**ACTIVE DIRECTORY**

**JELLEMZŐI:**

rugalmas lekérdezés

központosított rendszerfelügyelet

rugalmas rendszerfelügyelet (objektumjogok beállíthatók)

jogok átruházása

hatékony replikációk: több helyen szinkronban

* tulajdonság szintű
* frissítési sorszámok

DNS integrálás(nélkülözhetetlen): zónafájl helyett adatbázis

visszamenőleges kompatibilitás

más címtárakkal való együttműködés

**Címtár – directory**

hálózat felügyeletére szolgál

egy adminisztratív egységbe foglaljuk a kiszolgálókat és szolgáltatásokat

**Címtárszolgáltatás – directory services**

címtár működését teszi lehetővé

kiszolgáló oldali program

* a címtár alapján segít elérni a nyilvántartó egyes elemeit
* címtárkiszolgálók futtatják

tartomány vezérlés

**Címtár adatbázis – directory database**

a címtárkiszolgálók tárolják

elosztott: több helyen tárolják

központosított: egységes adatbázis

hierarchikus felépítésű

**Névtár – namespace**

azon nevek együttese, amellyel a címtárban lévő objektumokra hivatkozni lehet

objektumok elnevezési szabályai

hierarchikus felépítésű

**Névkörnyezet partíció – naming context „zóna”**

a címtár bármely összefüggő részfája

névkörnyezetek:

* séma
* konfiguráció
* felhasználói névkörnyezet

**Schema**

milyen objektumokat hozhatunk létre az AD-ben

azokhoz milyen tulajdonságokat rendelhetünk

bővíthető – új osztályokkal, tulajdonságokkal

ez is az AD-ben tárolódikaz erdőre vonatkozik

**Configuration**

a másodpéldányok (többszörözés, replikáció) kezelési rendszerének topológiáját tartalmazza, és az ezzel kapcsolatos adatokat

**Felhasználói névkörnyezet!!**

a címtár tényleges objektumokat tartalmazó részfái

minden egyes tartományban 1 van

**Objektumok**

* a címtár elemi egysége
* vannak tulajdonságai és metódusai
  + erőforrás objektum (levélelem): erőforrás objektumokat tartalmaz
  + tároló objektum (container): más objektumokat tartalmaz

az egyes tárolók újabb tárolókat tartalmazhatnak – hierarchia

* tulajdonságai lehetnek:
  + kötelező (required properties): létrehozásakor mindenképp rendelkezni kell vele; megváltoztatható, de nem törölhető
  + választható (optional properties): bármikor hozzárendelhető és törölhető

**Tároló objektumok típusai**

Szervezeti egység (organizational unit – OU)

* tartományon belül teszi lehetővé az objektumok hierarchiájának kialakítását
* tárolókat és más objektumokat tartalmazhat
* segíti az elosztott adminisztrációt
* 12 szint mélységben ágyazhatók egymásba

Tartomány (Domain)

* alapvető adminisztrációs egység
* egy címtár adatbázissal egy tartomány felügyelhető
* tartalmazza az OU fa-struktúráját
* tartományi környezet (Domain Context – DC)

Típus nélküli speciális tároló

* új felhasználók alapértelmezetten ide kerülnek
* megnevezése: common name – CN
  + az erőforrás objektumok és a típus nélküli tárolók

Címtárobjektumok megnevezése

* a címtár az LDAP () protokollal érhető el
* előírja az objektumok nevének megadását
* a tárolón belül egyedinek kell lennie  
  CN= Gipsz Jakab

megkülönböztethető név (distinguished name)

* objektumok neve a teljes címtárban

CN= Gipsz\_Jakab OU= Tanulók DC= Mechwart

kanonikus név

Gipsz\_Jakab/Tanulók/Mechwart

egyszerű felhasználói név – UPN

GipszJ@mechwart – levélelem

**Azonosítás a belső folyamatok szempontjából**

Globális egyedi azonosító – GUID

* automatikusan generálódik
* egyedi
* számokból áll
* 128 bit
* minden objektum rendelkezik vele
* nem változik, ha átnevezik az objektumot

Biztonsági azonosítószám – SID

* biztonsági objektumok
* egyedi a címtáron belül
* 2 része van
  + tartomány azonosító
  + objektumnak a tartományon belüli azonosítója – RID

Fák (Domain Tree)

* több hierarchikusan szervezett tartomány

Erdő (Forest)

* tartományfák halmaza, nincs közös gyökerük

Globális katalógus (GC –Global Catalog)

* tartományok feletti AD
* az AD erdő valamennyi tartományának objektumát tartalmazza
* „kivonat”, „indexfájl”

