Tartományi környezet

A tartomány koncepció és az ehhez kapcsolódó Active Directory címtárszolgáltatás a legtöbb szervezet esetén az informatikai rendszer legfontosabb alkotóeleme. A címtár tárolja a hálózat valamennyi objektumának és számos erőforrásának adatait, és ezeket egységes, jól kezelhető formában elérhetővé teszi a felhasználók és a rendszergazdák számára, így biztosítja a hálózat használatához és felügyeletéhez szükséges infrastruktúrát.

Ebben a fejezetben tehát az Active Directory, és a hozzá kapcsolódó szolgáltatások, felügyeleti eszközök használatával kapcsolatos tudnivalókról lesz szó. A következő témakörökkel fogunk foglalkozni:

- **Mire jó a címtár?** – Áttekintjük milyen szolgáltatásokat nyújt a címtár, és milyen gyakorlati haszonnal jár bevezetése a felhasználók és a rendszergazdák számára.
- **Az Active Directory címtárszolgáltatás alapjai** – Megismerkedünk a címtár felépítésével, alkotórészeivel és az üzemeltetéséhez, felügyeletéhez szükséges legfontosabb eszközökkel.
- **A DNS-szolgáltatás** – Áttekintjük az Active Directory működéséhez nélkülözhetetlen DNS-szolgáltatással kapcsolatos alapismereteket.
- **Az Active Directory telepítése** – Az alapismeretek után telepítjük a címtárszolgáltatást, sorra vesszük a telepítőprogram által elvégzett műveleteket és a hibalehetőségeket.
- **Tipikus címtárobjektumok** – A feltelepített címtárszolgáltatást meg kell töltenünk tartalommal, vagyis létre kell hoznunk a hálózatunk elemeit reprezentáló objektumokat. Ebben a részben a leggyakrabban előforduló objektumtípusokkal kapcsolatos tudnivalókat tekintjük át.
- **A címtár mentése és visszaállítása** – Mire idáig jutunk, már meglehetősen sok munkánk fekszik a címtárstruktúra kialakításában, így gondoskodnunk kell a rendszeres mentésről.
- **A csoportházirend** – A csoportházirend az Active Directory kiegészítő (de rendkívül fontos) komponense. Segítségével megvalósítható az ügyfélgépek, kiszolgálók és felhasználók tömeges felügyelete, vagyis az egyetlen helyen meghatározott beállítások valamennyi kiválasztott számítógépen, illetve felhasználón érvényesülni fognak. Ebben a részben bemutatjuk a csoportházirend működésére és kezelésére vonatkozó alapvető tudnivalókat.
- **A replikáció és a telephelyek** – Ebben a részben megismerkedünk az Active Directory tartományvezérlői között végbemenő adatbázis szinkronizáció, vagyis a replikáció működésével, és megtárgyaljuk a telephely struktúra kialakításával kapcsolatos ismereteket.

Mire jó a címtár?

Ha definiálni szeretnénk a címtár fogalmát, akkor egyszerűen mondhatjuk így: a címtár egy olyan adatbázis, ami képes a hálózat valamennyi erőforrásának azonosítására, és hierarchikus rendszerben való tárolására. Kiegészíthetjük a definíciót még azzal is, hogy az azonosítás és tárolás mellett a hálózat fizikai felépítését és protokolljait átláthatóvá teszi, így a hálózat erre feljogosított felhasználói elérhetik a hálózat erőforrásait anélkül, hogy tudnák, hol találhatóak azok valójában, vagy hogyan kapcsolódnak egymáshoz fizikailag. Ez a meghatározás persze nemcsak a Windows Server címtárszolgáltatására az Active Directoryra, hanem bármilyen más címtárra is igaz.

Ez eddig rendben is van, de vajon mégis mire jó a címtár a gyakorlatban, mennyiben teszi könnyebbé a felhasználók és az üzemeltetők életét? Mit fog látni (és használni) a címtárból a gépe előtt ülő felhasználó, és mit a rendszergazda, akinek a bevezetéstől kezdve ezzel az újabb technológiával is nap mint nap birkóznia kell?

Nos, a felhasználó azt fogja tapasztalni, hogy a korábbinál sokkal ritkábban látja a rendszergazdát, a gépe „magától” tud mindent, a munkakörnyezete szépen észrevétlenül, de folyamatosan alkalmazkodik az igényeihez. Ha új programot kell használnia, akkor az feltelepül a gépére, az Asztalán pedig megjelennek az új parancsikonok. Ha új gépet kap, vagy átmenetileg át kell ülnie egy kolléga gépéhez, akkor nemcsak, hogy minden további nélkül be tud jelentkezni a megszokott felhasználónevével és jelszavával, de a dokumentumai, parancsikonjai, levelei és nyomtatói is mind a helyükön lesznek.

