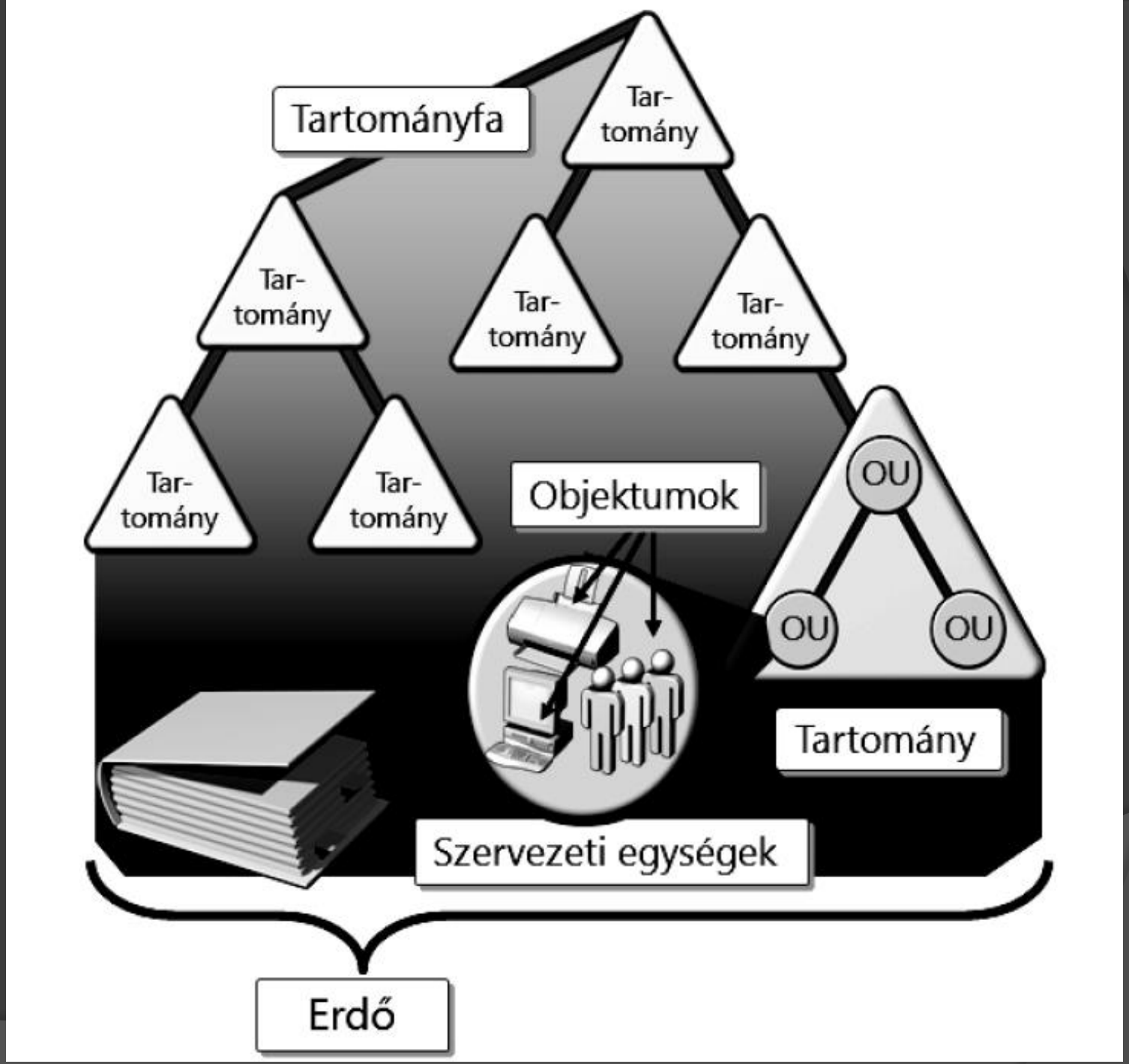
ACTIVE DIRECTORY

Címtár

- a címtár egy olyan adatbázis, ami képes a hálózat valamennyi erőforrásának
  - azonosítására,
  - és hierarchikus rendszerben való tárolására
- a hálózat fizikai felépítését és protokolljait átláthatóvá teszi


Tartományfa
Tar-
tomány
Tar-
tomány
Tar-
tomány
Tar-
tomány
Tar-
tomány
Tar-
tomány
Objektumok
OU
OU
OU
Tartomány
Szervezeti egységek
Erdő

Az Active Directory alkotóelemei

ERDŐ

- A legmagasabb szintű AD tároló.
- Az erdő közös sémát és globális katalógust használ.
- Egy vagy több tartományt foglal magába.
- Az erdő első tartományát
  az erdő gyökértartományának hívják.

