok



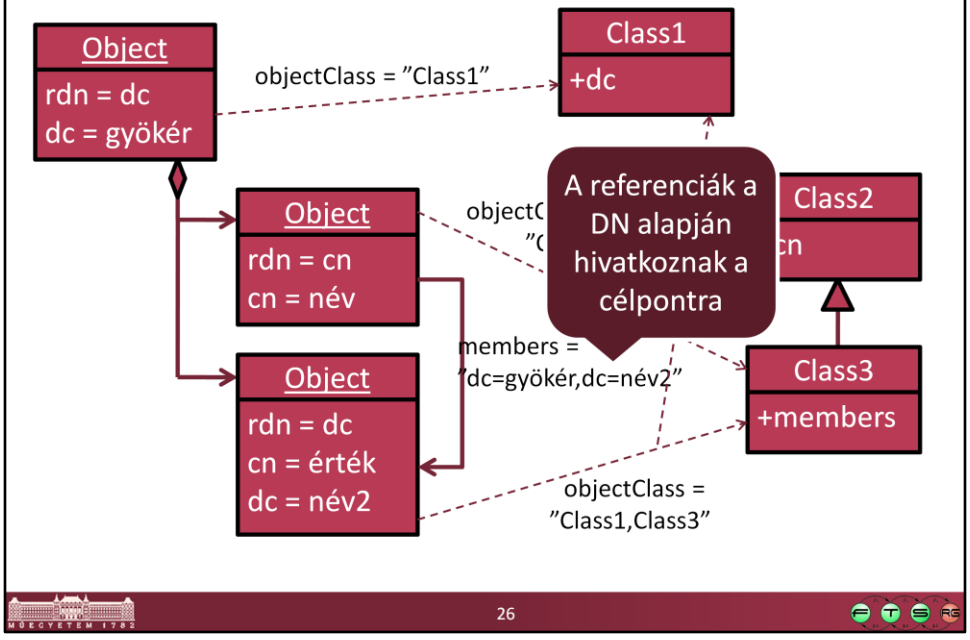
LDAP objektumok



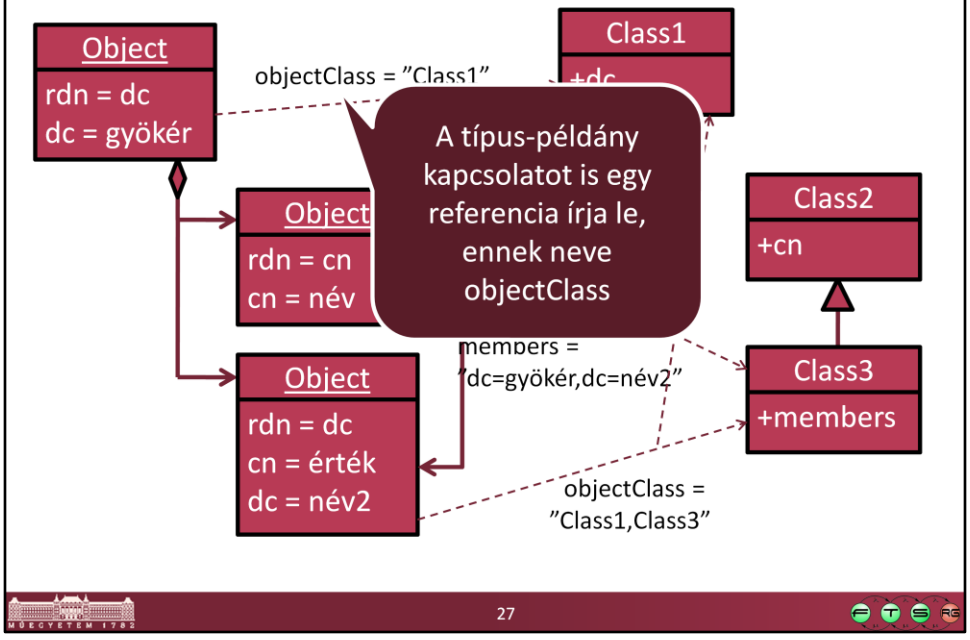
LDAP objektumok



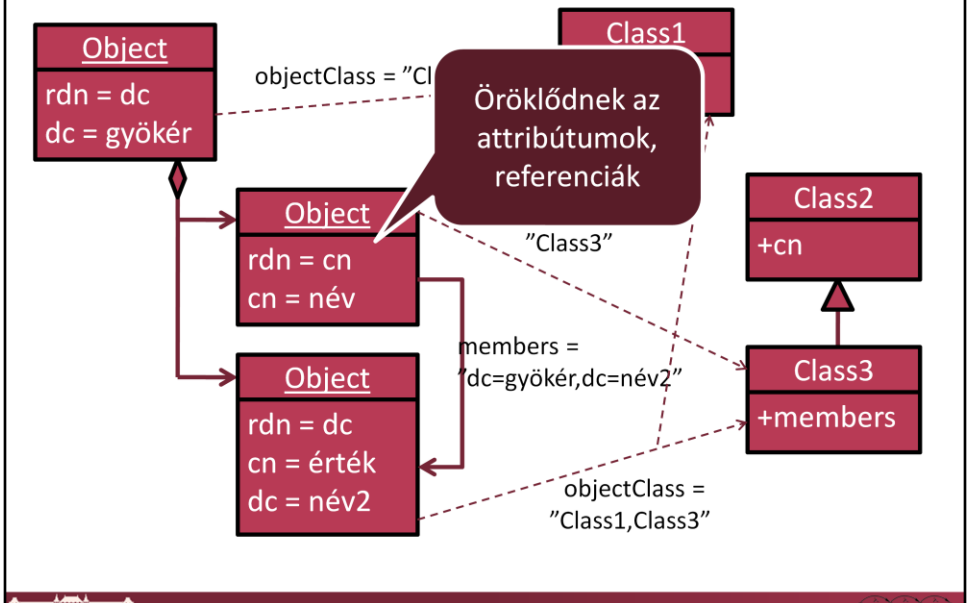
LDAP objektumok



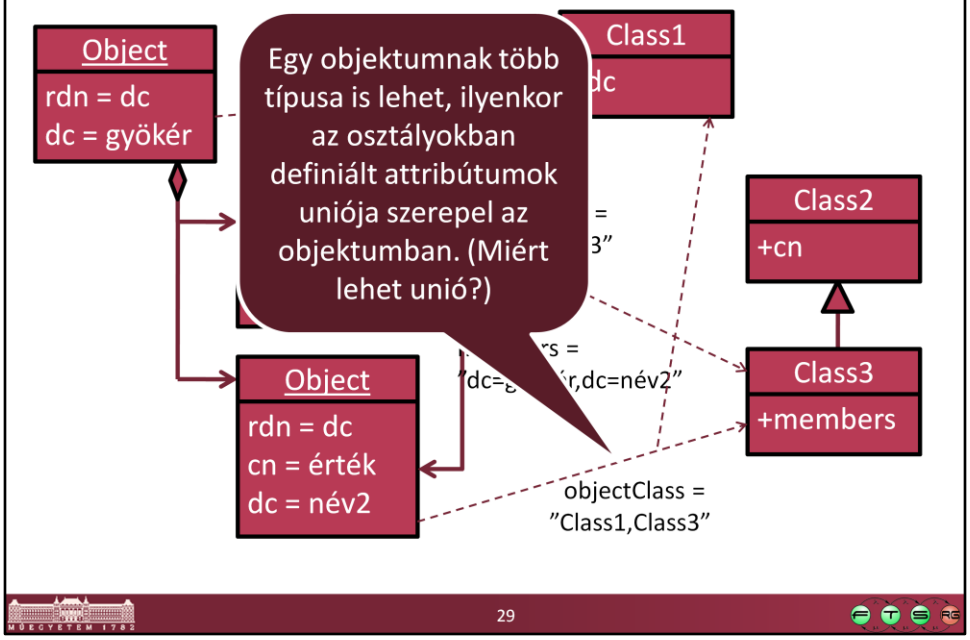
LDAP objektumok

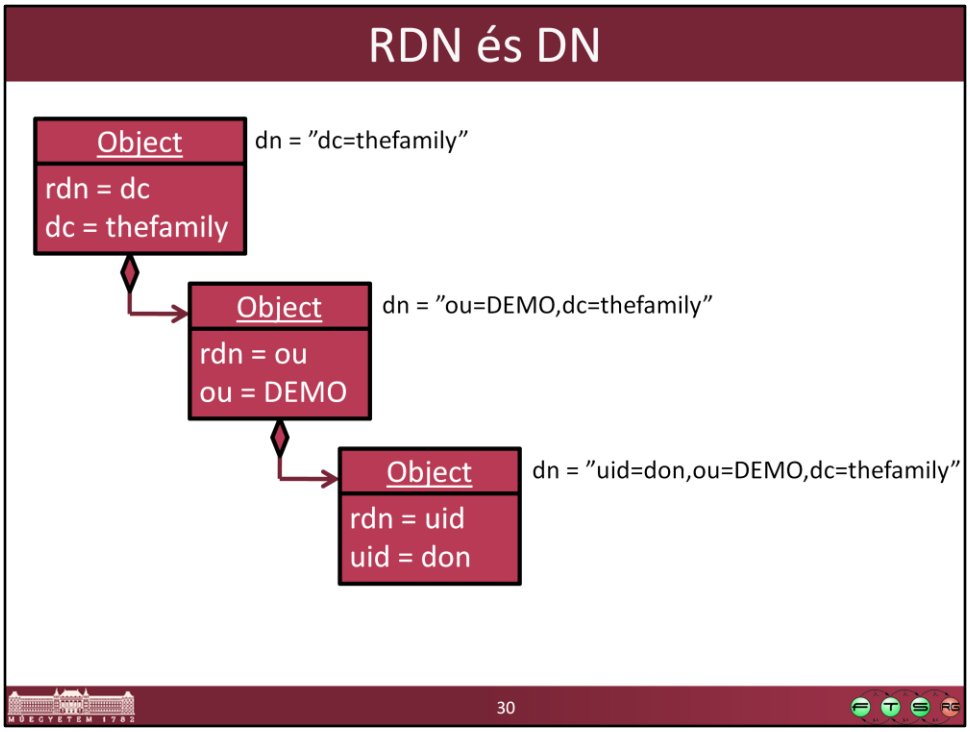


LDAP objektumok



LDAP objektumok





Megkülönböztetjük a szülő és az ős fogalmakat. Szülő alatt a