A felhasználók tehát szabadon (de ellenőrzötten) vándorolhatnak a gépek között, a megszokott környezetük árnyékként követi őket. A rendszergazda viszont majdnem mindent elintézhet a saját szobájában, a saját gépe előtt ülve. Kis túlzással azt mondhatjuk, hogy egy jól felépített tartományi hálózatban a rendszergazda csak akkor látja a felhasználók gépeit, ha csavarhúzót is kell magával vinnie, minden más probléma megoldható távolról is. Sőt, távolról és **csoportosan**, vagyis a különböző beállításokat nem kell egyesével megadni a gépeken, minden művelet a gépek előre definiált csoportjaira vonatkozhat. Így lehetségessé válik az, hogy a biztonsági beállítások és a jogosultságok kiosztása mindenütt egyformán és következetesen érvényesüljön, vagyis felhasználók jogosultságai (saját számítógépükön és a hálózaton is) pontosan megfeleljenek annak az elvnek, hogy mindenki csak annyi jogosultsággal rendelkezzen, amennyire feltétlenül szüksége van egy adott feladat ellátásához.

A címtár tehát megadja a rendszergazda számára azt a lehetőséget, hogy a központilag előírható beállítások és korlátozások révén garantálhassa a rendszer és az egyes gépek folyamatos működőképességét és biztonságát. Ez persze a felhasználók számára bizonyos korlátozásokkal jár, de egy nagyobb hálózat folyamatos működőképességének fenntartása érdekében erre mindenképpen szükség van.

Már tíz számítógép esetében is meglehetősen lehangoló feladat, ha minden egyes gépen létre kell hoznunk egy új felhasználói fiókot. Ha az új felhasználónak még jogokat is kell adnunk a fájlrendszerben, akkor már itt is van a délután öt óra. Másnap pedig elgondolkodunk rajta, hogy talán mégis jó lenne, ha mindenki a *user* felhasználónévvel jelentkezne be valamennyi gépre, a jelszót pedig esetleg kitehetnénk a faliújságra…

Active Directory környezetben nincsen szükség arra, hogy az új felhasználói fiókot vagy csoportot minden egyes gépen külön létrehozzuk, a címtár által tárolt egyetlen felhasználói fiók tulajdonosa valamennyi (a tartományhoz tartozó) számítógépen bejelentkezhet, a csoportok pedig jogosultságokat kaphatnak a hálózati és a helyi erőforrások eléréséhez is, és változás esetén is csak ezt az egy objektumot kell módosítanunk – értelemszerűen – egyetlen helyen.

Másrészt, amiből várhatóan sok van egy hálózatban (számítógépek, nyomtatók, felhasználói profilok stb.), azt a csoportházirend segítségével egyszerre érhetjük el, tulajdonságaik, beállításaik egyetlen mozdulattal módosíthatók.

Az Active Directory tehát az alábbi szolgáltatásokat nyújtja hálózatunk mindennapi üzemeltetéséhez:

- Biztosítja a szervezet működéséhez szükséges objektumok és a hálózat publikált erőforrásainak (felhasználói fiókok, csoportok, erőforrás-objektumok, jogosultságok, fájlok és megosztások, perifériák, gép kapcsolatok, adatbázisok, szolgáltatások stb.) egy helyen történő nyilvántartási lehetőségét.
- Az Active Directory a hálózat objektumait egységes és jól kereshető formátumban tárolja, így azok könnyen elérhetőek mind a felhasználók, mind pedig a rendszergazdák számára.
- Lehetővé teszi a fent említett hálózati erőforrások kezelését, létrehozását, törlését, tulajdonságaik beállítását.
- Lehetővé teszi a centralizált, vagy éppen a decentralizált felügyeletet és az engedélyek delegálását.
- Csökkenti, optimalizálja a hálózati forgalmat, és számos különböző erőforráshoz (megosztott mappák, nyomtatók, levelezés stb.) egyetlen felhasználónév, jelszó megadásával biztosít hozzáférést (*Single Sign On, SSO)*.
- A felügyeleti rendszer alapját képező, rendkívül összetett lehetőségekkel rendelkező csoportházirend megoldás megkönnyíti a legbonyolultabb hálózat felügyeletét is.
- Az Active Directory-címtárnak igen fontos szerepe van más technológiák használatával kapcsolatban is, többek között nincs nélküle Exchange, és jelentős szerepet kap például az RRAS, az ISA Server, a Certificate Services és még sok más kiszolgáló komponens életében is.

Az Active Directory alapjául egy JET (Joint Engine Technology) adatbázismotort felhasználó ESE (Extensible Storage Engine) adatbázis számos új tulajdonsággal és képességgel kiegészített változata szolgál. Az adatbázisban egyszerűen megtalálhatók elérhetők és „elolvashatók" a tárolt adatok, és az Active Directory hierarchia és hozzáférési modellje segítségével igen részletesen szabályozható az egyes elemekhez, vagyis a hálózat erőforrásaihoz való hozzáférés. Természetesen a hálózat elemei alatt itt nemcsak a tartományvezérlőkön, vagy kiszolgáló számítógépeken, hanem magukon az ügyfélgépeken elérhető erőforrásokat is értjük, a hozzáférési jogok szabályozása ezekre is kiterjedhet.