Az Active Directory alkotóelemei

FA

Ha az erdő több tartománya
összefüggő DNS-tartománynéveket használ,
(vagyis egymás gyermek, illetve szülőtartományai)
akkor a struktúrát ***tartományfának*** nevezzük.

Az Active Directory alkotóelemei:

TARTOMÁNY

- Az AD alapvető szervezeti és biztonsági egysége.
- A tartomány olyan ügyfelek, kiszolgálók és egyéb hálózati erőforrások gyűjteménye, amelyek közös címtáradatbázist alkotnak, és egyben a replikáció alapegységét képezik.
- Az Active Directory-címtárban minden tartományt egy-egy DNS-tartománynév azonosít, és minden tartomány legalább egy tartományvezérlőt (DC) tesz szükségessé.

Az Active Directory alkotóelemei

SZERVEZETI EGYSÉG

- Organizational Unit (OU)
- Az AD objektumtárolói (felhasználók, csoportok, számítógép-objektumok, szervezeti egységek).
- Fontos szerepet játszanak a csoportházirend érvényesítésével és a felügyeleti jogok delegálásával kapcsolatban.

Replikáció

- A DC-k mindegyike tartalmazza a teljes címtáradatbázist, és az mindegyik DC-n módosítható. Hogy a címtárpéldányok (replikák) mindegyike folyamatosan a helyes adatokat tartalmazhassa, szükség van a DC-k közötti folyamatos, és lehetőleg minél kevesebb erőforrást felhasználó szinkronizációra. Ezt a folyamatot nevezzük replikációnak.
- Ütközés esetén a replikáció a későbbi módosítást tekinti érvényesnek.
- Megfelelően működő replikáció ⇨ címtárpéldányok konzisztens állapotban maradnak

- A Windows Server 2008-ban bevezették az írásvédett/csak olvasható tartományvezérlő

(Read-Only Domain Controller, RODC)

üzemmódot a kevésbé biztonságos telephelyek számára.

- Ennek kapcsán a „*hagyományosan*” működő tartományvezérlőket, az RODC-től való megkülönböztetés miatt:

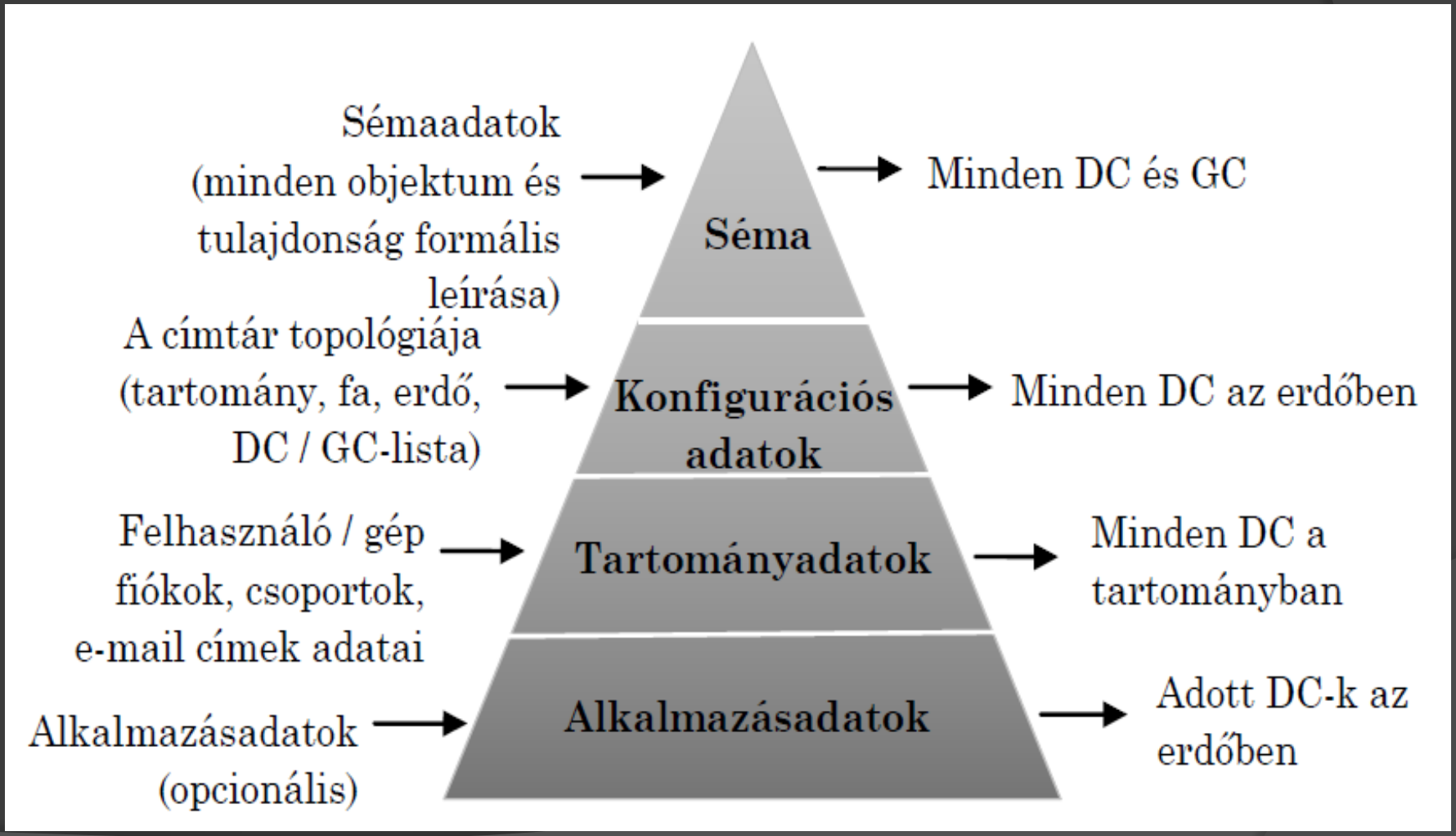
írható tartományvezérlőnek

(writable domain controller)

is nevezik.

- Az AD írható tartományvezérlőin *nincsenek helyi felhasználók*, csak tartományi felhasználókkal lehet bejelentkezni.
- Egy külön címtár-visszaállítási mód (Directory Services Restoration Mode) áll rendelkezésre az AD karbantartására, ahová az AD telepítésekor megadott jelszóval lehet bejelentkezni.
- Az írásvédett tartományvezérlőkön helyi rendszergazdai fiók is található, amivel rutin adminisztrációs feladatokat lehet végezni (hálózati kártya telepítése, particionálás stb.) a tartományhoz való rendszergazdai jogosultság nélkül.

Címtárpartíciók



Séma partíció *(Schema Partition)*

- Osztály- és attribútumdefiníciókat, vagyis az objektumok és tulajdonságok formális leírását tárolja.
- Az AD séma az egész erdőre vonatkozóan megegyezik.
- Minden DC-n és minden GC-ben megtalálható.

Konfigurációs partíció *(Configuration Partition)*

- A címtár topológiájára vonatkozó adatokat tárolja:
  - tartományokra, fákra és erdőre vonatkozó információk
- Itt tárolódik a replikációs topológia.
- A konfigurációs adatok az egész erdőre vonatkoznak, és megtalálhatók az erdő valamennyi DC-én.

Tartomány partíció *(Domain Partition)*

- Itt találhatjuk meg a felhasználókra, számítógépekre, csoportokra és egyéb tartomány szintű objektumokra vonatkozó adatokat.

- A partíció az adott tartomány minden DC-én megtalálható.