közvetlen szülő objektumot, míg ősök alatt a gyökérig visszavezető összes objektumot értjük.

Megvalósítások

IBM Tivoli Directory Server,
IBM DB2 backend adatbázissal

OpenLDAP (open source)
Pl. BerkleyDB 4.2 backend
adatbázissal (lehet más is)

Sun ONE Directory Server
Sun Java System Directory Server
JDBC alapú adatbázisokkal

Linux, UNIX (Pl. AIX),
VMware ESX server, stb.
PAM (Pluggable Authentication Modules)
használatával

Hálózati beléptetés (Pl VPN, WLAN esetén)

Webalkalmazások: Apache, PHP,
Tomcat stb.

Adatbáziskezelők: MySQL, PostgreSQL stb.

DEMO LDAP címtár a gyakorlatban

- OpenLDAP szerver
- phpLDAPadmin webes kliens

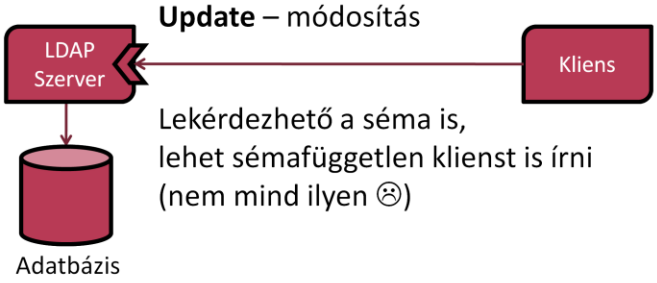
- Szervezeti egységekbe csoportosítás
- Felhasználók csoportokba rendelése
- Attribútumok