Az Active Directory szorosan integrálódik a Windows-rendszerek biztonsági modelljébe, a felhasználóazonosítással és hozzáférés-vezérléssel kapcsolatos feladatok legnagyobb részét átveszi az ügyfélgépektől. Ugyancsak az Active Directory végzi a felhasználók azonosítását számos kiszolgáló-alkalmazás esetében is, például az SQL Server, az Exchange és az IIS is az Active Directory segítségével tartja nyilván a felhasználókat, azok tulajdonságait és jogosultságait.

Az Active Directory beépített biztonsági szolgáltatása két alapvető részből áll: elvégzi a bejelentkezési azonosítást (ezzel összefüggésben tárolja és védi az azonosítókat), illetve szabályozza az egyes objektumokhoz való hozzáférést. Az üzemeltetők egyetlen bejelentkezéssel kezelhetik a címtár adatait a teljes hálózaton, a megfelelően hitelesített felhasználók pedig a hálózat bármelyik pontjából hozzáférhetnek az engedélyezett erőforrásokhoz.

Az Active Directory-címtárszolgáltatás alapjai

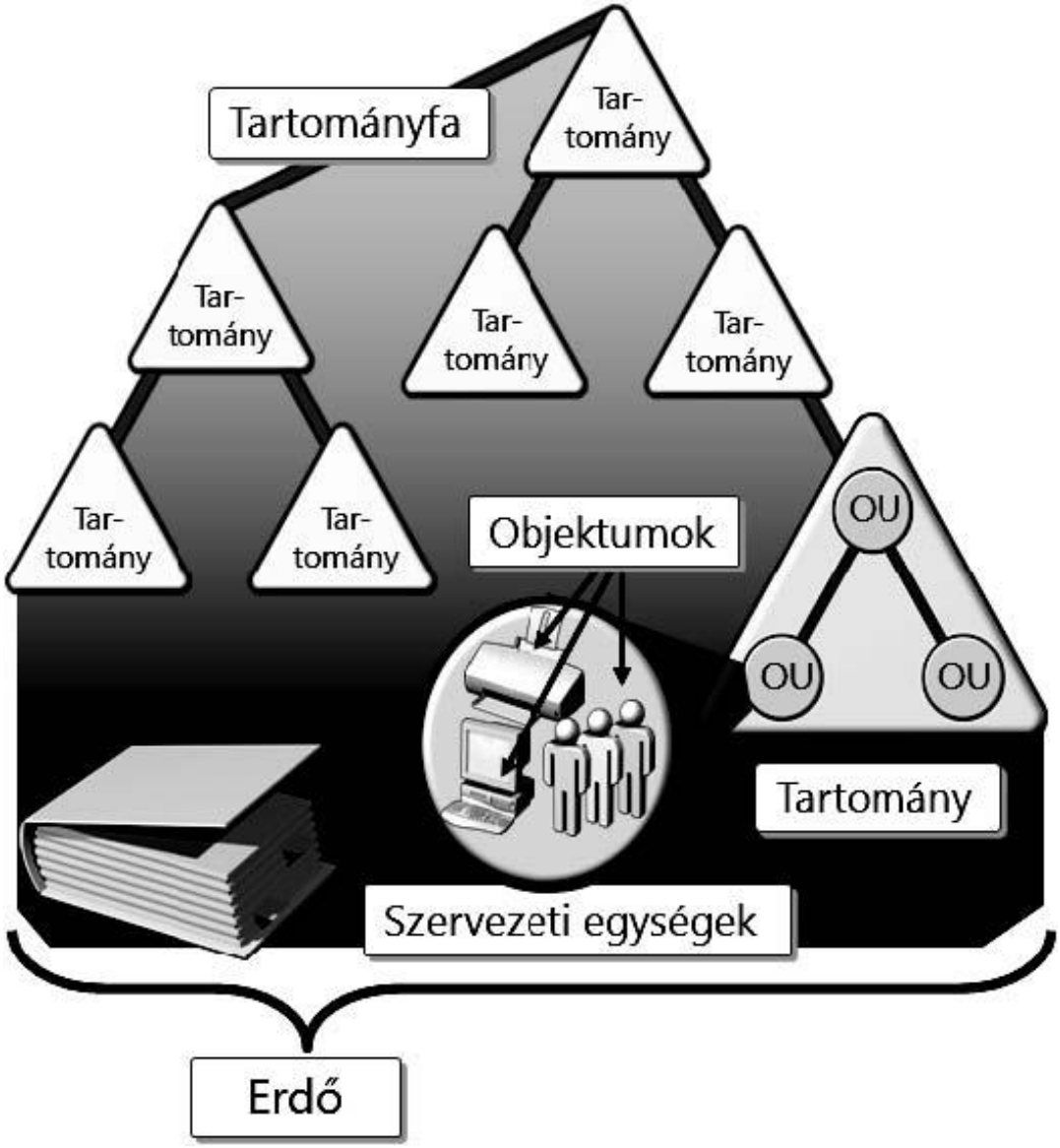
Természetesen ahhoz, hogy kiaknázhassuk az Active Directoryban rejlő lehetőségeket, először be is kell fektetnünk (nemcsak anyagi értelemben), vagyis meg kell szereznünk a hatékony használathoz és üzemeltetéshez nélkülözhetetlen tudást. Minél mélyebben ismeri a rendszergazda az általa üzemeltetett rendszert, annál kevesebbet kell dolgoznia, az ismétlődő rutinfeladatok automatizálása a megfelelő technológia és a megfelelő ismeretek birtokában nem jelenthet problémát. A következőkben az Active Directory üzemeltetéséhez szükséges alapismereteket fogjuk áttekinteni, megismerkedünk a címtár alkotórészeivel, és a felügyeletéhez szükséges legfontosabb eszközökkel.