Alkalmazás partíció *(Application Partition)*

- A DC-k egy vagy több alkalmazás-címtári partíciót is tárolhatnak.
- Opcionális

Az egyedi főkiszolgáló-műveletek (FSMO)

- Flexibile Single Master Operations, FSMO
  - RID Master
  - PDC Emulátor
  - Infrastructure Master
  - Domain Naming Master
  - Schema Master

RID-főkiszolgáló *(RID Master)*

- Minden tartományban legfeljebb egy lehet belőle.
- A saját, vagy valamelyik másik DC kérésére egy létrehozandó új objektum (felhasználói fiók, csoport stb.) számára kiadja a relatív azonosító *(Relative Identifier, RID) részt a leendő objektum biztonsági azonosítójához (Security Identifier, SID).*
- *A RID Mastertől a többi tartományvezérlő* 200-as csomagokban (RID Pool) kap relatív azonosítót, amivel azután önállóan gazdálkodik.
- A relatív azonosító rész teljesen egyértelműen azonosítja az objektumot a tartományon belül.
- Ha nem érhető el a RID-főkiszolgáló, csak addig lehet a tartományban új objektumokat létrehozni, amíg a korábban kiosztott RID Poolok el nem fogynak.

PDC-emulátor *(PDC Emulator)*

- Minden tartományban csak egy lehet belőle.
- Feladata, hogy a Windows 2000 előtti ügyfelek számára elsődleges Windows NT tartományvezérlőként *(Primary Domain Controller, PDC) működjön.*
- Ennek megfelelően feldolgozza az ügyfelek bejelentkezéseit, jelszóváltozásait, és replikálja a változásokat a többi tartományvezérlő felé.
- Feladatai közé tartozik még a tartomány összes tartományvezérlője által mutatott idő automatikus szinkronizálása a Windows Time szolgáltatás segítségével.

Infrastruktúra-főkiszolgáló *(Infrastructure Master)*

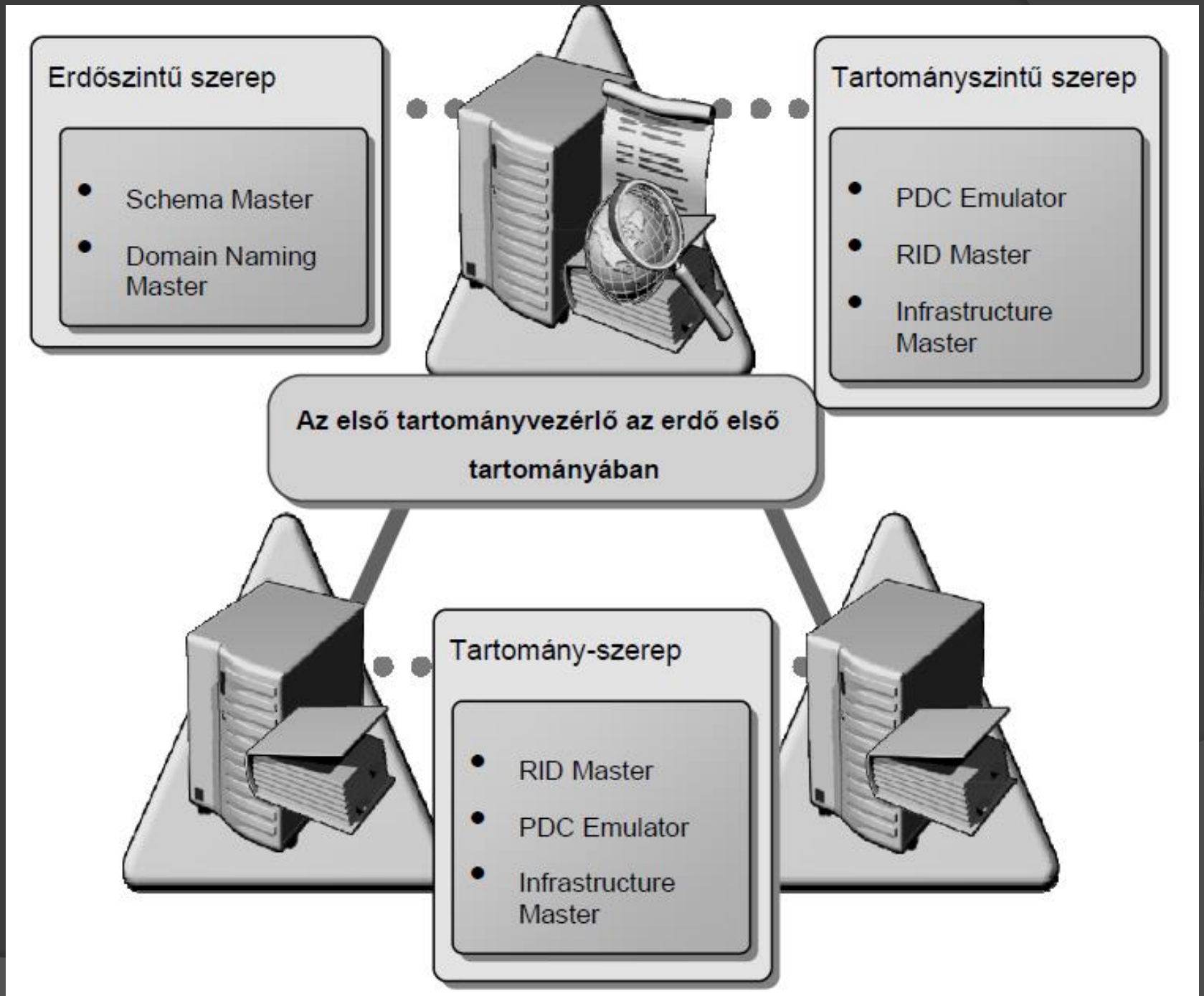
- Minden tartományban csak egy lehet belőle.
- Csak akkor van rá szükség, ha a hálózat több tartományból áll.
- Feladata a saját tartományának objektumai és a többi tartományban található objektumok közötti hivatkozások frissítése.
- Amennyiben nem érhető el, a tartományon belül nem veszünk észre változást, azonban a többi tartománnyal való kapcsolattartás során frissítési problémák keletkeznek.