Szöveges LDAP transzfer formátum

- LDIF (LDAP data interchange format)
- ```
  dn: uid=don,dc=thefamily,dc=local
  cn: Don Corleone
  givenName: Don
  sn: Corleone
  uid: don
  telephoneNumber: +1 888 555 6789
  mail: don@thefamily.local
  sons: cn=michael,dc=thefamily,dc=local
  sons: cn=santino,dc=thefamily,dc=local
  sons: cn=fredo,dc=thefamily,dc=local
  objectClass: inetOrgPerson
  objectClass: maffiaPerson
  objectClass: person
  objectClass: top
  ```
  ```

LDAP műveletek

Alapműveletek:
Bind – autentikáció
Search – lekérdezés, keresés
Update – módosítás



Lekérdezhető a séma is,
lehet sémafüggetlen klienst is írni
(nem mind ilyen ☹)

Adatbázis

Gyakori LDAP elemek

- Fő (leggyakrabban használt) elemek és RDN-nek használt attribútumai
  - Domain component (dc)
  - Country (c)
  - Organization (o)
  - Organizational unit (ou)
  - Person (common name cn, surname sn)
  - Group of names (common name cn)

LDAP URL

- Csomópontok egy halmazának kiválasztására
- `proto://host:port/DN?attributes?scope?filter`
  - Proto - ldap/ldaps
  - Host:port – a címtár szerver elérhetősége
  - DN – keresés kiindulóponja
  - Attributes - keresett attribútumok listája
  - Scope – keresés mélysége
    - base: pontosan azt az egy csomópontot keressük
    - one: csak egy szinten keresünk
    - sub: teljes részfában keresünk
  - Filter – keresőkifejezés
    - Pl: (&(objectClass=maffiaPerson)(uid=don))
    - kvázi szabványos „prefix” leíró nyelv

Hogyan építsünk LDAP-ot?

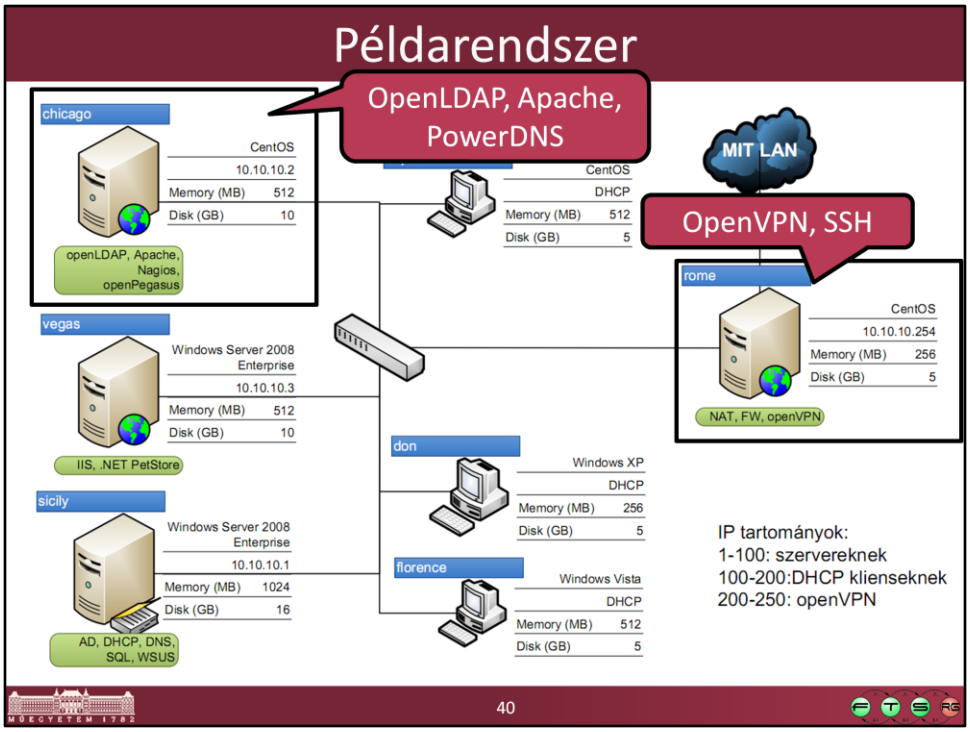
- Objektum struktúra ránk van bízva, de ne toljunk ki magunkkal!
  - Mindenkinek lehet gyereke, de célszerű csak `DomainComponent` vagy `OrganizationalUnit`okat használni tartalmazóelemként
  - A `DomainComponent`ek célszerű, ha követik a DNS névhierarchiát, de ez nem kötelező
  - Csoportosítsunk típusok szerint (pl. `Group`-ok és `Personok` külön részfába), illetve szervezeti egységek szerint is
  - A tartalmazás rendtartási célt szolgál, ne hordozzon funkcionális jelentést
  - Funkcionális csoportosításra `Role` vagy `GroupOfNames`