Az Active Directory a korábban létező meglehetősen egyedi megoldással ellentétben, teljes mértékben a bevált iparági szabványokon alapul. (A Windows NT „címtár" jellegű adatai a registryben tárolódtak.) Az Active Directory alapjául az X.500 szabvány szolgál, hozzáférési protokollja pedig a széles körben használt LDAPv3 (Lightweight Directory Access Protocol). Az Active Directory felépítése rendkívüli rugalmasságot és skálázhatóságot tesz lehetővé; képes alkalmazkodni az öt számítógépet használó kisvállalatok, és a több kontinensen elhelyezkedő, kiszolgálók százait vagy ezreit tartalmazó hálózatok igényeihez is. Az AD által tárolható objektumokat és azok tulajdonságait a hierarchikus és kiterjeszthető, módosítható névtér, a séma határozza meg, így könnyedén képes a speciális igények kiszolgálására is. Az Active Directory-adatbázis több, egymással automatikusan szinkronizálódó példányát a tartományvezérlők *(Domain Controller, DC)* tárolják. Az elosztott tárolás ellenére – az objektumok módosításainak nyilvántartásán alapuló multimaster *(több főkiszolgálós)* replikáció miatt – minden adatbázispéldány teljesen egyenértékű, a szükséges módosítások bármelyik tartományvezérlőn elvégezhetők.

Az Active Directory alkotóelemei

Az Active Directory névtér az alábbi elemekből épül fel:

• **Erdő** *(Forest)* – A legmagasabb szintű Active Directory tároló neve erdő. Az erdő közös sémát és globális katalógust használ, egy vagy több tartományt foglal magába. Az erdő első tartományát az erdő gyökértartományának hívják.



5.1. ábra: *Az Active Directory hierarchikus felépítése*

- **Fa** *(Tree)* – Ha az erdő több tartománya összefüggő DNS-tartománynéveket használ, vagyis egymás gyermek, illetve szülőtartományai, akkor a struktúrát tartományfának nevezzük.
- **Tartomány** *(Domain)* – A tartomány az Active Directory 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. Egy adott tartomány minden tartományvezérlője fogad módosításokat, és azokat a tartomány többi tartományvezérlőjére replikálja. Az Active Directory-címtárban minden tartományt egy-egy DNS-tartománynév azonosít, és minden tartomány legalább egy tartományvezérlőt tesz szükségessé.
- **Szervezeti egység** *(Organizational Unit, OU)* – A szervezeti egységek az Active Directory-objektumtárolói, amelyekbe felhasználók, csoportok, számítógép-objektumok, illetve más szervezeti egységek helyezhetők. A szervezeti egységek rendkívül fontos szerepet játszanak a csoportházirend érvényesítésével és a felügyeleti jogok delegálásával kapcsolatban is. A szervezeti egységek használatával a tartományon belüli hierarchia pontosan megfelelhet az adott szervezet hierarchikus felépítésének.

Bár az átlagos magyarországi vállalatok méretei miatt csak viszonylag ritkán lehet szükség egynél több tartományból álló hálózat létrehozására, a fenti fogalmak ismeretét mégsem kerülhetjük el, mivel egyetlen tartományunk is minden esetben a tartományfa része, az egyetlen fa pedig biztosan egy erdőhöz tartozik. Ebből következik, hogy bár mindennapi feladataink során többnyire csak szervezeti egységekkel és az egyetlen tartománnyal találkozunk, például az Active Directory-szolgáltatás telepítésekor mindenképpen válaszolnunk kell az erdőre és a tartományfára vonatkozó kérdésekre is.

A multimaster (több főkiszolgálós) replikáció

Az Active Directory a multimaster replikációs modellt alkalmazza a címtáradatok tartományvezérlők közötti szinkronizációjához. Ez azt jelenti, hogy a tartományvezérlők mindegyike tartalmazza a teljes címtáradatbázist, és az mindegyik tartományvezérlőn módosítható is. Hogy a címtárpéldányok (replikák) mindegyike folyamatosan a helyes adatokat tartalmazhassa, szükség van a tartományvezérlők közötti folyamatos, és lehetőleg minél kevesebb erőforrást felhasználó szinkronizációra. Ezt a folyamatot nevezzük replikációnak. Ha a replikáció megfelelően működik, akkor a címtárpéldányok a több ponton való módosítás ellenére is folyamatosan megtartják a többi példánnyal megegyező, konzisztens állapotukat.