Tartománynév-nyilvántartási főkiszolgáló *(Domain Naming Master)*

- Az erdőben kizárólag egy lehet belőle.
- Szabályozza az erdőben a tartományok hozzáadását és törlését.
- A tartományfákkal kapcsolatos változtatások nem hajtódnak végre, ha a szerepet megvalósító tartományvezérlő nem érhető el.

Séma-főkiszolgáló *(Schema Master)*

- Az erdőben kizárólag egy lehet belőle.
- Központosítva végzi el a séma összes frissítését és módosítását.
- Nem vesszük észre a hiányát, egészen addig, amíg nem kerül sor a séma frissítésére, vagy bővítésére.


Erdőszintű szerep
Schema Master
Domain Naming Master
Tartományszintű szerep
PDC Emulator
RID Master
Infrastructure Master
Az első tartományvezérlő az erdő első tartományában
Tartomány-szerep
RID Master
PDC Emulator
Infrastructure Master

- Az erdő első DC-jének telepítésekor valamennyi erdő és tartomány szintű szerepkör erre a kiszolgálóra kerül, de később áthelyezhetők.

- Active Directory Users and Computers
  - A tartományszintű szerepkörök (RID Master, PDC Emulator, Infrastructure Master)

- Active Directory Domains and Trusts
  - Domain Naming Master szerepkör

- Active Directory Schema
  - Schema Master

A séma

- A séma az AD-adatbázis szerkezete (a címtárban tárolható objektumok definícióinak összessége)
- Minden objektumosztály számára meghatározza a kötelező és lehetséges attribútumok körét, valamint a szülőként megadható objektumosztályokat.