  - Néha sajnos a kliensek megkötik, hogy milyen osztályt használhatunk, ilyenkor jó a többszörös típusozás

Hozzáférés vezérlés

- Nem jó, ha akárki módosíthatja
- Az LDAP-ban tárolunk jelszavakat is → nem jó, ha bárki bármit olvashat
  - Jelszó lehet cleartext, vagy MD5, SHA1 hash is
  - Nem lehetetlen visszafejteni a hash-et sem…
- Hozzáférés szabályozható:
  - Objektum vagy részfa szinten
  - Séma szinten (osztály típus, vagy attribútumra szűrés)
- Az LDAP felhasználói is az LDAP-ban tárolódnak

LDAP vs RDBMS

- Miért LDAP, miért nem relációs adatbázis?
  - Mindegyiknek van előnye és hátránya
  - LDAP
    - Hatékony keresés
    - Széles támogatottság
    - Lassú módosítás
    - Többszörös öröklődés
  - RDBMS
    - Hatékony keresés
    - Merev adatmodell


Példarendszer
OpenLDAP, Apache, PowerDNS
chicago
CentOS
10.10.10.2
Memory (MB) 512
Disk (GB) 10
openLDAP, Apache, Nagios, openPegasus
CentOS
DHCP
Memory (MB) 512
Disk (GB) 5
MIT LAN
OpenVPN, SSH
rome
CentOS
10.10.10.254
Memory (MB) 256
Disk (GB) 5
NAT, FW, openVPN
vegas
Windows Server 2008 Enterprise
10.10.10.3
Memory (MB) 512
Disk (GB) 10
IIS, .NET PetStore
don
Windows XP
DHCP
Memory (MB) 256
Disk (GB) 5
sicily
Windows Server 2008 Enterprise
10.10.10.1
Memory (MB) 1024
Disk (GB) 16
AD, DHCP, DNS, SQL, WSUS
florence
Windows Vista
DHCP
Memory (MB) 512
Disk (GB) 5
IP tartományok:
1-100: szervereknek
100-200:DHCP klienseknek
200-250: openVPN
40

Mire figyeljünk

- Akkor hatékony, ha
  - sok a keresés jellegű művelet
  - atomi műveleteket használunk
- Veszélyes, ha
  - felhasználókat csak ebben tároljuk
    - Ki indítja el az LDAP-ot? („róka fogta csuka” esete)
  - rendszerfelhasználókat belepakoljuk
    - Csomagkezelő törli a felhasználót, holott máshol még kellhet
    - Létrejöhet olyan felhasználó ami adott hoszton nem kell

DEMO Egyéb LDAP lehetőségek

- Apache mod_auth_ldap konfiguráció
  - VirtualHost konfiguráció
  - LDAP autentikáció
- OpenVPN ldap_auth_plugin konfiguráció

Kapcsolódó Apache konfigurációs fájl részlet
- Figyeljük meg az LDAP specifikus beállításokat!