A több ponton való módosítás általában nem okoz problémát, mert a módosítások többnyire függetlenek egymástól, így a replikáció során könnyen „összefésülhetőek" az adatbázisok. De mi történik, ha két különböző helyen egyszerre módosítunk egy objektumot, például egy felhasználói fiókot? Nos, ebben az esetben sem történik semmi különös, mivel a replikáció alapegysége nem a teljes objektum, hanem az objektumok egyes tulajdonságai, vagyis az adatbázis egyesítése nem az objektumok, hanem azok tulajdonságainak szintjén történik. Ritkábban ugyan, de az is előfordulhat, hogy a módosítások nem egyesíthetők konfliktus nélkül, ütközés esetén a replikáció a későbbi módosítást tekinti érvényesnek.

A multimaster replikáció úgynevezett laza konzisztenciát tart fenn a címtáron belül, ami azt jelenti, hogy az egyes példányok bármikor tartalmazhatnak ugyan ideiglenes, a teljesen konzisztens állapotnak nem megfelelő adatot, de a konfliktusok a replikáció során előbb-utóbb valamilyen módon biztosan feloldódnak.

Címtárpartíciók

A partíció az Active Directory egy összefüggő részfája, amely egy egységként replikálódik az erdő más, ugyanennek a részfának egy-egy replikáját magukban foglaló tartományvezérlői számára. Az Active Directoryban minden tartományvezérlő egyenként legalább a következő három címtárpartícióval rendelkezik:

5.2. ábra: *Az Active Directory-címtáradatbázis négy különálló partícióra oszlik*

- **Séma partíció** *(Schema Partition)* – A séma partíció az osztály- és attribútum-definíciókat, vagyis az objektumok és tulajdonságok formális leírását tárolja. A partíció minden tartományvezérlőn és minden globális katalógusban megtalálható. Az Active Directory séma az egész erdőre vonatkozóan megegyezik.

- **Konfigurációs partíció** *(Configuration Partition)* – Ez a partíció a címtár topológiájára vonatkozó adatokat tárolja. Megtalálhatók benne a tartományokra, a fákra és az erdőre vonatkozó információk, valamint itt tárolódik a replikációs topológia, és az ehhez kapcsolódó metaadatok is. A konfigurációs adatok az egész erdőre vonatkoznak, és megtalálhatók az erdő valamennyi tartományvezérlőjén.

- **Tartomány partíció** *(Domain Partition)* – itt találhatjuk meg a felhasználókra, számítógépekre, csoportokra és egyéb tartomány szintű objektumokra vonatkozó adatokat. A partíció az adott tartomány minden tartományvezérlőjén megtalálható.

- **Alkalmazás partíció** *(Application Partition)* – a Windows Server rendszert futtató tartományvezérlők a fentieken kívül egy vagy több alkalmazás-címtári partíciót is tárolhatnak.

Az egyedi főkiszolgáló-műveletek (FSMO)

A Windows Server tartományvezérlői funkcióinak legnagyobb részét elosztottan valósították meg, ezek a funkciók az összes tartományvezérlőn elérhetők és használhatók. Öt funkció azonban továbbra is csak a tartomány, illetve a teljes erdő egyetlen kiszolgálójához kapcsolható, mivel ezek elosztott megvalósítása nem lehetséges. Az egyes szerepköröket önálló kiszolgálókon is elhelyezhetjük, de akár egyetlen tartományvezérlő is megvalósíthatja valamennyit.

Az öt úgynevezett egyedi főkiszolgáló-művelet (Flexibile Single Master Operations, FSMO) a következő:

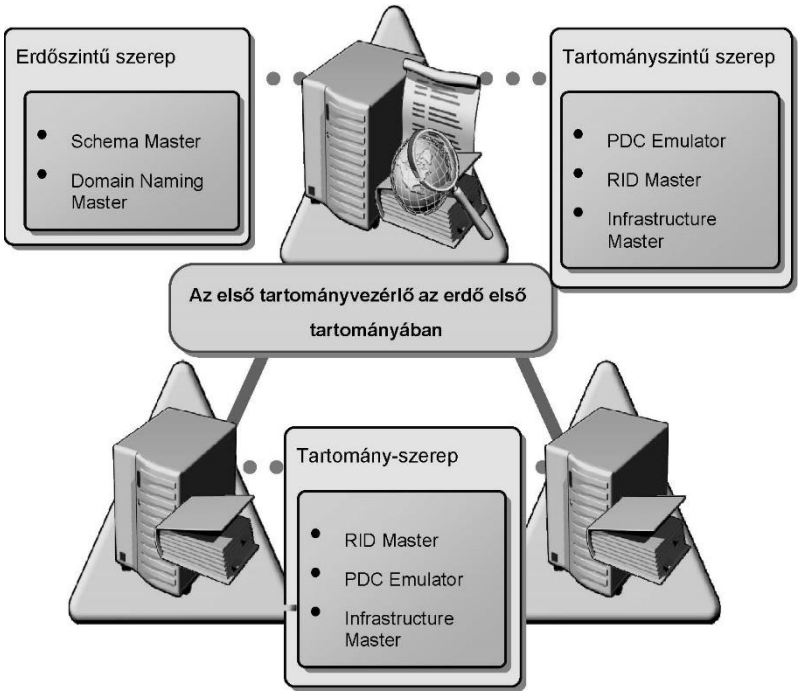
- **RID-főkiszolgáló** *(RID Master)* – Tartományszintű műveleti főkiszolgáló szerepkör, vagyis minden tartományban legfeljebb egy lehet belőle. A szerepkörrel felvértezett tartományvezérlő képes arra, hogy a saját, vagy valamelyik másik tartományvezérlő kérésére egy létrehozandó új objektum (felhasználói 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 rendszer éppen úgy működik, mint a vonalkódok, hálózati kártyacímek (MAC-address), vagy egyéb egyedi sorszámozású termékek kiadása: az ütközések elkerülése érdekében a sorszámokat egy központ bocsátja ki. 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)* – Tartományszintű műveleti főkiszolgáló szerepkör, 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)* – Szintén tartományszintű műveleti főkiszolgáló szerepkör, amelyből szintén egy lehet a tartományon belül, de 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)* – Erdőszintű műveleti-főkiszolgáló szerepkör, amelyből az erdőben kizárólag egy lehet. A speciális szereppel bíró tartományvezérlő 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)* – Erdőszintű műveleti-főkiszolgáló szerepkör, központosítva végzi el a séma összes frissítését és módosítását. Amennyiben az erdő sémáját frissíteni kívánjuk, hozzáférési joggal kell rendelkeznünk a séma-főkiszolgálóhoz. Az előző szerephez hasonlóan séma-főkiszolgálóból is csak egy lehet az erdőben, és szintén nem vesszük észre a hiányát, egészen addig, amíg nem kerül sor a séma frissítésére, vagy bővítésére.



5.3. ábra: *Az erdő első tartományvezérlője kapja az erdő szintű, az egyes tartományok első tartományvezérlői pedig a tartományszintű szerepeket*

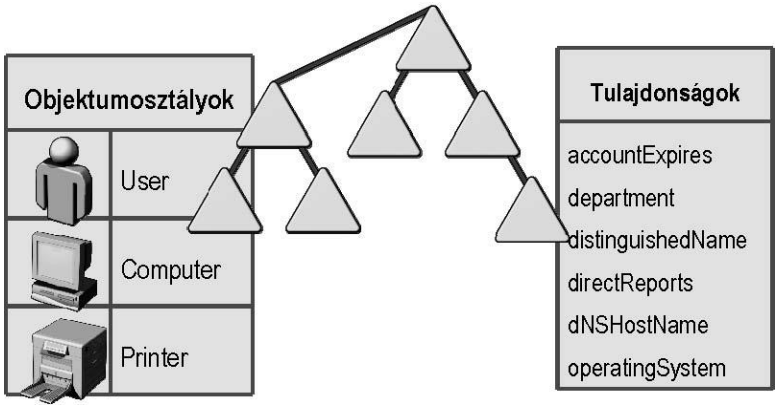
Az erdő első tartományvezérlőjének (ez egyben az elsőként létrehozott tartomány első tartományvezérlője is) telepítésekor valamennyi erdő és tartomány szintű szerepkör erre a kiszolgálóra kerül, de később – ha már több tartományvezérlőnk is van –, az egyes szerepeket tetszés szerint bárhová áthelyezhetjük. Ha egy adott szerepkört megvalósító tartományvezérlőt lefokozunk, illetve eltávolítunk a tartományból, akkor az adott szerepkör áthelyezéséről (lehetőleg még akkor, amikor a régi kiszolgáló is elérhető) mindenképpen gondoskodnunk kell.

A tartományszintű szerepkörök (RID Master, PDC Emulator, Infrastructure Master) áthelyezésére az Active Directory Users and Computers *(Active Directory – felhasználók és számítógépek)* konzol használható, a Domain Naming Master szerepkört az Active Directory Domains and Trusts *(Active Directory – tartományok és bizalmi kapcsolatok)*, a Schema Master szerepet pedig az Active Directory Schema *(Active Directory Séma)* MMC-modul használatával adhatjuk át másik tartományvezérlőnek.

A séma

A séma az Active Directory-adatbázis szerkezete, vagyis a címtárban tárolható objektumok definícióinak összessége. A séma minden egyes objektumosztály számára meghatározza a kötelező és lehetséges attribútumok körét, valamint a szülőként megadható objektumosztályokat. Az alapséma (vagy alapértelmezett séma) rengeteg objektumosztályt és attribútumot tartalmaz, így a legtöbb esetben nincs szükség ennek módosítására. Számtalan különböző adatot tartalmazhat például minden egyes felhasználó objektum, a működéssel kapcsolatos beállítások mellett (pl. login szkript, csoporttagság, dial-up engedélyek stb.) informális adatok tucatjait is tárolhatjuk (cím, telefonszám, iroda, ország, cég adatai stb.).