A séma

- Van alapséma, ami módosítható.
- A módosítás késlekedés nélkül replikálódik az erdő valamennyi DC-jére, a művelet minden esetben a teljes hálózatot érinti.
- A sémából semmi nem törölhető (csak deaktiválás lehetséges)

Active Directory Schema

- A séma kezelésére szolgál
- Ennek segítségével mozgathatjuk másik DC-re a Schema Master szerepet
- A modul nincs regisztrálva
- Regisztráláshoz:

```
C:\>regsvr32 schmmgmt.dll
```

A globális katalógus szerepkör - *Global Catalog (GC)*

- Olyan tartományvezérlői szerep, amelynek hordozója a címtár összes objektumának alapadataival, elérhetőségeiknek információjával rendelkezik a teljes erdőre vonatkozóan.
- A saját tartományából teljes, a további tartományokból részleges objektummásolatokat tartalmaz, így a GC segítségével kereshetőek a címtáradatok függetlenül attól, hogy valójában a címtár melyik tartománya tartalmazza azokat.
- Alapértelmezés szerint az erdő első tartományvezérlője tartalmazza a globális katalógust,
- de más tartományvezérlőket is kijelölhetünk erre a célra.

A működési (funkcionalitási) szintek

- A tartományok és erdők működési szintjeinek segítségével engedélyezhetők bizonyos tartományi és erdőszintű AD szolgáltatások.
- A működési szint egyrészt meghatározza a tartományban, illetve erdőben elérhető szolgáltatások körét,
- másrészt a működési szint emelésével régebbi tartományvezérlők már nem adhatók a tartományhoz.

Active Directory Sites and Services

- A telephelyek kialakítására és a DC-k közötti replikáció beállítására szolgál.
- Kijelölhetjük azokat a DC-ket, amelyek a globális katalógus szerepkört fogják tartalmazni.

Active Directory Domains and Trusts

- A tartományok közötti bizalmi kapcsolatok (trust relationship) kezelésére szolgál.
- A bizalmi kapcsolat a tartományok közötti olyan kapcsolat, amely lehetővé teszi, hogy valamely tartomány felhasználóit egy másik tartomány vezérlője hitelesítse.
- Domain Naming Master szerepet megvalósító kiszolgáló kijelölése.

Bizalmi kapcsolatok

- **Egyirányú bizalmi kapcsolat** *(One way trust)* az egyik tartomány felhasználói hozzáférhetnek a másik tartomány erőforrásaihoz, de a másik tartomány felhasználóinak nem enged hozzáférést az elsőhöz.
- **Kétirányú bizalmi kapcsolat** *(Two way trust)* két tartomány felhasználói hozzáférnek egymás erőforrásaihoz

Bizalmi kapcsolatok

- **Tranzitív bizalmi kapcsolat** *(Transitive trust)* olyan bizalmi kapcsolat, ami a résztvevő két tartományon túl is kiterjeszthető.

- **Nem tranzitív bizalmi kapcsolat** *(Intransitive trust)* olyan bizalmi kapcsolat, aminek a hatálya csak a résztvevő két tartományra terjed ki.

Bizalmi kapcsolatok

- **Explicit bizalmi kapcsolat**

  (Explicit trust)

  a rendszergazda által létrehozott bizalmi kapcsolat. Nem tranzitív, és egyirányú (két egyirányú kapcsolat létrehozásával kvázi kétirányúvá tehető).

- **Közvetlen bizalmi kapcsolat**

  (Cross link/shortcut trust)

  két külön tartományfában lévő tartományok, vagy egy tartományfán belüli, de szülő-gyermek viszonyban nem álló tartományok között létrehozott explicit bizalmi kapcsolat. Tranzitív, egy- vagy kétirányú.

Alapértelmezett bizalmi kapcsolatok

Kapcsolat típusa	Tranzitivitás	Irány	Leírás
Szülő–gyermek	Tranzitív	Kétirányú	Új gyermektartomány létező tartományfához adásakor jön létre.
Tartománygyökér szintű	Tranzitív	Kétirányú	Új tartományfa létező erdőben történő létrehozásakor új, tartománygyökér szintű bizalmi kapcsolat jön létre

Egyéb bizalmi kapcsolatok

Külső	Nem tranzitív	A külső bizalmi kapcsolat olyan erőforrásokhoz nyújt hozzáférést, amelyek Windows NT 4.0 alapú tartományban vagy egy másik erdőben lévő, erdőszintű bizalmi kapcsolattal nem rendelkező tartományban találhatók.
Tartományi	Tranzitív vagy nem tranzitív	A tartományi bizalmi kapcsolat egy nem Windows-alapú Kerberos-tartomány és egy Windows Server 2003 alapú tartomány között jöhet létre
Erdő-szintű	Tranzitív	Az erdőszintű bizalmi kapcsolat Windows 2003 rendszerű erdők közötti erőforrás-megosztásra használható.
Közvetlen	Tranzitív	A közvetlen bizalmi kapcsolat csökkenti az erdőn belül a két tartomány közötti bejelentkezési időt. Használata különösen hasznos, ha a két tartomány két külön tartományfában található.