```
<VirtualHost *:80>
   ServerAdmin webmaster@chicago
   DocumentRoot /var/vhosts/accounts
   ServerName accounts.thefamily.local

   <Directory /var/vhosts/accounts>
            AuthType Basic
            AuthName "Maffia FTSRG LDAP Authorization"
            AuthBasicProvider ldap
            AuthzLDAPAuthoritative on
            AuthLDAPBindDN cn=apache,ou=administrative,dc=thefamily,dc=local
            AuthLDAPBindPassword alma
            AuthLDAPURL ldap://127.0.0.1/ou=DEMO,dc=thefamily,dc=local?uid?sub

            Require ldap-group
         cn=chicago2group,ou=groups,ou=DEMO,dc=thefamily,dc=local
            Satisfy all
   </Directory>
</VirtualHost>
```

DEMO DNS

- Dnsdomain.schema
- PowerDNS DNS szerver
  - LDAP paraméterek beállítása
- Domainek felvétele
- Let test it! Nslookup, dig

- http://www.linuxnetworks.de/doc/index.php/PowerDNS_LDAP_Backend

LDAP elérése JAVA alkalmazásból

```
Hashtable<String, String> authEnv = new Hashtable<String, String>(11);
String user = "cn=zeedemo,ou=users,ou=DEMO,dc=thefamily,dc=local";
String passWord = "alma";        // NOT SECURE!!!
String ldapURL = "ldap://10.10.10.2:389";
authEnv.put(Context.INITIAL_CONTEXT_FACTORY,"com.sun.jndi.ldap.LdapCtxFactory");
authEnv.put(Context.SECURITY_AUTHENTICATION, "simple");
authEnv.put(Context.PROVIDER_URL, ldapURL);
authEnv.put(Context.SECURITY_PRINCIPAL, user);
authEnv.put(Context.SECURITY_CREDENTIALS, passWord);

try {
    DirContext authContext = new InitialDirContext(authEnv);
    System.out.println("Authentication Success!");
} catch (AuthenticationException authEx) {
    System.out.println("Authentication failed!");
} catch (NamingException namEx) {
    System.out.println("Something went wrong!");
    namEx.printStackTrace();
}
```

DEMO Programozás óra

- Autentikáció JAVA alkalmazásból LDAP alapján
  - JNDI -> DirContext
- Keresés, módosítás LDAP adatbázisban

Példa kód LDAP elem keresésére:

```
Hashtable<String, String> env = new Hashtable<String, String>();
env.put(Context.INITIAL_CONTEXT_FACTORY,"com.sun.jndi.ldap.LdapCtxFactory");
env.put(Context.PROVIDER_URL, "ldap://10.10.10.2:389");
env.put(Context.SECURITY_AUTHENTICATION,"simple");
try{
        env.put(Context.SECURITY_PRINCIPAL,"cn=java,ou=administrative,dc=thefamil
        y,dc=local"); // specify the username
        env.put(Context.SECURITY_CREDENTIALS,"javapass");        // specify the
        password
        DirContext ctx = new InitialDirContext(env);
        Attributes matchAttrs = new BasicAttributes(true); // ignore attribute name
        case
        matchAttrs.put(new BasicAttribute("uid", "zeedemo"));
        // Search for objects with those matching attributes
        NamingEnumeration answer =
        ctx.search("ou=users,ou=DEMO,dc=thefamily,dc=local", matchAttrs);
        formatResults(answer);
} catch (Exception E){
                E.printStackTrace();
}
```

DEMO ldapsearch, ldapadd, ldapmodify

- LDAP adatbázis parancssorból történő használata
  - Jellemző ldapsearch kapcsolók
    - -x : Egyszerű azonosítás használata
    - -b: Keresés gyökér eleme
    - -D: Felhasználó DN-je
    - -W: jelszó bekérése
    - -h: LDAP szerver címe
    - ‘(ObjectClass=posixAccount)’: keresési kritérium

ldapsearch -x -h 10.10.10.2 -D "cn=apache,ou=administrative,dc=thefamily,dc=local" -W -b "dc=thefamily,dc=local" -s sub '(objectClass=posixAccount)'