Ha azonban olyan adatokat is tárolni szeretnénk a címtárban, ami nem fér bele az alapsémába, akkor lehetőség van a meglévő osztályok és attribútumok módosítására, illetve újak hozzáadására is. Alaposan meg kell azonban fontolnunk minden módosítást, mert a megváltozott séma késlekedés nélkül replikálódik az erdő valamennyi tartományvezérlőjére, vagyis a művelet minden esetben a teljes hálózatot érinti. Ráadásul a módosítások visszavonására egyáltalán nincs lehetőség, a sémából semmi nem törölhető (csak a deaktiválás lehetséges), hiszen a séma alapján létrehozott objektumokban élő hivatkozások lehetnek a törölni kívánt elemekre.



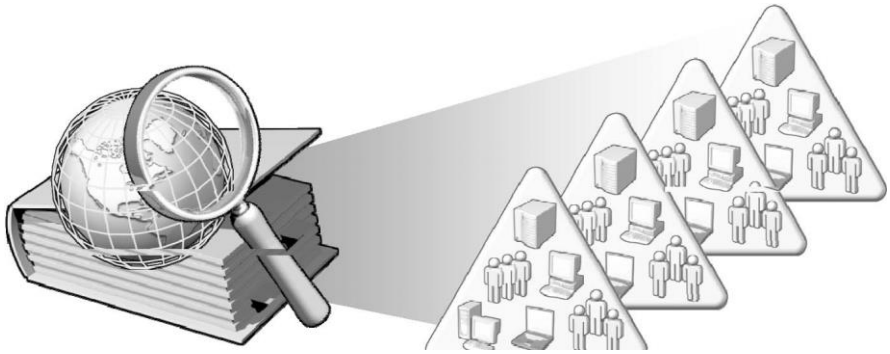
5.4. ábra: *A létrehozható objektumokat, és azok szerkezetét a séma definiálja*

Jelentős sémabővítést hajt végre például az Exchange Server telepítője, mivel az Exchange a felhasználók nyilvántartásával és azonosításával kapcsolatos feladatait teljes egészében az Active Directoryra bízza.

Minden létrehozott címtárobjektum a sémában tárolt objektumosztály egy példánya. Az objektumosztályok tartalmazzák a hozzájuk tartozó attribútumok listáját, ami meghatározza az objektumokban tárolható adatokat. Az osztályok és attribútumok egymástól függetlenek, ezért egy attribútum több osztályhoz is társítható.

A globális katalógus szerepkör

A globális katalógus *(Global Catalog, GC)* olyan tartományvezérlői szerep, amelynek hordozója a címtár összes objektumának alapadataival, elérhetőségeiknek információjával rendelkezik a teljes erdőre vonatkozóan, vagyis minden objektumról tud „valamit”. A saját tartományából teljes, a további, szorosan kapcsolódó tartományokból részleges objektummásolatokat tartalmaz, így a globális katalógus 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 (több tartományvezérlő esetén célszerű, ha legalább két globális katalógus is van a hálózatban), illetve máshová helyezhetjük az automatikusan létrehozott globális katalógust is.



Globális katalógus

5.5. ábra: *A globális katalógus az erdő összes tartományának valamennyi objektumáról tud valamit*

A globális katalógusban lévő részleges másolatok azokat az attribútumokat tartalmazzák, amelyek gyakran előfordulnak a felhasználói keresésekben. A globális katalógusba bekerülő attribútumok körét a séma határozza meg, a kiválasztottak meg vannak jelölve az objektumosztályban. A globális katalógusban történő objektumtárolás segítségével a felhasználók gyorsan és hatékonyan tudnak keresni a címtárban anélkül, hogy a tartományvezérlők közötti kommunikáció terhelné a hálózatot.

A működési (funkcionalitási) szintek

A tartományok és erdők Windows Server Active Directoryban bevezetett működési szintjeinek segítségével engedélyezhetők bizonyos tartományi és erdőszintű Active Directory szolgáltatások. A hálózati környezettől függően másféle beállítások állnak rendelkezésre a tartományok és az erdők különböző működési szintjein. A működési szint egyrészt meghatározza a tartományban, illetve erdőben elérhető szolgáltatások körét, másrészt a működési szint emelésével régebbi tartományvezérlők már nem adhatók a tartományhoz.

A tartományok működési szintjei a teljes tartományban, és csakis az adott tartományban elérhető szolgáltatásokat befolyásolják.

Az alábbi táblázat a tartományi működési szinteket és az azokhoz használható tartományvezérlőket sorolja fel.