Telephely (Site)

* egy alhálózatba tartozó gépek
* (egy alhálózatba tartozók)
* minden telephelyen ajánlott DNS+GC kiszolgáló

Tartományvezérlők

* a címtárat tartja nyílván
* csak 1 tartományt felügyel
* cél: 1 tartományt 2 tartományvezérlő szolgáljon ki – egyenrangúak  
  2008: Read-Only Domain Controller – RODC

**Tartományvezérlő funkciók**

Global Catalog Server

* erdőnként 1 található kezdetben
* később tartományonként

Műveleti kiszolgáló – Operation Server

* bizonyos műveletek ezen végezhetők el
* egész erdőre vonatkozó

Séma kiszolgáló – Schema Master

* a séma ezen módosítható
* 1 db van tartományonként

**Felhasználók és csoportok**

Biztonsági csoport

* felhasználható biztonsági objektumként – kaphat hozzáférési jogot erőforrásokhoz
* használható csoportos levélküldésre
* terjesztési csoporttá alakítható – ideiglenesen hatálytalanítjuk a hozzáférési jogokat

Terjesztési csoport

* felhasználók egybefogására alkalmas (pl.: csoportos levélküldés)
* rendelkezik biztonsági azonosítóval, csak inaktív
* biztonsági csoporttá alakítható

**Felhasználócsoportok hatóköre**

Tartományi helyi csoportok (Domain Local Groups)

* csak a saját tartományuk számítógépein kaphatnak hozzáférési jogot  
  (ha biztonsági csoport)
* csak az őket tartalmazó címtárban vehetők fel más csoportokba
* univerzális és globális csoportokat vehetünk fel más tartományokból
* a tartomány helyi csoportjai egymásba ágyazhatók

Globális csoportok (Global Groups)

* az erdőn belül tetszőlegesen felhasználható más tartományokban – felvehetők más csoportokba, és hozzáférési jogokat kaphat
* csak saját tartományukból tartalmazhat tagokat

Univerzális csoportok (Universal Groups)

* tetszés szerinti tartományból tartalmazhat tagokat, felhasználókat, globális-, univerzális csoportokat
* tetszés szerinti tartományban használható fel csoportok tagjaiként és hozzáférési jogok adásakor

Hatókör megváltoztatása

* a tartomány helyi és globális csoportjai univerzálissá alakíthatók
* az univerzális csoportok tartományi helyi, vagy globális csoporttá alakíthatók
* az átalakítás csak akkor végezhető el, ha olyan tagot tartalmaz, amely az új hatókörrel nem rendelkezik

Csoportok egymásba ágyazása

felhasználó – globális csoport – univerzális csoportok – helyi csoport – jog

Beépített csoportok

* a rendszer automatikusan hozza létre
* különböző hozzáférési jogokkal rendelkeznek – vannak olyan jogok, amelyekkel csak ezek rendelkezhetnek
* tagsága módosítható, de nem törölhető – átnevezhető

Speciális beépített azonosítók (pl.:mindenki)

* nem rendelkeznek speciális csoporttagsággal, amely módosítható lenne
* a számítógép erőforrásaihoz való hozzáférésre vonatkozik
* különböző időpillanatokban a felhasználók különböző csoportjait képviselik
* nem tudjuk kilistázni a tagjait és nem látjuk a csoportok kezelésében
* jogokat adhatunk nekik
* névtelen bejelentkezés
* hitelesített felhasználónév
* létrehozó tulajdonos
* mindenki
* interaktív: helyileg bejelentkezés
* szolgáltatás
* rendszer

**Jogok és megosztások**

FAT

* hozzáférési jogok nem definiálhatók
* attribútum
  + rejtett
  + rendszer

NTFS

* hozzáférési jogokkal védhetőek a mappák, állományok
* újabb attribútumok
  + tömörített
  + titkosított

Jogok beállítása

* csoport
* felhasználó
* beépített speciális azonosítók

mindig csoportnak adjuk → megfelelő csoporttagság beállítása

Jogok: fájlok, mappák

* engedélyezők
* tiltók ⇨ erősebb
* effektív jog: jogok uniója  
  felhasználó több forrásból kap jogot, kivéve a tiltás
* elemi jogok: írás, olvasás, listázás
* összetett jogok: (elemi jogokból:) olvasás, módosítás, teljes hozzáférés

Tulajdonos: objektum létrehozója 🢡 teljes hozzáférés

tulajdonjog átvehető – saját tulajdonjogba vételi jog szükséges hozzá

visszafejthető titkosítással?