DNS szolgáltatás új rekordjai

- **WINS-rekord:**

A WINS-erőforrásrekordban egy WINS-kiszolgálót adhatunk meg, ide továbbítódnak majd a DNS-adatok alapján meg nem válaszolható IP-cím lekérdezések.

- **WINS-R-rekord:**

ugyancsak egy WINS-kiszolgáló címét adhatjuk meg ebben a rekordban, ide a sikertelen fordított lekérdezések (ilyenkor név alapján keresünk IP-címet) fognak továbbítódni.

- **SRV-rekord:**

az SRV-rekordok az Active Directoryhoz kapcsolódó szolgáltatások megtalálását teszik lehetővé.

SRV-rekord

Az SRV-erőforrásrekordok egyes mezőinek rendeltetése a következő:

- **Szolgáltatás:** A keresett szolgáltatás szimbolikus neve (*_ldap, _kerberos)*
- **Protokoll:** Az átviteli protokoll típusát jelzi (TCP, UDP)
- **Név:** A DNS-tartománynév, amelyhez az erőforrásrekord tartozik
- **Prioritás:** Meghatározza a cél mezőben szereplő kiszolgáló prioritását.
- **Súlyozás:** A prioritás mellett a súlyozás is terheléselosztásra használható. Azonos prioritású kiszolgálók esetén ez az érték határozza meg a lekérdezés eredményét.
- **Port:** A célállomás kiszolgálóportjának száma, amelyen az adott szolgáltatás elérhető.
- **Cél:** A kért szolgáltatás nyújtására képes kiszolgáló DNS-tartománynevét tartalmazza. Az itt szereplő névhez tartoznia kell egy megfelelő A-rekordnak

AD fiókok típusai

- Felhasználói fiók
- Számítógép fiók
- Csoport fiók
  - Terjesztési csoport
  - Biztonsági csoport
    - Helyi csoport
    - Tartományon belüli csoport
    - Globális csoport
    - Univerzális csoport

Terjesztési csoport

- Csak emailek terjesztésére használt, biztonsági szolgáltatásokkal nem rendelkező csoport.
- A terjesztési csoportnak nem adható semmiféle jogosultság.

Biztonsági csoport

- A jogosultságok kiosztásának megkönnyítésére szolgál.
- Egymásba is ágyazhatók.
- Elektronikus levelezési egységként is használható (mindenki megkapja a levelet a csoportból).

Helyi csoport

- ***(Machine Local Group)***
- Olyan biztonsági csoport, amely csak annak a számítógépnek az erőforrásaihoz kaphat jogokat és engedélyeket, amelyen a csoportot létrehozták.

Tartományon belüli csoport

- ***(Domain Local Group)***
- A tartományon belüli csoportok tagjai a tartományok csoportjai és fiókjai lehetnek.
- A tartományon belüli csoportoknak csak a tartományon belül adható engedély.

Globális csoport

- ***(Global Group)***
- Olyan biztonsági vagy terjesztési csoport, amelynek tagjai a saját tartományában található felhasználók, csoportok és számítógépek.
- Az erdő bármely tartományának erőforrásaira kaphat jogosultságokat és engedélyeket.

Univerzális csoport

- ***(Universal Group)***
- Az univerzális hatókörű csoport tagjai a tartományfa vagy az erdő bármely tartományában lévő csoportok és fiókok lehetnek.
- A tartományfa vagy az erdő bármely tartományában adható engedély.
- Az univerzális csoport csak *legalább Windows 2000 – natív* módban működő tartományban használható.
- Az ilyen csoportok tagjai a globális katalógusban tárolódnak.