Tartomány működési szintje (Windows 2012 r2 esetén)

Támogatott tartományvezérlők:

Windows 2003

Windows 2008

Windows 2008 r2

Windows Server 2012

A működési szint előléptetését követően *a korábbi operációs rendszereket futtató tartományvezérlőket nem lehet a tartományba beléptetni*. Ha például a tartomány működési szintjét előléptetjük a Windows Server 2012 szintre, Windows 2008 Servert futtató kiszolgálókat tartományvezérlőként már nem lehet hozzáadni a tartományhoz. Természetesen továbbra is beléptethető a tartományba a Windows 2008 Server, bármiféle funkciót elláthat, csak tartományvezérlő nem lehet többé.

Az erdők működési szintjének beállításával az erdő összes tartományán engedélyezhetők szolgáltatások. Az erdőkhöz négy működési szint áll rendelkezésre: Windows 2003, Windows Server 2008 és Windows Server 2012. Alapértelmezés szerint az erdők Windows 2003 szinten működnek, és ezt Windows Server 2012 szintre lehet előléptetni.

Az alábbi táblázat az erdők egyes működési szintjeit és az azokhoz használható tartományvezérlőket sorolja fel.

Erdő működési szintje	Támogatott tartományvezérlők
Windows 2003	Windows 2003, Windows 2008 termékcsalád, Windows 2012 termékcsalád
Windows Server 2008	Windows Server 2008 termékcsalád, Windows 2012 termékcsalád
Windows Server 2012	Windows Server 2003 család

Az erdő működési szintjének előléptetését követően, a korábbi operációs rendszereket futtató számítógépeket tartományvezérlőként nem lehet az erdőbe beléptetni. Ha például az erdő működési szintjét előléptetjük a Windows Server 2012 szintre, Windows 2008 Server rendszert futtató ***tartományvezérlőket*** már nem lehet hozzáadni az erdőhöz.

A működési szint emelése több előnnyel is jár, például így tehetjük lehetővé bizonyos erdő- vagy tartományszintű új szolgáltatások, megoldások használatát (univerzális csoportok stb.), és az R2 bizonyos szolgáltatásai is csak magasabb működési szinteken használhatók.

Fizikai tárolás

Bár szerencsére nehezen képzelhető el olyan helyzet, amikor az Active Directoryt tároló fájlokkal közvetlen kapcsolatba kell kerülnünk, nem árthat, ha mégis megismerkedünk az egyes fájlok funkcióival és az általuk tárolt adatok jellegével.

Valamennyi fájl a *%systemroot%**NTDS*-mappában található.

- **Ntds.dit** – a legfontosabb fájl az ntds.dit, ami magát az Active Directory-adatbázist tárolja. A dit kiterjesztés a „directory information tree" kifejezésre utal.
- **Edb.log** – a fájlban a tranzakciónapló található, amelynek tartalma azonnal követi a címtár minden változását. A változások aztán később, a megfelelő pillanatban átkerülnek végleges helyükre, az ntds.dit-be. A fájl maximális mérete 10 MB.
- **Edbxxxxx.log** – ezek a fájlok akkor jönnek létre, ha az Edb.log túllépi az említett 10 MB-os mérethatárt. Ebben az esetben az aktív tranzakciónapló ebbe a fájlba költözik. A 10 MB méretkorlát természetesen ezekre az állományokra is érvényes.
- **Edb.chk** – a fájl a címtárba még be nem került adatok „helyzetének" jelzője.
- **Res1.log és Res2.log** – ezek a fájlok semmiféle hasznos adatot nem tartalmaznak, egyszerűen kétszer 10 MB helyet foglalnak a később esetleg létrejövő tranzakciónapló-állományok számára.
- **Temp.edb** – a fájl, amint a nevéből is látszik, ideiglenes adatokat tárola tranzakciókról. Átmenetileg ide kerülnek az ntds.dit tömörítése közben eltárolandó adatok is.

A SYSVOL-mappa

A címtárszolgáltatás fontos eleme a valamennyi tartományvezérlőn megtalálható SYSVOL nevű megosztott mappa. A mappa tartalmazza azokat az elemeket (fájlokat), amelyek az Active Directory-szolgáltatásokhoz kapcsolódnak ugyan, de mégsem tárolhatók a címtáradatbázisban. Itt találhatjuk meg azokat a fájlokat, amelyeket az ügyfélrendszerek indítás, illetve bejelentkezés közben letöltenek a tartományvezérlőről, itt tárolódnak például a csoportházirend fájlok és sablonok (Policies mappa), valamint a bejelentkezési szkriptek (a scripts mappában, ami a NETLOGON megosztáson keresztül érhető el az ügyfelek számára) stb. A megosztott mappa létrehozását és az engedélyek beállítását az Active Directory telepítőprogramja automatikusan elvégzi. A SYSVOL-mappa tartalmát a File Replication Service (FRS) komponens rendszeresen szinkronizálja a tartományvezérlők között, így bármelyik tartományvezérlőn is végezzük el a szükséges módosításokat, a megfelelő fájlok rövid időn belül a többi példányban is megjelennek.